Release Notes for the Cisco Catalyst Blade Switch 3020 for HP, Cisco IOS Release 12.2(58)SE and Later

Revised April 23, 2011

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

Note If you are using Enclosure Bay IP Addressing (EBIPA), you must upgrade the HP Onboard Administrator (OA) to firmware version 3.55 *before* you upgrade to Cisco IOS Release 12.2(58)SE or later. If you do not upgrade the firmware, the HP OA will fail to assign an IP address to the Cisco Catalyst Blade Switch 3020 module.

Cisco IOS Release 12.2(58)SE1 runs on the Cisco Catalyst Blade Switch 3020 for HP, referred to as the *switch*.

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.

These release notes include important information about Cisco IOS Release 12.2(58)SE1 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 21.

You can download the switch software from this site (registered Cisco.com users with a login password):

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

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

Contents

System Requirements

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

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.122-58.se1.tar	Cisco Catalyst Blade Switch 3020 for HP image file and device manager files. This image has Layer 2+ features.
cbs30x0-ipbasek9-tar.122-58.se1.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 4 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

- Protocol storm protection to control the rate of incoming protocol traffic to a switch by dropping packets that exceed a specified ingress rate.
- VACL Logging to generate syslog messages for ACL denied IP packets.
- Call Home to provide e-mail-based and web-based notification of critical system events. Users with a service contract directly with Cisco Systems can register Call Home devices for the Cisco Smart Call Home service that generates automatic service requests with the Cisco TAC.
- IETF IP-MIB and IP-FORWARD-MIB(RFC4292 and RFC4293) updates to support the IP version 6 (IPv6)-only and the IPv6 part of the protocol-version independent (PVI) objects and tables.
- Network Time Protocol version 4 (NTPv4) to support both IPv4 and IPv6 and compatibility with NTPv3.
- DHCPv6 bulk-lease query to support new bulk lease query type (as defined in RFC5460).
- The DHCPv6 relay source configuration feature to configure a source address for DHCPv6 relay agent.
- Enhancements to RADIUS, TACACS+, and SSH to function over IPv6.
- Support for the Virtual Router Redundancy Protocol (VRRP for IPv4), which dynamically assigns responsibility for one or more virtual routers to the VRRP routers on a LAN, allowing multiple routers on a multiaccess link to utilize the same virtual IP address.

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

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

- 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.

Open Caveats

- CSCtg98453

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

  There is no workaround.

- CSCtl32991

  Unicast EIGRP packets destined for the switch are sent to the host queue instead of to the higher priority routing protocol queue.

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

  There is no workaround.

- CSCtl60247

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

  There is no workaround.

- CSCtl81217

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

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

  ip rip authentication mode

  ip rip key-chain

- CSCtq01926

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

  The workaround is to configure static VLANs for these ports.

Resolved Caveats

- CSCtg00542

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

  The workaround is to disable NetFlow sampling.

- CSCtg11547

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

  The workaround is to remove the VRF configuration.

- CSCtg71149

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

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

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

- CSCth44403

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

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

- CSCti27620

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

  There is no workaround.

- CSCti37197

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

Note Tunnels are not supported on these platforms.

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

- CSCti61145

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

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

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

- CSCti69845

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

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

- CSCti78365

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

  There is no workaround.

- CSCti95834

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

  There is no workaround.

- CSCtj03875

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

  There is no workaround.

- CSCtj75471

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

  There is no workaround.

- CSCtj83964

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

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

- CSCtj88307

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

  There is no workaround.

- CSCtk11275

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

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

- CSCtk13113

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

  There is no workaround.

- CSCtl42740

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

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

  There is no workaround.

- CSCtl51859

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

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

- CSCtl80678

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

  – Link comes up simultaneously on multiple dot1q trunk ports.

  – VLAN Trunking Protocol (VTP) pruning is enabled.

  The workaround is to disable VTP pruning.

- CSCto62631

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

  – SSH version 2 is configured on the switch, and

  – a customized login banner was configured by using the **banner login** *message* global configuration command

  Use one of these workarounds:

  – Disable the login banner by entering the **no login banner** command.

  – Disable SSH on the switch.

  – Downgrade to a software version prior to Cisco IOS Release 12.2(58)SE.

Documentation Updates

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

Updates to the Software Configuration Guide

Correction to the "Unsupported Commands" Chapter

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

Updates to the System Message Guide

New System Messages

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

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

Recommended Action No action is required.

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

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

Recommended Action No action is required.

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

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

Recommended Action No action is required.

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

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

Recommended Action No action is required.

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

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

Recommended Action No action is required.

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

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

Recommended Action No action is required.

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

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

Recommended Action No action is required.

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

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

Recommended Action No action is required.

Modified System Messages

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

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

Recommended Action No action is required.

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

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

Recommended Action No action is required.

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

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

Recommended Action No action is required.

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

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

Recommended Action No action is required.

Deleted System Messages

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

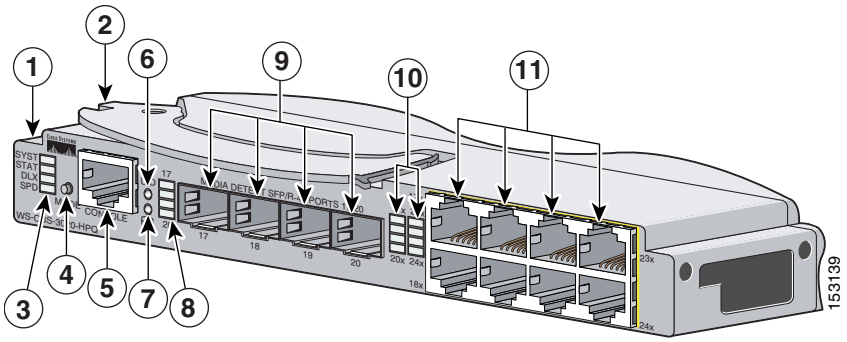
Explanation Multiple stations are configured with the same IP address in a private VLAN. (This could be a case of IP address theft.) [inet] is the IP address that is configured, the first [enet] is the original MAC address associated with the IP address, and the second [enet] is the MAC address that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

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

Updates to the Getting Started Guide

This illustration in the *Cisco Catalyst Blade Switch 3020 for HP Getting Started Guide* has been updated:

Figure 1 The Catalyst Blade Switch 3020 for HP



1	Switch module	**7**	Health LED
2	Release latch	**8**	SFP module port LEDs for ports 17 to 20
3	System status LEDs	**9**	SFP module ports 17 to 20
4	Mode button	**10**	Gigabit Ethernet ports LEDs for ports 17x to 24x
5	Console port	**11**	Gigabit Ethernet ports 17x to 24x
6	UID[1] LED		

1. UID: unit identifier.

This information in the *Cisco Catalyst Blade Switch 3020 for HP Getting Started Guide* has been updated:

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

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

---