Release Notes for the Cisco Catalyst Blade Switch 3130 for Dell and Cisco Catalyst Blade Switch 3032 for Dell, Cisco IOS Release 12.2(40)EX1

Cisco IOS Release 12.2(40)EX1 runs on the Cisco Catalyst Blade Switch 3130 for Dell and Cisco Catalyst Blade Switch 3032 for Dell switches. These switches support stacking through Cisco StackWise Plus technology. Unless otherwise noted, the term *switch* refers to a standalone switch and to a switch stack.

These release notes include important information about Cisco IOS Release 12.2(40)EX1 and any limitations, restrictions, and caveats that apply to it. Verify that these release notes are correct for your switch:

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

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

http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=268438038

This software release is part of a special release of Cisco IOS software that is not released on the same 8-week maintenance cycle that is used for other platforms. As maintenance releases and future software releases become available, they will be posted to Cisco.com in the Cisco IOS software area.

For the complete list of the Cisco Catalyst Blade Switch 3130 for Dell and 3032 for Dell documentation, see the "Related Documentation" section on page 21.

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

Contents

These sections provide information about this release:

- "System Requirements" section on page 2
- "Upgrading the Switch Software" section on page 4
- "Installation Notes" section on page 7
- "Minimum Cisco IOS Release for Major Features" section on page 7
- "Limitations and Restrictions" section on page 8
- "Important Notes" section on page 15
- "Open Caveats" section on page 17
- "Documentation Updates" section on page 21
- "Related Documentation" section on page 21
- "Obtaining Documentation and Submitting a Service Request" section on page 22

System Requirements

The system requirements are described in these sections:

- "Hardware Supported" section on page 2
- "Device Manager System Requirements" section on page 3
- "Cisco Network Assistant Compatibility" section on page 4

Hardware Supported

Table 1 lists the hardware supported on this release.

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

Switch Hardware	Description	Supported by Minimum Cisco IOS Release
CBS3032G[1], CBS3130G-S, and CBS3130X-S	• 16 internal Gigabit Ethernet 1000BASE-X downlink ports that connect to the 16 blade servers in the Dell chassis • 4 Gigabit Ethernet (RJ-45) uplink ports • 4 SFP module slots/2 10-Gigabit Ethernet X2 module slots[2] • 1 Ethernet management port (Fa0) used only for switch module management traffic	Cisco IOS Release 12.2(40)EX1
Cisco X2 transceiver modules (supported only on the CBS3130X-S model)	X2-10GB-SR V02 or later X2-10GB-CX4 V03 or later X2-10GB-LRM V03 or later	Cisco IOS Release 12.2(40)EX1

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

Switch Hardware	Description	Supported by Minimum Cisco IOS Release
Cisco TwinGig Converter Module	Dual SFP[3] X2 converter module to allow the switch to support SFP Gigabit Ethernet modules	Cisco IOS Release 12.2(40)EX1
SFP modules	1000BASE-LX/LH 1000BASE-SX 1000BASE-T	Cisco IOS Release 12.2(40)EX1

1. This switch supports only the IP base software image.
2. X2 supported only on the CBS3130X-S model.
3. SFP = small form-factor pluggable.

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

Device Manager System Requirements

These sections describe the hardware and software requirements for using the device manager:

- "Hardware Requirements" section on page 3
- "Software Requirements" section on page 3

Hardware Requirements

Table 2 lists the minimum hardware requirements for running the device manager.

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

Table 3 lists the supported operating systems and browsers for using the device manager. The device manager verifies the browser version when starting a session to ensure that the browser is supported.

Table 3 Supported Operating Systems and Browsers

Operating System	Minimum Service Pack or Patch	Microsoft Internet Explorer[1]	Mozilla FireFox
Windows 2000	None	6.0 or 7.0	1.5 or 2.0
Windows XP	None	6.0 or 7.0	1.5 or 2.0

Table 3 Supported Operating Systems and Browsers (continued)

Operating System	Minimum Service Pack or Patch	Microsoft Internet Explorer[1]	Mozilla FireFox
Windows 2003	None	6.0 or 7.0	1.5 or 2.0
Vista	None	6.0 or 7.0	1.5 or 2.0

1. Service Pack 1 or higher is required for Internet Explorer 5.5.

Cisco Network Assistant Compatibility

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

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

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

Upgrading the Switch Software

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

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

Finding the Software Version and Feature Set

The Cisco IOS image is stored as a bin file in a directory that is named with the Cisco IOS release. A subdirectory contains the files needed for web management. The image is stored on the system board flash device (flash:).

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

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

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

Deciding Which Files to Use

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

Table 4 lists the filenames for this software release.

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

Table 4 Cisco IOS Software Image Files

Filename	Description
cbs31x0-universal-tar.122-40.EX1.tar	Cisco Catalyst Blade Switch 3130 for Dell and Cisco Catalyst Blade Switch 3032 for Dell universal image and device manager files. This image has all the supported features that are enabled by the software license installed on the switch.
cbs31x0-universalk9-tar.122-40.EX1.tar	Cisco Catalyst Blade Switch 3130 for Dell and Cisco Catalyst Blade Switch 3032 for Dell universal cryptographic image and device manager files. This image has the Kerberos, SSH, SSL, and SNMPv3 in addition to the features supported in the universal image.

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

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

Archiving Software Images

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

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

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/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/products/sw/iosswrel/ps1835/products_command_reference_book09186a00800811e0.html

Upgrading a Switch by Using the Device Manager or Network Assistant

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

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

Upgrading a Switch by Using the CLI

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

To download software, follow these steps:

Step 1 Use Table 4 on page 5 to identify the file that you want to download.

Step 2 Download the software image file. If you have a SmartNet support contract, go to this URL, and log in to download the appropriate files:

http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=268438038

To download the universal software image files for a Cisco Catalyst Blade Switch 3130 for Dell or a Cisco Catalyst Blade Switch 3032 for Dell, click **Blade Switches > Cisco Catalyst Blade Switch 3000 Series for Dell >**. To obtain authorization and to download the cryptographic software files, click **Cisco Catalyst Blade Switch 3000 Series for Dell Cryptographic Software**.

Step 3 Copy the image to the appropriate TFTP directory on the workstation, and make sure that the TFTP server is properly configured.

For more information, see Appendix B in the software configuration guide for this release.

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

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

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

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

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

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

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

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

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

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

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

```
Switch# archive download-sw /overwrite
tftp://198.30.20.19/cbs31x0-universal-tar.122-40.EX1.tar
```

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

Recovering from a Software Failure

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

Installation Notes

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

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

Minimum Cisco IOS Release for Major Features

Table 5 lists the minimum software release required to support the major features.

Table 5 Features and the Cisco IOS Release Required

Feature	Minimum Cisco IOS Release Required
Automatic quality of service (QoS) Voice over IP (VoIP) enhancement	12.2(40)EX1
Configuration replacement and rollback	12.2(40)EX1
Dynamic voice virtual LAN (VLAN) for multidomain authentication (MDA)	12.2(40)EX1
Internet Group Management Protocol (IGMP) Helper	12.2(40)EX1
IP Service Level Agreements (IP SLAs)	12.2(40)EX1
IP SLAs EOT	12.2(40)EX1

Table 5 Features and the Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required
Multicast virtual routing and forwarding (VRF) Lite	12.2(40)EX1
SSM PIM protocol	12.2(40)EX1
Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6	12.2(40)EX1
Support for VRF-aware services	12.2(40)EX1
Support for the Link Layer Discovery Protocol Media Extensions (LLDP-MED) location TLV	12.2(40)EX1
Support for the CISCO-MAC-NOTIFICATION-MIB	12.2(40)EX1
Support for the CISCO-POWER-ETHERNET-EXT-MIB	12.2(40)EX1
DHCP Snooping Statistics **show** and **clear** commands	12.2(40)EX1
IP phone detection enhancement	12.2(40)EX1
IP unicast reverse path forwarding (unicast RPF)	12.2(40)EX1
Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (LLDP-MED)	12.2(40)EX1
PIM stub routing in the IP base image	12.2(40)EX1
Port security on a PVLAN host	12.2(40)EX1
VLAN aware port security option	12.2(40)EX1
Support for auto-rendezvous point (auto-RP) for IP multicast	12.2(40)EX1
VLAN Flex Link Load Balancing	12.2(40)EX1
Web Cache Communication Protocol (WCCP)	12.2(40)EX1
SNMP support for the Port Error Disable MIB	12.2(40)EX1
Support for the Time Domain Reflectometry MIB	12.2(40)EX1

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.

This section contains these limitations:

- "Cisco IOS Limitations" section on page 8
- "Device Manager Limitations" section on page 15

Cisco IOS Limitations

These limitations apply to the Cisco Catalyst Blade Switch 3130 for Dell and Cisco Catalyst Blade Switch 3032 for Dell:

- "Access Control List" section on page 9
- "Address Resolution Protocol" section on page 9

- "Cisco X2 Transceiver Modules and SFP Modules" section on page 9
- "Configuration" section on page 10
- "EtherChannel" section on page 11
- "IEEE 802.1x Authentication" section on page 11
- "Multicasting" section on page 12
- "QoS" section on page 13
- "Routing" section on page 13
- "SPAN and RSPAN" section on page 14
- "Stacking" section on page 14

Access Control List

These are the access control list (ACL) limitations:

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

  There is no workaround. (CSCse33114)

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

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

Address Resolution Protocol

This is an Address Resolution Protocol limitation:

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

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

Cisco X2 Transceiver Modules and SFP Modules

These are the Cisco X2 transceiver module and SFP module limitations:

- Cisco X2-10GB-LR transceiver modules with a version identification number lower than V03 might show intermittent frame check sequence (FCS) errors or be ejected from the switch during periods of operational shock greater than 50g. There is no workaround. (CSCse14048)
- Cisco X2-10GB-CX4 transceiver modules with a version identification number lower than V03 might be difficult to insert because of a dimensional tolerance discrepancy. The workaround is to use modules with a version identification number of V03 or later. (CSCsg28558)
- Switches with the Cisco X2-10GB-LX4 transceiver modules with a version identification number prior to V03 might intermittently fail. The workaround is to use Cisco X2-10GB-LX4 transceiver modules with a version identification number of V03 or later. (CSCsh60076)

- Cisco GLC-GE-100FX SFP modules with a serial number between OPC0926xxxx and OPC0945xxxx might show intermittent *module not valid*, data, status, link-flapping, and FCS errors. The workaround is to use modules with serial numbers that are not in the specified range. (CSCsh59585)
- When switches are installed closely together and the uplink ports of adjacent switches are in use, you might have problems accessing the SFP module bale-clasp latch to remove the SFP module or the SFP cable (Ethernet or fiber). Use one of these workarounds:
  - Allow space between the switches when installing them.
  - In a switch stack, plan the SFP module and cable installation so that uplinks in adjacent stack members are not all in use.
  - Use long, small screwdriver to access the latch then remove the SFP module and cable. (CSCsd57938)
- When a Cisco X2-10GB-CX4 transceiver module is in the X2 transceiver module port and you enter the **show controllers ethernet-controller tengigabitethernet** privileged EXEC command, the command displays some fields as unspecified. This is the expected behavior based IEEE 802.3ae. (CSCsd47344)
- The far-end fault optional facility is not supported on the GLC-GE-100FX SFP module. The workaround is to configure aggressive UDLD. (CSCsh70244).

Configuration

These are the configuration limitations:

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

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

  No workaround is necessary. Under normal conditions, the switch generates this notification when snooping the next ARP packet. (CSCse47548)
- When there is a VLAN with protected ports configured in fallback bridge group, packets might not be forwarded between the protected ports.

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

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

  The workaround is to stop the traffic in the direction in which it is not being forwarded, and then restart it after 2 seconds. You can also use the **shutdown** interface configuration command followed by the **no shutdown** command on the interface. (CSCsh04301)
- When line rate traffic is passing through a dynamic port, and you enter the **switchport access vlan dynamic** interface configuration command for a range of ports, the VLANs might not be assigned correctly. One or more VLANs with a null ID appears in the MAC address table instead.

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

EtherChannel

These are the EtherChannel limitations:

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

  The EtherChannel ports are put in the suspended state because each partitioned stack sends LACP packets with different LACP Link Aggregation IDs (the system IDs are different). The ports that receive the packets detect the incompatibility and shut down some of the ports. Use one of these workarounds for ports in this error-disabled state:
  - Enable the switch to recover from the error-disabled state.
  - Enter the **shutdown** and the **no shutdown** interface configuration commands to enable the port.

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

  After the partitioned stacks merge, ports in the suspended state should automatically recover. (CSCse33842)
- When a switch stack is configured with a cross-stack EtherChannel, it might transmit duplicate packets across the EtherChannel when a physical port in the EtherChannel has a link-up or link-down event. This can occur for a few milliseconds while the switch stack adjusts the EtherChannel for the new set of active physical ports and can happen when the cross-stack EtherChannel is configured with either mode ON or LACP. This problem might not occur with all link-up or link-down events.

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

IEEE 802.1x Authentication

These are the IEEE 802.1x authentication limitations:

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

  Use one of these workarounds (CSCsd90495):
  - Configure the port for single-host mode to prevent the extra MAC address from appearing in the MAC address table.
  - Replace the NIC card with a new card.

- When MAC authentication bypass is configured to use Extensible Authentication Protocol (EAP) for authorization and critical authentication is configured to assign a critical port to an access VLAN:
  - If the connected device is supposed to be unauthorized, the connected device might be authorized on the VLAN that is assigned to the critical port instead of to a guest VLAN.
  - If the device is supposed to be authorized, it is authorized on the VLAN that is assigned to the critical port.

  Use one of these workarounds (CSCse04534):
  - Configure MAC authentication bypass to not use EAP.
  - Define your network access profiles to not use MAC authentication bypass. For more information, see the Cisco Access Control Server (ACS) documentation.
- When IEEE 802.1x authentication with VLAN assignment is enabled, a CPUHOG message might appear if the switch is authenticating supplicants in a switch stack.

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

Multicasting

These are the multicasting limitations:

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

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

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

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

  There is no workaround. (CSCsd45753)
- When you configure the **ip igmp max-groups** *number* and **ip igmp max-groups action replace** interface configuration commands and the number of reports exceed the configured max-groups value, the number of groups might temporarily exceed the configured max-groups value. No workaround is necessary because the problem corrects itself when the rate or number of IGMP reports are reduced. (CSCse27757)

- When you configure the IGMP snooping throttle limit by using the **ip igmp max-groups** *number* interface configuration on a port-channel interface, the groups learned on the port-channel might exceed the configured throttle limit number, when all of these conditions are true:
  - The port-channel is configured with member ports across different switches in the stack.
  - When one of the member switches reloads.
  - The member switch that is reloading has a high rate of IP IGMP joins arriving on the port-channel member port.

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

QoS

These are the quality of service (QoS) limitations:

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

  There is no workaround. (CSCeh18677)
- Egress shaped round robin (SRR) sharing weights do not work properly with system jumbo MTU frames.

  There is no workaround. (CSCsc63334)
- In a hierarchical policy map, if the VLAN-level policy map is attached to a VLAN interface and the name of the interface-level policy map is the same as that for another VLAN-level policy map, the switch rejects the configuration, and the VLAN-level policy map is removed from the interface.

  The workaround is to use a different name for the interface-level policy map. (CSCsd84001)
- If the ingress queue has low buffer settings and the switch sends multiple data streams of system jumbo MTU frames at the same time at the line rate, the frames are dropped at the ingress.

  There is no workaround. (CSCsd72001)
- When you use the **srr-queue bandwidth limit** interface configuration command to limit port bandwidth, packets that are less than 256 bytes can cause inaccurate port bandwidth readings. The accuracy is improved when the packet size is greater than 512 bytes. There is no workaround. (CSCsg79627)

Routing

These are the routing limitations:

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

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

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

SPAN and RSPAN

These are the SPAN and Remote SPAN (RSPAN) limitations.

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

  There is no workaround. This is a hardware limitation. (CSCei10129)

- When the **logging event-spanning-tree** interface configuration command is configured and logging to the console is enabled, a topology change might generate a large number of logging messages, causing high CPU utilization. CPU utilization can increase with the number of spanning-tree instances and the number of interfaces configured with the **logging event-spanning-tree** interface configuration command. This condition adversely affects how the switch operates and could cause problems such as STP convergence delay.

  High CPU utilization can also occur with other conditions, such as when debug messages are logged at a high rate to the console.

  Use one of these workarounds:

  - Disable logging to the console.
  - Rate-limit logging messages to the console. (CSCsg91027)
  - Remove the **logging event spanning-tree** interface configuration command from the interfaces.

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

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

VLANs

This is a VLAN limitation:

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

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

Stacking

These are the switch stack limitations:

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

  The workaround is to use the **logging monitor** global configuration command to set the severity level to block the low-level messages on the stack member consoles. (CSCsd79037)

- If a new member switch joins a switch stack within 30 seconds of a command to copy the switch configuration to the running configuration of the stack master, the new member might not get the latest running configuration and might not operate properly.

  The workaround is to reboot the new member switch. Use the **remote command all show run** privileged EXEC command to compare the running configurations of the stack members. (CSCsf31301)

- When the flash memory of a stack member is almost full, it might take longer to start up than other member switches. This might cause that switch to miss the stack-master election window. As a result, the switch might fail to become the stack master even though it has the highest priority.

  The workaround is to delete files in the flash memory to create more free space. (CSCsg30073)

Device Manager Limitations

This is the device manager limitation:

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

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

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

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

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

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

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

Important Notes

These sections describe the important notes related to this software release:

- "Cisco IOS Notes" section on page 15
- "Device Manager Notes" section on page 16

Cisco IOS Notes

These notes apply to Cisco IOS software:

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

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

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

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

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

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

Device Manager Notes

These notes apply to the device manager:

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

  From Microsoft Internet Explorer:

  1. Choose **Tools** > **Internet Options**.
  2. Click **Settings** in the "Temporary Internet files" area.
  3. From the Settings window, choose **Automatically**.
  4. Click **OK**.
  5. Click **OK** to exit the Internet Options window.
- The HTTP server interface must be enabled to display the device manager. By default, the HTTP server is enabled on the switch. Use the **show running-config** privileged EXEC command to see if the HTTP server is enabled or disabled.

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

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

	Command	Purpose
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.

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

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

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

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

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

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

Open Caveats

This section describes the open caveats with possible unexpected activity in this software release.

- CSCsg58889

  If IEEE 802.1Q tunneling and Layer 2 protocol tunneling are configured first on physical ports, and the ports are then added to an unconfigured port channel, the port channel might stop forwarding traffic if one or more physical ports in the EtherChannel are shut down.

  These are the workarounds:

  – Remove and reapply the Layer 2 protocol tunneling configuration on the port channel.

  – Configure the port channel first, next configure the physical ports, and then add them to the port channel.

- CSCsg67684

  When a cross-stack LACP EtherChannel has a maximum configuration, such as eight active and eight hot-standby ports, and there are multiple rapid sequential master failovers and stack rejoins that cause extreme stress, it is possible that the port channel will not function as expected. Some ports might not join the EtherChannel, and traffic might be lost. You can detect the condition by using the **remote command all show etherchannel summary** privileged EXEC command.

  There is no workaround. The out-of-sync switches must be reloaded.

- CSCsg77818

  When a switch interface is configured with trust boundary and Cisco Discovery Protocol (CDP) or the CDP table is repeatedly disabled, enabled, or cleared, the switch might reload.

  The workaround is to avoid repeatedly disabling, enabling, or clearing CDP or the CDP table when trust boundary is configured on an interface. Or, disable trust boundary first before repeatedly disabling, enabling, or clearing CDP or the CDP table.

- CSCsh12472

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

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

  There is no workaround.

- CSCsh70377

  When a secondary VLAN is disassociated from the primary VLAN, duplicate MAC addresses on the primary VLAN remain in the MAC address table.

  The workaround is to disassociate the secondary VLAN from the primary VLAN by entering these commands (in this order):

  clear port-security {**all** | **interface** *interface-id*) privileged EXEC command

  primary-vlan association remove *vlan-id* VLAN configuration mode command.

- CSCsi01526

  Traceback messages appear if you enter the **no switchport** interface configuration command to change a Layer 2 interface that belongs to a port channel to a routed port.

  There is no workaround.

- CSCsi06399

  When a RIP network and IP address are configured on an interface, a traceback error occurs after you enter the **shutdown**, **no shutdown, switchport** and **no switchport** interface configuration commands.

  The workaround is to configure the RIP network and the IP address after you configure the interface.

- CSCsi14303

  When booting a switch stack configured for IP source guard with port security and dynamic ARP inspection, a message similar to this might appear:

  ```
  SYS-2-LINKED: Bad enqueue of 2A3DE74 in queue 22881BC (l3a3-9) -Process=
  "Port-Security", ipl= 6, pid= 161 (l3a3-9) -Traceback= 119CC50 11D2264 9571E0 119B4E0
  95D41C 80DBD8 80E734 80B998 80AAD4 80B55C 9EB158 9E2544 (l3a3-9)
  ```

  There is no workaround. This message is only information, switch functionality is not affected.

- CSCsi16162

  When you enter an all 0s route with an all 1s mask in the routing table and the next hop is entered as an interface, a traceback message appears.

  The workaround is to use an IP address as the next hop instead of an interface.

- CSCsi26444

  The error message `%DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND` might appear for a switch stack under these conditions:

  - IEEE 802.1 is enabled.
  - A supplicant is authenticated on at least one port.
  - A new member joins a switch stack.

  You can use one of these workarounds:

  - Enter the **shutdown** and the **no shutdown** interface configuration commands to reset the port.
  - Remove and reconfigure the VLAN.

- CSCsi50367

  When changing a switch port access VLAN from static to dynamic or the reverse, a message similar to this might appear:

  ```
  01:43:55: PSECURE: Assert failure: is_etherchnl(hwidb_or_null swidb)):
  ../switch/psecure/psecure_ifc.c: 412: psecure_get_vlanid (l2a1-5) 01:43:55Traceback=
  804484 809604 802258 806904 70FC 8D70 5C97BC 6901DC 6903CC 9EF8D8 9E6CC4 (l2a1-5)
  ```

  There is no workaround necessary. This message does not affect switch functionality.

- CSCsi52914

  When you are configuring a SPAN session, this message might erroneously appear even when two source sessions are not configured:

  ```
  % Platform can support a maximum of 2 source sessions
  ```

  The workaround is to reboot the switch stack.

- CSCsi65551

  In certain situations, during master switch failover, a VLAN that has been error disabled on a port might be re-enabled after the master switchover, even though the port has not been configured for automatic recovery.

  There is no workaround.

- CSCsi67680 platforms

  When unicast routing is disabled and then re-enabled, virtual routing and forwarding (VRF) routing is disabled on the switch interfaces.

  The workaround is to enter the **shut** and **no shut** interface configuration commands on the affected interfaces.

- CSCsi70454

  The configuration file used for the configuration replacement feature requires the character string *end\n* at the end of the file. The Windows Notepad text editor does not add the *end\n* string, and the configuration rollback does not work.

These are the workarounds. (You only need to do one of these.)

- Do not use a configuration file that is stored by or edited with Windows Notepad.
- Manually add the character string *end\n* to the end of the file.

The workaround is to configure routed IPv4 multicast and IPv6 unicast traffic in different switch ports.

- CSCsi73653

  After a stack-master failover, switch ports in the stack cannot detect new devices. This only affects new devices connected to the switch ports. Devices that were connected to active ports before the failover remain in a trusted state.

  There is no workaround.

- CSCsj10198

  When a per-port per-VLAN policy map (a hierarchical VLAN-based policy map) is attached to a VLAN interface, and you remove the child-policy policer from the policy map and then add it back, the policy map fails to re-attach to the same SVI

  The workaround is to delete the child policy, which removes it from the parent policy. Then recreate the child policy (with the same or a different name) and reference it in the parent policy. The parent policy then successfully attaches to the SVI.

- CSCsj22678

  A delay can occur you remove an access control list (ACL) from a switch stack under these conditions:

  - A QoS, per-port policy map is attached to a large number of switched virtual interfaces (SVIs) in the stack.
  - A per-VLAN QoS, per-port policer policy map is attached to a large number of switched virtual interfaces (SVIs) in the stack
  - The ACL to be removed is being used by the policy map.
  - There are three or more switches in the stack.

  The delay can increase, up to 30 minutes, depending on the number of SVIs that are attached to the policy map. The delay does not affect the operation of the policy-map. However, either of these workarounds will reduce the length of the delay:

  - Remove the access control entries (ACEs) from the destination ACL, leaving the ACL empty. (The effect is the same as removing the ACL itself.)
  - Detach the affected policy-map(s) from all the attached VLAN(s) and SVIs, remove the ACL from the policy-map(s), and then *reattach* the policy-map(s) back to the original SVIs.

- CSCsj77933

  In Cisco IOS Release 12.2(35)SE and Cisco IOS Release 12.2(37)SE, if you enter a space before a comma in the **define interface-range** or the **interface range global** configuration command, the space before the comma is not saved in the switch configuration.

  There is no workaround.

- CSCsk19926

  Traffic is not received on a member port in a switch stack under these conditions:

  - The port is in a cross-stack EtherChannel.
  - One or more of the master switch Cisco TwinGig Converter Module ports are in the cross-stack EtherChannel.
  - This member switch has been reloaded.

  The workaround is to enter the **shutdown** and **no shutdown** interface configuration commands on the affected interface, or to reload the entire stack instead of a single member switch.

- CSCsl49153

  You might receive a traceback message when you use the **no interface port-channel** global configuration command to delete interfaces from an EtherChannel that has port channels on multiple stack members.

  The workaround is to save the configuration and to reload the stack.

- CSCsl63862

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

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

Documentation Updates

This update is for the software configuration guide:

If the switch is running the IP base image, you can configure complete EIGRP routing. However, the configuration is not implemented because the IP base image supports only EIGRP stub routing, as described in the "Configuring IP Unicast Routing" chapter of the software configuration guide.

After you have entered the **eigrp stub** router configuration command, only the **eigrp stub connected summary** command takes effect. Although the CLI help might show the **receive-only** and **static** keywords and the you can enter these keywords, the switch running the IP base image always behaves as if the **connected** and **summary** keywords were configured.

Related Documentation

These documents provide complete information about the Cisco Catalyst Blade Switch 3130 for Dell and 3032 for Dell and are available on Cisco.com:

You can order printed copies of documents with a DOC-xxxxxx= number. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 22.

These documents provide complete information about the switch module and are available from this Cisco.com site:

http://www.cisco.com/en/US/products/ps6748/tsd_products_support_series_home.html

- *Cisco Catalyst Blade Switch 3130 for Dell and Cisco Catalyst Blade Switch 3032 for Dell Getting Started Guide* (not orderable but available on Cisco.com)
- *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3000 Series for Dell* (order number DOC-7817053=)
- *Release Notes for the Cisco Catalyst Blade Switch 3130 for Dell and the Cisco Catalyst Blade Switch 3032 for Dell* (not orderable but available on Cisco.com)

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

- *Cisco Catalyst Blade Switch 3130 for Dell Software Configuration Guide* (not orderable but available on Cisco.com)
- *Cisco Catalyst Blade Switch 3130 for Dell Command Reference* (not orderable but available on Cisco.com)
- *Cisco Catalyst Blade Switch 3130 for Dell System Message Guide* (not orderable but available on Cisco.com)
- *Cisco Software Activation Document for Dell*
- These compatibility matrix documents are available from this Cisco.com site:

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

  - *Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix*
  - *Cisco Small Form-Factor Pluggable Modules Compatibility Matrix*
  - *Compatibility Matrix for 1000BASE-T Small Form-Factor Pluggable Modules*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

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

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