



# Release Notes for the Cisco Catalyst Blade Switch 3040 for FSC, Cisco IOS Release 12.2(44)SE and Later

---

Revised March 25, 2009

Cisco IOS Release 12.2(44)SE and later runs on the Cisco Catalyst Blade Switch 3040 for FSC, referred to as the *switch*. The switch is installed in the Fujitsu Siemens Computers (FSC) PRIMERGY BX600 system, referred to as the *BX600 system*.

Unless otherwise noted, the term *switch* refers to a standalone switch.



**Note**

---

Before you install the switch in the BX600 system, upgrade the BX600 system management software to version 1.68 or later for the switch to operate properly.

---

Check for updates to this document at this URL for information about compatibility with the BX600 system software:

[http://www.cisco.com/en/US/products/ps8743/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps8743/prod_release_notes_list.html)



**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(44)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(44)SE and any limitations, restrictions, and caveats that apply to them. Verify that these release notes are correct for your switch:

- If you are installing a new switch, see the Cisco IOS release label on the switch packaging.
- If your switch is on, use the **show version** privileged EXEC command. See the “[Finding the Software Version and Feature Set](#)” section on page 3.
- If you are upgrading to a new release, see the software upgrade filename for the software version. See the “[Deciding Which Files to Use](#)” section on page 4.



---

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

© 2008-2009 Cisco Systems, Inc. All rights reserved.

For the complete list of Cisco Catalyst Blade Switch 3040 for FSC documentation, see the “[Related Documentation](#)” section on page 23.

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

<http://tools.cisco.com/support/downloads/go/MDFTree.x?butype=switches>

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.

## Contents

This information is in the release notes:

- “[System Requirements](#)” section on page 2
- “[Upgrading the Switch Software](#)” section on page 3
- “[Installation Notes](#)” section on page 6
- “[New Software Features](#)” section on page 6
- “[Limitations and Restrictions](#)” section on page 7
- “[Important Notes](#)” section on page 11
- “[Open Caveats](#)” section on page 13
- “[Resolved Caveats](#)” section on page 14
- “[Documentation Updates](#)” section on page 22
- “[Obtaining Documentation, Obtaining Support, and Security Guidelines](#)” section on page 23

## System Requirements

The system requirements are described in these sections:

- “[Hardware Supported](#)” section on page 2
- “[Device Manager System Requirements](#)” section on page 2

## Hardware Supported

The hardware supported on this release is the Cisco Catalyst Blade Switch 3040.

## Device Manager System Requirements

These sections describes 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 1 lists the minimum hardware requirements for running the device manager.

**Table 1** Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum <sup>1</sup>	512 MB <sup>2</sup>	256	1024 x 768	Small

1. We recommend 1 GHz.
2. We recommend 1 GB DRAM.

## Software Requirements

Table 2 lists the supported operating systems and browsers for using the device manager, which does not require a plug-in. The device manager verifies the browser version when starting a session to ensure that the browser is supported.



**Note**

Windows NT and Windows 98 are no longer supported.

**Table 2** Supported Operating Systems and Browsers

Operating System	Minimum Service Pack or Patch	Microsoft Internet Explorer <sup>1</sup>	Netscape Navigator
Windows 2000	None	5.5 or 6.0	7.1
Windows XP	None	5.5 or 6.0	7.1

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

## 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 3
- “Deciding Which Files to Use” section on page 4
- “Upgrading a Switch by Using the Device Manager” section on page 5
- “Upgrading a Switch by Using the CLI” section on page 5
- “Recovering from a Software Failure” section on page 6

## 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(44)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.122-44.SE6.tar	Cisco Catalyst Blade Switch 3040 for FSC image file and device manager files. This image has Layer 2+ features.
cbs30x0-ipbasek9-tar.122-44.SE6.tar	Cisco Catalyst Blade Switch 3040 for FSC 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/products/sw/iosswrel/ps5187/prod\\_bulletin0900aecd80281c0e.html](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](http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a00800811e0.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. If you have a SmartNet support contract, go to this URL, and log in to download the appropriate files:

<http://www.cisco.com/kobayashi/sw-center/sw-lan.shtml>

- 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/c3750-ipservices-tar.122-44.SE.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 BX600 Management Blade WEB GUI 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

These are the new software features for this release:

- DHCP-based autoconfiguration and image update to download a specified configuration and image to a large number of switches
- Configurable small-frame arrival threshold to prevent storm control when small frames (64 bytes or less) arrive on an interface at a specified rate (the threshold)
- Support for the `*`, `ip-address`, `interface interface-id`, and `vlan vlan-id` keywords with the `clear ip dhcp snooping` command
- HTTP and HTTP(s) support over IPv6, which eliminates the need to run dual stack on the switch
- Simple Network and Management Protocol (SNMP) can be configured over IPv6 transport so that an IPv6 host can send SNMP queries and receive SNMP notifications from a device running IPv6
- IPv6 supports stateless autoconfiguration to manage link, subnet, and site addressing changes, such as management of host and mobile IP addresses

- IEEE 802.1x readiness check to determine the readiness of connected end hosts before configuring IEEE 802.1x on the switch
- The switch now ships with the IP base image installed, which provides Layer 2+ features, including static routing, EIGRP and PIM stub routing, the Hot Standby Router Protocol (HSRP), the Routing Information Protocol (RIP), IPv6 host management, and IPv6 MLD snooping

## 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 7](#)
- [“Device Manager Limitations” section on page 11](#)

## Cisco IOS Limitations

These limitations apply to the switch:

- [“Configuration” section on page 7](#)
- [“Dynamic ARP Inspection” section on page 8](#)
- [“Ethernet” section on page 8](#)
- [“IP” section on page 8](#)
- [“IP Telephony” section on page 9](#)
- [“MAC Addressing Multicasting” section on page 9](#)
- [“QoS” section on page 10](#)
- [“SPAN and RSPAN” section on page 10](#)
- [“Trunking” section on page 10](#)
- [“VLAN” section on page 11](#)

## 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)

## Dynamic ARP Inspection

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. (CSCse06827)

## 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. This limitation is unlikely to affect the Cisco Catalyst Blade Switch 3040 for FSC because IP phones are not usually connected to the switch uplink ports. (CSCea85312)

## MAC Addressing 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)

## 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)

## 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)

## 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)

## Important Notes

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

- [“Cisco IOS Notes” section on page 11](#)
- [“Device Manager Notes” section on page 12](#)

## Cisco IOS Notes

These notes apply to Cisco IOS software:

- 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

These notes apply to the device manager:

- 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.

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

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>ip http authentication {aaa   enable   local}</b>	Configure the HTTP server interface for the type of authentication that you want to use. <ul style="list-style-type: none"> <li>• <b>aaa</b>—Enable the authentication, authorization, and accounting feature. You must enter the <b>aaa new-model</b> interface configuration command for the <b>aaa</b> keyword to appear.</li> <li>• <b>enable</b>—Enable password, which is the default method of HTTP server user authentication, is used.</li> <li>• <b>local</b>—Local user database, as defined on the Cisco router or access server, is used.</li> </ul>
Step 3	<b>end</b>	Return to privileged EXEC mode.
Step 4	<b>show running-config</b>	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	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>ip http authentication {enable   local   tacacs}</code>	Configure the HTTP server interface for the type of authentication that you want to use. <ul style="list-style-type: none"> <li><b>enable</b>—Enable password, which is the default method of HTTP server user authentication, is used.</li> <li><b>local</b>—Local user database, as defined on the Cisco router or access server, is used.</li> <li><b>tacacs</b>—TACACS server is used.</li> </ul>
Step 3	<code>end</code>	Return to privileged EXEC mode.
Step 4	<code>show running-config</code>	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 start the device manager.

## Open Caveats

This section describes the open severity 3 Cisco IOS configuration caveats with possible unexpected activity in this software release:

- CSCsc96474

The switch might display tracebacks similar to these examples when a large number of IEEE 802.1x supplicants try to repeatedly log in and log out.

Examples:

```
Jan 3 17:54:32 L3A3 307: Jan 3 18:04:13.459: %SM-4-BADEVENT: Event 'eapReq' is invalid
for the current state 'auth_bend_idle': dot1x_auth_bend Fa9
```

```
Jan 3 17:54:32 L3A3 308: -Traceback= B37A84 18DAB0 2FF6C0 2FF260 8F2B64 8E912C Jan 3
19:06:13 L3A3 309: Jan 3 19:15:54.720: %SM-4-BADEVENT: Event 'eapReq_no_reAuthMax' is
invalid for the current ate 'auth_restart': dot1x_auth Fa4
```

```
Jan 3 19:06:13 L3A3 310: -Traceback= B37A84 18DAB0 3046F4 302C80 303228 8F2B64 8E912C
Jan 3 20:41:44 L3A3 315: .Jan 3 20:51:26.249: %SM-4-BADEVENT: Event 'eapSuccess' is
invalid for the current state 'auth_restart': dot1x_auth Fa9
```

```
Jan 3 20:41:44 L3A3 316: -Traceback= B37A84 18DAB0 304648 302C80 303228 8F2B64 8E912C
```

There is no workaround.

- CSCsd03580  
When IEEE 802.1x is globally disabled on the switch by using the **no dot1x system-auth-control** global configuration command, some interface level configuration commands, including the **dot1x timeout** and **dot1x mac-auth-bypass commands**, become unavailable.  
The workaround is to enable the **dot1x system-auth-control** global configuration command before attempting to configure interface level IEEE 802.1x parameters.
- CSCsi70454  
The configuration file used for the configuration replacement feature requires the character string *endn* at the end of the file. The Windows Notepad text editor does not add the *endn* 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 *endn* to the end of the file.
 The workaround is to configure routed IPv4 multicast and IPv6 unicast traffic in different switch ports.
- CSCsj74022  
The switch does not correctly update the entPhysicalChildIndex objects from the ENTITY-MIB, and some of the entPhysicalChildIndex entries are missing from the table. This adversely affects network management applications such as CiscoWorks CiscoView because they cannot manage the switch.  
There is no workaround.
- CSCsk65142  
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.

## Resolved Caveats

This section describes the caveats that have been resolved in these releases:

- [“Cisco IOS Caveats Resolved in Cisco IOS Release 12.2\(44\)SE6” section on page 15](#)
- [“Cisco IOS Caveats Resolved in Cisco IOS Release 12.2\(44\)SE5” section on page 16](#)
- [“Cisco IOS Caveats Resolved in Cisco IOS Release 12.2\(44\)SE3” section on page 18](#)
- [“Cisco IOS Caveats Resolved in Cisco IOS Release 12.2\(44\)SE2” section on page 19](#)
- [“Cisco IOS Caveats Resolved in Cisco IOS Release 12.2\(44\)SE1” section on page 20](#)
- [“Cisco IOS Caveats Resolved in Cisco IOS Release 12.2\(44\)SE” section on page 20](#)

## Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(44)SE6

- CSCsk64158
 

Symptoms: Several features within Cisco IOS software are affected by a crafted UDP packet vulnerability. If any of the affected features are enabled, a successful attack will result in a blocked input queue on the inbound interface. Only crafted UDP packets destined for the device could result in the interface being blocked, transit traffic will not block the interface.

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available in the workarounds section of the advisory. This advisory is posted at the following link:  
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-udp.shtml>.
- CSCsm27071
 

A vulnerability in the handling of IP sockets can cause devices to be vulnerable to a denial of service attack when any of several features of Cisco IOS software are enabled. A sequence of specially crafted TCP/IP packets could cause any of the following results:

  - The configured feature may stop accepting new connections or sessions.
  - The memory of the device may be consumed.
  - The device may experience prolonged high CPU utilization.
  - The device may reload. Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available in the “workarounds” section of the advisory. The advisory is posted at  
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-ip.shtml>
- CSCso75640
 

When MAC authentication bypass (MAB) authentication fails, a memory leak no longer occurs.
- CSCsq89564
 

When a VLAN is assigned for IEEE 802.1x authentication and no VLAN is assigned for other types of authentication (such as user authentication or reauthentication), the 802.1x VLAN assignment no longer persists across subsequent authentication attempts.
- CSCsr29468
 

Cisco IOS software contains a vulnerability in multiple features that could allow an attacker to cause a denial of service (DoS) condition on the affected device. A sequence of specially crafted TCP packets can cause the vulnerable device to reload.

Cisco has released free software updates that address this vulnerability.

Several mitigation strategies are outlined in the workarounds section of this advisory.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090325-tcp.shtml>
- CSCsr54797
 

When the switch uses HTTP (web-based) authentication, a memory leak no longer occurs after authorization and policy download.
- CSCsv38166
 

The server side of the Secure Copy (SCP) implementation in Cisco IOS software contains a vulnerability that could allow authenticated users with an attached command-line interface (CLI) view to transfer files to and from a Cisco IOS device that is configured to be an SCP server, regardless of what users are authorized to do, per the CLI view configuration. This vulnerability

could allow valid users to retrieve or write to any file on the device's file system, including the device's saved configuration and Cisco IOS image files, even if the CLI view attached to the user does not allow it. This configuration file may include passwords or other sensitive information.

The Cisco IOS SCP server is an optional service that is disabled by default. CLI views are a fundamental component of the Cisco IOS Role-Based CLI Access feature, which is also disabled by default. Devices that are not specifically configured to enable the Cisco IOS SCP server, or that are configured to use it but do not use role-based CLI access, are not affected by this vulnerability.

This vulnerability does not apply to the Cisco IOS SCP client feature.

Cisco has released free software updates that address this vulnerability.

There are no workarounds available for this vulnerability apart from disabling either the SCP server or the CLI view feature if these services are not required by administrators.

This advisory is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20090325-scp.shtml>.

- CSCsx42798

A switch no longer displays processor memory-allocation failure messages under these conditions:

- The switch is running IOS release 12.2(44)SE4 or 12.2(44)SE5.
- Authentication, authorization, and accounting (AAA) is configured on the switch.
- Memory in the primary processor pool is depleted.



**Note**

If the hardware configuration is not a switch stack, AAA requests might fail and the switch might experience high CPU usage for the authentication manager process. In addition, if the hardware configuration is a switch stack and 802.1x, web authentication, or MAC address bypass (MAB) are configured, the switch software might reload after reporting the memory-allocation failure.

This is resolved in Cisco IOS 12.2(44)SE6 and later.

## Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(44)SE5

- CSCsd73245

Excessive IPRT-3-PATHIDX error messages no longer appear in the log file.

- CSCsf10850

When configuring an IP SSH version 2 connection, you can no longer create an RSA key that is less than 768 bits.

- CSCsg51695

RIP routes now correctly update when the **maximum-paths 16** option is used.

- CSCsk16821

The DHCP server can be configured to send DHCP Not Acknowledge(DHCPNAK) messages to unknown clients.

- CSCsq26873

The **dot1x timeout reauth-period server** interface configuration command now works correctly. In previous releases, the switch would reauthenticate correctly after the command was entered, but the switch would then reauthenticate every 10 minutes.

- CSCsu10229  
The `cdpCacheAddress` value now appears in a `GLOBAL_UNICAST` address.
- CSCsu40077  
The switch now correctly processes ingress traffic when a port is configured with a short `802.1x tx-period timer` value (such as `dot1x timeout tx-period 3`).
- CSCsu47056  
The username is now properly logged when the **remote command** privileged EXEC command is used to configure a cluster member.
- CSCsu67705  
Avaya IP phones now correctly authenticate on an 802.1x-enabled switch port.

## Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(44)SE3

- CSCee55603  
An SNMP access-control list (ACL) now works correctly on virtual routing and forwarding (VRF) interfaces.
- CSCsl66074  
Intermittently switch reloads no longer occur when IP helper addresses are configured on a VLAN.
- CSCsm88601  
When multiple voice-over-IP phones are connected to a switch or switch stack with MAC authentication bypass enabled, setting the IEEE 802.1x timeout period too low no longer causes a switch in single-host mode to authenticate the phones using MAC authentication bypass, except when other data packets are received before CDP packets.
- CSCso72052  
An end host no longer remains in the guest VLAN after an IEEE 802.1X authentication.
- CSCso87307  
A switch no longer drops Cisco Group Management Protocol (CGMP) packets.
- CSCsq71492  
The switch no longer reloads with an address error if the TACACS+ server sends an authentication error when the access control system is configured and a timeout request occurs.
- CSCsr55949  
When IEEE 802.1x port-based authentication is enabled on the switch, Extensible Authentication Protocol (EAP) notification packets from the supplicant are no longer discarded.
- CSCsu04337  
In environments using Layer 2 IP Network Admission Control (NAC), long downloadable ACLs (dACLs) with source or destination Layer 4 ports no longer cause unpredictable events in which all traffic is dropped and URL redirects are not enforced.

## Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(44)SE2

- CSCsg91027

When the logging event-spanning-tree interface configuration command is configured and logging to the console is enabled, a topology change no longer generates a large number of logging messages.

- CSCsI76599

The switch no longer unexpectedly reloads while configured with IEEE 802.1x authentication and the MAC authentication bypass feature.

- CSCsI77063

When you enable detection of Cisco IP phones by entering the **switchport voice detect cisco-phone** interface configuration command, the interface is no longer disabled if you connect a third-party IP phone is connected to the interface.




---

**Note** This command was designed to work with Cisco IP phones; you should not enable it on interfaces connected to third-party IP phones.

---

- CSCsI93313

When you configure a port channel as trusted by entering the **ip dhcp snooping trust** interface configuration command, the configuration is no longer lost when the link goes from down to up.

- CSCsm08603

This traceback error no longer appears when you enter the **show aaa subscriber profile** privileged EXEC command:

```
*Mar 2 01:50:41.127: %PARSER-3-BADSUBCMD: Unrecognized subcommand 10 in exec command
'show aaa subscriber profile WORD'
-Traceback= D003B4 D00AC8 C908A0 C2F040 C8CA18 CB8984 93B670 932338
```




---

**Note** In Cisco IOS Release 12.2(44)SE2 and later, the **subscriber** keyword is no longer supported. (The **show aaa subscriber profile** command is not supported, and you cannot configure the aaa subscriber profile command.)

---

- CSCsm26406

Enhanced IGRP (EIGRP) now works correctly when you enter the **ip authentication key-chain eigrp** interface configuration command.

- CSCsm61718

A switch no longer unexpectedly reloads when you configure two or more authentication, authorization, and accounting (AAA) broadcast groups.

- CSCso75848

The switch no longer experiences a memory leak during an HTTP core process.

## Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(44)SE1

- CSCec51750  
A router that is configured for HTTP and voice-based services no longer unexpectedly reloads due to memory corruption.
- CSCsd45672  
When AAA is enabled and you use the **aaa group server radius** *group-name* global configuration command to put the switch in server group configuration mode, entering the **server-private** command no longer causes the switch to reload.
- CSCsh46990  
The switch no longer reloads when you use the **aaa authentication eou default group radius enable** global configuration command to configure an EAP over UDP (EOU) method list.
- CSCsj85065  
A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.  
  
Cisco has released free software updates that address this vulnerability.  
  
Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.  
  
This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-ssl.shtml>.
- CSCsm41883  
High CPU usage (greater than 90 percent) no longer occurs on the switch when you first connect a new device.
- CSCsm57520  
A switch no longer unexpectedly reloads when you configure the switch ports as dynamic ports by using the VLAN Membership Policy Server (VMPS).

## Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(44)SE

- CSCeg67844  
The switch no longer returns an incorrect value for the ciscoFlashPartitionFileCount MIB.
- CSCei63394  
Syslog messages are no longer generated when two or more IEEE 802.1x-capable hosts are connected through a hub and the port is in single-host mode.
- CSCsb85001  
When traffic passes through a VMPS port and you enter the **shut** interface configuration command, a dynamic VLAN is now assigned.
- CSCsc30733  
This error message no longer appears during authentication when a method list is used and one of the methods in the method list is removed:  
  
AAA-3-BADMETHODERROR:Cannot process authentication method 218959117

- CSCsd01180  
The switch no longer reloads when you use a Kron command scheduler routine to automatically copy configuration data using the Secure Copy Protocol (SCP). (Kron is a Cisco IOS utility for scheduling non-prompting CLI commands to execute at a later time.)
- CSCsd78044  
When IGMP snooping is enabled and an EtherChannel member interface fails, the switch no longer stops forwarding multicast traffic on the EtherChannel. In previous releases, this occurred when multicast routing was enabled and the EtherChannel interface was a member of a multicast group not directly connected (that is, the multicast group that did not have the C flag set in the **show ip mroute** privileged EXEC command output).
- CSCse14774  
When a switch is connected to a third-party router through an EtherChannel and the EtherChannel is running in Link Aggregation Control Protocol (LACP) mode, the interfaces in the EtherChannel no longer fail after you enter the **switchport trunk native vlan vlan-id** interface configuration command to change the native VLAN from VLAN 1 (the default) to a different VLAN ID.
- CSCsg18176  
When dynamic ARP inspection is enabled and IP validation is disabled, the switch no longer drops ARP requests that have a source address of 0.0.0.0. When you are enabling IP validation, use the **allow zeros** keyword to allow the 0.0.0.0 source address.
- CSCsg21537  
When MAC addresses are learned on an EtherChannel port, the addresses are now correctly deleted from the MAC address table.
- CSCsg30295  
When you configure an IP address on a switch virtual interface (SVI) with DHCP and enable DHCP snooping on the SVI VLAN, the switch SVI can now obtain an IP address.
- CSCsh74395  
When a VLAN includes multiple MAC addresses, the number of MAC addresses shown in SNMP now matches the output of the **show mac-address count vlan vlan-id** privileged EXEC command.
- CSCsi08513  
MAC flap-notification no longer occurs when a switch is running VLAN bridge spanning-tree protocol (STP) and fallback bridging is configured on the VLANs running STP.
- CSCsi10584  
Multiple Spanning-Tree Protocol (MSTP) convergence time has been improved for Cisco IOS Release 12.2.
- CSCsi63999  
Changing the spanning tree mode from MSTP to other spanning modes no longer causes tracebacks.
- CSCsj52956  
The TxBufferFullDropCount counter no longer increments when the switch is a standalone switch.
- CSCsj53001  
The Total- output-drops field in the **show interfaces** privileged EXEC command output now displays accurate ASIC drops.

- CSCsj77933

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 now saved in the switch configuration.

- CSCsj87991

A switch configured for Link Layer Discovery Protocol (LLDP) now correctly reports the enabled switch capabilities in the LLDP type, length, and value (TLV) attributes.

## Documentation Updates

This section contains these documentation updates:

- [“Updates to the Software Configuration Guide” section on page 22](#)
- [“Updates to the System Message Guide” section on page 22](#)

## Updates to the Software Configuration Guide

These are the updates to the software configuration guide:

- This information in the “Enabling BPDU Guard” section of the “Configuring Optional Spanning-Tree Features” chapter in the software configuration guide is incorrect:

When you globally enable BPDU guard on ports that are Port Fast-enabled (the ports are in a Port Fast-operational state), spanning tree shuts down Port Fast-enabled ports that receive BPDUs.

This is the correct information:

When you globally enable BPDU guard on ports that are Port Fast-enabled (the ports are in a Port Fast-operational state), spanning tree continues to run on the ports. They remain up unless they receive a BPDU.

- When routing is enabled on the switch, you can configure complete EIGRP routing. However, the configuration is not implemented because the software 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 you can enter these keywords, the switch always behaves as if the **connected** and **summary** keywords were configured.

## Updates to the System Message Guide

These are the updates to the system message guide:

**Error Message** VQPCCLIENT-2-TOOMANY: Interface [chars] shutdown by active host limit.

**Explanation** The system has shut down the specified interface because too many hosts have requested access to that interface. [chars] is the interface name.

**Recommended Action** To enable the interface, remove the excess hosts, and enter the **no shutdown** interface configuration command.

**Error Message** VQPCLIENT-3-VLANNAME: Invalid VLAN [chars] in response.

**Explanation** The VLAN membership policy server (VMPS) has specified a VLAN name that is unknown to the switch. [chars] is the VLAN name.

**Recommended Action** Ensure that the VLAN exists on the switch. Verify the VMPS configuration by entering the **show vmmps** privileged EXEC command.

**Error Message** WCCP-5-CACHEFOUND: Web Cache [IP\_address] acquired.

**Explanation** The switch has acquired the specified web cache. [IP\_address] is the web cache IP address.

**Recommended Action** No action is required.

**Error Message** WCCP-1-CACHELOST: Web Cache [IP\_address] lost.

**Explanation** The switch has lost contact with the specified web cache. [IP\_address] is the web cache IP address.

**Recommended Action** Verify the operation of the web cache by entering the **show ip wccp web-cache** privileged EXEC command.

## Related Documentation

These documents provide complete information about the Cisco Catalyst Blade Switch 3040 for FSC and are available at Cisco.com:

[http://www.cisco.com/en/US/products/ps8743/tsd\\_products\\_support\\_series\\_home.html](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 3040 for FSC:

- *Cisco Catalyst Blade Switch 3040 for FSC Getting Started Guide*
- *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3040 for FSC*
- *Cisco Catalyst Blade Switch 3040 for FSC Software Configuration Guide*
- *Cisco Catalyst Blade Switch 3040 for FSC Command Reference*
- *Cisco Catalyst Blade Switch 3040 for FSC 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>

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved.

