



Release Notes for the Cisco Catalyst Blade Switch 3040 for FSC, Cisco IOS Release 12.2(35)SE and Later

Revised June 10, 2008

Cisco IOS Release 12.2(35)SE 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*.



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

These release notes include important information about Cisco IOS Release 12.2(35)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 4.
- If you are upgrading to a new release, see the software upgrade filename for the software version. See the “[Deciding Which Files to Use](#)” section on page 4.

For the complete list of Cisco Catalyst Blade Switch 3040 for FSC documentation, see the “[Related Documentation](#)” section on page 31.

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

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

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.



Corporate Headquarters:

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

© 2007 Cisco Systems, Inc. All rights reserved.

Contents

This information is in the release notes:

- [“System Requirements” section on page 3](#)
- [“Upgrading the Switch Software” section on page 4](#)
- [“Installation Notes” section on page 6](#)
- [“New Software Feature” section on page 7](#)
- [“Limitations and Restrictions” section on page 7](#)
- [“Important Notes” section on page 11](#)
- [“Open Caveats” section on page 13](#)
- [“Resolved Caveats” section on page 15](#)
- [“Related Documentation” section on page 31](#)
- [“Documentation Updates” section on page 19](#)
- [“Obtaining Documentation” section on page 31](#)
- [“Documentation Feedback” section on page 32](#)
- [“Cisco Product Security Overview” section on page 32](#)
- [“Product Alerts and Field Notices” section on page 33](#)
- [“Obtaining Technical Assistance” section on page 34](#)
- [“Obtaining Additional Publications and Information” section on page 35](#)

System Requirements

The system requirements are described in these sections:

- [“Hardware Supported” section on page 3](#)
- [“Device Manager System Requirements” section on page 3](#)

Hardware Supported

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

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
Intel Pentium II ¹	64 MB ²	256	1024 x 768	Small

1. We recommend Intel Pentium 4.
2. We recommend 256-MB 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 ¹	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 4
- “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 CLI, use the tar file and the **archive download-sw** privileged EXEC command.

Table 3 lists the filenames for this software release.

Table 3 Cisco IOS Software Image Files

Filename	Description
cbs40x0-lanbase-tar.122-35.SE.tar	Cisco Catalyst Blade Switch 3040 for FSC image file and device manager files. This image has Layer 2+ features.
cbs40x0-lanbasek9-tar.122-35.SE.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

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/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_r/ffrprt2/frf011.htm#wp1018426

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.122-35.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 HP Onboard Administrator program described in the getting started guide.
- The CLI-based setup program, as described in the hardware installation guide.
- The DHCP-based autoconfiguration, as described in the software configuration guide.
- Manually assigning an IP address, as described in the software configuration guide.

New Software Feature

This release supports Web authentication to authenticate a supplicant (client) that does not support IEEE 802.1x functionality. For more information, see the [“Documentation Updates” section on page 19](#).

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](#)
- [“Ethernet” section on page 8](#)
- [“IP” section on page 8](#)
- [“IP Telephony” section on page 9](#)
- [“MAC Addressing Multicasting” 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

These are the configuration limitations:

- 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. (CSCe71176 and CSCdz11708)

- When connected to some third-party devices that send early preambles, a switch port operating at 100 Mbps full duplex or 100 Mbps 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 Mbps 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)

Ethernet

This is the Ethernet limitation:

- 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

This is the IP limitation:

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

This is the IP telephony limitation:

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

These are the multicasting limitations:

- 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

These are the quality of service (QoS) limitations:

- 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)

SPAN and RSPAN

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

- 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

These are the trunking limitations:

- 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

This is the VLAN limitation:

- 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

These are the device manager limitations for this release:

- 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.

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:

- Choose **Tools > Internet Options**.
 - Click **Settings** in the Temporary Internet files area.
 - From the Settings window, choose **Automatically**.
 - Click **OK**.
 - 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. <ul style="list-style-type: none"> aaa—Enable the authentication, authorization, and accounting feature. You must enter the aaa new-model interface configuration command for the aaa keyword to appear. enable—Enable password, which is the default method of HTTP server user authentication, is used. local—Local user database, as defined on the Cisco router or access server, is used.
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config	Verify your entries.

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

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

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

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

	Command	Purpose
Step 1	<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"> • 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	<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 caveats for this software release.

Open Cisco IOS Caveats

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

- CSCsb85001

If traffic is passing through VMPS ports and you perform a **shut** operation, a dynamic VLAN is not assigned and a VLAN with a null ID appears.

The workaround is to clear the MAC address table. This forces the VMPS server to correctly reassign the VLAN.

- CSCsc30733

This error message 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
```

There is no workaround. However, this is only an informational message and does not affect switch functionality.

- CSCsc59418

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.

- 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.

- CSCse06827

When dynamic ARP inspection is configured on a VLAN, and the ARP traffic on a port in the VLAN is within the configured rate limit, the port might go into an error-disabled state.

The workaround is to configure the burst interval to more than 1 second.

- CSCsg18176

When dynamic ARP inspection is enabled and IP validation is disabled, the switch drops ARP requests that have a source address of 0.0.0.0.

The workaround is to configure an ARP access control list (ACL) that permits IP packets with a source IP address of 0.0.0.0 (and any MAC) address) and apply the ARP ACL to the desired DAI VLANs.

- CSCsg21537

When MAC addresses are learned on an Etherchannel port, the addresses are incorrectly deleted from the MAC address table even when the MAC address table aging timeout value is configured to be longer than the ARP timeout value. This causes intermittent unicast packet flooding in the network.

- 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 cannot obtain an IP address.

The workaround is to not enable DHCP snooping on the SVI VLAN or to use a static IP address for the SVI.

- CSCsg79506

During repeated reauthentication of supplicants on an IEEE 802.1x-enabled switch, if the RADIUS server is repeatedly going out of service and then coming back up, the available switch memory might deplete over time, eventually causing the switch to shut down.

There is no work-around, except to ensure that the RADIUS server is stable.

- CSCsg81334

If IEEE 802.1x critical authentication is not enabled and the RADIUS authentication server is temporarily unavailable during a reauthentication, when the RADIUS server comes back up, MAC authentication bypass (MAB) does not authenticate a previously authenticated client.

The workaround is to enter the **shutdown** interface configuration command followed by the **no shutdown** command on the port connected to the client. An alternative, to prevent the problem from occurring, is to enable critical authentication by entering the **dot1x critical {eapol | recovery delay milliseconds}** global configuration command.

Resolved Caveats

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

- [“Resolved Caveats in Cisco IOS Release 12.2\(35\)SE5”](#)
- [“Resolved Caveats in Cisco IOS Release 12.2\(35\)SE”](#)

Resolved Caveats in Cisco IOS Release 12.2(35)SE5

This section describes the caveats that have been resolved in Cisco IOS Release 12.2(35)SE5.

- CSCed87897

The output of the **show ip route** privileged EXEC command now correctly displays the default gateway.

- CSCsh89429

The switch no longer reloads when the **write core** privileged EXEC command is entered when testing a core dump configuration and FTP is selected as the file transfer protocol.

- CSCsi74508

A switch no longer displays this error message when reading from or writing to the configuration file:

```
%DATACORRUPTION-1-DATAINCONSISTENCY: write of 11 bytes to 10 bytes
-Traceback= 0x41186A90 0x411A3960 0x411C1F88 0x413C24B8 0x4031EEDC 0x4032D144
0x411C3974 0x41193D9C 0x4119420C 0x411DF55C 0x411C70AC 0x411E3184 0x425590F4
0x4254BD7C 0x421B5CE0 0x421B5CC4
```

- CSCsi94450

When DHCP snooping is enabled on a VLAN, the broadcast DHCP request is now correctly sent over the trusted port and the connected hosts correctly receive their IP addresses.

Resolved Caveats in Cisco IOS Release 12.2(35)SE

This section describes the caveats that have been resolved in Cisco IOS Release 12.2(35)SE.

- CSCei63394

When an IEEE 802.1x restricted VLAN is configured on a port and a hub with multiple devices are connected to that port, syslog messages are now generated.

This is not a supported configuration. Only one host should be connected to an IEEE 802.1x restricted VLAN port.

- CSCsb11849

When the Control Plane Policing (CoPP) policy is configured to drop packets that have IP options, packets with incorrectly created IP options are no longer ignored.

- CSCsb12598

Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

Cisco IOS is affected by the following vulnerabilities:

- Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
- Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
- Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml>.



Note

Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml>.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml>.

- CSCsb40304

Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

Cisco IOS is affected by the following vulnerabilities:

- Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
- Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
- Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml>.



Note

Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml>.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml>.

- CSCsb56438

An extra index no longer appears in the port table of the ciscoStpExtensions MIB.

- CSCsb74648

When a Cisco device is configured for Network Admission Control and the EAP over UDP port number changes from its default value and then changes back with the *eou* default switch configuration command, the port change now takes effect.

- CSCsb75245

When you configure a Cisco IP Phone to use Network Admission Control, the CDP packet is no longer delayed, and the phone is no longer identified as an agentless host without an identity profile.

- CSCsb81283

MAC address notification traps now work when port security is enabled on the interface.

- CSCsb97854

When a source port for a SPAN session has IEEE 802.1x enabled, Extensible Authentication Protocol over LAN (EAPOL) packets are now visible to the packet sniffing tool.

- CSCsc05371

When you configure a MAC address filter by entering the **mac-address-table static vlan drop** global configuration command, IEEE 802.1X no longer authenticates supplicants using that address. If a supplicant with that address is authenticated, its authorization is revoked.

- CSCsc13467

A switch no longer fails or displays illegal memory access messages during the SNMP Timer process.

- CSCsc29225

When you remove the bridge topology change trap with the **no snmp-server enable traps bridge topologychange** configuration command, the stpx root-inconsistency trap is now active.

- CSCsd08314

When you remove a voice VLAN that has no per-VLAN configuration from a secure port, a `PORT_SECURITY-6-VLAN_REMOVED` message no longer appears.



Note If an address was learned on a VLAN, the error message still appears when that VLAN is aged out or removed. However, this does not affect switch functionality.

- CSCsd92405

Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

Cisco IOS is affected by the following vulnerabilities:

- Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
- Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
- Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml>.



Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml>.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml>.

- CSCsf04754

Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.

The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities.

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0960 has been assigned to these vulnerabilities.

This advisory will be posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20080610-snmpv3.shtml>

Documentation Updates

These sections contain these documentation updates:

- [Update to the Software Configuration Guide](#)
- [Updates to the Command Reference](#)
- [Updates to System Message Guide](#)

Update to the Software Configuration Guide

These sections were added to the “Configuring IEEE 802.1x” chapter:

Using Web Authentication

You can use a web browser to authenticate a client that does not support IEEE 802.1x functionality.

You can configure a port to use only web authentication. You can also configure the port to first try and use IEEE 802.1x authentication and then to use web authorization if the client does not support IEEE 802.1x authentication.

Web authentication requires two Cisco Attribute-Value (AV) pair attributes:

- The first attribute, `priv-lvl=15`, must always be set to `15`. This sets the privilege level of the user who is logging into the switch.
- The second attribute is an access list to be applied for web authenticated hosts. The syntax is similar to IEEE 802.1X per-user ACLs. However, instead of `ip:inacl`, this attribute must begin with `proxyacl`, and the `source` field in each entry must be `any`. (After authentication, the client IP address replaces the `any` field when the ACL is applied.)

For example:

```
proxyacl# 10=permit ip any 10.0.0.0 255.0.0.0
proxyacl# 20=permit ip any 11.1.0.0 255.255.0.0
proxyacl# 30=permit udp any any eq syslog
proxyacl# 40=permit udp any any eq tftp
```



Note The `proxyacl` entry determines the type of allowed network access.

For more information, see the “[Configuring Web Authentication](#)” section on page 20.

Configuring Web Authentication

Beginning in privileged EXEC mode, follow these steps to configure authentication, authorization, accounting (AAA) and RADIUS on a switch before configuring web authentication. The steps enable AAA by using RADIUS authentication and enable device tracking.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	aaa new-model	Enable AAA.
Step 3	aaa authentication login default group radius	Use RADIUS authentication. Before you can use this authentication method, you must configure the RADIUS server. For more information, see Chapter 9, “Configuring Switch-Based Authentication.” The console prompts you for a username and password on future attempts to access the switch console after entering the aaa authentication login command. If you do not want to be prompted for a username and password, configure a second login authentication list: Switch# config t Switch(config)# aaa authentication login line-console none Switch(config)# line console 0 Switch(config-line)# login authentication line-console Switch(config-line)# end
Step 4	aaa authorization auth-proxy default group radius	Use RADIUS for authentication-proxy (auth-proxy) authorization.
Step 5	radius-server host key radius-key	Specify the authentication and encryption key for RADIUS communication between the switch and the RADIUS daemon.
Step 6	radius-server attribute 8 include-in-access-req	Configure the switch to send the Framed-IP-Address RADIUS attribute (Attribute[8]) in access-request or accounting-request packets.
Step 7	radius-server vsa send authentication	Configure the network access server to recognize and use vendor-specific attributes (VSAs).
Step 8	ip device tracking	Enable the IP device tracking table. To disable the IP device tracking table, use the no ip device tracking global configuration commands.
Step 9	end	Return to privileged EXEC mode.

This example shows how to enable AAA, use RADIUS authentication and enable device tracking:

```
Switch(config) configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authentication login default group radius
Switch(config)# aaa authorization auth-proxy default group radius
Switch(config)# radius-server host key key1
Switch(config)# radius-server attribute 8 include-in-access-req
Switch(config)# radius-server vsa send authentication
Switch(config)# ip device tracking
Switch(config) end
```

Beginning in privileged EXEC mode, follow these steps to configure a port to use web authentication:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip admission name rule proxy http	Define a web authentication rule. Note The same rule cannot be used for both web authentication and NAC Layer 2 IP validation.
Step 3	interface interface-id	Specify the port to be configured, and enter interface configuration mode.
Step 4	switchport mode access	Set the port to access mode.
Step 5	ip access-group access-list in	Specify the default access control list to be applied to network traffic before web authentication.
Step 6	ip admission rule	Apply an IP admission rule to the interface.
Step 7	end	Return to privileged EXEC mode.
Step 8	show running-config interface interface-id	Verify your configuration.
Step 9	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure only web authentication on a switch port:

```
Switch# configure terminal
Switch(config)# ip admission name rule1 proxy http
Switch(config)# interface gigabit1/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# ip access-group policy1 in
Switch(config-if)# ip admission rule1
Switch(config-if)# end
```

Beginning in privileged EXEC mode, follow these steps to configure a switch port for IEEE 802.1x authentication with web authentication as a fallback method:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip admission name rule proxy http	Define a web authentication rule.
Step 3	fallback profile fallback-profile	Define a fallback profile to allow an IEEE 802.1x port to authenticate a client by using web authentication.
Step 4	ip access-group policy in	Specify the default access control list to apply to network traffic before web authentication.
Step 5	ip admission rule	Associate an IP admission rule with the profile, and specify that a client connecting by web authentication uses this rule.
Step 6	end	Return to privileged EXEC mode.
Step 7	interface interface-id	Specify the port to be configured, and enter interface configuration mode.
Step 8	switchport mode access	Set the port to access mode.
Step 9	dot1x port-control auto	Enable IEEE 802.1x authentication on the interface.

	Command	Purpose
Step 10	dot1x fallback fallback-profile	Configure the port to authenticate a client by using web authentication when no IEEE 802.1x supplicant is detected on the port. Any change to the fallback-profile global configuration takes effect the next time IEEE 802.1x fallback is invoked on the interface. Note Web authorization cannot be used as a fallback method for IEEE 802.1x if the port is configured for multidomain authentication.
Step 11	exit	Return to privileged EXEC mode.
Step 12	show dot1x interface <i>interface-id</i>	Verify your configuration.
Step 13	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure IEEE 802.1x authentication with web authentication as a fallback method.

```
Switch(config) configure terminal
Switch(config)# ip admission name rule1 proxy http
Switch(config)# fallback profile fallback1
Switch(config-fallback-profile)# ip access-group default-policy in
Switch(config-fallback-profile)# ip admission rule1
Switch(config-fallback-profile)# exit
Switch(config)# interface gigabit1/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x fallback fallback1
Switch(config-if)# end
```

For more information about the **ip admission name** and **dot1x fallback** commands, see the command reference for this release.

Updates to the Command Reference

These commands were added:

- [dot1x fallback](#), page 22
- [fallback profile](#), page 23
- [ip admission](#), page 25
- [ip admission name proxy http](#), page 26
- [show fallback profile](#), page 27

dot1x fallback

Use the **dot1xfallback** interface configuration command on the switch stack or on a standalone switch to configure a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication. To return to the default setting, use the **no** form of this command.

dot1x fallback *profile*

no dot1x fallback

Syntax Description	profile	Specify a fallback profile for clients that do not support IEEE 802.1x authentication.
---------------------------	----------------	--

Defaults No fallback is enabled.

Command Modes Interface configuration

Command History	Release	Modification
	12.2(35)SE	This command was introduced.

Usage Guidelines You must enter the **dot1x port-control** auto interface configuration command on a switch port before entering this command.

Examples This example shows how to specify a fallback profile to a switch port that has been configured for IEEE 802.1x authentication:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# dot1x fallback profile1
Switch(config-fallback-profile)# exit
Switch(config)# end
```

You can verify your settings by entering the **show dot1x [interface interface-id]** privileged EXEC command.

Related Commands	Command	Description
	show dot1x [interface interface-id]	Displays IEEE 802.1x status for the specified port.
	fallback profile	Create a web authentication fallback profile.
	ip admission	Enable web authentication on a port
	ip admission name proxy http	Enable web authentication globally on a switch

fallback profile

Use the **fallback profile** global configuration command on the switch stack or on a standalone switch to create a fallback profile for web authentication. To return to the default setting, use the **no** form of this command.

fallback profile *profile*

no fallback profile

Syntax Description	profile	Specify the fallback profile for clients that do not support IEEE 802.1x authentication.
---------------------------	----------------	--

Defaults No fallback profile is configured.

Command Modes Global configuration

Command History	Release	Modification
	12.2(35)SE	This command was introduced.

Usage Guidelines The fallback profile is used to define the IEEE 802.1x fallback behavior for IEEE 802.1x ports that do not have supplicants. The only supported behavior is to fall back to web authentication.

After entering the **fallback profile** command, you enter profile configuration mode, and these configuration commands are available:

- **ip:** Create an IP configuration.
- **access-group:** Specify access control for packets sent by hosts that have not yet been authenticated.
- **admission:** Apply an IP admission rule.

Examples This example shows how to create a fallback profile to be used with web authentication:

```
Switch# configure terminal
Switch(config)# ip admission name rule1 proxy http
Switch(config)# fallback profile profile1
Switch(config-fallback-profile)# ip access-group default-policy in
Switch(config-fallback-profile)# ip admission rule1
Switch(config-fallback-profile)# exit
Switch(config)# interface gigabitethernet 1/0/1
Switch(config-if)# dot1x fallback profile1
Switch(config-if)# end
```

You can verify your settings by entering the **show running-configuration [interface interface-id]** privileged EXEC command.

Related Commands	Command	Description
	dot1x fallback	Configure a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
	ip admission	Enable web authentication on a switch port
	ip admission name proxy http	Enable web authentication globally on a switch
	show dot1x [interface interface-id]	Displays IEEE 802.1x status for the specified port.
	show fallback profile	Display the configured profiles on a switch.

ip admission

Use the **ip admission** interface configuration command to enable web authentication. You can also use this command in fallback-profile mode. Use the **no** form of this command to disable web authentication.

ip admission rule

no ip admission

Syntax Description

rule	Apply an IP admission rule to the interface.
------	--

Command Modes

Global configuration

Command History

Release	Modification
12.2(35)SE	This command was introduced.

Usage Guidelines

The **ip admission** command applies a web authentication rule to a switch port.

Examples

This example shows how to apply a web authentication rule to a switchport:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip admission rule1
```

This example shows how to apply a web authentication rule to a fallback profile for use on an IEEE 802.1x enabled switch port.

```
Switch# configure terminal
Switch(config)# fallback profile profile1
Switch(config)# ip admission name rule1
Switch(config)# end
```

Related Commands

Command	Description
dot1x fallback	Configure a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
fallback profile	Enable web authentication on a port
ip admission name	Enable web authentication globally on a switch
proxy http	
show ip admission	Displays information about NAC cached entries or the NAC configuration. For more information, see the <i>Network Admission Control Software Configuration Guide</i> on Cisco.com.

ip admission name proxy http

Use the **ip admission name proxy http** global configuration command to enable web authentication. Use the **no** form of this command to disable web authentication.

ip admission name proxy http

no ip admission name proxy http

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	Web authentication is disabled.
-----------------	---------------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.2(35)SE	This command was introduced.

Usage Guidelines	<p>The ip admission name proxy http command globally enables web authentication on a switch.</p> <p>After you enable web authentication on a switch, use the ip access-group in and ip admission web-rule interface configuration commands to enable web authentication on a specific interface.</p>
-------------------------	---

Examples	This example shows how to configure only web authentication on a switchport:
-----------------	--

```
Switch# configure terminal
Switch(config) ip admission name http-rule proxy http
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group 101 in
Switch(config-if)# ip admission rule
Switch(config-if)# end
```

This example shows how to configure IEEE 802.1x authentication with web authentication as a fallback mechanism on a switchport.

```
Switch# configure terminal
Switch(config)# ip admission name rule2 proxy http
Switch(config)# fallback profile profile1
Switch(config)# ip access group 101 in
Switch(config)# ip admission name rule2
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x fallback profile1
Switch(config-if)# end
```

Related Commands	Command	Description
	dot1x fallback	Configure a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
	fallback profile	Create a web authentication fallback profile.
	ip admission	Enable web authentication on a port
	show ip admission	Displays information about NAC cached entries or the NAC configuration. For more information, see the <i>Network Admission Control Software Configuration Guide</i> on Cisco.com.

show fallback profile

Use the **show fallback profile** privileged EXEC command to display the fallback profiles that are configured on a switch.

```
show fallback profile [ append | begin | exclude | include | { [redirect | tee ] url } expression ]
```

Syntax Description		
	 append	(Optional) Append redirected output to a specified URL
	 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	 include	(Optional) Display includes lines that match the specified <i>expression</i> .
	 redirect	(Optional) Copy output to a specified URL.
	 tee	(Optional) Copy output to a specified URL.
	<i>expression</i>	Expression in the output to use as a reference point.
	<i>url</i>	Specified URL where output is directed.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(35)SE	This command was introduced.

Usage Guidelines Use the **show fallback profile** privileged EXEC command to display profiles that are configured on the switch.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show fallback profile** command:

```
switch# show fall profile
Profile Name: dot1x-www
-----
Description      : NONE
IP Admission Rule : webauth-fallback
IP Access-Group IN: default-policy
Profile Name: dot1x-www-lpip
-----
Description      : NONE
IP Admission Rule : web-lpip
IP Access-Group IN: default-policy
Profile Name: profile1
-----
Description      : NONE
IP Admission Rule : NONE
IP Access-Group IN: NONE
```

Related Commands

Command	Description
dot1x fallback	Configure a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
fallback profile	Create a web authentication fallback profile.
ip admission	Enable web authentication on a switch port
ip admission name proxy http	Enable web authentication globally on a switch
show dot1x [interface interface-id]	Displays IEEE 802.1x status for the specified port.

Updates to System Message Guide

This section contains updates to the system message guide.

Error Message DOT1X-5-SECURITY_VIOLATION: Security violation on the interface [chars], new MAC address [enet] is seen.

Explanation A host on the specified interface is trying to access the network or to authenticate in a host mode that does not support the number of hosts attached to the interface. This is a security violation, and the port is put in the error-disabled state.

Recommended Action Ensure that the interface is configured to support the number of attached hosts. Enter the **shutdown** interface configuration command and then the **no shutdown** interface configuration command to restart the port.

Error Message DOT1X_SWITCH-5-ERR_VLAN_EQ_VVLAN: Data VLAN [dec] on port [chars] cannot be equivalent to the Voice VLAN.

Explanation The IEEE 802.1x-assigned VLAN on a port cannot be the same as the voice VLAN. [dec] is the data VLAN ID, and [chars] is the port.

Recommended Action Configure either a different voice VLAN or a different IEEE 802.1x-assigned access VLAN on the interface. The authentication then proceeds normally on the next retry.

Error Message FRNTEND_CTRLR-1-MGR_TXQ_FULL: The front end controller Tx queue reached watermark level

Explanation There are too many messages in the queue between the front-end controller and the switch software.

Recommended Action Try reloading the switch. If this does not resolve the issue, this might be a hardware problem. Contact the Cisco technical support representative.

Error Message GBIC_SECURITY_CRYPT-4-ID_MISMATCH: Identification check failed for GBIC in port [chars]

Explanation The small form-factor pluggable (SFP) module was identified as a Cisco SFP module, but the system could not verify its identity. [chars] is the port.

Recommended Action Ensure that the Cisco IOS software running on the switch supports the SFP module. You might need to upgrade your software. Otherwise, verify that the SFP module was obtained from Cisco or from a supported vendor.

Error Message GBIC_SECURITY_CRYPT-4-UNRECOGNIZED_VENDOR: GBIC in port [chars] manufactured by an unrecognized vendor

Explanation The small form-factor pluggable (SFP) module was identified as a Cisco SFP module, but the switch could not match its manufacturer with one on the known list of Cisco SFP module vendors. [chars] is the port.

Recommended Action Ensure that the Cisco IOS software running on the switch supports the SFP module. You might need to upgrade your software.

Error Message GBIC_SECURITY_CRYPT-4-VN_DATA_CRC_ERROR: GBIC in port [chars] has bad crc

Explanation The small form-factor pluggable (SFP) module was identified as a Cisco SFP module, but it does not have a valid cyclic redundancy check (CRC) in the EEPROM data. [chars] is the port.

Recommended Action Ensure that the Cisco IOS software running on the switch supports the SFP module. You might need to upgrade your software. Even if the switch does not recognize the SFP module, it might still operate properly but have limited functionality.

Error Message PHY-4-UNSUPPORTED_SFP_CARRIER: Unsupported SFP carrier module found in [chars]

Explanation The switch has identified the small form-factor pluggable (SFP) module as an unsupported non-Cisco SFP module. [chars] is the interface.

Recommended Action Remove the unsupported SFP module, and use a supported module.

Error Message PORT_SECURITY-6-ADDR_REMOVED: Address [dec]:[enet] exists on port [chars]. It has been removed from port [chars].

Explanation A routed port is reconfigured as a switch port. The address in the previous switch configuration conflicts with the running configuration and has been deleted. [dec]:[enet] is the MAC address of the port. [chars] is the reconfigured port.

Recommended Action No action is required.

Error Message WCCP-5-SERVICEFOUND: Service [chars] acquired on WCCP Client [IP_address]

Explanation Web Cache Communication Protocol (WCCP) has found a service on the specified WCCP client. [chars] is the name of the service, and [IP_address] is the client IP address.

Recommended Action No action is required.

Error Message WCCP-1-SERVICELOST: Service [chars] lost on WCCP Client [IP_address]

Explanation WCCP has lost the service associated with the specified WCCP client. [chars] is the name of the service, and [IP_address] is the client IP address.

Recommended Action Verify the operational state of the WCCP client.

These system messages were updated in the system message guide:

Error Message EC-5-CANNOT_BUNDLE_LACP: [chars] is not compatible with aggregators in channel [dec] and cannot attach to them ([chars]).

Explanation The port has different port attributes than the port channel or ports within the port channel. [chars] is the incompatible port. [chars] is the short interface name, such as Gi1/0/1 on a Catalyst 3750 switch, [dec] is the channel group number, and the last [chars] is the reason.

Recommended Action For the port to join the bundle, change the port attributes so that they match the port.

Error Message EC-5-DONTBNL: [chars] suspended: incompatible remote port with [chars]

Recommended Action The configuration of the remote port differs from the configuration of other remote ports in the bundle. A port can only join the bundle when its global configuration and the configuration of the remote port are the same as other ports in the bundle. The first [chars] is the suspended local interface, and the second [chars] is the local interface that is already bundled.

Error Message PORT_SECURITY-6-VLAN_REMOVED: VLAN [int] is no longer allowed on port [chars]. Its port security configuration has been removed.

Explanation A configured VLAN has been excluded either due to a port-mode change or an allowed VLAN list change and is removed from the configuration. [int] is the VLAN ID, and [chars] is the switch port assigned to the VLAN.

Recommended Action No action is required.

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

You can order printed copies of documents with a DOC-xxxxxx= number from the Cisco.com sites listed in the “Cisco.com” section on page Boilerplate 2.

These documents provide complete information about the Cisco Catalyst Blade Switch 3040 for FSC:

- *Cisco Catalyst Blade Switch 3040 for FSC Getting Started Guide* (order number DOC-7817759=)
- *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3040 for FSC* (order number DOC-7817760=)
- *Release Notes for the Cisco Catalyst Blade Switch 3040 for FSC, Cisco IOS Release 12.2(35)SE* (not orderable but available on Cisco.com)
- *Cisco Catalyst Blade Switch 3040 for FSC Software Configuration Guide* (not orderable but available on Cisco.com)
- *Cisco Catalyst Blade Switch 3040 for FSC Command Reference* (not orderable but available on Cisco.com)
- *Cisco Catalyst Blade Switch 3040 for FSC System Message Guide* (not orderable but available on Cisco.com)

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

<http://www.cisco.com/univercd/home/home.htm>

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

If you do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

<http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

To register as a Cisco.com user, go to this URL:

<http://tools.cisco.com/RPF/register/register.do>

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Support Website

The Cisco Support website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

<http://www.cisco.com/en/US/support/index.html>

Access to all tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

**Tip****Displaying and Searching on Cisco.com**

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing **F5**.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411

Australia: 1 800 805 227

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

<http://www.cisco.com/offer/subscribe>

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:
<http://www.cisco.com/go/guide>
 - Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
 - Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
 - *Internet Protocol Journal* is a quarterly journal published by Cisco for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:
<http://www.cisco.com/ipj>
 - Networking products offered by Cisco, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
 - Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
 - “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:
<http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm>
 - World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>
-

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0609R)

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

© 2007 Cisco Systems, Inc. All rights reserved.

