IBM

@server

# Cisco Systems Intelligent Gigabit Ethernet Switch Modules for the IBM @server BladeCenter

# Release Notes

Cisco IOS Release 12.1(22)EA6

**Note:** Before using this information and the product it supports, read the general information in Appendix B, "Getting Help and Technical Assistance" and Appendix C, "Notices."

**Ninth Edition (November 2005)**

# Release Notes for the Cisco Systems Intelligent Gigabit Ethernet Switch Modules for the IBM eServer BladeCenter

**Revised November 2, 2005**

This document provides important information about the Cisco Systems Intelligent Gigabit Ethernet Switch Modules, hereafter referred to as *the switch*, running Cisco IOS Release 12.1(22)EA6.

Review the new software features, open caveats, and resolved caveats sections for information specific to your switch. The information in this document refers to all the switches, unless otherwise noted.

These release notes include important information about this release and any limitations, restrictions, and caveats that apply to it. To verify that these are the correct release notes for your switch:

- If your switch is running, you can use the **show version** user 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 Cisco IOS version.

For the complete list of switch documentation, see the "Related Documentation" section on page 19.

## Contents

This information is in the release notes:

# System Requirements

The system requirements for this release are described in these sections:



## Hardware Supported

These switches are supported by Cisco IOS Release 12.1(22)EA6:

- Cisco Systems Intelligent Gigabit Ethernet Switch Module for the IBM eServer BladeCenter
- Cisco Systems Intelligent Gigabit Fiber Ethernet Switch Module for the IBM eServer BladeCenter

## Device Manager System Requirements

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



### 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. The device manager verifies the browser version when starting a session to ensure that the browser is supported.

**Note** The device manager does not require a plug-in.

*Table 2 Supported Operating Systems and Browsers*

| Operating System | Minimum Service Pack or Patch | Microsoft Internet Explorer[1] | Netscape Navigator |
|---|---|---|---|
| Windows 98 | None | 5.5 or 6.0 | 7.1 |
| Windows NT 4.0 | Service Pack 6 or later | 5.5 or 6.0 | 7.1 |
| 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

Before downloading software, read this section for important information. This section describes these procedures for downloading software:

- "Finding the Software Version and Feature Set" section on page 3
- "Deciding Which Files to Download from the Web" section on page 4
- "Recovering from Software Failure" section on page 6

When you upgrade a switch, the switch continues to operate while the new software is copied to flash memory. If flash memory has enough space, the new image is copied to the selected switch but does not replace the running image until you reboot the switch. If a failure occurs during the copy process, you can still reboot your switch by using the old image. If flash memory does not have enough space for two images, the new image is copied over the existing one. Features provided by the new software are not available until you reload the switch.

If a failure occurs while copying a new image to the switch, and the old image has already been deleted, see the "Recovering from Corrupted Software" section in the "Troubleshooting" chapter of the software configuration guide for this release.

**Caution** Do not power cycle the switch while you are copying an image to the switch. If a power failure occurs while you are copying the software image to the switch, and there are no other images on the switch, see the "Troubleshooting" chapter in the software configuration guide for detailed recovery procedures.

## Finding the Software Version and Feature Set

The 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** user EXEC command to see the software version that is running on your switch. In the display, check the line that begins with `System image file is`. This line shows the directory name in flash memory where the image is stored.

Although the **show version** output always shows the software version running on the switch, the model name shown at the end of this display is the factory configuration and does not change if you upgrade the software image.

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 Download from the Web

To determine the latest level of the Cisco IOS software that is available from IBM, follow these steps:

**Step 1** Go to http://www.ibm.com/bladecenter.

**Step 2** At the top of the window, click **Support & Downloads**, and the window refreshes.

**Step 3** In the Support by Servers section, click **Servers**, and the window refreshes.

**Step 4** Click on **BladeServers**, and the window refreshes.

**Step 5** Click **Go**, and the window refreshes.

**Step 6** Click **Download**, and the window refreshes.

**Step 7** Click **BIOS, drivers, and firmware for Windows 2000**, and the window refreshes.

**Step 8** In the Refine Results drop-down box, click **Networking**, and the window refreshes.

**Step 9** Click on the Cisco software release, and follow the instructions.

The upgrade procedures in these release notes describe how to perform the upgrade by using a combined tar file. This file contains both the Cisco IOS image file and the embedded device manager files. You must use the combined tar file to upgrade the switch through the device manager. The tar file is an archive file from which you can extract files by using the **archive download-sw** command.

Table 3 lists the software filenames for this release.

***Table 3 Cisco IOS Software Image Files for This Release***

| Filename | Description |
|---|---|
| cigesm-i6q4l2-tar.121-22.EA6.tar | Noncryptographic Cisco IOS 12.1(22)EA6 image and device manager files |
| cigesm-i6k212q4-tar.121-22.EA6.tar | Cryptographic Cisco IOS 12.1(22)EA6 image and device manager files |

# Upgrading a Switch by Using the CLI

The upgrade procedure in this section describes how to perform the upgrade by using a combined tar file. The procedure assumes that you have already downloaded the tar file for this release from ibm.com to your TFTP server or management station. The tar file is an archive file from which you can extract files by using the **archive download-sw** command.

For information about where to access the tar files on ibm.com and the names of the tar files for this release, see the "Deciding Which Files to Download from the Web" section on page 4.

**Caution** Do not power cycle the switch while you are copying an image to the switch. If a power failure occurs while you are copying the software image to the switch, call your technical support representative immediately.

The upgrade procedure uses the **archive download-sw** privileged EXEC command to automatically extract and download the images to the switch. The **archive download-sw** command automatically deletes the old version and copies the new version to flash memory if the flash memory does not have space to store the old and new versions simultaneously. The **archive download-sw** command initiates this process:

- It verifies adequate space on the flash memory before downloading the new image.
- If there is insufficient space on the flash memory to hold both the old and the new images, it deletes the old image. The image is always stored in a subdirectory on the flash memory. The subdirectory name is the same as the image release name, for example cigesm-i6q4l2-tar.121-22.AY.tar.
- After the new image is downloaded, it automatically sets the BOOT environment variable. You do not have to change the names of old file names to new file names.
- If you enter the command with the **/reload** or the **/force-reload** option, it automatically reloads the switch after the upgrade.

For more information on using these commands, see the command reference for this release.

Follow these steps to upgrade the switch software by using the CLI:

**Step 1** If your PC or workstation cannot act as a TFTP server, copy the file to a TFTP server to which you have access.

**Step 2** Access the CLI by starting a Telnet session or by connecting to the switch service port.

To start a Telnet session on your PC or workstation, enter this command:

```
server% telnet switch_ip_address
```

Enter the Telnet username and password if you are prompted to do so.

**Step 3** Enter privileged EXEC mode:

```
switch> enable
switch#
```

Enter the password if you are prompted to do so.

**Step 4** Display the name of the running (default) image file (BOOT path-list). This example shows the name in italic:

```
switch# show boot
BOOT path-list:    flash:current_image
Config file:       flash:config.text
Enable Break:      1
Manual Boot:       no
HELPER path-list:
NVRAM/Config file
buffer size: 32768
```

**Step 5** If there is no software image defined in the BOOT path-list, enter **dir flash:** to display the contents of flash memory.

**Step 6** Enter the **archive download-sw /reload** command.

**Step 7** Press **Return** to confirm the reload.

Your Telnet session ends when the switch resets.

**Step 8** After the switch reboots, use Telnet to return to the switch, and enter the **show version** user EXEC command to verify the upgrade procedure. If you have a previously opened browser session to the upgraded switch, close the browser, and start it again to ensure that you are using the latest HTML files.

## Recovering from Software Failure

If the software fails, you can reload the software. For detailed recovery procedures, see the "Troubleshooting" chapter in the software configuration guide for your switch.

# Installation Notes

Use the BladeCenter Management Module web page to assign IP information to the switch. For more information, refer to the Cisco Systems Intelligent Gigabit Ethernet Switch Module for the IBM eServer BladeCenter Installation Guide or the Cisco Systems Intelligent Gb Fiber Ethernet Switch Module for the IBM eServer BladeCenter Installation Guide.

# New Features

These sections describe the new supported hardware and the new software features provided in this release:


- "New Hardware Features" section on page 6
- "New Software Features" section on page 6


## New Hardware Features

For a complete list of supported hardware, see the "Hardware Supported" section on page 2.

## New Software Features

This release contains these new software features and enhancements:

- Supports multiple management interfaces, each with a unique IP address and VLAN assignment.
- 4095 Vlan ID Serial over LAN (SOL) support so that customers can communicate with the processor blades without having to configure a special VLAN on the switch. The SOL function defaults to Vlan ID 4095, with no additional customer configuration.
- IEEE 802.1x with wake-on-LAN to power on dormant PCs by a receipt of a specific Ethernet frame.

# Limitations and Restrictions

You should review this section before you begin working with the switches. 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.

**Note** These limitations and restrictions apply to all switches unless otherwise noted.

These sections describe the limitations and restrictions:


- "Cisco IOS Limitations and Restrictions" section on page 7
- "Device Manager Limitations and Restriction" section on page 13


## Cisco IOS Limitations and Restrictions

These limitations and restrictions apply to the Cisco IOS configuration:

- Root guard is inconsistent when configured on a port that is in the STP blocked state at the time of configuration. (CSCdp85954)
- Aging of dynamic addresses does not always occur exactly after the specified aging time elapses. It might take up to three times this time period before the entries are removed from the table. (CSCdr96565)
- Internal loopback in half-duplex mode causes input errors. We recommend that you configure the PHY to operate in full duplex before setting the internal loopback. (CSCds20365)
- A source-based distribution port group does not share the broadcast with all the group members. When the destination of the packets is a broadcast, or an unknown unicast, or a multicast, the packets are forwarded on only one port member of a port group, not being shared among all members of the port group. (CSCdt24814)
- When you enter the **show controllers ethernet-controller** *interface-id* or **show interfaces** *interface-id* **counters** privileged EXEC commandand a large number of erroneous frames are received on an interface, the receive-error counts might be smaller than the actual values, and the receive-unicast frame count might be larger than the actual frame count. (CSCdt27223)
- Two problems occur when a switch is in transparent mode:
  - If the switch is a leaf switch, any new VLANs added to it are not propagated upstream through VTP messages. As a result, the switch does not receive flooded traffic for that VLAN.
  - If the switch is connected to two VTP servers, it forwards their pruning messages. If the switch has a port on a VLAN that is not requested by other servers through their pruning messages, it does not receive flooded traffic for that VLAN.

  There is no workaround. (CSCdt48011)
- The receive count output for the **show controllers ethernet-controller** *interface-id* privileged EXEC command shows the incoming packets count before the ASIC either drops or allows the packet or not. Therefore, for ports in the STP blocking states, even though the receive count shows incoming frames, the packet is not forwarded to the other port. (CSCdu83640)
- In some network topologies, when UplinkFast is enabled on all switches but BackboneFast is not enabled on all switches, a temporary loop might occur when the STP root switch is changed.

  The workaround is to enable BackboneFast on all switches. (CSCdv02941)

- At times, the Window XP pop-up window might not appear while authenticating a client (supplicant) because the user information is already stored in Windows XP. However, the Extensible Authentication Protocol over LAN (EAPOL) response to the switch (authenticator) might have an empty user ID that causes the IEEE 802.1x port to be unauthenticated.

  The workaround is to manually re-initiate authentication by either logging off or by detaching the link and then reconnecting it. (CSCdv19671)

- If two switches are connected and access ports connect two VLANs whose VLAN IDs are separated by the correct multiple of 64, the two switches might use the same bridge ID in the same spanning-tree instances. This might cause a loss of connectivity in the VLANs as the spanning tree blocks the ports that should be forwarding.

  The workaround is to not cross-connect VLANs. For example, do not use an access port to connect VLAN 1 to VLAN 65 on either the same switch or from one switch to another switch. (CSCdv27247)

- You can configure up to 256 multicast VLAN registration (MVR) groups by using the **mvr vlan group** interface configuration command, but only 255 groups are supported on a switch at one time. If you statically add a 256th group, and 255 groups are already configured, the switch continues trying (and failing) to add the new group.

  The workaround is to set the mode to **dynamic** for switches that are connected to IGMP-capable devices. The new group can join the multicast stream if another stream is dynamically removed from the group. (CSCdv45190)

- A command switch can discover only the first Catalyst 3550 switch if the link between the Catalyst 3550 switches is an IEEE 802.1Q trunk and the native VLAN is not the same as the management VLAN of the switch or if the link between the Catalyst 3550 switches is an Inter-Switch Link (ISL) trunk and the management VLAN is not VLAN 1.

  The workaround is to connect Catalyst 3550 switches by using the access link on the command switches management VLAN or to configure an IEEE 802.1Q trunk with a native VLAN that is the same as the management VLAN of the command switch. (CSCdv49871)

- The **ip http authentication enable** global configuration command is not saved to the configuration file. Therefore, this configuration is lost after a reboot.

  The workaround is to manually enter the command again after a reboot. (CSCdv67047)

- If a port is configured as a secure port with the violation mode as restrict, the secure ports might process packets even after the maximum number of MAC addresses is reached, but those packets are not forwarded to other ports. (CSCdw02638)

- You can apply ACLs to a management VLAN or to any traffic that is going directly to the CPU, such as SNMP, Telnet, or web traffic. For information on creating ACLs for these interfaces, see the "Configuring IP Services" section of the *Cisco IOS IP and IP Routing Configuration Guide for Cisco IOS Release 12.1* and the *Cisco IOS IP and IP Routing Command Reference for Cisco IOS Release 12.1*.

- The SSH feature uses a large amount of switch memory, which limits the number of VLANs, trunk ports, and cluster members that you can configure on the switch. Before you download the cryptographic software image, your switch configuration must meet these conditions:
  - The number of trunk ports multiplied by the number of VLANs on the switch must be less than or equal to 128. These are examples of switch configurations that meet this condition:

    If the switch has 2 trunk ports, it can have up to 64 VLANs.

    If the switch has 32 VLANs, it can have up to 4 trunk ports.

  If your switch has a saved configuration that does not meet these conditions and you upgrade the switch software to the cryptographic software image, the switch might run out of memory. If this happens, the switch does not operate properly. For example, it might continuously reload.

  If the switch runs out of memory, this message appears:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of (number_of_bytes) bytes failed ...
  ```

  The workaround is to check your switch configuration and to ensure that it meets the previous conditions. (CSCdw66805)

- When you use the **policy-map** global configuration command to create a policy map and do not specify any action for a class map, the association between that class map and policy map is not saved when you exit **policy-map** configuration mode.

  The workaround is to specify an action in the policy map. (CSCdx75308)

- When a community string is assigned by the cluster command switch, you cannot get any dot1dBridge MIB objects by using a community string with a VLAN entity from a cluster member switch.

  The workaround is to manually add the cluster community string with the VLAN entity on the member switches for all active VLANs shown in the **show spanning-tree summary** display. This is an example of such a change, where *cluster member 3* has spanning tree on *vlan 1-3,* and the cluster commander community string is *public@es3*.

  ```
  Switch(config)# snmp community public@es3@1 RO
  Switch(config)# snmp community public@es3@2 RO
  Switch(config)# snmp community public@es3@3 RO
  ```

  (CSCdx95501)

- When the Internet Group Management Protocol (IGMP) Immediate Leave is configured, new ports are added to the group membership each time a join message is received, and ports are pruned (removed) each time a leave message is received.

  If the join and leave messages arrive at high rate, the CPU can become busy processing these messages. For example, the CPU usage is approximately 50 percent when 50 pairs of join and leave messages are received each second. Depending on the rate at which join and leave messages are received, the CPU usage can go very high, even up to 100 percent, as the switch continues processing these messages.

  The workaround is to only use the Immediate Leave processing feature on VLANs where a single host is connected to each port. (CSCdx95638)

- In a Remote Switched Port Analyzer (RSPAN) session, if at least one switch is used as an intermediate or destination switch *and* if traffic for a port is monitored in both directions, traffic does not reach the destination switch.

  These are the workarounds:

  - Use a Catalyst 3550 or Catalyst 6000 switch as an intermediate or destination switch.
  - Monitor traffic in only one direction if a switch module is used as an intermediate or destination switch. (CSCdy38476)

- If you assign a nonexistent VLAN ID to a static-access EtherChannel by setting the ciscoVlanMembershipMIB:vmVlan object, the switch does not create the VLAN in the VLAN database. (CSCdy65850)
- When you configure a dynamic switch port by using the **switchport access vlan dynamic** interface configuration command, the port might allow unauthorized users to access network resources if the interface changes from access mode to trunk mode through Dynamic Trunking Protocol (DTP) negotiation.

  The workaround is to configure the port as a static access port. (CSCdz32556)

- The output from the **show stack** privileged EXEC command might show a large number of false interrupts.

  There is no workaround. The number of interrupts does not affect the switch functionality. (CSCdz34545)

- If you configure a static secure MAC address on an interface before enabling port security on the interface, the same MAC address is allowed on multiple interfaces. If the same MAC address is added on multiple ports before enabling port security and port security is later enabled on those ports, only the first MAC address can be added to the hardware database. If port security is first enabled on the interface, the same static MAC address is not allowed on multiple interfaces. (CSCdz74685)
- If you press and hold the spacebar while the output of any **show** user EXEC command is being displayed, the Telnet session stops, and you can no longer communicate with the management VLAN.

  These are the workarounds:

  - Enter the show commands from privileged EXEC mode, and use this command to set the terminal length to zero:

    ```
    switch# terminal length 0
    ```

  - Open a Telnet session directly from a PC or workstation to the switch.
  - Do not hold down the spacebar while scrolling through the output of a **show** user EXEC command. Instead, slowly press and release the spacebar. (CSCea12888)

- When you connect a switch to another switch through a trunk port and the number of VLANs on the first switch is lower than the number on the connected switch, interface errors are received on the management VLAN of the first switch.

  The workaround is to match the configured VLANs on each side of the trunk port. (CSCea23138)

- When you enable Port Fast on a static-access port and then change the port to dynamic, Port Fast remains enabled. However, if you change the port back to static, Port Fast is disabled.

  The workaround is to configure Port Fast globally by using the **spanning-tree portfast** global configuration command. (CSCea24969)

- When using the SPAN feature, the monitoring port receives copies of sent and received traffic for all monitored ports. If the monitoring port is oversubscribed, it will probably become congested. This might also affect how one or more of the monitored ports forwards traffic.
- If there is not a good distribution of MAC addresses on a port channel, the switch might drop packets even though the port-channel has not reached 100 percent utilization.

  The workaround is to use a different load balancing method (for example, use destination-based forwarding instead of source-based forwarding). (CSCeb75386)
- If the switch has learned over 4000 MAC addresses, the **clear mac address-table dynamic** user EXEC command does not clear all of the addresses from the MAC address table.

  The workaround is to repeatedly enter the **clear mac address-table dynamic** user EXEC command until the address table is cleared. (CSCec02055)
- Port security is not supported on the internal 100 Mbps management module ports (ports 15 and 16). Preventing port security on these ports prevents the blocking of communication between the management module and the switch. (CSCec10814)
- After a topology change in STP, some terminals connected to the management VLAN can transfer data because the affected switch ports start forwarding before they move to the forwarding state.

**Note** If the terminal does not belong to management VLAN, this failure does not occur.

  The workaround is to place the ports in static-access mode for a single VLAN if the topology supports this configuration. (CSCec13986)
- The output of the **show flowcontrol** user EXEC command incorrectly shows that the switch is not receiving and sending pause frames.

  The workaround is to use the **show controllers ethernet-controller** privileged EXEC command to display the sent and received pause packets for a specific port. (CSCec74979)
- If the internal 100 Mbps management module ports (ports 15 and 16) and the external 10/100/1000 ports (ports 17 to 20) are members of a VLAN or multiple VLANs, the spanning-tree states incorrectly show that a Layer 2 loop has occurred. In reality, there is no STP loop. (CSCed03370)
- When QoS and Differentiated Services Code Point (DSCP) marking are enabled on a switch, ports 8, 16, 24, 32, 40, and 48 do not mark the correct DSCP values when sending frames.

  There is no workaround. (CSCed11617)
- The Ethernet ports on the management module have a fixed static trunk configuration. This configuration cannot be changed. IP phones should not be connected to these management module ports. (CSCed11638)
- The monitor session is placed in *inactive state* if a port is configured to be a Switched Port Analyzer (SPAN) destination port in a SPAN session and if a source port is not configured. While in this state, the source port cannot send and receive traffic, and no address learning occurs on the destination port. (CSCed20563)

  These are the workarounds:
  - Identify a source port for the SPAN session.
  - Disable the SPAN session, and remove the designation of destination port for the port.
  - Use the **shutdown** and **no shutdown** interface configuration commands on the designated destination port.

- Note that the switch default native vlan is VLAN 2, *not* VLAN 1, on the switch external 10/100/1000 ports (ports 17 to 20). The native VLAN of a trunk interface can be removed from the allowed VLAN list. This can affect IP connectivity to the switch management VLAN.

  The workaround is to add the native VLAN back to the allowed VLAN list on the trunk interface. (CSCed25956)

- 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 occurs only when the switch is receiving frames.

  The workaround is to configure the port for 1000 Mbps and full duplex or to connect a hub or a nonaffected device to the switch. (CSCed39091)

- If the switch is running IEEE 802.1w rapid STP (RSTP) mode and a directly connected switch is running IEEE 802.1D per-VLAN spanning-tree plus (PVST+), the switch runs PVST+ as expected. However, if the connected switch changes its configuration to RSTP, the switch continues to send IEEE 802.1D BPDUs instead of sending IEEE 802.1w BPDUs.

  The workaround is to use the **clear spanning-tree detected-protocols** privileged EXEC command to restart the protocol migration process (force the renegotiation with neighboring switches). (CSCed40295)

- All unknown unicast and broadcast traffic in an EtherChannel are sent to the port configured as the designated port. If this is the only type of traffic on the EtherChannel, it could reduce the aggregate bandwidth and speed on this port. (CSCed47701)

- When using the **police** policy-map class configuration command on Gigabit-capable Ethernet ports, a value less than 8192 can cause the service policy configuration to fail.

  The workaround is to enter a burst-byte value that is greater than or equal to 8192. (CSCed63013)

- If a switch receives STP packets and non-STP packets that have a CoS value of 6 or 7 and all of these packets belong to the same management VLAN, a loop might occur.

  These are the workarounds:

  - Change the CoS value of the non-STP packets to a value other than 6 or 7.
  - If the CoS value of the non-STP packets *must* be 6 or 7, configure these packets to belong to a VLAN other than the management VLAN. (CSCed88622)

- If the switch does not receive traffic from stations in the network, it prematurely removes and then re-adds their dynamic MAC addresses from the MAC address table. This causes temporary flooding when the switch receives a packet for the affected addresses.

  There is no workaround. (CSCed92062)

- Using the **spanning-tree bpduguard enable** interface configuration command on the internal management module ports (ports 15 and 16) might change the port state to error -disabled. Because the switch does not allow the administrative state on the management module ports to be changed through the CLI, HTTP, or SNMP, the internal management module port remains in the error-disabled state. An entry in the system message log is added.

  This problem only occurs when there are two switches in the BladeCenter chassis. The first switch sends out the BPDU packet on its interface, and it is received by the second switch being monitored. If there are no other switches present in the chassis, the interface does not go into error-disabled state.

  The workaround is to reboot the switch after disabling BPDU guard on the switch or on the internal management module ports. Make sure that the saved configuration for the switch does not have BPDU guard enabled. (CSCee27729)

- When a PC is attached to a switch through a hub, is authenticated on an IEEE 802.1x multiple-hosts port, is moved to another port, and is then attached through another hub, the switch does not authenticate the PC.

  The workaround is to decrease the number of seconds between re-authentication attempts by entering the **dot1x timeout reauth-period** *seconds* interface configuration command. (CSCeg41561)

- Certain combinations of features create conflicts with the port security feature. In Table 4, *No* means that port security cannot be enabled on a port if the referenced feature is also running on the same port. *Yes* means that both port security and the referenced feature can be enabled on the same port at the same time.

***Table 4 Port Security Incompatibility with Other Switch Features***

| | |
|---|---|
| DTP[1] port[2] | No |
| Trunk port | No |
| Dynamic-access port[3] | No |
| SPAN source port | Yes |
| SPAN destination port | No |
| EtherChannel | No |
| Protected port | Yes |
| IEEE 802.1x port | Yes |

1. DTP = Dynamic Trunking Protocol
2. A port configured with the **switchport mode dynamic** interface configuration command
3. A VLAN Query Protocol (VQP) port configured with the **switchport access vlan dynamic** interface configuration command

## Device Manager Limitations and Restriction

These are the device manager limitations and restrictions:

- Clustering is not supported in releases later than Cisco IOS 12.1(14)AY4.
- When you are prompted to accept the security certificate and you click *No*, you see only 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 important notes apply to all switches unless otherwise noted.

This section describes important informations related to this release:


- "Cisco IOS Notes" section on page 14
- "Device Manager Notes" section on page 14

# Cisco IOS Notes

These are the Cisco IOS configuration notes related to this release:

- IGMP filtering controls only group specific query and membership reports, including join and leave reports. It does not control general IGMP queries.
- When an IEEE 802.1x-authenticated client is disconnected from an IP phone, hub, or switch and does not send an EAPOL-Logoff message, the switch interface does not change to the unauthorized state. If this happens, it can take up to 60 minutes for the interface to change to the unauthorized state when the re-authentication time is the default value (3600 seconds).

  The workaround is to change the number of seconds between re-authentication attempts by using the **dot1x timeout re-authperiod** *seconds* global configuration command. (CSCdz38483)
- The guest VLAN might not assign a DHCP address to some clients. This is a problem with the IEEE 802.1x client, not with the switch.

  The workaround is to either release and renew the IP address or to change the default timers. These examples show typical interface timer changes:

  ```
  dot1x timeout quiet-period 3
  dot1x timeout tx-period 5
  ```
- The **transmit-interface** *type number* interface configuration command is not supported.

# Device Manager Notes

These notes apply to the device manager:

- We recommend this browser setting to speed up the time to display the device manager from Microsoft Internet Explorer.

  From Microsoft Internet Explorer:

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

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

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

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

# Open Caveats

These are the caveats in this release.



## Open Cisco IOS Caveats

These are the open Cisco IOS configuration caveats:

- CSCed89186

  If the STP root port changes on the switch, the connections between the switch and the internal 100 Mbps management module ports (ports 15 and 16) do not immediately change to the forwarding state. They remain in the listening state for a few seconds, during which time any traffic between the switch and management module is lost. This occurs if all of these conditions exist:

  - The switch is in IEEE 802.1w rapid STP (RSTP) mode.
  - An EtherChannel is configured between the switch external ports and any directly connected switches.
  - The STP root port is part of the EtherChannel group.

  There is no workaround.

- CSCeg09032

  Open Shortest Path First (OSPF) routes might not appear in the routing table after a topology change if Incremental SPF (iSPF) is enabled.

  The workaround is to disable iSPF.

- CSCeg71620

  Downstream interfaces in a link-state group that are added to an EtherChannel group do not recover their link state when the link-state group is disabled. The correct behavior is for the link state of all downstream interfaces to recover when link-state tracking is disabled for the group.

  These are the workarounds:

  - Remove the downstream interfaces from the link-state group.
  - Remove the downstream interfaces from the EtherChannel group. Downstream interfaces in an EtherChannel group are not supported.

- CSCeg72946

  Downstream interfaces that are members of a link-state group can be incorrectly placed in an *up* state when only one upstream interface is active and this upstream interface is made the destination interface for a local SPAN session.

  The workaround is to disable the link-state group or to remove the interface from the link-state group.

- CSCeh28776

  In the device manager express setup page, Telnet access is shown as disabled. Telnet access is enabled on the device by configuring the **username** and then **login local** on the vty lines.

  The workaround is to use the CLI to check for Telnet status or to configure passwords on vty lines to enable Telnet access.

- CSCeh45771

  When the multicast traffic for a group enters the switch it is directed to the interface that joined the group entering the **ip igmp join** interface configuration command, but not to the interface with the static multicast MAC address. This happens when a multicast router is deleted after at least one other client has entered the **ip igmp join** interface configuration command on another interface where IGMP snooping is configured and another multicast router is statically configured or learned.

  The workaround is to reconfigure the static multicast router.

- CSCeh58774

  The duplex setting shown by the device manager for an Ethernet interface is not the same as the duplex setting in the running configuration. This occurs when you change the only duplex setting on the device manager from Auto to Full. The speed setting remains Auto. When the device manager page is refreshed after the configuration change, the duplex setting is reported as Auto.

  The workaround is to configure the Ethernet interface at 10, 100, or 1000 Mbps, remove the full duplex setting on the Ethernet interface and let the duplex return to Auto. If you had configured full duplex because the Ethernet interface was autonegotiating to half duplex, configure the speed and duplex settings on both link partners.

- CSCsb82422

  The switch does not forward an IEEE802.1x request that has *null* credentials.

  There is no workaround.

- CSCsb82459

  When a supplicant is IEEE 802.1x-capable and also performs DHCP, the switch might send an interim update before DHCP is complete but after an EAP-Success message is sent. When this happens, the interim update might be inaccurate.

  There is no workaround.

# Resolved Cisco IOS Caveats

These are the resolved caveats:

- CSCeg15130

  If multiple switches are configured in a multicast television application with Multicast VLAN Registration (MVR) is enabled and MVR ports statically configured, IGMP leave messages are no longer sent to the router, and the multicast stream to the set-top boxes is not disrupted.

- CSCeg53741

  If frame sizes larger than 1518 bytes are received and the system MTU is configured as 1530 bytes, the counters no longer display the packets as *giants*.

- CSCeg52581

  If you start a session on a switch cluster member by using the **rcommand** user EXEC command, the allowable commands that you enter in the rcommand session now depend on the respective authorization status.

- CSCeg57925

  The switch no longer stops if a port that is assigned to the management VLAN does not have a corresponding access VLAN.

- CSCeg58877

  If a switch uses rapid per-VLAN spanning tree plus (rapid PVST+), a loop no longer occurs when you reconfigure the allowed VLANs on a trunk and remove VLAN 1 from the trunk.

- CSCeg05952

  When the destination-MAC address for data packets is statically configured in a logical EtherChannel port group, the egress traffic on the EtherChannel group no longer uses the default port instead of following the configured load-balancing scheme.

- CSCeg09791

  When you configure an interface for trust CoS and CoS-to-DSCP mapping, the DSCP values of the untagged IP packets received on the interface are now modified as expected.

- CSCeg12120

  When packets matching the permitted UDP fields are attached on an ingress interface, Layer 4 ACLs no longer fail, and Ethernet packets matching the UDP fields are not dropped.

- CSCeh28757

  CiscoView can now distinguish between the switch deployed in the BladeCenter and the BladeCenter T-type chassis.

- CSCeh58797

  If you connect a router FE port to the external port of the switch and set the router FE port to fixed 100 M and half-duplex, the switch negotiates a link to auto-100 M and auto-half duplex.

- CSCeh77474

  On the external Ethernet interfaces of the switch (Gi0/17 - Gi0/20), the LED no longer remains on when the switch has put the Ethernet interface in a shutdown state.

- CSCei13927

  When the management VLAN for the switch is greater than 255, IP communication is nolonger lost. This only effects the IP communication to the switch, not the Ethernet data being switched from data port to data port. This will occur when the VLAN ID of the management VLAN is changed from some number less than 256 to a number greater than 255.

- CSCei61732

  Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml.

- CSCei77627

  Server Blades no longer fail to detect an Ethernet link-down event from the switch. This was on the internal Ethernet interfaces (Gi0/1 to Gi0/14). When the switch brings down the Ethernet interface to the Server Blade, the Server Blade can adequately detect this, and keeps the link as Ethernet link-up.

- CSCei22387

  CDP and VTP protocols no longer fail when trunk ports are not members of VLAN 1.

- CSCsb79318

  if the re-authentication timer and re-authentication action is downloaded from the RADIUS server using the Session-Timeout and Termination-Action RADIUS attributes, the switch performs the termination action even when the port is not configured with the **dot1x timeout reauth server** global configuration command and uses the Termination-Action downloaded from a RADIUS server as part of IEEE 802.1x authorization.

  The workaround is to remove the Termination-Action attribute from the IEEE 802.1x policy on the RADIUS server if **dot1x timeout reauth server** is not configured on the port.

# Related Documentation

In addition to this document, the following related documentation comes with the switch modules:

- *Cisco Systems Intelligent Gigabit Ethernet Switch Modules for the IBM eServer BladeCenter Software Configuration Guide*

  This Cisco document is in PDF format on the *IBM BladeCenter Documentation CD*. It has software configuration information for the switch modules. It provides:

  - Configuration instructions
  - Information about features
  - Information about getting help
  - Guidance for planning, implementing, and administering LAN operating system software
  - Usage examples
  - Troubleshooting information

- *Cisco Systems Intelligent Gigabit Ethernet Switch Modules for the IBM eServer BladeCenter System Command Reference*

  This document is in PDF format on the *IBM BladeCenter Documentation CD*. It includes:

  - Command-line interface (CLI) modes
  - CLI commands and examples
  - Syntax description
  - Defaults
  - Command history
  - Usage guidelines
  - Related commands

- *Cisco Systems Intelligent Gigabit Ethernet Switch Modules for the IBM eServer BladeCenter System Message Guide*

  This document is in PDF format on the IBM *BladeCenter Documentation* CD. It has information about the switch-specific system messages. During operation, the system software sends these messages to the console or logging server on another system. Not all system messages indicate problems with the system. Some messages are informational, while others can help diagnose problems with communication lines, internal hardware, or the system software. This document also includes error messages that display when the system fails.

- *Cisco Systems Intelligent Gigabit Ethernet Switch Module for the IBM eServer BladeCenter Installation Guide*

- *Cisco Systems Intelligent Gb Fiber Ethernet Switch Module for the IBM eServer BladeCenter Installation Guide*

  These documents contain installation and configuration instructions for the modules. They also provide general information about your module, including warranty information, and how to get help. These documents are also on the IBM BladeCenter Documentation CD.

- *eServer BladeCenter Type 8677 Installation and User's Guide*

  This document is in PDF format on the *IBM BladeCenter Documentation CD*. It contains general information about your BladeCenter unit, including:

  - Information about features
  - How to set up, cable, and start the BladeCenter unit
  - How to install options on the BladeCenter unit
  - How to configure the BladeCenter unit
  - How to perform basic troubleshooting of the BladeCenter unit
  - How to get help

- *BladeCenter Management Module User's Guide*

  This document is in PDF format on the *IBM BladeCenter Documentation CD*. It provides general information about the management module, including:

  - Information about features
  - How to start the management module
  - How to install the management module
  - How to configure and use the management module

- *BladeCenter HS20 Installation and User's Guide* (for each blade server type)

  These documents are in PDF format on the *IBM BladeCenter Documentation CD*. Each provides general information about a blade server, including:

  - Information about features
  - How to set up and start your blade server
  - How to install options on your blade server
  - How to configure your blade server
  - How to install an operating system on your blade server
  - How to perform basic troubleshooting of your blade server
  - How to get help

- Cisco IOS Release 12.1 documentation at

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/index.html

For information about related products, see this document:

*Cisco Small Form-Factor Pluggable Modules Installation Notes*

# Getting Help and Technical Assistance

If you need help, service, or technical assistance or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you. This appendix contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your BladeCenter system, and whom to call for service, if it is necessary.

## Before You Call

Before you call, make sure that you have taken these steps to try to solve the problem yourself:

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system is turned on.
- Use the troubleshooting information in your system documentation, and use the diagnostic tools that come with your system. Information about diagnostic tools is in the *Hardware Maintenance Manual and Troubleshooting Guide* on the *IBM BladeCenter Documentation CD* or at the IBM Support Web site.
- Go to the IBM Support Web site at http://www.ibm.com/pc/support/ to check for technical information, hints, tips, and new device drivers.

You can solve many problems without outside assistance by following the troubleshooting procedures that IBM provides in the online help or in the publications that are provided with your system and software. The information that comes with your system also describes the diagnostic tests that you can perform. Most xSeries and IntelliStation® systems, operating systems, and programs come with information that contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the information for the operating system or program.

## Using the Documentation

Information about your IBM BladeCenter, xSeries, or IntelliStation system and preinstalled software, if any, is available in the documentation that comes with your system. That documentation includes printed books, online books, readme files, and help files. See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. To access these pages, go to http://www.ibm.com/pc/support/ and follow the instructions. Also, you can order publications through the IBM Publications Ordering System at http://www.elink.ibmlink.ibm.com/public/applications/publications/cgibin/pbi.cgi.

## Getting Help and Information from the World Wide Web

On the World Wide Web, the IBM Web site has up-to-date information about IBM BladeCenter, xSeries, and IntelliStation products, services, and support. The address for IBM BladeCenter and xSeries information is http://www.ibm.com/eserver/xseries/. The address for IBM IntelliStation information is http://www.ibm.com/pc/intellistation/.

You can find service information for your IBM products, including supported options, at http://www.ibm.com/pc/support/.

## Software Service and Support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with BladeCenter and xSeries servers, IntelliStation workstations, and appliances. For information about which products are supported by Support Line in your country or region, go to http://www.ibm.com/services/sl/products/.

For more information about Support Line and other IBM services, go to http://www.ibm.com/services/, or go to http://www.ibm.com/planetwide/ for support telephone numbers. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

## Hardware Service and Support

You can receive hardware service through IBM Integrated Technology Services or through your IBM reseller, if your reseller is authorized by IBM to provide warranty service. Go to http://www.ibm.com/planetwide/ for support telephone numbers, or in the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

In the U.S. and Canada, hardware service and support is available 24 hours a day, 7 days a week. In the U.K., these services are available Monday through Friday, from 9 a.m. to 6 p.m.

# Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product, and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

# Edition Notice



# Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

| Active Memory | Predictive Failure Analysis |
|---|---|
| Active PCI | PS/2 |
| Active PCI-X | ServeRAID |
| Alert on LAN | ServerGuide |
| BladeCenter | ServerProven |
| C2T Interconnect | TechConnect |
| Chipkill | ThinkPad |
| EtherJet | Tivoli |
| e-business logo | Tivoli Enterprise |
| <eserver>Eserver | Update Connector |
| FlashCopy | Wake on LAN |
| IBM | XA-32 |
| IBM (logo) | XA-64 |
| IntelliStation | X-Architecture |
| NetBAY | XceL4 |
| Netfinity | XpandOnDemand |
| NetView | xSeries |
| OS/2 WARP | |

Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, Catalyst, EtherChannel, IOS, IP/TV, Packet, and SwitchProbe are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Intel, MMX, and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

Part Number: 24R9745