IBM

@server

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

Release Notes

Cisco IOS Release 12.1(14)AY1

July 2004 Release Notes

This document provides important information about the Cisco Systems Intelligent Gigabit Ethernet Switch Module running Cisco IOS Release 12.1(14)AY1. It includes any limitations, restrictions, and caveats that apply to it. Hereafter, the switch is referred to as the *IGESM switch* or the *switch*.

Use this document with the other documentation listed in the "Related documentation" section on page 22.

Contents

This information is in the release notes:

Software compatibility

These are the software compatibility requirements for this release:

Recommended platform configuration for Web-based management

Table 1 lists the recommended platforms for Web-based management.

Table 1. Recommended Platform Configuration for Web-Based Management.

OS	Processor Speed	DRAM	Number of Colors	Resolution	Font Size
Windows NT 4.0[1]	Pentium 300 MHz	128 MB	65,536	1024 x 768	Small
Solaris 2.5.1 or higher	SPARC 333 MHz	128 MB	Most colors for applications	—	Small (3)

1.Service Pack 3 or higher is required.

The minimum PC requirement is a Pentium processor running at 233 MHz with 64 MB of DRAM. The minimum UNIX workstation requirement is a Sun Ultra 1 running at 143 MHz with 64 MB of DRAM.

Note: These are only the recommended configurations for running CMS. For information about all supported operating systems, see the next section.

Operating system and browser support

You can access the Web-based interfaces by using the operating systems and browsers listed in Table 2. CMS checks the browser version when starting a session to ensure that the browser is supported.

Table 2. Supported Operating Systems and Browsers.

Operating System	Minimum Service Pack or Patch	Netscape Communicator[1]	Microsoft Internet Explorer[2]
Windows 98	Second Edition	4.75, 6.22, or 6.23	5.5 or 6.0
Windows NT 4.0	Service Pack 3 or later	4.75, 6.22, or 6.23	5.5 or 6.0
Windows 2000	None	4.75, 6.22, or 6.23	5.5 or 6.0
Windows XP	None	4.75, 6.22, or 6.23	5.5 or 6.0
Solaris 2.5.1 or later	Sun-recommended patch cluster for the OS and Motif library patch 103461-24	4.75, 6.22, or 6.23	Not supported

1.Netscape Communicator Version 6.0 is not supported.

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

Note: If your browser is Internet Explorer and you receive an error message stating that the page might not display correctly because your security settings prohibit running activeX controls, this might mean that your security settings are set too high. To lower security settings, go to **Tools ->** **Internet Options**, and select the **Security** tab. Select the indicated **Zone**, and move the **Security Level for this Zone** slider from **High** to **Medium** (the default).

Note: In Cluster Management displays, Internet Explorer Versions 4.01 and 5.0 might not display edge devices that are not connected to the command switch. Other functionality is similar to that of Netscape Communicator.

Supported Java plug-ins

One of the these Java plug-ins is required for the browser to access and run the Java-based CMS:

- Java plug-in 1.4
- Java plug-in 1.3.1

These Java plug-ins are supported both in Windows environments and on Solaris platforms. You can download the plug-ins and installation instructions from the following URL:

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

Note: Only one of these Java plug-ins is required for CMS. Do not install more than one Java plug-in.

On Solaris platforms, follow the instructions in the README_FIRST.txt file to install the Java plug-in.

Notes on Java plug-in configuration

- To verify that a supported version of the Java plug-in is installed, select **Start -> Settings-> Control Panel**. The Java plug-in is listed with the version number in the Control Panel menu.
- If you have installed the Java plug-in but CMS still does not launch, make sure that the plug-in is enabled by selecting **Start -> Settings- > Control Panel -> Java Plug-in**. Click the **Basic** tab, select **Enable Java Plug-in**, and click **Apply**.
- If the Java applet does not initialize after you have installed and enabled the plug-in, open the Java Plug-in Control Panel (**Start** > **Programs ->** **Java Plug-in Control Panel**), and verify these settings:

  In the Proxies tab, verify that **Use browser settings** is checked and that no proxies are enabled.
- If you are running an Internet virus checker on Windows 2000 and the plug-in takes a long time to load, you can speed up CMS operation by disabling the virus checker filter option or download option or both.

  From the Start menu on McAfee VirusScan, disable the VirusScan Internet Filter option, the Download Scan option, or both by selecting **Start** -> **Programs** -> **Network Associates** -> **Virus Scan Console** -> **Configure**.

  or

  From the taskbar, right-click the Virus Shield icon and in the Quick Enable menu, disable the options by deselecting **Internet Filter** or **Download Scan**. Windows XP, Windows 2000, Windows 95, Windows 98, and Windows NT 4.0 Plug-Ins

Cluster capability

The switch can be a command switch or a member of a switch cluster. Other cluster-capable switches are the Catalyst 3750, 3560, 3550, 2970, and 2950 switches. For more information about these switches, refer to their documentation.

Note: To manage the IGESM switch through CMS, the IGESM switch must be the command switch of the switch cluster.

Upgrading the switch

This section describes these procedures for upgrading the switch:

Note: Before upgrading the switch, read this section for important information.

Notes about upgrading the switch

When you upgrade the switch, the switch continues to operate while the new software is copied to flash memory. Features provided by the new software are not available until you reload the switch.

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 flash memory does not have enough space for two images, the new image is copied over the existing one.

Note: If a failure occurs during the copy process, you can still reboot your switch by using the old image. If a failure occurs while copying a new image to the switch, and the old image has already been deleted, refer to the "Recovering from Corrupted Software" section in the "Troubleshooting" chapter of the switch software configuration guide.

Note: If you are upgrading a switch that uses the 802.1X security feature, you must re-enable 802.1X after upgrading the software. After the upgrade is complete, make sure to globally enable 802.1X by using the **dot1x system-auth-control** global configuration command.

Determining the software version on your switch

The Cisco IOS image is stored as a .bin file in a directory that is named with the Cisco IOS release number. 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 file is stored.

Note: 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.

Determining which image file to download from the Web

New software releases are posted on ibm.com and are also available through authorized resellers. You can download the switch software from this site, and click **Support & downloads**:

http://www.ibm.com/pc/support/

Table 3 lists the image filenames that you can download from the Web to your switch:

Table 3. Cisco IOS Image Files for This Release.

Filename	Description
cigesm-i6q4l2-tar.121-14.AY1.tar	Switch non-cryptographic Cisco IOS image and CMS files.
cigesm-i6k2l2q4 -tar.121-14.AY1.tar	Switch cryptographic Cisco IOS image and CMS files.

Using CMS to upgrade the switch

The upgrade procedure in this section describes how to perform the upgrade by using a combined .tar file. You must use the combined .tar file to upgrade the switch through the CMS. The procedure assumes 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 tar** 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 "Determining which image file to download from the Web" section on page 6.

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

You can upgrade switch software by using CMS. From the menu bar, select **Administration -> Software Upgrade**. For detailed instructions, click **Help**.

Using the CLI to upgrade the switch

The upgrade procedure in this section describes how to perform the upgrade by using a combined .tar file. The procedure assumes 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 tar** 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 "Determining which image file to download from the Web" section on page 6.

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 set of images.

  If there is insufficient space on the flash memory to hold both the old and the new images, it deletes the old set of images. The images are 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.121-14.AY1.tar.
- It replaces the old set of images with the new set of images. The set includes the CMS firmwares. You do not have to manually delete the CMS directory from flash memory.
- After the new set 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 further information on this command, see the command reference for this release.

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

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

3. Enter privileged EXEC mode:

```
switch> enable
switch#
```

Enter the password if you are prompted to do so.

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
```

5. If there is no software image defined in the BOOT path-list, enter **dir flash:** to display the contents of flash memory.
6. Enter the **archive download-sw /reload** command.
7. Press **Return** to confirm the reload.

Your Telnet session ends when the switch resets.

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, refer to the “Troubleshooting” chapter in the switch software configuration guide.

Installation notes

Use the BladeCenter Management Module Web page to assign IP information to the switch. For more information, refer to the *Cisco Intelligent Gigabit Ethernet Switch Module for the IBM eServer BladeCenter Installation Guide*.

New features

This is the first release of the switch. Refer to the *Cisco Intelligent Gigabit Ethernet Switch Module for the IBM eServer BladeCenter Installation Guide* and the *Cisco Systems Intelligent Gigabit Ethernet Switch Module for the IBM eServer BladeCenter Software Configuration Guide* for the features supported in this release.

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.

These are the limitations and restrictions:

- "Cisco IOS limitations and restrictions" section on page 9
- "CMS limitations and restrictions" section on page 15
- "Cluster limitations and restrictions" section on page 17

Cisco IOS limitations and restrictions

These limitations and restrictions apply to the Cisco IOS configuration:

- CSCdp85954

  Root guard is inconsistent when configured on a port that is in the STP blocked state at the time of configuration.

  There is no workaround.

- CSCdr96565

  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.

  There is no workaround.

- CSCds20365

  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.

- CSCdt24814

  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 unknown unicast or multicast, the packets are forwarded only on one port member of a port group, instead of being shared among all members of the port group.

  There is no workaround.

- CSCdt27223

  When you enter the **show controllers ethernet-controller** *interface-id* or **show interfaces** *interface-id* **counters** privileged EXEC command, if 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.

  There is no workaround.

- CSCdt48011

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.

- CSCdu83640

  The receive count output for the **show controllers ethernet-controller** *interface-id* privileged EXEC command shows the incoming packets count before the ASIC makes a decision of whether to drop 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.

  There is no workaround.

- CSCdv02941

  In some network topologies, when UplinkFast is enabled on all switches and BackboneFast is not enabled on all switches, a temporary loop might be caused when the STP root switch is changed.

  The workaround is to enable BackboneFast on all switches.

- CSCdv19671

  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 802.1X port to be de-authenticated.

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

- CSCdv27247

  If an IGESM switch and another switch are connected, and if the access ports are used to connect two different VLANs whose VLAN IDs are separated by the correct multiple of 64, it is possible to create a situation where the two switches use the same bridge ID in the same spanning-tree instances. This might cause a loss of connectivity in the VLAN 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.

- CSCdv45190

  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 an IGESM switch at one time. If you statically add a 256th group, and 255 groups are already configured on the switch, it continues trying (and failing) to add the new group.

  The workaround is to set the mode to **dynamic** for the 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.

- CSCdv49871

  An IGESM command switch can discover only the first Catalyst 3550 switch if the link between the Catalyst 3550 switches is an 802.1Q trunk and the native VLAN is not the same as the management VLAN of the IGESM switch or if the link between the Catalyst 3550 switches is an 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 802.1Q trunk with a native VLAN that is the same as the management VLAN of the command switch.

- CSCdv67047

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

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

- CSCdw02638

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

  There is no workaround.

- CSCdw66805

  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 crypto 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 is a cluster command switch, it can only support up to eight cluster members.

  If your switch has a saved configuration that does not meet the previous conditions and you upgrade the switch software to the crypto 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 ensure that it meets the previous conditions.

- CSCdx95638

  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.

- CSCdy38476

  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 an IGESM switch is used as an intermediate or destination switch.

- CSCdy65850

  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.

  There is no workaround.

- CSCdz32556

  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.

- CSCdz34545

  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.

- CSCdz74685

  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.

  There is no workaround.

- CSCea12888

  If you press and hold the spacebar while the output of any **show** user EXEC command is being displayed, the Telnet session is stopped, 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`

  — Telnet 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.

- CSCea23138

  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.

- CSCea24969

  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.

  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, refer to 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*.

  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.

- CSCeb75386

  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% utilization.

  The workaround is to use a different load balancing method (for example, use destination-based forwarding instead of source-based forwarding).

- CSCec02055

  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 execute the **clear mac address-table dynamic** user EXEC command repeatedly until the address table is cleared.

- CSCec10814

  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.

  There is no workaround.

- CSCec29644

  The switch does not detect if the VLAN configuration on a switch port is different from the VLAN configuration on the connected port of the other device. This misconfiguration can cause Ethernet traffic to be received on the wrong VLAN.

  The workaround is make sure that both connected ports have the same VLAN configuration.

- CSCec69748

  The switch does not detect EtherChannel misconfigurations between the switch and the connected device. Therefore, EtherChannel guard does not place the switch interfaces in the error-disabled state.

  There is no workaround.

- CSCec74979

  The output of the **show flowcontrol** user EXEC command incorrectly shows that the switch is not receiving and transmitting pause frames.

  The workaround is to use the **show controllers ethernet-controller** privileged EXEC command to display the transmit and receive pause packets for a specific port.

- CSCed03370

  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 indicate that a Layer 2 loop has been established. In actuality, there is no STP loop.

  There is no workaround.

- CSCed11638

  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.

  There is no workaround.

- CSCed20563

  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.

  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.

- CSCed25956

  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.

- CSCed40295

  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 802.1D BPDUs, instead of sending 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).

- CSCed47701

  All unknown unicast and broadcast traffic in an EtherChannel are sent to the port configured to be the protected port. If this is the only type of traffic on the EtherChannel, it could reduce the aggregate bandwidth and speed on this port.

  There is no workaround.

- CSCed63013

  When using the **police** policy-map class configuration command on Gigabit-capable Ethernet ports, enter a burst value that is greater than or equal to 8192 bytes. 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 8192.

CMS limitations and restrictions

These limitations apply to CMS configuration:

- The Cluster Management Suite (CMS) is not forward-compatible, which means that if a member switch is running a software version that is newer than the release running on the command switch, the new features are not available on the member switch. If the member switch is a new device supported by a software release that is later than the software release on the command switch, the command switch cannot recognize the member switch and it is displayed as an unknown device in the Front Panel view. You cannot configure any parameters or generate a report through CMS for that member; instead, you must launch the Device Manager application to perform configuration and obtain reports for that member.
- CSCdv82352

  A red border appears around the text-entering area of some CMS dialogs. The color of the border changes to green when text is entered. This is only a cosmetic error. The colored border does not prevent you from entering text.

  There is no workaround.

  Note: This error only occurs with Java plug-in 1.4.0.
- CSCdw87550

  You cannot switch modes (for example, from Guide Mode to Expert Mode) for an open CMS window.

  The workaround is to close the open window, select the mode that you want, and then reopen the CMS window.

  Note: For the mode change to take effect on any other CMS window that is open, you need to close that window and then reopen it after you select the new mode.
- CSCdz75666

  After you click **Apply** or **Refresh** in the SNMP window, the window size changes.

  There is no workaround.
- CSCdz81086

  When you enable log scaling for Link Graphs, the Y-axis scale becomes illegible.

  There is no workaround.
- CSCea01179

  The CMS window does not return to full size after resizing the NE or IE when using Netscape version 6.xx on Solaris and Linux. This is a Netscape browser problem.

  There is no workaround.
- CSCea27601

  The CMS files that are downloaded from the switch to your PC or terminal are not cached on the PC or terminal. The files are then downloaded again when CMS is relaunched.

  There is no workaround.

- CSCea25913

  If you launch CMS by using Netscape 4.75 and Java Runtime Environment (JRE) 1.3.1 or 1.4.0 on Windows 98 or by using Netscape 6.2 and JRE 1.3.1 on Windows 98, CMS stops running while it determines the network information.

  The workaround is to click once outside of the CMS window.

- CSCea27408

  On the Japanese versions of Windows 98 and Windows ME, if you launch CMS by using the Netscape 4.7 browser, CMS might stop running after you click the Apply button.

  The workaround is to use Netscape 6.0 or later or use Internet Explorer to launch CMS on Windows 98 and Windows ME.

- CSCea80753

  The icons on the tool bar are blank when you unlock the PC while CMS is running or you interrupt the screen saver on your PC.

  The workaround is to resize the CMS window so that the window is refreshed correctly.

- CSCeb33995

  If you change the password or start the authentication process while CMS is running, HTTP requests sent by the switch fail.

  The workaround is to close all browser sessions and then relaunch CMS.

- Host names and Domain Name System (DNS) server names that contain commas on a cluster command switch, member switch, or candidate switch can cause CMS to behave unexpectedly. You can avoid this instability in the interface by not using commas in host names or DNS names. Do not enter commas when also entering multiple DNS names in the IP Configuration tab of the IP Management window in CMS.

- ACEs that contain the **host** keyword precede all other access control entries (ACEs) in standard ACLs. You can reposition the ACEs in a standard ACL with one restriction: No ACE with the **any** keyword or a wildcard mask can precede an ACE with the **host** keyword.

- Certain combinations of port features create configuration conflicts (see Table 4 for the port configuration conflicts). If you try to enable incompatible features, a warning message appears in CMS, and you cannot make the change. Reload the page to refresh CMS.

  In Table 4, *No* means that the two referenced features are incompatible, and both should not be enabled; *Yes* means that both can be enabled at the same time and do not cause an incompatibility conflict. A dash means not applicable.

Table 4. Conflicting Features .

	Port Group	Port Security	SPAN Source Port	SPAN Destination Port	Connect to Cluster?	Protected Port	802.1X Port
Port Group	–	No	Yes	No	Yes	Yes	No
Port Security	No	–	Yes	No	Yes	Yes	Yes
SPAN Source Port	Yes	Yes	–	No	Yes	Yes	Yes
SPAN Destination Port	No	No	No	–	Yes	Yes	No
Connect to Cluster	Yes	Yes	Yes	Yes	–	Yes	–
Protected Port	Yes	Yes	Yes	Yes	Yes	–	–
802.1X Port	No	Yes	Yes	No	–	–	–

Cluster limitations and restrictions

This limitation and restriction applies to the cluster configuration:

- CSCdz88305

  When a cluster of switches have Network Time Protocol (NTP) configured, the command switch is not synchronized with the rest of the switches.

  There is no workaround.

Important notes

This section describes important information related to this release. These sections are included:

- “Cisco IOS notes” section on page 17
- “CMS notes” section on page 18

Cisco IOS notes

These notes applies to Cisco IOS configuration:

- IGMP filtering controls only group specific query and membership reports, including join and leave reports. It does not control general IGMP queries.
- When an 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 transition to the unauthorized state. If this happens, it can take up to 60 minutes for the interface to transition 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 802.1X client, not with the switch.

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

  ```
  dot1x timeout quiet-period 3
  ```

```
dot1x timeout tx-period 5
```

CMS notes

These notes apply to the CMS configuration:

- If you use CMS on Windows 2000, it might not apply configuration changes if the enable password is changed from the CLI during your CMS session. You have to restart CMS and enter the new password when prompted. Platforms other than Windows 2000 prompt you for the new enable password when it is changed.
- If you have a proxy server configured on your Web browser, CMS can run slowly and take 2 to 3 minutes to process each command that is entered.

  The workaround, if you do not want to disable the proxy server settings on the browser, is to download a browser from a different vendor and use it without the proxy server settings configured to access the CMS.
- CMS does not display QoS classes that are created through the CLI if these classes have multiple match statements. When using CMS, you cannot create classes that match more than one match statement. CMS does not display policies that have such classes.
- If you use Internet Explorer Version 5.5 and select a URL with a nonstandard port at the end of the address (for example, *www.cisco.com*:84), you must enter *http://* as the URL prefix. Otherwise, you cannot launch CMS.
- Within an ACL, you can change the sequence of ACEs that have the **host** keyword. However, because such ACEs are independent of each other, the change has no effect on the way the ACL filters traffic.

Open caveats

These are the open caveats in this release:

- "Open Cisco IOS caveats" section on page 18
- "Open CMS caveats" section on page 21

Open Cisco IOS caveats

These are the open Cisco IOS configuration caveats:

- CSCdx75308

  When you use the **policy-map** global configuration command to create a policy map, and you 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.
- CSCdx95501

  When a community string is assigned by the cluster command switch, you cannot get any dot1dBridge MIB objects 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
```

- CSCea63436

  When an IGESM switch is running Multicast VLAN Registration (MVR) dynamic mode, the source port MVR membership flaps.

  The workaround is to enter the **no ip igmp snooping report-suppression** interface configuration command.

- CSCeb05425

  If you configure an ACL such that a DHCP server allocates a specific IP address and configuration information on an interface, such as this ACL:

  ```
  access-list 104 permit ip host 192.5.0.0 any
  access-list 104 permit ip host 0.0.0.0 any
  ```

  The switch does not apply the ACL to the interface, and this error message appears:

  The field sets of all the ACEs in an ACL on Ethernet interface should match. Refer to the switch software configuration guide to understand mask restrictions for ACLs on Ethernet interfaces.

  The workaround is to configure the host with a static IP address and configure the DHCP server to not allocate an IP address to the host.

- CSCeb05733

  When an LACP channel group with hot standby ports is restarted by using the **shutdown** and **no shutdown** interface configuration commands, this following error message appears:

  ```
  %SM-4-BADEVENT: Event 'link_down' is invalid for the current state
  'link_down':
  ```

  There is no workaround.

- CSCeb33988

  If too many traps are enabled when a switch powers on, it might not generate the coldStart trap.

  There is no workaround.

- CSCeb49033

  Under the following conditions, configuring **mac-address-table notification** can cause the switch to run out of memory and fail. Using **mac-address-table notification history-size** and **mac-address-table notification interval** to tune the process does not resolve the problem.

  — Large number of MAC address flapping.
  With the wrong setup, a single host with multiple NICs can be connected to the switch using the same MAC address in the same VLAN. As the result, the MAC address flaps from port to port generating many *adds* and *drops* from the MAC address table.

  — MAC address flooding attack.
  With a MAC address flooding attack, a single NIC host sends out many packets with different source MAC addresses, which also generates many *adds* for the MAC address table.

The workaround for the first case is to turn off the MAC address table notification, and the workaround for the second case is to use port security to inhibit the attack.

- CSCeb55987

  When UplinkFast is configured on an IGESM switch, the MAC address of the switch is not forwarded to the uplink switch through the new link. This temporarily interrupts communication with the management VLAN and delays convergence of UplinkFast.

  There is no workaround.

- CSCeb62247

  With light Layer 2 multicast traffic (about 10 mbps line rate), IP IGMP query messages might fail to reach the IGESM switch, which causes the IP IGMP snooping feature to fail.

  The workaround is to disable source-only-learning or stop multicast traffic.

- CSCed88639

  If you disable and re-enable Internet Group Management Protocol (IGMP) snooping, this can cause multicast flooding on the VLAN.

  The workaround is to send IGMP reports to the switch for group membership, so that the hosts can rejoin the same groups. The multicast group entries are updated in the address table and multicast flooding control resumes.

- 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 transition 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 are 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.

- CSCed92062

  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.

- CSCee27729

  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 err-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 would remain in the err-disabled state. An entry in the the system message log is added.

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

The workaround is to reboot the switch after disabling BPDU guard on the switch or after disabling it on the internal management module ports. Also make sure that the saved configuration for the switch does not have BPDU guard enabled.

Open CMS caveats

These are the open CMS configuration caveats:

- CSCdz01037

  CMS does not work when a switch is running the crypto software image and the vty lines are configured to use only SSH by using the **transport input ssh** *line vty 0 15* interface configuration command.

  The workaround is to allow SSH and Telnet access through the vty lines by using the **transport input ssh telnet** interface configuration command.

- CSCdz15119

  If only one management VLAN interface is configured on a switch, you cannot change the management VLAN interface to another management VLAN interface by using CMS.

  The workaround is to create a second management VLAN interface before you use CMS to change the management interface.

- CSCdz23548

  When you use Visual Switch Manager (VSM) to configure Catalyst 2900 XL and Catalyst 3500 XL switches, the configuration is not saved if you save it in VSM.

  The workaround is to save the configuration by using the CLI.

- CSCeb05183

  On the Catalyst 2820 and Catalyst 1900 switches, the Port Settings table might show incorrect information in the interface description and duplex columns.

  There is no workaround.

- CSCeb25630

  The Link Graphs bar chart for Packet Drops and Errors might display incorrect information about the Ethernet interfaces.

  The workaround is to use the **show interfaces** or **show interfaces counter** privileged EXEC command.

- CSCeb38676

  If you are launching CMS in read-only mode, Java exceptions might occur. These exceptions do not affect the CMS functionality.

  There is no workaround.

- CSCeb38967

  When CMS is in read-only mode, an error message appears if the online help is launched from the QoS Graph window.

  There is no workaround.

- CSCeb40625

  Shaped bandwidth weights are invalid if the sum of their reciprocals is greater than 1 and the weight of a queue is zero. CMS does not configure these invalid bandwidth weights.

  There is no workaround.

- CSCed88490

Changing the spanning-tree mode from PVST+ to rapid PVST+ causes a Java exception. However, the new spanning-tree mode is still applied to the target device.

There is no workaround.

Related documentation

In addition to this document, the following related documentation comes with the Gigabit Ethernet switch module:

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

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

  — Command line interface (CLI) modes

  — Command line interface commands and examples

  — Syntax description

  — Defaults

  — Command history

  — Usage guidelines

  — Related commands

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

  This Cisco document is in PDF on the IBM *BladeCenter Documentation* CD. It contains software configuration information for the Gigabit Ethernet switch module. It provides:

  — Configuration instructions for your Gigabit Ethernet switch module

  — Information about features

  — Information about getting help

  — Guidance for planning, implementing, and administering LAN operating system software

  — Usage examples

  — Troubleshooting information for your Gigabit Ethernet switch module

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

  This document is in PDF on the IBM *BladeCenter Documentation* CD. It contains 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 Intelligent Gigabit Ethernet Switch Module for the IBM eServer BladeCenter Installation Guide*

  This document contains installation and configuration instructions for the Gigabit Ethernet switch module. This document also provides general information about your Gigabit Ethernet switch module, including warranty information, and how to get help. This document is also on the IBM *BladeCenter Documentation* CD.

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

This document is in PDF 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 in 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 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 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 in 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
- Cisco IOS Release 12.2 documentation at http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/index.html

Appendix A. 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.

AppendixB. 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	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, Cisco Networks, 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.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

Red Hat, the Red Hat “Shadow Man” logo, and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc., in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Part Number: 25K8412 Fourth edition