Release Notes for Cisco IOS Release 15.2(5)E

Last Updated: February 27, 2018
First Published: July 28, 2016

Cisco IOS Release 15.2(5)E runs on these platforms:

- Cisco 2500 Series Connected Grid Switches (CGS 2520)
- Cisco Embedded Service 2020 Series Switches (ESS 2020)
- Cisco Connected Grid Ethernet Switch Module (CGR 2010 ESM)
- Cisco Industrial Ethernet 2000 Series Switches (IE 2000)
- Cisco Industrial Ethernet 2000U Series Switches (IE 2000U)
- Cisco Industrial Ethernet 3000 Series Switches (IE 3000)
- Cisco Industrial Ethernet 3010 Series Switches (IE 3010)
- Cisco Industrial Ethernet 4000 Series Switches (IE 4000)
- Cisco Industrial Ethernet 5000 Series Switches (IE 5000)

These release notes include important information about Cisco IOS Release 15.2(5)E and any limitations, restrictions, and caveats that apply to the release. Verify that these release notes are correct for your switch:

- If you are installing a new switch, see the Cisco IOS release label on the rear panel of your switch.
- If your switch is on, use the **show version** command. See Finding the Software Version and Feature Set, page 6.
- If you are upgrading to a new release, see the software upgrade filename for the software version. See Deciding Which Files to Use, page 7.

For a complete list of documentation for the platforms associated with this release, see Related Documentation, page 25.

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

http://software.cisco.com/download/navigator.html

Organization

This document includes the following sections:

Conventions, page 2	Conventions used in this document.
New Features in Cisco IOS Release 15.2(5)E, page 3	New features in Release 15.2(5)E.
System Requirements, page 6	System requirements for Release 15.2(5)E.
Upgrading the Switch Software, page 6	Procedures for downloading software.
Limitations and Restrictions, page 12	Known limitations in this release.
Caveats, page 14	Open caveats in Release 15.2(5)E.
Documentation Updates, page 23	Updates to the IE switch product documentation.
Related Documentation, page 25	Links to the documentation for the hardware platforms associated with this release.
Obtain Documentation and Submit a Service Request, page 25	Link to information about Cisco documentation.

Conventions

This document uses the following conventions.

Conventions	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
courier font	Terminal sessions and information the system displays appear in `courier` font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note: Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution: **Means *reader be careful.* In this situation, you might perform an action that could result in equipment damage or loss of data.**

Warning: **IMPORTANT SAFETY INSTRUCTIONS**

Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Regulatory: Provided for additional information and to comply with regulatory and customer requirements.

New Features in Cisco IOS Release 15.2(5)E

Table 1 lists new features added in Cisco IOS Release 15.2(5)E.

This release supports all of the features introduced in Cisco IOS Release 15.2(4)EA1 that are summarized in the release notes below:

Release Notes for Cisco IE 2000, IE 2000U, IE 3000, IE 3010, IE 4000, IE 5000, CGS 2520, ESS 2020 Switches, and ESM for CGR 2010, Cisco IOS Release 15.2(4)EA1

This release also supports the IE 5000 features introduced in Cisco IOS Release 15.2(2)EB and EB1.

Table 1 New Feature Summary for Cisco IOS Release 15.2(5)E

Feature	Platform	Description	Related Documentation
PROFINET certification	IE 5000	IE 5000 10G and 1G platforms have received PROFINET certification: ■ IE-5000-12S12P-10G ■ IE-5000-16S12P	Cisco IE 5000 Hardened Aggregator Hardware Installation Guide
TrustSec Security Group Tagging (SGT) and Security Group ACL (SGACL)	IE 4000 IE 5000	IE 4000 and IE 5000 now support TrustSec SGT and SGACL. **Note:** These features do not work on the 10G SFP+ interface on the system noted below. However, they are supported when a 1G transceiver is used in the 10G slot. ■ IE-5000-12S12P-10G	Cisco TrustSec Switch Configuration Guide
MACsec (IEEE 802.1AE) on 10GE	IE 5000	MACsec is the IEEE 802.1AE standard for providing strong cryptographic protection at Layer 2. MACsec provides secure (encryption and authentication) MAC Service on a frame-by-frame basis. MACsec provides secure communications between stations that are attached to the same LAN. MACsec is supported on 1G and 10G uplinks. **Note** You must have the IP Service license installed to support the MACsec feature.	Configuring MACsec Encryption
Horizontal Stacking	IE 5000	Allows use of Cisco horizontal stacking between two to four IE 5000 10G switches (*see part number below*) at distances up to a few kilometers. Stacking allows the IE 5000 10G switches to appear as a single logical switch with a single IP address: ■ IE-5000-12S12P-10G	Horizontal Stacking Software Configuration Guide for IE 5000 Switches
IRIG-B time code	IE 5000	IRIG-B output signals will be transmitted on Analog Timecode I/O (output only) and Digital Timecode I/O (output only) coax connectors of the switch. Configurable using command-line interface. See new commands supported in Documentation Updates, page 23.	Cisco IE 5000 Hardened Aggregator Hardware Installation Guide Cisco Industrial Ethernet 5000 Hardened Aggregator Software Configuration Guide See Product Overview chapter.

Table 1 New Feature Summary for Cisco IOS Release 15.2(5)E

Feature	Platform	Description	Related Documentation
Media Redundancy Protocol (MRP) enhancements	IE 2000 IE 4000	■ MRP-STP Interoperability: Prevents unwanted broadcast loops in the event that a user accidentally connects a device that does not participate in the MRP ring. ■ Multiple MRP ring support allows connection of multiple MRP rings, which can be aggregated at the distribution layer (mrp-multi-manager MRP license required) ■ MRP 500ms profile ■ License portability: Allows MRP licensing to be easily transferred from a failed switch to another switch via a SD card to facilitate Zero Touch Deployment (ZTD).	■ Media Redundancy Protocol Configuration Guide for IE 2000 and IE 4000 Switches ■ Device Manager Online Help
Parallel Redundancy Protocol (PRP) Supervisory Frame	IE 2000U IE 4000, IE 5000,	Supervisory frames are automatically sent for any device connected to a redundancy box (RedBox) without the need for manual configuration. Device Manager interface and CLI command support added for IE 4000 and IE 5000. This capability is supported on: ■ IE 4000 uplinks (Gig1/1 to Gig1/4) only ■ IE 5000 Gigabit ports are downlinks only	■ Parallel Redundancy Protocol (PRP) for IE 4000 and IE 5000 Switches ■ Parallel Redundancy Protocol Software Configuration Guide for Industrial Ethernet (IE 2000U) and Connected Grid Switches ■ Device Manager Online Help
Resilient Ethernet Protocol (REP): Faster convergence time (<50ms) for unicast and multicast traffic on Fiber ports	IE 2000 IE 2000U IE 3000 IE 3010 IE 4000 IE 5000	Revised configuration recommendations for the following command: **lsl-age-timer** *timer-value* (CSCux92117)	■ REP chapter in LAN Switching Configuration Guide, Cisco IOS XE Release 3S
Express Setup enhancement	IE 2000 IE 3000 IE 3010 IE 4000 IE 5000 CGS 2520 ESS 2020	You can enable and disable SSH through the Express Setup page.	■ Refer to Table 3Methods for Assigning IP Information, page 11 for links to all Express Setup documents for the Industrial Ethernet switches.
Device Manager Platform Support Expanded	ESS 2020	You can now manage the ESS 2020 switches using the Device Manager.	■ Device Manager Online Help

Table 1 New Feature Summary for Cisco IOS Release 15.2(5)E

Feature	Platform	Description	Related Documentation
Device Manager Enhancement	CGS 2520 ESS 2020 IE 2000 IE 3000, IE 3010 IE 4000 IE 5000	DM login authentication page replaces a pop-up authentication page found in previous releases.	■ Device Manager Online Help

System Requirements

This section describes the following system requirements for Cisco IOS Release 15.2(5)E:

■ Express Setup Requirements, page 6

Express Setup Requirements

This section summarizes the hardware and software requirements for the Windows platform.

For a listing of Express Setup documentation, see Table 3Methods for Assigning IP Information, page 11.

Hardware

- 1 gigahertz (GHz) or faster 32-bit (x86) or 64-bit (x64) processor
- 1 gigabyte (GB) RAM (32-bit) or 2 GB RAM (64-bit)
- 16 GB available hard disk space (32-bit) or 20 GB (64-bit)

Software

- PC with Windows 7, or Mac OS 10.6.x
- Web browser (Internet Explorer 9.0, 10.0, and 11.0, or Firefox 32) with JavaScript enabled
- Straight-through or crossover Category 5 or 6 cable

Express Setup verifies the browser version when starting a session, and it does not require a plug-in.

Upgrading the Switch Software

These are the procedures for downloading software. Before downloading software, read these sections for important information:

■ Finding the Software Version and Feature Set, page 6

■ Deciding Which Files to Use, page 7

■ Archiving Software Images, page 7

■ Upgrading a Switch by Using the CLI, page 8

■ Installation Notes, page 10

Finding the Software Version and Feature Set

The Cisco IOS image is stored as a bin file in a directory that is named with the Cisco IOS release. A subdirectory contains the files needed for web management. The image is stored on the compact flash memory card.

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

You can also use the **dir** *filesystem***:** privileged EXEC command to see the directory names of other software images stored in flash memory. For example, use the **dir flash:** command to display the images in the flash memory.

Deciding Which Files to Use

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

Table 2 lists the filenames for this software release.

Note: If you download the IP services image and plan to use Layer 3 functionality, you must use the Switch Database Management (SDM) routing template. To determine the currently active template, enter the **show sdm prefer** privileged EXEC command. If necessary, enter the **sdm prefer** global configuration command to change the SDM template to a specific template. For example, if the switch uses Layer 3 routing, change the SDM template from the default to the routing template. You must reload the switch for the new template to take effect.

Note: Beginning with Cisco IOS Release 15.2(5)E, we **no longer release** the IE 3000 LAN base image. The latest release for LAN base image on the IE 3000 is 15.2(4)EA1.

Table 2 Cisco IOS Software Image Files

File Name	Description
cgs2520-ipserviceslmk9-tar.152-5.E.tar	CGS 2520 IP services image file
cgs2520-lanbaselmk9-tar.152-5.E.tar	CGS 2520 LAN base image file
c2020-universalk9-tar.152-5.E.tar	ESS 2020 universal image file
ie2000-universalk9-tar.152-5.E.tar	IE 2000 universal image file
ie2000u-ipserviceslmk9-tar.152-5.E.tar	IE 2000U IP services image file
ie2000u-lanbaselmk9-tar.152-5.E.tar	IE 2000U LAN base image file
ie3010-ipservicesk9-tar.152-5.E.tar	IE 3010 IP services image file
ie3010-lanbasek9-tar.152-5.E.tar	IE 3010 LAN base image file
ies-lanbasek9-tar.152-5.E.tar	IE 3000 LAN base image file
grwicdes-ipserviceslmk9-tar.152-5.E.tar	ESM IP services image file
grwicdes-lanbaselmk9-tar.152-5.E.tar	ESM LAN base image file
ie4000-universalk9-tar.152-5.E.tar	IE 4000 Universal image file
ie5000-universalk9-tar.152-5.E.tar	IE 5000 Universal image file

Archiving Software Images

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

Cisco routinely removes old Cisco IOS versions from Cisco.com. See *Product Bulletin 2863* for information:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6969/ps1835/prod_bulletin0900aecd80281c0e.html

You can copy the bin software image file on the flash memory to the appropriate TFTP directory on a host by using the **copy flash: tftp:** privileged EXEC command.

Note: Although you can copy any file on the flash memory to the TFTP server, it is time consuming to copy all of the HTML files in the tar file. We recommend that you download the tar file from Cisco.com and archive it on an internal host in your network.

You can also configure the switch as a TFTP server to copy files from one switch to another without using an external TFTP server by using the **tftp-server** global configuration command.

Upgrading a Switch by Using the CLI

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

Note: Make sure that the compact flash card is in the switch before downloading the software.

To download software, follow these steps:

1. Use Table 2 on page 7 to identify the file that you want to download.
2. Download the software image file. If you have a SMARTNet support contract, go to this URL, and log in to download the appropriate files:

   http://software.cisco.com/download/navigator.html

   For example, to download the image for an IE 2000 switch, select Products > Switches > Industrial Ethernet Switches > Cisco Industrial Ethernet 2000 Series Switches, then select your switch model. Select IOS Software for Software Type, then select the image you want to download.
3. Copy the image to the appropriate TFTP directory on the workstation, and make sure that the TFTP server is properly configured.

   For more information, see the “Assigning the Switch IP Address and Default Gateway” chapter in the applicable document for your switch as listed in Table 3.
4. Log into the switch through the console port or a Telnet session.
5. (Optional) Ensure that you have IP connectivity to the TFTP server by entering this privileged EXEC command:

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

   For more information about assigning an IP address and default gateway to the switch, see Table 3.
6. Download the image file from the TFTP server to the switch.

   If you are installing the same version of software that currently exists on the switch, overwrite the current image by entering this privileged EXEC command:

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

   The command above untars/unzips the file.The system prompts you when it completes successfully.

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

   If you specify the command without the **/overwrite** option, the download algorithm verifies that the new image is not the same as the one on the switch Flash device. If the images are the same, the download does not occur. If the images are different, the old image is deleted, and the new one is downloaded. If there is not enough space to install the new image and keep the current running image, the download process stops, and an error message displays.

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

- For **//** *location*, specify the IP address of the TFTP server. or hostname.
- For **/***directory***/***image-name***.tar**, specify the directory and the image to download. Directory and image names are case sensitive. The directory is for file organization and it is generally a *tftpboot/user-ID* path.

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

```
Switch# archive download-sw /overwrite tftp://198.30.20.19/image-name.tar
```

You can also download the image file from the TFTP server to the switch and keep the current image by replacing the **/overwrite** option with the **/leave-old-sw** option. If there is not enough space to install the new image and keep the current running image, the download process stops, and an error message displays.

Upgrading IOS and FPGA on the Ethernet Switch Module (ESM)

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

To download software, follow these steps:

1. Refer to Deciding Which Files to Use, page 7 to identify the file that you want to download.
2. Download the software image file. If you have a SMARTNet support contract, go to the URL below and log in to download the appropriate files.

   http://software.cisco.com/download/navigator.html

   For example, to download the image for a Connected Grid 10-Port Ethernet Switch Module Interface Card, select Products > Cisco Interfaces and Modules > Connected Grid Modules > Connected Grid 10-Port Ethernet Switch Module Interface Card. Select IOS Software for Software Type, then select the image you want to download.

   Copy the image to the appropriate TFTP directory on the workstation, and make sure that the TFTP server is properly configured. For more information, see the “Assigning the Switch IP Address and Default Gateway” chapter in the applicable document listed in Table 3Methods for Assigning IP Information, page 11.
3. Copy the image to the appropriate TFTP directory on the workstation, and make sure that the TFTP server is properly configured.
4. Log in to the switch through the console port or a Telnet session.
5. (Optional) Ensure that you IP connectivity to the TFTP server by entering this privileged EXEC command:

   Switch# ping *tftp-server-address*
6. Download the image file from the TFTP server to the switch.

   If you are installing the same version of software that currently exists on the switch, overwrite the current image by entering this privileged EXEC command:

   Switch# archive download-sw /overwrite tftp: //*location* **/***directory* **/***image-name***.tar**

   The command above untars/unzips the file.The system prompts you when it completes successfully.

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

   If you specify the command without the **/overwrite** option, the download algorithm verifies that the new image is not the same as the one on the switch Flash device. If the images are the same, the download does not occur. If the images are different, the old image is deleted, and the new one is downloaded. If there is not enough space to install the new image and keep the current running image, the download process stops, and an error message displays.

- The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved.
- For **//** *location*, specify the IP address of the TFTP server. or hostname.
- For **/***directory***/***image-name***.tar**, specify the directory and the image to download. Directory and image names are case sensitive. The directory is for file organization and it is generally a *tftpboot/user-ID* path.

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

```
Switch# archive download-sw /overwrite tftp://198.30.20.19/image-name.tar
```

You can also download the image file from the TFTP server to the switch and keep the current image by replacing the **/overwrite** option with the **/leave-old-sw** option. If there is not enough space to install the new image and keep the current running image, the download process stops, and an error message displays.

7. After the download and the untar are complete, power cycle the CGR2010.

Installation Notes

You can assign IP information to your switch using the methods shown in Table 3.

Table 3 Methods for Assigning IP Information

Method	Platform	Document
Express setup program	IE 2000	*Cisco IE 2000 Switch Hardware Installation Guide*
	IE 3000	*Cisco IE 3000 Switch Getting Started Guide,* Device Manager Online Help
	IE 3010	*Cisco IE 3000 Switch Getting Started Guide*, Device Manager Online Help **Note:** The *Cisco IE 3000 Switch Getting Started Guide* serves as Express Setup reference for the IE 3010.
	CGS 2520	*Cisco CGS 2520 Getting Started Guide*, Device Manager Online Help
	ESM	*Connected Grid Ethernet Switch Module Interface Card Getting Started Guide*
	IE 4000	*Cisco IE 4000 Switch Hardware Installation Guide*
	IE 5000	*Cisco IE 5000 Hardened Aggregator Hardware Installation Guide*
CLI-based setup program	ESS 2020	*Cisco Embedded Service 2020 Series Software Configuration Guide*
	IE 2000	*Cisco IE 2000 Switch Hardware Installation Guide*
	IE 2000U	*Cisco IE 2000U Switch Hardware Installation Guide*
	IE 3000	*Cisco IE 3000 Series Switch Hardware Installation Guide*
	IE 3010	*Cisco IE 3010 Switch Hardware Installation Guide*
	CGS 2520	*Cisco CGS 2520 Hardware Installation Guide*
	ESM	*Cisco CGS 2520 Hardware Installation Guide* **Note:** The *Cisco CGS 2520 Hardware Installation Guide* serves as CLI-based Setup reference for the ESM.
	IE 4000	*Cisco IE 4000 Switch Hardware Installation Guide*
	IE 5000	*Cisco IE 5000 Hardened Aggregator Hardware Installation Guide*

Table 3 Methods for Assigning IP Information (continued)

Method	Platform	Document
DHCP-based autoconfiguration	ESS 2020	*Cisco Embedded Service 2020 Series Software Configuration Guide*
	IE 2000	*Cisco IE 2000 Series Switch Software Configuration Guide*
	IE 2000U	*System Management Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches*
	IE 3000	*Cisco IE 3000 Series Switch Software Configuration Guide*
	IE 3010	*Cisco IE 3010 Series Switch Software Configuration Guide*
	CGS 2520	*CGS 2520 Switch Software Configuration Guide*
	ESM	*Cisco Connected Grid Ethernet Switch Module Interface Card Software Configuration Guide*
	IE 4000	*Cisco Industrial Ethernet 4000 Series Switch Software Configuration Guide*
	IE 5000	*Cisco IE 5000 Hardened Aggregator Hardware Installation Guide*
Manually assigning an IP address	IE 2000	*Cisco IE 2000 Series Switch Software Configuration Guide*
	IE 2000U	*System Management Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches*
	IE 3000	*Cisco IE 3000 Series Switch Software Configuration Guide*
	IE 3010	*Cisco IE 3010 Series Switch Software Configuration Guide*
	CGS 2520	*CGS 2520 Switch Software Configuration Guide*
	ESM	*Cisco Connected Grid Ethernet Switch Module Interface Card Software Configuration Guide*
	IE 4000	*Cisco Industrial Ethernet 4000 Series Switch Software Configuration Guide*
	IE 5000	*Cisco IE 5000 Hardened Aggregator Hardware Installation Guide*

Limitations and Restrictions

We recommend that you review this section before you begin working with the switch. These are known limitations that will not be fixed, and there is not always a workaround for these issues. Some features might not work as documented, and some features might be affected by recent changes to the switch hardware or software.

- **CSCuo83410**

Symptom When a port gets congested, classes with a larger queue-limit size are not receiving more frames per second than the classes with a smaller queue-limit size.

Conditions This issue occurs on the IE 4000 when queue-limit sizes are configured unequally in classes. Classes with a larger queue-limit size are not receiving more frames per second than the classes with a smaller queue-limit sizes.

Workaround There is no workaround for this issue.

- **CSCup58174**

Symptom CIP V4Router object does not display some metrics that **show run | i route** displays on the IE 2000.

Example of behavior:

```
---------------------------

IE2000_2016(config)#ip route 10.0.0.11 255.255.255.255 50.0.0.50 name ?
  WORD  Name of the next hop

IE2000_2016(config)#ip route 10.0.0.11 255.255.255.255 50.0.0.50 name fa1/1
IE2000_2016(config)#end
IE2000_2016#show run | i route

ip route profile
ip route 0.0.0.0 0.0.0.0 FastEthernet1/9 172.27.168.129
ip route 10.0.0.1 255.255.255.255 20.0.0.2
ip route 10.0.0.2 255.255.255.255 Loopback10
ip route 10.0.0.2 255.255.255.255 Loopback10 20.0.0.2
ip route 10.0.0.3 255.255.255.255 Vlan1
ip route 10.0.0.3 255.255.255.255 Vlan10
ip route 10.0.0.3 255.255.255.255 Vlan10 40.0.0.4
ip route 10.0.0.11 255.255.255.255 10.0.0.11
ip route 10.0.0.11 255.255.255.255 50.0.0.50 name fa1/1
ip route 10.0.0.7 255.255.255.255 50.0.0.7 permanent multicast
ip route 10.0.0.8 255.255.255.255 44.44.44.44 permanent multicast
ip route 10.0.0.6 255.255.255.255 dhcp

IE2000_2016#show cip object v4router 0
1: 0.0.0.0 0.0.0.0 0.0.255.255
2: 10.0.0.1 255.255.255.255 20.0.0.2
3: 10.0.0.2 255.255.255.255 0.0.255.255
4: 10.0.0.3 255.255.255.255 0.0.255.255
5: 10.0.0.11 255.255.255.255 50.0.0.50
6: 10.0.0.7 255.255.255.255 50.0.0.7
7: 10.0.0.8 255.255.255.255 44.44.44.44
8: 0.0.0.0 0.0.0.0
```

Conditions There are differences between **show run | i route** display and **show cip object v4router**.

Workaround There is no workaround for this issue.

- **CSCup75235**

Symptom SFP types SFP-GE-L and GLC-EX-SMD sometimes generate Rx power high warning without significant traffic.

Conditions Insert SFPs (SFP-GE-L and GLC-EX-SMD) into CGS 2520. You can sometimes observe that the Rx power high warning syslog message is generated at every monitoring interval. This also affects IE 4000 and IE 5000 switches.

If **snmp-server enable trap transceiver** is configured, a trap is also generated.

Workaround There is no workaround for this issue. The SFPs could have gone bad or the optical cable is bad. Observe the SFPs, cable and traffic, and if you find issues replace the SFPs.

There is no functionality issue observed under this condition. This seems to be a false positive.

- **CSCuq16134**

Symptom CPU protection and dot1x are mutually exclusive. When enabled, these features work fine. When the IE 2000U or CGS 2520 have TrustSec configured to work with ISE, dot1x fails to authenticate.

Conditions CPU protection is enabled.

Workaround Disable CPU protection by running the following command: **no policer cpu uni all**

- **CSCus02105**

Symptom **show cip object v4router 0** does not display correct routes in some scenarios. Issue was first seen on an IE 2000; however, it applies to all IE and CG switches that support VLAN configuration and CIP features.

Conditions If you configure a cip unsupported route, for example, ip route 0.0.0.0 0.0.0.0 fa1/1 172.27.168.129, the route will not be displayed properly in the **sh cip object v4router** command output. All following routes (including supported routes such as ip route 0.0.0.0 0.0.0.0 fa1/1 or ip route 0.0.0.0 0.0.0.0 vlan1) also will not be displayed properly.

Workaround Reload the switch.

Caveats

This section addresses the open and resolved caveats in this release and provides information on how to use the Bug Search Tool to find further details on those caveats. This section includes the following topics:

- Open Caveats, page 14
- Resolved Caveats, page 18
- Accessing Bug Search Tool, page 23

Open Caveats

- **CSCuq21005**

Symptom In-line editing becomes unresponsive on the Device Manager Port Thresholds page on IE 2000, IE 3000 and IE 4000 switches.

Conditions Editing a field too quickly can cause in-line editing to become unresponsive.

Workaround Editing the box repeatedly works if the user waits one or two seconds for Device Manager to push the update to the device.

- **CSCuq21253**

Symptom Boundary clock does not respond to IGMP query on an IE3000.

Conditions Network application is trying to synchronize time across the switch for alarms and events.

Workaround The following workaround was tested in networks using only Cisco IE switches.

Configure the following command on switches that are not PTP-aware (switches configured in PTP forward mode):

ip igmp snooping vlan *vlan-id* **static ip address interface** *interface-id*

where **vlan** is a PTP VLAN and **interface** is an interface on which PTP must be forwarded.

- **CSCuq72745**

Symptom On the IE 3010, the GE port shows speed as 100Mbps when another GE port is connected.

Conditions This issue occurs when the user changes media between SFP and RJ45 on the same combination interface.

Workaround Issue a **shut** and **no shut** on the interface.

- **CSCur00491**

Symptom Not able to configure the input alarm 3 and 4 in CGS 2520 and IE 3010 devices from the CLI (Relay, Notifies, and Syslog options).

Conditions Input alarms 3 and 4 appear to be enabled in **show alarm settings** output but the settings are not retained after reloading the device.

Workaround There is no workaround for this issue.

- **CSCur09517**

Symptom The PRP LED did not light up correctly. Observed anomalies in PRP LED in the events below:

Conditions Impacted platform: IE4K

1. Issue a **shut/no shut** on logical PRP interface (interface prp-channel 1|2).

2. Unplug and plug in cables for uplink ports.

3. Certain sequence issues observed with issuing **shut/no shut** on logical interface PRP-channel 1 followed by logical interface PRP-channel 2 and vice versa.

Workaround There is no workaround for this issue.

- **CSCur24288**

Symptom On the Cisco IE 2000 and IE 3000, the GetAttList time sync obj 0x43 Reply sequence is inconsistent with the request.

Conditions Get Attributes List was executed against the time sync object in the IE switches. The sequence was explicitly specified with attributes of variable size at the end in order to simplify parsing the reply. While the CIP specification does not explicitly require that the reply follow the sequence of the request, this is the typical (and therefore expected) behavior in released products so far observed.

The initial sequence attempted was

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 18, 19, 20, 27, 28, 12, 13

However the reply sequence received was

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 18, 19, 20, 27, 28

To verify this, a get attributes list with sequence was attempted

5, 4, 3, 2, 1, 6, 7, 8, 9, 10, 11, 18, 19, 20, 27, 28, 12, 13

However the reply sequence received was

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 18, 19, 20, 27, 28

Workaround There is no workaround for this issue.

- **CSCut31523**

Symptom Switch running Parallel Redundancy Protocol (PRP) disables PRP1 interface at least twice at random periods.

Conditions IE 4000 running release 15.2(2) with Parallel Redundancy Protocol (PRP) configured.

Workaround To re-enable PRP on the switch, connect to the switch via a console port and enter **shut** and then **no shut** commands.

- **CSCut57413**

Symptom .The PRP channel should not be in connected state when one of the ports is in suspended/not connected state.

Condition Any port configuration mismatch will put the port in a suspended state, and if that port is part of the PRP channel, the channel is still connected.

Workaround Remove the conflicts in the port configurations. Entering **shut**/**no shut** will bring the port UP.

- **CSCuv46039**

Symptom Interface link flaps occurred on the IE 4000 with use of aggressive **lsl-age** timer under REP port configuration.

Conditions This issue occurs in a REP Ring with three or more nodes with **lsl-age** timer set to 120 msecs and after a period of a few minutes to a couple of hours.

Another side affect could be a malloc failure (CAM flush) with repeated link flaps which may cause the switch to crash.

Workaround Increase **rep lsl-age** timer to a value greater then 120 msec. Recommended value is 3000 msec.

- **CSCuv49763**

Symptom HSRP Distribution on the IE 5000 gives high multicast traffic when one of the links goes down and REP convergences. Seeing over 5 seconds convergence time for L2 multicast.

Conditions Network set up:

- Distribution: IE 5000 HSRP, version: 15.2(2)EB

- Access: Twelve IE4000s connected in a ring with fiber link

- Resiliency protocol tested: REP

- Config: All links are trunk to allow tagged and untagged traffic

- Traffic pattern: IXIA L2 Unicast/Multicast traffic (500 packets per second)

- IE5K HSRP ports on both sides (connects to IE4000) as primary and secondary edge ports of REP ring

Workaround There is no workaround for this issue.

- **CSCuv82048**

Symptom In Device Manager, on the Configure > Security > ACL page, when you attempt to export ACLs and the combined number of access control entries (ACEs) is more than 10, the operation fails and an error message appears.

Conditions This issue occurs on the IE 3000.

Workaround Export ACLs in multiple operations so that the total number of ACEs in each operation does not have more than ten ACEs.

- **CSCuw28503**

Symptom On IE platforms, Flex-Link failover time could be around 700msec when using Gigabit Ethernet ports.

Conditions Steps to reproduce:

1. Configure two Gig links on the IE switch as flex links.
2. Shut a member link and wait for the traffic to switch over to the other link. Failover time of around 700 msec is seen.

Workaround Use Fast Ethernet ports to implement Flex-Link.

- **CSCuw95573**

Symptom ciscoenvMonAlarmContact MIB object is not supported in this release.

Conditions Switch (IE 2000, IE 3000, IE 4000) was running Cisco IOS 15.2(4)EA and SNMP was enabled.

Workaround Use the CLI for setting alarm contacts as follows:

```
switch(config)# alarm contact 1 descriptions TEST
```

You can view it from the following command:

```
switch# show run | inc alarm
alarm contact 1 description TEST
```

- **CSCux98673**

Symptom With GLC-FE-T-I, the FCS-Err/Rcv-Err counters (show interfaces counter errors) does not increment when Bad FCS frames are received.

Conditions The issue occurs on IE 2000, CGS 2520, ESM and IE 3000 and IE 3010 platforms.

Workaround There is no workaround for this issue.

- **CSCuz27193**

Symptom DHCP client connected to IE3000 is getting IP address initially with no problems, but after 50% lease-time expiry, the client cannot renew its IP address quickly, it takes around 2-3 minutes to renew the IP address. Switch fails to forward DHCP-ACK packets (received from the DHCP Server) to the client as it is not able to learn the mac-address of the PC connected and then drop the DHCP ACK.

Conditions Issue was found on the following system: Hardware: IE-3000-8TCSW:15.2(3)E3 with DHCP snooping and option82 enable.

Workaround Disable dhcp snooping or never release IP address.

- **CSCuz34012**

Symptom User is able to configure and generate alarms for ptc-heater and port-asic-junction-temperature on an IE 5000 when running the 15.2(4)EA1 release even though the commands and functionality are not supported in that release.

Conditions IE 5000 was running 15.2(4)EA1.

Workaround There is no workaround for this feature. Do not configure the unsupported functionality.

- **CSCva53722**

Symptom Standalone devices are in an initializing state before joining the stack, while other members are in different VLAN Trunking Protocol (VTP) modes. Issue is not observed when the existing stack is in different VTP modes. Issue is not observed when four standalone boxes in VTP server mode are combined to form a four member stack.

Conditions Changing VTP mode to server or disabling VTP on standalone devices before enabling stacking and rebooting them.

Workaround Members will join the stack but they remain in Initialized state.

- **CSCva53971**

Symptom Incorrect port details are displayed in the output of **show inventory** for stack enabled ports.The PID of SFP inserted is displayed correctly.

Conditions Observed in normal conditions.

Workaround No effect on functionality.

Resolved Caveats

- **CSCuq25098**

Symptom BX-40-DAI Description is shown as DA.

Conditions On the IE 2000, IE 3000, and IE 3010, the command **show inventory PID** on all SFP-pluggable ports with DA-I connected displays the SPF as DA.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E.

- **CSCuq52270**

Symptom Gi1/2 is not compatible with Gi1/1 and will be suspended (speed of Gi1/2 is 1000M, Gi1/1 is auto).

Conditions Affects IE 4000 and IE 5000 platforms.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E.

- **CSCur00491**

Symptom Not able to configure the input alarm 3 and 4 in CGS 2520 and IE 3010 devices from the CLI (Relay, Notifies, and Syslog options).

Conditions Input alarms 3 and 4 appear to be enabled in **show alarm settings** output but the settings are not retained after reloading the device.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E.

- **CSCur35236**

Symptom RJ45 Link comes up on combo port with different Media Type on both sides.

Conditions Configure different Media Type on both sides for Combo ports.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E.

- **CSCuv45285**

Symptom The MRP Manager blocked port shows the link up/LED color as flashing green (IE 2000). The LED should be solid amber/red instead.

Conditions When the MRP Ring is open, one of the ports is blocked. LED corresponding to the blocked MRP port should not have a flashing green light.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E.

- **CSCuv45287**

Symptom The MRP Manager blocked port shows STP in forwarding mode (IE 2000).

Conditions You can observe this issue when the MRP manager port status is blocked; and you display the STP status for the port.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E.

- **CSCuv84571**

Symptom On the IE 4000 in Device Manager, changing between IP assignment modes deletes the static IP address.

Conditions Steps to reproduce:

1. Launch the device in a browser.
2. Select Configure > Network > VLAN Management.
3. Add a VLAN with a static IP address and save it.
4. Edit the same VLAN and switch between IP assignment modes (No IP Address, Static, and DHCP).
5. The created static IP address is deleted.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E.

- **CSCuv91029**

Symptom Interface vlan in the range of 25 to 32 can disappear after reload on an IE 5000.

Conditions IE 5000 running 15.2(2)EB, 15.2(2)EB1 or 15.2(4)EA1 software.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E.

- **CSCuv91046**

Symptom On the IE 4000, igmp configurations under interface port-channel20 are not removed when the interface changes to a layer2 switch port and then back to layer3 port.

Conditions Steps to reproduce:

1. Configure igmp under layer3 interface po22.
2. Change interface po22 to a layer2 switchport.

   igmp configurations are removed from the interface as soon as it becomes a layer2 interface.
3. Change interface po22 back to a layer3 interface.

   The script expects igmp configurations to not be shown under interface change back to layer3 interface.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E.

- **CSCux52557**

Symptom IE2000 supports license upgrades from Lanlite to IPlite via LIC-IE2000-L-IP=. -L PID (Lanlite) failed to upgrade to IPlite with 15.2(3)EA.

Conditions Prior to 15.2(5)E, two steps were required to upgrade using LIC-IE2000-L-B= and LIC-ie2000-IP-L=, Starting with15.2(5)E you can now apply LIC-IE2000-L-IP= to upgrade from Lanlite to IPlite.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E.

- **CSCux59845**

Symptom Boundary Clock does not forward PTP Management packets across VLANs on IE4000 and IE5000. This issue also affects IE2000 and IE3000.

Conditions Previous design had PTP Management packets forwarded within the same vlan. Design changes have PTP packets forwarded across different VLANs and routed ports.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E.

- **CSCux75168**

Symptom Extra VLAN entry with a 5-digit value can be seen under **show vlan** command after the creation of an extended VLAN on an IE3010.

```
Switch#sh vlan | i active
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
100 VLAN0100 active
101 VLAN0101 active
102 VLAN0102 active
103 VLAN0103 active
104 VLAN0104 active
105 VLAN0105 active
106 VLAN0106 active
107 VLAN0107 active
108 VLAN0108 active
109 VLAN0109 active
110 VLAN0110 active
111 VLAN0111 active
112 VLAN0112 active
113 VLAN0113 active
114 VLAN0114 active
115 VLAN0115 active
116 VLAN0116 active
117 VLAN0117 active
118 VLAN0118 active
119 VLAN0119 active
120 VLAN0120 active
121 VLAN0121 active
122 VLAN0122 active
123 VLAN0123 active
124 VLAN0124 active
22345 VLAN2345 active <<<<<----
2345 VLAN2345 active
```

Issue is not seen under **show vlan brief** display.

Conditions Creation of an extended VLAN. Issue does not always appear immediately after VLAN creation.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E.

- **CSCux94263**

Symptom MRP licenses are not portable via SD card for IE2000 and IE4000.

Conditions An attempt to port an MRP license to a IE4000 switch using a SD card did not work. Issue occurs during a device replacement. The MRP license stays on the replaced device and does not 'travel' with the SD flash to the replacement device.

Workaround Need to activate MRP Licenses again using command line interface. See the “Right to Use (RTU) Licenses” chapter in the Cisco Industrial Ethernet 4000 Series Switch Software Configuration Guide.

- **CSCuy01664**

Symptom Input service-policy does not function after executing a reload on:

Platform: IE-2000U-16TC-GPSW Version: 15.0(2)EH SW Image: flash:/ie2000u-lanbasek9-mz.150-2.EH/ie2000u-lanbasek9-mz.150-2.EH.bin

Also present in latest release: 15.2(4)EA.

Conditions Reload triggers the problem, as long as the system is up and configured it will work but once reloaded/power-cycled QoS no longer functions as desired previous to reload/power-cycle.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E.

- **CSCuy12632**

Symptom IE-3000 switch does not include Option 12 in DHCPDISCOVER, this happens if any configuration applied to the switch (config.text in flash:), if no configuration (Switch default, no config.text in flash:) Option 12 is include DHCPDISCOVER.

Conditions DHCP server----Ethernet----Switch (with config.text in flash:, already configured in other words)

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E.

- **CSCuy13431**

Symptom A vulnerability in the packet processing microcode of Cisco Industrial Ethernet 4000 Series Switches and Cisco Industrial Ethernet 5000 Series Switches could allow an unauthenticated, remote attacker to cause corruption on packets enqueued on the device for further processing.The vulnerability is due to improper processing of some ICMP IPv4 packets. An attacker could exploit this vulnerability by sending ICMP IPv4 packets to an affected device. A successful exploit could allow an attacker to corrupt the packet enqueued immediately after the packet sent. This may impact control traffic to the device itself (ARP traffic) or traffic transiting the device.

Conditions The following Cisco products are affected by this vulnerability:

- Cisco Industrial Ethernet 4000 Series Switches when running Cisco IOS releases 15.2(2)EA, 15.2(2)EA1, 15.2(2)EA2 or 15.2(4)EA.
- Cisco Industrial Ethernet 5000 Series Switches when running Cisco IOS releases 15.2(2)EB or 15.2(2)EB1

Note: The following switches are not affected:

- The Cisco Industrial Ethernet 2000 Series Switches and the Cisco Industrial Ethernet 3000 Series Switches are NOT affected by this vulnerability. No other Cisco products are affected by this vulnerability.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E.

- **CSCuy40096**

Symptom GLC-FE-T-I SFP were not configured to handle frame sizes of length 1916 bytes, so the frames were dropped at the PHY itself. Jumbo frames larger than 1916 bytes were also dropped.

Conditions The issue happened on IE 2000, IE 2000U, CGS 2520, ESM, IE 3000 and IE 3010 platforms.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E.

- **CSCuy41805, CSCuy58243**

Symptom If the RX fiber is removed from the impacted IE switch when using a FE single mode optic, the remote switch will not be notified of the problem and the remote link will stay in an up state preventing fast network recovery.

Conditions Always will happen when using single mode FE optics when the RX strand is disconnected/broken when connected to an IE 4000 or IE 5000 switch.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E.

- **CSCuy76740**

Symptom A vulnerability in processing of crafted ARP packets of Cisco CGS-2520 switches could allow an unauthenticated, adjacent attacker to cause high CPU condition on the affected device that may eventually cause loss of BPDU frames and thus turn the device into a STP root.

The vulnerability is due to insufficient logic in processing of certain crafted ARP packets, causing them to be handled by the CPU. An attacker could exploit this vulnerability by sending a flood of crafted ARP packets to be processed by an affected device. An exploit could allow the attacker to cause high CPU condition on the affected device that may eventually cause loss of BPDU frames and thus turn the device into a STP root.

Conditions When invalid ARP packet with all zero destination mac address in it.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E.

- **CSCuy81921**

Symptom Traffic on Gig 1/4 ceases as soon as prp channel is added on IE 4000 and IE 5000. Observed the ping traffic did not go through.

Conditions When the SVI is created on both ends, assigned the IP address on both ends. Once the PRP channel is created, cannot ping the address of the other end.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E.

- **CSCuy83711**

Symptom User is able to configure and generate alarms for ptc-heater and port-asic-junction-temperature on an IE 5000 when running the 15.2(4)EA1 release even though the commands and functionality are not supported in that release.

Conditions IE 5000 was running 15.2(4)EA1.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E.

- **CSCuz26633**

Symptom IE-2000:MRP ring interface down/up caused OutDiscards.

Conditions MRP interface down/up.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E.

- **CSCuz48728**

Symptom Encounter crash occurred on an IE-4000-4T4P4G-E running 15.2(4)EA or 15.2(4)EA1 with an uplink to a Catalyst 2000 switch.

Conditions IE-4000-4T4P4G-E running 15.2(4)EA or EA1 with an uplink port-channel to Catalyst 2000.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E.

- **CSCuz56319**

Symptom Class 3 and 4 PDs do not reliably auto backup with the following setting on an IE3000: **power inline auto max 15400**

Conditions IE 3000 with IEM-3000-4PC running Cisco IOS release 15.0(2)EY3 operating with Class 3 and 4 PDs.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E.

- **CSCva25556**

Symptom **sh prp channel** detail shows the prp protocol is Disabled even the channel is up.

Conditions

1. Enable PRP on IE5000
2. Check the command **sh prp channel detail.** Protocol is coming up as disabled.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E.

Accessing Bug Search Tool

You can use the Bug Search Tool to find information about caveats for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

To access Bug Search Tool, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To access the Bug Search Tool, enter the following URL:

bst.cloudapps.cisco.com/bugsearch

Documentation Updates

This section includes the following latest updates to documentation for IE switches:

- Enabling Logging Alarms for Syslog Messages, page 23
- Resilient Ethernet Protocol (REP), page 23
- IRIG Protocol, page 23

Enabling Logging Alarms for Syslog Messages

The following information is relevant to all IE Switches software releases from Release 12.2(58)SE onward (CSCvg26502).

On IE switches, there is an option to configure temperature alarm levels as noted in the "Configuring the Switch Alarms: Associating the Temperature Alarms to a Relay" section within IE Switch Software Configuration Guides.

However, configured alarms do not generate any syslogs until you set Major alarm **logging alarm 2** and Minor alarm l**ogging alarm 3** for temperature threshold alarms.

IMPORTANT: The logging alarm **must be enabled** to generate syslog messages.

Resilient Ethernet Protocol (REP)

See the revised configuration recommendations for the **lsl-age-timer** *timer-value* command (CSCux92117) in the "Configuring REP Configurable Timers" section in the REP chapter of the LAN Switching Configuration Guide, Cisco IOS XE Release 3S.

IRIG Protocol

IRIG-B output support on IE 5000 platforms begins with Release 15.2(5)E.

Note: IRIG-B *input* is **not** supported.

The IRIG protocol will be implemented for format-B per IRIG standard 200-04 with support for TTL (B002, B003) and AM (B122, B123) time codes.

Listed below are the new **config** and **show** commands for IRIG-B on the IE 5000:

```
ie5000#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
irig_ie5k_10k_2022(config)#irig ?
  mode  setup mode

ie5000(config)#irig mode ?
  AM02   AM-B123 format
  AM03   AM-B123 format
  TTL02  TTL-B002 format
  TTL03  TTL-B003 format

ie5000(config)#irig mode AM
irig_ie5k_10k_2022(config)#irig mode AM02 ?
  dir  direction

ie5000(config)#irig mode AM02 dir ?
  in   input direction
  out  output direction

ie5000(config)#irig mode AM02 dir in
IRIG INPUT not currently supported

ie5000(config)#irig mode AM02 dir out ?

ie5000(config)#end
irig_ie5k_10k_2022#show run | i irig
hostname irig_ie5k_10k_2022
irig mode AM03 dir out
irig mode TTL03 dir out
irig_ie5k_10k_2022#

ie5000# show irig
IRIG-B Digital mode TTL03 dir out
IRIG-B Analog mode AM03 dir out

IRIG-B Clk Id 2 Source NTP  time: Year: 36 Day: 2 Hour 0 Min 41 Sec 45
                            ns 1136162505981032431 (0xFC475C7901DF7EF)
```

Related Documentation

Table 4 Related Documentation

Device or Feature	Related Documents
Cisco 2500 Series Connected Grid Switches	http://www.cisco.com/go/cgs2520
Cisco Embedded Service 2020 Series Switches (ESS 2020)	http://www.cisco.com/c/en/us/support/switches/embedded-service-2020-series-switches/tsd-products-support-series-home.html
Cisco Ethernet Switch Module (ESM) for CGR 2010	http://www.cisco.com/go/cgr2000
Cisco Industrial Ethernet 2000 Series Switches	http://www.cisco.com/go/ie2000
Cisco Industrial Ethernet 2000U Series Switches	http://www.cisco.com/go/ie2000u
Cisco Industrial Ethernet 3000 Series Switches	http://www.cisco.com/go/ie3000
Cisco Industrial Ethernet 3010 Series Switches	http://www.cisco.com/go/ie3010
Cisco Industrial Ethernet 4000 Series Switches	http://www.cisco.com/go/ie4000
Cisco Industrial Ethernet 5000 Series Switches	http://www.cisco.com/go/ie5000

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

No combinations are authorized or intended under this document.

© 2016–2018 Cisco Systems, Inc. All rights reserved.