Release Notes for Cisco IOS Release 15.2(4)EA1

Last Updated: March 1, 2017
First Published: March 31, 2016

Cisco IOS Release 15.2(4)EA1 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(4)EA1and 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 6.

For a complete list of documentation for the platforms associated with this release, see Related Documentation, page 28.

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

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(4)EA1

Table 1 lists new features added in Cisco IOS Release 15.2(4)EA1.

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

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

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(4)EA1

Feature	Platform	Description	Related Documentation
NTP to PTP Translation (Time Services)	IE 5000	This time service enhancement allows the IE switches to act as Grandmaster clocks to the PTP hierarchy with NTP as the time source. The NTP time source ties the PTP working clock to the everyday "wall clock." This allows the customer to use PTP and NTP generated timestamps together during troubleshooting and analysis. In addition, NTP is more cost effective and robust than GPS for applications that only need ~1 second precision for wide-area synchronization.	■ Precision Time Protocol Software Configuration Guide for IE 4000 and IE 5000 Switches ■ Device Manager Online Help
Media Redundancy Protocol (MRP) and PROFINET Enhancements	IE 4000	MRP (Media Redundancy Protocol), an open standard industrial protocol, can support up to 50 nodes with maximum recovery time up to 200ms. MRP operates at the MAC layer and is commonly used in conjunction with the PROFINET standard for industrial networking in manufacturing. This release supports MRP manager and client and includes the following enhancements to PROFINET: ■ PROFINET stack upgrade to version 2.31. ■ PROFINET support for MRP Manager (MRM) and Client (MRC) functionality. PROFINET (PNIO) Certification with v2.3	■ Media Redundancy Protocol Configuration Guide for IE 2000 and IE 4000 Switches ■ Device Manager Online Help
Hardware Watchdog Reset	IE 2000, IE 3000, IE 4000 IE 5000	The Hardware Watchdog Reset feature causes the switch to reload if IOS software is unresponsive for a certain period of time (5 minutes). The CPU Hardware Watchdog ensures that the switch reloads if software is hung for whatever reason.	Hardware Watchdog Reset, page 25
MACsec (IEEE 802.1AE)	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 only supported on 1G uplinks. **Note** You must have the IP Service license installed to support the MACsec feature.	Configuring MACsec Encryption

Table 1 New Feature Summary for Cisco IOS Release 15.2(4)EA1

Feature	Platform	Description	Related Documentation
Express Setup enhancements with CIP support for IE Switches	IE 5000	This feature enhances Express Startup to limit manual switch intervention. There are three options for using Express Setup: ■ You must configure a new in the box (NIB) switch that has no configuration file loaded (config.text / vlan.dat) directly via a console cable. ■ You can configure the switch with the existing Express Setup method. The existing Express Setup behavior is enhanced to improve the failure LED indication behavior. ■ You can have an IP address assigned to the switch without using Device Manager if you installed the switch in an already running environment with certain services available (DHCP).	■ Device Manager Online Help ■ Express Setup Enhancements, page 26 ■ For details on Express Setup documentation for all IE switches, see the Express Setup Program entry in Table 3Methods for Assigning IP Information, page 11

Locate Switch	IE 5000	When enabled, **Locate Switch** causes all possible LED to glow in ALT_RED and GREEN once the locate switch is enabled with a specific time. This performance varies from previous releases. (CSCux75707)
		The Locate Switch time setting has been changed from <9-255> to <0-255> time in seconds:
		0: Stop Blink
		9-255: Blink LED
		Enter the following **show** command to verify your settings:
		`Switch# sh locate-switch`
		`Locate Switch enabled!!`
		`total time: 255 sec`
		`time left: 249 sec`
			■ Device Manager Online Help

Device Manager (DM) Enhancements	Varied See Description.	■ Ability to launch Device Manager in Express Setup medium press mode (as well as previously supported short press mode). ■ Support for Wireless macros.	■ Device Manager Online Help

System Requirements

This section describes the following system requirements for Cisco IOS Release 15.2(4)EA1:

- 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 1New Feature Summary for Cisco IOS Release 15.2(4)EA1, page 4.

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 6
- Archiving Software Images, page 7
- Upgrading a Switch by Using the CLI, page 7
- 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(4)EA1, we will **no longer release** the IE 3000 IP services image. The latest release for IPService on the IE 3000 is Cisco IOS Release 15.2(4)EA.

Table 2 Cisco IOS Software Image Files

File Name	Description
c2020-universalk9-tar.152-4.EA1.tar	ESS 2020 universal image file
ie2000-universalk9-tar.152-4.EA1.tar	IE 2000 universal image file
ie3010-ipservicesk9-tar.152-4.EA1.tar	IE 3010 IP services image file
ie3010-lanbasek9-tar.152-4.EA1.tar	IE 3010 LAN base image file
ies-lanbasek9-tar.152-4.EA1.tar	IE 3000 LAN base image file
ie2000u-ipserviceslmk9-tar.152-4.EA1.tar	IE 2000U IP services image file
ie2000u-lanbaselmk9-tar.152-4.EA1.tar	IE 2000U LAN base image file
cgs2520-ipserviceslmk9-tar.152-4.EA1.tar	CGS 2520 IP services image file
cgs2520-lanbaselmk9-tar.152-4.EA1.tar	CGS 2520 LAN base image file
grwicdes-ipserviceslmk9-tar.152-4.EA1.tar	ESM IP services image file
grwicdes-lanbaselmk9-tar.152-4.EA1.tar	ESM LAN base image file
ie4000-universalk9-tar.152-4.EA1.tar	IE 4000 Universal image file
ie5000-universalk9-tar.152-4.EA1.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 6 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 19
- Accessing Bug Search Tool, page 25

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.

- **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 There is no workaround for this issue.

- **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.

- **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.System reload is required, a port shut/no shut will not reset.

Workaround There is no workaround for this issue.

- **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 There is no workaround for this issue.

- **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.

- **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 Manually input the static IP address again.

- **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 None. Do not use interface VLANs in the range 25 to 32 on IE 5000.

- **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 There is no workaround for this issue.

- **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 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
```

- **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.

- **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.

- **CSCuy40096**

Symptom GLC-T-FE-I SFP supports only a maximum frame size of 1916 bytes. Jumbo frames larger than 1916 bytes are dropped.

Conditions The issue happens with IE 2000, IE 2000U, CGS 2520, ESM, IE 3000 and IE 3010 platforms.

Workaround There is no workaround for this issue.

- **CSCuy41805**

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 No workaround to fix FEFI but impact could be lessened by using a higher level protocol to detect link failure such as BFD or by protocol timers.

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

- **CSCvd25567**

Symptom Inserting GLC-FE-T-I SFP puts FE ports of IE2000 unit in err-disable state.

Conditions The issue affects certain IE2000 SKU types on which the issue is always present. There are no pre-conditions.

Affected Cisco SKUs:

IE-2000-4TS-L (on uplinks)

IE-2000-4TS-B (on uplinks)

IE-2000-8TC-L (on uplinks)

IE-2000-8TC-B (on uplinks)

IE-2000-16TC-L (on both uplink and downlink)

IE-2000-16TC-B (on both uplink and downlink)

IE-2000-16TC-G-L (on downlink)

IE-2000-16TC-G-E (on downlink)

IE-2000-16TC-G-E-U (on downlink)

IE-2000-16TC-G-X (on downlink)

IE-2000-16TC-G-N (on downlink)

Workaround There is no workaround.

Resolved Caveats

- **CSCup53568**

Symptom The system allows you to configure more than 16 routes, but they are not visible in the ip route table.

Conditions On an IE 2000 with ip routing enabled, configure more than 16 routes. They are not visible in the ip route table or in **show running-configuration**. There is no error/warning message when you exceed the 16 route limit. Functionally, there is no impact.

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1.

- **CSCur62153**

Symptom Logging out of Device Manager in the IE browser terminates all tab sessions. The user must log in again to any web application sessions that were terminated.

Conditions This issue occurs only with the IE browser.

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1.

- **CSCus55821, CSCur38690**

Symptom DHCPv6 relay crashed when the router (ASR1000, ASR1006) configured as a DHCP relay, received a Relay-forward DHVPv6 packet with malformed options. Affected switches IE 2000 and IE 2000U.

Conditions The vulnerability was due to insufficient validation of DHCPv6 relay messages.

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1.

- **CSCut85937**

Symptom Poor clock synchronization with the grandmaster clock. IE 2000U does not synchronize in Cisco IOS Release 15.2(3)E2.

Conditions Occurs during normal operation when PTP is configured as the power profile.

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1,15.2(3)E3 and15.2(4)E.

- **CSCuv25569**

Symptom GLC-T was not working on IE 2000U.

Conditions GLC-T was not supported in the IE2000U Gigabit uplink port at initial release.

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1.

- **CSCuv37850**

Symptom A device connected to a switch is not able to calculate the Peer Delay.

Conditions This issue occurs when the **port-type uni** configuration is applied to a port, on any platform that supports the **port-type uni** configuration (CGS 2520, IE 2000U, IE 4000, or IE 5000).

The PDel messages share the 01-80-C2-00-00-0E destination MAC address with a variety of other hop-by-hop protocols. The **port-type uni** command causes the switch to drop all messages sent to the 01-80-C2-00-00-0E destination MAC, including the PDel messages.

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1.

- **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.System reload is required, a port shut/no shut will not reset.

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1.

- **CSCuv83923**

Symptom In Device Manager on the Configure > Spanning Tree > STP Settings Port Fast tab, Device Manager shows both BPDU Filtering and BPDU Guard as enabled.

Conditions This issue occurs on the IE 2000, IE 3000, and IE 4000 in Device Manager only. If either BPDU Guard or BPDU Filtering is enabled, Device Manager displays both features as enabled. By design, both BPDU Guard and BPDU Filtering cannot be configured at the same time.

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1.

- **CSCuv90642**

Symptom On the IE 3K platform, the unit boots into the secondary boot loader mode when the " boot manual" configuration command is issued. While in the secondary boot loader mode, the primary boot loader environment variables are not seen when the set command is issued.The primary boot loader environment variable contain the critical parameters like the system serial number, MAC address and Model Number.

Conditions The issue is seen if the IE3K unit goes for a boot loader upgrade while loading IOS images with the following versions: 15.2(2)E, 15.2(2)E1, 15.2(2)E2, 15.2(2)E3, 15.2(3)EA,15.2(3)E1 and 15.2(3)E2.

The unit will undergo a boot loader upgrade only if the earlier secondary boot loader version on the unit was 12.2(44r)EX5. If the IE3K unit was already running secondary boot loader version 12.2(53r)EZ3, then the unit will not go for a boot loader upgrade while loading the above mentioned IOS releases; and, the issue will not be seen.

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1.

- **CSCuw06435**

Symptom Siemens TIA Portal V12 may encounter a software application crash during an upgrade of the GSD via TIA Portal V12 from version dated V2.3-20140212.XML to IOS bundled GSD V2.31-20150807.XML.

Conditions The software crash occurs on the IE 2000 when upgrading GSD using the TIA GUI.

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1.

- **CSCuw15036**

Symptom On the IE 2000, IE 3000, and IE 4000, when the host name is changed to other than the default name through the CLI, then the DUT is reloaded without saving the configuration and deleting other configuration files. The switch does not boot up with the default hostname but instead boots up with the changed hostname.

Conditions This issue occurs when PROFINET is enabled and then is disabled, and then the hostname is set to the default name.

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1.

- **CSCuw20398**

Symptom Network-policy command is not available on IE 3010 and CGS 2520.

Conditions The network-policy command was not supported on IE 3010, CGS 2520, IE 2000U and ESM for CGR 2010. It was supported on IE 2000, IE 3000, IE 4000 and IE 5000.

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1.

- **CSCuw30659**

Symptom .save files accumulate in the flash folder when a new image is upgraded from CLI.

Conditions This issue occurs on the IE 2000 after upgrading the image on sdflash: and then selecting **Yes** to the Device Manager prompt “Switch software has been updated. Synchronize the new software between SD Card and Onboard Flash?”

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1.

- **CSCuw36207**

Symptom On the IE 3000, changing the Host Name in Device Manager Express Setup causes a Profinet notification to appear.

Conditions Steps to reproduce:

1. Launch the device in a browser.
2. Select Admin > Device management > Express setup.
3. Change the Host Name and click on **Submit**.
4. Observe that a Profinet notification appears.

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1. In earlier releases, click **OK** and the host name change is accepted.

- **CSCuw37216**

Symptom On the IE 2000 in Device Manager, after the **Locate Switch** configuration changes, the Prompt to Sync notification in Dashboard is unreadable.

Conditions This issue occurs when **Locate Switch** is enabled and disabled, and **Prompt to Sync** is enabled.

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1.

CSCuw37528

Symptom On all IE switches, restarting the switch in Device Manager without saving the running configuration saves the running configuration anyway.

Conditions Steps to reproduce:

1. Make some configuration changes using the CLI and do not save them; for example, create some VLANs.
2. Navigate to Admin > Device Management > Restart/Reset page.
3. Select the option to Restart the switch without saving running configuration.
4. After restarting the switch observe that the device is reloaded with the saved running configuration. (The configuration changes made in Step 1 are present in the running configuration).

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1.

- **CSCuw38479**

Symptom On the IE 4000, Device Manager does not allow you to enter the Source/Destination Ports and Source/Destination Operator when creating Extended IP ACL lists, after first creating the ACL using the CLI.

Conditions Steps to reproduce:

1. Create an Extended IP numbered ACL from the Cisco IOS CLI (for example, 2699):

   ```
   Switch(config)#ip access-list extended 2699
   ```

2. Launch the device in a browser.
3. Select Configure > Security > ACL.
4. On the ACL List page, add an ACE with Source Type Network.
5. Observe that all other fields can be configured except Source Operator, Source Port, Destination Operator, and Destination Port.

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1.

- **CSCuw40310**

Symptom PROFINET requires the following manually configured lldp settings to function and may encounter frequent disconnects without these settings (IE 2000).

lldp timer: 5
lldp holdtime: 20

Conditions When a PROFINET session connects, IO devices will transmit lldp packets every 5 sec and the holdtime will be 20 sec.

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1.

- **CSCuw40656**

Symptom In Device Manager online help, descriptions are missing for the **Reset** and **Reset All** buttons in NAT Statistics.

Conditions This issue exists on the IE 2000, IE 4000, and IE 5000 switch platforms in Device Manager online help under Monitor > Statistics > NAT Statistics.

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1.

- **CSCuw53738**

Symptom IE 4000 crashed while configuring the switch (when adding a VLAN and bringing up the interface) after the when configured with dying gasp for syslog and snmp.

Conditions Configured dying gasp for syslog and snmp; and then made some configuration changes (for example adding VLAN or bringing up an interface or media type change from SFP to RJ45 or vice versa).

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1.

- **CSCuw54163**

Symptom The **alarm facility power-supply rps** command, which enables an alarm for the RPS, is accepted and applied in the CLI but is not added to the running configuration file.

Conditions This issue occurs on the CGS 2520 running the 15.2(3)EA image and using the alarm-facility feature.

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1.

- **CSCux11078**

Symptom Profinet2.3: Profinet Topology Editor shows Wrong Partner Port when you import GSD file for IE 3000.

Conditions Incompatible GSD file for IE 3000.

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1 using GSDML-V2.31-IE3000-20160125.xml.

- **CSCux42341**

Symptom IE 3010 PoE ports do not recover after a brief power out affecting all installed power supplies on the unit. Issue is seen when the power outage is momentary and lasts only for a few tenths of a millisecond. Power glitch that brought down the switch could also cause the PoE ports to remain down after the system reload. communication with the micro controller and PoE controller, connected PDs in ports fa0/17-24 will go down.

Conditions Due to the initial power outage, the hardware logic on the IE 3010 initiates a PoE shutdown. If the power is restored before the unit is completely shutdown it results in a situation where the PoE ports continue to remain down. Since the PoE shutdown logic is in the hardware, the IOS software and the inline power state machines inside the software continue to believe that the PoE ports are still powered on.

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1.

- **CSCuy00244**

Symptom Certain IE 2000 units may fail to boot after upgrading to an IOS version which causes a boot loader upgrade on the system.

Conditions Issue may be seen on certain units which have lost their environment block.

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1.

- **CSCuy01664**

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

Platform: IE-2000U-16TC-GP

SW Version: 15.0(2)EH

SW Image: flash:/ie2000u-lanbasek9-mz.150-2.EH/ie2000u-lanbasek9-mz.150-2.EH.bin

Issue is also present in release: 15.2(4)EA.

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

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1.

- **CSCuy04636**

Symptom IE 4000 was not able to boot during the reload or power cycle and threw the Machine Check Exception.

Conditions Issue seen intermittently during the reload or power cycle.

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1.

- **CSCuy13431**

Symptom ICMP error packets may corrupt the following IPv4 or ARP frame. This occurs on IE 4000 and IE 5000 running Cisco IOS 15.2(2)EA, 15.2(2)EB or 15.2(4)EA.

Conditions IE 4000 and IE 5000 switches were running Cisco IOS 15.2(2)EA, 15.2(2)EB or 15.2(4)EA.

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1, 15.2(2)EA3 and 15.2(2)EB2.

- **CSCuy23861**

Symptom The Last reload reason in the **show version** output for IE 2000 is always shown as power-on when the unit is coming up after a crash, which is not correct behavior. Instead, the appropriate crash reason should display in **show version** output.

Conditions Incorrect last reload reason was displayed for the IE 2000.

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1.

- **CSCuy32217**

Symptom A vulnerability in the Internet Key Exchange (IKE) version 2 (v2) fragmentation code of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to cause a reload of the affected system.

Conditions Only traffic directed to the affected system can be used to exploit this vulnerability. This vulnerability can be triggered by IPv4 and IPv6 traffic.

This occurred on the IE 4000 and IE 5000.

For more details on this issue, please refer to:

Cisco IOS and IOS XE Software Internet Key Exchange Version 2 Fragmentation Denial of Service Vulnerability

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1.

- **CSCuz02957**

Symptom Using the Device Manager, on changing a smart port setting on a port in the management vlan, there is a warning message notifying users that they may lose connectivity and further displays smart port macro screen for user to apply macros but on pushing OK, it does not apply smart port macros on the device.

Conditions This issue applies to IE2000/S5700, IE3000/S8000/S8300, IE4000/S5400 and IE5000/S5410 platforms. Also the issue happens when changing the smartport macro setting on a port in the management vlan.

Workaround This issue is resolved in Cisco IOS Release 15.2(4)EA1.

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:

https://tools.cisco.com/bugsearch/search

To access the Bug Search Tool to search on a specific caveat, enter the following URL:

https://tools.cisco.com/bugsearch/search/<BUGID>

Documentation Updates

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

- Hardware Watchdog Reset, page 25
- network-policy command, page 26
- Express Setup Enhancements, page 26

Hardware Watchdog Reset

The expected behavior on the switch when there is an IOS software problem is for the switch to crash, save the information that helps software engineers debug the crash, and then reload. However, there can be rare occurrences of the switch hanging without crashing. Hangs are very hard to reproduce and even harder to fix because there is no trace of what caused the hang. Following are some of the symptoms when the switch hangs:

- Switch becomes totally unresponsive to the CLI
- Traffic forwarding stops
- LEDs stop blinking
- Switch does not save any crash information
- Switch does not reload

The switch not reloading is a very serious issue, especially for IoT deployments in remote and sometimes hard to reach locations where sending personnel to reload the box is expensive, time consuming, and leads to the system being rendered unusable for that time.

The Hardware Watchdog Reset feature causes the switch to reload if IOS software is unresponsive for a certain period of time (5 minutes). The CPU Hardware Watchdog ensures that the switch reloads if software is hung for whatever reason.

Configuring Hardware Watchdog Reset

This feature is enabled by default. The following CLI command disables and re-enables this feature:

```
(config)# boot hardware-watchdog disable
(config)# no boot hardware-watchdog disable
```

This command requires a reboot to take effect.

The scheduler process-watchdog (software) remains in effect even after this feature is disabled.

network-policy command

The *Cisco IE 3010 Switch Software Configuration Guide* incorrectly states that the **network-policy** command is supported on the IE 3010. The IE 3010 does not support this command.

This issue is in *Cisco IE 3010 Switch Software Configuration Guide* Release 12.2(53)EZ, 15.0(2)SE1, or later. (CSCuw22362)

Express Setup Enhancements

Note: IE 2000U **does not** support Express Setup.

Express Setup has three options to meet the needs of different installer roles. You select an option based on how long you press the Express Setup button.

- Short press mode—You want to use the existing Express Setup method.

  The existing Express Setup behavior has improved failure LED indication.

- Medium press mode—You are installing a switch into an already running environment with certain services available (DHCP) or you want to have the device receive an IP address without using Device Manager.
- Long press mode—You are confident and knowledgeable in the use of Cisco IOS CLI and can configure the switch directly using a console cable.

Table 4 summarizes Express Setup for each mode.

Table 4 Express Setup Modes

	Short Press Mode	Medium Press Mode	Long Press Mode
Press duration	1-4 seconds.	5-10 seconds.	15-20 seconds.
LED blinking pattern (start and end of Express Setup)	Blinks green from 1-4 seconds.	Blinks red from 4-10 seconds.	Blinks alternating green and red from 15-20 seconds.
Abort Express Setup	Express Setup button released between 10-15 seconds (Express Setup Indicator LED is off).	Express Setup button released between 10-15 seconds (Express Setup Indicator LED is off).	Express Setup button released after 20 seconds (Express Setup Indicator LED is off).

Table 4 Express Setup Modes (continued)

	Short Press Mode	Medium Press Mode	Long Press Mode
Description	■ Express Setup management interface is selected. ■ DHCP Server is set up on VLAN 1000 with an address of 192.168.1.254. ■ The port LED changes from blinking green to solid green once the PC - Switch link comes up. ■ Once DHCP session is successfully established, the PC is assigned an IP address of 192.168.1.1 on VLAN 1 and the Express Setup indicator LED changes from blinking green to solid green. ■ The user starts a browser session and Device Manager (DM) Express Setup page opens with default username and password set to “no username” / cisco. ■ The user configures the Switch from DM Express Setup page.	■ DHCP request is sent out of all ports on VLAN 1. ■ Express Setup indicator LED blinks alternating green and red while waiting for DHCP response. ■ Upon DHCP response, Express Setup indicator LED blinks green for 5 seconds and is then turned off. ■ VLAN 1 is configured for the IP address returned, and default password is set to “no username”/cisco ■ CIP is enabled on VLAN 1 with CIP security password set to “switch”. ■ If non-default switch configuration is detected or If no DHCP response is received for 5 minutes from when the DHCP request was transmitted, Express Setup is aborted and the EXP/Setup indicator LED turns solid red (for 10 seconds).	■ All configuration and settings (config.text, vlan.dat, and private-config.text files) on on-board and SD Flash are reset to factory defaults. ■ Switch reloads and comes up with factory default settings.

Locate Switch

You can configure Locate Switch using CLI and the Device Manager.

When enabled, **Locate Switch** causes all possible LEDs to glow ALT_RED and GREEN (LEDs that are in one color blink) once the switch is enabled with a specific time. This performance varies from previous releases (CSCux75707).

The Locate Switch time setting has been changed from <9-255> to <0-255> time in seconds:

```
switch# locate-switch ?
<0-255> time in seconds
0      : Stop Blink
9-255:  Blink LED
```

Enter the following **show** command to verify your settings:

```
Switch# sh locate-switch
Locate Switch enabled!!
total time: 255 secspecific
time left: 249 sec
```

The **locate-switch** command is a volatile command and will not be saved or displayed in running or startup configuration.

Related Documentation

Table 5 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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

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 SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND 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 are considered un-Controlled copies and the original on-line version should be referred to for 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.

No combinations are authorized or intended under this document.