Release Notes for Cisco IOS Release 15.2(5)E1

Last Updated: February 27, 2018
First Published: November 23, 2016

Cisco IOS Release 15.2(5)E1 runs on these platforms:

- Cisco 2500 Series Connected Grid Switches (CGS 2520)
- Cisco Connected Grid Ethernet Switch Module (CGR 2010 ESM)
- Cisco Embedded Service 2020 Series Switches (ESS 2020)
- 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 4010 Series Switches (IE 4010)
- Cisco Industrial Ethernet 5000 Series Switches (IE 5000)

These release notes include important information about Cisco IOS Release 15.2(5)E1 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 6.

For a complete list of documentation for the platforms associated with this release, see Related Documentation, page 26.

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(5)E1

Table 1 lists new features added in Cisco IOS Release 15.2(5)E1.

Table 1 New Feature Summary for Cisco IOS Release 15.2(5)E1

Feature	Platform	Description	Related Documentation
Cisco IOx support	IE 4000	IE 4000 supports Cisco IOx, which allows support for a second core image that is independent from Cisco IOS.	Device Manager Online Help Release Notes for Cisco IOx, Release 1.2.0
VLAN 0 Tagging	CGS 2520 ESM for CGR 2010 IE 2000, IE2000U IE 4000, IE 5000	The VLAN 0 Priority Tagging feature enables 802.1Q Ethernet frames transmitted with the VLAN ID to be set to zero. These priority tagged frames allow the VLAN ID tag to be ignored and the Ethernet frame to be processed according to the priority configured in the 802.1P bits of the 802.1Q Ethernet frame header.	VLAN 0 Priority Tagging Support Device Manager Online Help
TrustSec Security Group Tagging (SGT) and Security Group ACL (SGACL) 10G uplink ports	IE 5000	TrustSec SGT and SGACL is now supported on IE 500010G uplink ports.	Cisco TrustSec Switch Configuration Guide
NetFlow Lite	IE 4000, IE 5000	NetFlow Lite uses flows to provide statistics for accounting, network monitoring, and network planning. A flow is unidirectional stream of packets that arrives on a source interface and has the same values for the keys. A key is an identified value for a field within the packet. You create a flow using a flow record to define the unique keys for your flow.	NetFlow Lite Configuration Guide (Catalyst 2960-X Switch) **Note:** Please see Documentation Updates, page 24 for details on NetFlow Lite new command options and exceptions.

Table 1 New Feature Summary for Cisco IOS Release 15.2(5)E1

Feature	Platform	Description	Related Documentation
Media Redundancy Protocol (MRP) enhancements	IE 2000, IE 4000, IE 5000	■ MRP is only supported on IE 5000 downlinks ports. (There is no uplink support) ■ 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. — In a network operating with MRP and STP, spanning tree BPDUs are not sent on MRP-enabled ports. If ports are unconfigured from an MRP ring, then the ports are added to the spanning tree. ■ Multiple MRP ring support allows connection of multiple MRP rings, which can be aggregated at the distribution layer (mrp-multi-manager MRP license required) ■ 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, IE 4000 and IE 5000 Switches ■ Device Manager Online Help
Layer 3 feature set IP LITE	ESS 2020	SWIFT license PID L-ESS-2020-IPLITE= is required.	■ Cisco Embedded Service 2020 Series Switches
Device Manager Platform Support Expanded	IE 2000U	You can now manage the IE 2000U switch using the Device Manager.	■ Device Manager Online Help
Device Manager Localization		Online help for the Device Manager is available in the following languages: ■ Chinese (Traditional) (code: 2052) ■ Chinese (Simplified) (code: 1028) ■ Default: English (code: 1033) ■ French (code: 1036) ■ German (code: 1031) ■ Japanese (code: 1041) ■ Spanish (LATAM) (code: 9226)	■ 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 10.

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 9

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 IP services image. The latest release for the IP services 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.E1.tar	CGS 2520 IP services image file
cgs2520-lanbaselmk9-tar.152-5.E1.tar	CGS 2520 LAN base image file
c2020-universalk9-tar.152-5.E1.tar	ESS 2020 universal image file
ie2000-universalk9-tar.152-5.E1.tar	IE 2000 universal image file
ie2000u-ipserviceslmk9-tar.152-5.E1.tar	IE 2000U IP services image file
ie2000u-lanbaselmk9-tar.152-5.E1.tar	IE 2000U LAN base image file
ie3010-ipservicesk9-tar.152-5.E1.tar	IE 3010 IP services image file
ie3010-lanbasek9-tar.152-5.E1.tar	IE 3010 LAN base image file
ies-lanbasek9-tar.152-5.E1.tar	IE 3000 LAN base image file
grwicdes-ipserviceslmk9-tar.152-5.E1.tar	ESM IP services image file
grwicdes-lanbaselmk9-tar.152-5.E1.tar	ESM LAN base image file
ie4000-universalk9_iox-tar.152-5.E1.tar	IE 4000 Universal image file bundles Cisco IOx and IOS
ie4000-universalk9-tar.152-5.E1.tar	IE 4000 Universal image file (Cisco IOS only)
ie4010-universalk9-tar.152-5.E1.tar	IE 4010 Universal image file
ie5000-universalk9-tar.152-5.E1.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 10.

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
	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*
	IE4010	*Cisco Industrial Ethernet 4000, 4010 and 5000 Switch Software Configuration Guide*
	IE 5000	*Cisco IE 5000 Hardened Aggregator Hardware Installation Guide*
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*
	IE4010	*Cisco Industrial Ethernet 4000, 4010 and 5000 Switch Software Configuration Guide*
	IE 5000	*Cisco IE 5000 Hardened Aggregator Hardware Installation Guide*

Table 3 Methods for Assigning IP Information (continued)

Method	Platform	Document
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*
	IE4010	*Cisco Industrial Ethernet 4000, 4010 and 5000 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**

- **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.

- **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.

- **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. This issue was seen on IE 4000.

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

- **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, and 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 drops 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.

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 13
- Resolved Caveats, page 17
- Accessing Bug Search Tool, page 24

Open Caveats

- **CSCvb17036**

Symptom By using GSD files, unable to configure media type as ‘fiber’. Only “Copper” as a media type can be configurable.

Conditions Problem seen on IE2K and 4K. Working fine on IE5000.

Workaround Use CLI to configure media type.

- **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.

- **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.

- **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.

- **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.

- **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.

- **CSCuy86869**

Symptom When PTP mode is ‘End to End transparent clock' enabled and the number of slaves is 5 for each port (total 2 ports, number of slaves =10), we see “Failed to find DELAY_REQ DB record hash” errors frequently. Issue is not seen in boundary mode.

Conditions The issue occurs on the IE2000U platform.

Workaround There is no workaround for this issue.

- **CSCuz34012**

Symptom IE2000 is modifying IP header checksum of packets to 0xFFFF intermittently, it is causing receiving devices to drop such packets due to bad checksum and that is further leading to TCP re-transmissions for TCP flows

Conditions IE 2000 was running 15.2(4)EA.

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

Conditions 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.

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

- **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 on IE5000 15.2(5)E.

Workaround None. Display issue. No feature functionality impact.

- **CSCva84668**

Symptom VLAN 0 packets (64 bytes) on IE4000 and IE5000 are not treated as error packets (undersize) on ingress and traffic passes through. On IE2000 the packets are reported as undersized.

Conditions Issue seen when VLAN 1 is UP. Error goes away if VLAN 1 is assigned an IP address.

Workaround There is no workaround for this issue.

- **CSCvb01492**

Symptom Configuration of incomplete record for Horizontal Stack not rejected by members.

Conditions Issue is seen on IE5000. Behavior on standalone device is normal.

Workaround There is no workaround for this issue.

- **CSCvb73198**

Symptom IE4000: HTTPS fails upon removal and insertion of SD card and reboots device with SD card .

Conditions Issue not seen every time. It occurs randomly. If issue occurs below message appears in the browser:

<<<

Secure Connection Failed

The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.

<<<

Workaround Remove and regenerate crypto certificates.

```
(config)#crypto key zeroize

% No Signature Keys found in configuration.

#(config)crypto key zeroize

>>>yes

#(config)ip domain-name thegeek ("make dummy, imperative else cannot exec next command")

#(config)crypto key generate rsa modulus 4096 ("it takes a few minutes")
```

- **CSCvc04363**

Symptom If user opens online help (OLH) for features (such as PRP, IOx or Global Macro) that are not yet translated, the page displays in English instead of the selected language. Table of Contents on the left side pane will not point to that feature but rather a random selection.

Conditions Selected text does not appear as desired translated text. Feature text has not yet been translated.

Workaround Refer to the English text.

- **CSCvc19241**

Symptom IE and Safari browsers are not recommended for IOx Local Manager Application in IE4000.

Conditions DM > IOx tab displays message "Content was blocked because it was not signed by valid security certificate" even though Local Manager certificate is accepted in the same browser in a different tab as a prerequisite.

Workaround Recommended browsers are Firefox and Chrome.

- **CSCvc28935**

Symptom Platform crashes with the following:

```
Machine Check Exception (0x0200)!
ESR: 0x00000000
SRR0: 0x03AFBF90 SRR1: 0x00029200 SRR2: 0x03AFBF9C SRR3: 0x00029200
MCSR: 0xC0000000
L2MCSR: 0x80004000
```

Afterwards, the device will get stuck in a boot loop, of which it only comes out after a power cycle.

Conditions Configuring "ntp server x.x.x.x" with no interface/SVI on the unit in ip-state with IP address.

Workaround Remove NTP configuration.

- **CSCvc53353**

Symptom IRIG-B TTL02, TTL03, AM02 and AM03 OUT functionality is not working

Conditions IRIG-B TTL02, TTL03, AM02 and AM03 OUT functionality is not working with 152-5.E1 image.

Workaround Downgrade to 15.2(5)E to use IRIG-B functionality for TTL02, TTL03, AM02 and AM03 OUT mode.

http://www.cisco.com/c/en/us/td/docs/switches/connectedgrid/cg-switch-sw-master/software/release/notes/rn-15-2-5e.html

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)E1.

- **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)E1.

- **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)E1.

- **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)E1.

- **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)E1.

- **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)E1.

- **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 This issue is resolved in Cisco IOS Release 15.2(5)E1.

- **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)E1.

- **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)E1.

- **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)E1.

- **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)E1.

- **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)E1.

- **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 This issue is resolved in Cisco IOS Release 15.2(5)E1.

- **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)E1.

- **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)E1.

- **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)E1.

- **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)E1.

- **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)E1.

- **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)E1.

- **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)E1.

- **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)E1.

- **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)E1.

- **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)E1.

- **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)E1.

- **CSCuz65513**

Symptom The default ACL is not editable from DM but is editable from CLI.

Conditions This issue is seen when attempting to edit default ACL CISCO-CWA-URL-REDIRECT-ACL in Device Manager.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

CSCva06712

Symptom In Device Manager, there is no notification for the same VLAN name.

Conditions This issue is seen when adding a duplicate VLAN on the ESS 2020 with Device Manager.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

- **CSCva25556**

Symptom **sh prp channel detail** shows the prp protocol is Disabled even when 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)E1.

- **CSCva68230**

Symptom POE stopped working, PDs dropped and did not re-connect after the 48VDC input recovered, the 24VDC remained the primary PSU, and POE remained down.

Conditions This issue occurs on the IE-4000-4GC4GP4G-E with 2 PSUs = 24VDC + 48VDC and providing POE to two AIR-CAP2702I-E-K9.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

- **CSCva68824**

Symptom An attempt to create Port Channel interface with ID number 2 incorrectly results in creating PRP Channel interface.

Conditions This issue occurs with IE2000U and only with channel ID number 2.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

- **CSCva80784**

Symptom Any RJ-45 interface (G1/1 THROUGH G1/12), if configured with speed auto 1000 / duplex full, permits a switch or other device configured for auto-negotiation on a Fast Ethernet only-capable adapter to connect and operate at 100/full.

Conditions

SKU: IE-4010-16S12P, IOS: 15.2(4.5.12)EC IE4010-UNIVERSALK9-M

SKU: IE-5000-16S12P, IOS: 15.2(5)E IE5000-UNIVERSALK9-M

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

- **CSCva85646**

Symptom Alarm setting for SD card not present on the IE 4010.

Conditions This issue is seen on the IE-4010-4S24P running Cisco IOS 15.2(4.5.14)EC.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

- **CSCva96583**

Symptom PRP duplication removes weakness against introduced delay/jitter.

Conditions PRP duplication failure to remove percentage is reaching 100 percent when introduced delay is 3 ms for two flows; also PRP duplication failure to remove percentage is 32.9 percent when introduced jitter is 3 ms even for single flow.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

- **CSCvb04298**

Symptom There are periodic leap second events which can add or delete a second to global time. With the NTP-PTP time conversion feature (NTP-PTP Flywheel) configured, when the NTP leap second is inserted, PTP generates an invalid time for a few seconds.

Conditions NTP client is configured. PTP mode is GMC-BC.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

- **CSCvb04864**

Symptom Profinet check box is not enabled by default.

Conditions

1. Perform a short press or medium press.
2. Open the DM Express Setup page from PC.

3. The second Express Setup page should show the Profinet check box enabled by default, but it is not enabled.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

- **CSCvb11859**

Symptom In Device Manager on the IE 4010, Port Settings-Auto mdix options should not be grayed out.

Conditions Steps to reproduce the issue:

1. Launch the device manager using Firefox.
2. Go to Configure-->Network--Port Settings.
3. Click on Edit interface option by selecting any of the one interface.
4. Auto MDIX option is grayed out and cannot be enabled or disabled.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

- **CSCvb21597**

Symptom On the E 2000 and S5700, DM upgrade does not succeed and leaves old .save files.

Conditions Steps to reproduce:

1. Use Device manager, Admin-> Software Upgrade page.
2. Choose tar image by browsing the file.
3. Click Update.
4. The file gets copied and .save file is also created, but when device comes up it comes up with old files.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

- **CSCvb32407**

Symptom Device Manager login page displays “undefined” instead of “Confirm password”.

Conditions Steps to reproduce:

1. Perform a short press on the device.
2. Connect to the PC to open the DM Express Setup page.
3. Enter the first login password.
4. The second login configuration should show the login name and password and “Confirm password”.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

- **CSCvb40748**

Symptom A timed-out CIP connection class 1 connection that is missing its associated session crashes CIP connection manager when it tries to close its UDP socket.

Conditions A session may be missing for a variety of reasons, such as switch IP address removed/updated, UCMM unregister, ENIP encap timeout or error, or UDP socket block or send error.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

- **CSCvb45849**

Symptom Device Manager Port Settings page on the IE 4010 did not show port type in edit window.

Conditions Steps to reproduce:

1. Go to Configure -->Port Settings.
2. Select the port and click edit window.
3. Check for the port type in the edit window. The port type is mentioned in online help and seen in the console but this is not available in the port setting page on DM page.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

- **CSCvb54977** I

Symptom Third party PRP RedBox devices when connected to an IE-2000U running IOS 15.0(2)EK1 in Redbox configuration may suffer loss of traffic.

Conditions The behavior is seen with a third party PRP driver software/hardware as remote side Redbox connecting the two LANs.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

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 latest updates to documentation for IE switches:

- Enabling Logging Alarms for Syslog Messages, page 24
- NetFlow Lite, page 25
- Related Documentation, page 26

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.

NetFlow Lite

Please note the following variances in NetFlow Lite support on the IE 4000 or IE 5000 switches and NetFlow Lite user documentation:

IE 4000 and IE 5000

- New configuration options for the feature supported on the platforms:

```
NACstack(config)#flow exporter exporter1
NACstack(config-flow-exporter)#?
default  Set a command to its defaults
description  Provide a description for this Flow Exporter
destination  Export destination configuration
dscp  Optional DSCP
exit  Exit from Flow Exporter configuration mode
export-protocol  Export protocol version
no  Negate a command or set its defaults
option  Select an option for exporting
output-features  Send export packets via IOS output feature path
source  Originating interface
template  Flow Exporter template configuration
transport  Transport protocol
ttl  Optional TTL or hop limit
```

- Missing **cache** command options in user Netflow Lite documentation:

```
switch(config-flow-monitor)#cache ?
entries Maximum flow entries in the Flow Cache
timeout Configure flow cache timeout parameters
type Set the type of the Flow Cache
```

- New options, **sort** and **aggregate**, for **show flow monitor cache format** command (as shown below):

show flow monitor cache format has only three options as shown below:

```
Switch2#sh flow monitor cache format ?
csv Flow monitor cache contents in csv format
record Flow monitor cache contents in record format
table Flow monitor cache contents in table format
```

aggregate counters for flow monitor have below options:

```
Switch2# sh flow monitor monitor1 cache aggregate ?
counter Counter fields
ipv4 IPv4 fields
record Aggregate using a predefined flow record
timestamp Timestamp fields
transport Transport layer fields
```

IE 5000 Only

- Only supports homogenous stacking. Maximum stack member support of 4.
- No support for Flow Record field, Match Wireless.
- Default Settings: Flow Active Timeout supports a lower value range of 60 seconds (rather than 180 or 300 only).

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 4010 Series Switches	http://www.cisco.com/go/ie4010
Cisco Industrial Ethernet 5000 Series Switches	http://www.cisco.com/go/ie5000

Obtain Documentation and Submit 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 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.