Release Notes for Cisco IOS Release 15.2(4)EA

Last Updated: March 1, 2017
First Published: October 21, 2015

Cisco IOS Release 15.2(4)EA 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)

These release notes include important information about Cisco IOS Release 15.2(4)EA 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 8.
- If you are upgrading to a new release, see the software upgrade filename for the software version. See Deciding Which Files to Use, page 8.

For a complete list of documentation for the platforms associated with this release, see Related Documentation, page 24.

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

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

Organization

This document includes the following sections:

Conventions, page 2	Conventions used in this document.
New Features in Cisco IOS Release 15.2(4)EA, page 4	New features in Release 15.2(4)EA.
System Requirements, page 7	System requirements for Release 15.2(4)EA.
Upgrading the Switch Software, page 7	Procedures for downloading software.
Limitations and Restrictions, page 11	Known limitations in this release.
Caveats, page 13	Open caveats in Release 15.2(4)EA.
Documentation Updates, page 22	Updates to the IE switch product documentation.
Related Documentation, page 24	Links to the documentation for the hardware platforms associated with this release.
Obtaining Documentation and Submitting a Service Request, page 24	Link to information about Cisco documentation.

Conventions

This document uses the following conventions.

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

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

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

Warning: **IMPORTANT SAFETY INSTRUCTIONS**

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

SAVE THESE INSTRUCTIONS

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

New Features in Cisco IOS Release 15.2(4)EA

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

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

Feature	Platform	Description	Related Documentation
Media Redundancy Protocol (MRP) and PROFINET Enhancements	IE 2000	MRP (Media Redundancy Protocol), an open standard industrial protocol for the IE2000, 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 Switches ■ Device Manager Online Help
TACACS Server Host command change	IE 2000, IE 2000U, IE 3000, IE 4000, IE 5000	The new command syntax is: **tacacs server** <server name> **ipv4 address** <ip_address> **key** <string>.	■ TACACS+ Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)

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

Feature	Platform	Description	Related Documentation
Express Setup Enhancements for IE Switches	IE 2000, IE 3000, IE 4000	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). A new command, **locate-switch**, causes the EXP/Setup indicator LED to blink green, providing a visual indication of the switch's location. This feature also includes the ability to set up the switch through Add-On Profile (AOP) by enhancing CIP.	■ Cisco IE 2000 Switch Hardware Installation Guide ■ Cisco IE 3000 Switch Getting Started Guide ■ Cisco IE 4000 Switch Hardware Installation Guide ■ Device Manager Online Help ■ Express Setup Enhancements, page 22
MACsec (IEEE 802.1AE)	IE 4000	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.	■ Configuring MACsec Encryption

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

Feature	Platform	Description	Related Documentation
NTP to PTP Translation (Time Services)	IE 4000	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 Switches
Configurable Boundary Clock Synchronization Algorithm (Time Services)	CGS 2520, CGR 2010 ESM, IE 2000U, IE 2000, IE 3000, IE 4000	This feature adds options for Boundary Clock (BC) synchronization to accommodate various PTP use cases. For improved convergence time in PTP networks, you can configure Boundary Clocks to use a feedforward algorithm to measure the delay added by the network elements forwarding plane (the disturbance) and use that measured delay to control the time output. You can configure the switch for linear packet delay variation (PDV) filtering or adaptive filtering, which filters as much PDV as possible. Note that adaptive filtering is not supported in Power Profile mode.	■ Precision Time Protocol Software Configuration Guide for IE 2000U and Connected Grid Switches ■ Precision Time Protocol Software Configuration Guide for IE 4000 Switches
MODBUS TCP server support	IE 2000, IE 3000	MODBUS is an application layer messaging protocol that provides client/server communication between devices connected on different types of buses or networks. MODBUS on TCP provides a Client/Server communication between devices connected on an Ethernet TCP/IP network. A MODBUS request or response message is encapsulated into a MODBUS/TCP Application Data Unit (ADU) to be carried over a TCP/IP network. All MODBUS messages are sent via TCP to registered port 502. The IE switch works as a MODBUS/TCP server, which activates a local action to read/write internal registers, or to achieve some other actions, on reception of a MODBUS request from a MODBUS/TCP client.	Refer to the Configuring MODBUS TCP chapter of the Cisco Industrial Ethernet 4000 Series Switch Software Configuration Guide for IE 2000 and IE 3000 MODBUS TCP information.

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

Feature	Platform	Description	Related Documentation
Device Manager Enhancements	CGS 2520, IE 2000, IE 3000, IE 3010, IE 4000	■ ACL support (all platforms) ■ OSPF and EIGRP protocol support (IE 3000, IE 3010, and IE 4000) ■ PRP interface support (IE 4000) ■ MRP support (IE 2000) ■ Profinet Enhancements (IE 2000, IE 3000, and IE 4000) ■ Locate Switch support (IE 2000, IE 3000, IE 4000)	■ Device Manager Online Help

System Requirements

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

■ Express Setup Requirements, page 7

Express Setup Requirements

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

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 8

■ Deciding Which Files to Use, page 8

■ Archiving Software Images, page 8

■ Upgrading a Switch by Using the CLI, page 9

- 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.

Table 2 Cisco IOS Software Image Files

File Name	Description
c2020-universalk9-tar.152-4.EA.tar	ESS 2020 universal image file
ie2000-universalk9-tar.152-4.EA.tar	IE 2000 universal image file
ie3010-ipservicesk9-tar.152-4.EA.tar	IE 3010 IP services image file
ie3010-lanbasek9-tar.152-4.EA.tar	IE 3010 LAN base image file
ies-ipservicesk9-tar.152-4.EA.tar	IE 3000 IP services image file
ies-lanbasek9-tar.152-4.EA.tar	IE 3000 LAN base image file
ie2000u-ipserviceslmk9-tar.152-4.EA.tar	IE 2000U IP services image file
ie2000u-lanbaselmk9-tar.152-4.EA.tar	IE 2000U LAN base image file
cgs2520-ipserviceslmk9-tar.152-4.EA.tar	CGS 2520 IP services image file
cgs2520-lanbaselmk9-tar.152-4.EA.tar	CGS 2520 LAN base image file
grwicdes-ipserviceslmk9-tar.152-4.EA.tar	ESM IP services image file
grwicdes-lanbaselmk9-tar.152-4.EA.tar	ESM LAN base image file
ie4000-universalk9-tar.152-4.EA.tar	IE 4000 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 8 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 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 **/overwrite** option overwrites the software image in flash memory with the downloaded one.

   – 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.
- For **/***directory***/***image-name***.tar**, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

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.

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*, Device Manager Online Help
	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*
CLI-based setup program	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*

Table 3 Methods for Assigning IP Information (continued)

Method	Platform	Document
DHCP-based autoconfiguration	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*
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*

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.

- **CSCup58174**

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

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 Applies to all switches that have routing.

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.

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.

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. Applies to all switches that support VLAN configuration and CIP features.

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 13
- Resolved Caveats, page 20
- Accessing Bug Search Tool, page 21

Open Caveats

- **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.

Workaround There is no workaround for this issue.

- **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 There is a CLI error message when the maximum number of static routes is exceeded. To see this error message, set the following debugging CLI: **debug ip routing static db**. When too many routes are configured, you will see the following messages on the console:

```
>Mar 30 23:49:09.912: IP-ST-DB(default): Maximum allowed static route count reached :16
>Mar 30 23:49:09.912: IP-ST-DB(default):  ip_addstatic_route(), failed
>Mar 30 23:49:09.912:  10.0.0.15/32 via 3.3.3.1 ,tag 0,fg 0x40020004,dis 1,name ,lfg 0x0,own M
```

- **CSCuq21005**

Symptom In-line editing becomes unresponsive on the Device Manager Port Thresholds page on IE 2000, IE3000 and IE4000 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.

- **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.

- **CSCur19703**

Symptom Inconsistent **show license** output.

Conditions This issue occurs in the output of **show license** and **license boot level** on IE2000 PIDs that do not support Lanlite, IPLite, or Enhanced Lanbase licenses.

Workaround If you set a license level (based on the list displayed in **show license**), after reload, if the license does not take effect (based on **show license** output), verify the license support for that SKU instead of relying on **show license** output.

- **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.

- **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 Use the Firefox browser.

- **CSCur72678**

Symptom MRP convergence time is longer with multicast traffic than it is with unicast traffic.

Conditions This issue occurs on the IE 2000 with multicast traffic in an MRP ring. Currently, 10 multicast groups are supported for an MRP ring.

Workaround There is no workaround for this issue.

- **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 (CGS2520, IE2000U, IE4000, or IE5000).

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 Set the port-type to NNI.

- **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 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 Use **show mrp ring 1** (no-profinet mrp mode) or **show profinet mrp ring 1** (profinet mrp mode) to display MRP port information.

- **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.

- **CSCuv46857**

Symptom When updating from Release 15.2(3)E to 15.2(4)E there is a problem with the GSD file (IE 2000).

Conditions Cisco IOS updates only, when going from 15.2(3)E to 15.2(4)E.

Workaround Downgrade to Release 15.2(2)E GSD before upgrading to 15.2(4)E.

CSCuv75858

Symptom Trace back messages are seen after reloading the IE3010 SKU.

Conditions This issue occurs on SKU IE-3010-16S-8PC only when 100FE SFPs are inserted in all 16 FE SFP and 2 Gigi SFP slots, with loopbacks created using all of them, and the device is reloaded during the boot up process.

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.

- **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 You can verify the configuration using the CLI command **show run | in bpdu**.

- **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.

- **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.

- **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 Remove the older GSD and restart from scratch to build Hardware for TIA12, or use the older GSD from IOS release 15.2(2)E.

- **CSCuw09603**

Symptom On Cisco IE 3010 and CGS 2520 switches using redundant power supplies (2x PSUs), a syslog message may be seen right after the switch is power cycled or reloaded:

"%ENVIRONMENT-3-POWER_ERROR: PSU x model is not supported"

Conditions This issue occurs when redundant power supplies are installed.

Workaround The syslog does not affect any functionality of the system and does not appear any time after its first appearance after a reload. You can use the CLI command **show env all** to verify that power supplies are functioning normally.

- **CSCuw15036**

Symptom On the IE2000, IE3000, and IE4000, 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 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.

- **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 Delete the .save files from flash, after the ios-image sync between sdflash and flash is complete, as follows:

switch# **del /f /r flash:<***image name.save***>**

- **CSCuw34470**

Symptom The OSPF virtual link authentication type is configured as MD5 in the Cisco IOS CLI, but it is displayed as Password in Device Manager on the IE 4000.

Conditions Steps to reproduce:

1. Launch the device in a browser.
2. Use the Cisco IOS CLI to configure the OSPF virtual link authentication type as MD5.
3. Observe that in Device Manager Configure > Routing Protocols > OSPF, the Virtual Link tab, Password is shown as the authentication type instead of MD5.

Workaround

1. Configure the virtual link from DM, with MD5 as authentication type. Specify MD5 key id and MD5 key and submit.
2. Verify configurations using the command **show running-config | inc ospf** <*id*>

- **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 Re-edit the created Extended IP ACLs to add source and destination ports.

- **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 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 In Admin > File Management > Sync under the Auto Sync tab, disable **Prompt to Sync**.

- **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 Use the CLI to reload the switch without saving the running configuration.

- **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 Manually configure the lldp advertise (**lldp timer**) and holdover (**lldp holdtime**) timers for PROFINET through CLI on the switch as follows:

switch# **conf t**
switch# **lldp timer 5**
switch# **lldp holdtime 20**
switch# **end**

- **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 all IE switch platforms in Device Manager online help under Monitor > Statistics > NAT Statistics.

Workaround There is no workaround for this issue.

- **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 Verify that the actual functionality works. Be aware that **show running-config** will not display the RPS alarm information and/or the RPS alarm configuration will not survive reload. Note that this is not related to a customer alarm-profile (default).

- **CSCuw68005**

Symptom Ping fails when **cts dot1x** is configured and the SAP mode is configured with **no-encap**. Dot1x is authenticated, interfaces are up, and CDP is fine, but the peer SVI does not respond to ping.

Conditions This issue occurs on the IE 4000 when the **sap** mode in use is **no-encap**.

Workaround Use **gcm-encrypt**, **gmac** or **null** modes.

- **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

- **CSCut77329**

Symptom When booting a switch from sdflash, **no cdp enable** is added to the port-channel members. When booting a switch from flash, the issue is not seen.

Before boot:

```
interface Port-channel1
interface FastEthernet1/9
    channel-group 1 mode desirable
```

After boot:

```
interface Port-channel1
interface FastEthernet1/9
    no cdp enable
    channel-group 1 mode desirable
```

Conditions This issue is seen with all released IE 2000 images: 15.0 and 15.2.

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

For previous releases, use one of these workarounds:

Workaround 1: Enable cdp after the switch boots up from sdflash:

```
config t
interface FastEthernet1/9
cdp enable
```

Workaround 2: Boot the switch from flash:

- **CSCut85937**

Symptom Poor clock synchronization with grandmaster.

Conditions This issue occurred on the IE 2000U during normal operation, when PTP was configured in Power Profile mode.

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

- **CSCut86361**

Symptom IE 3010 and CGS 2520 Temperature and Power monitor SNMP status report incorrectly.

Conditions This issue occurred on the IE 3010.

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

- **CSCuv71972**

Symptom CGS 2520 crashes and reloads when executing the command: **#sh policy-map control-plane ?**

Conditions This issue occurs during normal operation.

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

For previous releases, avoid executing the command **#sh policy-map control-plane** or **#sh policy-map control-plane ?**

Accessing Bug Search Tool

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

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

- Internet connection
- Web browser

- Cisco.com user ID and password

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

bst.cloudapps.cisco.com/bugsearch

Documentation Updates

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

- network-policy command, page 22
- Express Setup Enhancements, page 22

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 or Device Manager.

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 1 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

If you need to physically connect or disconnect ports or move a device in a group of similar devices, the locate switch feature helps you to identify the specific device in the group.

The **locate-switch** command (also available in Device Manager as a check box on the Dashboard page) has the following actions when activated:

- The EXP/Setup indicator LED blinks green to visually notify you that the **locate-switch** command has been enabled.
  - CLI command to enable: Switch# **locate-switch**
  - CLI command to disable: Switch# **no locate-switch**
- The EXP/Setup indicator LED blinking rate is faster to easily distinguish from the EXP/Setup indicator LED pattern while in Express Setup short press mode.
- The EXP/Setup indicator LED will continue the above pattern for 60 minutes or until the **locate-switch** command is deactivated.

Note: The **locate-switch** command is also available through the supporting Add-On Profile (AOP) (through the Switch CIP interface).

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

No combinations are authorized or intended under this document.

© 2015–2019 Cisco Systems, Inc. All rights reserved.