Release Notes for Cisco IOS Release 15.2(3)E1

First Published: April 20, 2015
Last Updated: December 8, 2016

Cisco IOS Release 15.2(3)E1 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)

These release notes include important information about Cisco IOS Release 15.2(3)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 4.
- If you are upgrading to a new release, see the software upgrade filename for the software version. See Deciding Which Files to Use, page 4.

For a complete list of documentation for the platforms associated with this release, see Related Documentation, page 15.

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(3)E1, page 3	New features in Release 15.2(3)E1.
System Requirements, page 3	System requirements for Release 15.2(3)E1.
Upgrading the Switch Software, page 3	Procedures for downloading software.
Limitations and Restrictions, page 7	Known limitations in this release.
Caveats, page 9	Open caveats in Release 15.2(3)E1.
Related Documentation, page 15	Links to the documentation for the hardware platforms associated with this release.
Obtaining Documentation and Submitting a Service Request, page 16	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(3)E1

Table 1 New Features Summary for Cisco IOS Release 15.2(3)E1

Feature	Platform	Description	Related Documentation
10/100/1000Base-TX SFP Module (GLC-FE-T-I)	IE 2000, IE 2000U, IE 3010 and CGS 2520	Provides copper SFP support within the Cisco switch platform.	*Cisco Industrial Ethernet 2000 Series Switches* *Cisco Industrial Ethernet 2000U Series Switches* *Cisco Industrial Ethernet 3010 Series Switches* *Cisco 2500 Series Connected Grid Switches*
ODVA compliance	IE 2000, IE 3000	Ensures compliance with Common Industrial Protocol (CIP) network specifications.	

System Requirements

This section describes the following system requirements for Cisco IOS Release 15.2(3)E1:

- Express Setup Requirements, page 3

Express Setup Requirements

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 4
- Deciding Which Files to Use, page 4
- Archiving Software Images, page 4
- Upgrading a Switch by Using the CLI, page 5

- Installation Notes, page 6

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.152-3.E1.tar	ESS 2020 universal image file
ie2000-universalk9-tar.152-3.E1.tar	IE 2000 universal image file
ie3010-ipservicesk9-tar.152-3.E1.tar	IE 3010 IP services image file
ie3010-lanbasek9-tar.152-3.E1.tar	IE 3010 LAN base image file
ies-ipservicesk9-tar.152-3.E1.tar	IE 3000 IP services image file
ies-lanbasek9-tar.152-3.E1.tar	IE 3000 LAN base image file
ie2000u-ipservicesk9-tar.152-3.E1.tar	IE 2000U IP services image file
ie2000u-lanbasek9-tar.152-3.E1.tar	IE 2000U LAN base image file
cgs2520-ipservicesk9-tar.152-3.E1.tar	CGS 2520 IP services image file
cgs2520-lanbasek9-tar.152-3.E1.tar	CGS 2520 LAN base image file
grwicdes-ipservicesk9-tar.152-3.E1.tar	ESM IP services image file
grwicdes-lanbasek9-tar.152-3.E1.tar	ESM LAN base 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 4 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	Device Manager Online Help
	IE 2000U	*Cisco IE 2000U Switch Getting Started Guide*
	IE 3000	*Cisco IE 3000 Switch Getting Started Guide*
	IE 3010	Device Manager Online Help
	CGS 2520	*Cisco CGS 2520 Getting Started Guide*
	ESM	*Connected Grid Ethernet Switch Module Interface Card Getting Started 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	*CGS 2520 Switch Software Configuration Guide*
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*

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*

Limitations and Restrictions

Cisco recommends 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 Not applicable.

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**

- **CSCuq43566**

Symptom Unsupported VLAN v4r cip object configuration causes issues.

Conditions If you configure a route with a VLAN interface as the next hop, it affects the display of other routes in the v4r output.

Workaround Remove all VLAN routes in order to view the routes configured after the VLAN v4r configuration. CIP does not support VLAN for static routes.

- **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.

Workaround Reload the switch.

- **CSCuw22362**

Symptom The **network-policy profile** command is not supported on the IE 3010 in this release and earlier 15.x and 12.x Cisco IOS releases.

Conditions Entering the **network-policy profile** command on an IE 3010 indicates that it is an Unrecognized command.

Workaround There is no workaround. The IE 3010 does not support the command in this release.

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 9
- Resolved Caveats, page 11
- Accessing Bug Search Tool, page 15

Open Caveats

- **CSCuo87734**

Symptom When a system is reloaded after its startup configuration has been erased, sometimes the VLAN 1 interface goes to admin down state.

Conditions Boot a system with empty startup configuration.

Workaround Issue **no shut** on the VLAN interface.

- **CSCup53568**

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

Conditions With the IE 2000 running the enhanced lanbase image and 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.

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.

- **CSCuq63577**

Symptom Match Input interface option cannot be configured while configuring class map on the IE 2000.

Conditions The IPLite license is applied.

Workaround There is no workaround for this issue.

- **CSCuq64362**

Symptom QoS VLAN-based and hierarchical queuing is not configurable on the IE 2000 with the IPLite license.

Conditions None.

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.

- **CSCur01466**

Symptom Sometimes a memory leak can be seen originating from psecure_vlan_info_find.

Conditions The leak is occasionally seen when a user tries to enable port-security with a duplicate MAC address and receives an error.

Workaround Reload the system.

- **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.

- **CSCur45858**

Symptom Cisco MAC notification MIB entries are not reported correctly.

Conditions cmnUtilizationUtilization.1001 = 4194258 << This entry is percentage. It is showing > 100.

The Value is shown higher on a device when the mac address entries reach the maximum value.

On another device the value is shown by default as the one above.

Also the cmnUtilizationTable (5) is always shown as zero.

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.

Resolved Caveats

- **CSCuo63008**

  Symptom The SD card cannot be disabled through the CLI.

  Conditions This issue is seen on systems running Cisco IOS Release 15.2(2)E and Cisco IOS Release 15.2(3)EA.

  Workaround This issue is resolved in Cisco IOS Release 15.2(3)E1.

  A new global configuration command, [**no**] **sdflash**, was added for disabling and enabling the SD card.

- **CSCup68260**

  Symptom After some time, traffic will cease to pass on an interface. Shut/no shut of port resolves the issue.

  Conditions This issue can be triggered by using non-shielded Ethernet cables that are in close proximity to electrical wire.

  Workaround Perform the following procedure to set a bootloader variable, SSSMIILOCKUP_WORKAROUND_EN, on CGS 2520 and ESM switches:

1. Make sure there is a valid image in the flash.
2. Set the switch to boot in bootloader mode:

```
Switch> enable
Switch# config t
Switch(config)# boot manual
Switch(config)# end
```

3. Verify that the MANUAL_BOOT variable is set to **yes**:

```
Switch# show boot
```

4. Save the running configuration to flash:

```
Switch# write memory
```

5. Reload the switch:

```
Switch# reload
```

6. When in bootloader mode (at the switch: prompt), set the variable as follows to enable the workaround:

```
switch: set SSSMIILOCKUP_WORKAROUND_EN 1
```

Note: To disable the workaround, set the same variable to **0**.

7. Verify the variable setting:

```
switch: set

Env Vars for Primary Flash:

BAUD=115200
CLEI_CODE_NUMBER=IPML900KRA
DAUGHTERBOARD_ASSEMBLY_NUM=73-12830-02
DAUGHTERBOARD_REVISION_NUM=B0
DAUGHTERBOARD_SERIAL_NUM=FOC16245WB8
MAC_ADDR=5C:50:15:DF:3D:80
MANUAL_BOOT=yes
MODEL_NUM=CGS-2520-24TC
MODEL_REVISION_NUM=B0
MOTHERBOARD_ASSEMBLY_NUM=73-12491-04
MOTHERBOARD_REVISION_NUM=D0
MOTHERBOARD_SERIAL_NUM=FOC16245WDZ
SYSTEM_SERIAL_NUM=FOC1627V38M
TAN_NUM=800-32556-01
TAN_REVISION_NUMBER=F0
VERSION_ID=V01

Env Vars for Secondary Flash:
-- MORE --

!=-
BAUD=115200
BOOT=flash:/
CONFIG_FILE=flash:/config.text
DEBUG_SASQ_READ=1
DEBUG_SASQ_WRITE=1
IMAGE_UPGRADE=yes
MANUAL_BOOT=yes
RESET_REASON=Reload command
SDM_TEMPLATE_ID=0
SSSMIILOCKUP_WORKAROUND_EN=1 <<<<<<< should be 1 == enabled >>>>>>
SWITCH_PRIORITY=1

switch:boot flash:/<path to .bin ios image file in flash:>
```

8. **Important**: Once in IOS mode, configure the switch to disable manual boot so it can load the configured IOS image automatically on the next reload or power cycle event:

```
Switch# config t
Switch(config)# no boot manual
Switch(config)# end
```

9. Check the **show boot** output in Cisco IOS to make sure the correct Cisco IOS image file is configured in BOOT path-list.

- **CSCuq37498**

  Symptom Temperature sensor does not show up in entitySensorMib.

  Conditions entityMib shows IE-2000-16PTC-G-E - Sensor 0 as a sensor. However, on doing a walk of entitySensorMib, no value corresponding to this entity appears.

  A walk of ciscoEntitySensorMib query returns 0 results.

  This issue is seen on the IE 2000 with the IPLite license.

Workaround This issue is resolved in Cisco IOS Release 15.2(3)E1.

- **CSCuq49187**

  Symptom The message "% IPv6 ACL is not supported" appears on boot-up of the switch.

  Conditions This occurs when the SDM template is dual-ipv4-ipv6 routing/default.

  Workaround This issue is resolved in Cisco IOS Release 15.2(3)E1.

- **CSCur21110**

  Symptom The VACL feature cannot be configured.

  Conditions IPLite license needs to be enabled.

  Workaround This issue is resolved in Cisco IOS Release 15.2(3)E1.

- **CSCur43148**

  Symptom "Input errors" and "CRC" errors are increasing on duplex half interface.

  Conditions IE-2000-16PTC-G-E (copper) running with 15.2(2)E.

  Workaround This issue is resolved in Cisco IOS Release 15.2(3)E1.

- **CSCur63376**

  Symptom Tracebacks seen during IE 3010 device reloads.

  Conditions Tracebacks are seen when IE 3010 device is reloaded during a SW upgrade from 152-3.2.88.E to 152-3.2.93.E IOS image versions with the prior configurations available in the device.

  Workaround This issue is resolved in Cisco IOS Release 15.2(3)E1.

- **CSCur81423**

  Symptom Support is required for HTTP access with privileges less than 15.

  Conditions To support the Device Manager read-only user feature, the following Cisco IoT switches need to support read-only user HTTP access: IE 2000, IE 3000, CGS 2520, and IE 3010.

  Other switch platforms do not allow HTTP access with less than privilege 15.

  Workaround This issue is resolved in Cisco IOS Release 15.2(3)E1.

- **CSCus18066, CSCuj85454**

  Symptom Profinet is working only on default VLAN 1.

  Conditions This issue is seen when using DCP and a VLAN other than VLAN 1.

  Workaround This issue is resolved in Cisco IOS Release 15.2(3)E1.

- **CSCus43391**

  Symptom The incorrect syslog message "%ENVIRONMENT-3-POWER_ERROR: PSU x model is not supported - Voltage threshold monitor is skipped" is generated every 30 minutes.

  Conditions This issue is seen on IE 2000 switches that are connected to the PS PWR-IE50W-AC, which is a supported model according to the Cisco IE 2000 Switch Hardware Installation Guide.

Workaround This issue is resolved in Cisco IOS Release 15.2(3)E1.

- **CSCus64918**

  Symptom Software upgrade should remove the previous tar directory completely.

  Conditions This issue is seen when upgrading software using Device Manager. The Device Manager software upgrade should remove the previous directory completely. This way the flash does not accumulate files over time, which requires the user to manually the delete files from the flash to free up space for upgrading.

  Workaround This issue is resolved in Cisco IOS Release 15.2(3)E1.

- **CSCus95881**

  Symptom CIP File object security permissions always fail.

  Conditions CIP File object access fails when security window opened.

  Workaround This issue is resolved in Cisco IOS Release 15.2(3)E1.

- **CSCut12594**

  Symptom When configuring L2NAT on an IE Switch, all traffic on the L2NAT VLAN that does not match the L2NAT translation is dropped.

  Conditions This issue is seen when configuring L2NAT on interfaces in a ring. This issue is also seen when a subset of the traffic on the VLAN is being translated via L2NAT. This is only seen on IE switches that support L2NAT.

  Workaround This issue is resolved in Cisco IOS Release 15.2(3)E1.

- **CSCut21605**

  Symptom Fixes are required for ODVA CT11 warnings.

  Conditions The following warnings are flagged by ODVA CT10/CT11 tests in final reports for DOC certificate:

  * DHCP / static config through TCP/IP object

  * Tcpip object gateway must be reachable from cip interface

  Workaround This issue is resolved in Cisco IOS Release 15.2(3)E1.

- **CSCut45490**

  Symptom Fixes are required for ODVA CT11 warnings, File object.

  Conditions The following warnings are flagged by ODVA CT11 tests in final reports for DOC certificate:

  * File status (attr 1) reported as loaded when file is nonexistent

  * File service 0x4b (Init_Upload) returns incorrect codes when file missing or empty

  * CLI 'show cip file license' NULL

  * File service 0x15 (restore) fails to restore missing file

  * Predefined file instances access is defaulted to read-write except file EDSCollection.gz

  Workaround This issue is resolved in Cisco IOS Release 15.2(3)E1.

- **CSCut51454**

  Symptom CIP EDSCollection.gz missing.

Conditions The code to set EDS files (file instance 0xC9) is missing from the software.

Workaround This issue is resolved in Cisco IOS Release 15.2(3)E1.

- **CSCut51489**

  Symptom Attribute 13 for the Time Sync always returns disabled State.

  Conditions The CT11 tests for Time Sync object always return the port status as disabled when it is actually enabled by default.

  Workaround This issue is resolved in Cisco IOS Release 15.2(3)E1.

- **CSCut56223**

  Symptom Error in TCPIP object set attr 5 (config).

  Conditions IP address, netmask or gateway is unspecified.

  Workaround This issue is resolved in Cisco IOS Release 15.2(3)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:

bst.cloudapps.cisco.com/bugsearch

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

Communications, Services, and Additional Information

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

Cisco Bug Search Tool

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

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

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

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

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

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

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

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

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

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

No combinations are authorized or intended under this document.

© 2015 Cisco Systems, Inc. All rights reserved.