Release Notes for Cisco ISR 1100 Series, Cisco IOS XE Gibraltar 16.10.x

First Published: 2017-11-17

Last Modified: 2019-05-27

Overview of Cisco 1100 Series Integrated Services Routers

The Cisco 1100 Series Integrated Services Routers (ISR) are powerful fixed branch routers based on the Cisco IOS XE operating system. They are multi-core routers with separate core for data plane and control plane. There are two primary models with 8 LAN ports and 4 LAN ports. Features such as Smart Licensing, VDSL2 and ADSL2/2+, 802.11ac with Wave 2, 4G LTE-Advanced and 3G/4G LTE and LTEA Omnidirectional Dipole Antenna (LTE-ANTM-SMA-D) are supported on Cisco 1100 Series ISRs.

Note Explore the Content Hub, the all new portal that offers an enhanced product documentation experience.

- Use faceted search to locate content that is most relevant to you.
- Create customized PDFs for ready reference.
- Benefit from context-based recommendations.

Get started with the Content Hub at content.cisco.com to craft a personalized documentation experience.

Do provide feedback about your experience with the Content Hub.

The following table lists the router models that belong to the Cisco 1100 Series ISRs.

Cisco 1100 Series ISRs	
C1111-8P	C1111-4P
C1111-8PLTEEA	C1111-4PLTEEA
C1111-8PLTELA	C1111-4PLTELA
C1111-8PWE	C1111-4PWE
C1111-8PWB	C1111-4PWB
C1111-8PWA	C1111-4PWA
C1111-8PWZ	C1111-4PWZ
C1111-8PWQ	C1111-4PWN
C1111-8PWN	C1111-4PWQ

Cisco 1100 Series ISRs	
C1111-8PWH	C1111-4PWH
C1111-8PWR	C1111-4PWR
C1111-8PWF	C1111-4PWF
C1111-8PLTEEAWE	C1111-4PWD
C1111-8PLTEEAWB	
C1111-8PLTEEAWA	
C1111-8PLTEEAWR	
C1111-8PLTELAWZ	
C1111-8PLTELAWN	
C1111-8PLTELAWQ	
C1111-8PLTELAWH	
C1111-8PLTELAWF	
C1111-8PLTELAWD	

C1101-4P
C1101-4PLTEP
C1101-4PLTEPWX

C1116-4P
C1116-4PLTEEA
C1116-4PWE
C1116-4PLTEEAWE

C1117-4P
C1117-4PLTEEA
C1117-4PLTELA
C1117-4PWE
C1117-4PWA
C1117-4PWZ

C1117-4PM
C1117-4PMLTEEA
C1117-4PMWE
C1117-4PLTEEAWE
C1117-4PLTEEAWA
C1117-4PLTELAWZ
C1117-4PMLTEEAWE

Product Field Notice

Cisco publishes Field Notices to notify customers and partners about significant issues in Cisco products that typically require an upgrade, workaround or other user action. For more information, see https://www.cisco.com/c/en/us/support/web/field-notice-overview.html.

We recommend that you review the field notices to determine whether your software or hardware platforms are affected. You can access the field notices from https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html#%7Etab-product-categories.

System Requirements

The following are the minimum system requirements:

- Memory: 4GB DDR4
- Flash Storage: 4GB

Determining the Software Version

You can use the following commands to verify your software version:

- For a consolidated package, use the **show version** command
- For individual sub-packages, use the **show version installed** command

Installing a New Software Release

To install, obtain a Cisco IOS XE 16.x consolidated package (image) from Cisco.com. You can find software images at http://software.cisco.com/download/navigator.html. To run the router using individual sub-packages, you also need to first download the consolidated package and extract the individual sub-packages from a consolidated package.

For information about upgrading software, see the “Installing the Software” section in the Software Configuration Guide for the Cisco 1100 Series ISRs.

Upgrading the ROMMON Version on the Cisco 1100 Series ISR

For information about ROMMON and upgrading procedure, see the "ROMMON Overview and Basic Procedures" section in the Hardware Installation Guide for the Cisco 1100 Series Integrated Services Routers.

Feature Navigator

You can use Cisco Feature Navigator to find information about feature, platform, and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on cisco.com is not required.

New and Modified Features for Cisco IOS XE Gibraltar 16.10.x

This section describes new and modified features in Cisco IOS XE Gibralter 16.10.x that are supported on the Cisco 1000 Series ISRs.

New Hardware Features in Cisco 1100 Series ISR Release 16.10.1b

For the hardware features on Cisco 1100 Series Integrated Service Routers for the Cisco IOS XE Gibraltar 16.10.1b release, see the following document:

Cisco 1000 Series Hardware Installation Guide

New Software Features in Cisco IOS XE Gibraltar 16.10.1b

The following are the new software features introduced in Cisco 1000 Series Integrated Service Routers for Cisco IOS XE Gibraltar 16.10.1b release:

APPNAV-XE APP-ID Classification Filter

For detailed information, see the following Cisco document:

https://www.cisco.com/c/en/us/td/docs/routers/access/4400/appnav/isr/isr_appnav/isr_detail_config.html#95623

Syslog Message when Queued Packet Reaches the VPDN Control-Plane

For detailed information, see the following Cisco document:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/vpdn/configuration/xe-16-10/vpdn-xe-16-10-book/vpdn-additional-feat.html#GUID-E8AC4A4E-384A-4208-AB42-ADB750B40E0C

Improvement in Crypto Performance with Crypto Offload

With Cisco IOS XE Gibralter 16.10.1, Crypto performance has been improved with more efficient methods to offload Crypto operations using out-of-band Hardware assists. There are no additional CLI configuration changes needed to leverage this feature. For more information on this contact your local Cisco representative.

Scale Improvement for IPSec VPN tunnels

With Cisco IOS XE Gibralter 16.10.1, the total number of IPSec VPN tunnels supported on C1100 series has increased to 1000, with HSECK9 license. The change in scale is to take effect for all variations of C1100 series (4G 8G 4-port 8-port).

MPLS over DMVPN

For detailed information, see the following Cisco document:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sc_comm_dmvpn/configuration/xe-16-10/sec-comm-dmvpn-xe-16-10-book/sec-comm-dmvpn-xe-16-10-book_chapter_01000.html#id_87580

IOS-XE PMIPv6 Unequal Load Balance

For detailed information, see the following Cisco document:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mob_pmipv6/configuration/xe-16-10/mob-pmipv6-xe-16-10-book/imo-pmipv6-multipath-support.html#id_86067

Optimized APM for Assurance

For detailed information, see the following Cisco document:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/media_monitoring/configuration/xe-16-10/mm-xe-16-10-book.html

NTT Fallback Timer

For detailed information, see the following Cisco document:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/pfrv3/configuration/xe-16-10/pfrv3-xe-16-10-book/pfrv3.html

IOS-XE: PPPoE Control Traffic P-BIT Settings

For detailed information, see the following Cisco document:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_plcshp/configuration/xe-16-8/qos-plcshp-xe-16-8-book/qos-plcshp-ctrl-pln-plc.html

Programmability—gRPC Dial-in and Dial-out

Expands existing Model Driven Telemetry capabilities with the addition of gRPC protocol support and Dial-Out (configured) telemetry subscriptions (Network Essentials and Network Advantage).

For detailed information, see the following Cisco document:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/1610/b_1610_programmability_cg/model_driven_telemetry.html

Programmability—YANG Data Models

For the list of Cisco IOS XE YANG models available with this release, navigate to https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/16101. Revision statements embedded in the YANG files indicate if there has been a model revision. The README.md file in the same GitHub location highlights changes that have been made in the release.

show tech routing

For detailed information, see the following Cisco document:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/isg/command/isg-cr-book/isg_m1.html#wp3145726977

Web User Interface

Supports an embedded Graphical User Interface based device-management tool that helps to provision the device, simplifies device deployment and manageability, and enhances user experience. The following features aresupported on the web user interface:

- Smart Licensing and Specific License Reservation
- Quality of Service/Cisco Application Visibility and Control (AVC)
- VLAN/VTP

For a more detailed overview on Cisco Licensing, go to https://cisco.com/go/licensingguide.

Note The VLANs feature is supported only on routers with switch port module or routers with built-in switch port.

Entering the Configuration Commands Manually

To enter the Cisco IOS commands manually, complete the following steps:

Before you begin

If you do not want to use the factory default configuration because the router already has a configuration, or for any other reason, you can use the procedure in this section to add each required command to the configuration.

Procedure

Step 1 Log on to the router through the Console port or through an Ethernet port.

Step 2 If you use the Console port, and no running configuration is present in the router, the Setup command Facility starts automatically, and displays the following text:

```
--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]:
```

Enter no so that you can enter Cisco IOS CLI commands directly.

If the Setup Command Facility does not start automatically, a running configuration is present, and you should go to the next step.

Step 3 When the router displays the user EXEC mode prompt, enter the **enable** command, and the enable password, if one is configured, as shown in the following example:

```
Router> enable
password password
```

Step 4 Enter config mode by entering the **configure terminal** command, as shown in the following example.

```
Router> config terminal
Router(config)#
```

Step 5 Using the command syntax shown, create a user account with privilege level 15.

Step 6 If no router interface is configured with an IP address, configure one so that you can access the router over the network. The following example shows the interface Fast Ethernet 0 configured.

```
Router(config)# int FastEthernet0
Router(config-if)# ip address 10.10.10.1 255.255.255.248
Router(config-if)# no shutdown
Router(config-if)# exit
```

Step 7 Configure the router as an http server for nonsecure communication, or as an https server for secure communication. To configure the router as an http server, enter the **ip http server** command shown in the example:

```
Router(config)# ip http secure-server
```

Step 8 Configure the router for local authentication, by entering the ip http authentication local command, as shown in the example:

```
Router(config)# ip http authentication local
```

Step 9 Configure the vty lines for privilege level 15. For nonsecure access, enter the transport input telnet command. For secure access, enter the transport input telnet ssh command. An example of these commands follows:

```
Router(config)# line vty 0 4
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport output telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# transport output telnet ssh
Router(config-line)# exit
Router(config)# line vty 5 15
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport output telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# transport output telnet ssh
Router(config-line)# end
```

Open and Resolved Bugs for Cisco IOS XE Gibraltar 16.10.1b

This section provides information about the caveats in Cisco 1100 Series Integrated Services Routers and describe unexpected behavior. Severity 1 caveats are the most serious caveats. Severity 2 caveats are less serious. Severity 3 caveats are moderate caveats. This section includes severity 1, severity 2, and selected severity 3 caveats.

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products. Within the Cisco Bug Search Tool, each bug is given a unique identifier (ID) with a pattern of CSCxxNNNNN, where x is any letter (a-z) and N is any number (0-9). The bug IDs are frequently referenced in Cisco documentation, such as Security Advisories, Field Notices and other Cisco support documents. Technical Assistance Center (TAC) engineers or other Cisco staff can also provide you with the ID for a specific bug. The Cisco Bug Search Tool enables you to filter the bugs so that you only see those in which you are interested.

In addition to being able to search for a specific bug ID, or for all bugs in a product and release, you can filter the open and/or resolved bugs by one or more of the following criteria:

- Last modified date
- Status, such as fixed (resolved) or open
- Severity
- Support cases

You can save searches that you perform frequently. You can also bookmark the URL for a search and email the URL for those search results.

Note If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.

We recommend that you view the field notices for the current release to determine whether your software or hardware platforms are affected. You can access the field notices from the following location:

Product Field Notice Summary

Using the Cisco Bug Search Tool

For more information about how to use the Cisco Bug Search Tool , including how to set email alerts for bugs and to save bugs and searches, see Bug Search Tool Help & FAQ.

Before You Begin

Note You must have a Cisco.com account to log in and access the Cisco Bug Search Tool . If you do not have one, you can register for an account.

Procedure

Step 1 In your browser, navigate to the Cisco Bug Search Tool .

Step 2 If you are redirected to a Log In page, enter your registered Cisco.com username and password and then, click Log In.

Step 3 To search for a specific bug, enter the bug ID in the Search For field and press Enter.

Step 4 To search for bugs related to a specific software release, do the following:

a) In the Product field, choose Series/Model from the drop-down list and then enter the product name in the text field. If you begin to type the product name, the Cisco Bug Search Tool provides you with a drop-down list of the top ten matches. If you do not see this product listed, continue typing to narrow the search results.

b) In the Releases field, enter the release for which you want to see bugs.

The Cisco Bug Search Tool displays a preview of the results of your search below your search criteria.

Step 5 To see more content about a specific bug, you can do the following:

- Mouse over a bug in the preview to display a pop-up with more information about that bug.
- Click on the hyperlinked bug headline to open a page with the detailed bug information.

Step 6 To restrict the results of a search, choose from one or more of the following filters:

Filter	Description
Modified Date	A predefined date range, such as last week or last six months.
Status	A specific type of bug, such as open or fixed.

Filter	Description
Severity	The bug severity level as defined by Cisco. For definitions of the bug severity levels, see Bug Search Tool Help & FAQ.
Rating	The rating assigned to the bug by users of the Cisco Bug Search Tool .
Support Cases	Whether a support case has been opened or not.

Your search results update when you choose a filter.

Related Documentation