Release Notes for Cisco Catalyst IR1101 Rugged Series Router - (Cisco IOS XE 17.2.1)

First Published: 2020-03-30

Last Modified: 2023-05-05

Introduction

The Cisco Catalyst IR1101 Rugged Series Router is a next generation modular industrial router which has a base module with additional Pluggable Modules that can be added. The Pluggable Module provides the flexibility of adding different interfaces to the IR1101 platform, for example, a cellular module.

The IR1101 also has an Expansion Module that adds key capabilities to the IR1101, such as mSATA SSD FRU, Ethernet SFP port, and Digital GPIO connections. It also makes the IR1101 dual LTE capable, with one module in the base and the other in the expansion module.

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Note The IR-1100-SP Expansion Module is the same as the IR-1100-SPMI module, without the Digital I/O and mSATA components.

Interface Naming Conventions

Port	Naming Convention
Gigabit Ethernet combo port	Gigabitethernet 0/0/0
Gigabit Ethernet SFP port on Expansion Module	Gigabitethernet 0/0/5
Fast Ethernet ports	Fastethernet 0/0/1-0/0/4
Cellular Interface on IR1101 Base	Cellular 0/1/0 and Cellular 0/1/1
Cellular Interface on Expansion Module	Cellular 0/3/0 and Cellular 0/3/1
Asynchronous Serial Interface	Async 0/2/0

Port	Naming Convention
USB	usbflash0:
mSATA	msata
IR1101 Base Unit Alarm input	alarm contact 0
GPIO on Expansion Module	alarm contact 1-4

Software Images for IoT Routers

Note You must have a Cisco.com account to download the software.

Table 1: Software Images 17.2.1

Router	Image Type	Filename
IR1101	Universal	ir1101-universalk9.17.02.01.SPA.bin
	NPE	ir1101-universal9_npe.17.02.01.SPA.bin

The latest software downloads for the Routers can be found at:

https://software.cisco.com/download/home/286319772/type

Click on the IR1101 link to take you to the specific software you are looking for.

New Features in Cisco IOS XE 17.2.1

These are the new features for the IR1101.

Support for New Modem

There is a new LTE pluggable module available, the P-LTEAP18-GL 4G module based on Telit LM960 Cat18 4G LTE modem.

Native docker support

Native Docker Support has been added to the 17.2.1 release. This feature enables users to deploy the docker applications on the IR1101. The application lifecycle process is similar to the procedure in the Installing and Uninstalling Apps section. For docker applications, entry point configuration is required as part of the application configuration. Please refer to the following example for the entry point configuration.

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#app-hosting appid app3
Router(config-app-hosting)#app-vnic gateway0 virtualportgroup 0 guest-interface 0
Router(config-app-hosting-gateway0)#guest-ipaddress 192.168.0.7 netmask 255.255.255.0
Router(config-app-hosting-gateway0)#app-default-gateway 192.168.0.1 guest-interface 0
```

```
Router(config-app-hosting)#app-resource docker
Router(config-app-hosting-docker)#run-opts 1 "--entrypoint '/bin/sleep 10000'"
Router(config-app-hosting-docker)#end
Router#
```

The output for docker applications is shown in the following example:

```
Router#show app-hosting detail
App id : app1
Owner : iox
State : RUNNING
Application
Type : docker
Name : aarch64/busybox
Version : latest
Description :
Path : bootflash:busybox.tar
Activated profile name : custom

Resource reservation
Memory : 431 MB
Disk : 10 MB
CPU : 577 units
VCPU : 1

Attached devices
Type Name Alias
---------------------------------------------
serial/shell iox_console_shell serial0
serial/aux iox_console_aux serial1
serial/syslog iox_syslog serial2
serial/trace iox_trace serial3

Network interfaces
---------------------------------------
eth0:
MAC address : 52:54:dd:e9:ab:7a
IPv4 address : 192.168.0.7
Network name : VPG0


Docker
------
Run-time information
Command :
Entry-point : /bin/sleep 10000
Run options in use : --entrypoint '/bin/sleep 10000'
Application health information
Status : 0
Last probe error :
Last probe output :

Router#
```

Yang Data Model Support for Raw Socket Transport

Release 17.2.1 adds support for additional Yang Data Models. These additional models include Raw Socket Transport.

Yang Data Models can be found here:

https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1721

There are two feature modules available for raw socket that belong to the main Cisco-IOS-XE-native model. They are:

Cisco-IOS-XE-rawsocket.yang

This module contains a collection of YANG definitions for Raw Socket Transport Configuration commands.

This module has the following corresponding CLI commands:

```
# encapsulation raw-tcp
# encapsulation raw-udp
# raw-socket packet-length <length>
# raw-socket packet-timer <timer>
# raw-socket special-char <value>
# raw-socket tcp server <port> <ip>
# raw-socket tcp idle-timeout <value>
# raw-socket tcp client <dest-ip> <dest-port>
# raw-socket tcp idle-timeout <timeout>
# raw-socket tcp tcp-session <value>
# raw-socket tcp dscp <value>
# raw-socket udp connection <dest-ip> <dest-port> <local_port>
```

Cisco-IOS-XE-rawsocket-oper.yang

This module contains a collection of YANG definitions for Raw Socket Transport operational data.

This module has the following corresponding CLI commands:

```
# show raw udp statistics
# show raw tcp statistics
# show raw tcp session
# show raw udp session
# show raw tcp session local
# show raw udp session local
```

The following is a list of the Dependent Modules:

- Cisco-IOS-XE-native
- Cisco-IOS-XE-features
- ietf-inet-types
- Cisco-IOS-XE-interfaces
- Cisco-IOS-XE-ip
- Cisco-IOS-XE-vlan
- ietf-yang-types @ (any revision)
- cisco-semver

Digital IO for IOx container applications

Release 17.2.1 provides support for IOx container applications to be able to access the digital IO. There is a new CLI that has been added to the alarm contact command.

```
Router(config)# alarm contact ?
<0-4> Alarm contact number (0: Alarm port, 1-4: Digital I/O)
attach-to-iox Enable Digital IO Ports access from IOX
Router (config)# alarm contact attach-to-iox
```

Enabling the **attach-to-iox** command will provide complete control of all Digital IO ports to IOx. The ports will be exposed as four character devices /dev/dio-[1-4] to IOX applications. You can use read/write functions to get/set values of the Digital IO ports.

If you wish to update the mode, you can write the mode value to the character device file. This is accomplished by IOCTL calls to read/write the state, change mode, and read the true analog voltage of the port. Following this method, you can attach analog sensors to the IR1101. All ports are initially set to Input mode with voltage pulled up to 3.3v.

The following are examples of IOCTL calls:

Read Digital IO Port:

```
cat /dev/dio-1
```

Write to Digital IO Port:

```
echo 0 > /dev/dio-1
echo 1 > /dev/dio-1
```

Change mode:

```
echo out > /dev/dio-1
echo in > /dev/dio-1
```

List of IOCTLs supported:

```
DIO_GET_STATE = 0x1001
DIO_SET_STATE = 0x1002
DIO_GET_MODE = 0x1003
DIO_SET_MODE_OUTPUT = 0x1004
DIO_SET_MODE_INPUT = 0x1005
DIO_GET_THRESHOLD 0x1006
DIO_SET_THRESHOLD = 0x1007
DIO_GET_VOLTAGE = 0x1009
```

Read State using IOCTL:

```
import fcntl, array
file = open("/dev/dio-1","rw")
state = array.array('L',[0])
fcntl.ioctl(file, DIO_GET_STATE, state)
print(state[0])
```

Change mode using IOCTL:

```
import fcntl
file = open("/dev/dio-1","rw")
fcntl.ioctl(file, DIO_SET_MODE_OUTPUT, 0)
```

L2 Sticky Secure MAC Addresses

You can configure an interface to convert the dynamic MAC addresses to sticky secure MAC addresses and to add them to the running configuration by enabling sticky learning. The interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses. All sticky secure MAC addresses are added to the running configuration.

The sticky secure MAC addresses do not automatically become part of the configuration file, which is the startup configuration used each time the switch restarts. If you save the sticky secure MAC addresses in the configuration file, when the switch restarts, the interface does not need to relearn these addresses. If you do not save the sticky secure addresses, they are lost.

Security Violations

It is a security violation when one of these situations occurs:

- The maximum number of secure MAC addresses have been added to the address table, and a station whose MAC address is not in the address table attempts to access the interface.
- An address learned or configured on one secure interface is seen on another secure interface in the same VLAN.

You can configure the interface for one of three violation modes, based on the action to be taken if a violation occurs:

- protect—when the number of secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred.

Note If sticky learning is disabled, the sticky secure MAC addresses are converted to dynamic secure addresses and are removed from the running configuration.

- restrict—when the number of secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. In this mode, you are notified that a security violation has occurred. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.
- shutdown—a port security violation causes the interface to become error-disabled and to shut down immediately, and the port LED turns off. When a secure port is in the error-disabled state, you can bring it out of this state by entering the errdisable recovery cause psecure-violation global configuration command, or you can manually re-enable it by entering the shutdown and no shut down interface configuration commands. This is the default mode.
- shutdown vlan—Use to set the security violation mode per-VLAN. In this mode, the VLAN is error disabled instead of the entire port when a violation occurs

Command Line Interface

Under switch interface, add port-security cli.

```
Router(config-if)#switchport port-security ?
aging Port-security aging commands
mac-address Secure mac address
maximum Max secure addresses
violation Security violation mode
<cr> <cr>
Router(config-if)#switchport port-security mac-address sticky
```

Signed Application Support

Cisco Signed applications are now supported on the IR1101. In order to install a signed application, signed verification has to be enabled on the device. Signed verification can be enabled by following the following instructions.

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#app-hosting signed-verification
```

```
Router(config)#
Router(config)#exit
```

After enabling the signed verification, follow the instructions in the Installing and Uninstalling Apps section under IOx Application Hosting in order to install the application.

Related Documentation

Cisco Catalyst IR1101 Rugged Series Router

IR1101 documentation landing page.

Product Independent Documentation

Cisco IOS XE 17.x

Cisco SD-WAN

Known Limitations

This release has the following limitations or deviations for expected behavior:

Downgrading from 16.12.1 to 16.11.1x

Symptoms: If an IR1101 with RJ45 Gig0/0/0 WAN is downgraded from 16.12.1 to 16.11.1 *x* or earlier, it will cause the Gig0/0/0 to fail to come up because its media-type is set to **media-type sfp**. The problem occurs because 16.12.1 or later automatically selects the correct media-type of the Gig0/0/0 interface, while 16.11.1x and earlier does not have that capability.

Workaround: Specifically set the correct media-type for the Gig0/0/0 interface (e.g. media-type rj45) prior to any downgrade.

An IR1101 operating in SDWAN Controller-mode must not downgrade to Cisco IOS XE Release 17.1.1. This is not supported for SDWAN. Instead, use Cisco IOS XE Release 16.12.1.

Note Cisco IOS XE Release 16.12.1 supports separate Autonomous (non-SDWAN) and SDWAN Controller-mode images.

Day-0 WebUI Feature Not Supported

The Day-0 WebUI feature is not supported with the 17.2.1 release. Users need to configure the Router to access Day-1 WebUI. Refer the Day-1 WebUI configuration webpage for further details.

https://www.cisco.com/c/en/us/td/docs/routers/access/1101/software/configuration/guide/b_IR1101config/m-open_plug_n_play_chapter.html

Caveats

Caveats describe unexpected behavior in Cisco IOS XE releases. Caveats listed as open in a prior release are carried forward to the next release as either open or resolved.

The Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

To view the details of a caveat, click on the identifier.

Open Caveats in Cisco IOS XE 17.2.1

Caveats describe unexpected behavior in Cisco IOS XE releases. Caveats listed as open in a prior release are carried forward to the next release as either open or resolved.

To view the details of a caveat, click on the identifier.

Identifier	Description
CSCvu75971	Benign bootup warning messages appear on the console.
CSCvt74109	mSATA module incorrectly displays OID value.
CSCvv66502	When a Specific License Reservation (SLR) is applied, it will appear as authorized until the next reload. It does not persist through the router reload, but instead is reported as evaluation mode.

Resolved Caveats in Cisco IOS XE 17.2.1

To view the details of a caveat, click on the identifier.

Identifier	Description
CSCvs73854	SPAN capture in both directions is only capturing in one direction.
CSCvs39466	Changing the out of the box baud rate in ROMMON to be 9600.

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 DevNet.
- 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 gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.