Release Notes for Cisco Catalyst IR1101, IR1800, IR8140, IR8340, and Cisco ESR 6300 Routers - (Cisco IOS XE Dublin 17.10.1a)

First Published: 2022-12-15

Last Modified: 2023-08-14

Introduction to this Document

This Release Notes document provides information about the Cisco Catalyst IR1101 Rugged Series Routers, Cisco Catalyst IR1800 Rugged Series Routers, Cisco Catalyst IR8140 Heavy Duty Series Routers, Cisco Catalyst IR8340 Rugged Series Routers, and Cisco ESR6300 Embedded Series Routers running Cisco IOS XE 17.10.1.

This document describes the new features, limitations, troubleshooting, besides providing recommended configurations, caveats, and information on how to obtain support and documentation.

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.

Cisco Catalyst IR1101 Rugged Series Router

The Cisco Catalyst IR1101 Rugged Series Router is a next-generation modular industrial router, which has a base platform with additional pluggable modules that can be added. The pluggable modules provide the flexibility of adding different interfaces to the IR1101 platform, for example, a cellular module, which provides 5G and Fourth-Generation Long-Term Evolution (4G LTE) cellular networks.

The IR1101 also has expansion modules that adds key capabilities to the IR1101. The expansion modules are:

SKU ID	Description
IRM-1100-SPMI	Expansion Module with 1 GE SFP, 1 Pluggable Module, 4 GPIO ports on 1 Digital I/O Connector, and 1 mSATA SSD Slot.
IRM-1100-SP	Expansion Module with 1 GE SFP and1 Pluggable Module.
IRM-1100-4A2T	Expansion Module with an additional four asynchronous serial ports and two Ethernet RJ45 LAN interfaces.
Cellular pluggable modules	A number of pluggable modules are available for cellular connectivity.
IRM-SSD-100G	100 GB pluggable industrial SSD.
P-LPWA-XXX	Cisco LoRaWAN Pluggable Interface Module

Cisco Catalyst IR1800 Rugged Series Router

The Cisco Catalyst IR1800 Rugged Series Router is a modular industrial router. The IR1800 series has four base platforms with additional pluggable modules that can be added. The pluggable modules provide the flexibility of adding different interfaces to the base platform.

The IR1800 series consists of four base platforms:

- IR1821
- IR1831
- IR1833
- IR1835

The IR1800 series features a base platform with modularity, which includes:

SKU ID	Description
IRM-GNSS-ADR	GPS Module with automotive dead reckoning.
WP-WIFI6-x	Wi-Fi 6 Network Interface Module (NIM).
Cellular pluggable modules	A number of pluggable modules are available for cellular connectivity.
IRM-SSD-100G	100 GB pluggable industrial SSD.

Table 1: Differences Between the IR1800 Series Routers' Features

Feature	IR1821	IR1831	IR1833	IR1835
Processor Frequency	600 MHz	600 MHz	600 MHz	1200 MHz
DDR Memory	4 GB	4 GB	4 GB	8 GB
Flash Storage	4 GB	4 GB	4 GB	8 GB
PIM Slot	1	2	2	2
Wi-Fi NIM Module Slot	1	1	1	1

Feature	IR1821	IR1831	IR1833	IR1835
PoE	No	No	Yes	Yes
SSD Module Slot	No	No	Yes	Yes
GPS FRU Module Slot	No	No	Yes	Yes
Digital I/O	No	No	No	Yes
Asynchronous Serial Interface	(1) RS232 DTE	(1) RS232 DTE (1) RS232 DCE	(1) RS232 DTE (1) RS232 DCE	(1) RS232 DTE (1) RS232 DCE/RS485

Cisco Catalyst IR8140 Heavy Duty Series Router

The Cisco Catalyst IR8140 Heavy Duty Series Router (IR8140H), is a next-generation modular IP67 Industrial Router for outdoor use.

These are the two IR8140H models:

- IR8140H-P-K9 (with PoE PSE)
- IR8140H-K9 (without PoE PSE)

The IR8140H series features contains four external module slots plus two onboard WAN ports, and supports the following:

- 60-W PSU
- CPU 1.2 GHz
- 8GB RAM
- 8GB Flash Storage
- GPS onboard receiver
- 900-MHz WPAN – OFDM/FSK Module
- 4G/LTE and 5G IRMH modules
- mSATA module
- 1x 1-Gigabit Ethernet SFP WAN
- 1x 1-Gigabit Ethernet Cu WAN
- PoE (15 W) supported only in the IR8140H-P-K9 PID
- 12VDC_OUT port (only available when PoE is not in use)
- Battery Backup Units (BBUs): Up to three
- 2x Alarm ports (Digital I/O)

Cisco Catalyst IR8340 Rugged Series Router

The Cisco Catalyst IR8340 Rugged Series Router, is the first all-in-one industrial-grade, integrated routing, switching, and security platform.

The IR8340 router features two Pluggable Interface Module (PIM) slots, two single-wide IRM-NIM slots, plus 12 onboard LAN ports, and two WAN ports, and supports the following:

- 150W or 250W PSU, low-voltage DC and high-voltage AC/DC options
- PTP on LAN ports - Default, power and Dot1as profiles
- 5G and 4G LTE PIM
- T1/E1 Network Interface Modules (NIM)
- 8-port Asynchronous/Synchronous Network Interface Module (NIM) IRM-NIM-RS232
- mSATA module
- 2 x 1-G Combo WAN ports
- 4 x 1-G Copper LAN ports
- 4 x 1-G Combo LAN ports
- 4 x 1-G SFP LAN ports
- PoE PoE+ UPoE (up to 60 W) support on LAN ports 1-4
- 2 x IN and 1 x OUT Alarm ports (RJ45)

Cisco ESR6300 Embedded Series Router

The ESR6300 is a small form factor embedded router module with a board size of 3.0 in. x 3.775 in. (76.2 mm x 95.885 mm).

The more compact design simplifies integration and offers system integrators the ability to use the Cisco ESR6300 in a wide variety of embedded applications. The ESR module is available with a Cisco-designed cooling plate customized to the ESR, as well as without the cooling plate for system integrators who want to design their own custom thermal solution.

There are two ESR6300 SKUs:

- ESR-6300-NCP-K9: Embedded Router Board without a cooling plate
- ESR-6300-CON-K9: Embedded Router Board with a cooling plate

Both SKUs offer the following port and module interfaces:

- Four GE LAN ports
- Two combo GE WAN ports
- One USB 3.0 port
- One mSATA module interface

Interface Naming Conventions

Cisco Catalyst IR1101 Rugged Series Router

The following section shows the names of the interfaces on each of the IoT routers.

Port	Naming Convention
Gigabit Ethernet combo port	GigabitEthernet0/0/0
Gigabit Ethernet SFP port on IRM-1100	GigabitEthernet0/0/5
Gigabit Ethernet on IRM-1100-4A2T mounted on the Expansion side	gigabitetherenet 0/0/5 gigabitetherenet 0/0/6
Fast Ethernet ports	FastEthernet0/0/1 FastEthernet0/0/2 FastEthernet0/0/3 FastEthernet0/0/4
Cellular Interface on IR1101 Base	Cellular 0/1/0 Cellular 0/1/1
Cellular Interface on IRM-1100 mounted on the top (EM) side	Cellular 0/3/0 Cellular 0/3/1
Cellular Interface on IRM-1100 mounted on the bottom (CM) side	Cellular 0/4/0 Cellular 0/4/1
Asynchronous Serial Interface Base	Async0/2/0

Port	Naming Convention
IRM-1100-4A2T is mounted on the top (EM) side	async 0/3/0 async 0/3/1 async 0/3/2 async 0/3/3
IRM-1100-4A2T is mounted on the bottom (CM) side	async 0/4/0 async 0/4/1 async 0/4/2 async 0/4/3
USB	usbflash0:
mSATA	msata
IR1101 Base Unit Alarm input	alarm contact 0
GPIO on IRM-1100	alarm contact 1-4
LoRaWAN interface on IR1101 Base	LORAWAN0/1/0

Cisco Catalyst IR1800 Rugged Series Router

Port	Naming Convention
Gigabit Ethernet combo port	GigabitEthernet0/0/0
Gigabit Ethernet ports	GigabitEthernet0/1/0 GigabitEthernet0/1/1 GigabitEthernet0/1/2 GigabitEthernet0/1/3
Cellular Interface	Cellular 0/4/0 Cellular 0/4/1 Cellular 0/5/0 Cellular 0/5/1
Asynchronous Serial Interface	Async0/2/0 Async0/2/1 (when the base platform supports two asynchronous serial interfaces)
Wi-Fi Interface	Wl0/1/4
USB	usbflash0:
mSATA	msata

Port	Naming Convention
GPIO	alarm contact 1-4

Cisco Catalyst IR8140 Heavy Duty Series Router

Port	Naming Convention
Gigabit Ethernet ports	GigabitEthernet0/0/0 GigabitEthernet0/0/1
Cellular Interface	Cellular 0/2/0 OR Cellular 0/3/0
SSD	Virtual port Group0
WPAN	Wpan 0/1/0 Wpan 0/2/0 Wpan 0/3/0
Digital IO	alarm contact 1-2

Cisco Catalyst IR8340 Rugged Series Router

Port	Naming Convention
Gigabit Ethernet WAN ports	GigabitEthernet0/0/0 GigabitEthernet0/0/1
Gigabit Ethernet LAN ports	GigabitEthernet0/1/0 GigabitEthernet0/1/1 GigabitEthernet0/1/2 GigabitEthernet0/1/3 GigabitEthernet0/1/4 GigabitEthernet0/1/5 GigabitEthernet0/1/6 GigabitEthernet0/1/7 GigabitEthernet0/1/8 GigabitEthernet0/1/9 GigabitEthernet0/1/10 GigabitEthernet0/1/11

Port	Naming Convention
Cellular Interface	Cellular 0/4/0 Cellular 0/4/1 Cellular 0/5/0 Cellular 0/5/1
NIM Interface (Asynchronous/Synchronous Serial Ports or E1/T1 ports)	0/2/0 0/2/1 0/3/0 0/3/1
mSATA SSD	msata
GPIO	alarm contact 1-2
USB Port	usb0:
Console Port	Line console 0

Cisco ESR6300 Embedded Series Router

Port	Naming Convention
Gigabit Ethernet combo port WAN Layer3	GigabitEthernet0/0/0 GigabitEthernet0/0/1
Gigabit Ethernet LAN Layer 2 ports	GigabitEthernet0/1/0 GigabitEthernet0/1/1 GigabitEthernet0/1/2 GigabitEthernet0/1/3
Cellular Interface	Cellular 0/3/0
USB Port	usbflash0: (IOS and rommon)
Console Port	Line console 0

Software Images for Cisco IOS XE Release 17.10.1a

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

Cisco IOS XE Release 17.10.1a includes the following Cisco images.

Table 2: Software Images for Cisco IOS-XE, Release 17.10.1a

Router	Image Type	Filename
IR1101	Universal	ir1101-universalk9.17.10.01a.SPA.bin
	NPE	ir1101-universal9_npe.17.10.01a.SPA.bin
IR1800	Universal	IR1800-universalk9.17.10.01a.SPA.bin
	NPE	IR1800-universal9_npe.17.10.01a.SPA.bin
IR8140	Universal	IR8100-universalk9.17.10.01a.SPA.bin
	NPE	IR8100-universal9_npe.17.10.01aa.SPA.bin
IR8340	Universal	IR8340-universalk9.17.10.01a.SPA.bin
	NPE	IR8340-universalk9_npe.17.10.01a.SPA.bin
ESR6300	Universal	c6300-universalk9.17.10.01a.SPA.bin

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

https://software.cisco.com/download/home/286323433

Click the link corresponding to your device to take you to the specific software you are looking for.

New Features in Cisco IOS XE 17.10.1a

The following sections describe the major enhancements available in Cisco IOS XE 17.10.1a on each of the routers.

Major Enhancements in IR1101

The following are the new features for the IR1101.

Also see the Major Enhancements Common to all IoT Routers, on page 18.

Software Supported MACsec

Overview

All existing Cisco IOS XE based router/switch use special transceiver to do MACsec encryption/decryption. This software MACsec uses CDAL infrastructure in QFP to do crypto operation. Comparing to the hardware choice, the way configuration/status/datapath is done is different thus creating some limitation on the functionality.

Release 17.10.1a only supports MACsec on L2 interfaces. The MACsec port must be put into access mode. As the encryption happens on the egress SVI interface, the vlan used for the port should be unique, meaning no other interface can use that vlan. This limitation is because the QFP does not have MAC table information.

Note Since MACsec is being done through software, performances are not line rate on L2 interfaces.

Note Cisco supports only the should secure MACsec mode for IR1101, which allows unencrypted traffic even in a secured state.

Limitation:

The IR1101 does not support the must secure mode.

For an egress packet, SVI only know the packet needs to go out on a vlan without info about any specific interface. It is up to the switch chip to decide which port to go. All the packets without MACsec tag can come in as usual. Outgoing L2 packet will also egress without encryption or modification.

Both the NE and NA license support GCM-AES-128. This feature is not available running the NPE image.

The MACsec protocol is defined in IEEE802.1AE.

Feature Limitations

- MACsec is not supported in controller mode in this release.
- There must be a unique vlan id for a MACsec interface.
- Only gcm-aes-128 is supported in this initial release.
- Both explicit and non-explicit SCI are supported on ingress side. The IR1101 sends out only explicit SCI packets as it is not an end system.
- The IR1101 does not support confidentiality offset.
- Integrity only is not supported in this first release.
- For gcm-aes-128, up to 32 bytes are added to an encrypted packet compared to a plain packet. So the MTU setup should add 32 for it to work properly.
- The MACsec key is managed by the MKA module. For that device, it requires a static key for MKA to negotiate MACsec key.
- There is no MIB support.
- IP Device Tracking (IPDT) is not supported in the host-to-switch MACsec configurations.

Related Documentation

Further information can be found at the following:

- MACsec and the MACsec Key Agreement (MKA) Protocol
- MACSEC and MKA Configuration Guide, Cisco IOS XE 17

Sample MKA Configuration

See the following example:

```
conf t
   aaa new-model
   mka policy p1
       key-server priority 1
       macsec-cipher-suite gcm-aes-128
       sak-rekey interval 3600
end
conf t
   key chain cak1 macsec
      key 414243
         cryptographic-algorithm aes-128-cmac
         key-string 0 12345678901234567890123456789012
         lifetime local 00:00:00 29 November 2021 infinite
end
conf t
   int fa 0/0/2
      switchport mode access
      switchport access vlan 77
      mtu 1532
      mka policy p1
      mka pre-shared-key key-chain cak1
      macsec network-link
      macsec replay-protection window-size 128
end
```

Show Commands

Show cpp_cp internal info:

```
show platform hardware cpp active feature soft-macsec server tx [dp] [item]
show platform hardware cpp active feature soft-macsec server rx [dp] [item]
show platform hardware cpp active feature soft-macsec server control [dp] [item]
```

Other show commands:

```
show macsec summary
show macsec status int fa 0/0/2
show macsec statistics int fa 0/0/2A
```

Clear Statistics

```
Clear macsec statis int fa 0/0/2
```

Test Command

Print 10 MKA packet for debug:

```
test platform software smacsec mka-ingress
```

High Security (HSEC) License

HSEC (High Security) license is a feature license that can be configured in addition to the network license (NE/NA). An HSEC license provides export controls for strong levels of encryption. HSEC is available to customers in all currently non-embargoed countries as listed by the U.S. Department of Commerce. Without an HSEC license, SEC performance is limited to a total of 250 Mbps of IPsec throughput in each direction. An HSEC license removes this limitation.

Command Line Interface

The configuration mode CLI to enable HSEC on the IR1101 is the following:

```
IR1101(config)# license feature hsec9
```

To benefit from the HSEC license, a new bandwidth will be available. The new bandwidth is called **uncapped**, and it is available with the following CLI from configuration mode:

```
IR1101(config)# platform hardware throughput level ?
250M throughput in bps
uncapped throughput in bps
IR1101# platform hardware throughput level uncapped
```

After performing the above commands, write mem and reload the router. The configuration will take effect when the router comes back up.

License Types

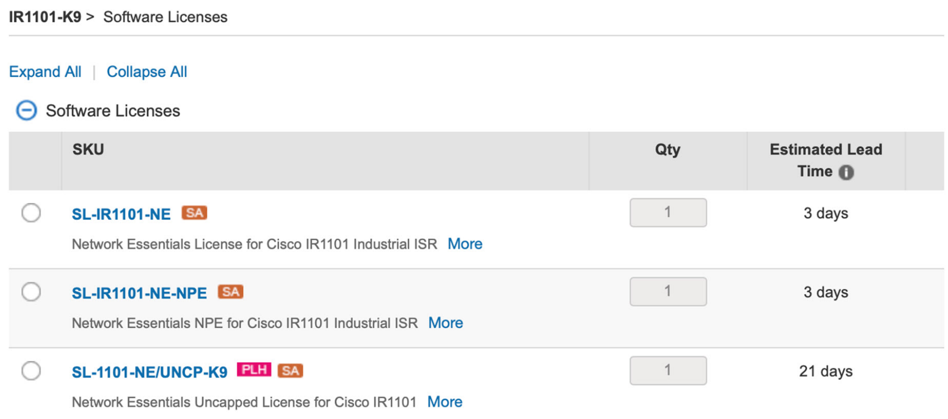
With this new feature, the IR1101 will support the following bandwidth/license types:

- Network-essentials 250 Mbps
- Network-advantage 250 Mbps
- Network-essentials uncapped
- Network-advantage uncapped
- HSEC

Ordering

The following is an example from the IR1101-K9. The license will be available on the IR1101-A-K9 as well.

In the following example, select the SL-1101-NE/UNCP-K9 (Network Essentials Uncapped License):



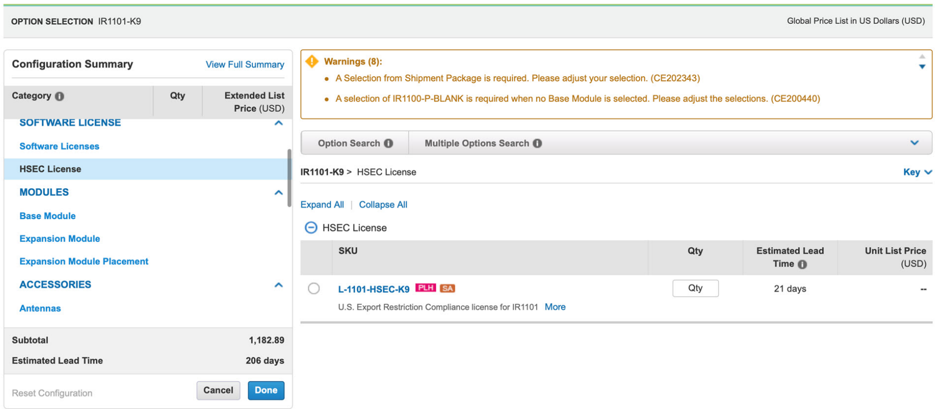
IR1101-K9 > Software Licenses

Expand All | Collapse All

⊖ Software Licenses

	SKU	Qty	Estimated Lead Time
○	**SL-IR1101-NE** SA Network Essentials License for Cisco IR1101 Industrial ISR More	1	3 days
○	**SL-IR1101-NE-NPE** SA Network Essentials NPE for Cisco IR1101 Industrial ISR More	1	3 days
○	**SL-1101-NE/UNCP-K9** PLH SA Network Essentials Uncapped License for Cisco IR1101 More	1	21 days

The L-1101-HSEC-K9 license will get auto included when you select the uncapped license, as shown in the following:



OPTION SELECTION IR1101-K9 | Global Price List in US Dollars (USD)

Configuration Summary | View Full Summary

Category	Qty	Extended List Price (USD)
SOFTWARE LICENSE		
Software Licenses		
HSEC License		
MODULES		
Base Module		
Expansion Module		
Expansion Module Placement		
ACCESSORIES		
Antennas		
Subtotal		1,182.89
Estimated Lead Time		206 days

Reset Configuration | Cancel | Done

Warnings (8):

- A Selection from Shipment Package is required. Please adjust your selection. (CE202343)
- A selection of IR1100-P-BLANK is required when no Base Module is selected. Please adjust the selections. (CE200440)

Option Search | Multiple Options Search

IR1101-K9 > HSEC License | Key

Expand All | Collapse All

HSEC License

	SKU	Qty	Estimated Lead Time	Unit List Price (USD)
○	L-1101-HSEC-K9 PLH SA U.S. Export Restriction Compliance license for IR1101 More	Qty	21 days	--

Cisco Software Central

This guide provides information on how to order, activate, and manage your Cisco Smart Licenses.

https://software.cisco.com/software/csws/ws/platform/home?locale=en_US&locale=en_US&locale=en_US#

Support for LoRaWAN Pluggable Module

The Cisco LoRaWAN Pluggable Interface Module supports eight channels of LoRa connectivity.

There are two different P-LPWA modules:

- The P-LPWA-900 is designed for RF regional profile US915, AS923 and AU915 as defined by the LoRa Alliance RF regional profile specifications.
- The P-LPWA-800 is designed for the EU868, IND865 and RU864 RF regional profile as defined by the LoRa Alliance RF regional profile specifications.

The Cisco LoRaWAN pluggable modules can be managed by command line interface (CLI), or the Cisco IOS XE Web User Interface (WebUI).

Yang operational model support has been added for the information that is currently available in the lorawan show commands. Yang configuration model support for lorawan configuration commands, including interface and packet forwarder configurations (command packet forwarder and lrr packet forwarder).

For complete information on the LoRaWAN Pluggable Interface Module see the Cisco LoRaWAN Pluggable Interface Module Installation and Configuration Guide.

Major Enhancements in IR1800

The following are the new features for the IR1800:

Also see the Major Enhancements Common to all IoT Routers, on page 18.

Digital Subscriber Line (DSL) SFP Support on the IR1800

The IR1800 now supports the DSL SFP in the same manner as the IR1101. For complete details, see the Configuring Digital Subscriber Line (DSL) chapter in the IR1101 Configuration Guide.

vManage Support for the WP-WIFI6-x Module

This release will enable configuration and monitoring of the WP-WIFI6-x module through vManage from SDWAN. This applies only when the module is running in EWC mode.

For further information about vManage, see the product landing page here: https://www.cisco.com/site/us/en/products/networking/wan/vmanage/index.html

Major Enhancements in IR8140

The following are the new features for the IR8140:

Also see the Major Enhancements Common to all IoT Routers, on page 18.

Wi-SUN 1.1 Limited Function Nodes (LFN) Security Support and L & G Interoperability

Wi-SUN FAN 1.1 introduces support for Limited Function Nodes (LFN), which are optimized for low power operation. To achieve this, several enhancements are added to the Wi-SUN FAN Technical Profile Specification to optimize the protocols to reduce the number of messages for LFNs.

The IR8140 implements a Wi-SUN FAN Border Router. The Border Router must support LFN Security for any topology that includes LFNs.

Note Note: if an LFN is allowed to join directly to a Border Router, then the Border Router needs to support LFN Neighbor Discovery and needs MAC layer enhancements for LFN support.

This feature only covers the LFN security portion and does not include functionality needed to support topologies where the LFN joins directly to the Border Router.

Major Enhancements in IR8340

The following are the new features for the IR8340:

Also see the Major Enhancements Common to all IoT Routers, on page 18.

Private VLAN

Private VLAN is used to divide a normal VLAN into isolated L2 partitions. Every host port in a private VLAN is one of three types:

- Isolated — An isolated port cannot talk to any other port in that PVLAN, except the promiscuous port. If an end device only wants to have access to a gateway router, then it would be attached to an isolated port.
- Community — A community port is part of a group of ports. The ports within the same community can have layer 2 communications with one another and can also talk to the promiscuous port.
- Promiscuous — A promiscuous port can talk to all other types of ports. A promiscuous port can talk to isolated ports and community ports and vice versa. Layer 3 gateways are typically connected to the switch via a promiscuous port.

The following is a summary of the supported features:

- Isolated access port: Access port which can only communicate with promiscuous port.

- Promiscuous access port: Access ports which can communicate with all ports in private VLAN.
- Community access port: Access ports which can communicate with ports in same community and promiscuous ports.
- Private VLAN across switches: Private VLAN traffic can be carried across normal trunk ports and the feature can span across switches.
- Promiscuous trunk port: A trunk port carrying primary VLAN traffic for multiple private VLAN. The secondary VLANs are explicitly mapped to primary VLAN for multiple private VLAN.
- Multicast in Private VLAN: Multicast communication in and out of private VLAN.
- Layer 3 communication between isolated ports: Isolated ports can communicate at layer 3

The following features are NOT supported:

- 2-way community VLAN: The community ports send and receive traffic in same VLAN.
- Trunk isolated/community ports: Isolated and community ports are trunk with secondary VLANs of multiple private VLAN.

IGMP Filtering and Throttling

In some environments, for example, metropolitan or multiple-dwelling unit (MDU) installations, you might want to control the set of multicast groups to which a user on a switch port can belong. You can control the distribution of multicast services, such as IP/TV, based on some type of subscription or service plan. You might also want to limit the number of multicast groups to which a user on a switch port can belong.

With the IGMP filtering feature, you can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating them with individual switch ports. An IGMP profile can contain one or more multicast groups and specifies whether access to the group is permitted or denied. If an IGMP profile denying access to a multicast group is applied to a switch port, the IGMP join report requesting the stream of IP multicast traffic is dropped, and the port is not allowed to receive IP multicast traffic from that group. If the filtering action permits access to the multicast group, the IGMP report from the port is forwarded for normal processing. You can also set the maximum number of IGMP groups that a Layer 2 interface can join.

IGMP filtering controls only group-specific query and membership reports, including join and leave reports. It does not control general IGMP queries. IGMP filtering has no relationship with the function that directs the forwarding of IP multicast traffic. The filtering feature operates in the same manner whether CGMP or MVR is used to forward the multicast traffic. IGMP filtering applies only to the dynamic learning of IP multicast group addresses, not static configuration.

With the IGMP throttling feature, you can set the maximum number of IGMP groups that a Layer 2 interface can join. If the maximum number of IGMP groups is set, the IGMP snooping forwarding table contains the maximum number of entries, and the interface receives an IGMP join report, you can configure an interface to drop the IGMP report or to replace the randomly selected multicast entry with the received IGMP report.

Major Enhancements in ESR6300

The following are the new features for the ESR6300:

Also see the Major Enhancements Common to all IoT Routers, on page 18.

Support for the P-5GS6-GL Pluggable Module on the ESR6300

Support for the P-5GS6-GL Pluggable Module works the same on the ESR6300 as it does on the other IoT Routers. For details, see 5G Sub-6 GHz Pluggable Interface Module and Cellular Pluggable Interface Module Configuration Guide.

MAB 802.1x Support

Standalone MAC Authentication Bypass (MAB) is an authentication method that grants network access to specific MAC addresses regardless of 802.1X capability or credentials. As a result, devices such as cash registers, fax machines, and printers can be readily authenticated, and network features that are based on authorization policies can be made available.

For further information, see the Authentication Authorization and Accounting Configuration Guide, Cisco IOS XE

Major Enhancements Common to all IoT Routers

The following are the new features that are common to all routers:

Enable Secure Data Wipe Capabilities

Secure data wipe is a Cisco wide initiative to ensure storage devices on all the IOS XE based platforms to be properly purged using NIST SP 800-88r1 compliant secure erase commands. Whenever possible, IoT platforms will leverage the corresponding ENG design and implementation available so far on their platforms.

This feature is supported on the following IoT platforms:

- IR1101
- IR1800
- IR8140
- ESR6300

When the enable secure data wipe is executed, the following will get wiped out:

- IR1101, IR1800, IR8140: NVRAM, rommon variables, and bootflash
- ESR6300: NVARM, rommon variables, bootflash

The router will be in rommon prompt with default factory settings (baud rate 9600) after the command is executed. The bootflash will not get formatted until booting with IOS image thru usbflash or tftp download if the platform is supported.

Performing a Secure Data Wipe

To enable the feature, perform the following:

```
Router#factory-reset all secure
The factory reset operation is irreversible for securely reset all. Are you sure? [confirm]Y
```

Important This operation may take hours. Please do not power cycle.

To check the log after the command is executed, and booting up IOS XE, perform the following:

```
Router#show platform software factory-reset secure log
Factory reset log:
#CISCO DATA SANITIZATION REPORT:# IR1800
Purge ACT2 chip at 12-08-2022, 15:17:28
ACT2 chip Purge done at 12-08-2022, 15:17:29
mtd and backup flash wipe start at 12-08-2022, 15:17:29
mtd and backup flash wipe done at 12-08-2022, 15:17:29.
```

Rawsocket Keepalive Configuration CLI

Rawsocket keepalive for async interfaces is a feature that existed in classic IOS platforms. As part of 17.10.1a, the feature will be extended to IOS-XE based platforms. A new CLI with the following syntax will be added under rawsocket.

```
Router(config-line)#raw-socket tcp keepalive interval
```

CLI Changes

On IOS-XE platforms starting from 17.10.1a, there is a CLI correction and an additional CLI was added as part of raw-socket.

The correction is for the **raw-socket idle timeout** command. There is now an option to configure the timeout based on minutes and seconds, whereas the previous configuration used only minutes.

```
Router(config-line)# raw-socket tcp idle-timeout [0-1440] [<0-59> | cr]
```

The additional CLI is for clearing the raw-socket TCP clients. The command syntax is **clear raw-socket line** *[1-145|tty|x/y/z]* for example:

```
Router# clear raw-socket line 0/2/0
```

Note When initiating clear raw-socket line, raw-socket sessions will be cleared for raw-socket clients from the **show raw-socket tcp sessions** command. Connections will be re-established after a TCP hand-shake, which can be done by doing shut/no shut on TCP connection interface.

Related Documentation

Cisco Catalyst IR1101 Rugged Series Router

IR1101 documentation landing page

Cisco Catalyst IR1800 Rugged Series Router

IR1800 documentation landing page

Cisco Catalyst IR8140 Heavy Duty Series Router

IR8100 documentation landing page

Cisco Catalyst IR8340 Rugged Series Router

IR8340 documentation landing page

Cisco ESR6300 Embedded Series Router

ESR6300 documentation landing page

Product Independent Documentation

Cisco Industrial Routers and Industrial Wireless Access Points Antenna Guide

Cisco IOS XE 17.x

Cisco SD-WAN

Cisco IoT Field Network Director

Cisco Industrial Network Director

Known Limitations

Smart Licensing Using Policy

Starting with Cisco IOS XE 17.6.1, with the introduction of Smart Licensing Using Policy, even if you configure a hostname for a product instance or device, only the Unique Device Identifier (UDI) is displayed. This change in the display can be observed in all licensing utilities and user interfaces where the hostname was displayed in earlier releases. It does not affect any licensing functionality. There is no workaround for this limitation.

The licensing utilities and user interfaces that are affected by this limitation include only the following: Cisco Smart Software Manager (CSSM), Cisco Smart License Utility (CSLU), and Smart Software Manager On-Prem (SSM On-Prem).

IOx on the ESR6300

Note IOx development is not supported on the ESR6300. While this is platform independent code, it is unsupported and untested on this device.

Expansion Module on the IR1101

The expansion module IR1101 does not support +1500 MT size on LAN interfaces. See this Caveat for details.

Standalone MAC Authentication Bypass (MAB) Limitation

Standalone MAC Authentication Bypass (MAB) is an authentication method that grants network access to specific MAC addresses regardless of 802.1X capability or credentials.

Refer to the following table for details:

Details	Release Affected	Release Fixed
MAB/Dot1x may not work if the global type-6 encryption setting is enabled. If users still want to use MAB/Dot1x, they should disable the type-6 encryption and enable type-7 encryption.	17.4.X 17.5.X 17.6.1 17.6.2 17.7.1	17.3.5 Fixed in these future releases: 17.6.3 17.7.2 17.8.1 and later.
dACL and device-tracking features are not supported on the IR1101 and ESR6300 due to a hardware limitation. dACL is supported on the IR1800 series. Therefore, features such as MAB and Dot1x should not be used with the optional dACL/device-tracking enabled.	**Note** Occurs in all releases.	Hardware limitation, no software fix available.

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.

Open Caveats in Cisco IOS XE 17.10.1a

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

Identifier	Description	Platform
CSCwc31184	FN980: ATT sim attached with wrong profile during sim switching.	P-5GS6-GL
CSCwa91102	VMI Neighbor counters for input packets always show as 0 with DLEP data path traffic.	ESR6300
CSCwc25912	PUNT Policer messages when DLEP conf is attached.	ESR6300
CSCwa76815	Line range limitations on controller mode.	IR1101
CSCvz30726	High CF/TE,Turnaround and Latency number after reload of router.	IR8340

Identifier	Description	Platform
CSCwa92737	IR8340 throws CPP/FMAN Download errors on attaching ngsw class-map using etype classification.	IR8340
CSCwb13098	GLC-T on WAN interface G 0/0/0 is admin down post booting with latest 17.8.1	IR8340
CSCwb40769	PTP Dot1as Latency accuracy is seen 13ms on latest 1781 image	IR8340
CSCvz19429	PTP Forward mode functionality is not working.	IR8340
CSCvw58347	Last reporter of IGMPV3 report is all "0" if receiver connected on SVI interface.	IR8340
CSCwc24547	Cellular serviceability feature is not enabled on IR8340	IR8340
CSCwc44403	Telit Modem LM960 SIM slot switch may affect the other Telit modems present in platform	IR8140
CSCwc44795	"show archive" not displaying & limiting archived configurations=> consuming space + firmw upg fails	IR1101
CSCwc28468	SDWAN mode: vManage always fails to push any template to device if device is running in FIPS mode.	ESR6300
CSCwc50075	WP7607: Sim in slot 1 can't attach with network	WP7607
CSCwd56131	LTE modem doesn't show GSM bands. **Note** This defect started with release 17.5.1	IR1101
CSCwd09947	Day0 Webui Error: Router failed to issue 192.168.x.x address to workstation for dayzero WebUI launch.	IR1101 IR1800
CSCwd28373	ESR-6300 can´t ping from SVI to another ESR-6300 SVI.	ESR 6300
CSCwd58723	IR1100 crashes with concurrent IPSec traffic and macsec traffic (device to client)	IR1101
CSCwf22381	WAN SFP link goes down after reloading Peer.	IR1800
CSCwf84896	Bootflash doesn't have enough space to install new image	IR1101

Resolved Caveats in Cisco IOS XE 17.10.1a

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

Identifier	Description	Platform
CSCwb26015	FN980: Modem not able to load correct attach profiles as in controller context.	FN980
CSCwc23225	IR8340: GPS mode of controller cellular shows not configured.	IR8340
CSCwc18190	IR8140: Telit Modem LM960 FN980 FW upgrade may fail when two Telit modems present in platform.	IR8140
CSCwa54792	Configure replace fails to handle eem applet removal.	IR1101 ESR6300

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.

Documentation Feedback

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

Cisco Support Community

Cisco Support Community is a forum for you to ask and answer questions, share suggestions, and collaborate with your peers. Join the forum at: https://supportforums.cisco.com/index.jspa.

Cisco Bug Search Tool (BST)

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.

Abbreviated Cisco Trademarks