Release Notes for Cisco Embedded Service 6300 Series Router – Release 17.4.1

Revised February 11, 2022

The following release notes support the Cisco ESR6300 router. These release notes are updated to describe new features, limitations, troubleshooting, recommended configurations, caveats, and provide information on how to obtain support and documentation.

Table 1 provides the hardware product IDs and brief descriptions for the boards.

Table 1 Cisco ESR 6300 SKUs

SKU	Description	Ports/Module Interfaces
ESR-6300-NCP-K9	Embedded Router Board without a cooling plate. (NCP = No Cooling Plate)	4 GE LAN ports 2 combo GE WAN ports 1 USB 3.0 port 1 mSATA module interface
ESR-6300-CON-K9	Embedded Router Board with cooling plate. (CON = Conduction cooled).	4 GE LAN ports 2 combo GE WAN ports 1 USB 3.0 port 1 mSATA module interface

Contents

This publication consists of the following sections:

- General Description, page 2
- Image Information and Supported Platforms, page 2
- Interface Naming Conventions, page 2
- Related Documentation, page 5
- Caveats, page 6
- Communications, Services, and Additional Information, page 6

General Description

The ESR6300 is a small form factor embedded router module with a board size of 3.0" x 3.775" (76.2mm x 95.885mm). The more compact design simplifies integration and offers system integrators the ability to use the Cisco ESR 6300 in a wide variety of embedded applications. The ESR card 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.

Image Information and Supported Platforms

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

Cisco IOS-XE Release 17.4.1 includes the following Cisco image:

- c6300-universalk9.17.04.01.SPA.bin

The latest software downloads for the ESR6300 can be found at:

https://software.cisco.com/download/home/286323493/type

Click on the ESR6300 link to take you to the specific software you are looking for.

Interface Naming Conventions

The following table shows the naming conventions.

Table 2 Hardware Interface Naming Convention

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

Known Limitations

The following features are not supported on the ESR6300 with software release 17.4.1:

- No support for MacSec or DLEP in this release. (MQC: modular quality of service command line).
- Layer 2 COS to DSCP mapping does not work due to no ASIC chipset support for the feature.
- Copper FE SFPs are not supported on the ESR6300.
- Copper GE SFPs are only supported in config terminal > service internal > service unsupported-transceiver mode.
- Cisco does not claim IP Mobility for Ethernet support on the ESR6300.
- Auto-negotiation for 10Mbps, 100Mbps, 1000Mbps in full-duplex mode is supported. For half duplex, support is only on 10Mbps and 100Mbps.
- Refer to the Cisco Approved Vendor List (AVL]) for Cisco USBs. Kingston USB 3.0 works as well. Ensure the USB has a single partition and ext2, Fat16, or Fat32 format only.
- Cellular functionality is not supported.
- Radio Aware Routing is not supported.
- For Security: No support for TLS, TrustSec, MacSec , CWS [Cloud Web Security], IDS/IPS.

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

- The WebUI Licensing Page is unsupported for release 17.4.1. For all licensing configuration, please use CLI mode or CSSM.
- In the Web User Interface (WebUI), there are two known issues where erroneous information is displayed. In both of these cases, the information is present in the WebUI even though the functionality is **NOT** supported on the ESR6300.
  - Under **Configuration > Security > Threat Defense > snort** there is a RAM and DISK size prerequisite check that fails.

- Under **Configuration > Security >** there is a category for Trustsec.

These are both cosmetic issues due to the features being unavailable in the 17.4.1 release.

- The IOS boot system setting allows users to specify any flash-based storage URL for IOS image booting.

  The rommon on the ESR6300 does not expose the non-IOX msata partition, therefore auto-booting from mSATA will not work even if it is configured in IOS.

  Example: Users must not configure a boot system setting as follows:

  ```
  (config)#boot system flash msata:ios-image
  ```

- Receive a message 'unable to open bootflash:golden.bin (14)' during bootup.

  Example: Pushing the reset button displays the unable to open message.

  ```
  ESR-6300-CON-K9 platform with 4194304 Kbytes of main memory

  MCU Version - Bootloader: 4, App: 10

  MCU is in application mode.

  Reset button push detected

  unable to open bootflash:golden.bin (14)
  ```

  This message is intended by design to inform the user they have not setup a golden.bin config file.

Note: Starting with Cisco IOS XE Amsterdam 17.3.2, 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).

Major Enhancements

The following features are included in the Cisco IOS-XE release 17.4.1:

Cyber Vision Support

Cisco Cyber Vision Center (CVC) gives more visibility into Industrial IoT networks across Industrial Control Systems (ICS) with real-time monitoring of control and data networks. On IoT IOS-XE platforms beginning with release 17.4, integration of CVC is supported by deploying IOX Cyber Vision sensor. With this sensor deployed on IoT Routers, the platform can forward the traffic from IOX applications to Cyber Vision Center for real-time monitoring and can forward any captured PCAP files to Vision center from IOX application.

This feature is covered in the ESR6300 Software Configuration Guide here:

https://www.cisco.com/c/en/us/td/docs/routers/embedded/6300/software/config/b_ESR6300_config/m-new-features-17-4-1.html#con_1166351

Release Notes for Cisco Cyber Vision Release 3.1.1:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco-Cyber-Vision_Release-Note-3-1-1.pdf

Cisco Edge Intelligence

Cisco Edge Intelligence allows for simplified data extraction from IoT sensors, transformation, governance and delivery to applications that need this data. The release for the IR1101 is version 1.0.6

Complete information is found at:

https://developer.cisco.com/edge-intelligence/

Native Docker Support

This feature enables users to deploy the docker applications on the ESR6300. The application life-cycle 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.

This feature is covered in the ESR6300 Software Configuration Guide here:

https://www.cisco.com/c/en/us/td/docs/routers/embedded/6300/software/config/b_ESR6300_config/m-new-features-17-4-1.html#con_1169769

Plug and Play (PnP) Support

The out of box configuration boots the platform up to the configuration wizard. The control stops at a prompt where the user is given an option to enter the startup configuration wizard or not. If the user does not have access to the router, or does not enter any options, PnP discovery kicks in. If the PnP agent successfully establishes a connection to the PnP Server, the device configurations are pushed from the Server. The platform gets configured according to the user preference.

If PnP is not setup for the Router, the WebUI is accessible without having to access the platform console.

Cisco DNA Center Support for Smart Licensing Using Policy

Cisco DNA Center supports Smart Licensing Using Policy functionality starting with Cisco DNA Center Release 2.2.2. The corresponding minimum required Cisco IOS XE Release for this platform is release 17.4.1.

Implement the “Connected to CSSM Through a Controller” topology to have Cisco DNA Center manage a product instance. When you do, the product instance records license usage, but it is the Cisco DNA Center that initiates communication with the product instance to retrieve and report usage to Cisco Smart Software Manager (CSSM), and returns the acknowledgment (RUM ACK).

In order to meet reporting requirements, Cisco DNA Center provides ad hoc or on-demand reporting, as well as scheduled reporting options.

Cisco DNA Center also provides workflows for the installation and removal of the Smart Licensing Authorization Code (SLAC) for a product instance, if applicable.

Note: On the Cisco DNA Center GUI, you can generate a SLAC only for HSECK9 licenses, and only for these product instances: Cisco Embedded Services 6300 Series Routers.

Related Documentation

The following documentation is available:

- All of the Cisco ESR6300 documentation can be found here:

https://www.cisco.com/c/en/us/support/routers/6300-series-embedded-service-routers/tsd-products-support-series-home.html

Caveats

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

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.

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

Open Caveats

None at this time.

Resolved Caveats

None at this time.

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.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

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.

© 2020–2022 Cisco Systems, Inc. All rights reserved.