Release Notes for Cisco Catalyst Micro Switch Series, Cisco IOS Release 15.2(7)Ex

First Published: 2021-02-23

Last Modified: 2024-03-29

Release Notes for Cisco Catalyst Micro Switch Series, Cisco IOS Release 15.2(7)Ex

Introduction

This release note describes the features, modifications, and caveats for the Cisco IOS Release 15.2(7)Ex software on the Cisco Catalyst Micro Switch Series.

Supported Hardware

Cisco Catalyst Micro Switch Series—Model Numbers

The following table lists the supported hardware models.

Switch Model	Description
Cisco Catalyst Switch Models and Description	
CMICR-4PS	Four 1 Gigabit Ethernet downlink PoE+ ports; two 1 Gigabit Ethernet SFP uplink ports; uses external AC/DC adapters for power sourcing.
CMICR-4PC	Four 1 Gigabit Ethernet downlink PoE+ ports; one 1 Gigabit Ethernet SFP and one 1-Gigabit Ethernet RJ-45 uplink ports; uses external AC/DC adapters for power sourcing.
CMICR-4PT	Four 1 Gigabit Ethernet downlink PoE+ ports; one 1 Gigabit Ethernet RJ-45 uplink port and one 1 Gigabit Ethernet RJ-45 or SFP combo uplink ports; two USB-C connectors for power sourcing; uses external AC/DC adapters or external PSE through PD ports for power sourcing.

Optics Modules

The Cisco Catalyst Micro Switch Series support a wide range of optics. Because the list of supported optics is updated on a regular basis, consult the tables at this URL for the latest SFP+ and SFP module compatibility information: https://tmgmatrix.cisco.com

Features of the Switch

Ease of Operation

This section lists the ease-of-operation features supported by Cisco Catalyst Micro Switch Series:

- Cisco Catalyst Smart Operations is a comprehensive set of features that simplify LAN deployment, configuration, and troubleshooting. Catalyst Smart Operations is a set of features that includes Auto Smartports, Smart Configuration, and Smart Troubleshooting to enhance operational excellence:
  - Auto Configuration determines the level of network access provided to an endpoint based on the type of the endpoint device.
  - Cisco Auto Smartports provide automatic configuration as devices connect to the switch port, allowing auto detection, and plug and play of the device onto the network.
  - Cisco Smart Troubleshooting is an extensive array of debug diagnostic commands and system health checks within the switch, including Generic Online Diagnostics (GOLD) and Onboard Failure Logging (OBFL).
  - Interface templates provide a mechanism to configure multiple commands at the same time and associate it with a target (such as an interface). An interface template is a container of configurations or policies that can be applied to specific ports.

Network Security

The Cisco Catalyst Micro Switch Series provide a range of security features to limit access to the network and mitigate threats.

- In Cisco IOS Release 15.2(7)E3 and later releases, SSH is enabled by default to connect to networks, and Telnet is disabled by default.
- 802.1x monitor mode: Enables authentication across the wired infrastructure in an audit mode without affecting wired users or devices. It helps IT administrators to smoothly manage 802.1x transitions by allowing access and logging system messages when a device requires reconfiguration or is missing an 802.1x supplicant.
- Bidirectional data support on the Switched Port Analyzer (SPAN) port: Allows Cisco intrusion detection.
- Bridge protocol data unit (BPDU) Guard: Shuts down Spanning Tree Port Fast-enabled interfaces when BPDUs are received to avoid accidental topology loops.
- Dynamic Address Resolution Protocol (ARP) Inspection (DAI): Prevents malicious attacks on the device by not relaying invalid ARP requests and responses to other ports in the same VLAN.
- Dynamic Host Control Protocol (DHCP) snooping: Filters untrusted DHCP messages between untrusted hosts and DHCP servers.

- Internet Group Management Protocol (IGMP) filtering: Provides multicast authentication by filtering out non-subscribers and limits the number of concurrent multicast streams available per port.
- MAC address notification: Notifies administrators about users added to or removed from the network.
- Multilevel security on console access: Prevents unauthorized users from altering the device configuration.
- Flexible authentication: Supports multiple authentication mechanisms including 802.1X and MAC Authentication Bypass.
- Open mode: Creates a user-friendly environment for 802.1X operations.
- Port security: Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding.
- Port-based ACLs for Layer 2 interfaces: Allow security policies to be applied on individual switch ports.
- RADIUS Change of Authorization (CoA): Enables asynchronous policy management.
- Secure Shell (SSH) Protocol and Simple Network Management Protocol Version 3 (SNMPv3): Provides network security by encrypting administrator traffic during Telnet and SNMP sessions. SSH Protocol, Kerberos, and the cryptographic version of SNMPv3 require a special cryptographic software image because of U.S. export restrictions.
- Standard and extended access control lists (ACLs): Define security policies on routed interfaces for control-plane and data-plane traffic. IPv6 ACLs can be applied to filter IPv6 traffic.
- TACACS+ and RADIUS authentication: Facilitates the centralized control of a device and restricts unauthorized users from altering the configuration.

Deployment and Control Features

This section lists the deployment and control features:

- Auto-negotiation on all ports automatically selects half- or full-duplex transmission mode to optimize bandwidth.
- Dynamic Host Configuration Protocol (DHCP) auto-configuration of multiple switches through a boot server eases switch deployment.
- Dynamic Trunking Protocol (DTP) facilitates dynamic trunk configuration across all switch ports.
- IEEE 802.1s/w Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) provide rapid spanning-tree convergence independent of spanning-tree timers and also offers the benefit of Layer 2 load balancing and distributed processing.
- Internet Group Management Protocol (IGMP) v1, v2, v3, snooping for IPv4. Multicast Listener Discovery (MLD) v1 and v2 Snooping provide fast client joins and leaves of multicast streams and limit bandwidth-intensive video traffic to only the requester.
- Layer 2 traceroute eases troubleshooting by identifying the physical path that a packet takes from source to destination.
- Link Aggregation Control Protocol (LACP) allows the creation of Ethernet channeling with devices that conform to IEEE 802.3ad.
- Network Timing Protocol (NTP) provides an accurate and consistent timestamp to all intranet switches.

- Port Aggregation Protocol (PAgP) automates the creation of Cisco Fast EtherChannel groups and Gigabit groups.
- TFTP reduces the cost of administering software upgrades by downloading from a centralized location.
- Switch-port auto-recovery (error-disable) automatically attempts to reactivate a link that is disabled because of a network error
- Storm control for unicast, broadcast and multicast traffic to prevent disruption in the network due to packet flooding on the LAN.
- Unidirectional Link Detection Protocol (UDLD) and Aggressive UDLD allow unidirectional links caused by incorrect wiring. Also, port faults can be detected and disabled on the interfaces.
- Voice VLAN simplifies telephony installations by keeping voice traffic on a separate VLAN for easier administration and troubleshooting.

Quality of Service

This section lists the quality of service (QoS) features:

- Multilayer Switching (MLS) QoS provides the ability to configure granular policies and classes on every interface. These policies include policers, markers, and classifiers.
- Supports up to 4 egress queues per port, and finer flow segregation using 2 threshold markers for non-strict-priority queues.
- Strict priority queuing to ensure that the highest-priority packets are serviced ahead of all other traffic.
- Weighted Round Robin (WRR) scheduling to ensure differential prioritization of packet flows.

Software Features in Cisco IOS Release 15.2(7)E3k

New Software Features

Feature Name	Description
SSH File Transfer Protocol (SFTP)	Allows any SFTP server user with the appropriate permission to copy files to and from the device. The SFTP client functionality is provided as part of the SSH component and is always enabled on the corresponding device.
Password Strength and Management for Common Criteria	Allows to configure password policies, security mechanisms for storing and retrieving, and rules to specify user passwords for local and remote users.

Software Features in Cisco IOS Release 15.2(7)E4

New Software Features

None.

Software Features in Cisco IOS Release 15.2(7)E5

New Software Features

None.

Software Features in Cisco IOS Release 15.2(7)E6

None.

Software Features in Cisco IOS Release 15.2(7)E7

Data Sanitization: Supports the use of the National Institute of Standards and Technology (NIST) purge method that renders data unrecoverable through simple, non-invasive data recovery techniques or through state-of-the-art laboratory techniques.

For more information, see the "Data Sanitization" chapter of the *System Management Configuration Guide*.

Software Features in Cisco IOS Release 15.2(7)E8

None.

Software Features in Cisco IOS Release 15.2(7)E9

None.

Software Features in Cisco IOS Release 15.2(7)E10

None.

Compatibility Matrix

The following table provides software compatibility information.

Catalyst Micro Switches	Cisco Identity Services Engine
Cisco IOS Release 15.2(7)E3k	2.7

Upgrading the Switch Software

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 number. The files necessary for web management are contained in a subdirectory. The image is stored on the system board flash device (flash:).

You can use the **show version** privileged EXEC command to see the software version that is running on your switch.

Note Although the show version output always shows the software image running on the switch, the model name shown at the end of this display is the factory configuration and does not change if you upgrade the software license.

You can also use the **dir** *filesystem:* privileged EXEC command to see the directory names of other software images that you might have stored in flash memory.

Software Image

If you have a service support contract and order a software license or if you order a switch, you receive the universal software image and a specific software license.

Table 1: Software Image for Cisco Catalyst Micro Switch

Image	Filename
Universal image	cmicr-universalk9-mz
Universal image	cmicr-universalk9-tar

Scaling Guidelines

For information about feature scaling guidelines, see the Cisco Catalyst Micro Switch Series datasheet at: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-micro-switches/nb-06-cat-micro-switch-series-ds-cte-en.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.

Cisco Bug Search Tool

The Cisco Bug Search Tool (BST) allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The BST is designed to improve the effectiveness in network risk management and device troubleshooting. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

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

Open Caveats in Cisco IOS Release 15.2(7)Ex

Open Caveats

None

Resolved Caveats in Cisco IOS Release 15.2(7)E4

Table 2: Resolved Caveats

Caveat ID Number	Description
CSCvv93417	Stack Member Switch fails wired dot1x; MasterSwitch passes dot1x using the same configs

Resolved Caveats in Cisco IOS Release 15.2(7)E5

Table 3: Resolved Caveats

Caveat ID Number	Description
CSCvx66699	Cisco IOS and IOS XE Software TrustSec CLI Parser Denial of Service Vulnerability.

Resolved Caveats in Cisco IOS Release 15.2(7)E6

None.

Resolved Caveats in Cisco IOS Release 15.2(7)E7

Table 4: Resolved Caveats

Caveat ID Number	Description
CSCvs25888	PNP always rollbacks configuration during DNAC onboarding provisioning.
CSCvw60355	DHCPv6: Memory allocation of DHCPv6 relay option results in crash.
CSCvx63027	Cisco IOS and IOS XE Software SSH Denial of Service Vulnerability.
CSCwa96810	Cisco IOS and IOS XE Software Common Industrial Protocol Request Denial of Service Vulnerability.

Resolved Caveats in Cisco IOS Release 15.2(7)E8

None.

Resolved Caveats in Cisco IOS Release 15.2(7)E9

None.

Resolved Caveats in Cisco IOS Release 15.2(7)E10

Table 5: Resolved Caveats

Bug ID	Headline
CSCwf54007	Cisco IOS and IOS XE Software IS-IS Denial of Service Vulnerability
CSCwh96519	For PoE used and remaining power on 3560, the SNMP walk result is sh data

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at this URL:

https://www.cisco.com/en/US/support/index.html

Go to **Product Support** and select your product from the list or enter the name of your product. Look under Troubleshoot and Alerts, to find information for the problem that you are experiencing.

Related Documentation

Cisco Validated Designs documents at this URL: https://www.cisco.com/go/designzone

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

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.

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 and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.