



Release Notes for Cisco NCS 560 Series Routers, Cisco IOS XR Release 26.2.1

Contents

Cisco NCS 560 Series Routers, Release 26.2.1	3
New software features.....	3
New hardware	4
Changes in behavior	4
Open issues.....	7
Known Issues.....	7
Compatibility.....	7
Supported software packages	8
Related resources.....	9
Legal information	10

Cisco NCS 560 Series Routers, Release 26.2.1

Cisco IOS XR Release 26.2.1 is a new feature release for Cisco NCS 560 Series routers.

For more details on the Cisco IOS XR release model and associated support, see [Software Lifecycle Support Statement - IOS XR](#).

New software features

Table 1. New software features for NCS 560 Series Routers, Release 26.2.1

Product impact	Feature	Description
Segment Routing		
Ease of Use	SRv6 traffic accounting	<p>You can now enable the router to record the number of packets and bytes transmitted on a specific egress interface for IPv6 traffic using the SRv6 locator counter. You can use this data to create deterministic data tools to anticipate and plan for future capacity planning solutions.</p> <p>The feature introduces these changes:</p> <p>*CLI:*</p> <ul style="list-style-type: none">* accounting prefixes ipv6 mode per-prefix per-nexthop srv6-locators <p>*YANG Data Models:*</p> <ul style="list-style-type: none">* Cisco-IOS-XR-accounting-cfg* Cisco-IOS-XR-fib-common-oper.yang <p>(see GitHub, YANG Data Models Navigator)</p>
Ease of Use	SRv6 policy counters (POL.CP.SL.INT.E)	<p>Network administrators can now monitor and manage network performance, capacity planning, and traffic engineering by reviewing the policy counters (POL.CP.SL.INT.E) in SRv6-TE. The feature is enabled by default.</p> <p>The feature introduces these changes:</p> <p>*YANG Data Models:*</p> <p>The Yang models allow operators to disable all the policy counters that are enabled by default.</p> <ul style="list-style-type: none">* Native model: Cisco-IOS-XR-accounting-cfg* UM model: Cisco-IOS-XR-um-cef-accounting-cfg <p>(see GitHub, YANG Data Models Navigator)</p>
Setup and Upgrade		
Upgrade	Deprecated insecure protocols in optional RPMs	<p>This feature improves platform security and reduces the threat surface of the Cisco Networking products by restricting insecure protocols such as Telnet, FTP, TFTP, and RCP (which were deprecated in Cisco IOS XR Release 25.4.1) from Cisco IOS XR base package.</p> <p>In this release, Telnet is added to the optional RPM, {{Telnet.rpm}}, and FTP, TFTP, and RCP are added to the optional RPM, {{IP-Insecure-Apps.rpm}}.</p> <p>We recommend you to migrate to secure alternatives such as SSH, SCP, SFTP as Telnet, FTP, TFTP, and RCP protocols will not be supported anymore starting from an upcoming Cisco IOS XR</p>

Product impact	Feature	Description
		release.
System Security		
Software Reliability	uRPF strict mode	<p>uRPF strict mode increases network security by blocking IP spoofing and dropping packets whose source IP does not match the expected return path interface. It checks that incoming traffic uses the same interface that the router would use to reach the source IP address. uRPF strict modes supports up to 16 Equal-Cost Multipath (ECMP) paths.</p> <p>This release extends uRPF strict mode to devices with external TCAM.</p>

New hardware

There is no new hardware introduced in this release.

Changes in behavior

This section provides a brief description of the behavior changes introduced in this release.

- Removal of Model-driven CLI Commands:

Starting from Cisco IOS-XR software release 26.2.1, the Model-driven CLI specifically the show YANG operational data commands have been removed.

- SNMP Traps Dropped in the Buffer Queue:

Starting with IOS-XR software release 24.1.2, SNMP traps will be dropped from the trap queue during the first five minutes after configuring a new NMS server or after a device reload.

- This issue is observed on all current releases of the Cisco IOS XR routers running IOS XR Release 24.1.2.
- The defect applies only to NMS servers that are located behind a firewall or within a security network where ICMP packets are blocked.

- Updated Command Syntax and Usage Guidelines

As an enhancement to the **show cef** commands, the **internal**, **brief**, and **hardware** keywords have been removed from these commands:

- show cef unresolved
- show cef ipv6 linklocal unresolved

The **internal** and **brief** keywords have been removed from these commands:

- show cef mpls unresolved
- show cef mpls local-label

Exceptions

This command retains support for the **internal** and **brief** keywords when a specific prefix is provided: **show cef unresolved <prefix>**

Usage Constraints for **show cef mpls**: When executing any command beginning with **show cef mpls**, you may use only one of these keywords at a time: **brief**, **detail**, or **internal**

Note: The exception mentioned above applies: if the command includes **unresolved** or **local-label**, the **internal** and **brief** keywords are explicitly blocked.

- Change in forwarding information base manager identifier reporting:

Previously, all forwarding information base manager (fib_mgr) instances across different locations—such as the Route Processor (RP) and Line Cards (LCs)—shared the same identifier, fib_mgr. Consequently, the show command output displayed only a single entry for application fib_mgr.

With this update, each fib_mgr instance is assigned a unique identifier corresponding to its specific location. As a result, the show route afi-all summary command now lists all instances individually. For example, the output will display fib_mgr for the RP and FIB node0_3_CPU0 for the LC located at node0_3_CPU0.

- Manual Remediation of Forward-Referenced SRLG Interfaces:

The existing Shared Risk Link Groups (SRLG) feature allows configuring SRLG values on interfaces that do not yet exist (forward-reference interfaces). These configurations appear in the output of the **show srlg** command. To avoid inconsistencies, manually remove all SRLG configurations related to non-existent or forward-referenced interfaces. This manual cleanup is essential to maintain system consistency and prevent misleading information in the SRLG display.

- Enhanced MPLS interface activation for IS-IS address-family lifecycle events:

Starting with Cisco IOS XR Release 26.2.1, IS-IS enables or disables MPLS on an interface when the first or last MPLS-enabled address family is created or deleted, instead of waiting for operational UP or DOWN state transitions. Previously, MPLS state changes occurred only during interface shutdown or link-down events. With this enhancement, MPLS state updates now also occur when the interface configuration is removed at the root level or when the last IPv4 or IPv6 address associated with an MPLS-enabled address family is removed from the interface.

- MPLS-TE tunnel event history for insufficient bandwidth events:

Starting with Cisco IOS XR Release 26.2.1, MPLS-TE tunnel events for insufficient bandwidth conditions are recorded in the tunnel event history. Previously, when a tunnel failed to reoptimize because the requested bandwidth was unavailable, the router generated syslog messages, but the event was not shown in the **show mpls traffic-eng event-history tunnels** output. This update adds a tunnel event for insufficient bandwidth so that you can review historical bandwidth-demand failures for debugging and capacity planning.

- Mandatory LDAP TLS Validation:

LDAP server certificate validation for TLS connections is now enabled by default. Unlike previous versions that skipped validation when no trustpoint was defined, the current implementation mandates the use of a configured ldaps trustpoint to establish a secure connection. If this trustpoint is absent, the connection is automatically rejected, ensuring that all LDAP traffic is strictly authenticated and verified.

These behaviors apply based on the configuration of the ldaps trustpoint:

- No trustpoint configured: The TLS connection to the LDAP server is rejected by the router.

- CA certificate only: The router uses the configured CA certificate to validate the LDAP server's certificate; the connection is established only upon successful validation.
- CA and client certificate configured: The router uses the CA certificate to validate the server's certificate while presenting the client certificate to satisfy mTLS requirements; the connection is established only if both validation checks pass.
- MACsec Licensing Tier Update:

Effective with Cisco IOS XR Software Release 26.2.1, MACsec on Cisco IOS XR routers utilizing the FCM 2.0 Access licensing model now requires the Advantage tier instead of the Premier tier. When MACsec is enabled on a physical interface, the interface bandwidth triggers Right-to-Use (RTU) consumption for the Access Advantage tier, calculated in 10G increments. This license consumption is reclaimed once the MACsec configuration is removed or the interface is shut down.
- Deprecated Security Algorithms:

Starting Cisco IOS XR Release 26.2.1, the 3DES-CBC cipher and Diffie-Hellman Group 1 SHA1 key exchange are insecure and deprecated. You will see syslog warning messages for deprecated commands.
- Change in show media CLI output:

The directory path previously shown as **/var/lib/docker** now appears as **apphost** in the **show media** CLI output. This change enhances clarity for users managing third-party applications and Docker containers. It also accurately reflects the directory's role within the Cisco IOS XR application hosting architecture.
- A deprecation notice is shown when you run the **show tech-support netconf** command.
- Starting Cisco IOS XR Release 26.2.1, you can set the **ipv6 nd ns-interval** value to less than 60 seconds on these virtual interfaces:
 - Bundle Ethernet interfaces
 - BVI interfaces
 - Pseudowire Ethernet interfaces
- NACM show command visibility improvements:

Starting from Release 26.2.1, you get better visibility of NACM rules and groups in **show nacm** command outputs when dynamic NACM is used. This enhancement improves how information is displayed without changing existing functionality, ensuring NACM rules continue to operate as before.
- Enhanced syslog reporting for discard-extra-paths limits:
- Starting in Release 26.2.1, syslog notifications for the **discard-extra-paths** limit have been enhanced to provide **per-neighbor** and **per-address-family** reporting. This replaces the previous global notification behavior, which applied a 5-minute rate limit across the entire BGP process. The updated notifications are rate-limited to 30 seconds and reset automatically if the neighbor session flaps.

Open issues

Table 2. Open issues for Cisco NCS 560 Series Routers, Release 26.2.1

Bug ID	Description
CSCwt81929	The process restart of ifmgr results in route flapping and traffic loss.
CSCwu13912	When file is opened by process: /usr/lib/systemd/systemd-journald OS-SYSLOG-3-LOG_ERR: error is observed after completing ISSU.
CSCwu32085	The CFMD process may restart intermittently.

Known Issues

There are no known issues in this release.

Compatibility

Compatibility Matrix for EPNM and Crosswork with Cisco IOS XR Software

The compatibility matrix lists the version of EPNM and Crosswork that are supported with Cisco IOS XR Release in this release.

Table 3. Compatibility matrix for Cisco NCS 560 Series Routers, Release 26.2.1

Cisco IOS XR	Crosswork	EPNM
Release 26.2.1	Crosswork Optimization Engine 6.0	Evolved Programmable Network Manager 8.1.1

System requirements

Use the **show hw-module fpd** command in EXEC and Admin mode to view the hardware components with their current FPD version and status. The status of the hardware must be CURRENT; Running and Programed version must be the same. You can also use the **show fpd package** command in Admin mode to check the fpd versions.

Software version

To verify the software version running on the router, use show version command in the EXEC mode.

```
Router# show version
Tue Jun  9 09:08:31.309 UTC
Cisco IOS XR Software, Version 26.2.1
Copyright (c) 2013-2026 by Cisco Systems, Inc.
```

Build Information:

```
Built By      : swtools
Built On     : Mon Jun  8 07:24:15 PDT 2026
Built Host   : iox-lnx-055
Workspace    : /auto/srcarchive13/prod/26.2.1/ncs560/ws
Version     : 26.2.1
```

```
Location      : /opt/cisco/XR/packages/
Label         : 26.2.1-iso
```

```
cisco NCS-560 () processor
System uptime is 1 hour 16 minutes
```

Supported software packages

This table lists the Cisco IOS XR Software feature set matrix (packages) with associated filenames.

Visit the [Cisco Software Download page](#) to download the Cisco IOS XR software images.

Feature Set	Filename	Description
Cisco IOS XR IP Unicast Routing Core Bundle	ncs560-mini-x-26.2.1.iso	Contains base image contents that includes: Host operating system System Admin boot image IOS XR boot image BGP packages OS Admin Base Forwarding Modular Services Card Routing SNMP Agent Alarm Correlation
Cisco IOS XR Manageability Package	ncs560-mgbl-1.0.0.0-r2621.x86_64.rpm	Telemetry, Extensible Markup Language (XML), Parser, and HTTP server packages, NETCONF, YANG Models, gRPC.
Cisco IOS XR OSPF package	ncs560-ospf-1.0.0.0-r2621.x86_64.rpm	Supports OSPF
Cisco IOS XR Security Package	ncs560-k9sec-1.0.0.0-r2621.x86_64.rpm	k9sec is needed for IPsec or MACsec and Dot1x and for basic crypto services such as Decryption, Secure Shell (SSH), Secure Socket Layer (SSL), and Public-key infrastructure (PKI).
Multicast Package	ncs560-mcast-1.0.0.0-r2621.x86_64.rpm	Supports Multicast Supports Automatic Multicast Tunneling (AMT), IGMP Multicast Listener Discovery (MLD), Multicast Label Distribution Protocol (MLDP), Multicast Source Discovery Protocol (MSDP) and PIM.
Cisco IOS XR ISIS package	ncs560-isis-1.0.0.0-r2621.x86_64.rpm	Supports Intermediate System to Intermediate System (IS-IS).
Cisco IOS XR USB Boot Package	ncs560-usb_boot-26.2.1.zip	Supports Cisco IOS XR USB Boot Package

Feature Set	Filename	Description
Cisco IOS XR MPLS Package	ncs560-mpls-1.0.0.0-r2621.x86_64.rpm ncs560-mpls-te-rsvp-1.0.0.0-r2621.x86_64.rpm	Supports MPLS and MPLS Traffic Engineering (MPLS-TE) RPM. Label Distribution Protocol (LDP), MPLS Forwarding, MPLS Operations, Administration, and Maintenance (OAM), Link Manager Protocol (LMP), Optical User Network Interface (OUNI) and Layer-3 VPN. Cisco IOS XR MPLS-TE and RSVP Package MPLS Traffic Engineering (MPLS-TE) and Resource Reservation Protocol (RSVP).
Cisco IOS XR LI Package	ncs560-li-1.0.0.0-r2621.x86_64.rpm	Lawful Intercept
Cisco IOS XR EIGRP Package	ncs560-eigrp-1.0.0.0-r2621.x86_64.rpm	(Optional) Includes EIGRP protocol support software

Related resources

Table 4. Related resources

Document	Description
Ask AI about this product	Provides access to Cisco product documentation for checking feature support details.
Cisco feature finder	An interactive tool that assists in locating features introduced across Cisco IOS XR releases and platforms.
Cisco IOS XR error messages	Search by release number, error strings, or compare release numbers to view a detailed repository of error messages and descriptions.
Cisco IOS XR MIBs	Select the MIB of your choice from a drop-down to explore an extensive repository of MIB information.
Cisco NCS 560 documentation	CCO Documentation for Cisco NCS 560 Series Routers
Feature deprecation and removal details	Outlines the features currently supported by each operating system.
Feature deprecation phasing out insecure capabilities	Provides a list of insecure features and protocols that are scheduled for systematic deprecation and eventual removal from specified Cisco products.
Feature removal and suggested alternatives	Details the reasons why certain features or protocols are deemed insecure and offers secure alternatives when available.
Smart licensing	Information about Smart Licensing Using Policy solutions and their deployment on IOS XR Routers.
Transceiver Module Group (TMG) compatibility matrix	Search by product family, product ID, data rate, reach, cable type, or form factor to determine the transceivers that Cisco hardware device supports.
YANG data models	A user-friendly reference designed to easily explore and understand the various data models supported in Cisco IOS XR platforms and releases.
Yang data models in Github	Repository containing the folders with yang data models introduced and enhanced in every

Document	Description
	IOS XR release.

Legal information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.

© 2026 Cisco Systems, Inc. All rights reserved.