Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 26.2.1

Contents

Cisco NCS 5500 Series Routers, IOS XR Release 26.2.1

Cisco IOS XR Release 26.2.1 is a new feature and hardware release for Cisco NCS 5500 Series routers. This release extends support for advanced 400G QSFP-DD optical modules, including Ultra Long-Haul (ULH) and Long Haul (LLH) variants, on modular chassis and line cards. L2VPN services gain Down MEP support in bridge domains, improving fault detection and failover for attachment circuits. The L3VPN feature overcomes recursion limits by enabling label swap over BGP labeled unicast and IGP, enhancing scalability for complex VPN traffic. MPLS-TE commands now support regular expressions for tunnel name filtering, boosting operational usability without impacting security. Security is strengthened by deprecating insecure protocols like Telnet, FTP, TFTP, and RCP in optional RPMs, encouraging migration to secure alternatives such as SSH and SFTP. Additionally, uRPF strict mode is extended to devices with external TCAM, increasing protection against IP spoofing. FIDO2 authentication for SSH enables secure, passwordless logins using hardware security keys, enhancing protection against phishing attacks. These updates collectively improve scalability, operational control, and security across the NCS 5500 fixed and modular platforms.

New software features

Table 1. New software features for Network Convergence System 5500 Series, Release 26.2.1

Product impact	Feature	Description
Interface and Hardware Component		
Hardware Reliability	Extended Support for DP04QSDD-ULH optical module	Introduced in this release on: NCS 5700 fixed port routers (select variants only*); NCS 5700 line cards [Mode: Native] (select variants only*) *This release extends support for the Cisco 400G QSFP-DD Ultra Long-Haul (ULH) coherent optical module, on the Cisco NCS 5500 series modular chassis using these line cards. • NC57-MOD-S via NC57-MPA-2D4H-S • NC-57-48Q2D-S/SE
Hardware Reliability	Support for DP04QSDD-LLH-A1 optical module	Introduced in this release on: NCS 5500 modular routers; NCS 5700 line cards [Mode: Native] (select variants only*) *This release extends support for the Cisco 400G Coherent QSFP-DD Ultra Long Haul reach L-band, on this line card: • NC57-24DD
Ease of Setup	DWDM-SFP10G-E-I tunable optics for NCS-55A1-24Q6H-SS and NCS-57C1-48Q6-SYS routers	Introduced in this release on: NCS 5500 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Native]) This feature enables full DWDM channel tuning

Product impact	Feature	Description
		capability for the DWDM-SFP10G-E-I optics on NCS-55A1-24Q6H-SS and NCS-57C1-48Q6-SYS routers, allowing operation up to 196.3 THz and ensuring proper integration with your optical transport infrastructure.
Software Reliability	L3-only hash algorithm	You can now ensure path consistency for fragmented packets and IPSec sessions. This feature prevents traffic from traversing different firewalls, allowing IPSec sessions to establish successfully. The L3-only hash algorithm bases load balancing decisions exclusively on source and destination IP addresses. It ignores Layer 4 headers and IPv6 flow labels during hash calculations. You configure this hardware module profile to restrict hashing parameters to Layer 3 information only. This feature is extended to: ○ NCS 5700 fixed port routers ○ NCS 5700 line cards
L2VPN		
Software Reliability	Down MEP support in bridge domains	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers Down MEP support in bridge domains gives you direct visibility and control over attachment circuit failures within L2VPN services. By enabling fault detection at the source and propagating failures across attachment circuits, it helps ensure faster failover, improved service reliability, and consistent end-to-end monitoring.
Software Reliability	VLAN switch mode	Introduced in this release on: NCS 5700 fixed port routers (select variants only*); NCS 5500 modular routers (NCS 5700 line cards [Mode: Native]) (select variants only*) You can increase scalability and efficiency by enabling a single trunk interface to carry traffic for multiple VLANs, which allows for flexible, isolated Layer 2 services and simplifies network operations. The router automatically creates bridge domains for each VLAN and switches traffic among defined trunk ports. Only one instance is supported per router, with configuration limited to matching VLAN, EVI, and BVI ranges using trunk interfaces. *This feature is supported on: • NC57-24DD • NC57-18DD-SE

Product impact	Feature	Description
		• NC57-36H-SE • NC57-36H6D-S • NC57-MOD-S • NCS-57C3-MOD-SYS • NCS-57C3-MODS-SYS • NCS-57B1-6D24-SYS • NCS-57B1-5DSE-SYS
L3VPN		
Software Reliability	L3VPN label swap over BGP labeled unicast and IGP	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers You can enhance your network scalability and operational efficiency by overcoming the recursion limit on your router. With large networks that cannot be managed by a single protocol or a single administrative domain, forwarding VPN traffic necessitates a three-layer label stack (VPN, Labeled Unicast, and IGP). The L3VPN label swap over BGP labeled unicast and IGP feature overcomes the recursion limit and manages VPN traffic that necessitates a three-layer label stack. The router's two-pass processing mechanism handles the three-layer label stack without manual intervention.
MPLS		
Software Reliability	Regular expressions in MPLS-TE tunnel names	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Native]). This feature enhances operational scalability and usability by allowing regex-based tunnel name filtering for MPLS-TE show and execution commands, without changing configuration models, architecture, or security posture. This feature supports regular expression in all MPLS-TE show and execution commands using tunnel names.
Setup and Upgrade		
Upgrade	Deprecated insecure protocols in optional RPMs	Introduced in this release on: NCS 5500 fixed port routers; NCS 5500 modular routers; NCS 5500 line cards. 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

Product impact	Feature	Description
		Release 25.4.1) from Cisco IOS XR base package. 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 }}. 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 release.
System Security		
Software Reliability	uRPF strict mode	Introduced in this release on: NCS 5500 fixed port routers; NCS 5500 modular routers 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. This release extends uRPF strict mode to devices with external TCAM.
Ease of Use	FIDO2 authentication for SSH	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Native] FIDO2 support for SSH enables secure and passwordless logins on Cisco IOS XR platforms. It uses hardware security keys to store private keys and requires physical user presence to authenticate sessions. This feature protects against phishing by verifying a signature from the security device during the login process.
Routing		
Software Reliability	VRF-specific BFD multipath location assignment	This feature allows you to pin BFD MP sessions to specific LCs by associating a destination IP and VRF with a physical location. When configured, the system automatically migrates matching sessions to the designated LC. This prevents collateral service disruption for unrelated tenants by ensuring that an LC reload only impacts sessions pinned to that specific hardware.

New hardware

Hardware	Description
Optics	This release introduces the following new optic on selective hardware within the product portfolio. For details, refer to the Transceiver Module Group (TMG) Compatibility Matrix. Cisco 25GBASE SFP28 Module • SFP-25G-ZR-I Cisco 400G QSFP-DD Ultra Long Haul Coherent Optics • DP04QSDD-LLH-A1

Changes in behavior

- 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.

- LOS Alarm Based on Total Power Support: Starting with IOS-XR software release 26.1.1, a new Loss of Signal (LOS) alarm based on total received power has been introduced.

  Alarm Behavior

  - The existing payload-based LOS alarm has been renamed to LOS-P to accurately reflect its function.
  - Automation scripts and operational procedures that previously relied on the old LOS alarm may misinterpret alarms if not updated.

- Carrier Delay Support for 100G LOL/LOS Switchover:

  When both carrier-delay down and the new serdes-holdoff-time are configured on 8k series router interfaces, the link remains in the "up" state during transient 50ms DWDM switchovers (LOS flaps). This behavior prevents unnecessary link flaps and improves network stability during optical layer protection switching.

  To enable this functionality, use the following interface configuration command:

serdes-holdoff-time msec

- FTP usage during installation triggers deprecated syslog warning

  If you use FTP either with a configured repository or a remote tarball, or ISO during installation, the syslog warning message appears that FTP is deprecated.

- Deprecation of RPM installation via remote repository configuration

  RPM Installation through remote repository configuration is deprecated when using CLI and YANG. We recommend that you perform the following workflows to install RPM:

  - Install a GISO (can be on a remote server) with all RPMs included
  - Install from a tarball (can be on a remote server) with all RPMs included
  - Copy desired RPMs onto the router and then configure a local repository.

- Fault Recovery Location-ID Usage

  Users can identify the location-ID for fault recovery by entering ? in the hw-module fault-recovery location command. For example, hw-module fault-recovery location ? displays the list of available locations. Also, from this release onward, the count range displayed for the count keyword in the hw-module fault-recovery location location-id count command is 1 to 3.

Open issues

Bug ID	Description
CSCwt81929	The process restart of ifmgr results in route flapping and traffic loss.
CSCwu32085	cfmd abnormal process restart

Known issues

- The Cisco NCS 5500 series modular routers with Cisco NCS 5700 line cards no longer support new features in compatibility mode. All Cisco IOS XR releases will continue to support features that were already enabled in compatibility mode until release 25.1.1. However, no new features will be added to compatibility mode. To take advantage of new features in current and subsequent releases, enable native mode by using the hw-module profile npu native-mode-enable command.

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 2. Compatibility Matrix for EPNM and Crosswork with Cisco IOS XR Software

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 02:03:33.349 PDT
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 07:38:57 PDT 2026
Built Host   : iox-lnx-050
Workspace    : /auto/srcarchive13/prod/26.2.1/ncs5500/ws
Version      : 26.2.1
Location     : /opt/cisco/XR/packages/
Label        : 26.2.1-iso

cisco NCS-5500 () processor
System uptime is 1 hour 10 minutes
```

Supported software packages

The following tables 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.

Table 3. Supported software for NCS 5500 Series Routers, Release 26.2.1

Feature Set	Filename	Description
Composite Package		
Cisco IOS XR IP Unicast Routing Core Bundle	ncs5500-mini-x.iso	Contains base image contents that includes: Host operating system System Admin boot image IOS XR boot image BGP packages
Individually-Installable Optional Packages		
Cisco IOS XR Manageability Package	ncs5500-mgbl-3.0.0.0-r2621.x86_64.rpm	Extensible Markup Language (XML) Parser, Telemetry, Netconf, gRPC and HTTP server packages.
Cisco IOS XR MPLS Package	ncs5500-mpls-2.1.0.0-r2621.x86_64.rpm ncs5500-mpls-te-rsvp-2.2.0.0-r2621.x86_64.rpm	MPLS and MPLS Traffic Engineering (MPLS-TE) RPM.

Feature Set	Filename	Description
Cisco IOS XR Security Package	ncs5500-k9sec-3.1.0.0-r2621.x86_64.rpm	Support for Encryption, Decryption, Secure Shell (SSH), Secure Socket Layer (SSL), and Public-key infrastructure (PKI)
Cisco IOS XR ISIS package	ncs5500-isis-1.2.0.0-r2621.x86_64.rpm	Support ISIS
Cisco IOS XR OSPF package	ncs5500-ospf-2.0.0.0-r2621.x86_64.rpm	Support OSPF
Lawful Intercept (LI) Package	ncs5500-li-1.0.0.0-r2621.x86_64.rpm	Includes LI software images
Multicast Package	ncs5500-mcast-1.0.0.0-r2621.x86_64rpm	Support Multicast
EIGRP	ncs5500-eigrp-1.0.0.0-r2621.x86_64.rpm	Supports Enhanced Interior Gateway Routing Protocol
Lawful Intercept Control	ncs5500-lictrl-1.0.0.0-r2621x86_64.rpm	Supports Lawful Intercept Control
Healthcheck	ncs5500-healthcheck-1.0.0.0-r2621.x86_64.rpm	Supports System Health Check

Table 4. TAR files for Cisco NCS 5500 Series Router, Release 26.2.1

Feature Set	Filename
NCS 5500 IOS XR Software 3DES	NCS5500-iosxr-k9-26.2.1.tar
NCS 5500 IOS XR Software	NCS5500-iosxr-26.2.1.tar
NCS 5500 IOS XR Software	NCS5500-docs-26.2.1.tar
NCS 5500 IOS XR Software 3DES	NCS5500-iosxr-k9-26.2.1.tar
NCS 5500 IOS XR Software	NCS5500-iosxr-26.2.1.tar

Table 5. Packages for Cisco NCS 5700 Series Router, Release 26.2.1

Feature Set	Filename
NCS 5700 IOS XR Software	ncs5700-x64-26.2.1.iso
NCS 5700 IOS XR Software (only k9 RPMs)	ncs5700-k9sec-rpms.26.2.1.tar
NCS 5700 IOS XR Software Optional Package	NCS5700-optional-rpms.26.2.1.tar This TAR file contains the following RPMS: optional-rpms/cdp/* optional-rpms/eigrp/* optional-rpms/telnet/*

Related resources

Table 6. Related resources

Resource	Description
Ask AI about this product	Provides access to Cisco product documentation for checking feature support details.
Cisco IOS XR MIBs	Allows selecting the MIB of your choice from a drop-down to explore an extensive repository of MIB information.
Cisco IOS XR Error messages	Allows searching by release number, error strings, or comparing release numbers to view a detailed repository of error messages and descriptions.
Cisco NCS 5500 documentation	Provides CDC documentation for Cisco NCS 5500 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.
Recommended release	Provides a general guide in case of upgrading IOS XR routers or new deployments that involve IOS XR routers.
Smart licensing	Provides information about Smart Licensing Using Policy solutions and their deployment on IOS XR routers.
Transceiver Module Group (TMG) compatibility matrix	Allows searching 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 in GitHub	Provides yang data models introduced and enhanced in every IOS XR release.

Legal information