Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 26.1.1

Contents

Cisco NCS 5500 Series Routers, IOS XR Release 26.1.1

Cisco IOS XR Release 26.1.1 is a new feature and hardware release for Cisco NCS 5500 Series routers. Key highlights include automated ISIS metric provisioning, DHCPv6 relay subscriber ID support, L3 EVPN IGMP and MLD state synchronization for improved multicast delivery, modular QoS scale enhancements, and configurable restore timers. The release also introduces MACSec support, TLS RFC 5289 compliance, centralized security template framework, enhanced programmability with gRPC RemoveContainer RPC, streamlined smart licensing, and robust timing with SyncE and PTP support

New software features

Table 1. New software features for Network Convergence System 5500 Series, Release 26.1.1

Product impact	Feature	Description
L2VPN		
Ease of setup	Flexible cross-connect service	Introduced in this release on: NCS 5700 fixed port routers; NCS 5700 line cards [Mode: Native] You can configure flexible cross-connect service with the inner VLAN tag set to any.
Multicast		
Software Reliability	MBB duplicate packet mitigation	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]) MLDP (Multicast Label Distribution Protocol) Make-Before-Break (MBB) duplicate packet mitigation is designed to minimize packet loss during the transition from an old Label Switched Path (LSP) to a new one. This process is particularly important in dynamic network environments where path changes can occur due to link-up or link-down events. This feature prevents duplicate packets during MLDP MBB events, especially during link-up and due to differential path latency.
Software Reliability	LSM egress statistics	Introduced in this release on: NCS 5700 fixed port routers; NCS 5700 line cards [Mode: Native]) You can now monitor egress multicast traffic accounting for mLDP labels on NCS 5700 routers and line cards. This feature provides visibility into Label Switched Multicast (LSM) forwarding for transit P-nodes and leaf nodes. The system allocates egress statistics resources from the stats infrastructure and associates them with mLDP labels. This functionality supports mLDP-based profiles running over segment routing cores, ensuring accurate traffic tracking per label switched path.
Programmability		
Software Reliability	Maintain reliable gRPC server operation on the router	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]) You can achieve reliable server operations, a consistent system state, and secure communication between gRPC clients and the router by ensuring that client access is delayed until the router is fully configured. This approach prevents inconsistent responses, errors, and incomplete enforcement of security policies.

		With this feature, the gRPC server on the router accepts client requests only after the startup configuration is fully applied. The External Management Service Daemon (EMSD) manages gRPC services, listens for connection requests on designated network ports, and ensures that the server initiates only after the router completes its configuration. This seamless coordination guarantees robust communication and operational consistency.
Segment Routing		
Software Reliability	BGP SID locator tracking for SRv6 services	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]) You can now improve SRv6 path selection by extending BGP next-hop tracking to monitor the reachability and metric of SRv6 SID locators. BGP tracks locators stored in the Routing Information Base (RIB) for both Layer 2 and Layer 3 services and updates path selection when a locator becomes unreachable, even if the next hop remains reachable.
Ease of Use	BFD CPU offload support for IPv6	Introduced in this release on: NCS 5500 fixed port routers You can now enable CPU offloading for IPv6 BFD sessions, allowing the CPU to handle packet transmission and reception directly. This functionality is now supported on all Cisco NCS 5500 router variants.
Ease of Use	SRv6-TE explicit BSID and remote steering	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]) You can now manually configure a deterministic and persistent binding SID, also known as an explicit BSID, for an SRv6-TE policy. The router also supports remote BSID steering, which allows it to recognize traffic whose destination address matches a local policy BSID and steer the traffic directly into the associated SRv6-TE policy. Previously, the router allocated SRv6-TE policy binding SIDs dynamically and could change the BSID during reloads or policy reinstallation. This behavior limited deterministic policy stitching and integration with external controllers. The feature introduces these changes: *CLI:* * show segment-routing traffic-eng database explicit-bsid srv6 summary detail * *clear segment-routing srv6 sid* _<address>_ * The *enforce* keyword is introduced as an explicit option in binding-sid command. * The following show commands are updated to display the requested BSID and binding SID behavior: show segment-routing traffic-eng policy show segment-routing srv6 static-endpoint

		YANG Data Models: * Cisco-IOS-XR-infra-xtc-agent-oper.yang * Cisco-IOS-XR-fib-common-oper.yang * Cisco-IOS-XR-segment-routing-srv6-cfg.yang see GitHub , YANG Data Models Navigator)
Setup and Upgrade		
Upgrade	Signature verification for owner RPMs using owner public keys	Introduced in this release on: NCS 5700 fixed port routers; NCS 5700 line cards [Mode: Native] This feature ensures integrity of owner RPMs and validates the authenticity of these RPMs by enabling the router to securely verify the owner RPM signatures using owner public keys onboarded on to the router. With this feature, you can now control whether or not to enable signature verification for owner RPMs based on defined security levels. When the signature verification for owner RPMs is enabled, all owner RPMs must be verified prior to IOS XR package installation.
Software Reliability	Security profiles for Cisco IOS XR software	Introduced in this release on: NCS 5700 fixed port routers; NCS 5700 line cards [Mode: Native] This feature supports different security profiles to ensure integrity and protection of the IOS XR system when transitioning between security profiles. The supported security profiles are Strict, Default, Relaxed, and Custom.
Software Reliability	Customer consent token configuration	Introduced in this release on: NCS 5700 fixed port routers; NCS 5700 line cards [Mode: Native] This feature allows you to enable the customer consent token workflow so that the key name is linked to the key package.
Software Reliability	Key package enhancements	Introduced in this release on: NCS 5700 fixed port routers; NCS 5700 line cards [Mode: Native] This feature introduces you to the version 3 key package. With the version 3 key package, you can create, validate, sign a key package before the key package is provisioned on the router. Unlike the reserved customer consent token name, CUS-CT, used in version 1 and version 2 key packages, you can now use any name for the customer consent token that you include in the key package.
System Security		
Software Reliability	SSH key strength: 3072 bits by default	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 update enhances device security by automatically generating RSA 3072-bit SSH host keys during system boot, replacing the previous default of RSA 2048-bit keys. The stronger key size

		aligns with industry best practices and provides improved cryptographic protection, ensuring secure SSH access and compliance with future security requirements.
Software Reliability	Syslog warnings for RSA keys and DSA keys	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 enhancement ensures Cisco IOS XR devices comply with evolving security standards by sending syslog warnings if weak SSH host keys are found during system reboot where an Rivest, Shamir, and Adelman (RSA) key less than 3072 bits or any Digital Signature Algorithm (DSA) keys are detected. The default RSA key size has been increased from 2048 to 3072 bits to strengthen security. Additionally, DSA keys are no longer auto-generated at boot, and if found, a syslog warning prompts their removal to align with current best practices.
Software Reliability	Syslog alerts on public keys generated in XR config mode	Introduced in this release: 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 enhancement ensures Cisco IOS XR devices comply with evolving security standards by sending syslog warnings if weak SSH host keys are found during system reboot where an Rivest, Shamir, and Adelman (RSA) key less than 3072 bits or any Digital Signature Algorithm (DSA) keys are detected. The default RSA key size has been increased from 2048 to 3072 bits to strengthen security. Additionally, DSA keys are no longer auto-generated at boot, and if found, a syslog warning prompts their removal to align with current best practices.

New hardware

There are no new hardware introduced in this release.

Changes in behavior

- The default minimum syslog TLS version is now TLS 1.2 to enhance security. A one-time syslog warning will be generated if TLS 1.0 or TLS 1.1 is used, and a continuous warning will occur if the syslog minimum TLS version is configured as TLS 1.0 or 1.1.
- Starting with the Cisco IOS XR Software Release 26.1.1, if the route-policy applied to the eBGP neighbor includes the set next-hop unchanged command, the system preserves and advertises both the received remote SRv6 SID and the remote next-hop when advertising the leaked route from GRT to the VRF table. The local SRv6 SID is no longer always sent.
- DCO Optics FPD Upgrades: The firmware upgrade process for Digital Coherent Optics has been optimized to eliminate redundant upgrades and system reloads. Previously, inconsistent firmware version reporting between the optics driver and FPD infrastructure resulted in an " RLOAD REQ" status, requiring a second upgrade and a chassis reload.
  Efficiency: Now you can perform a single upgrade cycle to achieve a CURRENT status.
  Impact: Eliminates the requirement for a costly box reload following DCO firmware upgrades.

Open issues

There are no open issues in this release.

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.
- During a software upgrade to IOS XR Release 26.1.1, the system may not complete the Auto-FPD upgrade as expected. After the upgrade, the FPD status shows 'RLOAD REQ', indicating that you must perform an additional reload to activate the updated FPD.

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 26.1.1	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
Fri Feb 27 00:52:46.157 PST
Cisco IOS XR Software, Version 26.1.1
Copyright (c) 2013-2026 by Cisco Systems, Inc.

Build Information:
 Built By     : swtools
 Built On     : Wed Feb 25 22:00:10 PST 2026
 Built Host   : iox-lnx-117
 Workspace    : /auto/srcarchive12/prod/26.1.1/ncs5500/ws
 Version      : 26.1.1
 Location     : /opt/cisco/XR/packages/
```

```
 Label         : 26.1.1

cisco NCS-5500 () processor
System uptime is 37 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 26.1.1

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-r2611.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-r2611.x86_64.rpm ncs5500-mpls-te-rsvp-2.2.0.0-r2611.x86_64.rpm	MPLS and MPLS Traffic Engineering (MPLS-TE) RPM.
Cisco IOS XR Security Package	ncs5500-k9sec-3.1.0.0-r2611.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-r2611.x86_64.rpm	Support ISIS
Cisco IOS XR OSPF package	ncs5500-ospf-2.0.0.0-r2611.x86_64.rpm	Support OSPF
Lawful Intercept (LI) Package	ncs5500-li-1.0.0.0-r2611.x86_64.rpm	Includes LI software images
Multicast Package	ncs5500-mcast-1.0.0.0-r2611.x86_64rpm	Support Multicast
EIGRP	ncs5500-eigrp-1.0.0.0-r2611.x86_64.rpm	Supports Enhanced Interior Gateway Routing Protocol
Lawful Intercept Control	ncs5500-lictrl-1.0.0.0-r2611x86_64.rpm	Supports Lawful Intercept Control

Feature Set	Filename	Description
Healthcheck	ncs5500-healthcheck-1.0.0.0-r2611.x86_64.rpm	Supports System Health Check

Table 4. TAR files for Cisco NCS 5500 Series Router, Release 26.1.1

Feature Set	Filename
NCS 5500 IOS XR Software 3DES	NCS5500-iosxr-k9-26.1.1.tar
NCS 5500 IOS XR Software	NCS5500-iosxr-26.1.1.tar
NCS 5500 IOS XR Software	NCS5500-docs-26.1.1.tar
NCS 5500 IOS XR Software 3DES	NCS5500-iosxr-k9-26.1.1.tar
NCS 5500 IOS XR Software	NCS5500-iosxr-26.1.1.tar

Table 5. Packages for Cisco NCS 5700 Series Router, Release 26.1.1

Feature Set	Filename
NCS 5700 IOS XR Software	ncs5700-x64-26.1.1.iso
NCS 5700 IOS XR Software (only k9 RPMs)	ncs5700-k9sec-rpms.26.1.1.tar
NCS 5700 IOS XR Software Optional Package	NCS5700-optional-rpms.26.1.1.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
Cisco feature finder	Assists in locating features introduced across Cisco IOS XR releases and platforms.
Smart licensing	Provides information about Smart Licensing Using Policy solutions and their deployment on IOS XR routers.
Cisco NCS 5500 documentation	Provides CDC documentation for Cisco NCS 5500 series 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.
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.

Resource	Description
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.
Cisco IOS XR MIBs	Allows selecting the MIB of your choice from a drop-down to explore an extensive repository of MIB information.
Yang data models in GitHub	Provides yang data models introduced and enhanced in every IOS XR release.
Recommended release	Provides a general guide in case of upgrading IOS XR routers or new deployments that involve IOS XR routers.

Legal information