



Release Notes for Cisco NCS 540 Series Routers, Cisco IOS XR Release 26.3.1

Contents

Cisco NCS 540 Series Routers, Release 26.3.1 3

New software features..... 3

New hardware 4

Changes in behavior 5

Open issues..... 8

Known issues..... 8

Compatibility..... 8

Supported software packages 9

Related resources..... 12

Legal information 13

Cisco NCS 540 Series Routers, Release 26.3.1

Cisco IOS XR Release 26.3.1 is a new feature release for Cisco NCS 540 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

This section provides a brief description of the new software features introduced in this release.

Table 1. New software features for Cisco NCS 540 Series Routers, Release 26.3.1

Product impact	Feature	Description
BGP		
Software Reliability	eBGP RT-constraint multipath	This feature enables more complete and resilient VPN route propagation in environments with redundant external peers, while preserving existing best-path behavior and operational consistency by extending RTC (route target constraint) processing on ASBRs (autonomous systems border routers). This is achieved by installing RT membership state on all qualified eBGP multipath neighbors instead of only the best-path neighbor.
Software Reliability	BGP RT-constraint default prefix suppression	This feature allows you to suppress automatic generation of the default RT membership prefix, preventing unnecessary route propagation. This feature adds operator control to suppress automatic generation of the default RT-constraint membership prefix {{0:0x0000:0:0/0}} when a peer does not negotiate RT-constraint capability.
Interface and Hardware Component		
Software Reliability	Admin sleep mode for optical transceivers	This feature provides a controlled way to reduce transceiver power consumption while keeping the optics accessible by adding an admin sleep mode or low power mode for optical transceivers on NCS 5500 routers. When a user applies shutdown under controller optics, the router places the corresponding optical module into a low power state.
Routing		
Software reliability	Inter-area route propagation limits in IS-IS	This feature helps protect the network from excessive inter-area route propagation caused by misconfiguration or unexpected route growth by limiting the number of prefixes propagated between IS-IS levels. This feature, using the new maximum-propagated-prefixes command, allows operators to define propagation thresholds, receive early warnings, and optionally stop advertising additional prefixes when limits are exceeded.
Setup and Upgrade		
Upgrade	XR version formats for service packs and special releases	This enhancement introduces support for new XR release version formats for service pack (SP) and special release (SR) in the install infrastructure so that XR software can correctly recognize, compare, display, and validate SP and SR versions.
System Management		

Product impact	Feature	Description
Ease of Use	Configure device data privacy for Smart Licensing	Provides controls to suppress the device hostname and smart agent version in smart licensing usage reports.
Upgrade	Configure SNMP secure-v3	You enhance SNMP security by configuring only SNMPv3 with SHA-2 authentication and AES-based privacy using the secure-v3 CLI. Insecure SNMP versions and options are blocked, and attempts to use legacy or mixed configurations are automatically rejected with syslog warnings.
System Monitoring		
Software Reliability	Persistent logging	This feature preserves the contents of the IOS XR logging buffer across node reloads, router reloads, and RP failovers. Syslog messages are written to both the in-memory logging buffer and a persistent file on local storage. After a reload or failover, the system restores the logging buffer from persistent storage so that retained log messages before the event and current logs, are displayed.
System Security		
Software Reliability	IPSec for management traffic	IPSec for management traffic protects eligible management traffic generated by or destined for the router. The feature uses IKEv2, IPSec, Tunnel MA, and associated virtual tunnel interfaces.
Software Reliability	Gated shell access	Gated shell access requires consent token authorization for direct root shell access initiated through supported shell commands. You gain secure, auditable control over root shell access by requiring cryptographic Consent Token authorization before granting access. This feature persists your security settings across reloads and high-availability events, helping prevent unauthorized or accidental changes while retaining familiar shell workflows after authorization.
Software Reliability	SSH client strict host key check	You enhance SSH security by enforcing strict host key checking, allowing you to control how the SSH client handles new or changed server keys - accept, reject, or prompt for approval. Trusted host keys are stored system-wide and persist across reloads, ensuring consistent validation for your outbound SSH connections.
Timing and Synchronization		
Software reliability	PTP frequency-assisted holdover	The frequency-assisted holdover feature enhances network stability by allowing for an extended holdover duration within the network-limits specification, when a Primary Reference Clock (PRC) frequency source remains available. This ensures that even if the GNSS or PTP time source is lost, the system can advertise timing stability for a longer, user-defined period without significant degradation. CLI: holdover-spec-frequency-assisted-duration

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.

- Deprecation of PCE NETCONF CLI

Starting with Cisco IOS XR Release 26.3.1, the PCE NETCONF CLI configuration is deprecated. Previously, you could configure NETCONF attributes directly for the Path Computation Element by using the `pce netconf` CLI commands. Because there is no actual operational use case for this configuration, it has been removed entirely. You do not need to perform any configuration migration or apply replacement commands, as there is no impact from this deprecation.

- Service layer API route redistribution

Starting with Cisco IOS XR Release 26.3.1, Service Layer API routes use a separate routing protocol type. To redistribute these routes into BGP, replace `redistribute application service-layer` with `redistribute service-layer` in existing BGP address-family configurations.

The `service-layer` keyword redistributes routes programmed through the Service Layer API into BGP. The `application` keyword continues to select application routes.

- gRIBI Route Redistribution

Starting with Cisco IOS XR Release 26.3.1, gRPC RIB Interface (gRIBI) routes use a separate routing protocol type. To redistribute these routes into BGP, replace `redistribute application gribi` with `redistribute gribi` in existing BGP address-family configurations.

The **gribi** keyword redistributes routes programmed through gRIBI into BGP. The `application` keyword continues to select application routes.

- Logging Bootz, Authz, and Pathz policy updates

Changes to certificates or other credentials related to Bootz, Authz, and gNSI (Pathz) are explicitly logged through IOS messages.

Example logs:

#Bootconfig through boot up flow

```
RP/0/RP0/CPU0:Feb 4 01:30:02.403 UTC: emsd[1122]: %MGBL-EMS-6-EMSD_POLICY_UPDATE :  
Bootz policy committed. source: bootconfig
```

#Bootconfig through SetBootConfig RPC

```
RP/0/RP0/CPU0:Feb 5 08:10:41.711 UTC: emsd[1122]: %MGBL-EMS-6-EMSD_POLICY_UPDATE :  
Bootz policy committed. source: bootconfig
```

#Authz and Pathz through rotate CLI

```
RP/0/RP0/CPU0:Feb 4 00:44:57.349 UTC: emsd[1122]: %MGBL-EMS-6-EMSD_POLICY_UPDATE :  
Authz policy committed. source: CLI
```

```
RP/0/RP0/CPU0:Feb 4 00:45:23.470 UTC: emsd[1122]: %MGBL-EMS-6-EMSD_POLICY_UPDATE :  
PathZ policy committed. source: CLI
```

#Authz and Pathz through Rotate RPC

```
RP/0/RP0/CPU0:Feb 4 21:05:06.591 UTC: emsd[1122]: %MGBL-EMS-6-EMSD_POLICY_UPDATE :  
Authz policy committed. source: Rotate
```

- Boolean values in gNMI path keys

Starting with Cisco IOS XR Release 26.3.1, Boolean list keys in gNMI Subscribe responses that use proto or JSON_IETF encoding are represented by the canonical strings **true** and **false** instead of **1** and **0**. If your collector explicitly expects or compares the earlier numeric strings, update its parsing logic. You do not need to make any router configuration changes.

- Enable automatic Docker Daemon startup with Application Manager

The **appmgr docker start** command enables the Docker daemon to start automatically when Application Manager starts.

```
Router(config)# appmgr docker start
Router(config)# commit
```

- Increased CPU and memory limits for TPAs

Starting with Cisco IOS XR Release 26.3.1, the maximum configurable hard resource limits for Third-Party Applications (TPAs) are increased to 100 percent of total system CPU and 80 percent of overall system memory. These limits prevent TPAs from exceeding the CPU and memory thresholds, regardless of resource usage by other IOS XR processes.

- VRF Naming Restriction

Starting with Cisco IOS-XR Release 26.3.1, the uppercase name "DEFAULT" is reserved for the OpenConfig default network instance. You must choose a different name for any user-defined VRF. This restriction applies to global VRF configuration, interface VRF assignments, and dynamic-template VRF configurations across both CLI and YANG management interfaces. Before upgrading, you must rename or remove any user-defined VRF named "DEFAULT" to prevent startup configuration validation failures. Note that VRF names are case-sensitive; variations such as "Default" or "DEFAULT1" remain valid, and the system default VRF is not affected.

- Standards-compliant OpenConfig BGP identity values

Starting with Cisco IOS XR Release 26.3.1, selected OpenConfig BGP operational values use the module-qualified identity format, such as `openconfig-bgp-types:<identity>`, instead of `<identity>`. This format clearly identifies the YANG module defining each identity. These values include notification error codes and subcodes, remove-private-AS state, and supported capabilities. Clients and automation should process the module-qualified format.

- Default values restored after delete operations

Starting with Cisco IOS XR Release 26.3.1, deleting a leaf in a native YANG configuration container restores its defined default value, ensuring consistent configuration data in `show running-config` and `NETCONF get-config` output.

- Deprecation of the show install packages command family

Starting with Cisco IOS XR Release 26.3.1, the "show install packages..." family of commands such as the commands to show install packages information, `show install packages search`, and `show install packages` are marked as deprecated. For package names and repository information for uninstalled packages, use the **show install active**, **show install committed**, and **show install available** commands.

- Recommended workflows for removing or deactivating bug fixes

The show install fixes deactivate command is no longer the recommended workflow for removing or deactivating a bug fix. Select one of the following workflows based on the software images and rollback points available in your environment:

- Use install rollback when a previous rollback point exists where the same Cisco IOS XR version was loaded without the bug fix.
 - Use show install rollback ? to identify a suitable rollback point.
 - Use install replace when a suitable previous golden ISO image is available without the bug fix.
 - If no previous rollback point or suitable golden ISO image exists, build a new golden ISO image with the desired set of fixes.
 - If the golden ISO build fails or still includes the unwanted bug fix, the desired set of fixes cannot be built with the available fixes. Contact Cisco Support for a new version of the unwanted fix.
- Application manager is supported on the following NCS 540 routers, you can deploy the owner or partner TPA RPMs using the standard XR install CLI:
 - N540X-4Z14G2Q-A
 - N540X-6Z18G-SYS-A
 - N540X-8Z16G-SYS-A
 - N540-6Z14G-SYS-D
 - N540-8Z12G-SYS-D
 - From Release 26.3.1, Cisco IOS XR software deprecates additional insecure TLS and SSH capabilities. Cisco recommends moving to the secure alternatives listed below to maintain stronger security posture and compliance.

If you are using the following insecure features...	Then follow these secure alternatives...
TLS 1.0 TLS 1.1	Use TLS 1.2 or TLS 1.3.
SSH key-exchange algorithm diffie-hellman-group1-sha1	Use stronger SSH key-exchange algorithms. Do not configure diffie-hellman-group1-sha1 .
SSH ciphers 3des-cbc	Use stronger SSH ciphers.
SSH host-key DSA algorithm	Use ECDSA, ED25519, or RSA host keys. Note: The SSH host-key DSA algorithm is not recommended. However, it has not been removed. If required, you can still generate and use DSA host keys. Cisco recommends using ECDSA, ED25519, or RSA host keys.
SSHv1	Use SSHv2.

Open issues

There are no open issues in this release.

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 software in this release.

Table 2. Compatibility Matrix for Cisco NCS 540 Series Routers, Release 26.3.1

Cisco IOS XR	Crosswork	EPNM
Release 26.3.1	Cisco Crosswork Network Controller 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 Programmed 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 Sep 11 08:48:50.056 IST
Cisco IOS XR Software, Version 26.3.1
Copyright (c) 2013-2026 by Cisco Systems, Inc.
```

```
Build Information:
Built By      : swtools
Built On     : Thu Sep 10 03:55:58 PDT 2026
Built Host   : iox-lnx-046
Workspace    : /auto/srcarchive13/prod/26.3.1/ncs540/ws
Version      : 26.3.1
Location     : /opt/cisco/XR/packages/
Label       : 26.3.1-iso
```

```
cisco NCS-540 () processor
System uptime is 29 minutes
```

Supported software packages

The following tables list the supported base images and optional packages and their corresponding file names.

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

Table 3. Release 26.3.1 software for N540-24Z8Q2C-SYS, N540-ACC-SYS, and N540X-ACC-SYS

Package	Filename	Description
Base image		
IOS XR Base Image	ncs540-mini-x-26.3.1.iso	IOS XR mandatory base image.
USB Boot Package	ncs540-usb_boot-26.3.1.zip	Package required to perform USB Boot. Includes the same packages as the base image.
Optional packages not included in the base image		
IOS XR Manageability	ncs540-mgbl-1.0.0.0-r2631.x86_64.rpm	Supports Extensible Markup Language (XML) Parser, Telemetry, Netconf, gRPC and HTTP server
IOS XR MPLS	ncs540-mpls-1.0.0.0-r2631.x86_64.rpm ncs540-mpls-te-rsvp-1.0.0.0-r2631.x86_64.rpm	Supports MPLS and MPLS Traffic Engineering (MPLS-TE)
IOS XR Security	ncs540-k9sec-1.0.0.0-r2631.x86_64.rpm	Supports MACsec and 802.1X
IOS XR ISIS	ncs540-isis-1.0.0.0-r2631.x86_64.rpm	Supports ISIS
IOS XR OSPF	ncs540-ospf-1.0.0.0-r2631.x86_64.rpm	Supports OSPF
IOS XR Lawful Intercept	ncs540-li-1.0.0.0-r2631.x86_64.rpm	Supports Lawful Intercept (LI)
IOS XR Multicast	ncs540-mcast-1.0.0.0-r2631.x86_64.rpm	Supports Multicast
IOS XR EIGRP	ncs540-eigrp-1.0.0.0-r2631.x86_64.rpm	Supports EIGRP
IOS XR LI-CTRL	ncs540-lictrl-1.0.0.0-r2631.x86_64.rpm	Supports LI-CTRL

Table 4. Release 26.3.1 Software for N540-24Q8L2DD-SYS, N540-24Q2C2DD-SYS, N540X-16Z4G8Q2C-A/D, N540-28Z4C-SYS-A/D, N540X-12Z16G-SYS-A/D, N540-12Z20G-SYS-A/D, N540-FH-CSR-SYS, N540X-16Z8Q2C-D, and N540-FH-AGG-SYS

Package	Filename	Description
Base Image		

Package	Filename	Description
IOS XR Base Image	ncs540l-x64-26.3.1.iso	IOS XR base image with mandatory packages. The base ISO image also includes the following optional packages: - xr-bgp - xr-cdp - xr-eigrp - xr-ipsla - xr-is-is - xr-k9sec - xr-lictrl - xr-ldp - xr-mcast - xr-mpls-oam - xr-netflow - xr-ospf - xr-perf-meas - xr-perfmgmt - xr-rip - xr-telnet - xr-track These optional packages are also included in NCS540l-iosxr-26.3.1.tar.
USB Boot Package	ncs540l-usb_boot-26.3.1.zip	Package required to perform USB Boot. Includes the same packages as the base image.
Optional packages not included in the base image		
IOS XR Telnet (xr-telnet)	NCS540l-iosxr-26.3.1.tar	Supports Telnet
IOS XR EIGRP (xr-eigrp)	NCS540l-iosxr-26.3.1.tar	Supports EIGRP
IOS XR CDP (xr-cdp)	NCS540l-iosxr-26.3.1.tar	Supports CDP
IOS XR k9sec (xr-k9sec)	NCS540l-k9sec-rpms.26.3.1.tar	Supports 802.1X
IOS XR RIP (xr-rip)	NCS540l-iosxr-26.3.1.tar	Supports RIP

Table 5. Release 26.3.1 Software for N540X-4Z14G2Q-A/D, N540X-8Z16G-SYS-A/D, N540-6Z14S-SYS-D, N540-6Z18G-SYS-A/D, N540X-6Z18G-SYS-A/D, and N540X-6Z6G-SYS

Package	Filename	Description
Base image		
IOS XR Base Image	ncs540l-aarch64-26.3.1.iso	IOS XR base image with mandatory packages. The ISO image also includes the following optional packages: - xr-bgp - xr-cdp - xr-eigrp - xr-ipsla - xr-is-is - xr-k9sec - xr-lictrl - xr-lldp - xr-mcast - xr-mpls-oam - xr-ncs540l-mcast - xr-ncs540l-netflow - xr-netflow - xr-ospf - xr-perf-meas - xr-perfmgmt - xr-rip - xr-telnet - xr-track These optional packages are also included in NCS540l aarch64 iosxr optional rpms-26.3.1.tar.
USB Boot Package	ncs540l-aarch64-usb_boot-26.3.1.zip	Package required to perform USB Boot. Includes the same packages as the base image.
Optional packages not included in the base image		
Package	Filename	Description
IOS XR Telnet (xr-telnet)	NCS540l-aarch64-iosxr-optional-rpms-26.3.1.tar	Supports Telnet
IOS XR EIGRP (xr-eigrp)	NCS540l-aarch64-iosxr-optional-rpms-26.3.1.tar	Supports EIGRP

Package	Filename	Description
IOS XR CDP (xr-cdp)	NCS540I-aarch64-iosxr-optional-rpms-26.3.1.tar	Supports CDP
IOS XR k9sec (xr-k9sec)	NCS540I-aarch64-k9sec-rpms.26.3.1.tar	Supports 802.1X
IOS XR RIP (xr-rip)	NCS540I-aarch64-iosxr-optional-rpms-26.3.1.tar	Supports RIP

Related resources

Table 6. 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 540 documentation	CCO Documentation for Cisco NCS 540 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 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.