



Release Notes for Cisco IOS XRd, IOS XR Release 26.2.1

Contents

Cisco IOS XRd, IOS XR Release 26.2.1	3
New software features	3
Changes in behavior	3
Open issues.....	5
Known issues.....	6
Compatibility.....	6
Related resource	6
Legal information	8

Cisco IOS XRd, IOS XR Release 26.2.1

There are no new software features or hardware introduced in this release.

New software features

There are no new software features 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.

- **Enhancing BGP Routing Security:**

You improve BGP routing security by enabling RPKI origin validation for both outbound advertisements and iBGP peer routes. This feature ensures only prefixes with valid or not-found ROA status are sent, while invalid prefixes are filtered, maintaining consistent and compliant routing across your network.

- **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.

Open issues

There are no open issues in this release.

Known issues

There are no known issues in this release.

Compatibility

Supported deployments

This section details the supported XRd deployments in this release.

Table 1. Supported deployments for Cisco IOS XRd, Release 26.2.1

Deployment	Reference
Amazon Elastic Kubernetes Service (AWS EKS)	XRd vRouter or XRd Control Plane on AWS EKS
XRd lab deployments	XR docs virtual routing

Related resource

Table 2. Related resource

Resource	Description
Smart licensing	Provides information about Smart Licensing Using Policy solutions and their deployment on IOS XR routers.
Cisco XRd documentation	Provides CDC documentation for Cisco XRd.
XRd tools	Provides utilities to: <ul style="list-style-type: none">- Apply bugfixes to XRd images- Verify the host is setup correctly to run XRd- Assist in launching XRd instances in a lab environment
XR docs virtual routing	Provides instructions for deploying XRd in lab settings, along with information on other deployment environments that are not yet officially supported.
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 IOS XR MIBs	Allows selecting the MIB of your choice from a drop-down to explore an extensive repository of MIB information.
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.
Yang data models in GitHub	Provides yang data models introduced and enhanced in every IOS XR release.



Resource	Description
Recommended release	Provides a general guide in case of upgrading IOS XR routers or new deployments that involve IOS XR routers.

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.