Release Notes for Cisco 8000 Series Routers, IOS XR Release 26.1.1

© 2026 Cisco and/or its affiliates. All rights reserved.

Contents

Cisco 8000 Series Routers, IOS XR Release 26.1.1 3
New software features 3
New hardware 3
Changes in behavior 10
Open issues 11
Known issues 11
Compatibility 11
Supported hardware 13
Supported software packages 17
Related resources 18
Legal information 19

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco 8000 Series Routers, IOS XR Release 26.1.1

Cisco IOS XR Release 26.1.1 introduces new software reliability, operational visibility, and service validation enhancements for Cisco 8000 Series Routers. Key updates include controller-programmed BGP best-path selection, enabling deterministic steering of overlay traffic across optimal underlay paths on fixed, modular, and system platforms. EVPN enhancements extend hardware offload support for Connectivity Check Message (CCM) timers up to 1 second, improving scale and reducing CPU utilization on supported fixed systems. Interface monitoring is expanded with support for Two-Way Active Measurement Protocol (TWAMP) and TWAMP-Light, providing flexible, lightweight performance measurement for latency, jitter, and packet loss across multiple platforms. Additionally, L2VPN capabilities are strengthened with Y.1564 Ethernet Service Activation Testing, enabling standardized service turn-up, SLA validation, and KPI measurement across supported hardware. These enhancements improve traffic engineering control, operational simplicity, and service assurance across the Cisco 8000 series router portfolio.

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 Cisco 8000 Series Routers, Release 26.1.1

Product impact	Feature	Description
BGP		
Software Reliability	BGP best-path selection using controller-programmed metrics	Introduced in this release on: Fixed Systems(8200, 8700)(select variants only*); Centralized Systems (8600); Modular Systems (8800 [LC ASIC: Q100, Q200, P100])(select variants only*) You can steer BGP overlay traffic along controller-selected underlay paths by enabling BGP best-path selection using controller-programmed metrics. The network controller injects preferred path metrics into the Routing Information Base (RIB) via SL-APIv2, and BGP uses these metrics to select the best path for overlay routes. This enables precise traffic engineering, seamless Segment Routing (SR) label transitions, simpler migration from legacy protocols, and better per-prefix traffic visibility.
EVPN		
Software Reliability	Extended Hardware offload of Connectivity Check Messages (CCM) timers	Introduced in this release on: Fixed Systems (8010 [ASIC: A100]; 8700 [ASIC: K100]; 8400 [ASIC: K100]) (select variants only*) This release extends the hardware offload support for Connectivity Check Messages (CCM) timers to a range of up to 1 second (1000 ms). Previously, hardware offload CCM timers were supported only from 3.3 milliseconds to 100 milliseconds. By enabling hardware offload for longer timer intervals, the processing load on the router's CPU is reduced, which can enhance overall device performance and scalability. This improvement allows for more efficient network monitoring with less CPU utilization. *This functionality is now extended to these routers: • Cisco 8011-4G24Y4H-I • Cisco 8011-32Y8L2H2FH • Cisco 8712-MOD-M • Cisco 8711-48Z-M • Cisco 8404-SYS-D • Cisco 8011-12G12X4Y-A

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		• Cisco 8011-12G12X4Y-D
Software Reliability	EVPN IRB over SRv6 core	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100, K100]); Centralized Systems (8400 [ASIC: K100]); Modular Systems (8800 [LC ASIC: P100]) EVPN IRB enhances network flexibility by enabling seamless Layer 3 connectivity between hosts on different subnets over an SRv6 network. This feature allows Layer 3 forwarding among hosts across IP subnets, maintains EVPN multi-homing capabilities, and facilitates communication between EVPN hosts or subnets and IP VPNs. Leveraging SRv6's programmable and flexible transport, the solution streamlines the integration and management of modern, diverse network environments.
Interfaces		
Ease of Use	Two-Way Active Measurement Protocol (TWAMP)	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC:Q200], 8400 [ASIC: K100]); Modular Systems (8800 [LC ASIC: Q200, P100]) The TWAMP is a protocol designed to measure and monitor the performance of IP networks by testing round-trip performance metrics between two devices. TWAMP enables the assessment of IP Service Level Agreement (SLA) compliance through active measurement of key performance indicators such as latency, jitter, and packet loss. This is particularly valuable for service providers and enterprise networks to ensure high-quality service delivery.
Ease of Use	TWAMP-Light	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC:Q200], 8400 [ASIC: K100]); Modular Systems (8800 [LC ASIC: Q200, P100]) TWAMP-light is a lightweight model of TWAMP, which eliminates the need for a control session. It removes the overhead of establishing and terminating the control session on both end devices.
L2VPN		
Software Reliability	Y.1564 - Ethernet service activation test	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8400 [ASIC: K100]) Use the Y.1564 Ethernet Service Activation Test (SAT) to check SLA settings. Ensure all services meet SLA objectives at their maximum committed rate under maximum load. Conduct medium-term and long-term soak tests under stress. Use this procedure to turn up service, install, and troubleshoot Ethernet-based services. You can use this test to collect Key Performance Indicator (KPI) metrics, including Frame Transfer Delay (latency or Round Trip Time (RTT)) and Frame Loss Ratio (packet loss). Use the test to measure the non-drop rate and the maximum rate under stress conditions.
Modular QoS		
Upgrade	Extended display and filtering options for show interfaces	Introduced in this release on: Fixed Systems (8200 [ASIC: Q100, Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC:Q200], 8400 [ASIC: K100]); Modular Systems (8800 [LC ASIC: Q100, Q200, P100] This feature enhances the show interfaces CLI to improve monitoring of environments with large numbers of tunnel interfaces. It introduces a wide display option to show full interface names, a no-tunnels filter to exclude tunnel interfaces, and an additional field indicating the reason an interface is down. These optional enhancements preserve existing command behavior while enabling clearer, more actionable operational visibility.
Multicast		

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
Software Reliability	MLDP Recursive FEC for Inter-AS	Introduced in this release on: Fixed Systems (8200 [ASIC: Q100, Q200, P100], 8700 [ASIC: P100,K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC: Q200], 8400 [ASIC: K100]); Modular Systems (8800 [LC ASIC: Q100, Q200, P100]) MLDP Recursive FEC enables the transport of multicast VPN traffic across autonomous systems without requiring provider routers (P routers) to know all PE loopback addresses. It uses an inner and outer FEC to guide label switching, supporting interoperability between provider edge and ASBR routers. This feature adds support for mLDP Recursive FEC enabling Inter-AS multicast VPN scenarios (Options B and C) and extends support for profiles 1, 4, 6, and 14.
Programmability		
Software Reliability	Maintain reliable gRPC server operation on the router	Introduced in this release on: Fixed Systems (8200 [ASIC: Q100, Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC: Q200]); Modular Systems (8800 [LC ASIC: Q100, Q200, P100]) 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.
Routing		
Ease of use	ePBR on BVI	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100, K100]) (select variants only*); Centralized Systems (8400 [ASIC: K100]) (select variants only*); Modular Systems (8800 [LC ASIC: P100]) (select variants only*) You can ensure secure and efficient traffic handling at the network ingress by applying ePBR policies directly to the BVI. This feature allows the Cisco IOS XR software to intercept and steer inbound Layer 2 traffic before it transitions to Layer 3 routing. *This feature is supported on:
Software Reliability	Cross-Address Family Static Routing	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC: Q200]); Modular Systems (8800 [LC ASIC: Q100, Q200, P100]) With the introduction of this feature, you can now configure IPv4 prefixes with IPv6 next-hops. The router programs these routes into the routing table once the Routing Information Base (RIB) confirms the next-hop is reachable. This feature allows IPv4 traffic to traverse IPv6-capable infrastructure, providing a highly scalable solution for modern dual-stack network management. This feature introduces these changes: CLI: * router static address-family * show static vrf * show static interfaces
Software	Static IS-IS	Introduced in this release on: Fixed Systems (8200, 8700); Centralized Systems (8600 [ASIC:Q200], 8400 [ASIC: K100]); Modular Systems (8800 [LC ASIC: Q100, Q200, P100])

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
Reliability	BGP tracking	You can now boost network accuracy and reliability with the static IS-IS BGP tracking feature. It only advertises static IS-IS neighbors when the matching BGP peer is up, using a simple route-policy to track their status. Two-way connectivity checks are turned off for static neighbors to avoid false failures, and IS-IS extended TLVs make sure these neighbors are clearly shown in IS-IS LSPs for accurate network mapping.
Segment Routing		
Software Reliability	BGP SID locator tracking for SRv6 services	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC: Q200]); Modular Systems (8800 [LC ASIC: Q200, P100], 8400 [ASIC: K100]) 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.
Software Reliability	Link Residual Bit Error Rate Measurement using STAMP	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200, P100], 8700 [ASIC: P100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC: Q200]); Modular Systems (8800 [LC ASIC: Q200, P100]) You can now enable earlier detection of physical layer issues and faster troubleshooting before packet loss or service impact occurs by actively measuring residual bit errors and report metrics to identify link degradations.
Software Reliability	Performance Measurement for Link Bundle Members	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200, P100], 8700 [ASIC: P100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC: Q200]); Modular Systems (8800 [LC ASIC: Q200, P100]) Identify and isolate link issues for bundle members by measuring delay, loss, and bit errors for individual links. This feature provides visibility into performance at the member level and uses high-bandwidth STAMP to detect issues caused by variations in fiber or optical transport quality.
Ease of Use	SRv6-TE explicit BSID and remote steering	Introduced in this release on: Fixed Systems (8010 [ASIC: A100]; 8200 [ASIC: Q200, P100], 8700 [ASIC: P100, K100]); Centralized Systems (8600 [ASIC:Q200], 8400 [ASIC: K100]); Modular Systems (8800 [LC ASIC: Q200, P100]) 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

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		show segment-routing srv6 static-endpoint *YANG Data Models:* * Cisco-IOS-XR-infra-xtc-agent-oper.yang * Cisco-IOS-XR-segment-routing-srv6-cfg.yang see GitHub , YANG Data Models Navigator)
Setup and Upgrade		
Upgrade	Signature verification of owner RPMs using owner public keys	Introduced in this release on: Fixed Systems (8200 [ASIC: Q100, Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC:Q200]) ; Modular Systems (8800 [LC ASIC: Q100, Q200, P100]) 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: Fixed Systems (8200 [ASIC: Q100, Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC:Q200]) ; Modular Systems (8800 [LC ASIC: Q100, Q200, P100]) 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: Fixed Systems (8200 [ASIC: Q100, Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC:Q200]) ; Modular Systems (8800 [LC ASIC: Q100, Q200, P100]) 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: Fixed Systems (8200 [ASIC: Q100, Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC:Q200]) ; Modular Systems (8800 [LC ASIC: Q100, Q200, P100]) 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. However, to enable the customer consent token workflow, execute the *consent-token customer* command after the key package installation.
System Management		
Ease of Use	Monitor mount points	Introduced in this release on: Fixed Systems (8200 [ASIC: Q100, Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC: Q200]); Modular Systems (8800 [LC ASIC: Q100, Q200, P100])

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		You can prevent service disruptions by having a clear visibility into your router's storage resource allocation and usage. Adequate disk space is crucial for preventing application crashes, ensuring successful upgrades, and maintaining optimal router performance. This feature provides detailed information about the file system's name (mount point), storage component (file system type), total size, available space, and utilized space, allowing you to monitor and manage disk space effectively. Both Model-Driven Telemetry (MDT) and Event-Driven Telemetry (EDT) are supported.
Software Reliability	Enhanced SNMP FEC visibility for all optical modules	Introduced in this release on: Fixed Systems (8200 [ASIC: Q100, Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC:Q200]) ; Modular Systems (8800 [LC ASIC: Q100, Q200, P100]) Support for FEC (Forward Error Correction) statistics is now extended to all CMIS (Common Management Interface Specification)-compliant optical modules, including grey and ZR optics. The CISCO-OPTICAL-MIB now provides both host-side and media-side statistics, enabling unified monitoring, accurate signal degradation identification, and enhanced troubleshooting across optical networks. Previously, SNMP offered only limited media-side pre-FEC and post-FEC BER statistics for color optics, restricting comprehensive performance analysis for other optical modules and system components. For detailed information on the specific MIB, please refer the MIB Locator.
System Monitoring		
Software Reliability	SSD health metrics	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200]); Modular Systems (8800 [LC ASIC: Q200])(select variants only*) You can now maintain optimal health of Solid State Drives (SSDs) and promptly identify hardware issues to minimize the downtime of your router. The SSD in your router is crucial, as it stores critical data and system files necessary for the router's operation. To ensure proper working of the router, the feature utilizes Self-Monitoring, Analysis, and Reporting Technology (SMART) to monitor SSDs. By default, SMART continuously performs self-tests and logs errors and warnings to specific log files. You can promptly identify hardware issues by reviewing these logs. *This feature is supported on: * 8101-32H * 8102-64H * 8201-32FH * 8101-32FH * 8201-24H8FH * 8202-32FH-M * 8608-RP * 88-LC0-36FH * 88-LC0-36FH-M

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		* 88-LC0-34H14FH
System Security		
Software Reliability	SSH key strength:3072 bits by default	Introduced in this release on: Fixed Systems (8200 [ASIC: Q100, Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC:Q200]) ; Modular Systems (8800 [LC ASIC: Q100, Q200, P100]) 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: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100])(select variants only*); Modular Systems (8800 [LC ASIC: P100])(select variants only*) This enhancement ensures Cisco IOS XR devices comply with evolving security standards by sending syslog warnings during system boot if weak Rivest, Shamir, and Adelman (RSA) keys (less than 3072 bits) or 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 on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100])(select variants only*); Modular Systems (8800 [LC ASIC: P100])(select variants only*) This enhancement ensures Cisco IOS XR devices comply with evolving security standards by sending syslog warnings during system boot if weak RSA keys (less than 3072 bits) or 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	802.1X port-based authentication	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Modular Systems (8800 [LC ASIC: Q100, Q200, P100])(select variants only*) *This feature is extended to these hardware variants: * 8201 * 8201-32FH * 88-LC0-36FH-M * 8212-48FH-M * 8711-32FH-M * 88-LC1-36EH * 88-LC1-12TH24FH-E * 88-LC1-52Y8H-EM * 8712-MOD-M * 8711-48Z-M * 8011-4G24Y4H-I * 8011-32Y8L2H2FH * 8011-12G12X4Y-A/D

New hardware

Table 2. New hardware for Cisco 8000 Series Routers, Release 26.1.1

© 2026 Cisco and/or its affiliates. All rights reserved.

Hardware	Description
Cisco 8404-SYS-D	The Cisco 8404-SYS-D is a full-featured, modular and programmable aggregation 4 RU router. The Cisco 8404-SYS-D is a K100 Cisco Silicon One Network Processing Unit (NPU) router that offers a new breed of centralized architectures that combine the best aspects of distributed and fixed systems with 4.8 Tbps of network bandwidth. The Cisco 8404 supports two different MPAs: · Cisco 84-MPA-2H12Z-M with network bandwidth of 800 Gbps · Cisco 84-MPA-2FH/6H-M with network bandwidth of 800 Gbps The Cisco 8404-SYS-D supports QSFP56-DD, QSFP28, and SFP56 optical ports.
8818-FC1 Fabric Card based on F100 Silicon Chip	The Cisco 8818 Series Routers supports the Cisco 8818 fabric card (8818-FC1). The 8818-FC1 fabric card is based on a Silicon One F100 ASIC. Each fabric card provides 76 Tbps of switching capacity with Q200 or P100 Silicon One line cards. Because of the higher switching capacity, this fabric card offer benefits, such as faster communication, lower latency, and ability to manage higher data flows. By default, the fabric card only supports 8FC mode.
Optics	This release introduces the following new optics that are available on supported hardware in the product portfolio. For details refer to the Transceiver Module Group (TMG) Compatibility Matrix . Cisco 100GBASE Quad Small Form-Factor Pluggable • CVR-QSFP-SFP10G Cisco 10GBASE SFP28 (Small Form-Factor Pluggable) • SFP-10G-LR • SFP-10G-LR-S • SFP-10G-SR • SFP-10G-SR-S • SFP-10G-ZR • SFP-10G-ZR-S • SFP-10G-ER • SFP-10G-ER-S • SFP-10G-ZR-I

Changes in behavior

- The default minimum syslog TLS version is now TLS 1.2 to enhancesecurity. 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 isconfigured as TLS 1.0 or 1.1.
- On the Cisco 8404-SYS-D platform, dual Route Switch Processors (RSPs) can be installed. However, it is recommended to use a single active RSP and disable the second RSP. Note that Route Processor Failover (RPFO) is not supported in Cisco IOS XR release 26.1.1.
- Layer 3 service gateway for interconnecting SRv6 domains: From Release 26.1.1, Cisco IOS XR software sets the VLAN Priority Code Point (PCP) field based on the SRv6 header's Differentiated Services Code Point (DSCP) value rather than being fixed at zero. This optimization enables proper Quality of Service (QoS) marking and navigation through the VLAN header in the Interworking (IW) Gateway.

© 2026 Cisco and/or its affiliates. All rights reserved.

- Enhanced Inner-Header Hop-Limit Handling: Previously, the segment-routing srv6 encapsulation command affected only the encapsulation behavior. From Release 26.1.1, the command also updates the hop-limit value of the inner header after END.DT, END.DX, uDT, and uDX decapsulation.
- MPLS-TE PCE authentication: Starting from Release 26.1.1, you can use TCP Authentication Option (TCP-AO) for MPLS-TE PCE authentication. TCP-AO relies on Message Authentication Codes (MACs) to secure connections. With this option, you protect TCP connections against replay attacks, enjoy more robust and detailed security compared to the MD5 method, and benefit from a broader selection of authentication algorithms—all without needing significant changes to your system or operations.

Open issues

Table 3. Open issues for Cisco 8000 Series Routers, Release 26.1.1

Bug ID	Description
CSCwr67313	Redirect fails for IPv4 traffic in PBR policy-maps.
CSCws39506	BGP flow specification did not match certain policies after flowspec_mgr process restart.

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 4. Compatibility matrix for Cisco 8000 Series Routers, Release 26.1.1

Cisco IOS XR	Crosswork	EPNM
Release 26.1.1	Crosswork Optimization Engine 6.0	Evolved Programmable Network Manager 8.1.1

Upgrade and downgrade paths

To view all supported Cisco IOS XR Software upgrades from the current version according to the support data installed on the running system, enter the **show install upgrade-matrix running** command:

```
Router# show install upgrade-matrix running all
Matrix: XR version: 26.1.1, File version: 1.1, Version: N/A


The upgrade matrix indicates that the following system upgrades and downgrades are supported
from the current XR version:

From       To         Restrictions
---------- ---------- ----------------------------------------------------
26.1.1     24.1.2     Target fixes; Caveats; Replace performed via reimage
```

© 2026 Cisco and/or its affiliates. All rights reserved.

```
26.1.1     24.2.2     Target fixes; Caveats; Replace performed via reimage
26.1.1     24.2.20    Caveats; Replace performed via reimage
26.1.1     24.2.203   Caveats; Replace performed via reimage
26.1.1     24.2.204   Caveats; Replace performed via reimage
26.1.1     24.2.206   Caveats; Replace performed via reimage
26.1.1     24.2.207   Caveats; Replace performed via reimage
26.1.1     24.2.209   Caveats; Replace performed via reimage
26.1.1     24.2.21    Caveats; Replace performed via reimage
26.1.1     24.3.2     Target fixes; Caveats; Replace performed via reimage
26.1.1     24.3.20    Caveats; Replace performed via reimage
26.1.1     24.3.30    Caveats; Replace performed via reimage
26.1.1     24.4.2     Caveats; Replace performed via reimage
26.1.1     25.1.1     Caveats; Replace performed via reimage
26.1.1     25.1.2     Caveats; Replace performed via reimage
26.1.1     25.1.30    Caveats; Replace performed via reimage
26.1.1     25.2.1     Caveats; Replace performed via reimage
26.1.1     25.2.15    Caveats; Replace performed via reimage
26.1.1     25.2.16    Caveats; Replace performed via reimage
26.1.1     25.2.17    Caveats; Replace performed via reimage
26.1.1     25.2.18    Caveats; Replace performed via reimage
26.1.1     25.2.2     Caveats; Replace performed via reimage
26.1.1     25.3.1     Caveats; Replace performed via reimage
26.1.1     25.4.1     Caveats; Replace performed via reimage
26.1.1     25.4.2     Caveats; Replace performed via reimage
26.1.1     7.11.2     Target fixes; Caveats; Replace performed via reimage
26.1.1     7.11.21    Target fixes; Caveats; Replace performed via reimage

Add the from and to versions to the end of the CLI command, for data on versions with
additional restrictions

For example, to display restrictions for the 26.1.1->24.1.2 upgrade, use
        'show install upgrade-matrix running 26.1.1 24.1.2'
```

Software version

Log in to the router and enter the **show version** command:

```
RP/0/RP0/CPU0# show version
Cisco IOS XR Software, Version 26.1.1 LNT
Copyright (c) 2013-2026 by Cisco Systems, Inc.

Build Information:
 Built By     : swtools
 Built On     : Thu Feb 26 22:52:34 UTC 2026
 Build Host   : iox-lnx-102
```

© 2026 Cisco and/or its affiliates. All rights reserved.

```
 Workspace    : /auto/srcarchive12/prod/26.1.1/8000/ws
 Version      : 26.1.1
 Label        : 26.1.1

cisco 8000 (Intel(R) Xeon(R) CPU D-1530 @ 2.40GHz)
cisco 8804 (Intel(R) Xeon(R) CPU D-1530 @ 2.40GHz) processor with 32GB of memory
R3 uptime is 7 hours, 50 minutes
Cisco 8804 4-slot Chassis
```

Supported hardware

Table of supported hardware components and the minimum required software versions.

Table 5. Supported hardware for Cisco 8010 Series Routers

Part Number	Description	Support Initially Provided in IOS XR Release
Cisco 8010 Series Routers - Chassis		
8011-12G12X4Y-A	Cisco 8011 12x1G, 12x1/10G, 4X1/10/25G	Release 25.4.1
8011-12G12X4Y-D	Cisco 8011 12x1G, 12x1/10G, 4X1/10/25G	Release 25.4.1
8011-32Y8L2H2FH	Cisco 8010 32X25G SFP28, 8x50G, 2x100GQSFP28, 2x400G QSFP-DD	Release 25.4.1
8011-4G24Y4H-I	Cisco 8010 1 RU Fixed System - 4 QSFP28 100GbE, 24 SFP28 25GbE, and 4 RJ-45 100MbE	Release 25.1.1
Cisco 8010 Series Routers - Power Supply Unit (PSU)		
PWR-650-AC-R	Cisco 650W AC Power Module	Release 25.4.1
PWR-930-DC-R	Cisco 930W DC Power Module	Release 25.4.1
PWR-400-AC	Cisco 400W AC Power Module	Release 25.1.1
PWR-400-DC	Cisco 400W DC Power Module	Release 25.1.1

Table 6. Supported hardware for Cisco 8200 Series Routers

Part Number	Description	Support Initially Provided in IOS XR Release
Cisco 8200 Series Routers - Chassis		
8201-SYS	Cisco 8200 1 RU Fixed System - 24 QSFP56-DD 400GbE and 12 QSFP28 100GbE	Release 7.0.12
8202-SYS	Cisco 8200 2 RU Fixed System - 12 QSFP56-DD 400GbE and 60 QSFP28 100GbE	Release 7.3.1

© 2026 Cisco and/or its affiliates. All rights reserved.

Part Number	Description	Support Initially Provided in IOS XR Release
8201-32FH	Cisco 8200 1 RU Fixed System - 32 QSFP56-DD 400GbE	Release 7.3.15
8201-24H8FH	Cisco 8200 1 RU Fixed System - 8 QSFP56-DD 400GbE and 24 QSFP28 100GbE	Release 7.7.1
8202-32FH-M	Cisco 8200 2 RU Fixed System - 32 QSFP56-DD 400GbE with MACsec	Release 7.5.2
8212-48FH-M	Cisco 8200 2 RU Fixed System - 24 QSFP-DD 800G or 48 QSFP56-DD 400GbE with MACsec	Release 24.3.1
Cisco 8200 Series Routers - Power Supply Unit (PSU)		
PSU1.4KW-ACPI	Cisco 1.4KW AC Power Module with Port-side Air Intake	Release 7.0.12
PSU1.4KW-ACPE	Cisco 1.4KW AC Power Module with Port-side Air Exhaust	Release 7.0.12
PSU2KW-ACPI	Cisco 2KW AC Power Module with Port-side Air Intake	Release 7.3.1
PSU2KW-ACPE	Cisco 2KW AC Power Module with Port-side Air Exhaust	Release 7.3.1
PSU3KW-HVPI	Cisco 3KW HV AC/DC Power Supply Unit	Release 7.5.3

Table 7. Supported hardware for Cisco 8400 Series Routers

Part Number	Description	Support Initially Provided in IOS XR Release
Cisco 8400 Series Routers - Chassis		
8404-SYS-D	Cisco 8404 – 4-Slot Centralized Chassis	Release 26.1.1
Cisco 8400 Series Routers - Modular Port Adapters (MPA)		
84-MPA-2H12Z-M	Cisco 8404 MPA with 2x100G QSFP28 + 12x1/10/25/50G SFP56	Release 26.1.1
84-MPA-2FH/6H-M	Cisco 8404 MPA with 2x400G / 6x100G QSFP56-DD	Release 26.1.1
Cisco 8400 Series Routers - Power Entry Module (PEM)		
8404-DC-PEM	Cisco 8404 DC Power Entry Module	Release 26.1.1

Table 8. Supported hardware for Cisco 8600 Series Routers

Part Number	Description	Support Initially Provided in IOS XR Release
Cisco 8600 Series Routers - Chassis		
8608	Cisco 8600 7 RU Centralized System	Release 7.10.1

© 2026 Cisco and/or its affiliates. All rights reserved.

Part Number	Description	Support Initially Provided in IOS XR Release
Cisco 8600 Series Routers - Modular Port Adapters (MPA)		
86-MPA-14H2FH-M	Cisco 8608 MPA - 2 QSFP-DD 400GbE and 14 QSFP / 16 QSFP 100GbE	Release 7.10.1
86-MPA-24Z-M	Cisco 8608 MPA - 24 SFP56 10/25/50 GbE	Release 7.10.1
86-MPA-4FH-M	Cisco 8608 MPA - 4 QSFP-DD 400GbE	Release 7.10.1
Cisco 8600 Series Routers - Power Supply Unit (PSU)		
PSU3.2KW-ACPI	Cisco 3.2-kW AC Power Supply Unit	Release 7.10.1
PSU3.2KW-DCPI	Cisco 3.2-kW DC Power Supply Unit	Release 7.10.1
PSU4.3KW-HVPI	Cisco 4.3KW HV AC/DC Power Supply Unit	Release 7.10.1

Table 9. Supported hardware for Cisco 8700 Series Routers

Part Number	Description	Support Initially Provided in IOS XR Release
Cisco 8700 Series Routers - Chassis		
8711-48Z-M	Cisco 8700 1 RU Fixed System - 6 QSFP-DD, 4 QSFP56, and 48 SFP56 ports	Release 25.4.1
8711-32FH-M	Cisco 8700 1 RU Fixed System - 16 QSFP-DD800 and 16 QSFP56-DD	Release 24.3.1
8712-MOD-M	Cisco 8700 2 RU Fixed System	Release 24.4.1
Cisco 8700 Series Routers - Modular Port Adapters (MPA)		
8K-MPA-4D	Cisco 8712 MPA - 4 QSFP-DD 400GbE	Release 24.4.1
8K-MPA-16H	Cisco 8712 MPA - 16 QSFP-28 100GbE	Release 24.4.1
8K-MPA-16Z2D	Cisco 8712 MPA - 2 QSFP-DD 400GbE, 2 QSFP-DD 200GbE, and 16 SFP 50GbE	Release 24.4.1
8K-MPA-18Z1D	Cisco 8712 MPA - 1 QSFP-DD 400 GbE and 18 zSFP56+ 50GbE	Release 25.1.1
Cisco 8700 Series Routers - Power Supply Unit (PSU)		
PSU2KW-ACPI	Cisco 8711-32FH-M PSU - 2KW AC Power Module with Port-side Air Intake	Release 24.3.1
PSU2KW-ACPE	Cisco 8711-32FH-M PSU - 2KW AC Power Module with Port-side Air Exhaust	Release 24.3.1
PSU2KW-DCPI	Cisco 8711-32FH-M PSU - 2KW DC Power Module with Port-side Air Intake	Release 24.3.1
PSU2KW-DCPE	Cisco 8711-32FH-M PSU - 2KW DC Power Module with Port-side Air Exhaust	Release 24.3.1

© 2026 Cisco and/or its affiliates. All rights reserved.

Part Number	Description	Support Initially Provided in IOS XR Release
PSU2KW-DCPI	Cisco 8712-MOD-M PSU – 2KW 48V DC Power Module with Port-side Air Intake	Release 24.4.1
PSU2KW-DCPE	Cisco 8712-MOD-M PSU – 2KW 48V DC Power Module with Port-side Exhaust	Release 24.4.1
PSU2KW-ACPI	Cisco 8712-MOD-M PSU – 2KW AC Power Module with Port-side Air Intake	Release 24.4.1
PSU2KW-ACPE	Cisco 8712-MOD-M PSU – 2KW AC Power Module with Port-side Exhaust	Release 24.4.1

Table 10. Supported hardware for Cisco 8800 Series Routers

Part Number	Description	Support Initially Provided in IOS XR Release
Cisco 8800 Series Routers - Chassis		
8804-SYS	Cisco 8800 Modular System - 10 RU with 4 Line Card Slots	Release 7.3.2
8808-SYS	Cisco 8800 Modular System - 16 RU with 8 Line Card Slots	Release 7.0.12
8812-SYS	Cisco 8800 Modular System - 21 RU with 12 Line Card Slots	Release 7.0.12
8818-SYS	Cisco 8800 Modular System - 33 RU with 18 Line Card Slots	Release 7.0.14
Cisco 8800 Series Routers - Route Processors		
8800-RP	Cisco 8800 Route Processor - 4 Core	Release 7.0.12
8800-RP2	Cisco 8800 Route Processor - 8 Core	Release 7.11.1
Cisco 8800 Series Routers - Fabric Modules		
8808-FC	Cisco 8808 System Fabric Module - Q100-based fabric modules with 14.4T per LC slot	Release 7.0.12
8812-FC	Cisco 8812 System Fabric Module - Q100-based fabric modules with 14.4T per LC slot	Release 7.0.12
8818-FC	Cisco 8818 System Fabric Module - Q100-based fabric modules with 14.4T per LC slot	Release 7.0.14
8808-FC0	Cisco 8808 System Fabric Module - Q200-based fabric modules with 14.4T per LC slot	Release 7.3.15
8818-FC0	Cisco 8818 System Fabric Module - Q200-based fabric modules with 14.4T per LC slot	Release 7.3.16
8804-FC0	Cisco 8804 System Fabric Module - Q200-based fabric modules with 14.4T per LC slot	Release 7.3.16
8808-FC1	Cisco 8808 System Fabric Module - F100-based fabric modules with 28.8T per LC slot	Release 24.2.1

© 2026 Cisco and/or its affiliates. All rights reserved.

Part Number	Description	Support Initially Provided in IOS XR Release
8804-FC1	Cisco 8804 System Fabric Module - F100-based fabric modules with 28.8T per LC slot	Release 25.1.1
8818-FC1	Cisco 8818 System Fabric Module - F100-based fabric modules with 76T per LC slot	Release 26.1.1
Cisco 8800 Series Routers - Line Cards		
8800-LC-48H	Cisco 8800 Line Card with MACsec - Q100 ASIC based 4.8 Tbps line card	Release 7.0.12
8800-LC-36FH	Cisco 8800 Line Card - Q100 ASIC based 14.4 Tbps line card	Release 7.0.12
88-LC0-36FH	Cisco 8800 Line Card - Q200 ASIC based 14.4 Tbps line card	Release 7.3.15
88-LC0-36FH-M	Cisco 8800 Line Card with MACsec- Q200 ASIC based 14.4 Tbps line card	Release 7.3.15
88-LC0-34H14FH	Cisco 8800 Line Card - Q200 ASIC based 9 Tbps line card	Release 7.3.3 Release 7.5.1
88-LC1-36EH	Cisco 8800 Line Card - P100 ASIC based 28.8 Tbps line card	Release 24.2.11
88-LC1-12TH24FH-E	Cisco 8800 Line Card - P100 ASIC based 12 Tbps line card	Release 24.3.1
88-LC1-52Y8H-EM	Cisco 8800 Line Card - P100 ASIC based 3.7 Tbps line card	Release 24.3.1
Cisco 8800 Series Routers - Power Supply Unit (PSU)		
PSU4.8KW-DC100	4.8KW 48V 100A DC Power Supply	Release 7.3.2
PSU6.3KW-HV	6.3KW AC/HVAC/HVDC Power Supply	Release 7.0.12
PSU6.3KW-20A-HV	6.3KW AC/HVAC/HVDC Power Supply-20A	Release 7.0.12

Supported software packages

Overview of Cisco IOS XR software

The Cisco IOS XR software is composed of a base image (ISO) that provides the XR infrastructure. The ISO image is made up of a set of packages (also called RPMs). These packages are of three types:

- A mandatory package that is included in the ISO
- An optional package that is included in the ISO
- An optional package that is not included in the ISO

Visit the Cisco Software Download page to download the Cisco IOS XR software images.

View installed software packages

To determine the Cisco IOS XR Software packages installed on your router, log in to the router and enter the **show install active** command. To view the optional and bug fix RPM packages, first install the package and use the **show install active summary** command.

© 2026 Cisco and/or its affiliates. All rights reserved.

To know about all the RPMs installed including XR, OS and other components use the **show install active all** command.

Flexible software modularity

The software modularity approach provides a flexible model that allows you to install a subset of IOS XR packages on devices based on your individual requirements. All critical components are modularized as packages so that you can select the features that you want to run on your router.

Determine firmware support

To determine firmware support on your router, log in to the router and enter **show fpd package** command.

Related resources

Table 11. Related resources

Resource	Description
Smart licensing	Provides information about Smart Licensing Using Policy solutions and their deployment on IOS XR routers.
Cisco 8000 documentation	Provides CDC documentation for Cisco 8000 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.
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.

© 2026 Cisco and/or its affiliates. All rights reserved.

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.