Release Notes for Cisco 8000 Series Routers, IOS XR Release 25.4.1

© 2025 Cisco and/or its affiliates. All rights reserved.

Contents

Cisco 8000 Series Routers, IOS XR Release 25.4.1 3
New software features 3
New hardware 17
Changes in behavior 17
Open issues 19
Known issues 19
Compatibility 19
Supported hardware 21
Supported software packages 25
Related resources 25
Legal information 27

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco 8000 Series Routers, IOS XR Release 25.4.1

Cisco IOS XR Release 25.4.1 introduces new features and hardware enhancements for the Cisco 8000 Series Routers. Key features include BGP fast reroute for rapid convergence, automated EVPN service steering with segment routing and SR-TE, expanded ACL and two-pass QoS support on BVIs, MACsec encryption and TCG-compliant TPM for stronger security, 400G port and higher tunnel scale for improved hardware flexibility, and advanced timing and monitoring tools for greater operational visibility and reliability.

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 25.4.1

Product impact	Feature	Description
BGP		
Ease of Use	BGP Quick-withdraw	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]) BGP Quick-withdraw improves network responsiveness, reduces the risk of blackholing traffic, and maintains stable application performance during network events, such as nexthop failures or interface outages. It sends route withdraw messages as soon as bestpath computation determines that a prefix is unreachable. The feature triggers early withdraws, allowing the remaining internal process, such as RIB deletion and label release, to continue in parallel. It is enabled by default for the supported address-families. Previously, withdrawing unreachable routes was often delayed because BGP update generation waited for the entire prefix-processing pipeline to complete, including import, label allocation, and RIB installation.
Software Reliability	Policy-based cumulative bandwidth advertisements	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 now reduce unnecessary BGP updates, such as frequent route advertisements caused by small, insignificant bandwidth changes, and improve network stability by suppressing minor bandwidth changes, rounding advertised bandwidth to a specified value, and setting outbound policy actions based on bandwidth thresholds.
Ease of Use	BGP per-link FRR for multipath backups	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200]); Centralized Systems (8600 [ASIC: Q200]) ; Modular Systems (8800 [LC ASIC: Q100, Q200]) The feature enhances network resilience and accelerates convergence by allowing network operators to explicitly select a backup path for each primary next-hop. This approach ensures

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		true path diversity and avoids common failure points, such as Shared Risk Link Groups (SRLG). It enables you to achieve convergence in approximately 50 milliseconds for prefixes, ensuring service continuity during primary link failures. Previously, Fast Reroute (FRR) mechanisms like Prefix-Independent Convergence (PIC) automatically selected backup paths without explicit user control, which could lead to suboptimal path selection.
Software Reliability	Improved BGP-PIC convergence for multilink failures	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200]); Centralized Systems (8600 [ASIC: Q200]; Modular Systems (8800 [LC ASIC: Q100, Q200]) The enhancement improves BGP-PIC convergence for multilink failures by aggregating multiple link-down events into a single hardware update to the FIB. This approach reduces hardware programming time required for FIB updates, speeds up recovery, and maintains network stability during clustered failures. Previously, BGP-PIC processed each link failure one at a time, and each event triggered its own hardware update, which caused multiple hardware updates and longer convergence time.
EVPN		
Software Reliability	EVPN ELAN automated steering to flex-algorithms	Introduced in this release on: Fixed Systems (8100 [ASIC: Q200], 8200 [ASIC: Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC: Q200]); Modular Systems (8800 [LC ASIC: Q200, P100]) You can now automatically steer EVPN ELAN traffic onto paths computed by Segment Routing flex-algorithms. Flex-algorithms enable the definition of custom routing computations in the IGP (IS-IS or OSPF) based on specific network constraints, such as minimizing latency or maximizing bandwidth. Automated steering then applies policies to classify EVPN traffic and direct it to the appropriate flex-algorithm path, ensuring that different types of EVPN services can utilize network resources optimally according to their requirements.
Software Reliability	EVPN ELAN services with SR-TE ODN, RT1, and RT3	Introduced in this release on: Fixed Systems (8100 [ASIC: Q200], 8200 [ASIC: Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC: Q200]); Modular Systems (8800 [LC ASIC: Q200, P100]) You can now enable dynamic traffic steering through SR-TE policy, improving traffic management by directing BUM and unicast traffic over optimized SR-TE paths. This capability is achieved by coloring route type 1 (RT1) and route type 3 (RT3) routes with a non-zero extended community color, which triggers traffic to follow the SR-TE policy path instead of the default IGP path.
Software Reliability	EVPN E-Line with FXC service in VLAN unaware mode	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Modular Systems (8800 [LC ASIC: P100]) You can reduce BGP state complexity and improve scalability with EVPN E-Line in FXC VLAN unaware mode. This mode combines multiple normalized ACs on a single ES into one EVPN E-Line tunnel using a single service ID, advertising one EVI-EAD route per FXC instead of per AC. Additionally, VLAN failures are not signaled over BGP, reducing unnecessary state changes.

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		This feature supports both single-homing and multihoming scenarios, providing flexible and efficient connectivity options.
Software Reliability	Multisegment pseudowires	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Modular Systems (8800 [LC ASIC: P100]) You can improve network scalability and flexibility in delivering network services by extending Layer 2 services across multiple network segments through end-to-end stitching of several pseudowires. This capability simplifies service deployment and broadens network reach by allowing data to flow across multiple provider networks as a single virtual connection.
IP Addresses and Services		
Hardware Reliability	Egress hybrid ACL support	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100]); Modular Systems (8800 [LC ASIC: P100]) P100-based ASICs now support a larger bincode size of 18 bits instead of 14 bits. This increase allows the forwarding pipeline to encode more feature states simultaneously, enabling support for complex egress processing scenarios such as hybrid egress ACL deployments.
Software Reliability	Enhanced hashing functions using extended entropy profiles	Introduced in this release on: Fixed Systems(8200 [ASIC: Q200]);Modular Systems (8800 [LC ASIC: Q200]) This enhancement significantly reduces the risk of traffic polarization thus ensuring more even and efficient distribution of traffic across multiple network paths in large-scale networks. This capability on certain user-defined header fields allows thousands of unique hash function selections.
Software Reliability	Egress hybrid ACL support to A100-based and K100-based ASICs	Introduced in this release on: Fixed Systems (8700 [ASIC: K100], 8010 [ASIC: A100]) You can now apply compression levels for object-group ACLs or hybrid ACLs to egress traffic on Cisco Silicon One K100-based and A100-based routers. This feature enables the router to accommodate additional ACLs or features and optimizes the usage of the TCAM space so that the available limited number of TCAM resources can be used efficiently.
Software Reliability	Extend support for ACLs on BVI to K100-based ASICs	Introduced in this release on: Fixed Systems (8700 [ASIC: K100]) You can now apply ACLs on Bridged Virtual Interfaces (BVIs) on Cisco Silicon One K100-based routers. This feature allows the router to block malicious traffic that targets the router. You can apply ACLs in both ingress and egress directions on a BVI.
Ease of Setup	Host route scale support	This feature provides an alternative programming approach to configure the connected host route, enhancing the scalability for both IPv4 and IPv6. Introduced in this release on: Fixed Systems (8010 [ASIC: A100], 8200 [ASIC: P100], 8700 [ASIC: P100], 8700 [ASIC: K100])(select variants only*) *This feature is supported on:

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		* 8011-12G12X4Y-A * 8011-12G12X4Y-D * 8011-32Y8L2H2FH * 8011-4G24Y4H-I * 8212-48FH-M * 8711-32FH-M * 8712-MOD-M
Ease of Use	Unified CEF error counters	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]) Prior to this enhancement, error counters were spread across several CLI commands, making it difficult to assess FIB process health. This feature consolidates those metrics under a unified command.
Ease of Use	Enhanced ICMP error messages for traceroute	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 enhances the existing traceroute utility by adding detailed diagnostic information to ICMP error messages. Instead of just showing an IP address, traceroute can now display specifics about the incoming and outgoing interfaces and the next hop IP address at each hop. This provides deeper insights into the network path for troubleshooting.
Ease of Use	ICMP probe utility	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 a new network diagnostic tool called PROBE, similar to ping but with enhanced capabilities. It allows users to query the operational status of local interfaces or directly connected remote neighbors, providing details like Probe can report whether the interface is active, and whether IPv4 and IPv6 are running. PROBE operates via a proxy device, making it suitable for troubleshooting scenarios where direct bidirectional connectivity to the probed interface is not available.
Interface and Hardware Component		
API Experience	Single UDP port for IPv4 and IPv6 packets	Introduced in this release on: Fixed Systems(8200 [ASIC: Q200]) This feature enhances memory and network performance by using a single UDP port for both IPv4 and IPv6 packets in GUE variant 1 UDP encapsulation and decapsulation. The default UDP port for IPv4 and IPv6 is 6080. As part of this enhancement, the **hw-module profile gue udp-dest-port** command is deprecated.
Software Reliability	PRBS support for high-speed optical interfaces	Introduced in this release on: Modular Systems (8800 [ASIC: Q200]) The Pseudo Random Binary Sequence (PRBS) feature provides data integrity checks on router interfaces by generating and

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		analyzing pseudo-random bit patterns, PRBS15 and PRBS31 between the Cisco 88-LC0-36FH router line card and QDD-400G-FR4 optics.
Ease of use	GUEv1 static tunnel configuration over IPv4 networks	Introduced in this release on: Fixed Systems(8200 [ASIC: Q200]);Centralized Systems (8600 [ASIC:Q200]);Modular Systems (8800 [LC ASIC: Q200]) This feature enables highly efficient, scalable, and secure deployment of Generic UDP Encapsulation variant 1 (GUEv1) static tunnels to carry IPv4 and IPv6 traffic over IPv4 networks. In addition, this feature enables the router to use GUEv1 as the overlay encapsulation type for NVE and send encapsulated overlay traffic to IPv4, IPv6, and MPLS destinations using UDP ports. With this feature, you can also increase the GUEv1 scale up to 12K tunnels.
Hardware Reliability	Increased IP-in-IP tunnel scale for gRIBI-based nexthops	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200]); Centralized Systems (8600 [ASIC:Q200]) ; Modular Systems (8800 [LC ASIC: Q200]) This feature enables the router to efficiently load balance and manage high traffic volumes by increasing the scale for encapsulation and decapsulation nexthops programmed using gRPC Routing Information Base Interface (gRIBI) to 12K IP-in-IP tunnels.
Software Reliability	Configure Compatibility Mode for P200-based Line Cards	You can now configure the compatibility settings for line cards installed in a router to operate in P200 mode. When the router is configured to operate in P200 compatibility mode, only F100-based Fabric Cards (FCs) and P200-based line cards are supported. To switch the router to P200 NPU compatibility mode, use the **hw-module profile npu-compatibility** command.
Hardware Reliability	Support for DP08QSDD-ZRB-19B optics on 88-LC1-36EH line card	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]) We have introduced support for the DP08QSDD-ZRB-19B 800G-ZR+ C-band coherent QSFP-DD module on the Cisco 88-LC1-36EH line card. This module enables 800G ZR/ZR+ coherent transmission over amplified C-band DWDM systems, providing high-capacity routed optical networking directly from the router port.
L2VPN		
Software Reliability	VPLS preferred path over SR-TE policy	Introduced in this release on: Fixed Systems (8100 [ASIC: Q200], 8200 [ASIC: Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC: Q200]); Modular Systems (8800 [LC ASIC: Q200, P100]) You can now steer VPLS pseudowire traffic over a specific SR-TE policy, ensuring precise control over routing, bandwidth, or latency for Layer 2 VPN services. This feature allows you to bind a VPLS pseudowire to an SR-TE tunnel interface, overriding the default IGP shortest path. By doing so, you can enforce traffic engineering

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		constraints and optimize network performance.
Licensing		
Licensing Process	Smart Licensing Perpetual Mode	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]) Smart Licensing Perpetual Mode simplifies licensing operations for customers with full-capacity perpetual licenses that cover the entire chassis or all line cards. These customers do not need to enable Smart Licensing Using Policy or report usage, which reduces administrative overhead across these deployments.
Licensing process	Support for Smart Licensing using Policy	Introduced in this release on: Fixed Systems (8010 [ASIC: A100], 8700 [ASIC: K100]) (select variants only*) Cisco Smart Licensing Using Policy streamlines the licensing process for Cisco IOS XR products. You no longer need to register your device during installation, and there is no evaluation license state or period. * This feature is supported on: * 8011-12G12X4Y-A * 8011-12G12X4Y-D * 8011-32Y8L2H2FH * 8711-48Z-M
Licensing process	Support for Flexible Consumption Model 2	Introduced in this release on: Fixed Systems (8010 [ASIC: A100])(select variants only*) The Flexible Consumption Model (FCM) provides the capability and flexibility to purchase software capacity as needed. This release introduces the FCM 2 that offers Essentials, Advantage, and Premier license suites. Premier license suite offers additional licenses that are required on top of Advantage licenses for high scale services. * This feature is supported on: * 8011-12G12X4Y-A * 8011-12G12X4Y-D * 8011-32Y8L2H2FH
MPLS		
Software Reliability	Event history for MPLS-TE headend tunnels	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 a granular and configurable event tracking mechanism for operational visibility into MPLS-TE tunnels. You can enable event history with the **mpls traffic-eng event-history tunnel** command and set the number of tracked events with the **mpls traffic-eng event-history tunnel event-count** command.

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
Software Reliability	MPLS-TE IPv6-only autoroute announce	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 disable IPv4 autoroute announce without turning off autoroute announce entirely. To achieve IPv6-only announcements over MPLS-TE tunnels, use the new exclude-ipv4 option along with the include-ipv6 option in the autoroute announce configuration.
Modular QoS		
Software Reliability	BVI two-pass QoS ingress TC and EXP marking	Introduced in this release on: Fixed Systems (8200 Series [ASIC: P100], 8700 Series [ASIC: P100]) (select variants only*) You can now apply consistent QoS treatment for traffic that moves from a bridge domain to a routed BVI. Your router performs two independent ingress QoS processing passes: it first classifies and marks traffic using Layer 2 attributes inside the bridge domain, and then applies a second Layer 3-based classification at the BVI ingress. At the BVI ingress, only traffic class (TC) or MPLS EXP marking actions are supported. This helps with accurate class assignment and predictable queuing for bridged-to-routed flows. * This feature is supported on: * 8212-48FH-M * 8711-32FH-M
Software reliability	Short-pipe mode	Introduced on Fixed Systems (8200 [ASIC:Q200], Centralized Systems (8600 [ASIC:Q200]), Modular Systems (8800 [LC ASIC: Q200]) Short-pipe mode ensures that your device applies QoS policies only to customer traffic, excluding network overhead such as tunnel headers or the MPLS encapsulation header. This helps you achieve fairer bandwidth allocation and better prioritization of user data, especially in service provider or large-scale enterprise networks.
Multicast		
Ease of Use	EVPN IRB with distributed anycast gateway	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100, K100]; Modular Systems (8800 [LC ASIC: P100]) The feature enables multicast forwarding in EVPN IRB deployments that use a distributed anycast gateway. Provider Edge (PE) routers use a shared BVI address to operate as local gateways for the same subnet. This shared address allows each router to route and bridge traffic locally.
Ease of Use	EVPN Layer 2 multicast	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Modular Systems (8800 [LC ASIC: P100]) The feature enables Layer 2 multicast forwarding across an EVPN network by extending multicast services into the existing EVPN framework. It builds on EVPN signaling to deliver efficient multicast distribution, reduce unnecessary replication, and improve scalability across the EVPN core.

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
NetFlow and sFlow		
Software reliability	DSCP support for mirroring of forward-drop packets through sflow	Introduced in this release on: Modular Systems (8800 [LC ASIC: P100]) You can now configure the DSCP value as part of the flow exporter configuration. The DSCP value is set using the **dscp** command in the flow exporter-map configuration. This allows marking of packets during export, including forwarded or dropped packets through sFlow. This feature helps in traffic management and monitoring capabilities.
Programmability		
API Experience	gNOI RemoveContainer RPC	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]) We have introduced support for RemoveContainer RPC to give you direct, automated control over the removal of application containers managed by App Manager, allowing you to efficiently decommission unneeded or malfunctioning containers and maintain a clean, resource-optimized system.
API Experience	Multiple gRPC servers	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]) You can now address diverse operational requirements and overcome the single-server limitation. The re-architected Extensible Manageability Services Daemon (EMSd) now supports multiple gRPC servers within a single process. This enables granular control and isolation. Each server can be independently configured with distinct settings for parameters that include listening ports, TLS profiles, network instances (VRFs), and DSCP values. Use this enhancement to support both OpenConfig and proprietary gRPC services.
Software Reliability	gRPC Network Packet Sampling Interface	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]) gNPSI offers more reliable and secure flow data transport by replacing traditional UDP with encrypted, authenticated gRPC connections, reducing packet loss and simplifying secure deployments. gNPSI uses gRPC to transmit flow data between routers and controllers. After you configure NetFlow or sFlow with gNPSI settings, the export process of the router starts and waits for a streaming request from a controller. Flow data is securely streamed using gNPSI once a connection is established.
Software Reliability	TCG-compliant TPM, ECC P384, and PCR 0-8 based enrollment and attestation	Introduced in this release on: Modular Systems (8800 [LC ASIC: Q100, Q200, P100]) Strengthen device security and trust for enrollz and attestz by leveraging a TCG-compliant Trusted Platform Module (TPM) with upgraded ECC P-384 cryptographic key pairs for SUDI/IdevID and IAK, replacing legacy RSA. This enhancement enables hardware-rooted device identity, supports secure TLS 1.3 communication,

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		and utilizes TPM PCR 0-8 measurements to anchor attestation in early boot stages. Together, these capabilities ensure robust, standards-based onboarding and attestation workflows, with seamless AIKIDO fallback for resilient and trusted operations even if TPM is unavailable.
Ease of use	Transceiver optics resets	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]) Remote transceiver optics reset using gNOI Reboot RPC enables rapid, automated recovery of optical modules, reducing manual intervention and improving network uptime. This feature allows remote power-cycling of optics modules with a single API call or CLI command, helping maintain optimal performance and quickly resolve faults at scale.
Software Reliability	gRIBI default route resolution without recirculation	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]) You can now resolve gRIBI default routes in VRF without using recirculation, eliminating extra internal traffic that reduces available bandwidth during route lookups. The router marks next-hop addresses and actions at route programming, ensuring clear routing decisions with minimal memory usage and no effect on performance. You configure the router dynamically using controllers instead of relying on static settings, which provides greater flexibility.
Routing		
Ease of use	IS-IS auto-cost reference bandwidth	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]) The IS-IS auto-cost reference bandwidth feature automates IS-IS metric provisioning based on physical link bandwidth, optimizing path selection and reducing operational overhead. This feature allows you to configure a reference bandwidth, which IS-IS then uses to automatically calculate interface metrics. It also dynamically adjusts metrics for bundle interfaces when member links change, ensuring accurate and efficient routing without manual intervention.
Software Reliability	Share ECMP group between IPv4 and IPv6 routes based on RFC RFC5549	Introduced in this release on: Modular Systems (8800 [ASIC: Q200]) The load-balancing objects (representing ECMP groups) are shared across IPv4 and IPv6 routes and this helps in saving hardware resources and improving convergence. This stack uses IP BGP prefixes without any encapsulation where BGP next hops are directly connected.
Segment Routing		
Ease of Use	EVPNv6 ELAN single-	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Modular Systems

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
	homing	(8800 [LC ASIC: P100]) EVPNv6 ELAN single-homing provides seamless multipoint-to-multipoint Layer 2 connectivity, enabling efficient communication between multiple customer sites or data centers. This solution delivers a cost-effective and simplified approach for connecting sites within the same service provider network using EVPN single-homing mode.
Setup and Upgrade		
Software reliability	Transactionality for release upgrades and downgrades	Introduced in this release on:Fixed Systems(8200 [ASIC: Q200]);Centralized Systems (8600 [ASIC: Q200]);Modular Systems (8800 [LC ASIC: Q200]) This feature ensures reliable rollback and system recovery by enabling a robust transactionality capability to release upgrade and downgrade operations thus allowing to rollback to the original software version if the upgrade to a new software fails. This feature, which was removed in Cisco IOS XR Release 25.2.1 as part of the caveats associated with the disk encryption feature is supported again from this release. This feature is supported only in a reimage operation where both the original image and the target image support transactionality.
System Monitoring		
Software reliability	Insecure features warning syslog messages	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]) Cisco IOS XR software warns you with a syslog message each time you use an insecure command and repeats the warning every 30 days until you remove the command. This helps you identify potential security risks and suggests safer alternatives to improve your network security. Cisco will systematically deprecate and eventually remove these insecure features and protocols in future IOS XR releases. For more information on insecure commands and their alternatives, see Feature deprecation phasing out insecure capabilities.
Hardware Reliability	Lookup engine test in data plane health check utility	Introduced in this release on: Fixed Systems (8200 [ASIC: Q100, Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100])(select variants only*); Centralized Systems (8600 [ASIC:Q200]) ; Modular Systems (8800 [LC ASIC: Q100, Q200, P100])(select variants only*) This feature detects mis-routed packets due to hardware defects causing bit corruption in route prefix lookups. This feature implements a new lookup engine test mode in the data plane health check utility to detect such mis-routed packets. This test requires a router reload upon completion.
Ease of Use	Port rate histogram	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200, P100](select variants only*); Centralized Systems (8600 [ASIC:Q200])(select variants only*); Modular Systems (8800 [LC

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		ASIC: Q200, P100])(select variants only*) Port rate histogram view enables rapid detection of network performance issues by providing detailed, real-time port utilization analysis. The feature displays port traffic rates in a histogram, breaking down data into specific time intervals and utilization bins. Data is collected and displayed using the CLI, allowing you to monitor and compare all network ports on supported line cards, and detect anomalies and performance issues efficiently. * This feature is supported on: * 8202-32FH-M * 8608-SYS * 88-LC0-36FH * 88-LC0-36FH-M * 88-LC0-34H14FH * 88-LC1-36EH * 88-LC1-12TH24FH-E * 88-LC1-52Y8H-EM
Upgrade	Aggregated drop counters for software packet path node counters	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]) You can use the **show spp node-counters drops** command to view aggregated drop counters for the SPP. This displays a summary of dropped packets at the node level to identify and troubleshoot drop issues efficiently.
System Security		
Ease of Setup	TLS RFC 5289 compliance for security template framework	The security template framework is based on RFC 5289 , which specifies new cipher suites for the Transport Layer Security (TLS) protocol. This feature supports Common Criteria (CC) mode which is an enhanced security mode that enforces stricter compliance-focused behavior. It enhances TLS security by introducing stronger Elliptic Curve Cryptography (ECC) algorithms.
Ease of Setup	Security template framework for TLS enabled applications	Security templates reduce misconfiguration risks and operational overhead by centralizing and standardizing security policy configuration for TLS-enabled applications. A security template bundles certificate authentication policy, TLS controls, and compliance mode settings. It acts as a single source of truth that applications reference, avoiding local embedding of security settings. This template defines how certificates are handled and controls various aspects of the TLS handshake.
Software Reliability	Netconf access controls	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]) When this feature is enabled, NETCONF sessions will be blocked on the SSH port. However, SCP and SFTP will continue to function on the SSH port.
Software Reliability	MACsec capability	Introduced in this release on: Fixed Systems (8010 [ASIC: A100],

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		8700 [ASIC: K100])(select variants only*) *This feature is supported on: * 8011-12G12X4Y-A * 8011-12G12X4Y-D * 8711-48Z-M
Software Reliability	TCG-compliant Trusted Platform Module	Introduced in this release on: Modular Systems (8800 [LC ASIC: Q100, Q200, P100]) Device security and cryptographic identity are enhanced through new support for a TCG-compliant Trusted Platform Module (TPM) with ECC P-384 key pairs. This feature enables TLS 1.3-based secure communication for critical onboarding workflows such as BootZ and sZTP. Enrolment and attestation are strengthened through TPM PCR 0-8 measurements, establishing a hardware-rooted chain of trust from early boot stage.
Timing and Synchronization		
Software Reliability	PTP holdover traceability suppression	Introduced in this release on: 8010 [ASIC: A100])(select variants only*) You can now extend PTP holdover traceability suppression to devices operating as Boundary Clocks (T-BC), Grandmaster Clocks (T-GM), and T-GM with VP/APTS modes. When a device loses synchronization with a quality primary clock, this feature ensures that downstream nodes continue to receive the configured clock class and maintain traceability for a specified duration, enhancing overall network timing reliability. * This feature is supported on: * 8011-12G12X4Y-A * 8011-12G12X4Y-D * 8011-4G24Y4H-I * 8011-32Y8L2H2FH
Software Reliability	Advance monitoring	Introduced in this release on: Fixed Systems (8010 [ASIC: A100])(select variants only*) You can now enhance the detection of network issues, such as clock failures or asymmetries, by using advanced monitoring. This optional extension to the ITU-defined PTP G.8275.1 profile offers additional capabilities for monitoring alternative time transmitter information through the PTP port. *This feature is supported on: * 8011-12G12X4Y-A * 8011-12G12X4Y-D * 8011-4G24Y4H-I * 8011-32Y8L2H2FH
Software Reliability	Isolate Foreign Masters Causing Packet Timing Signal Fail	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 permits the flexible selection of timing sources by filtering out Foreign Master (FM) clocks that exhibit unstable timing. This filtering causes the secondary clocks to produce a signal deemed Packet Timing Signal Fail (PTSF)-unusable, from consideration within the Best Master Clock Algorithm (BMCA). The system continuously monitors these clocks for timing stabilization,

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		and upon detecting enhanced stability, it may reevaluate and possibly reintegrate them as suitable time sources.
Software Reliability	PTP Phase Difference Threshold Between Passive and Secondary Ports	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]) Passive ports can now be included in the Delay Request-Response Mechanism (DRRM), which allows for the monitoring of PTP phase differences between a passive port and a secondary port. If these PTP phase differences surpass a predefined limit, system logs are triggered. This feature enables you to detect potential errors such as fiber asymmetry or a clock failure in the PTP network.
Software Reliability	Synchronous Ethernet ESMC and SSM on Cisco 8711-48Z-M routers	Introduced in this release on: Fixed Systems (8700 [ASIC: K100])(select variants only*) SyncE provides synchronization signals transmitted over the Ethernet physical layer to downstream devices, while the Synchronization Status Message (SSM) indicates the quality level of the transmitting clock to the neighboring nodes, informing the nodes about the level of the network's reliability. Ethernet Synchronization Message Channel (ESMC) is the logical channel that uses an Ethernet PDU (protocol data unit) to exchange SSM information over the SyncE link. Supported SyncE profiles: * G.8262 * G.8264 *This feature is supported on Cisco 8711-48Z-M routers.
Software Reliability	PTP profiles support on Cisco 8711-48Z-M routers	Introduced in this release on: Fixed Systems (8700 [ASIC: K100])(select variants only*) Based on the IEEE 1588-2008 standard, Precision Time Protocol (PTP) is a protocol that defines a method to synchronize clocks in a network for networked measurement and control systems. Supported PTP profiles: * G.8265.1 * G.8273.2 Class C * G.8275.1 * G.8275.2 *This feature is supported on Cisco 8711-48Z-M routers.
Software Reliability	Global Navigation Satellite System (GNSS) support on Cisco 8711-48Z-M routers	Introduced in this release on: Fixed Systems (8700 [ASIC: K100])(select variants only*) Global Navigation Satellite System (GNSS) is a satellite system used as a timing interface. GNSS receiver receives signals from GNSS satellites and decodes the information from multiple satellites to determine its distance from each satellite. Based on this data, the GNSS receiver identifies the location of each satellite. The supported GNSS class is PRTC-B. *This feature is supported on Cisco 8711-48Z-M routers.
Software Reliability	Synchronous Ethernet ESMC and SSM on 8011-	SyncE provides synchronization signals transmitted over the Ethernet physical layer to downstream devices, while the

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
	12G12X4Y-D and 8011-12G12X4Y-A	Synchronization Status Message (SSM) indicates the quality level of the transmitting clock to the neighboring nodes, informing the nodes about the level of the network's reliability. Ethernet Synchronization Message Channel (ESMC) is the logical channel that uses an Ethernet PDU (protocol data unit) to exchange SSM information over the SyncE link. G.8262 and G.8264 synchronous ethernet ESMC and SSM are now supported on: * 8011-12G12X4Y-D * 8011-12G12X4Y-A
Software Reliability	PTP profiles support on 8011-12G12X4Y-D and 8011-12G12X4Y-A	Based on the IEEE 1588-2008 standard, Precision Time Protocol (PTP) is a protocol that defines a method to synchronize clocks in a network for networked measurement and control systems. G.8265.1, G.8275.1, G.8275.2, and G.8273.2 (Class C) PTP profiles are now supported on the following Cisco 8000 Series router variant: * 8011-12G12X4Y-D * 8011-12G12X4Y-A
Upgrade	Synchronous Ethernet (SyncE) support on Cisco 8011-32Y8L2H2FH routers	Introduced in this release on: Fixed Systems (8010 [ASIC: A100]) (select variants only*) SyncE provides synchronization signals transmitted over the Ethernet physical layer to downstream devices, while the Synchronization Status Message (SSM) indicates the quality level of the transmitting clock to the neighboring nodes, informing the nodes about the level of the network's reliability. Ethernet Synchronization Message Channel (ESMC) is the logical channel that uses an Ethernet PDU (protocol data unit) to exchange SSM information over the SyncE link. With this release, the Cisco 8011-32Y8L2H2FH router supports these SyncE ITU-T profiles: * G.8262 – Enables synchronous ethernet clock support. * G.8264 – Ensures high-quality timing and synchronization, particularly in the context of Ethernet networks. *This feature is supported on 8011-32Y8L2H2FH.
Upgrade	PTP on Cisco 8011-32Y8L2H2FH routers	Introduced in this release on: Fixed Systems (8010 [ASIC: A100]) (select variants only*) Based on the IEEE 1588-2008 standard, Precision Time Protocol (PTP) is a protocol that defines a method to synchronize clocks in a network for networked measurement and control systems. With this release, Cisco 8011-32Y8L2H2FH router supports these PTP telecom profiles: * G.8265.1 * G.8273.2 * G.8275.1 * G.8275.2 *This feature is supported on 8011-32Y8L2H2FH.
Upgrade	Global Navigation Satellite System (GNSS) support on Cisco 8011-32Y8L2H2FH routers	Introduced in this release on: Fixed Systems (8010 [ASIC: A100]) (select variants only*) Global Navigation Satellite System (GNSS) is a satellite system used as a timing interface. GNSS receiver receives signals from

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		GNSS satellites and decodes the information from multiple satellites to determine its distance from each satellite. Based on this data, the GNSS receiver identifies the location of each satellite. *This feature is supported on 8011-32Y8L2H2FH.
Traffic Mirroring		
Ease of Use	Selective packet capture for protocol and drops	Selective packet capture provides greater control over mirrored traffic by enabling the filtering and capture of specific dropped packets and protocol packets. By applying filters during the configuration of a monitor session, you can optimize SPAN packet capture to improve network troubleshooting. These filters reduce the volume of captured data, ensuring attention is focused on the most relevant packets.

New hardware

Table 2. New hardware for Cisco 8000 Series Routers, Release 25.4.1

Hardware	Description
8711-48Z-M	The Cisco 8711-48Z-M is a K100 silicon chip-based router that provides 5.6 Tbps of network bandwidth. The Cisco 8711-48Z-M is a fixed-port, high density, one rack-unit form factor router. The Cisco 8711-48Z-M supports QSFP-DD 400GbE, QSFP 200GbE, and SFP56 ports.
8011-12G12X4Y-A 8011-12G12X4Y-D	The Cisco 8011-12G12X4Y-A and 8011-12G12X4Y-D are A100 silicon chip-based routers that provide 244 Gbps of network bandwidth. The Cisco 8011-12G12X4Y-A and 8011-12G12X4Y-D are fixed-port, medium-density, one rack-unit form factor routers. The Cisco 8011-12G12X4Y-A and 8011-12G12X4Y-D support 1/10/25G SFP28, 1/10G SFP10, and 1G cSFP ports.
8011-32Y8L2H2FH	The Cisco 8011-32Y8L2H2FH is an A100 silicon chip-based router that provides 1.6 Tbps of network bandwidth. The Cisco 8011-32Y8L2H2FH is a fixed-port, one rack-unit form factor router. The Cisco 8011-32Y8L2H2FH supports 400G QSFP-DD, 100G QSFP28, 10/25/50G SFP56, and 1/10/25G SFP28 ports.
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 QSFP28 100G ZR modules * DP01QS28-E20 * DP01QS28-E25 Cisco 25GBASE SFP28 (Small Form-Factor Pluggable) * SFP-25G-SR-S

Changes in behavior

- **Deprecation and phasing out features with insecure capabilities and its secure alternatives**
  From Release 25.4.1, Cisco IOS XR software displays warning messages when you configure features or protocols that lack sufficient security, such as those that transmit sensitive data without encryption or use outdated encryption mechanisms. The software also shows warnings when you do

© 2025 Cisco and/or its affiliates. All rights reserved.

not follow security best practices, and it provides suggestions for secure alternatives.

This list may change, but Cisco plans to generate warnings for the following features and protocols from Release 25.4.1. Each Release Notes will describe the exact changes for that version. These documents list all features planned for removal, including insecure commands, and provide recommended secure alternatives to help you maintain network security and compliance.

- **Feature deprecation phasing out insecure capabilities**
- **Feature deprecation and removal details**
- **Feature removal and suggested alternatives**

Table 3. Deprecation and phasing out features with insecure capabilities and its secure alternatives

If you are using the following insecure features...	Then follow these secure alternatives...
HTTP	Use HTTPS.
FTP client install FTP install TFTP	Use SFTP.
IPV4 source route	There is no alternative. Do not enable IPv4 source routing.
Telnet client Telnet dscp	There is no alternative. Do not use Telnet client.
Telnet server	Use SSH.
TFTP client	Use SFTP.
TFTP server	Use SSH.
copy ftp copy ftp running-config copy running-config ftp copy running-config tftp copy tftp copy tftp running-config copy xml-schema tftp	Use SFTP or SCP.
install FTP install TFTP	Use SFTP.
TCP or UDP small_servers	There is no alternative. Do not use TCP or UDP small_servers.
SSHv1	Use ssh server v2.
SSH host-key DSA algorithm	Use ECDSA, ED25519, or RSA and so on.
Syslog TLS Version 1.1 (server1)	Configure TLS Version 1.2 or higher.
TLS 1.0 TLS 1.1	Use TLS 1.2 or TLS 1.3.

© 2025 Cisco and/or its affiliates. All rights reserved.

If you are using the following insecure features...	Then follow these secure alternatives...
utility mv ftp utility mv tftp	There is no alternative. Do not use utility mv ftp and utility mv tftp.
load ftp load tftp load script ftp load script tftp load diff ftp load diff tftp load diff reverse ftp load diff reverse tftp	Use scp or sftp.
tacacs and radius server with type-7 shared secret	Use type 6 secret.
NTPv2 NTPv3	Use NTPv4.

Open issues

Table 4. Open issues for Cisco 8000 Series Routers, Release 25.4.1

Bug ID	Description
CSCwr84474	Bundle between 8000 and DNX goes down with BFD state error after removing and adding the bundle when ERSPAN rate limit is set.
CSCwq77382	Suppressing info messages in TPM Core Infra from STO.

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 5. Compatibility matrix for Cisco 8000 Series Routers, Release 25.4.1

Cisco IOS XR	Crosswork	EPNM
Release 25.4.1	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
Matrix: XR version: 25.4.1, File version: 1.0, Version: N/A
```

© 2025 Cisco and/or its affiliates. All rights reserved.

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

From       To         Restrictions
---------- ---------- ----------------------------------------------------
25.4.1     24.1.2     Target fixes; Caveats; Replace performed via reimage
25.4.1     24.2.2     Target fixes; Caveats; Replace performed via reimage
25.4.1     24.2.20    Caveats; Replace performed via reimage
25.4.1     24.2.203   Caveats; Replace performed via reimage
25.4.1     24.2.204   Caveats; Replace performed via reimage
25.4.1     24.2.206   Caveats; Replace performed via reimage
25.4.1     24.2.207   Caveats; Replace performed via reimage
25.4.1     24.2.21    Caveats; Replace performed via reimage
25.4.1     24.3.2     Target fixes; Caveats; Replace performed via reimage
25.4.1     24.3.20    Caveats; Replace performed via reimage
25.4.1     24.3.30    Caveats; Replace performed via reimage
25.4.1     24.4.1     Caveats; Replace performed via reimage
25.4.1     24.4.2     Caveats; Replace performed via reimage
25.4.1     25.1.1     Caveats; Replace performed via reimage
25.4.1     25.1.2     Caveats; Replace performed via reimage
25.4.1     25.1.30    Caveats; Replace performed via reimage
25.4.1     25.2.1     Caveats; Replace performed via reimage
25.4.1     25.2.15    Caveats; Replace performed via reimage
25.4.1     25.2.16    Caveats; Replace performed via reimage
25.4.1     25.2.17    Caveats; Replace performed via reimage
25.4.1     25.2.18    Caveats; Replace performed via reimage
25.4.1     25.2.2     Caveats; Replace performed via reimage
25.4.1     25.3.1     Caveats; Replace performed via reimage
25.4.1     7.10.2     Target fixes; Caveats; Replace performed via reimage
25.4.1     7.11.2     Target fixes; Caveats; Replace performed via reimage
25.4.1     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 25.4.1->24.1.2 upgrade, use
        'show install upgrade-matrix running 25.4.1 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 25.4.1 LNT
```

© 2025 Cisco and/or its affiliates. All rights reserved.

```
Copyright (c) 2013-2025 by Cisco Systems, Inc.

Build Information:
 Built By     : swtools
 Built On     : Wed Dec 17 09:40:58 UTC 2025
 Build Host   : iox-lnx-005
 Workspace    : /auto/srcarchive12/prod/25.4.1/8000/ws
 Version      : 25.4.1
 Label        : 25.4.1

cisco 8000 (Intel(R) Xeon(R) CPU D-1530 @ 2.40GHz)
cisco 8201-32FH (Intel(R) Xeon(R) CPU D-1530 @ 2.40GHz) processor with 32GB of memory
PE6-8201-Churchil uptime is 29 minutes
Cisco 8000 Series 32x400G QSFPDD 1RU Fixed System w/HBM
```

Supported hardware

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

Table 6. 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 7. Supported hardware for Cisco 8200 Series Routers

© 2025 Cisco and/or its affiliates. All rights reserved.

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
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 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
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

© 2025 Cisco and/or its affiliates. All rights reserved.

Part Number	Description	Support Initially Provided in IOS XR Release
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
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

© 2025 Cisco and/or its affiliates. All rights reserved.

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
8804-FC1	Cisco 8804 System Fabric Module - F100-based fabric modules with 28.8T per LC slot	Release 25.1.1
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

© 2025 Cisco and/or its affiliates. All rights reserved.

Part Number	Description	Support Initially Provided in IOS XR Release
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.

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

© 2025 Cisco and/or its affiliates. All rights reserved.

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.
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.

© 2025 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.

© 2025 Cisco Systems, Inc. All rights reserved.