Release Notes for Cisco 8000 Series Routers, IOS XR Release 26.2.1

Cisco 8000 Series Routers, IOS XR Release 26.2.1 3
New software features 3
New hardware 16
Changes in behavior 16
Resolved issues 19
Open issues 19
Known issues 19
Compatibility 19
Supported hardware 21
Supported software packages 26
Related resources 26
Legal information 28

Cisco 8000 Series Routers, IOS XR Release 26.2.1

Cisco IOS XR Release 26.2.1 for the 8000 Series Routers introduces comprehensive enhancements across hardware reliability, software scalability, and network security. Key architectural improvements include slice-aware prefix programming for Egress-Object-Group ACLs, 24-bit bincode support, and expanded QoS capabilities such as BVI two-pass processing, configurable burst values, and egress queuing on Layer 2 sub-interfaces. Routing and programmability are optimized through asynchronous PBR, BGP hardware-acknowledged route advertisement, SRv6 Flow Label entropy via source address, and AFT state-synced flags in OpenConfig. Security is significantly hardened with FIDO2 authentication for SSH, hybrid Post-Quantum Cryptography key exchange, MACsec state reflection, and URPF source validation using VRF tables. The release further expands hardware support for QDD OLS and DP04QSDD-ULH-A1 modules, simplifies multicast deployments with Global Table Multicast, and streamlines operations through GUEv6, sFlow support for PBR, and the deprecation of legacy insecure protocols and health check metrics.

For more details on the Cisco IOS XR release model and associated support, see Software Lifecycle Support Statement - IOS XR.

New software features

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

Table 1. New software features for Cisco 8000 Series Routers, Release 26.2.1

Product impact	Feature	Description
BGP		
Software Reliability	BGP RPKI-based origin validation on inbound iBGP prefixes	You can now enhance internal routing security by validating iBGP-learned routes against RPKI origin-AS data. The feature accepts only routes with valid or not-found ROA status and drops invalid ones, preventing propagation of unauthorized prefixes within your network.
Software Reliability	BGP RPKI-based origin validation for outbound eBGP prefixes	You can now prevent propagation of unauthorized routes, reduce manual filtering errors, and strengthens routing security. by validating prefix origin-AS against the local RPKI ROA database before advertising routes to external BGP peers. You apply a route-policy with the drop-post-policy-if-RPKI-invalid keyword to automatically drop prefixes with invalid ROA status.
IP Addresses and Services		
Software Reliability	Slice-aware Prefix Programming for Egress-Object-Group ACLs	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]) This feature enhances hardware efficiency by programming Egress Object-Group ACL (OG-ACL) prefixes only on the active slices where an ACL is applied, rather than replicating them across all slices. Previously, prefixes were duplicated on every slice, leading to higher TCAM and HCAM usage and reduced performance. The software now automatically identifies, and programs prefixes only for relevant slices, dynamically replicating them when new interfaces or bundle members are added. This optimization increases scalability for other hardware-based applications,

Product impact	Feature	Description
		supports both IPv4 and IPv6 OG-ACLs, and requires no additional configuration.
Ease of setup	Extend support for ACLs on BVI to A100-based ASICs	Introduced in this release on: Fixed Systems (8010 [ASIC: A100]) (select variants only*) You can now apply ACLs on Bridged Virtual Interfaces (BVIs) on A100-based ASICs. 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. *This feature support is now extended to: • 8011-32Y8L2H2FH • 8011-12G12X4Y-A/D • 8011-4G24Y4H-A
Software Reliability	TCP MSS adjustment	Introduced in this release on: Fixed Systems (8200, 8700, 8010) (select variants only*), Modular Systems (8800 [LC ASIC: P100]) (select variants only*) You can now prevent packet fragmentation and ensure TCP segments remain within the interface MTU by using TCP MSS adjustment. This feature modifies the Maximum Segment Size on transit IPv4 and IPv6 TCP SYN and TCP SYN-ACK packets. This helps ensure optimal traffic flow during session establishment. *This feature is now supported on: Line cards: • 88-LC1-36EH • 88-LC1-12TH24FH-E • 88-LC1-52Y8H-EM Fixed systems: • 8212-48FH-M • 8011-4G24Y4H-I • 8011-32Y8L2H2FH • 8011-24Y8L2FH-I • 8011-24X • 8011-12G12X4Y • 8711-32FH-M • 8711-48Z-M • 8712-MOD-M
Software Reliability	24 bit bincode support for egress object-group ACLs	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100]), 8010 [ASIC: A100]; Modular Systems (8800 [LC ASIC: P100]) You can now improve network policy granularity and control by supporting 24-bit bincode sizes for egress object-group ACLs. This enhancement improves the efficiency of handling extended network object-groups and supports the inclusion of larger, more detailed prefix lists.
Software Reliability	Configurable trap policers	Introduced in this release on: Fixed Systems (8200, 8700); Centralized Systems (8600); Modular Systems (8800 [LC ASIC: Q200, P100])

Product impact	Feature	Description
		Configurable trap policers give you precise control over control-plane traffic by allowing per-trap rate limiting and average packet size tuning. This flexibility helps prevent unnecessary packet drops, improves traffic handling, and enables efficient scaling across diverse deployment scenarios.
Interface and Hardware Component		
Software Reliability	DWDM-SFP10G-E-I tunable optics for Cisco 8711-48Z-M router	Introduced in this release on: Fixed Systems (8700 [ASIC: K100]) This feature enables full DWDM channel tuning capability for the DWDM-SFP10G-E-I optics on Cisco 8711-48Z-M, allowing operation up to 196.3 THz and ensuring proper integration with your optical transport infrastructure.
Software Reliability	Network Virtualization Generic Routing Encapsulation (NVGRE) hash field selections	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200]; Centralized Systems (8600 [ASIC: Q200]; Modular Systems (8800 [LC ASIC: Q200, Q100]) You can now improve load balancing for Network Virtualization using Generic Routing Encapsulation (NVGRE) traffic by excluding the NVGRE payload from the hash calculation. This feature optimizes traffic distribution across multiple paths, preventing uneven load caused by hashing on the NVGRE payload. The feature works by modifying the Cisco Express Forwarding (CEF) load-balancing hash algorithm to exclude the NVGRE payload field. This adjustment ensures that the hash calculation uses only relevant header fields, leading to better traffic distribution and network performance.
Software Reliability	Support for DP04QSDD-LLH-A1 optical module	This release introduces support for the Cisco 400G QSFP-DD Ultra Long-Haul (ULH) L-band coherent optical module on these line cards and routers: • 88-LC1-36EH • 88-LC1-52Y8H-EM • 88-LC1-12TH24FH-E • Cisco 8212-48FH-M • Cisco 8202-32FH-M • Cisco 8608-SYS • Cisco 8201-24H8FH • Cisco 8201-32FH
Ease of Use	Generic UDP Encapsulation for IPv6 Traffic	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200]); Centralized Systems (8600 [ASIC: Q200]); Modular Systems (8800 [LC ASIC: Q200]) This release introduces support for Generic UDP Encapsulation (GUE) tunnels operating over IPv6 underlays (GUEv6). With this feature, you can enable the highly efficient, scalable, and secure deployment of Generic UDP Encapsulation variant 1 (GUEv1) static tunnels to carry IPv4 and IPv6 traffic over IPv6 networks.
Software Reliability	Extend support for BVI and IRB infrastructure to A100-based ASICs.	Introduced in this release on: Fixed Systems (8010 [ASIC: A100]) We have enabled support for Bridge-Group Virtual Interface (BVI) and Integrated Routing and Bridging (IRB) infrastructure on A100-

Product impact	Feature	Description
		based routers. This functionality is now available on these routers: • 8011-4G24Y4H-I • 8011-32Y8L2H2FH • 8011-12G12X4Y-D/A
Software Reliability	Link flap err-disables	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: K100)] You can achieve reliable network performance and a stable system state by isolating unstable interfaces that flap excessively, preventing routing protocol disruptions and ensuring effective workload failover. With this feature, the system monitors link transitions and automatically moves physical, breakout, or bundle member interfaces into an error-disabled state if a defined flap-count threshold is breached within a specific time window. This automated mechanism guarantees traffic redirection to stable paths while providing the flexibility of manual restoration or a timer-based automatic recovery once the link stabilizes.
Hardware Reliability	QDD OLS support	Introduced in this release on: Fixed Systems (8010 ASIC: A100 The QDD Optical Line System (OLS) pluggable optical amplifier is now supported on these ports. *This feature is supported on: • Cisco 8011-4G24Y4H-I
Software Reliability	Support for DP04QSDD-ULH-A1 optical module	Introduced in this release on: Modular Systems (8800 [LC ASIC: Q200]) This release introduces support for the Cisco 400G QSFP-DD Ultra Long-Haul (ULH) coherent optical module on these line cards: • 88-LC0-36FH • 88-LC0-36FH-M The 400G QSFP-DD ULH optics are supported on even-numbered ports only. The supported port numbers are: 0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34.
Software Reliability	Support for DP04QSDD-ULH-A1 optical module	This release introduces support for the Cisco 400G QSFP-DD Ultra Long-Haul (ULH) C-band coherent optical module on these line cards and routers: • 88-LC1-36EH • 88-LC1-52Y8H-EM • 88-LC1-12TH24FH-E • Cisco 8212-48FH-M • Cisco 8202-32FH-M • Cisco 8201-24H8FH • Cisco 8201-32FH
L3VPN		

Product impact	Feature	Description
Ease of setup	Extend support for BVI in L3VPN over SRv6	Introduced in this release on: Fixed Systems (8010 [ASIC: A100]) (select variants only*) *This feature support is supported on: • 8011-32Y8L2H2FH • 8011-12G12X4Y-A/D • 8011-4G24Y4H-I
Licensing		
Licensing process	Support for Smart Licensing Using Policy	Introduced in this release on: Modular Systems (8800 [LC 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. *Support for Smart Licensing Using Policy is now extended to 88-LC1-48Y8H-EM.
MPLS		
API experience	Regular expressions in MPLS-TE tunnel names	Introduced in this release on: Fixed Systems(8200 [ASIC: 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 enhances operational scalability and usability by allowing regex-based tunnel name filtering for MPLS-TE show and execution commands, without changing configuration models, architecture, or security posture. This feature supports regular expression in all MPLS-TE show and execution commands using tunnel names.
Multicast		
Ease of Use	Global table multicast	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: Q100, Q200, P100]) Global Table Multicast (GTM) simplifies multicast deployments by allowing Next-Generation Multicast VPN (NG-mVPN) profiles to operate directly within the global routing table with the default VRF on PE routers. Service providers can now transport multicast traffic in a global context without creating dedicated VRFs, while still using NG-mVPN for signaling and transport. Previously, NG-mVPN required deployment within a VRF, which added configuration overhead for multicast services.
Netflow		
Software Reliability	sFlow support for policy-based routing (PBR) IP-in-IP tunnel traffic	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: K100)]

Product impact	Feature	Description
		sFlow now supports policy-based routing (PBR) IP-in-IP tunnel traffic, providing enhanced visibility into tunneled and decapsulated flows. The feature enables sampling, export, and reporting of both inner and outer packet headers while preserving platform and forwarding context, allowing more accurate flow records and improved traffic monitoring and load-balancing decisions.
Upgrade	Flow monitoring on egress interface	Introduced in this release on: Fixed Systems (8700 [ASIC: K100]) (select variants only*) This feature requires Egress Feature Capability (EFC) on supported platforms. Use the hw-module profile edge-mode CLI command to enable the EFC feature. The feature introduces these changes: CLI: • hw-module profile edge-mode • show hw-module profile edge-mode *This feature is now supported on: • 8711-48Z-M • 8712-MOD-M
Software Reliability	Increased sampling interval support for NetFlow and sFlow	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: K100)] You can now significantly reduce analytics and collector load by setting much higher NetFlow or sFlow sampling intervals by up to 8 million packets. Just configure your desired interval, and we automatically combine hardware sampling and software filtering to achieve this rate, ensuring accurate exports and minimal resource usage while keeping setup simple.
Programmability		
Software Reliability	AFT state-synced flag in OpenConfig	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: K100)] You can now monitor forwarding state convergence with the AFT state-synced flag in OpenConfig, which provides per-VRF visibility into when FIB entries have fully synchronized with INSIGHT. The flag is set to TRUE once synchronization completes for a VRF and remains TRUE until a new synchronization event occurs or the VRF is removed, enabling automated monitoring and validation through OpenConfig telemetry or CLI.
QoS		
Upgrade	Configurable burst values for QoS policers	Introduced in this release on: Fixed Systems (8200 [ASIC: P100, A100], 8700 [ASIC: P100, K100]); Centralized Systems (8400 [ASIC: K100]); Modular Systems (8800 [LC ASIC: P100]) You can now configure conform and exceed burst values for 1R2C and 2R3C QoS policers instead of relying on platform-calculated default burst values. This capability provides finer control over

Product impact	Feature	Description
		burst tolerance and traffic policing behavior enabling granular control of traffic differentiation.
Upgrade	Egress queuing on L2 subinterfaces	Introduced in this release on: Fixed Systems (8700 [ASIC: K100], 8010 [ASIC: A100]); Centralized Systems (8400 [ASIC: K100])(select variants only*) You can now apply egress queuing policies on Layer 2 subinterfaces to allocate dedicated VOQs for subinterface traffic. This enhancement enables independent traffic management for Layer 2 and Layer 3 services that share the same physical or bundle interface. This capability provides more granular bandwidth control for multi-customer services, such as such as cloud, content-provider, VPWS, and so on. This release also adds child-level shaping support for Layer 2 subinterface queuing. *This feature is supported on 8404-SYS-D.
Upgrade	Multicast traffic scheduling on egress queues	Introduced in this release on: Fixed Systems (8700 [ASIC: K100]) (select variants only*) This feature requires Egress Feature Capability (EFC) on supported platforms. Use the hw-module profile edge-mode CLI command to enable the EFC feature. The feature introduces these changes: CLI: • hw-module profile edge-mode • show hw-module profile edge-mode *This feature is now supported on: • 8711-48Z-M • 8712-MOD-M
Upgrade	QoS on PWHE	Introduced in this release on: Fixed Systems (8700 [ASIC: K100]) (select variants only*) This feature requires Egress Feature Capability (EFC) on supported platforms. Use the hw-module profile edge-mode CLI command to enable the EFC feature. The feature introduces these changes: CLI: • hw-module profile edge-mode • show hw-module profile edge-mode *This feature is now supported on: • 8711-48Z-M • 8712-MOD-M
Upgrade	Increased class-map scale for egress QoS policies	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])

Product impact	Feature	Description
		Now you can configure up to 16 class maps per egress QoS policy instead of the earlier limit of 8, giving you more granular control over outbound traffic classification and marking.
Ease of Use	VOQ CGM profile prefitting	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100]; Modular Systems (8800 [LC ASIC: P100]) Now you can use a unified VOQ CGM profile allocation model improving interoperability between K100 and P100 line cards for QL, DQL, and RED configurations. This feature introduces the prefit model for P100 line cards, maps QL configurations to reserved prefit profiles, and provides 12 dedicated custom profiles for DQL and RED.
Upgrade	Egress feature capability	Introduced in this release on: Fixed Systems (8700 [ASIC: K100]) (select variants only*) You can now enable Egress Feature Capability (EFC) on supported platforms to expand support for egress traffic management features. EFC uses an egress processing path to enable capabilities such as egress queuing, egress policing, and multicast QoS scheduling. The feature introduces these changes: CLI: • hw-module profile edge-mode • show hw-module profile edge-mode *This feature is now supported on: • 8711-48Z-M • 8712-MOD-M
Upgrade	Bridged Virtual Interface two-pass QoS	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100]; Modular Systems (8800 [LC ASIC: P100]) You can now apply ingress policing and egress QoS policies on BVI interfaces. The feature extends QoS processing beyond ingress classification and marking and preserves QoS metadata across BVI recycle operations for consistent traffic treatment throughout the forwarding pipeline.
Routing		
Software Reliability	VRF-specific BFD multipath location assignment	This feature allows you to pin BFD MP sessions to specific LCs by associating a destination IP and VRF with a physical location. When configured, the system automatically migrates matching sessions to the designated LC. This prevents collateral service disruption for unrelated tenants by ensuring that an LC reload only impacts sessions pinned to that specific hardware.
Software Reliability	BGP RPKI-based origin validation on inbound iBGP prefixes	You can now enhance internal routing security by validating iBGP-learned routes against RPKI origin-AS data. The feature accepts only routes with valid or not-found ROA status and drops invalid ones, preventing propagation of unauthorized prefixes within your network.
Upgrade	BFD over pseudowire	Introduced in this release on: Fixed Systems (8700 [ASIC: K100])

Product impact	Feature	Description
	headend	(select variants only*) This feature requires Egress Feature Capability (EFC) on supported platforms. Use the hw-module profile edge-mode CLI command to enable the EFC feature. The feature introduces these changes: CLI: • hw-module profile edge-mode • show hw-module profile edge-mode *This feature is now supported on: • 8711-48Z-M • 8712-MOD-M
Software Reliability	BGP RPKI-based origin validation for outbound eBGP prefixes	You can now prevent propagation of unauthorized routes, reduces manual filtering errors, and strengthens routing security. by validating prefix origin-AS against the local RPKI ROA database before advertising routes to external BGP peers. You apply a route-policy with the drop-post-policy-if-RPKI-invalid keyword to automatically drop prefixes with invalid ROA status.
Software Reliability	BGP hardware-acknowledged route advertisement	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: K100)] This feature delays BGP route advertisement until routes are confirmed programmed in hardware, preventing traffic loss from premature advertising. It uses synchronization markers and hardware acknowledgments to ensure routes are only advertised after hardware installation, enhancing network stability and performance with minimal manual intervention.
Ease of Use	Fast Reroute recirculation avoidance	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200]); Centralized Systems (8600 [ASIC: Q200]); Modular Systems (8800 [LC ASIC: Q200]) You can now eliminate packet recirculation during Fast Reroute (FRR) events in PE routers. The feature ensures that traffic switches to backup paths without requiring recycle operations during both first and subsequent FRR events. Previously, traffic switched to backup paths during FRR events that required one or more recycle passes, increasing bandwidth and reducing efficiency.
Ease of Use	PBR asynchronous HW-ACK over SL-API	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200, P100], 8700 [ASIC: P100]); Centralized Systems (8600 [ASIC: Q200]); Modular Systems (8800 [LC ASIC: Q200, P100]) This feature improves the reliability of PBR readiness signaling over SL-API. The router now returns a fast Sync-Ack for request acceptance and a separate asynchronous HW-ACK after it programs the NHG in hardware. This change helps the controller send traffic only after the NHG is ready. The enhancement allows PBR policies to be programmed in the background without blocking the controller.
Ease of setup	Extend support for bidirectional forwarding detection on BVI to A100-	Introduced in this release on: Fixed Systems (8010 [ASIC: A100]) You can now extend the advantage of BFD low-overhead and

Product impact	Feature	Description
	based ASICs	short-duration path failure detection to an IRB deployment by configuring BFD on multi-path single-hop sessions using a BVI.
Segment Routing		
Software Reliability	One-Way IP measurement with 3L monitoring and hardware offload	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]) The one-way IP Measurement probe utilizes hardware offload to provide high-performance ECMP path monitoring while eliminating return path exposure. It integrates automated path discovery with 3L monitoring, delivering 20ns latency accuracy, alternate marking for loss, and 2ms liveness detection. The primary advantage is the ability to achieve granular, real-time visibility across large-scale environments without the complexity of bidirectional traffic. This enhancement ensures superior network reliability and faster troubleshooting by accurately measuring performance across all discovered ECMP paths.
Ease of Use	SRv6 Flow Label entropy via source address	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8400 [ASIC: K100]); Modular Systems (8800 [LC ASIC: P100]) You can now improve SRv6 load balancing by encoding entropy from the IPv6 Flow Label into the IPv6 source address during SRv6 encapsulation. The ingress node generates a flow-aware source address. This allows downstream devices to use standard IP-based hashing for consistent ECMP load balancing. With this feature, devices use the modified source address for hashing so effective end-to-end load balancing occurs, even when the flow label is not considered. Previously, SRv6 relied on Flow Label-based entropy for load balancing. Some backbone nodes, especially in cloud environments ignore the Flow Label. This caused traffic polarization and inefficient bandwidth utilization.
Setup and Upgrade		
API experience	BootstrapStream RPC for Bootz Process	Introduced in this release on: Centralized Systems (8400 [ASIC: K100])(select variants only*) BootstrapStream RPC enhances the security, flexibility, and future-readiness of Bootz process by enabling TLS 1.3-based device bootstrapping in Cisco IOS XR regardless of the hardware limitations in SUDI certificate. With the BootstrapStream RPC, backward compatibility with the existing Bootz infrastructure is preserved.
Upgrade	Traffic mirroring on PWHE	Introduced in this release on: Fixed Systems (8700 [ASIC: K100]) (select variants only*) This feature requires Egress Feature Capability (EFC) on supported platforms. Use the hw-module profile edge-mode CLI command to enable the EFC feature. The feature introduces these changes:

Product impact	Feature	Description
		CLI: • hw-module profile edge-mode • show hw-module profile edge-mode *This feature is now supported on: • 8711-48Z-M • 8712-MOD-M
Upgrade	Deprecated insecure protocols in optional RPMs	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]) This feature improves platform security and reduces the threat surface of the Cisco Networking products by restricting insecure protocols such as Telnet, FTP, TFTP, and RCP (which were deprecated in Cisco IOS XR Release 25.4.1) from Cisco IOS XR base package. In this release, Telnet is added to the optional RPM, {{Telnet.rpm}}, and FTP, TFTP, and RCP are added to the optional RPM, {{IP-Insecure-Apps.rpm }}. We recommend you to migrate to secure alternatives such as SSH, SCP, SFTP as Telnet, FTP, TFTP, and RCP protocols will not be supported anymore starting from an upcoming Cisco IOS XR release.
System Security		
Ease of Use	FIDO2 authentication for SSH	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]) FIDO2 support for SSH enables secure, passwordless logins by using hardware security keys to store private keys. This feature requires physical user presence to authenticate sessions and protects against phishing by verifying a signature from the security device during the login process.
Software Reliability	Post-Quantum Cryptography key exchange support for Cisco SSH	Introduced in this release on: Fixed Systems (8200 [ASIC: 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*) CiscoSSH mitigates quantum threats to ensure long term confidentiality and integrity of remote access and data transfer by introducing PQC (Post-Quantum Cryptography) hybrid key exchange algorithms. Supported algorithms include ML-KEM and NTRU Prime hybrids: * mlkem768x25519-sha256 * sntrup761x25519-sha512 * sntrup761x25519-sha512@openssh.com
Upgrade	Lawful intercept	Introduced in this release on: Fixed Systems (8700 [ASIC: K100])

Product impact	Feature	Description
		(select variants only*) This feature requires Egress Feature Capability (EFC) on supported platforms. Use the hw-module profile edge-mode CLI command to enable the EFC feature. The feature introduces these changes: CLI: • hw-module profile edge-mode • show hw-module profile edge-mode *This feature is now supported on: • 8711-48Z-M • 8712-MOD-M
Ease of Use	MACsec state reflection on line protocol	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]) MACsec State Reflection on line protocol synchronizes the interface line protocol state with the MACsec session state. When the session is not secured and the security policy is set to must-secure, the interface is brought Down to prevent traffic blackholing. When the session is secured, the interface is restored to Up. This enables faster failure detection and traffic rerouting by upper-layer protocols such as LACP and BGP. Previously, MACsec session failures did not affect the interface's line protocol status, often resulting in silent traffic drops and delayed network convergence.
Software Reliability	URPF source validation using VRF table	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200]) Modular Systems (8000 [ASIC: Q200]) (select variants only*) This feature provides secure traffic validation by supporting high prefix scales and high-speed updates that exceed the capabilities of standard Access Control Lists. It implements a new loose mode Unicast Reverse Path Forwarding (URPF) by using a dedicated URPF Virtual Routing and Forwarding (VRF) table for source lookups. This process enables efficient source validation within existing platform routing limits. *This feature is supported on: • Cisco 8202-32FH-M • 88-LC0-36FH • 88-LC0-36FH-M
Ease of Use	ECC P-256 integration	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200], (select variants only*) ECC256 enablement enhances device security by migrating identity and attestation workflows to ECCp256-based SUDI via the Trust Anchor Module (TAM). This transition enables the adoption of TLS 1.3 for critical services such as BootZ, secure Zero-Touch Provisioning (sZTP), and EMSD. Operational continuity is ensured through a resilient fallback to legacy RSA-based keys if needed.

Product impact	Feature	Description
		ECC p256 is automatically enabled when certificates are present; no additional configuration steps are required. *This feature is applicable on: • 8202-32FH-M • 8202-32FH-MO
System Monitoring		
Software Reliability	Deprecation of legacy uni-dimensional healthcheck metrics	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]) Effective Cisco IOS XR Software Release 26.2.1, the legacy uni-dimensional infrastructure health check metrics are deprecated, and hence the support for the show healthcheck metric command syntax is removed and will no longer be supported in future releases. This change simplifies command-line operations and eliminates redundant workflows. We recommend you to use YANG models available from resmon, wdmon and shell-utils which provide the same data. This approach provides more granular, scalable, and standardized access to metrics data, aligning with modern network automation and telemetry practices.
L2VPN		
Upgrade	Enhance network efficiency and scalability with GIL pruning for PWHE interfaces	Introduced in this release on: Fixed Systems (8700 [ASIC: K100]) (select variants only*) This feature requires Egress Feature Capability (EFC) on supported platforms. Use the hw-module profile edge-mode CLI command to enable the EFC feature. The feature introduces these changes: CLI: • hw-module profile edge-mode • show hw-module profile edge-mode *This feature is now supported on: • 8711-48Z-M • 8712-MOD-M
Upgrade	Pseudowire Headend	Introduced in this release on: Fixed Systems (8700 [ASIC: K100]) (select variants only*) This feature requires Egress Feature Capability (EFC) on supported platforms. Use the hw-module profile edge-mode CLI command to enable the EFC feature. The feature introduces these changes: CLI: • hw-module profile edge-mode • show hw-module profile edge-mode

Product impact	Feature	Description
		*This feature is now supported on: • 8711-48Z-M • 8712-MOD-M

New hardware

Table 2. New hardware for Cisco 8000 Series Routers, Release 26.2.1

Hardware	Description
Optics	This release introduces the following new optic on selective hardware within the product portfolio. For details, refer to the Transceiver Module Group (TMG) Compatibility Matrix. Cisco 400G QSFP-DD Ultra Long Haul Coherent Optics • DP04QSDD-LLH-A1
8804-FAN-V2, 8808-FAN-V2, and 8818-FAN-V2 fan trays	To maintain optimal cooling, the 8804-FAN-V2, 8808-FAN-V2, and 8818-FAN-V2 high-performance fan trays must be installed if the router is configured with: • P200-based line cards • P100-based line cards using ZRP optical modules

Changes in behavior

- Remove of Model-driven CLI Commands: Starting from Cisco IOS-XR software release 26.2.1, the Model-driven CLI specifically the show YANG operational data commands have been removed.
- SNMP Traps Dropped in the Buffer Queue: Starting with IOS-XR software release 24.1.2, SNMP traps will be dropped from the trap queue during the first five minutes after configuring a new NMS server or after a device reload.
  - This issue is observed on all current releases of the Cisco IOS XR routers running IOS XR Release 24.1.2.
  - The defect applies only to NMS servers that are located behind a firewall or within a security network where ICMP packets are blocked.
- Updated Command Syntax and Usage Guidelines

  As an enhancement to the show cef commands, the internal, brief, and hardware keywords have been removed from these commands:
  - show cef unresolved
  - show cef ipv6 linklocal unresolved

  The internal and brief keywords have been removed from these commands:
  - show cef mpls unresolved
  - show cef mpls local-label

  Exceptions

- This command retains support for the internal and brief keywords when a specific prefix is provided: show cef unresolved <prefix>
- Usage Constraints for show cef mpls: When executing any command beginning with show cef mpls, you may use only one of these keywords at a time: brief, detail, or internal
- Note: The exception mentioned above applies: if the command includes unresolved or local-label, the internal and brief keywords are explicitly blocked.

- Change in forwarding information base manager identifier reporting: Previously, all forwarding information base manager (fib_mgr) instances across different locations—such as the Route Processor (RP) and Line Cards (LCs)—shared the same identifier, fib_mgr. Consequently, the show command output displayed only a single entry for application fib_mgr.

  With this update, each fib_mgr instance is assigned a unique identifier corresponding to its specific location. As a result, the show route afi-all summary command now lists all instances individually. For example, the output will display fib_mgr for the RP and FIB node0_3_CPU0 for the LC located at node0_3_CPU0.
- Manual Remediation of Forward-Referenced SRLG Interfaces: The existing Shared Risk Link Groups (SRLG) feature allows configuring SRLG values on interfaces that do not yet exist (forward-reference interfaces). These configurations appear in the output of the show srlg command. To avoid inconsistencies, manually remove all SRLG configurations related to non-existent or forward-referenced interfaces. This manual cleanup is essential to maintain system consistency and prevent misleading information in the SRLG display.
- Enhanced MPLS interface activation for IS-IS address-family lifecycle events: Starting with Cisco IOS XR Release 26.2.1, IS-IS enables or disables MPLS on an interface when the first or last MPLS-enabled address family is created or deleted, instead of waiting for operational UP or DOWN state transitions. Previously, MPLS state changes occurred only during interface shutdown or link-down events. With this enhancement, MPLS state updates now also occur when the interface configuration is removed at the root level or when the last IPv4 or IPv6 address associated with an MPLS-enabled address family is removed from the interface.
- MPLS-TE tunnel event history for insufficient bandwidth events: Starting with Cisco IOS XR Release 26.2.1, MPLS-TE tunnel events for insufficient bandwidth conditions are recorded in the tunnel event history. Previously, when a tunnel failed to reoptimize because the requested bandwidth was unavailable, the router generated syslog messages, but the event was not shown in the show mpls traffic-eng event-history tunnels output. This update adds a tunnel event for insufficient bandwidth so that you can review historical bandwidth-demand failures for debugging and capacity planning.
- Mandatory LDAP TLS Validation: LDAP server certificate validation for TLS connections is now enabled by default. Unlike previous versions that skipped validation when no trustpoint was defined, the current implementation mandates the use of a configured ldaps trustpoint to establish a secure connection. If this trustpoint is absent, the connection is automatically rejected, ensuring that all LDAP traffic is strictly authenticated and verified.

  These behaviors apply based on the configuration of the ldaps trustpoint:
  - No trustpoint configured: The TLS connection to the LDAP server is rejected by the router.
  - CA certificate only: The router uses the configured CA certificate to validate the LDAP server's certificate; the connection is established only upon successful validation.

    - CA and client certificate configured: The router uses the CA certificate to validate the server's certificate while presenting the client certificate to satisfy mTLS requirements; the connection is established only if both validation checks pass.
- MACsec Licensing Tier Update: Effective with Cisco IOS XR Software Release 26.2.1, MACsec on Cisco IOS XR routers utilizing the FCM 2.0 Access licensing model now requires the Advantage tier instead of the Premier tier. When MACsec is enabled on a physical interface, the interface bandwidth triggers Right-to-Use (RTU) consumption for the Access Advantage tier, calculated in 10G increments. This license consumption is reclaimed once the MACsec configuration is removed or the interface is shut down.
- Deprecated Security Algorithms: Starting Cisco IOS XR Release 26.2.1, the 3DES-CBC cipher and Diffie-Hellman Group 1 SHA1 key exchange are insecure and deprecated. You will see syslog warning messages for deprecated commands.
- Change in show media CLI output: The directory path previously shown as /var/lib/docker now appears as apphost in the show media CLI output. This change enhances clarity for users managing third-party applications and Docker containers. It also accurately reflects the directory's role within the Cisco IOS XR application hosting architecture.
- A deprecation notice is shown when you run the show tech-support netconf command.
- Starting Cisco IOS XR Release 26.2.1, you can set the ipv6 nd ns-interval value to less than 60 seconds on these virtual interfaces:
    - Bundle Ethernet interfaces
    - BVI interfaces
    - Pseudowire Ethernet interfaces
- NACM show command visibility improvements: Starting from Release 26.2.1, you get better visibility of NACM rules and groups in show nacm command outputs when dynamic NACM is used. This enhancement improves how information is displayed without changing existing functionality, ensuring NACM rules continue to operate as before.
- Enhanced syslog reporting for discard-extra-paths limits: Starting in Release 26.2.1, syslog notifications for the discard-extra-paths limit have been enhanced to provide per-neighbor and per-address-family reporting. This replaces the previous global notification behavior, which applied a 5-minute rate limit across the entire BGP process. The updated notifications are rate-limited to 30 seconds and reset automatically if the neighbor session flaps.
- LOS Alarm Based on Total Power Support: Starting with IOS-XR software release 26.1.1, a new Loss of Signal (LOS) alarm based on total received power has been introduced.

  Alarm Behavior
    - The existing payload-based LOS alarm has been renamed to LOS-P to accurately reflect its function.
    - Automation scripts and operational procedures that previously relied on the old LOS alarm may misinterpret alarms if not updated.
- Enhancing BGP Routing Security: You improve BGP routing security by enabling RPKI origin validation for both outbound advertisements and iBGP peer routes. This feature ensures only prefixes with valid or not-found ROA status are sent, while invalid prefixes are filtered, maintaining consistent and compliant routing across your network.

- Restriction for 800G ZR Modules on Cisco 88-LC1-36EH: To ensure optimal thermal and electrical performance, support for 800G ZR modules on the Cisco 88-LC1-36EH line card is now restricted to the top row of the port configuration.

Resolved issues

There are no resolved issues in this release.

Open issues

This table lists the open issues in this specific software release.

Note: This software release may contain open bugs first identified in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool.

Table 3. Open issues for Cisco 8000 Series Routers, Release 26.2.1

Bug ID	Description
CSCws46053	K100 pwhe: Ping does not work with 4K L3 sub-interface with triggers.
CSCwu08833	The new local SID is not updated to PD L2FIB for the down PW after removing/rolling back the SRv6 configuration.
CSCwt81929	The process restart of ifmgr results in route flapping and traffic loss.
CSCwu32085	cfmd abnormal process restart
CSCwu51305	bfd_agent mem leak at sysdb_edm_finddata_datalist_create sysdb_lib_edm_list.c:443

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 26.2.1

Cisco IOS XR	Crosswork	EPNM
Release 26.2.1	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: 26.2.1, File version: 1.0, Version: N/A
The upgrade matrix indicates that the following system upgrades and downgrades are supported
from the current XR version:

From       To         Restrictions
---------- ---------- ----------------------------------------------------
26.2.1     24.1.2     Target fixes; Caveats; Replace performed via reimage
26.2.1     24.2.2     Target fixes; Caveats; Replace performed via reimage
26.2.1     24.2.20    Caveats; Replace performed via reimage
26.2.1     24.2.200   Caveats; Replace performed via reimage
26.2.1     24.2.204   Caveats; Replace performed via reimage
26.2.1     24.2.206   Caveats; Replace performed via reimage
26.2.1     24.2.21    Caveats; Replace performed via reimage
26.2.1     24.2.210   Caveats; Replace performed via reimage
26.2.1     24.2.215   Caveats; Replace performed via reimage
26.2.1     24.3.2     Target fixes; Caveats; Replace performed via reimage
26.2.1     24.3.20    Caveats; Replace performed via reimage
26.2.1     24.3.30    Caveats; Replace performed via reimage
26.2.1     24.4.1     Caveats; Replace performed via reimage
26.2.1     24.4.2     Caveats; Replace performed via reimage
26.2.1     25.1.1     Caveats; Replace performed via reimage
26.2.1     25.1.2     Caveats; Replace performed via reimage
26.2.1     25.1.30    Caveats; Replace performed via reimage
26.2.1     25.2.1     Caveats; Replace performed via reimage
26.2.1     25.2.15    Caveats; Replace performed via reimage
26.2.1     25.2.16    Caveats; Replace performed via reimage
26.2.1     25.2.17    Caveats; Replace performed via reimage
26.2.1     25.2.18    Caveats; Replace performed via reimage
26.2.1     25.2.2     Caveats; Replace performed via reimage
26.2.1     25.2.21    Caveats; Replace performed via reimage
26.2.1     25.3.1     Caveats; Replace performed via reimage
26.2.1     25.4.1     Replace performed via reimage
26.2.1     25.4.15    Replace performed via reimage
26.2.1     25.4.2     Replace performed via reimage
26.2.1     26.1.1     Replace performed via reimage
26.2.1     26.1.2     Replace performed via reimage
26.2.1     26.2.300   Replace performed via reimage
26.2.1     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 26.2.1->24.1.2 upgrade, use
        'show install upgrade-matrix running 26.2.1 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 26.2.1 LNT
Copyright (c) 2013-2026 by Cisco Systems, Inc.

Build Information:
 Built By: cisco
 Built On: Sun Jun 07 13:01:37 UTC 2026
 Build Host: iox-lnx-014
 Workspace: /auto/srcarchive13/prod/26.2.1/8000-aarch64/ws/
 Version: 26.2.1
 Label: 26.2.1

cisco 8000 (CN9130H board)
cisco 8011-4G24Y4H-I (CN9130H board) processor with 16GB of memory
8000-AARCH64 uptime is 1 hour, 1 minute
Cisco 8011 Series Fixed 1RU Router 4x100G, 24x1/10/25G, 4xCu
```

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

Part Number	Description	Support Initially Provided in IOS XR Release
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		
8201-32FH	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

Part Number	Description	Support Initially Provided in IOS XR Release
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
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

Part Number	Description	Support Initially Provided in IOS XR Release
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

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

Part Number	Description	Support Initially Provided in IOS XR Release
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
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

Part Number	Description	Support Initially Provided in IOS XR Release
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

Resource	Description
Ask AI about this product	Provides access to Cisco product documentation for checking product support details. Start by selecting the product family, then use *Ask AI About This Product* tab for further information.
Cisco 8000 documentation	Provides CDC documentation for Cisco 8000 series routers.
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.

Resource	Description
Feature deprecation and removal details	Outlines the features currently supported by each operating system.
Feature deprecation phasing out insecure capabilities	Provides a list of insecure features and protocols that are scheduled for systematic deprecation and eventual removal from specified Cisco products.
Feature removal and suggested alternatives	Details the reasons why certain features or protocols are deemed insecure and offers secure alternatives when available.
Recommended release	Provides a general guide in case of upgrading IOS XR routers or new deployments that involve IOS XR routers.
Smart licensing	Provides information about Smart Licensing Using Policy solutions and their deployment on IOS XR 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.
Yang data models in GitHub	Provides yang data models introduced and enhanced in every IOS XR release.

Legal information