Release Notes for Cisco 8000 Series Routers, IOS XR Release 25.3.1

Contents

Cisco 8000 Series Routers, IOS XR Release 25.3.1

Cisco IOS XR Release 25.3.1 introduces new features and hardware for the Cisco 8000 Series Routers. Key features include enhanced BGP stability, sub-second EVPN convergence, expanded ACL and QoS support, advanced segment routing, and improved security—including TACACS+ over TLS and MACsec. The release also introduces new monitoring, timing, and hardware features, offering greater scalability, reliability, and security.

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 25.3.1

Product impact	Feature	Description
BGP		
Software Reliability	BGP inbound route delays	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 prevent premature traffic shifts during planned network changes. This feature holds selected BGP routes in a queue for a configurable time, delaying their processing and advertisement until the network is ready. This approach ensures controlled and stable network transitions.
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 churn in your network by precisely controlling which BGP prefixes advertise cumulative bandwidth information. With this feature, you can apply route policies to choose which prefixes include bandwidth data, limit bandwidth cumulation to specific routes or domains.
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.
Software Reliability	Improved BGP next-hop resolution handling	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 improve network routing stability by enabling or

Product impact	Feature	Description
		disabling BGP nexthop resolution using the default route without resetting active BGP sessions. This enhancement maintains BGP session continuity, prevents traffic disruption, avoids service interruption, and improves operational flexibility. Previously, applying or removing the bgp nexthop resolution allow-default command reset all BGP sessions, even when the reset was not required for nexthop resolution.
API Experience	Service Layer API	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]) The Service Layer API enhances the system's performance by directly accessing the routing infrastructure layer using gRPC. It also allows flexible integration of custom protocols. For detailed information on Service Layer API for BGP, see Service Layer APIs for BGP.
EVPN		
Software reliability	Sub-second convergence for EVPN with BGP PIC-edge	Introduced in this release on: Fixed Systems(8010 [ASIC: A100], 8200 [ASIC: P100], 8700 [ASIC: P100, K100]); Modular Systems (8800 [LC ASIC: P100]) You can maintain continuous service in multi-homed EVPN deployments using sub-second convergence for EVPN with BGP PIC-edge. This functionality rapidly switches traffic to a backup nexthop path when the preferred nexthop fails, delivering fast convergence and high availability for active-active EVPN E-LAN and E-Line services.
API experience	Layer 3 EVPN IGMP and MLD state synchronization	Introduced in this release on: Fixed Systems(8200, 8700, 8011)(select variants only*); Modular Systems (8800 [LC ASIC: P100]) You can ensure seamless and reliable multicast delivery in residential FTTH networks with IGMP and MLD state synchronization for L3 using EVPN. This feature synchronizes IPv4 IGMP and IPv6 Multicast Listener Discovery (MLD) states across multiple PE devices using L3 sub-interfaces, eliminating the need for complex L2 or IRB configurations. It supports both VRF and global routing table deployments, providing flexibility for various network designs. - This feature is supported on: - 8212-48FH-M - 8711-32FH-M - 8712-MOD-M - 8011-4G24Y4H-I
IP Addresses and Services		
Ease of Use	Extending ACLs on BVI support to P100-based ASICs	Introduced in this release on: Fixed Systems (8200 [ASIC: P100]); Fixed Systems (8700 [ASIC: P100]); Modular Systems (8800 [LC ASIC: P100]) You can now enable ACLs on Bridged Virtual Interfaces (BVIs) for ingress and egress traffic on Cisco Silicon One P100 ASIC-based systems.

Product impact	Feature	Description
Interface and Hardware Component		
Software Reliability	Increase in IP-in-IP decapsulation tunnels support	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200]; Centralized Systems (8600 [ASIC:Q200]); Modular Systems (8800 [LC ASIC: Q200]) With this release, we have revised the maximum number of IPv4 and IPv6 IP-in-IP decapsulation tunnels from 64 to 200 on Cisco Silicon One Q200 ASIC-based systems. An increased number enhances the router's ability to support larger and more complex IP-in-IP tunneling scenarios improving scalability, efficiency, and flexibility in network design.
Upgrade	Y.1731 support on CFM	Introduced in this release on: Fixed Systems (8010 [ASIC: A100], 8700 [ASIC: P100])(select variants only*); Modular Systems (8800 [LC ASIC: P100])(select variants only*) This feature is now supported on: ▪ 8011-4G24Y4H-I ▪ 8711-32FH-M ▪ 88-LC1-52Y8H-EM ▪ 88-LC1-12TH24FH-E
Software Reliability	QoS support with auto-negotiated speeds	Introduced in this release on: Fixed Systems (8010 [ASIC: A100]) (select variants only*) You can now maintain optimal network efficiency by applying QoS on Gigabit Ethernet interfaces that operate at lower speeds through auto-negotiation. Auto-negotiation detects and matches the highest common speed between connected routers, allowing seamless interoperability. With this enhancement, you can use QoS on interfaces connecting to legacy devices that support only 10 Mbps or 100 Mbps speeds. This capability improves traffic management, leading to enhanced network performance and reliability across diverse deployment scenarios. ▪ This feature is supported on: 8011-4G24Y4H-I
Software Reliability	ERSPAN rate limit Per-destination	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 control the amount of mirrored traffic sent to ERSPAN (Encapsulated Remote SPAN) destinations by applying a rate limit per source NPU, helping to prevent network congestion and optimize resource usage.
L2VPN		
Software Reliability	MPLS static label support for EVPN ELAN	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200, P100], 8700 [ASIC: P100, K100]); Centralized Systems (8600 [ASIC:Q200]); Modular Systems (8800 [LC ASIC: Q100, Q200, P100]) You can configure local static MPLS labels for unicast IP traffic under the EVPN EVI configuration, which ensures remote PEs use a consistent, common label for the same EVPN service, improving forwarding consistency and operational control.
Software Reliability	MPLS static label support for	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200,

Product impact	Feature	Description
	EVPN VPWS	P100], 8700 [ASIC: P100, K100]); Centralized Systems (8600 [ASIC:Q200]); Modular Systems (8800 [LC ASIC: Q100, Q200, P100]) You can configure local static MPLS labels for EVPN VPWS under the L2VPN cross-connect P2P EVPN EVI configuration, which ensures remote PEs use a consistent, common label for the same EVPN service, improving forwarding consistency and operational control.
API Experience	Layer-3 route synchronization for EVPN multi-homing	Introduced in this release on:Fixed Systems(8200, 8700, 8011)(select variants only*); Modular Systems (8800 [LC ASIC: P100]) With Layer-3 route synchronization, you can ensure seamless failover and optimal traffic distribution in multi-homing environments by synchronizing critical Layer-3 routing information, such as ARP/ND entries and multicast routes, across redundant Provider Edge (PE) routers. This feature leverages the BGP-EVPN route synchronization mechanism to maintain consistent routing states and accelerate convergence across your network. *This feature is supported on: • 8212-48FH-M • 8711-32FH-M • 8712-MOD-M • 8011-4G24Y4H-I
Modular QoS		
Ease of Use	Priority Flow Control	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200]) (select variants only*) You can now enable Priority Flow Control (PFC) to pause specific classes of traffic without impacting others during network congestion. This feature allows the device to apply flow control on a per-priority basis, preventing packet loss for critical traffic while maintaining overall network performance. • This feature is supported on: • 8201-32FH
Ease of Use	Explicit Congestion Notification	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200]) (select variants only*) You can now enable Explicit Congestion Notification (ECN) to mark packets instead of dropping them when network congestion is detected. ECN enables better congestion management and reduced packet loss for sensitive applications. This feature allows network devices to signal congestion to endpoints by setting ECN bits in the IP header, enabling endpoints to react and adjust their transmission rate. • This feature is supported on: • 8201-32FH
Software Reliability	HBM enhancement for buffer-extended hybrid mode	Introduced in this release on: Modular Systems (8800 [LC ASIC: Q200]) (select variants only*) With this release, we've enhanced the High Bandwidth Memory

Product impact	Feature	Description
		(HBM) pools for lossy and lossless traffic from 4GB to 8GB. As a result, each traffic type can utilize up to 8GB of HBM independently, which significantly reduces tail drops for lossy traffic. You can configure the HBM pool size for lossy traffic to allow flexible resource allocation and to improve buffer management. Previously, both traffic types shared a single 4GB HBM pool, leading to lossy tail drops during congestion.
Ease of Use	Traffic Class Queue High Water Marks Monitoring	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100]); Modular Systems (8800 [LC ASIC: P100]) This feature monitors egress interface traffic class queues and records the queue occupancy and queue delay high water marks information for each traffic class. This information includes the virtual output queue that experienced the high water mark and a timestamp indicating when the high water mark was recorded. You can use this data to identify network bottlenecks and prevent traffic congestion.
Ease of Use	Available Shared Memory System and High Bandwidth Memory	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100]) (select variants only); Modular Systems (8800 [LC ASIC: P100]) (select variants only) You can now view buffer availability for Shared Memory System (SMS) and High Bandwidth Memory (HBM) with higher accuracy without any lag between the minimum and maximum watermark readings, especially when the packet buffers are used and released rapidly. This is possible because we've enabled the instantaneous display of available or free SMS and HBM. Previously, you could view details only for the highest watermark readings for SMS and HBM. You must configure PFC in the buffer-extended mode for this option, and this functionality is available only for Cisco Silicon One Q200-based routers and line cards. - This feature is supported on: - 8711-32FH-M - 8212-48FH-M - 88-LC1-36EH
Multicast		
Software Reliability	Layer 2 multicast ingress route statistics	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 introduces statistics collection for Layer 2 multicast routes by programming multicast route counters directly on the ingress line card. This implementation allows for more accurate and efficient traffic measurement and provides detailed per-route statistics at ingress. These statistics are essential for operational tasks such as network performance monitoring, usage-based billing, and troubleshooting multicast forwarding and replication issues. Previously, multicast route statistics was available only for Layer 3 multicast routes.
MPLS		

Product impact	Feature	Description
Software Reliability	Self-ping probe for current LSP	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]) The self-ping probe functionality is extended to support the current LSP that allows the network to promptly confirm the readiness of existing LSP to handle traffic. This immediate verification helps prevent traffic drops by ensuring that the data path is fully operational before forwarding actual user traffic. The **self-ping** option is configured under a named tunnel and the operational status of the tunnel is determined by probe packet or during session timeout.
NetFlow and sFlow		
API experience	BGP community and AS path information elements for IPFIX	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 export flow records with BGP community and AS path information elements in IPFIX. This allows you to monitor and analyze traffic based on precise BGP routing metadata, including community tags and AS paths. This ensures more granular visibility and control over your routing environment.
Programmability		
API Experience	Eco Mode Power Saving for Fabric and NPU	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 reduce overall hardware power consumption and streamline energy management by enabling eco mode for supported components like fabric and NPU. With this feature, you can configure power-saving settings globally or tailor them for specific subcategories and features. Eco mode allows hardware components to operate in their lowest supported power states, minimizing manual steps and helping organizations optimize power usage across the system.
Software Reliability	YANG-Push	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]) YANG-Push provides a real-time telemetry solution by allowing applications to subscribe to specific YANG datastore updates. This feature enables efficient, low-latency streaming of operational state data to subscribed receivers. By reducing the reliance on traditional polling methods, YANG-Push enhances network observability, accelerates troubleshooting, and optimizes data collection for modern network automation and assurance workflows.
Software Reliability	Non-recursive next-hop lookup for static routes	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])

Product impact	Feature	Description
		Non-recursive next-hop lookup for static routes enhances routing security and predictability by ensuring that static routes are installed only when their next hop is directly reachable through a connected interface. By preventing recursive resolution through other routing table entries, this feature gives administrators granular control over static route installation and traffic forwarding. Non-recursive lookup supports compliance and network integrity requirements, and can be configured via IOS XR CLI or OpenConfig YANG models for both manual and automated deployments.
Software Reliability	Lossless next-hop group updates	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] Lossless Next-Hop Group (NHG) updates ensure zero traffic loss during next-hop group (NHG) changes, improving network reliability and performance by preventing service disruptions during maintenance or reconfiguration. The system uses Make-Before-Break (MBB) programming, updating or switching NHGs so that packets have an active path throughout the process. This allows seamless updates when modifying NHG content or switching NHGs, ensuring continuous data flow and lower operational risk during routing changes.
Routing		
Ease of Use	ePBR drop and transmit actions	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100], 8010 [ASIC: A100]); Modular Systems (8800 [LC ASIC: P100]) The feature adds two critical forwarding actions, such as drop and transmit to enhanced Policy-Based Routing (ePBR) policies, giving network administrators precise control over how traffic matching specific criteria in a PBR policy is handled. These actions simplify policy creation, remove complex workarounds, and allow administrators to manage exceptions or security scenarios with granular per-traffic control.
Ease of Use	Bidirectional forwarding detection on BVI	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100]); Modular Systems (8800 [LC ASIC: P100]) You can now extend the advantage of BFD low-overhead and short-duration path failure detection to an IRB deployment by configuring BFD on multipath single-hop sessions using a BVI. By configuring BFD on a multipath session, you enable its use over virtual interfaces or between interfaces that are multiple hops apart.
Segment Routing		
Ease of Use	Cisco Network Controller (CNC) v7.2: Multiple SID-List with Preserve or Transactional gRPC API	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 enables advanced segment routing path computation by supporting multiple SID lists and atomic, transactional updates through gRPC API. This ensures reliable, consistent policy changes and enhances network stability. It supports high availability with state synchronization across

Product impact	Feature	Description
		multiple SR-PCEs and integrates with Path Computation Clients for comprehensive traffic engineering across multi-AS topologies. This improves network programmability, scalability, and reduces configuration errors.
Ease of Use	SRv6 per-flow manual steering: ABF redirect into VRF	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 enables precise manual control of traffic flows by steering them into specific VRFs using ABF redirect mechanisms. This allows optimized routing, improved network segmentation, and flexible policy enforcement, enhancing network performance, security, and resource utilization for complex business needs.
Software Reliability	Multiple Segment Routing Global Blocks	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 enhance network scalability and flexibility by enabling the allocation of additional SR label ranges, which prevents label space conflicts and supports efficient label management. By allowing multiple Segment Routing Global Blocks (SRGBs) to operate in parallel on the single node, it expands label space to meet growing network demands without causing widespread re-planning or ripple effects. This capability aligns with segment routing standards such as RFC8660, ensuring a standardized, future-proof approach to label management and network evolution.
Ease of Use	SRv6 policy counters (POL.CP.SL.INT.E)	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]) Network administrators can now monitor and manage network performance, capacity planning, and traffic engineering by reviewing the policy counters (POL.CP.SL.INT.E) in SRv6-TE. This feature is enabled by default.
API experience	Layer 3 service gateway for interconnecting SRv6 domains	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]) Optimize network scalability and interoperability by reducing SID resource usage, and enabling seamless integration between distinct SRv6 domains. The Layer 3 service gateway provides a flexible mechanism to extend Layer 3 services across different SRv6 networks, supporting efficient route summarization, cross-locator compatibility, and consistent service continuity on both control and data planes.
Setup and Upgrade		
Software reliability	Implementing audit monitoring	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 enhance your router's security and compliance by enabling audit monitoring. This feature lets you configure predefined rules that enable the router to monitor, log, and

Product impact	Feature	Description
		optionally forward audit logs to a remote syslog server for centralized analysis and incident response.
Upgrade	Changes to supported software upgrade or downgrade IOS XR versions due to the underlying OS package manager upgrade	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 upgrade Cisco IOS XR software from an earlier version to version 25.3.1 or later, and downgrade from version 25.3.1 or later to an earlier version, with certain limitations. These limitations are designed to help prevent failures during the upgrade or downgrade process.
Upgrade	Restrictions on rollback operation	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 release simplifies the upgrade process between XR versions by improving the underlying implementation, resulting in a more robust and scalable solution. From this release, packages for rollback are no longer available. You can still use the install rollback command on specific PIDs where it is supported for reversing install operations within an XR release. Also, you can use the existing rollback commands to roll back install operations performed with multiple SMU or optional packages.
Ease of Use	Ownership voucher request enhancement	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200, P100], 8700 [ASIC: P100, K100]); Modular Systems (8800 [LC ASIC: Q100, Q200, P100]) From this release onwards, when requesting an ownership voucher for fixed systems, you must use the chassis serial numbers in the Ownership Voucher request. Additionally, for both modular and fixed chassis systems, the serial number included in the ownership voucher request must match the SUDI subject name or the certificate on the device. This ensures accurate device identification and owner verification.
System Management		
Software Reliability	Performance monitoring for PTP networks	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 get statistical information with Performance Monitoring in PTP networks, such as clock accuracy, synchronization status, and network delays by defining Performance Monitoring Parameters and Port Specific Parameters. This feature empowers operators with comprehensive performance monitoring and precise time-stamp analysis, offering enhanced granularity for time synchronization in telecommunication networks. By providing detailed insights, it enables operators to make well-informed decisions and take proactive actions to ensure optimal network performance.
Ease of Setup	Use PTP Virtual Port to Select Timing Source	Introduced in this release on: Fixed Systems (8010 [ASIC: A100]) (select variants only*)

Product impact	Feature	Description
		This feature is now supported on: • 8011-4G24Y4H-I You can now select the best available timing source for your routers by using the PTP Virtual Port (VP) feature. This feature allows you to compare, select, and advertise the best clock source between a PTP server and other local timing sources connected to the routers. VP is an external frequency, phase, and time input interface on a Telecom Boundary Clock (T-BC), and thus participates in the timing source selection.
Ease of Setup	Use APTS to Select Timing Source	Introduced in this release on: Fixed Systems (8010 [ASIC: A100]) (select variants only*) This feature is now supported on: • 8011-4G24Y4H-I Assisted Partial Timing Support (APTS) enables you to select timing and synchronization for mobile backhaul networks. APTS allows for proper distribution of phase and time synchronization in the network.
System Monitoring		
Ease of use	Fabric link health and capacity monitoring with a single command	Introduced in this release on: Modular Systems (8800 [LC ASIC: Q100, Q200, P100]) In this release, we've introduced a single command that monitors fabric link quality, monitors capacity, and allows you to diagnose hardware and software issues. Previously, users encountered issues like links stopping, flapping, or dropping packets due to poor quality. These issues often required collecting multiple Command Line Interface (CLI) outputs and using external scripts for analysis.
Hardware Reliability	Enhancing FIB hardware programming failure recovery in non-OOR scenarios	Introduced in this release on: Cisco 8000 with ASIC Q100, Q200, P100, K100, and A100: 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]) FIB hardware programming failure recovery enhancement increases network stability and reduces performance impact during hardware programming issues in non-OOR situations by taking these actions: • Reduces churn by limiting the recovery attempts to twice, instead of retrying every 15 seconds. • Removes the errored object from the forwarding tree. • Displays syslog messages with details about the hardware failure and its cause. • Attempts recovery by deleting and then re-creating the affected hardware programming entry.
API Experience	Packet Tracer	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100]); Modular Systems (8800 [LC ASIC: P100]) We now extend the Packet Tracer support on P100 based line cards and fixed chasis. • This feature is now supported on: • 88-LC1-36EH • 88-LC1-12TH24FH-E

Product impact	Feature	Description
		▪ 88-LC1-52Y8H-EM ▪ 8212-48FH-M ▪ 8711-32FH-M
Ease of use	Traffic class latency histogram	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200]); Centralized Systems (8600 [ASIC: Q200]); Modular Systems (8800 [LC ASIC: Q200]) You can now monitor packet delays between ingress and egress on specific ports using a new visual representation featuring latency histograms. These histograms provide detailed insights into packet delays and jitter, enabling you to identify bottlenecks, optimize traffic flows, and enhance network efficiency. The feature offers latency analysis for each TC across multiple levels, including Network Processing Unit (NPU), slice, Inter-Frame Gap (IFG), and specific TCs.
System Security		
Software Reliability	Unused connection timeout for SSH sessions	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 prevent session limit exhaustion and maintain optimal system performance by automatically disconnecting SSH connections with no active channels. The feature introduces a configurable timeout for unused SSH connections, ensuring stale sessions do not occupy resources on your routers. The router monitors each SSH connection and terminates it when all channels remain closed and SSH clients do not create new channels within the configured timeout period.
Software Reliability	Channel timeout for SSH sessions	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 improve resource efficiency and minimize potential security risks by automatically closing idle SSH channels on the routers after a specific period of inactivity. The feature introduces a configurable timeout for SSH channels which ensures that unused channels do not persist while the parent SSH connection remains active. The router monitors each SSH channel and closes any channel where no data is sent or received within the configured timeout period.
Software Reliability	MACsec encryption on layer 3 sub-interfaces	Introduced in this release on: 8700 [ASIC: P100] (select variants only*) You can now configure MACsec policy on Layer 3 sub-interfaces, which gives you the flexibility to apply MACsec policies to different L3 sub-interfaces that belong to the same main physical interface. This capability is possible because we've enabled the router to keep the VLAN tags unencrypted, enabling the L3 sub-interfaces to be the MACsec endpoints. When you apply MACsec policies on these sub-interfaces, you can enhance the overall security of your network by adding an extra layer of security to the communication between different subnets. *This feature is now extended to 8711-32FH-M.
Software Reliability	Port mode MACsec over multipoint L2VPN services	Introduced in this release on: 8700 [ASIC: P100] (select variants only*)

Product impact	Feature	Description
		You can achieve secure Layer 2 connectivity over multipoint VPN services by encrypting traffic at the customer edge (CE) port of the router before it traverses the provider network. We've enabled the functionality on your routers to support customer edge port mode MACsec over multipoint L2VPN services such as Virtual Private LAN Service (VPLS) or Ethernet VPN (EVPN). *This feature is now extended to 8711-32FH-M.
Security Efficacy	TACACS+ over TLS	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 enhance security and reduce the risk of attacks on weak encryptions by using TACACS+ over TLS, ensuring secure transmission of AAA data between the client and server. This feature supports mutual authentication through a TLS X.509 certificate-based infrastructure and is compatible with TLS versions 1.3 and 1.2, providing robust protection for sensitive environments.
Ease of Use	802.1X port-based access control with MAB fallback	Introduced in this release on: Fixed Systems (8200 [ASIC: P100]); Modular Systems (8800 [LC ASIC: Q200, P100]) (select variants only*) You can use MAC Authentication Bypass (MAB) as a fallback method to enhance network security and flexibility when routers do not support the 802.1X protocol. By default, 802.1X authentication is set as the primary authentication method. In multi-authentication mode, a router supports up to 20 MAB clients simultaneously, in networks with a mix of 802.1X-capable and non-802.1X-capable devices. ▪ This feature is supported on: ▪ 8212-48FH-M ▪ 88-LC0-36FH-M ▪ 88-LC1-36EH ▪ 88-LC1-12TH24FH-E ▪ 88-LC1-52Y8H-EM
Software Reliability	RADIUS Change of Authorization for 802.1X and MAB sessions	Introduced in this release on: Fixed Systems (8200 [ASIC: Q100, Q200], 8700 [ASIC: K100], 8010 [ASIC: A100]); Modular Systems (8800 [LC ASIC: Q100, Q200]) You can now prioritize 802.1X authentication method on a 802.1X-enabled port that is already running in fallback MAC Authentication Bypass (MAB) mode on your router. This feature allows change in re-authentication method for 802.1X- or MAB-authenticated clients through RADIUS Change of Authorization (CoA) requests from an external AAA server or policy server. This capability allows external servers to dynamically update client session authentication without requiring session disconnection and reconnection. The feature thereby ensures seamless and efficient access control management.
Hardware Reliability	MACsec Encryption on 8711-48Z-M	Introduced in this release on: Fixed Systems (8000 [ASIC: K100]) (select variants only*) MACsec, the Layer 2 encryption protocol, secures data on physical media and provides data integrity and confidentiality. *We now support MACsec encryption on all ports of 8711-48Z-M.

New hardware

There is no new hardware introduced in this release

Changes in behavior

- Full Outgoing Interface Name in Cisco-IOS-XR-mpls-forwarding-oper: The outgoing-interface leaf of Cisco-IOS-XR-mpls-forwarding-oper has been updated to include the full outgoing interface name instead of the shortened interface name.
- Deprecation of `show grpc status` command: The `show grpc status` command is deprecated and future releases will not support this command. Use the existing `show grpc` command instead of `show grpc status` command to display the status and operational details of the gRPC server.
- Scale enhancement: Starting with Release 25.3.1, to meet new capacity requirements, the scale for the BGP Label Unicast (LU) Prefix and Local Label has been increased from 32,000 to 56,000 on all Cisco 8000 systems, except for the Q100 ASIC-based systems, which will maintain the existing scale of 32,000.
- Call Home transport mode deprecated: Starting with Release 25.3.1, IOS XR software no longer supports Call Home transport mode for Licensing. Please configure CSLU or Smart Transport to ensure seamless operation of the licensing solution.
- You can use Access Control Lists (ACLs) on Bridge Virtual Interfaces (BVIs) to filter network traffic. However, if you configure ACLs on the router, you cannot configure BVI ARP suppression concurrently.

Open issues

Table 2. Open issues for Cisco 8000 Series Routers, Release 25.3.1

Bug ID	Description
CSCwp19275	CFM LLF functionality is not working on SF [Q200/K100/A100/P100] platform.
CSCwp19348	After software upgrade, ASIC Initialization Failed causing another reload to the system.
CSCwp30814	8712-MOD-M - counters.top.interrupt_reg.collision_tx continuous interrupt on running EVPN ELAN L2 traffic.
CSCwq35727	8712-MOD-M - Flowspec rules are matching wrong packets - ICMP match rule matching non ICMP packets.
CSCwq56242	25.3.1- Glandon - EVPN MH = Next-hop-Tracking - Convergence time for Known Unicast Traffic seen as 31 secs.
CSCwq75206	ERSPAN ACL not working after rate-limit change.
CSCwq31498	Unable to remove link-OAM from interface after breakout rollback.
CSCwq52327	8712-MOD-M - RSVP mid node traffic silent drop with queuing applied on bundle subinterface.
CSCwq52351	8712-MOD-M - VPN swap/Option-B not working with queuing policy applied on subinterface.

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 3. Compatibility matrix for Cisco 8000 Series Routers, Release 25.3.1

Cisco IOS XR	Crosswork	EPNM
Release 25.3.1	Crosswork Optimization Engine 6.0	Evolved Programmable Network Manager 7.1.1

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: 25.3.1, File version: 1.0, Version: N/A


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


From       To         Restrictions
---------- ---------- ----------------------------------------------------
25.3.1     24.1.2     Target fixes; Caveats; Replace performed via reimage
25.3.1     24.2.2     Target fixes; Caveats; Replace performed via reimage
25.3.1     24.2.20    Caveats; Replace performed via reimage
25.3.1     24.2.201   Caveats; Replace performed via reimage
25.3.1     24.2.203   Caveats; Replace performed via reimage
25.3.1     24.2.204   Caveats; Replace performed via reimage
25.3.1     24.2.21    Caveats; Replace performed via reimage
25.3.1     24.3.1     Target fixes; Caveats; Replace performed via reimage
25.3.1     24.3.2     Target fixes; Caveats; Replace performed via reimage
25.3.1     24.3.20    Caveats; Replace performed via reimage
25.3.1     24.3.30    Caveats; Replace performed via reimage
25.3.1     24.4.1     Caveats; Replace performed via reimage
25.3.1     24.4.2     Caveats; Replace performed via reimage
25.3.1     25.1.1     Caveats; Replace performed via reimage
25.3.1     25.1.2     Caveats; Replace performed via reimage
25.3.1     25.2.1     Caveats; Replace performed via reimage
25.3.1     25.2.15    Caveats; Replace performed via reimage
25.3.1     7.10.2     Target fixes; Caveats; Replace performed via reimage
25.3.1     7.11.2     Target fixes; Caveats; Replace performed via reimage
25.3.1     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 25.3.1->24.1.2 upgrade, use
        'show install upgrade-matrix running 25.3.1 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 25.3.1
Copyright (c) 2013-2025 by Cisco Systems, Inc.

Build Information:
 Built By     : swtools
 Built On     : Mon Sep 15 07:19:49 PDT 2025
 Built Host   : iox-lnx-026
 Workspace    : /auto/srcarchive12/prod/25.3.1/ncs5500/ws
 Version      : 25.3.1
 Location     : /opt/cisco/XR/packages/
 Label        : 25.3.1-iso

cisco NCS-5500 () processor
System uptime is 50 minutes
```

Supported hardware

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

Table 4. Supported hardware for Cisco 8010 Series Routers

Part Number	Description	Support Initially Provided in IOS XR Release
Cisco 8010 Series Routers - Chassis		
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-400-AC	Cisco 400W AC Power Module	Release 25.1.1
PWR-400-DC	Cisco 400W DC Power Module	Release 25.1.1

Table 5. Supported hardware for Cisco 8200 Series Routers

Part Number	Description	Support Initially Provided in IOS XR Release
Cisco 8200 Series Routers - Chassis		
8201-SYS	Cisco 8200 1 RU Fixed System - 24 QSFP56-DD 400GbE and 12 QSFP28 100GbE	Release 7.0.12
8202-SYS	Cisco 8200 2 RU Fixed System - 12 QSFP56-DD 400GbE and 60 QSFP28 100GbE	Release 7.3.1
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 6. 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

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 7. Supported hardware for Cisco 8700 Series Routers

Part Number	Description	Support Initially Provided in IOS XR Release
Cisco 8700 Series Routers - Chassis		
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 8. Supported hardware for Cisco 8800 Series Routers

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

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 9. Related resources

Resource	Description
Smart licensing	Provides information about Smart Licensing Using Policy solutions and their deployment on IOS XR routers.
Cisco 8000 documentation	Provides CDC documentation for Cisco 8000 series routers.
Transceiver Module Group (TMG) compatibility matrix	Allows searching by product family, product ID, data rate, reach, cable type, or form factor to determine the transceivers that Cisco hardware device supports.
Cisco IOS XR Error messages	Allows searching by release number, error strings, or comparing release numbers to view a detailed repository of error messages and descriptions.
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.

Legal information