



Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.11.1

[Network Convergence System 5500 Series Routers](#) 2

[What's New in Cisco IOS XR Release](#) 2

[Caveats](#) 28

[Release Package](#) 28

[Determine Software Version](#) 28

[Determine Firmware Support](#) 28

[Important Notes](#) 29

Revised: May 7, 2024

Network Convergence System 5500 Series Routers

What's New in Cisco IOS XR Release

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

Software Features Enhanced and Introduced

To learn about features introduced in other Cisco IOS XR releases, select the release from the [Documentation Landing Page](#).

Feature	Description
Application Hosting	
Cisco Secure DDoS Edge Protection	<p>Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])</p> <p>We have now moved DDoS protection to the network edge, ensuring you can mitigate any DDoS attacks at the ingress points and minimize the impact of such attacks on your network and applications running on it. This solution deploys a centralized controller that manages a distributed network of edge detectors that analyze and mitigate threats across networks.</p>
Docker Application Management using IPv6 Address	<p>In this release, you gain the ability to manage Docker applications within containers using IPv6 addresses via the router's management interface. Leveraging IPv6 addresses provides expanded addressing options, enhances network scalability, and enables better segmentation and isolation of applications within the network.</p> <p>Prior to this update, only IPv4 addresses could be used to manage docker applications.</p>
Programmability	
Automatic Resynchronization of OpenConfig Configuration	<p>Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])</p> <p>OpenConfig infrastructure can now reapply all the OpenConfig configurations automatically if there are any discrepancies in the running configuration.</p> <p>With this feature, there is no need for manual replacement of the OpenConfig configuration using Netconf or gNMI.</p> <p>The re-sync operation is triggered if the running configurations and the OpenConfig configuration go out of sync after any system event that removes some running configurations from the system. A corresponding system log gets generated to indicate the re-sync status.</p>

Feature	Description
gRPC Network Security Interface	<p>Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])</p> <p>This release implements authorization mechanisms to restrict access to gRPC applications and services based on client permissions. This is made possible by introducing an authorization protocol buffer service for gRPC Network Security Interface (gNSI).</p> <p>Prior to this release, the gRPC services in the gNSI systems could be accessed by unauthorized users.</p> <p>This feature introduces the following change:</p> <p>CLI:</p> <ul style="list-style-type: none"> • gnsi load service authorization policy • show gnsi service authorization policy <p>To view the specification of gNSI, see Github repository.</p>
BGP	
Peering Between BGP Routers Within the Same Confederation	<p>Introduced in this release on: NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Native])</p> <p>You can now enable BGP peering between routers in the sub-autonomous system (AS) within a confederation to advertise specific router updates using iBGP. This capability ensures that the mesh of routers between sub-ASes in a confederation maintains consistent routing tables, ensuring proper network reachability. Enabling this feature helps improve preventing performance reduction and traffic management challenges.</p> <p>The feature introduces these changes:</p> <p>CLI:</p> <p>New Command:</p> <ul style="list-style-type: none"> • allowconfedas-in <p>YANG Data Models</p> <ul style="list-style-type: none"> • New XPath for <ul style="list-style-type: none"> • <code>Cisco-IOS-XR-ipv4-bgp-cfg.yang</code> • <code>Cisco-IOS-XR-um-router-bgp-cfg</code> <p>(see GitHub, YANG Data Models Navigator)</p>

Feature	Description
Preventing Label Churn Using Secondary Label Allocation	<p>Introduced in this release on: NCS 5700 line cards [Mode: Compatibility; Native]</p> <p>You can now prevent label churn and ensure that traffic forwarding continues without interruption.</p> <p>In certain scenarios, route reflectors (RRs) are configured as backup routers to each other through Prefix Independent Convergence (PIC) configuration, and the same VPN prefix is learnt from other routers. In such cases, if the label allocation mode used in RRs is per-next-hop-received-label, then label churn happens, and labels are exhausted quickly. This feature uses the secondary label allocation method to prevent the label churn issue.</p> <p>The feature introduces these changes:</p> <p>CLI:</p> <ul style="list-style-type: none"> • The allocate-secondary-label keyword is introduced in the label mode command. <p>YANG Data Model:</p> <ul style="list-style-type: none"> • <code>Cisco-IOS-XR-um-router-bgp-cfg.yang</code> (see GitHub, YANG Data Models Navigator)
Ternary Content-Addressable Memory Enhancement to Improve L3VPN Routing Capability	<p>Introduced in this release on: NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5700 line cards [Mode: Native])</p> <p>You can improve your router's performance by introducing two additional Ternary Content-Addressable Memory (TCAM) labels. This enhancement removes the dependence on the Forwarding Equivalence Class (FEC) scale for handling more routes, which means that the router's capacity is no longer limited by FEC capacity. As a result, we have significantly increased the number of routes for L3VPN.</p> <p>The feature introduces these changes:</p> <p>CLI:</p> <ul style="list-style-type: none"> • remote-bgp-label-mode-per-prefix • hw-module fib mpls two-label-tcam-optimized

Feature	Description
Virtual Routing Forwarding Next Hop Routing Policy	<p>Introduced in this release on: NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Native])</p> <p>You can now enable a route policy at the BGP next-hop attach point to limit notifications delivered to BGP for specific prefixes, which equips you with better control over routing decisions, and allows for precise traffic engineering and security compliance for each VRF instance, and helps establish redundant paths specific to each VRF.</p> <p>The feature introduces these changes:</p> <p>CLI:</p> <p>Modified Command:</p> <ul style="list-style-type: none"> • The nexthop route-policy command is extended to VRF address-family configuration mode. <p>YANG Data Models</p> <ul style="list-style-type: none"> • New XPaths for <ul style="list-style-type: none"> • <code>Cisco-IOS-XR-ipv4-bgp-cfg.yang</code> • <code>Cisco-IOS-XR-um-router-bgp-cfg</code> <p>(see GitHub, YANG Data Models Navigator)</p>
Interface and Hardware Component	
Disable Auto-Squelch on Coherent Optics	<p>Introduced in this release on: NCS 5500 modular routers; NCS 5700 fixed port routers</p> <p>This release introduces the support to disable auto-squelch on coherent optics. By disabling auto-squelch, you can detect weak signals embedded within the laser source noise and simultaneously reduce processing overhead in systems with stable laser sources and minimal noise. When laser squelch is enabled, the system shuts down the laser in case of an Optical Transport Network (OTN) failure.</p> <p>The feature introduces these changes:</p> <p>CLI:</p> <ul style="list-style-type: none"> • host auto-squelch disable <p>YANG DATA models:</p> <ul style="list-style-type: none"> • New XPaths for <code>Cisco-IOS-XR-controller-optics-cfg</code> (see Github, YANG Data Models Navigator)

Feature	Description
Independent MTUs for IPv4 and IPv6	<p>Introduced in this release on: NCS 5700 line cards [Mode: Native]</p> <p>You can now ensure reduced fragmentation or packet drops by configuring separate IPv4 and IPv6 Maximum Transmission Units (MTUs). You can configure independent IPv4 and IPv6 MTUs on the physical interface and subinterface, bundle interface and subinterface, and Bridge-Group Virtual Interface (BVI).</p> <p>This feature introduces these changes:</p> <p>CLI: The following commands are extended to subinterface configuration mode:</p> <ul style="list-style-type: none"> • ipv4 mtu • ipv6 mtu • mtu
Traffic Mirroring of Incoming and Outgoing Traffic Separately over Pseudowire	<p>Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5700 line cards [Mode: Native]</p> <p>You can now distribute the monitoring load by separating the Rx and Tx traffic mirroring over the pseudowire. Earlier, you could mirror the entire traffic without distinguishing between Rx and Tx directions.</p> <p>The separation of traffic direction gives the flexibility of monitoring and analyzing the nature of data being sent and received using independent network traffic analysis tools. The separation also helps in distributing the monitoring load and eases troubleshooting.</p> <p>The feature modifies the monitor-session command. The keywords destination rx and destination tx of the command are extended to monitor session configuration mode. Earlier, this configuration resulted in verification failure.</p>
TSoP Smart SFP for SDH and SONET Encapsulation	<p>Introduced in this release on NCS 5500 fixed port routers</p> <p>This release introduces support for the Clear Channel Synchronous Transport Module Level-1 (STM1) Smart SFP (SFP-TS-OC3STM1-I) for the Transparent SONET or SDH over Packet (TSoP) protocol. This allows you to leverage your existing packet-switched network to transport traditional time-division multiplexing (TDM) traffic. TSoP Smart SFPs offer the following advantages:</p> <ul style="list-style-type: none"> • Encapsulation of SDH or SONET bit streams into packet-switched network format • Improved suitability for pseudowire transport over an Ethernet network
L2VPN and Ethernet Services	

Feature	Description
Control Word and Flow Label Signaling Attributes in Extended Community Field	<p>Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])</p> <p>We have enhanced the information that the Extended Community carries for a route by including details such as frame sequencing information, type of payload, identifying encapsulated traffic, and identifying packets belonging to the same traffic flow (or sharing characteristics such as source or destination addresses). Such additional information helps in proper encapsulation, identification, and handling of traffic flows at the receiving end, and is possible because we've included the control word and flow label signaling attributes to the extended community field.</p> <p>The feature introduces these changes:</p> <p>CLI:</p> <p>The control word and flow label signaling attributes are added to:</p> <ul style="list-style-type: none"> • show bgp l2vpn evpn • show evpn evi
Storm Control Configuration for Subinterfaces on NCS 5700 fixed port routers (non-SE)	<p>Introduced in this release on: NCS 5700 fixed port routers</p> <p>Storm Control is now supported on the NCS 5700 fixed port routers (non-SE) variants.</p>
VXLAN Static Routing	<p>Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Native])</p> <p>You can now configure the source and destination virtual tunnel endpoints (VTEPs) for a particular traffic flow, which is particularly useful for scenarios where your data center is connected to an enterprise network, so multiple servers in the data center provide cloud services to your customers and the enterprise edge router. These endpoints help provide rapid convergence in case of failure. Plus, using the UDP header in the VXLAN packet, the VXLAN static routing (also called unicast VXLAN) facilitates network balancing by preventing the transmission of replicated packets.</p> <p>The feature introduces these changes:</p> <p>CLI:</p> <ul style="list-style-type: none"> • host-reachability protocol static • overlay-encapsulation vxlan • interface nve • member vni <p>YANG Data Model:</p> <ul style="list-style-type: none"> • Cisco-IOS-XR-l2vpn-cfg (see GitHub, YANG Data Models Navigator)
MPLS	

Feature	Description
Teardown and Reestablishment of RSVP-TE Tunnels	<p>Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])</p> <p>You can now teardown and reestablish the existing tunnels of headend, midend, or tailend router tunnels of an MPLS network for optimized distribution of the traffic across MPLS and RSVP-TE to improve network performance and enhance resource utilization.</p> <p>Previously, you could reestablish tunnels only at the headend router using the mpls traffic-eng resetup command.</p> <p>The feature introduces these changes:</p> <p>CLI: mpls traffic-eng teardown</p> <p>YANG Data Model: Cisco-IOS-XR-mpls-te-act.yang (see GitHub, YANG Data Models Navigator)</p>
Multicast	
EVPN All-Active Multi-homed Multicast Source Behind a BVI	<p>Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])</p> <p>We have enhanced multicast routing efficiency, load balancing, and latency in EVPN topology by optimizing redundancy and enabling support for All-Active (AA) multicast multi-homed sources. The multi-homed multicast data sources are located behind a Bridge-Group Virtual Interface (BVI), while multicast receivers can be in either the core or a bridge domain.</p> <p>This feature introduces the following changes:</p> <ul style="list-style-type: none"> • CLI <ul style="list-style-type: none"> • The ole-collapse-disable keyword is introduced in the hw-module multicast evpn command. • YANG Data Model <ul style="list-style-type: none"> • New leaf evpn-ole-collapse-disable added in <code>Cisco-IOS-XR-fia-hw-profile-cfg.yang</code> (see GitHub, YANG Data Models Navigator).
MLD Snooping Synchronization for EVPN Multi-Homing	<p>Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])</p> <p>The Designated Forwarder (DF) PE router in an EVPN multi-homed network can now efficiently forward multicast traffic from the source to the interested receivers, avoiding unnecessary replication and reducing network bandwidth consumption.</p> <p>This is made possible by introducing support for Multicast Listener Discovery, MLDv1, and MLDv2 (IPv6) snooping state synchronization for EVPN multi-homing peers or provider edge (PE) devices, expanding the scope of the previous support for IGMP (IPv4) snooping state synchronization.</p>

Feature	Description
Statistics for Egress Multicast Traffic Route Rate	<p>Introduced in this release on: NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])</p> <p>With the ability to now view the route rates or rate of data being forwarded or transmitted per interface, you can monitor your network performance at a granular level, effectively troubleshoot network issues, and have greater control over bandwidth management.</p> <p>Previously, you could view the route rates only at the line card level.</p> <p>This feature introduces the following changes:</p> <ul style="list-style-type: none"> • CLI <ul style="list-style-type: none"> • The rate keyword is introduced in the show mrib route command. • YANG Data Model <ul style="list-style-type: none"> • New XPathS for <code>Cisco-IOS-XR-mfwd-oper.yang</code> (see GitHub, YANG Data Models Navigator).
IP Addresses and Services	
Unicast VRRP	<p>Introduced in this release on: NCS 5500 modular routers (NCS 5500 line cards).</p> <p>We have now enabled Layer 3 unicast transport mode in VRRP, allowing it to enhance its capacity to send data to other networks, including cloud networks. Pairwise router redundancy enables high availability in cloud network scenarios. However, a virtual IP (VIP) address is required by the default route of the cloud native function because there is no pre-designated active member in paired routers. HSRP can provide a VIP, but cloud networks do not support Layer 2 multicast or broadcast transports. You can configure VRRP to support Layer 3 unicast transport to overcome the limitation of Layer 2 multicast and broadcast transports.</p> <p>The feature introduces these changes:</p> <p>New Command:</p> <p>CLI:</p> <ul style="list-style-type: none"> • unicast-peer <p>Modified Commands:</p> <ul style="list-style-type: none"> • show vrrp command is modified to support new fields: Mcast packet in Ucast mode , IPv4 Unicast Peer , and IPv4 Unicast Peer . <p>YANG Data Model:</p> <p>New Xpaths for:</p> <ul style="list-style-type: none"> • <code>Cisco-IOS-XR-ipv4-vrrp-cfg.yang</code> • <code>Cisco-IOS-XR-ipv4-vrrp-oper.yang</code> <p>(see GitHub, YANG Data Models Navigator)</p>
Modular QoS	

Feature	Description
Burst Size for Port-Level Shaper	<p>Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])</p> <p>You can now achieve a predictable and accurate burst size at the link level by configuring port-level shaper burst size, thus ensuring better adherence to traffic SLAs. Also, with the port-level shaper burst size configured in the egress policy maps, the predictability in peak burst ensures that you can configure any next-hop low-capacity device to handle these bursts.</p> <p>Previously, you could configure burst sizes, which impacted traffic flow only at the Virtual Output Queue (VOQ) level but didn't control packet transmission at the link level.</p>
View Packet Processing and Traffic Management Resources	<p>Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])</p> <p>You can now view the utilization of some packet processing and traffic management resources, such as policer banks and connectors. Insights into their consumption and availability help you prevent or mitigate an Out of Resource (OOR) situation, thus ensuring optimal QoS operations with minimal impact on network performance.</p> <p>The feature introduces the following changes:</p> <p>CLI:</p> <p>show controllers npu resources qos</p> <p>YANG:</p> <ul style="list-style-type: none"> • Cisco-IOS-XR-fretta-bcm-dpa-qos-resources-oper • Cisco-IOS-XR-5500-qos-oper • Cisco-IOS-XR-fretta-bcm-dpa-qos-rate-profile-resources-oper • Cisco-IOS-XR-fretta-bcm-dpa-qos-egq-resources-oper <p>(see GitHub, YANG Data Models Navigator)</p>
Routing	

Feature	Description
Maximum Paths Per Flexible Algorithm Per Prefix	<p>Previously, you could configure a maximum number of Equal-Cost Multi-path (ECMP) to be set for SPF algo 0.</p> <p>This feature provides additional granularity to the IS-IS Maximum Paths Per-Algorithm feature by allowing you to specify a set of prefixes for SPF algo 0.</p> <p>Now you can achieve a balance between path diversity and computational and memory requirements by controlling the number of paths for each specific algorithm and destination prefix combination.</p> <p>This feature introduces these changes:</p> <p>CLI</p> <ul style="list-style-type: none"> • maximum-paths route-policy <i>name</i> <p>YANG Data Models:</p> <ul style="list-style-type: none"> • This feature extends the native <code>Cisco-IOS-XR-clns-isis-cfg.yang</code> model <p>See GitHub, Yang Data Models Navigator</p>
Increased ECMP Maximum Paths for BGP within VRF	<p>Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])</p> <p>We have increased the maximum ECMP paths available for BGP within a VRF to 128. This increases the number of next hops that are added for ECMP in the Forwarding Information Base (FIB) table, which in turn ensures that the network is geared up to deal with sudden increase in bandwidth, without compromising on the load balancing and performance aspects.</p> <p>Previously, the maximum number of ECMP paths supported for IGP, BGP, and labeled paths was 64. With this release, the support is enhanced to 128 ECMP paths for IPv4 and IPv6 prefixes over iBGP and eBGP within a VRF.</p> <p>This feature modifies the maximum-paths command.</p>
<p>Segment Routing</p>	
Configure Flow Labels in SRv6 Header for PM Liveness	<p>Introduced in this release on: NCS 5500 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards).</p> <p>You can now monitor the activeness of multiple paths for a given segment list using flow labels in the SRv6 header.</p> <p>In earlier releases, the SRv6 header didn't include flow labels.</p> <p>The feature introduces these changes:</p> <p>CLI:</p> <ul style="list-style-type: none"> • The flow-label keyword is introduced in the performance-measurement liveness-profile command. <p>YANG Data Models:</p> <ul style="list-style-type: none"> • <code>Cisco-IOS-XR-um-performance-measurement-cfg.yang</code> • <code>Cisco-IOS-XR-perf-meas-oper.yang</code> <p>See (GitHub, Yang Data Models Navigator)</p>

Feature	Description
Configure Segment Lists to Activate Candidate Paths in SRv6 for PM Liveness	<p>Introduced in this release on: NCS 5500 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards).</p> <p>You can now enable a candidate path to be up by configuring the minimum number of active segment lists associated with the candidate path. The head-end router determines that a candidate path is up based on the minimum number of active segment lists configured.</p> <p>In earlier releases, the head-end router identified a candidate path as up only when all the segment lists associated with the path were active.</p> <p>The feature introduces these changes:</p> <p>CLI:</p> <ul style="list-style-type: none"> The validation-cp minimum-active segment-lists option is introduced in the performance-measurement liveness-detection command. <p>YANG Data Models:</p> <ul style="list-style-type: none"> <code>Cisco-IOS-XR-infra-xtc-agent-cfg.yang</code> <p>See (GitHub, Yang Data Models Navigator)</p>
Flexible Algorithm Constraint for Tree-SID Path Computation	<p>This feature introduces support for Static and mVPN/Dynamic TreeSID with Flexible Algorithm constraint.</p> <p>Unlike SR-TE point-to-point (P2P) policies, where the primary objective for Flexible Algorithm is to reduce or compress the number of segments on the packet, the objective for Flexible Algorithm-based point-to-multipoint (P2MP) policies:</p> <ul style="list-style-type: none"> Another method of traffic engineering LFA FRR – Without Flex-Algo, the primary and backup paths chosen by the local node might not follow the traffic engineering constraints specified in the policy. <p>This feature introduces these changes:</p> <p>CLI</p> <ul style="list-style-type: none"> The sid-algorithm algo keyword is introduced in the command. The output of the show pce lsp p2mp command is modified to display Flex-Algo associated with a Tree, the Metric Type from Flex-Algo definition at Root, and the hop node-SIDs. The output of the show segment-routing traffic-eng p2mp policy command is modified to display Flex-Algo associated with Tree SID state, and the hop node-SIDs.

Feature	Description
IS-IS Flexible Algorithm with Exclude Maximum Delay Constraint	<p>Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])</p> <p>This feature enables you to configure topologies that exclude links that have delays over a specific threshold. This is especially critical for high-frequency trading applications, in satellite networks, or wherever there are fluctuations in link delays.</p> <p>This feature introduces these changes:</p> <p>CLI:</p> <ul style="list-style-type: none"> • The router isis instance flex-algo algo command is modified with the new maximum-delay value option. <p>YANG Data Model:</p> <ul style="list-style-type: none"> • This feature extends the native Cisco-IOS-XR-clns-isis-cfg.yang model (see GitHub, YANG Data Models Navigator)
IS-IS Flexible Algorithm with Exclude Minimum Bandwidth Constraint	<p>Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])</p> <p>Traffic engineering in networks can be optimized by avoiding low-bandwidth links that may not be capable of handling high volumes of traffic.</p> <p>This feature allows you to use Flexible Algorithm to create topologies in your network that explicitly exclude high bandwidth traffic from utilizing links below a specified capacity. This constraint is achieved by introducing a new bandwidth-based metric type within the Flexible Algorithm framework. Links that do not satisfy the constraint are ignored when computing the associated Flexible Algorithm topology.</p> <p>This feature introduces these changes:</p> <p>CLI:</p> <ul style="list-style-type: none"> • The router isis instance flex-algo algo command is modified with the new minimum-bandwidth value option. <p>YANG Data Model:</p> <ul style="list-style-type: none"> • This feature extends the native Cisco-IOS-XR-clns-isis-cfg.yang model (see GitHub, YANG Data Models Navigator)

Feature	Description
Maximum Paths Per IS-IS Flexible Algorithm Per Prefix	<p>Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])</p> <p>Previously, you could configure a maximum number of Equal-Cost Multi-path (ECMP) to be set for individual Flex Algorithms.</p> <p>This feature provides additional granularity to the IS-IS Maximum Paths Per-Algorithm feature by allowing you to specify a set of prefixes for Flexible Algorithm.</p> <p>Now you can achieve a balance between path diversity and computational and memory requirements by controlling the number of paths for each specific algorithm and destination prefix combination.</p> <p>This feature introduces these changes:</p> <p>CLI:</p> <ul style="list-style-type: none"> • maximum-paths route-policy <i>name</i> <p>YANG Data Models:</p> <ul style="list-style-type: none"> • This feature extends the native <code>Cisco-IOS-XR-clns-isis-cfg.yang</code> model <p>See GitHub, Yang Data Models Navigator</p>
Microloop Avoidance for IS-IS with Per-Prefix Filtering	<p>Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])</p> <p>Currently, when SR Microloop Avoidance for IS-IS is enabled, it applies to all prefixes.</p> <p>This feature allows you to selectively allow or deny specific IPv4 or IPv6 prefixes or routes that may cause microloops, which allows for efficient use of hardware resources and ensures overall network stability.</p> <p>This feature introduces these changes:</p> <p>CLI:</p> <ul style="list-style-type: none"> • The microloop avoidance segment-routing command is modified with the new route-policy <i>name</i> option for IS-IS. <p>YANG Data Model:</p> <ul style="list-style-type: none"> • This feature extends the native <code>Cisco-IOS-XR-um-router-isis-cfg.yang</code> model (see GitHub, YANG Data Models Navigator)

Feature	Description
Microloop Avoidance for OSPFv2 Single-Node Cost-in and Single-Node Cost-out Events	<p>Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])</p> <p>Microloops disrupt network connectivity and cause suboptimal routing decisions. This feature avoids microloops by implementing the Greedy walk algorithm, which is similar to TI-LFA computation.</p> <p>This feature extends the microloop avoidance support for additional scenarios in OSPFv2, such as cost-in and cost-out events.</p> <p>This feature introduces these changes:</p> <p>YANG Data Model:</p> <ul style="list-style-type: none"> • <code>Cisco-IOS-XR-ipv4-ospf-oper.yang</code> <p>(see GitHub, YANG Data Models Navigator)</p>
Path MTU discovery for SRv6 Packets on Ingress PE	<p>Introduced in this release on: NCS 5500 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards).</p> <p>This feature prevents packet losses when one SRv6-enabled router sends an oversized packet to another. The functionality enables a router to send an ICMP error message to the source in such cases, prompting the sender to resend a packet whose size is within the MTU value, thus ensuring the packet moves ahead. The feature is critical for SRv6-enabled routers as these routers don't support packet fragmentation.</p> <p>Previously, a router dropped oversized packets without notifying the source, resulting in packet loss.</p> <p>The feature introduces these changes:</p> <p>CLI:</p> <ul style="list-style-type: none"> • The path-mtu keyword is introduced in the hw-module profile segment-routing srv6 mode command.
SR Policy Liveness Monitoring on Segment Routing over IPv6 (SRv6)	<p>Introduced in this release on: NCS 5500 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards).</p> <p>In segment routing over IPv6 (SRv6), you can now verify end-to-end traffic forwarding over an SR policy candidate path by periodically sending probe messages. Performance monitoring on an SRv6 network enables you to track and monitor traffic flows at a granular level.</p> <p>Earlier releases supported SR policy liveness monitoring over an SR policy candidate path on MPLS.</p>

Feature	Description
SR-TE Application Programming Interface (API)	<p>Introduced in this release on: NCS 5500 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards)</p> <p>This feature introduces an API solution that simplifies the task of building SR-TE controllers and managing SRTE policies. It does so by defining gRPC API services that allow applications to request SR policy operations.</p> <p>The solution leverages the gRPC Service API and GPB Data models, providing a unified, scalable, and secure method for network programming.</p> <p>This feature introduces these changes:</p> <p>New CLI</p> <ul style="list-style-type: none"> • <code>grpc segment-routing traffic-eng policy-service</code> <p>YANG Data Models:</p> <p>EMSD Yang model is updated to have this config under "segment-routing" container.</p> <ul style="list-style-type: none"> • Native model: <code>Cisco-IOS-XR-man-ems-cfg.yang</code> • UM model: <code>Cisco-IOS-XR-um-grpc-cfg.yang</code> <p>(see GitHub, YANG Data Models Navigator)</p>
SR-TE Explicit Path with a BGP Prefix SID as First Segment	<p>Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])</p> <p>This feature allows you to configure an SR-TE policy with an explicit path that uses a remote BGP prefix SID as its first segment. This path is achieved by leveraging the recursive resolution of the first SID, which is a BGP-Label Unicast (BGP-LU) SID. BGP-LU labels are used as the first SID in the SR policy to determine the egress paths for the traffic and program the SR-TE forwarding chain accordingly.</p> <p>This allows users to enable Segment Routing to leverage their existing BGP infrastructure and integrate it with the required Segment Routing functionalities.</p>
SRv6 ESI Filtering	<p>Introduced in this release on: NCS 5500 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards)</p> <p>Split Horizon Group (SHG) labels and Ethernet Segment Identifier (ESI) filtering functionalities exist on MPLS underlay networks.</p> <p>This feature introduces ESI filtering functionality to SRv6 underlay networks, using the End.DT2M SRv6 endpoint behavior. This behavior uses the "Arg.FE2" argument for SRv6, which is similar to the SHG label for MPLS.</p> <p>This feature allows nodes to identify BUM traffic based on the advertised ESI and prevent a loop by avoiding re-broadcasting the same traffic back towards the access node.</p> <p>This functionality is enabled by default.</p>

Feature	Description
SRv6 Traffic Accounting	<p>Introduced in this release on: NCS 5500 fixed port routers, NCS 5500 modular routers (NCS 5500 line cards).</p> <p>You can now enable the router to record the number of packets and bytes transmitted on a specific egress interface for IPv6 traffic using the SRv6 locator counter.</p> <p>You can use this data to create deterministic data tools to anticipate and plan for future capacity planning solutions.</p> <p>This feature introduces or modifies the following changes:</p> <p>CLI:</p> <ul style="list-style-type: none"> • accounting prefixes ipv6 mode per-prefix per-nexthop srv6-locators <p>YANG Data Models:</p> <ul style="list-style-type: none"> • <code>Cisco-IOS-XR-accounting-cfg</code> • <code>Cisco-IOS-XR-fib-common-oper.yang</code> <p>(see GitHub, YANG Data Models Navigator)</p>
SRv6-Services: L3 Services with Local SIDs from W-LIB	<p>Introduced in this release on: NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5700 line cards [Mode: Native])</p> <p>This feature enables an SRv6 headend node to allocate and advertise local SIDs with Wide (32-bit) functions (Local W-LIB).</p> <p>The headend router utilizes the local W-LIB functionality to define and implement SR policies using SRv6 SIDs.</p> <p>The Local W-LIB is supported for Layer 3 (VPNv4/VPNv6/BGPv4/BGPv6 global) services.</p> <p>This feature introduces the usid allocation wide-local-id-block command.</p>

Feature	Description
Two-Way Active Measurement Protocol Light Source Address Filtering	<p>Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])</p> <p>You can now restrict unauthorized users from sending packets to the network and prevent compromising the network security and reliability. For a destination UDP port, you can configure the list of IP addresses that can send Two-Way Active Measurement Protocol (TWAMP)-light packets to responder or querier nodes.</p> <p>In earlier releases, the responder or querier node accepted TWAMP-light packets from all IP addresses.</p> <p>The feature introduces these changes:</p> <p>CLI:</p> <ul style="list-style-type: none"> • The querier and responder keywords are introduced in the performance-measurement protocol twamp-light measurement delay command. <p>YANG Data Models:</p> <ul style="list-style-type: none"> • <code>Cisco-IOS-XR-um-performance-measurement-cfg.yang</code> • <code>Cisco-IOS-XR-perf-meas-oper.yang</code> <p>See (GitHub, Yang Data Models Navigator)</p>
System Management	
PTP on NCS-57B1-6D24-SYS, NCS-57B1-5DSE-SYS and NCS-57D2-18DD-SYS	<p>Introduced in this release on: NCS 5700 fixed port routers</p> <p>Based on the IEEE 1588-2008 standard, Precision Time Protocol (PTP) is a protocol that defines a method to synchronize clocks in a network for networked measurement and control systems.</p> <p>With this release, PTP Class C performance and QSFP-DD optics are now supported on 400G port speed for the following hardware:</p> <ul style="list-style-type: none"> • NCS-57B1-6D24-SYS • NCS-57B1-5DSE-SYS • NCS-57D2-18DD-SYS
PTP and SyncE support on breakout ports of NCS-57D2-18DD-SYS and NCS-57B1-6D24-SYS Routers	<p>Introduced in this release on: NCS 5700 fixed port routers.</p> <p>Based on the IEEE 1588-2008 standard, Precision Time Protocol (PTP) is a protocol that defines a method to synchronize clocks in a network for networked measurement and control systems. And, SyncE provides synchronization signals transmitted over the Ethernet physical layer to downstream devices, while the Synchronization Status Message (SSM) indicates the quality level of the transmitting clock to the neighboring nodes, informing the nodes about the level of the network's reliability. Ethernet Synchronization Message Channel (ESMC) is the logical channel that uses an Ethernet PDU (protocol data unit) to exchange SSM information over the SyncE link.</p> <p>With this release, timing support for PTP and SyncE is extended to 4x10G and 4x25G breakout ports of NCS-57D2-18DD-SYS and NCS-57B1-6D24-SYS routers.</p> <p>Class B and Class C performances are supported on 4x10G and 4x25G breakout ports of NCS-57D2-18DD-SYS and NCS-57B1-6D24-SYS routers.</p>

Feature	Description
System Monitoring	
System Logging Message Count	<p>Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])</p> <p>Instead of calculating the bytes consumed by Syslog as you did previously, you can now easily and effectively manage the buffer size of the system log messages by specifying the number of entries the system log displays.</p> <p>The feature introduces these changes:</p> <p>CLI:</p> <ul style="list-style-type: none"> • The entries-count keyword is added to the logging buffered command. <p>YANG Data Model:</p> <ul style="list-style-type: none"> • New Xpaths for Cisco-IOS-XR-infra-syslog-cfg • New Xpaths for Cisco-IOS-XR-um-logging-cfg
System Security	
Multiple Public Keys per User for Public Key-based Authentication	<p>Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])</p> <p>We provide greater flexibility to access secure routers by allowing four public keys to be used for authentication. With the ability to associate multiple public keys with your user account on the router, we've also simplified the authentication process by eliminating the need to create unique users for each SSH client device.</p> <p>The feature introduces these changes:</p> <p>CLI:</p> <ul style="list-style-type: none"> • The second , third , and fourth keywords are introduced in the crypto key import authentication rsa command. • The second , third , and fourth keywords are introduced in the crypto key zeroize authentication rsa command. • The second , third , and fourth keywords are introduced in the keystring command. <p>YANG Data Models:</p> <ul style="list-style-type: none"> • Cisco-IOS-XR-crypto-act • Cisco-IOS-XR-um-ssh-cfg <p>(See GitHub, YANG Data Models Navigator)</p>

YANG Data Models Introduced and Enhanced

This release introduces or enhances the following data models. For detailed information about the supported and unsupported sensor paths of all the data models, see the [Github](#) repository. To get a comprehensive list of the data models supported in a release, navigate to the Available-Content.md file for the release in the Github repository. The unsupported sensor paths are documented as deviations.

For example, `openconfig-acl.yang` provides details about the supported sensor paths, whereas `cisco-xr-openconfig-acl-deviations.yang` provides the unsupported sensor paths for `openconfig-acl.yang` on Cisco IOS XR routers.

You can also view the data model definitions using the [YANG Data Models Navigator](#) tool. This GUI-based and easy-to-use tool helps you explore the nuances of the data model and view the dependencies between various containers in the model. You can view the list of models supported across Cisco IOS XR releases and platforms, locate a specific model, view the containers and their respective lists, leaves, and leaf lists presented visually in a tree structure.

Feature	Description
Programmability	
openconfig-system.yang Version 0.13.1	This OpenConfig data model is revised from version 0.6.0 to 0.13.1. There are no functional changes between these two versions.
openconfig-vlan.yang Version 3.2.2	This OpenConfig data model is revised from version 3.2.0 to 3.2.2. There are no functional changes between these two versions.
openconfig-mpls-static.yang Version 3.3.0	The OpenConfig data model is revised from version 3.2.2 to 3.3.0. There are no functional changes between these two versions.

Feature	Description
openconfig-network-instance.yang Version 1.3.0	<p>This OpenConfig data model introduces the following changes to the BGP container:</p> <ul style="list-style-type: none"> • Enable the parameters related to the use of multiple paths for the same Network Layer Reachability Information (NLRI) using use-multiple-paths leaf. The router uses this information in Address Family Indicator (AFI) and Subsequent Address Family Indicator (SAFI) in multi-protocol extensions during exchange of neighbor capabilities when loading the peers. • Enable the route dampening to minimize the propagation of flapping routes across an internetwork and learn the dampened routes from neighbor or peers using route-flap-damping leaf. • Configure the default metric within the RIB for entries that are installed by the protocol instance using default-metric leaf. The lower the metric specified the more preferable the RIB entry is to be selected for use within the network instance. • Specify the type of extended community to be sent to the neighbor group or address family group using send-community leaf. • Specify the number of occurrences to allow the BGP speaker to accept the BGP updates even if its own BGP autonomous system (AS) number is in the AS-Path attribute using allow-own-as leaf. • Replace occurrences of the peer's AS in the AS_Path with the local AS number using replace-peer-as leaf. • Use disable-peer-as-filter for filtering the routes. When set to true, the system advertises routes to a peer even if the peer's AS was in the AS-Path. The default behavior (false) suppresses advertisements to peers if their AS number is in the AS-Path of the route. • Ignore the Interior Gateway Protocol (IGP) metric to the next-hop when calculating the best-path using ignore-next-hop-igp-metric leaf. The default is to select the route for which the metric to the next-hop is lowest.

Feature	Description
openconfig-lldp.yang	<p>This OpenConfig data model supports streaming model-driven telemetry (MDT) data for the leaves deviated in the previous releases.</p> <p>You can stream cadence-driven telemetry data for the following nodes:</p> <ul style="list-style-type: none"> • Retrieve the counters cleared and the number number of valid TLVs received using last-clear and tlv-accepted leaves • Gather data about LLDP interface counters using frame-in, frame-out, frame-error-in, frame-discard, tlv-discard, tlv-unknown, last-clear, and frame-error-out leaves • Stream operational state data for LLDP neighbors using age and last-update leaves <p>You can stream event-driven telemetry (EDT) data for system-name, system-description, chassis-id, and chassis-id-type leaves.</p>
openconfig-mpls-igp.yang Version 3.3.0	<p>This OpenConfig data model is revised from version 2.3.0 to 3.3.0. There are no functional changes between these two versions.</p>
openconfig-platform.yang	<p>This OpenConfig data model supports improved cadence of under 30 seconds to stream cadence-driven telemetry data for the operational state of the following components—power supply, fan, software modules, linecards and subcomponents.</p> <p>Event-driven telemetry is already supported for these components in the previous releases.</p>
openconfig-if-tunnel.yang	<p>This release introduces streaming model-driven telemetry (MDT) data for the operational state of source, destination, time-to-live (hop limit) and GRE key of tunnel interfaces using src, dest, ttl, and gre-key nodes respectively.</p>
openconfig-spanning-tree.yang	<p>This release introduces support for the following OpenConfig data models to define the configuration for Spanning Tree Protocol (STP):</p> <ul style="list-style-type: none"> • openconfig-spanning-tree.yang version 0.3.1 • openconfig-spanning-tree-types.yang version 0.4.1 <p>Using these data models, you can configure STP for a loop free topology within Ethernet networks, allowing redundancy within the network to deal with link failures.</p> <p>Rapid STP (RSTP) and streaming telemetry data for the operational state of nodes is not supported.</p>

Feature	Description
openconfig-mpls-te.yang Version 3.3.0	This OpenConfig data model, which is part of the openconfig-network-instance.yang data model is revised from version 3.0.1 to 3.3.0. There are no functional changes between these two versions.
openconfig-mpls-rsvp.yang Version 4.0.0	This OpenConfig data model, which is part of the openconfig-network-instance.yang data model is revised from version 3.0.2 to 4.0.0. There are no functional changes between these two versions.
openconfig-procmon.yang version 0.4.0	<p>This OpenConfig data model is revised from version 0.3.1 to 0.4.0. It is used to retrieve the operational data for processes running on a node. It is introduced to support the openconfig-system.yang data model to configure the following xpaths:</p> <ul style="list-style-type: none"> • Fetch the process related information using the the pid leaf. • View the process name using the name leaf. • Fetch the current process command line arguments using args leaf. • View the time at which the process started using start-time leaf. • Check the CPU time consumed by the process in user mode using the cpu-usage-user leaf. • Check the CPU time consumed by this process in kernel mode using cpu-usage-system leaf. • Check the percentage of CPU that is being used by the process using cpu-utilization leaf. • Check the bytes allocated and still in use by the process using memory-usage leaf. • View the percentage of RAM that is being used by a process using memory-utilization leaf.
openconfig-mpls.yang Version 3.3.0	<p>This OpenConfig data model is revised from version 3.2.2 to 3.3.0. It is a part of the openconfig-network-instance.yang data model and introduces the following leaves:</p> <ul style="list-style-type: none"> • Enable Time To Live (TTL) propagation in the MPLS domain using the ttl-propagation leaf. • Enable MPLS forwarding capability on an interface using mpls-enabled leaf. <p>You can stream model-driven telemetry data (MDT) for the operational state of the nodes.</p>

Feature	Description
openconfig-mpls-types.yang Version 3.4.0	This OpenConfig data model, which is part of the openconfig-network-instance.yang data model is revised from version 3.2.0 to 3.4.0. There are no functional changes between these two versions.
openconfig-network-instance.yang	<p>This OpenConfig data model introduces cadence-driven telemetry support to obtain and monitor the total active route counts on IPv4 or IPv6 default tables in a route processor using <code>installed-routes</code> leaf.</p> <p>Model-driven telemetry (MDT) sensor subscription can be enabled.</p> <p>Event-driven telemetry and Netconf protocol for default VRF table are not supported.</p>
Cisco-IOS-XR-um-performance-measurement-cfg.yang	<p>This unified data model is enhanced as follows:</p> <ul style="list-style-type: none"> • New containers <i>allow-querier</i> and <i>allow-responder</i>, to configure the list of IP addresses that can send TWAMP-light packets to responder or querier nodes. • A new container, <i>flow-label</i>, to monitor the liveness of multiple paths for a given segment list.
Cisco-IOS-XR-perf-meas-oper.yang	<p>This native data model is enhanced as follows:</p> <ul style="list-style-type: none"> • New containers, <i>allowed-responder-summary</i> and <i>allowed-querier-summary</i>, to configure the list of IP addresses that can send TWAMP-light packets to responder or querier nodes. • new container, <i>usid-info</i>, and new leaves such as <i>sid-value</i>, <i>usid-length</i>, <i>sid-format</i>, and <i>sid-behavior</i> in the <i>PM-USID-INFO</i> grouping, to monitor the liveness of a SRv6 candidate path.
Cisco-IOS-XR-infra-xtc-agent-cfg.yang	This native data model is enhanced with a new leaf, <i>minimum-active-segment-lists</i> , to configure the minimum number of active segment lists associated with the candidate path.
Cisco-IOS-XR-fretta-bcm-dpa-qos-resources-oper	You can now fetch details of the number of NPU connectors or Fabric Access Processors (FAPs) that QoS uses. The connector resource dictates the number of VOQs you can create. The egress policy map scale is bound to VOQ availability and, in turn, connector availability.

Feature	Description
Cisco-IOS-XR-5500-qos-oper	<p>You can now fetch details of:</p> <ul style="list-style-type: none"> • the number the of policers that are allocated and that you can create. • number of Virtual Output Queues (VOQs) used at a global level from a common pool. • resources used in creating traffic class and drop precedence (or discard class) maps for egress traffic.
Cisco-IOS-XR-fretta-bcm-dpa-qos-rate-profile-resources-oper	<p>You can now fetch details of the rate profile pool used. Interfaces with different line rates and policies with significantly differing shaper and queue lengths use rate profiles.</p>
Cisco-IOS-XR-fretta-bcm-dpa-qos-egq-resources-oper	<p>You can now fetch details of the number of egress queue maps used. They are consumed when you create egress policies with priority marking.</p>
Cisco-IOS-XR-crypto-act.yang	<p>This native data model is enhanced with a new leaf, <i>key-num</i>, under the following containers:</p> <p><i>key-import-authentication-rsa</i>: To import SSH public keys to the router for the currently logged-in user</p> <p><i>key-import-authentication-rsa-username</i>: To import SSH public keys to the router for a specific user</p> <p><i>key-zeroize-authentication-rsa</i>: To delete SSH public keys in the router for the currently logged-in user</p> <p><i>key-zeroize-authentication-rsa-username</i>: To delete SSH public keys in the router for a specific user</p> <p>The data model supports the following values for the <i>key-num</i> leaf:</p> <ul style="list-style-type: none"> • 2: second key • 4: third key • 8: fourth key
Cisco-IOS-XR-um-ssh-cfg.yang	<p>This unified data model is enhanced with the following new leaves under the <code>ssh server username</code> container to add up to 4 multiple public keys per user for public key-based authentication.</p> <p><code>keystring-second</code>: Adds a second SSH public key for a user in the router.</p> <p><code>keystring-third</code>: Adds a third SSH public key for a user in the router.</p> <p><code>keystring-fourth</code>: Adds a fourth SSH public key for a user in the router.</p>

Feature	Description
openconfig-aft.yang Revision 0.9.0	<p>The Abstract Forwarding Table (AFT) OpenConfig data model is enhanced to support the following features:</p> <ul style="list-style-type: none"> • The gRPC Network Management Interface (gNMI) proto is revised from version 0.7.0 to 0.8.0 to set the atomic flag to send AFT next-hop group notifications in JSON and PROTO encodings using gNMI subscribe RPC. Network events can be represented as multiple updates in the data models. The atomic flag allows NMS to interpret those multiple updates as a single event. • Stream telemetry data for conditional next-hop groups (CNHG) to provide DSCP information per prefix and list of input interfaces. This model helps to monitor the DSCP-based policy routing configuration at the forwarding layer. It now eliminates multiple lookups to map an IP prefix to an outgoing interface and IP address when internal labels are involved in that route. This is accomplished internally by reducing the hierarchy levels or flattening the nested next-hop telemetry updates. <p>You can stream Event-driven telemetry (EDT) data.</p>

Hardware Introduced

Cisco IOS XR Release 7.11.1 introduces the following hardware support:

Hardware Feature	Description
Optics	<p>This release launches the following new optics on selective hardware within the product portfolio. For details refer to the Transceiver Module Group (TMG) Compatibility Matrix.</p> <ul style="list-style-type: none"> • Cisco 10GBASE Dense Wavelength-Division Multiplexing SFP+ <ul style="list-style-type: none"> • DWDM-SFP10G-C-I

Features Supported on Cisco NC5700 Line Cards and NCS 5700 Fixed Port Routers

The following table lists the features supported on Cisco NC5700 line cards in compatibility mode (NC5700 line cards with previous generation NCS 5500 line cards in the same NCS 5500 modular routers) and native mode (NCS 5500 modular routers with only NCS 5700 line cards and NCS 5700 fixed port routers).

To enable the native mode on Cisco NCS 5500 series modular routers having Cisco NCS 5700 line cards, use the **hw-module profile npu native-mode-enable** command in the configuration mode. Ensure that you reload the router after configuring the native mode.

Table 1: Features Supported on Cisco NC5700 Line Cards and NCS 5700 fixed port routers

Feature	Compatible Mode	Native Mode
Label Space Conservation Using Secondary Label Allocation	×	✓
Cisco Secure DDoS Edge	✓	✓
Automatic Resynchronization of OpenConfig Configuration	✓	✓
gRPC Network Security Interface	✓	✓
Preventing Label Churn Using Secondary Label Allocation	✓	✓
Ternary Content-Addressable Memory Enhancement to Improve L3VPN Routing Capability	×	✓
Independent MTUs for IPv4 and IPv6	×	✓
Traffic Mirroring of Incoming and Outgoing Traffic Separately over Pseudowire	×	✓
Control Word and Flow Label Signaling Attributes in Extended Community Field	✓	✓
VXLAN Static Routing	×	✓
Teardown and Reestablishment of RSVP-TE Tunnels	✓	✓
EVPN All-Active Multi-homed Multicast Source Behind a BVI	✓	✓
MLD Snooping Synchronization for EVPN Multi-Homing	✓	✓
Statistics for Egress Multicast Traffic Route Rate	✓	✓
Burst Size for Port-Level Shaper	✓	✓
View Packet Processing and Traffic Management Resources	✓	✓
Increased ECMP Maximum Paths for BGP within VRF	✓	✓
Two-Way Active Measurement Protocol Light Source Address Filtering	✓	✓

For the complete list of features supported on Cisco NC57 line cards until Cisco IOS XR Release 7.11.1. see:

- [Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.10.1](#)
- [Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.9.2](#)
- [Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.9.1](#)
- [Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.8.2](#)
- [Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.8.1](#)
- [Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.7.2](#)
- [Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.7.1](#)

- [Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.6.2](#)
- [Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.6.1](#)
- [Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.5.3](#)
- [Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.5.2](#)
- [Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.5.1](#)
- [Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.4.2](#)
- [Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.4.1](#)
- [Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.3.1](#)

Caveats

Table 2: Cisco NCS 5500 Series Router Specific Bugs

Bug ID	Headline
CSCwi11464	After route churn trigger, SRV6 traffic is down with HW Programming failed for SRv6 nexthop

Release Package

This table lists the Cisco IOS XR Software feature set matrix (packages) with associated filenames.

Visit the [Cisco Software Download page](#) to download the Cisco IOS XR software images.

Determine Software Version

To verify the software version running on the router, use **show version** command in the EXEC mode.

Determine Firmware Support

Use the **show hw-module fpd** command in EXEC and Admin mode to view the hardware components with their current FPD version and status. The status of the hardware must be CURRENT; Running and Programed version must be the same.]

You can also use the **show fpd package** command in Admin mode to check the fpd versions.

NCS 5500 Fixed Port Routers

NCS 5700 Fixed Port Routers

This sample output is for **show hw-module fpd** command from the Admin mode:

Important Notes

- The total number of bridge-domains (2*BDs) and GRE tunnels put together should not exceed 1518. Here the number 1518 represents the multi-dimensional scale value.
- The offline diagnostics functionality is not supported in NCS 5500 platform. Therefore, the **hw-module service offline location** command will not work. However, you can use the **(sysadmin)# hw-module shutdown location** command to bring down the LC.

Supported Transceiver Modules

To determine the transceivers that Cisco hardware device supports, refer to the [Transceiver Module Group \(TMG\) Compatibility Matrix](#) tool.

Upgrading Cisco IOS XR Software

Cisco IOS XR Software is installed and activated from modular packages, allowing specific features or software patches to be installed, upgraded, or downgraded without affecting unrelated processes. Software packages can be upgraded or downgraded on all supported card types, or on a single card (node).

Before starting the software upgrade, use the **show install health** command in the admin mode. This command validates if the statuses of all relevant parameters of the system are ready for the software upgrade without interrupting the system.



Note

- If you use a TAR package to upgrade from a Cisco IOS XR release prior to 7.x, the output of the **show install health** command in admin mode displays the following error messages:

```
sysadmin-vm:0_RSP0# show install health
. . . .
ERROR /install_repo/gl/xr -rw-r--r--. 1 8413 floppy 3230320 Mar 14 05:45 <platform>-isis-2.2.0.0-r702.x86_64
ERROR /install_repo/gl/xr -rwxr-x---. 1 8413 165 1485781 Mar 14 06:02 <platform>-k9sec-3.1.0.0-r702.x86_64
ERROR /install_repo/gl/xr -rw-r--r--. 1 8413 floppy 345144 Mar 14 05:45 <platform>-li-1.0.0.0-r702.x86_64
```

You can ignore these messages and proceed with the installation operation.

- Quad configurations will be lost when you perform a software downgrade on a NCS-55A1-48Q6H device from IOS XR Release 7.5.1 onwards to a release prior to IOS XR Release 7.5.1 due to non-backward compatibility change. The lost configuration can be applied manually after the downgrade.



Note

A quad is a group of four ports with common speeds, 1G/10G or 25G. You can configure the ports speed by using the **hw-module quad** command.

Production Software Maintenance Updates (SMUs)

A production SMU is a SMU that is formally requested, developed, tested, and released. Production SMUs are intended for use in a live network environment and are formally supported by the Cisco TAC and the relevant development teams. Software bugs identified through software recommendations or Bug Search Tools are not a basis for production SMU requests.

For information on production SMU types, refer the [Production SMU Types](#) section of the *IOS XR Software Maintenance Updates (SMUs)* guide.

Cisco IOS XR Error messages

To view, search, compare, and download Cisco IOS XR Error Messages, refer to the [Cisco IOS XR Error messages](#) tool.

Cisco IOS XR MIBs

To determine the MIBs supported by platform and release, refer to the [Cisco IOS XR MIBs](#) tool.

Related Documentation

The most current Cisco NCS 5500 router documentation is located at the following URL:

<https://www.cisco.com/c/en/us/td/docs/iosxr/ios-xr.html>



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.