



# Release Notes for Cisco NCS 560 Series Routers, Cisco IOS XR Release 24.1.1

First Published: 2024-03-14

## Network Convergence System 560 Series Routers

### What's New in Cisco IOS XR Release 24.1.1

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
<b>Licensing</b>	
<a href="#">Smart Licensing Using Policy</a>	<p>Cisco Smart Licensing Using Policy (SLP) is an enhancement to the existing Cisco Smart Licensing model. It streamlines the licensing process for Cisco IOS XR products by introducing a more flexible and automated approach. With SLP, you no longer need to register your device during installation, and there is no evaluation license state or period. This simplifies the licensing process and reduces complexity. To use SLP, your devices must establish trust and send the initial license usage report within 90 days.</p> <p>Starting with this release, <b>cslu</b> is the default communication transport mode.</p> <p>The feature introduces these changes:</p> <p><b>YANG Data Models:</b></p> <ul style="list-style-type: none"><li>• Cisco-IOS-XR-smart-license-cfg.yang (see <a href="#">GitHub</a>, <a href="#">YANG Data Models Navigator</a>)</li></ul>
<b>MPLS</b>	

Feature	Description
<a href="#">Set Global RSVP Message Retransmission Interval</a>	<p>During Fast Reroute (FRR), an RSVP router sends multiple messages to neighbors. If a neighbor fails to acknowledge the messages due to an overload of RSVP message processing or a high frequency of failures, RSVP retransmits the messages, which can result in network congestion. You can now set a longer RSVP message retransmission interval to provide sufficient processing time for neighbors, reduce signaling overhead, and prevent network congestion.</p> <p>You can set this interval for all directly connected neighbors at once or remote neighbors connected through backup tunnels. Previously, you could only enable this option per interface.</p> <p>The feature introduces these changes:</p> <p><b>CLI:</b> <a href="#">signalling refresh reduction reliable retransmit-time</a></p> <p><b>YANG Data Model:</b> Cisco-IOS-XR-ip-rsvp-cfg.yang (see <a href="#">GitHub</a>, <a href="#">YANG Data Models Navigator</a>)</p>
<b>IP Addresses and Services</b>	
<a href="#">View NPU Information to Troubleshoot Forwarding Issues</a>	<p>You can now easily access NPU information such as the TCAM, Large Exact Match (LEM), Longest Prefix Match (LPM), Forwarding Equivalence Class (FEC) and Encapsulation DB (EEDB) database information for troubleshooting forwarding issues. Before this release, obtaining NPU information was a time-consuming process that required using the forwarding ASIC's diagnostic shell utility with varying commands across forwarding ASICs.</p> <p>The feature introduces these changes:</p> <p><b>CLI:</b></p> <p>This feature modifies the <b>show mpls forwarding labels hardware</b> command. The <b>npu</b> keyword is added to it.</p>
<b>Interface and Hardware Component</b>	
<a href="#">Autonegotiation Support on the A900-IMA-8CS1Z Interface Module</a>	<p>The A900-IMA-8CS1Z Interface Module now supports autonegotiation for speeds less than 1G (10/100/1000 Mbps) using <a href="#">Cisco 1000BASE-T Copper SFP</a>.</p> <p>By default, autonegotiation remains disabled. You can enable autonegotiation on the Gigabit Ethernet interface using the <a href="#">negotiation auto</a> command. After you enable autonegotiation, the link will auto-negotiate seamlessly to the configuration that is compatible with a peer device.</p>
<b>L2VPN and Ethernet Services</b>	

Feature	Description
<a href="#">EVPN Non-Revertive Designated Forwarder Election</a>	<p>In a preference-based Designated Forwarder (DF) election, non-revertive mode prevents the traffic disruption that occurs during the recovery of a node in a port-active multihomed network.</p> <p>While recovering from a link failure, an EVPN ethernet-segment (ES) performs DF re-election and re-carves the services among the multihomed nodes, which causes traffic interruption and interface flapping, leading to traffic loss. In the non-revertive mode, the EVPN ES does not re-carve the services after the recovery, thus avoiding the traffic disruption.</p> <p>The feature introduces these changes:</p> <p><b>CLI:</b></p> <ul style="list-style-type: none"> <li>• <b>non-revertive</b></li> <li>• <b>revert</b></li> <li>• The <b>ethernet-segment interface</b> <i>interface-name</i> <b>revert</b> keyword is introduced in the <b>l2vpn evpn</b> command.</li> </ul> <p><b>YANG Data Model:</b></p> <ul style="list-style-type: none"> <li>• Cisco-IOS-XR-evpn-oper.yang</li> <li>• Cisco-IOS-XR-l2vpn-cfg.yang</li> </ul> <p>(see <a href="#">GitHub</a>, <a href="#">YANG Data Models Navigator</a>)</p>
<b>Programmability</b>	
<a href="#">View Inconsistent OpenConfig Configuration</a>	<p>OpenConfig infrastructure now provides an operational data YANG model, <i>Cisco-IOS-XR-yiny-oper</i>, which can be queried to view the inconsistent OpenConfig configuration caused due to activities such as interface breakout operations, installation activities or insertion of a new line card.</p> <p>See <a href="#">GitHub</a>, <a href="#">YANG Data Models Navigator</a></p>
<a href="#">Certificate Common-Name For Dial-in Using gRPC Protocol</a>	<p>You can now specify a <b>common-name</b> for the certificate generated by the router while using gRPC dial-in and avoid failure during certificate verification. Earlier, the <b>common-name</b> in the certificate was fixed.</p> <p>The feature introduces these changes:</p> <p><b>CLI:</b></p> <ul style="list-style-type: none"> <li>• <b>gRPC certificate common-name</b></li> </ul> <p><b>YANG Data Model:</b></p> <ul style="list-style-type: none"> <li>• Cisco-IOS-XR-um-grpc-cfg.yang</li> <li>• Cisco-IOS-XR-man-ems-cfg</li> </ul> <p>(see <a href="#">GitHub</a>, <a href="#">YANG Data Models Navigator</a>)</p>

Feature	Description
<a href="#">gRPC Authentication Modes</a>	This feature lists the four types of authentication mechanisms for Extensible Manageability Services (EMS) to ensure the security and integrity of data exchange are: Metadata with TLS, Metadata without TLS, Metadata with Mutual TLS, and Certificate based.
<b>System Management</b>	
<a href="#">Combined Frame Delay and Frame Loss Measurement for Y.1564 Service Activation Test</a>	<p>We have enhanced the ITU-T Y.1564 Service Activation Testing (SAT) capabilities by enabling a comprehensive service quality measurement that includes network responsiveness, congestion, and other issues degrading network performance. This feature also allows a holistic testing of the QoS SLAs, which helps identify potential issues faster and troubleshoot effectively.</p> <p>This feature introduces the following change:</p> <p><b>CLI:</b></p> <p>The <b>measurement combined</b> keyword is added to the <b>ethernet service-activation-test profile</b> command.</p> <p><b>YANG DATA Model:</b></p> <ul style="list-style-type: none"> <li>• New XPath for Cisco-IOS-XR-ethernet-sat-cfg.yang (see <a href="#">Github</a>, <a href="#">YANG Data Models Navigator</a>)</li> </ul>
<a href="#">Loopback Frames for Y.1564 Service Activation Test</a>	<p>This feature enables the redirection of test traffic from the destination router to the source router in loopback message (LBM) format. Loopback message enables the measurement of various parameters and performance metrics, such as frame delay, frame loss rates, and QoS settings, after the traffic has completed its round trip.</p> <p>Such comprehensive measurement helps identify issues within the network setup. You can also use it to ensure the service is running and meets the SLA.</p> <p>This feature introduces the following change:</p> <p><b>CLI:</b></p> <p>The <b>packet-format lbm</b> keyword is added to the <b>ethernet service-activation-test profile</b> command.</p> <p><b>YANG DATA Model:</b> New XPath for Cisco-IOS-XR-ethernet-sat-cfg.yang (see <a href="#">Github</a>, <a href="#">YANG Data Models Navigator</a>)</p>
<a href="#">Optional Source MAC Address for Y.1564 Service Activation Test</a>	<p>By specifying the source MAC address to the ITU-T Y.1564 SAT, you can ensure that the test results are relevant and applicable to the specific service configuration for use in production and before deployment for your customers.</p> <p>This feature introduces the following change:</p> <p><b>Modified CLI:</b></p> <p>The <b>source</b> keyword is added to the <b>ethernet service-activation-test</b> command.</p> <p><b>YANG DATA Model:</b></p> <ul style="list-style-type: none"> <li>• New XPath for Cisco-IOS-XR-ethernet-sat-act.yang (see <a href="#">Github</a>, <a href="#">YANG Data Models Navigator</a>)</li> </ul>

Feature	Description
<b>Segment Routing</b>	
<a href="#">SR-MPLSv6 Traffic Engineering</a>	We have introduced the capability for SR Policy to support segment lists with IPv6 addresses, which can be either dynamically computed or explicitly set at the SRTE headend.
<a href="#">Identical Route Distinguisher (RD) for Interworking Gateways between MPLS and SRv6 Domains</a>	<p>You can now configure the same Route Distinguisher (RD) for interworking gateways catering to both MPLS and SRv6 domains that help conserve hardware resources, reduce the BGP table scale and minimize the processing load on routers. At the same time, it ensures seamless connectivity across SRv6 and MPLS L3 EVPN domains, thus promoting interoperability and efficiency in modern network environments.</p> <p>Previously, a unique RD was required to extend L3 services between MPLS and SRv6 domains resulting in higher router load and resource consumption, which could have affected performance.</p>
Ability to Exclude Specific IP Addresses in Multi-Domain Path Computation	This release supports the ability to exclude specific IP addresses in multi-domain path computation. Segment Routing Path Computation Element (SR-PCE) needs to remove the excluded nodes or links from its topology when computing the CSPF path from headend to endpoint.
<a href="#">Reporting of SR-TE Policies Using BGP-Link State for SRv6</a>	<p>You can gather the Traffic Engineering Policy information that is locally available in a node and advertise it in BGP-LS for SRv6. Previous versions only supported SR-MPLS.</p> <p>There are no changes to the configuration procedures from previous releases and works on the same configuration as the SR-MPLS feature.</p>
Calculate candidate paths and SR-TE policies with IP exclusion, while enforcing affinity and disjointness constraints	<p>For new services using Pseudo-wire (PW) over SR-TE policies, you can now calculate, customize, and preview candidate paths. With this feature, you can now exclude network resources by IP address, and enforce affinity for a specific candidate path.</p> <p>Previously, affinity constraints and candidate path disjointness were mutually exclusive. The feature introduces these changes:</p> <p><b>CLI:</b></p> <ul style="list-style-type: none"> <li>The feature introduces <b>shortest-path</b> and <b>exclude-resources</b> keywords in the <b>segment-routing traffic-eng policy</b> and <b>segment-routing traffic-eng on-demand color</b> commands.</li> </ul> <p><b>YANG Data Models:</b></p> <ul style="list-style-type: none"> <li>Cisco-IOS-XR-infra-xtc-oper.yang</li> <li>Cisco-IOS-XR-infra-xtc-agent-oper.yang</li> <li>Cisco-IOS-XR-infra-xtc-agent-cfg.yang</li> </ul>
<b>System Security</b>	

Feature	Description
<a href="#">Interaction with MASA through gRPC</a>	From this release, you can use the gRPC protocol to interact with MASA APIs in addition to the current HTTP protocols. Through structured serialization of data with gRPC's Protocol Buffers, the communication between services is made more efficient, type-safe, and consistent.
<a href="#">Multi-Factor Authentication for SSH</a>	You can now deploy robust authentication mechanisms for SSH connections to your routers and reduce security risks due to compromised or weak passwords. We now support multi-factor authentication (MFA)—a secure access management solution that verifies the identity of a user using multiple verification factors—for SSH login on Cisco IOS XR routers. These verification factors include a combination of login credentials such as username and password and a token, a cryptographic device, or a mobile phone with MFA application installed.  No new commands or data models were introduced or modified as part of this feature.
<a href="#">Pre-upload Pinned-Domain Certificate</a>	You can now pre-upload your Pinned-Domain Certificate (PDC) credentials before requesting OV's Ownership Vouchers (OVs) from the MASA server, thus making the voucher request process easier.
<b>Network Synchronization</b>	
<a href="#">PTP-NTP Interworking</a>	We have improved NTP synchronization and reliability to achieve nanosecond-level accuracy for applications that require high-precision timing. This is achieved by enabling NTP-PTP interworking which allows the use of PTP as the reference clock.  As in previous releases, the NTP client continues to support polling NTP protocol-based external time servers to synchronize the local system clock and achieve accuracy within the millisecond range.

## 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.

To get started with using data models, see the *Programmability Configuration Guide for Cisco NCS 560 Series Routers*.

Feature	Description
<b>Programmability</b>	

Feature	Description
openconfig-mpls-ldp.yang Version 3.1.0	<p>This OpenConfig data model introduces the following changes:</p> <ul style="list-style-type: none"> <li>• Enable and authenticate LDP signalling messages using <b>enable</b> and <b>authentication-key</b> leaves globally for all interfaces or for LDP neighbors.</li> <li>• Configure the global and neighbor label switch identifier for the router using <b>lsr-id</b> leaf</li> <li>• Define the time for which a neighbor adjacency will be kept by the router while it waits for a new "hello" message using <b>hello-holdtime</b> leaf</li> <li>• Define the interval for sending these "hello" messages on each link LDP adjacency using <b>hello-interval</b> leaf</li> <li>• Enable and configure the address family name for IPv4 and IPv6 interfaces using <b>enabled</b> and <b>afi-name</b> leaves</li> <li>• Configure the list of LDP configurations for each interface using <b>interface-id</b> leaf where the interface referenced is based on the interface and subinterface leaves within the <b>interface-ref</b> container</li> <li>• Define the list of LDP neighbors and their attributes using <b>label-space-id</b> leaf</li> <li>• Configure the list for attributes related to address families for targeted LDP using <b>afi-name</b> leaf</li> <li>• Specify the neighbor address of the targeted LDP session using <b>remote-address</b> leaf</li> <li>• Enable or disable the acceptance of targeted LDP "hello" messages using <b>hello-accept</b> leaf</li> <li>• Enable and configure the interval for which the remote LDP peers wait for the local node to reconnect gracefully after a failure using <b>enable</b> and <b>reconnect-time</b> leaves</li> <li>• Configure the time interval to gracefully restart a Label Switch Router's (LSR) forwarding when in recovery mode using <b>forwarding-holdtime</b> leaf</li> </ul>
Cisco-IOS-XR-evpn-oper.yang	<p>This YANG model is modified to enable non-revertive mode on preference based EVPN DF election.</p>

Feature	Description
Cisco-IOS-XR-infra-xtc-agent-oper.yang	This native data model is enhanced with a new container, <i>excluded-resources</i> to display associated resource lists for policies.
Cisco-IOS-XR-infra-xtc-oper.yang	This native data model is enhanced with a new container, <i>constraints-information</i> , to exclude IP constraints for candidate paths and includes the shortest-path flag in the disjoint constraints.
Cisco-IOS-XR-infra-xtc-agent-cfg.yang	This native data model is enhanced with a new container, <i>resources</i> , and a new leaf, <i>exclude-resource-rule</i> in the <i>resources-rule-table</i> container to configure and associate resource lists as constraints to policies. Additionally, new leaves such as <i>shortest-path</i> and <i>fallback-disable</i> are added in the <i>disjoint-path</i> container to extend the disjoint constraint configuration.

## Hardware Introduced



**Note** Before you install the Cisco router, you must prepare your site for the installation, for more details on site planning and environmental requirements, see [Hardware Installation Guide](#).

Hardware	Description
Optics	<p>This release launches 400G Digital Coherent QSFP-DD transceiver optics on selective hardware within the product portfolio. For details and other new supported transceivers, refer to the <a href="#">Transceiver Module Group (TMG) Compatibility Matrix</a>.</p> <ul style="list-style-type: none"> <li>Cisco Quad Small Form-Factor Pluggable Double Density (QSFP-DD) <ul style="list-style-type: none"> <li><a href="#">DP04QSDD-HE0</a></li> </ul> </li> </ul>

## Behavior Changes

- From this release, the default order of authentication methods for SSH clients on Cisco IOS XR routers running Cisco IOS XR SSH is changed to: **public-key**, **keyboard-interactive**, and **password**.  
Prior to this release, the default order was: **public-key**, **password**, and **keyboard-interactive**.
- Prior to Cisco IOS XR Release 7.2.1, a segment of an explicit segment list can be configured as an IPv4 address (representing a Node or a Link) using the **index indexaddress ipv4 address** command.



Starting with Cisco IOS XR Release 7.2.1, an IPv4-based segment (representing a Node or a Link) can also be configured with the new **index index mpls adjacencyaddress** command. The configuration is stored in NVRAM in the same CLI format used to create it. There is no conversion from the old CLI to the new CLI.

Starting with Cisco IOS XR Release 7.9.1, the old CLI has been deprecated. Old configurations stored in NVRAM will be rejected at boot-up.

As a result, explicit segment lists with IPv4-based segments using the old CLI must be re-configured using the new CLI.

There are no CLI changes for segments configured as MPLS labels using the **index index mpls label label** command.

- If you are on a release before Cisco IOS XR Release 7.4.1, you can configure SR-ODN with Flexible Algorithm constraints using the **segment-routing traffic-eng on-demand color color dynamic sid-algorithm algorithm-number** command.

Starting with Cisco IOS XR Release 7.4.1, you can also configure SR-ODN with Flexible Algorithm constraints using the new **segment-routing traffic-eng on-demand color color constraints segments sid-algorithm algorithm-number** command.

From Cisco IOS XR Release 7.9.1, the **segment-routing traffic-eng on-demand color color dynamic sid-algorithm algorithm-number** command is deprecated. Previous configurations stored in NVRAM will be rejected at boot-up. (Performing In-Service Software Upgrade (ISSU) to Cisco IOS XR Release 7.9.1 will also be rejected.)

Hence, for Cisco IOS XR Release 7.9.1, you must reconfigure all SR-ODN configurations with Flexible Algorithm constraints that use the [on-demand dynamic sid-algorithm](#) with the [on-demand constraints](#) command.

## Restrictions and Limitations

- The standby RP may get into 'NOT\_READY' state intermittently due to some network churn, though the corresponding VM is up and running. But this is a transient state and shows that some data aren't in sync between active and standby due to the network churn. After both active and standby are in sync with respect to all the parameters, then the standby RP comes into 'READY' state.

## Caveats

**Table 1: Cisco IOS XR NCS 560 Routers Specific Bugs**

Bug ID	Headline
<a href="#">CSCwj07339</a>	The call-home configurations displayed in the show run call-home command are missing in the show running-config command output.

## Release Package

This following 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.

**Table 2: Release 24.1.1 Packages for Cisco NCS 560 Series Router**

<b>Composite Package</b>		
<b>Feature Set</b>	<b>Filename</b>	<b>Description</b>
Cisco IOS XR IP Unicast Routing Core Bundle	ncs560-mini-x-24.1.1.iso	Contains base image contents that includes: <ul style="list-style-type: none"> <li>• Host operating system</li> <li>• System Admin boot image</li> <li>• IOS XR boot image</li> <li>• BGP packages</li> <li>• OS</li> <li>• Admin</li> <li>• Base</li> <li>• Forwarding</li> <li>• Modular Services Card</li> <li>• Routing</li> <li>• SNMP Agent</li> <li>• Alarm Correlation</li> </ul>
Cisco IOS XR Manageability Package	ncs560-mgbl-1.0.0.0-r2411.x86_64.rpm	Telemetry, Extensible Markup Language (XML), Parser, and HTTP server packages, NETCONF, YANG Models, gRPC.
Cisco IOS XR OSPF package	ncs560-ospf-1.0.0.0-r2411.x86_64.rpm	Supports OSPF
Cisco IOS XR Security Package	ncs560-k9sec-1.0.0.0-r2411.x86_64.rpm	k9sec is needed for IPsec or MACsec and Dot1x and for basic crypto services such as Decryption, Secure Shell (SSH), Secure Socket Layer (SSL), and Public-key infrastructure (PKI).

Composite Package		
Feature Set	Filename	Description
Multicast Package	ncs560-mcast-1.0.0.0-r2411.x86_64.rpm	Supports Multicast  Supports Automatic Multicast Tunneling (AMT), IGMP Multicast Listener Discovery (MLD), Multicast Label Distribution Protocol (MLDP), Multicast Source Discovery Protocol (MSDP) and PIM.
Cisco IOS XR ISIS package	ncs560-isis-1.0.0.0-r2411.x86_64.rpm	Supports Intermediate System to Intermediate System (IS-IS).
Cisco IOS XR USB Boot Package	ncs560-usb_boot-24.1.1.zip	Supports Cisco IOS XR USB Boot Package
Cisco IOS XR MPLS Package	ncs560-mpls-1.0.0.0-r2411.x86_64.rpm ncs560-mpls-te-rsvp-1.0.0.0-r2411.x86_64.rpm	Supports MPLS and MPLS Traffic Engineering (MPLS-TE) RPM. Label Distribution Protocol (LDP), MPLS Forwarding, MPLS Operations, Administration, and Maintenance (OAM), Link Manager Protocol (LMP), Optical User Network Interface (OUNI) and Layer-3 VPN.  Cisco IOS XR MPLS-TE and RSVP Package  MPLS Traffic Engineering (MPLS-TE) and Resource Reservation Protocol (RSVP).
Cisco IOS XR LI Package	ncs560-li-1.0.0.0-r2411.x86_64.rpm	Lawful Intercept
Cisco IOS XR EIGRP Package	ncs560-eigrp-1.0.0.0-r2411.x86_64.rpm	(Optional) Includes EIGRP protocol support software

## Determine Software Version

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

```
RP/0/RP0/CPU0:Router#show version
Cisco IOS XR Software, Version 24.1.1
Copyright (c) 2013-2024 by Cisco Systems, Inc.

Build Information:
  Built By      : swtools
  Built On     : Mon Mar 11 20:01:21 PDT 2024
  Built Host   : iox-ucs-055
  Workspace    : /auto/srcarchive15/prod/24.1.1/ncs560/ws
```

## Determine Firmware Support

```

Version      : 24.1.1
Location     : /opt/cisco/XR/packages/
Label       : 24.1.1

```

```

cisco NCS-560 () processor
System uptime is 3 hours 42 minutes

```

## Determine Firmware Support

Log in to the router and enter the **show fpd package** command to know the release image.

```
RP/0/RP0/CPU0:Router#show fpd package
```

```

=====
                                Field Programmable Device Package
                                =====
Card Type                FPD Description                Req   SW   Min Req  Min Req
=====                =====                Reload Ver   SW Ver   Board Ver
-----                -----
A900-IMA-8Z-L-CC        IMFPGA                          YES   1.50   1.50     0.0
-----
A900-IMA8CS1Z-CC       IMFPGA                          YES   1.115  1.115    0.0
-----
A900-IMA8CS1Z-M        IMFPGA                          YES   1.115  1.115    0.0
-----
A900-IMA8Z              IMFPGA                          YES   17.05  17.05    0.0
-----
A900-IMA8Z-CC          IMFPGA                          YES   17.05  17.05    0.0
-----
A900-IMA8Z-L           IMFPGA                          YES   1.50   1.50     0.0
-----
A900-PWR1200-A         DCA-PrimMCU (A)                 NO    0.11   0.11     0.0
                        DCA-SecMCU (A)                 NO    1.04   1.04     0.0
-----
A900-PWR1200-D         LIT-PrimMCU (A)                 NO    2.04   0.04     0.0
                        LIT-SecMCU (A)                 NO    1.27   1.27     0.0
-----
A900-PWR900-D2         LIT-PrimMCU (A)                 NO    1.82   1.82     0.0
                        LIT-SecMCU (A)                 NO    1.84   1.84     0.0
-----
A907-FAN-E             PSOC (A)                        NO    1.65   1.65     0.0
                        PSOC (A)                        NO    1.66   1.66     0.4
-----
A907-FAN-H             PSOC (A)                        NO    1.65   1.65     0.0
-----
ASR914-F2B-FAN         PSOC (A)                        NO    44.08  44.08    0.0
-----
N560-4-FAN-H           PSOC (A)                        NO    177.02 177.02   0.0
-----
N560-4-FAN-H-CC       PSOC (A)                        NO    177.02 177.02   0.0
-----
N560-4-FAN-H-R        PSOC (A)                        NO    177.02 177.02   0.0
-----
N560-4-PWR-FAN         PSOC (A)                        NO    177.08 177.08   0.0
-----
N560-4-PWR-FAN-CC     PSOC (A)                        NO    177.08 177.08   0.0
-----
N560-4-PWR-FAN-R      PSOC (A)                        NO    177.08 177.08   0.0
-----
N560-4-RSP4           ADM (A)                         NO    1.06   1.06     0.0
                        IOFPGA (A)                      YES   0.68   0.68     0.0
                        PRIMARY-BIOS (A)                YES   0.23   0.23     0.0

```

	SATA (A)	NO	2.20	2.20	0.0
	SATA_MAR (A)	NO	1.30	1.30	0.0
	SATA_MAR_B4 (A)	NO	1.10	1.10	0.0
	SATA_SMI (A)	NO	1.10	1.10	0.0
-----					
N560-4-RSP4-CC	ADM (A)	NO	1.06	1.06	0.0
	IOFPGA (A)	YES	0.68	0.68	0.0
	PRIMARY-BIOS (A)	YES	0.23	0.23	0.0
	SATA (A)	NO	2.20	2.20	0.0
	SATA_MAR (A)	NO	1.30	1.30	0.0
	SATA_MAR_B4 (A)	NO	1.10	1.10	0.0
	SATA_SMI (A)	NO	1.10	1.10	0.0
-----					
N560-4-RSP4E	ADM (A)	NO	1.06	1.06	0.0
	IOFPGA (A)	YES	0.68	0.68	0.0
	PRIMARY-BIOS (A)	YES	0.23	0.23	0.0
	SATA (A)	NO	2.20	2.20	0.0
	SATA_MAR (A)	NO	1.30	1.30	0.0
	SATA_MAR_B4 (A)	NO	1.10	1.10	0.0
	SATA_SMI (A)	NO	1.10	1.10	0.0
-----					
N560-4-RSP4E-CC	ADM (A)	NO	1.06	1.06	0.0
	IOFPGA (A)	YES	0.68	0.68	0.0
	PRIMARY-BIOS (A)	YES	0.23	0.23	0.0
	SATA (A)	NO	2.20	2.20	0.0
	SATA_MAR (A)	NO	1.30	1.30	0.0
	SATA_MAR_B4 (A)	NO	1.10	1.10	0.0
	SATA_SMI (A)	NO	1.10	1.10	0.0
-----					
N560-FAN-H	PSOC (A)	NO	2.02	2.02	0.0
-----					
N560-IMA-8Q/4L	IMFPGA	YES	1.27	1.27	0.0
-----					
N560-IMA1W	CFP2-D-DCO	NO	38.27397	38.27397	0.0
	CFP2-DE-DCO	NO	38.27397	38.27397	0.0
	CFP2-DET-DCO	NO	38.27397	38.27397	0.0
	CFP2-DETS-DCO	NO	38.27397	38.27397	0.0
	CFP2-DS-DCO	NO	38.27397	38.27397	0.0
	CFP2-DS100-DCO	NO	38.27397	38.27397	0.0
	IMFPGA	YES	1.28	1.28	0.0
-----					
N560-IMA2C	IMFPGA	YES	6.06	6.06	0.0
-----					
N560-IMA2C-CC	IMFPGA	YES	6.06	6.06	0.0
-----					
N560-IMA2C-DD	IMFPGA	YES	1.28	1.28	0.0
	QDD_100_BRT_FW_P0	NO	70.130	70.130	0.0
	QDD_100_BRT_FW_P1	NO	70.130	70.130	0.0
	QDD_100_FW_P0	NO	61.23	61.23	0.0
	QDD_100_FW_P1	NO	61.23	61.23	0.0
-----					
N560-IMA2C-L	IMFPGA	YES	1.28	1.28	0.0
-----					
N560-PWR1200-D-E	QCS-PrimMCU (A)	NO	1.82	1.82	0.0
	QCS-SecMCU (A)	NO	1.84	1.84	0.0
-----					
N560-RSP4	ADM (A)	NO	1.06	1.06	0.0
	IOFPGA (A)	YES	0.79	0.79	0.0
	PRIMARY-BIOS (A)	YES	0.23	0.23	0.0
	SATA (A)	NO	2.20	2.20	0.0
	SATA_MAR (A)	NO	1.30	1.30	0.0
	SATA_MAR_B4 (A)	NO	1.10	1.10	0.0
	SATA_SMI (A)	NO	1.10	1.10	0.0
-----					

## Determine Firmware Support

N560-RSP4-E	ADM (A)	NO	1.06	1.06	0.0
	IOFPGA (A)	YES	0.79	0.79	0.0
	PRIMARY-BIOS (A)	YES	0.23	0.23	0.0
	SATA (A)	NO	2.20	2.20	0.0
	SATA_MAR (A)	NO	1.30	1.30	0.0
	SATA_MAR_B4 (A)	NO	1.10	1.10	0.0
	SATA_SMI (A)	NO	1.10	1.10	0.0
-----					
NCS4200-1T16G-PS	IMFPGA	YES	1.115	1.115	0.0
-----					
NCS4200-2H-PQ	IMFPGA	YES	6.06	6.06	0.0
-----					
NCS4200-8T-PS	IMFPGA	YES	17.05	17.05	0.0
-----					
NCS4216-F2B-FAN	PSOC (A)	NO	44.08	44.08	0.0
-----					
NCS4216-RSP-800	ADM (A)	NO	1.06	1.06	0.0
	IOFPGA (A)	YES	0.02	0.02	0.0
	PRIMARY-BIOS (A)	YES	0.23	0.23	0.0
	SATA (A)	NO	2.20	2.20	0.0
	SATA_MAR (A)	NO	1.30	1.30	0.0
	SATA_MAR_B4 (A)	NO	1.10	1.10	0.0
	SATA_SMI (A)	NO	1.10	1.10	0.0

Log in to the router and enter the **show hw-module fpd** command to know the current version.

```
RP/0/RP0/CPU0:Router#show hw-module fpd
Auto-upgrade:Enabled
```

Location	Card type	HWver	FPD device	ATR Status	FPD Versions	
					Running	Programd
0/0	A900-IMA8Z	0.0	IMFPGA	CURRENT	17.05	17.05
0/2	A900-IMA8CS1Z-M	0.0	IMFPGA	CURRENT	1.115	1.115
0/3	A900-IMA8CS1Z-M	0.0	IMFPGA	CURRENT	1.115	1.115
0/4	A900-IMA8Z	0.0	IMFPGA	CURRENT	17.05	17.05
0/5	A900-IMA8Z	0.0	IMFPGA	CURRENT	17.05	17.05
0/RP0	N560-4-RSP4E	0.0	ADM	CURRENT	1.06	1.06
0/RP0	N560-4-RSP4E	0.0	IOFPGA	CURRENT	0.68	0.68
0/RP0	N560-4-RSP4E	0.0	PRIMARY-BIOS	CURRENT	0.23	0.23
0/RP0	N560-4-RSP4E	0.0	SATA	CURRENT	2.20	2.20
0/RP1	N560-4-RSP4E	0.0	ADM	CURRENT	1.06	1.06
0/RP1	N560-4-RSP4E	0.0	IOFPGA	CURRENT	0.68	0.68
0/RP1	N560-4-RSP4E	0.0	PRIMARY-BIOS	CURRENT	0.23	0.23
0/RP1	N560-4-RSP4E	0.0	SATA	CURRENT	2.20	2.20
0/FT0	N560-4-PWR-FAN-R	1.0	PSOC	CURRENT	177.08	177.08
0/FT1	N560-4-FAN-H-R	1.0	PSOC	CURRENT	177.02	177.02
0/FT2	N560-4-FAN-H-R	1.0	PSOC	CURRENT	177.02	177.02
0/PM1	A900-PWR1200-A	0.1	DCA-PrimCU	CURRENT	0.14	0.14

0/PM1

A900-PWR1200-A

0.1

DCA-SecMCU

CURRENT

3.00

3.00

## Important Notes

### Licensing

Starting with Cisco IOS XR Release 24.1.1, Smart Licensing Using Policy (SLP) is the default Licensing model. When you upgrade to the Cisco IOS XR Release 24.1.1 release or later, the Smart Licensing Using Policy is enabled by default.

You can migrate your devices to Smart Licensing with Policy model, see *Migrating from Smart Licensing to Smart Licensing Using Policy*, [Smart Licensing Using Policy on Cisco IOS XR Routers](#).

We recommend that you update to the latest version of [SSM On-Prem](#) or [Cisco Smart Licensing Utility](#).



---

**Note** SSM On-Prem and CSSM both support SLP devices and SL devices. SLP devices and SL devices can coexist in a network. The Smart Licensing (SL) model is available in releases Cisco IOS XR Release 7.11.1 and earlier.

---

### Supported Transceiver Modules

For more information on the supported transceiver modules, see [Transceiver Module Group \(TMG\) Compatibility Matrix](#). In the **Begin your Search** search box, enter the keyword NCS560 and click **Enter**.

### Upgrading Cisco IOS XR Software

For software installation and upgrades, refer to the respective upgrade/downgrade docs *.tar* files based on your [560 router variant](#).

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).

The upgrade document for Cisco NCS 560 router is available along with the software image in *NCS560\_Upgrade\_MOP\_24.1.1.tar* file.

### 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 560 router documentation is located at the following URL:

<https://www.cisco.com/c/en/us/td/docs/iosxr/ncs-560-series-routers.html>



---

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.