Release Notes for Cisco NCS 560 Series Routers, Cisco IOS XR Release 7.2.1

First Published: 2020-08-14

Network Convergence System 560 Series Routers

Note *This software release has reached end-of-life status. For more information, see the* End-of-Life and End-of-Sale Notices.

Note Explore the Content Hub, the all new portal that offers an enhanced product documentation experience.

- Use faceted search to locate content that is most relevant to you.
- Create customized PDFs for ready reference.
- Benefit from context-based recommendations.

Get started with the Content Hub at content.cisco.com to craft a personalized documentation experience.

Do provide feedback about your experience with the Content Hub.

What's New in Cisco IOS XR Release 7.2.1

Cisco is continuously enhancing the product with every release and this section covers a brief description of key features and enhancements. It also includes links to detailed documentation, where available.

Software

802.1X Control for VLAN Tag Subinterfaces with Multi-host and Multi-auth Capability

Previously, by default, 802.1X allowed only one MAC address on each port at a time. This lead to major constraint in current network deployments where multiple hosts or MAC addresses were connected on a single port. Now, multi-auth and multi-host modes are supported by 802.1X to allow multiple hosts or MAC addresses on a single port. By default, dot1x configured port is in multi-auth mode. However, this behaviour can be altered by changing the host mode under dot1x profile. 802.1X port-control is also supported on pre-configured VLAN sub-interfaces along with multi-auth and multi-host modes. For VLAN sub-interfaces with VLAN IDs to be pre-configured, VLAN tagged traffic is allowed only after successful 802.1X authentication of the port.

For more information, see Protect Network using IEEE 802.1X Port-Based Authentication.

The command, dot1x host-mode is introduced.

BFD over Bundle with IPv4 Unnumbered Interface

BFD over Bundle with IPv4 Unnumbered Interface feature enables BFD to run on IP unnumbered interfaces, which take the IP address from the loopback address. This feature saves IP addresses space or range. The same loopback address is used on multiple interfaces.

For more information, see BFD over Bundle with IPv4 Unnumbered Interface

BFD Support on HSRP/VRRP

With the introduction of the BFD support on HSRP/VRRP, HSRP/VRRP will use BFD to detect a link failure and facilitate fast failover times without excessive control packet overhead.

With this feature, you can:

- Identify failure detection in less than one second.
- Support all types of encapsulation.
- Have support for almost all routing protocols.

For more information, see:

- Implementing HSRP
- Implementing VRRP

BGP Flowspec

This feature allows you to construct instructions to match a particular flow with IPv4 and IPv6 source, IPv4 and IPv6 destination, L4 parameters and packet specifics such as length, fragment, destination port and source port, actions that must be taken, such as dropping the traffic, or policing it at a definite rate, or redirect the traffic, through a BGP update.

For more information, see BGP Flowspec Overview.

BVI with Double-Tagged AC Support

The Bridge-group Virtual Interface (BVI) with Double-Tagged AC Support feature allows you to configure the attachment circuit (AC) with double-VLAN tag encapsulation on the BVI. You must specify the rewrite ingress pop 2 symmetric option when you configure the AC on the BVI with double-VLAN tag encapsulation.

For more information, see Configure VLAN Sub-Interfaces.

Conform Aware Hierarchical Policy

Traditional Hierarchical QoS (H-QoS), while allowing for granular and multi-level management of traffic, does not allow for conforming traffic from a child-level policy to a parent-level policy to get priority. This inability means that in case of excess traffic, the parent policer drops conforming traffic packets as well.

With the conform-aware hierarchical policy feature, the parent policer is prevented from dropping any conforming traffic from child policers, thus increasing traffic throughput and efficiency.

For more information, see Conform Aware Hierarchical Policy Overview.

The command, hw-module profile qos conform-aware-policer is introduced.

Egress Interface Published as Part of Ingress NetFlow

With the introduction of egress interface published as part of ingress NetFlow, you can capture traffic flow for IP packets on the egress interface or on the outgoing interface of a router.

For more information, see IPFIX 315 Implementation Considerations.

EVPN Convergence Improvements

With the introduction of the EVPN convergence improvements for BGP PIC, the following networks are supported, which rides over BGP PIC as transport:

- LxVPN
- EVPN
- 6PE
- 6VPE

For more information, see BGP PIC Implementation Considerations.

EVPN E-Tree Using RT Constraints

The EVPN E-Tree using Route Target (RT) constraints feature enables you to configure BGP RT import and export policies for an attachment circuit (AC). This feature allows you to define communication between the leaf and root nodes. The provider edge (PE) nodes can receive L2 traffic either from the attachment circuit (AC) of a bridge domain (BD) or from the remote PE node. For a given BD, L2 communication can only happen from a root to leaf and leaf to root nodes. This feature does not allow any L2 communication between the ACs of two or more leafs.

This feature provides the following benefits:

- Achieve efficiency of the BGP MAC routes scale
- Reduce the consumption of hardware resources
- Utilize the link bandwidth efficiently

For more information, see EVPN E-Tree Using RT Constraints.

The command, etree rt-leaf is introduced.

GTP Load Balancing

The GPRS Tunneling Protocol (GTP) Load Balancing feature enables efficient distribution of traffic in mobile networks, and provides increased reliability and availability for the network.

GTP load balancing is performed on IPv4 or IPv6 incoming packets with GTP payloads and on MPLS incoming labeled packets. This feature supports GTP hashing only when the GTP UDP port is 2152.

The number of MPLS label stack in the transport layer is limited to three for GTP hashing. GTP hashing is not considered when the MPLS label stack exceeds three.

For more information, see GTP Load Balancing.

Manual BGP Peering SIDs for Segment Routing Egress Peer Engineering

This release introduces support for manually configured BGP Egress Peer Engineering (EPE) Peer SIDs. The ability to manually configure BGP-EPE peer SIDs allows for persistent EPE label values. Manual BGP-EPE SIDs are advertised through BGP-LS and are allocated from the Segment Routing Local Block (SRLB).

For more information, see Configuring Manual BGP-EPE Peering SIDs.

Network Convergence Using Core Isolation Protection

The Network Convergence using Core Isolation Protection feature allows the router to converge fast when remote links and local interfaces fail. This feature reduces the duration of traffic drop by rapidly rerouting traffic to alternate paths. This feature uses Object Tracking (OT) to detect remote link failure and failure of connected interfaces.

Tracking interfaces can only detect failure of connected interfaces and not failure of a remote router interfaces that provides connectivity to the core. Tracking one or more BGP neighbor sessions along with one or more of the neighbor's address-families enables you to detect remote link failure.

For more information, see Network Convergence using Core Isolation Protection.

The command, if track is is introduced.

Per-Flow Automated Steering

Currently, the steering of traffic through a Segment Routing (SR) policy is based on the candidate paths of that policy. For a given policy, a candidate path specifies the path to be used to steer traffic to the policy's destination. The policy determines which candidate path to use based on the candidate path's preference and state. The candidate path that is valid and has the highest preference is used to steer all traffic using the given policy. This type of policy is called a Per-Destination Policy (PDP).

Per-Flow Automated Traffic Steering introduces a way to steer traffic on an SR policy based on the attributes of the incoming packets, called a Per-Flow Policy (PFP). A PFP provides up to 8 "ways" or options to the endpoint. With a PFP, packets are classified by a classification policy and marked using internal tags called forward classes (FCs). The FC setting of the packet selects the "way". For example, this "way" can be a traffic-engineered SR path, using a low-delay path to the endpoint. The FC is represented as a numeral with a value of 0 to 7.

For more information, see Per-Flow Automated Steering.

Queueing Support for BUM Traffic on Attachment Circuits

This feature allows you to add BUM traffic queueing support for attachment circuits in a bridge domain. BUM traffic is replicated through Ingress Replication, and the replicated packets use the Ingress VOQ. This feature is only supported on single NPU devices, and not on devices with multiple NPUs or line cards.

For more information, see Queueing Support for BUM Traffic on Attachment Circuits.

The command, flood mode ac-ingress-replication is introduced.

Segment Routing BGP Peer-Set SID

Segment routing egress peer engineering (EPE) uses a controller to instruct an ingress provider edge, or a content source (node) within the segment routing domain, to use a specific egress provider edge (node) and a specific external interface to reach a destination. BGP peer SIDs are used to express source-routed interdomain paths. BGP peer SID types include Peer Node SIDs and Peer Adjacency SIDs.

This release adds support for a new type of BGP peering SID, called BGP Peer Set SID. A BGP Peer Set SID is a group or set of BGP peer SIDs, and can be associated with any combination of Peer Node SIDs or Peer Adjacency SIDs. Peer Set SIDs provide load balancing over BGP neighbors (nodes) or links (adjacencies).

For more information, see Segment Routing Egress Peer Engineering.

Segment Routing On-Demand Next Hop for EVPN

Segment Routing On-Demand Next Hop (SR-ODN) allows a service head-end router to automatically instantiate an SR policy to a BGP next-hop when required (on-demand). SR-ODN provides per-destination steering behaviors where a prefix, a set of prefixes, or all prefixes from a service can be associated with a desired underlay SLA. The functionality applies equally to single-domain and multidomain networks.

An on-demand SR policy is created dynamically for BGP global or VPN (service) routes. This release introduces SR-ODN support for EVPN services with either single-homing or multi-homing configurations.

For more information, see On-Demand SR Policy – SR On-Demand Next-Hop.

Segment Routing On-Demand Next Hop for EVPN-VPWS with Multi-Homing

Segment Routing On-Demand Next Hop (SR-ODN) allows a service head-end router to automatically instantiate an SR policy to a BGP next-hop when required (on-demand). SR-ODN provides per-destination steering behaviors where a prefix, a set of prefixes, or all prefixes from a service can be associated with a desired underlay SLA. The functionality applies equally to single-domain and multi-domain networks.

An on-demand SR policy is created dynamically for BGP global or VPN (service) routes. This release introduces SR-ODN support for EVPN-VPWS services with multi-homing configurations.

For more information, see On-Demand SR Policy – SR On-Demand Next-Hop.

Segment Routing Path Computation Element Flexible Algorithm Multi-Domain Path Computation

Currently, a Flexible Algorithm definition is unknown to the Segment Routing Path Computation Element (SR-PCE). In order to select a Flexible Algorithm across domains, Flexible Algorithm definition can now be distributed to a PCE topology database from the gateway ABR/ASBR. The SR-PCE Flexible Algorithm Multi-Domain Path Computation feature incorporates the following changes:

- BGP-LS has been augmented to carry a Flexible Algorithm definition (FAD)
- PCEP vendor-specific objects have been added to indicate SR policy Flexible Algorithm constraints to the PCE and to request a path computation based on the Flexible Algorithm number
- PCE algorithms have been augmented to compute paths based on a Flexible Algorithm constraint

For more information, see SR-PCE Flexible Algorithm Multi-Domain Path Computation.

Segment Routing TI-LFA Support for GRE Tunnels

The Segment Routing TI-LFA (Topology independent Loop-free alternate) Support for GRE Tunnels feature extends the TI-LFA logic to span different instances or different IGP domains by using a Generic Routing Encapsulation (GRE) tunnel that runs between two ABRs as a backup path for TI-LFA protection in an SR Core. GRE is a tunneling protocol that provides a simple generic approach to transport packets of one protocol over another protocol by means of encapsulation.

For more information, see SR-MPLS over GRE as TI-LFA Backup Path.

Set Peak Burst Size for Egress Shaping

From Release 7.2.1 onwards, you can configure peak burst size for egress shaping. This configuration gives your router interface the ability to manage the traffic burst for a particular traffic class such that the peer node can accommodate the burst and does not drop packets either due to lower burst policing or due to shorter queue depth.

For more information, see Configure Traffic Shaping.

The command, shape average is modified.

Shared Policer Feature

With the shared policer feature, you can now share a policer bucket among two or more classes. You can also view the statistics in aggregated mode or per-class mode.

For more information, see Shared Policer.

The command, hw-module profile qos shared-policer-per-class-stats is introduced.

SR-PCE Inter-Domain Path Computation Using SID Redistribution

A Path Computation Element (PCE) computes SR-TE that is paths based on the SR-topology database that stores the connectivity, state, and TE attributes of SR network nodes and links. BGP Labeled Unicast (BGP-LU) provides MPLS transport across IGP boundaries by advertising the loopbacks and label binding of edge and border routers across IGP boundaries.

The SR-PCE Inter-Domain Path Computation Using SID Redistribution feature adds new functionality to the SR-PCE that enables it to compute a path for remote non-SR end-point devices that are distributed by BGP-LU.

For more information, see Inter-Domain Path Computation Using Redistributed SID.

SRv6 Anycast Locator

This feature introduces support for SRv6 Anycast Locator. An SRv6 Anycast locator is a type of locator that identifies a set of nodes (END SIDs). SRv6 Anycast Locators and their associated END SIDs may be provisioned at multiple places in a topology. Anycast routing enables the steering of traffic toward multiple advertising nodes. Packets addressed to an Anycast address are forwarded to the topologically nearest nodes.

One use case is to advertise Anycast END SIDs at exit points from an SRv6 network. Any of the nodes that advertise the common END SID could be used to forward traffic out of the SRv6 portion of the network to the topologically nearest node.

For more information, see Segment Routing over IPv6 Overview.

Support for Chained ACLs

In Cisco NCS 560 Series Routers, you can configure only one ACL per direction on an interface. With the feature, Chained ACLs, you can apply more than one IPv4 or IPv6 ACL (common-acl and interface acl) on an interface for packet filtering at the ingress direction of a router. This feature enables you to separate various types of ACLs for management and other reasons, yet apply both of them on the same interface, in a defined order.

For more information, see Configuring Chained ACLs.

Commands modified for this feature:

- ipv4 access-group

- ipv6 access-group

Support for DHCPv4 and DHCPv6 Client on BVI

The Support for DHCPv4 and DHCPv6 Client over the BVI feature allows you to configure DHCPv4 and DHCPv6 client on the Bridged Virtual Interface (BVI). You can configure a BVI, and request DHCP IPv4 or IPv6 address on the BVI. This configiration allows your customer's device to have initial connectivity to your network without any user intervention in the field. After the device is connected to your network, the customer devices can push a node-specific configuration with static IP addresses on a different BVI for a customer deployment.

For more information, see Support for DHCPv4 and DHCPv6 Client over BVI.

Support for DHCPv6 Client Options

This feature enables the support of DHCPv6 client on BVI interfaces. You can configure different types of DHCP IPv6 client options to enable different types of functionalities for clients as required.

For more information, see Enabling DHCP Client on an Interface.

The command, ipv6 address dhcp-client-options is introduced.

TCP Authentication Option for Segment Routing Path Computation Element

TCP Message Digest 5 (MD5) authentication is used for authenticating PCEP (TCP) sessions by using clear text or encrypted password. This feature introduces TCP Authentication Option (TCP-AO), which replaces the TCP MD5 option. TCP-AO is compatible with Master Key Tuple (MKT) configuration. TCP-AO also protects connections when using the same MKT across repeated instances of a connection. TCP-AO protects the connections by using traffic key that are derived from the MKT, and then coordinates changes between the endpoints.

For more information, see TCP Authentication Option.

UCMP Over MPLS-TE

With this feature, you can lperform oad-balance for incoming traffic over multiple paths of varying costs. UCMP applies a weight to a path, and adds more forwarding instances to a path that has a higher weight (or larger bandwidth). This feature results in an equal load distribution over paths of varying bandwidths (and costs).

For more information, see UCMP Over MPLS-TE.

Hardware

1-port 100G/200G CFP2 DCO Interface Module

The 1-port 100G/200G CFP2 DCO Interface Module (N560-IMA1W) is a single-width-single-height IM for the Cisco NCS 560-4 router and Cisco ASR 907 router with RSP4. This IM supports one CFP2 Digital Coherent Optics (DCO) at 100G/200G (Ethernet/OTU4) capacity.

For more information see Cisco N560-RSP4 and Cisco N560-RSP4-E Route Processor Hardware Installation Guide and Cisco NCS 560-4 Router Hardware Installation Guide.

Interface Module IMA2C Slots

The interface module IMA2C supports new interface slots and optics.

For more information see Cisco N560-RSP4 and Cisco N560-RSP4-E Route Processor Hardware Installation Guide and Cisco NCS 560-4 Router Hardware Installation Guide.

Behavior Change Introduced in this Release

Behavior change refers to any modification of an existing software feature, configuration, or a command. This release introduces following behavior change:

Guidelines for Enabling FIPS

You must follow these guidelines while enabling FIPS mode:

- You must configure the session with a FIPS-approved cryptographic algorithm. A session configured with non-approved cryptographic algorithm for FIPS (such as, MD5 and HMAC-MD5) does not work. This is applicable for OSPF, BGP, RSVP, ISIS, or any application using key chain with non-approved cryptographic algorithm, and only for FIPS mode (that is, when **crypto fips-mode** command is configured).
- If you are using any HMAC-SHA algorithm for a session, then you must ensure that the configured key-string has a minimum length of 14 characters. Otherwise, the session goes down. This is applicable only for FIPS mode.
- If you try to execute the telnet configuration on a system where the FIPS mode is already enabled, then the system rejects the telnet configuration.
- If telnet configuration already exists on the system, and if FIPS mode is enabled later, then the system rejects the telnet connection. But, it does not affect the telnet configuration as such.
- It is recommended to configure the **crypto fips-mode** command first, followed by the FIPS-related commands in a separate commit. The list of commands related to FIPS with non-approved cryptographic algorithms are:
  - **key chain** *key-chain-name* **key** *key-id* **cryptographic-algorithm MD5**
  - **key chain** *key-chain-name* **key** *key-id* **cryptographic-algorithm HMAC-MD5**
  - **router ospfv3 1 authentication ipsec spi 256 md5** *md5-value*
  - **router ospfv3 1 encryption ipsec spi 256 esp des** *des-value*
  - **router ospfv3 1 encryption ipsec spi 256 esp des** *des-value* **authentication md5** *md5-value*
  - **snmp-server user** *username usergroup-name* **v3 auth md5 priv des56**
  - **ssh server algorithms key-exchange diffie-hellman-group1-sha1**
  - **telnet vrf default ipv4 server max-servers** *server-limit*

PSU Redundancy Lost Alarm:

PSU redundancy lost alarms are generated when there is no proper input feed applied on any one of Power Modules (PMs) (PM0 or PM1). The alarms are also generated when the output for PM0 or PM1 is not proper.

The following alarms are raised for PSU redundancy lost event with a faulty PM0:

- Power Module Generic Fault
- Power Module Error
- Power Group Redundancy Lost

This is applicable to the following routers with fixed PSUs:

- N540-28Z4C-SYS-A/D
- N540X-16Z4G8Q2C-A/D
- N540-12Z20G-SYS-A/D
- N540X-12Z16G-SYS-A/D
- N540X-6Z18G-SYS-A/D
- N540X-8Z16G-SYS-A/D
- N540X-4Z14G2Q-A/D

Restrictions and Limitations on the Cisco NCS 560 Series Router

- The **show inventory** and the **show diagnostic** commands do not display the fan serial number.
- The **hw-module profile mfib statistics** command is not supported.
- Ensure that the ISIS hello interval-timer value is not greater than six seconds, otherwise it may result in an ISIS adjacency flap.
- Do not use the Cisco N560-RSP4 and Cisco N560-RSP4-E route processors together in the same router.

Caveats

This section describes open and resolved severity 1 and 2 caveats and select severity 3 caveats:

- The “Open Caveats” sections list open caveats that apply to the current release and may apply to previous releases. A caveat that is open for a prior release and is still unresolved applies to all future releases until it is resolved.
- The “Resolved Caveats” sections list caveats resolved in a specific release, but open in previous releases.

The bug IDs are sorted alphanumerically.

Note The Caveats section includes the bug ID and a short description of the bug. For details on the symptoms, conditions, and workaround for a specific caveat you must use the Bug Search Tool.

Resolved Caveats

The following caveat is applicable for this release.

Bug ID	Headline
CSCvu45149	N560-IMA1W: Standby RP going for reload on IM PCI failure

Bug Search Tool

Use the Cisco Bug Search Tool to access open and resolved bugs for a release.

The tool allows you to search for a specific bug ID, or for all bugs specific to a product and a release.

Supported Packages and System Requirements

For more information on system upgrade and package installation process, see Perform System Upgrade and Install Feature Packages.

For a complete list of supported optics, hardware and ordering information, see the Cisco NCS 560 Series Routers Interface Modules Data Sheet and Cisco Network Convergence System 560-4 Router Data Sheet.

To install the Cisco NCS 560 Series Routers, see Cisco N560-RSP4 and Cisco N560-RSP4-E Route Processor Hardware Installation Guide and Cisco NCS 560-4 Router Hardware Installation Guide.

Release 7.2.1 Packages

This following table lists the supported packages and their corresponding file names.

Table 1: Release 7.2.1 Packages for Cisco NCS 560 Series Router

Composite Package		
Feature Set	**Filename**	**Description**
Cisco IOS XR IP Unicast Routing Core Bundle	ncs560-mini-x-7.2.1.iso	Contains base image contents that includes: • Host operating system • System Admin boot image • IOS XR boot image • BGP packages • OS • Admin • Base • Forwarding • Modular Services Card • Routing • SNMP Agent • Alarm Correlation

Composite Package		
Feature Set	**Filename**	**Description**
Cisco IOS XR Manageability Package	ncs560-mgbl-2.0.0.0-r721.x86_64.rpm	Telemetry, Extensible Markup Language (XML), Parser, and HTTP server packages, NETCONF, YANG Models, gRPC.
Cisco IOS XR OSPF package	ncs560-ospf-2.0.0.0-r721.x86_64.rpm	Supports OSPF
Cisco IOS XR Security Package	ncs560-k9sec-2.0.0.0-r721.x86_64.rpm	Support for Encryption, Decryption, Secure Shell (SSH), Secure Socket Layer (SSL), and Public-key infrastructure (PKI)
Multicast Package	ncs560-mcast-2.0.0.0-r721.x86_64.rpm	Supports Multicast Supports Automatic Multicast Tunneling (AMT), IGMP Multicast Listener Discovery (MLD), Multicast Source Discovery Protocol (MSDP) and PIM.
Cisco IOS XR ISIS package	ncs560-isis-2.0.0.0-r721.x86_64.rpm	Supports Intermediate System to Intermediate System (IS-IS).
Cisco IOS XR USB Boot Package	ncs560-usb_boot-7.2.1.zip	Supports Cisco IOS XR USB Boot Package
Cisco IOS XR MPLS Package	ncs560-mpls-1.0.0.0-r721.x86_64.rpm ncs560-mpls-te-rsvp-2.0.0.0-r721.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-r721.x86_64.rpm	Lawful Intercept
Cisco IOS XR EIGRP Package	ncs560-eigrp-1.0.0.0-r721.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/RP1/CPU0:ROUTER#show version

Thu Aug 13 16:40:16.316 IST
Cisco IOS XR Software, Version 7.2.1
Copyright (c) 2013-2020 by Cisco Systems, Inc.

Build Information:
 Built By     : gopalk2
 Built On     : Wed Aug 12 06:03:09 PDT 2020
 Built Host   : iox-ucs-016
 Workspace    : /auto/srcarchive13/prod/7.2.1/ncs560/ws
 Version      : 7.2.1
 Location     : /opt/cisco/XR/packages/
 Label        : 7.2.1

cisco NCS-560 () processor
System uptime is 4 hours 3 minutes
```

Determine Firmware Support

Log in to the router and enter the **show fpd package** and **show hw-module fpd** commands.

```
RP/0/RP1/CPU0:ROUTER#show hw-module fpd

Thu Aug 13 16:40:28.906 IST
                                                                      FPD Versions
                                                                     ===============
Location  Card type         HWver FPD device       ATR Status   Run    Programd
-------------------------------------------------------------------------------
0/RP0     N560-RSP4-E       0.0   ADM                CURRENT    1.05    1.05
0/RP0     N560-RSP4-E       0.0   IOFPGA             CURRENT    0.56    0.56
0/RP0     N560-RSP4-E       0.0   PRIMARY-BIOS       CURRENT    0.17    0.17
0/RP0     N560-RSP4-E       0.0   SATA               CURRENT    2.10    2.10
0/RP1     N560-RSP4-E       0.0   ADM                CURRENT    1.05    1.05
0/RP1     N560-RSP4-E       0.0   IOFPGA             CURRENT    0.56    0.56
0/RP1     N560-RSP4-E       0.0   PRIMARY-BIOS       CURRENT    0.17    0.17
0/RP1     N560-RSP4-E       0.0   SATA               CURRENT    2.10    2.10
0/FT0     N560-FAN-H        1.0   PSOC               CURRENT    2.02    2.02

RP/0/RP0/CPU0:PE4-RSP4#admin show fpd package

Thu Aug 13 16:40:43.602 IST

================================ ================================================
                                        Field Programmable Device Package
                                 ================================================
                                           Req      SW       Min Req   Min Req
Card Type           FPD Description        Reload   Ver      SW Ver    Board Ver
================== ========================= ====== ======= ======== =========
A900-PWR1200-A      DCA-PriMCU                NO      0.11      0.11      0.0
                    DCA-SecMCU                NO      1.04      1.04      0.0
--------------------------------------------------------------------------------
A900-PWR1200-D      LIT-PriMCU                NO      2.04      0.04      0.0
                    LIT-SecMCU                NO      1.23      1.23      0.0

A907-FAN-E          PSOC                      NO      1.65      1.65      0.0
--------------------------------------------------------------------------------
A907-FAN-E          PSOC                      NO      1.66      1.66      0.4
```

```
--------------------------------------------------------------------------------
N560-4-FAN-H          PSOC                      NO    177.02    177.02       0.0
--------------------------------------------------------------------------------
N560-4-FAN-H-CC       PSOC                      NO    177.02    177.02       0.0
--------------------------------------------------------------------------------
N560-4-PWR-FAN        PSOC                      NO    177.08    177.08       0.0
--------------------------------------------------------------------------------
N560-4-PWR-FAN-CC     PSOC                      NO    177.08    177.08       0.0

N560-4-RSP4           ADM                       NO      1.05      1.05       0.0
                      IOFPGA                    YES     0.55      0.55       0.0
                      PRIMARY-BIOS              YES     0.17      0.17       0.0
                      SATA                      YES     2.10      2.10       0.0
--------------------------------------------------------------------------------
N560-4-RSP4-CC        ADM                       NO      1.05      1.05       0.0
                      IOFPGA                    YES     0.55      0.55       0.0
                      PRIMARY-BIOS              YES     0.17      0.17       0.0
                      SATA                      YES     2.10      2.10       0.0
--------------------------------------------------------------------------------
N560-4-RSP4E          ADM                       NO      1.05      1.05       0.0
                      IOFPGA                    YES     0.55      0.55       0.0
                      PRIMARY-BIOS              YES     0.17      0.17       0.0
                      SATA                      YES     2.10      2.10       0.0
--------------------------------------------------------------------------------
N560-4-RSP4E-CC       ADM                       NO      1.05      1.05       0.0
                      IOFPGA                    YES     0.55      0.55       0.0
                      PRIMARY-BIOS              YES     0.17      0.17       0.0
                      SATA                      YES     2.10      2.10       0.0
--------------------------------------------------------------------------------
N560-FAN-H            PSOC                      NO      2.02      2.02       0.0
--------------------------------------------------------------------------------

                      QCS-SecMCU                NO      1.84      1.84       0.0
--------------------------------------------------------------------------------
N560-RSP4             ADM                       NO      1.05      1.05       0.0
                      IOFPGA                    YES     0.56      0.56       0.0
                      PRIMARY-BIOS              YES     0.17      0.17       0.0
                      SATA                      YES     2.10      2.10       0.0
--------------------------------------------------------------------------------
N560-RSP4-E           ADM                       NO      1.05      1.05       0.0
                      IOFPGA                    YES     0.56      0.56       0.0
                      PRIMARY-BIOS              YES     0.17      0.17       0.0
                      SATA                      YES     2.10      2.10       0.0
--------------------------------------------------------------------------------
```

Other Important Information

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

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 (*NCS560_Upgrade_MOP_7.2.1.tar*) is available along with the software images.

Additional References

Supported MIBs

The Cisco NCS 5500 MIB support list is also applicable to the Cisco NCS 560 Series Routers. For the list of supported MIBs, see the Cisco NCS5500 MIB Support List.

Full Cisco Trademarks with Software License

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.

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)