Release Notes for Cisco NCS 5500 Series Routers, Release 6.1.2

Revised: April 9, 2021

Network Convergence System 5500 Series Routers—Opening the Architecture

Note This product 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.

Key Capabilities

Flexible Packaging—Easy Routine Upgrades and Maintenance

Flexible packaging is an enhancement that modularizes and delivers the Cisco IOS XR operating system as RPM packages.

The base software is becoming leaner that contains only required mandatory packages. Other optional packages are separated out and made available as individually installable RPM packages. Users have the flexibility to select and install the services they want by choosing relevant RPMs. Redhat Package Manager (RPM) based delivery of packages enable easier and faster system updates.

Flexible packaging also supports automatic dependency management whereby, while the user is updating an RPM, the system identifies all relevant dependent packages and updates them. The system uses standard LINUX tools to manage dependency during upgrades.

For the detailed list of release specific feature set matrix (packages) and associated filenames, see , Release 6.1.2 Packages, on page 9

Data Models—Faster Programmatic and Standards-based Configuration

Data models are a programmatic and standards-based way of configuring and collecting operational data of a network device, replacing the process of manual configuration. Using Data models, Cisco IOS XR operating system supports the automating of configurations that belong to multiple routers across the network. Data models are written in a standard, industry-defined language, which can define a new configuration and state an existing configuration on a network.

Traditional CLI-based configurations, are proprietary, cumbersome, and highly text-based. Managing automated operations on a large network using CLIs is a challenge.

Cisco IOS XR supports the YANG data modeling language. YANG can be used with the Network Configuration Protocol (Netconf) or with gRPC (google-defined Remote Procedure Calls) to automate programmable network operations. Data models allow administrators to customize settings easily and automatically, without wasting time on manual configuration.

To get started with using data models, see the Obtain Data Models section in Cisco IOS XR Programmability Configuration Guide for the NCS 5500 Series Router.

Application Hosting—Efficient Leverage of Third-Party Tools

Application hosting gives administrators a platform for leveraging their own tools and utilities. Cisco IOS XR supports third-party off-the-shelf applications built using Linux tool chains. Users can run custom applications cross-compiled with the software development kit that Cisco provides. Application hosting is offered in two variants: Native and Container.

With networking rapidly moving to virtual environments, the need for a network operating system that supports operational agility and efficiency through seamless integration with existing tool chains became a key requirement for our customers.

Cisco IOS XR uses a 64-bit Linux-based operating system that simplifies the integration of applications, configuration management tools, and industry-standard zero touch provisioning mechanisms to meet the DevOps style workflows for service providers.

To access the SDK to build packages that use the Linux distribution offered by Cisco, and to host applications natively, see *Build RPMs for Native Application Hosting* section in the *Cisco IOS XR Application Hosting Configuration Guide* .

Telemetry—Push Towards Smarter Visibility

Streaming telemetry lets users direct data to a configured receiver for analysis and troubleshooting purposes in order to maintain the health of the network. This is achieved by leveraging the capabilities of machine-to-machine communication.

Traditionally, organizations used the pull model to collect data, where a client pulls data from network elements. This pull model, however, does not scale when there is more than one network management station in the network. These traditional techniques do not cater to all the underlying information of the router, and they require manual intervention.

Tuning a network based on real-time data is crucial for seamless operation of the network. Instead of a pull model, using a push model to continuously stream data out of the network enhances the operational performance and reduces the troubleshooting time. Data can be pushed out at intervals determined by the administrator, at a cadence as low as 10 seconds. Using sophisticated algorithms, a back-end server can then analyze data received from the Cisco IOS XR operating system. The data can be encoded in JavaScript Object Notation (JSON) or Google Protocol Buffers (GPB). This analysis enables back-end management systems to measure and even predict control-plane and data-plane trends.

To get started with streaming telemetry data, see Cisco IOS XR Telemetry Configuration Guide.

Software Features Introduced in Release 6.1.2

- DHCPv4 Relay Agent—The DHCPv4 is a host that forwards DHCP packets between clients and servers that do not reside on a shared physical subnet. Relay agent forwarding is distinct from the normal forwarding of an IP router where IP datagrams are switched between networks transparently.

  

  Note DHCPv6 Relay is not supported in Cisco IOS XR Release 6.1.2.

  For information, see the chapter *Implementing the Dynamic Host Configuration Protocol* in the *IP Addresses and Services Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.1.x*

- Percentage-based Thresholds for Queue Limit—This feature allows you to specify queue limit thresholds as a percentage of the total buffer limit for each port. The calculation is based on the assumption that a port takes 40 milli-seconds of buffering at port-rate. This feature makes your provisioning model simpler and makes it easier for you to adjust the queue burst limit, irrespective of the queue's service rate.

  For more information about this feature, see the, *Modular QoS Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.1.x.*

- NetFlow on Layer 2 Bundle—NetFlow support on Layer 2 bundles has been introduced in this release. This feature is supported on ingress L2 bundle for IPv4, IPv6, and MPLS.

  These restrictions apply:

  - Netflow is not supported on Bridge Virtual Interface (BVI) and needs to be applied to the bundle directly.
  - Netflow is not supported on sub-interfaces.

  For more information, see *Netflow Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.1.x*.

- MSTP-BPDU Guard—The Multiple Spanning Tree Protocol (MSTP) bridge protocol data units (BPDU) Guard is a Cisco feature that protects against misconfiguration of edge ports. When MSTP port fast is configured on an interface, MSTP considers that interface to be an edge port and removes it from consideration when calculating the spanning tree. When BPDU Guard is configured, MSTP additionally shuts down the interface using error-disable if an MSTP BPDU is received.

- Layer 2 Access Control Lists—An Ethernet services access control lists (ACLs) consist of one or more access control entries (ACE) that collectively define the Layer 2 network traffic profile. This profile can then be referenced by Cisco IOS XR software features. Each Ethernet services ACL includes an action element (permit or deny) based on criteria such as source and destination address, Class of Service (CoS), ether-type, or 802.1ad DEI.

  Layer 2 ACLs are supported on ingress traffic only. Layer 2 ACLs are not supported on egress traffic.

- Unequal Cost Multipath for Routing—In a network where traffic has to be load balanced on two or more links, configuring equal metrics on the links would create Equal Cost Multipath (ECMP) next hops. Since the bandwidth of the links is not taken into consideration while load balancing, the higher bandwidth links are underutilized. To avoid this problem, you can configure Unequal Cost Multipath (UCMP), either locally (local UCMP), or natively (native UCMP) so that the higher bandwidth links carry traffic in proportion to the capacity of the links. UCMP supports IPv4 and IPv6 VRF routes.

- Platform Automated Monitoring—Platform Automated Monitoring (PAM) is a system monitoring tool integrated into Cisco IOS XR software image to monitor issues such as process crash, memory leak, CPU hog, tracebacks, syslog and disk usage. When PAM tool detects any of these system issues, it collects the required data to troubleshoot the issue, and generates a syslog message stating the issue. The auto-collected troubleshooting information is then stored in a separate file located at the harddisk:. The files are located at harddisk:/cisco_support/ or at /misc/disk1/cisco_support. PAM is enabled by default on all Cisco IOS XR 64 bit platforms.

  For more information about this feature, see the *Implementing Logging Services* chapter in *System Monitoring Configuration Guide for Cisco NCS 5500 Series Routers*. For complete command reference, see the *Logging Services Commands* chapter in *System Monitoring Command Reference for Cisco NCS 5500 Series Routers and Cisco NCS 540 and NCS 560 Series Routers*.

- Autoroute Announce—Configure the autoroute announce feature on the source router for the routing tunnel to be advertised into an Interior Gateway Protocol (IGP) as a next hop. The IGP then installs routes in the Routing Information Base (RIB) for shortest paths that involve the tunnel destination. Autoroute announcement of IPv4 prefixes are carried through either OSPF or IS-IS. Autoroute announcement of IPv6 prefixes are carried only through IS-IS.

  For more information see, *MPLS Configuration Guide for Cisco NCS 5500 Series Routers*.

- VPWS with BGP Auto Discovery—An important aspect of VPN technologies is the ability of network devices to automatically signal to other devices about an association with a particular VPN. Autodiscovery refers to the process of finding all the provider edge routers that participates in a given VPWS instance.

  When a VPWS cross-connect is configured with BGP auto-discovery and signaling enabled, BGP needs to distribute NLRI for the xconnect with the PE as the BGP next-hop and appropriate CE-ID. Additionally, the cross-connect is associated with one or more BGP export Route Targets (RTs) that are also distributed (along with NLRI).

  For more information about the feature, see the *BGP Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.1.x*

- 802.3ah Ethernet OAM—802.3ah Ethernet link OAM features allow Service Providers to monitor the quality of the connections on a MAN or WAN. Service providers can monitor specific events, take actions on events, and if necessary, put specific interfaces into loopback mode for troubleshooting. Ethernet link OAM operates on a single, physical link and it can be configured to monitor either side or both sides of that link.

  For more information, see *Interface and Hardware Component Configuration Guide for Cisco NCS 5500 Series Routers*.

- Selective FIB Download—The NCS5508 system supports LOW-FIB scale and HIGH-FIB scale (with external TCAM) line cards. The Selective FIB Download feature enables the combination of both these cards to be used in the same chassis. This feature helps to maximize resources available and to improve routing scalability

  For more information about the Selective FIB Download feature, see the *BGP Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.1.x*

- Static GRE—Generic Routing Encapsulation (GRE) is a tunneling protocol that provides a simple generic approach to transport packets of one protocol over another protocol by means of encapsulation. The GRE tunnel behave as virtual point-to-point link that have two endpoints identified by the tunnel source and tunnel destination address.

  For more information, see *Interface and Hardware Component Configuration Guide for Cisco NCS 5500 Series Routers*.

- L2 QoS—Quality of Service (QoS) is the technique of prioritizing traffic flows and providing preferential forwarding for higher-priority packets. The fundamental reason for implementing QoS in your network is to provide better service for certain traffic flows. QoS techniques can be applied on Layer2 and Layer3 interfaces.

  For more information about configuring QoS features, see *Modular QoS Configuration Guide for Cisco NCS5500 Series Routers*.

- BFD over Bundle (BoB) mode—BFD over Bundle (BoB) mode is a standard based fast failure detection of link aggregation (LAG) member links that is interoperable between different platforms. BoB support on a per bundle basis provides an option to choose IETF standard per bundle, without necessitating reloads or process restarts across various systems. The default is IETF mode.

  

  Note Only IETF mode is supported in this release.

- IRB Unicast—IRB provides the ability to route between a bridge group and a routed interface using a BVI. The BVI is a virtual interface within the router that acts like a normal routed interface. A BVI is associated with a single bridge domain and represents the link between the bridging and the routing domains on the router. To support receipt of packets from a bridged interface that are destined to a routed interface, the BVI must be configured with the appropriate IP addresses and relevant Layer 3 attributes.

  For more information on this feature, see the *Implementing Integrated Routing and Bridging* chapter in the *Routing Configuration Guide for Cisco NCS 5500 Series Routers*

- Application Hosting with Vagrant—Application hosting gives administrators a platform for leveraging their own tools and utilities. By using Vagrant with Cisco IOS XR, you can host native and container-based applications, and develop complex network topologies. Cisco IOS XR supports the use of a Linux-based container, or a docker-based container for hosting

applications. In addition to using the IOS XR Linux shell, you can use configuration management tools such as Chef, Puppet, or Ansible on Vagrant to provision the router running Cisco IOS XR

For more information, see the *Cisco IOS XR Application Hosting Configuration Guide*.

- ACL Based Forwarding (ABF)—The ACL Based Forwarding (ABF) feature enables routing certain traffic through specific paths instead of using the paths computed by routing protocols. This is achieved by specifying the next-hop address in ACL configurations so that the configured next-hop address from ACL is used for forwarding packet towards its destination instead of routing packet-based destination address lookup.

  ABF enables you to choose service from multiple providers for broadcast TV over IP, IP telephony, data, and so on. Service providers can divert user traffic to various content providers.

  For information about configuration procedures, see the *Implementing ABF* section in the *IP Addresses and Services Configuration Guide for Cisco NCS 5500 Series Routers, Release 6.1.x*.

  For information about the commands, see the *ABF Commands* section in the *IP Addresses and Services Command Reference for Cisco NCS 5500 Series Routers*.

- Bidirectional forwarding detection (BFD)—BFD provides low-overhead, short-duration detection of failures in the path between adjacent forwarding engines. BFD allows a single mechanism to be used for failure detection over any media and at any protocol layer, with a wide range of detection times and overhead. The fast detection of failures provides immediate reaction to failure in the event of a failed link or neighbor.

  Note Only BFD single-hop for IPv4 is supported.

- BGP/T-LDP VPWS—The EVPN-VPWS is a BGP control plane solution for point-to-point services. It implements the signaling and encapsulation techniques for establishing an EVPN instance between a pair of PEs. It has the ability to forward traffic from one network to another without MAC lookup. The use of EVPN for VPWS eliminates the need for signaling single-segment and multi-segment PWs for point-to-point Ethernet services. You can also configure the PWHE interface and a bridge domain access pseudowire using EVPN-VPWS. EVPN-VPWS single homed technology works on IP and MPLS core; IP core to support BGP and MPLS core for switching packets between the endpoints.

- Ethernet Connectivity Fault Management (CFM)—CFM is a service-level OAM protocol that provides tools for monitoring and troubleshooting end-to-end Ethernet services for each VLAN. This includes proactive connectivity monitoring, fault verification, and fault isolation. CFM uses standard Ethernet frames and can be run on any physical media that is capable of transporting Ethernet service frames. Cisco NCS 5500 Series Routers support the IEEE 802.1ag standard for CFM.

  For more information, see *Interface and Hardware Component Configuration Guide for Cisco NCS 5500 Series Routers*.

- IRB—Cisco NCS 5500 Series Routers support IRB. IRB provides the ability to exchange traffic between bridging services on the Cisco NCS 5500 Series Router and a routed interface using a Bridge-Group Virtual Interface (BVI). The BVI is a virtual interface within the router that acts like a normal routed interface. A BVI is associated with a single bridge domain and represents the link between the bridging and the routing domains on the router.

  For more information, see *Interface and Hardware Component Configuration Guide for Cisco NCS 5500 Series Routers*.

- Ethernet link OAM—This features allow Service Providers to monitor the quality of the connections on a MAN or WAN. Service providers can monitor specific events, take actions on events, and if necessary, put specific interfaces into loopback mode for troubleshooting. Ethernet link OAM operates on a single, physical link and it can be configured to monitor either side or both sides of that link.

  For more information, see *Interface and Hardware Component Configuration Guide for Cisco NCS 5500 Series Routers*.

- VLAN on Bundles and Subinterfaces—Cisco NCS 5500 Series Routers support VLANs on bundles and subinterfaces. Subinterfaces are logical interfaces created on a hardware interface. These software-defined interfaces allow for segregation of traffic into separate logical channels on a single hardware interface as well as allowing for better utilization of the available bandwidth on the physical interface.

  For more information, see *Interface and Hardware Component Configuration Guide for Cisco NCS 5500 Series Routers*.

- Traffic Mirroring—Traffic mirroring or Switched Port Analyzer (SPAN) is a Cisco proprietary feature that enables you to monitor Layer 2 or Layer 3 network traffic passing in, or out of, a set of Ethernet interfaces. You can then pass this traffic to a network analyzer for analysis.

  For more information, see *Interface and Hardware Component Configuration Guide for Cisco NCS 5500 Series Routers*.

- VRRP—The Virtual Router Redundancy Protocol (VRRP) feature allows for transparent failover at the first-hop IP router, enabling a group of routers to form a single virtual router. The LAN clients can then be configured with the virtual router as their default gateway. The virtual router, representing a group of routers, is also known as a VRRP group.

  For information about configuration procedures, see the *Implementing VRRP* section in the *IP Addresses and Services Configuration Guide for Cisco NCS 5500 Series Routers*.

  For information about the commands, see the *VRRP Commands* section in the *IP Addresses and Services Command Reference Guide for Cisco NCS 5500 Series Routers*.

- Support for mixed bandwidth bundles—Cisco NCS 5500 Series Routers support mixed bandwidth bundles. The maximum ratio difference in the bandwidth between the bundle members can be 1:10

- EVPN-VPWS—The EVPN-VPWS is a BGP control plane solution for point-to-point services. It implements the signaling and encapsulation techniques for establishing an EVPN instance between a pair of PEs. It has the ability to forward traffic from one network to another without MAC lookup. The use of EVPN for VPWS eliminates the need for signaling single-segment and multi-segment PWs for point-to-point Ethernet services. You can also configure the PWHE interface and a bridge domain access pseudowire using EVPN-VPWS.

  EVPN-VPWS single homed technology works on IP and MPLS core; IP core to support BGP and MPLS core for switching packets between the endpoints.

  For more information on this feature, see the topic under *Implementing BGP* chapter in the *BGP Configuration Guide for Cisco NCS 5500 Series Routers.*

- PIM SSM—Protocol Independent Multicast in Source-Specific Multicast (PIM-SSM) has the ability to report interest in receiving packets from specific source addresses (or from all but the specific source addresses), to an IP multicast address.

  PIM SSM supports IPv4 addresses.

- IGMP—IGMPv3 is used between hosts on a LAN and the routers on that LAN to track the multicast groups of which hosts are members

- Flexible Cross-Connect Service—The flexible cross-connect service feature enables aggregation of attachment circuits (ACs) across multiple endpoints in a single Ethernet VPN Virtual Private Wire Service (EVPN-VPWS) service instance on the same Provider Edge (PE). This feature reduces the number of tunnels by muxing VLANs across many interfaces and also reduces the number of MPLS labels used by a router.

  For more information on this feature, see the *Configure Point-to-Point Layer 2 Services* chapter in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5500 Series Routers.*

- Ingress and Egress IPv4 ACL—From this release onwards, you can configure ingress and egress IPv4 ACL on Layer 2 interfaces (also referred to as Ethernet-Services ACL). This ACL includes rules/ACEs defined in terms of match on source MAC address, destination MAC address, VLAN ID and Port Control Protocol (PCP).

For information about configuration procedures, see the *Implementing Access Lists and Prefix Lists* section in the *IP Addresses and Services Configuration Guide for Cisco NCS 5500 Series Routers*.

For information about the commands, see the *Access List Commands* section in the *IP Addresses and Services Commad Reference for Cisco NCS 5500 Series Routers*.

- BGP PIC Core—The BGP PIC core improves convergence after a network failure. When a failure is detected, the IGP finds an alternate path to the BGP remote PE. This alternate path immediately takes over, enabling fast failover. It speeds up the convergence of the FIB in failover conditions.

  With BGP PIC core, BGP's convergence value is based on IGP's convergence value and does not vary with BGP route scale.

- Enhancement to Telemetry—Streaming telemetry lets users direct data to a configured receiver for analysis and troubleshooting purposes in order to maintain the health of the network.

  The enhancements to Data Models includes support for:

  - Model-driven telemetry (MDT) that provides a mechanism to stream data from an MDT-capable device to a destination. The data to be streamed is driven through subscription from a dataset in a YANG model. The data from the subscribed dataset is streamed out to the destination at a configured interval.

    Note Streaming Model-driven Telemetry over the dataport that is in a VRF is not supported.

  - Policy-based telemetry provides enhanced time stamping functionality.

- To get started with streaming telemetry data, see Cisco IOS XR Telemetry Configuration Guide.

- Enhancement to Data Models—Data models are a programmatic and standards-based way of configuring and collecting operational data of a network device, replacing the process of manual configuration.

  The enhancements to Data Models includes support for:

  - Flexible CLI group and apply-group configuration can be created using NETCONF YANG client. The flexible CLI configuration groups provide the ability to minimize repetitive configurations by defining a series of configuration statements in a configuration group, and then applying this group to multiple hierarchical levels in the router configuration tree.

  - Additional Cisco-specific and native models.

- Zero Touch Provisioning—Zero Touch Provisioning (ZTP) supports auto provisioning of router by running customized scripts using DHCP server.

  The enhancements to ZTP support includes:

  - Running ZTP scripts within the global VPN routing/forwarding (VRF) namespace and thus supporting line card interfaces.

  - Configuring and bringing up the interfaces, and invoking ZTP manually.

  For more information about ZTP, see the Perform Disaster Recovery section in the *System Setup and Software Installation Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.1.x*

Hardware Introduced in Release 6.1.2

This release introduces four new chassis:

- Cisco NCS 5501—This chassis is a fixed port, high density, 1RU form-factor router that supports port density of 48 x SFP/SFP+ ports, each capable of supporting 1GE or 10GE and 6 x QSFP+/QSFP28 ports each capable of supporting 10GE (via cable breakout), 40GE, or 100GE receivers.
- Cisco NCS-5501-SE—This chassis is capable of supporting 1GE or 10GE and 4 x QSFP+/QSFP28 ports, each capable of supporting 10GE (via cable breakout), 40GE, or 100GE receivers.
- Cisco NCS-5502—This chassis is a fixed port, high density, 2 RU form-factor Router that supports 48 QSFP ports, each of which is capable of supporting 10GE (via cable breakout), 40GE, or 100GE receivers.
- Cisco NCS-5502-SE—This chassis is a fixed port, high density, 2 RU form-factor router that supports 48 QSFP ports, each of which is capable of supporting 10GE (via cable breakout), 40GE, or 100GE receivers. It has 8 BRCM JERICHO ASIC for forwarding traffic and external TCAM connected to each of these ASIC for supporting large prefix scale.

Note All NCS 5500 series chassis provide NEBS compliance

This release also introduces a new line card for the NCS5500 router:

- NC55-24H12F-SE—This linecard supports 24 ports of 100GE and 12 ports of 40GE. The 100GE ports can be used as either 100G / 40G or 4x10G through breakout. The 40GE ports can be used as either 40G or 4x10G through breakout.

For more information, see the *Hardware Installation Guide for Cisco NCS 5500 Series Routers*

For information on the optics supported and other specifications, refer theNCS 5500 Data Sheet

Release 6.1.2 Packages

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

Table 1: Release 6.1.2 Packages for Cisco NCS 5500 Series Router

Composite Package		
Feature Set	**Filename**	**Description**
Cisco IOS XR IP Unicast Routing Core Bundle	ncs5500-mini-x.iso	Contains base image contents that includes: • Host operating system • System Admin boot image • IOS XR boot image
Individually-Installable Optional Packages		
Feature Set	**Filename**	**Description**
Cisco IOS XR Manageability Package	ncs5500-mgbl-1.0.0.0-r612.x86_64.rpm	Extensible Markup Language (XML) Parser, Telemetry, Netconf, gRPC and HTTP server packages.

Cisco IOS XR MPLS Package	ncs5500-mpls-1.0.0.0-r612.x86_64.rpm ncs5500-mpls-te-rsvp-1.0.0.0-r612.x86_64.rpm	MPLS and MPLS Traffic Engineering (MPLS-TE) RPM.
Cisco IOS XR Security Package	ncs5500-k9sec-1.0.0.0-r612.x86_64.rpm	Support for Encryption, Decryption, Secure Shell (SSH), Secure Socket Layer (SSL), and Public-key infrastructure (PKI)
Cisco IOS XR ISIS package	ncs5500-isis*.rpm	Support ISIS
Cisco IOS XR OSPF package	ncs5500-ospf*.rpm	Support OSPF

Supported Hardware

For a complete list of hardware and ordering information, see the *Cisco NCS 5500 Series Data Sheet*

Use the Cisco Optics-to-Device Compatibility Matrix tool to determine transceivers supported in Cisco hardware devices.

To install the Cisco NCS 5500 router, see *Hardware Installation Guide for Cisco NCS 5500 Series Routers*.

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 6.1.4
Copyright (c) 2013-2016 by Cisco Systems, Inc.

Build Information:
Built By : <username>
Built On : Thu Jun 29 15:31:09 PDT 2017
Build Host : iox-lnx-032
Workspace : /auto/srcarchive13/production/6.1.4/ncs5500/workspace
Version : 6.1.4
Location : /opt/cisco/XR/packages/

cisco NCS-5500 () processor
System uptime is 4 hours, 36 minutes
```

```
RP/0/RP0/CPU0:router# show version
Cisco IOS XR Software, Version 6.1.2
Copyright (c) 2013-2016 by Cisco Systems, Inc.

Build Information:
 Built By     : <username>
 Built On     : Thu Nov 10 22:20:21 PST 2016
 Build Host   : iox-lnx-032
 Workspace    : /auto/srcarchive11/production/6.1.2/ncs5500/workspace
 Version      : 6.1.2
 Location     : /opt/cisco/XR/packages/

cisco NCS-5500 () processor
System uptime is 1 day, 23 hours, 59 minutes
```

Caveats

Caveats describe unexpected behavior in Cisco IOS XR Software releases.

The following open caveats apply to the current Cisco IOS XR Software Release

There are no caveats in this release.

Determine Firmware Support

Log in to the router and enter **show fpd package** command in EXEC mode:

For NCS 5501

```
RP/0/RP0/CPU0:router# show fpd package
                                                                 FPD Versions
                                                                 ================
Location   Card type        HWver FPD device       ATR Status   Running Programd
-------------------------------------------------------------------------------
0/RP0      NCS-5501          0.2   MB-MIFPGA            CURRENT    1.01    1.01
0/RP0      NCS-5501          0.2   Bootloader           CURRENT    1.05    1.05
0/RP0      NCS-5501          0.2   CPU-IOFPGA           CURRENT    1.08    1.08
0/RP0      NCS-5501          0.2   MB-IOFPGA            CURRENT    1.02    1.02
```

For NCS 5501-SE

```
RP/0/RP0/CPU0:router# show fpd package
                                                                 FPD Versions
                                                                 ================
Location   Card type        HWver FPD device       ATR Status   Running Programd
-------------------------------------------------------------------------------
0/RP0      NCS-5501-SE       0.4   MB-MIFPGA            CURRENT    1.00    1.00
0/RP0      NCS-5501-SE       0.4   Bootloader           CURRENT    1.11    1.11
0/RP0      NCS-5501-SE       0.4   CPU-IOFPGA           CURRENT    1.08    1.08
0/RP0      NCS-5501-SE       0.4   MB-IOFPGA            CURRENT    1.04    1.04
```

For NCS 5502

```
RP/0/RP0/CPU0:router# show fpd package
                                                                 FPD Versions
                                                                 ================
Location   Card type        HWver FPD device       ATR Status   Running Programd
-------------------------------------------------------------------------------
0/RP0      NCS-5502          0.2   DC-MIFPGA            CURRENT    1.02    1.02
0/RP0      NCS-5502          0.2   MB-MIFPGA            CURRENT    1.02    1.02
0/RP0      NCS-5502          0.2   Bootloader           CURRENT    1.11    1.11
0/RP0      NCS-5502          0.2   CPU-IOFPGA           CURRENT    1.08    1.08
0/RP0      NCS-5502          0.2   DC-IOFPGA            CURRENT    1.01    1.01
0/RP0      NCS-5502          0.2   MB-IOFPGA            CURRENT    1.01    1.01
```

For NCS 5502-SE

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

                                                                 FPD Versions
                                                                 ================
Location   Card type        HWver FPD device       ATR Status   Running Programd
-------------------------------------------------------------------------------
0/RP0      NCS-5502-SE       0.4   DC-MIFPGA            CURRENT    1.02    1.02
0/RP0      NCS-5502-SE       0.4   MB-MIFPGA            CURRENT    1.02    1.02
0/RP0      NCS-5502-SE       0.4   Bootloader           CURRENT    1.11    1.11
```

```
0/RP0     NCS-5502-SE       0.4   CPU-IOFPGA           CURRENT    1.08    1.08
0/RP0     NCS-5502-SE       0.4   DC-IOFPGA            CURRENT    1.01    1.01
0/RP0     NCS-5502-SE       0.4   MB-IOFPGA            CURRENT    1.01    1.01
```

For NCS 5508

```
RP/0/RP0/CPU0:router# show fpd package
                                                                  FPD Versions
                                                                  ================
Location   Card type        HWver FPD device       ATR Status   Running Programd
----------------------------------------------------------------------------------
0/0        NC55-18H18F       1.0   MIFPGA              CURRENT    0.03    0.03
0/0        NC55-18H18F       1.0   Bootloader          CURRENT    1.11    1.11
0/0        NC55-18H18F       1.0   IOFPGA              CURRENT    0.19    0.19
0/1        NC55-24X100G-SE   1.0   MIFPGA              CURRENT    0.03    0.03
0/1        NC55-24X100G-SE   1.0   Bootloader          CURRENT    1.11    1.11
0/1        NC55-24X100G-SE   1.0   IOFPGA              CURRENT    0.12    0.12
0/2        NC55-36X100G      1.1   MIFPGA              CURRENT    0.09    0.09
0/2        NC55-36X100G      1.1   Bootloader          CURRENT    1.17    1.17
0/2        NC55-36X100G      1.1   IOFPGA              CURRENT    0.14    0.14
0/3        NC55-24H12F-SE    0.201 MIFPGA              CURRENT    0.02    0.02
0/3        NC55-24H12F-SE    0.201 Bootloader          CURRENT    1.11    1.11
0/3        NC55-24H12F-SE    0.201 IOFPGA              CURRENT    0.08    0.08
0/4        NC55-36X100G      0.106 MIFPGA              CURRENT    0.09    0.09
0/4        NC55-36X100G      0.106 Bootloader          CURRENT    1.17    1.17
0/4        NC55-36X100G      0.106 IOFPGA              CURRENT    0.14    0.14
0/5        NC55-36X40G       0.1   MIFPGA              CURRENT    0.03    0.03
0/5        NC55-36X40G       0.1   Bootloader          CURRENT    1.11    1.11
0/5        NC55-36X40G       0.1   IOFPGA              CURRENT    0.19    0.19
0/6        NC55-24X100G-SE   0.1   MIFPGA              CURRENT    0.03    0.03
0/6        NC55-24X100G-SE   0.1   Bootloader          CURRENT    1.11    1.11
0/6        NC55-24X100G-SE   0.1   IOFPGA              CURRENT    0.12    0.12
0/RP0      NC55-RP           1.1   Bootloader          CURRENT    9.24    9.24
0/RP0      NC55-RP           1.1   IOFPGA              CURRENT    0.09    0.09
0/RP1      NC55-RP         1.1   Bootloader          CURRENT    9.24    9.24
0/RP1      NC55-RP         1.1   IOFPGA              CURRENT    0.09    0.09
0/FC1      NC55-5508-FC      0.305 Bootloader          CURRENT    1.70    1.70
0/FC1      NC55-5508-FC      0.305 IOFPGA              CURRENT    0.15    0.15
0/FC3      NC55-5508-FC      0.109 Bootloader          CURRENT    1.70    1.70
0/FC3      NC55-5508-FC      0.109 IOFPGA              CURRENT    0.15    0.15
0/FC5      NC55-5508-FC      1.0   Bootloader          CURRENT    1.70    1.70
0/FC5      NC55-5508-FC      1.0   IOFPGA              CURRENT    0.15    0.15
0/SC0      NC55-SC           1.4   Bootloader          CURRENT    1.70    1.70
0/SC0      NC55-SC           1.4   IOFPGA              CURRENT    0.08    0.08
0/SC1      NC55-SC           1.4   Bootloader          CURRENT    1.70    1.70
0/SC1      NC55-SC           1.4   IOFPGA              CURRENT    0.08    0.08
```

Other Important Information

- 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.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

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)

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.