



Release Notes for Cisco NCS 5000 Series Routers, IOS XR Release 6.6.1

Network Convergence System 5000 Series Routers	2
Release 6.6.1 Packages	2
System Requirement	3
Software Features Introduced in this Release	4
Behavior Change Introduced in this release	4
Hardware Features Introduced in this Release	4
Caveats	5
Upgrading Cisco IOS XR Software	5
Related Documentation	5
Communications, Services, and Additional Information	6
Full Cisco Trademarks with Software License	8

Network Convergence System 5000 Series Routers



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.

Cisco IOS XR Release 6.6.1 is a limited availability (LA) release. All Cisco IOS XR Release 6.6.1 features are available in Cisco IOS XR Release 6.6.25, which is a general availability (GA) release. For more information on IOS XR Release 6.6.25, see *Release Notes for Cisco NCS 5000 Series Routers, Release 6.6.25*

The Network Convergence System 5000 Series offers a high-density, small-form-factor MPLS aggregation router for metro aggregation. It is designed to economically scale large enterprise, over-the-top (OTT), and service provider Data Center networking architectures.

The Cisco NCS 5000 Series is an extension to Cisco's routing platform portfolio enabling Service Providers and MPLS enabled data center architectures to offer elastic networks with improved business agility and simplified operations to deliver high-bandwidth mobile, video, and cloud services.

It can also operate as an extension shelf of Cisco ASR 9000 Series Aggregation Services Routers using Network Virtualization (nV) technology, consolidating multiple layers in the network and dramatically reducing operational costs.

The Cisco NCS 5000 series routers are small form factor dense aggregation systems. Powered by industry leading routing operation system, IOS-XR, the system also offers rich functions such as third party application hosting, machine-to-machine interface, telemetry and flexible package delivery.

The latest release of Cisco IOS XR operating system opens up the architecture of Cisco IOS XR using a 64-bit Linux-based operating system to deliver greater agility, automation and simplicity, while reducing cost of operating the networks.

Release 6.6.1 Packages

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

Table 1: Release 6.6.1 Packages for Cisco NCS 5000 Series Router

Composite Package		
Feature Set	Filename	Description

Cisco IOS XR IP Unicast Routing Core Bundle	ncs5k-mini-x.iso	Contains base image contents that includes: <ul style="list-style-type: none"> • Host operating system • System Admin boot image • IOS XR boot image • Alarm co-relation
Individually-Installable Optional Packages		
Feature Set	Filename	Description
Cisco IOS XR Manageability Package	ncs5k-mgbl-3.0.0.0-r661.x86_64.rpm	XML, Parser, HTTP Server, Telemetry, and gRPC.
Cisco IOS XR MPLS Package	ncs5k-mpls-3.1.0.0-r661.x86_64.rpm	Label Distribution Protocol (LDP), MPLS forwarding , MPLS operations , Administration and maintenance (OAM), Layer3-vpn , layer-2 vpn.
Cisco IOS XR MPLS RSVP TE package	ncs5k-mpls-te-rsvp-1.1.0.0-r661.x86_64.rpm	Supports MPLS RSVP-TE (Resource Reservation Protocol with Traffic Engineering extensions)
Cisco IOS XR Security Package	ncs5k-k9sec-3.2.0.0-r661.x86_64.rpm	Support for Encryption, Decryption, and Secure Shell (SSH),
Cisco IOS XR Multicast Package	ncs5k-mcast-2.2.0.0-r661.x86_64.rpm	Multicast routing protocols (PIM, IGMP, Auto-rp, BSR) and infrastructure (Multicast routing information Base) , Multicast forwarding (mfwd)
Cisco IOS XR ISIS package	ncs5k-isis-2.2.0.0-r661.x86_64.rpm	Supports ISIS
Cisco IOS XR OSPF package	ncs5k-ospf-2.0.0.0-r661.x86_64.rpm	Supports OSPF

System Requirement

Supported Hardware

For a complete list of supported optics, hardware and ordering information for NCS 5001 and NCS 5002 series router, see the [Cisco NCS 5000 Series Data Sheet](#)

For a complete list of supported optics, hardware and ordering information for NCS 5011 router, see the [Cisco NCS 5011 Series Data Sheet](#)

To install the Cisco NCS 5000 series routers, see [Hardware Installation Guide for Cisco NCS 5000 Series Routers](#).

Software Features Introduced in this Release

Encapsulation Untagged

Encapsulation Untagged feature enables a Layer 2 sub-interface to carry only untagged Layer 2 traffic. You can enable this feature by configuring the **encapsulation untagged** command under the Layer 2 sub-interface. Normally, when an untagged sub-interface is unavailable, untagged traffic is routed through the main interface. When a Layer 2 untagged sub-interface is configured and is made a part of a Bridge Domain (BD), the untagged traffic is bridged across the BD.

Revised OC-platform model version

Support for openconfig-platform.yang (OC-platform) model is revised from version 0.4.0 to version 0.11.0. In addition to retrieving basic component information, this revised version of the model extracts additional details such as operational state, available and utilized memory, allocated and used power, temperature, power-supply, fan, linecard and so on.

Support for new XR NETCONF actions

IOS-XR and System admin actions are RPC statements that trigger an operation or execute a command on the router. The following NETCONF actions are introduced in this release:

- copy
- delete

Telemetry support for OC LACP

The OpenConfig-Link Aggregation Control Protocol (OC-LACP) model defined by the OC community, helps manage LACP-enabled bundles and member interfaces. Cisco IOS XR supports OC-LACP version 1.0.2. Currently, the support is extended to version 1.1.0. Telemetry support for (OC-LACP) is provided only for LACP state data at global, bundle and member level.

Behavior Change Introduced in this release

From this release onwards the **ispf** command is deprecated.

This command was used to calculate network topology using the incremental shortest path first (iSPF) algorithm.

Hardware Features Introduced in this Release

A new chassis, Cisco NCS 5064 is introduced in this release.

The Cisco NCS 5064 chassis, which is also an extension to Cisco's routing platform portfolio enabling Service Providers and MPLS enabled data center architectures to offer elastic networks with improved business agility and simplified operations to deliver high-bandwidth mobile, video, and cloud services.

The Cisco NCS 5064 chassis is a small form factor dense 100GE aggregation systems in 2RU form factor. Powered by industry leading routing operation system, IOS-XR, the system also offers rich functions such as third party application hosting, machine-to-machine interface, telemetry and flexible package delivery.

The Cisco NCS 5064 chassis has the following features:

- Two hot-swappable power supply (PSUs) that support 1+1 redundancy under most conditions. Only when the 930W DC supplies (NC5K-PDC-930W-FR and NC5K-PDC-930W-BK) are used, both the PSUs must be inserted and operational in a non-redundant 2+0 mode.
- Different power supply units (PSUs) are available for different air flow configurations.
- Three hot-swappable fan modules that provide port side intake or port side exhaust cooling in 2+1 redundancy mode.
- A management, console, and the USB interface on fan side of the chassis.

Caveats

Caveats describe unexpected behavior in Cisco IOS XR Software releases. Severity-1 caveats are the most critical caveats; severity-2 caveats are less critical.

Cisco IOS XR Caveats

There are no caveats specific to Cisco IOS XR Software Release.

There are no caveats specific to Cisco IOS XR Software Release.

Caveats Specific to the NCS 5000 Routers

There are no caveats in this release.

Upgrading Cisco IOS XR Software

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

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

The upgrade document is available along with the software images.

Cisco Software Manager (CSM) application provides an intuitive user interface to manage Cisco IOS XR installations, with pre-installation and post-installation checks and reports. CSM helps manage the process of software maintenance upgrades (SMUs) and service packs (SPs) on devices that run the Cisco IOS XR Software.

For information on how to use CSM, see [Cisco Software Manager User Guide](#).

Related Documentation

The most current Cisco Network Convergence System 5000 Series documentation is located at this URL:

<http://www.cisco.com/c/en/us/support/routers/network-convergence-system-5000-series/tsd-products-support-series-home.html>

The document containing Cisco IOS XR System Error Messages (SEM) is located at this URL:

https://www.cisco.com/c/en/us/td/docs/ios_xr_sw/error/message/ios-xr-sem-guide.html

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.

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.

© 2020 Cisco and/or its affiliates. All rights reserved.