Release Notes for Cisco NCS 6000 Series Routers, IOS XR Release 6.3.1

6.3.1 2

What's New in Release 6.3.1 2

Caveats 4

Release 6.3.1 Packages 5

Determining Installed Active Packages 6

Supported Packages and System Requirements 7

Upgrading Cisco IOS XR Software 7

Related Documentation 7

Communications, Services, and Additional Information 7

Full Cisco Trademarks with Software License 9

Revised: June 10, 2021

6.3.1

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.

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

What's New in Release 6.3.1

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 Features Introduced in Cisco IOS XR Software Release 6.3.1

Pseudowire Headend (PWHE)

The Pseudowire Headend (PWHE) feature provides a Layer 3 (L3) virtual interface representation of a pseudowire (PW) on an service provider edge (PE), that allows the backhaul of customer packets over PWs and the application of L3 features, such as QoS (for example: policing and shaping) and access lists (ACLs) on customer packets on the PW. In Release 6.3.1, PWs operate in bridged interworking mode; only VC type 4 or VC type 5 is supported.

For more information on this feature, see the *Implementing MPLS Layer 3 VPNs* chapter in the *Virtual Private Network Configuration Guide for Cisco NCS 6000 Series Routers, IOS XR Release 6.3.1*.

ISSU for BFD session over MPLS-TE tunnel

In-Service Software Upgrade (ISSU) is supported for BFD session over MPLS-TE tunnel (BFDoTE) feature. For more information about ISSU, see *System Setup and Software Installation Guide for Cisco NCS 6000 Series Routers*.

ISSU for BGP Flowspec

In-Service Software Upgrade (ISSU) is supported for BGP flow specification (flowspec) feature. For more information about ISSU, see *System Setup and Software Installation Guide for Cisco NCS 6000 Series Routers*.

Cross Rack Pairing

Cross rack pairing allows inter-rack pairing where route processor (RP) of one rack is paired with the RP of another rack through an algorithm. This daisy-chain pairing of racks provides high availability against rack failures.

To enable pairing RPs between racks, and associated scenarios, see *Perform Cross Rack Pairing* chapter in the System Setup and Software Installation Guide for Cisco NCS 6000 Series Routers.

IP-in-IP Decapsulation

IP datagrams that are encapsulated with an outer IP header before transmission through an IP tunnel are stripped of the header on exiting the tunnel. IP-in-IP decapsulation is now supported on NCS 6000.

For more information on this feature, see the *Interfaces and Hardware Component Configuration Guide for Cisco NCS 6000 Series Routers, IOS XR Release 6.2.x*.

YANG Model Support for IOS XR Admin Plane

YANG data models are supported for IOS XR admin plane. All the IOS XR actions are supported in System Admin plane.The actions introduced in this release are:

- System Process Mgmt : process (restart)
- System Process Mgmt : Reload (System Admin virtual machine (VM) reload, line card (LC) reload)
- System Process Mgmt : Reload (IOS XR VM node reload from System Admin)

To see the list of actions and an example to use a System Admin action, see *Components to Use Data Models* chapter in the .

Event-based Telemetry

Telemetry provides a mechanism to stream data from the router at regular intervals. Event-based telemetry is used to collect data when a state transition occurs. This feature optimises the need to collect state information even when a change in the state does not occur, thus eliminating the data overhead at the router and the receiver.

For more information about state transitions, and collecting event-based telemetry data, see *Configure Event-based Telemetry* chapter in the .

OAM for BGP-SR

The OAM for BGP-SR feature provides support for ping, traceroute, and treetrace (traceroute multipath) operations for LSPs signaled via BGP for IPv4 Prefix SIDs. This feature adds support for Segment Routing OAM operations in deployments with combinations of BGP and LDP signaled LSPs.

For more information on this feature, see the Using Segment Routing OAM chapter in the

ERSPAN with UDF

ERSPAN with UDF feature enables the device to match on user-defined fields (UDFs) of the outer packet fields, either header or payload, and to send the matching packets to the ERSPAN destination. This feature helps you to analyze and isolate packet drops in the network.

For more information, see the *Interface and Hardware Component Configuration Guide for Cisco NCS 6000 Series Routers, IOS XR Release 6.3.x*.

Multi-chassis SDR

The Secure Domain Routers (SDRs) are a means of dividing a single physical system into multiple logically separated routers. The Multi-chassis SDR feature enables you to create named SDRs on a NCS6K multi-chassis system. In previous releases, named SDR creation was possible only on single-chassis system. As in previous releases, a maximum of three named SDRs can be created. However, with multi-chassis setup more resources like line cards and its memory and CPU can be allocated to each SDR. This results in more compute power with each SDR.

For more information on, see the *Configuring Secure Domain Routers* chapter in the *System Management Configuration Guide for Cisco NCS 6000 Series Routers.*

Online Diagnostics Support

Cisco NCS 6000 Series Routers supports Online Diagnostics. This feature enables you to test and verify the hardware functionality when connected to a live network. Scheduled health monitoring and diagnostics ensures system High Availability (HA). You can take appropriate resolution measures in less time as the diagnostic test results help in isolating the location of the problem.

Cisco NCS 6000 Series Routers supports File System Diagnostic tests. For more information on this, see *Online Diagnostics Software* chapter in *System Monitoring Configuration Guide for Cisco NCS 6000 Series Routers, IOS XR Release 6.3.x*. For the list of Online Diagnostic commands and other command details, see *Online Diagnostic Software commands* chapter in *System Monitoring Command Reference for Cisco NCS 6000 Series Routers*.

Hardware Features

There are no new hardware features introduced in this release.

Other Important Information

- Country-specific laws, regulations, and licenses—In certain countries, use of these products may be prohibited and subject to laws, regulations, or licenses, including requirements applicable to the use of the products under telecommunications and other laws and regulations; customers must comply with all such applicable laws in the countries in which they intend to use the products.
- Exceeding Cisco testing—If you intend to test beyond the combined maximum configuration tested and published by Cisco, contact your Cisco Technical Support representative to discuss how to engineer a large-scale configuration for your purpose.

Caveats

Caveats describe unexpected behavior in . 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

Release 6.3.1 Packages

This table lists the Cisco IOS XR Software feature set matrix (packages) and associated filenames available for the Cisco IOS XR Software Release 6.3.1 that is supported on the Cisco NCS 6008 router.

Table 1: Cisco IOS XR Software Release 6.3.1 Packages

Feature Set	Filename	Description
Composite Package		
Cisco IOS XR IP Unicast Routing Core Bundle	ncs6k-mini-x.iso-6.3.1	Contains required core packages, including OS, Admin, Base, Forwarding, Modular Services Card, Routing, SNMP Agent, FPD, and Alarm Correlation.
Optional Individual Packages (packages that are installed individually)		
Cisco IOS XR Manageability Package	ncs6k-mgbl.pkg-6.3.1	Extensible Markup Language (XML) Parser and HTTP server packages.
Cisco IOS XR MPLS Package	ncs6k-mpls.pkg-6.3.1	MPLS Traffic Engineering (MPLS-TE), Label Distribution Protocol (LDP), MPLS Forwarding, MPLS Operations, Administration, and Maintenance (OAM), Link Manager Protocol (LMP), Optical User Network Interface (OUNI), Resource Reservation Protocol (RSVP), and Layer-3 VPN.
Cisco IOS XR Multicast Package	ncs6k-mcast.pkg-6.3.1	Multicast Routing Protocols (PIM, Multicast Source Discovery Protocol [MSDP], Internet Group Management Protocol [IGMP], Auto-RP), Tools (SAP, MTrace), and Infrastructure [(Multicast Routing Information Base [MRIB], Multicast-Unicast RIB [MURIB], Multicast forwarding [MFWD]).
Cisco IOS XR Security Package	ncs6k-k9sec.pkg-6.3.1	Support for Encryption, Decryption, IP Security (IPSec), Secure Shell (SSH), Secure Socket Layer (SSL), and Public-key infrastructure (PKI) (Software based IPSec support—maximum of 500 tunnels)
Cisco IOS XR Lawful Intercept (LI) Package	ncs6k-li.pkg-6.3.1	Supports Lawful Intercept (LI) features.
Cisco IOS XR Documentation Package	ncs6k-doc.pkg-6.3.1	*.man* pages for Cisco IOS XR Software.

Table 2: Cisco IOS XR Software Release 6.3.1 TAR Files

Feature Set	Filename	Description
Cisco IOS XR IP/MPLS Core Software	ncs6k-iosxr-6.3.1.tar	• Cisco IOS XR IP Unicast Routing Core Bundle • Cisco IOS XR Manageability Package • Cisco IOS MPLS Package • Cisco IOS XR Multicast Package • Cisco IOS XR Lawful Intercept (LI) Package • Cisco IOS XR Documentation package
Cisco IOS XR IP/MPLS Core Software 3DES	ncs6k-iosxr-k9-6.3.1.tar	• Cisco IOS XR IP Unicast Routing Core Bundle • Cisco IOS XR Manageability Package • Cisco IOS XR MPLS Package • Cisco IOS XR Multicast Package • Cisco IOS XR Security Package • Cisco IOS XR Lawful Intercept (LI) Package • Cisco IOS XR Documentation package

Determining Installed Active Packages

To determine active software packages installed on the router, log in to the router and enter the **show install active** command in EXEC mode:

```
RP/0/# show install active

  Active Packages: 7
        ncs6k-xr-6.3.1 version=6.3.1 [Boot image]
        ncs6k-mcast-1.0.0.0-r631
        ncs6k-mpls-1.0.0.0-r631
        ncs6k-mgbl-1.0.0.0-r631
        ncs6k-doc-1.0.0.0-r631
        ncs6k-k9sec-1.0.0.0-r631
        ncs6k-li-1.0.0.0-r631
```

Supported Packages and System Requirements

Memory Requirements

Supported Hardware

The following table lists the supported hardware components on the and the minimum required software release. For more information, see the *Firmware Support* section.

Firmware Support

To check the firmware code running on the , run the **show fpd package** command in admin mode.

Refer to the documents at http://www.cisco.com/web/Cisco_IOS_XR_Software/index.html for upgrade instructions.

Minimum Firmware Requirement

Upgrading Cisco IOS XR Software

Related Documentation

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.

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.

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.