Release Notes for Cisco NCS 4000 Series, Cisco IOS XR Release 6.1.22

First Published: 2017-06-22

Release Notes for Cisco NCS 4000 Series, Cisco IOS XR Release 6.1.22

The release notes contain information about the new features introduced in the Cisco NCS 4000 Series. For detailed information regarding features, capabilities, hardware, and software introduced with this release, see the guides listed in the *Additional References* section.

Revision History

Date	Notes
June 2017	This is the first release of this publication.

Software and Hardware Requirements

Before you begin to install the software, you must check whether your system meets the minimum software and hardware requirements.

- Hardware— Intel Core i5, i7, or faster processor. A minimum of 4 GB RAM, 100 GB hard disk with 250 MB of available hard drive space.
- One of these operating System:
  - Windows 7, Windows Server 2008, or later.
  - Apple Mac OS X
  - UNIX workstation with Solaris Version 9 or 10 on an UltraSPARC-III or faster processor, with a minimum of 1 GB RAM and a minimum of 250 MB of available hard drive space.
  - Ubuntu 12.10
- Java Runtime Environment—Java Runtime Environment Version 1.8.
- Browser:
  - Internet Explorer
  - Mozilla
  - Safari
  - Google Chrome

New Features for Release 6.1.22

This section highlights new NCS 4000 features for Release 6.1.22. For detailed documentation of each of these features, see the user documentation:

- Hardware
- Software

Hardware

The following hardware has been introduced in Release 6.1.22:

NCS4K-4H-OPW-QC2 Line Card

The NCS4K-4H-OPW-QC2 line card supports OTN, packet and WDM switching for 400G traffic and contains:

- Two CFP2 ports. Each port can support 100 Gbps (DWDM QPSK) or 200Gbps (DWDM 16 QAM) WDM signals

  Note The QSFP28 ports also support QSFP+ optics and can be used as 1x40G ports or 4x10G ports.

- Four QSFP28/QSFP+ ports

  Note The QSFP+ ports can be split and used as 1x40G ports or 4x10G ports.

- Six QSFP+ ports

The NCS4K-4H-OPW-QC2 line card supports the following port configurations:

- 2-ports of 200 Gbps with CFP2 optics
- 4-ports of 100 Gbps with QSFP28 optics, 10-ports of 40 Gbps with QSFP+ optics, or 10Gbps x 40 ports (4x10G breakout) with QSFP+ optics

The card needs NCS4016-FC2-M fabric card to function in the NCS 4016 chassis. The card supports OTN and packet aggregation where both TDM switching and packet forwarding capabilities are combined in a single card. Hence, it can terminate both OTN control plane traffic as well as packet control plane traffic. For more information, see the *Hardware Installation Guide for the Cisco NCS 4000 Series Routers*.

Software

These software features have been introduced in Release 6.1.22:

OCH Mutual Circuit Diversity

This feature enables the user to allocate different paths for two circuits. Both the circuits are defined in such a way that there are no overlapping nodes (except the source node), and the paths are independent of each other.

OTN features on NCS4K-4H-OPW-QC2 Cards

The following OTN features are supported:

- PRBS - Pseudo Random Binary Sequence (PRBS) feature allows users to perform data integrity checks on their encapsulated packet data payloads using a pseudo-random bit stream pattern. PRBS generates a bit pattern and sends it to the peer router that uses this feature to detect if the sent bit pattern is intact or not.
- Breakout - enables a 40 Gigabit lane of the card to be split into four independent and logical 10 Gigabit Ethernet or OTU2/OTU2e ports. All the QSFP+ ports are break-out capable.
- Interoperability - between NCS 4000 and MSTP nodes is achieved by creating a Link Management Protocol (LMP) numbered or unnumbered UNI link between NCS4K-4H-OPW-QC2 interface on the NCS 4000 node and the optical channel Add/Drop interface on the MSTP nodes. To create OTN circuits between the NCS 4000 nodes via the MSTP network, a GMPLS OCH Trail circuit must be created between the two NCS 4000 nodes that are connected to MSTP nodes. The traffic transmitted by the OCH Trail circuit is used as a OTU4 or OTUC2 link by the OTN layer.
- Alarms - the local fault and remote fault alarms are supported.
- Circuit diversity - enables the user to create a circuit that is diverse from an existing circuit in the network. This is to increase survivability and availability in case of link failures. During the computation of a diverse circuit, the GMPLS algorithm attempts to find a shared resource link group (SRLG) diverse path. If the path is not available, node and link diversity is used to compute the new path. Enabling circuit diversity on an existing circuit causes re-signaling of the circuit. The following restrictions are applicable to ODU TUNNEL circuits:
  - The diverse circuit must have the same head node.
  - Supported only for 1+0 circuits.
  - If a diverse path is not found, the circuit is not created.
- Mutual circuit diversity - For information, see OCH Mutual Circuit Diversity, on page 3 .

External Caveats

External Bugs in Release 6.1.22

The following list contains known issues for Release 6.1.22:

Caveat ID Number	Description
CSCvd07783	Traffic is impacted for two to four milliseconds during an active RP switchover , after an ISSU is performed from Release 6.1.12 to Release 6.1.22.

Caveat ID Number	Description
CSCvd02684	During a line card FPD upgrade, OTN Digi framer process crashes.
CSCvc78034	The CFP2 pluggable for NCS4K-4H-OPW-QC2 card displays incorrect serial and part number in the CTC inventory.
CSCvd16145	The Primary-MELKOR and Backup-MELKOR FPD programmed version of the NCS4K-4H-OPW-QC2 card is not displayed after an upgrade.
CSCvc53698	Non Stop Routing - Not Ready (NSR-NR) alarm is raised instead of the RP-REDUNDANCY-LOST alarm when a power cycle is performed with one RP.
CSCvc97074	Connection to the sysadmin failed after reload.
CSCvd36078	During reload of the active RP, the fabric card reloads silently.
CSCvc71959	PCI timeout errors displayed on each RP reload.
CSCvc92925	PLX FPDs display NEED UPGD status after a chassis power cycle or reload.
CSCvc78915	In the ODU TTI pane in CTC, the Transmit and Expected fields are editable for controllers where these fields must be disabled.
CSCvc51429	ISSU downgrade or upgrade window hangs on XR commit in CTC.
CSCvc87662	Optics history PM bucket is displayed as invalid in the CLI but valid on CTC.
CSCvc54909	FIA driver crashes during RP reload.
CSCve18072	Traffic is impacted during an ISSU upgrade from Release 6.1.12 to Release 6.1.22. The fabric cards reload during ISSU.
CSCve08108	During an active RP switch-over, the VM Manager restarts in sysadmin.
CSCvc87227	During an FPD upgrade for the NCS4K-2H10T-OP-KS card, traffic is impacted for 10 minutes and the "Unqualified PPM inserted" alarm is raised.

Supported FPD Versions

The following table lists the FPD versions supported in Release 6.1.22.

Card Type	FPD Description	Req. Reload	S/W Version	Min. Req. S/W Version
NCS4009-FC-S	CCC-FPGA	No	1.05	1.05
	CCC-Power-On	No	1.03	1.03
	PLX-8608(A)	Yes	0.03	0.03
	SB Certificates(A)	No	1.00	1.00
NCS4009-FC2-S	CCC-FPGA	No	1.11	1.11
	CCC-Power-On	No	1.01	1.01
	PLX-8608	Yes	0.03	0.03
	SB Certificates	No	1.00	1.00
NCS4016-FC-M	CCC-FPGA	No	4.40	4.40
	CCC-Power-On	No	1.12	1.12
	PLX-8649	Yes	0.08	0.08
	SB Certificates	No	1.00	1.00
NCS4016-FC-S	CCC-FPGA	No	5.07	5.07
	CCC-Power-On	No	1.01	1.01
	PLX-8649	Yes	0.08	0.08
	SB Certificates	No	1.00	1.00
	CCC-FPGA	Yes	0.05	0.01
	CCC-Power-On	Yes	1.12	1.08
	PLX-8649	Yes	0.08	0.08
	SB Certificates	No	1.00	1.00
NCS4016-FC2-M	CCC-FPGA	No	1.19	1.19
	CCC-Power-On	No	1.01	1.01
	PLX-8649	Yes	0.14	0.14
	SB Certificates	No	1.00	1.00

NCS4K-2OT-O-S	Backup-ZYNQ	Yes	1.68	1.00
	CCC-FPGA	No	3.27	3.27
	CCC-Power-On	No	1.17	1.17
	DIGI1	No	2.03	2.03
	DIGI2	No	2.03	2.03
	Ethernet - Switch	Yes	1.40	1.40
	GENNUM	No	3.01	3.01
	PLX-8618	Yes	0.09	0.09
	Primary-ZYNQ	No	1.68	1.68
	SB Certificates	No	1.00	1.00
NCS4K-2OT-OP-S	CCC-FPGA	No	1.10	1.10
	CCC-Power-On	No	1.06	1.06
	Ethernet - Switch	Yes	1.02	1.02
	PLX-8632	Yes	1.00	1.00
	SB Certificates	No	1.00	1.00
	DIGI1	No	2.03	2.03
	DIGI2	No	2.03	2.03
	Primary-ZYNQ	No	1.01	1.01
NCS4K-24LR-O-S	Backup-ZYNQ	Yes	4.15	0.01
	CCC-FPGA	No	4.39	4.39
	CCC-Power-On	No	1.17	1.17
	Ethernet - Switch	Yes	1.37	1.37
	PLX-8618	Yes	0.10	0.10
	Primary-ZYNQ	No	4.17	4.17
	SB Certificates	No	1.00	1.00

NCS4K-2H-O-K	Backup-ZYNQ	Yes	1.55	0.01
	CCC-FPGA	No	3.38	3.38
	CCC-Power-On	No	1.17	1.17
	DIGI1	No	2.03	2.03
	DIGI2	No	2.03	2.03
	Ethernet - Switch	Yes	1.40	1.40
	GENNUM	No	3.01	3.01
	LEPTON	No	4.02	4.02
	PLX-8618	Yes	0.10	0.10
	Primary-ZYNQ	No	1.56	1.56
	SB Certificates	No	1.00	1.00
NCS4K-2H-W	Backup-ZYNQ	No	1.53	1.00
	CCC-FPGA	No	4.30	4.30
	CCC-Power-On	No	1.16	1.16
	EAGLE-0-FPD	No	5.05	5.05
	EAGLE-1-FPD	No	5.05	5.05
	Ethernet - Switch	Yes	1.35	1.35
	GN2411-FPD-1	Yes	3.05	3.05
	GN2411-FPD-2	Yes	3.05	3.05
	GN2411-FPD-3	Yes	3.05	3.05
	GN2411-FPD-4	Yes	3.05	3.05
	PLX-8608	Yes	0.09	0.09
	Primary-ZYNQ	No	1.53	1.53
	SB Certificates	No	1.00	1.00
NCS4K-2H10T-OP-KS	Backup-ZYNQ	Yes	1.83	1.00
	CCC-FPGA	No	1.47	1.47
	CCC-Power-On	No	1.10	1.10
	DIGI1	No	2.03	2.03
	DIGI2	No	2.03	2.03
	Ethernet - Switch	Yes	1.02	1.02
	GRIMA	Yes	1.51	1.51
	PLX-8649	Yes	0.10	0.10
	Primary-ZYNQ	No	1.83	1.83
	SB Certificates	No	1.00	1.00

NCS4K-4H-OP-K	Backup-ZYNQ	Yes	0.09	0.09
	CCC-FPGA	Yes	2.02	2.02
	CCC-Power-On	Yes	1.06	1.06
	DIGI1	No	2.03	2.03
	DIGI2	No	2.03	2.03
	Ethernet - Switch	Yes	1.01	1.01
	LEPTON	No	5.00	5.00
	PLX-8649	Yes	0.01	0.01
	Primary-ZYNQ	No	1.09	1.09
	SB Certificates	No	1.00	1.00
NCS4K-4H-OPW-QC2	Backup-MELKOR	Yes	5.07	5.07
	Backup-ZYNQ	No	3.18	3.18
	CCC-FPGA	No	0.25	0.25
	CCC-Power-On	No	1.08	1.08
	DENALI	Yes	13.48	13.48
	DIGI1	No	2.02	2.02
	DIGI2	No	2.02	2.02
	Ethernet-Switch	Yes	1.51	1.51
	PLX-8750(A)	Yes	0.07	0.07
	Primary-MELKOR	Yes	5.07	5.07
	Primary-ZYNQ	No	3.18	3.18
	SB Certificates	No	1.00	1.00
	SMAUG	Yes	0.05	0.05
NCS4K-AC-PSU	AB-PriMCU	No	1.31	1.31
	AB-Sec54vMCU	No	1.49	1.49
	AB-Sec5vMCU	No	1.43	1.43
	DT-PriMCU	No	3.00	3.00
	DT-PriMCU	No	1.06	1.06
	DT-PriMCU	No	2.01	2.01
	DT-Sec54vMCU	No	4.00	4.00
	DT-Sec54vMCU	No	2.03	2.03
	DT-Sec54vMCU	No	3.02	3.02
	DT-Sec5vMCU	No	3.01	3.01
	DT-Sec5vMCU	No	1.09	1.09
	DT-Sec5vMCU	No	2.02	2.02

NCS4K-CRAFT	Craft-NCS4009	No	1.03	1.03
	Craft-NCS4016	No	1.04	1.04
NCS4K-DC-PSU-V1	AB-PriMCU	No	1.26	1.26
	AB-Sec54vMCU	No	1.41	1.41
	AB-Sec5vMCU	No	1.52	1.52
	DT-Pri2MCU	No	3.02	3.02
	DT-Pri2MCU	No	2.02	2.02
	DT-PriMCU	No	3.02	3.02
	DT-PriMCU	No	2.02	2.02
	DT-Sec54v2MCU	No	3.01	3.00
	DT-Sec54v2MCU	No	2.05	2.05
	DT-Sec54vMCU	No	3.01	3.00
	DT-Sec54vMCU	No	2.05	2.05
	DT-Sec5vMCU	No	3.04	3.02
	DT-Sec5vMCU	No	2.06	2.06
NCS4K-ECU	ECU-FPGA	No	3.01	3.01
NCS4K-FTA	Fantray-FPGA	No	3.01	3.01
NCS4K-RP	BACKUP-BIOS	Yes	14.02	1.00
	Backup-CCC-PwrOn	Yes	1.21	1.00
	Backup-Ethswitch	Yes	1.36	1.00
	Backup-Timing	Yes	3.50	3.00
	BP-FPGA	No	3.17	3.17
	CCC-Bootloader	Yes	4.27	4.08
	CCC-FPGA	Yes	4.27	4.27
	CCC-Power-On	Yes	1.21	1.21
	CPU-Complex-Boot	Yes	2.04	2.04
	CPU-Complex-FPGA	Yes	2.04	2.04
	Ethernet - Switch	Yes	1.36	1.36
	PLX-8649	Yes	0.08	0.08
	PLX-8696	Yes	0.05	0.05
	Primary-BIOS	Yes	14.03	14.03
	SMART - iSATA	No	7.05	7.05
	SMART - SATA	No	7.05	7.05
	Timing FPGA	Yes	3.50	3.50

P-S-FANTRAY	Fantray-FPGA	No	2.04	2.04

FPD Upgrade from Release 6.1.12 to Release 6.1.22

This procedure enables you to upgrade the FPD's for fabric card, route processor (RP), and line card (LC).

Perform this procedure after performing In Service Software Upgrade (ISSU) from release 6.1.12 to release 6.1.22

Step 1 Perform FPD Upgrade for LC.
For more details refer section *Upgrade FPD using CTC* in document *OTN and DWDM Configuration Guide for Cisco NCS 4000 Series*.

Note To complete the upgrade for some FPD's, line card reload is required.

Caution LC reload is traffic impacting and must be carried in a planned maintenance window.

Step 2 Perform a non-disruptive FPD upgrade for fabric card.
For more details refer section *Non Disruptive FPD Upgrade for Fabric Card using CTC* in document *OTN and DWDM Configuration Guide for Cisco NCS 4000 Series*

Step 3 Perform a non-disruptive FPD upgrade for RP.
For more details refer section *Non Disruptive FPD Upgrade for Route Processor using CTC* in document *OTN and DWDM Configuration Guide for Cisco NCS 4000 Series*.

Cisco Bug Search Tool

Use the Bug Search Tool (BST) to view the list of outstanding and resolved bugs in a release.

BST, the online successor to Bug Toolkit, is designed to improve the effectiveness in network risk management and device troubleshooting. The tool allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The tool has provision to filter bugs based on credentials to provide external and internal bug views for the search input.

Search Bugs in BST

Step 1 Go to https://tools.cisco.com/bugsearch/. You will be prompted to log into Cisco.com. After successful login, the Bug Toolkit page open.

Step 2 Enter the bug ID in the Search For: field. To search for release bugs, enter the following parameters in the page:

a) Search For – Enter NCS4k in the text box.

b) Releases – Enter the release number.

c) Show Bugs – Select Affecting or Fixed in these Releases

Step 3 Press Enter.

- By default, the search results include bugs with all severity levels and statuses, and bugs that were modified during the life cycle of the bug. After you perform a search, you can filter your search results to meet your search requirements.
- An initial set of 25 search results is shown in the bottom pane. Drag the scroll bar to display the next set of 25 results. Pagination of search results is not supported.

Additional References

Related Documentation

Use the release notes with the following publications:

Document Title	Description
Hardware Installation Guide for Cisco NCS 4000 Series	Provides installation information about the Cisco NCS 4009 and Cisco NCS 4016 chassis.
Cisco Network Convergence System 4000 Series Unpacking, Moving, and Securing Guide	Provides instructions for unpacking the Cisco NCS 4009 and Cisco NCS 4016 chassis, moving the chassis to its permanent location, and mounting the chassis in a rack.
Regulatory Compliance and Safety Information for the Cisco NCS 4000 Series	Provides the international agency compliance, safety, and statutory information that apply to Cisco NCS 4009 and Cisco NCS 4016 chassis.
Configuration Guide for Cisco NCS 4000 Series	Provides background and reference material, procedures to configure and maintain the Cisco NCS 4009 and Cisco NCS 4016 chassis.
Command Reference for Cisco NCS 4000 Series	Provides the various commands available to configure and maintain the Cisco NCS 4009 and Cisco NCS 4016 chassis.
System Setup and Software Installation Guide for Cisco NCS 4000 Series	Provides instructions to set up the system and perform software installation.
Alarms Troubleshooting Guide for Cisco NCS 4000 Series	Provides a description, severity, and troubleshooting procedure for each commonly encountered NCS 4000 alarm and condition.

Document Title	Description
Cisco IOS XR System Error Message Reference Guide	Provides a list of the Cisco IOS XR system error messages for all Cisco IOS XR platforms
Quality of Service Configuration Guide for Cisco NCS 4000 Series	Provides features available to configure and maintain Quality of Service (QoS) for the Cisco NCS 4000 Series Routers.
Quality of Service Command Reference for Cisco NCS 4000 Series	Provides various commands available to configure and maintain Quality of Service (QoS) for the Cisco NCS 4000 Series Routers.

Technical Assistance

Link	Description
http://www.cisco.com/cisco/web/support/index.html	The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.