

Cisco NCS 4016 System Features

The topics covered in this chapter are:

- Cisco NCS 4016 Product Overview, on page 1
- Virtual Machine based Routing and System Administration, on page 2
- Command Modes, on page 2
- System Setup Workflow, on page 3

Cisco NCS 4016 Product Overview

Cisco Network Convergence System 4000 Series

The Cisco Network Convergence System (NCS) 4000 Series System is a converged optical service platform and provides dense wavelength-division multiplexing (DWDM), Optical Transport Network (OTN), Multiprotocol Label Switching Transport Profile (MPLS-TP), Carrier Ethernet, and label switch router (LSR) or IP multi service capabilities. It facilitates:

- massive scale through a state-of-the-art silicon and system design.
- network efficiency and simplification.

In order to facilitate packet-optical integration, the form factor of the Cisco NCS 4000 is compliant with typical carrier environments, with a notably shallow footprint to address ANSI and ETSI transport equipment requirements. You can deploy the system in 19 inch or 23 inch width ANSI footprints and 300 mm width ETSI footprints.

Cisco Network Convergence System 4016 System

The Cisco NCS 4016 System, part of the Cisco NCS 4000 Series System, is the next generation converged optical service platform. The system has a 24-rack-unit (24RU), rack-mountable solution with 16 service line-card slots, each with a full-duplex bandwidth of 200 Gbps. It has different cards for packet forwarding, OTN switching, and coherent DWDM transponder or trunk capability. Depending on the specific card configuration, the NCS 4016 supports numerous capabilities, including:

- Packet switching and routing
- OTN switching
- DWDM transponding and muxponding

The Cisco NCS 4016 System can be used as a converged packet-optical platform by simultaneously combining all of these capabilities.

Virtual Machine based Routing and System Administration

On the Cisco NCS Series router, the routing functions and the System Administration functions are run on separate virtual machines (VMs) over a Linux host operating system. The VMs simulate individual physical computing environments over a common hardware.. Available hardware resources, like processor, memory, hard disk, and so on, are virtualized and allocated to individual virtual machines by the hypervisor.

Implementation of Virtualized IOS XR on Cisco NCS Series Router

- The hypervisor creates and manages individual VM environments.
- On every route processor (RP) there are two VMs; one for system administration (System Admin VM) and one for managing the routing functions (XR VM).
- The two VMs on each node operate on their respective planes. On each plane, the VMs are connected to each other using a dedicated VLAN over a high-speed Control Ethernet connection.
- The System Admin VMs can detect each other's presence by auto discovery and thus maintain complete system awareness.

To access the XR VM, connect to the XR VM console port on the RP. To access the System Admin VM, in the XR VM CLI, execute the **admin** command.

Advantages of Virtualized IOS XR on the Cisco NCS Series Router

- Faster boot time—Because the System Admin functions are on a dedicated VM, the boot time is considerably reduced.
- Independent upgrades—Software packages can be independently installed on the System Admin VM and the XR VM, resulting in minimal system downtime.
- Self-starting VMs—Both the System Admin VM and the XR VM are automatically launched during router boot-up without any user intervention. They have a default set-up that is ready for use.
- System redundancy—In spite of their interconnectivity, there is also a level of isolation between the VMs. Therefore, if a particular VM experiences any issues, it does not affect the functioning of other VMs.

Command Modes

The Cisco NCS 4000 Series system runs on virtualized Cisco IOS XR software. Therefore, the CLI commands must be executed on virtual machines, namely the XR VM and the System Admin VM. This table lists the command modes for the VMs.

Command Mode	Description
XR EXEC mode (XR VM execution mode)	Run commands on the XR VM to display the operational state of the entire secure domain router (SDR). Example: `RP/0/RP0:hostname#`

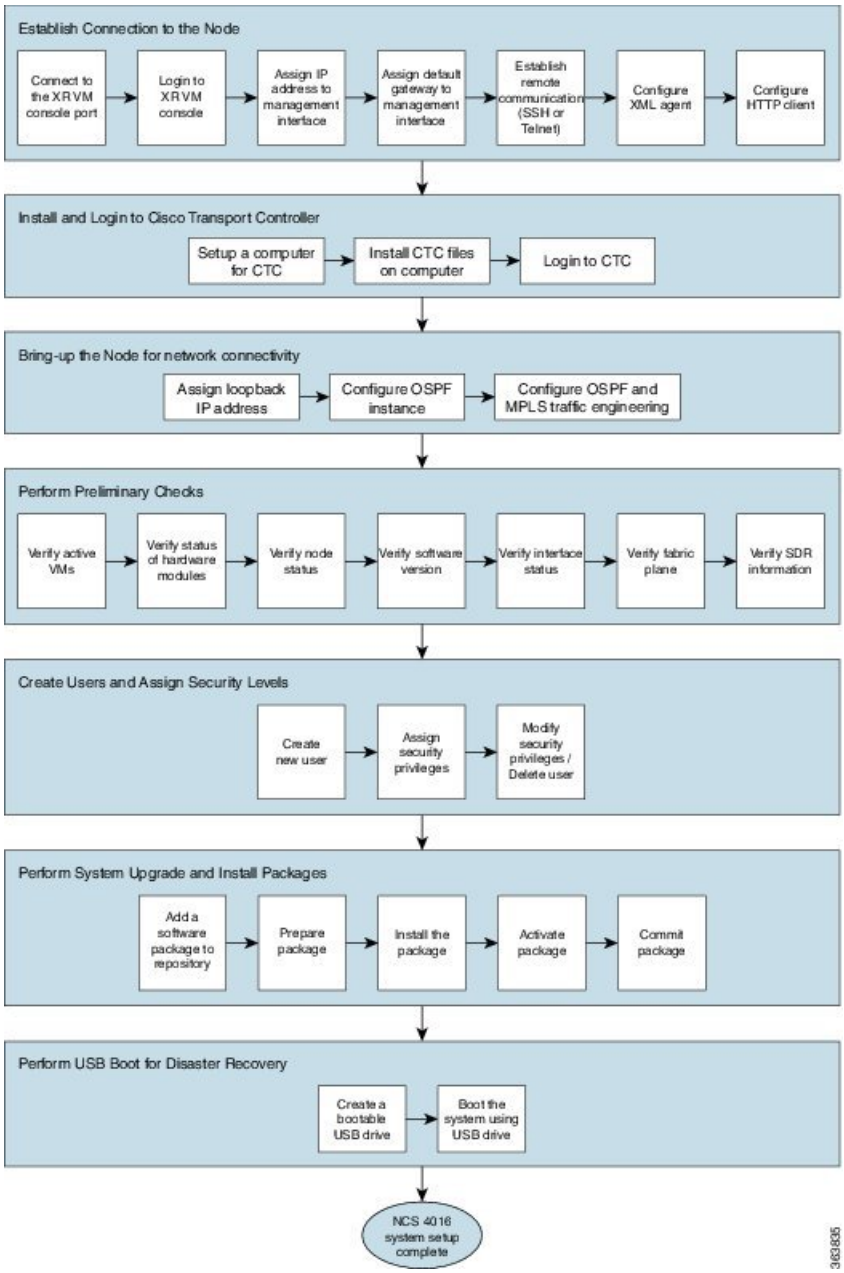
XR Config mode
(XR VM configuration mode)
	Perform security, routing, and other XR feature configurations on the XR VM.
	Example:
	`RP/0/RP0:hostname#configure`
	`RP/0/RP0:hostname(config)#`

System Admin EXEC mode
(System Admin VM execution mode)
	Run commands on the System Admin VM to display and monitor the operational state of the router hardware. The chassis or individual hardware modules can be reloaded from this mode.
	Example:
	`RP/0/RP0:hostname#admin`
	`sysadmin-vm:0_RP0#`

System Admin Config mode
(System Admin VM configuration mode)
	Run configuration commands on the System Admin VM to manage and operate the hardware modules of the entire chassis.
	Example:
	`RP/0/RP0:hostname#admin`
	`sysadmin-vm:0_RP0#config`
	`sysadmin-vm:0_RP0(config)#`

System Setup Workflow

The system setup of the Cisco NCS 4016 Series system involves these stages:



1. Establish Connection to a Node—Connect to the console port and boot-up the system. After booting is complete, bring-up the node by establishing a connection to the node using the console port.
2. Install and Login to Cisco Transport Controller— Setup a computer for Cisco Transport Controller (CTC) and login to CTC. CTC is used to perform operations, administration, maintenance and provisioning activities of the system.
3. Bring-up the Node for Network Connectivity— Configure the node to connect to the network.
4. Perform Preliminary Checks—Perform basic verification of the default setup of the system. This ensures that, if any setup issue is detected, corrective action is taken at an early stage.

5. Create User Profiles and Assign Privileges—Create users and assign privileges, as needed. Users are either permitted, or denied, the use of certain commands based on assigned privileges.
6. Perform System Upgrade and Install Feature Packages—Upgrade the operating system, if the default is not the latest version. Also, install relevant packages to deploy additional features and software patches on the system.
7. Perform Disaster Recovery—In the event of a system boot failure due to image corruption, boot the system using an external bootable USB drive.