System Setup and Software Installation Guide for Cisco NCS 4000 Series

First Published: May 26, 2015

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
   800 553-NETS (6387)
Fax: 408 527-0883
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.

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: http://www.cisco.com/go/trademarks. 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. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.
CONTENTS

Preface \( v \)

Changes to This Document \( v \)

Obtaining Documentation and Submitting a Service Request \( v \)

CHAPTER 1

Cisco NCS 4016 System Features \( 1 \)

Virtual Machine based Routing and System Administration \( 1 \)

Command Modes \( 2 \)

System Setup Workflow \( 2 \)

CHAPTER 2

Establish Connection to a Node \( 5 \)

Connect to the XR VM Console Port and Power the System \( 5 \)

Access the System Admin VM Console \( 6 \)

Configure the XR VM Management Port \( 7 \)

Connecting to the XR VM Management Port \( 8 \)

Setting up Remote Connection \( 10 \)

Configuring SSH \( 10 \)

Configuring Telnet \( 14 \)

Configuring XML Agent \( 15 \)

Configure HTTP \( 15 \)

CHAPTER 3

Install and Login to Cisco Transport Controller \( 17 \)

Setup Computer for CTC \( 17 \)

Login to CTC \( 18 \)

CHAPTER 4

Bring-up the Node for Network Connectivity \( 21 \)

Assign Loopback IP Address \( 21 \)

Configure OSPF Instance \( 22 \)
Configure OSPF and MPLS Traffic Engineering 22

CHAPTER 5
Perform Preliminary Checks 25
  Verify Active VMs 25
  Verify Status of Hardware Modules 27
  Verify Software Version 28
  Verify Firmware Version 28
  Verify Interface Status 30
  Verify Fabric Plane 30
  Verify SDR Information 31

CHAPTER 6
Create User Profiles and Assign Privileges 35
  Create a New User 35
  Modify User Settings and Security Levels 37
  Delete a User 37

CHAPTER 7
Perform System Upgrade and Install Feature Packages 39
  Upgrading the System 39
  Upgrading Features 39
  Install Packages 40
  Prepare and Install Package 42
  Install SMU using TAR 43
  Uninstall Packages 44

CHAPTER 8
Perform Disaster Recovery 47
  Boot the Router Using USB 51
  Perform System Upgrade Using USB 53
Preface

This Preface contains these sections:

- Changes to This Document, page v
- Obtaining Documentation and Submitting a Service Request, page v

Changes to This Document

This table lists technical changes made to this document since it was first released.

<table>
<thead>
<tr>
<th>Date</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 2014</td>
<td>Initial release of this document.</td>
</tr>
</tbody>
</table>

Obtaining Documentation and Submitting a Service Request


Subscribe to What's New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.
The topics covered in this chapter are:

- Virtual Machine based Routing and System Administration, page 1
- Command Modes, page 2
- System Setup Workflow, page 2

**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.

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>XR EXEC mode (XR VM execution mode)</td>
<td>Run commands on the XR VM to display the operational state of the entire secure domain router (SDR).</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>RP/0/RP0:hostname#</td>
</tr>
<tr>
<td>XR Config mode (XR VM configuration mode)</td>
<td>Perform security, routing, and other XR feature configurations on the XR VM.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>RP/0/RP0:hostname#configure</td>
</tr>
<tr>
<td></td>
<td>RP/0/RP0:hostname(config)#</td>
</tr>
<tr>
<td>System Admin EXEC mode (System Admin VM execution mode)</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>RP/0/RP0:hostname#admin</td>
</tr>
<tr>
<td></td>
<td>sysadmin-vm:0_RP0#</td>
</tr>
<tr>
<td>System Admin Config mode (System Admin VM configuration mode)</td>
<td>Run configuration commands on the System Admin VM to manage and operate the hardware modules of the entire chassis.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>RP/0/RP0:hostname#admin</td>
</tr>
<tr>
<td></td>
<td>sysadmin-vm:0_RP0#config</td>
</tr>
<tr>
<td></td>
<td>sysadmin-vm:0_RP0(config)#</td>
</tr>
</tbody>
</table>

System Setup Workflow

The system setup of the Cisco NCS 4016 Series system involves these stages:
1 Establish Connection to a Node, on page 5—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, on page 17—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, on page 21—Configure the node to connect to the network.

4 Perform Preliminary Checks, on page 25—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, on page 35—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, on page 39—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, on page 47—in the event of a system boot failure due to image corruption, boot the system using an external bootable USB drive.
Establish Connection to a Node

After installing the hardware, boot the Cisco NCS 4016 Series System. Connect to the XR VM console port and power on the system. The system completes the boot process using the pre-installed operating system (OS) image. If no image is available within the system, the system can be booted using an external bootable USB drive. For more details on booting the system using USB drive, see Perform Disaster Recovery, on page 47

After booting is complete, establish a connection to the node.

- Connect to the XR VM Console Port and Power the System, page 5
- Access the System Admin VM Console, page 6
- Configure the XR VM Management Port, page 7
- Connecting to the XR VM Management Port, page 8
- Setting up Remote Connection, page 10
- Configuring XML Agent, page 15
- Configure HTTP, page 15

Connect to the XR VM Console Port and Power the System

Use the XR VM console port on the Route Processor (RP) to connect to Network Convergence System (NCS) 4016 system. If required, subsequent connections can be established through the management port, after it is configured.

There are the three console ports on the RP. Console port 2 is for the XR VM.
### Establish Connection to a Node

#### Access the System Admin VM Console

All system administration and hardware management setups are performed from the System Admin VM.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>External USB Port</td>
</tr>
<tr>
<td>2</td>
<td>XR VM Console Port</td>
</tr>
<tr>
<td>3</td>
<td>XR VM Management Port</td>
</tr>
</tbody>
</table>

**Step 1** Connect a terminal to the XR VM console port of the RP.

**Step 2** Start the terminal emulation program on your workstation.

The console settings are 115200 bps, 8 data bits, 2 stop bits and no parity.

**Step 3** Power on the system.

Press the power switch up to turn on the power shelves. As the system boots up, you will see boot process details on the console screen of the terminal emulation program.

**Step 4** Press **Enter**.

When the system prompts you to enter the root-system username, it indicates that the boot process is complete. If the prompt does not appear, wait for a while to give the system more time to complete the initial boot procedure, then press **Enter**.

**Important** If the boot process fails, it may be because the pre-installed image on the system is corrupt. In this case, the router can be booted using an external bootable USB drive. For details see, Create a Bootable USB Drive Using Shell Script, on page 48 and Boot the Router Using USB, on page 51.

**What to Do Next**

Specify the root username and password.

---

**Step 1** Login to the XR VM console as the root user.

**Step 2** **admin**

**Example:**

```
RP/0/RP0:hostname#admin
```

After you enter the System Admin VM console, the router prompt changes to

```
sysadmin-vm:0_RP0#
```

**Step 3** (Optional) **exit**

**Example:**

```
sysadmin-vm:0_RP0#exit
```

Return to the XR VM CLI from the System Admin VM CLI.
Alternate Method to Access the System Admin VM

Instead of executing the \texttt{admin} command, you can access the System Admin prompt by directly connecting to the System Admin VM console port. Console port 1 on the RP is for System Admin VM. While connecting to the System Admin VM console port, enter the System Admin username and password, when prompted. For more details about System Admin VM username and password, see the chapter \textit{Create User Profiles and Assign Privileges}, on page 35.

\textbf{Important} It is not possible to access the XR VM through the System Admin VM console port.

Configure the XR VM Management Port

To use the XR VM Management port for system management and remote communication, you must configure an IP address and a subnet mask for the management ethernet interface. To communicate with devices on other networks (such as remote management stations or TFTP servers), configure the network subnet or host route to the default gateway.

\textbf{Before You Begin}

- Consult your network administrator or system planner to procure IP addresses and a subnet mask for the management interface.
- Physical port Ethernet 0 on RP is the management port. Ensure that the port is connected to management network.

\textbf{SUMMARY STEPS}

1. \texttt{configure}
2. \texttt{interface MgmtEth rack/slot/instanceport}
3. \texttt{ipv4 address ipv4-address subnet-mask}
4. \texttt{ipv4 address ipv4 virtual address subnet-mask}
5. \texttt{no shutdown}
6. \texttt{exit}
7. \texttt{router static address-family ipv4 unicast subnet or host route default-gateway}
8. \texttt{commit}

\textbf{DETAILED STEPS}

\begin{tabular}{lc}
\textbf{Step 1} & \texttt{configure} \\
\textbf{Step 2} & \texttt{interface MgmtEth rack/slot/instanceport} \\
\end{tabular}
Example:

```
RP/0/RP0:hostname(config)#interface mgmtEth 0/RP0/CPU0/0
```

Enters interface configuration mode for the management interface of the primary RP.

**Step 3**  
**ipv4 address ipv4-address subnet-mask**

Example:

```
RP/0/RP0:hostname(config-if)#ipv4 address 10.1.1.1 255.0.0.0
```

Assigns an IP address and a subnet mask to the interface.

**Step 4**  
**ipv4 address ipv4 virtual address subnet-mask**

Example:

```
RP/0/RP0:hostname(config-if)#ipv4 address 1.70.31.160 255.255.0.0
```

Assigns a virtual IP address and a subnet mask to the interface.

**Step 5**  
**no shutdown**

Example:

```
RP/0/RP0:hostname(config-if)#no shutdown
```

Places the interface in an "up" state.

**Step 6**  
**exit**

Example:

```
RP/0/RP0:hostname(config-if)#exit
```

Exits the Management interface configuration mode.

**Step 7**  
**router static address-family ipv4 unicast subnet or host route default-gateway**

Example:

```
RP/0/RP0:hostname(config)#router static address-family ipv4 unicast 0.0.0.0/0 12.25.0.1
```

Specifies the IP address of the default-gateway to configure a static route; this is to be used for communications with devices on other networks.

**Step 8**  
**commit**

---

**What to Do Next**

Connect to the management port to the ethernet network. See Connecting to the XR VM Management Port, on page 8.

**Connecting to the XR VM Management Port**

The XR VM management port supports 10/100G optical small form-factor pluggable (SFP) units to provide high speed network connectivity. The SFPs that can be connected to the XR VM management port are:
Datasheet

<table>
<thead>
<tr>
<th>SFP module</th>
<th>Datasheet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco SFP-10G-LR</td>
<td></td>
</tr>
<tr>
<td>1000BASE-LX/LH SFP</td>
<td></td>
</tr>
<tr>
<td>1000BASE-T SFP</td>
<td></td>
</tr>
</tbody>
</table>

Before You Begin

Configure the management port. See Configure the XR VM Management Port, on page 7.

Step 1

Connect the SFP module to the XR VM management port.

The XR VM management port on the RP is shown in this figure.

1 External USB Port
2 XR VM Console Port
3 XR VM Management Port

Step 2

Depending on the SFP module type, connect either an optical fiber or an ethernet cable to the SFP.

What to Do Next

With a terminal emulation program, establish a SSH or telnet connection to the management interface port using its IP address. For details on configuring the IP address of the management port, see Configure the XR VM Management Port, on page 7.

Before establishing a telnet session, use the `telnet ipv4|ipv6 server max-servers` command in the XR Config mode, to set number of allowable telnet sessions to the router.

For a SSH connection, the `ncs4k-k9sec` package must be installed on the router. For details about package installation, see Install Packages.
Setting up Remote Connection

Setup remote access to establish a connection to a system remotely over the network. With a terminal emulation program, establish a SSH or telnet connection to the management interface port using its IP address.

Configuring SSH

Complete this task to setup a remote connection using Secure Shell Connection (SSH). If you want to setup a remote connection using Telnet, complete Configuring Telnet, on page 14.

Before You Begin

Connect to the XR VM console port on the Route processor.
SUMMARY STEPS

1. configure
2. hostname hostname
3. domain name domain-name
4. commit
5. Perform one of the following steps based on the requirement:
   • Generate an RSA key pair.
     - To delete the RSA key pair, use the crypto key zeroize rsa command.
     - This command is used for SSHv1 only.
     
     crypto key generate rsa [usage keys | general-keys] [keypair-label]For example,
     RP/0/RP0:hostname# crypto key generate rsa general-keys

   • Enables the SSH server for local and remote authentication on the system.
     - The recommended minimum modulus size is 1024 bits.
     - Generates a DSA key pair.
     - To delete the DSA key pair, use the crypto key zeroize dsa command.
     - This command is used only for SSHv2.

     crypto key generate dsa
     For example,
     RP/0/RP0:hostname# crypto key generate dsa

6. configure
7. ssh timeout seconds
8. Do one of the following:
   • ssh server [vrf vrf-name]
   • ssh server v2

9. commit
10. show ssh
11. show ssh session details

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 2</th>
<th><code>hostname hostname</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td><code>RP/0/RP0:hostname(config)# hostname system1</code></td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Configures a hostname for your Network Convergence System (NCS) 4016 system.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th><code>domain name domain-name</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td><code>RP/0/RP0:hostname(config)# domain name cisco.com</code></td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Defines a default domain name that the software uses to complete unqualified host names.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th><code>commit</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose:</strong></td>
<td>Saves the configuration changes and remains within the configuration session.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Perform one of the following steps based on the requirement:</th>
</tr>
</thead>
</table>
| • Generate an RSA key pair. | `- To delete the RSA key pair, use the `crypto key zeroize rsa` command.`
| | `- This command is used for SSHv1 only.` |
| | `crypto key generate rsa [usage keys | general-keys] [keypair-label]` For example, `RP/0/RP0:hostname# crypto key generate rsa general-keys` |
| • Enables the SSH server for local and remote authentication on the system. | `- The recommended minimum modulus size is 1024 bits.`
| | `- Generates a DSA key pair.`
| | `- To delete the DSA key pair, use the `crypto key zeroize dsa` command.`
<p>| | <code>- This command is used only for SSHv2.</code> |
| crypto key generate dsa | For example, <code>RP/0/RP0:hostname# crypto key generate dsa</code> |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>configure</td>
<td>Enters XR Config mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RP0:hostname# configure</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>ssh timeout seconds</td>
<td>(Optional) Configures the timeout value for user authentication to AAA.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RP0:hostname(config)# ssh timeout 60</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If the user fails to authenticate itself to AAA within the configured time, the connection is aborted.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If no value is configured, the default value of 30 seconds is used. The range is from 5 to 120.</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Do one of the following:</td>
<td>• (Optional) Brings up an SSH server using a specified VRF of up to 32 characters. If no VRF is specified, the default VRF is used.</td>
</tr>
<tr>
<td></td>
<td>• ssh server [vrf vrf-name]</td>
<td>To stop the SSH server from receiving any further connections for the specified VRF, use the no form of this command. If no VRF is specified, the default is assumed.</td>
</tr>
<tr>
<td></td>
<td>• ssh server v2</td>
<td>Note  The SSH server can be configured for multiple VRF usage.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>• (Optional) Forces the SSH server to accept only SSHv2 clients if you configure the SSHv2 option by using the ssh server v2 command. If you choose the ssh server v2 command, only the SSH v2 client connections are accepted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RP0:hostname(config)# ssh or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RP0:hostname(config)# ssh server v2</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>commit</td>
<td>Saves the configuration changes and remains within the configuration session.</td>
</tr>
<tr>
<td>10</td>
<td>show ssh</td>
<td>(Optional) Displays all of the incoming and outgoing SSHv1 and SSHv2 connections to the system.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RP0:hostname# show ssh</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>show ssh session details</td>
<td>(Optional) Displays a detailed report of the SSHv2 connections to and from the system.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RP0:hostname# show ssh session details</td>
<td></td>
</tr>
</tbody>
</table>

The remote connection is configured using SSH.
What to Do Next
After the connection with the remote host is established, configure the XML agent.

Configuring Telnet

Complete this task if you want to establish a remote connection using Telnet. Is you choose to establish a remote connection using Secure Shell Connection (SSH), complete Configuring SSH, on page 10

Before You Begin
Connect to the XR VM console port on the Route processor.

SUMMARY STEPS

1. configure
2. vty-pooldefaultvalue line-template vty
3. feature telnet
4. telnet vrf-defaultipv4 servermax-servers 100

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>vty-pooldefaultvalue line-template vty</td>
</tr>
</tbody>
</table>
| **Example:** | ```
RP/0/RP0:hostname(config)# vty-pool default
0 99 line-template vty
``` | |
| **Step 3** | feature telnet | Enables the Telnet server. The default is disabled. |
| **Example:** | ```
RP/0/RP0:hostname(config)# feature telnet
``` | |
| **Step 4** | telnet vrf-defaultipv4 servermax-servers 100 | Sets the number of allowable telnet sessions to the router before establishing a telnet session. Starts a Telnet session to a remote device using IPv4. The default port number is 23. The range is from 1 to 65535. The default Virtual Routing and Forwarding (VRF) is the default VRF. |
| **Example:** | ```
RP/0/RP0:hostname(config)# telnet 10.0.0.1
``` | |

The remote connection is configured using Telnet.

What to Do Next
After the connection with the remote host is established, configure the XML agent.
Configuring XML Agent

Cisco Transport Controller (CTC) is used for operations, administration, maintenance and provisioning activities of the Network Convergence System (NCS) 4016 system. CTC communicates with the system using an Extensible Markup Language (XML) interface agent on the system. Before an XML session is established, use the console and enable the XML agent on the system.

To enable XML requests over Secure Shell (SSH) and Telnet, use the `xml agent tty` command in global configuration mode. To disable XML requests over SSH and Telnet, use the `no` form of this command.

**Before You Begin**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**SUMMARY STEPS**

1. `configure`
2. `xml agent tty`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td></td>
</tr>
<tr>
<td>Step 2 xml agent tty</td>
<td>The agent receives XML requests from external clients and returns XML responses.</td>
</tr>
</tbody>
</table>

**Example:**

```
RP/0/RP0:hostname(config)#xml agent tty
```

**What to Do Next**

After enabling the XML agent, configure HTTP server for non-secure connection and HTTPS for secure connection.

### Configure HTTP

To download the Cisco Transport Controller (CTC) application to the client workstation, and to establish initial connection between CTC and the network elements, use a standard HTTP server or a secure HTTPS server protocol.

**SUMMARY STEPS**

1. `configure`
2. `ip http server`
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ip http server</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>RP/0/RP0:hostname(config)#http server</td>
</tr>
<tr>
<td></td>
<td>RP/0/RP0:hostname(config)#http server ssl</td>
</tr>
</tbody>
</table>

**Note**: The http server and http server ssl are mutually exclusive. The HTTP or HTTPS server is enabled.

### What to Do Next

The system is configured to use CTC to access the node. Login to CTC and establish a connection to the node.
CHAPTER 3

Install and Login to Cisco Transport Controller

After you have established a connection to the node using the console port of the system, setup a computer for Cisco Transport Controller (CTC) and log into CTC. CTC is used to perform operations, administration, maintenance and provisioning activities of the system.

• Setup Computer for CTC, page 17
• Login to CTC, page 18

Setup Computer for CTC

<table>
<thead>
<tr>
<th>Component</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>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.</td>
</tr>
<tr>
<td>Operating Systems</td>
<td>One of the following:</td>
</tr>
<tr>
<td></td>
<td>• Windows:</td>
</tr>
<tr>
<td></td>
<td>• Windows 7</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008, or later</td>
</tr>
<tr>
<td></td>
<td>• Apple Mac OS X</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Ubuntu 12.10</td>
</tr>
<tr>
<td>Java Runtime Environment</td>
<td>JRE 1.6 with support for European languages</td>
</tr>
</tbody>
</table>
**Browser**

One of the following:

- Internet Explorer
- Mozilla Firefox
- Safari
- Google Chrome

### Before You Begin

Ensure that the basic configuration required to establish a connection to the node is complete. See [Establish Connection to a Node](#), on page 5.

### What to Do Next

Login to CTC and establish network connection to the node.

## Login to CTC

### Before You Begin

- Ensure that you have setup a computer that meets the hardware and software requirements to use Cisco Transport Controller (CTC).

- Ensure you have complete image installed. If you have mini.iso image installed, then the ncs4k-mgbl.pkg must be installed on the NCS 4000 system.

- Complete [Configuring XML Agent](#), on page 15.

- Complete [Configure HTTP](#), on page 15.

- Run the `snmp-server ifindex persist` command for Generalized Multi-Protocol Label Switching (GMPLS) to retain its links over a reload.

### Step 1

From the computer connected to the NCS 4016 shelves, start Windows Internet Explorer or Mozilla Firefox web browser.

### Step 2

In the browser URL field, enter the NCS 4016 IPv4 or IPv6 virtual address.

### Step 3

Press **Enter**. The browser displays a window with a Delete CTC Cache field and information about the Cisco Transport Controller Java and System environments.
• The Delete CTC Cache field deletes the CTC JAR (Java Archive) files that are downloaded to your computer when you log into NCS 4000. You perform this action if connectivity problems occur or you want to delete older CTC JAR file versions from your computer.

• If you are logging into NCS 4000 nodes in an operation network that are running different releases of CTC software, log into the node running the most recent release. If you log into a node running an older release, you will receive an INCOMPATIBLE–SW alarm for each node in the network running a new release, and CTC will not be able to manage these nodes. To check the software version of a node, select **About CTC** from the CTC Help menu. This will display the software version for each node visible on the network view. If the node is not visible, the software version can be read from the LCD display.

### Step 4
If a Java Plug-in Security Warning dialog box appears, install the public-key security certificate.

The first time you connect to NCS 4000, this process can take several minutes. After the download, a warning message window appears.

### Step 5
Click **OK**.

### Step 6
In the CTC login window, type a user name and password (both are case sensitive).

### Step 7
Each time you log in to CTC, you can select the following login options:

- **Additional Nodes** — Displays a list of current login node groups.

- **Disable Network Discovery** — Check this box to view only the NCS 4000 (and additional nodes within the login node group, if any) entered in the Node Name field. Nodes linked to this node through Data Communication Channels (DCC) are not discovered and will not appear in CTC network view. Using this option, you can decrease the CTC startup time in networks with many DCC-connected nodes, and can reduce memory consumption. If Disable Network Discovery is unchecked, CTC attempts to upgrade the CTC software by downloading more recent versions of the JAR files it finds during the network discovery. Click **Yes** to allow CTC to download the newer JAR files, or **No** to prevent CTC from downloading the JAR files.

  **Note** Upgrading the CTC software will overwrite your existing software. You must restart CTC after the upgrade is complete.

- **Disable Circuit Management** — Check this box to disable discovery of existing circuits. Using this option, you can decrease the CTC initialization time in networks with many existing circuits and reduce memory consumption. After you are logged in, you can enable circuit discovery at any time by choosing the **Enable Circuit Discovery** button on the Circuits tab.

- **SSH or Telnet** - Select an option to establish a remote connection with the node.

### Step 8
Click **Login**.

CTC is displayed with three views: Home Page, Network View, and Node View.

---

**What to Do Next**

Use CTC to bring up the node for network connectivity.
Login to CTC
Bring-up the Node for Network Connectivity

After logging into Cisco Transport Controller (CTC), bring up the node for network connectivity. This includes assigning a loopback IP address for the node, configuring an Open Shortest Path First (OSPF) instance, and configuring the OSPF and Multiprotocol Label Switching (MPLS) traffic engineering parameters.

- Assign Loopback IP Address, page 21
- Configure OSPF Instance, page 22
- Configure OSPF and MPLS Traffic Engineering, page 22

Assign Loopback IP Address

After logging into CTC, configure loopback interface. The loopback interface is a software-based logical interface, and is not associated with any physical interface, and are always in the up state. The packets routed to the loopback interface are rerouted back to the system and processed locally. The router ID must be same as the loopback address of the node.

Before You Begin
Login to Cisco Transport Controller (CTC).

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In node view, click Provisioning &gt; Network &gt; Loopback IP tab.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In Interface ID field, set the loopback interface ID.</td>
</tr>
</tbody>
</table>

Example:
For example, set the ID as Loopback0.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>In IP Address field, enter the IP address for the loopback interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>In NetMask field, enter the subnet mask for the loopback interface.</td>
</tr>
</tbody>
</table>

Example:
For example, set the subnet mask as 255.255.255.255.
Configure OSPF Instance

Configure an OSPF instance to include Network Convergence System (NCS) in OSPF-enabled networks. OSPF is used to discover the network. To enable OSPF, you need to create an OSPF routing process, specify the range of IP address associated with the routing process, and assign area IDs associated with that range of IP addresses.

An Area ID is an administrative identifier and has no relation to an IP address or IP network ID. Area IDs are not used to reflect routing data. Area 0 is the default. The area number can be changed to other number. All the nodes in the network can use the same area ID. You cannot have multiple areas inside the same instance.

Before You Begin
You must have an Open Shortest Path First (OSPF) Area ID.

Step 1
In node view, click Provisioning > Network > OSPF tab.

Step 2
In the Router ID field, select the address of the router.

Example:
For example, 1.0.0.44
This step defines the IP addresses on which OSPF runs.

Step 3
In the OSPF interfaces field, set the interface and area ID for the instance.
This defines the area ID for that interface. Areas allow the subdivision of an AS into smaller, more manageable networks or sets of adjacent networks. OSPF hides the topology of an area from the rest of the AS. An area's network topology is visible only to routers inside that area; it is not visible to routers outside that area. If you changed the Area ID, the control cards reset, one at a time. The reset takes approximately 10 to 15 minutes. The router ID is determined as the highest active loopback address.

What to Do Next
Configure the OSPF and Multiprotocol Label Switching (MPLS) traffic engineering parameters.

Configure OSPF and MPLS Traffic Engineering

To discover network topology and allocate resources, the node implements a routing protocol to distribute and maintain the topology and resource information. To reliably propagate the information, use standard IP routing protocols, such as Open Shortest Path First (OSPF) with Multiprotocol Label Switching (MPLS)-Traffic Engineering (TE) extensions. Using a common MPLS-based control plane, all network elements work as peers to dynamically establish optical paths through the network. To achieve this functionality, MPLS is assigned an ID that is same as the loopback ID and router ID. TE is enabled within a single OSPF area.

The network traffic engineering is configured using:
• OSPF-Traffic Engineering (OSPF-TE), an extension of OSPF, is a control plane protocol used to manage MPLS-based networks. OSPF-TE manages the traffic engineering information of all the nodes that are part of the same area. Any change in bandwidth availability or disruption is instantly shared between all the nodes. This helps to manage the network with accurate information.

• MPLS-TE maps traffic flows to a particular path based on the available resources. Since the router has to have the complete information about the topology and resources available in a network, OSPF is required for use with MPLS-TE. MPLS-TE builds uni-directional tunnels from a source to the destination in the form of Label Switched Paths (LSPs), which is then used for forwarding traffic.

Configure the area for which TE is enabled by issuing the mpls traffic-eng area x command, where refers to the area number Configure an IP address on the tunnel interface to forward IP packets. The IP address is configured as an unnumbered interface by using the address of a loopback interface.

To configure OSPF for OSPF-TE and MPLS-TE from Cisco Transport Controller (CTC), perform these steps:

Before You Begin
Loopback ID is set, and is same as the router ID

<table>
<thead>
<tr>
<th>Step</th>
<th>Configure MPLS-TE:</th>
</tr>
</thead>
<tbody>
<tr>
<td>a)</td>
<td>In node view, click <strong>Provisioning &gt; Network &gt; MPLS-TE</strong> tab.</td>
</tr>
<tr>
<td>b)</td>
<td>To flood the GMPLS Traffic Engineering link into a specific OSPF area and instance, specify values for these fields:</td>
</tr>
<tr>
<td></td>
<td>• Flooding-igp field as <strong>OSPF</strong></td>
</tr>
<tr>
<td></td>
<td>• OSPF Instance Name field as <strong>OTN</strong></td>
</tr>
<tr>
<td></td>
<td>• Area field as <strong>Area ID</strong>. For example, 0.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Configure OSPF-TE:</th>
</tr>
</thead>
<tbody>
<tr>
<td>a)</td>
<td>In node view, click <strong>Provisioning &gt; Network &gt; OSPF-TE</strong> tab.</td>
</tr>
<tr>
<td>b)</td>
<td>In MPLS_TE Router ID filed, select the loopback ID assigned to the system. For example, loopback0.</td>
</tr>
<tr>
<td>c)</td>
<td>In Area ID field, specify the area ID for which the MPLS is configured.</td>
</tr>
<tr>
<td>d)</td>
<td>In Autoconfig filed, select the checkbox to option to enable configuring Label Distribution Protocol (LDP) globally on each interface associated with a specific OSPF instance. LDP enables peer label switch routers (LSRs) to exchange label binding information for supporting hop-by-hop forwarding in an MPLS network.</td>
</tr>
</tbody>
</table>

Step 3 Click **Apply** to save the configuration.

What to Do Next
You have now setup the node for network connectivity. After the system is available for network connectivity, perform preliminary checks to verify that the system is setup correctly.
Configure OSPF and MPLS Traffic Engineering

Bring-up the Node for Network Connectivity
Perform Preliminary Checks

After successfully logging into the XR VM console, you must perform some preliminary checks to verify the default setup. If any setup issue is detected when these checks are performed, take corrective action before making further configurations. These preliminary checks are:

- Verify Active VMs, page 25
- Verify Status of Hardware Modules, page 27
- Verify Software Version, page 28
- Verify Firmware Version, page 28
- Verify Interface Status, page 30
- Verify Fabric Plane, page 30
- Verify SDR Information, page 31

Verify Active VMs

On the router both the XR VM and the System Admin VM must be operational. Instances of both VMs should be running on every RP. Complete this task to verify the VMs are active.

SUMMARY STEPS

1. admin
2. show redundancy summary
3. show vm

DETAILED STEPS

Step 1

admin

Example:

RP/0/RP0:hostname# admin
Enters System Admin EXEC mode.

**Step 2**

**show redundancy summary**

**Example:**
```
RP/0/RP0:hostname#show redundancy summary
Mon Mar 9 16:32:19.276 IST
Active Node Standby Node
----------- ------------
0/RP0 0/RP1 (Node Ready, NSR: Not Configured)
0/LC0 0/LC1 (Node Ready, NSR: Not Configured)
RP/0/RP0:hostname#
```

Displays the readiness of the VMs.

**Step 3**

**show vm**

**Example:**
```
sysadmin-vm:0_RP0#show vm
```

Displays the status of the VMs running on various nodes.
```
sysadmin-vm:0_RP0# sh vm
Mon Mar 9 07:52:06.173 UTC
-------- VMs found at location 0/RP0 --------
Id : sysadmin
Status : running
IP Addr: 192.0.44.1
HB Interval : NA
Last HB Sent: NA
Last HB Rec : NA
--------
Id : default-sdr
Status : running
IP Addr: 192.0.44.4
HB Interval : 0 s 500000000 ns
Last HB Sent: 663743
Last HB Rec : 663743
--------
Id : default-sdr
Status : running
IP Addr: 192.0.88.4
HB Interval : 0 s 500000000 ns
Last HB Sent: 663749
Last HB Rec : 663749
--------

-------- VMs found at location 0/RP1 --------
Id : sysadmin
Status : running
IP Addr: 192.0.88.1
HB Interval : NA
Last HB Sent: NA
Last HB Rec : NA
--------
Id : default-sdr
Status : running
IP Addr: 192.0.88.4
HB Interval : 0 s 500000000 ns
Last HB Sent: 663749
Last HB Rec : 663749
--------
Id : default-sdr
Status : running
IP Addr: 192.0.88.6
HB Interval : 10 s 0 ns
Last HB Sent: 33183
Last HB Rec : 33183
--------
sysadmin-vm:0_RP0#
```
In the above result:

- **Id**—Name of the VM. "sysadmin" represents System Admin VM; "default-sdr" represents XR VM or LC VM
- **Status**—Status of the VM
- **IP Addr**—Internal IP address of the VM

If a VM is not running on a node, in the output of the `show vm` command, no output is shown for that node.

---

**What to Do Next**

If the XR VM is not running on a node, try reloading the node. To do so, use the `hw-module location node-id reload` command in the System Admin EXEC mode. Also, use the `show sdr` command in the System Admin EXEC mode to verify that the SDR is running on the node.

---

**Verify Status of Hardware Modules**

Hardware modules include RPs, LCs, fan trays, fabric cards, and so on. On the router, multiple hardware modules are installed. Perform this task to verify that all hardware modules are installed correctly and are operational.

**Before You Begin**

Ensure that all required hardware modules have been installed on the router.

**SUMMARY STEPS**

1. Login to Cisco Transport Controller (CTC). For information on logging into CTC, see Login to CTC, on page 18.
2. In the node view, click the Inventory tab.

**DETAILED STEPS**

**Step 1**

Login to Cisco Transport Controller (CTC). For information on logging into CTC, see Login to CTC, on page 18.

**Step 2**

In the node view, click the Inventory tab.

Displays the list of hardware modules detected on the system, their location, hardware type and state. Verify that all the hardware modules installed on the chassis are listed. If a module is not listed, it indicates either that module is malfunctioning, or it is not properly installed. Remove and reinstall the hardware module.
Verify Software Version

The Cisco NCS 4018 system is shipped with the Cisco IOS XR software pre-installed. Verify that the latest version of the software is installed. If a newer version is available, perform a system upgrade. This will install the newer version of the software and provide the latest feature set on the router.

Perform this task to verify the version of Cisco IOS XR software running on the router.

SUMMARY STEPS

1. Login to Cisco Transport Controller (CTC). For information on logging into CTC, see Login to CTC, on page 18.
2. In the node view, verify the Navigation/Summary Pane in the left panel.

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Login to Cisco Transport Controller (CTC). For information on logging into CTC, see Login to CTC, on page 18.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the node view, verify the Navigation/Summary Pane in the left panel.</td>
</tr>
</tbody>
</table>

What to Do Next

Verify the result to ascertain whether a system upgrade or additional package installation is required. If that is required, refer to the tasks in the chapter Perform System Upgrade and Install Feature Packages, on page 39.

Verify Firmware Version

The firmware on various hardware components of the router must be compatible with the Cisco IOS XR image installed. Incompatibility might cause the router to malfunction. Complete this task to verify the firmware version.

SUMMARY STEPS

1. admin
2. show hw-module fpd

DETAILED STEPS

| Step 1 | admin |
Example:

RP0/RP0:hostname# admin
Enters System Admin EXEC mode.

Step 2

**show hw-module fpd**

Example:

sysadmin-vm:0_RP0#show hw-module fpd
Displays the firmware information for various hardware components of the router.

### FPD Versions

<table>
<thead>
<tr>
<th>Location</th>
<th>Card type</th>
<th>HWver</th>
<th>FPD device</th>
<th>ATR Status</th>
<th>Run Programd</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>NCS4K-20T-O-S</td>
<td>0.1</td>
<td>CCC-FPGA</td>
<td>CURRENT</td>
<td>3.26</td>
</tr>
<tr>
<td>0/2</td>
<td>NCS4K-20T-O-S</td>
<td>0.1</td>
<td>CCC-Power-On</td>
<td>CURRENT</td>
<td>1.14</td>
</tr>
<tr>
<td>0/3</td>
<td>NCS4K-20T-O-S</td>
<td>0.1</td>
<td>Ethernet-Switch</td>
<td>CURRENT</td>
<td>1.40</td>
</tr>
<tr>
<td>0/4</td>
<td>NCS4K-20T-O-S</td>
<td>0.1</td>
<td>PLX-8618</td>
<td>CURRENT</td>
<td>0.09</td>
</tr>
<tr>
<td>0/5</td>
<td>NCS4K-20T-O-S</td>
<td>0.1</td>
<td>CCC-FPGA</td>
<td>CURRENT</td>
<td>3.26</td>
</tr>
<tr>
<td>0/6</td>
<td>NCS4K-20T-O-S</td>
<td>0.1</td>
<td>CCC-Power-On</td>
<td>CURRENT</td>
<td>1.14</td>
</tr>
<tr>
<td>0/7</td>
<td>NCS4K-20T-O-S</td>
<td>0.1</td>
<td>Ethernet-Switch</td>
<td>CURRENT</td>
<td>1.40</td>
</tr>
<tr>
<td>0/8</td>
<td>NCS4K-20T-O-S</td>
<td>0.1</td>
<td>PLX-8618</td>
<td>CURRENT</td>
<td>0.09</td>
</tr>
<tr>
<td>0/9</td>
<td>NCS4K-20T-O-S</td>
<td>0.1</td>
<td>CCC-Power-On</td>
<td>CURRENT</td>
<td>1.14</td>
</tr>
<tr>
<td>0/10</td>
<td>NCS4K-20T-O-S</td>
<td>0.1</td>
<td>Ethernet-Switch</td>
<td>CURRENT</td>
<td>1.40</td>
</tr>
<tr>
<td>0/11</td>
<td>NCS4K-20T-O-S</td>
<td>0.1</td>
<td>PLX-8618</td>
<td>CURRENT</td>
<td>0.09</td>
</tr>
<tr>
<td>0/12</td>
<td>NCS4K-20T-O-S</td>
<td>0.1</td>
<td>CCC-Power-On</td>
<td>CURRENT</td>
<td>1.14</td>
</tr>
<tr>
<td>0/13</td>
<td>NCS4K-20T-O-S</td>
<td>0.1</td>
<td>Ethernet-Switch</td>
<td>CURRENT</td>
<td>1.35</td>
</tr>
<tr>
<td>0/14</td>
<td>NCS4K-20T-O-S</td>
<td>0.1</td>
<td>PLX-8608</td>
<td>CURRENT</td>
<td>0.08</td>
</tr>
<tr>
<td>0/RP0</td>
<td>NCS4K-RP</td>
<td>0.1</td>
<td>Backup-BIOS BSP</td>
<td>CURRENT</td>
<td>14.01</td>
</tr>
<tr>
<td>0/RP0</td>
<td>NCS4K-RP</td>
<td>0.1</td>
<td>Backup-CCC-PwrOn BSP</td>
<td>NEED UPGD</td>
<td>1.12</td>
</tr>
<tr>
<td>0/RP0</td>
<td>NCS4K-RP</td>
<td>0.1</td>
<td>Backup-EthSwitch BSP</td>
<td>CURRENT</td>
<td>1.36hu</td>
</tr>
</tbody>
</table>

In the result, the "RUN" column displays the current version of the firmware running on the FPD.

The "ATR Status" column displays the upgrade status of the firmware. It can display these states:

- **READY**—The firmware of the FPD is ready for an upgrade.
- **NOT READY**—The firmware of the FPD is not ready for an upgrade.
- **NEED UPGD**—A newer firmware version is available in the installed image. It is recommended that an upgrade be performed.
- **UPGD DONE**—The firmware upgrade is successful.
- **UPGD FAIL**—The firmware upgrade has failed.
- **BACK IMG**—The firmware is corrupted. Reinstall the firmware.
• UPGD SKIP—The upgrade has been skipped because the installed firmware version is higher than the one available in the image.

What to Do Next

• Upgrade the required firmware by using the upgrade hw-module location all fpd command in the System Admin EXEC mode. You can selectively update individual FPDs, or update all of them together. For the FPD upgrade to take effect, the router needs a power cycle.

• If required, turn on the auto fpd upgrade function. To do so, use the fpd auto-upgrade enable command in the System Admin Config mode. After it is enabled, if there are new FPD binaries present in the image being installed on the router, FPDs are automatically upgraded during the system upgrade operation.

Verify Interface Status

After the router has booted, all available interfaces must be discovered by the system. If interfaces are not discovered, it might indicate a malfunction in the unit. Complete this task to view the number of discovered interfaces.

SUMMARY STEPS

1. Login to Cisco Transport Controller (CTC). For information on logging into CTC, see Login to CTC, on page 18.
2. In the card view, click Provisioning > Controllers.

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 Login to Cisco Transport Controller (CTC). For information on logging into CTC, see Login to CTC, on page 18.</td>
<td>Displays the admin and service state for each controller.</td>
</tr>
<tr>
<td>Step 2 In the card view, click Provisioning &gt; Controllers.</td>
<td></td>
</tr>
</tbody>
</table>

Verify Fabric Plane

The packets traverse from the ingress to the egress interfaces over the fabric plane. There can be a maximum of four fabric planes. The Cisco NCS routing system fabric is implemented through multiple redundant fabric cards (FCs) installed in the line card chassis.

Complete this task to verify the status of the fabric planes.
Before You Begin

Install all required fabric cards on the router.

SUMMARY STEPS

1. admin
2. show controller fabric plane all

DETAILED STEPS

Step 1 admin

Example:
RP/0/RP0:hostname# admin
Enters System Admin EXEC mode.

Step 2 show controller fabric plane all

Example:
sysadmin-vm:0_RP0#show controller fabric plane all
Displays the status of the switch fabric plane.
Plane Admin Plane up->dn up->mcast
Id State State counter counter
--------------------------------------
0 UP UP 0 0
1 UP UP 0 0
2 UP UP 0 0
3 UP UP 0 0
sysadmin-vm:0_RP0#

Verify that the Admin State and Plane State for all operational planes is "UP". Each fabric card represents one plane. If the Plane State is "DN", it indicates that traffic is not able to reach any destination using the plane. If the Plane State is "MCAST_DN", it indicates that some destinations are not reachable using the plane. This indicates that one fabric card in the line card chassis (LCC) is not operational. Reinstall the fabric card and verify that its state is "OPERATIONAL" in the result of show platform command in the System Admin EXEC mode. For details, see Verify Node Status.

Verify SDR Information

Secure domain routers (SDRs) divide a single physical system into multiple logically-separated routers. SDRs are also known as logical routers (LRs). On the Cisco NCS 4000 system, only one SDR is supported. This SDR is termed the default-sdr. Every router is shipped with the default-sdr, which owns all RPs and LCs installed in the routing system. An instance of this SDR runs on all nodes. Complete this task to verify the details of the SDR instances.
SUMMARY STEPS

1. admin
2. show sdr

DETAILED STEPS

Step 1  admin

Example:

RP/0/RP0:hostname# admin
Enters System Admin EXEC mode.

Step 2  show sdr

Example:

sysadmin-vm:0_RP0# show sdr
Displays the SDR information for every node.

sdr default-sdr
location 0/RP0/VM1
sdr-id 2
IP Address of VM 192.0.44.4
MAC address of VM BE:CD:2B:84:5A:06
VM State RUNNING
start-time 2015-03-05T11:37:29.28203+00:00
Last Reload Reason CARD_SHUTDOWN
Reboot Count 1
location 0/RP0/VM2
sdr-id 2
IP Address of VM 192.0.44.6
MAC address of VM BE:CD:2B:84:5A:06
VM State RUNNING
start-time 2015-03-05T11:38:19.966782+00:00
Last Reload Reason CARD_SHUTDOWN
Reboot Count 1
location 0/RP1/VM1
sdr-id 2
IP Address of VM 192.0.88.4
MAC address of VM BE:CD:2B:84:5A:06
VM State RUNNING
start-time 2015-03-05T11:37:27.430983+00:00
Last Reload Reason CARD_SHUTDOWN
Reboot Count 1
location 0/RP1/VM2
sdr-id 2
IP Address of VM 192.0.88.6
MAC address of VM BE:CD:2B:84:5A:06
VM State RUNNING
start-time 2015-03-05T11:38:19.048927+00:00
Last Reload Reason CARD_SHUTDOWN
Reboot Count 1
sysadmin-vm:0_RP0#

For a functional SDR, the VM State is "RUNNING". If the SDR is not running on a node, no output is shown in the result, for that location. At times the node performs a core dump. During such times the VM State is "Paused & Core Dump in Progress".
What to Do Next

If you find SDR is not running on a node, try reloading the node. To do that, use the `hw-module location node-id reload` command in the System Admin EXEC mode.
Verify SDR Information
Create User Profiles and Assign Privileges

To provide controlled access to the System Admin configurations on the Cisco NCS 4016 system, user profiles are created with assigned security levels. The security levels are specified based on the operations that user is expected to perform. Users are authenticated using username and password. Authenticated users are entitled to perform operations based on their assigned security levels.

The workflow for creating user profile is represented in this flow chart:

*Figure 1: Workflow for creating user profiles*

The topics covered in this chapter are:

- Create a New User, page 35
- Modify User Settings and Security Levels, page 37
- Delete a User, page 37

Create a New User

To enable access to the node for multiple users, create new users and assign security levels. The user with username *root* can be used to set up other users.
Before You Begin
Login to Cisco Transport Controller (CTC). You must log in as a Superuser to create additional users.

Step 1
Log into the node where you need to create users.

Step 2
In node view, click the Provisioning > Security > Users tab.

Step 3
In the Users window, click Create.

Step 4
In the Create User dialog box, enter the following:

a) Name: Type the user name. The name must be a minimum of two and a maximum of 20 alphanumeric (a-z, A-Z, 0-9) characters.

b) Password: Type the user password.

Note
• The password length, by default, is set to a minimum of six and a maximum of 20 characters.
• You can configure the default values in node view using the Provisioning > NE Defaults > Node > security > passwordComplexity tabs. The minimum length can be set to two, four, eight, ten or twelve characters, and the maximum length to 80 characters.
• The password must be a combination of alphanumeric (a-z, A-Z, 0-9) and special (+, #,%) characters, where at least two characters are not alphabetic and at least one character is a special character; or the password can contain any character.
• The password must not contain the user name.

c) Confirm Password: Type the password again to confirm it.

d) Security Level: Choose a security level for the user - RETRIEVE, MAINTENANCE, PROVISIONING, or SUPERUSER.

Each security level has a different idle time. The idle time is the length of time that CTC can remain idle before the password must be reentered. The defaults are: Retrieve user = unlimited, Maintenance user = 60 minutes, Provisioning user = 30 minutes, and Superuser = 15 minutes.

e) Click OK.

Step 5
To create new user on multiple nodes:

Note All nodes where you want to add users must be accessible in network view.

a) Go to the Network View, and click Provisioning > Security > Users.

b) Follow steps 3 and 4.

c) In the Select Applicable Nodes area, deselect any nodes where you do not want to add the user (all network nodes are selected by default).

d) In the User Creation Results dialog box, verify that the user was added to all the nodes chosen in Step 5c. If not, click OK and repeat steps 2 to 6.

Step 6
Click OK.

The user is created on the node.

What to Do Next
If you want to modify the user settings, you can change the settings.
Modify User Settings and Security Levels

You can change the user settings of an existing user at one node or at multiple nodes. The modifications that you make will only be applicable when the user logs out and logs back into Cisco Transport Controller (CTC).

Before You Begin
Login to CTC. You must log in as a Superuser to modify user privileges.

Step 1
To change user setting on a single node:

a) In node view, click the Provisioning > Security > Users tab.

b) Click the user whose settings you want to modify, and click Edit.

c) In the Change User dialog box, you can:
   • Change a user password
   • Modify the user security level

d) Click OK.

Step 2
To change user settings on multiple nodes:

a) From the View menu, choose Go to Network View.

b) Click the Provisioning > Security > Users tab. Verify that you can access all the nodes where you want to change the user settings.

c) Click the user whose settings you want to modify, and click Change.

d) Change the settings.

e) In the Select Applicable Nodes area, uncheck any nodes where you do not want to change the user settings. All network nodes are selected by default.

   Note The Select Applicable Nodes area does not appear for users who are provisioned for only one node.

f) Click OK.

The user settings on the node is changed.

What to Do Next

If you want to delete a user from a single node or multiple nodes, you can delete the user.

Delete a User

You can delete a user at one node or at multiple nodes. The modifications that you make will only be applicable when the user logs out and logs back into Cisco Transport Controller (CTC). You cannot delete a user who is currently logged in.
CTC will allow you to delete a user with superusers security level only if another superuser is present. For example, you can delete the superuser with user name root, if you have created another superuser. Use this option with caution.

**Before You Begin**

Login to CTC. You must log in as a Superuser to delete users.

---

**Step 1**  
To delete a user from single node:

a) In node view, click the **Provisioning > Security > Users** tab.

b) Click the user you want to delete, and click **Delete**.

c) In the Delete User dialog box, verify that the user name displayed is the one that you want to delete.

d) Click **Logout before delete** if the user is currently logged in.

e) Click **OK**.

**Step 2**  
To change user settings on multiple nodes:

a) From the View menu, choose **Go to Network View**.

b) Click the **Provisioning > Security** tab.

c) Select the name of the user you want to delete, and click **Delete**.

d) In the Select Applicable Nodes area, uncheck any nodes where you do not want to delete the user settings.

   **Note**  
   The Select Applicable Nodes area does not appear for users who are provisioned for only one node.

e) Click **OK**.

---

The selected user is deleted from the node.
Perform System Upgrade and Install Feature Packages

In Cisco NCS 4016 systems, the system upgrade and package installation processes are run using Cisco Transport Controller (CTC). The processes involve adding and activating the iso images (.iso), feature packages (.pkg), and software maintenance upgrade files (.smu) on the system. These files are accessed from a network server and then activated on the system. If the installed package or SMU causes any issue on the router, it can be deactivated.

- Upgrading the System, page 39
- Upgrading Features, page 39
- Install Packages, page 40
- Prepare and Install Package, page 42
- Install SMU using TAR, page 43
- Uninstall Packages, page 44

Upgrading the System

The system upgrade is done using an ISO image file. Upgrading the system is the process of installing a new version of the Cisco IOS XR operating system on the router. The router comes pre-installed with the Cisco IOS XR image. You can install the new version to update to the latest features.

Related Topics

Install Prepared Packages
install prepare

Upgrading Features

Upgrading features is the process of deploying new features and software patches on the router. Feature upgrade is done by installing package files, termed simply, packages. Software patch installation is done by installing Software Maintenance Upgrade (SMU) files.
Installing a package on the router installs specific features that are part of that package. Cisco IOS XR software is divided into various software packages; this enables you to select the features to run on your router. Each package contains components that perform a specific set of router functions, such as routing, security, modular services card (MSC) support, and so on. Standard XR VM packages are:

- ncs4k-mpls.pkg
- ncs4k-mgbl.pkg
- ncs4k-k9sec.pkg

Package and SMU installation is performed using Cisco Transport Controller (CTC).

There are separate packages and SMUs for the XR VM and the System Admin VM. They can be identified by their filenames. The XR VM package has `ncs4k` as part of its filename, whereas the System Admin VM package has `ncs4k-sysadmin` as part of its filename. The XR VM packages or SMUs are activated from the XR VM, whereas the System Admin VM packages or SMUs are activated from the System Admin VM.

**Note**
Check the type of SMU before installing it in CTC.

---

**Install Packages**

Complete this task to upgrade or install a patch. The patch installation is done using packages and Software Maintenance Updates (SMUs). This task is also used to install .tar files. The .tar file contains multiple packages and SMUs that are merged into a single file. A single .tar file can contain up to 64 individual files.

In-Service Software Upgrade (ISSU) is used to perform planned software upgrades without affecting the traffic. You can use the ISSU Upgrade wizard to upgrade the XR and SysAdmin installation type without affecting the traffic. You cannot run ISSU upgrade if a package is present in prepare mode in the Prepare, Active and Commit packages area. You can either clean the prepared package or Activate the prepared packages before running ISSU upgrade. ISSU Upgrade wizard options are displayed according to the selected installation type.

**Note**
ISSU option is not available for System installation type but is available for XR and SysAdmin installation types only.

**Before You Begin**

- Two route processors (RP), one active and one stand-by must be installed in the system.
- Ensure both the RPs are in operational mode, active and running using the command `show platform`.
  
  For example:
  
  ```
  RP/0/RP0:J_59_60#show platform
  Thu Jan 5 03:24:20.535 UTC
  Node name Node type Node state Admin state Config state
  -----------------------------------------------
  0/6 NCS4K-20T-O-S OPERATIONAL UP NSHUT
  0/RP0 NCS4K-RP OPERATIONAL UP NSHUT
  0/RP1 NCS4K-RP OPERATIONAL UP NSHUT
  0/FC0 NCS4016-FC-M OPERATIONAL UP NSHUT
  0/FC1 NCS4016-FC-M OPERATIONAL UP NSHUT
  0/FC2 NCS4016-FC-M OPERATIONAL UP NSHUT
  0/FC3 NCS4016-FC-M OPERATIONAL UP NSHUT
  ```
Perform System Upgrade and Install Feature Packages

Install Packages

Step 1
In node view, click the Maintenance > Software tabs.

Step 2
Select the installation type and click Add to add new packages in the Inactive Packages area. XR installation type is selected by default.

Step 3
Type the location of the package in the Package Path field.

Step 4
Click Add to Install List to add the package to the Select Packages area. The Select Packages area displays a list of all the packages added for the installation.

Step 5
Select the packages.

Step 6
Continue with step 7 to install packages using ISSU, or step 8 to install packages using non-ISSU:

Step 7
Install package using ISSU:
   a) Click Extract (Required for ISSU).
   b) Click Install Add.
      A message to confirm whether to proceed with ISSU upgrade is displayed.
   c) Click Yes to continue with ISSU upgrade.
      Note: If you click No, the ISSU upgrade is discontinued. The XR ISO image is displayed in XR panel and SysAdmin and Host ISO images are displayed in SysAdmin panel. An ISSU Upgrade wizard is displayed. This wizard includes the installation on both XR and Sysadmin packages with the complete package information.
   d) Follow the ISSU Upgrade wizard to complete the installation of XR and Sysadmin packages using ISSU.
      The SysAdmin installation is completed first followed by the XR installation.
      Note: When the SysAdmin installation is completed, the node view is closed and the network view is displayed. Open the node view and go to the installation pane, a message System ISSU upgrade has not completed, do you want to proceed? is displayed. Click Yes to proceed with the ISSU XR installation.

Step 8
Install package using non-ISSU:
   a) Click Install Add to add the selected packages to the Inactive Packages area Software tab.
   b) Click Close in the Add Package dialog.
   c) From the Installation Type drop-down list, choose XR.
   d) Select the image and click Activate.
      The system reloads with the new full image.
   e) Click Commit to commit the activated package.
      Note: For SysAdmin or System installation, in step c, select SysAdmin or System respectively. Complete steps d and e.
      The committed package is displayed in green color in the right panel.

The package is installed.
What to Do Next

- Verify that the upgrade is successful by viewing the logs. To see the logs, click the Install Log button. The logs can be filtered based on date, time, operation type and so on. Three types of logs are available:
  - Current - Displays log for current install operation.
  - All - Displays logs for all sessions.
  - Last - Enter the number for which you want to view the logs run recently. For example, if you enter 5, the logs for the last 5 sessions are displayed.

Prepare and Install Package

A system upgrade or feature upgrade is performed by activating the ISO image file, packages, and SMUs. It is possible to prepare these installable files before activation. During the prepare phase, pre-activation checks are made and the components of the installable files are loaded on to the router setup. The prepare process runs in the background and the router is fully usable during this time. When the prepare phase is over, all the prepared files can be activated instantaneously. The advantages of preparing before activation are:

- If the installable file is corrupted, the prepare process fails. This provides an early warning of the problem. If the corrupted file was activated directly, it might cause router malfunction.
- Directly activating an ISO image for system upgrade takes considerable time during which the router is not usable. However, if the image is prepared before activation, not only does the prepare process run asynchronously, but when the prepared image is subsequently activated, the activation process too takes very less time. As a result, the router downtime is considerably reduced.

Complete this task to install packages after preparing the package:

---

**Step 1**
In node view, click the **Maintenance > Software** tabs.

**Step 2**
From the Installation Type drop-down list, choose **XR**, or **SysAdmin** based on installation type. The packages that can be installed depend on the chosen installation type.

**Step 3**
Click **Add** to add new packages in the Inactive Packages area. The Add Package dialog appears.

a) Type the location of the package in the Package Path field.
b) Click **Add to Install List** to add the package to the Select Packages area. The package is added locally.
c) The Select Packages area displays a list of all the packages added for the installation.
d) Check the required check boxes in the Select Packages area to select the packages.
e) Click **Install Add** to add the selected packages to the Inactive Packages area of the **Maintenance > Software** tabs. The package is added to the router.
f) Click **Close** in the Add Package dialog.

**Step 4**
Check the required packages in the Inactive Packages area and click **Prepare>>** to prepare the packages and move the selected packages from the Inactive Packages area to the Prepare, Active and Commit Packages area. All the packages in the prepare mode are highlighted in grey color.
If a package is in Prepare state, the options available are to:

- Activate the prepared package.
- Clean the install prepare operation.

**Step 5**  
Check the required packages in the prepare mode in the Prepare, Active and Commit Packages area and click **Activate** to activate the packages.

All the packages in the active mode are highlighted in Orange. The Activate button is enabled only when at least one prepare mode package exists in the Prepare, Active and Commit Packages area.

**Note**  
- Only one boot image can be in committed state at point of time, but there can be multiple boot images in active state.
- Boot image cannot be deactivated.
- If a package is in Active state, and if the system is rebooted, the active package will not appear in the Prepare, Active, and Commit Packages area, but will be moved to the Inactive packages list. So before reboot, the Active package must be committed for the changes to take effect.

**Step 6**  
Click **Commit** to install the active packages in Prepare, Active and Commit Packages area on the router.

All the packages in the commit mode are highlighted in Green. The boot image always appear in Prepare, Active and Commit Packages area in commit mode and cannot be deactivated.

The package in active mode moves to the Inactive Packages after the reboot of the system. The package in commit mode remains in the Prepare, Active and Commit Packages even after the reboot of the system.

**Step 7**  
Click **Install Log** to view the log details of the installed software packages.

The package is prepared and installed.

**What to Do Next**  
Verify that the package is installed successfully using the **Install Log** button. Select the type of logs: Current, All or Last. The logs display the information about the package installation.

**Install SMU using TAR**

Complete this task to install a patch. The patch installation is done using packages and SMUs. This task is used to install .tar files. The .tar file contains multiple packages and SMUs that are merged into a single file. A single .tar file can contain up to 64 individual files.

**Before You Begin**

Copy the .tar to be installed either on the router's hard disk or on a network server to which the router has access.

**Step 1**  
To add the package:

a) In node view, click the **Maintenance > Software** tabs.
b) In Installation Type field, select XR and click Add.

c) Type the location of the .tar file in the Package Path field.

Note: Do not select the Active package after the add operation when adding .tar file.

d) Click Install Add.

e) Click Refresh.

The package is displayed in the Inactive Packages area.

Step 2

To activate the package:

a) In Installation Type field, select XR for XR installation and select all inactive packages.

Note: Activation must first be done on XR and then on SysAdmin.

b) Click Activate and click Yes to confirm activation.

Note: In XR installation, the System or SDR will reload if there is a reload SMU.

• In SysAdmin installation, SysAdmin and XR will reload.

• The connection to the Node view will be lost due to the reload. After the reload, go to the node view and click Maintenance > Software tabs.

The active packages are displayed in Prepare, Active and Commit Packages section in orange color.

c) Select all active packages and click Commit.

The committed package is displayed in green color in the right pane.

d) In the Installation Type field, select SysAdmin for SysAdmin installation and select all inactive packages.

e) Follow steps b and c.

What to Do Next

• Verify that the upgrade is successful by viewing the logs. To see the logs, click the Install Log button.

• Verify the output of show platform from both XR and SysAdmin. Ensure that all cards are in operational state.

<table>
<thead>
<tr>
<th>Node name</th>
<th>Node type</th>
<th>Node state</th>
<th>Admin state</th>
<th>Config state</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/0</td>
<td>NCS4K-24LR-O-S</td>
<td>OPERATIONAL</td>
<td>UP</td>
<td>NSHUT</td>
</tr>
<tr>
<td>0/1</td>
<td>NCS4K-2H-O-K</td>
<td>OPERATIONAL</td>
<td>UP</td>
<td>NSHUT</td>
</tr>
<tr>
<td>0/3</td>
<td>NCS4K-20T-O-S</td>
<td>OPERATIONAL</td>
<td>UP</td>
<td>NSHUT</td>
</tr>
<tr>
<td>0/6</td>
<td>NCS4K-20T-O-S</td>
<td>OPERATIONAL</td>
<td>UP</td>
<td>NSHUT</td>
</tr>
</tbody>
</table>

Uninstall Packages

Complete this task to uninstall a package. All router functions that are part of the uninstalled package are deactivated. Packages that are added in the XR VM cannot be uninstalled from the System Admin VM, and vice versa.
Installed ISO images cannot be uninstalled. Also, kernel SMUs that install third party SMU on host, XR VM and System Admin VM, cannot be uninstalled. However, subsequent installation of ISO image or kernel SMU overwrites the existing installation.

The workflow for uninstalling a package is shown in this flowchart.

**Figure 2: Uninstalling Packages Workflow**

1. **Step 1**  
   In node view, click the **Maintenance > Software** tabs.

2. **Step 2**  
   In Prepare, Active and Commit Packages section, select the Active package to be deactivated. The Active package is displayed in orange color.

3. **Step 3**  
   Click **Deactivate**.  
   All features and software patches associated with the package are deactivated. You can deactivate multiple packages simultaneously.  
   The deactivated packages are now listed in the Inactive Packages area. Only inactive packages can be removed from the repository.

4. **Step 4**  
   To remove the inactive package from the repository, select the package from the Inactive Packages area.

5. **Step 5**  
   Click **Remove**.
The package is removed from the Inactive panel.

**What to Do Next**

Install required packages. For details, see Install Packages, on page 40.
Perform Disaster Recovery

The topics covered in this chapter are:

- Create a Bootable USB Drive, page 47
- Boot the Router Using USB, page 51
- Perform System Upgrade Using USB, page 53

Create a Bootable USB Drive

The bootable USB drive is used to re-image the router for the purpose of system upgrade or boot the router in case of boot failure. The bootable USB drive can be created in two ways:

- Create a Bootable USB Drive Using Compressed Boot File, on page 47 (applicable to Cisco IOS XR Software Release 5.0.1)
- Create a Bootable USB Drive Using Shell Script, on page 48

Create a Bootable USB Drive Using Compressed Boot File

A bootable USB drive is created by copying a compressed boot file into a USB drive. The USB drive becomes bootable after the contents of the compressed file are extracted.

This task can be completed using Windows, Linux, or MAC operating systems available on your local machine. The exact operation to be performed for each generic step outlined here depends on the operating system in use.

Before You Begin

- Have access to a USB drive with a storage capacity that is between 2GB (min) and 32 GB (max). USB 2.0 and USB 3.0 are supported.
- Copy the compressed boot file from the software download page at cisco.com to your local machine. The file name for the compressed boot file is in the format `ncs4k-usb-boot-<release_number>.zip`. For example, `ncs4k-usb-boot-3.2.3.zip`. 
SUMMARY STEPS

1. Connect the USB drive to your local machine and format it with FAT32 file system.
2. Copy the compressed boot file to the USB drive.
3. Unzip the compressed boot file inside the USB drive.
4. The contents of the compressed boot file ("EFI" and "Boot" directories) should be extracted to the root of the USB drive. If they are extracted to a separate folder, move them to the root of the USB drive.

DETAILED STEPS

Step 1  Connect the USB drive to your local machine and format it with FAT32 file system.
Step 2  Copy the compressed boot file to the USB drive.
Step 3  Unzip the compressed boot file inside the USB drive.
Step 4  The contents of the compressed boot file ("EFI" and "Boot" directories) should be extracted to the root of the USB drive. If they are extracted to a separate folder, move them to the root of the USB drive. USB drive is bootable when the "EFI" and "Boot" directories are in the root of the USB drive.

What to Do Next

Use the bootable USB drive to boot the router or upgrade its image. See:

- Boot the Router Using USB, on page 51
- Perform System Upgrade Using USB, on page 53

Create a Bootable USB Drive Using Shell Script

To create the bootable USB drive using shell script, you need an ISO image file and the shell script that creates the boot device. The shell script is available on the router itself. Create the bootable USB drive as an preemptive measure when the router is operational. If router is already unusable, create the bootable USB drive on another active router or as instructed in the procedure Create a Bootable USB Drive Using Compressed Boot File, on page 47.

Note

The contents of the USB drive is erased during the process of creating the bootable drive.

Before You Begin

- Have access to a USB drive with a storage capacity that is between 2GB (min) and 32 GB (max). USB 2.0 and USB 3.0 are supported.
- ISO image must be present on a network server.
SUMMARY STEPS

1. copy tftp:source disk1:destination
2. dir /disk1:
3. run ls /usr/bin/usb-install.sh
4. Connect the USB drive.
5. run
6. tail /var/log/messages
7. cd directory path
8. <shell_script_file_name> <location_of_iso_image> <mount_location_of_USB_device>

DETAILED STEPS

Step 1  copy tftp:source disk1:destination

Example:
RP/0/RP0:hostname# copy tftp://223.255.254.254/image/ncs4k-mini-x.iso disk1:/ncs4k-mini-x.iso
Copy the ISO image from a network server to the router hard disk.

Step 2  dir /disk1:

Example:
RP/0/RP0:hostname# dir /disk1:
Verify that the image is copied. The result of this command displays the ISO file name.

Directory of /disk1:/

```
12 -rw-r--r--  1 7864320 Jun 27 20:30 ncs4k-mini-x.iso
```

Step 3  run ls /usr/bin/usb-install.sh

Example:
RP/0/RP0:hostname# run ls /usr/bin/usb-install.sh
Verify that the shell script is available on the router. The *usb-install.sh* script must be present in the command output.

```
run ls /usr/bin/usb*.sh
430 -rwx------  1 8456 Jun 20 23:30 /usr/bin/usb-install.sh
```

Step 4  Connect the USB drive.
The USB drive must be connected to the USB port on the RP to which the *iso* image has been copied. The USB port is shown in this figure.
Step 5  run

Example:
RP/0/RP0:hostname# run
Enters the XR VM Linux shell. The router prompt changes to:
[xr-vm_node0_RP0_CPU0:/]$ 

Step 6  tail /var/log/messages

Example:
[xr-vm_node0_RP0_CPU0:/]$ tail /var/log/messages
Identifies the device name to which the USB drive is been mapped. The USB drive is auto-discoverable on the XR VM shell.

... 
Aug 16 18:56:07 xr-vm kernel: virtio-pci 0000:c0:08.0: setting latency timer to 64
Aug 16 18:56:07 xr-vm kernel: virtio-pci 0000:c0:08.0: irq 93 for MSI/MSI-X
Aug 16 18:56:07 xr-vm kernel: virtio-pci 0000:c0:08.0: irq 94 for MSI/MSI-X
Aug 16 18:56:07 xr-vm kernel: vde: vde1

In this example, we identify from the last entry that the USB is mapped as "vde".

Step 7  cd directory path

Example:
[xr-vm_node0_RP0_CPU0:/]$ cd /usr/bin
Access the directory where the shell script is present.

Step 8  <shell_script_file_name> <location_of_iso_image> <mount_location_of_USB_device>

Example:
[xr-vm_node0_RP0_CPU0:/usr/bin]$ ./usb-install.sh /disk1:/ncs4k-mini-x.iso /dev/vde/
Runs the script to create the bootable USB drive. After the process is complete, this message is displayed:
USB stick set up for EFI boot!

What to Do Next
Use the bootable USB drive to boot the router or upgrade its image. See:

- Boot the Router Using USB, on page 51
- Perform System Upgrade Using USB, on page 53
Boot the Router Using USB

The router can be booted using an external bootable USB drive. This might be required when the router is unable to boot from the installed image. Boot failure can happen when the image gets corrupted. During the USB boot process the router gets re-imaged with the version available on the USB drive.

The default boot sequence is USB disk, Sata disk and PXE boot.

**Note**
- During the USB boot process, the router is completely re-imaged with the iso image version present in the bootable USB drive. All existing configurations are deleted because the disk 0 content is erased. No optional packages are installed during the upgrade process; they need to be installed after the upgrade is complete.
- When the USB boots to a new image, the second RP must be physically unplugged or must be powered off. Else, while reloading after installation of new image, the system will pickup the old image from the other card.

**Before You Begin**
- Create a bootable USB drive. See Create a Bootable USB Drive Using Shell Script, on page 48 or Create a Bootable USB Drive Using Compressed Boot File, on page 47 based on requirement.
- Ensure that an external connection unit (ECU) with two solid-state drives (SSDs) are present.

**Step 1**
Connect the USB drive to an RP.
The USB port on the RP is shown in this figure.

1. External USB Port
2. XR VM Console Port
3. XR VM Management Port

**Step 2**
Connect to the console.
If it is not already connected, connect a terminal to the System Admin console port of the RP. If two RPs are installed on the router, connect to the System Admin console port of both RPs. Start the terminal emulation program on your workstation.
Step 3  Power on the router.

Step 4  Press F12 on the console of the RP to which the USB is not connected. This action displays the boot menu and pauses the boot process. The RP on which the USB is connected should boot normally. Only the RP having the USB should boot. The booting of other RP is paused.

Step 5  Select the USB drive to boot from USB.
According to the default boot sequence, the USB drive is the first boot source. Because the USB device is already connected, the router automatically boots from it. During the boot process, the OS image is installed on the router so that in future the router boots without the USB.

According to the default boot sequence, the Sata disk is the first boot source and the USB drive is the second boot source. During the boot process, the OS image is installed on the router so that in future the router boots without the USB.

Step 6  Remove the USB drive.
After the initial boot sequences are completed, this message is displayed:
Running install image: Please reboot the system
On receiving this message, remove the USB drive.

Note  The USB drive should not be left connected on the router during regular operation. If the router reloads when the USB drive is connected, all existing configurations will be deleted as the router gets re-imaged.

Step 7  Press Enter to get the host prompt.

Step 8  Login to the host using root and lab as username and password respectively.

Example:
host login: root
Password:
If there is no space in the RP, a prompt to either abort installation or to continue with formatting the disk is displayed.
The prompt changes to:
[Install image, reboot required host:~]$ 

Step 9  Run the reboot command.

Example:
[Install image, reboot required host:~]$ reboot
The RP reboots with the new image. After the booting is completed, specify the root-system username and password. For details, see Setup Root User Credentials and Login to XR VM Console.

Step 10  Access the System Admin EXEC mode and reload the RP for which the boot process was paused in Step 4.

Example:
sysadmin-vm:0_RP1#hw-module location 0/RP1 reload
The shut down RP is reloaded and gets synchronized with the other RP running the new image.

What to Do Next

- After the booting process is complete, specify the root username and password. For details, see Setup Root User Credentials and Login to XR VM Console.

- Install the required optional packages.
Perform System Upgrade Using USB

The router image can be upgraded using an external bootable USB drive. This might be required when the router is to be re-imaged, but the ISO image cannot be accessed over the network. It can happen when network connectivity is unavailable.

Note
During the upgrade all existing configurations are deleted because the disk 0 content is erased.

Before You Begin

• Create a bootable USB drive. See Create a Bootable USB Drive Using Shell Script, on page 48 or Create a Bootable USB Drive Using Compressed Boot File, on page 47 based on requirement.

• Ensure that the router BIOS version is 14.xx or higher.
  * Verify the BIOS version using the `show fpd package` command in the System Admin EXEC mode.
  * Verify the actual state of all FPGA of the system and whether it require an upgrade or not using the `show hw-module fpd` command in System Admin EXEC mode.
  * If required, upgrade the BIOS using the `upgrade hw-module location all fpd BIOS\FPD` command in the System Admin EXEC mode.

Step 1
`hw-module location node-id shutdown`

Example:
`sysadmin-vm:0_RP0#hw-module location 0/RP1 shutdown`
Shut down one RP. In this example, the RP1 is shut down. During the system upgrade, only one RP should be operational.

Step 2
Connect the USB drive.
The USB drive must be connected to the USB port on the operational RP. The USB port is shown in this figure.

```
1  External USB Port
2  XR VM Console Port
3  XR VM Management Port
```
Step 3  
\textit{hw-module location node-id reload}

\textbf{Example:}
```
sysadmin-vm:0_RP0#hw-module location 0/RP0 reload
```
Reload the RP on which the USB is connected. As the RP reloads, it boots from the USB drive and gets re-imaged.

Step 4  
Remove the USB drive.  
After the initial boot sequences are complete, this message is displayed:
```
Running install image: Please reboot the system
```
On receiving this message, remove the USB drive.

\textbf{Note}  
The USB drive should not be left connected on the router during regular operation. If the router reloads when the USB drive is connected, all existing configurations will be deleted as the router gets re-imaged.

Step 5  
Press \texttt{Enter} to get the host prompt.

Step 6  
Login to the host using \texttt{root} and \texttt{lab} as username and password respectively.

\textbf{Example:}
```
host login: root
Password:
```
The prompt changes to:
```
[Install image, reboot required host:~]$ 
```

Step 7  
Run the \texttt{reboot} command.

\textbf{Example:}
```
[Install image, reboot required host:~]$ reboot
```
The RP reboots with the new image. After the booting is completed, specify the root-system username and password. For details, see Setup Root User Credentials and Login to XR VM Console.

Step 8  
Access the System Admin EXEC mode and reload the RP that was shut down in Step 1.

\textbf{Example:}
```
sysadmin-vm:0_RP0#hw-module location 0/RP1 reload
```
The shut down RP is reloaded and gets synchronized with the other RP running the new image.

---

\textbf{What to Do Next}

- Run the \texttt{show version} command in the XR EXEC mode to verify that the new image version is successfully installed.
- Install the required optional packages.