

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

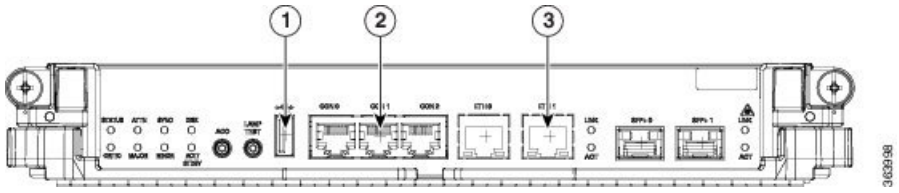
After booting is complete, establish a connection to the node.

- Connect to the XR VM Console Port and Power the System, on page 1
- Configure the XR VM Management Port, on page 2
- Connecting to the XR VM Management Port, on page 4
- Setting up Remote Connection, on page 5
- Configuring XML Agent, on page 9
- Configure HTTP, on page 10

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.



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

Procedure

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, 1 stop bit 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 Bootable USB Drive Using Shell Script and Boot the Router Using USB.

What to do next

Specify the root username and password.

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.

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.

SUMMARY STEPS

1. **configure**
2. **interface MgmtEth** *rack/slot/instanceport*
3. **ipv4 address** *ipv4-address subnet-mask*

4. **ipv4 address** *ipv4 virtual address subnet-mask*
5. **no shutdown**
6. **exit**
7. **router static address-family ipv4 unicast** *subnet or host route default-gateway*
8. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

Step 1 **configure**

Example:

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

Enters XR Config mode.

Step 2 **interface MgmtEth** *rack/slot/instanceport*

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 Use the **commit** or **end** command.

commit —Saves the configuration changes and remains within the configuration session.

end —Prompts user to take one of these actions:

- **Yes** — Saves configuration changes and exits the configuration session.
- **No** —Exits the configuration session without committing the configuration changes.
- **Cancel** —Remains in the configuration session, without committing the configuration changes.

What to do next

Connect to the management port to the ethernet network. See Connecting to the XR VM Management Port, on page 4.

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:

SFP module	Datasheet
Cisco SFP-10G-SR	http://www.cisco.com/en/US/prod/collateral/modules/ps5455/data_sheet_c78-455693.html
Cisco SFP-10G-LR	
1000BASE-SX SFP	http://www.cisco.com/en/US/prod/collateral/modules/ps5455/ps6577/product_data_sheet0900aecd8033f885.html
1000BASE-LX/LH SFP	
1000BASE-T SFP	

Before you begin

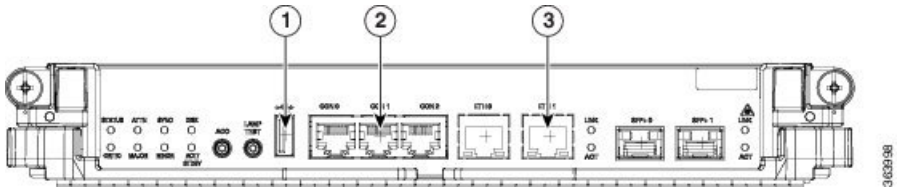
Configure the management port. See Configure the XR VM Management Port, on page 2.

Procedure

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.

Note
RJ-45 port is disabled by default. Do not use the RJ-45 port. Use only the 1G copper SFP port as showm in the image below.



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

Step 2 Depending on the SFP module type, connect either a 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 2.

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.

Note Telnet supports a maximum of 100 (including both IPv4 and IPv6) sessions.

For a SSH connection, the *ncs4k-k9sec* package must be installed on the router. For details about package installation, see the Install Packages section.

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 8.

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

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0:hostname# configure`	Enters XR Config mode.
Step 2	**hostname** *hostname* **Example:**	Configures a hostname for your Network Convergence System (NCS) 4016 system.

	Command or Action	Purpose
	`RP/0/RP0:hostname(config)# hostname system1`	
Step 3	**domain name** *domain-name* **Example:** `RP/0/RP0:hostname(config)# domain name cisco.com`	Defines a default domain name that the software uses to complete unqualified host names.
Step 4	**commit**	Saves the configuration changes and remains within the configuration session.

Step 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`	

Step 6	**configure** **Example:** `RP/0/RP0:hostname# configure`	Enters XR Config mode.
Step 7	**ssh timeout** *seconds* **Example:**	(Optional) Configures the timeout value for user authentication to AAA.

	Command or Action	Purpose
	`RP/0/RP0:hostname(config)# ssh timeout 60`	• If the user fails to authenticate itself to AAA within the configured time, the connection is cancelled. • If no value is configured, the default value of 30 seconds is used. The range is from 5 to 120.

Step 8	Do one of the following:
	• **ssh server** [**vrf** *vrf-name*]
	• **ssh server v2**
	Example:
	`RP/0/RP0:hostname(config)# ssh`
	or
	`RP/0/RP0:hostname(config)# ssh server v2`
		• (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.
		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.
		Note
		The SSH server can be configured for multiple VRF usage.
		• (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.

Step 9	**commit**	Saves the configuration changes and remains within the configuration session.
Step 10	**show ssh** **Example:** `RP/0/RP0:hostname# show ssh`	(Optional) Displays all of the incoming and outgoing SSHv1 and SSHv2 connections to the system.
Step 11	**show ssh session details** **Example:** `RP/0/RP0:hostname# show ssh session details`	(Optional) Displays a detailed report of the SSHv2 connections to and from the system.

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 5

Before you begin

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

SUMMARY STEPS

1. **configure**
2. **vty-pool default** *value* **line-template vty**
3. **telnet** *IPv4 address*
4. **telnet vrf default ipv4 server max-servers** *number*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0:hostname# configure`	Enters XR Config mode.
Step 2	**vty-pool default** *value* **line-template vty** **Example:** `RP/0/RP0:hostname(config)# vty-pool default 0 99 line-template vty`	Configures the VTY lines to control inbound telnet connections.
Step 3	**telnet** *IPv4 address* **Example:** `RP/0/RP0:hostname(config)# telnet 10.0.0.1`	Enables the Telnet server. The default is disabled.
Step 4	**telnet vrf default ipv4 server max-servers** *number* **Example:** `RP/0/RP0:hostname(config)# telnet vrf default ipv4 server max-servers 5`	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.

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

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0:hostname# configure`	Enters XR Config mode.
Step 2	**xml agent tty** **Example:** `RP/0/RP0:hostname(config)#xml agent tty`	The agent receives XML requests from external clients and returns XML responses.

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. **http server**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0:hostname# configure`	Enters XR Config mode.

Step 2	**http server**
	Example:
	`RP/0/RP0:hostname(config)#http server`
	`RP/0/RP0:hostname(config)#http server ssl`
		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.