



## Bring-up the Router

---

After installing the hardware, boot the router. Connect to the XR console port and power on the router. The router completes the boot process using the pre-installed operating system (OS) image. If no image is available within the router, the router can be booted using iPXE boot or an external bootable USB drive.

After booting is complete, create the root username and password, and then use it to log on to the XR console and get the router prompt. The first user created in XR console is synchronized to the System Admin console. From the XR console, access the System Admin console to configure system administration settings.

- [Boot the Router, on page 1](#)
- [Boot using USB Drive, on page 2](#)
- [Setup Root User Credentials, on page 3](#)
- [Access the System Admin Console, on page 5](#)
- [Configure the Management Port, on page 6](#)
- [Perform Clock Synchronization with NTP Server, on page 8](#)

## Boot the Router

Use the console port on the Route Processor (RP) to connect to a new router. The console port connect to the XR console by default. If required, subsequent connections can be established through the management port, after it is configured.

---

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

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

For NCS5001 and 5002 systems, the baud rate is 115200 bps, no parity, 2 stop bits and 8 data bits. For NCS5011 system, the console settings are baud rate 9600 bps, no parity, 2 stop bits and 8 data bits.

**Step 3** Power on the router.

Connect the power chord to Power Entry Module (PEM) and the router boots up. The boot process details is displayed on the console screen of the terminal emulation program.

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

The boot process is complete when the system prompts to enter the root-system username. If the prompt does not appear, wait for a while to give the router 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 router is corrupt. In this case, the router can be booted using an external bootable USB drive.

---

#### What to do next

Specify the root username and password.

## Boot using 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 using a compressed boot file.

### 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.



---

**Note** In case of failure to read or boot from USB drive, ensure that the drive is inserted correctly. If the drive is inserted correctly and still fails to read from USB drive, check the contents of the USB on another system.

---

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 8GB (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](http://cisco.com) to your local machine. The file name for the compressed boot file is in the format `ncs5k-usb-boot-<release_number>.zip`.

- 
- Step 1** Connect the USB drive to your local machine and format it with FAT32 or MS-DOS file system using the Windows Operating System or Apple MAC Disk Utility.
- Step 2** Copy the compressed boot file to the USB drive.
- Step 3** Verify that the copy operation is successful. To verify, compare the file size at source and destination. Additionally, verify the MD5 checksum value.
- Step 4** Extract the content of the compressed boot file by unzipping it inside the USB drive. This converts the USB drive to a bootable drive.

**Note** The content of the zipped file ("EFI" and "boot" directories) should be extracted directly into root of the USB drive. If the unzipping application places the extracted files in a new folder, move the "EFI" and "boot" directories to root of the USB drive.

**Step 5** Eject the USB drive from your local machine.

---

#### What to do next

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

## 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. A boot failure may happen when the image gets corrupted. During the USB boot, process the router gets re-imaged with the version available on the USB drive.



**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.

---

#### Before you begin

- Create a bootable USB drive. See [Create a Bootable USB Drive Using Compressed Boot File, on page 2](#).
  - Ensure that an external connection unit (ECU) with two solid-state drives (SSDs) is present.
- 

- Step 1** Connect the USB drive to the active RP.
- Step 2** Connect to the console
- Step 3** Power the router.
- Step 4** Press **Esc** to pause the boot process and get the RPs to BIOS menu.
- Step 5** Select the USB from the boot menu on the RP to which the USB is connected to.
- The image is copied in internal disk, and the router is restarted automatically.
- 

#### What to do next

- After the booting process is complete, specify the root username and password.
- Install the required optional packages.

## Setup Root User Credentials

When the router boots for the first time, the system prompts the user to configure root credentials (username and password). These credentials are configured as the root user on the XR (root-lr) console, the System Admin LXC (root-system), and as disaster-recovery credentials.

### Before you begin

The boot process must be complete. For details on how to initiate the boot process, see [Bring-up the Router, on page 1](#).

## SUMMARY STEPS

1. **Enter root-system username:** *username*
2. **Enter secret:** *password*
3. **Enter secret again:** *password*
4. **Username:** *username*
5. **Password:** *password*
6. (Optional) **show run username**

## DETAILED STEPS

---

### Step 1 Enter root-system username: *username*

Enter the username of the root user. The character limit is 1023. In this example, the name of the root user is "root".

**Important** The specified username is mapped to the "root-lr" group on the XR console. It is also mapped as the "root-system" user on the System Admin console.

When starting the router for the first time, or after a re-image, the router does not have any user configuration. In such cases, the router prompts you to specify the "root-system username". However, if the router has been configured previously, the router prompts you to enter the "username", as described in Step 4.

### Step 2 Enter secret: *password*

Enter the password for the root user. The character limit is 253. The password you type is not displayed on the CLI for security reasons.

The root username and password must be safeguarded as it has the superuser privileges. It is used to access the complete router configuration.

### Step 3 Enter secret again: *password*

Re-enter the password for the root user. The password is not accepted if it does not match the password entered in the previous step. The password you type is not displayed on the CLI for security reasons.

### Step 4 Username: *username*

Enter the root-system username to login to the XR LXC console.

### Step 5 Password: *password*

Enter the password of the root user. The correct password displays the router prompt. You are now logged into the XR LXC console.

### Step 6 (Optional) show run username

Displays user details.

```
username root
group root-lr
```

```
group cisco-support
secret 5 $1$NBg7$fHs1inKPZVvzqxMv775UE/
!
```

### Example



**Note** The NCS 5000 Routers running IOS-XR 64-bit OS can operate as a standalone device, ZTP controlled device or as an nV satellite.

When the router ships from the factory, the mode in which the router needs to operate is not predefined. Therefore, the software scans for a few events based on the usage, post-rack mounting, and power up, before deciding on the mode of operation. Now, there is a time window when the software is making this decision. During this duration, the router intended to operate in standalone or ZTP modes, could be compromised to fall into the nV satellite mode. Thereby, opening up privileged control of the router to a hostile external entity.

Ensure that the external entity has access to the same network as the auto-play ports (highest 10G and lowest 100G ports) in order to gain control as stated above. Once compromised, the router could become inaccessible to legitimate users but can be recovered by physical disconnection to the network and reset to factory defaults.

For deployments within insecure or public networks, it is strongly recommended to explicitly change the operating mode of NCS 5000 Router to the standalone mode through a utility option (using the “set sdac system-mode standalone” command in Exec mode). This will be a one-time staging step for the first boot after unboxing, or after factory reset of the router before it is connected to an insecure network. Especially, if the links connecting to the NCS 5000 Router on the lowest 100G and the highest 10G ports are not known to be secure.

### What to do next

- Configure routing functions from the XR console.
- Configure system administration settings from the System Admin prompt. The System Admin prompt is displayed on accessing the System Admin console. For details on how to get the System Admin prompt, see [Access the System Admin Console, on page 5](#).

## Access the System Admin Console

You must login to the System Admin console through the XR console to perform all system administration and hardware management setups.

### SUMMARY STEPS

1. Login to the XR console as the root user.
2. (Optional) Disable the login banner on console port when accessing the System Admin mode from XR mode.

3. **admin**
4. (Optional) **exit**

## DETAILED STEPS

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

**Step 2** (Optional) Disable the login banner on console port when accessing the System Admin mode from XR mode.

- a) **configure**
- b) **service sysadmin-login-banner disable**

**Example:**

```
RP/0/RP0/CPU0:router(config)#service sysadmin-login-banner disable
```

Disable the login banner on console port in System Admin mode.

- c) **commit**
- d) **end**

**Step 3** **admin**

**Example:**

The login banner is enabled by default. The following example shows the command output with the login banner enabled:

```
RP/0/RP0/CPU0:router#admin
Mon May 22 06:57:29.350 UTC
root connected from 127.0.0.1 using console on host
sysadmin-vm:0_RP0# exit
Mon May 22 06:57:32.360 UTC
```

The following example shows the command output with the login banner disabled:

```
RP/0/RP0/CPU0:router#admin
Thu Mar 01:07:14.509 UTC
sysadmin-vm:0_RP0# exit
```

**Step 4** (Optional) **exit**

Return to the XR mode from the System Admin mode.

## Configure the Management Port

To use the 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), you need to configure a default (static) route for the router.

### 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 and Ethernet 1 on RP are the management ports. Ensure that the port is connected to management network.

## SUMMARY STEPS

1. **configure**
2. **interface MgmtEth** *rack/slot/port*
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** *0.0.0.0/0 default-gateway*
8. **commit**

## DETAILED STEPS

**Step 1**     **configure**

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

**Example:**

```
RP/0/RP0/CPU0:router(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/CPU0:router(config-if)#ipv4 address 10.1.1.1/8
```

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

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

**Example:**

```
RP/0/RP0/CPU0:router(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/CPU0:router(config-if)#no shutdown
```

Places the interface in an "up" state.

**Step 6**     **exit**

**Example:**

```
RP/0/RP0/CPU0:router(config-if)#exit
```

Exits the Management interface configuration mode.

**Step 7**     **router static address-family ipv4 unicast** *0.0.0.0/0 default-gateway*

**Example:**

```
RP/0/RP0/CPU0:router(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. With a terminal emulation program, establish a SSH or telnet connection to the management interface port using its IP address. 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.

## Perform Clock Synchronization with NTP Server

There are independent system clocks for the XR console and the System Admin console. To ensure that these clocks do not deviate from true time, they need to be synchronized with the clock of a NTP server. In this task you will configure a NTP server for the XR console. After the XR console clock is synchronized, the System Admin console clock will automatically synchronize with the XR console clock.

**Before you begin**

Configure and connect to the management port.

**SUMMARY STEPS**

1. **configure**
2. **ntp server** *server\_address*

**DETAILED STEPS**

**Step 1**    **configure**

**Step 2**    **ntp server** *server\_address*

**Example:**

```
RP/0/RP0/CPU0:router#ntp server 64.90.182.55
```

The XR console clock is configured to be synchronized with the specified sever.