Setup Cisco NCS 5700 Series Routers with XR7 OS

The Cisco Network Convergence System 5700 Series builds on the Cisco NCS 5500 fixed systems by combining the forwarding ASIC design with the Cisco IOS XR7 OS. The Cisco NCS 5700 series chassis is a standalone 1RU router that offers aggregation, distributed core and peering fabric, and 100G Top of Rack (ToR).

The following variants of Cisco NCS 5700 series router run on XR7 OS:

- NCS-57B1-6D24-SYS
- NCS-57B1-5DSE-SYS

XR7 OS provides significant architectural enhancements to Cisco IOS XR in these areas:

- **Modularity:** Decoupled hardware and software; disintegrated software with the flexibility to consume software packages based on requirement
- **Programmability:** Cloud scale enhancement with model-drivel APIs at all layers
- **Manageability:** Simplified software management and installation that is based on Linux tools

This document helps you set up the Cisco NCS 5700 series routers with XR7 OS. You will bring-up the router, run a health check of the system, create user profiles, and assign privileges.

- Bring-up the Router, on page 1
- Perform Preliminary Checks with Router, on page 7
- Create Users and Assign Privileges on the Router, on page 13

Bring-up the Router

Connect to the console port of the router, and power ON the router. By default, this console port connects to the XR console. If necessary, after configuration, establish subsequent connections through the management port.

The following table shows the console settings:

Table 1: Console Settings

Baud rate (in bps)	Parity	Stop bits	Data bits
115200	None	2	8

The baud rate is set by default and cannot be changed.

The router can be accessed using remote management protocols, such as SSH, Telnet, SCP and FTP. SSH is included in the software image by default, but telnet is not part of the software image. You must manually install the telnet optional package to use it.

After booting is complete, you must create a username and password. This credential is used to log on to the XR console, and get to the router prompt.

You can start or stop the console by using the following keyboard shortcuts:

- To start the console, press Ctrl + q.
- To stop the console, press Ctrl + s.

Note that by using Ctrl + s, the console output will be locked and you will need to initiate a Ctrl + q sequence to restore the console prompt.

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.

Boot the Router Using Manual iPXE

Manually boot the router using iPXE if the router fails to boot when powered ON. An alternate method is to Boot the Router Using USB Drive.

iPXE is a pre-boot execution environment in the network card of the management interfaces. It works at the system firmware (UEFI) level of the router. iPXE boot re-images the system, boots the router in case of a boot failure, or in the absence of a valid bootable partition. iPXE downloads the ISO image, installs the image, and finally bootstraps inside the new installation.

iPXE acts as a bootloader. It provides the flexibility to choose the image that the system boots. The image is based on the Platform Identifier (PID), the serial number, or the management mac-address. iPXE is defined in the DHCP server configuration file.

You need a server running HTTPS, HTTP, or TFTP. Bring-up the PXE prompt using the following steps:

Step 1 Power ON the router.

Step 2 Press Esc or Del keys continuously (quick and repeated press and release) to pause the boot process, and get to the BIOS menu.

Step 3 Select `Boot Manager`, and then select `Built-in iPXE` option.

Step 4 When PXE boot starts reaching for a PXE server, press **Ctrl+B** keys to break into the PXE prompt.

Step 5 Add the following configuration for the router. This is required for the router to connect with the external server to download, and install the image. You can use HTTP, HTTPS or TFTP server.

Example:

```
iPXE> ifopen net0                    #Open the interface connecting outside world
```

```
iPXE> set net0/ip 10.0.0.2           #Configure the ip address of your router

iPXE> set net0/gateway 10.0.0.1      #configure the GW
iPXE> set net0/netmask 255.0.0.0     #Configure the Netmask
iPXE> ping 10.0.0.1                  #Check you can reach GW
iPXE> ping 192.0.2.0                 #check you can reach to your server running tftp or http or
https
iPXE> boot http://192.0.2.0/<directory-path>5700-x64.iso    #Copy the image on the http/https/tftp
server in any path and then point to download the image from there.
```

Note To rectify errors while typing the command, use **Ctrl+H** keys to delete a character.

If a PXE server is configured to run a DHCP server, it assigns an IP address to the Ethernet Management interface of the router. This provides a channel to download the image that is required to re-image a router in case of a boot failure.

```
Router#reload bootmedia network location all
Proceed with reload? [confirm]
```

Note Use the **force** option to perform an ungraceful reload of the specified location or hardware module. When **force** option is used along with the **all** location, the chassis undergoes an ungraceful reload. Use the **noprompt** option to avoid the prompt to confirm the operation. The **force** option is not recommended, and should not be used during regular operations.

Boot the Router Using USB Drive

Boot the router using USB drive if the router fails to boot when powered ON. An alternate method is to Boot the Router Using Manual iPXE.

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.

Note Use this procedure only on the active RP; the standby RP must either be powered OFF or removed from the chassis. After the active RP is installed with images from the USB drive, insert or power ON the standby RP as appropriate.

Step 1 Copy the bootable file to a USB disk.

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 If you are unable to boot from a USB drive, remove and insert the drive again. If the drive is inserted correctly, and still fails to read from the 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.

a) 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. To check if the disk is formatted as FAT32, right click on the USB disk, and view the properties.
b) Copy the compressed boot file in .zip format from the image file to the USB drive. This .zip file can be downloaded from the Cisco Software Download center.
c) Verify that the copy operation is successful. To verify, compare the file size at source and destination. Additionally, verify the MD5 checksum value.
d) Extract the contents of the compressed boot file by unzipping it inside the USB drive. This converts the USB drive to a bootable drive.

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

e) Eject the USB drive from your local machine.

Step 2 Use the bootable USB drive to boot the router or upgrade its image using one of the following methods:

- **Boot menu**

  a. Insert the USB drive, and connect to the console.

  b. Power ON the router.

  c. Press Esc or Del to pause the boot process, and get to the BIOS menu.

  d. Select `Boot Manager`, and then select the `USB` option from the boot menu.

```
Cisco BIOS Setup Utility - Copyright (C) 2019 Cisco Systems, Inc

Boot Override
UEFI: Micron_M600_MTFDDAT064MBF, Partition 4
UEFI: Built-in iPXE
URFI: Built-in Shell
URFI: Built-in Grub
UEFI: USB Flash Memory1.00, Partition 1
```

  The system boots the image from the USB drive, and installs the image onto the hard disk. The router boots from the hard disk after installation.

- **XR CLI**

  Use this method if you can access the XR prompt.

  a. Insert the USB device in the RP.

  b. Access the XR prompt and run the command:

```
Router#reload bootmedia usb noprompt

Welcome to GRUB!!
Verifying (hd0,msdos1)/EFI/BOOT/grub.cfg...
(hd0,msdos1)/EFI/BOOT/grub.cfg verified using Pkcs7 signature.
Loading Kernel..
Verifying (loop)/boot/bzImage...
(loop)/boot/bzImage verified using attached signature.
Loading initrd..
Verifying (loop)/boot/initrd.img
```

  Use the **force** option to perform an ungraceful reload of the specified location or hardware module. When **force** option is used along with the **all** location, the chassis undergoes an ungraceful reload. Use the **noprompt** option

to avoid the prompt to confirm the operation. The **force** option is not recommended, and should not be used during regular operations.

The system boots the image from the USB and installs the image onto the hard disk. The router boots from the hard disk after installation.

Note Execute the `install commit` command before proceeding to the next install iteration, while performing cyclic upgrade and downgrade tests.

Configure the Management Port on the Router

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.

Note We recommend that you use a Virtual Private Network (VPN) routing and the forwarding (VRF) on the Management Ethernet interface.

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 the management network.

Step 1 Configure a VRF.

Example:

```
Router#conf t
Router(config)#vrf <vrf-name>
Router(config-vrf)#exit
```

Step 2 Enter interface configuration mode for the management interface of the RP.

Example:

```
Router(config)#interface mgmtEth 0/RP0/CPU0/0
```

Step 3 Assign an IP address and a subnet mask to the interface.

Example:

```
Router(config-if)#ipv4 address 10.10.10.1/8
```

Step 4 Configure the Management Ethernet interface under the VRF.

Example:

```
Router(config-if)#vrf <vrf-name>
```

Step 5 Exit the management interface configuration mode.

Example:

```
Router(config-if)#exit
```

Step 6 Place the interface in `UP` state.

Example:

```
Router(config)#no shutdown
```

Step 7 Specify the IP address of the default-gateway to configure a static route; this is used for communications with devices on other networks.

Example:

```
Router(config)#router static vrf <vrf-name> address-family ipv4 unicast 0.0.0.0/0 10.10.10.1
```

Step 8 Commit the configuration.

Example:

```
Router(config)#commit
```

Step 9 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.

Synchronize Router Clock with NTP Server

Synchronize the XR clock with that of an NTP server to avoid a deviation from true time.

NTP uses the concept of a `stratum` to describe how many NTP hops away a machine is from an authoritative time source. A `stratum 1` time server typically has an authoritative time source (such as a radio or atomic clock, or a GPS time source) directly attached to the server. A `stratum 2` time server receives its time through NTP from a `stratum 1` time server, and so on.

Note The Cisco implementation of NTP does not support stratum 1 service.

Before you begin

Configure and connect to the management port.

Step 1 Enter the XR configuration mode.

Example:

```
Router#configure
```

Step 2 Synchronize the console clock with the specified sever.

Example:

```
Router(config)#ntp server <NTP-source-IP-address>
```

The NTP source IP address can either be an IPv4 or an IPv6 address. For example:

IPv4:

```
Router(config)#ntp server 192.0.2.0
```

IPv6:

```
Router(config)#ntp server 2001:DB8::1
```

Note The NTP server can also be reachable through a VRF if the Management Ethernet interface is in a VRF.

Step 3 Commit the configuration.

Example:

```
Router(config-ntp)#commit
```

Step 4 Verify that the clock is synchronised with the NTP server.

Example:

```
Router#show ntp status
Clock is synchronized, stratum 3, reference is 192.0.2.0
nominal freq is 1000000000.0000 Hz, actual freq is 1000000000.0000 Hz, precision is 2**24
reference time is E12B1B02.8BB13A2F (08:42:42.545 UTC Tue Sep 17 2019)
clock offset is -3.194 msec, root delay is 4.949 msec
root dispersion is 105.85 msec, peer dispersion is 2.84 msec
loopfilter state is 'FREQ' (Drift being measured), drift is 0.0000000000 s/s
system poll interval is 64, last update was 124 sec ago
authenticate is disabled
```

Perform Preliminary Checks with Router

After successfully logging into the console, you must perform some preliminary checks to verify the correctness of the default setup. Correct any issues that arise before proceeding with further configurations.

Verify Software Version on Router

The router 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. Installing the newer version of the software provides the latest feature set on the router.

You can view the overview of the running software. This includes the following information:

- Image name and version
- User who built the image
- Time the image was built
- Build workspace
- Build host
- ISO label

Note If any modifications are made to the running software on the booted ISO, only the IOS XR version is displayed in the label field and not the label included in the ISO.

- Copyright information
- Hardware information

Display the version of the Cisco IOS XR software, and its various software components that are installed on the router.

NCS 5700 Series Routers:

```
Router#show version
Cisco IOS XR Software, Version 7.3.1 LNT
Copyright (c) 2013-2022 by Cisco Systems, Inc.
Build Information:
Built By :   xyz
Built On :   Tue June 07 19:43:44 UTC 2021
Build Host : iox-lnx-064
Workspace :  ../ncs5700/ws
Version :    7.3.1
Label :      7.3.1
cisco NCS-57B1-5DSE-SYS (D-1563N @ 2.00GHz) processor with 32GB of memory
NCS5700 uptime is 3 weeks, 1 day, 10 hours, 11 minutes
NCS5700 Fixed Scale HW Flexible Consumption Need Smart Lic
```

Verify Status of Hardware Modules on Router

Hardware modules such as fan trays, and power modules are installed on the router. The firmware on various hardware components of the router must be compatible with the Cisco IOS XR image installed. Incompatibility may cause the router to malfunction. Verify that all hardware and firmware modules are installed correctly and are operational.

Before you begin

Ensure that all required hardware modules are installed on the router.

Step 1 View the status of the system.

Example:

NCS 5700 Series Routers:

```
Router#show platform
Node              Type                        State                    Config state
--------------------------------------------------------------------------------

0/RP0/CPU0        NCS-57B1-5DSE-SYS(Active) IOS XR RUN               NSHUT

0/PM0             PSU2KW-ACPI               OPERATIONAL              NSHUT

0/PM1             PSU2KW-ACPI               OPERATIONAL              NSHUT

0/FT0             N5700-FAN                 OPERATIONAL              NSHUT
```

```
0/FT1             N5700-FAN                OPERATIONAL             NSHUT

0/FT2             N5700-FAN                OPERATIONAL             NSHUT

0/FT3             N5700-FAN                OPERATIONAL             NSHUT

0/FT4             N5700-FAN                OPERATIONAL             NSHUT

0/FT5             N5700-FAN                OPERATIONAL             NSHUT
```

Step 2 View the list of hardware and firmware modules detected on the router.

Example:

NCS 5700 Series Routers:

```
Router#show hw-module fpd
Auto-upgrade:Enabled
Attribute codes: B golden, P protect, S secure
                   FPD Versions
                                                    ================
Location   Card type             HWver FPD device       ATR Status   Running Programd  Reload Loc
-------------------------------------------------------------------------------------------------
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   IoFpga               CURRENT    0.08    0.08          0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   IoFPgaGolden     B   CURRENT            0.02          0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   Primary-BIOS      S  CURRENT    1.10    1.10          0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   StdbyFpga         S  CURRENT    0.24    0.24          0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   StdbyFpgaGolden  BS  NEED UPGD          0.00          0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   TamFw             S  CURRENT    6.05    6.05          0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   TamFwGolden      BS  NEED UPGD          0.00          0/RP0
0/PM0      PSU2KW-ACPI           0.0   PO-PrimMCU           CURRENT    1.08    1.08       NOT REQ
0/PM1      PSU2KW-ACPI           0.0   PO-PrimMCU           CURRENT   17.56   17.56       NOT REQ
```

From the result, verify that all hardware modules that are installed on the chassis are listed. If a module is not listed, it indicates that the module is malfunctioning, or is not installed properly. Remove and reinstall that hardware module.

In the preceding output, some of the significant fields are:

- FPD Device—Name of the hardware component, such as IO FPGA, IM FPGA, or BIOS

  Note Golden FPDs are not field upgradable.

- Status—Upgrade status of the firmware. The different states are:

Status	Description
CURRENT	The firmware version is the latest version.
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. We recommend that you to perform an upgrade of the firmware version.
RLOAD REQ	The upgrade is complete, and the ISO image requires a reload.
UPGD DONE	The firmware upgrade is successful.

Status	Description
UPGD FAIL	The firmware upgrade has failed.
UPGD PREP	The FPD firmware is preparing for upgrade.
BACK IMG	The firmware is corrupt. Reinstall the firmware.
UPGD SKIP	The upgrade is skipped because the installed firmware version is higher than the one available in the image.

- Running—Current version of the firmware running on the FPD
- Programd—Version of the FPD programmed on the module

Step 3 If necessary, upgrade the required firmware.

Example:

```
Router#upgrade hw-module location all fpd all
```

Alarms are created showing all modules that needs to be upgraded.

```
Active Alarms
------------------------------------------------------------------------------------------------------------------
Location      Severity     Group        Set Time                    Description
------------------------------------------------------------------------------------------------------------------

0/6/CPU0       Major       FPD_Infra    09/16/2019 12:34:59 UTC     One Or More FPDs Need Upgrade Or
 Not In Current State
0/10/CPU0      Major       FPD_Infra    09/16/2019 12:34:59 UTC     One Or More FPDs Need Upgrade Or
 Not In Current State
0/RP0/CPU0     Major       FPD_Infra    09/16/2019 12:34:59 UTC     One Or More FPDs Need Upgrade Or
 Not In Current State
0/RP1/CPU0     Major       FPD_Infra    09/16/2019 12:34:59 UTC     One Or More FPDs Need Upgrade Or
 Not In Current State
0/FC0          Major       FPD_Infra    09/16/2019 12:34:59 UTC     One Or More FPDs Need Upgrade Or
 Not In Current State
0/FC1          Major       FPD_Infra    09/16/2019 12:34:59 UTC     One Or More FPDs Need Upgrade Or
 Not In Current State
```

Note BIOS and IOFPGA upgrades require a power cycle of the router for the new version to take effect.

Step 4 After the modules are upgraded verify the status of the modules.

Example:

NCS 5700 Series Routers:

```
Router#show hw-module fpd
Auto-upgrade:Enabled
Attribute codes: B golden, P protect, S secure
                   FPD Versions
                                                  =================
Location   Card type             HWver FPD device       ATR Status   Running Programd  Reload Loc
-------------------------------------------------------------------------------------------------
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   IoFpga               CURRENT    0.08    0.08         0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   IoFPgaGolden     B   CURRENT    0.02                 0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   Primary-BIOS      S  CURRENT    1.10    1.10         0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   StdbyFpga         S  CURRENT    0.24    0.24         0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   StdbyFpgaGolden  BS  CURRENT            0.00         0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   TamFw             S  CURRENT    6.05    6.05         0/RP0
```

```
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   TamFwGolden      BS  RLOAD REQ  0.00    0.01         0/RP0
0/PM0      PSU2KW-ACPI           0.0   PO-PrimMCU           CURRENT    1.08    1.08       NOT REQ
0/PM1      PSU2KW-ACPI           0.0   PO-PrimMCU           CURRENT   17.56   17.56       NOT REQ
```

The status of the upgraded nodes show that a reload is required.

Step 5 Reload the individual nodes that required an upgrade.

Example:

```
Router#reload location <node-location>
```

Step 6 Verify that all nodes that required an upgrade show an updated status of CURRENT with an updated FPD version.

Example:

NCS 5700 Series Routers:

```
Router#show hw-module fpd
Auto-upgrade:Enabled
Attribute codes: B golden, P protect, S secure
                   FPD Versions
                                                    ================
Location   Card type             HWver FPD device       ATR Status   Running Programd  Reload Loc
-------------------------------------------------------------------------------------------------
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   IoFpga               CURRENT    0.08    0.08         0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   IoFPgaGolden     B   CURRENT    0.02                 0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   Primary-BIOS      S  CURRENT    1.10    1.10         0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   StdbyFpga         S  CURRENT    0.24    0.24         0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   StdbyFpgaGolden  BS  CURRENT    0.00    0.01         0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   TamFw             S  CURRENT    6.05    6.05         0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   TamFwGolden      BS  CURRENT    0.00    0.01         0/RP0
0/PM0      PSU2KW-ACPI           0.0   PO-PrimMCU           CURRENT    1.08    1.08       NOT REQ
0/PM1      PSU2KW-ACPI           0.0   PO-PrimMCU           CURRENT   17.56   17.56       NOT REQ
```

Verify Interface Status on the Router

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.

View the interfaces discovered by the system.

Example:

```
Router#show ipv4 interfaces brief
Interface                      IP-Address      Status          Protocol Vrf-Name
-------------------------------------------------------------------------------HundredGigE0/0/0/0
             unassigned      Shutdown        Down     default
HundredGigE0/0/0/1             unassigned      Shutdown        Down     default
HundredGigE0/0/0/2             unassigned      Shutdown        Down     default
HundredGigE0/0/0/3             unassigned      Shutdown        Down     default
HundredGigE0/0/0/4             unassigned      Shutdown        Down     default
HundredGigE0/0/0/5             unassigned      Shutdown        Down     default
HundredGigE0/0/0/6             unassigned      Shutdown        Down     default
HundredGigE0/0/0/7             unassigned      Shutdown        Down     default
------------------------ <snip> --------------------------------TenGigE0/0/0/18/0
unassigned      Up              Up       default
TenGigE0/0/0/18/1              unassigned      Up              Up       default
TenGigE0/0/0/18/2              unassigned      Up              Up       default
```

```
TenGigE0/0/0/18/3              unassigned      Up             Up       default
MgmtEth0/RP0/CPU0/0            10.10.10.1      Up             Up       default
```

When a router is turned ON for the first time, all interfaces are in the `unassigned` state. Verify that the total number of interfaces displayed in the result matches with the actual number of interfaces present on the router.

Verify Node Status on Router

Each card on the router represents a node.

Verify the operational status of the node.

Example:

NCS 5700 Series Routers:

```
Router#show platform
Node              Type                         State                    Config state
--------------------------------------------------------------------------------

0/RP0/CPU0        NCS-57B1-5DSE-SYS(Active) IOS XR RUN               NSHUT

0/PM0             PSU2KW-ACPI               OPERATIONAL              NSHUT

0/PM1             PSU2KW-ACPI               OPERATIONAL              NSHUT

0/FT0             N5700-FAN                 OPERATIONAL              NSHUT

0/FT1             N5700-FAN                 OPERATIONAL              NSHUT

0/FT2             N5700-FAN                 OPERATIONAL              NSHUT

0/FT3             N5700-FAN                 OPERATIONAL              NSHUT

0/FT4             N5700-FAN                 OPERATIONAL              NSHUT

0/FT5             N5700-FAN                 OPERATIONAL              NSHUT
```

Displays the status of nodes present in the chassis.

Verify that the software state and the hardware state of FTs, and power modules are listed, and their state is `OPERATIONAL`. This indicates that the XR console is operational on the cards.

The platform states are described in the following table:

Card Type	State	Description
All	UNKNOWN	Error – Internal card record is not available
All	IDLE	Error – Card state is not initialized
All	DISCOVERED	Card is detected
All	POWERED_ON	Card is powered on

Card Type	State	Description
FC, FT, PT, PM	OPERATIONAL	Card is operating normally and is functional

Create Users and Assign Privileges on the Router

Users are authenticated using a username and a password. The authentication, authorization, and accounting (AAA) commands help with these services:

- create users, groups, command rules, or data rules
- change the disaster-recovery password

XR has its AAA separate from Linux. XR AAA is the primary AAA system. A user created through XR can log in directly to the EXEC prompt when connected to the router. A user created through Linux can connect to the router, but arrive at the bash prompt. The user must log in to XR explicitly in order to access the XR EXEC prompt.

Configure AAA authorization to restrict users from uncontrolled access. If AAA authorization is not configured, the command and data rules associated to the groups that are assigned to the user are bypassed. A user can have full read-write access to IOS XR configuration through Network Configuration Protocol (NETCONF), google-defined Remote Procedure Calls (gRPC), or any YANG-based agents. In order to avoid granting uncontrolled access, enable AAA authorization before setting up any configuration. To gain an understanding about AAA, and to explore the AAA services, see the *Configuring AAA Services* chapter in the *System Security Configuration Guide for Cisco NCS5500 Series Routers*.

Create a User Profile

Create new users and include the user in a user group with certain privileges. The router supports a maximum of 1024 user profiles.

In this task, you create a user, `user1`, password for this user, `pw123`, and assign the user to a group `root-lr`.

Step 1 Enter the XR configuration mode.

Example:

```
Router#config
```

Step 2 Create a new user.

Example:

```
Router(config)#username user1
```

Step 3 Create a password for the new user.

Example:

```
Router(config-un)#password pw123
```

Step 4 Assign the user to group `root-lr`.

Example:

```
Router(config-un)#group root-lr
```

All users have `read` privileges. However, users can be assigned to `root-lr` usergroup. These users inherit the `write` privileges where users can create configurations, create new users, and so on.

Step 5 Commit the configuration.

Example:

```
Router(config-un)#commit
```

What to do next

With the router set up, you can manage your system, install software packages, and configure your network.

Create a User Group

Create a new user group to associate command rules and data rules with it. The command rules and data rules are enforced on all users that are part of the user group.

The router supports a maximum of 32 user groups.

In this task, you create a group name, `group1`, and assign a user, `user1` to this group.

Before you begin

Create a user profile. See Create a User Profile, on page 13.

Step 1 Enter the XR configuration mode.

Example:

```
Router#config
```

Step 2 Create a new user group, `group1`.

Example:

```
Router#(config)#group group1
```

Step 3 Specify the name of the user, `user1` to assign to this user group.

Example:

```
Router#(config-GRP)#username user1
```

You can specify multiple user names enclosed withing double quotes. For example, users "*user1 user2* ...".

Step 4 Commit the configuration.

Example:

```
Router#commit
```

What to do next

With the router set up, you can manage your system, install software packages, and configure your network.