CHAPTER 3

Connecting to the Management Network and Securing Access

This chapter provides Cisco NX-OS recommended best practices for connecting a Cisco Nexus 7000 Series switch to the management network(s) and securing access to the CLI.

This chapter includes the following sections:

Out-of-Band Management Connectivity

A Nexus 7000 is typically managed using a combination of different connectivity methods that give the network administrator CLI access and the ability to manage the chassis using IP management protocols such as SNMP, Syslog and NTP. The following table illustrates the different connectivity methods available to manage a Nexus 7000 chassis. We recommend that you manage a chassis using a combination of out-of-band methods to separate the management traffic from the production traffic. This approach improves security by preventing Denial of Service (DoS) attacks originated from malicious users, or inadvertently by traffic over-subscription.

It is important to understand the functionality that the supervisor module CMP port provides. The CMP port provides lights-out CLI console access to the supervisor module over an IP network using SSHv2 or Telnet. The CMP port allows an administrator to attach to the console, monitor the console, reload the supervisor module or the entire chassis. It does not provide in-band management capabilities for IP protocols like SNMP or NTP.

Table 3-1 Connectivity Options for Port Types and Module Types

Connectivity Options	Port Type	Module Type
Out-of-band (RS-232 Serial CLI)	Console port (recommended)	Supervisor
	Auxiliary port	Supervisor

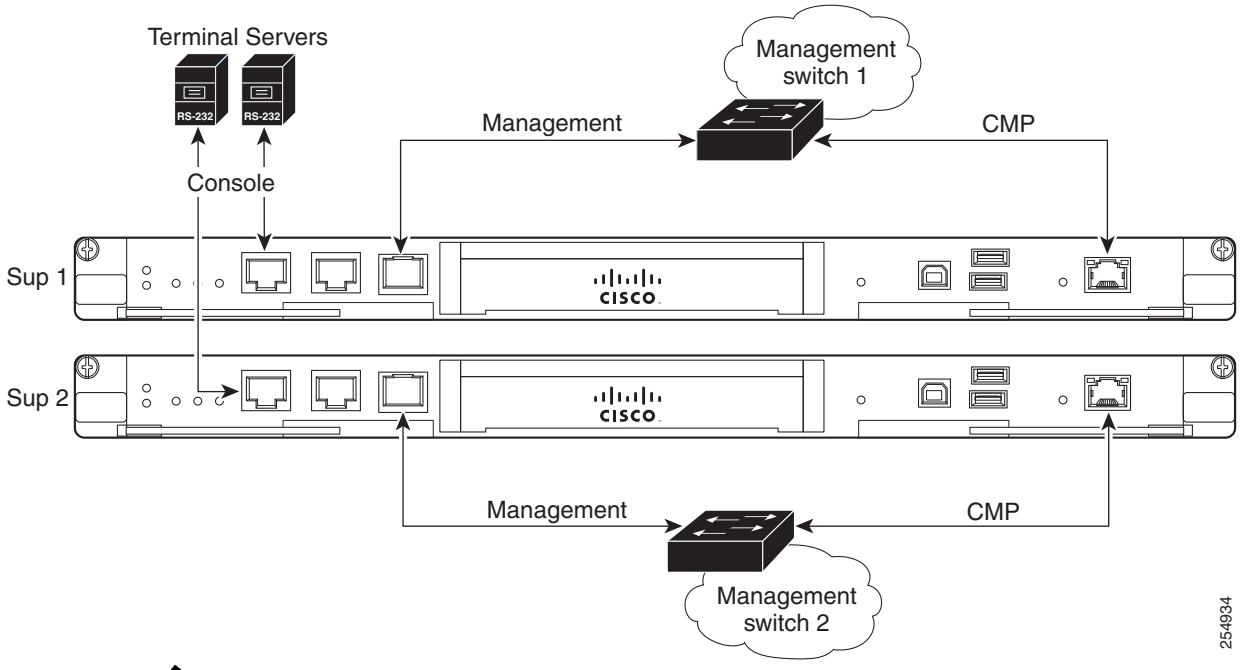
Table 3-1 Connectivity Options for Port Types and Module Types

Connectivity Options	Port Type	Module Type
Out-of-band (SSH/Telnet CLI)	Connectivity Management Port (CMP) recommended	Supervisor
Out-of-band (SSH/Telnet CLI and IP Mgmt)	Management port (mgmt0) recommended	Supervisor
In-band (SSH/Telnet CLI and IP Mgmt)	Ethernet/Loopback/SVI, etc.	I/O module

To reduce the likelihood for loosing connectivity to a Nexus 7000 with two supervisor modules, we recommend connecting the console port, CMP, and the management port per supervisor module.

The console ports should be connected to two different terminal servers and the supervisor CMP and mgmt0 ports should be connected to a redundant out-of-band Ethernet network to improve availability and security. The following diagram illustrates the connectivity required per chassis with redundant supervisor modules.

Figure 3-1 Connectivity per Chassis with Redundant Supervisor Modules



Note In this out-of-band management design, the CoPP policy should be modified to deny in-band management protocols if there are any IP addresses configured on I/O module ports such as Ethernet, loopbacks, port channels, SVIs, etc.

Note This is just a basic example. Redundant network management designs are beyond the scope of this document.

Console Port Configuration

This section contains Cisco NX-OS recommended best practices for the console port.

Exec-Timeout

Introduced: Cisco NX-OS Release 4.0(1)

The console port should be configured with a timeout to automatically log off administrators who are idle for a specified time period. The console **exec-timeout** is disabled by default. A ten or fifteen minute timeout is usually acceptable for most security policies.

```
n7000(config)# line console
n7000(config-console)# exec-timeout 10
```

Port Speed

Introduced: Cisco NX-OS Release 4.0(1)

The console port speed (baud rate) should be increased to the largest value supported by the connected terminal server. The console speed defaults to 9,600 bps and can be configured up to 115,200 bps. A larger value will improve the user experience by increasing the speed that data is displayed on the console port.

```
n7000(config)# line console
n7000(config-console)# speed 115200
```

VTY Port Configuration

This section contains Cisco NX-OS recommended best practices for the VTY (Terminal) port configuration used for SSHv2 and Telnet sessions.

Exec-Timeout

Introduced: Cisco NX-OS Release 4.0(1)

The VTY port should be configured with a timeout to automatically log off users that are idle for a specified time period. The VTY **exec-timeout** is disabled by default. A ten or fifteen minute timeout is usually acceptable for most security policies.

```
n7000(config)# line vty
n7000(config-line)# exec-timeout 10
```

Session Limit

Introduced: Cisco NX-OS Release 4.0(1)

The VTY session limit determines how many SSHv2 sessions, Telnet sessions, or both that can be active simultaneously. The session-limit defaults to 32 active sessions. This should be reduced to a more practical limit such as 5 or 10 sessions to improve security.

```
n7000(config)# line vty
n7000(config-line)# session-limit 5
```

Access-List

Introduced: Cisco NX-OS 5.1(1)

An access class should be applied to the VTY port to increase security by restricting SSH and Telnet access to specific source and destination IP addresses. An access class configured on the VTY port is applicable when using an in-band or out-of-band management strategy. An access-class is configured per traffic direction, **in** applies to inbound sessions and **out** applies to outbound sessions.

Statistics can be enabled with the access list **statistics per-entry**. The following example illustrates a basic policy that permits SSH traffic from a specific subnet to all IP addresses configured in the current VDC. All traffic is permitted if an access-class is applied to the VTY port and the associated access-list is deleted from the configuration.

```
n7000(config)# ip access-list vty-acl-in
n7000(config-acl)# permit tcp x.x.x.x/24 any eq 22

n7000(config)# line vty
n7000(config-line)# ip access-class vty-acl-in in
```

Supervisor Management Port Configuration

This section contains the Cisco NX-OS recommended best practices for the supervisor module mgmt0 port.

Access List

Introduced: Cisco NX-OS Release 4.0(1)

The supervisor module mgmt0 port should be configured with an inbound access list to increase security by restricting access to specific source host/subnet addresses destined to specific management protocols configured on the Nexus 7000. The access-list entries will vary depending on the management protocols that are enabled. Access-list statistics can be tracked per ACL entry if the ACL command **statistics per-entry** is configured. The supervisor module CPU performs access-list processing when an access-list is applied to the mgmt0 port.

```
n7000(config)# ip access-list mgmt0-access
n7000(config-acl)# statistics per-entry
n7000(config-acl)# permit tcp x.x.x.x/x b.b.b.b/32 eq 22
n7000(config-acl)# permit udp x.x.x.x/x b.b.b.b/32 eq snmp
n7000(config-acl)# permit tcp x.x.x.x/x b.b.b.b/32 eq tacacs
n7000(config-acl)# permit udp x.x.x.x/x b.b.b.b/32 eq ntp

n7000(config)# interface mgmt0
n7000(config-if)# ip access-group mgmt0-access in
n7000(config-if)# ip address b.b.b.b/xx
```

Access-List Logging

Introduced: Cisco NX-OS Release 5.0(2a)

Access lists can be configured on the mgmt0 port to collect additional data per entry using the **log** keyword. The access-list logging cache can be displayed to audit the data collected from the logged access-list entry.

```
n7000(config)# ip access-list mgmt0-access
n7000(config-acl)# permit tcp x.x.x.x/x b.b.b.b/32 eq 22 log

n7000# show log ip access-list cache
Source IP        Destination IP     S-Port  D-Port    Interface   Protocol          Hits
-------------------------------------------------------------------------------------
x.x.x.x          x.x.x.x             60741   22        mgmt0      (6)TCP            136


Number of cache entries: 1
-------------------------------------------------------------------------------------
```

Supervisor CMP Port Configuration

This section contains the Cisco NX-OS recommended best practices for configuring the supervisor module Connectivity Management Port (CMP).

Access List

Introduced: Cisco NX-OS Release 4.0(1)

The supervisor module CMP port should be configured with an access list to increase security by restricting access to specific source host/subnets addresses destined to specific management protocols enabled on the CMP port. SSHv2 is typically the only protocol required on the CMP port. Use the **attach cmp** command to configure the CMP port with an access-list.

```
n7000-cmp5(config)# ip access-list cmp-access
n7000-cmp5(config-acl)# permit tcp x.x.x.x 0.0.0.0 range 1024 65535 b.b.b.b 0.0.0.0 range 22 22

n7000-cmp5(config)# interface cmp-mgmt
n7000-cmp5(config-if)# ip address b.b.b.b/xx
n7000-cmp5(config-if)# ip access-group cmp-access in
```

Note The access-list syntax on the CMP port differs from the Cisco NX-OS access-list syntax.