CHAPTER 9

IP Management

This chapter provides Cisco NX-OS recommended best practices for configuring IP management protocols.

This chapter includes the following sections:

- Network Time Protocol (NTP)
- Simple Network Management Protocol (SNMP)
- System Message Logging
- Smart Call Home

Network Time Protocol (NTP)

We recommend configuring NTP on all network devices so that the timestamps in the logs and other management data are synchronized on all devices. Using NTP is beneficial when correlating network events across the network. Cisco NX-OS supports NTP client mode and peer mode operations.

Redundant NTP Servers

Introduced: Cisco NX-OS Release 4.0(1)

Multiple NTP servers should be configured for redundancy. The primary NTP server should be configured with the **prefer** option, and the VRF instance should be configured to use the management VRF instance for out-of-band connectivity.

```
n7000(config)# ntp server a.a.a.a prefer use-vrf management
n7000(config)# ntp server a.a.a.a use-vrf management

n7000(config)# ntp peer b.b.b.b prefer use-vrf management
n7000(config)# ntp peer b.b.b.b use-vrf management
```

Time zone / Daylight Savings

Introduced: Cisco NX-OS Release 4.0(1)

The clock time zone and daylight savings parameters should be configured if the default values are not desired.   If these values are not configured, the clock will default to UTC without daylight savings adjustments.

```
n7000(config)# clock timezone PST -8 0
n7000(config)# clock summer-time PST
```

NTP Source Interface / IP Address

Introduced: Cisco NX-OS Release 4.1(3)

Specifying a NTP source interface or IP address is recommended when using a VRF instance other than the management VRF instance. This allows security devices such as firewalls to identify the source of the NTP packet. It the source interface or IP address is not specified; the primary IP address on the originating (outbound) interface is used. If the NTP traffic is associated to the management VRF instance, the mgmt0 interface IP address is selected. You cannot configure an NTP interface and IP source address simultaneously.

```
n7000(config)# ntp source-interface ethernet 2/1

n7000(config)# ntp source x.x.x.x
```

NTP Logging

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

NTP logging is disabled by default. NTP messages can be logged to assist when troubleshooting NTP synchronization issues.

```
n7000(config)# ntp logging
```

MD5 Authentication

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

MD5 authentication should be enabled to prevent a device from synchronizing its clock from a rogue NTP server or peer. The same trusted authentication key needs to be configured on the NTP client(s), peer(s), and server(s). An NTP client will not synchronize its clock if it receives an NTP message from an NTP server or peer using a different authentication key.

```
n7000(config)# ntp server a.a.a.a use-vrf management key 1
n7000(config)# ntp peer b.b.b.b use-vrf management key 1

n7000(config)# ntp authentication-key 1 md5 <password>
n7000(config)# ntp trusted-key 1
n7000(config)# ntp authenticate
```

Access Control List

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

Access control lists (ACLs) should be configured to increase security by restricting access to specific NTP peers or servers. Collecting ACL statistics with the **statistics per-entry** is optional, but useful when verifying packets are being received from specific NTP peers or servers.

```
n7000(config)# ntp server a.a.a.a use-vrf management
n7000(config)# ntp peer b.b.b.b use-vrf management
n7000(config)# ntp source x.x.x.x
n7000(config)# ntp access-group peer ntp-peers
```

```
n7000(config)# ip access-list ntp-peers
n7000(config-acl)# statistics per-entry
n7000(config-acl)# permit udp a.a.a.a/32 x.x.x.x/32 eq ntp
n7000(config-acl)# permit udp b.b.b.b/32 x.x.x.x/32 eq ntp
```

Simple Network Management Protocol (SNMP)

Cisco NX-OS supports SNMP v1, v2c, and v3. We recommend that you use SNMPv3 to increase security because it has authentication and encryption capabilities for username, passwords, and payload data.

Basic Configuration (Contact/Location)

Introduced: Cisco NX-OS Release 4.0(1)

Specify the contact and location information so the device is identifiable when being polled by the SNMP management servers.

```
n7000(config)# snmp-server contact Cisco Systems
n7000(config)# snmp-server location San Jose, CA
```

Users (Version 3)

Introduced: Cisco NX-OS Release 4.0(1)

SNMPv3 is the recommended SNMP version because of the additional security authentication and encryption mechanisms. By default, all user accounts in the local database are synchronized to a SNMP user that can be used by an SNMP server to authenticate SNMPv3 requests. Additional user accounts/SNMP user accounts can be created for SNMP polling and sending SNMP inform notifications. In the following example the default “admin” user is displayed and another SNMP user called “snmp-user” is created. The Engine-ID only needs to be configured for SNMP users configured to send v3 notifications (The Engine ID value is based on the SNMP notification server’s engine ID).

```
n7000# show run snmp

snmp-server user admin network-admin auth md5 0x272298231264cbf31dbd423455345253 priv
aes-128 0x272298231264cbf31dbd423455345253 localizedkey

n7000(config)# snmp-server user snmp-user auth md5 <password> priv aes-128 <password>
engineID 80:00:00:09:03:00:0C:29:13:92:B9
```

Community Strings (Version 1 and 2c)

Introduced: Cisco NX-OS Release 4.0(1)

If an SNMPv3 capable management server is not available, SNMP version 1 and 2c can be enabled using the **snmp-server community** command. SNMP v2c provides additional capabilities beyond SNMPv1. SNMP can be configured for read-only or read-write access. Only enable read-only access (network-operator) to increase security.

```
n7000(config)# snmp-server community <password> group network-operator

n7000(config)# snmp-server community <password> group network-admin
```

Note The **snmp-server community <password> ro** command is automatically converted to the **snmp-server community <password> group network-operator** command. The **snmp-server community <password> rw** command is automatically converted to the **snmp-server <password> group network-admin** command.

Notification / Trap Receivers

Introduced: Cisco NX-OS Release 4.0(1)

SNMP notification receivers should be configured to inform the SNMP network management servers about network events. Receivers can be configured for SNMPv1, SNMPv2c, and SNMPv3 for a specific VRF instance. SNMP v3 is recommended because of the additional authentication and encryption capabilities. SNMPv3 requires an SNMP user that is configured with the SNMP recipients Engine-ID.

Version 3 (Recommended)

```
n7000(config)# snmp-server host x.x.x.x version 3 priv snmp-user
n7000(config)# snmp-server host x.x.x.x use-vrf management
```

Version 2c

```
n7000(config)# snmp-server host x.x.x.x traps version 2c <password>
n7000(config)# snmp-server host x.x.x.x informs version 2c <password>
n7000(config)# snmp-server host x.x.x.x use-vrf management
```

Version 1

```
n7000(config)# snmp-server host x.x.x.x traps version 1 <password>
n7000(config)# snmp-server host x.x.x.x use-vrf management
```

Notification / Trap Events

Introduced: Cisco NX-OS Release 4.0(1)

SNMP Notifications or Traps should be enabled to notify the SNMP management server(s) about important events. Enable all SNMP notifications/traps, or enable specific notifications/traps of interest depending on what features are enabled. Some notifications/traps are enabled by default. Use the **show snmp-server trap** command to verify what traps are enabled. SNMP Notifications or Traps will be sent depending on how the SNMP host recipients are configured.

Enable All Notifications/Traps

```
n7000(config)# snmp-server enable traps
```

Enable Individual Notifications/Traps

```
n7000(config)# snmp-server enable traps feature-control
n7000(config)# snmp-server enable traps callhome smtp-send-fail
n7000(config)# snmp-server enable traps snmp authentication
```

Interface Link-Status Traps

Introduced: Cisco NX-OS Release 4.0(1)

SNMP interface link-status traps are enabled by default. SNMP link-status traps can be disabled per interface. It may be beneficial to disable interface traps in certain environments. However, we always recommend that you keep interface traps enabled for critical infrastructure or server interfaces.

```
n7000(config)# interface ethernet 1/1
n7000(config-if)# no snmp trap link-status
```

Community String Access Control List

Introduced: Cisco NX-OS Release 4.2(1)

Access control lists (ACLs) should always be applied to community strings (SNMP v1 and v2c) to restrict access to specific source and destination IP addresses.

```
n7000(config)# ip access-list snmp-acl
n7000(config-acl)# permit udp host x.x.x.x host x.x.x.x eq snmp

n7000(config)# snmp-server community <password> group network-operator
n7000(config)# snmp-server community <password> use-acl snmp-acl
```

Source Interface

Introduced: Cisco NX-OS Release 4.2(1)

Specify the source interface for **informs** and **traps** if the management VRF instance is not being used. This allows security devices such as firewalls to identify the source of the SNMP packet. If the source interface or IP address is not specified the primary IP address on the originating (outbound) interface is selected. The **inform** feature only applies to SNMP v2c and v3. You can configure the source interface globally for all SNMP hosts or per SNMP host.

Global Configuration:

```
n7000(config)# snmp source-interface informs loopback0
n7000(config)# snmp source-interface traps loopback0
```

Per Server Configuration:

```
n7000(config)# snmp-server host a.a.a.a source-interface loopback0
```

Disabling SNMP

Introduced: Cisco NX-OS Release 4.2(1)

SNMP is enabled by default. However, SNMP v1 and v2c will not respond to SNMP requests unless a community string is configured. SNMPv3 will respond to SNMP requests if the SNMPv3 capable server polls the Cisco Nexus 7000 Series device. (The SNMP user “admin” is configured by default.) If SNMP is not a requirement it should be disabled with the following command to increase security.

```
n7000(config)# no snmp-server protocol enable
```

System Message Logging

Cisco NX-OS software saves system messages to a local log file (log:messages) in DRAM. (The most recent 100 severity 0, 1, or 2 messages are saved in NVRAM.) Cisco NX-OS software also logs system messages to the logflash (logflash://sup-local/log/messages) by default, which provides persistent logging data after a system reload.

Syslog Server

Introduced: Cisco NX-OS Release 4.0(1)

Up to eight Syslog servers can be configured to receive system messages. We recommend that you configure at least two Syslog servers for redundancy and use the management VRF instance for traffic isolation. The severity filter for log messages can be specified per server (the default severity filter is 5). In the following example, two servers are configured with a severity filter of 6. Setting the severity filter to 6 ensures that messages with a severity of 0 (emergency) through 6 (informational) are sent to each server. Selecting the severity filter will depend on how much information should be collected on the servers. We do not recommend configuring a severity filter less than 5.

```
n7000(config)# logging server a.a.a.a 6 use-vrf management
n7000(config)# logging server b.b.b.b 6 use-vrf management
```

Source Interface

Introduced: Cisco NX-OS Release 4.0(1)

If the default VRF instance is used to reach the Syslog server(s), a loopback interface can be specified as the source IP address. This allows security devices such as firewalls to identify the source of the Syslog packet. If a source interface is not specified, the primary IP address of the originating (outbound) interface is selected.

```
n7000(config)# logging source-interface loopback 0
```

Link Status Events

Introduced: Cisco NX-OS Release 4.0(1)

All interface link status (up/down) messages are logged by default. Link status events can be configured globally or per interface. The following global command disables link status logging messages for all interfaces. The interface command enables link status logging messages for a specific interface. This scenario may be beneficial to filter out excessive messages, except for mission critical infrastructure or server interfaces.

```
n7000(config)# no logging event link-status default

n7000(config)# interface ethernet x/x
n7000(config-if)# logging event port link-status
```

Timestamps

Introduced: Cisco NX-OS Release 4.0(1)

System message logging defaults to one-second time units. Timestamps can be configured for millisecond and microseconds for finer granularity. We recommend using timestamps in milliseconds or microseconds when troubleshooting time sensitive issues.

```
n7000(config)# logging timestamp milliseconds
```

Per Feature Severity Level

Introduced: Cisco NX-OS Release 4.0(1)

Cisco NX-OS software supports configured severity levels per feature. We recommend that you configure the severity level for the features that require a higher level of manageability in the network. The following example demonstrates the configuration and verification commands for NTP.   The **logging level all <severity #>** command can be used to change the current severity level for all features.

```
n7000(config)# logging level ntp 7

n7000# show logging level ntp
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
ntp                     2                       7

0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)

n7000(config)# logging level all 5
```

Viewing Log File Contents

Introduced: Cisco NX-OS Release 4.0(1)

The following **show logging** commands are useful when viewing and managing system message log files.

```
n7000# show logging logfile  <-  Displays the contents of the default log file.

n7000# show logging last 10  <-  Displays the last # of lines of the default log file.

n7000# show logging NVRAM   <- Displays contents of the log file stored in NVRAM.

n7000# show file logflash://sup-local/log/messages <- Displays contents in logflash.
```

Clearing Log File Contents

Introduced: Cisco NX-OS Release 4.0(1)

The following **clear** commands are useful if it is desirable to clear the contents of the system message log files.

```
n7000# clear logging logfile  <- Clears the contents of the default log file.
```

```
n7000# clear logging nvram    <- Clears the contents of the default log file stored in
NVRAM.
```

Smart Call Home

Smart Call Home provides an automated method for sending standard text e-mail or XML notifications to recipients such as a network operation center (NOC), a specific engineer, or the Cisco TAC to auto-generate a TAC case. Enabling Call Home for both internal and Cisco TAC recipients is recommended to speed up problem resolution.

Internal and Cisco TAC Recipients (Destination-Profiles)

Introduced: Cisco NX-OS Release 4.0(1)

Although Smart Call Home was introduced in Cisco NX-OS Release 4.0(1), the following example is based on Cisco NX-OS Release 5.0(2a) CLI syntax. In this example: Call Home is configured to send a full-text e-mail to two different e-mail servers for redundancy using the management VRF instance for traffic isolation. For the destination profile "Internal-NOC" the mail server a.a.a.a is preferred due to the lower priority. If it does not respond, mail server b.b.b.b will be used.

```
n7000(config)# callhome

n7000(config-callhome)# contract-id Cisco-Contract-#
n7000(config-callhome)# customer-id xyz.com

n7000(config-callhome)# site-id n7000-Kirkland-DC
n7000(config-callhome)# streetaddress 12345 Street NE, Kirkland, WA
n7000(config-callhome)# email-contact Cisco-Customer@xyz.com
n7000(config-callhome)# phone-contact +1-800-123-4567

n7000(config-callhome)# destination-profile Internal-NOC
n7000(config-callhome)# destination-profile Internal-NOC format full-txt
n7000(config-callhome)# destination-profile Internal-NOC email-addr call-home-noc@xyz.com
n7000(config-callhome)# destination-profile Internal-NOC alert-group all

n7000(config-callhome)# destination-profile CiscoTAC-1 email-addr callhome@cisco.com

n7000(config-callhome)# transport email mail-server a.a.a.a priority 10 use-vrf management
n7000(config-callhome)# transport email mail-server b.b.b.b use-vrf management

n7000(config-callhome)# transport email from call-home@xyz.com
n7000(config-callhome)# transport email reply-to call-home@xy.com
```

Note The **transport email snmp-server** command is the original command supported in Cisco NX-OS Release 4.x and NX-OS Release 5. X software. The **transport email mail-server** command was introduced in NX-OS Release 5.0(2a) to add support for multiple servers and priorities.

Testing Call Home Recipients

Introduced: Cisco NX-OS Release 4.0(1)

Always test the Call Home recipients during the initial Call Home configuration to ensure Call Home works as expected.

```
n7000# callhome test
```