



CHAPTER 3

Overview

This chapter describes the system management features that you can use to monitor and manage Cisco NX-OS devices.

This chapter includes the following sections:

- [Cisco NX-OS Device Configuration Methods, page 3-22](#)
- [Cisco Fabric Services, page 3-23](#)
- [Network Time Protocol, page 3-23](#)
- [Precision Time Protocol, page 3-23](#)
- [Cisco Discovery Protocol, page 3-24](#)
- [System Messages, page 3-24](#)
- [Call Home, page 3-24](#)
- [Rollback, page 3-24](#)
- [Session Manager, page 3-24](#)
- [Scheduler, page 3-25](#)
- [SNMP, page 3-25](#)
- [RMON, page 3-25](#)
- [Online Diagnostics, page 3-25](#)
- [Embedded Event Manager, page 3-25](#)
- [On-Board Failure Logging, page 3-25](#)
- [SPAN, page 3-26](#)
- [ERSPAN, page 3-26](#)
- [LLDP, page 3-26](#)
- [NetFlow, page 3-26](#)
- [FabricPath, page 3-27](#)
- [Troubleshooting Features, page 3-27](#)

Send document comments to nexus7k-docfeedback@cisco.com.

Cisco NX-OS Device Configuration Methods

You can configure devices using direct network configuration methods or web services hosted on a Cisco Data Center Network Management (Cisco DCNM) server.

Figure 3-1 shows the device configuration methods available to a network user.

Figure 3-1 Cisco NX-OS Device Configuration Methods

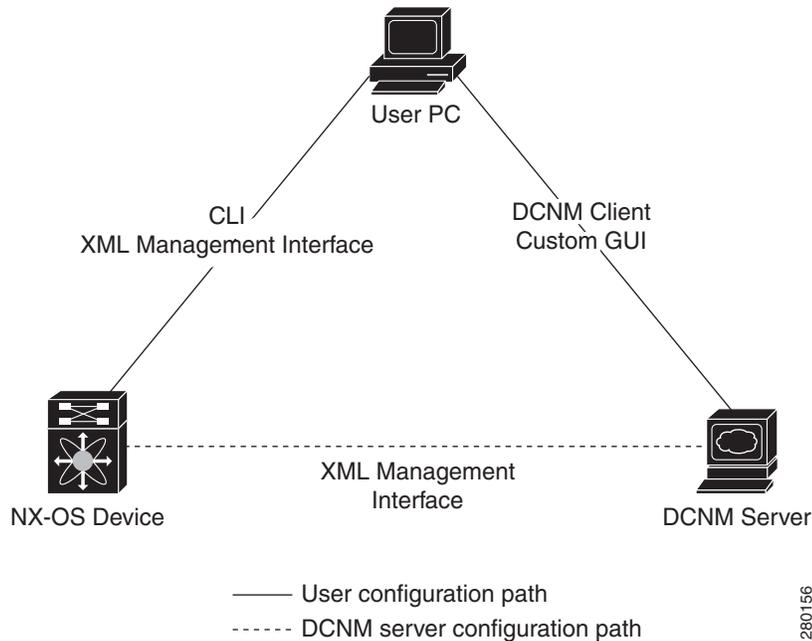


Table 3-1 lists the configuration method and the document where you can find more information.

Table 3-1 Configuration Methods Book Links

Configuration Method	Document
CLI from a Secure Shell (SSH) session, a Telnet session, or the console port	<i>Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 5.x</i>
XML management interface	<i>Cisco NX-OS XML Interface User Guide</i>
Cisco DCNM client	<i>Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 5.x</i>
User-defined GUI	<i>Web Services API Guide, Cisco DCNM for LAN, Release 5.x</i>

This section includes the following topics:

- [Configuring with CLI or XML Management Interface, page 3-23](#)
- [Configuring with Cisco DCNM or a Custom GUI, page 3-23](#)

Send document comments to nexus7k-docfeedback@cisco.com.

Configuring with CLI or XML Management Interface

You can configure Cisco NX-OS devices using the command-line interface (CLI) or the XML management interface over Secure Shell (SSH) as follows:

- CLI from an SSH session, a Telnet session, or the console port—You can configure devices using the CLI from an SSH session, a Telnet session, or the console port. SSH provides a secure connection to the device. For more information, see the *Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 5.x*.
- XML management interface over SSH—You can configure devices using the XML management interface, which is a programmatic method based on the NETCONF protocol that complements the CLI functionality. For more information, see the *Cisco NX-OS XML Interface User Guide*.

Configuring with Cisco DCNM or a Custom GUI

You can configure Cisco NX-OS devices using the Cisco DCNM client or from your own GUI as follows:

- Cisco DCNM Client—You can configure devices using the Cisco DCNM client, which runs on your local PC and uses web services on the Cisco DCNM server. The Cisco DCNM server configures the device over the XML management interface. For more information about the Cisco DCNM client, see the *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 5.x*.
- Custom GUI—You can create your own GUI to configure devices using the Cisco DCNM web services application program interface (API) on the Cisco DCNM server. You use the SOAP protocol to exchange XML-based configuration messages with the Cisco DCNM server. The Cisco DCNM server configures the device over the XML management interface. For more information about creating custom GUIs, see the *Web Services API Guide, Cisco DCNM for LAN, Release 5.x*.

Cisco Fabric Services

Cisco Fabric Services (CFS) is a Cisco proprietary feature that distributes data, including configuration changes, to all Cisco NX-OS devices in a network. For more information about CFS, see [Chapter 1, “Configuring CFS.”](#)

Network Time Protocol

The Network Time Protocol (NTP) synchronizes the time of day among a set of distributed time servers and clients so that you can correlate time-specific information, such as system logs, received from the devices in your network. For more information about NTP, see [Chapter 1, “Configuring NTP.”](#)

Precision Time Protocol

The Precision Time Protocol (PTP) is a time synchronization protocol for nodes distributed across a network. Its hardware timestamp feature provides greater accuracy than other time synchronization protocols such as Network Time Protocol (NTP). For more information about PTP, see [Chapter 1, “Configuring PTP.”](#)

Send document comments to nexus7k-docfeedback@cisco.com.

Cisco Discovery Protocol

You can use the Cisco Discovery Protocol (CDP) to discover and view information about all Cisco equipment that is directly attached to your device. CDP runs on all Cisco-manufactured equipment including routers, bridges, access and communication servers, and switches. CDP is media and protocol independent, and gathers the protocol addresses of neighboring devices, discovering the platform of those devices. CDP runs over the data link layer only. Two systems that support different Layer 3 protocols can learn about each other. For more information about CDP, see [Chapter 1, “Configuring CDP.”](#)

System Messages

You can use system message logging to control the destination and to filter the severity level of messages that system processes generate. You can configure logging to a terminal session, a log file, and syslog servers on remote systems.

System message logging is based on RFC 3164. For more information about the system message format and the messages that the device generates, see the *Cisco NX-OS System Messages Reference*. For information about configuring system messages, see [Chapter 1, “Configuring System Message Logging.”](#)

Call Home

Call Home provides an e-mail-based notification of critical system policies. Cisco NX-OS provides a range of message formats for optimal compatibility with pager services, standard e-mail, or XML-based automated parsing applications. You can use this feature to page a network support engineer, e-mail a Network Operations Center, or use Cisco Smart Call Home services to automatically generate a case with the Technical Assistance Center. For information about configuring Call Home, see [Chapter 1, “Configuring Smart Call Home.”](#)

Rollback

The rollback feature allows you to take a snapshot, or checkpoint, of the device configuration and then reapply that configuration at any point without having to reload. Rollback allows any authorized administrator to apply this checkpoint configuration without requiring expert knowledge of the features configured in the checkpoint.

Session Manager allows you to create a configuration session and apply all commands within that session atomically. For more information, see the [Chapter 1, “Configuring Rollback.”](#)

Session Manager

Session Manager allows you to create a configuration and apply it in batch mode after the configuration is reviewed and verified for accuracy and completeness. For more information, see [Chapter 1, “Configuring Session Manager.”](#)

Send document comments to nexus7k-docfeedback@cisco.com.

Scheduler

The scheduler allows you to create and manage jobs such as routinely backing up data or making QoS policy changes. The scheduler can start a job according to your needs—only once at a specified time or at periodic intervals. For more information, see [Chapter 1, “Configuring the Scheduler.”](#)

SNMP

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network. For more information, see [Chapter 1, “Configuring SNMP.”](#)

RMON

RMON is an Internet Engineering Task Force (IETF) standard monitoring specification that allows various network agents and console systems to exchange network monitoring data. Cisco NX-OS supports RMON alarms, events, and logs to monitor Cisco NX-OS devices. For more information, see [Chapter 1, “Configuring RMON.”](#)

Online Diagnostics

Cisco Generic Online Diagnostics (GOLD) define a common framework for diagnostic operations across Cisco platforms. The online diagnostic framework specifies the platform-independent fault-detection architecture for centralized and distributed systems, including the common diagnostics CLI and the platform-independent fault-detection procedures for boot-up and run-time diagnostics.

The platform-specific diagnostics provide hardware-specific fault-detection tests and allow you to take appropriate corrective action in response to diagnostic test results. For information about configuring online diagnostics, see [Chapter 1, “Configuring Online Diagnostics.”](#)

Embedded Event Manager

The Embedded Event Manager (EEM) allows you to detect and handle critical events in the system. EEM provides event detection and recovery, including monitoring of events either as they occur or as thresholds are crossed. For information about configuring EEM, see [Chapter 1, “Configuring the Embedded Event Manager.”](#)

On-Board Failure Logging

You can configure a device to log failure data to persistent storage, which you can retrieve and display for analysis at a later time. This on-board failure logging (OBFL) feature stores failure and environmental information in nonvolatile memory on the module. This information is useful for analysis of failed modules. For information about configuring OBFL, see [Chapter 1, “Configuring Onboard Failure Logging.”](#)

Send document comments to nexus7k-docfeedback@cisco.com.

SPAN

You can configure an Ethernet switched port analyzer (SPAN) to monitor traffic in and out of your device. The SPAN features allow you to duplicate packets from source ports to destination ports. For information about configuring SPAN, see [Chapter 1, “Configuring SPAN.”](#)

ERSPAN

Encapsulated remote switched port analyzer (ERSPAN) is used to transport mirrored traffic in an IP network. ERSPAN supports source ports, source VLANs, and destinations on different switches, which provide remote monitoring of multiple switches across your network. ERSPAN uses a generic routing encapsulation (GRE) tunnel to carry traffic between switches.

ERSPAN consists of an ERSPAN source session, routable ERSPAN GRE-encapsulated traffic, and an ERSPAN destination session. You separately configure ERSPAN source sessions and destination sessions on different switches.

To configure an ERSPAN source session on one switch, you associate a set of source ports or VLANs with a destination IP address, ERSPAN ID number, and virtual routing and forwarding (VRF) name. To configure an ERSPAN destination session on another switch, you associate the destinations with the source IP address, the ERSPAN ID number, and a VRF name.

The ERSPAN source session copies traffic from the source ports or source VLANs and forwards the traffic using routable GRE-encapsulated packets to the ERSPAN destination session. The ERSPAN destination session switches the traffic to the destinations. For information about configuring ERSPAN, see [Chapter 1, “Configuring ERSPAN.”](#)

LLDP

Link Layer Discovery Protocol (LLDP) is a vendor-neutral, one-way device discovery protocol that allows network devices to advertise information about themselves to other devices on the network. This protocol runs over the data-link layer, which allows two systems running different network layer protocols to learn about each other. You can enable LLDP globally or per interface. For information about configuring LLDP, see [Chapter 1, “Configuring LLDP.”](#)

NetFlow

NetFlow allows you to identify packet flows for both ingress and egress IP packets and provide statistics based on these packet flows. NetFlow does not require any change to either the packets themselves or to any networking device. For information about configuring NetFlow, see [Chapter 1, “Configuring NetFlow.”](#)

Send document comments to nexus7k-docfeedback@cisco.com.

FabricPath

FabricPath brings the benefits of Layer 3 routing to Layer 2 switched networks to build a highly resilient and scalable Layer 2 fabric. The system manager is responsible for starting the FabricPath resources process and monitoring its heartbeats. For information about configuring FabricPath, see the *Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide*.

Troubleshooting Features

Cisco NX-OS provides troubleshooting tools such as ping, traceroute, Ethanalyzer, and the Blue Beacon feature. See the *Cisco Nexus 7000 Series NX-OS Troubleshooting Guide* for details on these features.

When a service fails, the system generates information that can be used to determine the cause of the failure. The following sources of information are available:

- Every service restart generates a syslog message of level LOG_ERR.
- If the Smart Call Home service is enabled, every service restart generates a Smart Call Home event.
- If SNMP traps are enabled, the SNMP agent sends a trap when a service is restarted.
- When a service failure occurs on a local module, you can view a log of the event by entering the **show processes log** command in that module. The process logs are persistent across supervisor switchovers and resets.
- When a service fails, a system core image file is generated. You can view recent core images by entering the **show cores** command on the active supervisor. Core files are not persistent across supervisor switchovers and resets, but you can configure the system to export core files to an external server using a file transfer utility such as Trivial File Transfer Protocol (TFTP) by entering the **system cores** command.
- CISCO-SYSTEM-MIB contains a table for cores (cseSwCoresTable).

For information on collecting and using the generated information relating to service failures, see the *Cisco Nexus 7000 Series NX-OS Troubleshooting Guide*.

Send document comments to nexus7k-docfeedback@cisco.com.