CHAPTER 5

Administering Device Discovery

This chapter describes how to administer the Device Discovery feature in the Cisco Data Center Network Manager (DCNM).

This chapter includes the following sections:

Information About Device Discovery

This section includes the following topics:

Device Discovery

The Device Discovery feature creates devices in Cisco DCNM by connecting to a Cisco NX-OS device and retrieving data from the device, including its running configuration. Cisco DCNM can also discover Cisco NX-OS devices and network servers that are neighbors of the first device, which is known as the *seed device*.

If the device supports virtual device contexts (VDCs), Cisco DCNM retrieves the running configuration of each VDC that is configured on the physical device. Cisco DCNM displays each VDC as a device, including the default VDC. If the Cisco NX-OS device has only the default VDC, then device discovery creates only one device in Cisco DCNM.

When Cisco DCNM connects to a device to retrieve its configuration, it uses the XML management interface, which uses the XML-based Network Configuration Protocol (NETCONF) over Secure Shell (SSH). For more information, see the *Cisco NX-OS XML Management Interface User Guide, Release 5.x*.

Discovery Protocols

Cisco DCNM uses a variety of protocols to discover devices and servers in your data center network. This section includes the following topics:

Cisco Discovery Protocol

Device discovery uses the Cisco Discovery Protocol (CDP) to find devices that are connected to the initial device in the discovery process. CDP exchanges information between adjacent devices over the data link layer. The exchanged information is helpful in determining the network topology and physical configuration outside of the logical or IP layer.

CDP allows Cisco DCNM to discover devices that are one or more hops beyond the seed device in the discovery process. When you start the discovery process using the Device Discovery feature, you can limit the number of hops that the discovery process can make.

After Cisco DCNM discovers a Cisco NX-OS device using CDP, it connects to the device and retrieves information, such as the running configuration of the device. The information collected allows Cisco DCNM to manage the device.

Cisco DCNM supports CDP hops on some Cisco switches that run Cisco IOS software. Although Cisco DCNM cannot manage these devices, the Topology feature allows you to see unmanaged devices and the CDP links between unmanaged devices and managed devices.

Link Layer Discovery Protocol

Device discovery uses Link Layer Discovery Protocol (LLDP) to discover the network adapters of servers that are connected to Cisco NX-OS devices. For more information, see Chapter 9, “Configuring Network Servers.”

Fibre Channel

To discover network elements in a storage area network (SAN), Cisco DCNM uses Fibre Channel. Cisco DCNM can discover SAN switches, servers, and storage arrays.

Credentials and Discovery

Device discovery requires that you provide a username and password for a user account on the seed device. To successfully complete the discovery of a Cisco NX-OS device, the user account that you specify must be assigned to either the network-admin or the vdc-admin role.

If you want to discover devices that are one or more hops from the seed device, all devices in the chain of hops must be configured with a user account of the same username and password. All Cisco NX-OS devices in the chain of hops must assign the user account to the network-admin or the vdc-admin role.

Discovery Process

Cisco DCNM discovers devices in several phases, as follows:

1. CDP neighbor discovery—Discovers the topology of the interconnected devices, beginning with the seed device and preceding for the number of CDP hops specified when you initiate discovery.
2. Supported device selection—Determines which of the discovered devices are supported by Cisco DCNM. Discovery continues for the supported devices only.
3. Inventory discovery—Discovers the inventory of the devices selected in the previous phase. For example, if the device is a Cisco Nexus 7000 Series switch, inventory discovery determines the supervisor modules, I/O modules, power supplies, and fans. If the device is a Cisco Nexus 1000V switch, inventory discovery finds the Virtual Supervisor Module and Virtual Ethernet Modules.
4. Device configuration discovery—Discovers the details of feature configuration on each device, such as interfaces, access control lists, and VLANs.
5. Network discovery—Associates network features with the device configuration details discovered in the previous phase.

Cisco NX-OS System-Message Logging Requirements

To monitor and manage devices, Cisco DCNM depends partly on system messages that it retrieves from managed devices. This section describes the system-message requirements that all Cisco NX-OS devices must meet before they can be managed and monitored by Cisco DCNM.

This section includes the following topics:

Interface Link-Status Events Logging Requirement

Devices must be configured to log system messages about interface link-status change events. This requirement ensures that Cisco DCNM receives information about interface link-status changes. The following two commands must be present in the running configuration on the device:

logging event link-status enable

logging event link status default

To ensure that these commands are configured on the device, perform the steps in the "Verifying the Discovery Readiness of a Cisco NX-OS Device" section on page 5-7.

Logfile Requirements

Devices must be configured to store system messages that are severity level 6 or lower in the log file.

Although you can specify any name for the log file, we recommend that you do not change the name of the log file. When you change the name of the log file, the device clears previous system messages. The default name of the log file is "messages."

If you use the default name for the log file, the following command must be present in the running configuration on the device:

logging logfile messages 6

To ensure that this command is configured on the device, perform the steps in the "Verifying the Discovery Readiness of a Cisco NX-OS Device" section on page 5-7.

Logging Severity-Level Requirements

Cisco DCNM has minimum severity level requirements for some Cisco NX-OS logging facilities. All enabled features on a Cisco NX-OS have a default logging level. The logging level required by Cisco DCNM varies per logging facility but is often higher than the default logging level in Cisco NX-OS. For more information, see the "Automatic Logging-Level Configuration Support" section on page 5-4.

Automatic Logging-Level Configuration Support

Cisco DCNM provides support for automatic logging level configuration for all supported Cisco NX-OS releases with the exception of Cisco NX-OS Release 4.0, which is available on Cisco Nexus 7000 Series switches only. This section describes how Cisco DCNM supports automatic logging-level configuration. For information about manually configuring logging levels for Cisco NX-OS Release 4.0, see the "Verifying the Discovery Readiness of a Cisco NX-OS Device" section on page 5-7.

During Device Discovery

During device discovery, if Cisco DCNM finds that a logging level on a discovered device is below the minimum logging-level requirement for that logging facility, Cisco DCNM raises the logging level to meet the minimum requirement. If logging levels meet or exceed the requirements, Cisco DCNM does not change the logging levels during discovery.

At Feature Enablement in the Cisco DCNM Client

If you use the Cisco DCNM client to enable a feature on a device and the default logging level for the feature does not meet the minimum requirement, the Cisco DCNM client warns you that it will configure the logging level on the device to meet the requirement. If you reject the logging level change, Cisco DCNM does not enable the feature.

During Auto-Synchronization with Managed Devices

If you use another means, such as the command-line interface (CLI), to enable a feature on a managed device and the default logging level for the feature does not meet the minimum requirement, Cisco DCNM automatically configures the logging level to meet the requirement after Cisco DCNM detects that the feature is enabled.

If you use the CLI or any other method to lower a logging level below the minimum requirement of Cisco DCNM, after Cisco DCNM detects the logging level change, it changes the state of that device to unmanaged. When this occurs, the Devices and Credentials feature shows that logging levels are the reason that the device is unmanaged. You can use the Devices and Credentials feature to discover the device again. During rediscovery, Cisco DCNM sets logging levels that do not meet the minimum requirements.

VDC Support

When Cisco DCNM discovers a Cisco NX-OS device that supports VDCs, it determines how many VDCs are on the Cisco NX-OS device. In Cisco DCNM, each VDC is treated as a separate device. The status of each VDC is tracked separately and you can configure each VDC independently of other VDCs on a Cisco NX-OS device.

Before discovering a Cisco Nexus 7000 Series device that has nondefault VDCs, ensure that each VDC meets the prerequisites for discovery. For more information, see the "Prerequisites for Device Discovery" section on page 5-6.

Licensing Requirements for Device Discovery

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM	The Device Discovery feature requires no license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you. For information about obtaining and installing a Cisco DCNM LAN Enterprise license, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.

Prerequisites for Device Discovery

Prior to performing device discovery, you should be familiar with the following:

- VDCs, if you are discovering Cisco Nexus 7000 Series devices.
- CDP

The Device Discovery feature has the following prerequisites:

- The Cisco DCNM server must be able to connect to devices that it discovers.
- Cisco NX-OS devices must be running a supported release of Cisco NX-OS. For information about supported releases of Cisco NX-OS, see the *Cisco DCNM Release Notes, Release 5.x*.
- The Cisco NX-OS device must have the minimal configuration that is required to enable device discovery to succeed. For more information, see the "Verifying the Discovery Readiness of a Cisco NX-OS Device" section on page 5-7.
- For a Cisco Nexus 7000 Series device, each VDC that you want to discover must have a management interface configured. Cisco DCNM supports discovery of VDCs that are configured with a management interface that is the mgmt0 interface, which is an out-of-band virtual interface, or with an in-band Ethernet interface that is allocated to the VDC.
- To allow Cisco DCNM to discover devices that are CDP neighbors, CDP must be enabled both globally on each device and specifically on the device interfaces used for device discovery. For a Cisco Nexus 7000 Series device, CDP must be enabled globally in each VDC and on the management interface that each VDC is configured to use.
- Discovery of network servers requires that LLDP is enabled globally on devices connected to network servers and specifically on the device interfaces connected to the network adapters on network servers.

Guidelines and Limitations for Device Discovery

The Device Discovery feature has the following configuration guidelines and limitations:

- Ensure that Cisco NX-OS devices that you want to discover have been prepared for discovery. For more information, see the "Verifying the Discovery Readiness of a Cisco NX-OS Device" section on page 5-7.
- Cisco DCNM can manage only devices that run Cisco NX-OS. For more information about supported device operating systems and supported device hardware, see the *Cisco DCNM Release Notes, Release 5.x*.
- CDP-based discovery of devices requires that all devices in the chain of CDP hops use the same username and password specified for the seed device. If your security practices do not allow the same username and password to be used on each device, you can perform device discovery for each device individually.
- Devices that are CDP hops but which are not running Cisco IOS software appear in the Topology feature but cannot be managed by Cisco DCNM.

Performing Device Discovery

This section includes the following topics:

Verifying the Discovery Readiness of a Cisco NX-OS Device

Before you perform device discovery with Cisco DCNM, you should perform the following procedure on each Cisco NX-OS device that you want to manage and monitor with Cisco DCNM. This procedure helps to ensure that device discovery succeeds and that Cisco DCNM can effectively manage and monitor the device.

Note If you are preparing a physical device that supports virtual device contexts (VDCs), remember that Cisco DCNM considers each VDC to be a device. You must verify discovery readiness for each VDC that you want to manage and monitor with Cisco DCNM.

DETAILED STEPS

Step 1 Log into the CLI of the Cisco NX-OS device.

Step 2 Use the **configure terminal** command to access global configuration mode.

Step 3 Ensure that an RSA or DSA key exists so that secure shell (SSH) connections can succeed. To do so, use the **show ssh key rsa** or **show ssh key dsa** command.

If you need to generate a key, use the **ssh key** command.

Note You must disable the SSH server before you can generate a key. To do so, use the **no feature ssh** command.

Step 4 Ensure that the SSH server is enabled. To do so, use the **show ssh server** command.

If the SSH server is not enabled, use the **feature ssh** command to enable it.

Step 5 Ensure that CDP is enabled globally and on the interface that Cisco DCNM uses to connect to the device. Use the **show run cdp all** command to see whether CDP is enabled.

Step 6 Verify that the **logging event link-status default** and **logging event link-status enable** commands are configured.

```
switch(config)# show running-config all | include "logging event link-status"
logging event link-status default
logging event link-status enable
```

If either command is missing, enter it to add it to the running configuration.

Note The **logging event link-status enable** command is included in the default Cisco NX-OS configuration. The **show running-config** command displays the default configuration only if you use the **all** keyword.

Step 7 Verify that the device is configured to log system messages that are severity 6 or lower.

Note The default name of the log file is "messages"; however, we recommend that you use the log-file name currently configured on the device. If you change the name of the log file, the device clears previous system messages.

```
switch(config)# show running-config all | include logfile
logging logfile logfile-name 6
```

If the **logging logfile** command does not appear or if the severity level is less than 6, configure the **logging logfile** command.

```
switch(config)# logging logfile logfile-name 6
```

Step 8 If the device is a Cisco Nexus 7000 Series switch that is running Cisco NX-OS Release 4.0, you must manually verify that the logging level configuration of the device meets the Cisco DCNM logging level requirements. To do so, follow these steps:

a. Determine which nondefault features are enabled on the device.

```
switch(config)# show running-config | include feature
feature feature1
feature feature2
feature feature3
.
.
.
```

b. View the logging levels currently configured on the device. The **show logging level** command displays logging levels only for features that are enabled. The Current Session Severity column lists the current logging level.

```
switch(config)# show logging level
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
aaa                     3                       5
aclmgr                  3                       3
.
.
.
```

Note You can use the **show logging level** command with the facility name when you want to see the logging level of a single logging facility, such as **show logging level aaa**.

c. Determine which logging levels on the device are below the minimum Cisco DCNM-required logging levels. To do so, compare the logging levels displayed in b. to the minimum Cisco DCNM-required logging levels that are listed in Table 5-2.

d. For each logging facility with a logging level that is below the minimum Cisco DCNM-required logging level, configure the device with a logging level that meets or exceeds the Cisco DCNM requirement.

```
switch(config)# logging level facility severity-level
```

The *facility* argument is the applicable logging-facility keyword from Table 5-2, and *severity-level* is the applicable minimum Cisco DCNM-required logging level or higher (up to 7).

e. Use the **show logging level** command to verify your changes to the configuration.

Step 9 Copy the running configuration to the startup configuration to save your changes.

```
switch(config)# copy running-config startup-config
[########################################] 100%
switch(config)#
```

Discovering Devices

You can discover one or more devices. When a discovery task succeeds, Cisco DCNM retrieves the running configuration and status information of discovered Cisco NX-OS devices.

Use this procedure for the following purposes:

- To discover devices that are not currently managed by Cisco DCNM. For example, you should use this procedure when Cisco DCNM has not yet discovered any devices, such as after a new installation.
- To discover devices that you have added to your network without rediscovering devices that Cisco DCNM already has discovered.
- To rediscover the topology when CDP links have changed, without rediscovering devices that Cisco DCNM has already discovered.

Note You must successfully discover a Cisco NX-OS device before you can use Cisco DCNM to configure the device.

BEFORE YOU BEGIN

Ensure that you have configured the Cisco NX-OS device so that the Cisco DCNM server can connect to it and successfully discover it. For more information, see the "Verifying the Discovery Readiness of a Cisco NX-OS Device" section on page 5-7.

Determine the IPv4 address of the device that you want Cisco DCNM to connect to when it starts the discovery task. This is the seed device for the discovery.

Determine whether you want to discover devices that are CDP neighbors of the seed device. If so, determine the maximum number of hops from the seed device that the discovery process can make.

Note The discovery process can perform complete discovery of neighbors only if the neighboring devices are configured with the same credentials as the seed device.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Device Discovery**.

The discovery tasks appear in the Discovery Tasks area of the Contents pane.

Step 2 In the Seed Device field, enter the IPv4 address of the device that you want Cisco DCNM to connect to when it starts the discovery task. Valid entries are in dotted decimal format.

Step 3 In the User Name field, enter the username of a user account on the device. The user account must have a network-admin or vdc-admin role.

Step 4 In the Password field, enter the password for the user account that you entered in the User Name field.

Step 5 (Optional) If you want Cisco DCNM to discover devices that are CDP neighbors of the seed device, in the Maximum Hops of Neighbors to Discover field, enter the desired maximum number of hops. By default, the maximum hops is 0 (zero).

Step 6 Ensure that **Rediscover Configuration and Status for Existing Devices** is unchecked. By default, this check box is unchecked.

By leaving this check box unchecked, you enable Cisco DCNM to use previously discovered devices as CDP hops without retrieving their running configuration and status information.

Step 7 Click **Start Discovery**.

After a short delay, the discovery task appears at the bottom of the list of tasks in the Discovery Tasks area. Cisco DCNM updates the task status periodically.

Step 8 Wait until the status for the task is Successful. This step may take several minutes.

After the status is Successful, you can use Cisco DCNM to configure and monitor the discovered devices.

You do not need to save your changes.

Rediscovering Devices

You can rediscover one or more devices.

Note Rediscovery replaces any configuration data that Cisco DCNM has for a Cisco NX-OS device with the configuration data retrieved during the rediscovery. If you need to discover one or more devices without retrieving configuration and status information for already discovered devices, see the "Discovering Devices" section on page 5-9.

You must successfully discover a Cisco NX-OS device before you can use Cisco DCNM to configure the device.

BEFORE YOU BEGIN

Ensure that you have configured the Cisco NX-OS device so that the Cisco DCNM server can connect to it. For more information, see the "Verifying the Discovery Readiness of a Cisco NX-OS Device" section on page 5-7.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Device Discovery**.

The discovery tasks and their status appear in the Discovery Tasks area of the Contents pane.

Step 2 In the Seed Device field, enter the IPv4 address of the device that you want Cisco DCNM to connect to when it starts the discovery task. Valid entries are in dotted decimal format.

Step 3 In the User Name field, enter the username of a user account on the device. The user account must have a network-admin or vdc-admin role.

Step 4 In the Password field, enter the password for the user account that you entered in the User Name field.

Step 5 (Optional) If you want Cisco DCNM to rediscover devices that are CDP neighbors of the seed device, in the Maximum Hops of Neighbors to Discover field, enter the desired maximum number of hops. By default, the maximum hops is 0 (zero).

Step 6 Check **Rediscover Configuration and Status for Existing Devices**. By default, this check box is unchecked.

By checking this check box, you enable Cisco DCNM to replace any configuration and status information that it has about a previously discovered device with the running configuration and status information retrieved from the device.

Step 7 Click **Start Discovery**.

After a short delay, the discovery task appears at the bottom of the list of tasks in the Discovery Tasks area. Cisco DCNM updates the task status periodically.

Step 8 Wait until the status for the task is Successful. This step may take several minutes.

After the status is Successful, you can use Cisco DCNM to configure and monitor the discovered devices.

You do not need to save your changes.

Viewing the Status of Device Discovery Tasks

To view the status of device discovery tasks, from the Feature Selector pane, choose **DCNM Server Administration > Device Discovery**.

The tasks, including the task status, appear in the Discovery Tasks area in the Contents pane. For information about the fields that appear, see the "Field Descriptions for Device Discovery" section on page 5-12.

Where to Go Next

View the discovered devices and configure unique device credentials, as needed. For more information, see the "Administering Devices and Credentials" section on page 6-1.

Field Descriptions for Device Discovery

This section includes the following field descriptions for the Device Discovery feature:

Device Discovery Content Pane

Table 5-1 Device Discovery Content Pane

Field	Description
Discovery Setting	
Seed Device	IPv4 address of the first device that you want to discover. Valid entries are in dotted decimal format. By default, this field is blank.
User Name	Name of the device user account that the Cisco DCNM server uses to access the device. The user account must have network-admin or vdc-admin privileges on the device. By default, this field is blank.
Password	Password for the device user account specified in the User Name field. By default, this field is blank.
Maximum Hops of Neighbors to Discover	Largest permissible number of CDP hops between the Cisco DCNM server and the device. If the server connects to the device but exceeds this number of hops, the discovery fails. The default setting is 0 (zero), which disables the discovery of neighboring devices.
Rediscover Configuration and Status for Existing Devices	Whether the discovery task you are configuring is to replace an existing device discovery that has already completed. By default, this check box is unchecked.
Discovery Tasks	
Task ID	*Display only.* Number assigned to the discovery task. The task ID indicates the order in which discovery tasks occurred.
Owner	*Display only.* Cisco DCNM server user account used to start the discovery task.
Seed Device IP Address	*Display only.* IPv4 address of the seed device.
Discovered Time	*Display only.* Date and time of the most recent update to the Status field.
Reason	*Display only.* Why the discovery task was created.
Status	*Display only.* State of the discovery task. Valid values are as follows: • In progress—The discovery tasks are ongoing. • Successful—The discovery task completed without errors. • Failed—The discovery task completed with errors.

Related Fields

For information about fields that configure devices, see the "Administering Devices and Credentials" section on page 6-1.

Device System-Message Logging Level Reference

This section provides information about the minimum device logging-level requirements of Cisco DCNM. Cisco DCNM has logging-level requirements for only a subset of the logging facilities of supported devices. If a Cisco NX-OS logging facility is not specified in this section, then Cisco DCNM does not have a requirement for that logging facility.

Note Cisco DCNM provides automatic device logging-level support. For more information, see the Automatic Logging-Level Configuration Support, page 5-4.

This section provides the following topics that document Cisco DCNM minimum logging levels per supported device type:

- Cisco Nexus 7000 NX-OS Logging Levels per Cisco DCNM Feature, page 5-14
- Cisco Nexus 5000 NX-OS Logging Levels per Cisco DCNM Feature, page 5-15
- Cisco Nexus 4000 NX-OS Logging Levels per Cisco DCNM Feature, page 5-16
- Cisco Nexus 1000V NX-OS Logging Levels per Cisco DCNM Feature, page 5-17

Cisco Nexus 7000 NX-OS Logging Levels per Cisco DCNM Feature

Table 5-2 Cisco Nexus 7000 NX-OS Logging Levels per Cisco DCNM Feature

Cisco DCNM Feature	Cisco Nexus 7000 NX-OS Logging Facility	Enabled by Default?	Logging Facility Keyword	Cisco NX-OS Default Logging Level	Minimum Cisco DCNM-Required Logging Level[1]
AAA	AAA	Yes	aaa	3	**5**
	RADIUS	Yes	radius	3	**5**
	TACACS+	No	tacacs+	3	**5**
Device Discovery	CDP	Yes	cdp	2	**6**
Topology	LLDP	No	lldp	2	**5**
DHCP snooping	DHCP snooping	No	dhcp	2	**6**
Dynamic ARP Inspection					
IP Source Guard					
Dot1X	802.1X	No	dot1x	2	**5**
Ethernet Interfaces	Ethernet port manager	Yes	ethpm	5	5
Traffic Storm Control					
Gateway Load Balancing Protocol (GLBP)	GLBP	No	glbp	3	**6**
Hot Standby Router Protocol (HSRP)	HSRP engine	No	hsrp	3	**6**
Inventory	Module	Yes	module	5	5
	Platform	Yes	platform	5	5
	System manager	Yes	sysmgr	3	3
Object Tracking	Object tracking	Yes	track	3	**6**
Port-Channel Interfaces	Port-channel interfaces	Yes	port-channel	5	**6**
Port security	Port security	No	port-security	2	**5**
SPAN	SPAN	Yes	monitor	3	**6**
Spanning Tree	Spanning tree	Yes	spanning-tree	3	**6**
Unidirectional Link Detection (UDLD)	UDLD	No	udld	5	5
Virtual Device Contexts (VDCs)	VDC manager	Yes	vdc_mgr	6	6
Virtual Port Channel (vPC)	VPC	No	vpc	2	**6**
VLAN Network Interfaces	Interface VLAN	No	interface-vlan	2	**5**

1. Minimum Cisco DCNM logging levels appear in **bold** text for Cisco Nexus 7000 NX-OS logging facilities that have a default logging level that is too low.

Cisco Nexus 5000 NX-OS Logging Levels per Cisco DCNM Feature

Table 5-3 Cisco Nexus 5000 NX-OS Logging Levels per Cisco DCNM Feature

Cisco DCNM Feature	Cisco Nexus 5000 NX-OS Logging Facility	Enabled by Default?	Logging Facility Keyword	Cisco NX-OS Default Logging Level	Minimum Cisco DCNM-Required Logging Level[1]
AAA	AAA	Yes	aaa	3	**5**
	RADIUS	Yes	radius	3	**5**
	TACACS+	No	tacacs+	3	**5**
Device Discovery	CDP	Yes	cdp	2	**6**
Topology	LLDP	No	lldp	2	**5**
Ethernet Interfaces	Ethernet port manager	Yes	ethpm	5	5
Traffic Storm Control					
Fabric Extender	FEX	Yes	fex	5	5
Inventory	System manager	Yes	sysmgr	3	3
	Platform	Yes	pfm	5	5
	NOHMS	Yes	nohms	2	2
Port-Channel Interfaces	Port-channel interfaces	Yes	port-channel	5	**6**
SPAN	SPAN	Yes	monitor	3	**6**
Spanning Tree	Spanning tree	Yes	spanning-tree	3	**6**
Unidirectional Link Detection (UDLD)	UDLD	No	udld	5	5
Virtual Port Channel	VPC	No	vpc	2	**6**
VLAN Network Interfaces	Interface VLAN	No	interface-vlan	2	**5**

1. Minimum Cisco DCNM logging levels appear in **bold** text for Cisco Nexus 5000 NX-OS logging facilities that have a default logging level that is too low.

Cisco Nexus 4000 NX-OS Logging Levels per Cisco DCNM Feature

Table 5-4 Cisco Nexus 4000 NX-OS Logging Levels per Cisco DCNM Feature

Cisco DCNM Feature	Cisco Nexus 4000 NX-OS Logging Facility	Enabled by Default?	Logging Facility Keyword	Cisco NX-OS Default Logging Level	Minimum Cisco DCNM-Required Logging Level[1]
AAA	AAA	Yes	aaa	3	**5**
	RADIUS	Yes	radius	3	**5**
	TACACS+	No	tacacs+	3	**5**
Device Discovery	CDP	Yes	cdp	2	**6**
Topology					
Ethernet Interfaces	Ethernet port manager	Yes	ethpm	5	5
Traffic Storm Control					
FIP Snooping	FIPSM	Yes	fip-snooping	2	**5**
Inventory	System manager	Yes	sysmgr	3	3
Link State Tracking	LST	No	lstsvc	2	**4**
Port-Channel Interfaces	Port-channel interfaces	Yes	port-channel	5	**6**
SPAN	SPAN	Yes	monitor	3	**6**
Spanning Tree	Spanning tree	Yes	spanning-tree	3	**6**
Unidirectional Link Detection (UDLD)	UDLD	No	udld	5	5
VLAN Network Interfaces	Interface VLAN	No	interface-vlan	2	**5**

1. Minimum Cisco DCNM logging levels appear in **bold** text for Cisco Nexus 4000 NX-OS logging facilities that have a default logging level that is too low.

Cisco Nexus 1000V NX-OS Logging Levels per Cisco DCNM Feature

Table 5-5 Cisco Nexus 1000V NX-OS Logging Levels per Cisco DCNM Feature

Cisco DCNM Feature	Cisco Nexus 1000V NX-OS Logging Facility	Enabled by Default?	Logging Facility Keyword	Cisco NX-OS Default Logging Level	Minimum Cisco DCNM-Required Logging Level[1]
AAA	AAA	Yes	aaa	3	**5**
	RADIUS	Yes	radius	3	**5**
	TACACS+	No	tacacs+	3	**5**
Device Discovery Topology	CDP	Yes	cdp	2	**6**
Ethernet Interfaces	Ethernet port manager	Yes	ethpm	5	5
Virtual Ethernet Interfaces	Ifmgr	Yes	ifmgr	5	5
	VIM	Yes	vim	5	5
Inventory	Module	Yes	module	5	5
	Platform	Yes	platform	5	5
	System manager	Yes	sysmgr	3	3
Virtual Switches	MSP	Yes	msp	5	5
Port-Channel Interfaces	Port-channel interfaces	Yes	port-channel	5	**6**
Port Profiles	Port profile	Yes	port-profile	5	5
	VMS	Yes	vms	5	5
SPAN	SPAN	Yes	monitor	3	**6**

1. Minimum Cisco DCNM logging levels appear in **bold** text for Cisco Nexus 1000V NX-OS logging facilities that have a default logging level that is too low.

Additional References for Device Discovery

For additional information related to device discovery, see the following sections:

- Related Documents, page 5-17
- Standards, page 5-18

Related Documents

Related Topic	Document Title
Device and Credentials	Chapter 6, “Administering Devices and Credentials”

Related Topic	Document Title
Network servers	Chapter 9, "Configuring Network Servers"
Cisco NX-OS XML management interface	*Cisco NX-OS XML Management Interface User Guide, Release 5.x*

Standards

Standards	Title
NETCONF protocol over the Secure Shell (SSH)	RFC 4742

Feature History for Device Discovery

Table 5-6 lists the release history for this feature.

Table 5-6 Feature History for Device Discovery

Feature Name	Releases	Feature Information
LLDP discovery	5.0(2)	Support was added for this feature.
Fibre Channel discovery	5.0(2)	Support was added for this feature.
Automatic logging-level configuration support	5.0(2)	Support was added for this feature.