CHAPTER 29

Administering Device Discovery

The Device Discovery feature creates devices in Cisco DCNM by connecting to a Cisco NX-OS device and retrieving the running configuration of the device. Cisco DCNM can also discover Cisco NX-OS devices 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 virtual device context (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.

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

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

Note Staring from Cisco NX-OS Release 5.2.2(a) the Cisco DCNM-LAN supports the discovery of the following modules:

- N7K-F248XP-25 Line Card
- N55-M16FP 16-Port FC GEM
- N7K-C7010-FAB2 Fabric 2 module
- N7K-C7018-FAB2 Fabric 2 module
- N55-D160L3-V2 Daughter Card
- N55-M160L3-V2 Line Card
- N3K-C3048TP-1GE Layer 3 switch
- N3K-C3016Q- 40GE Layer 3 switch

If the device supports virtual device contexts (VDCs), DCNM-LAN retrieves the running configuration of each VDC that is configured on the physical device. DCNM-LAN 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 DCNM-LAN.

When DCNM-LAN 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 Interface User Guide*.

Discovery Protocols

DCNM-LAN 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 DCNM-LAN 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 DCNM-LAN 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 DCNM-LAN to manage the device.

DCNM-LAN supports CDP hops on some Cisco switches that run Cisco IOS software. Although DCNM-LAN 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.

Fibre Channel

To discover network elements in a storage area network (SAN), DCNM-LAN uses Fibre Channel. DCNM-LAN 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

DCNM-LAN 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 DCNM-LAN. 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, DCNM-LAN 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 DCNM-LAN.

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 DCNM-LAN 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 29-7.

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 29-7.

Logging Severity-Level Requirements

DCNM-LAN 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 DCNM-LAN 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 29-5.

Automatic Logging-Level Configuration Support

DCNM-LAN 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 DCNM-LAN 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 29-7.

During Device Discovery

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

At Feature Enablement in the DCNM-LAN Client

If you use the DCNM-LAN client to enable a feature on a device and the default logging level for the feature does not meet the minimum requirement, the DCNM-LAN client warns you that it will configure the logging level on the device to meet the requirement. If you reject the logging level change, DCNM-LAN 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, DCNM-LAN automatically configures the logging level to meet the requirement after DCNM-LAN 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 DCNM-LAN, after DCNM-LAN 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, DCNM-LAN sets logging levels that do not meet the minimum requirements.

VDC Support

When DCNM-LAN discovers a Cisco NX-OS device that supports VDCs, it determines how many VDCs are on the Cisco NX-OS device. In DCNM-LAN, 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 29-6.

Licensing Requirements for Device Discovery

The following table shows the licensing requirements for this feature:

Product	License Requirement
DCNM-LAN	The Device Discovery feature requires no license. Any feature not included in a license package is bundled with the DCNM-LAN 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 DCNM-LAN 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 7.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 29-7.
- For a Cisco Nexus 7000 Series device, each VDC that you want to discover must have a management interface configured. DCNM-LAN 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 DCNM-LAN 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 29-7.
- DCNM-LAN 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 7.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 DCNM-LAN.

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

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

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 DCNM-LAN 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 DCNM-LAN 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 DCNM-LAN required logging levels. To do so, compare the logging levels displayed on page 29-8 to the minimum DCNM-LAN required logging levels that are listed in Table 29-3.

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

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

The *facility* argument is the applicable logging-facility keyword from Table 29-3, and *severity-level* is the applicable minimum DCNM-LAN 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, DCNM-LAN retrieves the running configuration and status information of discovered Cisco NX-OS devices.

You can perform Deep Discovery by selecting one task at a time. You can also select all or multiple devices in a single task at a time.

Note You cannot select multiple tasks or multiple devices across tasks at one instance.

Use this procedure for the following purposes:

- To discover devices that are not currently managed by DCNM-LAN. For example, you should use this procedure when DCNM-LAN 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 DCNM-LAN already has discovered.
- To rediscover the topology when CDP links have changed without rediscovering devices that DCNM-LAN has already discovered.

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

BEFORE YOU BEGIN

Ensure that you have configured the Cisco NX-OS device so that the DCNM-LAN server can connect to it and successfully discover it. For more information, see the *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 5.x* "Verifying the Discovery Readiness of a Cisco NX-OS Device" section on page 29-7.

Determine the IPv4 address of the device that you want DCNM-LAN 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 Click **Here** in the Device Discovery pane to perform Shallow Discovery of the devices in the Cisco DCNM Web Client. The shallow discovery result web page pops out.

There are four types of discovery, they are **Fabric**, **LAN**, **VMWare**, and S**MI-S Storage**.

Step 3 In the first table of **Fabric**, you can **Edit**, **Remove**, **Add**, **Re-discover**, **Refresh** and **Purge unreachable devices or dead link** in selected fabric.

- To edit the fabric— Check the box before the fabric you want to select, and click the **edit** icon as a pencil. You can edit the **Fabric Name**, check/uncheck to use/disuse **SNMPv3/SSH** and select the **Auth-Privacy** from the drop-down list. Enter the **User Name** and **Password** and select the **Status** as **managed**, **unmanaged**, or **managedContinuously**. (Optional)You can click the **options** button to input the **UCS User Name** and the **UCS Password**.
- To remove the fabric— Select the fabric that you want to remove, and click the **remove** icon. Click yes to remove the selected fabric.
- To add a fabric— Click the **add** icon to add a fabric. Enter the information about **Fabric Seed Switch, SNMP, User Name** and **Password**. If you check **Limit Discovery by VSAN**, select which you want to limit by, **Included VSAN List** or **Excluded VSAN List**, and provide the **VSAN List**. Check/uncheck to enable/disable NPV Discovery in All Fabrics. (Optional)Click options buttion to input the **UCS User Name** and the **UCS Password**.
- To re-discover a fabric— Select the fabric that you want to be re-discovered, and click the **Re-discover Fabric** icon. Click yes to perform re-discovery of the fabric.
- To refresh the fabric discovery table— Click the **refresh** icon to manually refresh the discovery table.
- To purge down elements in the fabric— Select the fabric and click the **Purge** icon to purge unreachable devices or dead links in selected Fabric and click yes.
- To maximize the fabric table— Click the **Maximize** icon to maximize the fabric table and click **Normalize** to return the former view.

Step 4 In the second table of **LAN** discovery, you can **Add**, **Refresh**, **Purge unreachable devices or dead links in selected LAN** and **Toggle between Task and Device View**. You can **Edit LAN Task, Re-discover LAN** and **Remove LAN Task/Switch** by clicking the icons before the tasks/switches.

- To **Edit LAN Task**— Click the Edit icon, enter the username of a user account on the device in the **User Name** field. The user account must have a network-admin or vdc-admin role. In the **Password** field, enter the password for the user account. Choose the **Status** of the LAN task. For Catalyst 6500 devices, enter the enable password in the Enable Password field to allow for IOS privileged EXEC mode commands.

- To **Re-discover LAN**— A warning message pops out, click on yes to proceed rediscovery.
- To **Remove LAN Task**— Click on the remove icon and click yes to remove the LAN task.
- To **Add LAN Task**— Choose the **Discovery Type** from **Hops from Seed Switch/Switch List/FWSM**.

  If you choose the discovery type as **Hops from Seed Switch**, input the IP address or IP range string in **Seed Switch**. Drag the triangle to the number which represents the **Max Hops from Seed.** Choose the **Protocol** of the LAN. If you choose **SNMPv1**, select the **Scan Timeout** from the drop-down list and enter the **Community**. If you choose **SNMPv3/CLI**, select the auth-privacy and **Scan Timeout** from the drop-down list. Enter the **User Name** and **Password**. Select the group that you want to add the switch to and click **Next**. **Shallow LAN Discovery** window shows up. Select the switches and click Add to add the LAN task.

  It's quite similar with the other discovery type as **Switch List or FWSM**, only that you don't need to provide the max hops from seed.

Step 5 If there are VMWare and SMI-S storage devices discovered, you can perform similar function in the VMWare and SMI-S Storage discovery table.

Step 6 You can only perform deep discovery in the DCNM LAN client, please follow the steps in Deep Discovery.

Deep Discovery

Deep discovery is an ssh based discovery initiated from the DCNM-LAN client and allows DCNM to actually log in via ssh and configure the LAN devices.

To perform Deep Discovery of the devices so that you can configure LAN devices via DCNM, please follow below steps:

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

Step 2 Click the plus icon to expand the task under **Task based Discovery** pane, a list of devices under the single task shows up.

Step 3 You can either select one device or multiple devices under one task. Right click on the single device or multiple devices under one task and select **Deep Discovery**.

Note Deep Discovery is a requirement for any of the features found in the DCNM LAN client.

Step 4 Click **Refresh** button or press F5, the successfully deep discovered device will show **MANAGED** under **SSH/Telnet** of **Status**.

Step 5 You can also right click the discovered devices and select **Re-do deep discovery**.

Step 6 In the Device Discovery pane, click the **History** button to open the History of Discovery window. You can see **Task ID, Owner, Seed Device IP Address, Discovered Time, Reason** and **Status** history from the window.

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 29-12.

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 30-1.

Field Descriptions for Device Discovery

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

Device Discovery Content Pane

Table 29-1 Shallow Discovery Content Pane

Field	Description
Admin> Data Sources >Fabric	
Fabric Name	Name of the Fabric.
Seed Switch	The IP address of the fabric's seed switch. IPv4 address of the first device that you want to discover. Valid entries are in dotted decimal format.
Status	• managed • unmanaged • managedContinuouly
SNMPv3/SSH	True if the fabric is using SNMPv3/SSH.
User/Cmnty	Name of the device user account/community that the DCNM-LAN server uses to access the device. The user account must have network-admin or vdc-admin privileges on the device.
Auth/Privacy	The authorization method used by the fabric.
Included VSAN List	The IP address of the included VSAN list that the fabric is limited by.
Excluded VSAN List	The IP address of the excluded VSAN list that the fabric is limited by.
Licensed	If the fabric is licensed or not.
Last Updated Time	The last updated time of the fabric.
Admin> Data Sources> LAN	

Table 29-1 Shallow Discovery Content Pane

Field	Description
Discovery Task	The discovery task name of LAN.
Max Hops from Seed	The max hops from seed switch to be discovered.
Switch List	The IP address or string of the switch list.
FWSM IP Address	The FWSM IP address discovered.
Switch	The seed switch of the task.
Managed	True if the LAN discovery task is managed.
SNMP Status	Whether or not the SNMP is enabled.
Last Updated Time	The last updated time of the LAN.
Group	Which of the LAN group does the switches belong to.
SNMPv3/SSH	True if SNMPv3/SSH is used.
User/Cmnty	Name of the device user account that the DCNM-LAN 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.
Auth/Privacy	The authorization method used by the LAN.
Admin> Data Sources> VMWare	
Server	The server name of the VMWare.
Managed	True if the remote device is managed.
Status	The status of the server.
User	Name of the device user account that the DCNM-LAN server uses to access the device. The user account must have network-admin or vdc-admin privileges on the device.
Last Updated Time	The last updated time of the virtual machine.
Admin> Data Sources> SMI-S Storage	
Vendor	The vendor of the storage device.
Version	The version information of the storage device.
Provider URL	The URL of the provider.
Name Space	The name space of the storage.
Interop Name Space	The iinterop name space of the storage.
Port	The port used to access the storage.
Secure	The secure information of the storage.
Status	The status of the storage.
Discovery Status	The discovery status of the storage.
Last Updated Time	The last updated time of the storage.

Table 29-2 Deep Discovery Content Pane

History of Discovery	
Task ID	*Display only.* Number assigned to the discovery task. The task ID indicates the order in which discovery tasks occurred.
Owner	*Display only.* DCNM-LAN 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.
Task Based Discovery	
Name	*Display only.* The name of the task.
Switches	*Display only.* The devices under the single task.
Managed	*Display only.* Show if the task is managed by DCNM.
SNMP	*Display only.* SNMP status can be different as below: • ok—The device is accessible/reachable at current time. • Last Seen—The time when the device was last reachable. **Last Seen** will be in that state for few minutes, after which it will show up as **Discovery Timeout**. • Discovery Timeout—The device is not accessible/reachable because of discovery timeout.
SSH/Telnet	*Display only.* Status of the discovery task. • ENABLE DEEP DISCOVERY— Deep discovery is not enabled. • UNMANAGED (Connection Failure)—Connection to the device by SSH/Telnet failed. • UNMANAGED (Auth Failure)—Authentication of the device failed. • DISCOVERING—The device is in the process of discovering. MANAGED—The device is managed by DCNM.

Related Fields

For information about fields that configure devices, see the "Administering Devices and Credentials" section on page 30-1.

Device System-Message Logging Level Reference

This section provides information about the minimum device logging-level requirements of DCNM-LAN. DCNM-LAN 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, DCNM-LAN does not have a requirement for that logging facility.

Note DCNM-LAN provides automatic device logging-level support. For more information, see the Automatic Logging-Level Configuration Support, page 29-5.

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

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

Table 29-3 Cisco Nexus 7000 NX-OS Logging Levels per Cisco DCNM-LAN Feature

Cisco DCNM-LAN Feature	Cisco Nexus 7000 NX-OS Logging Facility	Enabled by Default?	Logging Facility Keyword	Cisco NX-OS Default Logging Level	Minimum Cisco DCNM-LAN-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**

Table 29-3 Cisco Nexus 7000 NX-OS Logging Levels per Cisco DCNM-LAN Feature (continued)

Cisco DCNM-LAN Feature	Cisco Nexus 7000 NX-OS Logging Facility	Enabled by Default?	Logging Facility Keyword	Cisco NX-OS Default Logging Level	Minimum Cisco DCNM-LAN-Required Logging Level[1]
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-LAN 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 DCNM-LAN Feature

Table 29-4 Cisco Nexus 5000 NX-OS Logging Levels per Cisco DCNM-LAN Feature

Cisco DCNM-LAN Feature	Cisco Nexus 5000 NX-OS Logging Facility	Enabled by Default?	Logging Facility Keyword	Cisco NX-OS Default Logging Level	Minimum Cisco DCNM-LAN-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

Table 29-4 Cisco Nexus 5000 NX-OS Logging Levels per Cisco DCNM-LAN Feature (continued)

Cisco DCNM-LAN Feature	Cisco Nexus 5000 NX-OS Logging Facility	Enabled by Default?	Logging Facility Keyword	Cisco NX-OS Default Logging Level	Minimum Cisco DCNM-LAN-Required Logging Level[1]
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-LAN 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 DCNM-LAN Feature

Table 29-5 Cisco Nexus 4000 NX-OS Logging Levels per Cisco DCNM-LAN Feature

Cisco DCNM-LAN Feature	Cisco Nexus 4000 NX-OS Logging Facility	Enabled by Default?	Logging Facility Keyword	Cisco NX-OS Default Logging Level	Minimum Cisco DCNM-LAN-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-LAN 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 DCNM-LAN Feature

Table 29-6 Cisco Nexus 1000V NX-OS Logging Levels per Cisco DCNM-LAN Feature

Cisco DCNM-LAN Feature	Cisco Nexus 1000V NX-OS Logging Facility	Enabled by Default?	Logging Facility Keyword	Cisco NX-OS Default Logging Level	Minimum Cisco DCNM-LAN-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-LAN 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 29-18
- Standards, page 29-19

Related Documents

Related Topic	Document Title
Device and Credentials	Chapter 30, “Administering Devices and Credentials”
Cisco NX-OS XML management interface	*Cisco NX-OS XML Interface User Guide*

Standards

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

Feature History for Device Discovery

Table 29-7 lists the release history for this feature.

Table 29-7 Feature History for Device Discovery

Feature Name	Releases	Feature Information
Discovery of various supported devices	5.2(2a)	Support was added for this feature.
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.