CHAPTER 12

Updating Device Inventory

Prime Infrastructure provides two ways to discover the devices in your network:

- Quick—Allows you to quickly discover the devices in your network based on the SNMP community string, seed IP address, and subnet mask you specify. Choose **Operate > Discovery**, then click **Quick Discovery**.
- Regular—Allows you to specify protocol, credential and filter settings for discovery and to schedule when to run the discovery job. See Changing Discovery Settings.

Changing Discovery Settings

Step 1 Choose **Operate > Discovery**, then click **Discovery Settings**.

Step 2 Click **New**. Enter the settings as described in Table 12-1.

Step 3 Click:

- **Save** to save the settings
- **Run Now** to save the settings and immediately start the discovery job.

Table 12-1 Discovery Settings

Field	Description
Protocol Settings	
Ping Sweep Module	Gets a list of IP Address ranges from a specified combination of IP address and subnet mask. This module pings each IP Address in the range to check the reachability of devices.
CDP Module	The discovery engine reads the cdpCacheAddress and cdpCacheAddressType MIB objects in cdpCacheTable from CISCO-CDP-MIB on every newly encountered device. 1. Fetch cdpCacheAddress MIB object from the current device. This provides a list of neighbor device addresses. 2. If the neighbor device addresses do not already exist in the global device list, add them to the local cache.
Advanced Protocols	
Routing Table	Queries and analyzes routing tables on seed routers to discover subnets and next-hop routers.
Address Resolution Protocol	The ARP Discovery Module depends on the Routing Table Discovery Module (RTDM), and is executed only when RTDM is processed. This precondition is identified based on the Discovery-module-processed flags, which are part of the DeviceObject. The entries coming out of the ARP Discovery Module need not necessarily pass through RTDM because (per the router Discovery algorithm) active routers are those that RTDM must process and identify. When the ARP table is fetched and the entries are not already discovered by RTDM, then these entries (though they may represent routers) are not active routers and need not be passed on to RTDM. This is ensured by setting the ARP Discovery Module flag to Processed and leaving the RTDM flag set to Unprocessed. When the RTDM comes across an entry with the RTDM flag unset and the ARP flag set, RTDM identifies the entry as a inactive router or other device and it leaves the entry as Unprocessed. The ARP Discovery Module also ignores the entry according to the algorithm, based on the Processed flag set against the ARP Discovery Module. When the ARP Discovery module is selected, the device MAC address needs to be updated in the device information. Applications can retrieve this information in the adapter through the DeviceInfo object. By scanning the device MAC address, the applications can distinguish between Cisco and non-Cisco devices. ARP cache from the device is collected using CidsARPInfoCollector. The MAC ID of the device is retrieved from this data and set in the DeviceInfo object.
Border Gateway Protocol	The BGP Discovery Module uses bgpPeerTable in the BGP4-MIB to find its BGP peer. The table contains its peers' IP addresses, which are added as clues to the local cache.
OSPF	Open Shortest Path First (OSPF) protocol is an interior gateway routing protocol. OSPF discovery uses the ospfNbrTable and ospfVirtNbrTable MIB to find neighbor IP addresses.
Filters	
System Location Filter	Filters the device based on the Sys Location string set on the device during discovery process.
Advanced Filters	
IP Filter	Filters the device based on the IP address string set on the device during discovery process.
System Object ID Filter	Filters the device based on the System Object ID string set on the device during discovery process.

Table 12-1 Discovery Settings (continued)

Field	Description
DNS Filter	Filters the device based on the DNS string set on the device during discovery process.
Credential Settings	
SNMP V2 Credential	SNMP community string is a required parameter to discover devices in the network. You can enter multiple rows of credentials mapped to a specific IP address, or the IP address can be a wild card e.g *.*.*.*, 1.2.3.*.
Telnet Credential	You can specify the telnet credentials during discovery setting creation to collect the device data.
SSH Credential	Prime Infrastructure support SSH V1 and V2. You can configure SSH before running discovery.
SNMP V3 Credential	Prime Infrastructure supports SNMP V3 discovery for devices.
Preferred Management	
IP Method	• Use Loopback • Use SysName • Use DNSReverseLookup

Scheduling Discovery Jobs

To create a discovery job to run at a future time you specify:

Step 1 Choose **Operate > Discovery**, then click **Discovery Settings**.

Step 2 Click **New**.

Step 3 Enter the settings as described in Table 12-1, then click **Save**.

Step 4 In the Discovery Settings window, select the discovery job you just created, then click **Schedule**.

Step 5 Enter the schedule information, then click **Save**.

Monitoring the Discovery Process

To monitor the discovery process:

Step 1 Choose **Operate > Discovery**.

Step 2 Select the discovery job for which you want to see details.

Discovery Protocols and CSV File Formats

Prime Infrastructure uses six protocols to discover devices:

- Ping Sweep
- Cisco Discovery Protocol (CDP)
- Routing Table
- Address Resolution Protocol (ARP)
- Border Gateway Protocol (BGP)
- Open Shortest Path First (OSPF)

You can import a CSV file to add data for the protocols. Table 12-2 describes the CSV file format for each of the protocols.

Note You can import a CSV file if you are using a supported version of Mozilla Firefox only.

Table 12-2 Discovery Protocols and CSV File Formats

Protocol	CSV File Format
Ping sweep	Any valid IP address and subnet mask, separated by a comma. You can specify multiple networks in a single discovery by adding additional rows, for example: 1.1.1.1,255.255.240.0 2.1.1.1,255.255.255.0
Cisco Discovery Protocol (CDP)	Any valid IP address and the hop count, separated by a comma, for example: 1.1.1.1,3 2.2.2.2,5
Routing table	Any valid IP address and the hop count, separated by a comma, for example: 1.1.1.1,3 2.2.2.2,5
Address Resolution Protocol (ARP)	Any valid IP address and the hop count, separated by a comma, for example: 1.1.1.1,3 2.2.2.2,5
Border Gateway Protocol (BGP)	Seed device IP address for any device that is BGP enabled, for example: 1.1.1.1 2.2.2.2 3.3.3.3
Open Shortest Path First (OSPF)	Seed device IP address for any device that is OSPF enabled, for example: 1.1.1.1 2.2.2.2 3.3.3.3

Updating Device Inventory Manually

It is recommended that you run discovery to update your device inventory. However, you can also add devices manually.

To update the device inventory manually:

Step 1 Choose **Operate > Device Work Center**, then click **Add**.

Step 2 Enter the required parameters.

Step 3 Click **Add** to add the device with the settings you specified.

Importing Device Inventory

If you have another management system in which your devices are imported or if you want to import a spreadsheet that contains all your devices and their attributes, you can import device information in bulk into Prime Infrastructure.

To import device inventory:

Step 1 Choose **Operate > Device Work Center**, then click **Bulk**.

Step 2 Click the link to download a sample file that contains all the fields and descriptions for the information that must be contained in your imported file.

Step 3 Click **Browse** to navigate to your file, then click **Import** and wait for the import to complete. (To check the status of the import, choose **Administration > Jobs Dashboard**).

Troubleshooting Unmanaged Devices

Table 12-3 describes the possible reasons a device is unmanageable by Prime Infrastructure:

Table 12-3 Reasons for Unmanageable Device

Possible Cause	Actions
Prime Infrastructure cannot reach the device because the device is down or because any device along the path from the Prime Infrastructure server to the device is down.	• Use the ping and traceroute tools to verify that the Prime Infrastructure can reach the device. See Getting Device Details Using the 360° View for more information. • If the device is reachable, verify that the retry and timeout values set for the device are sufficient. (Chose **Operate > Device Work Center**, select the device, then click **Edit**.) • Verify that SNMP is configured and enabled on the device: – If using SNMPv2, verify that the *read-write* community string configured on the device is the same as that entered in Prime Infrastructure. **Note** The read-write community string is required. – If using SMNPv3, verify that the following parameters are configured on the device, and that the configured parameters on the device match those entered in Prime Infrastructure: Username AuthPriv mode (noAuthNoPriv, authNoPriv, authPriv) Authentication algorithm (for example, MD5, SHA, etc.) and the authentication password Privacy algorithm (for example, AES, DES, etc.) and the privacy password • Verify that the SNMP credentials configured on the device match the SNMP credentials configured in Prime Infrastructure. • Re-enter the SNMP credentials in Prime Infrastructure, then resync the device. (Chose **Operate > Device Work Center**, select the device, then click **Sync**.) See Synchronizing Devices for more information.
Prime Infrastructure cannot gather information from the device because Telnet or SSH is not configured on the device.	• Verify that Telnet or SSH is configured and enabled on the device, and that the same protocol is configured on Prime Infrastructure. (Chose **Operate > Device Work Center**, select the device, then click **Edit**.) **Note** If the device type requires HTTP, verify that the Prime Infrastructure HTTP parameters match those configured on the device. • Verify that the username, Telnet or SSH passwords, and the enable mode password for Cisco IOS devices are configured correctly on the device and that the parameters entered in Prime Infrastructure match those configured on the device. If you did not configure a username on the device for authentication, you can leave this field empty in Prime Infrastructure. • Verify that the authorization level configured for the Telnet/SSH user is not limited to lower enable privilege levels.

Table 12-3 Reasons for Unmanageable Device (continued)

Possible Cause	Actions
Restrictions were placed for SNMP through SNMP views or access lists.	Remove any restrictions for SNMP through SNMP views or access lists.
TACACS+ "per-command authorization" is configured on the devices,	If TACACS+ is configured, verify the permissions for the Telnet/SSH user for the permitted CLI commands. It is recommended that you allow all CLI commands for the Prime Infrastructure user account; or alternatively, exclude only commands that need to be absolutely restricted.

For more information about configuring SNMP, Telnet, and SSH on Cisco IOS devices, see:

- Cisco IOS Software Releases 12.0 T SNMPv3
- Configuring Secure Shell on Routers and Switches Running Cisco IOS

Managing Device Groups

By default, Prime Infrastructure creates rule-based device groups and assigns devices to the appropriate Device Type folder. You cannot edit these device groups. You can view the rules for the device group by resting your cursor on the device group folder.

Device groups are logical groupings of devices. You create device groups to help you more efficiently update and manage your devices. For example, you can create a device group that includes devices that have a particular module. If you later want to configure a feature related specifically to that module, you use the device group you created to push the configuration change to all the devices contained in the group.

You can create a new group which can be one of two types:

- Static—You create and name a new device group to which you can add devices using the **Add to Group** button from **Operate > Device Work Center**.
- Dynamic—You create and name a new device group and specify the rules to which devices must comply in order to be added to this device group. See Creating Dynamic Device Groups for more information.

When you create a device group, you are distinguishing that group of devices from others in your network. For example, if you have devices that reside in different time zones, you can create device groups based on geographic regions so that the devices in one group can have a different time zone setting from the devices in another group.

In smaller deployments where all devices can be configured with the same settings, you may only need to create one general device group. This setup allows you to configure settings for the group, and then apply those settings consistently across all your devices.

Groups not only save you time when configuring multiple devices, but they also ensure that configuration settings are applied consistently across your network.

Note You cannot control which users have access to which device groups. All users can see all device groups. For role-based access control (RBAC), you need to create sites and virtual domains.

Creating device groups is a two-part process:

1. Create a new device group. See Creating Dynamic Device Groups.

2. Assign devices to the device group. See Assigning Devices to a Group.

Related Topic

- Device Accessibility in Parent-Child Device Groups

Device Accessibility in Parent-Child Device Groups

When you create a child group under a parent device group, the devices accessible to the child group depend on the device group you create:

- If the parent and child group are *both dynamic* device groups, the child group can access the devices available in the parent group only.
- If the parent group is *static* device group and the child group is a dynamic group, the child group is not limited to the devices available in the parent group.

In dynamic device groups only, the child group "inherits" its devices from the parent device group.

Related Topics

- Creating Dynamic Device Groups
- Assigning Devices to a Group

Creating Dynamic Device Groups

Before you create a dynamic device group, make sure you understand the unique properties that you want the group to contain. For example, you may want to set up two device groups that have different authentication settings or different time zone settings.

Note While there is no limit on the number of rules you can specify for a dynamic group, as the number of rules increases, the group update performance could become slower.

To create a dynamic device group:

Step 1 Choose **Operate > Device Work Center**.

Step 2 In the Groups menu on the left, click the Settings icon, then click **Create Group**.

Step 3 Enter the group name, group description, and select the parent group if applicable.

Step 4 Uncheck **Save as a Static Group** so you can specify rules to which all devices must comply to be added to the group. You can click **Save as a Static Group** if you want to manually add the devices to the group and not have the group be rule-based.

Step 5 Specify the rules for the devices must match.

Step 6 Click **Save** to add the device group with the settings you specified. The device group you created appears under the User Defined groups.

Assigning Devices to a Group

Step 1 Choose **Operate > Device Work Center**.

Step 2 Select the device you want to assign to a group, then click **Add To Group**.

Step 3 Select the group, then click **Save**.

Synchronizing Devices

You can force an inventory collection in order to sync the Prime Infrastructure database with the configuration currently running on a device.

Step 1 Choose **Operate > Device Work Center**.

Step 2 Select the device whose configuration you want synced with the configuration stored in Prime Infrastructure database.

Step 3 Click **Sync**.