CHAPTER 3

Setting up

After you install Prime NCS (WAN) and launch the browser, read the following sections to learn how to get started using Prime NCS (WAN):

Discovering the Network

To view and manage the devices in your network, Prime NCS (WAN) must first discover the devices and, after obtaining access, collect information about them. Prime NCS (WAN) uses both SNMP and SSH/Telnet to connect to supported devices and collect inventory data.

The following sections describe how to discover your network:

Planning Discovery Runs

Prime NCS (WAN) uses SNMP polling to gather information about your network devices within the range of IP addresses you specify. If you have CDP enabled on your network devices, Prime NCS (WAN) uses the seed device you specify to discover the devices in your network.

Before you run discovery, you must do the following:

1. Configure SNMP Credentials on Devices—Prime NCS (WAN) uses SNMP polling to gather information about your network devices. You must configure SNMP credentials on all devices you want to manage using Prime NCS (WAN).
2. Set Syslog and Trap Destinations on Devices—Specify the Prime NCS (WAN) server (using the Prime NCS (WAN) server IP address and port) as the syslog and trap destination on all devices you want to manage using Prime NCS (WAN).

3. Configure Mail Server Settings—You will then receive email notification when Prime NCS (WAN) has completed discovering the devices in your network.

Configure Mail Server Settings

By configuring mail server settings, you will receive e-mail notification when Prime NCS (WAN) has completed discovering the devices in your network.

Step 1 Choose **Administration > System > Mail Server Configuration**.

Step 2 Enter the hostname of the primary SMTP server.

Step 3 Enter a password for logging in to the SMTP server, and confirm the password.

Step 4 Provide the same information for the secondary SMTP server (if a secondary mail server is available).

By default, the From text box is populated with *NCS@<NCS server IP address>*. You can change it to a different sender.

Step 5 Enter the recipient's e-mail addresses in the To text box.

The e-mail address you provide serves as the default value for other functional areas, such as alarms or reports. You can add multiple e-mail addresses separated by commas.

Note Global changes you make to the recipient e-mail addresses in Step 6 are disregarded if e-mail notifications were set.

Step 6 If you want the e-mail recipient list applied to the existing e-mail notifications, check the **Apply recipient list to existing e-mail notifications** check box.

Step 7 Click **Test** to send a test e-mail to verify that the settings you entered are correct.

Step 8 Click **Save**.

Running Discovery

When you run discovery, Prime NCS (WAN) discovers the devices and, after access is obtained, collects device inventory data.

It is recommended that you run discovery when first getting started with Prime NCS (WAN), as shown in the following steps:

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

Step 2 Click **New**.

Step 3 Enter the Protocol Settings as described in Table 3-1.

Step 4 Do one of the following:

- Click **Save** to save your discovery settings and schedule your discovery to run at a specified time.
- Click **Run Now** to run the discovery now.

Table 3-1 Discovery Protocol 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 as follows: 1. The cdpCacheAddress MIB object is gathered 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, they are added 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 checked, 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 the discovery process.
Advanced Filters	
IP Filter	Filters the device based on the IP address string set on the device during the discovery process.
System Object ID Filter	Filters the device based on the System Object ID string set on the device during the discovery process.

Table 3-1 Discovery Protocol Settings

Field	Description
DNS Filter	Filters the device based on the DNS string set on the device during the discovery process.
Credential Settings	
SNMP V2 Credential	SNMP community string is a required parameter for discovering 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; for example, *.*.*.*, 1.2.3.*.
Telnet Credential	You can specify the Telnet credentials during discovery, setting creation to collect the device data.
SSH Credential	Prime NCS (WAN) support SSH V1 and V2. You can configure SSH before running discovery.
SNMP V3 Credential	Prime NCS (WAN) supports SNMP V3 discovery for devices.

Verifying Discovery

When discovery has completed, you can verify that the process was successful by following these steps:

Step 1 Choose **Operate > Discovery**.

Step 2 Choose the discovery job for which you want to view details.

Step 3 Under Discovery Job Instances, expand the arrow to view details about the devices that were discovered.

If devices are missing:

- Change your discovery settings, then rerun the discovery. See Table 3-1 for information about discovery settings.
- Add devices manually. See Adding Devices Manually for more information.

Adding Devices Manually

You can add devices manually, as shown in the following steps. This is helpful if you want to add a single device. If you want to add all of the devices in your network, it is recommended that you run discovery. (See Verifying Discovery for more information.)

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

Step 2 Enter the parameters.

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

Importing Devices in Bulk

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

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**.

Step 4 To view the status of the import, choose **Tools > Task Manager > Jobs Dashboard**.

Step 5 Click the arrow to expand the job details and view the details and history for the import job.

Setting Up Site Profiles

Site profiles help you manage large campuses by associating network elements to physical locations. Site profiles have a hierarchy that includes campuses and buildings, and allows you to segment the physical structure of your network and monitor your network based on location.

There are two areas in which you can set up and change sites:

- **Operate > Site Profiles & Maps**—Create a new site and change an existing site.
- **Operate > Device Work Center**—If a site has previously been created, you can add devices to a site by clicking **Add to Site** from the Device Work Center.

When you create site profiles, you need to decide how many campuses and buildings to include in your site. Table 3-2 explains how to determine which elements to include in your site profiles.

Table 3-2 Creating Elements in Site Profiles

Create a ...	When you have ...
Campus	More than one business location
Building	More than one location within your campus

To control which users have access to the devices in the sites, you need to create virtual domains. See Setting Up Virtual Domains for more information.

For additional information about sites, see Keeping Sites Organized.

Creating Site Profiles

To create a campus location, add a building to the campus:

Step 1 Choose **Operate > Site Profiles & Maps**.

Step 2 From the command menu, choose **New Campus**, then click **Go**.

Step 3 Enter the necessary parameters, then click **Next**.

Step 4 Change any settings, then click **OK**.

Step 5 Click the campus you just created; then, from the command menu, choose **New Building**, and then click **Go**.

Step 6 Enter the necessary parameters, then click **Save**.

You can now add devices to the site profile as described in Adding Devices to Site Profiles.

Adding Devices to Site Profiles

After you have created site profiles, you can assign devices to those sites. By associating devices with a campus and building, you can simplify maintenance tasks. When you need to perform maintenance tasks on devices, you can choose the site that contains the devices and apply the changes to all devices in the site.

To control which users have access to the devices in the sites, you need to create virtual domains. See Setting Up Virtual Domains for more information.

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

Step 2 Choose the devices you want to add to a site, then click the **>>** icon and click **Add to Site**.

Step 3 Choose the campus and building to which to assign the device, then click **Add**.

Note The Campus and Building fields are populated with the settings you previously entered in **Operate > Site Profiles & Maps**. See Creating Site Profiles for more information.

Setting Up Port Monitoring

To monitor your device ports, you can create a port group and then display monitoring information on the Prime NCS (WAN) dashboard.

Port Groups

Port groups are logical groupings of interfaces that allow you to monitor device ports by the function they serve. For example, you can create a port group for the WAN ports and create another port group for the internal distribution ports on the same router.

After you create port groups, you can more efficiently configure all the devices belonging to a port group.

You need to determine which types of ports you want to monitor as a group. The following port groups are typical of most networks:

- Port Type
- User Defined
- WAN Interfaces

Monitoring Templates

Monitoring templates monitor device features, usage, health, and other factors. After you create and deploy monitoring templates, Prime NCS (WAN) collects and processes data from specified devices and displays the information in dashboards, dashlets, and reports.

Setting Up WAN Interface Monitoring

You create a WAN interface port group in order to efficiently configure settings on all the WAN interfaces in a specific port group.

The following steps show you how to create a port group for the WAN interfaces for an edge router, create and deploy a WAN interface health monitoring template on those ports, and then view the results.

Step 1 Choose **Operate > Port Grouping**.

Step 2 Choose the device IP address(es) to add to the WAN interfaces port group, then click **Add to Group**.

Step 3 From the Select Group drop-down menu, choose **WAN Interfaces**, then click **Save**.

Now that you have designated the WAN interfaces, you need to create a WAN interface health monitoring template.

Step 4 Choose **Design > Monitoring**.

Step 5 Choose **Features > Metrics > Interface Health**.

Step 6 Enter the parameters for the interface health template. It is recommended that you check all parameters to be monitored for WAN interfaces.

Step 7 Click **Save as New Template**.

Now that you have created a WAN interface health monitoring template, you need to activate and deploy the template.

Step 8 Choose **Deploy > Monitoring Tasks**.

Step 9 Choose the template you created, then click **Activate**. Click **OK** to confirm.

Step 10 Choose the template you created, then click **Deploy**.

Step 11 Choose Port Groups, then click WAN Interfaces, then click **Submit**.

Now that you have deployed the template, you can view the monitoring results.

Step 12 Choose **Operate > Overview**. The Top N Interfaces by WAN Utilization dashboard is populated with the parameters you specified to monitor for the WAN interfaces.

Related Topic

- Updating Port Groups

Setting Up Virtual Domains

Virtual domains allow you to control who has access to specific sites and devices. After you add devices to Prime NCS (WAN), you can configure virtual domains. Virtual domains are logical groupings of devices and are used to control who can administer the group. By creating virtual domains, an

administrator allows users to view information relevant to them specifically and restricts their access to other areas. Virtual domain filters allow users to configure devices, view alarms, and generate reports for their assigned part of the network *only*.

Virtual domains can be based on physical sites, device types, user communities, or any other designation you choose.

Before you set up virtual domains, you should determine which users should have access to which sites and devices in your network.

Creating a Site-Oriented Virtual Domain

By default, there is only one virtual domain defined (*root*) in Prime NCS (WAN).

When you create a site-oriented virtual domain, you allows users to view information in a specific site and restrict their access to other areas.

The following steps explain how to choose a segment of all the devices at a particular location and make them part of the "Site 1 Routers" virtual domain.

Step 1 Choose **Administration > Virtual Domains**.

Step 2 From the left Virtual Domain Hierarchy sidebar menu, click **New**.

Note By default, only one virtual domain (*root*) is defined in Prime NCS (WAN). The selected virtual domain becomes the parent virtual domain of the newly created, subvirtual domain.

Step 3 Enter **Site 1 Routers** for the virtual domain name, then click **Submit**.

Step 4 On the Sites tab, move the sites that you want to associate with the virtual domain to the Selected Sites column, then click **Submit**.

Step 5 Click **OK** on the confirmation screens.

Assigning Users to a Virtual Domain

After you create a virtual domain, you can associate the virtual domain with specific users. This allows users to view information relevant to them specifically and restricts their access to other areas. Users assigned to a virtual domain can configure devices, view alarms, and generate reports for their assigned virtual domain *only*.

The following steps walk you through creating a user who is in charge of the Site 1 Routers virtual domain you previously created.

Step 1 Choose **Administration > Users, Roles, & AAA**.

Step 2 Click the username that you want to assign to a virtual domain.

Step 3 Click the Virtual Domains tab, then move the specific virtual domain from the Available list to the Selected list.

Step 4 Click **Submit**.

Note When using external AAA, be sure to add the custom attributes for virtual domains to the appropriate user or group configuration on the external AAA server.

Related Topic

- Controlling User Access

Next Steps

Now that you have completed the basic setup steps, you might want to do the following tasks:

Table 3-3 Next Steps after Completing Setup Tasks

Task	GUI Path	Documentation Reference
Set up additional users	**Administration > Users, Roles & AAA**, then click **Users**	Controlling User Access
Add additional virtual domains	**Administration > Virtual Domains**	Setting Up Virtual Domains
Refine your sites	**Operate > Site Profiles & Maps**	Keeping Sites Organized
Create additional port groups and change existing port groups	**Operate > Port Grouping**	Changing Port Groups
Start monitoring and responding to alarms	**Operate > Alarms & Events**	Monitoring Alarms