Cisco Prime Network Control System (WAN) 1.1 User Guide

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-26217-01

Cisco Prime Network Control System (WAN) 1.1 User Guide

CONTENTS

Preface

This guide describes how to administer and use Cisco Prime Network Control System (WAN).

Audience

This guide is for administrators who configure, monitor, and maintain networks, and who troubleshoot network problems.

Organization

This guide includes the following sections:

Part	Title	Description
1	Getting Started	Describes: • Prime NCS (WAN) key features. • Various elements of the Prime NCS (WAN) user interface. • Setting up Prime NCS (WAN).
2	Using Templates for Configuring and Monitoring	Explains how to use design and deploy configuration and monitoring templates.
3	Operating the Network	Explains how to: • Monitor the network • Maintain and update the device configuration inventory. • Maintain device configurations and software images
4	Administering	Explains how to monitor and maintain Prime NCS (WAN) and control user access.

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands, keywords, and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string, or the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*.

Tip Means *the following information will help you solve a problem.*

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning **Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.**

Related Documentation

You can access the entire documentation set for Prime NCS (WAN) at:

http://www.cisco.com/en/US/partner/products/ps11687/tsd_products_support_series_home.html

Note We sometimes update the documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

PART 1

Getting Started

This part contains the following sections:

CHAPTER 1

Introduction

The Cisco Prime Network Control System (WAN), or Prime NCS (WAN), is a Cisco LAN Solution network management tool that adds to the capabilities of the Web User Interface and the command-line interface (CLI). Prime NCS (WAN) provides network administrators with a single solution for policy provisioning, network optimization, troubleshooting, security monitoring, and wired LAN systems management. Robust graphical interfaces make wired LAN deployment and operations simple and cost-effective.

Supported Browsers

Prime NCS (WAN) is supported on the following browsers:

- Microsoft Internet Explorer 8.0 with the Flash and Chrome plugins.
- Mozilla Firefox 7.0

Prime NCS (WAN) requires Adobe Flash Player version 11.0.1.152.

Note You are strongly advised not to enable third-party browser extensions. In Internet Explorer, you can disable third-party browser extensions by choosing **Tools > Internet Options** and unchecking the Enable third-party browser extensions check box on the Advanced tab.

Understanding Prime NCS (WAN)

The Prime NCS (WAN) web interface is organized into a lifecycle workflow that includes the following high-level task areas described in Table 1-1.

Table 1-1 Prime NCS (WAN) Task Areas

Task Area	Description	Used By
Design	Design feature or device patterns, or *templates*. You create reusable design patterns, such as configuration templates, in the Design area. You may use predefined templates or create your own. Patterns and templates are used in the deployment phase of the lifecycle.	Network Engineers, Designers, and Architects
Deploy	Deploy previously defined designs, or *templates*, into your network. You specify how to deploy features, using templates created in the design phase. The deploy phase allows you to push configurations defined in your templates to one or many devices.	NOC Operators and Service Operators
Operate	Monitor your network on a daily basis and perform other day-to-day or ad hoc operations related to network device inventory and configuration management. The Operate tab contains dashboards, the Device Work Center, and the tools you need for day-to-day monitoring, troubleshooting, maintenance, and operations.	Network Engineers, NOC Operators, and Service Operators
Administration	Specify system configuration settings and data collection settings, and manage access control.	Network Engineers
Tools	The following are available: • Prime NCS (WAN) provides reports that you can use to monitor system and network health and to troubleshoot problems. • The Prime NCS (WAN) Task Manager provides status information and scheduling capabilities for jobs, and information about background tasks.	All users

Understanding Licenses

Prime NCS (WAN) licensing is based on the number of network devices that you want Prime NCS (WAN) to manage. A Prime NCS (WAN) device license provides full access to all Prime NCS (WAN) features to enable you to manage a set number of devices. You purchase a single base license, and then purchase add-on licenses as necessary to accommodate additional devices.

Prime NCS (WAN) is deployed through virtual appliances. You use the standard License Center GUI to add new licenses, which are locked by the standard Cisco Virtual Unique Device Identifier (VUDI).

The Prime NCS (WAN) License is recognized by the SKU, which is usually attached to every purchase order to clearly identify which software or package was purchased.

You can view your licenses in the Licensing Center by choosing **Administration > Licenses**.

See Managing and Updating Product Licenses for more information.

Device Count Licenses

Prime NCS (WAN) uses a single-tier licensing structure that includes all features and functionality in one tier. Part numbers are purchased based on the number of devices to be managed. Part numbers are available to support 50, 100, 500, 1000, 2500, 5000, or 10000 devices. See Managing and Updating Product Licenses for additional information.

CHAPTER 2

Working with the User Interface

Prime NCS (WAN) is a web-based application. Tabs on the user interface are either specific to a particular Cisco Prime product or can be shared across multiple Cisco Prime products. The options on application tabs are displayed when you rest your cursor on the tab.

Not all tabs or options are activated if any of your installed Cisco Prime products are not enabled through licensing.

This chapter contains the following sections:

Understanding Interface Components

The following sections provide details on the Prime NCS (WAN) user interface components that are visible on most of the pages:

Global Toolbars

Prime NCS (WAN) contains static global toolbars at the top-right of the page (see Figure 2-1):

Figure 2-1 Global Toolbar—Top-right

- **Login name**—Indicates your current login name. Click the arrow to change your user preferences, change your password, or log out.
- **Search**—See Searching for Devices or SSIDs for more information.

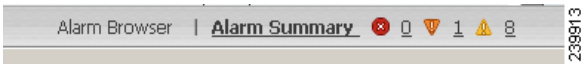
- **Refresh**—Refreshes the current active page.
- **Help**—Launches Prime NCS (WAN) online help.
- **Settings**—Allows you to specify settings for the current active page. Click the down triangle to view available options. The triangle icon does not appear on pages for which you cannot change settings.

The global toolbar on the bottom-left of the page includes:

- **Tools**—Contains links to:
  - Reports: Report Launchpad, scheduled run results, and saved report templates
  - Task Manager: Jobs dashboard, background tasks
  - Packet Capture
- **Help**—Launches online help, the feedback form, and About Prime NCS (WAN)

Prime NCS (WAN) contains the following static global toolbar at the bottom-right of the page (see Figure 2-2):

Figure 2-2 Global Toolbar—Bottom-right



- **Alarm Browser**—Launches the alarm browser within the active page (bottom half of the page).
- **Alarm Summary**—Launches the alarm summary window, displaying all critical, major, and minor alarms.
- **Critical, Major, and Minor**—Launches the alarm browser, listing the devices or sessions that contain the alarms.

Filters

You can use the Filter feature to display specific information on the Prime NCS (WAN) interface. The Filter icon is provided wherever the data is displayed in a tabular format. The following types of filters are available:

- Quick Filter
- Advanced Filter

Quick Filter

This filter allows you to narrow down the data inside a table by applying a filter to a specific table column or columns. To apply different operators, use the Advanced Filter option.

To launch the quick filter, choose **Quick Filter** from the Filter drop-down menu.

To clear the Quick Filter, click the **Filter** button.

Advanced Filter

This filter allows you to narrow down the data in a table by applying a filter using multiple operators such as Does not contain, Does not equal, Ends with, Is empty, and so on. For example, you can choose the filter pattern by table column names and operator from the drop-down menu. In addition, you must enter filter criteria based on the data available in the Prime NCS (WAN) database.

To launch advance filtering, choose **Advanced Filter** from the Filter drop-down list.

Figure 2-3 Advance Filter

To save the filter criteria used in the Advance filter (see Figure 2-3):

1. Enter the advance filter criteria, then click **Go**.

   The data is filtered based on the filter criteria.
2. Click the **Save** icon.

   The Save Preset Filter window appears.
3. Enter a name for the preset filter and click **Save**.

Common Tasks

You can perform the following actions from nearly any Prime NCS (WAN) screen:

- Changing Your Password
- Changing Your Active Domain
- Monitoring Alarms
- Using 360° View
- Launching Help

Changing Your Password

Step 1 Click the down arrow next to your username (at the top-right of the screen, to the left of the search box) and choose **Change Password**.

Step 2 Click the information icon to review the password policy.

Step 3 Enter a new password as directed.

Step 4 Click **Save**.

Changing Your Active Domain

Step 1 Rest your cursor on the Virtual Domain and click the icon that appears to the right.

Step 2 Choose a domain from the list of domains of which you are a member.

Monitoring Alarms

At the bottom of the window, rest your cursor on Alarm Summary or Alarm Browser to get information on the latest active alarms.

Using 360° View

The 360° view provides detailed device information including device status, interface status, and associated device information. You can see the 360° view from nearly all screens in which device IP addresses are displayed.

To launch the 360° view of any device, rest your cursor on a device IP address, then click the icon that appears.

Note The features that appear on the 360° view differ depending on the device type.

Table 2-1 360° Features

360° View Feature	Description
Device status	Indicates whether the device is reachable, is being managed, and is synchronized with the Prime NCS (WAN) database.
Tool icons	Allow you to launch the Alarm Browser, ping the device, and run traceroute on the device.
Modules tab	Lists the device modules and their name, type, state, and ports.
Alarms tab	Lists alarms on the device, including the alarm status, time stamp, and category.
Interfaces tab	Lists the device interfaces and the top three applications for each interface.
Neighbors	Lists the device neighbors, including their index, port, duplex status, and sysname.

Launching Help

You can access online help by:

- Clicking the question mark icon at the top right of any Prime NCS (WAN) screen.
- Choosing **Help > Online Help** from the Help menu at the bottom-left of any Prime NCS (WAN) screen.

Common Tasks For Dashboards

Dashboards display at-a-glance views of the most important data in your network. A quick scan of a dashboard should let you know if anything needs attention. Dashboards generally provide status and alerts, monitoring, and reporting information. Dashboards contain dashlets with visual displays such as tables and charts.

See Configuring Dashboards for more information.

Configuring Dashboards

Dashboards contains dashlets with visual displays such as tables and charts. Click the Settings icon to change the dashboards.

Note After upgrading, the arrangement of dashlets in the previous version is maintained. Therefore, dashlets or features added in a new release are not displayed. Click the Settings icon, then choose **Manage Dashboards** to display new dashlets.

Adding Dashboards

Step 1 Click the **Settings** icon, then choose **Add New Dashboard**.

Step 2 Enter a name for the new dashboard, then click **Add**.

Step 3 Choose the new dashboard and add dashlets to it. See Working with Dashlets for more information.

Restoring Default Dashboards

Step 1 From the Home page, click the **Edit Dashboard** icon.

Step 2 Click **Manage Dashboards**.

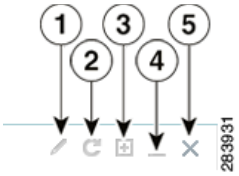
Step 3 Choose a dashboard from the list.

Step 4 Click **Reset**.

Working with Dashlets

Dashboards contains dashlets with visual displays such as tables and charts. Rest your cursor on any dashlet, and the icons shown in Figure 2-4 appear at the top-right corner of the dashboard.

Figure 2-4 Dashlet Icons



1	Click to change the dashlet title, refresh the dashlet, or change the dashlet refresh interval. (To disable refresh, uncheck Refresh Dashlet.)
2	Refresh the dashlet.
3	Maximize the dashlet. If you maximize the dashlet, a restore icon appears allowing you to restore the dashlet to its default size.
4	Collapse the dashlet so that only its title appears. If you collapse the dashlet, an expand icon appears.
5	Remove the dashlet.

Searching for Devices or SSIDs

Prime NCS (WAN) provides the following methods for searching for devices or SSIDs:

- Using Quick Search
- Using Advanced Search

You can access the search options from any page within Prime NCS (WAN).

Using Quick Search

For a quick search, enter a partial or complete IP address or name.

Note You can also enter a username if you are searching for a client.

To quickly search for a device, follow these steps:

Step 1 In the Search text box, enter the complete or partial IP address, device name, SSID, or MAC address of the device for which you are searching.

Step 2 Click **Search** to display all devices that match the Quick Search parameter.

The search results display the matching item type, the number of items that match your search parameter, and links to the list of matching results.

Step 3 Click **View List** to view the matching devices from the Monitor or Configuration page.

Using Advanced Search

To perform a more specific search for a device in Prime NCS (WAN), follow these steps:

Step 1 Click **Advanced Search** from the search menu.

Step 2 In the New Search dialog box, choose a category from the Search Category drop-down list.

Step 3 Choose all applicable filters or parameters for your search.

Note Search parameters change depending on the category you selected.

Step 4 To save this search, check the **Save Search** check box and enter a unique name for the search in the text box.

Step 5 Click **Go**.

Running Saved Searches

Note Saved searches apply only to the current partition.

To access and run a previously saved search, follow these steps:

Step 1 Click **Saved Search**.

Step 2 Choose a category from the Search Category drop-down list.

Step 3 Choose a saved search from the Saved Search List drop-down list.

Step 4 If necessary, change the current parameters for the saved search.

Step 5 Click **Go**.

Monitoring Background Tasks

A background task is a scheduled program running in the background with no visible pages or other user interfaces. In Prime NCS (WAN), background tasks can be anything from data collection to backing up configurations. You can monitor background tasks to see which background tasks are running, check their schedules, and find out whether the task was successfully completed.

Step 1 Choose **Tools > Task Manager > Background Tasks** to view scheduled tasks. The Background Tasks page appears.

Step 2 Choose a command from the drop-down list:

- **Execute Now**—Run all of the data sets with a checked check box.
- **Enable Tasks**—Enable the data set to run on its scheduled interval.

– **Disable Tasks**—Prevent the data set from running on its scheduled interval.

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

PART 2

Using Templates for Configuring and Monitoring

This part contains the following sections:

CHAPTER 4

Designing and Deploying Templates for Configuring

You use templates to define device parameters and settings, which you can later deploy to a specified number of devices based on device type. Templates enhance productivity when you are implementing new services or a new site. Altering configurations across a large number of devices can be tedious and time-consuming, and templates save you time by applying the necessary configurations and by ensuring consistency across devices.

Table 4-1 describes the process for creating and deploying templates.

Table 4-1 Process for Using Configuration Templates

Task	Additional Information
1. Create a template.	Under the **Design** menu, choose which type of template to create.
2. Publish the template.	After you have created the template, click the **Publish** icon to publish the template and make it available to be deployed.
3. Deploy the template.	Under the **Deploy** menu, choose which template to deploy.
4. Verify the status of the template deployment.	Choose **Tools > Task Manager > Jobs Dashboard** to verify the status of the template deployment.

This chapter contains the following sections:

About Templates for Branch Design and Deployment

When you have a site, office, or branch that uses a similar set of devices and configurations, you can use configuration templates to build a generic configuration that you can apply to one more or more devices in the branch. You can also use configuration templates when you have a new branch and want to quickly and accurately set up common configurations on the devices in the branch.

What Is Deploying a Branch?

Deploying a branch is creating the minimum configurations for the branch router. Prime NCS (WAN) allows you to create a set of required features that include:

- Feature templates for the Ethernet interface
- Feature templates for the routing configuration
- CLI template for additional features you require

All of the templates you create can then be added to a single *composite template*, which aggregates all the individual feature templates you need for the branch router. You can then use this composite template when you perform branch deployment operations and to replicate the configurations at other branches.

When you have a set of similar devices across a branch, you can deploy a composite template that includes “golden” configurations to simplify deployment and ensure consistency across your device configurations. You can also use the composite template to compare against an existing device configuration to determine if there are mismatches.

Related Topics

- Creating Configuration Templates for Branch Deployment, page 4-2
- Creating and Deploying Composite Templates for Branch Deployment, page 4-4

Creating Configuration Templates for Branch Deployment

The following sections explain how to create and deploy configuration templates that are commonly used in branch deployments:

- Creating an Ethernet Interface Configuration Template
- Creating an EIGRP Routing Configuration Template
- Creating a RIP Routing Configuration Template
- Creating a CLI Configuration Template

Creating an Ethernet Interface Configuration Template

Many branch deployments require an Ethernet interface configuration template, which you then include in the composite template for branch deployments.

To create an Ethernet interface configuration template:

Step 1 Choose **Design > Configuration Templates**.

Step 2 Under the Features and Technologies folder, expand **Interfaces**, then click **Ethernet Interfaces**.

Step 3 Enter the basic template information.

Step 4 From the Device Type drop-down list, choose **Routers**.

Step 5 Under Template Detail, click **Add Row** in the Ethernet Interfaces table.

Step 6 Complete the fields for an Ethernet interface that is configured on the device. (If, for example, you enter "GigabitEthernet0/1" in the Interface field, the GigabitEthernet0/1 interface must be physically present on the device.)

Step 7 In the IP Address field, enter a valid IP and mask configuration; for example, 192.168.1.1 255.255.255.0.

Step 8 Click **Save**.

Step 9 Click **Save as New Template**.

Creating an EIGRP Routing Configuration Template

Many branch deployments require an EIGRP routing configuration template, which you then include in the composite template for branch deployments.

To create an EIGRP routing configuration template:

Step 1 Choose **Design > *Templates* > Configuration**.

Step 2 Under the Features and Technologies folder, expand **Routing**, then click **EIGRP**.

Step 3 Enter the basic template information.

Step 4 From the Device Type drop-down list, choose **Routers**.

Step 5 Under Template Detail, click **Add Row** in the EIGRP Routes table.

Step 6 Enter an Autonomous System (AS) Number and a passive interface such as FastEthernet0/0, and choose a value for Auto Summary.

Step 7 Click **Save**.

Step 8 Click **Save as New Template**.

Creating a RIP Routing Configuration Template

Many branch deployments require a RIP routing configuration template, which you then include in the composite template for branch deployments.

To create a RIP routing configuration template:

Step 1 Choose **Design > *Templates* > Configuration**.

Step 2 Under the Features and Technologies folder, expand **Routing**, then click **RIP**.

Step 3 Enter the basic template information.

Step 4 From the Device Type drop-down list, choose **Routers**.

Step 5 Under Template Detail, click **Enable RIP**.

Step 6 Choose a RIP version.

Step 7 Under Advanced Configuration, choose:

- **IP Network List**—Enter network IP addresses, such as 10.10.10.10.
- **Passive Interfaces**—Enter a passive interface, such as **FastEthernet0/0**.

Step 8 Click **Save**.

Step 9 Click **Save as New Template**.

Creating a CLI Configuration Template

Many branch deployments require a CLI configuration template, which you then include in the composite template for branch deployments.

To create a CLI configuration template:

Step 1 Choose **Design > *Templates*** **> Configuration**.

Step 2 Under the Features and Technologies folder, expand **CLI Template**s, then click **CLI**.

Step 3 Enter the basic template information.

Step 4 From the Device Type drop-down list, choose **Routers**.

Step 5 Under Template Detail, click the **CLI Content** tab, and then enter the following text:

```
banner motd #Welcome to Prime NCS#
```

Step 6 Click **Save**.

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

Creating and Deploying Composite Templates for Branch Deployment

You create a composite template if you have a collection of existing feature or CLI templates that you want to apply collectively to devices. You specify the order in which the templates contained in the composite template are applied to devices.

If you have multiple similar devices replicated across a branch, you can create and deploy a “master” composite template to all the devices in the branch. This master composite template can also be used later when you create new branches.

Step 1 Choose **Design > Templates > Configuration**, then click C**omposite Template**.

Step 2 Enter parameters for the composite template.

Step 3 From the Validation Criteria drop-down list, choose the devices to which all of the templates contained in the composite template apply. For example, if in your composite template you have a template that applies to Cisco 7200 Series routers and another that applies to all routers, choose the Cisco 7200 Series routers in the Device Type drop-down menu.

Note If a device type is grayed out, the template cannot be applied on that device type.

Step 4 Under Template Details, choose the templates to include in the composite template.

Step 5 Using the arrows, put the templates in the composite into the order in which they should be deployed to the devices. For example, to create an ACL and associate it with an interface, put the ACL template first, followed by the interface template.

Step 6 Click **Save as New Template**.

Step 7 Navigate to the My Templates folder and choose the template you just saved.

Step 8 Click the **Publish** icon to publish the template so it can be deployed.

Step 9 Click the **Go to Deployment** icon and go to the **Deploy > Configuration Tasks** page.

Step 10 Click **Deploy** on the template you published.

Step 11 Specify the deployment options as explained in Specifying Template Deployment Options.

Step 12 Click **OK**.

Step 13 Choose **Tools > Task Manager > Jobs Dashboard** to verify the status of a template deployment.

Creating Configuration Templates

Prime NCS (WAN) provides the following types of configuration templates:

- CLI templates—User-defined templates that are created based on your own parameters. CLI templates allow you to choose the elements in the configurations. Prime NCS (WAN) provides variables that you replace with actual values and logic statements. You can also import templates from Cisco Prime LAN Management System. See Creating and Deploying CLI Templates.
- Feature and technology templates—Configurations that are specific to a feature or technology in a device's configuration. See Creating and Deploying Feature and Technology Templates.
- Composite templates—Two or more feature or CLI templates grouped together into one template. You specify the order in which the templates contained in the composite template are deployed to devices. See Creating and Deploying Composite Templates for Branch Deployment.

Note All templates must be *published* before they can be deployed to devices.

You use templates to define device parameters and settings, which you can later deploy to a specified number of devices based on device type. Altering configurations across a large number of devices can be tedious and time-consuming, and templates save you time by applying the necessary configurations and ensuring consistency across devices.

Default Configuration Templates

Prime NCS (WAN) ships with default configuration templates that you can find under **Design > Configuration Templates > My Templates > OOTB**. These templates are described in Table 4-2.

Table 4-2 Prime NCS (WAN)-Provided Configuration Templates

Use This Configuration Template ...	To Do This...
Medianet – PerfMon	Configure performance monitoring for Medianet.
PA with WAAS	Configure Cisco Performance Agent[1] and Wide Area Application Services (WAAS).
PA without WAAS	Configure Cisco Performance Agent without WAAS.
Collecting Traffic Statistics	Collect network traffic statistics.

1. Cisco Performance Agent is a licensed feature of Cisco IOS Software. It offers comprehensive application performance and network usage data to help network administrators accurately assess user experience and optimize the use of network resources.

Prerequisites for Creating CLI Templates

Creating CLI templates is an advanced function that should be done by expert users. Before you create a CLI template, you should:

- Have expert knowledge and understanding of the CLI and be able to write the CLI in Apache VTL. For more information about Apache Velocity Template Language, see http://velocity.apache.org.
- Understand to what devices the CLI you create can be applied.
- Understand the data types supported by Prime NCS (WAN).
- Understand and be able to manually label configurations in the template.

Creating and Deploying CLI Templates

Before creating a CLI template, make sure you have satisfied the prerequisites as described in Prerequisites for Creating CLI Templates.

Step 1 Choose **Design > Configuration Templates**.

Step 2 Expand the **CLI Template folder**, then click **CLI**.

Step 3 Enter the basic template information.

Step 4 From the Validation Criteria drop-down list, choose the device types to which this CLI template can be applied.

The Device Type field lists product types, product families, and model numbers.

Step 5 Under Template Detail, click **Manage Variables**.

This allows you to specify a variable for which you will define a value when you deploy the template.

Step 6 Click **Add Row** and enter the parameters for a new variable, then click **Save**.

Step 7 Enter the CLI information.

Note In the CLI field, you must enter code using Apache VTL.

Step 8 To view a list of all variables used in the template, click **Form View** (this is a read-only view), then click **Manage Variables** to change the variables.

Step 9 Click **Save As New Template**.

Step 10 Navigate to the My Templates folder and choose the template you just saved.

Step 11 Click the **Publish** icon at the top-right corner, then click **OK**.

Step 12 Click the **Go to Deployment** icon and go to the **Deploy > Configuration tasks** page.

Step 13 Click **Deploy** on the template you published.

Step 14 Specify the deployment options as explained in Specifying Template Deployment Options.

Step 15 Click **OK**.

Understanding Database Variables in CLI Templates

When a device is discovered and added to Prime NCS (WAN), you can use the database values that were gathered during the inventory collection to create CLI templates. For example, if you want to create and deploy a CLI template to shut down all interfaces in a branch, you can create a CLI template that contains the following commands:

```
#foreach ($interfaceName in $interfaceNameList)
interface $interfaceName \n
shutdown
#end
```

where *$interfaceNameList* is the database variable type whose value will be retrieved from the database. *$interfaceNameList* has a default value of `Inventory::EthernetProtocolEndpoint.IntfName`.

To populate *interfaceNameList* with the value from the database, you must create a properties file to capture the query string as described below and save it in the /opt/CSCOlumos/conf/ifm/template/InventoryTagsInTemplate folder.

Sample Property File

Filename: interface.properties

```
# for interface name tag->Name
EthernetProtocolEndpoint.IntfName=select u.name from EthernetProtocolEndpoint u where
u.owningEntityId =
# say for other attributes of EthernetProtocolEndpoint Model, should we define tags
# any good generic way of accepting tags -attr+its mapped query ?
```

After you create the CLI template and the property file and deploy the CLI template, the following CLI is configured on the devices. This output assumes the device has two interfaces (Gigabitethernet0/1 and Gigabitethernet0/0):

```
interface GigabitEthernet0/0
shutdown
interface GigabitEthernet0/1
shutdown
```

Note *InterfaceNameList* is a Prime NCS (WAN) default database variable.

Verify that the Enterprise JavaBeans Query Language (EJB QL) specified in the properties file returns a list of strings; or, if a single element is specified, the EJB QL should return a list containing one element.

Specifying Template Deployment Options

After you publish a template and want to deploy it to one or many devices, you can specify devices, values, and scheduling information to tailor your deployment. Table 4-3 explains the deployment options.

Table 4-3 Deploy > Configuration Task Options

Option	Description
Device Selection	Displays the list of devices to which you want to deploy the template.
Value Assignment	Allows you to specify a variable other than what was previously defined in the configuration template. Click a name, and the previously defined variables are displayed. To change any of the values, click the variable you want to change, enter a new value, and click **Apply**. **Note** The changes you make apply only to the specific configuration you are deploying. To change the configuration template for *all* future deployments, choose **Design > Configuration Templates** and change the template.
Schedule	Allows you to create a meaningful deployment job name, then specify whether to run the job now or in the future.
Summary	Summarizes your deployment option selections.

Creating Feature and Technology Templates

Feature and technology templates are templates that are based on device configuration. Feature and technology templates focus on specific features or technologies in a device's configuration. When you add a device to Prime NCS (WAN), Prime NCS (WAN) gathers the device configuration for the model you added.

Note Prime NCS (WAN) does not support every configurable option for all device types. If Prime NCS (WAN) does not have a feature and technology template for the specific feature or parameter you want configure, create a CLI template as described in Creating and Deploying CLI Templates.

Creating and Deploying Feature and Technology Templates

You create feature and technology templates to simplify the deployment of configuration changes. For example, you can create an SNMP feature and technology template and then quickly deploy it to the devices you specify. You can also add one or more feature and technology templates to a composite template. If you do, when you update the SNMP template, the composite template in which the SNMP template is contained automatically has your latest changes.

Step 1 Choose **Design > Configuration Templates**.

Step 2 Expand the **Features and Technologies** folder, choose an appropriate subfolder, then choose a template type to create.

Step 3 Enter the basic template information.

Step 4 From the Validation Criteria drop-down list, choose the device types to which this feature template can be applied. The Device Type field lists product types, product families, and model numbers.

Note If you are creating a feature template that applies only to a particular device type, the Device Type field lists only the applicable device type, and you cannot change the selection.

Step 5 Under Template Detail, enter the CLI information.

Step 6 Click **Save As New Template**.

Step 7 Navigate to the My Templates folder and choose the template you just saved.

Step 8 Click the **Publish** icon to publish the template so it can be deployed.

Step 9 Click the **Go to Deployment** icon and go to the **Deploy > Configuration Tasks** page.

Step 10 Click **Deploy** on the template you published.

Step 11 Specify the deployment options as explained in Specifying Template Deployment Options.

Step 12 Click **OK**.

Creating and Deploying a Static Routing Template

You can use a template to configure a static route. Static routes can be overwhelming in a large or complicated network. By creating a static routing template, you can avoid making manual changes each time there is a change in the network.

To create and deploy a static routing template:

Step 1 Choose **Design > Configuration Templates**.

Step 2 Expand the **Features and Technologies** folder, expand the **Routing** subfolder, then click **Static**.

Step 3 Enter the basic template information.

Step 4 Under Template Detail, click **Add Row**, then complete the fields.

Note For Permanent Route, choose

- **True** to specify that the route will not be removed from the routing table, even if the next-hop interface shuts down or next-hop IP address is not reachable.
- **False** to specify that the route will be removed from the routing table, even if the next-hop interface shuts down or next-hop IP address is not reachable.

Step 5 Click **Save As New Template**.

Step 6 Navigate to the My Templates folder and choose the template you just saved.

Step 7 Click the **Publish** icon to publish the template so it can be deployed.

Step 8 Click the **Go to Deployment** icon and go to the **Deploy > Configuration Tasks** page.

Step 9 Click **Deploy** on the template you published.

Step 10 Specify the deployment options as explained in Specifying Template Deployment Options.

Step 11 Click **OK**.

Creating and Deploying an ACL Template

To create and deploy a template to configure access lists:

Step 1 Choose **Design > Configuration Templates**.

Step 2 Expand the Features and Technologies folder, expand the Security subfolder, then click ACL.

Step 3 Enter the basic template information.

Step 4 Under Template Detail, click **Add Row**, then complete the fields described in Table 4-4.

Table 4-4 ACL Template Details

Field	Description
Name/Number	Name or number of the ACL.
Applied To	Enter the interface of the router on which to apply the ACL. It is recommended that you apply the ACL on the interface closest to the source of the traffic.
Type	Choose: **Standard**—Standard IP ACLs control traffic based on the source IP address. **Extended**—Extended IP ACLs identify traffic based on source IP address, source port, destination IP address, and destination port.
Description	Description of the ACL.

Step 5 Click **Save As New Template**.

Step 6 Navigate to the My Templates folder and choose the template you just saved.

Step 7 Click the **Publish** icon to publish the template so it can be deployed.

Step 8 Click the **Go to Deployment** icon and go to the **Deploy > Configuration Tasks** page.

Step 9 Click **Deploy** on the template you published.

Step 10 Specify the deployment options as explained in Specifying Template Deployment Options.

Step 11 Click **OK**.

Creating Security Configuration Templates

You can create security configuration templates for the following features:

- Dynamic Multipoint VPN (DMVPN)
- Group Encrypted Transport VPN (GETVPN)

Creating a DMVPN Template

To create a DMVPN template, follow these steps:

Step 1 Choose **Design > Configuration > Features and Technologies > Security > DMVPN**.

The Dynamic Multipoint VPN Configuration Template page opens.

Step 2 In the Template Basic section, enter a name and a description in the appropriate fields.

Step 3 From the Validation Criteria drop-down list, choose a device type from the drop-down list and enter the OS version.

Step 4 In the Template Detail section, enter the IKE Authentication and Encryption policy.

Step 5 In the IKE Authentication Type field, click the anchored plus button (**+**), and choose the IKE authentication type.

If you choose the default Pre-Shared key, you must provide the secret key and reconfirm it. If you choose the Digital Certificate as the authentication type, the router must have a digital certificate issued by a Certificate Authority to authenticate itself.

Step 6 In the IKE Authentication Policy section, click the **Add Row** button to add the IKE policies

Step 7 Enter the priority, and choose Authentication, Diffie-Hellman (D-H) Group, Encryption, Hash, and Lifetime from the drop-down list.

To delete the IKE policies, choose the policy and click **Delete**.

To edit the parameters of the IKE policy, click a row or field and edit its parameters.

Step 8 Click **Save** to save the configuration.

Step 9 In the Encryption policy field, click the anchored plus button (**+**) to add the Transform Set Profile.

Step 10 In the Transform Set Profile dialog box, enter a name and choose the acceptable combination of security protocols and algorithm from the drop-down list to configure the transform set.

Step 11 Enable IP compression and choose a mode for the transform set.

Step 12 To delete the transfer set, choose the transfer set and click **Delete**. To edit the parameters of the transfer set, click a row or field and edit its parameters.

Step 13 Click **Save** to save the configuration.

Step 14 In the Topology and Routing Information section, choose the topology and the device role. For the Routing Protocol, choose the Extended Interior Gateway Routing Protocol (EIGRP) or Routing Information Protocol Version 2 (RIPv2). Use the Other option to configure other protocols.

Note The routing information are disabled when you select Hub as the device role.

Step 15 Enter the required information in the NHRP and Tunnel Parameters section.

Step 16 In the NHS Server Information section, add the Next Hub server information, including the IP Address of Hub's physical interface and the IP address of Hub's tunnel interface.

Note If you check the Cluster Support check box, add the information, such as Cluster ID, Max Connection, and Next Hub Server. The template with the NHS cluster configuration will be applied only to the device running Cisco IOS Software version 15.1(2)T or later.

Step 17 Click **Save As New Template**.

The new template appears in the My Templates folder.

Step 18 Click the **Publish** icon to publish the template so it can be deployed.

Note After you create the template, publish it to make it available for deployment.

For a list and descriptions of elements on the Dynamic Multipoint VPN Template page, see Table 4-5.

Table 4-5 Dynamic Multipoint VPN Template Page

Element	Field Description
Template Basic tab	
Name	Enter a name for the DMVPN template.
Description	(Optional) Enter a description for the DMVPN template.
Validation Criteria tab	
Device Type	Choose the device type from the drop-down list.
OS Version	Enter the OS version for the device.
IPsec Information	
Authentication Type	Click the Preshared Keys or Digital Certificates radio button. • Preshared Keys—Allow for a secret key to be shared between two peers and to be used by IKE during the authentication phase. • Digital Certificates—Authentication method in which RSA key pairs are used to sign and encrypt IKE key management messages. Certificates provide nonrepudiation of communication between two peers, meaning that it can be proven that the communication actually took place.
Priority	The priority value of the IKE proposal. The priority value determines the order of the IKE proposals compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your first priority policy, the device tries to use the parameters defined in the policy with the next lowest priority number. Valid values range from 1 to 10000. The lower the number, the higher the priority. If you leave this field blank, Security Manager assigns the lowest unassigned value starting with 1, followed by 5, and continuing in increments of 5.
Authenticate	Choose the authentication type from the drop-down list.

Table 4-5 Dynamic Multipoint VPN Template Page

Element	Field Description
Diffie-Hellman Group	The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Options are: 1—Diffie-Hellman Group 1 (768-bit modulus). 2—Diffie-Hellman Group 2 (1024-bit modulus). 5—Diffie-Hellman Group 5 (1536-bit modulus, considered good protection for 128-bit keys, but group 14 is better). If you are using AES encryption, use this group (or higher). The ASA supports this group as the highest group.
Encryption policy	Choose the encryption policy from the drop-down list. Choose the encryption algorithm from the drop-down list. The encryption algorithm used to establish the Phase 1 SA for protecting phase 2 negotiations: AES-128—Encrypts according to the Advanced Encryption Standard using 128-bit keys. AES-192—Encrypts according to the Advanced Encryption Standard using 192-bit keys. AES-256—Encrypts according to the Advanced Encryption Standard using 256-bit keys. DES—Encrypts according to the Data Encryption Standard using 56-bit keys. 3DES—Encrypts three times using 56-bit keys. 3DES is more secure than DES, but requires more processing for encryption and decryption. It is less secure than AES. A 3DES license is required to use this option.
Hash	The hash algorithm used in the IKE proposal. The hash algorithm creates a message digest, which is used to ensure message integrity. Options are: • SHA (Secure Hash Algorithm)—Produces a 160-bit digest. SHA is more resistant to brute-force attacks than MD5. • MD5 (Message Digest 5)—Produces a 128-bit digest. MD5 uses less processing time than SHA.
Lifetime	The lifetime of the SA, in seconds. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes. You can specify a value from 60 to 2147483647 seconds. The default is 86400.
Transform Set	
Name	Enter the transform set name. The transform set encrypts the traffic on the tunnel.
ESP Encryption Algorithm	The algorithm used to encrypt the payload. Choose the encryption algorithm from the drop-down list. The options are: • ESP with the 128-bit Advanced Encryption Standard (AES) encryption algorithm. • ESP with the 192-bit AES encryption algorithm. • ESP with the 256-bit AES encryption algorithm. • ESP with the 168-bit DES encryption algorithm (3DES or Triple DES). • Null encryption algorithm.

Table 4-5 Dynamic Multipoint VPN Template Page

Element	Field Description
ESP Integrity Algorithm	The algorithm used to check the integrity of the payload. Choose the integrity algorithm from the drop-down list. The options are: • ESP with the MD5 (HMAC variant) authentication algorithm. • ESP with the SHA (HMAC variant) authentication algorithm.
AH Integrity	Choose the AH integrity from the drop-down list. The options are: • AH with the MD5 (Message Digest 5) (a Hash-based Message Authentication Code [HMAC] variant) authentication algorithm. • AH with the SHA (Secure Hash Algorithm) (an HMAC variant) authentication algorithm.
Compression	Enable the IP compression to compress payload. IP compression with the Lempel-Ziv-Stac (LZS) algorithm.
Mode	Choose the mode to transport the traffic.
Device Role and Topology	
Spoke radio button	Check the Spoke radio button to configure the router as a Spoke in the topology.
Hub radio button	Check the Hub radio button to configure the router as a Hub in the topology.
Dynamic Connection between Spokes	Check the Create Dynamic Connection between spokes check box to configure the dynamic connection between spokes.
EIGRP	Choose the routing information.
RIPV2	Choose the routing information.
Other	Check the **Other** check box to select other routing protocol.
NHRP and Tunnel Parameters	
Network ID	Enter the NHRP Network ID.The network ID is a globally unique, 32-bit network identifier from a nonbroadcast multiaccess (NBMA) network. The range is from 1 to 4294967295.
Hold Time	Enter the number of seconds that the Next Hop Resolution Protocol (NHRP) NBMA addresses should be advertised as valid. The default value is 7200 seconds.
Tunnel Key	Enter the tunnel key. The tunnel key is used to enable a key ID for a particular tunnel interface. The range is from 0 to 4294967295.
NHRP Authentication String	Enter the Authentication String.
IP MTU	Enter the MTU size of IP packets that are sent on a particular interface. The default value for Ethernet and the serial interface is 1500. The default value varies depending upon the media type.
TCP Maximum Segment Size	Enter the TCP maximum segment size. The range is from 500 to 1460.
Physical Interface	Enter the physical interface.
NHS Fallback Time	(Optional) Enter the NHS fallback time in seconds. The range is from 0 to 60.
NHS Server	
Cluster ID	Enter the cluster value to form a group having one or more hubs. The range is from 0 to 10.
Max Connections	Enter the maximum number of connections that can be active in a particular group/cluster.

Table 4-5 Dynamic Multipoint VPN Template Page

Element	Field Description
Priority	The priority of the particular hub in a cluster. Depends on the priority of the spoke router that will form a tunnel with the hub devices.
Next Hop server	Enter the IP address of the next-hop server.
Hub's Physical IP Address	Enter the IP address of the hub's physical interface.

Deploying DMVPN Templates

To deploy the DMVPN template, follow these steps.

Note You must publish the specified template before it can be deployed to devices.

Step 1 Choose **Deploy > Configuration Tasks > My Templates**.

Step 2 On the My Templates page, select the DMVPN template, and click the **Tasked View** button.

Step 3 From the Deploy Task pad, click **Deploy**.

The Template Deployment page opens.

Step 4 From the device selection section, select the list of devices on which to deploy the template.

Step 5 In the Value Assignment section, click the radio button to select the device.

Step 6 For DMVPN, you can change the values for GRE IP Address, Subnet Mask, and Tunnel Throughput Delay.

Step 7 If you have changed the values, click **Apply**. For elements on the page, see Table 4-5.

Note The spoke option for Cisco IOS Software version 15.1(2)T or later should display the NHS cluster configuration section.

Step 8 In the Schedule section, enter the Job Name, then click one of the following radio buttons:

- **Run**—To run the job immediately.
- **Run at Schedule Time**—To specify a time to run the job.

Step 9 Under Summary, verify your entries, then click **OK**.

Creating a GET VPN Group Member Template

To create a GETVPN group member template:

Step 1 Choose **Design > Configuration > Features and Technology > Security > GETVPN-GroupMember**.

The GETVPN-GroupMember Configuration Template page appears.

Step 2 In the Template Basic section, enter a name, description, and author name in the appropriate fields.

Step 3 From the Validation Criteria drop-down list, choose a device type from the drop-down list and enter the OS version.

Step 4 In the Group Information section, enter the group name and the group ID.

Step 5 Click the **IKE Authentication Policy +** button to add the IKE authentication information.

Step 6 In the IKE Authentication Policy dialog box, click the **Pre-Shared key** or **Digital Certificate** radio button.

The key server authenticates by using the digital certificate. The router must have a digital certificate issued by a Certificate Authority to authenticate itself.

Step 7 In the IKE Policy section, click **Add Row and** add the IKE policies, then click **Save**. Click on the **Row** or **Field** to edit the parameters. Select the IKE policies from the list and click **Delete** to delete the IKE policies.

Step 8 Enter the registration interface for the group member.

Step 9 In the Traffic Detail section, enter the Local Exception ACL and the Fail Close ACL.

Step 10 In the Key Servers section, enter the Primary Key Servers and Secondary Key Servers IP addresses/Hostname.

Step 11 Click **Add Row** or **Delete** to add or delete the secondary key server. If you want to edit the secondary key server, click on the **Row** or **Field** and edit the IP address of the key server.

Step 12 In the Migration section, check the Enable Passive SA check box to enable passive SA. Use this option to turn on the Passive SA mode on this group member.

For a list and description of elements on the GETVPN Group Member template page, see Table 4-6.

Note After you create the template, publish it to make it available for deployment.

Step 13 Click **Save As New Template**.

The template you created appears under My Templates.

Step 14 Click the **Publish** icon to publish the template so it can be deployed.

Table 4-6 GETVPN Group Member Template Page

Element	Field Description
Template Basic tab	
Name	Enter a name for the GETVPN group.
Description	(Optional) Enter a description for the GETVPN template.
Author	(Optional) Enter the author name.
Validation Criteria tab	
Device Type	Choose a device type from the drop-down list.
OS Version	Enter the OS version for the device type.
Template Detail	
Group Name	Enter the group name for the GETVPN group member template.
Group ID	Enter a unique identity for the GETVPN group member. This can be a number or an IP address. The range is from 0 to 2147483647.

Table 4-6 GETVPN Group Member Template Page

Element	Field Description
IKE Authentication Policy	
Authorization Type	Click the Preshared Keys or Digital Certificates radio button: • Preshared Keys—Preshared keys allow for a secret key to be shared between two peers and to be used by IKE during the authentication phase. • Digital Certificates—An authentication method in which RSA key pairs are used to sign and encrypt IKE key management messages. Certificates provide nonrepudiation of communication between two peers, meaning that it can be proven that the communication actually took place.
Priority	The priority value of the IKE proposal. The priority value determines the order of the IKE proposals compared by the two negotiating peers when attempting to find a common SA. If the remote IPsec peer does not support the parameters selected in your first priority policy, the device tries to use the parameters defined in the policy with the next lowest priority number. Valid values range from 1 to 10000. The lower the number, the higher the priority.
Encryption	Choose the encryption algorithm from the drop-down box.The encryption algorithm is used to establish the Phase 1 SA for protecting Phase 2 negotiations: • AES-128—Encrypts according to the Advanced Encryption Standard using 128-bit keys. • AES-192—Encrypts according to the Advanced Encryption Standard using 192-bit keys. • AES-256—Encrypts according to the Advanced Encryption Standard using 256-bit keys. • DES—Encrypts according to the Data Encryption Standard using 56-bit keys. • 3DES—Encrypts three times using 56-bit keys. 3DES is more secure than DES, but requires more processing for encryption and decryption. It is less secure than AES. A 3DES license is required to use this option.
Hash	The hash algorithm used in the IKE proposal. The hash algorithm creates a message digest, which is used to ensure message integrity. Options are: • SHA (Secure Hash Algorithm)—Produces a 160-bit digest. SHA is more resistant to brute-force attacks than MD5. • MD5 (Message Digest 5)—Produces a 128-bit digest. MD5 uses less processing time than SHA.
Diffie-Hellman Group	The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Options are: • 1—Diffie-Hellman Group 1 (768-bit modulus). • 2—Diffie-Hellman Group 2 (1024-bit modulus). • 5—Diffie-Hellman Group 5 (1536-bit modulus, considered good protection for 128-bit keys, but group 14 is better). If you are using AES encryption, use this group (or higher). The ASA supports this group as the highest group.

Table 4-6 GETVPN Group Member Template Page

Element	Field Description
Lifetime	The lifetime of the SA, in seconds. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes. You can specify a value from 60 to 2147483647 seconds. The default is 86400.
Registration Interface	Enter the interface to which the crypto map needs to be associated.
Traffic Details	
Local Exception ACL	Choose an ACL for the traffic that must be excluded from the encryption.
Fail Close ACL	Choose an ACL for the traffic that must be sent in clear text until the group member registers with the key server. If the Fail Close feature is configured, all the traffic passing through the group member will be dropped until the group member is registered successfully. Once the group member registers successfully and SAs are downloaded, this feature turns off by itself.
Key Server Information	
Primary Key Server	Specify the primary key server IP address to which the client connects. The primary key server is responsible for creating and distributing group policies to all group members and periodically synchronizing with the secondary key servers. The server with the highest priority is elected as a primary key server.
Secondary Key Server	Specify the secondary key server IP address to which the group member falls back when the primary key server registration fails. A group member can be configured to register to any available key server from a list of all secondary key servers. Group member configuration determines the registration order. The key server defined first is contacted first, followed by the second defined key server, and so on. You can have a maximum of eight key servers for a group member.
Migration	
Enable Passive SA	The Passive SA mode overrides the receive-only SA option on the key server and encrypts all outbound traffic. Use this option to turn on the Passive SA mode on the group member.

Creating a GET VPN Key Server Template

Use the GETVPN Key Server template to create the template.

To create a GETVPN Key Server template:

Step 1 Choose **Design > Configuration > Features Technologies > Security > GETVPN-KeyServer**.

The GETVPN-KeyServer Configuration Template page opens.

Step 2 In the Template Basic section, enter a name, description, and author in the appropriate fields.

Step 3 From the Validation Criteria drop-down list, choose a device type from the drop-down list and enter the OS version.

Step 4 In the Group Information section, enter the group name and group ID.

Step 5 Click the **IKE Authentication Policy +** button to add the IKE authentication information. The IKE Authentication Policy dialog box opens.

Step 6 Click the **Pre-Shared key** radio button or the **Digital Certificate** radio button.

Step 7 In the IKE Authentication Policy section, click **Add Row** to add the IKE policies.

Step 8 In the IKE Policy section, click **Add Row** and add the IKE policies. Click on the **Row** or **Field** to edit the parameters. Select the IKE policies from the list and click **Delete** to delete the IKE policies.

Step 9 Enter the WAN IP address of the device and check the Dead Peer Detection (DPD) check box to enable DPD on all key servers, to effectively keep track of the states of other key servers.

Step 10 In the Key Server Profile section, select the Rekey tab, and choose the Distribution method from the drop-down list. Enter the required information in the Rekey section.

Step 11 To encrypt rekey messages, use the RSA key. You can either select the existing RSA key from the drop-down list or click the **+** button to create a new RSA key.

Step 12 To generate an RSA key, provide the key label and modulus. Check the **Exportable** key check box, if you want to export the certificate.

Step 13 In the Add KeyServer dialog box, select the GETVPN Traffic tab, and enter the traffic to be encrypted, the encryption policy, and anti-replay.

Step 14 Choose the Rekey Encryption algorithm from the drop-down list to encrypt the rekey.

Step 15 In the Key Server Profile page, click the GETVPN Traffic tab.

Step 16 In the GETVPN Traffic dialog box, enter the Traffic to be encrypted, the encryption policy, and anti-replay.

Step 17 Click the **Encryption Policy +** button to add the transform sets that are to be part of this encryption policy.

Step 18 In the Migration section, check the **Enable Receive Only SA Feature** to send traffic in clear text to all group members. This feature can decrypt any arriving encrypted traffic.

Note After you create the template, publish it to make it available for deployment.

Step 19 Click **Save As New Template**.

The template you created appears under My Templates.

Step 20 Click the **Publish** icon to publish the template so it can be deployed.

For a list and descriptions of elements on the GETVPN Key Server template page, see Table 4-7.

Table 4-7 GETVPN Key Server Template Page

Element	Description
Template Basic tab	
Name	Enter a name for the GETVPN group.
Description	(Optional) Enter a description for the GETVPN template.
Author	(Optional) Enter the author name.
Validation Criteria tab	
Device Type	Choose a device type from the drop-down list.
OS Version	Enter the OS version.

Table 4-7 GETVPN Key Server Template Page (continued)

Element	Description
Template Detail	
Group Name	Enter the group name for the template.
Group ID	Enter a unique identity for the GETVPN group. This can be a number or an IP address. The range is from 0 to 2147483647.
WAN IP Address	Enter the WAN IP address.
IKE Authentication Policy	
Authorization type	Click the **Pre-shared key** or **Digital Certificates** radio button. This is for initial IKE authorization between the key servers and group members.
Priority	The priority value of the IKE proposal. The priority value determines the order of the IKE proposals compared by the two negotiating peers when attempting to find a common SA. If the remote IPsec peer does not support the parameters selected in your first priority policy, the device tries to use the parameters defined in the policy with the next lowest priority number. Valid values range from 1 to 10000. The lower the number, the higher the priority.
Encryption	Choose an encryption algorithm from the drop-down list.The encryption algorithm is used to establish the Phase 1 SA for protecting Phase 2 negotiations. • AES-128—Encrypts according to the Advanced Encryption Standard using 128-bit keys. • AES-192—Encrypts according to the Advanced Encryption Standard using 192-bit keys. • AES-256—Encrypts according to the Advanced Encryption Standard using 256-bit keys. • DES—Encrypts according to the Data Encryption Standard using 56-bit keys. • 3DES—Encrypts three times using 56-bit keys. 3DES is more secure than DES, but requires more processing for encryption and decryption. It is less secure than AES. A 3DES license is required to use this option.
Hash	The hash algorithm used in the IKE proposal. The hash algorithm creates a message digest, which is used to ensure message integrity. Options are: • SHA (Secure Hash Algorithm)—Produces a 160-bit digest. SHA is more resistant to brute-force attacks than MD5. • MD5 (Message Digest 5)—Produces a 128-bit digest. MD5 uses less processing time than SHA.
Diffie-Hellman Group	The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Options are: 1—Diffie-Hellman Group 1 (768-bit modulus). 2—Diffie-Hellman Group 2 (1024-bit modulus). 5—Diffie-Hellman Group 5 (1536-bit modulus, considered good protection for 128-bit keys, but group 14 is better). If you are using AES encryption, use this group (or higher). The ASA supports this group as the highest group.

Table 4-7 GETVPN Key Server Template Page (continued)

Element	Description
Lifetime	The lifetime of the SA, in seconds. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure the IKE negotiations will be. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes. You can specify a value from 60 to 86400 seconds. The default is 86400.
WAN IP Address	Enter the WAN IP address.
Dead Peer Detection	Check the Dead Peer Detection check box to enable dead peer detection for key servers to effectively keep track of their states.
Accordian Pane	
Distribution Method radio button	Choose a distribution method. The distribution method is used to send the rekey information from key server to group members. The options are Unicast or Multicast.
Multicast IP Address	When you choose Multicast as the distribution method, specify the multicast address to which the rekey must be transmitted.
KEK Lifetime	Enter the KEK lifetime, in seconds.The range is from 120 to 86400.
TEK Lifetime	Enter the TEK lifetime, in seconds. The range is from 120 to 86400.
Retransmit Key	Enter the frequency and duration of the rekey retransmission, in seconds.
RSA Key for Rekey encryption	Enter the details of the RSA key that is used to encrypt the rekey information.
Rekey Encryption Method	Choose the encryption algorithm from the drop-down list. The encryption algorithm is used to encrypt keys. • AES-128—Encrypts according to the Advanced Encryption Standard using 128-bit keys. • AES-192—Encrypts according to the Advanced Encryption Standard using 192-bit keys. • AES-256—Encrypts according to the Advanced Encryption Standard using 256-bit keys. • DES—Encrypts according to the Data Encryption Standard using 56-bit keys. • 3DES—Encrypts three times using 56-bit keys. 3DES is more secure than DES, but requires more processing for encryption and decryption. It is less secure than AES. A 3DES license is required to use this option.
GETVPN Traffic	
Traffic to encrypt	(Optional) Choose an ACL name from the drop-down list that corresponds to the traffic to be encrypted. The access list defines the traffic to be encrypted. Only the traffic that matches the “permit” lines will be encrypted. **Note** Be sure not to encrypt certain traffic that should always be permitted even if the encrypted sessions are not up.
Encryption Policy	Choose the transform sets from the drop-down list that should be used to encrypt the traffic. Add the transform set from the table, which is used to encrypt traffic between the peers. From the drop-down list, choose transform sets for encrypting traffic. From the table, add another transform set for encrypting traffic between peers.
Anti Replay	Choose the time-based or counter-based anti-replay option.

Table 4-7 GETVPN Key Server Template Page (continued)

Element	Description
Migration	
Enable Receive Only SA feature	Check the **Enabling Receive Only SA feature** check box to send the traffic in clear text, while retaining the capability to decrypt any arriving encrypted traffic.

Deploying GETVPN Templates

This task enables you to deploy the GETVPN group member and key server template.

Note Before you can deploy your template to devices, you must publish the template.

To deploy the GETVPN template:

Step 1 Choose **Deploy > Configuration Tasks > My Templates.**

Step 2 On the My Templates page, select the **GETVPN-GroupMember or KeyServer** template, and click the **Tasked View** button.

Step 3 From the Deploy Task Pad, click **Deploy**.

The Template Deployment page opens.

Step 4 From the Device Selection section, select the device and the location.

Step 5 In the Value Assignment section, click the radio button to select the device.

Step 6 For GETVPN-GroupMember, you can change the values for Registration Interface, Enable Passive SA, Local Exception Policy ACL, and Fail Close ACL.

Step 7 For GETVPN Key Server, you can change the values for Keyserver, WAN IP Address, ACL, Priority, and Cooperative servers.

Step 8 If you changed the values, click **Apply**. For elements on the page, refer to Table 4-6 and Table 4-7.

Step 9 Click the Schedule section, enter the Job Name, then click one of the following radio buttons:

- **Run**—To run the job immediately.
- **Run at Schedule Time**—To specify a time to run the job.

Step 10 Under Summary, verify your entries, then click **OK**.

Importing and Deploying a Configuration Template

In addition to creating new configuration templates, you can import configurations from Cisco Prime LAN Management Solution (LMS). If you have “golden” templates in Cisco Prime LMS, you can import those configurations into Prime NCS (WAN) and save them as configuration templates that you can deploy to the devices in your network.

Before you import a configuration, you must first export and save the configuration from Cisco Prime LMS.

Step 1 Choose **Design > Configuration Templates**.

Step 2 Expand the **CLI Template folder**, then choose the **CLI** template.

Step 3 Click the **Import** icon at the top right of the CLI template page.

Step 4 Browse to the configuration .xml file that you previously exported from Cisco Prime LMS, then click **OK**.

Step 5 Navigation to the My Templates folder and choose the configuration you imported.

Step 6 To view the contents of the configuration, click the **CLI Content** tab.

To view the parameters defined in the configuration, click the **Form View** tab. These values are read-only.

To change any of the variables defined in the configuration, click **Manage Variables**.

Step 7 Click the **Publish** icon to publish the template so it can be deployed.

Step 8 Click the **Go to Deployment** icon and go to the **Deploy > Configuration Tasks** page.

Step 9 Click **Deploy** on the template you published.

Step 10 Specify the deployment options as explained in Specifying Template Deployment Options.

Step 11 Click **OK**.

Troubleshooting Template Deployment

The most common reasons that a template might not be deployed are:

- One or more devices are unreachable—Verify that the device credentials are correct; ping the device to verify that it is reachable. (See Using 360° View for more information.)
- A device CLI returned an error because the CLI was incorrect—Verify that the CLI commands contained in the template are correct by running the commands on a test device.

CHAPTER 5

Designing and Deploying Templates for Monitoring

You use monitoring templates to enable Prime NCS (WAN) to monitor network device metrics such as CPU and memory utilization statistics and alert you of changing conditions before any issues can impact operation.

Table 5-1 describes the process for creating and deploying monitoring templates.

Table 5-1 Steps for Using Monitoring Templates

Task	Additional Information
1. Create a template.	Under the **Design** menu, choose which type of template to create.
2. Publish the template.	After you have created the template, click the **Publish** icon to publish the template and make it available to be deployed.
3. Deploy the template.	Under the **Deploy** menu, choose which template to deploy.
4. Verify the status of the template deployment.	Choose **Tools > Task Manager > Jobs Dashboard** to verify the status of the template deployment.

Prime NCS (WAN) provides the following types of monitoring templates:

- Device Health—See Creating and Deploying Health Monitoring Templates, page 5-1.
- Interface Health—See Creating and Deploying Health Monitoring Templates, page 5-1.
- Threshold—See Defining Thresholds, page 7-4.

Creating and Deploying Health Monitoring Templates

You use health monitoring templates to enable Prime NCS (WAN) to monitor network device metrics such as CPU and memory utilization statistics and alert you of changing conditions before the issues impact their operation.

To create a template to monitor overall device health:

Step 1 Choose **Design > Monitoring Templates**.

Step 2 Expand **Features**, then **Metrics**, then click **Device Health** or **Interface Health**.

Step 3 Enter the basic template information.

Step 4 Under Template Content, choose the parameters to monitor. To change a parameter, click the parameter name, description, or polling frequency value and change the field.

Step 5 Click **Save**.

Step 6 Click **Save As New Template**.

Step 7 Navigate to the My Templates folder and choose the template you just saved.

Step 8 Click the **Go to Deployment** icon at the top-right corner.

Step 9 Select the template you created, then click **Deploy**.

Step 10 Choose the devices or device groups on which to deploy the template, then click **Submit**.

Defining Monitoring Thresholds

You use monitoring templates to define thresholds. When the thresholds you specify are reached, Prime NCS (WAN) issues an alarm.

To define thresholds:

Step 1 Choose **Design > Monitoring Templates**.

Step 2 Under Features, choose **Threshold**.

Step 3 Complete the basic template fields.

Step 4 Under Feature Category, choose one of the following metrics:

- Device Health—Allows you to change threshold values for CPU utilization, memory pool utilization, and environment temperature
- Interface Health—Allows you to change threshold values for the number of outbound packets that are discarded.

Step 5 Under Metric Parameters, choose the threshold setting you want to change, then click **Edit Threshold Setting**.

Step 6 Enter a new value and choose the alarm severity for the threshold.

Step 7 Click **Done**.

Step 8 Click **Save as New Template**.

Step 9 Under the My Templates folder, navigate to the template you created and select it.

Step 10 Click **Go to Deployment**.

Step 11 Select the template you created, then click **Deploy**.

Troubleshooting Template Deployment

The most common reasons that a template might not be deployed are:

- One or more devices are unreachable.
- A device CLI returned an error because the CLI was incorrect.

PART 3

Operating the Network

This part contains the following sections:

CHAPTER 6

Operating and Monitoring the Network

Under the Operate tab, Prime NCS (WAN) provides tools to help you monitor your network on a daily basis, as well as perform other day-to-day or ad hoc operations relating to network device inventory and configuration management. The Operate tab contains dashboards, the Device Work Center, and the tools you need for day-to-day monitoring, troubleshooting, maintenance, and operations.

Monitoring Dashlets and Dashboards

Prime NCS (WAN) automatically displays monitoring data in dashboards and dashlets. You can choose one of the following dashboards under **Operate > Monitoring Dashboard** to view summary information:

- Overview—Displays overview information about your network such as device counts, and the top 5 devices by CPU and memory utilization. From the overview dashboard, you can click on device or interface alarms counts to view detailed dashboards and alarms and events in order to help troubleshoot and isolate issues.
- Incidents—Displays a summary of alarms and events for your entire network, for a particular site, or for a particular device. By clicking on an item in the dashboard, you can view details about the alarm or event and troubleshoot the problem.
- Performance—Displays CPU and memory utilization information.
- Detail Dashboards—Displays network health summaries for sites, devices, or interfaces. The detailed dashboards allow you to see congestion in your network and gather detailed site, device, and interface information. For example, you can view detailed dashboards for a particular site to determine which devices have the most alarms, device reachability status for the site, etc.

You can change the information displayed in the dashboards as explained in Common Tasks For Dashboards.

Table 6-1 describes where to find monitoring information in the Prime NCS (WAN) dashboards.

Table 6-1 Finding Monitoring Data

To View this Monitoring Data	Choose this Dashboard
Alarm information	**Operate > Monitoring Dashboard > Incidents**
CPU utilization	**Operate > Monitoring Dashboard > Performance**
Detailed device information	**Operate > Monitoring Dashboard > Detail Dashboards**
Detailed interface information	**Operate > Monitoring Dashboard > Detail Dashboards**

Table 6-1 Finding Monitoring Data

To View this Monitoring Data	Choose this Dashboard
Device reachability status	**Operate > Monitoring Dashboard > Overview**
Event information	**Operate > Monitoring Dashboard > Incidents**
Interface status, availability, and utilization information	**Operate > Monitoring Dashboard > Performance**
Licensing information	**Operate > Monitoring Dashboard > Overview**
Memory utilization	**Operate > Monitoring Dashboard > Performance**
Site information	**Operate > Monitoring Dashboard > Detail Dashboards**
Syslog sender information	**Operate > Monitoring Dashboard > Incidents**
Utilization statistics	**Operate > Monitoring Dashboard > Overview**

Monitoring Jobs

Choose **Tools > Task Manager > Jobs Dashboard** to view the status of jobs and to:

- View all running and completed jobs and corresponding job details
- Filter jobs to view the specific jobs for which you are interested
- View details of the most recently submitted job
- View job execution results
- Modify jobs including deleting, editing, running, canceling, pausing, and resuming jobs

If a job fails, you can get troubleshooting information from the Jobs Dashboard. When you expand a job to view its details, click the History tab, and rest your cursor over the Status field. The results window displays troubleshooting information that can help you determine why the job failed.

Configure Monitoring Settings

You can define how Prime NCS (WAN) monitors the devices and interfaces in your network.

By enabling the Auto Monitoring option, you can have Prime NCS (WAN) monitor the availability, CPU, memory and temperature of all your network devices automatically. By default, Prime NCS (WAN) polls all devices in your network every 15 minutes for device-health data. Most users will want to enable Auto Monitoring.

You may want to avoid enabling Auto Monitoring if you have a very large network or Prime NCS (WAN) deployment, to avoid excessive polling traffic. In this case, you can leave Auto Monitoring disabled, and create one or more device groups containing your business-critical devices only. You may also want to create a version of the default device health monitoring template with a polling frequency appropriate for these devices. When you deploy the default or custom device health monitoring template, you can select to apply it to your business-critical device group only.

You can also enable deduplication, if applicable, for Cisco IOS Netflow and Cisco Prime Assurance. If you have multiple routers and switches that send netflow to the Cisco Prime Assurance server and multiple NAMs that Cisco Prime Assurance retrieves data from, Cisco Prime Assurance could receive the same traffic statistic more than once. You can enable deduplication so that Cisco Prime Assurance doesn't count the same metrics more than once.

Step 1 Choose **Administration > System**, then select **Monitoring Settings**.

Step 2 Check the following options:

- **Auto monitoring** to have Prime NCS (WAN) monitor all devices and interfaces automatically.
- **Enable deduplication** to have Prime NCS (WAN) eliminate redundant data.

What is the Device Work Center?

From **Operate > Device Work Center**, you can view the device inventory and device configuration information. The Device Work Center contains general administrative functions at the top and configuration functions at the bottom as described in Table 6-2.

Table 6-2 Device Work Center Tasks

Task	Description	Location in Operate > Device Work Center
Manage devices	Add, edit, bulk import, and delete devices, and force data collection from devices.	Buttons located at the top of the Device Work Center.
View basic device information and collection status	View basic device information such as reachability status, IP address, device type, and collection status information.	Displayed in the top portion of the Device Work Center. Rest your cursor on the Collection Status cell and click on the icon to view errors related to the inventory collection.
Manage device groups	By default, Prime NCS (WAN) creates dynamic device groups and assigns devices to the appropriate Device Type folder. You can create new device groups that appear under the User Defined folder.	Displayed on the left pane of the Device Work Center. See Using Device Groups for more information about creating and using device groups.
Add devices to sites	After you set up a site profile, you can add devices to the site. **Note** A device can belong to one site only.	**Add to Site** button located at the top of the Device Work Center. See Creating Site Profiles for more information about adding devices to sites.
View device details	View device details such as memory, port, environment, and interface information.	Choose a device in the Device Work Center, then click the **Device Details** tab at the bottom of the screen.
	View device information, status, and associated modules, alarms, neighbors, and interfaces. See Using 360° View for more information.	Rest your cursor on a device IP address and click the icon that appears.
Create and deploy configuration templates	You can create and deploy configuration templates for the selected device. You can also preview the CLI that will be deployed to the device.	Click the **Configuration** tab at the bottom of the Device Work Center.

Table 6-2 Device Work Center Tasks (continued)

Task	Description	Location in Operate > Device Work Center
View device configurations	View archived configurations, schedule configuration rollbacks, and schedule archive collections.	Click the **Configuration Archive** tab at the bottom of the Device Work Center.
View software images	View details about the image on the selected device, the recommended software image for the device, and the latest software image operations for a device.	Click the **Image** tab at the bottom of the Device Work Center.

Configuring Features on a Device

You can create or change the feature configuration for the selected device. The following topics provide more information:

- Application Visibility, page 6-4
- Overview of NAT, page 6-7
- Dynamic Multipoint VPN, page 6-14
- GETVPN, page 6-19
- VPN Components, page 6-25
- Overview of Zones, page 6-34

Application Visibility

The Application Visibility (AV) feature helps in monitoring the traffic sent towards the internet. To configure AV, you need to perform the following:

- Create AV Configuration
- Assign AV policies on interfaces
- Change AV Advanced options

Note The Application Visibility feature is supported on ASR devices from the IOS version 3.5 or later. This feature is not supported on ISR devices. If you make any changes via CLI interface on objects/entities that starts with “EMS_” is unsupported and may cause unexpected behavior.

Configuring AV

The Application Visibility Configuration feature creates the required elements in the device to send the NetFlow messages for Transaction Records and Usage Records. To configure AV, follow these steps.

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

Step 2 Choose the device from the list or click **Add** to create a new device, then configure the device.

Step 3 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector panel, choose **Application Visibility > Configuration**. The AV Configuration page appears.

Step 5 From the AV Configuration page, set the Primary CM IP Address, Secondary CM IP Address, VPN Routing and Forwarding (VRF), and Source IP address.

Step 6 Set the advanced AV parameters. For more information on the Advanced AV parameters, see Changing AV Advanced Options, page 6-6.

Table 6-3 lists the elements on the AV Configuration page.

Table 6-3 Application Visibility Page

Element	Description
Primary CM IP	Enter the IP address of the primary CM.
Secondary CM IP	(Optional) Enter the IP address of the secondary CM.
VRF	The VRF for the primary CM IP, secondary CM IP and source IP. The Global VRF is the default VRF.
Source IP Address	Specifies the IP address for an interface, which will be used as the source for sending FNF messages towards the CM.

Step 7 Click **Save/ Apply** to save the changes in the server.

Managing Interface

To edit the existing AV policy, follow these steps.

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

Step 2 Choose the device from the list or click **Add** to create a new device, then configure the device.

Step 3 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector panel, choose **Application Visibility > Interfaces**.

Step 5 In the Interface page, select one or more interfaces to Enable/Disable AV Records. To enable the AV on the interface, select “Enable”, and then select the record to which you want to send the collector.

a. Usage Records (UR)—Usage Records are records of the different type of applications that run on a specific interface. The operator can use the Usage Records to monitor the bandwidth usage of different applications. The Usage Records can show the application usage over a specific time period, the peak and average usages, and usage for a specific application type. Usage Records perform periodic aggregation of the category information for the interface. (For example, export information for peer-to-peer traffic or email usage).

b. Transaction Records (TR)—A transaction is a set of logical exchanges between endpoints. There is normally one transaction within a flow. The Transaction Record monitors the traffic at transaction levels. These records provide a detailed analysis of the traffic flows. Transaction Records are bound to the input and output directions of the network side interfaces. These Transaction Records allow the system to capture each unidirectional flow once.

Step 6 Click **OK** to deploy the changes to the device.

Changing AV Advanced Options

To change the Application Visibility Advanced options, follow these steps.

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

Step 2 Select the device from the list or click **Add** to create a new device, then configure the device.

Step 3 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector panel, choose **Application Visibility > Configuration**. The AV Configuration page appears.

Step 5 In the AV Configuration page, set the new values for the AV configuration.

Step 6 Click on the title area to view the Advanced Options and Record Advanced Options. To customize the value, check the specific attribute check box and set the new value. To use the system default value, uncheck the check box of the specific attribute.

Step 7 Click **Save / Apply** to save the changes in the server.

Table 6-4 lists the elements on the AV Configuration page.

Table 6-4 Application Visibility Page

Element	Description
Primary CM IP	Enter the IP address of the primary CM.
Secondary CM IP	(Optional) Enter the IP address of the secondary CM.
VRF	The VRF for the primary CM IP, secondary CM IP and source IP. The Global VRF is the default VRF.
Source IP Address	Specifies the IP address for an interface, which will be used as the source for sending FNF messages towards the CM.
Advance Options	
DSCP Value	(Optional) Check the DSCP value check box to set the exporter DSCP service code point value. The range is from 0 to 63.
TTL	(Optional) Check the TTL check box to set the exporter TTL or hop limit. The range is from 1 to 255.
FNF Template Timeout	
Template Data Timeout	Set the template data timeout value in seconds.
Option Interface Timeout	Set the option interface timeout value in seconds.
Attributes Table Timeout	Set the attributes table timeout value in seconds
Attributes Sampler Timeout	Set the attribute sampler timeout value in seconds.
Option Application Timeout	Set the application timeout in seconds.
VRF Table Timeout	Set the VRF table id timeout value in seconds.
NetFlow Usage Records	

Table 6-4 Application Visibility Page

Element	Description
NetFlow Cache Size	Set the maximum flow entries in the Flow Cache.
NetFlow Exporting Interval	Specify the cache flow timeout.
NetFlow Sampled Transaction Records	
NetFlow Cache Size	Set the maximum flow entries in the Flow Cache.
Transaction Sampling	Specify the cache flow timeout.
NBAR Flow Table Size	Define the maximum allowed sessions.

Overview of NAT

The Network Address Translation (NAT) is the process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network. The NAT helps to limit the number of public IP addresses used by an organization or company, for both economy and security purposes.

The NAT feature allows organizations to resolve the problem of IP address depletion when they have existing networks and need to access the Internet. The NAT allows the IP network of an organization to use different IP address space for the outside network. Thus, NAT allows an organization that does not have globally routable addresses to connect to the Internet by translating those addresses into globally routable address space. The NAT also allows a more graceful renumbering strategy for organizations that are changing service providers or voluntarily renumbering into Classless Inter Domain Routing (CIDR) blocks. The NAT is described in RFC 1631.

A router configured with the NAT will have at least one interface to the inside network and one to the outside network. In a typical environment, the NAT is configured at the exit router between a sub domain and a backbone. When a packet leaves the domain, the NAT translates the locally significant source address into a globally unique address. When a packet enters the domain, the NAT translates the globally unique destination address into a local address. If more than one exit point exists, each NAT must have the same translation table. If the NAT cannot allocate an address because it has run out of addresses, it drops the packet and sends an Internet Control Message Protocol (ICMP) host unreachable packet.

For more information on NAT, see
http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_nat/configuration/xe-3s/iadnat-addr-consv.html.

Types of NAT

The NAT operates on a router—Generally connecting only two networks together—and translates your private (inside local) addresses within the internal network, into public (inside global) addresses before any packets are forwarded to another network. This functionality gives you the option to configure the NAT so that it will advertise only a single address for your entire network to the outside world. Doing this effectively hides the internal network from the world, giving you some additional security.

NAT types include:

- Static Address Translation (SAT) —Allows one-to-one mapping between local and global addresses.

- Dynamic Address Translation—Maps unregistered IP addresses to registered IP addresses of out of a pool of registered IP addresses.
- Overloading—A form of dynamic NAT that maps multiple unregistered IP addresses to a single registered IP address (many to one) using different ports. This method is also known as Port Address Translation (PAT). By using PAT (NAT Overload), thousands of users can be connected to the Internet using only one real global IP address.

How to Configure NAT for IP Address Conservation

To configure NAT, perform the following steps:

1. Create the NAT pool (required for Dynamic NAT)
2. Configure the ACL
3. Create the NAT44 rules
4. Assign rules on the interfaces
5. Set up the NAT maximum translation (Optional)

Note The NAT feature is supported on ASR platform from the IOS version 3.5 or later. The NAT feature is supported on ISR platform from the IOS version 12.4(24)T or later. If you make any changes via CLI interface on objects/entities that starts with "EMS_" is unsupported and may cause unexpected behavior.

IP Pools

The IP Pool is a device object that represents IP ranges to be used on the Dynamic NAT. The NAT IP Pools feature allows you to create a new pool that can be used in the Dynamic NAT, change existing the pool, and delete the pool from the device.

Creating, Editing, and Deleting IP Pools

To create, edit, and delete the IP Pools, follow these steps.

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

Step 2 Select the device from the list or click **Add** to create a new device, then configure the device.

Step 3 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector panel, choose **NAT > IP Pools**. The NAT Pools page appears.

Step 5 From this page, click the **Add IP Pool > IP+Prefix** or **IP Range + Prefix** button, and enter the Name, IP Address/Range, Prefix Length, and Description.

Step 6 Click **Ok** to save the configurations.

Table 6-5 lists the elements on the IP Pools page.

Table 6-5 IP Pools Page

Element	Description
Name	Enter the name for the IP Pool. You cannot change the name after creating the pool.
IP Address/Range	Enter a valid IPv4 address. A valid IPv4 address consists of 4 octets separated by a period'.'.
Prefix length	Enter the prefix length.
Description	(Optional) Enter the description for the zone.

Step 7 Click the **Apply** button to deploy the pool to the server data base.

Step 8 To edit the existing IP Pool, in the NAT IP Pools page do the following:

a. Click on the selected IP Pools parameters row, and edit the parameters. or

b. Select the IP Pools, and click the **Edit** button. The selected IP Pools entity opens for editing. You can edit all the parameters except the pool name.

Step 9 Click **Save / Apply** to save the changes in the server.

Step 10 To delete the existing IP Pools, select the IP Pool, and then click the **Delete** button.

Step 11 Click **Ok** on the warning message to delete the IP Pool. The selected IP Pool will be deleted.

NAT44

The NAT44 feature allows the user to create, delete, and change the NAT44 rules.

Creating, Editing, and Deleting NAT44 Rule

This section describes how to create the NAT44 rules.

There are three types of NAT rules:

- Static
- Dynamic
- Dynamic PAT

To create the NAT44 rule, follow these steps.

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

Step 2 Select the device from the list or click **Add** to create a new device, then configure the device.

Step 3 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector left panel, choose **NAT > NAT44**.

Step 5 From the NAT 44 Rule page, click the down arrow icon on the **Add NAT Rule** button.

- Click Static to create Static Rule. For elements on this page, see Table 6-6.
- Click Dynamic to create Dynamic NAT Rule. For elements on this page, see Table 6-7.

- Click Dynamic PAT to create Dynamic PAT Rule. For elements on this page, see Table 6-8.

Table 6-6 lists the elements on the Static Rule page.

Table 6-6 Static Rule Page

Element	Description
Direction	Displays the directions. This release supports only the Inbound to Outbound direction.
VRF	Displays the VRF on which the NAT translation process happens. The default value is default VRF.
Source A	Enter a valid IPv4 address. A valid IPv4 address consists of 4 octets separated by a period '.'. • If the Source A is defined, then the Source B must be defined. • If the Source A is defined, then the Destination A will be **Any** by default.
Destination A	Enter a valid IPv4 address. A valid IPv4 address consists of 4 octets separated by a period'.'. • If the Destination A is defined, then the Destination B must be defined. • If the Destination A is defined, then the Source A will be **Any** by default.
Translation	Displays the static translation type.
Source B	Enter a valid IPv4 address. A valid IPv4 address consists of 4 octets separated by a period '.'. • If the Source B is defined, then the Source A must be defined. • If the Source B is defined, then the Destination B will be **Any** by default.
Destination B	Enter a valid IPv4 address. A valid IPv4 address consists of 4 octets separated by a period '.'. • If the Destination B is defined, then the Destination A must be defined. • If the Destination B is defined, then the Source A and B will be **Any** by default.
Options	Displays the advance options for the Static type. Configure the following: • To ignore the embedded IP addresses (no-Payload), check the Ignore Embedded IP address check box. • To enable port translation, check the Enable Port Translation check box, and then define the following: – TCP or UDP – Original Port – Port Translation

Table 6-7 lists the elements on the Dynamic NAT page.

Table 6-7 Dynamic NAT Page

Element	Description
Direction	Displays the directions. This release supports only the Inbound to Outbound direction.
VRF	Displays the VRF on which the NAT translation process happens. The default value is default VRF.

Table 6-7 Dynamic NAT Page (continued)

Element	Description
Source A	Select the ACL name from the list. • If the Source A is defined, then the Source B must be defined. • If the Source A is defined, then the Destination A will be **Any** by default.
Destination A	Select the ACL name from the list. • If the Destination A is defined, then the Destination B must be defined. • If the Destination A is defined, then the Source A will be **Any** by default.
Translation	Displays the Dynamic NAT translation type.
Source B	Choose the NAT pool from the drop-down list. If the Source B is defined, then the Source A must be defined. If the Source B is defined, then the Destination B will be **Any** by default.
Destination B	Choose the NAT pool from the drop-down list. • If the Destination B is defined, then the Destination A must be defined. • If the Destination B is defined, then the Source A and B will be **Any** by default.
Options	Displays the advance options for the Dynamic type. • To ignore the embedded IP addresses (no-Payload), check the Ignore Embedded IP address check box. • To enable port translation, check the Enable Port Translation check box, and then define the following: – TCP or UDP – Original Port – Port Translation **Note** This option is supported only on the ISR devices.

Table 6-8 lists the elements on the Dynamic PAT page.

Table 6-8 Dynamic PAT Page

Element	Description
Direction	Displays the directions. This release support the Inbound to Outbound directions.
VRF	Displays the VRF on which the NAT translation process happens. The default value is default VRF.
Source A	Select the ACL name from the list.
Destination A	Not defined.
Translation	Displays the Dynamic PAT translation type.
Source B	Select the IP Pool Name from the list.
Destination B	Not defined.

Table 6-8 Dynamic PAT Page

Element	Description
Options	Displays the advance options for the Dynamic PAT. Select the Ignores embedded IP Addresses (no-Payload) options. The options are: **Yes** or **No**. **Note** This option is supported only on the ISR devices.

Step 6 Click:

- **Save** to save and deploy the changes to the device.
- Cancel to exit without saving.

Step 7 To edit the existing NAT44 rule, in the NAT44 page, do the following:

a. Click on the selected NAT44 rules parameters row, and edit the parameters. or

b. Select the NAT44 rule, and click the **Edit** button. The selected NAT44 rule entity opens for editing. You can edit all the parameters except the pool Name.

Step 8 You can change the Source and Destination according to the creation rules. You can also change the Options selection according to the creation rules.

Step 9 Click **Save/ Apply** to save the changes in the server.

Step 10 To delete the existing NAT44 rules, select the rules, and then click the **Delete** button.

Step 11 Click **Ok** on the warning message to delete the rules. The selected NAT44 rules will be deleted.

Managing Interfaces

A virtual interface is a logical interface configured with generic configuration information for a specific purpose or for configuration common to specific users, plus router-dependent information.

Configuring Interfaces

To assign the interfaces to a specific association, follow these steps.

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

Step 2 Select the device from the list or click **Add** to create a new device, then configure the device.

Step 3 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector left panel, choose **NAT > Interfaces**.

Step 5 In the Interface page, select the interface you want to change and enter the VRF and select the association from the drop-down list.

Table 6-9 lists the elements on the Interfaces page.

Table 6-9 Interfaces Page

Element	Description
Interface Name	Displays the name of the interface.

Table 6-9 Interfaces Page

Element	Description
VRF	Displays the name of the VRF that the interface belongs to.
Status	Displays the status of the interface.
Association	Select the association from the drop-down list. The options are: Inside, Outside, and None.

Step 6 Click:

- **Save/ Apply** to save the changes in the server.
- **Cancel** to exit without saving.

Managing NAT MAX Translation

The Rate Limiting NAT Translation feature provides the ability to limit the maximum number of concurrent NAT operations on a router. In addition, the NAT MAX feature gives more control to the users to use the NAT addresses. The Rate Limiting NAT Translation feature can be used to limit the effects of viruses, worms, and denial-of-service attacks.

The NAT Maximum Translations feature allows you to reset the global translation attribute values.

Setting NAT MAX Translation

To set the MAX Translation, follow these steps.

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

Step 2 Select the device from the list or click **Add** to create a new device, then configure the device.

Step 3 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector left panel, choose **NAT > Max. Translation**.

Step 5 Reset the parameter values as described in Table 6-10.

Table 6-10 lists the elements on the MAX Translation page.

Table 6-10 MAX Translation Page

Element	Description
Maximum number of global translation entries	Configures the maximum number of NAT entries that are allowed. The maximum number of allowed NAT entries is 2147483647. A typical range for a NAT rate limit is from 100 to 300 entries.
Maximum number of translations over all hosts	Configures the maximum number of NAT entries allowed from the all hosts. The maximum number of allowed NAT entries is 2147483647. A typical range for a NAT rate limit is from 100 to 300 entries.
Maximum number of translations over all VRF	Configures the maximum number of NAT entries allowed from all VRFs. The maximum number of allowed NAT entries is 2147483647, although a typical range for a NAT rate limit is 100 to 300 entries.

Table 6-10 MAX Translation Page

Element	Description
Maximum number of translations for ACL	Configures the maximum number of NAT entries allowed from the specified ACL. The maximum number of allowed NAT entries is 214748364. A typical range for a NAT rate limit is 100 to 300 entries.
Maximum number of translations for VRF	Configures the maximum number of NAT entries allowed from the specified VRF(s). The maximum number of allowed NAT entries is 2147483647. A typical range for a NAT rate limit is 100 to 300 entries.
Maximum number of translations for host	Configures the maximum number of NAT entries allowed from the specified Host(s). The maximum number of allowed NAT entries is 214748364. A typical range for a NAT rate limit is 100 to 300 entries.

Step 6 Click:

- **Save / Apply** to save the changes in the server.
- **Cancel** to exit without saving.

Dynamic Multipoint VPN

The DMVPN feature allows users to scale large and small IP Security (IPsec) VPNs by combining generic routing encapsulation (GRE) tunnels, IPsec encryption, and Next Hop Resolution Protocol (NHRP).

A typical VPN connection is a point-to-point IPSec tunnel connecting two routers. DMVPN enables you to create a network with a central hub that connects other remote routers, referred to as spokes using a GRE over IPSec tunnel. IPSec traffic is routed through the hub to the spokes in the network.

See *Dynamic Multipoint IPsec VPNs (Using Multipoint GRE/NHRP to Scale IPsec VPNs)* for more information about DMVPN (requires a CCO login ID).

Configuring DMVPN

Cisco Network Control System allows you to configure your router as a DMVPN hub or DMVPN spoke. You can configure the router in the following ways:

Hub

- Configuring Hub and Spoke Topology, page 6-17

Spoke

- Configuring Fully Mesh Topology, page 6-17

Creating DMVPN Tunnel

You should configure the following parameters to create the DMVPN tunnel:

- Device role and topology type

- Multipoint GRE interface information
- NHRP and tunnel parameters
- Next Hub Server (NHS) Server (Optional)

To create the DMVPN tunnel, follow these steps.

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

Step 2 Select the device from the list or click **Add** to create a new device, then configure the device.

Step 3 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector panel, choose **Security > DMVPN**, and click the **Add** button to create the DMVPN.

Step 5 In the Device Role and Topology Type section, select the topology and the device role. The options are: Spoke, Hub, and Dynamic Connection between Spokes.

Step 6 In the Multipoint GRE Interface Information section, select the WAN interface that connects to the Internet from the drop-down list.

Step 7 Enter the IP address of the Tunnel Interface, and Subnet Mask.

Step 8 In the NHRP and Tunnel Parameters section, enter the Network ID, Hold Time, NHRP Authentication String, Tunnel Key, Bandwidth, MTU, Tunnel Throughput Delay, and TCP Maximum Segment Size information.

Step 9 In the Encryption policy field, click the anchored plus button (+) to add the Transform Set Profile.

Step 10 In the Transform Set Profile dialog box, enter the Name and choose the acceptable combination of security protocols and algorithm from the drop-down list to configure the transform set. Enable the IP Compression to enable the IP compression for the transform set. Choose the mode for the transform set. The options are: Tunnel mode or Transport mode.

Step 11 In the NHS Server Information section, enter the IP address for the physical interface of the hub and tunnel and the Fallback Time. If the device supports the cluster then add the next hop server information, such as Cluster ID, Max Connection, Hub IP address, and Priority.

Note The NHS server information is required only for spoke configuration. If you check the Use Cluster for NHS check box, add the information, such as Cluster ID, Max Connection, and Next Hub Server. The template with the NHS cluster configuration will be applied only to the device running Cisco IOS Software version 15.1(2)T or later.

Step 12 In the Routing Information section, choose the routing information. The options are: EIGR, RIPV2, and Other.

Note The routing information is required only for hub configuration.

Step 13 Choose the existing EIGRP number from the drop-down list. or enter an EIGRP number. Use the Other option to configure other protocols.

Table 6-11 lists the elements on the Dynamic Multipoint VPN page.

Table 6-11 DMVPN Page

Element	Field Description
Device Role and Topology Tab	
Spoke radio button	Check the Spoke radio button to configure the router as a Spoke in the topology.
Hub radio button	Check the Hub radio button to configure the router as a Hub in the topology.
Dynamic Connection between Spokes	Check the Create Dynamic Connection between spokes check box to configure the dynamic connection between spokes.
Multipoint GRE Interface Information	
WAN Interface	Choose the WAN interface that connects to the internet from the drop-down list.
Interface IP address	Enter the IP address of the tunnel interface.
Subnet mask	Enter the subnet mask.
NHRP and Tunnel Parameters	
Network ID	Enter the NHRP Network ID. The network ID is globally unique, 32-bit network identifier from a Non Broadcast Multiaccess (NBMA) network. The range is from 1 to 4294967295.
Hold Time	Enter the number of seconds that the Next Hop Resolution Protocol (NHRP). NBMA addresses should be advertised as valid. The default value is 7200 seconds.
Tunnel Key	Enter the Tunnel key. The tunnel key is used to enable a key ID for a particular tunnel interface. The range value is from 0 to 4294967295.
Bandwidth	Enter the intended bandwidth, in kilobytes per second (kbps).
MTU	Enter the MTU size of IP packets that are sent on a particular interface. The default value for Ethernet and the serial interface is 1500. The default value varies depending upon the media type.
Tunnel Throughput Delay	Set a delay value for an interface, in tens of microseconds. Tunnel throughput delay is used to set the delay value for a particular interface.
TCP Maximum segment Size	Enter the TCP maximum segment size in bytes.
IPsec Information	
Encryption policy	Enter the encryption policy. Click the **Add** button to add the transform set profile.
Transform Set Profile	
Integrity Algorithm	Enter the integrity algorithm. The Algorithm used to check the integrity of the payload.
Encryption Algorithm	Enter the encryption algorithm.Algorithm used to encrypt the payload.
Mode	Enter the mode. Indicates the mode to transport the traffic.
IP Compression	Check the IP Compression check box to compress payload.
NHS Server	
Use Cluster For NHS	Check the Use Cluster For NHS check box and add the information, such as Cluster ID, Max Connections, Hub's Physical IP Address, Hub Tunnel IP, and Priority.
Hub Physical Interface	Enter the IP address of the hub’s physical interface.
Hub Tunnel Interlace	Enter the IP address of the hub’s tunnel interface.
Routing Information	
EIGRP	Check the EIGRP routing information check box.

Table 6-11 DMVPN Page (continued)

Element	Field Description
RIPV2	Check the RIPV2 routing information check box.
Other	Check the Other check box to select other routing protocol.
AS Number	Choose the existing EIGRP number from the drop-down list

Step 14 Click **Save** to save the single NHS server entry details and the priority of the server, save the entire group of server, and save the NHS cluster information. when save the NHS cluster information, the NHS server will be auto populated in the non-editable field.

Step 15 Click **OK** to save the configuration to the device.

Step 16 Click **Cancel** to cancel all the changes you have made without sending them to the router.

Configuring Hub and Spoke Topology

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

Step 2 Select the device from the list or click **Add** to create a new device, then configure the device.

Step 3 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector panel**,** choose **Security > DMVPN**, and click the **Add** button to create the DMVPN tunnel**.**

Step 5 In the Device Type and Topology section, choose Hub and Spoke as the topology, and select either Hub or Spoke as a device role.

Step 6 Select the WAN interface from the drop-down list, and then configure the Multipoint GRE IP Address and the subnet mask for the tunnel interface.

Step 7 Configure the NHRP and the Tunnel Interface parameters, such as the IP address, NHRP parameters and map, MTU value, Source of the Tunnel, Tunnel Mode, and Tunnel Key.

Step 8 Create the transform-set for protecting the data flow between the devices. You can specify up to four transforms: One Authentication Header (AH), one Encapsulating Security Payload (ESP) encryption, one ESP authentication, and one compression. These transforms define the IPSec security protocols and the algorithms.

Step 9 Configure the routing protocol to be used. For elements on this page, see Table 6-11.

Step 10 Click **Save** to save the configuration to the device.

Step 11 Click **Cancel** to close the Create DMVPN Tunnel page without applying the changes to the device.

Configuring Fully Mesh Topology

The dynamic spoke-to-spoke option allows you to configure the DMVPN fully meshed topology. In this topology, you can configure the router as a spoke, capable of establishing a direct IPSec tunnel to other spokes in the network.

To configure the hub and spoke topology, follow these steps.

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

Step 2 Select the device from the list or click **Add** to create a new device, then configure the device.

Step 3 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector panel**,** click **Security > DMVPN**, and click the **Add** button to create the DMVPN tunnel with fully meshed topology.

Step 5 From the Create DMVPN Tunnel configuration page, select the **Full Mesh** radio button to configure the network type as full mesh topology.

Step 6 Repeat Step 6 through Step 8 from the Configuring Hub and Spoke Topology section. For elements on this page, see Table 6-11.

Step 7 For Fully Mesh spoke topology, in the NHS Server Information section, add the next hub server information, such as the IP Address of Hub's physical interface and the IP address of Hub's tunnel interface.

Step 8 Click **Save** to save the configuration to the device.

Step 9 Click **Cancel** to close the Create DMVPN Tunnel page without applying the changes to the device.

Cluster Configuration

To configure the cluster, follow these steps.

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

Step 2 Select the device from the list or click **Add** to create a new device, then configure the device.

Step 3 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector panel**,** click **Security > DMVPN** and click the **Add** button to create the DMVPN tunnel**.**

Step 5 From the Create DMVPN Tunnel configuration page, select the **Spoke** radio button to configure the device role as a spoke.

Step 6 Repeat Step 6 through Step 8 from the Configuring Hub and Spoke Topology section. For elements on this page, see Table 6-11.

Note The device must running IOS version of 15.1(2)T or later.

Step 7 Click the **Add Row** button to configure the cluster related information, and add the Cluster-ID and Maximum Connection values.

Step 8 Click the **Expand Row** button (next to the radio button) and click the **Add Row** button to add the NHS server information.

Step 9 Enter the NHS server, the GRE Tunnel IP addresses, and the Priority of this NHS server. Click the **Save** button to save the NHS server entry configuration.

Step 10 Click the **Save** button to save the NHS server group information.

Step 11 Click the **Save** button again to save the NHS group information with the cluster configuration. It will automatically populate the NHS server IP address in the table.

Edit DMVPN

To edit the existing DMVPN tunnel, follow these steps.

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

Step 2 Select the device from the list or click **Add** to create a new device, then configure the device.

Step 3 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector panel**,** choose **Security > DMVPN**. The available tunnel is displayed.

Step 5 Select the tunnel, and click the **Edit** button. The Edit DMVPN Tunnel page opens.

Step 6 From the Edit DMVPN Tunnel page, you can edit the DMVPN parameters.

For elements on the Edit DMVPN Tunnel page, see Table 6-11.

Step 7 Click **Ok** to send the edited DMVPN tunnel configuration to the device.

Step 8 Click **Cancel** to close the Edit DMVPN Tunnel page without applying the configuration to the device.

Delete DMVPN

To delete the existing DMVPN tunnel, follow these steps.

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

Step 2 Select the device from the list to delete the DMVPN tunnel. If the device is not added, click the **Add** button to add the device.

Step 3 After selecting the device, click **Configuration**. The Feature Selector left panel appears.

Step 4 From the Feature Selector left panel**,** choose **Security > DMVPN**. The available tunnel is displayed.

Step 5 Select the tunnel, and click the **Delete** button.

Click **Yes** on the warning message to delete the selected tunnel. For elements on the Edit DMVPN Tunnel page, see Table 6-11.

Step 6 Click **No** on the warning message if you do not want to delete the selected tunnel.

Step 7 Click **Cancel** to cancel all the changes you have made without sending them to the router.

GETVPN

A Group Encrypted Transport VPN (GETVPN) deployment has primarily three components: Key Server (KS), Group Member (GM), and Group Domain of Interpretation (GDOI) protocol. GMs encrypt/decrypt the traffic and KS distributes the encryption key to all the group members. The KS decides on one single data encryption key for a given life time. Because all GMs use the same key, any GM can decrypt the traffic encrypted by any other GM. GDOI protocol is used between the GM and KS for group key and group Security Association (SA) management. Minimum one KS is required for a GETVPN deployment.

Unlike traditional IPSec encryption solutions, GETVPN uses the concept of group SA. All members in the GETVPN group can communicate with each other using a common encryption policy and a shared SA. Therefore, there is no need to negotiate IPSec between GMs on a peer-to-peer basis; thereby reducing the resource load on the GM routers.

Group Member

The GM registers with the key server to get the IPSec SA that is necessary to encrypt data traffic within the group. The GM provides the group identification number to the KS to get the respective policy and keys for this group. These keys are refreshed periodically by the KS, and before the current IPSec SAs expire, so that there is no loss of traffic.

Key Server

The KS is responsible for maintaining security policies, authenticating the GMs and providing the session key for encrypting traffic. KS authenticates the individual GMs at the time of registration. Only after successful registration can the GMs participate in group SA.

A GM can register at any time and receive the most current policy and keys. When a GM registers with the KS, the KS verifies the group identification number of the GM. If this identification number is valid, and the GM has provided valid Internet Key Exchange (IKE) credentials, the KS sends the SA policy and the Keys to the group member.

There are two types of keys that the GM will receive from the KS: the Key Encryption Key (KEK) and the Traffic Encryption Key (TEK). The TEK becomes part of the IPSec SA with which the group members within the same group encrypt the data. KEK is used to secure rekey messages between the KS and the GMs.

The KS sends out rekey messages either because of an impending IPSec SA expiration or because the security policy has changed on the KS. Keys can be distributed during re-key using either multicast or unicast transport. Multicast method is more scalable as keys need not be transmitted to each group member individually. Unlike in unicast, KS will not receive acknowledgement from GM about the success of the rekey reception in multicast rekey method. In unicast rekey method, KS will delete a GM from its database if three consecutive rekeys are not acknowledged by that particular GM.

GDOI protocol is used for Group key and group SA management. GDOI uses Internet Security Association Key Management Protocol (ISAKMP) for authenticating the GMs and KSs. All the standard ISAKMP authentication schemes like RSA Signature (certificates) and Pre-shared key can be used for GETVPN.

For more information on GETVPN, See http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6635/ps7180/deployment_guide_c07_554713.html.

Configuring GETVPN

The Cisco Network Control System allows you to configure the GETVPN. To configure the GETVPN, you should configure the following:

- Group member
- Key server

Creating GETVPN Group Member

Use the Add GroupMember configuration page to configure the GETVPN group member.

To create the GETVPN group member, follow these steps.

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

Step 2 Select the device from the list or click **Add** to add a new device, then configure the device. The device details appear on the lower part of the screen.

Step 3 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector panel**,** click **Security > GETVPN-GroupMember**, and click the **Add** button to create the GET VPN group member**.**

Step 5 In the Add GroupMember dialog box, select the General tab, and enter the Group Name and Group Identity. Choose the Registration Interface from the drop-down list.

Step 6 Enter the Primary Key Server and Secondary Key Server IP address. Click the **Add Row** or **Delete** buttons to add or delete the secondary key server IP address. Click on the **Row** or **Field** to edit the secondary key server IP address.

Step 7 Click:

- **Save** to save the configuration.
- **Cancel** to exit without saving your changes.

Step 8 In the Add Group Member dialog box, select the Advanced tab, and choose the Local Exception ACL and Fail Close ACL from the drop-down list.

Step 9 In the Add Group Member dialog box, select the Migration tab, and check the Enable Passive SA check box to enable passive SA. Use this option to turn on the Passive SA mode on this group member.

Table 6-12 lists the elements on the GETVPN GroupMember page.

Table 6-12 GETVPN Group Member Page

Element	Field Description
General	
Group Name	Enter the name of the GETVPN group.
Group Identity	Enter the unique identity for the GETVPN group. This can be a number or an IP address.The range is from 0 to 2147483647.
Registration Interface	Choose the interface from the drop-down list to which the crypto map needs to be associated.
Primary Key Server	Specify the primary key server IP address to which the client connects. The primary key server is responsible for creating and distributing group policies to all group members and periodically synchronizes with the secondary key servers. The server with the highest priority is elected as a primary key server.
Secondary Key Server	Specify the secondary key server IP address to which the group member falls back when the primary key server registration fails. A group member can be configured to register to any available key server from a list of all secondary key servers. The group member configuration determines the registration order. The key server defined first is contacted first, followed by the second defined key server, and so on.
Add Row	Click the **Add Row** button to add the secondary key servers.

Table 6-12 GETVPN Group Member Page

Element	Field Description
Delete	Click the **Delete** button to delete a secondary key server.
Advanced Tab	
Local Exception ACL	Choose an ACL for the traffic that should be excluded from the encryption.
Fail Close ACL	Choose an ACL for the traffic that needs to be sent in clear text until the group member registers with the key server. If the Fail Close feature is configured, all the traffic passing through the group member will be dropped until the group member is registered successfully. Once the group member registers successfully and SAs are downloaded, this feature turns off by itself.
Migration Tab	
Enable Passive SA	Use this option to turn on the Passive SA mode on the group member. The Passive SA mode overrides the receive only SA option on the key server and encrypts all the outbound traffic.

Step 10 Click:

- **Ok** to add the Group member in the table. To display the commands, click **CLI** preview. After the schedule deploy, the configuration is applied on the device.
- **Cancel** to cancel all the changes you have made without sending them to the router.
- **Close** to close the page.

Creating GETVPN Key Server

Use the Add KeyServer configuration page to configure the GETVPN key server.

To create the GETVPN key server, follow these steps.

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

Step 2 Select the device from the list or click **Add** to add a new device, then configure the device. The device details appear on the lower part of the screen.

Step 3 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector left panel**,** click **Security > GETVPN-KeyServer**, and click the **Add** button to create the GETVPN key server**.**

Step 5 In the Add Key Server dialog box, select the General tab, and enter the Group Name, Group Identity, WAN IP address, and Priority of this key server.

Step 6 Enter the Co-operative Key Servers IP address. Click the **Add Row** or **Delete** button to add or delete the Co-operative key server IP address. Click on the **Row** or **Field**, and edit the IP address.

Step 7 In the Add KeyServer dialog box, select the Rekey tab, and choose the Distribution method from the drop-down list. Enter the information, such as Multicast IP Address, KEK Lifetime, TEK Lifetime, Retransmit Key, RSA Key for Rekey Encryption, and Rekey Encryption Method.

Step 8 In the Add KeyServer dialog box, select the GETVPN Traffic tab, and enter the Traffic to be encrypted, Encryption Policy, and Anti Replay.

Table 6-13 lists the elements on the GETVPN KeyServer page.

Table 6-13 GETVPN Key Server Page

Element	Field Description
General	
Group Name	Enter the name of the GETVPN group.
Group Identity	Enter the unique identity for the GETVPN group.This can be a number or an IP address.The range is from 0 to 2147483647.
WAN IP Address	Enter the WAN IP address which is the IP address of the interface to which this key server will be associated.
Co-operative Key Server	Specify the Co-operative key server IP address to which the group member falls back when the primary key server registration fails. A Group member can be configured to register to any available key server from a list of all secondary key servers. Group member configuration determines the registration order. The key server defined first is contacted first, followed by the second defined key server, and so on.
Add Row	Click the **Add Row** button to add the Co-operative key server.
Delete Row	Click the **Delete Row** button to delete the Co-operative key server.
Rekey	
Distribution Method radio button	Choose the distribution method. The distribution method is used to send the rekey information from key server to group members. The options are: Unicast or Multicast.
Multicast IP Address	When you choose the distribution method as multicast, specify the multicast address to which the rekey needs to be transmitted.
KEK Lifetime	Enter the KEK lifetime in seconds. The range is from 120 to 86400.
TEK Lifetime	Enter the TEK lifetime in seconds. The range is from 120 to 86400.
Retransmit Key	Enter the frequency and the duration for the rekey retransmission in seconds.
RSA Key for Rekey Encryption	Enter the details of the RSA key that is used to encrypt the rekey information.
Rekey Encryption Method	Choose the encryption algorithm from the drop-down list. The encryption algorithm is used to encrypt the key. • AES-128—Encrypts according to the Advanced Encryption Standard using 128-bit keys. • AES-192—Encrypts according to the Advanced Encryption Standard using 192-bit keys. • AES-256—Encrypts according to the Advanced Encryption Standard using 256-bit keys. • DES—Encrypts according to the Data Encryption Standard using 56-bit keys. • 3DES—Encrypts three times using 56-bit keys. 3DES is more secure than DES, but requires more processing for encryption and decryption. It is less secure than AES. A 3DES license is required to use this option.
GETVPN Traffic	

Table 6-13 GETVPN Key Server Page (continued)

Element	Field Description
Traffic to Encrypt	Choose an ACL from the drop-down list for the traffic that needs to be encrypted between the participants. The access list defines the traffic to be encrypted. Only the traffic which matches the "permit" lines will be encrypted. **Note** Be sure not to encrypt certain traffic that should always be permitted even if the crypto sessions are not up.
Encryption Policy	Choose the transform sets from the drop-down list to be used to encrypt the traffic. Add the transform set from the table which is used to encrypt the traffic between peers.
Anti Replay	Choose the Time-based or Counter-based anti replay option.

Step 9 Click:

- **Ok** to add the Group member in the table. To display the commands, click **CLI** preview. After the schedule deploy, the configuration is applied on the device.
- **Cancel** to cancel all the changes you have made without sending them to the router.

Step 10 Click **Close** to close the page.

Editing GET VPN Group Member or Key Server

To edit the existing GETVPN group member or the GETVPN key server, follow these steps.

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

Step 2 Select the device from the list or click **Add** to add a new device, then configure the device. The device details appear on the lower part of the screen.

Step 3 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector panel**,** choose **Security > GETVPN-Group Member** or **GETVPN-KeyServer.** The GETVPN-GroupMember or GETVPN-KeyServer summary page opens.

Step 5 From the GETVPN summary page, select the group name and click **Edit**. The Edit GETVPN-GroupMember or GETVPN-Keyserver page appears.

Step 6 From the Edit GETVPN-GroupMember or GETVPN-KeyServer page, you can edit the GETVPN parameters.

For elements on the GETVPN-GroupMember or GETVPN-Keyserver page, see Table 6-12 and Table 6-13.

Step 7 Click:

- **Ok** to save the configurations.
- **Cancel** to cancel all the changes you have made without sending them to the router.

Step 8 Click **Close** to close the page.

Deleting GETVPN Group Member or Key Server

To delete the existing GETVPN group member or the GETVPN key server, follow these steps.

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

Step 2 Select the device from the list or click **Add** to add a new device, then configure the device. The device details appear on the lower part of the screen.

Step 3 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector pane, choose **Security > GETVPN-Group Member** or **GETVPN-KeyServer.** The GETVPN-GroupMember or GETVPN-KeyServer summary page opens.

Step 5 From the GETVPN summary page, select the group name and click **Delete**. For elements on the GETVPN-GroupMember or GETVPN-KeyServer page, see Table 6-12 and Table 6-13.

Step 6 Click:

- **Ok** to save the configurations.
- **Cancel** to cancel all the changes you have made without sending them to the router.

Step 7 Click **Close** to close the page.

VPN Components

The VPN components primarily include the following:

IKE Policies

The Internet Key Exchange (IKE) is a standard method for arranging secure and authenticated communications. The IKE establishes session keys (and associated cryptographic and networking configuration) between two hosts across the network. The IKE policies will protect the identities of peers during authentication.

The IKE negotiations must be protected; therefore, each IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states the security parameters that will be used to protect subsequent IKE negotiations. After the two peers agree on a policy, the security parameters of the policy are identified by a security association established at each peer. These security associations are applied to all the subsequent IKE traffic during the negotiation.

When the IKE negotiation begins, IKE looks for an IKE policy that is the same on both the peers. The peer that initiates the negotiation will send all its policies to the remote peer, and the remote peer will try to find a match. The remote peer looks for a match by comparing its own highest priority policy

against the other peer's received policies. The remote peer checks each of its policies in the order of its priority (highest first) until a match is found. A match is made when both the policies from the two peers contain the same encryption, hash, authentication, and Diffie-Hellman (D-H) parameter values, and when the remote peer's policy specifies a lifetime less than or equal to the lifetime in the policy being compared. If the lifetimes are not identical, the shorter lifetime from the remote peer's policy will be used.

Creating, Editing, and Deleting IKE Policies

The IKE Policies feature allows you to create, edit, and delete the IKE policies.

To create, edit, or delete the IKE policies, follow these steps.

Step 1 Choose **Operate > Device Work Center,** then select a device or click **Add** to add a new device, then configure the device. The device details appear on the lower part of the screen.

Step 2 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 3 From the Feature Selector panel**,** click **Security > VPN Components > IKE Policies**, and click the **Add Row** button to create the IKE policies**.**

Step 4 In the IKE Policies page, enter the Priority, Authentication, D-H Group, Encryption, Hash, and Lifetime.

Step 5 To edit the IKE policies parameters, click on the **Field** and edit the parameter of that IKE policy.

Step 6 To delete the IKE policies, select the IKE policies from the list, and click the **Delete** button.

Table 6-14 lists the elements on the IKE Policies page.

Table 6-14 IKE Policies Page

Element	Description
IKE Policies	
Priority	Enter the priority value of the IKE proposal. The priority value determines the order of the IKE proposals compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your first priority policy, the device tries to use the parameters defined in the policy with the next lowest priority number. The range is from 1 to 10000. The lower the number, the higher the priority.
Authentication	Choose the Pre-shared keys or RSA Signatures from the drop-down list. • Pre-SHARE—Authentication will be performed using pre-shared keys. • RSA_SIG— Authentication will be performed using digital signatures.

Table 6-14 IKE Policies Page (continued)

Element	Description
Encryption	Choose the encryption algorithm from the drop-down list. • AES-128—Encrypts according to the Advanced Encryption Standard using 128-bit keys. • AES-192—Encrypts according to the Advanced Encryption Standard using 192-bit keys. • AES-256—Encrypts according to the Advanced Encryption Standard using 256-bit keys. • DES—Encrypts according to the Data Encryption Standard using 56-bit keys. • 3DES—Encrypts three times using 56-bit keys. 3DES is more secure than DES, but requires more processing for encryption and decryption. It is less secure than AES. A 3DES license is required to use this option.
Diffie-Hellman Group	Choose the D-H group algorithm from the drop-down list. The Diffie-Hellman group is used for driving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Options are: • 1—Diffie-Hellman Group 1 (768-bit modulus). • 2—Diffie-Hellman Group 2 (1024-bit modulus). • 5—Diffie-Hellman Group 5 (1536-bit modulus, considered good protection for 128-bit keys).
Hash	Choose the hash algorithm used in the IKE proposal from the drop-down list. The hash algorithm creates a message digest, which is used to ensure message integrity. The options are: • SHA (Secure Hash Algorithm)—Produces a 160-bit digest. SHA is more resistant to brute-force attacks than MD5. • MD5 (Message Digest 5)—Produces a 128-bit digest. MD5 uses less processing time than SHA.
Lifetime	The lifetime of the security association (SA), in seconds. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes. The range is from 60 to 86400 seconds. The default value is 86400.

Step 7 Click:

- **Save** to save the configuration.
- **Cancel** to exit without saving your changes.
- **Save** again to generate the CLI commands.

IKE Settings

The IKE Settings feature allows you to globally enable the IKE for your peer router.

Creating IKE Settings

To enable the IKE policies and set the aggressive mode for the IKE, follow these steps.

Step 1 Choose **Operate > Device Work Center,** then select a device or click **Add** to add a new device, then configure the device. The device details appear on the lower part of the screen.

Step 2 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 3 From the Feature Selector panel**,** click **Security > VPN Components > IKE Settings**.

Step 4 Check the Enable IKE and Enable Aggressive Mode check box to enable the IKE policies and the aggressive mode.

Step 5 Choose the IKE Identity from the drop-down list.

Step 6 Enter the Dead Peer Detection Keepalive and Dead Peer Detection Retry time in seconds.

Table 6-15 lists the elements on the IKE Settings page.

Table 6-15 IKE Settings Page

Element	Description
IKE Settings	
Enable IKE	Check the Enable IKE check box to globally enable the IKE. By default, the IKE is enabled. You do not have to enable IKE for individual interfaces, but it can be enabled globally for all the interfaces at the router. If you do not want to use the IKE for your IP Security (IPSec) implementation, you can disable the IKE for all your IPSec peers. If you disable the IKE for one peer, you must disable it for all the IPSec peers.
Enable Aggressive Mode	Check the Enable Aggressive Mode check box to enable the Internet Security Association and Key Management Protocol (ISAKMP) aggressive mode. If you disable the aggressive mode, all aggressive mode requests to the device and all aggressive mode requests made by the device will be blocked.
IKE Identity	Choose the ISAKMP identity from the drop-down list. The options are: IP address, Distinguished Name and HostName. An ISAKMP identity is set whenever you specify pre-shared keys or RSA signature authentication. As a general rule, you should set all peers' identities in the same way, either by IP address or by host name. • IP Address—Sets the ISAKMP identity to the IP address of the interface that is used to communicate to the remote peer during the IKE negotiations. • Distinguished Name—Sets the ISAKMP identity to the distinguished name (DN) of the router certificate. • Host Name—Sets the ISAKMP identity to the host name concatenated with the domain name (for example, myhost.example.com).

Table 6-15 IKE Settings Page (continued)

Element	Description
Dead Peer Detection Keepalive	Enable the gateway to send the DPD messages to the peer. DPD is a keepalives scheme that allows the router to query the liveliness of its Internet Key Exchange (IKE) peer. Specify the number of seconds between DPD messages in the DPD Keepalive field. The range is from 10 to 3600 seconds.
Dead Peer Detection Retry	Specify the number of seconds between retries if the DPD messages fail in the DPD Retry. The range is from 2 to 60 seconds.

Step 7 Click:

- **Save** to save the configuration.
- **Refresh** to refresh the page.

IPsec Profile

The IPsec profiles, also called ISAKMP profiles, enable you to define a set of IKE parameters that you can associate with one or more IPSec tunnels. An IPsec profile applies parameters to an incoming IPSec connection identified uniquely through its concept of match identity criteria. These criteria are based on the IKE identity that is presented by incoming IKE connections and includes IP address, Fully Qualified Domain Name (FQDN), and group (the Virtual Private Network (VPN) remote client grouping).

Creating, Editing, and Deleting IPsec Profile

The IKE Profile feature allows you to create, edit, and delete the IPsec Profile.

To create, edit, or delete the IPsec Profile, follow these steps.

Step 1 Choose **Operate > Device Work Center,** then select a device or click **Add** to add a new device, and then configure the device. The device details appear on the lower part of the screen.

Step 2 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 3 From the Feature Selector panel**,** click **Security > VPN Components > IPsec Profile**, and click the **Add Row** button to create the IPsec profile**.**

Step 4 In the IPsec Profile page, enter the information such as Name, Description, Transform Set, and the IPsec SA Lifetime.

Step 5 To edit the IPsec profile parameters, click on the **Field** and edit the parameter of that IPsec profile.

Step 6 To delete the IPsec profile, select the IPsec Profile from the list, and click the **Delete** button.

Table 6-16 lists the elements on the IPsec Profile page.

Table 6-16 IPSec Profile Page

Element	Description
Name	Enter a name for this IPsec profile. When you edit a profile, you cannot edit the name of the IPsec profile.

Table 6-16 IPSec Profile Page

Element	Description
Description	Add a description for the IPsec profile that you are adding or editing.
Transform Sets	Choose the transform sets from the list. Displays the transform sets that are configured on this router. A transform set represents a certain combination of security protocols and algorithms. During the IPSec security association negotiation, the peers agree to use a particular transform set for protecting a particular data flow. A transform describes a particular security protocol with its corresponding algorithms.
IPsec SA Lifetime	Enter the IPSec SA Lifetime to establish a new SA after the set period of time elapses. Enter the time in seconds. The range is from 120 to 86400.

Step 7 Click:

- **Save** to save the configuration.
- **Cancel** to exit without saving your changes.
- **Save** again to generate the CLI commands.

Pre-shared Keys

The Pre-shared Keys feature allows you to share a secret key between two peers and will be used by the IKE during the authentication phase.

Creating, Editing, and Deleting Pre-shared Keys

To create, edit, or delete the pre-shared keys, follow these steps.

Step 1 Choose **Operate > Device Work Center,** then select a device or click **Add** to add a new device, and then configure the device. The device details appear on the lower part of the screen.

Step 2 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 3 From the Feature Selector panel**,** click **Security > VPN Components > Pre-Shared Keys**, and click the **Add Row** button to create the pre-shared key**.**

Step 4 In the Pre-Shared Keys page, enter the IP Address, Host Name, Subnet Mask, and Pre-Shared Keys.

Step 5 To edit the pre-shared key parameters, click on the **Field** and edit the parameter of that pre-shared key.

Step 6 To delete the pre-shared key, select the pre-shared key from the list, and click the **Delete** button.

Table 6-17 lists the elements on the Pre-Shared Keys page.

Table 6-17 Pre-Shared Keys Page

Element	Description
IP Address / Host Name	Enter the IP address or the hostname of the remote peer.
Subnet Mask	Enter the subnet mask.

Table 6-17 Pre-Shared Keys Page

Element	Description
Pre-shared Keys	Enter the Pre-shared key and re-enter the key to confirm the pre-shared key.

Step 7 Click:

- **Save** to save the configuration.
- **Cancel** to exit without saving your changes.
- **Save** again to save the configuration and generate the CLI commands.

RSA Keys

An RSA key pair consists of a public key and a private key. When setting up your Public Key Infrastructure (PKI), you must include the public key in the certificate enrollment request. After the certificate is granted, the public key will be included in the certificate so that the peers can use it to encrypt the data that is sent to the router. The private key is kept on the router and used for both to decrypt the data sent by the peers and to digitally sign transactions when negotiating with the peers.

The RSA key pairs contain a key modulus value. The modulus determines the size of the RSA key. The larger the modulus, the more secure the RSA key. However, keys with large modulus values take longer to generate, and encryption and decryption operations take longer with larger keys.

Creating, Importing, Exporting, and Deleting RSA Keys

To create, export, import, or delete the RSA keys, follow these steps.

Step 1 Choose **Operate > Device Work Center,** then select a device or click **Add** to add a new device, and then configure the device. The device details appear on the lower part of the screen.

Step 2 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 3 From the Feature Selector panel**,** click **Security > VPN Components > RSAKeys,** and click the **Add Row** button to create the RSA Keys**.**

Step 4 The Add RSA Keys dialog box appears.

Step 5 In the Add RSA Keys dialog box, enter the Label, Modulus, and Type.

Step 6 Check the Make the Key exportable check box to generate the RSA as a exportable key.

Step 7 Click:

- **OK** to save the configuration.
- **Cancel** to exit without saving your changes.

Step 8 To import the RSA key, click the **Import** button. The Import RSA Key dialog box appears.

Step 9 In the Import RSA Key dialog box, enter the label of the RSA key, Key type, and password to decrypt the key. If the key type is general-keys, signature or encryption, copy and paste the public and private key data that was saved. To import usage-key, enter the public and private key data of both the signature and encryption keys.

Step 10 Click:

- **Import** to import the RSA key.
- **Close** to exit without saving your changes.

Step 11 To export the RSA key, select the RSA key from the list and click the **Export** button. The Export RSA Key Pair dialog box appears.

Step 12 In the Export RSA Key Pair dialog box, enter the password to encrypt the RSA key and choose the encryption algorithm from the drop-down list.

Table 6-18 lists the elements on the RSA Keys page.

Table 6-18 RSA Keys Page

Element	Description
RSA Keys	
Label	Enter the name for the key pair.
Modulus	Enter the key modulus value. For a modulus value between 512 and 1024, enter an integer value that is a multiple of 64. If you want a value higher than 1024, you can enter 1536 or 2048. If you enter a value greater than 512, key generation may take a minute or longer. The modulus determines the size of the key. The larger the modulus, the more secure the key, but keys with a large modulus take longer to generate, and encryption/decryption operations take longer with larger keys.
Type	Select the type of the RSA key to be generated. The options are: General Purpose, Usages Keys, Encryption Keys, and Signature Keys.
Make Key Exportable	Check the Make the Key exportable check box to generate the RSA key as a exportable key and save the key in a different location.
Import RSA Key	
Decryption Password	Enter the decryption password.
Key Type	Choose the type of key to be imported from the drop-down list. The options are: General purpose, Usages keys, Encryption Keys, and Signature keys.
PEM-formatted Public Key or Certificate	Enter the PEM-formatted public key or certificate. The public key data generated while exporting the key.
PEM-formatted Encrypted Private Key	Enter the PEM-formatted encrypted private key. The private key data generated while exporting the key.
Export RSA Key	
Encryption Password	Enter the encryption password.
Encryption Algorithm	Select the encryption algorithm.

Step 13 Click:

- **OK** to display the exported keys.
- **Cancel** to exit without saving your changes.

Step 14 To delete the RSA key, select the RSA key from the list, and click the **Delete** button.

Transform Sets

A transform set is an acceptable combination of security protocols, algorithms and other settings to apply to Upset protected traffic. During the IPSec security association negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

Creating, Editing, and Deleting Transform Sets

To create, edit, or delete the transform sets, follow these steps.

Step 1 Choose **Operate > Device Work Center,** then select a device or click **Add** to add a new device, then configure the device. The device details appear on the lower part of the screen.

Step 2 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 3 From the Feature Selector panel**,** click **Security > VPN Components > Transform Sets**, and click the **Add Row** button to create the transform sets**.**

Step 4 In the Transform Sets page, enter the Name and select the acceptable combination of security protocols and algorithm to configure the transform set. Specify the mode for a transform set. The options are: Tunnel mode or Transport mode.

Step 5 To edit the Transform sets parameters, click on the **Field** and edit the parameter of that transform sets.

Step 6 To delete the transform set, select the transform set from the list, and click the **Delete** button.

Table 6-19 lists the elements on the Transform Set page.

Table 6-19 Transform Set Page

Element	Description
Name	Enter the name for the transform set.
ESP Encryption Algorithm	Choose the ESP encryption algorithm from the drop-down list. The algorithm used to encrypt the payload. The options are: • ESP with the 128-bit Advanced Encryption Standard (AES) encryption algorithm. • ESP with the 192-bit AES encryption algorithm. • ESP with the 256-bit AES encryption algorithm • ESP with the 168-bit DES encryption algorithm (3DES or Triple DES). • Null encryption algorithm.
ESP Integrity Algorithm	Choose the integrity algorithm from the drop-down list. The algorithm used to check the integrity of the payload. The options are: • ESP with the MD5 (HMAC variant) authentication algorithm. • ESP with the SHA (HMAC variant) authentication algorithm
AH Integrity	Choose the AH integrity from the drop-down list. The options are: • AH with the MD5 (Message Digest 5) (a Hash-based Message Authentication Code [HMAC] variant) authentication algorithm • AH with the SHA (Secure Hash Algorithm) (an HMAC variant) authentication algorithm.
Compression	Enable or Disable the IP compression with the Lempel-Ziv-Stac (LZS) algorithm.

Table 6-19 Transform Set Page (continued)

Element	Description
Mode	Choose the mode from the drop-down list. The options are: • Transport—Encrypt data only. Transport mode is used when both endpoints support IPsec. Transport mode places the authentication header or encapsulated security payload after the original IP header; thus, only the IP payload is encrypted. This method allows users to apply network services such as quality-of-service (QoS) controls to encrypted packets. • Tunnel—Encrypt data and IP header. Tunnel mode provides stronger protection than transport mode. Because the entire IP packet is encapsulated within AH or ESP, a new IP header is attached, and the entire datagram can be encrypted. Tunnel mode allows network devices such as a router to act as an IPsec proxy for multiple VPN users; tunnel mode should be used in those configurations.

Step 7 Click:

- **Save** to save the configuration.
- **Cancel** to exit without saving your changes.
- **Save** again to save the configuration changes.

Overview of Zones

The Zone Based Firewall (ZBFW) feature allows users to easily manage Cisco IOS unidirectional firewall policy between groups of interfaces known as zones.

A zone is a group of interfaces that have similar functions or features. For example, on a router, Gigabit Ethernet interface 0/0/0 and Gigabit Ethernet interface 0/0/1 may be connected to the local LAN. These two interfaces are similar because they represent the internal network, so they can be grouped into a zone for firewall configurations.

By default, the traffic between interfaces in the same zone is not subjected to any policy. The traffic passes freely. Firewall zones are used for security features.

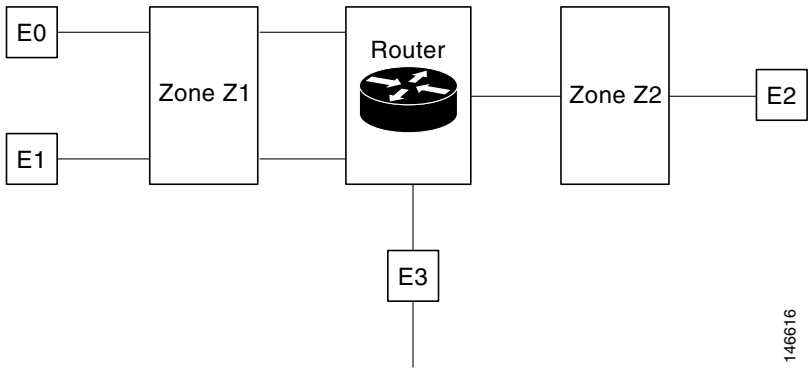
Security Zones

A security zone is a group of interfaces to which a policy can be applied. Grouping interfaces into zones involves the following two procedures:

- Creating a zone so that the interfaces can be attached to it.
- Configuring an interface as a member of a given zone.

By default, the traffic flows among the interfaces that are members of the same zone. When an interface is a member of a security zone, all traffic to and from that interface (except traffic going to the router or initiated by the router) is dropped. To permit the traffic to and from a zone-member interface, you must make that zone part of a zone pair, and then apply a policy to that zone pair. If the policy permits the traffic (through inspect or pass actions), traffic can flow through the interface.

Figure 6-1 Security Zone Diagram



- Interfaces E0 and E1 are members of the security zone Z1.
- Interface E2 is a member of the security zone Z2.
- Interface E3 is not a member of any of the security zone.

In this scenario, the following situations exist:

- Traffic flows freely between the interfaces E0 and E1 because they are members of the same security zone (Z1).
- If no policies are configured, traffic will not flow between interfaces (for example, E0 and E2, E1 and E2, E3 and E1, and E3 and E2).
- Traffic can flow between E0 or E1 and E2 interfaces only when an explicit policy is configured to permit the traffic between the zone Z1 and zone Z2.
- Traffic can never flow between E3 and E0/E1/E2 interfaces because E3 is not a part of any security zone.

The following topics provide more information:

- Managing Applications, page 6-35
- Managing Default Parameters, page 6-36
- Managing Interfaces, page 6-37
- Managing Policy Rules, page 6-37
- Managing Services, page 6-41
- Creating Security Zone, page 6-42

Managing Applications

This feature allows you to assign or un-assign the Transmission Control Protocol (TCP) / User Datagram Protocol (UDP) ports to an application.

Note When you click the **Save** or **Delete** button, the changes are deployed on the device. You cannot review the CLI of the requested operation and also, you cannot remove the operation request from the pending changes queue. If you make any changes in the CLI that starts with the "EMS_" to configure the objects is unsupported and may cause unexpected behavior.

Editing Applications

To assign or un-assign the TCP/UDP ports to an application, follow these steps.

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

Step 2 Select the device from the list or click **Add** to create a new device, then configure the device.

Step 3 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector panel, choose **Zone Based Firewall > Applications**. The Applications page appears.

Step 5 To assign or unassign the TCP/UDP ports to an application, click on the application and update its TCP/UDP ports value.

a. Assign port(s) by defining one or more ports separated by comma (For example: 1234, 2222 and so on).

b. Assign port(s) by defining the port range (For example: 1111-1118). You can also assign a group of ports or port range.

c. Unassign port(s) by deleting the existing port values.

Table 6-20 lists the elements on the Applications page.

Table 6-20 Applications Page

Element	Description
Application Name	Displays the application name that is driven from the device.
TCP Ports	(Optional) The TCP Port values assigned to the specific application
UDP Ports	(Optional) The UDP Port values assigned to the specific application

Step 6 Click **Save** to save the configurations.

Managing Default Parameters

To change the Default Parameters Map, follow these steps.

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

Step 2 Select the device from the list or click **Add** to create a new device, then configure the device.

Step 3 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector panel, choose **Zone Based Firewall > Default Parameters Map**.

Step 5 From the Default Parameters Map page, change the parameters map value.

Note You can change the default parameters only on ISR devices.

Step 6 Click **Save** to save the configuration.

Managing Interfaces

A virtual interface is a logical interface configured with generic configuration information for a specific purpose or configured for a common to specific users. The zone member information is acquired from a RADIUS server, and then the dynamically created interface is made as a member of that zone.

Configuring Interfaces

To assign the interfaces to the zone and un-assign the interface from a specific zone, follow these steps.

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

Step 2 Select the device from the list or click **Add** to create a new device, then configure the device.

Step 3 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector panel, choose **Zone Based Firewall > Interfaces**.

Step 5 In the Interface page, select the interface you want to change and click the down arrow icon. The Zone dialog box appears.

Step 6 In the Zone dialog box, select the new security zone for the interface. If the selected interface is already assigned to a zone, you will get a warning message.

Step 7 Click **Yes** on the warning message if you want to change the assignment of that interface.

Step 8 To un-assign the interface from the specific zone, select the interface and delete the zone information.

Table 6-21 lists the elements on the Interfaces page.

Table 6-21 Interface Page

Element	Description
Interface Name	Displays the interface name.
Zone	The name of the Security-Zone that the interface belongs to.
VRF	The name of the VRF the interface belongs to.

Step 9 Click:

- **Save** to save and apply your changes.
- **Cancel** to exit without saving.

Managing Policy Rules

The policy rule section allows you to create a new firewall policy rule, change the existing policy rule, delete the policy rule, and change the policy rule order. When you create the firewall policy rule, it is up to you to define the location in the policy table.

Creating Policy Rules

To create the policy rules, follow these steps.

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

Step 2 Select the device from the list or click **Add** to create a new device, then configure the device.

Step 3 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector panel, choose **Zone Based Firewall > Policy Rules**. The Firewall Rules page appears.

Step 5 From the Firewall Rules page, click the **Add Rule** button and enter the information, such as Name, Source Zone, Destination Zone, Source IP address, Destination IP address, Service, and Action. The source zone and the destination zone must be different. To move the rules, click on the down arrow icon on the **Add Rule** button. You can place the rule at the top of the list, bottom of the list or move the rule after or before the selected rule in the list.

Note The name field is optional. If you do not provide the name for the firewall rule, the system generates a name for the firewall rule. You cannot use these formats *rule_<number>* or *EMS_rule_<number>* to create the firewall rule name (For example, *rule_1*). These are system reserved formats.

Step 6 To add the source and the destination IP address, click the **add** icon. The Source/Destination IP address dialog box appears.

a. From the Source/Destination IP address dialog box, check the **Any** check box to set the value to any.

a. Enter the source/ destination IP addresses.

b. Click the **Add** button to add the new IP address and the subnet.

c. Click **Delete** to delete the existing value.

d. Click **Ok** to save the configurations.

e. Click **Cancel** to cancel all the changes you have made without sending them to the router.

Step 7 Set the Service values. To add or remove the Application, click the down arrow icon. The Firewall Service dialog box appears.

a. In the Firewall Service dialog box, check the Application check box to select the application to inspect.

b. To select an ACL Based Application, select either the TCP or UDP or ICMP application.

c. Use the navigation arrow buttons to navigate front and back.

d. Click the **plus +** button to save the configurations.

Step 8 Select the appropriate action. The options are: **Drop**, **Drop and Log**, **Inspect**, **Pass**, and **Pass** and **Log**.

Step 9 If you select the action to inspect, click the **Configure** button in the Advance options column. The Advanced Parameters Configuration dialog box appears.

Step 10 In the Advanced Parameters Configuration dialog box, do the following:

a. To customize the device default value, check the parameter check box and set the new value.

b. To apply the device default value, uncheck the parameter check box.

c. To view the firewall rule default parameters, see "Managing Default Parameters" section on page 6-36.

d. When you rest your cursor on the Advanced Options icon, the configured parameters will be displayed in the quick view window.

Table 6-22 lists the elements on the policy rule page.

Table 6-22 Policy Rule Page

Element	Description
Name	(Optional) Enter a name for the policy rule.
Source Zone	Enter the name of the source zone. The source zone specifies the name of the zone from which the traffic is originating.
Destination Zone	Enter the name of the destination zone. The destination zone specifies the name of the router to which the traffic is bound.
Source	Enter the source IP address of the inspected data. The valid parameters are: • Any • IP Address • Subnet
Destination	Enter the destination IP address of the inspected data. The valid parameters are: • Any • IP Address • Subnet
Service	The service of the inspected data. The valid parameters are: • L3/4 Applications, see "Managing Applications" section on page 6-35 • Services "Managing Services" section on page 6-41 • ACL Based application: TCP, UDP, ICMP
Action	Choose the action to perform on the traffic when there is a match on Rule condition. The rule matches when: • The traffic Source IP matches the Source Rule condition. • The traffic Destination IP matches the Destination Rule condition and the traffic inspected Service matches the Service Rule condition. The action options are: • Drop • Drop and Log • Inspect • Pass • Pass and Log
Advance Options	Specify the configuration parameters to set the Firewall Rule Parameter-Map behavior when the Action option is set to Inspect.

Step 11 Click **Save** to apply the rule to the device.

Editing Policy Rule

To edit the existing Policy Rule, follow these steps.

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

Step 2 Select the device from the list or click **Add** to create a new device, then configure the device.

Step 3 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector panel, choose **Zone Based Firewall > Policy Rules**.

Step 5 In the Firewall Rules page, choose one of the following options:

a. Click on the Rules parameters row and edit the parameters. or

b. Check the check box to select the rule, and then click the **Edit** button. The selected Rule entity opens for edit.

Step 6 Click **Save** to apply the changes in the device.

Deleting the Policy Rule

To delete the existing Policy Rule, follow these steps.

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

Step 2 Select the device from the list or click **Add** to create a new device, then configure the device.

Step 3 After selecting the device, click the **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector panel, choose **Zone Based Firewall > Policy Rules**.

Step 5 In the Firewall Rules page, check the check box to select the rules, and then click the **Delete** button.

Step 6 Click **Ok** on the warning message to delete the policy rule. The selected policy rule is deleted from the device.

Changing the Firewall Rule Order

The class-default rules always appear at the bottom of the list and their location is fixed. The regular rules cannot be moved beneath the class-default rules.

To change the Policy Rule order, follow these steps.

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

Step 2 Select the device from the list or click **Add** to create a new device, then configure the device.

Step 3 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector panel, choose **Zone Based Firewall > Policy Rules**.

Step 5 In the Firewall Rules page, to move the rule to a specific row, drag and drop the rule to the new location.

Managing Services

This feature allows you to create, update or delete the service element. You can assign or unassign the TCP/UDP ports to an application.

Creating Services

To create the services, follow these steps.

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

Step 2 Select the device from the list or click **Add** to create a new device, then configure the device.

Step 3 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector panel, choose **Zone Based Firewall > Services.** The Service page appears.

Step 5 In the Service page, click the **Add Service** button to create a new service.

Step 6 In the Service page, enter the Service Name.

Step 7 To assign Applications, click the down arrow icon. The Applications Object Selector dialog box appears.

a. In the Applications dialog box, check the Applications check box to select the applications from the list (can be multiple selection).

b. Click **OK** to accept the changes or **Cancel** to cancel the changes.

Table 6-23 lists the elements on the Service page.

Table 6-23 Service Page

Element	Description
Service Name	Enter the service name. You cannot change the name after creating the service. Also, you cannot create a service without an application.
Application	Displays the list of applications grouped together in the Service.

Step 8 Click **Save** to apply your changes to the device.

Editing Service

To edit the existing service, follow these steps.

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

Step 2 Select the device from the list or click **Add** to create a new device, then configure the device.

Step 3 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector panel, choose **Zone Based Firewall > Services**.

Step 5 In the Service page:

a. Click on the Service parameters row and edit the parameters. or

b. Select the service, and click the **Edit** button. The selected Service entity opens for editing. You can add new applications or remove an already selected application.

c. To remove an application from the selected list, rest your cursor on the application name, and click the **X** icon.

Step 6 Click **Save** to save the configuration.

Deleting the Service

To delete the existing service, follow these steps.

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

Step 2 Select the device from the list or click **Add** to create a new device, then configure the device.

Step 3 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector panel, choose **Zone Based Firewall > Services**.

Step 5 From the Service page, select the service, and then click the **Delete** button.

Step 6 Click **Ok** on the warning message to delete the service. The selected service is deleted.

Creating Security Zone

To create the security zone, follow these steps,

Note The Zone Based Firewall feature is supported on ASR platform from the IOS version 3.5 or later. The Zone Based Firewall feature is supported on ISR platform from the IOS release 12.4(24)T or later.

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

Step 2 Select the device from the list or click **Add** to create a new device, then configure the device.

Step 3 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector panel, choose **Zone Based Firewall > Zones**, and click the **Add Zone** button to create the security zone.

Step 5 In the security zone page, enter the Zone Name.

Step 6 Select the VRF of the zone.

a. VRF selection will affect the interface that can be assigned to the security zone

b. If the user selects the default VRF option, then the security zone can be assigned only to the interfaces that are not related to any other VRF.

Step 7 To assign the interfaces to the security zone, click the down arrow icon. The Interface Object Selector dialog box appears.

a. In the Interface selector dialog box, check the Interface check box to select the interface from the list (can be multiple selection).

b. Click **Ok** to save the configuration.

c. Click **Cancel** to cancel all the changes you have made without sending them to the router.

Step 8 In the Advance options column, click the **Configure** button. The Advanced Parameters Configuration dialog box appears.

Step 9 In the Advanced Parameters Configuration dialog box, do the following:

a. Check the Alert check box and click the **On** radio button to set the alert.

b. Check the Maximum Detection check box to set the maximum detection.

c. Check the TCP SYN-Flood Rate per Destination check box to set the TCP flood rate.

d. Check the Basic Threat Detection Parameters check box and click the **On** radio button to configure the FW drop threat detection rate, FW inspect threat detection rate, and FW SYN attack threat detection rate.

Step 10 Click:

- **Ok** to save configuration.
- **Cancel** to exit without saving.

Step 11 To edit the existing security zone parameters, select the zone, and click the **Configure** button on the Advance options column. The Advanced Parameters Configuration dialog box appears.

Step 12 In the Advanced Parameters Configuration dialog box, edit the values and click **Save** to save the changes. When you rest your cursor on the Advanced Options icon, the configured parameters will be displayed in the quick view window.

Note By default, the Advanced configurations parameters are disabled.

Table 6-24 lists the elements on the Security Zone page.

Table 6-24 Security Zone Page

Element	Description
Zone Name	Enter the zone name.
VRF	Select the VRF of the zone.
Interface	Displays the list of interfaces assigned to the security zone. When there are more than two interfaces, you can place the mouse on the icon to view full list.
Advance Options	Configure the advanced parameters such as Alert, Maximum Detection, TCP Synchronize-Flood Rate Per Destination, and Basic Threat Detection.
Description	(Optional) Enter the description for the zone.

Step 13 Enter the description for the zone.

Step 14 Click:

- **Save** to save the changes.
- **Cancel** to exit without saving.

Editing Security Zone

To edit the existing security zone, follow these steps.

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

Step 2 Select the device from the list or click **Add** to create a new device, then configure the device.

Step 3 After selecting the device, click the **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector left panel, choose **Zone Based Firewall > Zones**.

Step 5 In the Security Zone page, choose one of the following options:

a. Click on the Zone parameters row, and edit the parameters. or

b. Select the zone, and click the **Edit** button. The selected Zone entity opens for editing.

Step 6 Click the **add** icon to assign the interface to the zone or to un-assign the existing interfaces from the zone You can also change the Description of the zone.

Step 7 Click **Save** to save the configuration.

Deleting the Security Zone

To delete the existing security zone, follow these steps.

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

Step 2 Select the device from the list or click **Add** to create a new device, then configure the device.

Step 3 After selecting the device, click the **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector panel, choose **Zone Based Firewall > Zones**.

Step 5 In the Security Zone page, select the security zone, and then click the **Delete** button.

Step 6 Click **Ok** on the warning message to delete the security zone. The selected zone is deleted.

Configuring Default-Zone

To configure the default zone, follow these steps.

Note The Default-Zone feature is supported only on ASR platform.

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

Step 2 Select the device from the list or click **Add** to create a new device, then configure the device.

Step 3 After selecting the device, click **Configuration**. The Feature Selector panel appears.

Step 4 From the Feature Selector panel, choose **Zone Based Firewall > Zones**.

Step 5 In the Security Zone page, click the **Default Zone** button to enable or disable the default security zone in the device. The device will host all the interfaces that are not related to any zone.

Step 6 Click **OK** to save the configuration.

Using Reports for Monitoring

Prime NCS (WAN) reporting helps you monitor the system and network health as well as troubleshoot problems. Reports can be run immediately or scheduled to run at a time you specify. Once defined, the reports can be saved for future diagnostic use or scheduled to run and report on a regular basis.

Reports are saved in either CSV or PDF format and are either saved to a file on Prime NCS (WAN) for later download or e-mailed to a specific e-mail address.

Choose **Tools > Reports > Report Launch Pad** to view the list of available reports.

Tip Rest your cursor on the information icon next to the report type to view report details.

Creating and Running New Reports

Step 1 Choose **Tools > Reports > Report Launch Pad**.

Step 2 Click **New** next to the report you want to create.

Step 3 Enter report details, then click

- **Save**—To save this report setup without immediately running the report. The report will automatically run at the scheduled time.
- **Save and Run**—To save this report setup and to immediately run the report.
- **Run**—To run the report without saving the report setup.
- **Save and Export**—To save the report and export the results to either CSV or PDF format.
- **Save and Email**—To save the report and e-mail the results.

Viewing Scheduled Reports

To view and manage all currently scheduled reports, choose **Tools > Reports > Scheduled Run Results**.

Viewing Saved Report Templates

When you have created a report that contains all the parameters necessary, you can save that report template.

Step 1 Choose **Tools > Reports > Saved Report Templates**.

Step 2 Choose which saved report template to show by selecting from the following fields:

- Report Category—Choose the appropriate report category from the drop-down list or choose **All**.
- Report Type—Choose the appropriate report type from the drop-down list or choose **All**. The Report Type selections change depending on the selected report category.
- Scheduled—Choose **All**, **Enabled**, **Disabled**, or **Expired** to filter the Saved Report Templates list by scheduled status.

Using Packet Capture for Monitoring and Troubleshooting

Prime NCS (WAN) allows you to run capture traffic in your network to help monitor network usage, gather network statistics, and analyze network problems.

Step 1 Choose **Tools > Packet Capture**, then click **Create**.

Step 2 Specify the required capture session parameters, then click **Create**.

Diagnosing Site Connectivity Issues

You can use the Prime NCS (WAN) dahsboards to monitor your network and locate problematic devices in your network, and then use the Device Workcenter to change the device configuration.

Step 1 Choose **Operate > Detailed Dashboards**, choose the site for which you are experiencing connectivity issues, then click **Go**.

Step 2 View data reported under Device Reachability Status and Top *N* Devices with Most Alarms to determine the source of the issue.

Step 3 Click on the name of the device for which you see the most alarms. This launches the 360-degree view of the device.

Step 4 Click the Alarm Browser icon to view the alarms for that device. Expand the alarm to view details for the alarm.

Step 5 To compare the configuration on the device to a previously known good configuration, choose **Operate > Device Work Center**, then select the device whose configuration you want to change.

Step 6 Click the Configuration Archive tab, expand the arrow to view additional options, then select the configuration type and a configuration against which to compare.

Step 7 Change or rollback the configuration. See Rolling Back Device Configuration Versions for more information.

CHAPTER 7

Monitoring Alarms

An ***alarm*** is a Prime NCS (WAN) response to one or more related events. If an event is considered of high enough severity (critical, major, minor, or warning), Prime NCS (WAN) raises an alarm until the resulting condition no longer occurs.

What is an Event?

An *event* is an occurrence or detection of some condition in and around the network. An event is a distinct incident that occurs at a specific point in time. Examples of events include:

- Port status change
- Device reset
- Device becomes unreachable by the management station

An event can also be a:

- Possible symptom of a fault that is an error, failure, or exceptional condition in the network. For example, when a device becomes unreachable, an unreachable event is triggered.
- Possible symptom of a fault clearing. For example, when a device state changes from unreachable to reachable, a reachable event is triggered.

One or more events may generate an abnormal state or alarm. The alarm can be cleared, but the event remains. You can view the list of events using the Event Browser.

Choose **Operate > Alarms & Events**, then click Events to access the Events Browser page.

Event Creation

Prime NCS (WAN) maintains an event catalog and decides how and when an event is created and whether to associate an alarm with the event. Multiple events can be associated to the same alarm.

Prime NCS (WAN) discovers events in the following ways:

- By receiving notification events and analyzing them; for example, syslog and traps.
- By automatically polling devices and discovering changes; for example, device unreachable.
- By receiving events when a significant change occurs in the Prime NCS (WAN) server; for example, rebooting the server.
- By receiving events when the status of the alarm is changed; for example when the user acknowledges or clears an alarm.

Incoming event notifications (traps and syslogs) are identified by matching the event data to predefined patterns. A trap or syslog is considered supported by Prime NCS (WAN) if it has matching patterns and can be properly identified. If the event data does not match with predefined patterns, the event is considered as unsupported and it is dropped.

Faults are discovered by Prime NCS (WAN) through polling, traps, or syslog messages. Prime NCS (WAN) maintains the context of all faults and ensures that duplicate events or alarms are not maintained in the Prime NCS (WAN) database.

The following table provides examples of when Prime NCS (WAN) creates an event.

Time	Event	Prime NCS (WAN) Behavior
10:00AM PDT December 1, 2011	Device A becomes unreachable.	Creates a new unreachable event on device A.
10:30AM PDT December 1, 2011	Device A continues to be unreachable.	No change in the event status.
10:45AM PDT December 1, 2011	Device A becomes reachable.	Creates a new reachable event on device A.
11:00AM PDT December 1, 2011	Device A stays reachable.	No change in the event status.
12:00AM PDT December 1, 2011	Device A becomes unreachable.	Creates a new unreachable event on device A.

What is an Alarm?

An *alarm* is a Prime NCS (WAN) response to one or more related events. If an event is considered of high enough severity (critical, major, minor, or warning), Prime NCS (WAN) raises an alarm until the resulting condition no longer occurs.

One or more events can result in a single alarm being raised. An alarm is created in the following sequence:

1. A notification is triggered when a fault occurs in the network.
2. An event is created, based on the notification.
3. An alarm is created after checking if there is no active alarm corresponding to this event.

An alarm is associated with two types of events:

- Active events: Events that have not been cleared. An alarm remains in this state until the fault is resolved in a network.
- Historical events: Events that have been cleared. An event changes its state to an historical event when the fault is resolved in a network.

After an alarm is cleared, it indicates the end of an alarm life cycle. A cleared alarm can be revived if the same fault reoccurs within a preset period of time. The present period is set to 5 minutes in Prime NCS (WAN).

Event and Alarm Association

Prime NCS (WAN) maintains a catalog of events and alarms. The catalog contains the list of events managed by Prime NCS (WAN), and the relationship among the events and alarms. Events of different types can be attached to the same alarm type.

When a notification is received:

1. Prime NCS (WAN) compares an incoming notification against the event and alarm catalog.
2. Prime NCS (WAN) decides whether an event has to be raised.

3. If an event is raised, Prime NCS (WAN) decides whether the event triggers a new alarm or associates it to an existing alarm.

A new event is associated with an existing alarm, if the new event triggered is of the same type and occurs on the same source.

For example, an active interface error alarm. The interface error events that occur at the same interface, are all associated to the same alarm.

Alarm Status

The following are the supported statuses for an alarm:

- New—When an event triggers a new alarm or an event is associated with an existing alarm.
- Acknowledged—When you acknowledge an alarm, the status changes from New to Acknowledged.
- Cleared—An alarm can be in these statuses:
  - Auto-clear from the device—The fault is resolved on the device and an event is triggered for the same. For example, a device-reachable event clears the device-unreachable event. This in-turn, clears the device-unreachable alarm.
  - Manual-clear from Prime NCS (WAN) users: You can manually clear an active alarm without resolving the fault in the network. A clearing event is triggered and this event clears the alarm.

    If the fault continues to exist in the network, a new event and alarm are created subsequently based on the event notification (traps/syslogs).

Event and Alarm Severity

Each event has an assigned severity. Events fall broadly into the following severity categories, each with their associated color in Prime NCS (WAN):

- Flagging—Indicates a fault: Critical (red), Major (orange), Minor (yellow), or Warning (sky blue).
- Informational—Info (blue). Some of the Informational events clear the flagging events.

For example, a Link Down event might be assigned a Critical severity, while its corresponding Link Up event will be an Informational severity.

In a sequence of events, the event with the highest severity determines the severity of the alarm.

Finding Alarms

Table 7-1lists the places where you can find alarms.

Table 7-1 Where to Find Alarms

Location in GUI	Description
Operate > Alarms & Events	Displays a new page listing all alarms with details such as severity, status, source, timestamp. You can change the status of alarms, assign, annotate, delete, and specify email notifications from this page.
Rest your cursor on **Alarm Summary**	Displays a table listing the critical, major, and minor alarms currently detected by Prime NCS (WAN).
Alarm Browser	Opens a window that displays the same information as in the **Operate > Alarms & Events** but does not take you to a new page.

Table 7-1 Where to Find Alarms (continued)

Location in GUI	Description
From device 360° view	Click the Alarms tab to view alarms on the device, their status and category, or click the Alarm Browser icon to launch the Alarm Browser.
Operate > Monitoring Dashboard > Incidents	Displays dashlets that contain alarm summary information, top sites with the most alarms, top alarm types, top events, and top interfaces with issues.

Defining Thresholds

You use monitoring templates to define thresholds. When the thresholds you specify are reached, Prime NCS (WAN) issues an alarm.

To define thresholds:

Step 1 Choose **Design > Monitoring Templates**.

Step 2 Under Features, choose **Threshold**.

Step 3 Complete the basic template fields.

Step 4 Under Feature Category, choose one of the following metrics:

- Device Health—allows you to change threshold values for CPU utilization, memory pool utilization, and environment temperature
- Interface Health—allows you to change threshold values for the number of outbound packets which are discarded.

Step 5 Under Metric Parameters, choose the threshold setting you want to change, then click **Edit Threshold Setting**.

Step 6 Enter a new value and choose the alarm severity for the threshold.

Step 7 Click **Done**.

Step 8 Click **Save as New Template**.

Step 9 Under the My Templates folder, navigate to the template you created and select it.

Step 10 Click **Go to Deployment**.

Step 11 Choose the template you created, then click **Deploy**.

Changing Alarm Status

The view a single alarm, its associated events, and to change the alarm status:

Step 1 Choose **Operate > Alarms & Events**.

Step 2 Click the expand icon next to the alarm for which you want to view details.

Step 3 Choose **Change Status > Acknowledge** or **Clear**.

Acknowledged and **Cleared** alarms are removed from the list of alarms. No emails are generated for these alarms after you have marked them as acknowledged or cleared.

By default, acknowledged and cleared alarms are not included for any search criteria. To change this default, choose **Administration > System > Alarms and Events** and disable the Hide Acknowledged Alarms or Hide Cleared Alarms preference.

Cleared alarms remain in the Prime NCS (WAN) database, but in the Clear state. You clear an alarm when the condition that caused it no longer exists.

When to Acknowledge Alarms

You may want certain alarms to be removed from the Alarms List. For example, if you are continuously receiving an interference alarm from a certain device, you may want to stop that device from being counted as an active alarm on the Alarm Summary page or any alarms list. In this scenario, you can find the alarm for the device in the Alarms list, select the check box, and choose **Acknowledge** from the Select a command drop-down list.

Now if the device generates a new violation on the same interface, Prime NCS (WAN) will not create a new alarm, and the Alarm Summary page shows no new alarms. However, if the interference violation is created on another interface, a new alarm is created.

By default, acknowledged alarms are not displayed in either the Alarm Summary page or any alarm list page. Also, no emails are generated for these alarms after you have marked them as acknowledged. By default, acknowledged alarms are not included for any search criteria. To change this default, go to the **Administration > System > Alarms and Events** page and disable the **Hide Acknowledged Alarms** preference.

When you acknowledge an alarm, the following warning appears as a reminder that a recurrence of the problem does not generate another alarm unless this functionality is disabled.

Note When you acknowledge an alarm, a warning displays as a reminder that a recurrence of the problem does not generate another alarm unless this functionality is disabled. Use the **Administration > User Preferences** page to disable this warning message.

You can also search for all previously acknowledged alarms to reveal the alarms that were acknowledged during the last seven days. Prime NCS (WAN) automatically deletes cleared alerts that are more than seven days old so your results can only show activity for the last seven days. Until an existing alarm is deleted, a new alarm cannot be generated for any managed entity for which Prime NCS (WAN) has already generated an alarm.

Setting Alarm Display Options

To change alarm and event options such as when alarms are deleted, which alarm severities are displayed, and alarm email options:

Step 1 Choose **Administration > System > Alarms and Events**.

Step 2 Change the necessary settings for the alarms.

Step 3 Click **Save**.

Configuring Alarm Severity Levels

To configure the severity level for newly generated alarms:

Step 1 Choose **Administration > System**.

Step 2 From the left sidebar menu, choose **Severity Configuration**.

Step 3 Select the check box of the alarm condition whose severity level you want to change.

Step 4 From the Configure Security Level drop-down list, choose from the following severity levels:

- Critical
- Major
- Minor
- Warning
- Informational
- Reset to Default

Step 5 Click **Go**.

Step 6 Click **OK** to confirm the changes.

CHAPTER 8

Updating Device Inventory

Prime NCS (WAN) 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 8-1.

Table 8-1 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.

Table 8-1 Discovery Settings (continued)

Field	Description
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.
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 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.

Table 8-1 Discovery Settings (continued)

Field	Description
Preferred Management	
IP Method	• Use Loopback • Use SysName • Use DNSReverseLookup

Step 3 Click:

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

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 8-1, 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 view the discovery process:

Step 1 Choose **Operate > Discovery**.

Step 2 Select the discovery job for which you want to view details and the details are shown.

Repeating Discovery

The following steps explain how to repeat a discovery using your existing settings and how to monitor the job as it progresses.

Step 1 Choose **Operate > Discovery**.

Discovery Protocols and CSV File Formats

Prime NCS (WAN) 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 8-2 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. See Supported Browsers for more information.

Table 8-2 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 add devices manually as shown in the following steps:

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 NCS (WAN).

The following task explains how to add devices in bulk from an existing CSV file.

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 Choose **Tools > Task Manager > Jobs Dashboard** to view the status of the import.

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

Troubleshooting Unmanaged Devices

Table 8-3 describes the possible reasons a device is unmanageable by Prime NCS (WAN):

Table 8-3 Reasons for Unmanageable Device

Possible Cause	Actions
Prime NCS (WAN) cannot reach the device because the device is down or because any device along the path from the Prime NCS (WAN) server to the device is down.	• Use the ping and traceroute tools to verify that the Prime NCS (WAN) can reach the device. See Using 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 NCS (WAN). **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 NCS (WAN): 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 NCS (WAN). • Re-enter the SNMP credentials in Prime NCS (WAN), then resync the device. (Chose **Operate > Device Work Center**, select the device, then click **Sync**.) See Synchronizing Devices for more information.
Prime NCS (WAN) 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 NCS (WAN). (Chose **Operate > Device Work Center**, select the device, then click **Edit**.) **Note** If the device type requires HTTP, verify that the Prime NCS (WAN) 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 NCS (WAN) 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 NCS (WAN). • Verify that the authorization level configured for the Telnet/SSH user is not limited to lower enable privilege levels.

Table 8-3 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 NCS (WAN) 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

Using Device Groups

By default, Prime NCS (WAN) 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 a New Device Group 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

Table 8-4 describes how to create a new device group.

Table 8-4 Steps to Create a Device Group

Task	Additional Information
1. Create a new device group.	Defines general information about the new group, such as the group name and parent group assigned to this group. For more information, see Creating a New Device Group.
2. Assign devices to the device group.	Assigns devices to the group so they can inherit the group settings. For more information, see Assigning Devices to a Group.
3. Perform operations on the device group.	You can perform tasks that apply to all devices that are a member of the group.

Creating a New Device Group

Before you create a 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** to add the device to the selected group.
- **Cancel** to exit without saving your changes.

Synchronizing Devices

You can force an inventory collection in order to sync the Prime NCS (WAN) 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 NCS (WAN) database.

Step 3 Click **Sync**.

CHAPTER 9

Changing Port Groups

As you add and remove devices and modules, you will need to create new port groups and change existing port groups.

By default, Prime NCS (WAN) creates rule-based port groups and assigns ports or interfaces to the appropriate Port Group folder. You cannot edit these port groups. You can view the rules for the port group by resting your cursor on the port group folder.

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

- Static—You create and name a new port group to which you can add devices using the **Add to Group** button from **Operate > Port Grouping**.
- Dynamic—You create and name a new port group and specify the rules to which ports or interfaces must comply in order to be added to this port group.

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.

Updating Port Groups

To create a new dynamic port group:

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

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

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

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

Step 5 If you are creating a dynamic port group, you can specify the following rules that the ports or interfaces must match to be added to the group:

- Name—Enter the interface name configured on the device.
- Description—Enter a description of the interface.
- Speed—Enter the interface speed in bps. For example, if you specify *speed is exactly (or equals) 10000000*, the speed is 10 Mbps.
- Type—Select the interface type.

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

Deleting a Port Group

To delete a port group:

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

Step 2 Rest your cursor on the name of the name of the port group you want to delete, then click Delete Group.

Note If you are deleting a static port group, make sure the static port group does not contain any subgroups or members.

If you are deleting a dynamic port group, make sure the dynamic port group does not contain any subgroups; however, the dynamic group can be associated with members.

CHAPTER 10

Working with Device Configurations

Prime NCS (WAN) provides information such as the date of last configuration change, status of the configuration jobs, summary of inventory configuration protocol, etc.

About Configuration Archives

Prime NCS (WAN) attempts to collect and archive the following device configuration files:

- Startup configuration
- Running configuration
- VLAN configuration, if configured

You can specify how Prime NCS (WAN) archives the configurations:

- On demand— You can have Prime NCS (WAN) collect the configurations of selected devices by selecting **Operate > Configuration Archives**.
- During inventory—You can have Prime NCS (WAN) collected device configurations during the inventory collection process. See Device Configuration Settings for more information.
- Based on Syslogs— If device is configured to send syslogs, when there is any device configuration change, Prime NCS (WAN) collects and stores the configuration.

Device Configuration Settings

By default, Prime NCS (WAN) has the following configuration settings:

- Does not backup the running configuration before pushing configuration changes to a device.
- Does not have Prime NCS (WAN) attempt to roll back to the previously saved configuration in the archive if the configuration deployment fails
- When pushing CLI to a device, uses 5 thread pools.

To change the default configuration settings:

Step 1 Choose **Administration > System**, then click **Configuration**.

- Select **Backup Running Configuration** to have Prime NCS (WAN) backup the running configuration before pushing configuration changes to a device.

- Select **Rollback Configuration** to have Prime NCS (WAN) attempt to roll back to the previously saved configuration in the archive if the configuration deployment fails.

Step 2 Click **Save**.

Finding and Comparing Device Configurations

The following steps explain how to view a current device configuration, view its contents, and compare the current configuration with a previous version.

Step 1 Choose **Operate > Configuration Archives**.

Step 2 Click the expand icon for the device whose configuration you want to view. Then click the expand icon again to view the specific configuration version you want to compare.

Step 3 Under the Compare With column, choose the configuration for which you want to compare the configuration you selected in the previous step:

- Previous—Compares the selected version with the previously archived configuration.
- StartUp—Compares the selected version with the start up configuration.
- Other Version—Allows you to select with which version to compare the selected version.
- Other Device—Allows you to compare the selected configuration with the configuration from another device.

A report appears showing the differences between the configurations. The color key on the bottom describes the colors used in the configuration comparison.

Changing Device Configurations

You can change a device's configuration in two ways:

- **Operate > Device Work Center**—Use the Device Work Center to change the configuration of a single device. See Changing a Single Device Configuration.
- **Design > Configuration Template**—To change the configuration of more than one device and apply a common set of changes, use a configuration template to make the changes.

  Prime NCS (WAN) provides the following default configuration templates:

  - CLI templates—CLI templates are user-defined and created based on your own parameters. CLI templates allow you to select the elements in the configurations. Prime NCS (WAN) provides variables which you replace with actual values and logic statements. You can also import templates from Cisco Prime LAN Management System. See Creating and Deploying CLI Templates.
  - Feature and technology templates—Feature templates are configurations that are specific to a feature or technology in a device's configuration. See Creating and Deploying Feature and Technology Templates.

– Composite templates—Composite templates are two or more feature or CLI templates grouped together into one template. You specify the order in which the templates contained in the composite template are deployed to devices. See Creating and Deploying Composite Templates for Branch Deployment.

Changing a Single Device Configuration

Step 1 Choose **Operate > Device Work Center**, then click on a device name. The device details appear on the lower part of the screen.

Step 2 Click the Configuration tab. The Feature Selector displays the values, organized into features, for the device you selected.

Step 3 Select the feature you want to change, then make the necessary changes.

Step 4 Click **Save** to save your configuration changes in the Prime NCS (WAN) database.

Step 5 Click:

- The Configuration Updates CLI Preview icon to view the CLI that was generated for the change you specified.
- The Cancel Pending Deployment CLI icon to undo the change you made.
- The Schedule Deploy icon to push the change to the device immediately or schedule when to deploy the change. You can also specify the job name.

Step 6 Click **Tools > Jobs Dashboard** to view the status of the configuration change.

About Configuration Rollbacks

You can change the configuration on a device with a configuration stored in Prime NCS (WAN). You can select multiple archived versions or a single archived version to which you want to "rollback."

During the configuration rollback process, the configuration is converted into a set of commands which are them executed sequentially on the device.

When rolling back a configuration file you can specify the following options:

- The type of configuration file to which to rollback, for example running or startup configuration
- Whether to sync the running and startup configurations after rolling back the running configuration
- If rolling back a startup configuration only, specify to reboot the device so that startup configuration becomes the running configuration
- Before rolling back the configuration, specify whether to create new archived versions

Rolling Back Device Configuration Versions

You can use Prime NCS (WAN) to rollback a device's configuration to a previous version of the configuration.

To roll back a configuration change.

Step 1 Choose **Operate > Configuration Archives**.

Step 2 Click the expand icon for the device whose configuration you want to roll back.

Step 3 Click the specific configuration version you want to roll back, then click **Schedule Rollback**.

Step 4 Specify the rollback options.

Step 5 Specify the scheduling options.

Step 6 Click **Submit**.

Deleting Device Configurations

By default, Prime NCS (WAN) archives up to five device configuration versions for each device for seven days after:

- Every inventory collection
- Prime NCS (WAN) receives a configuration change event

You cannot delete configuration versions, but older configuration versions are replaced by newer configuration versions.

To change the number of configurations that Prime NCS (WAN) retains:

Step 1 Choose **Administration > System**, then click **Configuration Archive**.

Step 2 Enter a new value in the Number of Versions field. To archive an unlimited number of configuration versions, uncheck **Number of version to retain** and **Number of days to retain**.

Step 3 Click **Save**.

CHAPTER 11

Maintaining Device Configuration Inventory

Using the Device Configuration Archive

When Prime NCS (WAN) discovers the devices in your network, it retrieves and stores the device configurations. When you make a change to a device configuration, Prime NCS (WAN) stores the previous version as well as the current version. Prime NCS (WAN) stores all device configuration versions.

You can perform configuration archive tasks in two places:

- **Operate > Configuration Archives**—Lists all configuration archives by device type, site group, or user-defined group. You can schedule archives, rollbacks, and view details of configurations.
- **Operate > Device Work Center**—View a specific device's archived configurations, schedule a configuration rollback, and schedule archive collections for a specific device.

Changing Configuration Archive Settings

By default, Prime NCS (WAN) archives up to five device configuration versions for each device for seven days after:

- Every inventory collection
- Prime NCS (WAN) receives a configuration change event

To change when Prime NCS (WAN) archives configurations:

Step 1 Choose **Administration > System**, then click **Configuration Archive**.

Step 2 Change the necessary settings. To archive an unlimited number of configuration versions, uncheck **Number of version to retain** and **Number of days to retain**.

Step 3 To have Prime NCS (WAN) ignore commands for a particular device type, click the **Advanced** tab, choose the device type, and enter the commands to be ignored. If the device you specify has a change in its configuration and Prime NCS (WAN) detects that the change is in one of the commands in the exclude list, Prime NCS (WAN) does not create an archived version of the configuration with this change.

Step 4 Click **Save**.

Scheduling Configuration Archive Collection

To specify when to archive configurations:

Step 1 Choose **Operate > Configuration Archives**.

Step 2 Choose the device(s) whose configuration you want to archive, then click **Schedule Archive**. The Configuration Archive Schedule window appears.

Step 3 Enter the parameters for when you want to archive the configuration.

Step 4 Click:

- **Save** to save your changes.
- **Close** to exit without saving your changes.

Step 5 To view the progress of the configuration archive job, choose **Tools > Task Manager > Jobs Dashboard**.

Rolling Back Configuration Changes

You can use Prime NCS (WAN) to rollback a device's configuration to a previous version of the configuration.

The following steps explain how to roll back a configuration change.

Step 1 Choose **Operate > Configuration Archives**.

Step 2 Click the expand icon for the device whose configuration you want to roll back.

Step 3 Click the specific configuration version you want to roll back, then click **Schedule Rollback**.

Step 4 Specify the rollback options.

Step 5 Specify the scheduling options.

Step 6 Click **Submit**.

CHAPTER 12

Keeping Sites Organized

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 allow you to segment the physical structure of your network and monitor your network based on location.

As your organization changes, you need to change your sites. There are two areas in which you must 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.

Updating Sites

The following steps explain how to edit your sites and their parameters such as campuses and buildings.

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

Step 2 Choose the campus or building you want to change.

- If you select a campus, you can add a building or edit or delete the campus.
- If you select a building, you can edit, delete, or copy the building.

Step 3 Change any settings.

Removing Campuses or Buildings

Deleting a campus deletes all buildings assigned to the campus, but deleting a campus does not remove the inventory assigned to the campus.

To delete a campus or building:

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

Step 2 Choose the campus or building you want to remove.

Step 3 From the command menu, choose **Delete**, and then click **Go**.

Associating Devices to Sites

After you have created site profiles, you can assign devices to those sites. By associating devices with a campus or buildings, 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 the 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 choose **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 Setting Up Site Profiles for more information.

CHAPTER 13

Maintaining Software Images

Manually upgrading your devices to the latest software version can be error prone and time consuming. Prime NCS (WAN) simplifies the version management and routine deployment of software updates to your devices by helping you plan, schedule, download, and monitoring software image updates.

Prime NCS (WAN) stores all the software images for the devices in your network. The images are stored according to the image type and version.

Before you can upgrade software images, your devices must be configured with SNMP read-write community strings that match the community strings entered when the device was added to Prime NCS (WAN).

Setting Image Management and Distribution Preferences

You can specify image management preferences such as whether to reboot devices after successfully upgrading a software image, and whether images on Cisco.com should be included during image recommendation of the device.

Because collecting software images can slow the data collection process, by default, Prime NCS (WAN) does not collect and store device software images when it gathers inventory data from devices.

To change the default behavior and to specify additional image management preferences:

Step 1 Choose **Administration > System > Image Management**.

Step 2 Enter your Cisco.com user name and password so you can access software images from the cisco.com web site.

Step 3 To have Prime NCS (WAN) automatically retrieve and store device images when it collects device inventory data, check **Collect images along with inventory collection**.

Step 4 Select other options as necessary. Rest your cursor on the information icon to view details about the options.

Step 5 Click **Save**.

Step 6 Choose **Operate > Software Image Management > Image Dashboard** to view all the software images retrieved by Prime NCS (WAN). The images are organized by image type and stored in the corresponding software image group folder.

Using the Software Image Dashboard

The software image dashboard displays the top software images used in your network and allows you to change image requirements, see the devices on which an image is running, and distribute images.

Step 1 Choose **Operate > Software Image Management > Image Dashboard**.

Step 2 Click on a software image name to display details about the image.

Step 3 You can perform the following actions:

- Change image requirements. See Changing Software Image Requirements.
- View the devices on which the software image is running.
- Distribute the image. See Distributing Software Images.

Importing Software Images

It can be helpful to have a baseline of your network images by importing images from the devices in your network. You can also import software images from Cisco.com and store them in the image repository.

By default, Prime NCS (WAN) does not automatically retrieve and store device images when it collects device inventory data. (You can change this preference as described in Setting Image Management and Distribution Preferences.)

To import a software image:

Step 1 Choose **Operate > Software Image Management**.

Step 2 Click **Import**.

Step 3 Specify the source from where to import the software image:

- Device—Click on a device from the Collection Options field from which to import an image.
- Cisco.com—Provide your Cisco.com login credentials to import an image from Cisco.com. You must choose the device platform from which to retrieve the image, the image version, and the feature package.
- URL—Specify a URL from where to import an image.
- File—Browse to a file location from where to import an image.

Step 4 Specify Collection Options and when to import the image file. You can run the job immediately or schedule it to run at a later time.

Note The image import job is non-repetitive.

Step 5 Click **Submit**.

Step 6 Choose **Tools > Task Manager > Jobs Dashboard** to view details for the image management job.

Changing Software Image Requirements

To change the RAM, Flash, and boot ROM requirements that a device must meet in order for a software image to be distributed to the device:

Step 1 Choose **Operate > Software Image Management**.

Step 2 Navigate to and select the software image for which you want to change requirements, then click **Image Details**.

Step 3 Change any of the following fields:

- Minimum RAM (MB)—Minimum RAM that must be available on the device to store this image.
- Minimum Flash (MB)—Minimum Flash that must be available on the device to store this image.
- Minimum Boot ROM Version—Minimum boot ROM version required on the device to store this image.

Step 4 Click **Save**. Your changes are saved in the software version in which you made the change.

Distributing Software Images

You can distribute a software image to a device or set of similar devices in a single deployment. Prime NCS (WAN) verifies that the device and software image are compatible.

Step 1 Choose **Operate > Software Image Management**.

Step 2 Select the software image(s) you want to distribute, then click **Distribute**.

Step 3 By default, the devices for which the selected image is applicable are shown. Check **Show All Devices** to see all the devices available in Prime NCS (WAN), or from the Device Groups list, select the device(s) which are running the image you selected.

Note If you check **Show All Devices**, all devices are displayed even if the software image you selected is not applicable for all the devices.

Step 4 Click the image name in Distribute Image Name field to change your selection and pick a new image, then click **Save**.

Step 5 To change the location on the device in which to store the software image, click the value displayed in Distribute Location field, select a new location, then click **Save**.

The Status and Status Message fields display the validity of the selections you made. For example, if the status is green, there is adequate space available to store the image on the specified location on the device.

Step 6 Specify Distribution Options. You can change the default options in **Administration > System > Image Management**.

Step 7 Specify schedule options, then click **Submit**.

Note The distribute image job is non-repetitive.

Step 8 Choose **Tools > Task Manager > Jobs Dashboard** to view details for the image management job.

Distributing Software Images from Cisco.com

Step 1 Choose **Operate > Software Image Management**.

Step 2 Navigate to and select the software image for which you want to change requirements, then click **Image Details**.

Step 3 Expand Device Details, select a device or devices on which to distribute the image, then click **Distribute**.

Note Only the devices that are running the specific software image you modified are displayed as selection choices.

Step 4 Choose one of the following image sources:

- **Recommend Image from Cisco.com** to select an image available on Cisco.com. Specify options, then click **Start Recommendation**, then skip to Step 6.
- **Select Image from Local Repository** to select an image stored locally. Then, under Local Repository:
  - Select **Show All Images** to display all images available in the Prime NCS (WAN) repository.
  - Uncheck **Show All Images** to display the software images applicable to the selected device.

Step 5 Select the image to distribute, then click **Apply**. The device name, IP address, and image details appear.

Step 6 Click the image name in Distribute Image Name field to change your selection and pick a new image, then click **Save**.

Step 7 To change the location on the device in which to store the software image, click the value displayed in Distribute Location field, select a new location, then click **Save**.

The Status and Status Message fields display the validity of the selections you made. For example, if the status is green, there is adequate space available to store the image on the specified location on the device.

Step 8 Specify Distribution Options. You can change the default options in **Administration > System > Image Management**.

Step 9 Specify schedule options, then click **Submit**.

Viewing Recommended Software Images

You can view the recommended software image for a single device, and then import or distribute that image. If you want to distribute a software image to multiple devices, see Distributing Software Images.

Step 1 Choose **Operate > Device Work Center**, then select a device for which you want to view the recommended software image.

Step 2 Click the **Image** tab.

Step 3 Scroll down to Recommended Images to view the recommended image for the device you selected. Prime NCS (WAN) gathers the recommended images from both Cisco.com and from the local repository.

Step 4 You can import the recommended image (see Importing Software Images) or distribute (see Distributing Software Images) the recommended image.

Analyzing Software Image Upgrades

Prime NCS (WAN) can generate an Upgrade Analysis report to help you determine prerequisites for a new software image deployment. These reports analyze the software images to determine the hardware upgrades (boot ROM, Flash memory, RAM, and boot Flash, if applicable) required before you can perform the software upgrade.

The Upgrade Analysis report answers the following questions:

- Does the device have sufficient RAM to hold the new software?
- Is the device's Flash memory large enough to hold the new software?
- Do I need to add Telnet access information for the device?

To run the Upgrade Analysis report:

Step 1 Choose **Operate > Software Image Management**.

Step 2 Click **Upgrade Analysis**.

Step 3 Choose the source of the software image you want to analyze:

- Local repository
- Cisco.com. You must enter for your Cisco.com login credentials.

Step 4 Select the devices on which to analyze the software image.

Step 5 Select the image(s) to analyze for the selected devices.

Step 6 Click **Run Report**.

PART 4

Administering

This part contains the following sections:

CHAPTER 14

Maintaining System Health

This chapter contains the following sections:

Monitoring System Health

To view the system health dashboards, choose **Administration > Admin Dashboard**. Table 14-1 describes the information displayed on the dashboards.

Table 14-1 **Administration > Admin Dashboard Information**

Health Information Displayed	Description
System Health	Displays memory and CPU health information over a period of time.
System Events	Displays a list of events, time the event occurred, and the severity of the event.
System Information	Displays general system health information such as the server name, number of jobs scheduled and running, the number of supported MIB variables, number of users logged in, etc.

Using System Logs

Prime NCS (WAN) logs all error, informational, and trace messages generated by all devices that are managed by Prime NCS (WAN).

Prime NCS (WAN) also logs all SNMP messages and Syslogs it receives.

You can download and email the logs to use for troubleshooting Prime NCS (WAN).

Step 1 Choose **Administration > Logging**. The General Logging Options Screen appears.

Step 2 Choose a Message Level:

- Error
- Information
- Trace

Step 3 Check the check boxes within the Enable Log Module option to enable various administration modules. Check the **Log Modules** option to select all modules.

Step 4 In the Log File Settings portion, enter the following settings. These settings will be effective after restarting Prime NCS (WAN).

- Maximum file size—Maximum number of MBs allowed per log file.
- Number of files—Maximum number of log files allowed.
- File prefix—Log file prefix, which can include the characters "%g" to sequentially number of files.

Step 5 Click the Download button to download the log file to your local machine.

Note The logs.zip filename includes a prefix with the host name, date, and time so that you can easily identify the stored log file. Included in the zip file is an html file that documents the log files.

Step 6 Enter the Email ID or Email IDs separated by commas to send the log file.

Note To send the log file in a mail you must have Email Server Configured.

Step 7 Click **Submit**.

Changing SNMP Logging Options

Step 1 Choose **Administration > Logging**, then click SNMP Logging Options.

Step 2 Check the **Enable SNMP Trace** check box to enable sending SNMP messages (along with traps) between devices and Prime NCS (WAN).

Step 3 Check the **Display Values** check box to see the SNMP message values.

Step 4 Configure the IP address or IP addresses to trace the SNMP traps. You can add up to a maximum of 10 IP addresses in the text box.

Step 5 Specify the maximum SNMP file size and the number of SNMP files.

Step 6 Click **Save**.

Changing Syslog Logging Options

Step 1 Choose **Administration > Logging**, then click Syslog Logging Options.

Step 2 Check the **Enable Syslog** check box to enable collecting and processing system logs.

Step 3 Enter the Syslog Host IP address of the interface from which the message is to be transmitted.

Step 4 Choose the **Syslog Facility**. You can choose any of the eight local use facilities for sending syslog messages. The local use facilities are not reserved and are available for general use.

Step 5 Click **Save**.

Using Logging Options to Enhance Troubleshooting

The logging screen allows you to customize the amount of data Prime NCS (WAN) collects in order to debug an issue. For easily reproduced issues, follow these steps prior to contacting TAC. These steps may create a smoother troubleshooting session:

Step 1 Choose **Administration > Logging**.

Step 2 From the Message Level drop-down list, choose **Trace**.

Step 3 Check each check box to enable all log modules.

Step 4 Reproduce the current problem.

Step 5 Return to the Logging Options page.

Step 6 Click **Download** from the Download Log File section.

Note The logs.zip filename includes a prefix with the host name, date, and time so that you can easily identify the stored log file. Included in the zip file is an html file that documents the log files.

Step 7 After you have retrieved the logs, choose **Information** from the Message Level drop-down list.

Note Leaving the Message Level at *Trace* can adversely affect performance over a long period of time.

Changing Settings

When you choose **Administration > System**, you can change the Prime NCS (WAN) settings described in Table 14-2.

Table 14-2 Prime NCS (WAN) Settings

Click this Setting ...	To Specify ...
Alarms and events	Which alarms should be deleted, define which alarm types are displayed, specify alarm email options. **Note** Data cleanup tasks run nightly to delete old alarms. In addition to the data cleanup task, Prime NCS (WAN) has an hourly task to check alarm table size. When the alarm table size exceeds 300 K, the task deletes the oldest cleared alarms until the alarm table size is within 300 K. The Alarm Display Options apply to the Alarm Summary page only. Quick searches or alarms for any entity display all alarms regardless of the acknowledged or assigned state. E-mails are not generated for acknowledged alarms regardless of severity change.
Data retention	How long to retain data for the different data types. **Note** For the best interactive graph data views, change the default settings to the maximum possible: 90 days for daily aggregated data and 54 weeks for weekly aggregated data. You must also make the appropriate measures to increase RAM and CPU capacity to compensate for these adjustments.
Login disclaimer	The disclaimer text that is displayed at the bottom of the login page for all users.
Mail server configuration	Global e-mail parameters for sending e-mails from Prime NCS (WAN) reports and alarm notifications. You can set the primary and secondary SMTP server host and port, the sender's e-mail address, and the recipient's e-mail addresses. Click the "Configure email notification for individual alarm categories" link to specify the alarm categories and severity levels you want to enable. Email notifications are sent when an alarm occurs that matches categories and the severity levels you select.
Notification receivers	Receivers who will receive notifications from Prime NCS (WAN). Alerts and events are sent as SNMPv2 notifications to configured notification receivers. **Note** If you are adding a notification receiver with the notification type UDP, the receiver you add should be listening to UDP on the same port on which it is configured. By default only INFO level events are processed for the selected category. Only SNMPV2 traps are considered for northbound notification.
Report	The path where reports are stored and for how long the reports are retained.
Server settings	Whether to enable or disable server ports.
Severity Configuration	The severity level of the alarms.
SNMP Settings	Global SNMP settings such as trace display values such as reachability parameters and backoff algorithm. If you select Exponential (the default value) for the Backoff Algorithm, each SNMP try waits twice as long as the previous try, starting with the specified timeout for the first try. If you choose Constant Timeout, each SNMP try waits the same, specified amount of time. If you select to use reachability parameters, the Prime NCS (WAN) defaults to the global Reachability Retries and Timeout that you configure. If unchecked, Prime NCS (WAN) always uses the timeout and retries specified. The default is selected.
Image Management	Preference parameters for downloading, distributing, and recommending software Images.

Table 14-2 Prime NCS (WAN) Settings

Click this Setting ...	To Specify ...
Configuration	Whether to backup the running configuration, to rollback the configuration, or to get show commands output from cache.
Configuration Archive	Basic configuration archive settings such as protocol, timeout value, number of configuration versions to store, etc.
Audit	Audit log purge settings and where to send purged logs.
Monitoring Settings	Auto monitoring for device and interface health collection and enable deduplication for server heath collections.

Checking the Status of Prime NCS (WAN)

To check the status of Prime NCS (WAN) from the CLI, follow these steps:

Step 1 Log into the system as **admin** by entering the following command:

```
ssh admin NCS(WAN)_server_IP address or hostname
```

Step 2 Enter the following CLI:

```
# ncs status
```

The CLI displays messages indicating the status of Prime NCS (WAN).

Stopping Prime NCS (WAN)

You can stop Prime NCS (WAN) at any time by following these steps:

Note If any users are logged in when you stop Prime NCS (WAN), their sessions stop functioning.

Step 1 Log into the system as **admin** by entering the following command:

```
ssh admin (WAN)_server_IP address or hostname
```

Step 2 Enter the following CLI:

```
# ncs stop
```

The CLI displays messages indicating that Prime NCS (WAN) is stopping.

Backing Up the Database

This section provides instructions for backing up the Prime NCS (WAN) database. You can schedule regular backups through the Prime NCS (WAN) user interface or manually initiate a backup.

Note Machine specific settings (such as FTP enable and disable, FTP port, FTP root directory, TFTP enable and disable, TFTP port, TFTP root directory, HTTP forward enable and disable, HTTP port, HTTPS port, report repository directory, and all high availability settings) are not included in the backup and restore function if the backup is restored to a different device.

This section contains the following topic:

Scheduling Automatic Backups

To schedule automatic backups of the Prime NCS (WAN) database, follow these steps:

Step 1 Log into the Prime NCS (WAN) user interface.

Step 2 Click **Tools > Task Manager > Background Tasks** to display the Scheduled Tasks page.

Step 3 Click the **NCS Server Backup** task to display the **NCS Server Backup** page.

Step 4 Check the **Enabled** check box.

Step 5 At the **Backup Repository** parameter, Choose an existing backup repository or click create button to create a new repository.

Step 6 If you are backing up in remote location, select the FTP Repository check box. You need to enter the FTP location, Username and Password of the remote machine.

Step 7 In the Interval (Days) text box, enter a number representing the number of days between each backup. For example, 1 = a daily backup, 2 = a backup every other day, 7 = a weekly backup, and so on.

Range: 1 to 360

Default: 7

Step 8 In the Time of Day text box, enter the time when you want the backup to start. It must be in this format: *hh*:*mm* AM/PM (for example: 03:00 AM).

Note Backing up a large database affects the performance of the Prime NCS (WAN) server. Therefore, we recommend that you schedule backups to run when the Prime NCS (WAN) server is idle (for example, in the middle of the night).

Step 9 Click **Submit** to save your settings. The backup file is saved as a .zip file in the *ftp-install-dir*/ftp-server/root/NCSBackup directory using this format: *dd-mmm-yy_ hh-mm-ss*.zip (for example, 10-Dec-12_10-15-22.zip).

Uninstalling

You can uninstall Prime NCS (WAN) at any time, even while Prime NCS (WAN) is running.

To uninstall Prime NCS (WAN), follow these steps:

Step 1 Log into Prime NCS (WAN) as **root**, then enter the following command:

```
# ncs stop
```

Step 2 Using the Linux CLI, navigate to the /opt/NCS1.0.X.X directory (or the directory chosen during installation).

Step 3 Enter **./UninstallNCS**.

Step 4 Click **Yes** to continue the uninstall process.

Step 5 Click **Finish** when the uninstall process is complete.

Note If any part of the /opt/NCS1.0.X.X directory remains on the hard drive, manually delete the directory and all of its contents. If you fail to delete the previous Prime NCS (WAN) installation, this error message appears when you attempt to reinstall Prime NCS (WAN): "**Cisco Prime NCS (WAN) is already installed. Please uninstall the older version before installing this version.**"

Recovering the Prime NCS (WAN) Password

You can change the Prime NCS (WAN) application root user or FTP user password. This option provides a safeguard if you lose the root password. An executable was added to the installer /bin directory (passwd.bat for Windows and passwd.sh for Linux). To recover the passwords and regain access to Prime NCS (WAN), follow these steps:

Note If you are a Linux user, you must be the root user to run the command.

Note In Linux, use the ***passwd.sh*** to change the Prime NCS (WAN) password. The ***passwd*** is a built-in Linux command to change the OS password.

Step 1 Change to the Prime NCS (WAN) bin folder.

Step 2 For Linux, use the following command:

Enter **passwd.sh root-user** ***newpassword*** to change the Prime NCS (WAN) root password. The new password is the root login password you choose.
or
Enter **passwd.sh location-ftp-user** ***newuser newpassword*** to change the FTP user and password. The newuser and newpassword are the MSE or Location server user and password.

Step 3 The following options are available with these commands:

- -q — to quiet the output
- -pause — to pause before exiting-gui — to switch to the graphical user interface
- -force — to skip prompting for configuration

Step 4 Start Prime NCS (WAN).

Managing and Updating Product Licenses

Prime NCS (WAN) licensing is based on the number of network devices for which you want to use Prime NCS (WAN) to manage. An Prime NCS (WAN) device license provides full access to all Prime NCS (WAN) features in order to manage a set number of devices. You purchase a single base license and then purchase additional add-on licenses as necessary to accommodate additional devices.

Prime NCS (WAN) is deployed through physical or virtual appliances. You use the standard License Center Graphical User Interface to add new licenses, which are locked by the standard Cisco Unique Device Identifier (UDI). When Prime NCS (WAN) is deployed on a virtual appliance, the licensing is similar to that on a physical appliance, except instead of using a UDI, you use a Virtual Unique Device Identifier (VUDI).

Note To move licenses from one physical appliance to another, you need to call the Licensing TAC and rehost the licenses to a new UDI.

The Prime NCS (WAN) License is recognized by the SKU, which is usually attached to every purchase order to clearly identify which software or package is purchased by a customer.

Note If you are using an evaluation license, it is recommended that you add a base license before your evaluation license expires.

You can view license information by clicking **Help > About Prime NCS (WAN)**.

Caution Do not modify your license file; If you make any modifications, your license fill will be corrupted.

Viewing License Details

To view the license type you currently have, the device and interface limits, and the percentage used and remaining on the license:

Step 1 Choose **Administration > Licenses**.

Step 2 Rest your cursor on the icon that appears next to Licenses to view licensing ordering help.

Adding Licenses

To add a new license:

Step 1 Choose **Administration > Licenses**.

Step 2 Under the Summary folder, click Files.

Step 3 Click **License Files**.

Step 4 Click **Add**.

Step 5 Browse to the location of the license file, then click **OK**.

Note Make sure the license file does not have a .txt extension.

Deleting Licenses

You might need to delete a license when:

- You are currently using an evaluation license and want to apply a base license.
- You are currently using an add-on license and want to apply a new license to accommodate additional devices.

Step 1 Choose **Administration > Licenses**.

Step 2 Under the Summary folder, click Files.

Step 3 Click **License Files**.

Step 4 Select the license file you want to delete, then click **Delete**.

CHAPTER 15

Controlling User Access

This chapter contains the following sections:

Managing Users

All Prime NCS (WAN) users have basic parameters such as user name and password. Users with admin privileges can view active user sessions.

To view active sessions:

Step 1 Choose **Administration > Users, Roles & AAA**, then click **Active Sessions**.

Step 2 Click the **Audit Trail** icon to for the username for which you want to see the following data:

- User—User login name
- Operation—Type of operation audited
- Time—Time operation was audited
- Status—Success or failure
- Reason—Failure reason when the user login failed
- Configuration Changes—This field provides a Details link if there are any configuration changes. Click on the Details link for more information on the configuration changes done by an individual user.

Note The audit trail entries could be logged for individual device changes. For example, If a template is applied on multiple switches, then there will be multiple audit entries for each switch to which the template has been applied.

Adding a User

You can add a user and assign predefined static roles. Besides complete access, you can give administrative access with differentiated privileges to certain user groups. Prime NCS (WAN) supports external user authentication using these access restrictions and authenticates the users against the TACACS+ and RADIUS servers.

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

Step 2 Choose **Add a User**, then click **Go**.

Step 3 Enter the username, password, and confirm password for the new user, then choose the groups to which this user belongs.

Step 4 Click the Virtual Domains tab to assign a virtual domain to this user. See Changing Virtual Domains.

Step 5 Click **Save**.

Changing User Passwords

To change the password for a user:

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

Step 2 Select the user name who's password you want to change.

Step 3 Complete password fields, then click **Save**.

Changing User Privileges

Prime NCS (WAN) uses a list of tasks to control which part of Prime NCS (WAN) users can access and the functions they can perform in those parts. You change user privileges in Prime NCS (WAN) by changing the User Group to which each user belongs. You use the User Group Task List to change what users in each group are authorized to do and the screens they can access.

You can also assign the sites or devices to which a virtual domains has access.

To edit the task list for a user group:

Step 1 Choose **Administration > Users, Roles & AAA**, then click **User Groups**.

Step 2 Click on a group name to change the tasks this group is allowed to perform.

Step 3 Click the Members tab to view the users of this group.

Managing User Groups

Prime NCS (WAN) has pre-defined user groups as described in. You can change the privileges for the users, but you cannot add additional users. When you create a new user, you assign that user to a group.

Table 15-1 describes the Prime NCS (WAN) default user groups and their privileges.

Table 15-1 Default User Groups

Group Name	Privileges for Users in the Group
System Monitoring	Monitor Prime NCS (WAN) operations.
ConfigManagers	Monitor and configure Prime NCS (WAN) operations.
Admin	Monitor and configure Prime NCS (WAN) operations and perform all system administration tasks except administering Prime NCS (WAN) user accounts and passwords.
SuperUsers	Monitor and configure Prime NCS (WAN) operations and perform all system administration tasks including administering Prime NCS (WAN) user accounts and passwords. Superusers tasks can be changed.
North bound API	Used only with Prime NCS (WAN) Navigator.
User Assistant	Local net user administration only. User assistants cannot configure or monitor devices.
Lobby Ambassador	Guest access for only configuration and managing of user accounts.
Monitor lite	Monitoring of assets location.
Root	Monitor and configure Prime NCS (WAN) operations and perform all system administration tasks including changing any passwords. Only one user can be assigned to this group and is determined upon installation. It cannot be removed from the system, and no task changes can be made for this user.

To view user groups and their associated tasks:

Step 1 Choose **Administration > Users, Roles & AAA**, then click **User Groups**.

Step 2 Click on a group name to change the tasks this group is allowed to perform.

Step 3 Click the Members tab to view the users of this group.

Changing Virtual Domain Access

To edit the sites or devices to which a virtual domains has access:

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

Step 2 Select the domain to which you want to assign sites or devices.

Step 3 Click the **Sites** or **Devices** tab, then move the necessary items from the Available list to the Selected list.

Step 4 Click **Submit**.

To associate users to Virtual Domains, choose **Administration > Users, Roles & AAA**, then click **Users**. See Assigning Users to a Virtual Domain.

Changing Password Policy

Prime NCS (WAN) supports various password policy controls, such as minimum length, repeated characters, etc.

To change password policies:

Step 1 Choose **Administration > Users, Roles & AAA**, then click **Local Password Policy**.

Step 2 Chose the necessary policies, then click **Save**.

Setting the AAA Mode

Prime NCS (WAN) supports local as well as TACACS+ and RADIUS, but you must specify a TACACS+ or RADIUS server first.

To specify a TACACS+ server and then change the AAA mode to TACACS+:

Step 1 Choose **Administration > Users, Roles & AAA**, then click **TACACS+**.

Step 2 From the command pull-down menu, choose Add TACACS+ Server, then click **Go**.

Step 3 Enter the TACACS+ server parameters, then click **Save**.

Step 4 Click **AAA Mode**.

Step 5 Select TACACS+ and specify whether to enable fallback to the local condition.

Step 6 Click **Save**.

Changing Virtual Domains

A Prime NCS (WAN) Virtual Domain consists of a set of Prime NCS (WAN) devices and/or maps and restricts a user view to information relevant to these managed objects.

Through a virtual domain, an administrator can ensure that users are only able to view the devices and maps for which they are responsible. In addition, because of the virtual domain filters, users are able to configure, view alarms, generate reports for *only* their assigned part of the network.

The administrator specifies for each user a set of allowed virtual domains. Only one of these can be active for that user at login. The user can change the current virtual domain by selecting a different allowed virtual domain from the Virtual Domain drop-down list at the top of the page. All reports, alarms, and other functionality are now filtered by that virtual domain.

If there is only one virtual domain defined ("root") in the system AND the user does not have any virtual domains in the custom attributes fields in the TACACS+/RADIUS server, the user is assigned the "root" virtual domain by default. If there is more than one virtual domain, and the user does not have any specified attributes, then the user is blocked from logging in.

To add sites and devices to a virtual domain:

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

Step 2 From the left Virtual Domain Hierarchy sidebar menu, click the virtual domain to which you want to add a site or device.

Step 3 Move the sites and devices from the Available to the Selected column, then click **Submit**.

To add a user to a virtual domain:

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

Step 2 Click on the user you want to add to a virtual domain.

Step 3 Click the Virtual Domains tab.

Step 4 Move the virtual domain to which you want to add the user from the Available Virtual Domains column to the Selected Virtual Domains column, then click **Save**.

Note Each virtual domain may contain a subset of the elements included with its parent virtual domain. When a user is assigned a virtual domain, that user can view the devices that are assigned to its virtual domain.

Auditing Access

Prime NCS (WAN) maintains an audit record of user access.

To access the audit trail for a user or user's active sessions:

Step 1 Choose **Administration > Users, Roles & AAA**, then click **Active Sessions**.

Step 2 Click the **Audit Trail** icon to for the username for which you want to see the following data:

- User—User login name
- Operation—Type of operation audited
- Time—Time operation was audited
- Status—Success or failure

- Configuration Changes—This field provides a Details link if there are any configuration changes. Click on the Details link for more information on the configuration changes done by an individual user.

Note The audit trail entries could be logged for individual device changes. For example, If a template is applied on multiple switches, then there will be multiple audit entries for each switch to which the template has been applied.

To access the audit trail for a user group:

Step 1 Choose **Administration > Users, Roles & AAA**, then click **User Groups**.

Step 2 Click the **Audit Trail** icon to for the username for which you want to see the following data:

- User—User login name
- Operation—Type of operation audited
- Time—Time operation was audited
- Status—Success or failure
- Configuration Changes—This field provides a Details link if there are any configuration changes. Click on the Details link for more information on the configuration changes done by an individual user.

Note The audit trail entries could be logged for individual device changes. For example, If a template is applied on multiple switches, then there will be multiple audit entries for each switch to which the template has been applied.

Viewing Audit Logs

Prime NCS (WAN) provides two types of audit logs:

- Application Audit logs—Logs events that pertain to the Prime NCS (WAN) features. For example, you can view the application audit log to see when a particular user logged in and what actions were taken.
- Network Audit logs—Logs events related to the devices in your network. For example, you can view the network audit logs to see which user deployed a specific template and the date and time the template was deployed.

Step 1 Choose **Administration > Audit Logs**.

Step 2 Click the **Application Audit** or **Network Audit** tab.

Note For Application Audit, the User Group column is blank for TACACS+/RADIUS users.

Step 3 To view details about the log, click to expand the row for which you want to view details.

Adding TACACS+ Server

To configure Prime NCS (WAN) so it can communicate with the TACACS+ server:

Step 1 Choose **Administration > Users, Roles & AAA**, then click **TACACS+**.

Step 2 Choose Add TACACS+ Server, then click **Go**.

Step 3 Enter the TACACS+ server information, then click **Save**.

Note For Prime NCS (WAN) to communicate with the TACACS+ server, the shared secret you enter on this page must match the shared secret configured on the TACACS+ server.

Adding a RADIUS Server

To configure Prime NCS (WAN) so it can communicate with the RADIUS server:

Step 1 Choose **Administration > Users, Roles & AAA**, then click **RADIUS Servers**.

Step 2 Choose Add Radius Server, then click **Go**.

Step 3 Enter the RADIUS server information, then click **Save**.

Note For Prime NCS (WAN) to communicate with the RADIUS server, the shared secret you enter on this page must match the shared secret configured on the RADIUS server.

INDEX

O

P

Q

R

S

T

U