CHAPTER 1

Setting Up Devices and Using the GUI Clients

These topics introduce you to the Cisco Prime Network GUI clients:

- Overview of the GUI Clients, page 1-1
- Setting Up Devices and Validating Device Information, page 1-2
- Using Prime Network with Prime Central, page 1-8

Overview of the GUI Clients

Cisco Prime Network (Prime Network) provides the following GUI clients that offer an intuitive interface for managing your network and services, and for performing required system administration activities:

- Prime Network Vision, page 1-1
- Prime Network Events, page 1-2
- Prime Network Administration, page 1-2

Prime Network Vision

Prime Network Vision is the main GUI client for Prime Network. Maps of devices create a visualization of the network, from the intricacies of a single device physical and logical inventory, to multi-layer topological information on connections, traffic, and routes. Faults and alarms are graphically displayed with built-in troubleshooting tools. Network elements and links using color cues and graphic symbols to indicate status and alarms.

All user actions are controlled by *user roles* and *device scopes*. Each user is assigned a role which controls the GUI actions the user can perform. When a user does not have the required permission level to perform a function, the appropriate menu option or button is disabled. Similarly, device scopes, which are named collections of managed network elements, control which devices a user can access. User roles and device scopes are controlled from the Prime Network Administration GUI client.

Prime Network Vision is also the launching point for these features.

Feature	Provides this function:	Described in:
Path Tracer	Route tracing and performance	Chapter 12, "Using Cisco PathTracer to Diagnose Problems."
Change and Configuration Management	Manage software images and device configuration files	Chapter 4, "Device Configurations and Software Images"

Feature	Provides this function:	Described in:
Report Manager	Set up regular reports	Chapter 11, "Working with Reports."
Soft Properties Manager	Extend what is displayed in the GUI clients and monitored by Prime Network, and create new TCAs	*Cisco Prime Network 3.10 Customization Guide*
Command Builder	Create new device commands and add them to the GUI client	*Cisco Prime Network 3.10 Customization Guide*
Workflow	Create a series of sequential device tasks and add them to the GUI client	*Cisco Prime Network 3.10 Customization Guide*
Activation	Create wizards and add them to the GUI client	*Cisco Prime Network 3.10 Customization Guide*

For more information on the Prime Network Vision GUI client, see Working with the Cisco Prime Network Vision Client, page 2-1.

Prime Network Events

Prime Network Events is the interface used by system managers and administrators for viewing system events that occur in the network. You can use the GUI to retrieve detailed information about the different types of system events and tickets that are generated; it also helps predict and identify the sources of system problems. The GUI client also provides information about events within the Prime Network system. For more information, see Working with the Prime Network Events Client, page 8-1.

Prime Network Administration

Prime Network Administration is the GUI client used to manage the Prime Network system, which is comprised of gateway servers, units, AVMs, and VNEs. These components work together to create the information model, which is constantly updated. Administrators use this GUI client to create user accounts, device scopes, polling groups, redundancy settings, and so forth. For information on this GUI client, see the *Cisco Prime Network 3.10 Administrator Guide*.

Setting Up Devices and Validating Device Information

Prime Network provides a variety of management and configuration commands that you can launch from the Vision GUI client by right-clicking an NE and selecting **Commands**. These commands are executed on the actual physical device versus being performed on the network model that is stored in memory (and subsequently on the real device). This is useful to validate information displayed in a Prime Network GUI client against a device, using the device command line interface (CLI). Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands, if you have user permissions to do so.

Prime Network also provides a variety of technology-specific commands—such as configuring the clock source for signals on SONET ports, enabling global ELM-I, enabling OAM on an interface. Whether you can use these commands depends on whether the technology is enabled on the device.

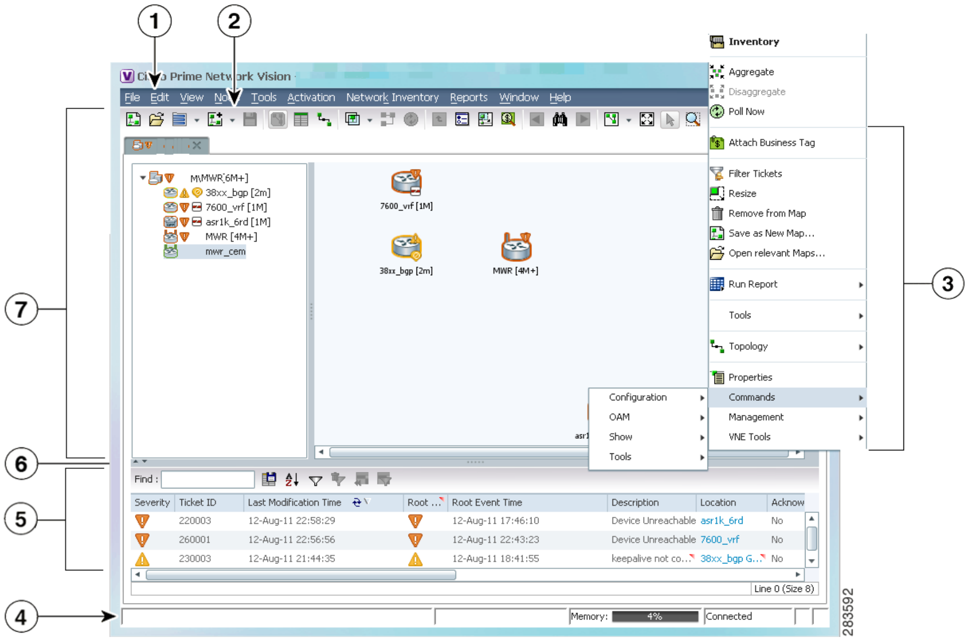
Note The basic operation commands in this chapter can be executed by all network elements that run on Cisco IOS software, Cisco IOS XR software, and Cisco NX OS software. You will not be able to execute these commands on network elements that have Cisco Catalyst OS software.

Note To view the basic operation commands in the Cisco Carrier Packet Transport (CPT) System, you must right-click the Cisco Carrier Packet Transport (CPT) System in the Prime Network Vision List or Map View and click **Logical Inventory > CPT Context Container**.

Execution of command builder scripts will fail under Managed Element and Physical Root

Figure 1-1 illustrates how to launch these commands.

Figure 1-1 Launching NE Management and Configuration Commands



Severity	Ticket ID	Last Modification Time	Root ...	Root Event Time	Description	Location	Acknow
▼	220003	12-Aug-11 22:58:29	▼	12-Aug-11 17:46:10	Device Unreachable	asr1k_6rd	No
▼	260001	12-Aug-11 22:56:56	▼	12-Aug-11 22:43:23	Device Unreachable	7600_vrf	No
⚠	230003	12-Aug-11 21:44:35	⚠	12-Aug-11 18:41:55	keepalive not co...	38xx_bgp G...	No

1	Menu Bar	**5**	Ticket Pane
2	Tool bar	**6**	Hide/display Ticket Pane
3	Device Right-click Menu	**7**	Navigation Pane
4	Status Bar		

Note You might be prompted to enter your device access credentials. Once you have entered them, these credentials will be used for every subsequent execution of a command in the same GUI client session. If you want to change the credentials, click **Edit Credentials**. The Edit Credentials button will not be available for SNMP commands or if the command is scheduled for a later time.

These topics describe the available commands:

- Configure Basic Device Settings: Name, DNS, NTP, RADIUS, TACACs, ACLs, page 1-4
- Configure SNMP and SNMP Traps on Device, page 1-5
- Configure Device Ports and Interfaces, page 1-6

- View Device and VRF Routing Tables and Device Interface Briefs, page 1-7
- Ping Destinations and VRFs, and View Trace Route from Device, page 1-7
- Change Device Syslog Logging Level, page 1-8
- View, Copy, and Overwrite Device Configuration Files, page 1-8
- View Users (Telnet Sessions) on Device, page 1-8

Configure Basic Device Settings: Name, DNS, NTP, RADIUS, TACACs, ACLs

Use the following commands to configure system-level settings on the real device. Unless otherwise noted, all of the following commands are launched by right-clicking the device and choosing **Commands > Configuration > System**.

Configure the Device Host Name and DNS

Command	Description
Add Host Name **Remove Host Name**	Configures the device hostname. **Note** Be sure to also apply any hostname changes to the device in Prime Network so that the name is also updated in the Prime Network model.
DNS > Add DNS Server **DNS > Remove DNS Server**	Assigns the device to a Domain Name System (DNS) server to manage translating the hostname to and from the device IP address.

Configure a Device NTP Server

Command	Description
NTP > Add NTP Server **NTP > Remove NTP Server**	Assigns the device to a Network Time Protocol (NTP) server to manage clock synchronization.

Configure RADIUS or TACACS Server on Device

Command	Description
TACACS > Add Tacacs Server **TACACS > Remove Tacacs Server**	Assigns the device to a Terminal Access Controller Access-Control System (TACACS) server to manage authentication (uses TCP or UDP).
TACACS+ > Add Tacacs+ Server **TACACS+ > Remove Tacacs+ Server**	Assigns the device to a TACACS+ server to manage authentication (uses TCP).
RADIUS > Add Radius Server **RADIUS > Remove Radius Server**	Assigns the device to a Remote Authentication Dial In User Service (RADIUS) server to manage centralized authentication, authorization, and accounting (uses UDP).

Configure IP Access Control Lists (ACL) on Device

Command	Navigation	Description	Supported On
Create Access List	*Right-click on a context* > **Commands** > **Configuration**	Use this command to create a new access list.	These commands are applicable only for ASR5000 and ASR5500 Modify Access devices.
Modify Access List Delete Access List	Expand **Access** List node **>** *right-click an access list* **>** **Commands >** **Configuration**	Use these commands to modify/delete an access list.	
Show Access List	Expand **Access List** node > *right-click an access list* > **Commands** > **Show**	Use this command to view and confirm configuration details of an access list.	

Configure SNMP and SNMP Traps on Device

Use the following commands to configure SNMP settings and SNMP traps on the real device. All of the following commands are launched by right-clicking the device and choosing **Commands > Configuration > System**.

Command	Description
SNMP > **Add SNMP Configuration** **SNMP** > **Update SNMP Configuration** **SNMP** > **Remove SNMP Configuration**	Configures SNMP on the device, including community settings, read-write access control, view-based access control, group settings, and so forth. **Note** Be sure to also apply any SNMP configuration changes to the device in Prime Network so that the settings are also updated in the Prime Network model.
SNMP > **Add Traps** **SNMP** > **Enable Traps** **SNMP** > **Remove Traps**	Configures traps on the device (for example, improper user authentication, restarts, the closing of a connection, loss of connection to a neighbor router, and so forth). You can choose traps from a drop-down list.

Configure Device Ports and Interfaces

Configure Device Ports

Note To apply description or status changes to an interface and port at the same time, use the interface commands listed in Configure Device Interfaces, page 1-6.

Command	Navigation	Description
Add / Remove / Update port description	**Physical Inventory >** *navigate to port* > **Commands > Configuration**	Configures the descriptive information that is displayed in GUI clients when the port is selected. Examples are customer information or business case details. **Note** Not supported on the Cisco Carrier Packet Transport (CPT) System.
Change Port Status		Disables (Shutdown) or enables (No Shutdown) the port. An example is disabling (No Shutdown) a port in response to a fault so that the port will not generate further errors. **Note** Not supported on the Cisco Carrier Packet Transport (CPT) System.
Modify Port	**Physical Inventory >** *Ethernet Slot* > *navigate to port* > **Commands > Configuration**	(Cisco ASR 5000 series only) Controls a variety of ASR 5000 port characteristics (bindings, contexts, link aggregations, and so forth). For more information, see the appropriate Cisco ASR 5000 documentation.
Assign Port to Vlan **DeAssign Port To Vlan**	**Logical Inventory > Routing Entities > Routing Entity >** *interface* > **Commands > Configuration**	Controls a port's VLAN assignment. Enter a VLAN between 1-4094. When assigned, the port can communicate only with or through other devices in that VLAN. When deassigned, you can move a port to a new VLAN.

Configure Device Interfaces

Command	Navigation	Description
Add Interface Configuration	**Physical Inventory >** *interface* > **Commands > Configuration**	Configures descriptive information that is displayed in GUI clients when the interface (or port) is selected. Examples are customer information or business case details.

Command	Navigation	Description
Enable Interface **Disable Interface**	**Logical Inventory** > **Routing Entities** > **Routing Entity** > *interface* > **Commands** > **Configuration**	Disables or enables an interface (and port). An example is disabling an interface in response to a fault so that the interface will not generate further errors.
Update Interface Configuration **Remove Interface Configuration**		Changes or removes descriptive information that is displayed in GUI clients when the interface (or port) is selected. Examples are customer information or business case details.
Add Loopback Interface	**Logical Inventory** > **Routing Entities** > **Routing Entity** > **Commands** > **Configuration**	Configures a software-only interface that emulates an interface. If the virtual interface receives traffic, it immediately reroutes it back to the device.

View Device and VRF Routing Tables and Device Interface Briefs

View Interface Briefs and IP Routes

Command	Navigation	Description
Show > **IP Route**	**Logical Inventory** > **Routing Entities** > **Routing Entity** > **Commands**	Displays the device routing table.
Show > **VRF IP route**	**Logical Inventory** > **VRFs** > *VRF* > **Commands**	Displays the routing table of a selected VRF.
Show > **IP** > **Interface Brief**	*NE* > **Commands**	Lists all IP interfaces on the device.

Ping Destinations and VRFs, and View Trace Route from Device

Command	Navigation	Description
OAM > **Trace Route from Device**	*NE* > **Commands**	Performs a traceroute to a destination address, showing how many hops were required and how long each hop takes.
OAM > **Ping** > **Destination From Device**		Pings a specified IP address to see if the IP address is accessible.
OAM > **Traceroute VRF**	**Logical Inventory** > **VRFs** > *VRF* > **Commands**	Performs a traceroute from selected VRF to a destination address, showing how many hops were required and how long each hop takes.
OAM > **Ping VRF**		Pings a specified VRF to see if the VRF is accessible.

Change Device Syslog Logging Level

.

Command	Navigation	Description
Syslog Host Logging	*NE* > **Commands** > **Configuration** > **System**	Changes the syslog logging level to one of the following: alerts, critical, debugging, emergencies, errors, informational, notifications, warnings

View, Copy, and Overwrite Device Configuration Files

Command	Navigation	Description
Write memory	*NE* > **Commands** > **Configuration**	Overwrites the startup-config file with the current running-config. **Note** Not supported on Cisco IOS XR devices.
Show > **Running Config**	*NE* > **Commands**	Displays the contents of the device's current running-config (which can be different from the running-config on file).
Show > **Running Config from file**		Displays the contents of the device's running-config file.
Show > **Startup Config**		Displays the contents of the device's current startup-config.
From FTP **From TFTP**	*NE* > **Commands** > **Tools** > **File copy** **Note** Not supported on Cisco Carrier Packet Transport (CPT) System.	Copies the starting-config or running-config file from a remote source to a local location. The remote source is identified by its IP address. FTP requires the FTP username and password.
To FTP **To TFTP**		Copies a local configuration file to a remote destination's starting-config or running-config file. The remote destination is identified by an IP address. FTP requires the FTP username and password.

View Users (Telnet Sessions) on Device

Command	Navigation	Description
Users (Telnet Sessions)	*NE* > **Commands** > **Show**	Provides details about the device's current Telnet sessions.

Using Prime Network with Prime Central

Prime Network can be installed as a standalone product or with Cisco Prime Central. When installed with Cisco Prime Central, you can launch Prime Network GUI clients from the Cisco Prime Portal. Cross-launch to and from other suite applications is also supported. The applications share a common inventory.

The Cisco Prime Portal uses a single sign-on (SSO) mechanism so that users need not reauthenticate with each GUI client. All session management features are controlled by the portal (such as client timeouts). If a user tries to log into a standalone GUI client, the user will be redirected to the portal login. The only exception is the emergency user, who will still be allowed to log into a standalone GUI client.

If the Cisco Prime Performance Manager application is also installed, the Prime Network Event Collector will receive threshold crossing alarm (TCA) events from Prime Performance Manager components and generate a ticket that you can view in Prime Network Events.

Prime Network also receives EPM-MIB traps from the network. By default Prime Network receives EPM-MIB traps from any source in the network. If desired, you can configure Prime Network to only process EPM-MIB traps arriving from a specific Prime Performance Manager server. The instructions for doing this are provided on the Cisco Developer Network at http://developer.cisco.com/web/prime-network/home.