Setting Up Devices and Using the GUI Clients

These topics provides an overview of the Prime Network GUI clients, the commands you can use to set up devices, and how to use Prime Network with Prime Central. It contains the following topics:

Note Command Manager and Transaction manager are accessed from the Change and Configuration Management GUI. Please see the *Cisco Prime Network 4.0 Customization Guide* for information about these components.

Overview of the GUI Clients

The following Prime Network GUI clients provide intuitive interface for managing your network and services, and for performing required system administration activities:

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 11, "Using Cisco PathTracer to Diagnose Problems."
Change and Configuration Management (CCM)	Management of software images and device configuration files. Use Compliance Audit feature to check compliance of device configurations to deployment policies.	Chapter 4, "Device Configurations and Software Images"
Transaction Manager (accessed from the CCM GUI)	Management and execution of activation workflows (transactions) that are made up of configuration scripts and designed to execute on devices according to a specific sequence or flow.	*Cisco Prime Network 4.0 Customization Guide*
Command Manager (accessed from the CCM GUI)	Repository of all configuration commands available in the system. It can be used to create new commands and command sequences, which can then be applied to groups of devices.	*Cisco Prime Network 4.0 Customization Guide*
Command Builder	Enables the creation and management of device configuration commands	*Cisco Prime Network 4.0 Customization Guide*
Report Manager	Scheduling and generation of fault, inventory, technology, and other standard reports.	Chapter 10, "Working with Reports."
Soft Properties Manager	Enables the display of additional properties in the GUI, and create new TCAs	*Cisco Prime Network 4.0 Customization Guide*

For more information on the Prime Network Vision GUI client, see Working with the 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 Tracking Faults Using Prime Network Events, 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 4.0 Administrator Guide*.

Prime Network Administration is also the launching point for the following Prime Network components which are launched in a Web GUI client.

Feature	Provides this function:	Described in:
VNE Customization Builder (VNE)	Enable support for unsupported device types, software versions, modules, and events.	*Cisco Prime Network 4.0 Customization Guide*
Network Discovery	Automatic discovery of network devices.	*Cisco Prime Network 4.0 Administrator Guide*

Prime Network Change and Configuration Management

This is a Web GUI component that provides tools for managing the software images and device configuration files used by the devices in your network. It is described in Device Configurations and Software Images, page 4-1.

CCM is also the launch point for the following Prime Network features:

- Transaction Manager, which is used to manage and execute activations on groups of devices. Information appears in the Transaction Manager tab only if transactions have been created and then added to Prime Network, as described in the *Cisco Prime Network 4.0 Customization Guide*.
- Command Manager, which provides a repository of all commands available in the system. It can be used to create new commands and command sequences, which can then be applied to groups of devices. Command Manager is described in the *Cisco Prime Network 4.0 Customization Guide*.

Prime Network Operations Reports

Prime Network Operations Reports is an optional add-on component to Prime Network 4.0 that provides extended reporting functionality. In addition to providing prepackaged, read-only fault, physical inventory, and technology-related reports, it also enables you to create your own reports and to customize some prepackaged reports. For information on this GUI client, see the *Cisco Prime Network 4.0 Operations Reports User 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.

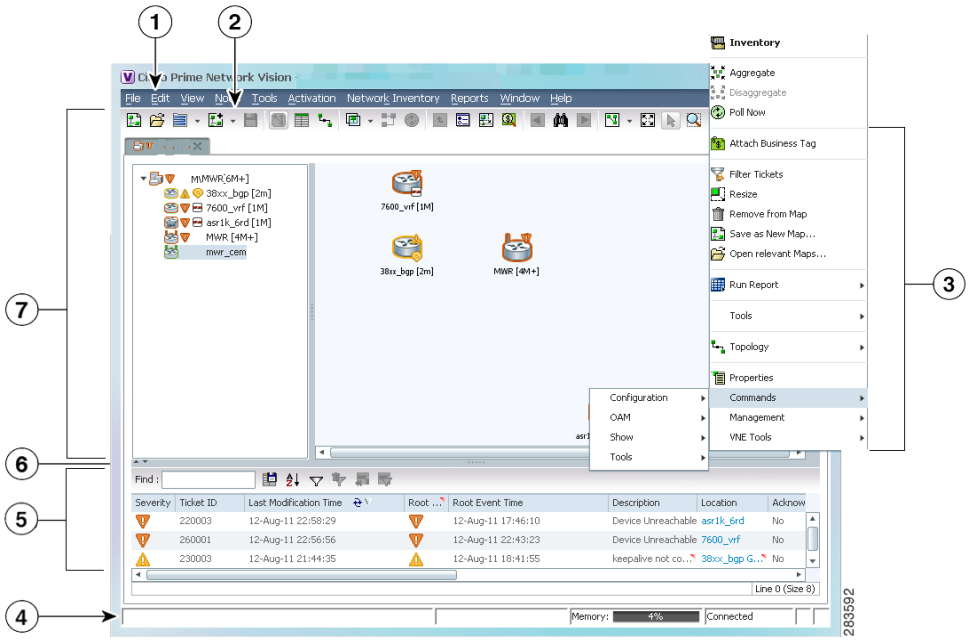
Note The basic operation commands in this chapter can be executed by all network elements that run on Cisco IOS software, Cisco IOS XR software, and Cisco NX OS software. You will not be able to execute these commands on network elements that have Cisco Catalyst OS software.

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



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**. 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

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**.

These commands can be executed on all network elements that run on Cisco IOS software, Cisco IOS XR software, Cisco NX OS, and Cisco IOS XE software. You will not be able to execute these commands on network elements that have Cisco Catalyst OS software.

Configure the Device Host Name and DNS

Command	Description
Add Host Name **Remove Host Name**	Configures the device host name. **Note** Be sure to also apply any host name 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 host name 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 (ACLs) on Device

Note These commands are not available on Cisco IOS XR devices.

Caution Only advanced users should change ACLs.

Command	Navigation	Description
Remove Access List	**Logical Inventory** > **Access Lists** > *ACL* > **Commands** > **Configuration** > **System**	Removes an NE's IP ACL, which filters traffic by forwarding or blocking routed packets depending on the ACL entry configurations.
Remove Access List Entry	**Logical Inventory** > **Access Lists** > *double-click ACL* > *ACL entry* > **Commands** > **Configuration** > **System**	Removes the specified ACL entry from the IP ACL.

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**.

Note These commands can be executed on all network elements that run on Cisco IOS software, Cisco IOS XR software, Cisco NX OS, and Cisco IOS XE software. You will not be able to execute these commands on network elements that have Cisco Catalyst OS software.

Command	Description
SNMP > Add SNMP Configuration **SNMP > Update SNMP Configuration**[1] **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.

1. The "Update SNMP configuration" command is not applicable for Cisco UBR10K and RFGW10 cards.

Configure Device Ports and Interfaces

These commands can be executed on all network elements that run on Cisco IOS software, Cisco IOS XR software, Cisco NX OS, and Cisco IOS XE

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 1-8.

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.
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

These commands can be executed on all network elements that run on Cisco IOS software, Cisco IOS XR software, and Cisco NX OS.

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[1]	**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[1]		Pings a specified VRF to see if the VRF is accessible.

1. Not applicable for Cisco UBR10K and RFGW10 cards.

Change Device Syslog Logging Level

These commands can be executed on all network elements that run on Cisco IOS software, Cisco IOS XR software, Cisco NX OS, and Cisco IOS XE software.

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

These commands can be executed on all network elements that run on Cisco IOS software, Cisco IOS XR software, Cisco NX OS, and Cisco IOS XE softwar

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 > 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.