Cisco Prime Network 3.8 Quick Start Guide

Released: November 14, 2011
Revised: January 30, 2012
Part No.: OL-23759-01

Table of Contents

1 Overview

This section provides an overview of the goals, assumptions, and content of the Quick Start Guide, as follows:

Purpose of the Quick Start Guide

The purpose of this Quick Start Guide is to get you up and running with Cisco Prime Network 3.8, to the point where you can create a map to visualize your network and you can take advantage of Prime Network's many capabilities to monitor and manage your network elements and services. This guide will lead you through the planning, installation, and post-installation tasks required to get to this point.

Note This Quick Start Guide does not replace other available Cisco Prime Network documentation, as it contains the minimum subset of information required to get started. For detailed information on any of the subjects mentioned in this guide , please see the Cisco Prime Network 3.8 guides listed in Appendix A: Additional Cisco Prime Network 3.8 Guides, page 32.

The Quick Start Guide covers planning and installation of the Prime Network 3.8 gateway, unit, and clients after which you will have access to the functionality available in Prime Network Vision, Events, and Administration (depending on user security level), as well as Change and Configuration Management and Cisco Prime Network Activation (Network Activation) components.

Assumptions and Caveats

This section describes the assumptions upon which the information in this Quick Start Guide is based. If your Prime Network deployment differs from what is described in these assumptions, please contact your Cisco account representative for assistance with planning and installation of Prime Network.

Note The Quick Start Guide is not intended for high scale environments, either at the network element level or the cross-network size. Details about hardware requirements for high scale setups, including database and memory sizing calculations, can be found in the *Capacity Planning Guide* which can be obtained from your Cisco account representative.

The guide assumes the following:

- This is a new Prime Network installation, not an upgrade from a previous version.
- Prime Network will be used to manage up to 100 network elements, i.e., a small-medium deployment of Prime Network. See Supported Deployment Options, page 3 for examples.
- The network can be managed by a maximum of one Prime Network gateway and one unit, either co-located on one server or on separate servers.
- The Prime Network embedded database (Oracle 11g 11.2.0.1.0) will be used, not an external database.
- Prime Network will be run in a production environment with a low rate of database operations:
  - 0-5 actionable events per second. Actionable events are events that can be parsed by Prime Network and can therefore participate in correlation.
  - Up to 50 incoming events per second
  - Up to 500 workflows per day
  - Up to 300 change and configuration management operations persisted in the database.
  - The default history size will be retained, i.e., 14 days for events, 7 days for workflows. If a longer history period is required, please consult your Cisco account representative.
- Telnet and SNMP will be used for device modeling and discovery when adding VNEs to the system, not SSH.
- The reader has experience in the Unix environment.

The Quick Start Guide does not cover the following:

- Integration
- Customization
- Package download

- Advanced configuration (e.g., polling)
- High availability
- LDAP
- External or remote database

Supported Deployment Options

Following are some examples of Prime Network network setups that fit within the Quick Start Guide scope. If your network setup is significantly larger than the examples below, please refer to the *Cisco Prime Network 3.8 Installation Guide* or contact your Cisco account representative for assistance with planning and installation of Prime Network.

Example 1

Deployment type: Carrier E Aggregation

Number of Managed Elements: 35 aggregation routers

Possible Device Types: ASR 9000, 7600

Example 2

Deployment type: MPLS Core

Number of Managed Elements: 75, of which 50 core routers (P, PE) and 25 aggregation routers

Possible Device Types for Core: CRS-1, 12k, 76xx, 72xx, 65xx

Possible Device Types for Aggregation: 76xx, 65xx

Example 3

Deployment type: Basic element management functionality, no network level services or topology

Number of Managed Elements: 100 small/medium access routers

Possible Device Types: ME3400, 4900, 3750, generic VNE

Example 4

Deployment type: IP RAN

Number of Managed Elements: 100, of which 5 aggregation devices, 30 cell site devices, 65 layer 2 switches

Possible Device Types for Aggregation: 7600

Possible Device Types for Cell Sites: MWR-2941, MWR2941-DC

Possible Layer 2 Switches: 3400, 3400 ME

Example 5

Deployment type: Carrier E

Number of Managed Elements: 100, of which 95 UPE devices, 5 NPE devices

Possible Device Types for UPE: 3400, 3750

Possible Device Types for NPE: 76xx, ASR 9000

2 Planning and Pre-Installation Tasks

To make Prime Network installation and setup as quick and seamless as possible, you need to plan your deployment in advance and perform the following pre-installation tasks:

- Read the *Cisco Prime Network 3.8 Release Notes*.
- Verify that the devices you intend to manage with Prime Network are supported, using the *Cisco Prime Network 3.8 Reference Guide*.
- Prepare Your Gateway, Unit, and Client Hardware and Software, page 4.
- Ensure that the Required Disk Space is Available Prior to Installation, page 7.
- Ensure that Ports to be Used by Prime Network are Open, page 8.
- Configure Your Devices to Enable Effective Cisco Prime Network Management, page 11.

Prepare Your Gateway, Unit, and Client Hardware and Software

This section provides prerequisites and recommendations for the hardware and software you need to support your Prime Network deployment. These recommendations are based on the assumptions and target setup for this Quick Start Guide, as described in Assumptions and Caveats, page 2 and Supported Deployment Options, page 3. If your network setup is not covered by this guide, please see "Installation Prerequisites" in the *Cisco Prime Network 3.8 Installation Guide*.

The recommended hardware options for the target setup are either:

- Gateway and unit co-located on one server (one-server setup). This option requires the installation of the gateway software only, as the gateway acts as both gateway and unit.

  or

- Gateway installed on one server, unit installed on a separate server (two-server setup).

Gateway and Unit Hardware and Software Prerequisites

This section provides the prerequisites for the hardware and software required for the Prime Network gateway and unit in the Quick Start Guide target setups. See Example Hardware for One-Server Setup, page 6 and Example Hardware for Two-Server Setup, page 6, for server recommendations.

The prerequisites are relevant for an embedded database installation, where the Oracle database is installed on the gateway during Prime Network installation and is fully integrated with Prime Network. The gateway and unit can run either Solaris or Linux operating systems.

Note The hardware requirements are provided under the assumption and recommendation that Prime Network 3.8 does not share the hardware with additional applications.

Table 1 Gateway and Unit Hardware and Software Prerequisites

Item	Specifications
System hardware	**Solaris:** • Sun T-series: T1, T2, or T3 8-core, 1.2-GHz UltraSPARC processor or Fujitsu SPARC 64 series processor with at least two CPUs. • One DVD drive. • Two 146-GB hard disk drives. **Linux:** • Intel Xeon 5500.
Software	Solaris 10 64-bit update 6 or later (English language) or Red Hat Enterprise Linux Server Release 5.3 64-bit or later. **Note** Linux must be installed with the default software packages (RPMs). Do not customize the RPMs.
Database Requirements	On Linux, the following Red Hat packages are required for Oracle Database 11g R2. If any of these packages is missing, the installation will fail. • binutils • compat-libstdc++-33-3.2.3 • elfutils-libelf • elfutils-libelf-devel • gcc-4.1.2 • gcc-c++-4.1.2 • glibc-2.5 • glibc-common-2.5 • glibc-devel-2.5 • glibc-headers-2.5 • ksh • libaio • libaio-devel • libgcc-4.1.2 • libstdc++ • libstdc++-devel • make • numactl-devel • sysstat-7.0.2
Memory (RAM)	• Gateway: 32 GB RAM (this covers both gateway and database memory requirements) • Unit: 32 GB RAM • Gateway and unit on the same server: 64 GB RAM • Memory-to-CPU ratio: – Gateway—At least 4 threads and the same memory as the Solaris server. (Each Intel Xeon 5500 has 8 threads.) – Unit (VNE)—4 threads.

Table 1 Gateway and Unit Hardware and Software Prerequisites (continued)

Item	Specifications
Swap space	• Solaris: 96 GB • Linux: 10 GB
Required Configuration	• Domain Name System (DNS) must be enabled on the Prime Network gateway, unit, and client. • For time zone, use GMT (with 0 offset) on the Prime Network servers because Prime Network stores events in the database in Greenwich Mean Time (GMT) format. The Prime Network client converts events to the time zone that is configured on the client workstation.

Example Hardware for One-Server Setup

For a one-server setup where the gateway, unit, and database are co-located (with no LDOM partitioning), you could choose one of the examples below:

- Cisco UCS C210 M1 General-Purpose Rack-Mount Server with:
  - 2 Xeon 5500 processors
  - Red Hat Enterprise Linux Server Release 5.3 64-bit
  - 64 GB RAM
  - No VMWare
- Sun SPARC Enterprise T5240 server with:
  - 2 UltraSPARC T2+ processors
  - 64 GB RAM
  - Solaris 10 64-bit update 6

Example Hardware for Two-Server Setup

For a two-server setup, you could choose to use one server with two virtual partitions, or two separate machines, as in the examples below:

- One Sun SPARC Enterprise T5240 server with:
  - 2 UltraSPARC T2+ processors
  - 64 GB RAM divided into two logical domains of 32 GB each (one for the gateway and the database, and one for the unit).
  - Solaris 10 64-bit update 6
- Two separate Sun SPARC Enterprise T5220 servers (one for the gateway and one for the unit) with:
  - UltraSPARC T2 processor
  - 32 GB RAM
  - Solaris 10 64-bit update 6
- Two Cisco UCS C210 M1 General-Purpose Rack-Mount servers (one for the gateway and one for the unit) with:
  - 1 Xeon 5500 processor
  - Red Hat Enterprise Linux Server Release 5.3 64-bit
  - 32 GB RAM
  - No VMWare

Client Prerequisites

Table 2 Cisco Prime Network Client Minimum Installation Prerequisites

Item	Specifications
Minimum Hardware Requirements	
IBM PC or PC-compatible workstation	• Pentium IV, 2.66-GHz or better processor • 1 GB RAM • 2 GB of free disk space • 512 MB of free nonvirtual memory per running instance
Screen	• Minimum screen resolution of 1024 x 768 pixels • True color (32-bit) setting
Minimum Software Requirements	
Operating system	• Windows 2000, Windows XP, Windows Vista, or Windows 7 • Citrix XenApp 5 with the Citrix Hotfix patch CTX120923, available at http://support.citrix.com/article/CTX120923 **Note** The Citrix Hotfix patch requires an upgraded Citrix License Server (version 11.6.1). A single Citrix server supports multiple Citrix clients, each of which can run Prime Network clients.
Internet Connection	
Requirement	1.5 MB/s bandwidth (to download)
Supported browsers	• Microsoft Internet Explorer 7.0 or later, on Windows XP • Firefox 3.0 or later, on Windows XP **Note** You must turn off the pop-up blocker so that all Change and Configuration Management operations will work correctly.

Ensure that the Required Disk Space is Available Prior to Installation

Before installing Cisco Prime Network, please verify that the disk space and storage requirements for the installation and for the database are fulfilled:

Table 3 Minimum Disk Space Required for Cisco Prime Network Installation

Directory	Minimum Required Disk Space
/ (root)	1 GB
Cisco Prime Network installation directory (default is /export/home/*network-user*)	5 GB
/tmp	1 GB
Oracle user home directory. The default is /export/home/oracle	4 GB

Table 4 Database Storage Requirements

Item	Minimum Required Disk Space	Location Recommendations
Data files	92 GB	Internal or external disk.
Redo logs	6 GB	Redo log files should not reside on the same disk as the data files. For online redo log files on Solaris servers, prepare a dedicated file system mounted on a mount point with the forcedirectio option. For example: `/dev/dsk/c0t1d0s6 /dev/rdsk/c0t1d0s6 /directio ufs 1 yes forcedirectio`
Archive logs	110 GB	Archive log files should not reside on the same disk as the data files.
Data files backup	138 GB	Data files backup should not reside on the same disk as the data files.

Note The system administrator must back up the archive logs to tape daily and must transfer the data files backups to external storage.

Ensure that Ports to be Used by Prime Network are Open

The following ports are used by Prime Network and must be open prior to installation or the installation process will fail:

Table 5 Ports Used by Prime Network

Port	Protocol	Direction	Usage
21 and 22	TCP	Gateway > Remote FTP/SFTP Server	Exporting CCM configurations to remote FTP server
21 and 22	TCP	Gateway > Network Elements	Transferring images to Network Elements
23	TCP	Unit > Network Elements	Telnet collector
25	TCP	Gateway > SMTP Server	SMTP port that is optional for an external database, but recommended for an embedded database
69	UDP	Gateway > Network Elements	Transferring images to Network Elements
69	UDP	Network Elements > Unit	TFTP server on Prime Network units
123	UDP	Unit > Gateway	NTP synchronization between gateway and units
123	UDP	Gateway > NTP Server	NTP synchronization for gateway
1161	UDP, Linux only	Network Elements > Unit **Note** For 161 (UDP), if AVM100 resides on the gateway, the Network Elements sends to the Gateway.	SNMP engine discovery requests and replies
1162	UDP, Linux only	Network Elements > Unit **Note** For 162 (UDP), if AVM100 resides on the gateway, the Network Elements sends to the Gateway.	SNMP trap
161	UDP	Unit > Network Elements	SNMP polling and SNMP engine discovery requests

Table 5 Ports Used by Prime Network (continued)

Port	Protocol	Direction	Usage
161	UDP	Network Elements > Unit **Note** For 161 (UDP), if AVM100 resides on the gateway, the Network Elements sends to the Gateway.	SNMP engine discovery requests and replies
162	UDP	Network Elements > Unit **Note** For 162 (UDP), if AVM100 resides on the gateway, the Network Elements sends to the Gateway.	SNMP traps
162	TCP/UDP	Gateway > Northbound NMS	Event Forwarded through SNMPv2 traps wrapped in CISCO-EPM-NOTIFICATION-MIB
514	UDP	Network Elements > Unit **Note** If AVM100 resides on the gateway, the Network Elements sends to the Gateway.	Syslogs
1101	TCP	Unit > Gateway	Prime Network user exclusive bidirectional hardened SSH connection for system administration operations
1102	TCP	Gateway > Database Server	Prime Network user exclusive bidirectional hardened SSH connection for system administration operations.
1102	TCP	Database Server > Gateway	Prime Network user exclusive bidirectional hardened SSH connection for system administration operations.
1311	TCP	Client > Gateway	Prime Network monitoring system (SSL over HTTP)
1521	TCP	Client > Database Server	Prime Network Events database access
1521	TCP	Unit > Database Server	Event persistency
1521	TCP	Gateway > Database Server	Gateway persistency services
2077	TCP	Client > Gateway	Spring DM OSGi console, used for Change and Configuration Management
6080	TCP	Client > Gateway	HTTP for web access and web-start. Used to download the client from the gateway server, client updates (jar files), and online help files.
6081	TCP	Client > Gateway	HTTP over SSL for web access and web services
6081	TCP	Unit > Gateway	HTTP over SSL for unit configuration
8000	TCP	Unit > Gateway	XML RPC over SSL
8009	TCP	Client > Gateway	Tomcat server AJP connector port, used for Change and Configuration Management
8011	TCP	Unit > Gateway	XML RPC over SSL
8043	HTTPS	Client > Gateway	Secure HTTP port for Change and Configuration Management web clients

Table 5 Ports Used by Prime Network (continued)

Port	Protocol	Direction	Usage
8080	HTTP	Client > Gateway	HTTP port for Change and Configuration Management web clients **Note** By default, this port is disabled and the secure 8043 HTTP port is enabled for Change and Configuration Managment client. To use 8080 for Change and Configuration Management client, you must enable it manually. For more information, see "Enabling and Disabling Port 8080 Manually" in the *Cisco Prime Network 3.8 Change and Configuration Management User and Administrator Guide*.
8099	TCP	Unit > Gateway	XML RPC over SSL
9002	TCP	Internal gateway	Prime Network BQL - a **local** port only
9003	SSL	Client > Gateway	Prime Network BQL over SSL
9005	TCP	Client > Gateway	Tomcat server port, used for Change and Configuration Management
9009	TCP	Client > Gateway	Tomcat AJP connector port, used for Change and Configuration Management
9080	TCP	Client > Gateway	Tomcat HTTP connector port, used for Change and Configuration Management
9443	TCP	Client > Web GUI server	Tomcat HTTPS connector port, used for Change and Configuration Management
9490	TCP	Unit > Gateway	Secured SSL transport
9770 and 9771	TCP	Client > Gateway	Prime Network Vision, Prime Network Administration, Prime Network Events, Prime Network Workflow
9875	TCP	Client > Gateway	JMX console port, used for Change and Configuration Management

Configure Your Devices to Enable Effective Cisco Prime Network Management

Before adding your devices to the system, you need to run some commands on each device so that Prime Network can model the devices accurately and perform management tasks, such as processing syslogs, traps, logging, and so on. This section lists the device configuration prerequisites. Please see "Device Configuration Required Before Adding VNEs" in the *Cisco Prime Network 3.8 Administrator Guide* for details.

Table 6 Device Configuration Prerequisites

Required Configuration	To be configured on...	Details
Configure devices to send SNMP traps	All Cisco devices to be managed by Prime Network	See "Device Configuration Required Before Adding VNEs," in the *Cisco Prime Network 3.8 Administrator Guide*.
Configure devices to send syslogs	All Cisco devices to be managed by Prime Network	"Device Configuration Required Before Adding VNEs," in the *Cisco Prime Network 3.8 Administrator Guide*.

Configure devices to forward events to the server hosting the Prime Network Event Collector	All Cisco devices to be managed by the Prime Network	For traps:
		`snmp-server community public RO`
		`snmp-server host <IP> public`
		For syslogs:
		`logging <IP>`
		where <IP> is the IP address of the server hosting the Event Collector (usually the gateway).

Enable XML	IOS-XR devices	Prime Network VNEs use XML mode to communicate with IOS XR devices. Enable XML command: `xml agent tty`
Configure Virtual Device Contexts (VDCs)	Devices running Nexus operating system	"Device Configuration Required Before Adding VNEs," in the *Cisco Prime Network 3.8 Administrator Guide*.

3 Installation Tasks

This section provides step-by-step instructions for installing the Prime Network gateway, unit, and client software:

- Install the Gateway, page 12
- Install the Client, page 16
- Install the Unit, page 17

Note If you have a one-server setup, you need to install the gateway only. There is no need to install the unit because the gateway acts as both gateway and unit.

Install the Gateway

Installation of the gateway consists of two parts:

1. Installation, which involves running the install.pl command to install the gateway software on the designated server. This part should take between 10 and 20 minutes.
2. Configuration, which involves running the network-conf script to configure the gateway. This part might take up to an hour.

To install and configure the Cisco Prime Network gateway:

Step 1 Insert "Disk 1: New Install" in the DVD drive of the server on which you will be installing the gateway.

Step 2 Open a Telnet or SSH session to the server on which the gateway will be installed and log in as the user root.

Step 3 Go to the DVD directory:

```
cd /cdrom/cdrom0/Server
```

Note If you decide not to run the installation directly from the DVD, you must copy all the files including ivne-drivers.tar into the same directory as install.pl.

Step 4 Run the following command to start the installation and install the gateway in the default directory /export/home/*network-user*:

```
perl ./install.pl -user network-user
```

where *network-user* is the operating system user account for the Prime Network application.

For example, if the name of the user is network38, enter:

```
perl ./install.pl -user network38
```

To install the gateway in a different directory, specify the directory at the end of the install command. For example:

```
perl install.pl -user network38 -dir /opt/network38
```

The installation is initiated.

Step 5 After the installation is complete, you will be prompted to configure Prime Network. Enter **Yes** to continue to the next step or **No** to configure later using the **network-conf** command.

Note *Do not* rerun the **network-conf** script after AVMs or units are added. Rerunning the **network-conf** script could cause problems with the Prime Network registry.

Step 6 After entering **Yes** in the previous step, select **Set machine as Prime Network gateway,** then press **Enter.**

The Prime Network configuration utility configures the system by running a number of procedures, including generation of SSH keys.

Step 7 Copy the Oracle installation .zip files :

a. Open a separate Telnet or SSH session and log in as the root user

b. Change the password of the network-user, enter:

```
passwd network-user
```

c. Log in as the new user, enter:

```
su - network-user
```

d. Copy the Oracle installation .zip files as the *network-user* (user created in Step 4) from the installation DVD (Disk 3: Database Binaries for Solaris or Disk 4: Database Binaries for Linux) to export/home/ana-user/local/scripts/embedded_oracle.

For Solaris, copy solaris.sparc64_11gR2_database_1of2.zip and solaris.sparc64_11gR2_database_2of2.zip.

For Linux, copy linux.x64_11gR2_database_1of2.zip and linux.x64_11gR2_database_2of2.zip

Step 8 Return to the first Telnet or SSH session and press **Enter** to continue configuration.

Step 9 Enter the required information at the prompts. The following table lists the prompts that appears at various stages of the configuration and their required settings:

Table 7 Gateway Installation Prompts and Required Input

Prompt for...	Enter...	Notes
Is NTP configured on this machine?	Yes/No	Default is Yes.
Password for OS root user	The Unix root password. For example, admin.	Prime Network uses the root password to set machine-level settings and to execute scripts as “root”.
Password for internal, automatically created users (root, bosenable, bosconfig, bosusermngr, web monitoring user)	The password that will be used to access the various Prime Network system components.	This password will also be used as the database schemes password. The password cannot contain the at sign (@) or forward slash (/) characters, and it cannot begin with an exclamation point (!). You can change the password for each of these users at a later stage.
Prime Network to install the database?	Yes	Prime Network will install the database internally. You do not need an external database installation and setup. Ensure that you have copied the embedded database files from Installation Disk 3: Database Binaries for Solaris or Disk 4: Database Binaries for Linux to local/scripts/embedded_oracle. A message will be displayed if the files are not found in this location.
Select a single interface for Prime Network backend services (This prompt appears if more than one interface is detected during the network-conf).	The number corresponding with the IP address of the back-end interface to be used for gateway-to-unit communication.	Prime Network 3.8 supports dual network interface cards (NICs). You are prompted to specify the NIC to use for Prime Network back-end services (such as transport, xmlrpc, and so on) for gateway-to-unit communication. Dual NICs let you isolate the northbound interface from the back-end interface.
Install database on a remote server?	No	This Quick Start Guide assumes that the database will be installed locally on the gateway server. If you decide to install the database on a remote server, you need to specify the IP address of the remote server.
OS user of the database	The username of the Unix user of the database. The default is oracle.	
Oracle user home directory	Path to the Oracle user home directory. The default is /export/home/oracle.	The directory must have a minimum of 6 GB of disk space for oracle binaries.

Table 7 Gateway Installation Prompts and Required Input (continued)

Prompt for...	Enter...	Notes
Remove previous installation of Oracle?	Yes/No	If you already have Oracle on the designated server, you can have Prime Network remove it before installing the new database.
Your Prime Network database profile	2. Small deployment (requires a minimum 8 GB RAM for the database).	
Destination for the database's datafiles	Path to the directory containing the datafiles.	The locations of the database datafiles.
Destination for the redo logs	Path to the directory containing the redo logs.	The locations of the redo logs.
Automatic database backups?	Yes	
Destination for archive logs	Path to the directory containing the archive logs.	The locations of the redo logs, archive and backup files should not reside on the same disk as the data files.
Destination for backup files	Path to the directory containing the backup files.	The locations of the redo logs, archive and backup files should not reside on the same disk as the data files.
SMTP server IP/Hostname	company-email-server-address	You must have SMTP server access from the gateway in order to receive email notifications. Port 25 must be available.
Is Prime Network being installed as part of the Prime IP-NGN Suite?	Default is No	
Email for receiving alerts	username@company-name.com	E-mail address to receive notification when database errors occur.
Starting Prime Network when the gateway installation is complete, upon receipt of this message: `+ Done setting the machine as gateway. Would you like to start Prime Network?`	Yes	

The installation is completed.

The following logs are available:

- Installation logs at /var/adm/cisco/ana/logs/.
- Embedded database configuration logs at $ANAHOME/local/scripts/embedded_oracle.
- Configuration logs at $ANAHOME/Main/logs.

Step 10 Run the add_emdb_storage.pl script to add the database files required for your database profile, as follows:

a. Change directories to $ANAHOME/Main/scripts/embedded_db and enter the following command:

```
# ./add_emdb_storage.pl
```

b. Choose option 2—Small deployment (up to 5 actionable events per second) => required disk space for database files and redologs: 98 GB.

c. Insert the event archiving size in days. Prime Network default archive is 14 days: [default 14]

d. Insert the workflow archiving size in days. Prime Network default archive is 7 days: [default 7]

Verify That the Gateway Installation was Successful

To verify the gateway installation:

Step 1 If you did not start the gateway at the end of the installation process, launch the gateway by entering the following command:

```
anactl start
```

The gateway might take a while to load.

Step 2 Check the status of all processes and daemons by entering the following command:

```
status
```

The output shows the status of each process and the number of exceptions found in the total number of log file lines for that process. For example, [OK 0/39] means 0 exceptions found in the 39 log file lines that were checked:

```
--------------------------------------------------------------------------------
.-= Welcome to server-name, running Cisco Prime Network gateway (v3.8 (build number)) =-.
--------------------------------------------------------------------------------
+ Checking for services integrity:
  - Checking if host's time server is up and running                [OK]
  - Checking if webserver daemon is up and running                  [OK]
  - Checking if secured connectivity daemon is up and running       [OK]
  - Checking XMP runtime DM                                         [UP]
+ Detected AVM99 is up, checking AVMs
  - Checking for AVM83's status                                     [OK 0/22]
  - Checking for AVM0's status                                      [OK 0/39]
  - Checking for AVM100's status                                    [OK 0/119]
  - Checking for AVM25's status                                     [OK 0/28]
  - Checking for AVM11's status                                     [OK 1/141]
  - Checking for AVM84's status                                     [OK 0/29]
```

Note Check the log files for each AVM if there are any problems. The log files are located under main/logs.

Install the Client

The client installation wizard guides you step-by-step through the process for installing the Prime Network client which covers Prime Network Administration, Prime Network Vision, and Prime Network Events clients.

Step 1 Use either of the following options to begin the client installation:

- Insert "Disk 1: New Install" in your DVD drive. The client installation wizard launches automatically and the Welcome window is displayed.

  If the client installation wizard does not launch automatically, browse to the DVD directory and launch the prime_network_webstart.exe executable.
- Open a web browser and download the client executable from http://*GatewayIP*:6080/anaclient, where *GatewayIP* is the IP address of the newly installed gateway. After the download is complete, launch the prime_network_webstart.exe executable. The client installation wizard launches and the Welcome window is displayed.

Note The web browser option is available only if the gateway is up.

Step 2 Click **Next**. The Destination Location window is displayed. The default installation location is C:\Cisco Systems\prime_network\.

Note For Windows 7 only: We recommend that you do not install the Cisco Prime Network GUI clients in the Program Files folder. Only Windows Administrators can run the GUI clients if they are installed in that folder.

Step 3 Click **Next** to accept the default installation location. If you want to change the installation location, click **Browse**, select the preferred installation directory, click **OK**, and then click **Next**.

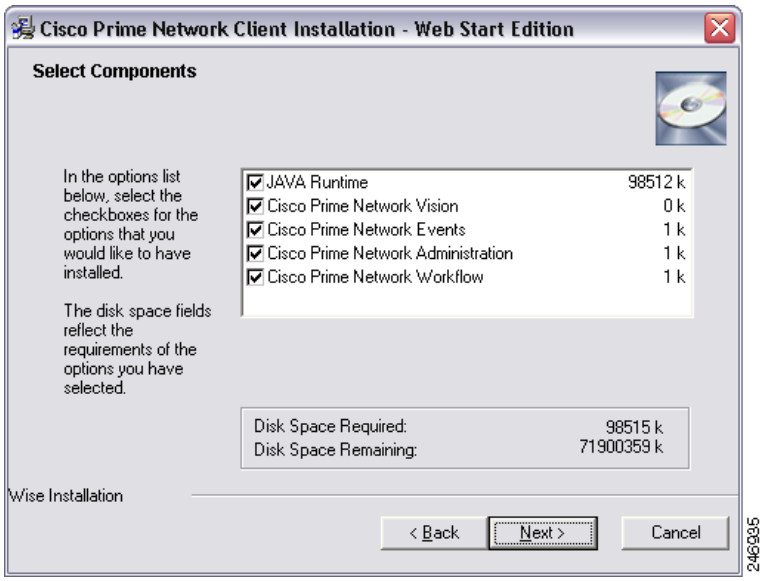
Step 4 In the Select Components window, do the following:

a. Make sure that the JAVA Runtime check box is checked.

b. Select all the available installation options (Prime Network Vision, Prime Network Events, Prime Network Administration, Prime Network Workflow).

c. Click **Next**.

Figure 1 Select Components



Step 5 In the Select Program Manager Group window, click **Next** to accept the default program manager group. If you want to change the default program manager group, enter your preference and then click **Next**.

Step 6 In the Start Installation window, click **Next** to start the installation. The Installing window is displayed.

Step 7 When the installation is complete, choose the options displayed in the final installation window, according to your preference:

- Create "Quick Launch" icons—Create a Quick Launch icon for Prime Network Vision and Prime Network Administration on the Quick Launch toolbar.
- Launch Prime Network Vision—Immediately launch Prime Network Vision.

Step 8 Click **Finish**.

Install the Unit

Installing the unit involves running the installation and configuration scripts from the Prime Network DVD.

To install the Prime Network unit:

Step 1 Insert "Disk 1: New Install" in the DVD drive of the server on which the unit will be installed.

Step 2 Open a Telnet or SSH session to the server on which the unit will be installed and log in as the user root.

Step 3 Go to the DVD directory:

```
cd /cdrom/cdrom0/Server
```

Step 4 Run the following command to start the installation and install the unit in the default directory /export/home/*network-user*:

```
perl ./install.pl -user network-user
```

where *network-user* is the operating system user account for the Prime Network application

For example, if the name of the user is network38, enter:

```
perl ./install.pl -user network38
```

Note You must enter the same username that you used when you installed the gateway. If the gateway and unit have different usernames, the unit will not start.

The installation is initiated.

Step 5 After the installation is complete, you will be prompted to configure Prime Network. Enter **Yes** to continue to the next step or **No** to configure later using the **network-conf** command and then proceed to the next steps.

Step 6 Select **Set machine as unit**, then press **Enter**

Step 7 Enter the required information at the prompts. The following table lists the prompts and the required settings:

Table 8 Unit Installation Prompts and Required Input

Prompt for...	Enter...	Notes
Is NTP configured on this machine?	Yes/No	Default is Yes.
Gateway IP address	The IP address of the gateway.	Make sure that the gateway is up and running before proceeding.
OS root user password	The Unix root password.	Prime Network uses the root password to set machine-level settings and to execute scripts as "root".
Prime Network administrator username and password	The username and password for the Prime Network administrator.	Prime Network internal admin user, used for secure communication with the gateway.
Select the unit protection group name	Choose from the listed options.	
Is this a standby unit?	Yes/No	Default is No.
Enter a unique name for this unit	Unit username	
Enable Unit Protection?	Yes/No	Default is Yes.

After entering the information at the prompts, a connection is made to the gateway to retrieve SSH keys. If the SSH keys are not retrieved automatically within 60 seconds, the following message is displayed: "Connection to *gateway-IP-address* failed. 60 seconds timeout exceeded." To resolve this issue, verify that the unit can reach port 6081 on the gateway and then run ana-conf again.

Note If more than one IP address is defined on the unit server, Prime Network automatically chooses the IP address of the network interface card (NIC) that acts as a default route to the gateway. If required, you can use the choose_nic.pl tool to change the NIC.

The unit installation ends with the following message:

```
+ Done setting the machine as unit.
+ Would you like to start Prime Network unit?(yes,no) [default yes]
- Finished installing and configuring Prime Network to user network38, directory /export/home/network38
- Please take a minute to set network38's password
```

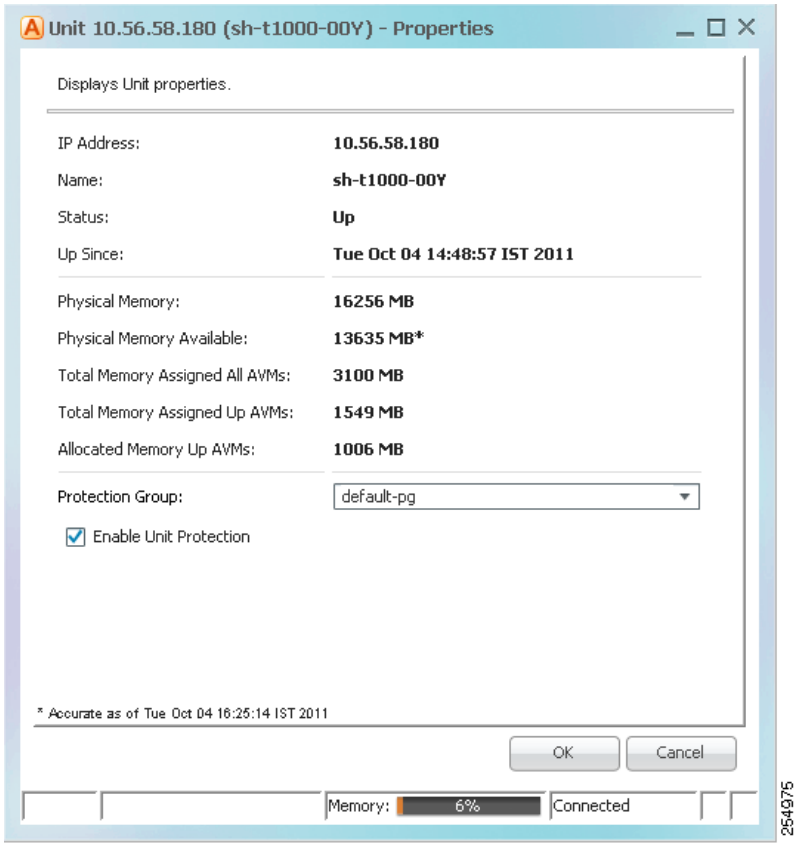
When the unit is installed, the new unit is displayed in the Prime Network Administration navigation tree and content area. It is automatically registered in the registry and a transport uplink between the unit and the gateway is created. The gateway starts the unit automatically, if the unit is reachable.

The unit is displayed as Down at first but the status changes to Up after a few minutes.

Note Remote procedure call (RPC) services (such as Prime Network SSH and XML-RPC) must be enabled in the gateway so that the gateway and the unit can communicate.

Right-click on the unit and select **Properties** to view memory allocation information for the unit, and other unit properties.

Figure 2 Unit Properties Dialog



Verify that the Unit Installation was Successful

Return to your Telnet/SSH session to the unit or open a new one. Follow the steps below to verify that the unit was installed properly. If there are any problems, rerun the installation.

Step 1 Check the status of all processes and daemons by entering the following command:

```
status
```

The output shows the status of each process and the number of exceptions found in the total number of log file lines for that process. For example, [OK 0/39] means 0 exceptions found in the 39 log file lines that were checked.

Step 2 In the ~/Main directory, confirm that:

- **a.** The scheme subdirectory exists and contains the correct scheme files.
- **b.** The scripts and UNIX subdirectories were created correctly.
- **c.** The registry directory exists and contains the necessary files.

Step 3 Check that the golden source was configured correctly on the server:

- **a.** Open the ~/Main/registry/avm99.xml file.
- **b.** Confirm that the file contains an entry for the key parent, which is the value of the IP address of the gateway.

1

4 Post-Installation Setup Tasks

After you have installed Prime Network, you must perform the following tasks:

Get a Valid Cisco Prime Network License

You must activate a valid Prime Network license within 120 days of installation. Until you activate the license, you will be running an evaluation version of Prime Network, with full functionality. After 120 days, this evaluation version will expire and if Prime Network is closed, it will not restart.

Prime Network software must be registered via Cisco.com in order to obtain a license file (*.lic). The license file will be sent to you by e-mail and must be installed on the Prime Network gateway server.

Note The license file is bound to the server credentials that are provided during license generation. The license file will only be usable on that server only and cannot be ported from one server to another.

For any licensing issues, please contact your Cisco account representative or send an e-mail to ask-ana-licensing@cisco.com for assistance. For further details about licensing, see "Prime Network Licensing" in the *Cisco Prime Network 3.8 Administrator Guide*.

To obtain the license file:

Step 1 Go to the licensing web page at http://www.cisco.com/go/license and enter your Cisco.com user credentials to start the Product License Registration process. If you are not a registered Cisco.com user, create an account and log in.

Step 2 Enter the Product Authorization Key (PAK number) that appears at the bottom of the Software License Claim Certificate you received with your Cisco Prime Network package. The PAK number is a unique, automatically generated identification key that represents the specific software and hardware covered by the license. An example PAK number is ANA-3X-JAB-XXXXXX. Click **Submit** after entering the PAK number.

Step 3 Enter the hostname and host ID of the Prime Network gateway server.

Note If you do not know the host ID, log into the Prime Network gateway server and enter the command **hostid**.

Step 4 Fill in the rest of the requested information, including your e-mail address, and submit the request.

Your license file and user information will be sent within 1 hour to the e-mail address you specified. If you do not receive an e-mail within 1 hour, contact your Cisco account representative or send an e-mail to ask-ana-licensing@cisco.com for assistance.

Caution Do not edit the contents of the .lic file in any way. The contents of the file are signed and must remain intact.

Step 5 Copy the license file to the $FLEXNET_HOME/licenses directory in the Prime Network gateway server.

Step 6 Enter the following status command to verify that the license is loaded:

```
status
```

The output should include the following:

```
- Checking if license server is up and running                    [LOADED]
```

If this is an additional file (i.e, you already have one file in the system path and the license server is up and running), use the following command to load the new file:

```
liccontrol reread
```

This command will make sure the new license was loaded to the server.

Set Up AVMs and VNEs

AVMs are Java processes (independent JVMs) with their own dedicated memory. AVMs are mostly used to provide the necessary distribution support platform for executing and monitoring multiple VNEs.

Each VNE is a virtual representation of a single network element. VNEs are distributed between the AVMs.

The distribution of VNEs to AVMs depends mainly on the VNE memory footprint. A single AVM may hold tens of smaller VNEs (U-PE, access, CEs) or fewer very large VNEs (Aggregation, PE, P).

Follow these general guidelines for AVMs and VNEs:

- Allocate 1.5 GB per AVM.
- Assign VNEs with similar device types to the same AVM. This will reduce the AVMs memory consumption.
- You should have up to 13 AVMs with 1.5 GB each for your entire setup. (This guideline assumes your setup meets the assumptions and caveats described in Assumptions and Caveats.)

Following are more specific guidelines for AVM-VNE distribution based on the Supported Deployment Options for the Quick Start Guide setup:

Table 9 AVM-VNE Distribution Examples

Supported Deployment Option Example	Number and Type of Devices	AVM-VNE Distribution
Carrier E Aggregation	36 aggregation routers (Vikings and 7600 routers)	12 AVMs with 3 VNEs each
MPLS Core	50 core routers (CRS, GSR, 7600, 7200, 6500) 25 aggregation devices (7600, 6500)	5 AVMs with 10 core router devices each 7 AVMs with 4 aggregation devices each
Basic EMS	100 small/medium access routers (ME3400, 4900, 3750, generic VNEs)	2 AVMs with 50 VNEs each If using generic VNEs: 10 AVMS, each with 10 VNEs
IP RAN	5 aggregation routers (7600) 30 cell site devices (MWR2941) 65 layer 2 switches (ME3400)	2 AVMs with 2 and 3 aggregation routers respectively 1 AVM with 30 cell site devices 2 AVMs with 30 and 35 switches
Carrier E	5 NPE devices (7600, Viking) 95 UPE switches (3400, 3750)	2 AVMs with 2 and 3 NPEs each 2 AVMs with 45 and 50 UPEs each

Use the following procedures to create AVMs and assign VNEs:

- Create AVMs, page 22
- Add VNEs, page 23

Create AVMs

You can add AVMs to units or directly to a gateway (in a one-server setup). The AVM must have a unique ID between 101-999 (AVMs 1-100 are reserved by Cisco Prime Network). Every AVM requires a dedicated TCP port which is created using the following naming convention:

AVM-ID + 2000

For example, if you created AVM 711, it would use port 2711. The appropriate TCP port must be available or the AVM creation will fail.

Each AVM has its own log in $ANAHOME/Main/logs.

Note Before you add AVMs, confirm that AVM 0, AVM 99, and AVM 100 are running on the gateway. For more information on the status of AVMs, see "Understanding AVM Status" in the *Cisco Prime Network 3.8 Administrator Guide*.

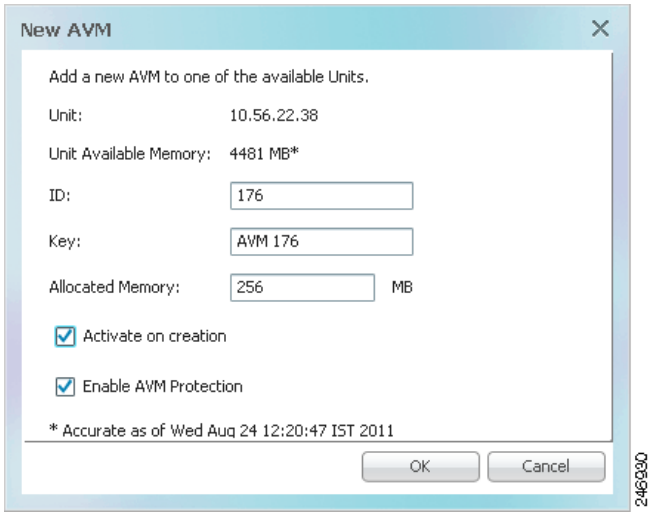
To create an AVM:

Step 1 In Prime Network Administration, expand the Prime Network Servers branch.

Step 2 Right-click the unit (or gateway) on which the AVM will be created, and select **New AVM**. The New AVM dialog is displayed. It provides the following pre-populated information for the AVM:

- The parent unit's IP address, in the Prime Network Unit field.
- The available memory on the unit.
- The allocated memory for the AVM (default is 256 MB).

Figure 3 New AVM Dialog



Step 3 Enter a unique ID for the AVM in the ID field. The ID can be a number between 101-999.

Step 4 Enter a name for the AVM in the Key field. This key will be used as the AVM's unique identifier and display name in Prime Network Administration. If you do not enter a key, the default *ID+time_stamp* is used.

Step 5 Change the maximum allocated memory in the Allocated Memory field. The recommended size for the Quick Start Guide setup is 1536 MB (1.5 GB).

Step 6 Check the Activate on Creation check box to load the AVM, change its administrative status to Up, to ensure that the AVM is loaded on subsequent restarts of the unit.

Step 7 Click **OK**. The new AVM is added to the selected unit and is activated. The AVM can now host VNEs.

Add VNEs

To manage your network elements (NEs) with Cisco Prime Network, you must add VNEs to the system. Each VNE represents a single NE. Adding a VNE involves specifying identifying information and defining the communication protocols the VNE will use to communicate with the NE. When the VNE loads, Cisco Prime Network starts investigating the NE and automatically builds a live model of it, including its physical and logical inventory, its configuration, and its status. The logic and method used by Cisco Prime Network is described in the *Cisco Prime Network 3.7.2 Theory of Operations Guide*. (The *Theory of Operations Guide* was not revised for Cisco Prime Network 3.8)

For detailed information about adding and managing VNEs, see "Managing VNEs" in the *Cisco Prime Network 3.8 Administrator Guide*.

For the purposes of this Quick Start Guide, we assume the following:

- The default Telnet protocol (not SSH) will be used for network element access (reachability) and modeling.
- ICMP will not be enabled.
- The default polling values will be used to determine polling intervals.
- No additional IP addresses other than the management IP address will be monitored for events.

Before you begin to add VNEs:

1. Make sure that the devices to be managed by Prime Network are configured according to the prerequisites. See Configure Your Devices to Enable Effective Cisco Prime Network Management, page 11.
2. Identify which AVMs will hold which VNEs. See Ensure that Ports to be Used by Prime Network are Open, page 8.

Tip Place devices of the same type together in an AVM to reduce the memory consumption of the VNEs.

3. To speed up the procedure for adding VNEs to Prime Network, prepare the following information for each device in advance:
   a. Device management IP address
   b. SNMPv1 or v2: read and write community strings
   c. SNMPv3: The username and, optionally, the authentication or privacy configuration.
   d. Telnet port number and login sequence.
4. Consider which VNE scheme to specify for your VNEs, Product or IPcore. The VNE scheme determines the network element information that is collected by a VNE and populated in its model. You should choose the scheme based on the device's role in the network. If you want to designate a router as a core Provider or Provider Edge device in an MPLS VPN network, use IPCore, otherwise you can use Product. For details, see "Choosing a Scheme" in the *Cisco Prime Network 3.8 Administrator Guide*.
5. Make sure that the status of the AVM to which you will be adding VNEs is Up.

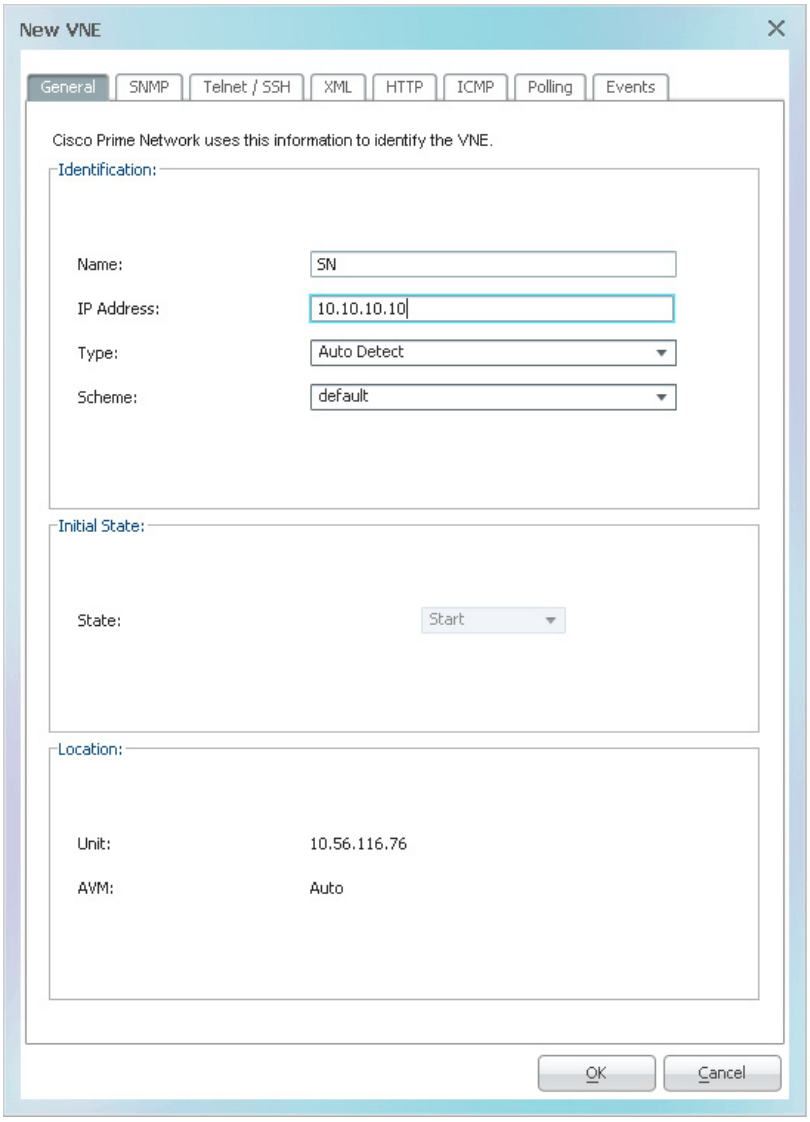
To add VNEs to an AVM:

Step 1 Navigate to the required AVM in the navigation tree.

Step 2 Right-click the AVM, then choose **New VNE**. The New VNE dialog box is displayed.

Step 3 In the General tab, specify the following mandatory information in the relevant fields:
   a. VNE name, which will server as a unique identifier for the VNE.
   b. Device management IP address of the network element.
   c. In most cases, you should be able to use the default values for the other fields. For a full description of all the fields in this tab, see "VNE General Settings" in the *Cisco Prime Network 3.8 Administrator Guide*. You can change these settings at a later stage, if necessary, by right-clicking the VNE and selecting **Properties**.

Figure 4 New VNE - General Tab



Step 4 In the SNMP tab, enter SNMP credentials. For a full description of all the fields in this tab, see "VNE SNMP Settings" in the *Cisco Prime Network 3.8 Administrator Guide*.

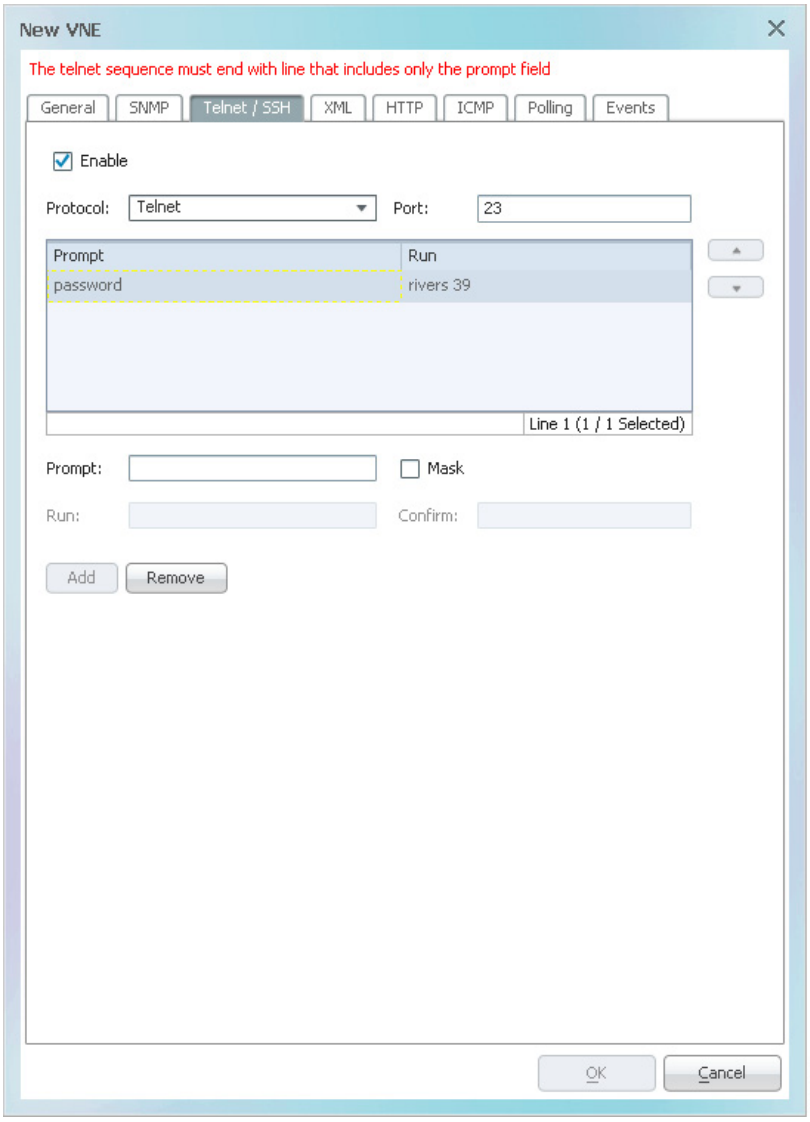
Step 5 In the Telnet/SSH tab, select the Enable checkbox and enter Telnet prompt information, as follows:

a. In the Prompt field, enter the prompt expected from the device.

b. In the Run field, enter the response to the expected prompt.

Note Click **Mask** if you do not want your entries to be displayed in clear text. The Confirm field will be enabled so that you can confirm your Run entry.

Figure 5 New VNE - Telnet/SSH Tab



c. Click **Add**. The prompt-run sequence line is added to the table.

d. Continue to add lines as necessary, ending with a line that includes only the prompt.

For examples of how to enter the Telnet login sequence, see "Telnet and SSH Login Sequences: Notes and Examples" in the *Cisco Prime Network 3.8 Administrator Guide*.

Note Telnet is the default protocol used for network element access (reachability) and modeling. The assumption in this guide is that you will not be using SSH for this purpose. It is also assumed that you will not be using ICMP polling.

Step 6 Click **OK** to create the VNE.

Timesaver For similar VNEs, use the Clone VNE feature. Add the first VNE, then right-click on it and select **Clone VNE**. Specify the VNE name and IP address; other definitions are copied from the source VNE and you can change them if necessary.

Set Up Users and Security

Cisco Prime Network uses two methods to control user access and security:

- Security access roles determine the actions a user can perform in the GUI clients
- Scopes determine which devices a user can access, and the actions they can perform on those devices.

When you create a user in the system, you assign one user access role and one or more scopes to the user.

Cisco Prime Network provides five predefined security access roles that can be assigned to users:

- Viewer—Read-only access to Prime Network Vision to view devices, links, events and inventory.
- Operator—Can perform most day-to-day business operations, such as managing alarms, manipulating maps, viewing network-related information, and managing business tags.
- OperatorPlus—Can manage the alarm lifecycle, in addition to the functions available to the Operator.
- Configurator—Can perform tasks and tests related to configuration and activation of services, through Command Builder, Configuration Archive, NEIM, and activation commands.
- Administrator—Full access to all devices and system functions. Only the Administrator has access to Prime Network Administration and Prime Network Events.

For details about the tasks available for the different user roles and scopes, see "Managing User Security: Roles and Scopes" in the *Cisco Prime Network 3.8 Administrator Guide*.

Add Scopes

Scopes are groups of network elements. Using scopes, you can determine the devices to which users have access. Each scope has a security level that determines which actions the user can take on the devices in the scope.

It is useful to create scopes before creating users so that the scopes will be readily available for assigning to the users. You can also create scopes on-the-fly during the user creation process.

To create a scope:

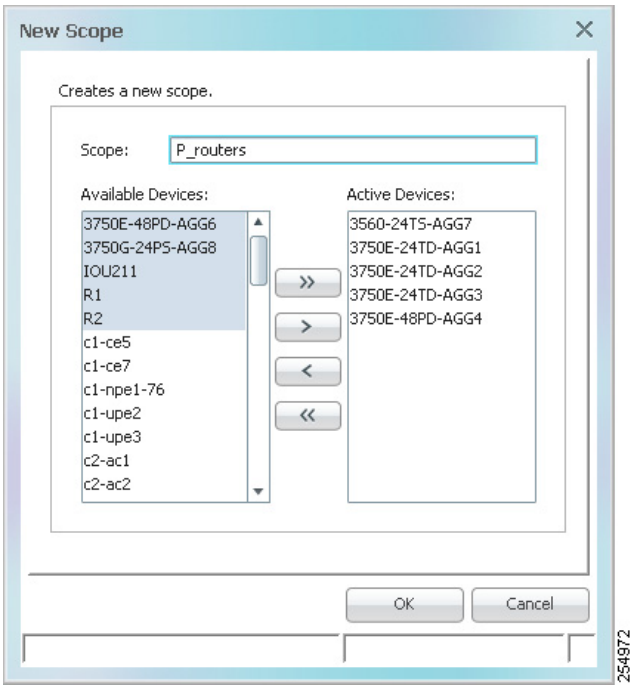
Step 1 Right-click on Scopes in the Prime Network Administration navigation tree, and select **New Scope**.

Step 2 Enter a unique identifying name for the scope in the Scope field.

Step 3 Specify the devices to include in the scope by selecting the required devices from the Available Devices list and then clicking Add All or Add Selected to move the devices to the Active Devices list.

Tip You can use the Ctrl or Shift keys to select multiple devices.

Figure 6 New Scope



Step 4 Click **OK**. The scope is created and is displayed in the content area.

Add Users

You need to create a user account for each person who will be accessing the Prime Network GUI. This involves defining the username and password and other user account settings, assigning a user role, and assigning scopes.

To create a user account:

Step 1 Right-click on Users in the Prime Network Administration navigation tree, and select **New User**. The New User wizard is launched. For detailed information about all the fields in the New User wizard, see "Creating User Accounts and Assigning Default Permissions" in the *Cisco Prime Network 3.8 Administrator Guide*.

Step 2 In the General Information area, enter a unique identifying name for the user in the User Name field, and enter a password in the Password and Confirm Password fields. Follow these guidelines for creating a valid password:

- At least 8 characters long, but not more than 20 characters.
- Must contain at least 3 of the following: lowercase letters, uppercase letters, digits, and special characters.
- Must not contain the user name.
- Must not contain the words Cisco or Prime Network.

Step 3 Click **Next**.

Step 4 In the Prime Network User Role area, select the relevant user role for this user.

Tip When you select a radio button, a description of that role is displayed on the right.

Step 5 In the Device Security area, assign one or more scopes to define the user's device access rights, as follows:

a. Click **Add**. The Add Scope dialog is displayed.

b. Select the required scope(s) in the Available Scopes area.

c. Select a security level for the selected scope(s). This determines what actions the user will be able to perform on the devices in the scope.

d. Click **OK**. The scopes appear in the list of assigned scopes.

Tip Click **Edit** if you want to change the scope's security level.

Note If the scope you need does not exist, click **New Scope** to create it. You will then be able to assign it to the user.

Step 6 Click **Next** if you want to change the User Account settings, or click **Finish** to create the user. The user appears in the table of Prime Network users.

5 First Steps with Cisco Prime Network Vision

After installing and setting up Prime Network, you can start creating maps and monitoring your network elements in Prime Network Vision. This section contains the following subsections:

Log Into Cisco Prime Network Vision

To log into Prime Network Vision:

Step 1 Choose **Start > Programs > Cisco Prime Network > Cisco Prime Network Vision.**The Cisco Prime Network Vision Login dialog box is displayed.

Step 2 Enter your username and password.

Step 3 In the Host field, enter the IP address (as specified during gateway installation) or the hostname of the Cisco Prime Network gateway server.

Step 4 Click **OK**. The Cisco Prime Network Vision window appears empty when it is opened for the first time.

Quick Overview of the Cisco Prime Network Vision GUI

Cisco Prime Network Vision is the main GUI application used to visualize the network through network and service maps, to view device physical and logical inventories and connectivity, and to manage device configuration and software images.

Cisco Prime Network Vision enables you to:

- View network inventory and multiple-layer connectivity.
- Troubleshoot, monitor, and manage network elements (NEs).
- Model and view network maps, maintaining up-to-date topological information on device connections, traffic, and routes.

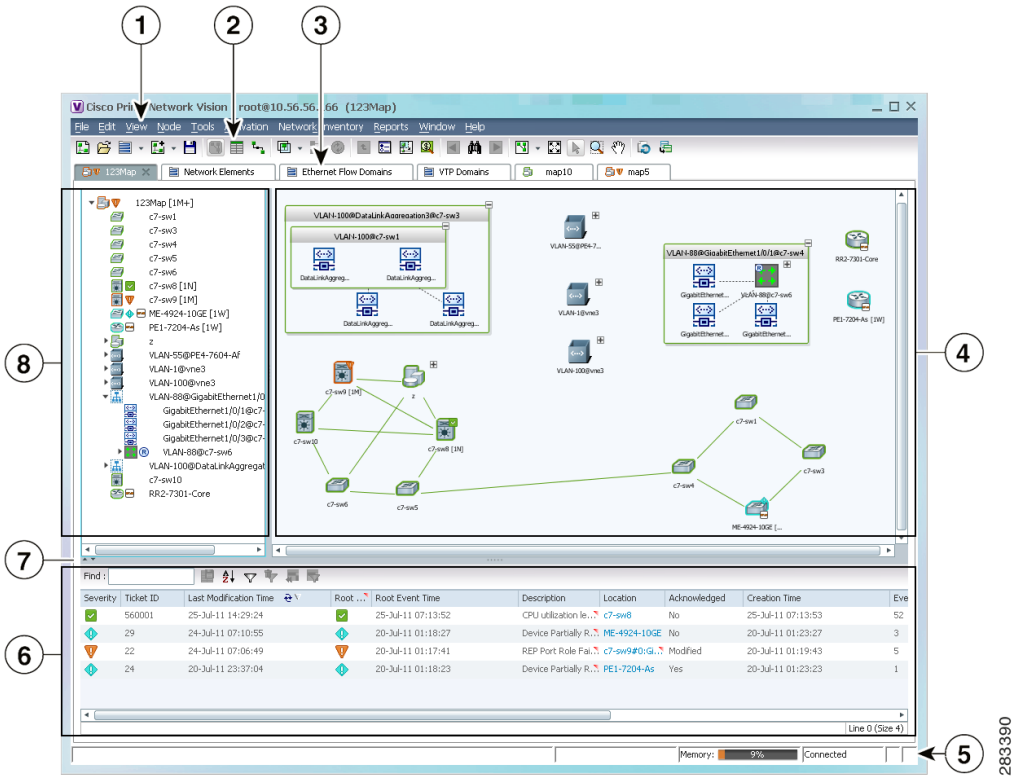
Figure 7 shows the Cisco Prime Network Vision window. The window includes a tree-and-branch representation of the network elements on the left, and a map view representation of the network elements, links, and logical entities such as VLAN, VPNs and other entities that comprise the network on the right.

Map view icons are displayed in aggregated or expanded view. Any icon that has a + in the upper right corner is closed aggregation. Double-clicking it expands the aggregation. Right-clicking and selecting **Show Thumbnail** displays the aggregation contents within the parent map. Anything that has a green frame around it and a - (minus sign) in the upper right corner is an open aggregation. Almost all the items in the upper right corner of Figure 7 are aggregations as indicated by the + symbol. Aggregations can contain other aggregations.

Bell icons displayed in different colors can be attached to network element icons. These are alarm severity badges. The color indicates the highest severity alarm raised for the network element. Beneath the severity badges are the management state badges. The management state indicates the state or mode of the VNE managing a network element and the communication with it. This enables you to determine the accuracy of the network information and the availability of VNEs to carry out network operations.

For a list of all icons and buttons displayed in Cisco Prime Network Vision, see “Icon and Button Reference” in the *Cisco Prime Network 3.8 User Guide* .

Figure 7 Cisco Prime Network Vision Primary Window with an Open Map



1	Menu bar—The functionality that a user can access depends on the user role and the security level of the scopes assigned to the user. The menus are context-sensitive and the options vary depending on your selection in the application. See “Prime Network Vision Window” in the *Cisco Prime Network 3.8 User Guide* for details.
2	Toolbar—The toolbar is context-sensitive and the options vary depending on your selection in the application. See “Cisco Prime Network Vision Toolbar” in the *Cisco Prime Network 3.8 User Guide* for details.
3	Inventory and map tabs—The inventory tabs enables you to access many Prime Network Vision features and functions without opening a map. See “Prime Network Vision Inventory Tabs” in the *Cisco Prime Network 3.8 User Guide* for details.

4	Map view content pane. The content pane displays three views: map, list and links. For details, see "Content Pane: Map, List, and Links Views" in the *Cisco Prime Network 3.8 User Guide* . • Map view—Topological view of managed elements. • List view—Tabular view of managed elements contained in the map. • Links view—Tabular view of links and link aggregations.
5	Status bar—Displays the view's current connection status and status of any issued commands. The memory utilization bar in the status bar displays the amount of memory used by the client. By default, if memory utilization exceeds 60%, it is colored yellow, and if it exceeds 80%, it is colored red.
6	Ticket pane—Displays tickets relating to all the network elements in the map.
7	Hide/display ticket pane.
8	Navigation pane—Displays a tree-and-branch representation of the network elements and aggregations defined for the loaded map.

Create a Map for Network Visualization

Prime Network Vision enables you to create multiple network maps to represent specific network views. Views can cover specific network segments, customer networks, or any other mix of network elements desired. When you create a map, it is available to other users if they have sufficient access and security privileges.

The network maps provide a graphic display of active faults and alarms, and serve as an easy access point for activating services.

To create a new map:

Step 1 Do one of the following:

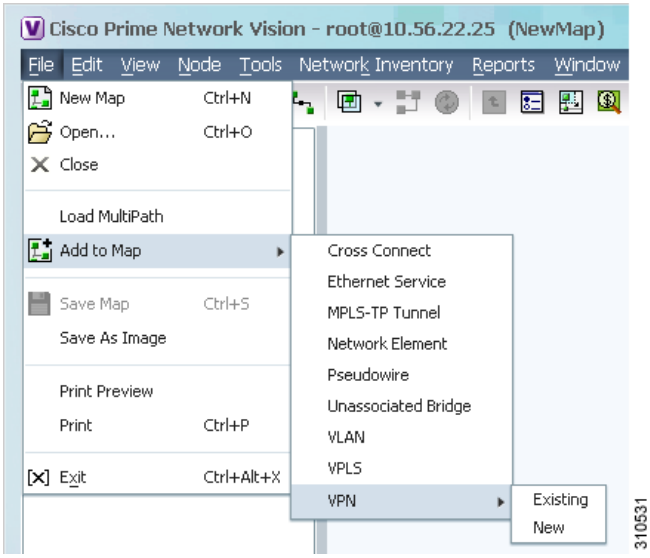
- Click **New Map** in the main toolbar.
- Choose **File > New Map** in the main menu.

The Create Map dialog box is displayed.

Step 2 Enter a name for the new map and click **OK**.

Step 3 Add elements to your new map. Choose **File > Add to Map** or click the down arrow next to the **Add to Map** icon in the main toolbar. Choose the type of element you want to add to the map, for example, network element, VPN, VPLS, VLAN, and so on.

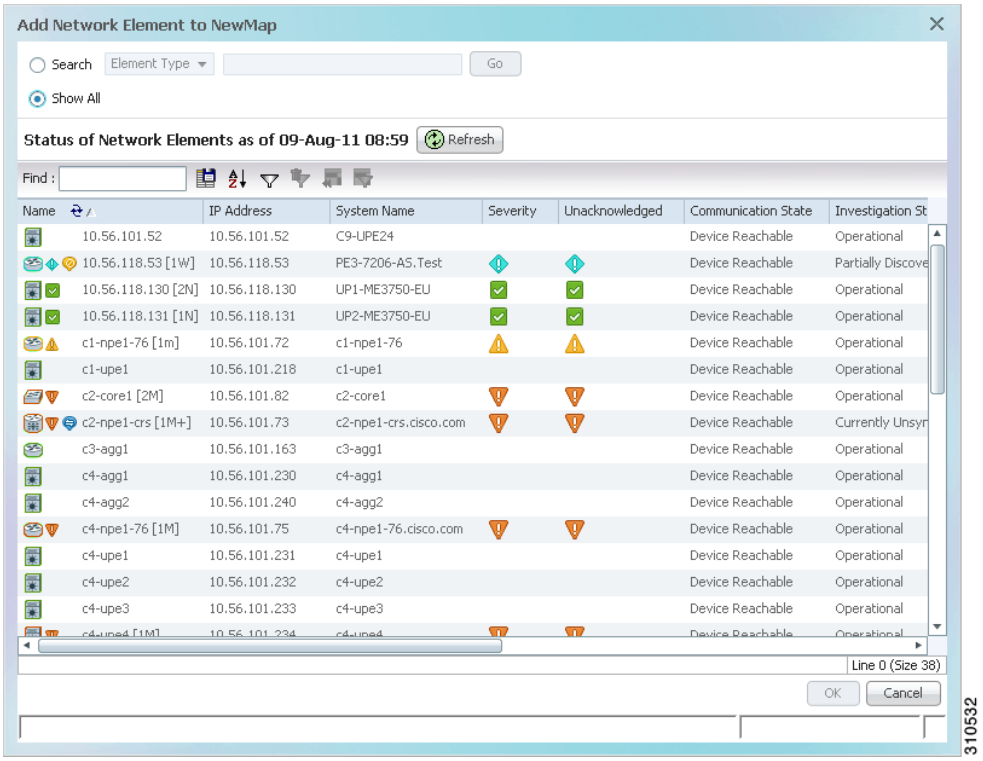
Figure 8 Select Element Type



Step 4 In the Add Element dialog box, either select **Show All** to display all available elements of that type, or run a search for specific elements.

Note If a network element is not included in your scope, it is displayed with the locked device icon.

Figure 9 Select Elements to Add to Map



Step 5 Select the elements that you want to add to the map. You can select and add multiple elements by pressing **Ctrl** while selecting individual network elements or by pressing **Ctrl +Shift** to select a group of elements.

Step 6 Click **OK**. The elements are displayed in the navigation pane and in the map. In addition, any associated tickets are displayed in the ticket pane.

Fault Management Basics

Prime Network analyzes and manages faults through event collection, identification, and correlation. After identifying the event, and associating it to the right device component represented in the VNE, Prime Network groups the events related to it, then uses the virtual network model to inspect the fault and perform correlation to find the root cause and create a ticket.

An *event* is a distinct incident that occurs at a specific point in time, for example, a port status change, connectivity loss, device unreachable, etc. Examples of events include:

- Port status change
- Connectivity loss (for example, BGP Neighbor Loss) between routing protocol processes on peer routers
- Device reset
- Device becoming unreachable by the management station

An event is a possible symptom of a *fault*, which is an error, failure, or exceptional condition in the network.

In Prime Network Vision and Prime Network Events, an icon appears for each ticket or event in the Prime Network (based on the severity). Events have an associated severity, and each severity is represented by a specific color—Critical (red), Major (orange), Minor (yellow), Warning (light blue), Cleared/Normal (green), Information (medium blue), and Indeterminate (dark blue). For more details about event status indicators, see "Prime Network Events Window" in the *Cisco Prime Network 3.8 User Guide* .

The lifecycle of a fault scenario is called an *alarm*. An alarm is characterized by a sequence of related events, such as port-down and port-up. A *ticket* represents an attention-worthy root alarm whose type is marked as ticketable.

For details about tracking faults and working with tickets in Prime Network, see "Tracking Faults using Cisco Prime Network Events" and "Working with Tickets in Cisco Prime Network Vision" in the *Cisco Prime Network 3.8 User Guide* .

Appendix A: Additional Cisco Prime Network 3.8 Guides

The Cisco Prime Network 3.8 documentation set contains the following guides:

- *Cisco Prime Network 3.8 Administrator Guide*
- *Cisco Prime Network 3.8 Customization User Guide*
- *Cisco Prime Network 3.8 Documentation Guide*
- *Cisco Prime Network 3.8 Installation Guide*
- *Cisco Prime Network 3.8 Reference Guide*
- *Cisco Prime Network 3.8 Release Notes*
- *Cisco Prime Network 3.8 User Guide*
- *Cisco Prime Network 3.8 Change and Configuration Management User and Administration Guide*
- *Cisco Prime Network 3.8 Activation User Guide*
- *Cisco Prime Network 3.8 Activation Customization Guide*
- *Open Source Used in Cisco Prime Network 3.8*
- *Cisco Prime Network 3.8 Integration Developer Guide*

Appendix B: Device Information Form

You can print this table and use it to organize your AVM-VNE distribution and list the information you will need when creating VNEs.

VNE Name	Device Type	AVM	Management IP Address	SNMP Credentials	Telnet Port and Login