Configuring Device VNEs and Troubleshooting VNE Problems

VNEs are the building blocks of Prime Network model because each VNE maintains a real-time model of a single device, and together, VNEs maintain a model of the entire network. These topics focus on VNEs—how devices are discovered by VNEs, how to check and troubleshoot VNE problems, and how to make changes to VNEs. Adding Devices to Prime Network, page 4-10, explains the various methods you can use to create VNEs and thus add devices to the model, including how to decide which method is best for your configuration.

See these topics for step-by-step procedures for troubleshooting modeling and connectivity problems:

What is the Difference Between a VNE and a Device?

Actions you perform on VNEs are different from actions you perform on devices. It is important to understand the difference between VNEs and devices. VNEs are autonomous, miniature engines, and each VNE is in charge of a single device. The VNE maintains a real-time virtual model of the device (both physical and logical), and its connectivity references to its immediate neighbors. *The VNE is an entity that only exists within* Prime Network*; the real device is a separate entity.* For example:

- A *VNE* has properties such as a VNE scheme, a VNE driver, and a VNE location. The scheme and driver determine the information that is modeled and monitored by Prime Network, and the location identifies where the autonomous engine is running and how it is connected to the gateway. These items are listed on the VNE Properties dialog which you can launch by right-clicking a VNE and choosing **Properties**. These properties are managed using the Administration GUI client.
- A *device* has properties such as a device series and model number, an NE software version, a chassis with slots, and a routing entities table. Device information and actions are managed using the Vision and Events GUI clients (Vision and Events users are normally unaware of VNEs and other backend processes). You can also see a subset of NE properties from the Administration GUI client by right-clicking an NE and choosing **Inventory**. (To see the complete physical and logical inventory and device events, you must use the Vision or Events GUI clients.)

Operators are shielded from much of the backend workings of the VNE because their concern is the real NE being managed. But the VNE process must be completely functional in order for Prime Network to properly model and monitor the device. This administrative condition of the VNE is expressed through the *VNE status*.

Checking Device Discovery, VNE Status, and VNE States

The Prime Network GUI clients provide some common information so that you do not have to switch between clients. For example, just as you can get a subset of VNE information from the Vision GUI client, you can also get a subset of device information from the Administration GUI client. The following table shows what type of information is displayed in the Administration GUI client when you right-click a VNE and choose either **Properties** or **Inventory**.

From VNE Menu	Displays:	For more information, see:
Properties	VNE-related properties: • Name, scheme, type, status, VNE driver version • Protocol settings: SNMP, Telnet/SSH, XML, HTTP, ICMP, TL1, and so forth • Adaptive polling settings (for high CPU events) • Events settings (if the VNE is listening to additional IP addresses)	VNE Properties Reference, page D-1
Inventory	Device-related properties: • Device vendor, product, device series, serial number, and so forth. • Software system and version • "Up since" data, contact, location Clicking **VNE Status** displays communication details: • Protocol version and connectivity status • Whether the device is using event-based (reduced) polling • Whether the device is generating syslogs or traps Clicking **VNE Details** opens the VNE Properties window (listed in the first row of this table).	*Cisco Prime Network 4.3.1 User Guide* Checking VNE Communication States (Connectivity), page 4-6

These topics explain how Prime Network discovers devices and how to check on the status of modeling and connectivity.

Modeling and Monitoring Device VNEs

When you add a device to Prime Network, Prime Network creates an autonomous VNE that models that single device. The VNE then uses the NE's IP address and southbound management interfaces (such as SNMP or Telnet) to identify the NE by vendor, device family, device subfamily, device type and software version. When the NE type is determined, the VNE collects the basic inventory, both physical and logical, determines its status, and attempts to determine its place in the network topology. The VNE negotiates with peer VNEs (which represent peer NEs) to determine the connectivity and topology at different layers. This model of the network topology, device state, and device inventory is constantly being updated by the VNE, which tracks every change that occurs in the NE or in the network.

VNE Schemes

The information that the VNE collects is determined by the *VNE scheme*. You choose a scheme when you create a VNE. VNE schemes determine what data should be retrieved for each device, and which commands and protocols Prime Network should use to collect that data. When you create a VNE, Prime Network provides a drop-down of available schemes:

Scheme	Use this scheme:
Product	For devices that are not part of the network core, such as the Cisco 800 Series or 2900 Series.
IpCore	For devices that are part of the network core, such as the Cisco 3600 Series or CRS (Carrier Routing System) Series.
EMS	For devices where only system information and physical inventory should be polled (that is, the minimum amount of data). It is supported on all devices but does not support any technologies.
Default	For cases where you are not sure which scheme to choose. Prime Network will use the Product scheme.

For example, devices poll with SNMP, but might also use CLI to poll additional information. Because the IpCore scheme assumes that the device is used as part of an MPLS VPN network containing P and PE devices, Prime Network therefore models these VNEs in a slightly different way. In most cases you can use the Product scheme with customer edge (CE) devices. You can designate a VNE as a core router by setting it to work with the IpCore scheme, or as an edge router by setting it to work with the Product scheme.

If you only want to model a certain set of technologies, create a custom scheme. The scheme is added to the gateway, and you can apply it to VNEs using the Administration client. See Creating a Custom VNE Scheme, page 4-11.

For guidance on choosing a scheme, refer to the *Cisco Prime Network 4.3.1 Supported Technologies and Topologies*.

VNE Communication and Investigation States

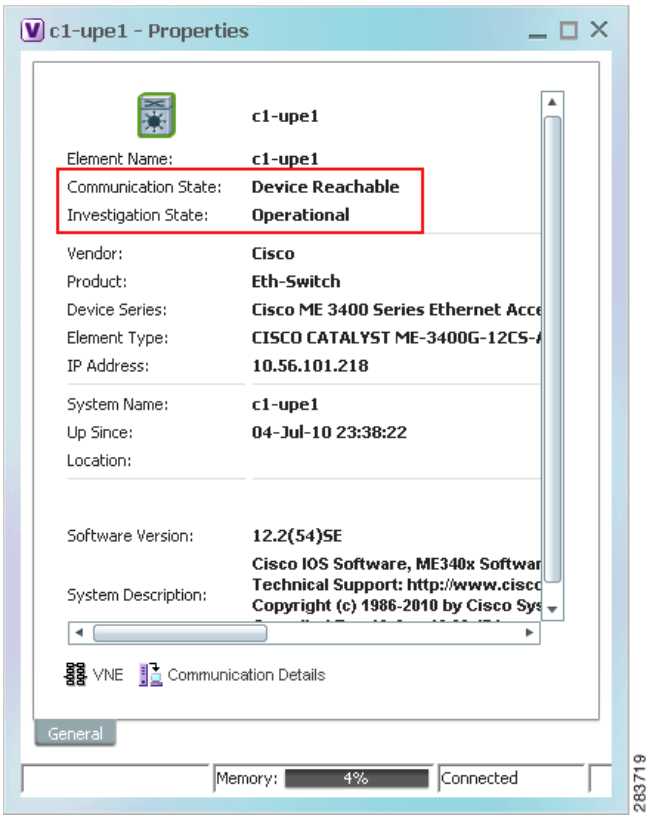
A VNE's administrative condition is conveyed by its VNE *status*—for example, if you stop a VNE, its VNE status will be Down. VNE *states*, on the other hand, describe the degree to which the VNE has discovered and modeled a device, and the disposition of the communication between the VNE and the device it models. VNE state information is intentionally granular so that you can use it to troubleshoot problems.

All VNEs have two states:

VNE State	Description	For more information:
Communication state	Describes the status of communication between devices and VNEs, and VNEs and the gateway server. If a communication state changes, Prime Network generates a Service event.	Checking VNE Communication States (Connectivity), page 4-6
Investigation state	Describes the degree to which the VNE has successfully discovered and modeled a network element. In other words, it gives you an idea of the quality and stability of the device inventory. Because investigation states frequently change, Prime Network does not generate a Service event whenever a VNE's investigation state changes (although you can configure it to do so).	Checking VNE Investigation States (Modeling), page 4-7

Both the communication and investigation states are displayed in Prime Network Vision when you open a device properties window, as shown in Figure 4-1.

Figure 4-1 VNE Communication and Investigation States (in Prime Network Vision)



Note If a VNE was stopped, you will see a message and a refresh button at the top of the properties window. When the VNE is restarted, refresh the window to repopulate the information. If you receive an error message, it means the VNE is still down. To start the VNE, see Stopping, Starting, and Moving VNEs to Maintenance Mode, page 4-9.

If you want more information about the communication state, click **Communication Details** to get information on the status of:

- Protocols the device uses to communicate with the VNE.
- Traps and syslog forwarding from the device to the VNE.

This information is helpful for troubleshooting device reachability problems. For more information, see Checking VNE Communication States (Connectivity), page 4-6.

Checking VNE General Status (Up, Down, Disconnected, Unreachable)

Like AVM status, VNE *status* indicates the administrative condition of the VNE: Starting Up, Up, Shutting Down, Down. If the gateway server cannot communicate with the VNE, the VNE status will be Unreachable. (Remember that this is the status of the VNE, *not* the status of the physical device.) This information is displayed in the Administration GUI client when you select an AVM.

Starting and stopping VNEs is entirely user-directed, as explained in Stopping, Starting, and Moving VNEs to Maintenance Mode, page 4-9. Table 4-1 lists the possible VNE status values that you may see in a table of VNEs.

Table 4-1 VNE Status

VNE Status	Description
Starting Up	A **Start** (command) option was issued.
Up	The VNE process is reachable, was loaded, and has started. This is the status when a **Start** command is issued (or when you create a VNE and choose **Start** as its initial status), and no problems are encountered (such as an overloaded server).
Shutting Down	A **Stop** (command) option was issued and, while the command is being run, some processes are still running, the status of the VNE is Shutting Down.
Down	The VNE process is reachable, but was stopped. This is the status when a **Stop** command is issued. The VNE is both operationally and administratively down. VNEs that were in maintenance mode will move to the Down state in the following circumstances: • The VNE was moved. • The AVM was restarted or moved. • The unit was disconnected or was switched to a standby server. • The gateway was restarted.
Unreachable	The VNE cannot be reached by the gateway, so the VNE cannot be managed. **Note** This is the VNE status, not the device status; the device may be fully reachable.
Disconnected	The VNE is on a unit that was disconnected from the gateway (the unit has a Disconnected status).

Checking VNE Communication States (Connectivity)

VNE *communication* states convey the status of connectivity between:

- The VNE and the device it models (*management* communication)
- The VNE and the gateway (*agent* communication)

When connectivity problems occur, it is normally in the management area—that is, between a VNE and a device. Devices and VNEs communicate using SNMP, Telnet, ICMP, traps, syslogs, and others—all of which determine whether a device is truly reachable. If a problem occurs, Prime Network runs tests tailored to each (enabled) protocol to determine the seriousness of the problem. Prime Network does not change the communication state to Device Unreachable unless *all* of the enabled device management protocols are unresponsive, *and* the device is not generating syslogs or traps.

Table 4-2 describes all of the possible VNE communication states. It also shows the GUI decorator for each state, where applicable. For information on troubleshooting communication state issues, see Troubleshooting VNE Communication State Issues: The Steps, page 4-45.

The  icon indicates a network element has been deleted (or moved). The state will show N/A for Cloud VNEs because Cloud VNEs do not represent a real network element (see Creating Connections Between Unmanaged Network Segments (Cloud VNEs and Links), page 12-42).

Table 4-2 VNE Communication States

State Name	Description	Badge
Agent Not Loaded	The VNE is not responding to the gateway because it was stopped, or it was just created. This communication state is the equivalent of the Defined Not Started investigation state.	None
VNE/Agent Unreachable	The VNE is not responding to the gateway. This can happen if the unit or AVM is overutilized, the connection between the gateway and unit or AVM was lost, or the VNE is not responding in a timely fashion. (A VNE in this state does not mean the device is down; it might still be processing network traffic.)	
Connecting	The VNE is starting and the initial connection has not yet been made to the device. This is a momentary state. Because the investigation state decorator (the hourglass) will already be displayed, a special GUI decorator is not required.	None
Device Partially Reachable	The element is not fully reachable because at least one protocol is not operational. **Note** This is the default behavior. You can change the settings that determine when Cisco Prime Network moves a VNE to Device Unreachable. For more information, see Changing Reachability Settings for VNEs, page 12-25.	
Device Reachable	All element protocols are enabled and connected. **Note** This is the default behavior. You can change the settings that determine when Cisco Prime Network moves a VNE to Device Unreachable. For more information, see Changing Reachability Settings for VNEs, page 12-25.	None
Device Unreachable	The connection between the VNE and the device id down because all of the protocols are down (though the device might be sending traps or syslogs). **Note** This is the default behavior. You can change the settings that determine when Cisco Prime Network moves a VNE to Device Unreachable. For more information, see Changing Reachability Settings for VNEs, page 12-25.	
Tracking Disabled	The reachability detection process is not enabled for any of the protocols used by the VNE. The VNE will not perform reachability tests nor will Cisco Prime Network generate reachability-related events. In some cases this is desirable; for example, tracking for Cloud VNEs should be disabled because Cloud VNEs represent unmanaged network segments. Because this is a user-defined mode (rather than an error or transitional mode), Cisco Prime Network does not display a decorator for this state. To troubleshoot a VNE that is in this state, check the VNE Status Details window; see Troubleshooting Device Connectivity Issues (VNE Communication States), page 4-43.	None

Checking VNE Investigation States (Modeling)

VNE *investigation* states describe how successfully a VNE has modeled the device it represents. These states describe all of the possibilities in the VNE life cycle, from when the VNE is added to Prime Network, through the device modeling, until the VNE is stopped. Table 4-3 describes all of the possible VNE investigation states. It also shows the GUI decorator for each state, where applicable.

Note At any time you can restart the VNE discovery process by restarting the VNE (see Stopping, Starting, and Moving VNEs to Maintenance Mode, page 4-9). If you want to rediscover only a certain element within a device, go to the Prime Network Vision GUI client, open the device inventory, and right-click the element and choose **Poll Now**.

For troubleshooting information, see Troubleshooting Device Modeling Issues (VNE Investigation States), page 4-56.

The  icon indicates a network element has been deleted (or moved). The state will show N/A for Cloud VNEs because Cloud VNEs do not represent a real network element (see Creating Connections Between Unmanaged Network Segments (Cloud VNEs and Links), page 12-42).

Table 4-3 VNE Investigation States

State Name	Description	Badge
Defined Not Started	A new VNE was created and has not yet started, or an existing VNE was stopped. In this state, A VNE remains in this state until it is started (or restarted).	None
Initializing	The VNE is managed and support of its device type is being validated.	None
Unsupported	The device type is either not supported by Prime Network or is misconfigured (it is using the wrong scheme, or is using reduced polling but the device does not support it). To extend Cisco Prime Network functionality so that it recognizes unsupported devices, use the VNE Customization Builder. Refer to the *Cisco Prime Network 4.3.1 Customization Guide*.	
Discovering	The VNE is building the model of the device (the device type was found and is supported by Cisco Prime Network). A VNE remains in this state until all device commands are successfully executed at least once, or until there is a discovery timeout.	
Operational	The VNE has a stable model of the device. Modeling may not be fully complete, but there is enough information to monitor the device and make its data available to other applications, such as transactions (activation workflows). A VNE remains in this state unless it is stopped or moved to the maintenance state, or there are device errors.	None
Currently Unsynchronized	The VNE model is inconsistent with the device; however, this is often recoverable, or may indicated a small inconsistency (such as a minor inventory component not being properly modeled). Because this state can be due to a variety of reasons, check the VNE Status Details window for: • Modeling information; see Table 4-12 on page 4-63. • Device connectivity information; see Table 4-10 on page 4-49.	
Maintenance	VNE polling was suspended because it was manually moved to this state (by right-clicking the VNE and choosing **Actions > Maintenance**). The VNE remains in this state until it is manually restarted (**Actions > Start**). A VNE in the maintenance state has the following characteristics: • It does not poll the device or process traps and syslogs. • It maintains the status of any existing links. • It responds to VNE reachability requests. • It passively participates in correlation flow issues (but is not an initiator). The VNE is moved to the Stopped state if: it is VNE is moved, the parent AVM is moved or restarted, the parent unit switches to a standby unit, or the gateway is restarted.	

Table 4-3 VNE Investigation States (continued)

State Name	Description	Badge
Partially Discovered	The VNE model is inconsistent with the device because a required device command failed, even after repeated retries. A common cause is that the device contains an unsupported module (in which case you can extend Prime Network to recognize the module using the VNE Customization Builder; refer to the *Cisco Prime Network 4.3.1 Customization Guide*). It could also be due to a more serious issue, such as an inability to reach a configured protocol on the device.	
Shutting Down	The VNE has been stopped or deleted by the user, and the VNE is terminating its connection to the device.	

Stopping, Starting, and Moving VNEs to Maintenance Mode

You can start or stop a VNE, or move a VNE to maintenance mode using the Administration GUI client. When you change the status of a VNE, some information is persisted. Persisted information is data that is stored for later use. (For information on the VNE persistency mechanism, see Persistency Overview, page 12-37.)

Restarting a VNE reinitiates the discovery process. If you want to rediscover only a certain element within a device, go to the Prime Network Vision GUI client, open the device inventory, and right-click the *element* and choose **Poll Now**.

To change a VNE's status, select the VNE and choose one of the following from the right-click **Actions** menu.

- **Start**—Starts the VNE process and triggers its discovery process. The VNE will move through a status of Starting Up to Up. When the VNE is Up, its process is running and it is reachable.
- **Stop**—Stops the VNE process. The VNE will move through a status of Shutting Down to Down. In the GUI, the Maintenance indicator in the AVMs window will display **false**. (If you stop a VNE that was in maintenance mode, its Maintenance indicator will change to **false**. This is also true if the VNE is moved, if its parent AVM is moved or stopped, if the gateway is restarted, or if it is on a unit that is switched to a standby unit.)
- **Maintenance**—Stops some VNE functionality so that you can perform maintenance operations without affecting the overall functionality of the active network. This is useful during planned outages such as software upgrades, hardware modifications, or cold reboots. For more details about what a VNE in the maintenance state does or does not do, see Table 4-3 on page 4-8.

If you change the device software—for example, you install a newer version of Cisco Cat OS—you do not need to restart the VNE. The VNE will gather the new information at its next scheduled poll. However, if you change *VNE* software, you must restart the VNE for your changes to take effect; see Adding New Device Support with Device Packages, page 4-27.

The following table shows the badge used to indicate that a VNE is in maintenance mode.

Badge	Description
	Indicates that a VNE is in maintenance mode in Prime Network Vision (and when pressed in a toolbar, moves a VNE to maintenance mode). In Prime Network Administration, the AVMs window will show the VNE Maintenance indicator as **true**.

To change the state of a VNE or move it to maintenance mode:

Step 1 Expand the All Servers branch, and select the required AVM in the navigation tree.

Step 2 Select the required VNE in the VNEs Properties table.

Step 3 Perform one of the following actions:

- To start the VNE, right-click **Actions > Start**, or click **Start** in the toolbar. A confirmation message is displayed. Click **OK**. An Up status is eventually displayed in the VNEs Properties table. You might see a Starting Up status if the gateway is overloaded or if the VNE is still being loaded. If the AVM hosting the VNE is in a Down status, the VNE status remains Starting Up until the VNE is brought up.
- To stop the VNE, right-click **Actions > Stop**, or click **Stop** in the toolbar. A confirmation message is displayed. Click **OK**. A Down status is eventually displayed in the VNEs Properties table. You might see a Shutting Down status while processes are shutting down.
- To place the VNE in maintenance mode, right-click **Actions > Maintenance**, or click **Maintenance** in the toolbar. A confirmation message is displayed. Click **OK**. A Maintenance status is displayed in the VNEs Properties table.

Adding Devices to Prime Network

These topics provide the information you need to create VNEs so that Prime Network can model and manage the devices in your network.

Adding VNEs: The Steps

Always perform these steps before adding VNEs, regardless of which method you use. These prerequisites have a direct effect on how successfully Prime Network will model and monitor the device.

Table 4-4 Basic Steps for Adding VNEs

Step	Task	Description, or where to get more information
Step 1	Choose a VNE scheme, or create a new one (this controls the data that is retrieved, and which protocols are used)	*Cisco Prime Network 4.3.1 Supported Technologies and Topologies*.

Table 4-4 Basic Steps for Adding VNEs (continued)

Step	Task	Description, or where to get more information
Step 2	Gather all prerequisite information **Tip** Set up defaults for SNMP, Telnet, and SSH, and Prime Network will automatically apply those settings. See Configuring Default SNMP and Telnet/SSH Settings, page 4-12.	• IP address and device name • SNMP—Supported version, read/write community strings, username, authentication or privacy information • Telnet—Port, login sequence (username, password, prompt) • SSH—Supported version, username and password and any other configuration information (cipher, authentication, key exchange, etc.)[1] • XML—Protocol use, port, login sequence • HTTP—Version, port number, URL to connect to device, authentication credentials • TL1— Port, user, password (used by Change and Configuration Management only)
Step 3	(Optional) Set up VNE defaults for SNMP and Telnet/SSH	Configuring Default SNMP and Telnet/SSH Settings, page 4-12
Step 4	Perform all mandatory device configuration tasks	See Configuring Devices, page A-1
Step 5	Choose the best method for creating VNEs, and add them	Choosing a Method for Adding Devices (Creating VNEs), page 4-12

1. We recommend that you first use any SSH client application (such as UNIX SSH or OpenSSH) to determine the device SSH login sequence. Also be sure to perform the required device configuration described in Cisco StarOS Devices—Required Settings, page A-6

Creating Custom VNE Schemes and VNE Defaults for SNMP and Telnet/SSH

You can make the process of creating VNEs much easier by creating new schemes and defaults, as described in these topics:

- Creating a Custom VNE Scheme, page 4-11, so that VNEs will only model the information you are interested.
- Configuring Default SNMP and Telnet/SSH Settings, page 4-12, to specify protocol settings that will be applied by default to all VNEs.

Creating a Custom VNE Scheme

A VNE's scheme determine what data should be retrieved from the device, and which commands and protocols Prime Network should use to collect the data. Three schemes are provided by default: Product, EMS, and IpCore; they are described in VNE Schemes, page 4-3. If none of these schemes meet your needs, you can create a custom VNE scheme. After it is created, the scheme is added to the Schemes drop-down menu in the Administration GUI client.

A best practice is to create a new scheme for one VNE and test it before applying the new scheme to other VNEs. This is suggested because Prime Network does not perform an validation on your chosen technologies.

You cannot delete schemes that are currently being used by any VNEs. If you edit a scheme that is being used by a VNE, the changes are only applied to the VNE if the VNE is restarted.

Step 1 Choose **Global Settings > Scheme Management**. All of the existing schemes are listed. You can edit all schemes except for Product, EMS, and IpCore.

Step 2 Right-click **Scheme Management** and choose **New Customized Scheme**. Prime Network displays a dialog box that lists all technologies.

Step 3 Enter a name and description, and then choose the technologies you want to model or not model by selecting them and clicking **Enable** or **Disable**. The category column can help you decide whether you should include a technology, based on the network type.

Step 4 Verify your changes, and click **OK**.

The new scheme is added to the list of supported schemes and is listed on the Schemes drop-down list in the VNE properties dialog.

Configuring Default SNMP and Telnet/SSH Settings

When you create default settings for the SNMP and Telnet/SSH protocols, the settings are automatically applied to all new VNEs.

Note Be sure the protocols are enabled in the VNE properties dialog box.

To configure default VNE settings, choose **Global Settings > Default VNE Settings**.

- **Default Telnet SSH Setting** are described in Telnet/SSH VNE Properties Reference, page D-6.
- **Default SNMP Settings** are described in SNMP VNE Properties Reference, page D-5.

To find out what version of SNMP or SSH a VNE is using, right-click the VNE and choose **Inventory** and click **VNE Status**.

Choosing a Method for Adding Devices (Creating VNEs)

Prime Network provides a variety of ways to add VNEs. The recommended best practice is the VNE auto-add feature. The auto-add mechanism calculates the predicted memory consumption based on a VNE's role and type. Using that information, Prime Network assigns VNEs to units and AVMs, and balances AVM memory as the VNEs are added. You can monitor the VNEs as Prime Network adds them to the system.

Tip Start your operations from the All Servers branch (that is, right-click **All Servers** and choose the operation). Prime Network will use the auto-add feature.

Table 4-5 briefly describes the methods for creating VNEs and the scenarios for which they are suitable. In all of these cases, you can let Prime Network choose the best unit and AVM, or you can specify them yourself.

Note If Prime Network is installed with Cisco Prime Central, be sure to use a device's SYSNAME as its VNE name. This allows the device to be recognized across the common inventory. Also, do not use **None** or **All** as the SYSNAME, because those names have internal meaning to Cisco Prime Central.

Table 4-5 Methods for Adding VNEs to Prime Network

If this is your situation:	Use this method:	For instructions, see:
The devices you want to add are similar to devices are already managed by Prime Network	Clone an existing VNE and use auto-add	Cloning an Existing Device, page 4-14
The devices you want to add are *not* similar to devices are already managed by Prime Network	Create a VNE "from scratch" and use auto-add	Adding a New Device Type to Prime Network, page 4-17
You are testing a new VNE driver on an existing device		
You are adding many devices and they already exist in your network, and none of the IP addresses are duplicated	Use Network Discovery (uses auto-add)	Using Network Discovery to Add VNEs, page 4-19
You are adding many devices and you want to adjust individual properties using a spreadsheet	Create a CSV file of properties and then use it to create VNEs (uses auto-add, but you can disable it)	Adding Devices Using a CSV File, page 4-22

How VNE Auto-Add Works

When you use the VNE auto-add feature—that is, you create VNEs from the All Servers branch—Prime Network will choose the appropriate unit and AVM for the VNE. If you want the VNEs to be hosted by a specific unit, you can perform the operation from the unit (in the navigation tree), and Prime Network will only choose the appropriate AVM.

Prime Network locates the best AVM by identifying *safe target AVMs*. A safe target AVM has the following characteristics:

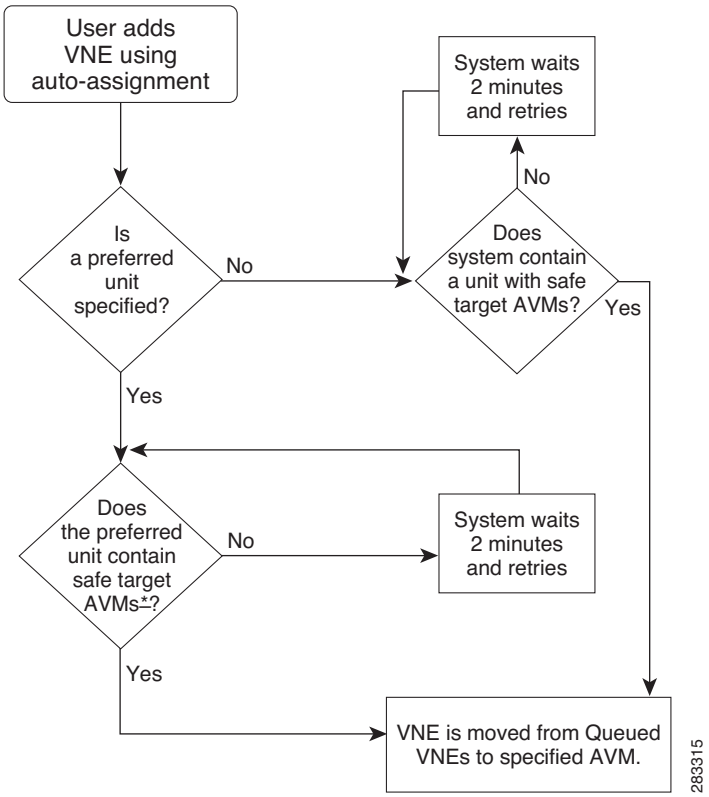
- The AVMs should be up and running.
- It should have sufficient memory to accommodate the VNEs initial memory estimation.

Auto-added VNEs are listed in the **Queued VNEs** tab (under **All Servers**) as the VNEs are assigned to AVMs. They are removed once they are assigned to an AVM and unit.

If Prime Network cannot locate an appropriate AVM, it waits two minutes and tries again. It will continue retrying until an AVM is found. Note that even when you use the auto-add feature, before the VNEs are created, you can choose a unit or AVM for a drop-down list in the VNE properties dialog.

Figure 4-2 illustrates how Prime Network identifies the best AVM and unit in the auto-add process.

Figure 4-2 VNE Auto-Add



Cloning an Existing Device

A clone VNE inherits all of the properties of an existing VNE (including the Device Package being used by the existing VNE). You only have to specify a different name and IP address. Prime Network will choose the best unit and AVM for the VNE, but you can override this with your own choice. Once you have created the clone VNEs, you can still edit their properties before creating them.

Before You Begin

Make sure you have performed any required tasks that are described in Adding VNEs: The Steps, page 4-10. This will ensure that the VNE is properly modeled and updated.

Step 1 Choose the appropriate launch point, depending on whether you want to use the auto-add feature:

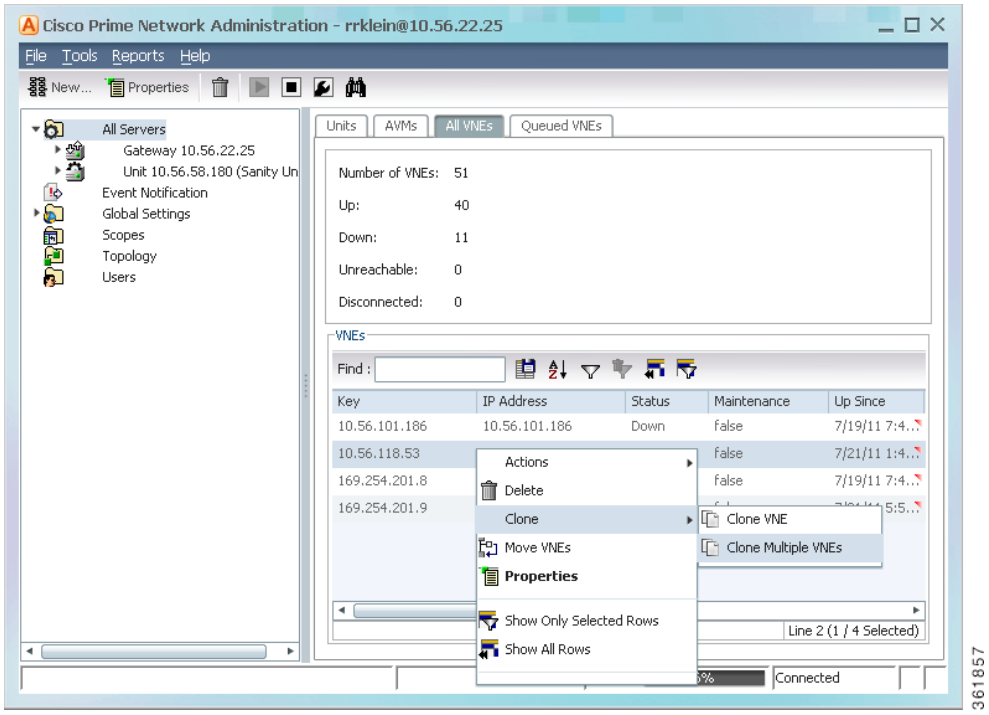
To create VNEs where:	Start the clone operation from this point in the GUI client:
Prime Network chooses the unit and AVM	From **All Servers** in the navigation area, click **All VNEs** tab.
Prime Network chooses the AVM but you choose the unit	From desired unit in the navigation area, click **Unit's VNEs** tab.
You choose the unit and AVM	From desired unit in the navigation area, click the desired AVM

Step 2 In the VNEs table, find the VNE type that you want to replicate.

Step 3 Right-click the VNE you want to replicate and choose **Clone > Clone VNE** or **Clone > Clone Multiple VNEs**.

In Figure 4-3, the user is creating several clone VNEs based on the VNE with the key (name) 10.56.118.53. Because the action was performed while the **All Servers** branch is selected, Prime Network will choose the appropriate unit and AVM.

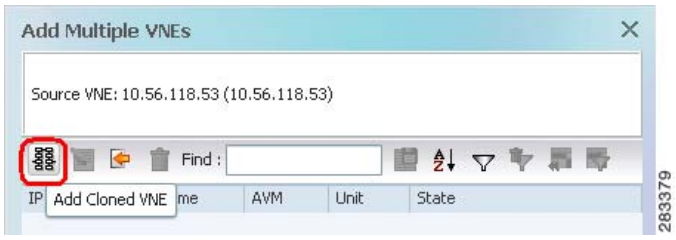
Figure 4-3 Creating a Clone VNE Using Auto-Add—Selecting the VNE



Step 4 Create the clone VNE(s).

a. In the Add VNEs from Clone dialog box, click the Add Cloned VNE icon (see Figure 4-4).

Figure 4-4 Creating a Clone VNE Using Auto-Add—Creating the Clones



A Clone VNE dialog box is displayed. It contains all of the properties of the target VNE except for the VNE name and IP address.

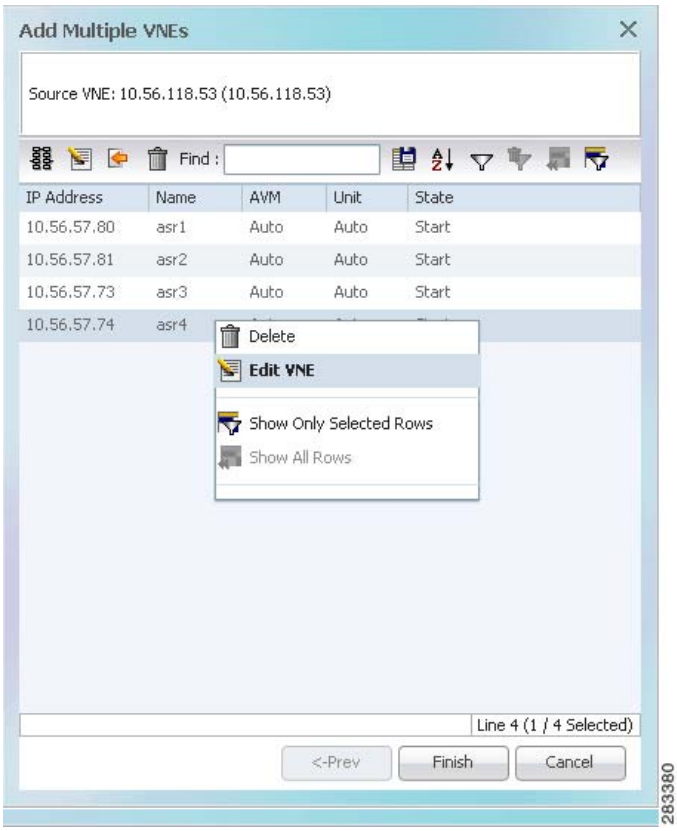
b. Enter the new VNE name and IP address. When finished, click **OK**.

Note If Prime Network is installed with Cisco Prime Central, be sure to use a device's SYSNAME as its VNE name. This allows the device to be recognized across the common inventory. Also, do not use **None** or **All** as the SYSNAME, because those names have internal meaning to Cisco Prime Central.

c. Repeat this step to create additional clones of the VNE. As you create more clones, they are added to the dialog box.

Step 5 To edit the VNE properties before creating the VNEs (for example, to specify a unit or AVM, use a different scheme, and so forth), right-click the VNE and choose **Edit VNE** (see Figure 4-5). If you want, you can specify the unit and AVM you want the VNE to use.

Figure 4-5 Creating a Clone VNE Using Auto-Add—Viewing and Editing the Clones



Step 6 Click **Finish**. To check the status of the VNEs:

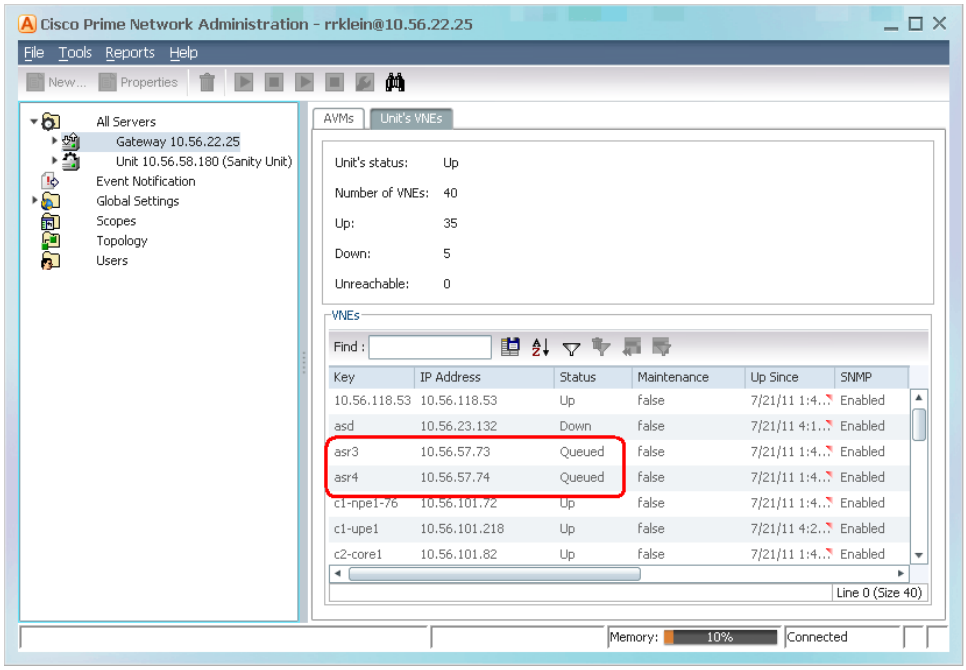
a. For auto-added VNEs (the unit or AVM was selected by Prime Network), select **All Servers** branch and click the **Queued VNEs** tab. If it is empty, the VNEs have been assigned.

b. To find the VNE's assignment, click the **All VNEs** tab and check the unit column.

c. Go to the unit and click the **Unit's VNEs** tab to check the AVM.

Figure 4-6 shows two new VNEs that were added to the gateway but are using AVM auto-assignment. Their assignment is pending.

Figure 4-6 Creating a Clone VNE Using Auto-Add—Checking the Assignment



Adding a New Device Type to Prime Network

If you are creating a VNE for a new device type, you should create a single VNE instance "from scratch" and test it to ensure its settings are correct. You can then clone it as described in Cloning an Existing Device, page 4-14.

Before You Begin

Make sure you have performed any required tasks in Adding VNEs: The Steps, page 4-10. This will ensure that the VNE is properly modeled and updated.

Step 1 Choose the appropriate launch point, depending on how much control you want over the unit and AVM:

To create the VNE(s) where:	Start from this point in the GUI client:
Prime Network chooses the unit and AVM	**All Servers > New VNE**
Prime Network chooses the AVM but you choose the unit	*Unit* > **New VNE**
You choose the unit and AVM	*Unit* > *AVM* > **New VNE**

Step 2 The New VNE dialog box is displayed, opened to the General tab. The following table lists the tabs in the VNE properties window and where you can get more information on the fields in those tabs. Most VNEs only require a VNE name and IP address.

VNE Tab	Description	Described in:
General	Enter general information such as VNE name, IP address, and scheme. By default, Prime Network uses the newest DP installed on the gateway or unit. If you are creating a single VNE, you can specify a different DP from the drop-down list. **Note** When you add a VNE with the same IP address that you have already added but by using a different VNE name, then the New VNE or Clone VNE window displays the following warning message: IP address is already configured on VNE [VNE Name].However, You can proceed the operation based on your decision. If Prime Network is installed with Cisco Prime Central, be sure to use a device's SYSNAME as its VNE name. This allows the device to be recognized across the common inventory.	General VNE Properties Reference, page D-2
SNMP	Specifies SNMP information and credentials to support polling and device reachability. The fields displayed in the dialog box depend on the protocol you select.	SNMP VNE Properties Reference, page D-5
Telnet/SSH	Enables Telnet and SSH for device reachability and investigation, including the Telnet sequence and SSH prompts. The fields displayed in the dialog box depend on the protocol you select.	Telnet/SSH VNE Properties Reference, page D-6
XML	Enables XML for device reachability and investigation.	XML VNE Properties Reference, page D-12
HTTP	Enables HTTP or HTTPS for device reachability and investigation.	HTTP VNE Properties Reference, page D-13
TL1	Enables the TL1 management protocol for running scripts on the device (used by Change and Configuration Management only).	VNE TL1 Properties Reference, page D-14
ICMP	Enables ICMP and the ICMP polling rate (in seconds) for device reachability testing.	ICMP VNE Properties Reference, page D-13
Polling	Associates a VNE with a previously created polling group or allows you to configure different polling settings according to the type of VNE information you want (status, configuration, and so forth).	VNE Polling Properties Reference, page D-14
Adaptive Polling	Controls how the VNE should respond to high CPU events.	VNE Properties: Adaptive Polling, page D-16
Events	Specifies other IP addresses on which the VNE should listen for syslogs and traps.	VNE Properties: Events, page D-17

Step 3 Click **Finish**. Check the status of the VNEs in the VNEs table. For auto-added VNEs:

a. Select **All Servers** branch and click the **Queued VNEs** tab. If it is empty, the VNEs have been assigned.

b. To find the VNE's assignment, click the **All VNEs** tab and check the unit column.

c. Go to the unit and click the **Unit's VNEs** tab to check the AVM.

Using Network Discovery to Add VNEs

Note Refer to the *Cisco Prime Network 4.3.1 Installation Guide* for a list of supported browsers for the Network Discovery feature.

The Network Discovery feature will automatically discover your network devices by traversing the network. Use this method if you are not very familiar with the types of devices in your network. The only required information is an IP address for a seed device, and the SNMPv 2 or SNMPv 3 credentials. This information is added to a discovery profile that specifies the IP and SNMP information, along with any additional protocols or filters you want Prime Network to use. You can use multiple discovery techniques in your filter in order to locate and discover the largest number of devices.

Once your profile is complete, run the discovery job. Prime Network will use its auto-add feature to assign VNEs to AVMs. When the job is finished, a result report provides a listing of devices that were successfully located, devices that were filtered out, and devices that reported credential errors. Prime Network will not create any VNEs until it receives confirmation to proceed. After the discovery job completes, you can instruct Prime Network to create VNEs for the devices that were successfully located. For the devices with credential errors, you can correct or create a new profile, or create the VNEs manually.

Note Network discovery is supported on the following device operating systems: Cisco IOS, Cisco IOS XR, Cisco IOS XE, Cisco NX-OS, Cisco Catalyst, and Juniper operating systems. The Network Discovery feature is not supported in networks that have duplicate IP addresses.

For UCS devices, the Network Discovery feature does the following when it creates UCS VNEs:

- If Telnet is being used, it enables HTTP on the VNE and populates the HTTP credentials fields with the Telnet credentials.
- If SSH is being used, it enables HTTPS on the VNE and populates the HTTPS credentials fields with the SSH credentials.

Before You Begin

Make sure of the following:

- You have performed any necessary tasks that are described in Adding VNEs: The Steps, page 4-10. This will ensure that the VNE is properly modeled and updated.
- The gateway running the discovery process must be able to reach the target devices using the management protocols (SNMP and Telnet/SSH).

Step 1 Choose **Tools > Network Discovery**.

Step 2 Click New to create a new discovery profile. The profile determines how Prime Network can locate, identify, and communicate with devices in order to discover them. To add profile information:

- Click the plus sign next to the technique you want to add.
- Check the enable check box for the technique.
- Click **Add Row** and enter your data.
- Click **Save** to save the discovery techniques.

Provide a unique name, and configure the discovery profile.

Profile Information	Description	
Discovery Technique	Methods Prime Network should use to discover devices. You can specify multiple techniques in order to locate and discover the largest number of devices	
	Ping Sweep	Instructs Prime Network to ping a range of IP addresses, and add any devices that respond to the ping. You must specify a seed device IP address and subnet mask to specify a range of IP addresses. **Note** Ping Sweep is the most commonly-used method.
	Protocol Data Techniques	Instructs Prime Network to use other protocols to discover devices, and when a device is found, how many hops further to discover. You must specify a seed device IP address and the allowed number of hops from the device. **Note** If both BGP and OSPF are specified in the same discovery profile, the seed devices specified for each protocol will be combined. For example, if you specify 192.0.2.1 as a seed device for BGP and 192.0.2.2 as a seed device for OSPF, both 192.0.2.1 and 192.0.2.2 will be used for BGP and OSPF. To avoid this, you can create separate discovery profiles – one using BGP and one using OSPF for discovery.
Credential Settings	Pool of credentials Prime Network should use to communicate with and discover the devices. You can use SNMPv2, SNMPv3, Telnet, and SSH. **Note** SNMPv2 or SNMPv3 credentials are required.	

Profile Information	Description	
Management IP Selection Method	Method the system should use to identify which device IP address should be used as the management IP address:	
	Discovered IP	This is default method. Use discovered IP as management IP address.
	Loopback	If the IP address is a loopback, Ethernet, Token Ring, or Serial interface, use its highest IP address as the management IP address.
	System Name	Perform a DNS lookup of the system name to verify the validity of the IP address, and: • If it is verified, use that IP address as the management IP address. • If it is not verified, use the original IP address used to discover the device as the management IP address.
	DNS Reverse Lookup	Perform a reverse DNS lookup of the system name to verify the validity of the IP address, and: • If it is verified, use that IP address as the management IP address. • If it is not verified, use the original IP address used to discover the device as the management IP address.
Filters	(Optional) Criteria for including or excluding devices from the list of discovered devices.	
	System Location	Filter by physical/geographic location of the device as specified in the SYSTEM-MIB). If your network devices are configured with the system location, you can use this filter option.
	Optional Filters	• IP—Filter by IP address. • System Object ID—Filter by device type as specified in the SYSTEM-MIB. • DNS Filter—Filter by domain name (after the system resolves the name of the device from the DNS server).

d. Click **Save** to save your profile. It is automatically added to the Discovery Profiles table.

Step 3 Start the network discovery by selecting the discovery profile and clicking **Run**.

Step 4 Choose **Network Discovery > Discovery Results** and choose your job. The table provides the following information; click the Refresh button at the top right of the window to update the information.

Column	Description	
Name	Discovery job name (profile name plus system-assigned number)	
Status	Status of discovery job	
		Job is running or is completed with no credential errors
		Job is running or completed and encountered credential errors. Consider running the job again or creating the VNE manually.
		Job was aborted

Column	Description
Start Time, End Time	Start and end time of discovery job
Discovery Profile	Name of profile being used by job
Reachable	Number of discovered devices that are reachable and manageable using the specified credentials (before creating the VNEs, you can change the VNE scheme and reduced polling setting; Step 5)
Filtered	Number of devices that were filtered out (for a list of these devices, click the Filtered tab at the bottom of the Discovery Results window)
Credential Error	Number of devices that were identified but could not be managed because of credential problems (for a list of these devices, click the Credential Errors tab at the bottom of the Discovery Results window)

Step 5 To create VNEs for the reachable devices, use this procedure. Prime Network will auto-add the VNEs—that is, it will choose the unit and AVM for each VNE.

a. Click the Reachable tab at the bottom of the Discovery Results window.

b. If you want to change the VNE scheme or reduced polling setting before creating the VNEs, click the **Edit** button and change the settings. For information on schemes and reduced polling, refer to the *Cisco Prime Network 4.3.1 Supported Technologies and Topologies*.

c. Select the devices you want Prime Network to manage, and click **Create VNEs**. The Status column will change as the VNE goes through the creation process.

Status	Description
Found	Device has been located.
In Progress	VNE creation process is starting.
Queued	VNE was created but has not yet been assigned to an AVM (in the Administration GUI client, they will show a status of Queued).
Naming Conflict	A VNE with that name or IP address already exists. (Correct it and try again.)
IP Conflict	
Assigned	VNE was created and assigned to an AVM. You can check the AVM assignment by located the VNE is the Administration GUI client.

Adding Devices Using a CSV File

Using a CSV file to add VNEs is helpful when you have a large number of VNEs to create and you want to organize your information using a spreadsheet template. After you create the spreadsheet, copy it to the gateway server, and then provide it as input to the Add Multiple VNEs dialog box. Prime Network will auto-add the VNEs—that is, it will choose the unit and AVMs for the VNEs. The new VNEs will use the latest installed DP (the newest DP that is installed on the gateway or unit). If there are any errors, Prime Network will clearly display them. If any fields are left blank, Prime Network uses the defaults specified in Table 4-6.

Format of a CSV File

The CSV file supports all of the entry names listed in Table 4-6. A general guideline is that you should supply the following entries in your file, at a minimum:

```
elementName,ip,SNMPEnabled,SnmpVersionEnum,adminStatusEnum
,SchemeName,avm,unitIP,ICMPPollingRate,ICMPEnabled,PollingGroup,TrapSyslogSources,Telne
tSequence,telnetEnabled
```

The following is the text of a sample CSV file. This CSV file is also provided on the gateway server at *NETWORKHOME*/Main/scripts/BulkVNEImportExample.csv.

```
elementName,ip,SNMPEnabled,SnmpVersionEnum,adminStatusEnum,SchemeName,avm,PrimaryDomain
,unitIP,ICMPPollingRate,ICMPEnabled,PollingGroup,TrapSyslogSources,TelnetSequence,telne
tEnabled
m1,1.1.1.1,TRUE,1,0,ipcore,,Domain1,,50000000,TRUE,slow,,">,prompt,#,",TRUE
m2,1.1.1.2,TRUE,2,1,product,,Domain1,,856000,FALSE,default,,#,TRUE
m3,1.1.1.3 ,TRUE,2,1,,,Domain2,,,TRUE,,"129.5.6.2,55.23.6.5,9.5.2.1",">,text,#,",FALSE
m4,1.1.1.4,TRUE,1,0,,,Domain3,,,FALSE,,121.2.3.4,,TRUE
m5,1.1.1.5,TRUE ,1,0,ipcore,,Domain3,,5600000,FALSE ,slow,121.2.3.4,">,admin,#,",FALSE
```

Table 4-6 Supported Values for CSV File (Creating VNEs)

CSV Entry	Supported Values	Default Setting and Notes
General Properties		
elementName **Note** If Prime Network is installed with Cisco Prime Central, be sure to use a device's SYSNAME as its VNE name. This allows the device to be recognized across the common inventory. Also, do not use **None** or **All** as the SYSNAME, because those names have internal meaning to Cisco Prime Central.	*string* or *IP address*	Mandatory field[1]
ip	*vne IP address*	Mandatory field
elementClassEnum	**0**=AutoDetect, **1**=Generic SNMP, **2**=Cloud, **3**=ICMP	0 (AutoDetect)
SchemeName	**default** (= product), **product, ipcore**, **ems**, existing custom schemes	product
adminStatusEnum	**0**=Disabled (do not start VNE), **1**=Enabled (start VNE)	1 (start VNE)[2]

Table 4-6 Supported Values for CSV File (Creating VNEs) (continued)

CSV Entry	Supported Values	Default Setting and Notes
avm	*avm ID*	(null) (Use auto-add)
PrimaryDomain	*domain name*	(null)
unitIP	*unit IP address*	(null) (Use auto-add)
SNMP Properties		
SNMPEnabled	**TRUE**=Enabled, **FALSE**=Disabled	TRUE
SnmpVersionEnum	**0**=SNMPv1, **1**=SNMPv2, **2**=SNMPv3	1 (SNMPv1)
SNMPReadCommunity	*string*	public
SNMPWriteCommunity	*string*	private
SnmpV3AuthenticationEnum	**0**=noauth, **1**=auth_no_priv, **2**=priv	0 (noauth)
SnmpV3AuthenticationUserProfile	*string*	(null)
SnmpV3AuthenticationPassword	*string*	(null)
SnmpV3AuthenticationProtocolEnum	**0**=md5, **1**=sha	(null)
SnmpV3EncryptionPassword	*string*	(null)
SnmpV3EncryptionTypeEnum	**0**=des, **1**=aes128, **2**=aes192, **3**=aes256	(null)
Telnet/SSH Properties		
TelnetEnabled	**TRUE**=Enabled, **FALSE**=Disabled	FALSE
TelnetProtocolEnum	**0**=Telnet, **1**=SSHv1, **2**=SSHv2	0 (Telnet)
TelnetPortNumber	*port-number*	23 (Telnet), 22 (SSHv1/v2)
TelnetSequence	*"sequence"*	(null)
SshCipherEnum	**0**=DES, **1**=3DES, **2**=Blowfish	1 (3DES)
SshAuthenticationEnum	**0**=password	0 (password)
SshV1Username	*string*	(null)
SshV1Password	*string*	(null)
SshV2Username	*string*	(null)
SshV2Password	*string*	(null)
XML Properties		
XMLPortNumber	*port-number*	38751 (Telnet), 52 (SSL)
XmlProtocolEnum	**0**=Telnet, **1**=SSL	0 (Telnet)

Table 4-6 Supported Values for CSV File (Creating VNEs) (continued)

CSV Entry	Supported Values	Default Setting and Notes
XMLEnabled	**TRUE**=Enabled, **FALSE**=Disabled	FALSE
XMLSequence	*string*	(null)
HTTP Properties[3]		
HTTPPortNumber	*port-number*	80
HttpProtocolEnum	**0**=HTTP, **1**=HTTPS	0 (HTTP)
HTTPEnabled	**TRUE**=Enabled, **FALSE**=Disabled	FALSE
HTTPManagementPath	*string*	(null)
HTTPAuthenticationRequired	**TRUE**=Required, **FALSE**=Not required	FALSE
HTTPUserName	*string*	(null)
HTTPPassword	*string*	(null)
TL1Enabled	**TRUE**=Enabled, **FALSE**=Disabled	FALSE
TL1PortNumber	*port-number*	(null)
TL1Username	*string*	(null)
TL1Password	*string*	(null)
ClientAuthEnum	**0**=password, **1**=public	0 (password)
ClientPrivateKey	*string*	(null)
ServerAuthEnum	**0**=none, **1**=save-first-auth, **2**=preconfigured	2 (preconfigured)
ServerPublicKey	*string*	(null)
FingerPrint	*string*	(null)
ServerAuthDataTypeEnum	**0**=fingerprint, **1**=public-key	0 (fingerprint)
KeyExchange	*string*	(null)
MAC	0=sha1, 1=md5, 2=sha1-96, 3=md5-96	(null)
Cipher	0-3DES, 1=AES-128, 2=AES-192, 3=AES-256	(null)
HostKeyAlgo	0-DSA, 1=RSA	(null)

Table 4-6 Supported Values for CSV File (Creating VNEs) (continued)

CSV Entry	Supported Values	Default Setting and Notes
IsActionNotAllowed	**TRUE**=Not allowed, **FALSE**=Allowed	(null)
ICMP Properties		
ICMPEnabled	**TRUE**=Enabled, **FALSE**=Disabled	FALSE
ICMPPollingRate	*number* (milliseconds)	(null)
Polling Properties		
PollingGroup	**slow**, **default**	default
AdaptivePollingSettingEnum	**0**=Prime Network Settings, **1**=Device Type Settings, **2**=Local Settings	1 (Device Type Settings)
Events Properties		
TrapSyslogSources	"*IP address[,IP address,...]*"	(null)

1. For existing VNEs, you cannot overwrite the VNE name or IP address using a CSV file. To change a VNE name or IP address you must delete the existing VNE and create a new one.
2. If you use auto-add, the VNE will automatically be started regardless of this setting.
3. These settings are not used by VNEs provided with the initial release of Prime Network 4.2. Future Device Packages will introduce new device support for devices that will use this feature.

Before You Begin

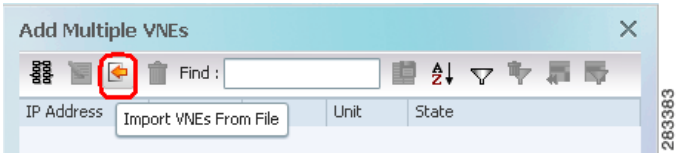
Make sure you have performed any necessary tasks that are described in Adding VNEs: The Steps, page 4-10. This will ensure that the VNE is properly modeled and updated.

Step 1 Select **All Servers > Add Multiple VNEs > Using Default Values**.

Step 2 In the Add Multiple VNEs dialog box:

a. Click the **Import VNEs from File** icon as shown in Figure 4-7.

Figure 4-7 Creating VNEs from a CSV File—Selecting the CSV File



b. Navigate to the file location, select the file, and click **Open**. The Add Multiple VNEs dialog box is populated with the data from the CSV file.

Red text indicates a conflict with an existing VNE. Fix the problem by proceeding to the next step.

Step 3 To edit any VNE properties before creating the VNEs (for example, to specify a unit or AVM, use a different scheme, and so forth), right-click the VNE and choose **Edit VNE** (see Figure 4-5).

Note You can still add individual VNEs using the Clone VNE icon shown in Figure 4-4 on page 4-15.

Step 4 To check the status of the VNEs:

a. For auto-added VNEs (the unit or AVM was selected by Prime Network), select **All Servers** branch and click the **Queued VNEs** tab. If it is empty, the VNEs have been assigned.

b. To find the VNE's assignment, click the **All VNEs** tab and check the unit column.

c. Go to the unit and click the **Unit's VNEs** tab to check the AVM.

Adding New Device Support with Device Packages

These topics explain how to extend Prime Network NE support using the Device Package mechanism, including how to use the **ivne** script to install and manage DPs:

Note When you upgrade a device's operating system (such as installing a Cisco Catalyst OS update), you do not need to restart the VNE. When the VNE polls for configuration information, it will detect the changes and will restart itself. When the VNE reloads, it will update any required registry information, such as the VNE registry path.

Between releases of Prime Network, you can get support for additional device software versions, physical and logical entities, syslogs, traps, and command scripts by downloading and installing Device Packages (DPs) on the gateway server.

As new DPs become available, the DP is placed on the Prime Network Software Download site on Cisco.com. Once you download a Device Package, you can install it using the **ivne** script. Once a DP is installed, if you right-click a VNE and choose **Update VNE Device Package**, the new DP is listed along will available DPs.

Versioning for DPs and Driver Jar Files

VNE driver jar files are cumulative and contain all the enhancements that are provided in earlier versions. All jar files use the following versioning practice:

Vendor-*JarType*-*VNEJarVersion*.**jar**

JarType can be Modules, Commons, or device-specific. For example:

Jar File Example	Description
Cisco-Commons-v1.0.0.0.jar	First release of jar file with support common to all Cisco devices.
Cisco-Modules-v1.0.0.0.jar	First release of jar file with support common to all Cisco modules.
Cisco-ASR90xx-v2.0.0.0.jar	Second release of jar file with support common to all ASR 9000 Series Aggregation Services Routers. Contains all of the support provided in version 1.0.0.0.
Cisco-3750ME-v1.0.0.0.jar	First release of jar file with support common to all Cisco Catalyst 3750 Metro Series Switches.

Similarly, DPs contain the latest version of *all* available jars. Even if a jar is not revised for a DP, it is still included in to ensure that all available enhancements are installed. After installing a DP using the **ivne** script, no changes are applied to a VNE until you restart it.

Prime Network 4.2 DPs use the following versioning practice:

PrimeNetwork-4.2-DP*yymm*

For example, PrimeNetwork-4.2-DP1309 would be the September 2013 DP for Prime Network 4.2.

Finding Out if New Device Support is Available

When a new DP is released, the new support is documented in the *Cisco Prime Network 4.3.1 Supported Cisco VNEs—Addendum*. The addendum is a companion guide to the *Cisco Prime Network 4.3.1 Supported Cisco VNEs* and other supported documents on Cisco.com, which lists the support provided with the base release.

There are DP-specific documents that describe the DP contents and how to install the DP. They are provided with the DP on the Prime Network Software Download site (thus they are available when the the first DP is released):

- A Readme file that describes the DP, including the new support, resolved and open bugs, and links to previous Readmes.
- *Cisco Prime Network 4.3.1 VNE Device Package Installation Guide* (available from the download site when the first DP is released).

Identifying Which DPs Are Installed on the Gateway

This procedure explains how to find out which DP and jar files are installed on the gateway server in *NETWORKHOME*/Main/drivers. Many different versions of DP can be installed at one time and many of them may not be being used.

By default, when a VNE is restarted, it uses the latest DP installed on the gateway or unit. Prime Network will detect the device type and identify the newest DP for that device type (for both Cisco and non-Cisco devices). You can also choose a different driver at a later time as described in Changing the Device Package a VNE Is Using, page 4-30.

Note To identify which driver version is being used by a VNE, see Identifying Which Driver a VNE Is Using, page 4-30.

Step 1 Log into the gateway as *pnuser* and start the **ivne** script.

Note If you receive an error messages that says `Invalid value for width: 80`, it means the terminal window is not wide enough. Enlarge the window and try again.

```
# ivne
-------------------------------------------------------------------------------
|           Cisco Prime Network VNE Device Package Installer
-------------------------------------------------------------------------------
| 1 | Install VNE Device Package from a local directory
| 2 | Install VNE Device Package from a Web repository
| 3 | List installed Device Packages
| 4 | Show latest installed Device Packages
| 5 | Uninstall a Device Package
| q | Quit
-------------------------------------------------------------------------------
```

Step 2 To display *all* DPs that are installed on the gateway server and the jar files they contain, choose **3 - List installed Device Packages**.

Note The following DPs are hypothetical examples.

```
-------------------------------------------------------------------------------
|       Select Device Package (DP) to display the included drivers.
-------------------------------------------------------------------------------
| 1 | PrimeNetwork-4.2-DP0
| 2 | PrimeNetwork-4.2-DP1309
| 3 | PrimeNetwork-4.2-DP1310
| 4 | PrimeNetwork-4.2-DP1311
| 5 | PrimeNetwork-4.2-TPDP1309
| 6 | Back
-------------------------------------------------------------------------------
```

The script lists the contents of the specified DP, as in the following example:

```
Gathering information from /export/home/pn41/Main/drivers/

Name                 Driver File Name            Version    Device Package
Cisco-100xx-PN4.2    Cisco-100xx-v4.2.0.0.jar    4.2.0.0    PrimeNetwork-4.2-DP1311
Cisco-12xxx-PN4.2    Cisco-12xxx-v4.2.0.0.jar    4.2.0.0    PrimeNetwork-4.2-DP1311
Cisco-3400ME-PN4.2   Cisco-3400ME-v4.2.0.0.jar   4.2.0.0    PrimeNetwork-4.2-DP1311
```

Step 3 To display *only* the most recently-installed Cisco DP and the most recently-installed Third Party DP (with no jar details), choose **4 - Show latest installed Device Packages.** (These are hypothetical DPs.)

```
-------------------------------------------------------------------------------
|       Latest installed device packages.
-------------------------------------------------------------------------------
|   | PrimeNetwork-4.2-DP1311
|   | PrimeNetwork-4.2-TPDP1309
| b | Back
-------------------------------------------------------------------------------
```

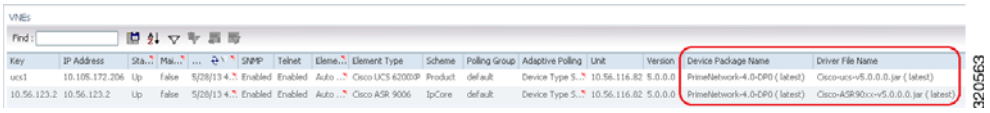
No further information is displayed. Click **Back** to return to the main **ivne** menu. Remember that this is a list of what is installed; it does not mean that any VNEs are necessarily using the jar files. To find out what is being used by VNEs, see Identifying Which Driver a VNE Is Using, page 4-30.

Identifying Which Driver a VNE Is Using

When a VNE is started, it checks the gateway for the most recent DP and uses the applicable driver from that DP. DPs are installed on the gateway server in *NETWORKHOME*/Main/drivers. You can specify a different DP when you create the VNE, or by updating the VNE (see Changing the Device Package a VNE Is Using, page 4-30).

The VNEs table displays the device driver file and version that VNEs are using. Figure 4-8 illustrates the driver jar file information that is shown when you list all VNEs. This information is also provided on the VNE properties page.

Figure 4-8 VNE Driver Jar File Name (By Selecting AVM in Navigation Pane)



To find out if a newer device driver is available, check the *Cisco Prime Network 4.3.1 Supported Cisco VNEs—Addendum.* That document becomes available when the Prime Network DP is published. The "New Support" section lists all new functionality that is available via DP. If new support is available, download and install the DP as described in Downloading and Installing New Driver Files, page 4-31.

Changing the Device Package a VNE Is Using

The update function allows you to choose from all DPs that are installed on the gateway or unit, and apply a DP's corresponding jar file to a VNE. You can choose an earlier DP, effectively rolling back to an earlier driver installation. You must restart the VNE for the changes to take effect.

Tip Test a new DP on one VNE before applying it to the other device types.

If you choose **latest**, Prime Network will use the newest DP installed on the gateway server.

Step 1 If needed, download a copy of the *Cisco Prime Network 4.3.1 Supported Cisco VNEs—Addendum* which lists:

- The support added in a specific DP, by device series.
- The versions of VNE drivers that were with each DP.

Step 2 Right-click a single or group of VNEs and choose **Update VNE Driver Package**. Prime Network displays all installed DPs along with a **latest** choice. These are hypothetical examples:

```
latest
PrimeNetwork-4.2-DP1311
PrimeNetwork-4.2-DP1310
PrimeNetwork-4.2-DP1309
```

In this example, **latest** corresponds to DP1311 (the November 2013 Device Package).

Step 3 Select a DP and click **OK**.

Step 4 Restart the VNEs to apply the changes by right-clicking the VNEs and choosing **Actions > Stop**. When the status changes to Down, right-click the VNEs and select **Actions > Start**.

Downloading and Installing New Driver Files

Use this procedure to download and install new driver files to your gateway server. The new drivers are not applied until you restart the VNEs.

	Step	See:
1.	Check the documentation for new support, and run a report to identify which VNEs should be updated.	Preparing to Install a New VNE Device Package, page 4-31
2.	Download the Device Package tar file according to the instructions on the download site.	Downloading the Device Package, page 4-32
3.	Download the DP installation instructions use **ivne** to install the DP.	Installing the Device Package, page 4-32
4.	Apply the new drivers to the VNEs.	Restarting the VNEs to Apply the New Driver Files, page 4-33

Preparing to Install a New VNE Device Package

Step 1 Check the *Cisco Prime Network 4.3.1 Supported Cisco VNEs—Addendum* to find out what support is available, and note the device types you want to update.

Step 2 If you are not sure what is installed on the gateway server, check it by performing the procedure in Identifying Which DPs Are Installed on the Gateway, page 4-28.

Step 3 Identify the VNEs of that device type. You can do this is several ways; here are two examples:

- Select **All Servers** and click the All VNEs tab. Click the Element Type column to sort the table, and identify the device type you are looking for.
- For long lists, choose **Reports > Run Report > Inventory Report > Hardware Summary (By Selected Property**). When you select devices, enter the device type in the search field, and save and print your list.

Downloading the Device Package

For the current instructions on downloading the DP, use the documentation that is on the download site. This procedure explains how to get the documentation.

Step 1 Log into Cisco.com

Step 2 Go to the Prime Network Software Download site and navigate to the Prime Network VNE Drivers.

Step 3 From the download site, click the hyperlink for the *Cisco Prime Network 4.2 VNE Device Package Installation Guide* (available from the download site when the first DP is released).

Step 4 Follow the instructions in the guide.

Installing the Device Package

The **ivne** script installs DP on the gateway server. The changes are not applied to the VNEs until they are restarted. If any new drivers depend on the support provided in other driver, those jar files are also installed.

Step 1 Make sure you have the necessary information, such as the location of the jar file, by checking the procedure in the *Cisco Prime Network 4.2 VNE Device Package Installation Guide*. (You should have downloaded that file as instructed in Downloading the Device Package, page 4-32.).

Step 2 Log into the gateway as *pnuser* and enter the **ivne** command:

```
# ivne

-------------------------------------------------------------------------------
|           Cisco Prime Network VNE Device Package Installer
-------------------------------------------------------------------------------
| 1 | Install VNE Device Package from a local directory
| 2 | Install VNE Device Package from a Web repository
| 3 | List installed Device Packages
| 4 | Show latest installed Device Packages
| 5 | Uninstall a Device Package
| q | Quit
-------------------------------------------------------------------------------
```

Step 3 Choose **1** or **2**:

- Choose **1** if the new DP is on a local folder on the gateway server.
- Choose ***2*** if the new DP is on a remote host, such as a web server that is providing central support to multiple gateway servers.

The script creates an installation log file in *NETWORKHOME*/Main/drivers/log/ivne-install-log-*mmddyy*-*hhmmss*.

Step 4 Provide the location of the DP files:

If you chose...	Provide the location in this format:
1 (install from tar file)	Enter the full pathname.
2 (install from web repository)	Enter the repository address in one of these formats: *IP-address/full-pathname-to-DP-repository* *hostname/full-pathname-to-DP-repository* Example: 120.56.57.58/drivers

If you use the web repository method and receive an error message, do the following:

- Verify that you entered the correct IP address and hostname.
- Verify that you entered the complete path. For example, **120.56.576.58/drivers** is a complete path, while **120.56.57.58** is not.
- Check if the web server is down.

Restarting the VNEs to Apply the New Driver Files

Click the All VNE tab to view the VNEs table. You can restart individual or groups of VNEs by right-clicking the VNEs and choosing **Actions > Stop**. When the status changes to Down, right-click the VNEs and choose **Actions > Start**.

Uninstalling a Device Package

When you uninstall a DP, the DP files are deleted from the gateway.

Step 1 Check whether any VNEs are using the DP you plan to uninstall (see Identifying Which Driver a VNE Is Using, page 4-30). If any VNEs are using the DP, you need to reconfigure the VNEs to use a different DP. See Changing the Device Package a VNE Is Using, page 4-30.

Step 2 Log into the gateway as *pnuser*.

Step 3 Start the **ivne** script and choose the option to uninstall a DP:

```
# ivne

--------------------------------------------------------------------------------
|           Cisco Prime Network VNE Device Package Installer
--------------------------------------------------------------------------------
| 1 | Install VNE Device Package from a local directory
| 2 | Install VNE Device Package from a Web repository
| 3 | List installed Device Packages
| 4 | Show latest installed Device Packages
| 5 | Uninstall a Device Package
| q | Quit
--------------------------------------------------------------------------------
```

Step 4 The script displays a submenu that lists the installed DPs. The following are hypothetical DPs. Choose one to list the DP contents.

```
-------------------------------------------------------------------------------
|       Select Device Package (DP) to display the included drivers.
-------------------------------------------------------------------------------
| 1 | PrimeNetwork-4.2-DP0
| 2 | PrimeNetwork-4.2-DP1309
| 3 | PrimeNetwork-4.2-DP1310
| 4 | PrimeNetwork-4.2-DP1311
| 5 | PrimeNetwork-4.2-TPDP1309
-------------------------------------------------------------------------------
```

Step 5 Select the DP you want to uninstall from the list that is displayed. The script creates an uninstallation log file in *NETWORKHOME*/Main/drivers/log/ivne-uninstall-log-*mmddyy*-*hhmmss* and uninstalls the DP.

Changing a VNE IP Address and Other VNE Properties

You can edit many of a VNE's properties, such as the IP address, by making changes in the VNE's Properties dialog box, and then stopping and restarting the VNE. The VNE type determines which properties you can edit. For example, you can only edit General settings for Cloud VNEs; for ICMP type VNEs, you cannot edit Polling settings. If you cannot change the desired property, you must create a new VNE.

You do not have to restart a VNE after changing its SNMP, Telnet, SSH, XML, HTTP, or TL1 credentials.

To change a VNE's properties, right-click the VNE and select **Properties** to open the Properties dialog box. When you finish making your change, stop and restart the VNE. See these topics for more information:

- VNE Properties Reference, page D-1, which describes all of the information provided in the various VNE properties dialog boxes.

  For example, if a device is generating configuration change events but Prime Network is not recognizing them, edit the VNE properties (Events tab) and add the IP address you want the VNE to listen to. See VNE Properties: Events, page D-17.
- Changing a VNE IP Address, page 4-35, for a procedure that guides you through changing a VNE's IP address.
- Managing Duplicate IP Addresses, page 4-36, explains any configuration tasks you may have to perform in order to manage duplicate IP addresses.

Some VNE characteristics are controlled by global settings that affect all or groups of VNEs. Some of these can be changed using the Administration GUI client, while others require changes to the registry. These topics describe how to change VNE behavior and properties, and where to get more information:

Table 4-7 Making Advanced Changes to VNEs

For information on how to:	See:
Adjust VNE polling settings, such as: • Reduced (event-based) polling settings • Adaptive polling (for high CPU usage issues) • Smooth polling so VNE registrations use a timer-based approach • Smart polling to introduce a polling protection interval between repetitive queries	Changing VNE Polling Settings, page 12-1
Change the criteria Prime Network uses to designate the Unreachable and Partially Reachable VNE investigation states	Changing VNE and Protocol Settings That Determine Device Reachability, page 12-24
Change how device registration commands (that discover and model the devices) are executed	Changing How VNE Commands Are Executed (Collectors and Command Priorities), page 12-32
Adjust the alarm, modeling, and topology data that is saved across VNE restarts	Changing Settings That Control VNE Data Saved After Restarts, page 12-37
Create a Cloud VNEs to represent an *unmanaged* network segment (so alarms can still be correlated and information can be passed across the segment)	Creating Connections Between Unmanaged Network Segments (Cloud VNEs and Links), page 12-42
Adjust the rate at which VNEs initiate Telnet/SSH connections across the network (to prevent degraded performance on servers such as TACACS)	Improving TACACS Server Performance by Changing VNE Telnet/SSH Login Rates (Staggering VNEs), page 12-51

Changing a VNE IP Address

You can change a VNE's IP address by editing its properties and restarting the VNE. See Managing Duplicate IP Addresses, page 4-36 for information on how Prime Network manages networks in which VNEs have the same IP address.

Note If a device is generating configuration change events but Prime Network is not recognizing them, edit the VNE properties (Events tab) and add the IP address you want the VNE to listen to. See VNE Properties: Events, page D-17.

Step 1 Stop the VNE by right-clicking it and selecting **Actions > Stop**.

Step 2 (Optional) In the Vision GUI client, clear any uncleared tickets for the device.

a. Double-click the device to open its inventory.

b. In the device's ticket pane, right-click all of the tickets and choose **Clear**.

Step 3 In the Administration GUI client, right-click the VNE and select **Properties**.

Step 4 Change the IP address in the General tab.

Step 5 Start the VNE by right-clicking it and selecting **Actions > Start**.

Managing Duplicate IP Addresses

Note Adding VNEs using auto-assign or Network Discovery is not supported in deployments with duplicate IP addresses.

Prime Network can manage networks where two VNEs have the same IP address. If your network has only a single domain, you do not have to perform any extra configuration steps.

For networks with multiple domains, you may have to perform special steps to make sure that Prime Network correctly associate VNEs with their IP addresses. This ensures that Prime Network will properly model the device topology and correlate device alarms. The need to perform extra steps depends on:

- Whether static NAT is configured on the multi-domain network
- Whether the duplicate IP addresses are used *only* as management IPs (and not for any other purposes on devices)

If the IP addresses are used *only* as management IPs, and your network is configured with static NAT, you do not have to perform any extra steps when creating two VNEs with the same IP address. Prime Network will treat the two IP addresses as unique addresses.

Table 4-8 shows the scenarios in which Prime Network can support two VNEs with the same IP address, along with the required configurations you may have to perform for each scenario.

Table 4-8 Supported Scenarios: for Two VNEs with the Same IP Address

Do both VNEs use the IP address ONLY as management IPs?	
Yes	**No**
If the network has static NAT, no special configurations are required when creating two VNEs	If the network has static NAT, do one of the following to the two VNEs: • Configure the VNEs with different domain IDs, OR • Place the VNEs on different units and configure each unit with a different domain ID
If the network does *not* have static NAT, place the two VNEs on different units	If the network does not have static NAT, do one of the following to the two VNEs: • Place the VNEs on different units and configure the VNEs with different domain IDs, OR • Place the VNEs on different units and configure each unit with a different domain ID

Configuring Domain IDs on VNEs

This procedure shows you how to retrieve and set a domain ID on a VNE. If a device spans multiple domains, you can configure the VNE with multiple domain IDs.

Step 1 Log into the gateway as *pnuser* and change to the Main directory.

```
# cd $ANAHOME/Main
```

Step 2 Locate an existing VNE from the same domain, and retrieve its domain ID. In this command, *unit-ip* is the hosting unit, **avm***xxx* is the AVM ID, and *vne-key* is the vne name:

runRegTool.sh -gs 127.0.0.1 get *unit-ip* **avm***xxx***/agents/da/***vne-key*/*topologyDomainsId*

This example retrieves the domain ID from a VNE named c1-npe1-76 which resides on AVM 850 on the gateway server.

```
# ./runRegTool.sh -gs 127.0.0.1 get 127.0.0.1
"avm850/agents/da/c1-npe1-76/topologyDomainsId"
101
#
```

Step 3 Set the domain ID for the VNE.

runRegTool.sh -gs 127.0.0.1 set *unit-ip* **avm***xxx***/agents/da/***vne-key*/*topologyDomainsId*

This example sets a domain ID of 101 on the VNE c1-npe1-76:

```
# ./runRegTool.sh -gs 127.0.0.1 set 127.0.0.1
"avm850/agents/da/c1-npe1-76/topologyDomainsId" 101
success
```

To set multiple domains on the VNE c1-npe1-76 (for example, the device bridges over multiple domains):

```
# ./runRegTool.sh -gs 127.0.0.1 set 127.0.0.1
"avm850/agents/da/c1-npe1-76/topologyDomainsId" "101,102"
success
```

Configuring Domain IDs on Units

This procedure shows you how to retrieve and set a domain ID on a unit.

Step 1 Log into the gateway as *pnuser* and change to the Main directory.

```
# cd $ANAHOME/Main
```

Step 2 Verify whether a domain ID is already set on the unit. Specify the unit with *unit-IP* (for the gateway server, the *unit-IP* is 127.0.0.1).

runRegTool.sh -gs 127.0.0.1 get *unit-ip* **agentdefaults/da/topologyDomainsId**

This example retrieves the domain ID from a unit with the IP address 192.0.2.0 (in this example, no domain ID is set on the unit):

```
# ./runRegTool.sh -gs 127.0.0.1 get 192.0.2.0 agentdefaults/agents/da/topologyDomainsId
null
#
```

Step 3 Set the domain ID for the unit.

```
# ./runRegTool.sh -gs 127.0.0.1 set 192.0.2.0 agentdefaults/agents/da/topologyDomainsId
101
success
```

Moving VNEs to Another AVM

Prime Network automatically load balances the AVM memory usage. However, if you do need to move VNEs to different AVMs, you can certainly do so. When you move VNEs between different AVMs, the VNEs retain their original status, except for VNEs that were in maintenance mode. Those VNEs will be moved out of Maintenance and into the Down status.

Note When you move a VNE to another AVM, the VNE alarm persistency information is saved. Persistency information is data that is stored for later use. For information on the VNE persistency mechanism, see Persistency Overview, page 12-37.

To move one or more VNEs:

Step 1 Expand the All Servers branch, and select the required AVM in the navigation tree. The VNEs are displayed in the content area.

Step 2 Select one or more VNEs using the mouse or keyboard, then right-click one of the selected VNEs.

Step 3 Choose **Move VNEs** from the shortcut menu. The Move To dialog box is displayed.

Step 4 In the Move To dialog box, browse to and select the AVM where you want to move the VNEs.

Step 5 Click **OK**. The VNE is moved to its new location, and now appears beneath the selected AVM in the VNEs Properties table.

You can verify that the VNE has been moved by selecting the appropriate AVM in the navigation tree and viewing the moved VNE in the VNEs Properties table.

Deleting VNEs

When you attempt to delete a running VNE or multiple VNEs from a unit with active services, Single level of caution message will be displayed for confirmation before the removal of devices. Also, you can verify the list of VNE(s) that contain active ports before you confirm the deletion.

During deletion process, the VNE is stopped and all VNE references are deleted from the system and registry. A VNE that has been removed no longer appears in any future system reports.

Note The active ports does not include management ports. VNE information is deleted only if the VNE is Up when you perform the delete operation. If after deleting a VNE you are still seeing tickets and alarms related to the VNE, remove the VNE information manually, as described in the following procedure.

When you delete a VNE, you also delete all Layer 3 VPN site and virtual router business element data associated with the VNE. You can delete business elements separately by using Prime Network Vision. For more information about deleting business elements using Prime Network Vision, see the *Cisco Prime Network 4.3.1 User Guide*.

Since all VNE information is deleted, adding the VNE again requires you to reenter all VNE information.

Note A VNE that has static links configured cannot be deleted without first removing all static links configured for the VNE. Dynamic links are automatically removed.

To delete a VNE:

Step 1 Expand the All Servers branch, and then click the **All VNEs** tab.

Step 2 Right-click the required VNE in the VNEs Properties table, then choose **Delete**. A confirmation prompt is displayed.

Note You can also select multiple VNE(s) in the Properties table for deletion.

Step 3 Before deleting a single VNE or multiple VNEs with no active services, verify the caution messages and choose either one of the following action:

a. In the **Delete VNE** dialog box, If you check the **Remove all services configured on the VNE from the Cisco Prime Network System** check box and click **Yes**, the selected VNE will be deleted and also an alarm will be sent to the plug-ins, such as alarm plug-in or base VPN plug-ins.

b. If you uncheck the **Remove all services configured on the VNE from the Cisco Prime Network System** check box and then click **Yes**, the selected VNE will be deleted and no alarms will be sent to the plug-ins.

c. Click **No** to exit the deletion.

Before deleting a single VNE or multiple VNEs with active services, verify the following messages and choose either one of the following action:

a. If you check the **Remove all services configured on the VNE from the Cisco Prime Network System** check box, all the configured services will be removed when you click **Yes,** and alarms will be sent to the plug-ins; alarm plug-in or base VPN plug-in, otherwise, click **Yes**, to delete the VNEs and no alarms will be sent to the plug-ins.

The VNEs with active services will be deleted only if you select the **Delete VNE(s) with Active services** check box along with VNE(s) without active services or else PN will delete only the VNE(s) without active services that are selected by you for deletion.

b. In the **Delete VNEs** dialog box, click the VNE hyperlink to view the VNEs with active services. The VNEs with active services displayed does not include management ports.

Note If a single VNE or multiple VNEs selected has active services running the **Yes** button will be disabled. For example, If only one device is selected for deletion and if there are running active services detected in that device then, a warning message appears with **Yes** button disabled, and a note is displayed. If you still want to delete the VNE(s) check the **Delete VNE with Active Services** check box to enable the **Yes** option.

c. Click **No**, to exit the deletion.

Step 4 If you click **Yes**, a dialog box appears, asking if you want to delete all Layer 3 VPN business element data for the VNE from Prime Network.

Step 5 Do one of the following:

- Click **Yes** to remove all Layer 3 VPN site and virtual router business element data from Prime Network. This option removes all VPN business elements associated with the selected VNE from Prime Network. Prime Network updates the VPN topology views in Prime Network Vision accordingly by removing the deleted business elements.
- Click **No** to retain the Layer 3 VPN site and virtual router business element data in Prime Network. This option retains the VPN business element associated with the selected VNE in Prime Network. Prime Network updates the VPN topology views in Prime Network Vision; the orphaned business elements are identified by a white X on a red background ( ). To remove these orphaned business elements, delete them manually in Prime Network Vision.
- Click **Cancel** to exit the procedure without deleting the VNE and its Layer 3 VPN site and virtual router business element data.

Step 6 If the VNE was not running when you deleted it from Prime Network, manually delete any remaining VNE ticket and ticket and alarm data. Otherwise Prime Network may generate tickets and alarms related to that VNE, and the tickets and alarms will never clear. To delete the proper files, you will need the following information:

- The VNE IP address
- The VNE's agent ID

To identify the VNE agent ID:

a. Log into the gateway as *pnuser* and change to the Main directory.

```
# cd $ANAHOME/Main
```

b. List the parent AVM's existing VNEs using the following command.

unit-IP is the IP address of the unit hosting the AVM. You can get the *ID* of the hosting AVM by selecting the AVM in the navigation area; the ID will be displayed above the table of VNEs.

runRegTool.sh -gs localhost get *unit-IP* **avm***ID***/agents/da | grep agentId**

The output will show the existing VNEs in the AVM, as in the following example:

```
<entry name="agentId">2</entry>
<entry name="agentId">3</entry>
```

c. List the existing persistency files for that AVM.

ls $ANAHOME/unit/AVM*ID***/persistency/event**

The output will show the existing persistency files in the AVM, as in the following example:

```
1.per
2.per
3.per
```

d. Compare the output of the two commands and identify the extra agent ID. In this example, the extra agent ID is **1**. That is the agent ID of the deleted VNE.

Step 7 Delete the persistency files from the following directories. You will need the VNE IP address for the final location:

$ANAHOME/unit/AVM*ID*/persistency/event/*agentId*.per

$ANAHOME/unit/AVM*ID*/persistency/alarm/*agentId*.per

$ANAHOME/unit/AVM*ID*/instrumentor-persistency/*vne-IP*/*

Assigning VNEs Automatically in Prime Network

The VNEs added are automatically assigned to the best available AVMs. There should be sufficient memory in AVM to accommodate the VNEs initial memory estimation. The Automatic VNE assignment and Automatic AVM generation are controlled by the configurations listed below.

Configuring Registry Controller for Automatically Generating AVMs and Assigning VNEs

To generate AVMs automatically and assign VNEs automatically to the generated AVMs, configure the registry controller:

Step 1 Select the **Tools** option and choose **Registry Controller**.

Step 2 Select the **Automatic VNE assignment** option and specify the required information.

Field	Description
Enable Automatic AVM creation	Generate AVMs automatically. Select **True** to generate AVMS automatically. The default value is **True**.
Enable Automatic VNE assignment	Assigning VNEs automatically to the AVMs. Select **True** to assign VNEs automatically to AVMs. The default value is **True**.
Reassign VNE when AVM is out of memory	Reassigns VNEs to other AVMs when Out of Memory Threshold is reached. Select **True** to reassign VNEs to other AVMs. The default value is **True**.
Out of Memory threshold (%)	Threshold limit of AVM size.The threshold limit ranges between **0** to **100.** When the memory exceeds the threshold limit, the VNE state of the unit changes to Shutdown followed by Down. The VNEs assigned to the unit are automatically queued and are reassigned. The default value is **95%**
AVM size	The size of the AVM in MB. The size of the AVM ranges between **256** to **5000 MB**.
Start AVM numbering from	The AVM number ranges between **101** and **999** MB. The default value is **101**.
Estimated Max VNE size	The estimated initial VNE size in MB.The Estimated Max VNE size ranges between **20** to **500** MB The default value is **100**.
AVM memory Buffer factor	The AVM memory buffer factor ranges between 0.0 to 999999.0. The factor that determines the amount of buffer to be reserved in AVM for internal operations and to accommodate VNE modeling changes. The initial value is 0.5, which reserves 50% of allocated AVM memory. The default value is **0.5**.

Step 3 Click **Apply**.

Assigning VNEs to Gateways or Units Using Network Domains

Network domain is introduced to support VNE assignment based on domain name for the devices behind NAT.

To assign VNEs to gateways or units using network domains:

Step 1 Click **Global Settings** and select **Network Domains** to view the list of available domains.

Step 2 Right click the **Gateway** or **Unit** and choose **Network Domains**.

Step 3 Assign the domain from the available list in the **Assign Gateway to Network Domains** window.

Step 4 Click **OK**.

Step 5 Right click the **All Servers and** choose **Add Multiple VNEs > Using Default Values**.

Step 6 Click the Open icon and select the required CSV file.

Step 7 Click **Open**. The VNEs are listed in the **Add Multiple VNEs** window.

Step 8 Click **Finish**. The VNEs are queued and are listed in the **Queued VNEs** window under the **All Servers** option.

Step 9 Right click the **Gateway** and choose **Network Domains**.

Step 10 Assign the domain from the available list in the **Assign Gateway to Network Domains** window.

Step 11 Click **OK**. The multiple VNEs are assigned to the gateway.

Note Auto Assignment to AVMs is also supported when VNEs are added through network discovery, bulk import through CSV file, adding a single device, and so on.

Troubleshooting Device Connectivity Issues (VNE Communication States)

These topics help you understand how Prime Network determines connectivity and how to troubleshoot common connectivity problems.

- What Determines the VNE Communication State (Device Reachability)?, page 4-43, describes agent and management communication, and how together their state determines the overall communication state of a VNE.
- Troubleshooting VNE Communication State Issues: The Steps, page 4-45, describes what to do if a VNE is in an unexpected communication state. Troubleshooting for investigation states is provided in Troubleshooting Device Modeling Issues (VNE Investigation States), page 4-56.

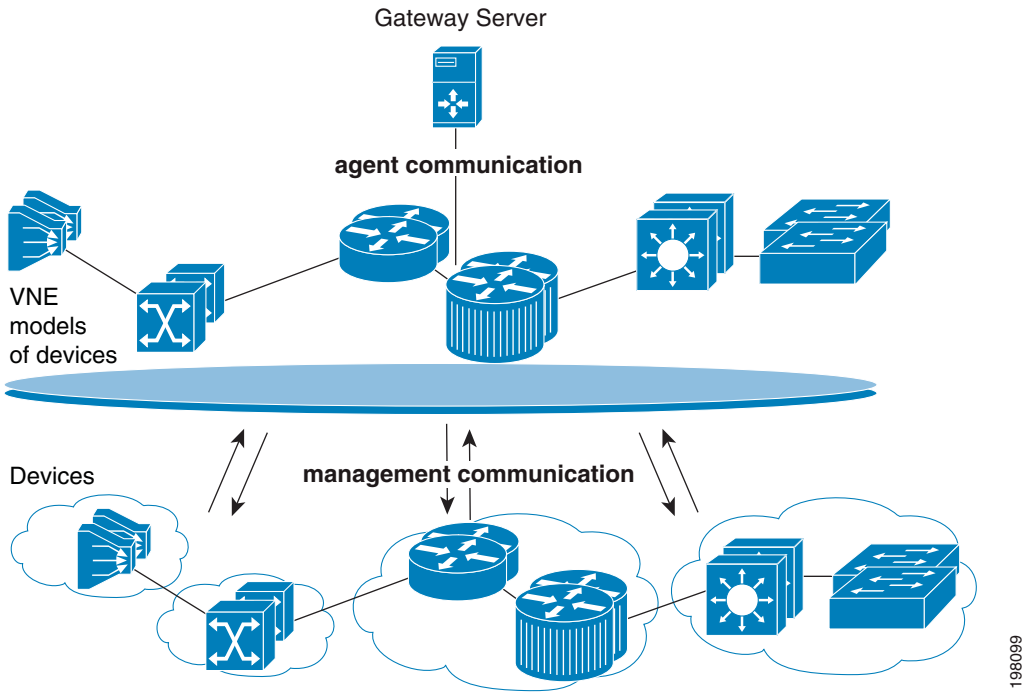
What Determines the VNE Communication State (Device Reachability)?

Figure 4-9 is a simple illustrations that shows the two aspects that determine a VNE's communication state:

- *Agent communication*, which is between the Prime Network gateway server and the VNEs
- *Management communication*, which is between a Prime Network VNE and the network device it is modeling.

Both must function in order for Prime Network to properly model and manage a device.

Figure 4-9 VNE Communication States—Management and Agent



Management communication is the more challenging domain because devices commonly go down; VNEs do not. But there can be different degrees to which a device is down. Perhaps only the Telnet protocol is down but everything else is fine; or all protocols are down but the device is still "alive" (sending syslogs and traps); or *all* protocols down, and the device is not even generating traps or syslogs.

To provide the most accurate reachability status, Prime Network does the following:

- Tracks protocol health by performing reachability tests that are tailored to the different types of protocols.
- Allows you to choose the appropriate *management communication policy* that will determine how more or less strictly you want to track protocol health.
- Allows you to fine-tune both of the above to fit the needs of your network.
- Provides detailed information for troubleshooting purposes.

For details about how Prime Network does all of the above, see Changing VNE and Protocol Settings That Determine Device Reachability, page 12-24.

The most common management problem is when Prime Network reports that a VNE communication state is Device Partially Reachable because at least one protocol is not operational. To help in these situations, the VNE Status Details window often provides valuable information to help you solve the problem. Table 4-10 provides information about the fields in the VNE Status Details window, and suggestions for troubleshooting steps based on the information you see.

When a VNE's communication state changes, Prime Network generates a Service event. For newly-added VNEs, an event is generated only after all protocols have been tested. Reachability-related events are also correlated to each other and to any relevant tickets on the managed device. New events will also be correlated to the relevant ticket.

If a Service event indicates a possible problem, check the event details, which may have valuable information about the device problem. For example, a Device Unreachable event could signal a device protocol problem, or it could indicate that a VNE was shut down as part of normal maintenance.

Note If an AVM or unit crashes, Prime Network will *not* generate a Service event for the communication state change. This is because the event-generating entity (the AVM or unit) is down. However, the GUI will display a VNE/Agent Unreachable icon. Any tickets related to the problem (that were sent before the crash) will remain open until the VNE restarts and generates a clearing event. If no related tickets were sent before the crash, check Prime Network Events for other related information.

Troubleshooting VNE Communication State Issues: The Steps

Use this procedure to troubleshoot an unexpected VNE communication state.

Step	Description	See:
1	Verify the current VNE communication (and investigation) states in Prime Network Vision.	Step 1: Checking the Communication State on the VNE, page 4-45
2	Check the VNE Status Details window to find out if any protocols are failing and why; and check the management communication policy that is being used.You can optionally check the Service event to see if it can provide any new information.	Step 2: Checking the VNE Status Details Window for Protocol and Connectivity Information, page 4-48
3	Test the protocol connectivity.	Step 3: Troubleshooting Device Connectivity Issues, page 4-54

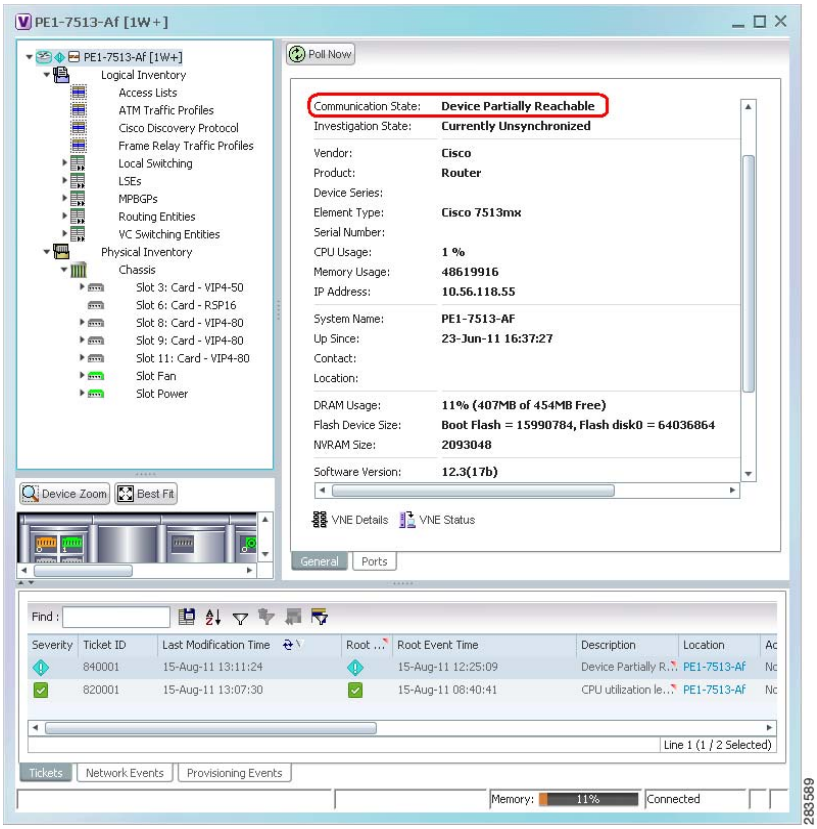
Step 1: Checking the Communication State on the VNE

Step 1 From the Prime Network Vision map view, double-click the icon in which you are interested. This opens the device properties window.

Note You can also launch the device properties window from Prime Network Administration by right-clicking the VNE and choosing **Inventory**.

Step 2 Check the current Communication State (as shown in Figure 4-10).

Figure 4-10 VNE Communication State (in Prime Network Vision)



The  icon indicates a network element has been deleted (or moved).

Note the state and refer to Table 4-2, which explains why a VNE may be in that state and how to proceed.

Table 4-9 VNE Communication States and Troubleshooting Tips

State Name	Description	Badge
Agent Not Loaded	The VNE is not responding to the gateway because it was stopped, or it was just created. This communication state is the equivalent of the Defined Not Started investigation state. To troubleshoot a VNE in this state, check the VNE, AVM, and unit status using Prime Network Administration. Although a Service event is generated whenever the communication state changes, when a VNE is started, an event is generated only after: • All protocols have been tested and a new problem is found (one that was not previously reported). • A problem that was found has been resolved. **Note** If the VNE was stopped, you will see a message and a refresh button at the top of the properties window. If the VNE was restarted, refreshing the window will repopulate the information. However, if the VNE is still down, refreshing the window will result in an error message. To start the VNE, see Stopping, Starting, and Moving VNEs to Maintenance Mode, page 4-9.	None
VNE/Agent Unreachable	The VNE is not responding to the gateway. This can happen if the unit or AVM is overutilized, the connection between the gateway and unit or AVM was lost, or the VNE is not responding in a timely fashion. (A VNE in this state does not mean the device is down; it might still be processing network traffic.) To troubleshoot a VNE in this state: 1. Check the VNE, AVM, and unit status using Prime Network Administration and check the amount of available memory. 2. Use the diagnostics tool to check memory usage, GC, and CPU usage; see Responding to Event Floods and Poor System Performance, page 8-23. 3. Examine the AVM to see if a specific VNE is causing the problem. VNE or AVM reachability issues are often due to CPU-related resource problems.	
Connecting	The VNE is starting and the initial connection has not yet been made to the device. This is a momentary state. Because the investigation state decorator (the hourglass) will already be displayed, a special GUI decorator is not required.	None
Device Partially Reachable	The element is not fully reachable because at least one protocol is not operational. To troubleshoot this state, continue to Step 2: Checking the VNE Status Details Window for Protocol and Connectivity Information, page 4-48. **Note** This is the default behavior. You can change the settings that determine when Cisco Prime Network moves a VNE to Device Unreachable. For more information, see Changing Reachability Settings for VNEs, page 12-25.	
Device Reachable	All element protocols are enabled and connected. **Note** This is the default behavior. You can change the settings that determine when Cisco Prime Network moves a VNE to Device Unreachable. For more information, see Changing Reachability Settings for VNEs, page 12-25.	None

Table 4-9 VNE Communication States and Troubleshooting Tips (continued)

State Name	Description	Badge
Device Unreachable	The connection between the VNE and the device is down because all of the enabled protocols are down (though the device might be sending traps or syslogs). To troubleshoot this state, continue to Step 2: Checking the VNE Status Details Window for Protocol and Connectivity Information, page 4-48. **Note** This is the default behavior. You can change the settings that determine when Cisco Prime Network moves a VNE to Device Unreachable. For more information, see Changing Reachability Settings for VNEs, page 12-25.	
Tracking Disabled	The reachability detection process is not enabled for any of the protocols used by the VNE (specifically, the trackreachability registry key is not set to true; see Changing VNE and Protocol Settings That Determine Device Reachability, page 12-24). The VNE will not perform reachability tests nor will Cisco Prime Network generate reachability-related events. In some cases this is desirable; for example, tracking for Cloud VNEs should be disabled because Cloud VNEs represent unmanaged network segments. Because this is a user-defined mode (rather than an error or transitional mode), Cisco Prime Network does not display a decorator for this state. To troubleshoot this state, continue to Step 2: Checking the VNE Status Details Window for Protocol and Connectivity Information, page 4-48.	None

Step 2: Checking the VNE Status Details Window for Protocol and Connectivity Information

Step 1 From the VNE properties window (see Figure 4-10 on page 4-46), click **VNE Status** at the bottom of the properties window to open the VNE Status Details window. Figure 4-11 shows an example of this window. In this case, the VNE is fully functional.

For an example of a VNE with communication problems, see Figure 4-12 on page 4-53.

Figure 4-11 VNE Status Details Window

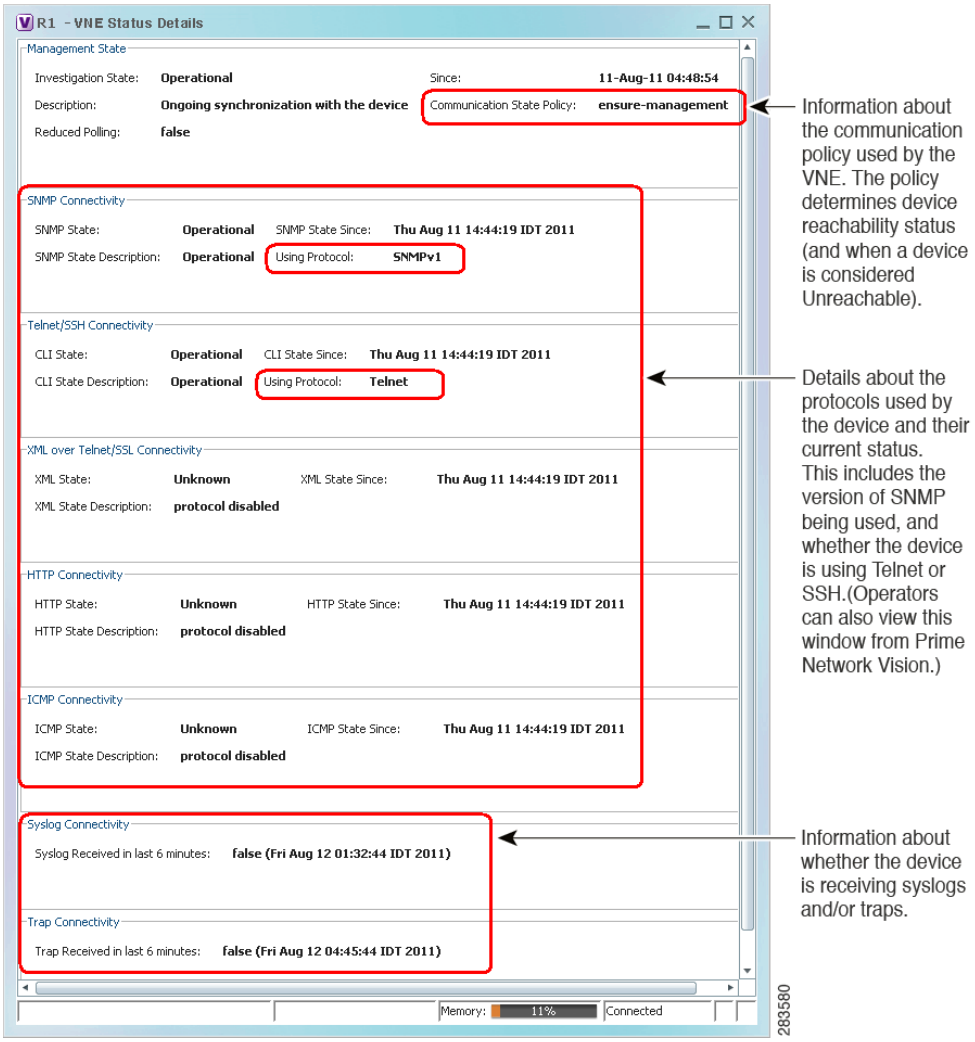


Table 4-10 provides a description of the fields in the window.

Table 4-10 VNE Communication State Information (from VNE Status Details Window)

Field	Description
Management State	The current investigation state, which pertains to device modeling (not communication). For an explanation of the Investigation State, Description, and Reduced Polling fields, see Table 4-12 on page 4-63.
Since	Timestamp of when the management state fields were last updated.

Table 4-10 VNE Communication State Information (from VNE Status Details Window) (continued)

Field	Description	
Communication State Policy	Policy being used by Prime Network to determine device reachability and when to change the communication state to Device Unreachable.	
	notstrict	Change state to Device Unreachable when: • *All* of the enabled protocols are down, and • *No* traps or syslogs were sent by the device for the past 6 minutes. Change state to Device Partially Reachable when: • *All* of the enabled protocols are down. • Traps or syslogs are being sent by device.
	ensure-management	Change state to Device Unreachable when: • *All* of the enabled protocols are down. The status of traps/syslogs is not considered. This is the default policy.
	strict	Change state to Device Unreachable when: • *At least one* of the enabled protocols are down. The status of traps/syslogs is not considered. (Because the state goes directly to Device Unreachable, you will never see the Device Partially Reachable communication state when using this policy.)
Protocol Connectivity		
State	Functional state of the protocol (see the State Description for more details): • Operational • Protocol Partially Functional • Down • Unknown (protocol is disabled) **Reachability is not determined yet i**s a transitional state indicating that the VNE has not yet established whether it can access the device using the specified protocol. This state lasts 1-2 minutes and will change to Down or Operational.	

Table 4-10 VNE Communication State Information (from VNE Status Details Window) (continued)

Field	Description
State Description	Details about the protocol state. Though problems can be due to a variety of issues, the following messages are grouped together by likely cause. • Improper configuration of the VNE or the device. These can normally be solved by verifying that the VNE is using the proper credentials to connect to the device. If that does not solve the problem, proceed to Step 3: Troubleshooting Device Connectivity Issues, page 4-54. **Protocol failed to login** **Protocol failed to get first prompt** **Protocol failed to login when sending leading CR** **Protocol failed to get expected prompt** **Protocol failed to initiate login** **Protocol login authorization refused** **Protocol login authorization timeout** **Authentication failed** • Connectivity issues. Troubleshooting steps for this kind of problem are provided in Step 3: Troubleshooting Device Connectivity Issues, page 4-54. **Protocol failed to handle connection** **Protocol failed to connect to host** **Problem trying to ping host** **Destination host unreachable** • A specific command failed (note that the other commands may have successfully completed). **Protocol failed to send command** **Protocol says: Command authorization failed** **Command execution exception**
State Since	Timestamp of when the protocol information was last updated.
Using Protocol	(Telnet/SSH Connectivity Only) Whether VNE is using Telnet or SSH. This provides an easy way for operators to check which protocol is being used.

Table 4-10 VNE Communication State Information (from VNE Status Details Window) (continued)

Field	Description
Syslog/Trap Connectivity	
Syslog/Trap received in last 6 minutes	Tells you whether the device is sending traps or syslogs (an indication of whether the device is still "alive"). The format is *value* (*time*), where: • *value*—Indicates whether a syslog or trap was (true) or was not (false) received in the last 6 minutes. This field is updated whenever a syslog or trap is received. • *timestamp*—Indicates when the last change occurred. This field is refreshed whenever you open the VNE Status Details window. For example: **false (Mon Jul 19 23:03:33 PDT 2012)** means the VNE has not received any syslogs or traps since the time and date listed. **true (Tue Jul 20 05:09:25 PDT 2012)** means the VNE has been receiving syslogs or traps at least every 6 minutes since the time and date listed. If this field is blank, either no syslogs or traps were sent since the VNE was started, or Prime Network is using a management policy that does not track syslogs and traps. If syslogs or traps are not arriving, do the following: 1. Check the status of Event Collector (AVM 100). See Getting AVM Status and Property Information (Including Reserved AVMs), page 3-8. 2. Check whether the device is configured to forward traps and syslogs to the unit or gateway that has the running Event Collector. See Controlling Event Monitoring, page 9-1.

Figure 4-12 shows a VNE Status Details window for a VNE that is only partially reachable.

Figure 4-12 Communication State Information in VNE Status Details Window

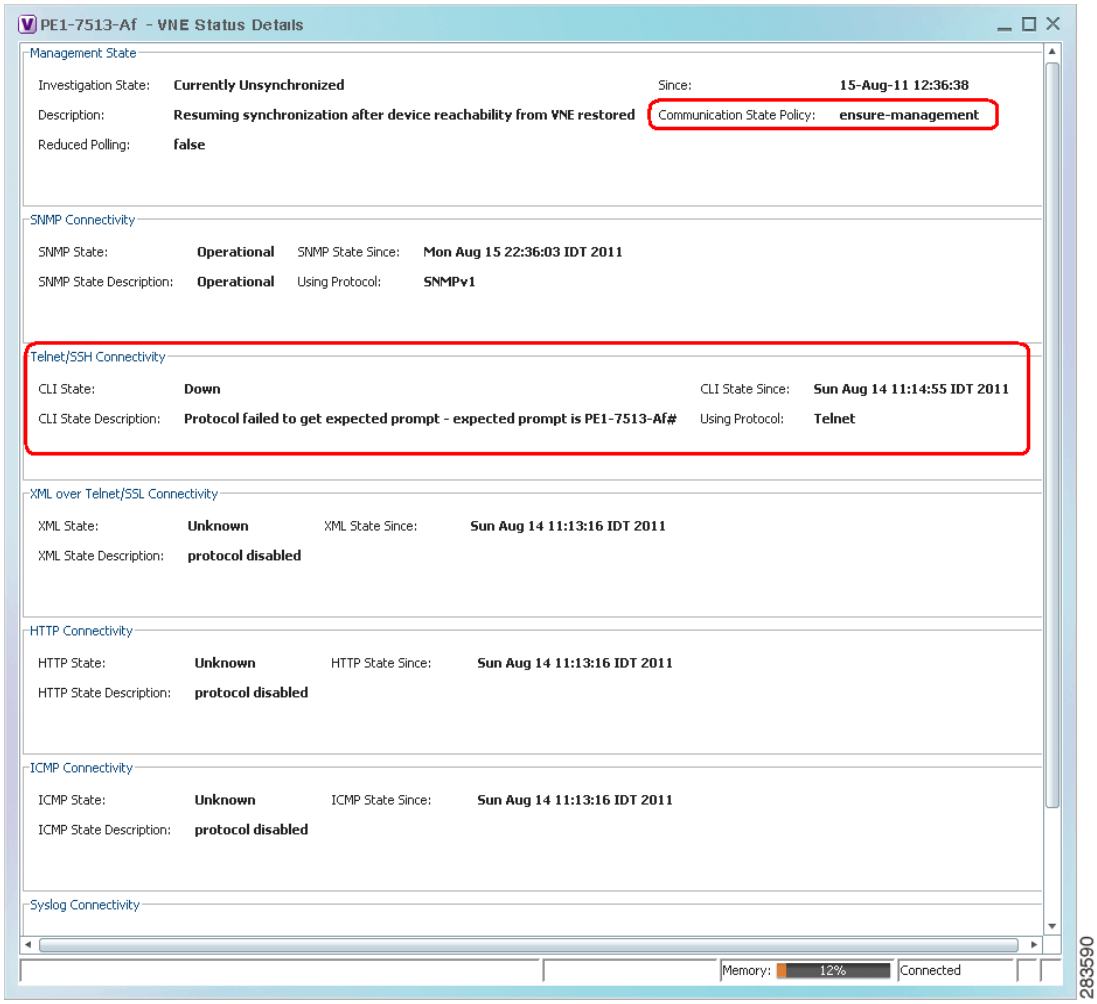


Figure 4-12 provides the following information:

- The VNE is using Telnet and the Telnet protocol failed to connect to the device because the prompt was incorrect. You should correct the Telnet sequence in the VNE properties; see Troubleshooting Device Modeling Issues (VNE Investigation States), page 4-56.
- The VNE is using the ensure-management communication policy which means the device is considered reachable when all enabled protocols are fully functional. So when the Telnet problem is fixed, the VNE should move to the reachable state.

Step 2 Optionally check the System event in Prime Network Events to see if it can provide more details.

Note Keep in mind that if an AVM or unit crashes, Prime Network will not generate a Service event for the communication state change, because event-generating entity (the AVM or unit) is itself down. However, the GUI will display the VNE/Agent Unreachable icon. Any tickets related to the problem (that were sent before the crash) will remain open until the VNE restarts and generates a clearing event. If no related tickets were sent before the crash, check Prime Network Events for other related information.

If you want more information, you can adjust the registry setting so that Prime Network Events generates an elaborated report about state changes. See Table 4-10 on page 4-49.

Step 3: Troubleshooting Device Connectivity Issues

Before you begin these steps, get the following information in order to avoid common mistakes that are made when checking VNE connectivity.

- In Prime Network Administration, get the following information (see Telnet/SSH VNE Properties Reference, page D-6):
  - The protocol and protocol version.
  - The authentication credentials used by the VNE. (For example, if the VNE uses Telnet, you will need the Telnet sequence.)
- Verify that you are using a machine on the same subnet as that on which the VNE resides. (We recommend you run this procedure from the VNE's gateway or unit.)

Follow this procedure to troubleshoot the connectivity problem. Some steps may not apply, depending on your configuration.

Step 1 Try to ping the device. If you cannot, it is likely a network connectivity issue and you will have to work with your system administrator.

Step 2 For Telnet, run the following test to see if the problem is that the device may not recognize **\n** as an end-of-line terminator (a common scenario). You can confirm this problem by opening a Telnet connection to the device and looking for output similar to the following:

```
[64] collector failed to get expected prompt Password: after sending command admin
```

Step 3 If you *do not* see this prompt, proceed to Step 4. If you do see this prompt, use the following procedure to change the end-of-line terminator.

a. Log into the gateway as *pnuser* and change to the Main directory.

```
# cd $ANAHOME/Main
```

b. This example changes the end-of-line terminator to **\r** for an individual VNE; you should check the device and find out what end-of-line terminator to use. In this example, *avmxxx* is the AVM ID, *vne-key* is the VNE name, and *vne-ip* is the VNE P address:

If the VNE is on the gateway server, the *unit-IP* should be **127.0.0.1**.
If the VNE is not on the gateway server, the *unit-IP* should be the unit's IP address.

```
# ./runRegTool.sh -gs 127.0.0.1 set unit-IP
"avmxxx/agents/da/vne-key/ips/vne-ip/protocols/telnet/line-terminator "\r"
```

c. Restart the VNE by right-clicking it and choosing **Actions >Stop**, and then **Actions >Start**.

Step 4 Try to connect to the device.

a. If you are using SSH, check the version the *device* is using, and the versions that are supported in connections.

- Check the SSH version on the device. For Cisco devices, use the **show ip ssh** command. The following example was run on a Cisco 7600:

```
c7-npe1-76#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
c7-npe1-76#
```

- Check the following chart to identify which connection versions are supported.

Device SSH Version	Will Support Connections Using:
SSH 2.*x*	SSHv2
SSH 1.*x*	SSHv1
SSH 1.99	SSHv2 and earlier

b. Using the same protocol that is configured *on the VNE*, open a direct connection to the device.

Note Be sure to perform the test using the same subnet on which the VNE resides (preferably from the same machine). Devices are not always accessible from all subnets.

- For SNMP, use a MIB browser to the sample SNMP MIBs from the device.

Note When you connect, be sure you select the correct version; many SSH client application use a default of SSHv2.

- For Telnet, log into the device from the CLI.

If you *cannot* connect to the device, the likely source of the problem is something in your local configuration. Possible causes you can investigate are:

- Device issues:
  - If the device requires an SSH pseudo-terminal. If a communication snoop reveals an error similar to “client did not request a pseudo terminal,” follow the procedure in Step 5.
  - If you cannot get to the user/password stage, there is probably a device issue, such as an ACL or another configuration that is blocking the access.
- VNE issues:
  - If the VNE is using device credentials that are incorrect or unauthorized.
  - If the VNE is using a communication protocol which is not configured on or allowed by the device. (If you are using SSH, see Step 5.)
  - If the VNE cannot access the device from the VNE’s subnetwork. (A configured route to the device may not exist, or there is some other network accessibility issue.) Try this procedure using the VNE’s unit or gateway.

If you *can* connect to the device, the likely cause of the problem is that the VNE driver was not correctly implemented. Check the Cisco Bug Toolkit for possible open caveats, or open a bug as explained in Opening a Bug Report, page 4-66.

Step 5 Open an SSH Pseudo-terminal, if required by the device (for example, a snoop can revealed an error similar to "client did not request a pseudo terminal"). Edit the registry so that SSH on the VNE requests a pseudo-terminal:

a. Log into the gateway as *pnuser* and change to the Main directory.

```
# cd $ANAHOME/Main
```

b. Edit the VNE's registry as follows, where *avmxxx* is the AVM ID, *vne-key* is the VNE name, and *vne-ip* is the VNE P address.

If the VNE is on the gateway server, the *unit-IP* should be **127.0.0.1**.
If the VNE is not on the gateway server, the *unit-IP* should be the unit's IP address.

```
# ./runRegTool.sh -gs 127.0.0.1 set unit-IP
"avmxxx/agents/da/vne-key/ips/vne-ip/protocols/telnet/connection/explicitly-ask-for
-pty" true
# ./runRegTool.sh -gs 127.0.0.1 add unit-IP
"avmxxx/agents/da/vne-key/ips/vne-ip/protocols/telnet/connection/transport"
# ./runRegTool.sh -gs 127.0.0.1 set unit-IP
"avmxxx/agents/da/vne-key/ips/vne-ip/protocols/telnet/connection/transport/pty-supp
ort" enable
# ./runRegTool.sh -gs 127.0.0.1 set unit-IP
"avmxxx/agents/da/vne-key/ips/vne-ip/protocols/telnet/telnet-over-sshv1/leadingcren
abled" false
# ./runRegTool.sh -gs 127.0.0.1 set unit-IP
"avmxxx/agents/da/vne-key/ips/vne-ip/protocols/telnet/telnet-over-sshv2/leadingcren
abled" false
```

c. Restart the VNE by right-clicking it and choosing **Actions > Sto**p, then **Actions > Start**.

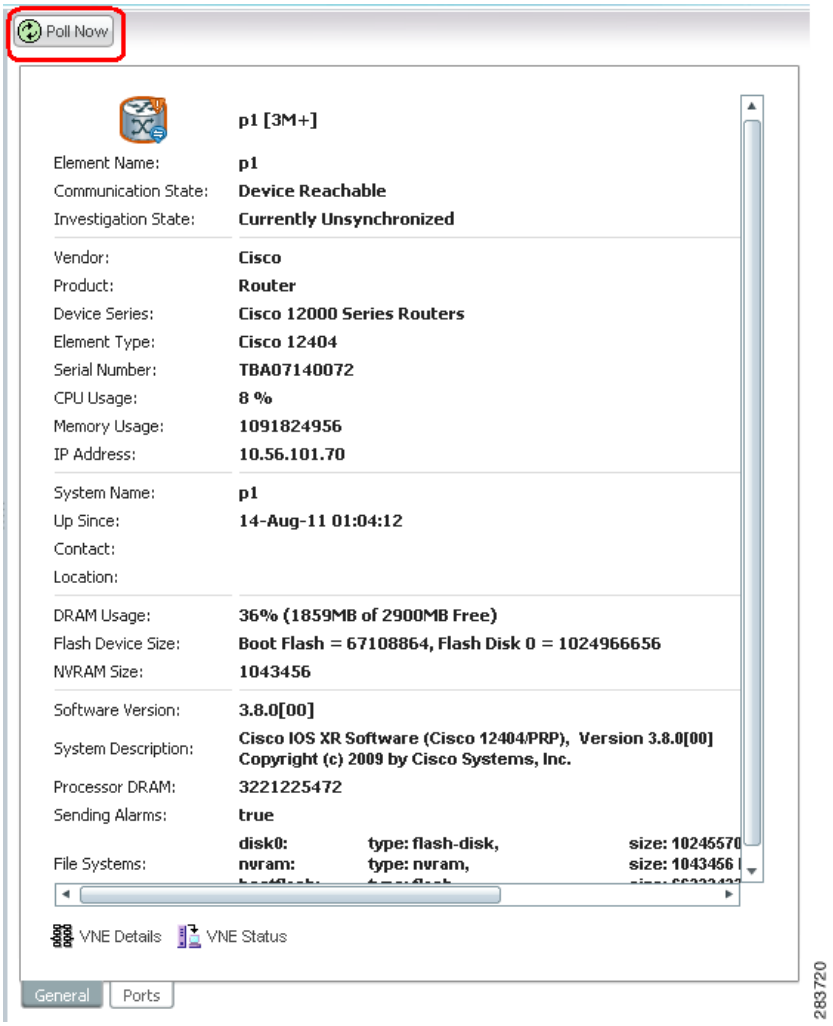
If you need more information about protocols and the tests and settings Prime Network uses to determine reachability, see Changing Reachability Settings for Individual Protocols', page 12-26.

Troubleshooting Device Modeling Issues (VNE Investigation States)

The Administration and Vision GUI clients provide a **Poll Now** tool for rediscovering a network element or an NE component. The launch point determines the entity that is rediscovered. If you right-click a device and choose **Poll Now**, the whole device is rediscovered. If you right-click a device *component* and choose **Poll Now** (from the inventory window), only the component is rediscovered. Vision GUI client users must have Operator privileges to use this feature.

Figure 4-13 shows the device inventory window with the Poll Now button at the top left. When launched from this window, the entire device is rediscovered. Although the Poll Now button is provided for use by all VNEs, it is specifically useful for VNEs using reduced polling because it provides a quick way to synchronize the VNE model without having to wait for the next polling cycle.

Figure 4-13 Poll Now Button in Prime Network Device Inventory



Troubleshooting VNE Investigation State Issues: The Steps

Use this procedure to troubleshoot an unexpected VNE investigation state.

Step	Description	See:
1	Verify the current VNE investigation (and communication) states in Prime Network Vision.	Step 1: Checking the Investigation State on the VNE, page 4-58
2	Check the investigation state description in the VNE Status Details window, especially if you are seeing the Currently Unsynchronized state. You can optionally check the Service event to see if it can provide any new information.	Step 2: Check the VNE Status Details for the Cause of the Modeling Problem, page 4-61

Step	Description	See:
3	If needed, perform these additional steps depending on the information you need: • Verify that all required device configuration tasks have been performed. • Verify that there are no communication state issues. • Change Prime Network so that it generates an elaborated report about state changes. • Get more information to provide to the Cisco Technical Assistance Center.	Step 3: Performing Additional Troubleshooting Steps for Investigation State Problems, page 4-65

Note At any time you can restart the VNE discovery process by restarting the VNE (see Stopping, Starting, and Moving VNEs to Maintenance Mode, page 4-9).

Step 1: Checking the Investigation State on the VNE

Step 1 From the Prime Network Vision map view, double-click the icon in which you are interested. This opens the device properties window.

Note You can launch the device properties window from Prime Network Administration by right-clicking the VNE and choosing **Inventory**.

Step 2 Check the current Investigation State (as shown in Figure 4-14). The various states are described in Table 4-11, which follows the figure.

Figure 4-14 VNE Investigation State (in Prime Network Vision)

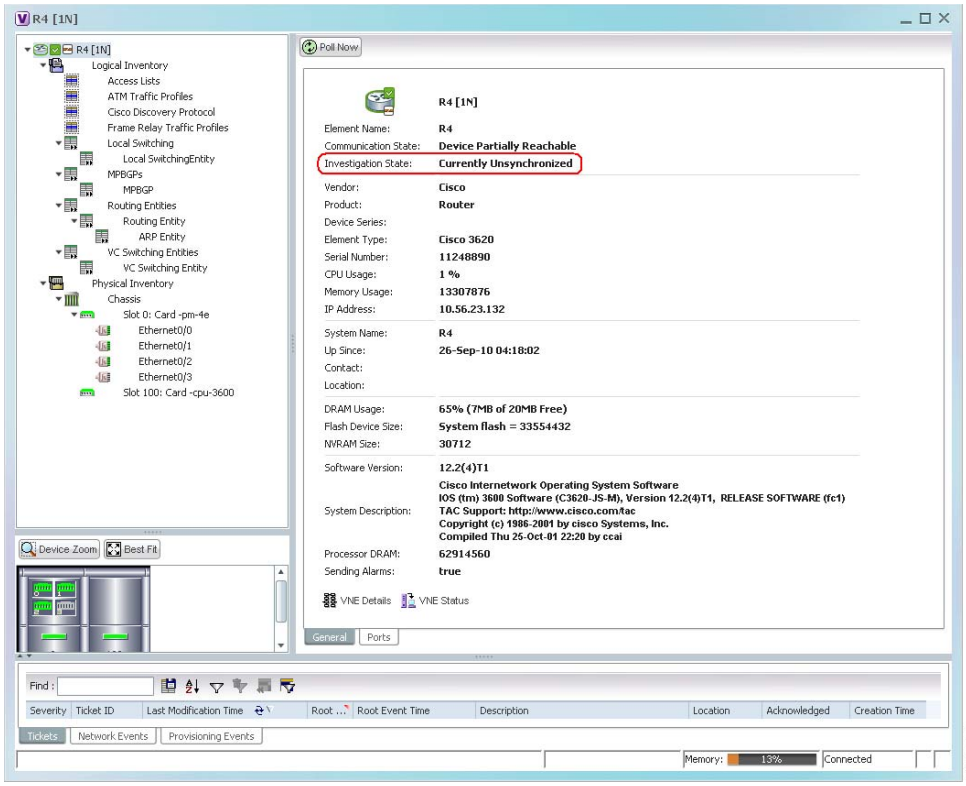


Table 4-11 VNE Investigation States

State Name	Description	Badge
Defined Not Started	A new VNE was created (and is starting); or an existing VNE was stopped. In this state, the VNE is managed and is validating support for the device type. (This investigation state is the equivalent of the Agent Not Loaded communication state.) A VNE remains in this state until it is started (or restarted). In the VNE Status Details window, the description will say **VNE is down**.	None
Unsupported	The device type is either not supported by Prime Network or is misconfigured (it is using the wrong scheme, or is using reduced polling but the device does not support it). See Table 4-12 on page 4-63 for troubleshooting steps.	
Discovering	The VNE is building the model of the device (the device type was found and is supported by Cisco Prime Network). A VNE remains in this state until all device commands are successfully executed at least once, or until there is a discovery timeout. In the VNE Status Details window, the description will say **Initial investigation of the device**. To troubleshoot a VNE that does not move out of this state, perform the following steps: 1. Verify that all required device configuration tasks have been performed. If they were not, Prime Network cannot properly model the device. See Configuring Devices, page A-1. 2. Verify that there are no communication state issues. See Troubleshooting VNE Communication State Issues: The Steps, page 4-45. Also see Troubleshooting Device Connectivity Issues (VNE Communication States), page 4-43. 3. Verify that the VNE is using the proper scheme. Refer to the *Cisco Prime Network 4.3.1 Supported Technologies and Topologies*. 4. Verify that the device is using the proper polling method. See Finding Out Whether a VNE is Using Reduced Polling, page 12-7. The default discovery timeout is 30 minutes but you can adjust it. To change the timeout, see Tracking VNE-Related Events, page 12-53.	
Operational	The VNE has a stable model of the device. Modeling may not be fully complete, but there is enough information to monitor the device and make its data available to other applications, such as transactions (activation workflows). A VNE remains in this state unless it is stopped or moved to the maintenance state, or there are device errors. In the VNE Status Details window, the description will say **Ongoing synchronization with the device.**	None
Currently Unsynchronized	The VNE model is inconsistent with the device; however, this is often recoverable, or may indicated a small inconsistency (such as a minor inventory component not being properly modeled). Because this state can be due to a variety of reasons, check the VNE Status Details window for: • Modeling information; see Table 4-12 on page 4-63. • Device connectivity information; see Table 4-10 on page 4-49.	

Table 4-11 VNE Investigation States (continued)

State Name	Description	Badge
Maintenance	VNE polling was suspended because it was manually moved to this state (by right-clicking the VNE and choosing **Actions > Maintenance**). The VNE remains in this state until it is manually restarted. A VNE in the maintenance state has the following characteristics: • It does not poll the device or process traps and syslogs. • It maintains the status of any existing links. • It responds to VNE reachability requests. • It passively participates in correlation flow issues (but is not an initiator). The VNE is moved to the Stopped state if: it is VNE is moved, the parent AVM is moved or restarted, the parent unit switches to a standby unit, or the gateway is restarted.	
Partially Discovered	The VNE model is inconsistent with the device because a required device command failed, even after repeated retries. A common cause is that the device contains an unsupported module (in which case you can extend Prime Network to recognize the module using the VNE Customization Builder; refer to the *Cisco Prime Network 4.3.1 Customization Guide*). It could also be due to a more serious issue, such as an inability to reach a configured protocol on the device.	
Shutting Down	The VNE has been stopped or deleted by the user, and the VNE is terminating its connection to the device. The VNE Status Details window, the description will say **Device synchronization aborted**.	

Step 2: Check the VNE Status Details for the Cause of the Modeling Problem

Step 1 From the VNE properties window (see Figure 4-14 on page 4-59), click **VNE Status** at the bottom of the properties window to open the VNE Status Details window and check the investigation state information, comparing it against the information in Table 4-12 on page 4-63.

Figure 4-15 Investigation State Information in VNE Status Details Window

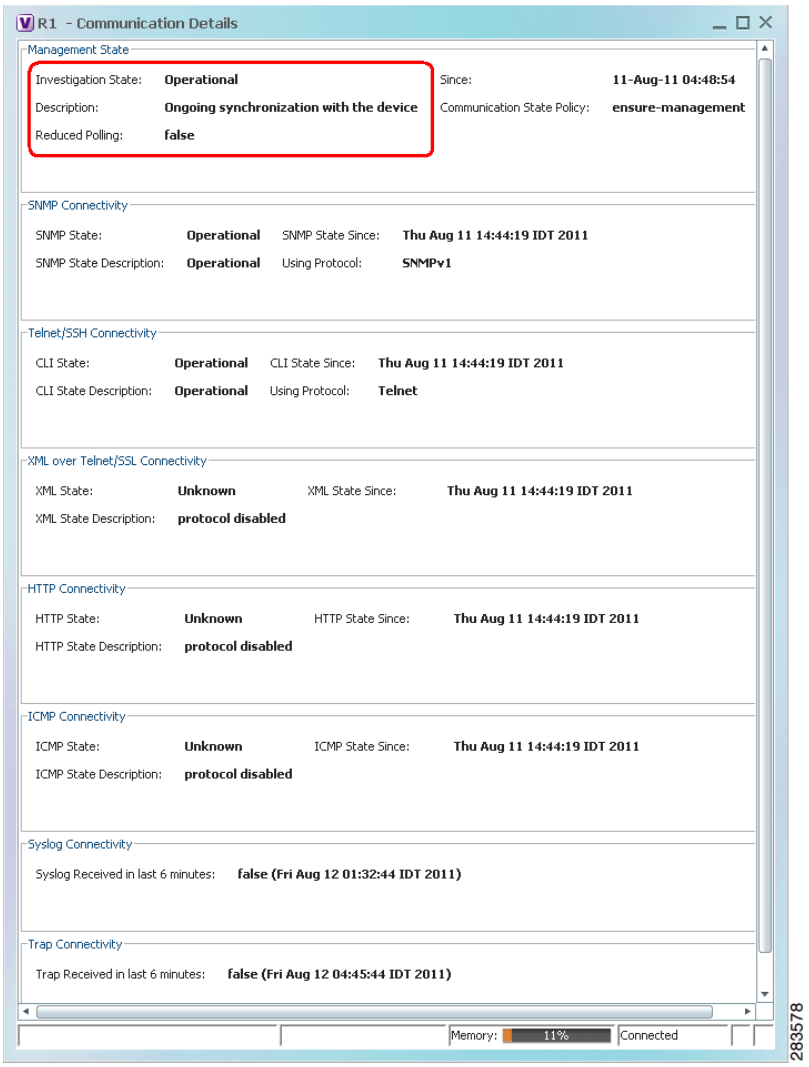


Table 4-12 VNE Investigation State Information (from VNE Status Details Window

Field	Description
Investigation State	VNE investigation state. Basic descriptions of all of the investigation states is provided in Table 4-3 on page 4-8.
Description: **Unsupported**	The device type is either not supported by Prime Network or is misconfigured (it is using the wrong scheme, or is using reduced polling but the device does not support it). T his is the probable message you will see: • **VNE cannot synchronize with the device**—The device type is not supported by Cisco Prime Network (no VNE driver was found for the device). Possible causes are: – The VNE is using the wrong scheme. Verify the device type against the supported schemes by checking the *Cisco Prime Network 4.3.1 Supported Technologies and Topologies*. – The VNE is using the reduced polling method, but the VNE does not support that method. To check whether the device type supports reduced polling, use the procedure described in Finding Out Which Device Types Support Reduced Polling, page 12-5. – Check whether the element is supported in a released device package. See Finding Out if New Device Support is Available, page 4-28. If the device type is not supported: – You can add the VNE as Generic VNE or ICMP VNE. These VNE types are specified in the VNE General properties; see General VNE Properties Reference, page D-2. – You can add the support using the Prime Network VNE Customization Builder. Refer to the *Cisco Prime Network 4.3.1 Customization Guide*.

Table 4-12 VNE Investigation State Information (from VNE Status Details Window (continued)

Field	Description
Description: **Currently Unsynchronized**	The VNE model is inconsistent with the device. This is often recoverable or may indicate a small inconsistency such as a minor inventory component not being properly modeled. These are some of the messages you may see for this state. • **User initiated device re-synchronization**—A user clicked Poll Now in Prime Network Vision (or issued a BQL command that performs this operation). • **Resuming synchronization after maintenance**—The VNE is moving out of a user-induced maintenance state and restarted the VNE. • **Device CPU is high. Synchronization temporarily suspended**—The adaptive polling mechanism moved the VNE to this state because the device exceeded its maximum CPU usage threshold. For troubleshooting tips, see Responding to High CPU Utilization Problems, page 12-2. • **Resuming synchronization after device CPU normalized**—The adaptive polling mechanism is moving the VNE back to its normal polling state because CPU usage has stabilized. • **System initiated device synchronization due to missed device configuration changes**—The VNE is using reduced polling and has identified a gap in the configuration log (specifically, the configuration archive buffer), or has failed to identify one or more changes. (VNEs using reduced polling are more sensitive to these changes due to their different polling frequency.) For more information, see Configuring Reduced (Event-Based) Polling, page 12-3. • **VNE cannot reach the device. Synchronization temporarily suspended**—The device did not respond in a timely fashion. Follow the troubleshooting steps in Troubleshooting VNE Communication State Issues: The Steps, page 4-45. • **Resuming synchronization after device reachability from VNE restored**—The VNE is moving out of an unreachable state. • **Temporarily missing or failed VNE driver component**—A required, recoverable device command failed. Prime Network retries the command at the next polling cycle, up to 3 retries. The problem normally clears upon retrying the command, but if it fails, the VNE is moved to Partially Discovered. • **Device synchronization suspended by system**—The system temporarily stopped the synchronization process because it suspects the device was reloaded (this prevents the VNE from collecting irrelevant information). The synchronization process will normally restart within 5 minutes. This investigation state can also be caused by a communication state issue. See Troubleshooting Device Connectivity Issues (VNE Communication States), page 4-43.
Description: **Partially Discovered**	The VNE model is inconsistent with the device because a required device command failed, even after repeated retries. This is the probable message you will see: • **Missing or failed VNE driver component**—Prime Network could not recognize an element in the device. Consider the following troubleshooting options: – Check whether the element is supported in a released device package. See Finding Out if New Device Support is Available, page 4-28. – To extend Cisco Prime Network functionality so that it recognizes unsupported parts of devices, use the VNE Customization Builder. Refer to the *Cisco Prime Network 4.3.1 Customization Guide*. It could also be due to an inability to reach a configured protocol on the device; see Troubleshooting Device Connectivity Issues (VNE Communication States), page 4-43.

Table 4-12 VNE Investigation State Information (from VNE Status Details Window (continued)

Field	Description
Reduced Polling	Reports whether VNE is using reduced polling mechanism to control polling (**true**=enabled). Reduced polling means polling is performed only when a poll-worthy event is received from device, thus reducing the overall polling (true if enabled, false if disabled). For information on the reduced polling mechanism, see Configuring Reduced (Event-Based) Polling, page 12-3.
Since	Timestamp of when the state information was last updated.

Step 2 Optionally, check the System event in Prime Network Events to see if it can provide additional information.

Note Keep in mind that if an AVM or unit crashes, Prime Network will not generate a Service event for the communication state change, because event-generating entity (the AVM or unit) is itself down. However, the GUI will display the VNE/Agent Unreachable icon. Any tickets related to the problem (that were sent before the crash) will remain open until the VNE restarts and generates a clearing event. If no related tickets were sent before the crash, check Prime Network Events for other related information.

Step 3: Performing Additional Troubleshooting Steps for Investigation State Problems

Step 1 Verify that all required device configuration tasks have been performed. If they were not, Prime Network cannot properly model the device. See Configuring Devices, page A-1.

Step 2 Verify that there are no communication state issues; specifically, check for a System event in Prime Network Vision. The problem may be due to the fact that the device did not respond in a timely manner.

Step 3 Optionally perform the following tasks:

- Adjust the registry setting so that Prime Network Events generates an elaborated report about state changes. See Table 4-12 on page 4-63.
- Open the device properties window in Prime Network Vision. Place your cursor in the inventory window, and press F2. Click Managed State Aspect and review the information. This information is especially useful when working with the Cisco Technical Assistance Center.

Opening a Bug Report

After performing the troubleshooting steps in the previous sections, if you still have a problem, you may consider opening a bug (or enhancement request).

Before You Open a Bug

1. Verify that the network element, event, etc. is supported by checking these documents:
   - The lists of supported VNEs and events on Cisco.com
   - *Cisco Prime Network 4.3.1 Supported Cisco VNEs—Addendum* (this document is released when the first DP becomes available; see Adding New Device Support with Device Packages, page 4-27.

Note If the device is not supported, you can add the support using the Prime Network VNE Customization Builder. Refer to the *Cisco Prime Network 4.3.1 Customization Guide*. Also, this guide contains an extended procedure for finding out which traps and syslogs are not supported and how to troubleshoot them.

2. Make sure you have tried all of the troubleshooting steps provided in these topics:
   - Troubleshooting Device Connectivity Issues (VNE Communication States), page 4-43
   - Troubleshooting VNE Communication State Issues: The Steps, page 4-45
   - Troubleshooting Device Modeling Issues (VNE Investigation States), page 4-56
3. Provide all of the necessary details for the bug report (reproduce the problem if necessary).

Information You Must Provide

1. Describe the actual behavior versus the expected behavior. For example, “Module serial numbers are missing from Vision.”
2. Describe how to recreate the error scenario.
3. Provide the following device details:
   - Device type.
   - Device operating system (including service and patches applied on the NE).
   - Device configuration information. If possible, attach a running config.
   - For device physical modeling issues, details on the physical module.
   - For device logical modeling issues, details on the service.
4. Collect the following Prime Network information:
   - Pertinent AVM log files from *NETWORKHOME*/Main/logs.
   - List of VNE drivers that are installed.
   - Prime Network version. From the gateway, run **networkctl status** and note the version and build number that are displayed at the top of the status message.
   - Patch level details. You can use this command:

     checkPatchInstallation.pl -v -p

5. For physical model issues, provide screen captures (of the Prime Network GUI clients and the EMS) that show the discrepancies.
6. For NBI-related issues, provide the IMO or BQL citation.

Track VNE-Related Events

When you audit VNE behavior, you are checking the backend process that models and monitors a device in the network. The following table provides ways you can get historical information on VNE-related events. You can tailor your search or reports by specifying keywords (such as *VNE*).

For historical events related to:	See:
Adding/deleting, starting/stopping, editing and moving VNEs	AVM and other appropriate log files (see Log Files Reference, page C-3)
Modeling (investigation state) changes Reachability (communication state) problems Device Package-related VNE Changes	The following reports, which you can launch from the main menu by choosing **Reports > Run Report > Events Reports** >: • Detailed System Events • Detailed Security Events • Detailed Service Events