CHAPTER 19

VNE Administration: VNE Lifecycle and Creating VNEs

These topics provide information about advanced VNE administration tasks:

Additional VNE administration tasks are described in:

- Basic AVM and VNE Administration Tasks, page 4-1
- Troubleshooting VNE Modeling, page 20-1
- VNE Updates, page 21-1

What Are VNE Communication and Investigation States?

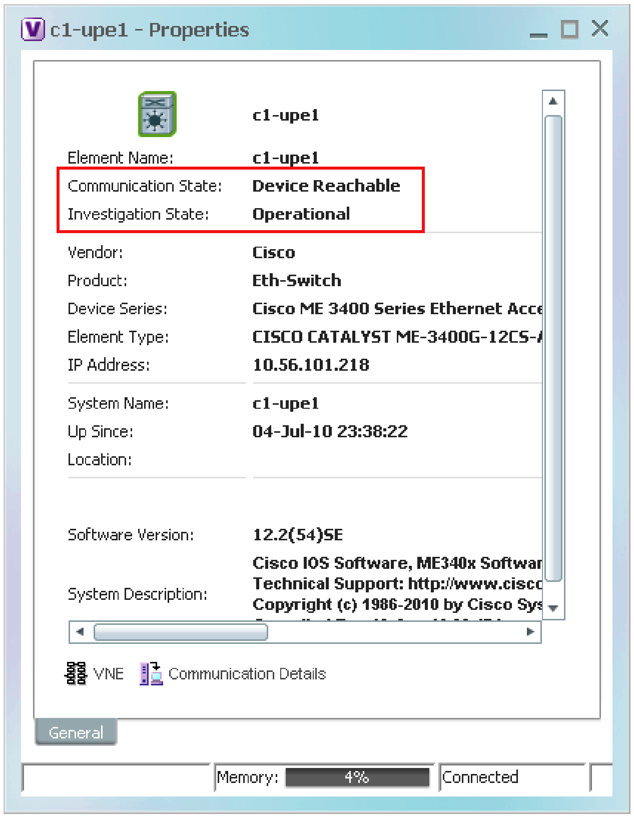
VNE states describe to what degree the VNE has discovered and modeled a device, and the disposition of the communication between the VNE and the device it models. This information is very granular and can help you pinpoint why a device is not completely modeled or why it is unreachable.

There are two types of VNE states:

- VNE *communication* states convey the status of communication between devices and VNEs, and VNEs and the gateway server. The states and their GUI decorators are listed in VNE Communication States, page 19-3. Prime Network generates a Service event whenever a VNE's communication state changes.
- VNE *investigation* states represent the different degrees 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. These states and their GUI decorators are listed in VNE Investigation States, page 19-4. 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; see Registry Settings for VNE Discovery Timeout and Investigation State Reporting, page 20-23).

Both the communication and investigation states are displayed in text format in Prime Network Vision when you open a device properties window, as shown in Figure 19-1.

Figure 19-1 VNE Communication and Investigation States (in Prime Network Vision)



c1-upe1 - Properties

c1-upe1

Element Name: c1-upe1
Communication State: Device Reachable
Investigation State: Operational

Vendor: Cisco
Product: Eth-Switch
Device Series: Cisco ME 3400 Series Ethernet Acce
Element Type: CISCO CATALYST ME-3400G-12CS-/
IP Address: 10.56.101.218

System Name: c1-upe1
Up Since: 04-Jul-10 23:38:22
Location:

Software Version: 12.2(54)SE
System Description: Cisco IOS Software, ME340x Softwar
Technical Support: http://www.ciscc
Copyright (c) 1986-2010 by Cisco Sys

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 Changing VNE Status and Lifecycle (Start, Stop, Maintenance), page 19-38.

If you want more information about the communication state, click **VNE Status** 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 VNE Communication States, page 19-3.

VNE Communication States

VNE *communication* states convey the status of two types of connections, both of which are needed for Prime Network to successfully manage a device:

- Communication status between the VNE and the device it is monitoring (*management* issues).
- Communication status between the VNE and the gateway (*agent* issues).

Management communication—between a VNE and a device—is where problems normally occur. Devices and VNEs communicate using SNMP, Telnet, ICMP and notification protocols such as traps and syslogs—all of which determine whether a device is truly reachable. Prime Network runs tests tailored to each (enabled) protocol to determine the seriousness of a reachability problem. By default, Prime Network does not mark a device as Device Unreachable unless *all* of the enabled device management protocols are unresponsive, and the device is not generating syslogs or traps. You can adjust the settings that control when a device is considered unreachable. For information on how to do this, and details about how Prime Network determines reachability for different protocols, see How Prime Network Determines Protocol Reachability, page 24-3.

When a VNE's communication state changes, Prime Network generates a Service event which you can view in Prime Network Events and Vision. An event is generated for newly-started VNEs only when 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 to see if there is a genuine problem with the device. For example, a Device Unreachable event could signal a device protocol problem, or it may indicate that a VNE was shutdown as part of normal maintenance.

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 (see Table 19-1). 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.

Table 19-1 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 Steps to Troubleshoot VNE Communication State Issues, page 20-3.

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 Unmanaged Segments and Cloud VNEs, page 23-1).

Table 19-1 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.)	▨

Table 19-1 VNE Communication States (continued)

State Name	Description	Badge
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 VNE Management Communication Policies and How To Change Them, page 24-1.	▣
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 VNE Management Communication Policies and How To Change Them, page 24-1.	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 VNE Management Communication Policies and How To Change Them, page 24-1.	▣
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 Customizing Protocol Reachability Testing, page 24-7). 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 VNE Communication State Issues, page 20-1.	None

VNE Investigation States

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 modelling, until the VNE is stopped. Table 19-2 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 Changing VNE Status and Lifecycle (Start, Stop, Maintenance), page 19-38). 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 VNE Modeling, page 20-1.

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 Unmanaged Segments and Cloud VNEs, page 23-1).

Table 19-2 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).	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. See the *Cisco Prime Network 3.8 Customization User 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 activation scripts. 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. This can be due to a variety of reasons; for a list of these reasons along with troubleshooting tips, see Troubleshooting VNE Investigation State (Discovery) Issues, page 20-14.	⇆
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: • Does not poll the device, but handles syslogs and traps. • Maintains the status of any existing links. • Does not fail on VNE reachability requests. • Handles events for correlation flow issues. It does not initiate new service alarms, but does receive events from adjacent VNEs, such as in the case of a Link Down alarm. 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 of this state is that the device contains an unsupported module. To extend Cisco Prime Network functionality so that it recognizes unsupported modules, use the VNE Customization Builder. See the *Cisco Prime Network 3.8 Customization User Guide*.	⊘
Shutting Down	The VNE has been stopped or deleted by the user, and the VNE is terminating its connection to the device.	⏻
Stopped	The VNE process has terminated; it will immediately move to Defined Not Started.	None

Choosing a VNE Scheme

VNE schemes determine what data should be retrieved for each device, along with the commands and protocols Prime Network should use to collect that data. The scheme settings are arranged in an inheritance tree and incorporated into the configuration registry to support default values at any level—and the option to inherit or override default settings—on the basis of device vendor, type, model, version etc. The scheme settings can be changed at a very granular level, such as specific device instances or specific aspects of inventory within devices. For example, different polling frequencies can be set for different port types within a device.

If you chose the wrong scheme when you created the VNE, you will have to delete and recreate the VNE.

Note You can also supplement what is modeled by creating new soft properties. These allows you to model additional attributes and create new threshold crossing alarms. For more information on the Soft Properties Manager, see the *Cisco Prime Network 3.8 Customization User Guide*.

When creating a VNE, choose a scheme that is based on the device family and on the technologies you want Prime Network to manage. This enables you to define different behavior for different devices. For example, some devices poll only with SNMP, while other devices poll with Telnet. Soft properties and activation scripts are also attached to a specific scheme.

Note When you create a VNE, Prime Network provides a drop-down list of available schemes. The list includes a “default” choice. If you choose default, Prime Network sets the scheme to Product.

Prime Network uses the following schemes:

- Product—This scheme is used for all device types in this release, except for Cisco CRS and Cisco 3750ME devices.
- IpCore—This scheme is used only for routers serving as Provider (P) or Provider Edge (PE) devices.

The difference between the two schemes is that IpCore assumes that the device is used as part of an MPLS VPN network containing P and PE devices. Prime Network therefore models these VNEs slightly differently. Use Product for all other instances, including customer edge (CE) devices. The Product scheme assumes that no MPLS or VRF configuration exists and thus does not retrieve it.

These schemes provide users with the flexibility to specify the registrations (device commands, or methods the VNE uses to query the device for information) that the VNEs modeling their routers are to use. 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.

Table 19-3 identifies the technologies supported by each scheme.

Table 19-3 Technology Support Based on Schemes

	Scheme	
Technology	Product	IpCore
ACL	Yes	Yes
ATM	Yes	Yes
6PE and 6VPE-based IPv6 Connectivity	Yes	Yes
6RD	Yes	Yes

Table 19-3 Technology Support Based on Schemes (continued)

	Scheme	
Technology	**Product**	**IpCore**
ATM PW	No	Yes
Backup Pseudowire	No	Yes
BFD	Yes	Yes
BGP	Yes	Yes
Carrier Supporting Carrier (CSC)	No	Yes
CDP	Yes	Yes
CEM Group	Yes	Yes
CFM	Yes	Yes
CGN	No	Yes
Clocking Enhancements	No	Yes
DSx	Yes	Yes
EFP	No	Yes
Ethernet	Yes	Yes
Ethernet Channel	Yes	Yes
Ethernet IEEE 802.3 Dot1Q/VLAN	Yes	Yes
Ethernet LMI	Yes	Yes
Ethernet OAM	Yes	Yes
Frame Relay	Yes	Yes
GRE	Yes	Yes
HDLC	Yes	Yes
Hierarchical VPLS	No	Yes
IMA	Yes	Yes
IP Routing	Yes	Yes
IP and ARP	Yes	Yes
IPoDWDM	No	Yes
IPSLA Responder	Yes	No
IPv6	Yes	Yes
IRB/BVI	Yes	Yes
ISIS	No	Yes
ISIS IGPv6	No	Yes
L3 VPN and VRF	No	Yes
LAG (IEEE 802.3ad)	Yes	Yes
LLDP	Yes	Yes
Local Switching	Yes	Yes
MLACP	Yes	Yes

Table 19-3 Technology Support Based on Schemes (continued)

	Scheme	
Technology	**Product**	**IpCore**
MLPPP	Yes	Yes
MP-BGP	No	Yes
MPLS	No	Yes
MPLS P2MP TE	No	Yes
MPLS TE-Tunnel (including FRR)	No	Yes
MPLS TP	No	Yes
MST-AG/REP-AG	Yes	Yes
OSPF	Yes	Yes
POS	Yes	Yes
PPP	Yes	Yes
PTP 1588	Yes	Yes
PWE3, L2 VPN (Martini)	No	Yes
PW VCCV	No	Yes
Q-in-Q (IEEE 802.1ad)	Yes	Yes
REP	Yes	Yes
SBC	No	Yes
SL-XLAT	No	Yes
SONET/SDH	Yes	Yes
STP/MSTP/PVST	Yes	Yes
SVI	No	Yes
SynCE	Yes	Yes
TDM	Yes	Yes
TDM PW	No	Yes
VC Switching	Yes	Yes
VLAN Bridging	Yes	Yes
VPLS	No	Yes
VRRP	No	Yes
VTP (VLAN Trunk and Tunneling)	Yes	Yes

Table 19-4 identifies the schemes that are supported by device type.

Table 19-4 Schemes Used by Device Type

Device Types	Scheme	
	Product	**IpCore**
Security Appliances		
Cisco Adaptive Security Appliance 5550 Series	X	—
Application Networking Appliances		
Cisco ACE 4700 Series Application Control Engine Appliances	X	—
Gateways		
Cisco AS5300 Series Universal Gateways	X	—
Routers		
Cisco 800 Series Routers	X	—
Cisco 1000 Series Routers	X	—
Cisco 1600 Series Routers	X	—
Cisco 1700 Series Modular Access Routers	X	—
Cisco 1800 Series Integrated Services Routers	X	—
Cisco 2500 Series Routers	X	—
Cisco 2600 Series Multiservice Platform Routers	X	—
Cisco 2800 Series Integrated Services Routers	X	—
Cisco 2900 Series Integrated Services Routers	X	—
Cisco 3600 Series Multiservice Platform Routers	X	X
Cisco 3700 Series Multiservice Access Routers	X	X
Cisco 3800 Series Integrated Services Routers	X	X
Cisco 4700 Series Routers	X	X
Cisco 7200 Series Routers	X	X
Cisco 7300 Series Routers	X	X
Cisco 7400 Series Routers	X	X
Cisco 7500 Series Routers	X	X
Cisco 7600 Series Routers	X	X
Cisco 10000 Series Routers	X	X
Cisco 12000 Series Routers	X	X
Cisco XR 12000 Series Routers	X[1]	X
Cisco CRS Carrier Routing System (CRS-1 and CRS-3)	—	X
Cisco ASR 1000 Series Routers	X	X
Cisco ASR 9000 Series Aggregation Services Routers	X	X
Cisco MWR 2900 Series Mobile Wireless Routers	X	X

Table 19-4 Schemes Used by Device Type (continued)

Device Types	Scheme	
	Product	IpCore
Switches		
Cisco Catalyst 2900 Series Switches	X	—
Cisco ME 3400 Series Ethernet Access Switches	X	—
Cisco Catalyst 3500 XL Series Switches	X	—
Cisco Catalyst 3550 Series Switches	X	—
Cisco Catalyst 3560 Series Switches	X	—
Cisco ME 3600X Series Ethernet Access Switches	X	X
Cisco Catalyst 3750 Series Switches	X	—
Cisco Catalyst 3750 Metro Series Switches	—	X
Cisco ME 3800X Series Carrier Ethernet Switch Routers	X	X
Cisco Catalyst 4000 Series Switches	X	—
Cisco Catalyst 4500 Series Switches	X	—
Cisco Catalyst 4900 Series Switches	X	—
Cisco ME 4900 Series Ethernet Switch	X	—
Cisco Nexus 5000 Series Switches	X	—
Cisco Catalyst 6500 Series (CatOS) Switches	X	X
Cisco Catalyst 6500 Series (Cisco IOS) Switches	X	X
Cisco ME 6500 Series Ethernet Switches (6524)	X	X
Cisco Nexus 7000 Series Switches	X	—
Cisco SCE 2000 Series Service Control Engine	X	—
Optical Networking		
Cisco Carrier Packet Transport (CPT) 50	X	—
Cisco Carrier Packet Transport (CPT) 500	X	—
Cisco Carrier Packet Transport (CPT) 600	X	—
Unified Computing and Servers		
Cisco Unified Computing System	X	—
Generic Devices		
Generic devices	X	—

[1] The product scheme is supported Cisco XR 12000 Gigabit Switch Routers.

Adding VNEs

You can add VNEs manually if desired, but Prime Network provides a variety of VNE auto-add features that will distribute VNEs between units and AVMs. The auto-add feature calculates in advance the predicated memory consumption of a VNE based on its role and type, and balances AVM memory as the VNEs are added. You can also monitor the VNEs as the auto-add feature creates them and distributes them across the system.

Methods for Adding VNEs

Prime Network can choose the best unit and AVM for a VNE. The general rule is that if you want Prime Network to decide where the VNE should go, start from the All Servers branch (that is, right-click **All Servers** and choose the operation).

Table 19-5 briefly describes the various methods and scenarios for which they are suitable. You can use a combination of methods at the same time. 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 19-5 Methods for Adding VNEs to Prime Network

Action	For instructions, see:
Clone an existing VNE	Cloning VNEs, page 19-14
Create a CSV file of properties and then use it to create VNEs	Creating VNEs Using a CSV File, page 19-17
Create a VNE "from scratch" by going through all of the properties	Creating VNEs for New Device Types, page 19-21

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 decide you want to choose your own AVM, you can still do that using auto-add because all available units and AVMs are displayed in a drop-down list. If you want the VNEs on a specific unit, right-click the unit to perform the operation, and Prime Network will choose the appropriate AVM. Prime Network does this by finding *safe target AVMs*. A safe target AVM has the following characteristics:

- All of its VNEs are modeled (the discovery process is not running).
- Its available memory is below the AVM Memory Warning Threshold (specified in **Global Settings > Automatic AVM Management**).
- It is not experiencing any memory consumption problems.

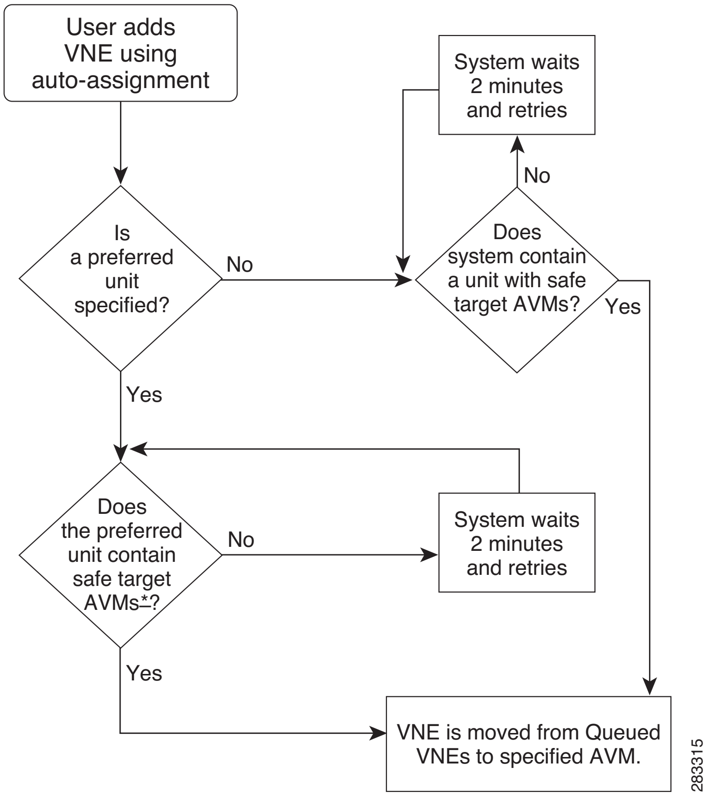
When you finish defining the VNE properties, the VNEs are listed in the **Queued VNEs** tab (under **All Servers**). As the VNEs are assigned to AVMs, they disappear from that tab.

If Prime Network cannot locate an appropriate AVM is not identified, it waits 2 minutes, and attempts to find a suitable AVM 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 19-2 illustrates the VNE auto-add process.

Figure 19-2 VNE Auto-Add


User adds VNE using auto-assignment
Is a preferred unit specified?
No
Yes
Does system contain a unit with safe target AVMs?
No
Yes
System waits 2 minutes and retries
Does the preferred unit contain safe target AVMs*?
No
Yes
System waits 2 minutes and retries
VNE is moved from Queued VNEs to specified AVM.
283315

Before You Create VNEs

The following table provides a list of steps you should perform before adding a VNE.

Note For troubleshooting help, see Troubleshooting VNE Modeling, page 20-1 and Device Reachability, page 24-1.

1. Choose a VNE scheme. See Choosing a VNE Scheme, page 19-6.
2. Gather all prerequisite information:

IP address	Device management IP address
Name	Device name
SNMP	• Supported version (v1, v2, or v3). • For SNMPv1 or v2: The SNMP read and write community strings. • For SNMPv3: The username and, optionally, the authentication or privacy configuration.

Telnet	• Port number. • Telnet login sequence: Username, password, and prompt. **Note** The Telnet login sequence is required for Cisco IOS, Cisco IOS XE, and Cisco IOS XR devices.
SSH	• Supported version (v1 or v2). • SSH username and password and any other configuration information (cipher, authentication, key exchange [v2], MAC [v2]). **Note** 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 All Cisco Devices Added Using SSH—Required, Recommended, and Rollback Device Settings, page A-5
XML	• Protocol used for XML (Telnet or SSL). • Protocol port number. • Protocol login sequence.
HTTP	**Note** These settings are not used by VNEs provided with the initial release of Prime Network 3.8. Future Device Packages will introduce new device support for devices that will use this feature. • Version (HTTP or HTTPS). • Port number. • HTTP URL used to connect to the device. • Authentication credentials, if needed.

3. Perform all mandatory configurations on the network element so that it can be properly modeled and managed by Prime Network.

For these settings:	See:
Cisco IOS, Cisco IOS XE, and CatOS devices	Cisco IOS, Cisco IOS XE, and CatOS Devices—Required Settings, page A-2
Cisco IOS XR devices	Cisco IOS XR Devices—Required and Recommended Settings, page A-3
Devices you will add using SSH	All Cisco Devices Added Using SSH—Required, Recommended, and Rollback Device Settings, page A-5
SNMP traps setup	SNMP Traps and Informs—Required Device Settings, page A-5
Syslogs setup	Syslogs—Required Device Settings, page A-10
For configurations where the traps and syslogs source IP address is *different* from the VNE IP address	IP Address Configuration for Traps, Syslogs, and VNEs, page A-11
Nexus OS devices:	VDC Configuration for Nexus OS, page A-11

4. (Optional) Get deployment information and recommendations, such as best practices for assigning VNEs to AVMs by contacting your Cisco representative.

Cloning VNEs

A clone VNE inherits all of the properties of an 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 necessary tasks that are described in Before You Create VNEs, page 19-12. 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:

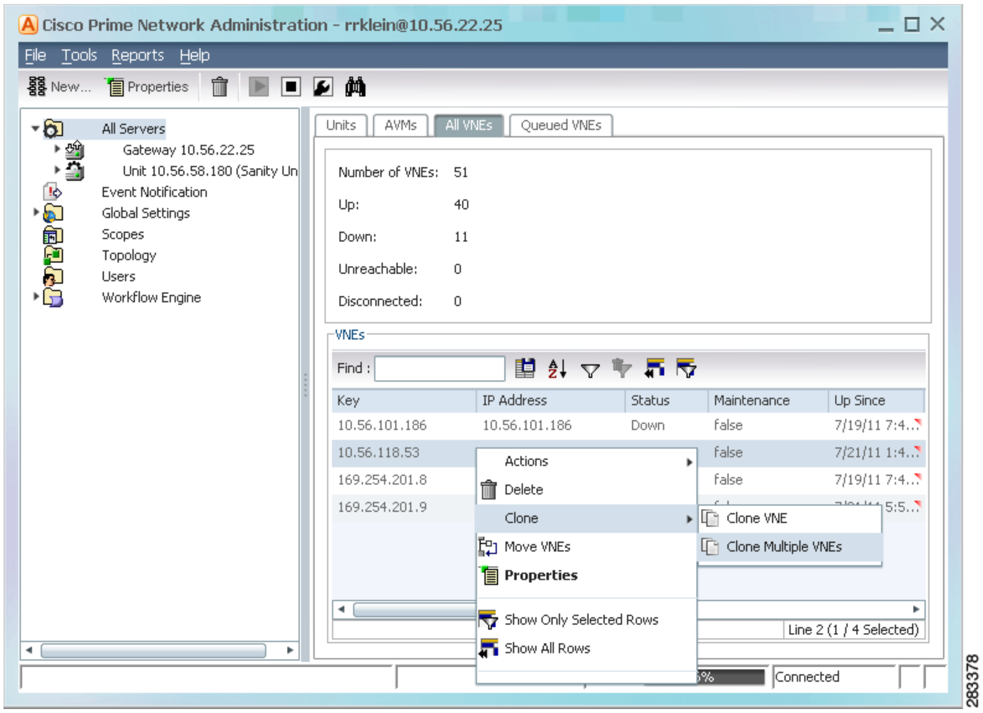
To create VNEs where:	Start the clone operation from this point in the GUI client:
Prime Network chooses the unit and AVM	From **All Servers** in the navigation area, click **All VNEs** tab.
Prime Network chooses the AVM but you choose the unit	From desired unit in the navigation area, click **Unit's 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 19-3, the user is creating several clone VNEs based on the VNE with the key 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 19-3 Creating a Clone VNE Using Auto-Add—Selecting the VNE



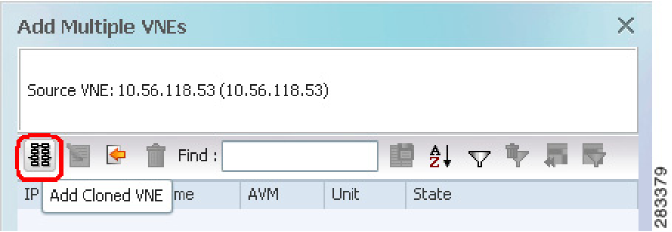
Number of VNEs: 51
Up: 40
Down: 11
Unreachable: 0
Disconnected: 0

Key	IP Address	Status	Maintenance	Up Since
10.56.101.186	10.56.101.186	Down	false	7/19/11 7:4...
10.56.118.53			false	7/21/11 1:4...
169.254.201.8			false	7/19/11 7:4...
169.254.201.9				5:5...

Step 4 Create the clone VNE(s).

a. In the Add VNEs from Clone dialog box, click the Add Cloned VNE icon (see Figure 19-4).

Figure 19-4 Creating a Clone VNE Using Auto-Add—Creating the Clones



Source VNE: 10.56.118.53 (10.56.118.53)

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.

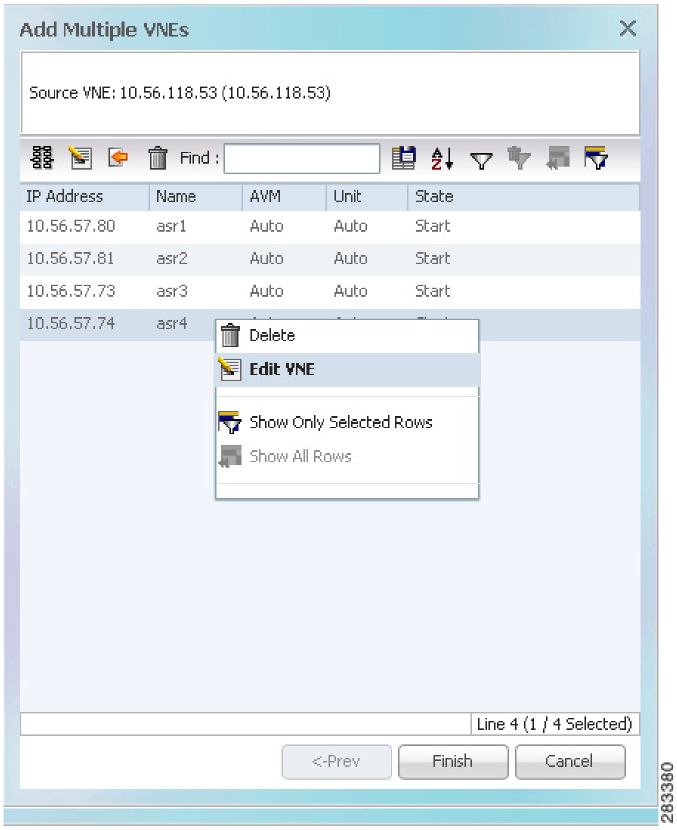
b. Enter the new VNE name and IP address. When finished, click **OK**.

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 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 select **Edit VNE** (see Figure 19-5). If you want, you can specify the unit and AVM you want the VNE to use.

Figure 19-5 Creating a Clone VNE Using Auto-Add—Viewing and Editing the Clones



Source VNE: 10.56.118.53 (10.56.118.53)

IP Address	Name	AVM	Unit	State
10.56.57.80	asr1	Auto	Auto	Start
10.56.57.81	asr2	Auto	Auto	Start
10.56.57.73	asr3	Auto	Auto	Start
10.56.57.74	asr4			

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

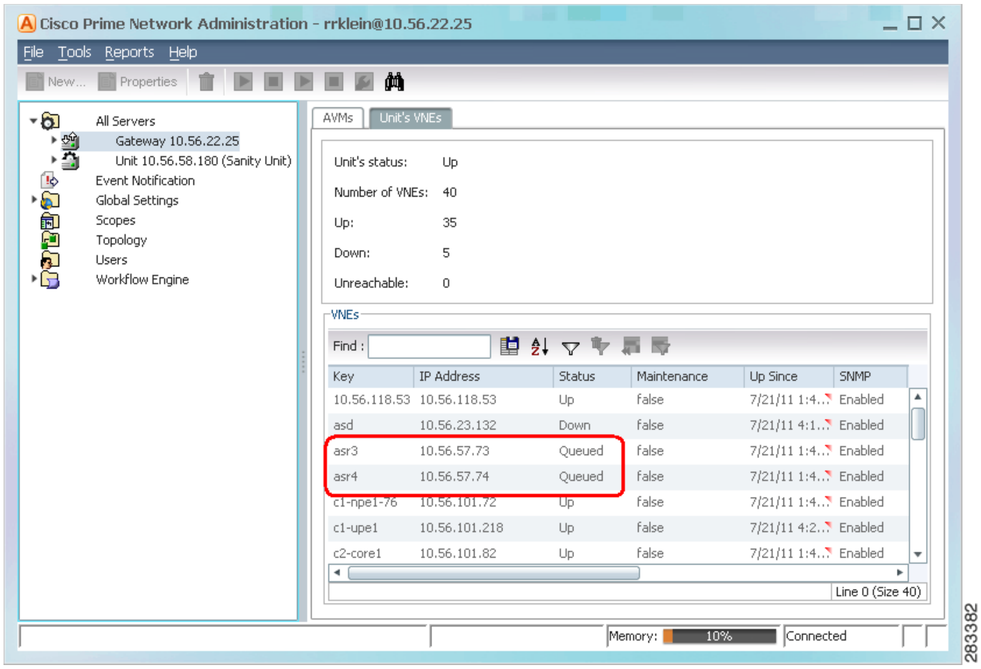
a. For auto-added VNEs (the unit or AVM was selected by Prime Network), select **All Servers** branch and click the **Queued VNEs** tab. If it is empty, the VNEs have been assigned.

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 19-6 shows two new VNEs that were added to the gateway but are using AVM auto-assignment. Their assignment is pending.

Figure 19-6 Creating a Clone VNE Using Auto-Add—Checking the Assignment



Unit's status: Up

Number of VNEs: 40

Up: 35

Down: 5

Unreachable: 0

Key	IP Address	Status	Maintenance	Up Since	SNMP
10.56.118.53	10.56.118.53	Up	false	7/21/11 1:4...	Enabled
asd	10.56.23.132	Down	false	7/21/11 4:1...	Enabled
asr3	10.56.57.73	Queued	false	7/21/11 1:4...	Enabled
asr4	10.56.57.74	Queued	false	7/21/11 1:4...	Enabled
c1-npe1-76	10.56.101.72	Up	false	7/21/11 1:4...	Enabled
c1-upe1	10.56.101.218	Up	false	7/21/11 4:2...	Enabled
c2-core1	10.56.101.82	Up	false	7/21/11 1:4...	Enabled

Line 0 (Size 40)

Memory: 10% Connected

Prime Network starts investigating the network element and builds a live model of the network element, including its physical and logical inventory, its configuration, and its status. Prime Network also creates the registry information of the new VNE in the unit. After a few minutes, verify that the VNE status is Up.

Creating VNEs 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 customizations using a spreadsheet template. Prime Network will choose the unit and AVMs for the VNEs. 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 19-6.

Format of a CSV File

The CSV file supports all of the entry names listed in Table 19-6. 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,TelnetSe
quence,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,unitIP,ICMPPollingRate,ICMPEnabled,PollingGroup,TrapSyslogSources,TelnetSe
quence,telnetEnabled
m1,1.1.1.1,TRUE,1,0,ipcore ,,,50000000,TRUE,slow,,">,prompt,#,",TRUE
m2,1.1.1.2,TRUE,2,1,product,,,856000,FALSE,default,,#,TRUE
```

```
m3,1.1.1.3 ,TRUE,2,1,,,,,TRUE,,"129.5.6.2,55.23.6.5,9.5.2.1",">,text,#,",FALSE
m4,1.1.1.4,TRUE,1,0,,,,,FALSE,,121.2.3.4,,TRUE
m5,1.1.1.5,TRUE ,1,0, ipcore ,,,5600000,FALSE ,slow,121.2.3.4,">,admin,#,",FALSE
```

Table 19-6 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**	product
adminStatusEnum	**0**=Disabled (do not start VNE), **1**=Enabled (start VNE)	1 (start VNE)[2]
avm	*avm ID*	(null) (Use auto-add)
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)

Table 19-6 Supported Values for CSV File (Creating VNEs) (continued)

CSV Entry	Supported Values	Default Setting and Notes
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)
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)
TL1PortNumber	*port-number*	(null)
ClientAuthEnum	**0**=password, **1**=public	0 (password)
ClientPrivateKey	*string*	(null)

Table 19-6 Supported Values for CSV File (Creating VNEs) (continued)

CSV Entry	Supported Values	Default Setting and Notes
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)
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 3.8. Future Device Packages will introduce new device support for devices that will use this feature.

Before You Begin

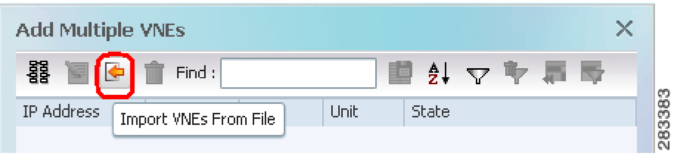
Make sure you have performed any necessary tasks that are described in Before You Create VNEs, page 19-12. This will ensure that the VNE is properly modeled and updated.

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 19-7.

Figure 19-7 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 select **Edit VNE** (see Figure 19-5).

Note You can still add individual VNEs using the Clone VNE icon shown in Figure 19-4 on page 19-15.

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.

Prime Network starts investigating the network element and builds a live model of the network element, including its physical and logical inventory, its configuration, and its status. Prime Network also creates the registry information of the new VNE in the unit. After a few minutes, verify that the VNE status is Up.

Creating VNEs for New Device Types

When you create a VNE for a new device type, you should create a single VNE and test it to ensure its settings are correct, and then clone it.

Before You Begin

Make sure you have performed any necessary tasks that are described in Before You Create VNEs, page 19-12. 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.

VNE Tab	Description	Described in:
General	Enter general information such as VNE name, IP address, scheme, and VNE driver file and version being used by the VNE. The VNE name and IP address are mandatory (Cloud VNEs do not require an IP address). **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.	VNE General Settings, page 19-24
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.	VNE SNMP Settings, page 19-26
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.	VNE Telnet/SSH Settings, page 19-27
XML	Enables XML for device reachability and investigation.	VNE XML Settings, page 19-33
HTTP	Enables HTTP. **Note** These settings are not used by VNEs provided with the initial release of Prime Network 3.8. Future Device Packages will introduce new device support for devices that will use this feature.	VNE HTTP Settings, page 19-34
ICMP	Enables ICMP and the ICMP polling rate (in seconds) for device reachability testing.	VNE ICMP Settings, page 19-34
Polling	Associates a VNE with a previously created polling group or allows you to customize different polling settings according to the type of VNE information you want (status, configuration, and so forth); and lets you specify VNE adaptive polling.	VNE Polling Settings, page 19-34
Events	Specifies other IP addresses on which the VNE should listen for syslogs and traps. (This is useful when devices have components using IP addresses that are different from the management IP address, especially if the device driver cannot automatically detect these additional addresses.)	VNE Events Settings, page 19-36

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.

Prime Network starts investigating the network element and builds a live model of the network element, including its physical and logical inventory, its configuration, and its status. Prime Network also creates the registry information of the new VNE in the unit. After a few minutes, verify that the VNE status is Up.

Viewing and Editing VNE Properties

Prime Network Administration enables you to view and edit the properties of a VNE in a unit, such as the status or Telnet settings. You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

Note For troubleshooting help, see Troubleshooting VNE Modeling, page 20-1 and Device Reachability, page 24-1.

To view the properties of a VNE:

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

Step 2 Open the VNE Properties dialog box by right-clicking the required VNE in the VNE Properties table, then choose **Properties**.

VNE Tab	Description	Described in:
General	Contains general information such as VNE name, IP address, scheme, and VNE driver file and version being used by the VNE.	VNE General Settings, page 19-24
SNMP	Specifies SNMP settings to support polling and device reachability.	VNE SNMP Settings, page 19-26
Telnet/SSH	Enables Telnet and SSH for device reachability and investigation.	VNE Telnet/SSH Settings, page 19-27
XML	Enables XML for device reachability and investigation.	VNE XML Settings, page 19-33
HTTP	Enables HTTP. **Note** These settings are not used by VNEs provided with the initial release of Prime Network 3.8. Future Device Packages will introduce new device support for devices that will use this feature.	VNE HTTP Settings, page 19-34
ICMP	Enables ICMP and the ICMP polling rate for device reachability testing.	VNE ICMP Settings, page 19-34
Polling	Associates a VNE with a previously created polling group or allows you to customize different polling settings according to the type of VNE information you want (status, configuration, and so forth); and lets you specify VNE adaptive polling.	VNE Polling Settings, page 19-34
Events	Specifies other IP addresses on which the VNE should listen for syslogs and traps.	VNE Events Settings, page 19-36

To edit VNE properties, see Editing VNE Properties, page 19-37.

VNE General Settings

To view a VNE's General properties, right-click the VNE in the Servers drawer and select **Properties**. By default it opens to the General tab. Table 19-7 describes the fields in the VNE General properties dialog box.

Table 19-7 Fields in the VNE General Tab

Field	Description
Identification Area	
Name	Name of the VNE, which will be used as a unique key in Prime Network. It is also used for commands that manipulate the VNE. **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. You cannot change a VNE name once you have created the VNE. To change the name you must delete and add a new VNE.
IP Address	Device management IP address of the network element.
Type	Defines the protocol Prime Network will use to model the element, and the extent to which you want the element to be modeled. In the drop-down list, choose the VNE device type: • Auto Detect—Use this type if SNMP is enabled on the element. Prime Network will use SNMP to gather all available inventory information. • Generic SNMP—Use this type if SNMP is enabled on the element, and either Prime Network does not support the element, or Prime Network does support the element but you only want basic information to be modeled. Prime Network will use SNMP to gather the most basic inventory information that is normally provided by all network elements. See Notes on Generic SNMP VNEs, page 19-25. • Cloud—Use this type for an unmanaged network segment. Specific Cloud configuration is provided on a per-project basis. All other tabs will be disabled. • ICMP—Use this type if ICMP is enabled on the element, and either Prime Network does not support the element, or Prime Network does support the element but you only want basic information to be modeled. Prime Network will use ICMP to gather the most basic inventory information that is normally provided by all network elements, and will perform reachability testing only. The Polling tab (which controls polling group settings) will be disabled.

Table 19-7 Fields in the VNE General Tab (continued)

Field	Description
Scheme	Defines the VNE modeling components investigated during the discovery process and then populated in the VNE model. This enables the administrator to define different behavior for some network elements; for example, some network elements poll only with SNMP, and other network elements poll with Telnet. Soft properties and activation scripts are also attached to a specific scheme. By default, the VNE inherits the VNE scheme from the default scheme. Where more than one scheme exists in the network, the VNE loads the selected scheme. • Default—Sets the scheme to Product. • Product—This scheme is used for all device types in this release, except for Cisco CRS and Cisco 3750ME devices. • IpCore—This scheme is used only for routers serving as Provider (P) or Provider Edge (PE) devices. For more information, see Choosing a VNE Scheme, page 19-6.
Initial State Area	
State	Sets the initial disposition of the VNE. Normally you should set it to Stop, especially if you want to verify the VNE configuration, or if you know the VNE is very complex and might need extra processing to complete the loading procedure. **Note** If you use auto-add, the VNE will automatically be started. • Stop—The VNE is not loaded. This is the default state. • Start—The VNE is loaded and starts collecting data. To move an existing VNE to the maintenance state, see Changing VNE Status and Lifecycle (Start, Stop, Maintenance), page 19-38.
Location and VNE Driver Details	
Unit	IP address of the unit that hosts the AVM for the VNE.
AVM	AVM ID associated with this VNE.
Version	Version of the VNE device driver that the VNE is currently using.
Device Package Name	Device Package that is installed on the gateway server. You can use this and the driver file name information to verify whether a newer driver is available, which might supply additional functionality. See Identifying Driver Files That Are Installed on Prime Network, page 21-5.
Driver File Name	VNE device driver that is currently being used by the VNE.

Notes on Generic SNMP VNEs

The generic SNMP VNE is a VNE that is not related to any vendor, can represent any vendor (with certain limitations), and provides lightweight management support for network devices. A generic SNMP VNE does the following:

- Provides basic management capabilities for a device with the following technologies:
  - IP (restricted to basic IP only; does not include modeling of IPsec, MPLS, or routing protocols)
  - Ethernet switching
  - 802.1q

- Supports these inventory items:
  - Physical inventory (specific port types only)
  - Routing table
  - ARP table
  - Default bridge
  - IP interfaces
- Supports these topologies:
  - Physical Layer Connectivity
  - MAC-based ethernet topologies

If a VNE is identified as unsupported (because its type was not recognized), Prime Network gives the VNE a status of Unsupported. You can either leave the VNE as Unsupported or load it as a Generic SNMP VNE.

Every VNE in agentdefaults/da has the entry “load generic agent for unsupported device type,” where you can set the value as true or false (the default). If the value is true, it sets 1.3.999.3 as the property. It looks for this property in agentdefaults/da/deviceTypes and finds sheer/genericda. It then skips the investigation of the device software versions and builds the VNE (generic SNMP) from the default version.

VNE SNMP Settings

To view a VNE’s SNMP settings, right-click the VNE in the Servers drawer and select **Properties**, and click the SNMP tab. Table 19-8 describes the fields in the VNE SNMP properties dialog box.

Table 19-8 Fields in the VNE SNMP Tab

Field	Description	
SNMP Version Area		
Enable SNMP	If checked, enables the SNMP communication protocol so that the user can work with it. A VNE can have SNMP enabled or disabled at any time; however, when the Auto Detect check box is checked (in the General tab), it cannot be disabled.	
SNMP V1/V2 Settings (activated using SNMP V1 or SNMP V2)		
SNMP V1 and V2 fields are available only when SNMP is enabled.		
Read	SNMP read community status, public (default) or private, as defined by the user.	
Write	(Optional) SNMP write community status, public or private (default), as defined by the user.	
SNMP V3 Settings (activated if using SNMP V3)		
SNMP V3 fields are available only when SNMP V3 is chosen. Make sure you have performed the required SNMPv3 device configuration tasks listed in SNMP Traps and Informs—Required Device Settings, page A-5.		
Authentication	Type of authentication to be used: • No—Authentication is not required (default). • md5—Uses Message Digest 5 (MD5) for the authentication mechanism. • sha—Uses Secure Hash Algorithm (SHA) for the authentication mechanism.	
	User	Authentication username.
	Password	Authentication password. This field is enabled if you choose md5 or sha.

Table 19-8 Fields in the VNE SNMP Tab (continued)

Field	Description	
Encryption	Type of encryption method to be used. These choices are disabled if you choose No authentication. • No—Encryption is not required (default). • des—Uses Data Encryption Standard (DES) for encryption. • aes128—Uses 128-bit Advanced Encryption Standard (AES) for authentication. • aes192—Uses 192-bit AES for authentication. • aes256—Uses 256-bit AES for authentication.	
	Password	Encryption password. This field is enabled if you choose des, aes128, aes192, or aes256 encryption.

VNE Telnet/SSH Settings

To view a VNE's Telnet/SSH settings, right-click the VNE in the Servers drawer and select **Properties**, and click the Telnet/SSH tab.

You can find out if a VNE is using Telnet or SSH (along with the specific version) by opening the device properties window and click **VNE Status**. The VNE Status Details window provides details about the protocols. (You can open the device properties window from both Prime Network Administration (right-click the VNE and choose **Inventory**) and Prime Network Vision (right-click the device and choose **Inventory**.)

Table 19-9 describes the fields in the VNE Telnet/SSH properties dialog box.

For examples of how to enter Telnet or SSH prompt information, see Telnet and SSH Login Sequences: Notes and Examples, page 19-30. For more information on SSHv2 host key algorithms, also see Notes on SSHv2 Public Key and Private Key File Formats, page 19-32.

Table 19-9 Fields in the VNE Telnet/SSH Tab

Field	Description
Enable	Enables the communication protocol so Prime Network will investigate the network element. Checking this check box activates the other fields in this tab.
Protocol	Type of protocol to be used: Telnet (default), SSHv1, or SSHv2. **Note** By default, when a VNE opens a Telnet session with a network element in order to model and monitor the element, the Telnet session remains open for 5 minutes, even if the VNE is idle (did not query the device during the session). After 5 minutes, the VNE closes the session and reopens it when it needs to query the device. If you would like to change this configuration, contact your Cisco account representative.
Port	Port the protocol will use. This field is prepopulated depending on your protocol choice. If you are not using the default port, enter the appropriate port number. • 23—Default port for Telnet. • 22—Default port for SSHv1 or SSHv2.

Table 19-9 Fields in the VNE Telnet/SSH Tab (continued)

<table>
<tr><th>Field</th><th colspan="2">Description</th></tr>
<tr><td rowspan="3">Prompt and Run</td><td colspan="2">The network element's expected prompt, and the string Prime Network should send to the network element (when the expected prompt is detected). The table shows the current settings; you can change the settings using the controls below the table. Entering a string in the Prompt field activates the Run field. After making your entries in the Prompt and Run fields, check <b>Mask</b> if you do not want the password entered as clear text. Finally, click <b>Add</b> to add them to the login sequence. Click <b>Remove</b> to remove any lines. Use the up and down controls to the right of the table to change the order.
<b>Note</b> After an SSH session is established between the VNE and the device, the VNE starts the login sequence. This sequence is usually shorter than the corresponding Telnet login sequence, as the username or password might have been sent as a step in establishing the SSH session (see the example in Telnet and SSH Login Sequences: Notes and Examples, page 19-30).</td></tr>
<tr><td>If you selected Telnet:</td><td>Telnet prompt information. The sequence (the order of the commands) must end with a line that includes only the prompt field. Prime Network VNEs can handle partial device prompts as well. For examples, see Telnet and SSH Login Sequences: Notes and Examples, page 19-30.
The Prompt field should contain the prompt expected from the device; the Run field should contain the response to the expected prompt. When entering the Run information, you must confirm the entry in the Confirm field. The values in Run and Confirm are displayed as clear text if you have not checked the Hide the Run value while typing check box.</td></tr>
<tr><td>If you selected SSH V1 or V2:</td><td>SSH prompt information. This sequence is usually shorter than the corresponding Telnet login sequence, because the username or password may already be sent during the process of establishing the SSH session. We recommend that you first use any SSH client application (such as UNIX SSH or OpenSSH) to determine the device SSH login sequence, and then enter that information.</td></tr>
<tr><td>Mask</td><td colspan="2">Masks the password so it is not displayed as clear text in the Run and Confirm fields.</td></tr>
<tr><td>Add and Remove</td><td colspan="2">Used to manipulate the order of the prompt and run strings.</td></tr>
<tr><td colspan="3"><b>SSHv1 Area (activated if using SSHv1)</b></td></tr>
<tr><td>User Name</td><td colspan="2">Device name.</td></tr>
<tr><td>Password</td><td colspan="2">Device password.</td></tr>
<tr><td>Cipher</td><td colspan="2">Encryption algorithm to be used. By default, all methods are used.
• DES—Use the Data Encryption Standard algorithms.
• 3DES—Use the Triple Data Encryption Standard algorithm.
• Blowfish—Use the blowfish algorithms.</td></tr>
<tr><td>Authentication</td><td colspan="2">Authentication method; currently password is the only supported method.</td></tr>
</table>

Table 19-9 Fields in the VNE Telnet/SSH Tab (continued)

Field	Description	
SSHv2 Area (activated if using SSHv2)		
User Name	SSHv2 username.	
Client Authentication	Client-driven authentication method to be used.	
	password	Use a password to authenticate the client. Enter the password in the Password field.
	public-key	Optionally, use public key authentication, which uses a key pair system in which the client application is configured with the secret private key, and the device is configured with the public (non-secret) key (of this pair). To create a pair of keys: 1. In the Private Key field, click **. . .** to import the private key from a file. You cannot manually enter they key, but you can edit a key that you import from file. If you change it to the wrong key, you will see an error message. 2. In the Public Key area, generate the public key in any of the following ways: – Click **. . .** to import the public key from a file. – Manually enter a public key. – Click **Generate** to autogenerate a public key.
Server Authentication	Server authentication method to be used.	
	none	No server authentication. (This method does not do any authentication and is not recommended, because it poses a security risk for "man-in-the-middle" attacks.)
	save-first-auth	Uses the public key that was used for the first connection attempt with the server. This method assumes the first connection was legitimate. (A security risk exists if the connection was compromised.) After the first connection, the server authentication method is changed to preconfigured, and the public key data is inserted as the preconfigured data.
	preconfigured	Uses the server public key or fingerprint that was configured in the application event before the first connection was attempted. This is the default and is the recommended method. Selecting this method activates the Finger Print or Public Key field. Select one of the following (and be sure to read the description, provided later in this table, of the Host Key Algorithm field): • Finger Print—Uses a short checksum of the server public key (this serves the same purpose, but is much shorter). • Public Key—Uses the public key in one of the permitted formats (see Notes on SSHv2 Public Key and Private Key File Formats, page 19-32). Click **. . .** to import the public key from a file.
By default, the SSHv2 Key, MAC, ciphers, and host key algorithms[1] are allowed (enabled): • Key exchange: DH-group1-sha1, DH-group1-exchange-sha1 • MAC algorithm: SHA1, MD5, SHA1-96, MD5-96 • Ciphers: 3DES, AES-128, AES-192, AES-256, Blowfish, Arcfour • Host Key Algorithm: DSA, RSA For information on how to change these settings, see Device Communication Security: SSH and SNMPv3, page 13-4.		

[1] You can select multiple algorithms by pressing Ctrl while choosing a method. If more than one is selected, the application will try to use all of the algorithms until one is accepted by the server. There is no priority in the way the algorithms are tried.

Telnet and SSH Login Sequences: Notes and Examples

When you add a VNE, Prime Network uses the specified communication protocol to connect to the network element and gather modeling and status information. You must provide the information Prime Network will need: the characters and order of the network element's expected prompts, and the string Prime Network should send to the network element in response (so that you can get to enable mode for Cisco IOS and Cisco IOS XE devices, and XML mode for Cisco IOS XR devices).

Note VNEs can understand partial and complete device prompts.

After an SSH session is established between the VNE and the device, the VNE starts the SSH login sequence. This sequence is usually shorter than the corresponding Telnet login sequence.

This topic provides two examples (with complete procedures) that show how to enter Telnet sequences:

- Telnet Login Sequence for a Cisco IOS Device: Example, page 19-30
- Telnet Sequence for a Cisco IOS XR Device: Example, page 19-31

A Telnet sequence (the order of the commands) must end with a line that includes only the enable prompt (for Cisco IOS and Cisco IOS XE devices) or the router CLI prompt (for Cisco IOS XR devices). Not all device families will have the same Telnet sequence; this is especially true for Cisco IOS devices. For RAD ACE-2300 devices, because SNMP is used for device modeling, we recommend disabling Telnet to avoid unnecessary queries.

Telnet Login Sequence for a Cisco IOS Device: Example

This sample procedure describes how you could enter a Telnet sequence for a hypothetical Cisco IOS device or Cisco IOS XE device.

Step 1 Check the **Enable** check box to activate the Telnet prompt fields.

Step 2 Enter the expected device prompt and response:

Note To verify a device's Telnet sequence, open a Telnet session to the device and copy the information. The following is an example.

a. Enter **Password:** in the Prompt field.

Note If you do not want the password displayed in clear text, check **Mask**.

b. Enter **Rivers39*** in the Run field.

c. Click **Add**.

Step 3 Enter the device prompt and the command required to place the device in enable mode:

a. Enter **R3745>** in the Prompt field.

b. Enter **enable** in the Run field.

c. Click **Add**.

Step 4 Enter the enable mode password information:

a. Enter **Password:** in the Prompt field.

Note If you do not want the password displayed in clear text, check **Mask**.

b. Enter **!Tribal41_** in the Run field.

c. Click **Add**.

Step 5 Enter the enable prompt information:

a. Enter **R3745#** in the Prompt field.

Note VNEs can also understand partial prompts. For example, if you enter the string **#** instead of **R3745#**, the VNE will still be able to recognize the expected prompt.

Leave the Run field blank.

b. Click **Add**.

Telnet Sequence for a Cisco IOS XR Device: Example

This sample procedure describes how you could enter a Telnet sequence for a hypothetical Cisco IOS XR device.

Step 1 Check the **Enable** check box to activate the Telnet prompt fields.

Step 2 Enter the expected device prompt and response:

Note To verify a device's Telnet sequence, open a Telnet session to the device and copy the information. The following is an example.

a. Enter **Username:** in the Prompt field.

b. Enter **crs1-oak** in the Run field.

c. Click **Add**.

Step 3 Enter the device password information:

Note Enter **Password:** in the Prompt field.

Note If you do not want the password displayed in clear text, check **Mask**.

d. Enter **sunFlower108!** in the Run field.

e. Click **Add**.

Step 4 Enter the device prompt:

a. Enter **EC-A#** in the Prompt field.

> **Note** For devices with multiple processors (such as Cisco CRS), the prompt comprises the active CPU plus the device name (for example, **RP/0/RSP0/CPU0:EC-A#**). A CPU failover could change the prompt and report a different CPU. In these cases, you should insert a prompt that specifies only the device name (for example, **EC-A#**). (Also, as with Cisco IOS, VNEs can also understand partial prompts. For example, if you enter the string **#** instead of **EC-A#**, the VNE will still be able to recognize the expected prompt.)

Leave the Run field blank.

b. Click **Add**.

Notes on SSHv2 Public Key and Private Key File Formats

There are several file formats for public and private RSA and DSA keys. The same key can be written differently according to the format that is used.

This application officially supports the openSSH format. For more details, see http://www.openssh.com/manual.html.

Make sure that the keys you provide as input parameters are in this format. If they are not, you need to convert them to the open SSH format before applying them.

Use Case Example: When working with Cisco IOS, the public key is retrieved using the **show crypto key mypubkey** command. This format is not compatible with the OpenSSH format, and is not supported. There are several ways to convert the format.

The easiest solution is to use public key scan by the (free) openSSH application to retrieve the public key in the supported format. For more details, see http://www.openssh.com/manual.html.

Another option is to convert the files to the required format either manually or by using a script.

The following are examples of valid file formats.

```
RSA- private key
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgQDvdpW8ItfbSp/hTbWZJqCPmjRyh9S+EpTJ0Aq3fnGpFPTR+
……. .
TiOfhiuX5+M1cTaE/if8sScj6jE9A0MpShBrnDU/0A==
-----END RSA PRIVATE KEY-----

DSA private key
-----BEGIN DSA PRIVATE KEY-----
MIIBuwIBAAKBgQDNGO+l2XW+W+YtVnWSYbKXr6qkrH9nOl+
………
7wO4+FR9afoRjDusrQrL
-----END DSA PRIVATE KEY-----

DSA public key
ssh-dss AAAAB3………HfuNYu+ DdGY7njEYrN++iWs= aslehr@aslehr-wxp01

RSA - public key
ssh-rsa AAAAB3…lot more…qc8Hc= aslehr@aslehr-wxp01
```

VNE XML Settings

To view a VNE's XML properties, right-click the VNE in the Servers drawer and select **Properties** and click the XML tab. XML is used by some devices such as those that use Cisco IOS XR. Table 19-10 describes the fields in the VNE XML properties dialog box.

Table 19-10 Fields in the VNE XML Tab

Field	Description
Enable	Enables the XML communication protocol so Prime Network will investigate the network element. Checking this check box activates the other fields in this tab.
Protocol	Type of protocol to be used: Telnet (default) or SSL. **Note** By default, when a VNE opens a Telnet session with a network element in order to model and monitor the element, the Telnet session remains open for 5 minutes, even if the VNE is idle (did not query the device during the session). After 5 minutes, the VNE closes the session and reopens it when it needs to query the device. If you would like to change this configuration, contact your Cisco account representative.
Port	Port the protocol will use. This field is prepopulated depending on your protocol choice. If you are not using the default port, enter the appropriate port number. • 38751—Default port for Telnet. • 38752—Default port for SSL.
Prompt and Run	The network element's expected Telnet or SSL prompt, and the string Prime Network should send to the network element (when the expected prompt is detected). The table shows the current settings; you can change the settings using the controls below the table. Entering a string in the Prompt field activates the Run field. After making your entries in the Prompt and Run fields, check **Mask** if you do not want the password entered as clear text. Finally, click **Add** to add them to the login sequence. Click **Remove** to remove any lines. Use the up and down controls to the right of the table to change the order. **Note** After an SSH session is established between the VNE and the device, the VNE starts the login sequence. This sequence is usually shorter than the corresponding Telnet login sequence, as the username or password might have been sent as a step in establishing the SSH session (see the example in Telnet and SSH Login Sequences: Notes and Examples, page 19-30). The sequence (the order of the commands) must end with a line that includes only the prompt field. The Prompt field should contain the prompt expected from the device; the Run field should contain the response to the expected prompt. When entering the Run information, you must confirm the entry in the Confirm field. The values in Run and Confirm are displayed as clear text if you have not checked the Hide the Run value while typing check box.
Mask	Masks the password so it is not displayed as clear text in the Run and Confirm fields.
Add and Remove	Used to manipulate the order of the prompt and run strings.

VNE HTTP Settings

To view a VNE's HTTP settings, right-click the VNE in the Servers drawer and select **Properties**, and click the HTTP tab.

Note These settings are not used by VNEs provided with the initial release of Prime Network 3.8. Future Device Packages will introduce new device support for devices that will use this feature.

Table 19-11 describes the fields in the VNE HTTP properties dialog box.

Table 19-11 Fields in the VNE HTTP Tab

Field	Description
Enable	Enables the HTTP communication protocol so Prime Network will investigate the network element. Checking this check box activates the other fields in this tab.
Enable HTTPS	Enables the secure HTTP communication protocol.
Port	Port the protocol will use. By default, HTTP uses port 80.
Management Path	HTTP URL to use to connect the device.
Use Authentication	Enables requiring credentials for HTTP to log in to the device.

VNE ICMP Settings

To view a VNE's ICMP settings, right-click the VNE in the Servers drawer and select **Properties**, and click the ICMP tab. Table 19-12 describes the fields in the VNE ICMP properties dialog box.

Table 19-12 Fields in the VNE ICMP Tab

Field	Description
Enable	Instructs Prime Network to use the ICMP communication protocol to verify that the network element is reachable. You can enable or disable ICMP polling at any time by checking or unchecking the check box (except for ICMP type VNEs, which require this setting to be enabled).
Polling Rate	Polling rate in seconds. If ICMP is enabled, this is a required field.

VNE Polling Settings

To view a VNE's Polling settings, right-click the VNE in the Servers drawer and select **Properties**, and click the Polling tab. This tab is disabled if you chose ICMP as the VNE type (in the General tab). In addition to controlling the intervals at which a network element is polled, this dialog box specifies the adaptive polling settings, which specify how a VNE should respond to high device CPU usage.

Note If you want to apply polling settings at a global level (rather than per VNE), create a polling group that can then be applied across VNEs. See VNE Polling Groups and Slow Polling, page 22-23.

Table 19-13 describes the fields in the VNE Polling properties dialog box.

Table 19-13 Fields in the VNE Polling Tab

<table>
<tr><th>Field</th><th colspan="2">Description</th></tr>
<tr><td colspan="3"><b>Polling Method</b></td></tr>
<tr><td rowspan="4">Polling approach for model updates</td><td colspan="2">Specifies whether to use normal or reduced polling. The reduced polling mechanism polls a device only when a configuration change syslog is received (which results in less polling overall). You can verify whether a device supports reduced polling by clicking the <b>Supported on selected devices only</b> link.
By default, reduced polling is disabled and devices are polled according to the standard methods. For more information see Reduced Polling, page 22-2.</td></tr>
<tr><td>Prime Network default for device type</td><td>Use the dependency level that is the default for this device type.</td></tr>
<tr><td>Reduced polling (event-based)*</td><td>Poll the device when an event is received from the device. This results in less overall device polls.</td></tr>
<tr><td>Regular polling</td><td>Do not poll the device when an event is received from the device; instead use the normal polling mechanisms. This results in more device polls, overall.</td></tr>
<tr><td colspan="3"><b>Polling Parameters</b></td></tr>
<tr><td>Group</td><td colspan="2">Use polling rates from one of the polling groups listed in the drop-down list. This allows you to apply polling rates more globally, to devices of similar type. By default, Prime Network uses Group (not Instance), and the polling group named <b>default</b> (which is provided out-of-the-box).
<b>Note</b> You can create new polling groups that will appear in the drop-down list by using the procedure in VNE Polling Groups and Slow Polling, page 22-23.</td></tr>
<tr><td>Instance</td><td colspan="2">Uses a user-specified polling rate created by changing the polling rates of any one of the built-in polling intervals displayed in the dialog box. When you select Instance, the Polling Intervals and Topology areas are activated. These settings are applied to only this VNE.
<b>Note</b> A polling rate that is not changed inherits its settings from the group specified in the drop-down list.</td></tr>
<tr><td colspan="3"><b>Polling Intervals Area (activated if using Instance)</b>
<b>Note</b> We recommend that you use the default settings for these polling intervals. Setting the fields below the default values can result in an overload of the Prime Network unit or polled device.</td></tr>
<tr><td>Status</td><td colspan="2">Polling rate for status-related information, such as network element status (up or down), port status, administrative status, and so on. This is typically the most frequently polled information, reflecting the current operational and administrative state of the element and its components. The default setting is 180 seconds.</td></tr>
<tr><td>Configuration</td><td colspan="2">Polling rate for configuration-related information, such as VC tables, scrambling, and so on. These reflect more dynamic element configuration such as forwarding, routing, and switching tables. The default setting is 900 seconds.</td></tr>
<tr><td>System</td><td colspan="2">Polling rate for system-related information, such as network element name, network element location, and so on. These reflect element configurations that are less dynamic in nature. The default setting is 86400 seconds.</td></tr>
<tr><td colspan="3"><b>Topology Area (activated if using Instance)</b></td></tr>
<tr><td>Layer 1</td><td colspan="2">Polling rate of the topology process as an interval for the Layer 1 counter. This is an ongoing process. The default setting is 90 seconds.</td></tr>
<tr><td>Layer 2</td><td colspan="2">Polling rate of the topology process as an interval for the Layer 2 counter. This process is available on demand. The default setting is 30 seconds.</td></tr>
</table>

Table 19-13 Fields in the VNE Polling Tab (continued)

Field	Description	
Adaptive Polling Area		
Prime Network Settings	Uses the default settings for controlling VNE adaptive polling (see Adaptive Polling, page 22-15).	
Device Type Settings	(Default) Uses the VNE adaptive polling settings specified for this device type (as delivered with Prime Network). If no setting exists for the device type, the Prime Network Settings are used.	
Local Settings	Overrides the default settings and uses the values specified in the Upper and Lower Threshold fields. Any values you specify here are used only for this VNE instance. • To enter your own adaptive polling settings, click **Local Settings** and enter the thresholds. The changes are not applied until you check the **Enable** check box. • To turn off adaptive polling for the VNE, click **Local Settings** and uncheck the **Enable** check box. You must click **Apply** and restart the VNE for your changes to take effect.	
	Upper Threshold	When CPU usage exceeds this value, the adaptive polling mechanism is triggered. The VNE switches to slow polling or maintenance mode.
	Lower Threshold	When CPU usage drops below this value, the VNE moves to normal polling and related alarms are cleared.

VNE Events Settings

Note For troubleshooting help, see Troubleshooting VNE Modeling, page 20-1 and Device Reachability, page 24-1. Also make sure you performed all necessary device configuration tasks in Before You Create VNEs, page 19-12.

To view a VNE's Event settings, right-click the VNE in the Servers drawer and select **Properties**, and click the Events tab. These settings allow you to configure the VNE to listen to additional IP addresses. Existing addresses that are being listened to are listed on the right; you can enter a new address on the left. This is useful when devices have components using IP addresses that are different from the management IP address, especially if the device driver cannot automatically detect these additional addresses.

For example, traps and syslogs maybe dropped if any of the VNEs managed by Prime Network are configured in such a way that the following addresses are *different*:

- The traps and syslogs source IP address
- The VNE IP address (entered when the VNE was created and displayed in the VNE properties)

To avoid missing any traps or syslogs, configure the VNE to receive traps and syslogs using both IP addresses. For Cisco IOS XR devices, if the device has a configured virtual IP address *and* the VNE was added using that address, the device can receive the traps and syslogs through the virtual IP address. You do not need to configure the source for the SNMP traps and syslogs. For more information, see Recommended and Optional SNMP Settings for Cisco IOS XR Devices, page A-8.

Table 19-14 describes the fields in the VNE Events properties dialog box.

Table 19-14 Fields in the VNE Events Tab

Field	Description
Enter IP Address	Field in which to enter new IP address, where you want the VNE to listen for syslogs and traps.
Event-Generating IP Addresses	Existing IP addresses the VNE is already listening to, for syslogs and traps.

After entering the address and clicking **Add**, the new IP address is listed under Event-Generating IP Addresses. When the VNE is saved, it will be begin listening for events at the new IP address.

Editing VNE Properties

You can edit all VNE settings except for the scheme. When you change the settings, you must restart the VNE for your changes to take effect. You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

For troubleshooting help, see Troubleshooting VNE Modeling, page 20-1 and Device Reachability, page 24-1. Also make sure you performed all necessary device configuration tasks in Before You Create VNEs, page 19-12.

You cannot change the name of a VNE. You must delete the VNE and create a new one.

Note For deployment information and recommendations, such as best practices for assigning VNEs to AVMs, contact your Cisco account representative.

To edit a VNE:

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

Step 2 Open the VNE Properties dialog box by right-clicking the required VNE in the VNE Properties table, then choose **Properties**.

Step 3 Edit or view the properties as required. Information that is dimmed cannot be edited. The settings that are available for editing depend on the VNE type. (For example, for Cloud VNEs, you can only edit General settings; for ICMP type VNEs, you cannot edit Polling settings.) If a field is dimmed, meaning you cannot edit it, to change the setting you must delete and recreate the VNE.

Step 4 Details about the fields in the VNE properties tabs are described in these topics:

- VNE General Settings, page 19-24
- VNE SNMP Settings, page 19-26
- VNE Telnet/SSH Settings, page 19-27
- VNE ICMP Settings, page 19-34
- VNE Polling Settings, page 19-34
- VNE Events Settings, page 19-36

Step 5 After making your required changes, click **Apply** and **OK**. The VNE properties are updated with your entries.

Step 6 Stop and restart the VNE as described in Changing VNE Status and Lifecycle (Start, Stop, Maintenance), page 19-38.

Changing VNE Status and Lifecycle (Start, Stop, Maintenance)

You can use the Prime Network Administration GUI to start or stop a VNE, or move a VNE to maintenance mode. When you change the status of a VNE, the VNE persistency information is retained. Persistency information is data that is stored for later use. (For information on the VNE persistency mechanism, see Persistency Overview, page 26-1.)

Restarting a VNE also 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 (for example, neighboring VNEs will not generate alarms that are related to links to or from the maintained VNE). 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 19-2 on page 19-5.

You do not need to restart a VNE after a device is upgraded. 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 VNE Updates, page 21-1.

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**.

You must have Administrator privileges (user access role) to use this and all other functions in Prime Network Administration.

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.

Controlling Concurrent VNE Telnet Logins (Staggering VNEs)

The VNE staggering mechanism controls the rate at which VNEs initiate Telnet/SSH connections across a network managed by Prime Network. This prevents degraded performance on TACACS servers, which can result when there are many concurrent connections.

The mechanism is implemented across the following Prime Network components:

- A gateway service that controls whether VNEs on the unit are permitted to initiate Telnet login sequences. It does this by controlling the number of concurrent connections, and distributing those connections based on how AVMs and VNEs are allocated. The service runs on AVM 99 on the gateway server and units. If there are multiple unit servers, it runs in a distributed fashion across all units. The service ensures that the requests are distributed (it does not specifically monitor the TACACS server).
- A VNE service that requests login permission from its unit server’s management service.
- A Telnet protocol service that requests authorization before initiating a login sequence with a device (Telnet and SSH login requests).

When the gateway receives a Telnet authorization request, it queues the requests in a FIFO (first in, first out) manner. If the gateway denies the request, the VNE communication state is changed to Device Partially Managed and a System event is generated (discovery can be prolonged if the VNE is not granted permission). In addition, the VNE Status Details window is updated to say the gateway denied the service. The VNE will continue to request the login, and once a connection is permitted, the VNE communication state changes accordingly and a clearing System event is generated.

Enabling the VNE Staggering Mechanism

This service is disabled by default; in other words, all VNEs are allowed to initiate login sequences. To enable it, use the following procedure:

Step 1 Log into the gateway as *network-user* and change to the Main directory by entering the following command. (*network-user* is the operating system account for the Prime Network application, created when Prime Network is installed; for example, **network38**.)

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

Step 2 Configure the VNE service. You must perform this procedure on all units in the system.

For the gateway, unit-IP should be **0.0.0.0**. For units, the unit-IP should be the unit's IP address.

a. Start the service on all VNEs in a unit.

```
# ./runRegTool.sh -gs 127.0.0.1 set unit-IP
site/mcvm/services/agentbootstrap/VLAA/enable true
```

b. Configure the protocol to request authorization before initiating a login:

```
# ./runRegTool.sh -gs 127.0.0.1 set unit-IP
site/agentdefaults/da/ip_default/protocols/telnet/authorizedlogin true
```

c. Restart the AVMs on the unit.

Step 3 Configure the gateway service. You must perform this procedure on all units in the system. When you perform these commands on the gateway server, both *gateway-IP* and *unit-IP* should be 127.0.0.1.

a. Configure the parameters that control the connections.

– Specify the number of permitted concurrent logins:

```
# ./runRegTool.sh -gs gateway-IP set unit-IP
avm99/services/vneLoginSupervisor/allowedConcurrentLoginsNum logins
```

We recommend an initial concurrent login setting of 1000:

```
# ./runRegTool.sh -gs gateway-IP set unit-IP
avm99/services/vneLoginSupervisor/allowedConcurrentLoginsNum 1000
```

– Specify the amount of time allotted for the VNE to successfully log in. If exceeded, the login is disallowed. (This allows the next VNE in the queue to proceed with its login.)

```
# ./runRegTool.sh -gs gateway-IP set unit-IP
avm99/services/vneLoginSupervisor/vneFinishedLoginTimeout milliseconds
```

We recommend an initial setting of 5000 milliseconds (5 seconds):

```
# ./runRegTool.sh -gs gateway-IP set unit-IP
avm99/services/vneLoginSupervisor/vneFinishedLoginTimeout 5000
```

b. Start the gateway service

```
# ./runRegTool.sh -gs gateway-IP set unit-IP avm99/services/vneLoginSupervisor
com.sheer.system.os.services.vne.login.VneLoginSupervisorServiceImpl
```

c. Restart AVM 99 on all units.

```
# runall.csh networkctl -avm 99 restart
```