APPENDIX D

VNE Properties Reference

The following tables provide a list of all VNE properties. The tabs that are listed depend on the device type—for example, the vCenter tab is displayed only for Cisco Unified Computing System devices.

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, 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** 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 Properties: General, 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.	VNE Properties: SNMP, 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.	VNE Properties: Telnet/SSH, page D-6
XML	Enables XML for device reachability and investigation.	VNE Properties: XML, page D-12
HTTP	Enables HTTP or HTTPS for device reachability and investigation.	VNE Properties: HTTP, page D-13
TL1	Enables the TL1 management protocol for running scripts on the device (used by Change and Configuration Management only).	VNE Properties: TL1, page D-14
ICMP	Enables ICMP and the ICMP polling rate (in seconds) for device reachability testing.	VNE Properties: ICMP, page D-13

VNE Tab	Description	Described in:
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 Properties: Polling, page D-14
Adaptive Polling	Controls how the VNE responds to high CPU situations.	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
vCenter	Enables connections to a Cisco UCS vCenter server using the HTTP or HTTPS communication protocol for vCenter reachability and investigation. (This tab appears after you add a UCS VNE.)	VNE Properties: vCenter, page D-18

To edit VNE properties, see Change a VNE IP Address and Other VNE Properties, page 4-33.

VNE Properties: General

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 D-1 describes the fields in the VNE General properties dialog box.

Table D-1   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. You can change the IP address of an existing VNE by changing it in this field. You must stop and restart the VNE to apply your change.

Table D-1   Fields in the VNE General Tab (continued)

Field	Description
Type	Defines the protocol Prime Network will use to model the element, and the extent to which you want the element to be modeled. For information on how Prime Network responds when an NE is unreachable, see Change Settings That Determine Device Reachability, page 12-24. 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 D-4. • 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. See Create Connections for Unmanaged Network Segments (Cloud VNEs and Links), page 12-43. • 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. ICMP VNEs can connect to other VNEs using static links. If you want to connect ICMP VNEs using physical links, you must configure the ICMP VNE's MAC address, as described in Notes on ICMP VNEs, page D-13.
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. • 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, 12000 GSR (Gigabit Switch Router) 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 more information, see Choosing a VNE Scheme (Check Technologies and Device Types), page A-2.

Table D-1   Fields in the VNE General Tab (continued)

Field	Description
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 Stop, Start, and Move VNEs to Maintenance Mode, page 4-9.
VNE Location	
Unit	IP address of the unit that hosts the AVM for the VNE.
AVM	AVM ID associated with this VNE.
VNE Driver Details	
Version	(Existing VNEs only) Version of the VNE device driver being used.
Device Package Name	For existing VNEs, this is the 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 Find Out if New Device Support is Available, page 4-27. For new VNEs, this is a drop-down list that displays all available Device Packages. By default, the VNE uses the latest DP that is installed on the gateway or unit. After creating the VNE, you can update it to use new driver files as described in Change the Device Package a VNE Is Using, page 4-30.
Driver File Name	(Existing VNEs only) Name of the VNE device driver being used (this driver corresponds to the DP that is listed).

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 Properties: SNMP

To view a VNE's SNMP settings, right-click the VNE in the Servers drawer and select **Properties**, and click the SNMP tab. Table D-2 describes the fields in the VNE SNMP properties dialog box.

Table D-2   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-15.	
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 D-2   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 Properties: Telnet/SSH

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 D-3 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 D-9. For more information on SSHv2 host key algorithms, also see Notes on SSHv2 Public Key and Private Key File Formats, page D-11.

Table D-3   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 D-3   Fields in the VNE Telnet/SSH Tab (continued)

Field	Description	
Prompt and Run	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 **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 D-9).	
	If you selected Telnet:	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 D-9.
		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.
	If you selected SSH V1 or V2:	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.
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.	
SSHv1 Area (activated if using SSHv1)		
User Name	Device name.	
Password	Device password.	
Cipher	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.	
Authentication	Authentication method; currently password is the only supported method.	

Table D-3   *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 D-11). 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 Communication Security with Devices: SSH and SNMPv3, page 11-5.

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).

Before creating the login sequences, check for device-specific prerequisites and other details in Device Configuration Tasks for Modeling, page A-1.

> **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 D-9
- Telnet Sequence for a Cisco IOS XR Device: Example, page D-10

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 Properties: XML

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 D-4 describes the fields in the VNE XML properties dialog box.

Table D-4   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 D-9).
	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 Properties: HTTP

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

Table D-5 describes the fields in the VNE HTTP properties dialog box.

Table D-5   Fields in the VNE HTTP Tab

Field	Description
Enable	Enables the HTTP communication protocol so Prime Network can 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, and HTTPS uses 443.
Management Path	HTTP URL to use to connect the device.
Use Authentication	Enables requiring credentials for HTTP to log in to the device.

VNE Properties: ICMP

To view a VNE's ICMP settings, right-click the VNE in the Servers drawer and select **Properties**, and click the ICMP tab. Table 4-6 describes the fields in the VNE ICMP properties dialog box.

Table 4-6   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.

Notes on ICMP VNEs

ICMP VNEs are used to test the reachability to a device. For ICMP VNEs, Prime Network does not poll the device to create a physical and logical inventory. But to connect the ICMP VNE to another VNE and visualize a link on the map, the ICMP VNE must have a port in its physical inventory. Therefore, when Prime Network creates an ICMP VNE, it creates a physical inventory model that contains only an Ethernet port.

You can use static links to connect ICMP VNEs to other VNEs.

Prime Network will autodiscover physical links between the ICMP VNE and other VNEs if the following conditions are met:

- The real MAC address of the port is configured for the ICMP VNE.
- The port on the ICMP VNE is a routed port and terminates the Layer 2 domain.

To specify a MAC address for an ICMP VNE, use the following procedure.

Step 1   Log into the gateway as *pnuser* and change to the Main directory by entering the following command.
(*pnuser* is the operating system account for the Prime Network application, created when Prime Network
is installed; for example, **pn310**.)

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

Step 2   Configure the MAC address for the VNE. For the gateway, *unit-IP* should be **0.0.0.0**. For units, the
unit-IP should be the unit's IP address.

```
# ./runRegTool.sh -gs gateway-IP set unit-IP site/sheericmp/base/product/software
versions/default
version/spec/dcs/com.sheer.metrocentral.coretech.common.equipment.dc.Chassis/ethMacAddress
mac-address
```

Step 3   Restart the VNE.

VNE Properties: TL1

TL1 is used by the Prime Network Change and Configuration Management feature. To view a VNE's
TL1 settings, right-click the VNE in the Servers drawer and select **Properties**, and click the TL1 tab.

Table D-5 describes the fields in the VNE TL1 properties dialog box.

Table D-7   Fields in the VNE TL1 Tab

Field	Description
Enable	Enables the TL1 management protocol for CPT devices. Checking this box activates the other fields in this tab.
Port	Port the protocol will use.
User	TL1 user name
Password	Password for TL1 user.

VNE Properties: Polling

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 Regular Polling (VNE Polling Groups), page 12-18.

Table D-8 describes the fields in the VNE Polling properties dialog box.

Table D-8   Fields in the VNE Polling Tab

Field	Description
Polling Method	
Polling approach for model updates	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 **Supported on selected devices only** link. By default, reduced polling is enabled. For more information see Reduced Polling, page 12-3.
	Always use reduced polling — Prime Network will define the settings based on the recommended offset of model fidelity vs. interference. If the device type does not support event-based polling, Prime Network generates a Device Unsupported event. Use this when you want to be notified if the device type does not support reduced polling.
	Used reduced polling if possible — Prime Network will define the settings based on the recommended offset of model fidelity vs. interference. If the device type does not support event-based polling, Prime Network uses regular polling. **Note** This is the default method for all VNEs. Use this when you do *not* want to be notified if the device type does not support reduced polling.
	Use regular polling — Instructs Prime Network to proactively poll configuration data using a configuration interval (usually every 15 minutes). This means that even in extreme circumstances where events are lost, the VNE would be synchronized after a maximum of 15 minutes (not 24 hours). Use this when you want the device to use regular polling regardless of whether its device type supports reduced polling.
Polling Parameters	
Group	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 **default** (which is provided out-of-the-box). **Note** You can create new polling groups that will appear in the drop-down list by using the procedure in Regular Polling (VNE Polling Groups), page 12-18.
Instance	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. **Note** A polling rate that is not changed inherits its settings from the group specified in the drop-down list.
Polling Intervals Area (activated if using Instance)	
Note 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.	
Status	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.
Configuration	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.

Table D-8   Fields in the VNE Polling Tab (continued)

Field	Description
System	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.
Topology Area (activated if using Instance)	
Layer 1	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.
Layer 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.

VNE Properties: Adaptive Polling

Table D-9 describes the fields in the VNE Adaptive Polling tab.

Table D-9   Fields in the VNE Adaptive Polling Tab

Field	Description	
Prime Network Settings	Uses the default settings for controlling VNE adaptive polling (see Adaptive Polling, page 12-11).	
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.	
Thresholds	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.
	Upper Tolerance	When upper threshold is crossed this number of consecutive CPU polls, move the VNE to slow polling. To be more conservative, enter a lower number. (Using the settings in this table and in Table 12-4, this means the VNE would move to slow polling after 5 minutes.).
	Lower Tolerance	When CPU utilization falls below the lower threshold for this number of consecutive polls, move the VNE to normal polling. To be more conservative, enter a higher number.
	Maintenance Tolerance	When upper threshold is crossed this number of consecutive CPU polls, move the VNE to CPU-only polling. (This number will include the upper tolerance polls, which is 5 by default.)
	SNMP Delay	Delay (in milliseconds) between SNMP commands that are sent from the VNE to the device.
	Telnet Delay	Delay (in milliseconds) between Telnet commands that are sent from the VNE to the device.

VNE Properties: Events

> **Note** If a VNE is using reduced polling, add the event-generating IP address to the VNE's Events tab so the VNE will listen to that address for syslogs and traps. For more information, see Turn Reduced Polling On or Off for a Single VNE, page 12-7.

The VNE Event settings configures the VNE to listen to additional IP addresses. If your deployment has virtual entities that generate events, such as applications running on virtual machines, add the entity's IP address here. For example, if you are running Cisco Policy Manager (CPM) on a Cisco Unified Computing Server (UCS) and you want Prime Network to process the SNMP traps from the CPM application, you must configure the CPM application's source IP address as an Event-Generating IP Address in this dialog box.

If a device components that have IP addresses that are different from the management IP address, enter them here, especially if the device driver cannot automatically detect these additional addresses.

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.

Table 4-10 describes the fields in the VNE Events properties dialog box.

Table 4-10   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.

Enter the new address in the Enter IP Address field and click **Add**, and 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.

VNE Properties: vCenter

Prime Network uses the VMWare vCenter to obtain information about virtualization inventory and events information for Cisco UCS devices. Table D-5 describes the fields in the VNE vCenter properties dialog box. This tab is displayed after the UCS VNE is created. For information on the prerequisites and the overall procedure for creating UCS VNEs, see Cisco Unified Computing System Devices—Required Settings, page A-14.

Table D-11   Fields in the VNE vCenter Tab

Field	Description
Enable	Enables the HTTP communication protocol so Prime Network can investigate the network element. Checking this check box activates the other fields in this tab.
Enable HTTPS	Enables the secure HTTP communication protocol. Uses port 443 by default.
Port	Port the protocol will use. By default, HTTP uses port 80, and HTTPS uses 443.
Server Address	IP address for vCenter server.
Use Authentication	Enables requiring credentials for HTTP/HTTPS to connect in to the device.