CHAPTER 20

Troubleshooting VNE Modeling

These topics provide procedures to help you troubleshoot VNE modeling problems.

- Troubleshooting VNE Communication State Issues, page 20-1
- Troubleshooting VNE Investigation State (Discovery) Issues, page 20-14
- Opening a Bug Report, page 20-24

Additional VNE administration tasks are described in:

- Basic AVM and VNE Administration Tasks, page 4-1
- VNE Administration: VNE Lifecycle and Creating VNEs, page 19-1
- VNE Updates, page 21-1

Troubleshooting VNE Communication State Issues

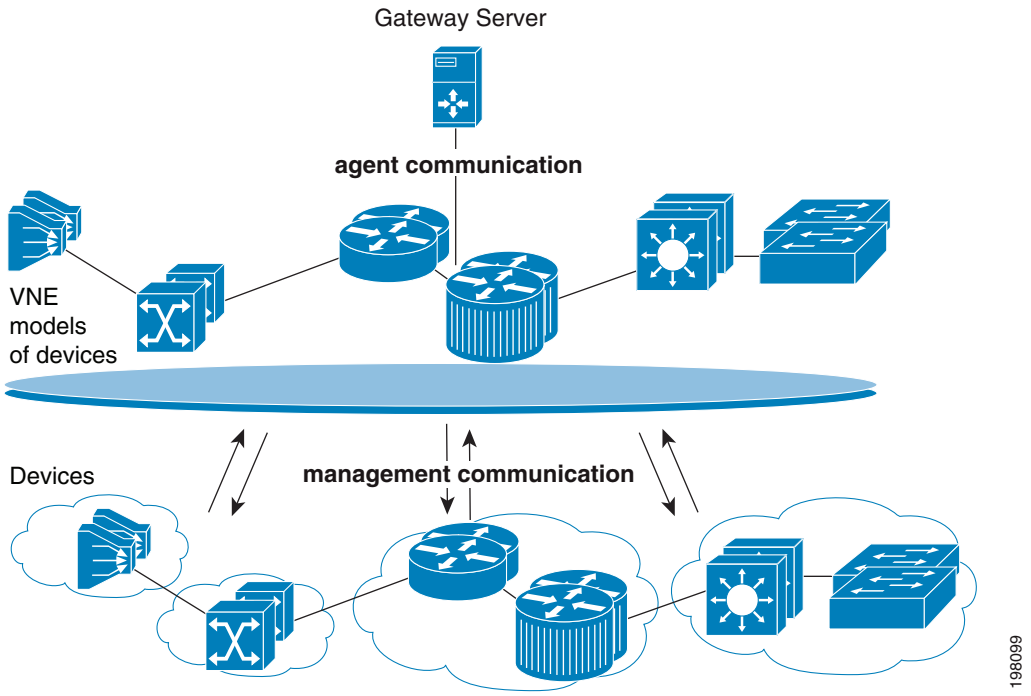
These topics help you understand what determines a VNE's communication state and how to troubleshoot a problematic state.

- What Determines the VNE Communication State (Device Reachability)?, page 20-1, describes agent and management communication, and how together their state determines the overall communication state of a VNE.
- Steps to Troubleshoot VNE Communication State Issues, page 20-3, describes what to do if a VNE is in an unexpected communication state. Troubleshooting for investigation states is provided in Troubleshooting VNE Investigation State (Discovery) Issues, page 20-14.

What Determines the VNE Communication State (Device Reachability)?

Figure 20-1 illustrate the two aspects that determine a VNE's communication state: *agent communication*, which describes reachability between the Prime Network gateway server and the VNEs, and *management communication*, which describes the reachability between a Prime Network VNE and the network device it is modeling. Both must function in order for Prime Network to properly model and manage a device.

Figure 20-1 VNE Communication States—Management and Agent



Management communication is the more challenging domain because it is far more common for devices to become unreachable than for a VNE to go down. There can be many scenarios: perhaps only the Telnet protocol is down but everything else is fine; or all protocols are down but the device is still "alive" (sending syslogs and traps); or all protocols down, and the device is not even generating traps or syslogs. To provide the most accurate reachability status, Prime Network does the following:

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

For details about how Prime Network does all of the above, see Device Reachability, page 24-1.

The most common management problem is when Prime Network reports that a VNE communication state is Device Partially Reachable because at least one protocol is not operational (this is the default behavior for protocol reporting and can be changed; see VNE Management Communication Policies and How To Change Them, page 24-1).

Table 20-2 provides information about the fields in the VNE Status Details window, and suggestions for troubleshooting steps based on the information you see.

See Device Reachability, page 24-1, for more information on management communication policies, including the following:

- How to change management communication policies
- How Prime Network determines protocol reachability
- How to customize protocol reachability testing
- How to troubleshooting SSH and Telnet connectivity issues

Steps to Troubleshoot VNE Communication State Issues

The following steps provide an overall procedure for responding to an unexpected VNE communication state.

Step	Description	See:
1	Verify the current VNE communication (and investigation) states in Prime Network Vision.	Step 1: Check the Communication State, page 20-3
2	Check the VNE Status Details window to find out if any protocols are failing and why; and check the management communication policy that is being used. (These policies determine when a VNE is moved to Device Partially Reachable, and they allow you to decide how more or less strictly you want to track protocol health.) You can optionally check the System event to see if it can provide any new information.	Step 2: Check the VNE Status Details Window for Protocol and Connectivity Information, page 20-6
3	Test the protocol connectivity.	Step 3: Troubleshoot the Connectivity Issue, page 20-12

Prime Network uses a variety of protocols to determine device reachability as described in How Prime Network Determines Protocol Reachability, page 24-3. Probably the most common communication problem is when the VNE communication state changes to Device Partially Reachable, which normally indicates that at least one protocol is experiencing a problem. On the other hand, it could mean the VNE was stopped or moved to maintenance mode.

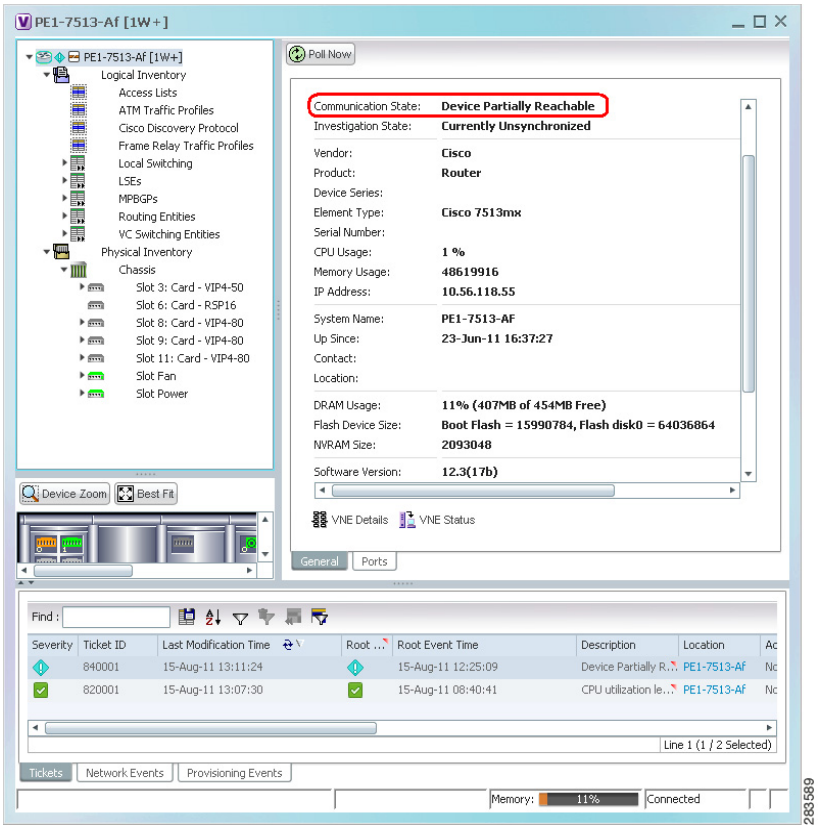
Step 1: Check the Communication State

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

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

Step 2 Check the current Communication State (as shown in Figure 20-2).

Figure 20-2 VNE Communication State (in Prime Network Vision)



The  icon indicates a network element has been deleted (or moved). Check Table 20-1 for an explanation of the state and how to proceed.

Table 20-1 VNE Communication States and Troubleshooting Tips

State Name	Description	Badge
Agent Not Loaded	The VNE is not responding to the gateway because it was stopped, or it was just created. This communication state is the equivalent of the Defined Not Started investigation state. To troubleshoot a VNE in this state, check the VNE, AVM, and unit status using Prime Network Administration. Although a System event is generated whenever the communication state changes, when a VNE is started, an event is generated only after: • All protocols have been tested and a new problem is found (one that was not previously reported). • A problem that was found has been resolved. **Note** If the VNE was stopped, you will see a message and a refresh button at the top of the properties window. If the VNE was restarted, refreshing the window will repopulate the information. However, if the VNE is still down, refreshing the window will result in an error message. To start the VNE, see Changing VNE Status and Lifecycle (Start, Stop, Maintenance), page 19-38.	None
VNE/Agent Unreachable	The VNE is not responding to the gateway. This can happen if the unit or AVM is overutilized, the connection between the gateway and unit or AVM was lost, or the VNE is not responding in a timely fashion. (A VNE in this state does not mean the device is down; it might still be processing network traffic.) To troubleshoot a VNE in this state: 1. Check the VNE, AVM, and unit status using Prime Network Administration and check the amount of available memory. 2. Use the diagnostics tool to check memory usage, GC, and CPU usage; see Obtaining Diagnostic Information Using Graphs, page 9-7. 3. Examine the AVM to see if a specific VNE is causing the problem. See VNE or AVM reachability issues are often due to CPU-related resource problems.	
Connecting	The VNE is starting and the initial connection has not yet been made to the device. This is a momentary state. Because the investigation state decorator (the hourglass) will already be displayed, a special GUI decorator is not required.	None
Device Partially Reachable	The element is not fully reachable because at least one protocol is not operational. To troubleshoot this state, continue to Step 2: Check the VNE Status Details Window for Protocol and Connectivity Information, page 20-6. **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

Table 20-1 VNE Communication States and Troubleshooting Tips (continued)

State Name	Description	Badge
Device Unreachable	The connection between the VNE and the device id down because all of the enabled protocols are down (though the device might be sending traps or syslogs). To troubleshoot this state, continue to Step 2: Check the VNE Status Details Window for Protocol and Connectivity Information, page 20-6. **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 this state, continue to Step 2: Check the VNE Status Details Window for Protocol and Connectivity Information, page 20-6.	None

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

Step 1 From the VNE properties window (see Figure 20-2 on page 20-4), click **VNE Status** at the bottom of the properties window to open the VNE Status Details window. Figure 20-3 shows an example of this window. In this case, the VNE is fully functional.

For an example of a VNE with communication problems, see Figure 20-4 on page 20-11.

Figure 20-3 Information Provided by the VNE Status Details Window

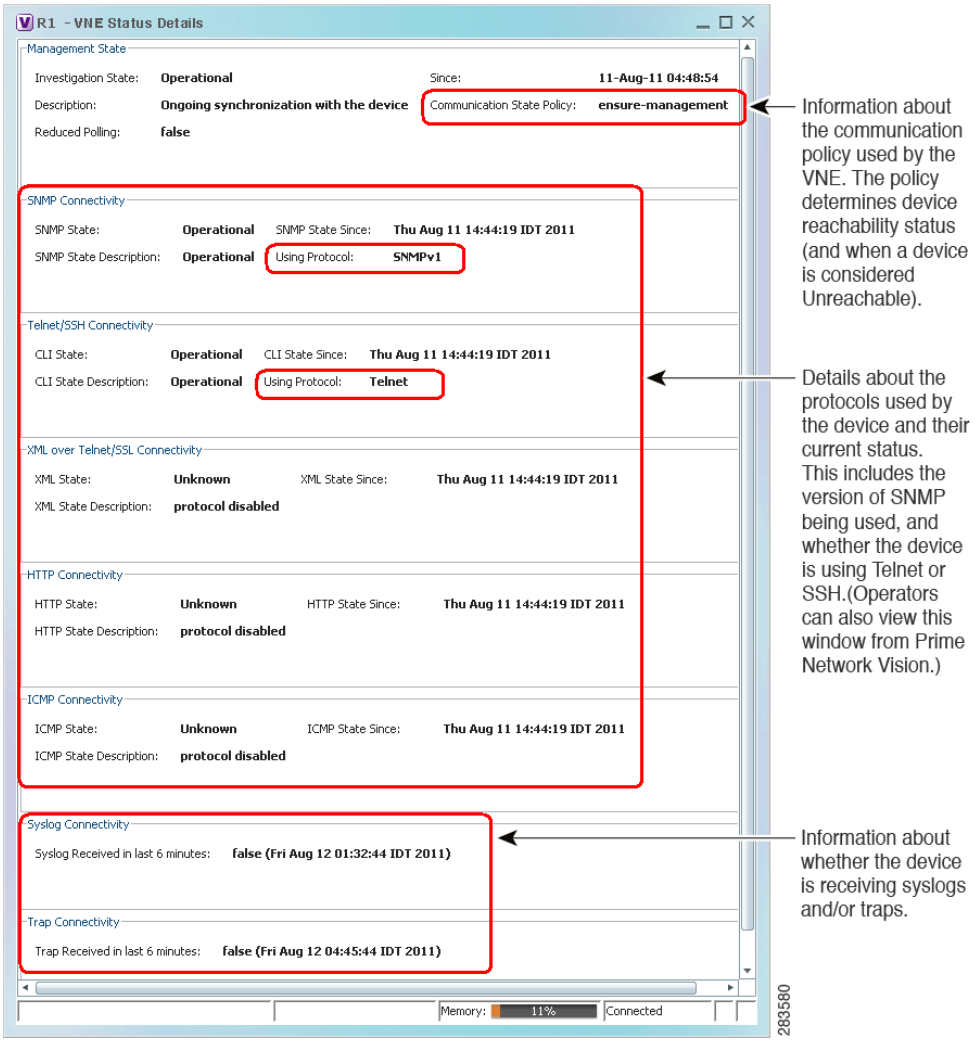


Table 20-2 provides a description of the fields in the window.

Table 20-2 VNE Communication State Information (from VNE Status Details Window)

Field	Description
Management State	The current investigation state, which pertains to device modeling (not communication). For an explanation of the Investigation State, Description, and Reduced Polling fields, see Table 20-4 on page 20-21.
Since	Timestamp of when the management state fields were last updated.

Table 20-2 VNE Communication State Information (from VNE Status Details Window) (continued)

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

Table 20-2 VNE Communication State Information (from VNE Status Details Window) (continued)

Field	Description
State Description	Details about the protocol state. Though problems can be due to a variety of issues, the following messages are grouped together by likely cause. • Improper configuration of the VNE or the device. These can normally be solved by verifying that the VNE is using the proper credentials to connect to the device. If that does not solve the problem, proceed to Step 3: Troubleshoot the Connectivity Issue, page 20-12. **Protocol failed to login** **Protocol failed to get first prompt** **Protocol failed to login when sending leading CR** **Protocol failed to get expected prompt** **Protocol failed to initiate login** **Protocol login authorization refused** **Protocol login authorization timeout** **Authentication failed** • Connectivity issues. Troubleshooting steps for this kind of problem are provided in Step 3: Troubleshoot the Connectivity Issue, page 20-12. **Protocol failed to handle connection** **Protocol failed to connect to host** **Problem trying to ping host** **Destination host unreachable** • A specific command failed (note that the other commands may have successfully completed). **Protocol failed to send command** **Protocol says: Command authorization failed** **Command execution exception**
State Since	Timestamp of when the protocol information was last updated.
Using Protocol	(Telnet/SSH Connectivity Only) Whether VNE is using Telnet or SSH. This provides an easy way for operators to check which protocol is being used.

Table 20-2 VNE Communication State Information (from VNE Status Details Window) (continued)

Field	Description
Syslog/Trap Connectivity	
Syslog/Trap received in last 6 minutes	Tells you whether the device is sending traps or syslogs (an indication of whether the device is still "alive"). The format is *value* (*time*), where: • *value*—Indicates whether a syslog or trap was (true) or was not (false) received in the last 6 minutes. This field is updated whenever a syslog or trap is received. • *timestamp*—Indicates when the last change occurred. This field is refreshed whenever you open the VNE Status Details window. For example: **false (Mon Jul 19 23:03:33 PDT 2010)** means the VNE has not received any syslogs or traps since the time and date listed. **true (Tue Jul 20 05:09:25 PDT 2010)** means the VNE has been receiving syslogs or traps at least every 6 minutes since the time and date listed. If this field is blank, either no syslogs or traps were sent since the VNE was started, or Prime Network is using a management policy that does not track syslogs and traps. If syslogs or traps are not arriving, do the following: 1. Check the status of Event Collector (AVM 100). See Viewing AVM Properties, page 4-6. 2. Check whether the device is configured to forward traps and syslogs to the unit or gateway that has the running Event Collector. See Managing the Event Collector (AVM 100), page 14-1.

Figure 20-4 shows a VNE Status Details window for a VNE that is only partially reachable.

Figure 20-4 Communication State Information in VNE Status Details Window

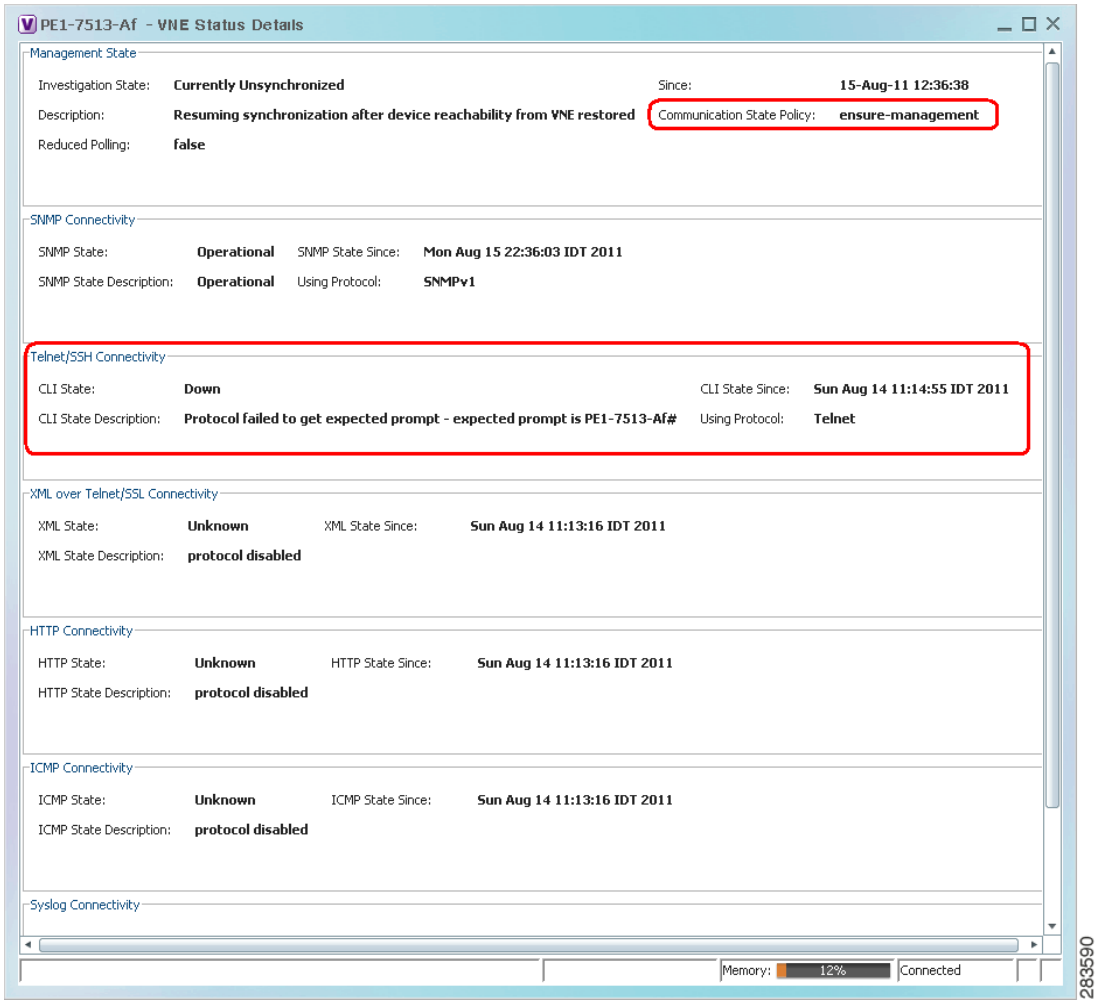


Figure 20-4 provides the following information:

- The VNE is using Telnet and the Telnet protocol failed to connect to the device because the prompt was incorrect. You should correct the Telnet sequence in the VNE properties; see Editing VNE Properties, page 19-37.
- The VNE is using the ensure-management communication policy which means the device is considered reachable when all enabled protocols are fully functional. So when the Telnet problem is fixed, the VNE should move to the reachable state.

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

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

If you want more information, you can adjust the registry setting so that Prime Network Events generates an elaborated report about state changes. See Table 20-5 on page 20-24.

Step 3: Troubleshoot the Connectivity Issue

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

- In Prime Network Administration, get the following information (see VNE Telnet/SSH Settings, page 19-27):
  - The protocol and protocol version.
  - The authentication credentials used by the VNE. (For example, if the VNE uses Telnet, you will need the Telnet sequence.)
- Verify that you are using a machine on the same subnet as that on which the VNE resides. (We recommend you run this procedure from the VNE's gateway or unit.)

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

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

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

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

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

a. Log into the gateway as *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
```

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

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

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

c. Restart the VNE.

Step 4 Try to connect to the device.

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

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

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

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

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

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

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

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

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

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

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

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

If you *can* connect to the device, the likely cause of the problem is that the VNE driver was not correctly implemented. Check the Cisco Bug Toolkit for possible open caveats, or open a bug as explained in Opening a Bug Report, page 20-24.

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

a. Log into the gateway as *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
```

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

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

```
# ./runRegTool.sh -gs 127.0.0.1 set unit-IP
"avmxxx/agents/da/vne-key/ips/vne-ip/protocols/telnet/connection/explicitly-ask-for-pt
y" true
# ./runRegTool.sh -gs 127.0.0.1 add unit-IP
"avmxxx/agents/da/vne-key/ips/vne-ip/protocols/telnet/connection/transport"
# ./runRegTool.sh -gs 127.0.0.1 set unit-IP
"avmxxx/agents/da/vne-key/ips/vne-ip/protocols/telnet/connection/transport/pty-support
" enable
# ./runRegTool.sh -gs 127.0.0.1 set unit-IP
"avmxxx/agents/da/vne-key/ips/vne-ip/protocols/telnet/telnet-over-sshv1/leadingcrenabl
ed" false
# ./runRegTool.sh -gs 127.0.0.1 set unit-IP "avmxxx/agent
s/da/vne-key/ips/vne-ip/protocols/telnet/telnet-over-sshv2/leadingcrenabled" false
```

c. Restart the VNE.

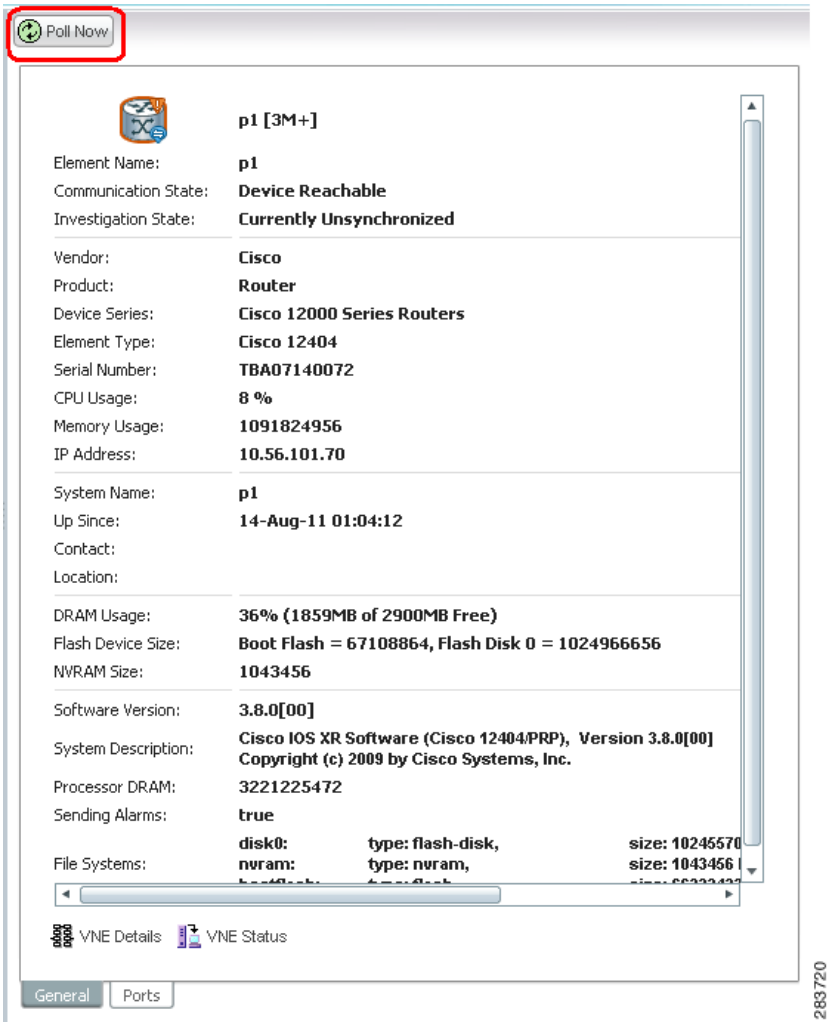
If you need more information about protocols and the tests and settings Prime Network uses to determine reachability, see How Prime Network Determines Protocol Reachability, page 24-3.

Troubleshooting VNE Investigation State (Discovery) Issues

Users with Operator privileges can rediscover complete network elements or individual components within network elements using Prime Network Vision. This is done by right-clicking a device or device component and selecting **Poll Now**.

Rediscovering an entire device can also be done from the Prime Network Administration GUI client by right-clicking a VNE and selecting **Inventory**. Figure 20-5 shows the device inventory window with the Poll Now button at the top left. Although the Poll Now button is provided for use by all VNEs, it is specifically useful for VNEs using reduced polling because it provides a quick way to synchronize the VNE model without having to wait for the next polling cycle.

Figure 20-5 Poll Now Button in Prime Network Device Inventory



The following steps provide an overall procedure for responding to an unexpected VNE investigation state.

Step	Description	See:
1	Verify the current VNE investigation (and communication) states in Prime Network Vision.	Step 1: Check the Investigation State, page 20-16
2	Check the investigation state description in the VNE Status Details window, especially if you are seeing the Currently Unsychronized state. You can optionally check the System event to see if it can provide any new information.	Step 2: Check the VNE Status Details for the Cause of the Modeling Problem, page 20-19

Step	Description	See:
3	If needed, perform these additional steps depending on the information you need: • Verify that all required device configuration tasks have been performed. • Verify that there are no communication state issues. • Change Prime Network so that it generates an elaborated report about state changes. • Get more information to provide to the Cisco Technical Assistance Center.	Step 3: Additional Troubleshooting Steps for Investigation State Problems, page 20-23

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).

Step 1: Check the Investigation State

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

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

Step 2 Check the current Investigation State (as shown in Figure 20-6). The various states are described in Table 20-3, which follows the figure.

Figure 20-6 VNE Investigation State (in Prime Network Vision)

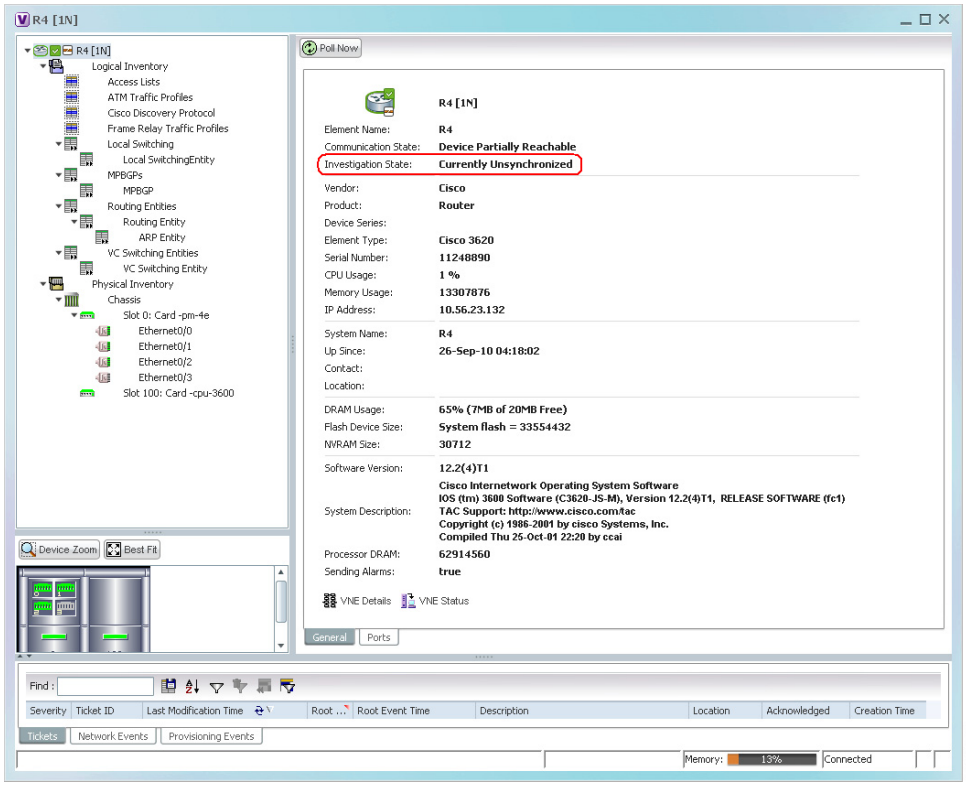


Table 20-3 VNE Investigation States

State Name	Description	Badge
Defined Not Started	A new VNE was created (and is starting); or an existing VNE was stopped. In this state, the VNE is managed and is validating support for the device type. (This investigation state is the equivalent of the Agent Not Loaded communication state.) A VNE remains in this state until it is started (or restarted). In the VNE Status Details window, the description will say **VNE is down**.	None
Unsupported	The device type is either not supported by Prime Network or is misconfigured (it is using the wrong scheme, or is using reduced polling but the device does not support it). See Table 20-4 on page 20-21 for troubleshooting steps.	
Discovering	The VNE is building the model of the device (the device type was found and is supported by Cisco Prime Network). A VNE remains in this state until all device commands are successfully executed at least once, or until there is a discovery timeout. In the VNE Status Details window, the description will say **Initial investigation of the device**. To troubleshoot a VNE that does not move out of this state, perform the following steps: 1. Verify that all required device configuration tasks have been performed. If they were not, Prime Network cannot properly model the device. See Device Configuration Tasks for VNE Creation, page A-1. 2. Verify that there are no communication state issues. See Steps to Troubleshoot VNE Communication State Issues, page 20-3. Also see Troubleshooting VNE Communication State Issues, page 20-1. 3. Verify that the VNE is using the proper scheme. See Choosing a VNE Scheme, page 19-6. 4. Verify that the device is using the proper polling method. See Finding Out Whether a VNE is Using Reduced Polling, page 22-4. The default discovery timeout is 30 minutes but is customizable. To change the timeout, see Registry Settings for VNE Discovery Timeout and Investigation State Reporting, page 20-23.	
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. In the VNE Status Details window, the description will say **Ongoing synchronization with the device.**	None
Currently Unsynchronized	The VNE model is inconsistent with the device. This can be due to a variety of reasons; check the VNE Status Details window can provide more information (see Step 2: Check the VNE Status Details for the Cause of the Modeling Problem, page 20-19).	

Table 20-3 VNE Investigation States (continued)

State Name	Description	Badge
Maintenance	VNE polling was suspended because it was manually moved to this state. In the VNE Status Details window, the description will say **Device synchronization was suspended by user or system**. 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. See Table 20-4 on page 20-21 for troubleshooting steps.	
Shutting Down	The VNE has been stopped or deleted by the user, and the VNE is terminating its connection to the device. The VNE Status Details window, the description will say **Device synchronization aborted**.	
Stopped	The VNE process has terminated; it will immediately move to Defined Not Started.	None

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

Step 1 From the VNE properties window (see Figure 20-6 on page 20-17), click **VNE Status** at the bottom of the properties window to open the VNE Status Details window and check the investigation state information, comparing it against the information in Table 20-4 on page 20-21.

Figure 20-7 Investigation State Information in VNE Status Details Window

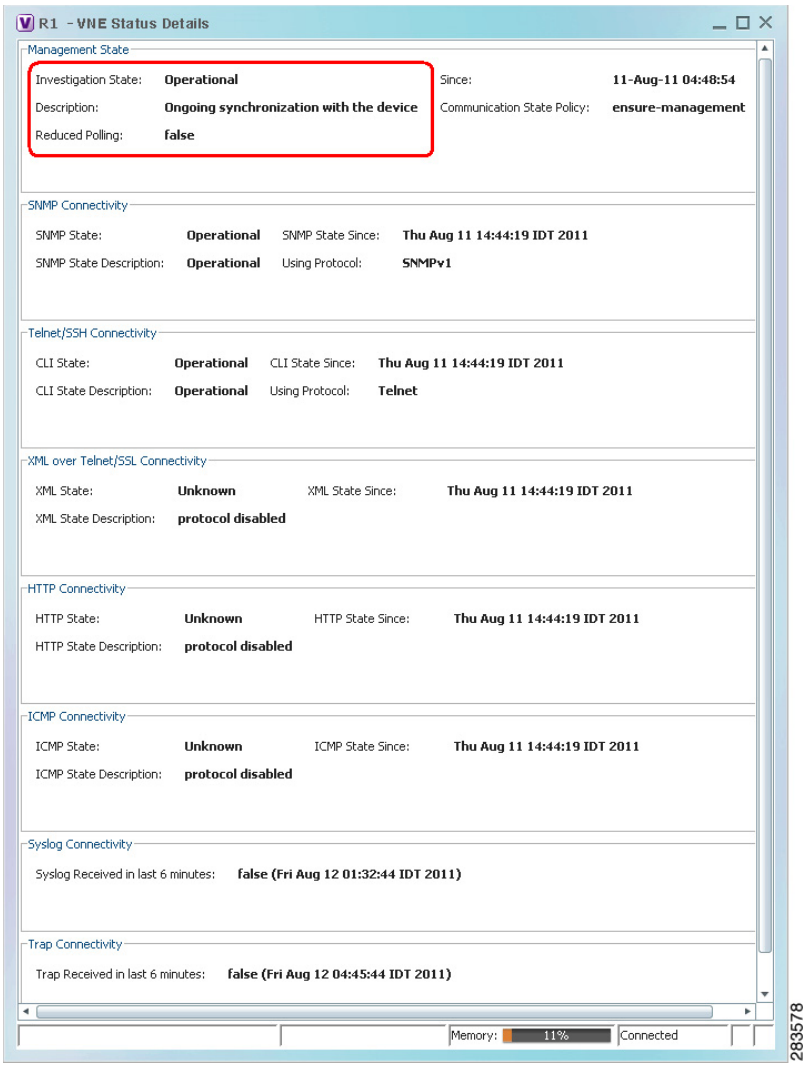


Table 20-4 VNE Investigation State Information (from VNE Status Details Window)

Field	Description	
Management State		
Investigation State	VNE investigation state. Basic descriptions of all of the investigation states is provided in Table 19-2 on page 19-5.	
Description	Cause of the current investigation state. Registry Settings for VNE Discovery Timeout and Investigation State Reporting, page 20-23. The following is a partial list of messages you may see and how to troubleshoot the problem indicated by the message.	
	Unsupported	**VNE cannot synchronize with the device**—The device type is not supported by Cisco Prime Network (no VNE driver was found for the device). Possible causes: • The VNE is using the wrong scheme. Verify the device type against the supported schemes in Table 19-4 on page 19-9. • The VNE is using the reduced polling method, but the VNE does not support that method. To check whether the device type supports reduced polling, use the procedure described in Finding Out Whether a Device Type Supports Reduced Polling, page 22-5. • Check whether the element is supported in a released device package. See What Are Device Packages and Independent VNE Drivers?, page 21-1. If the device type is not supported: – You can add the VNE as Generic VNE or ICMP VNE. These VNE types are specified in the VNE General properties; see Table 19-7 on page 19-24. – You can add the support using the Prime Network VNE Customization Builder. See the *Cisco Prime Network 3.8 Customization User Guide*. 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*.

Table 20-4 VNE Investigation State Information (from VNE Status Details Window) (continued)

Field	Description	
Description (continued)	**Currently Unsynchronized**	The VNE model is inconsistent with the device. This can be due to a variety of reasons: • **User initiated device re-synchronization**—A user clicked **Poll Now** in Cisco Prime Network Vision (or issued a BQL command that performs this operation). • **Resuming synchronization after maintenance**—The VNE is moving out of a user-induced Maintenance state (a user restarted the VNE). • **Device CPU is high. Synchronization temporarily suspended**—The adaptive polling mechanism moved the VNE to this state because the device exceeded its maximum CPU usage threshold. For troubleshooting tips see CPU Utilization Problems: Where to Begin, page 22-2. • **Resuming synchronization after device CPU normalized**—The adaptive polling mechanism is moving the VNE back to its normal polling because device CPU usage has stabilized. • **System initiated device resynchronization due to missed device configuration changes**—The VNE is using reduced polling and has identified a gap in the configuration log (specifically, the configuration archive buffer), or has failed to identify one or more changes. (VNEs using reduced polling are more sensitive to these changes due to their different polling frequency. For more information, see Reduced Polling, page 22-2. • **VNE cannot reach the device, Synchronization temporarily suspended**—The device did not respond in a timely fashion. Follow the troubleshooting steps in Steps to Troubleshoot VNE Communication State Issues, page 20-3. • **Resuming synchronization after device reachability from VNE restored**—The VNE is moving out of an unreachable state. • **Temporarily missing or failed VNE driver component**—A required, recoverable device command failed. Prime Network retries the command at the next polling cycle, up to 3 retries. (If it fails, the VNE is moved to Partially Discovered.) • **Device synchronization was suspended by system**—The system temporarily stopped the synchronization process because it suspects the device was reloaded (this prevents the VNE from collecting irrelevant information). The synchronization process will normally restart within 5 minutes. The Currently Unsynchronized state can also be caused by a communication state issue. See Steps to Troubleshoot VNE Communication State Issues, page 20-3.
	Partially Discovered	**Missing or failed VNE driver component**—Prime Network could not recognize an element in the device. Consider the following troubleshooting options: • Check whether the element is supported in a released device package. See What Are Device Packages and Independent VNE Drivers?, page 21-1. • To extend Cisco Prime Network functionality so that it recognizes unsupported parts of devices, use the VNE Customization Builder. See the *Cisco Prime Network 3.8 Customization User Guide*.

Table 20-4 VNE Investigation State Information (from VNE Status Details Window) (continued)

Field	Description
Reduced Polling	Reports whether VNE is using reduced polling mechanism to control polling (**true**=enabled). Reduced polling means polling is performed only when a poll-worthy event is received from device, thus reducing the overall polling (true if enabled, false if disabled). For information on the reduced polling mechanism, see Reduced Polling, page 22-2.
Since	Timestamp of when the state information was last updated.
For information on the communication state details that are provided in this window, see Table 20-2 on page 20-7.	

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

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

Step 3: Additional Troubleshooting Steps for Investigation State Problems

Step 1 Verify that all required device configuration tasks have been performed. If they were not, Prime Network cannot properly model the device. See Device Configuration Tasks for VNE Creation, page A-1.

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

Step 3 Optionally perform the following tasks:

- Adjust the registry setting so that Prime Network Events generates an elaborated report about state changes. See Table 20-5 on page 20-24.
- Open the device properties window in Prime Network Vision. Place your cursor in the inventory window, and press F2. Click Managed State Aspect and review the information. This information is especially useful when working with the Cisco Technical Assistance Center.

Registry Settings for VNE Discovery Timeout and Investigation State Reporting

Table 20-5 lists registry settings you can change to control the following discovery and state reporting behaviors:

- Whether Prime Network should generate a Service event and long event description when an investigation state changes. This is not done by default because it can affect performance and cause unnecessary concern to operators. (Service events are generated for communication state changes by default.)

- The number of retries for device commands issued during the discovery process, and whether the device command is required.
- Whether Prime Network should use the timeout mechanism or the convergence mechanism to determine when the discovery process is complete. (You can also adjust the length of the discovery timeout.)

Note All changes to the registry should only be carried out with the support of Cisco. For details, contact your Cisco account representative.

Table 20-5 Registry Settings for Discovery and Investigation States

Registry Entry	Description	Default Value
Investigation and Communication State Reporting		
site/agentdefaults/da/investigation-progress/investigation-state-update-event	Generate a Service event (in Prime Network Events) when investigation state changes	false
site/agentdefaults/da/investigation-progress/investigation-state-result-summary-event	Include an elaborated report about the investigation state change in the Long Description field of the Service event	false
Device Commands Used for Discovery		
site/interfacebasedscheme/default registration/error update tolerance	Allowable number of device command failures, after which an error is generated	3
site/interfacebasedscheme/default registration/required	Designate the device command as required for evaluating an investigation state (insert this after the device command key name)	false
VNE Discovery Period Controls		
site/agentdefaults/da/investigation-progress/max-delay-before-managed-state-in-milliseconds	Timeout for VNE discovery process (in milliseconds) (ignored if convergence is being used)	1800000 (30 minutes)
site/agentdefaults/da/investigation-progress/convergence	Use the VNE convergence mechanism to control discovery	false

Opening a Bug Report

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

Before You Open a Bug

1. Verify that the network element, event, script, etc. is supported by checking these documents:
   - *Cisco Prime Network 3.8 Reference Guide*
   - *Addendum: Additional VNE Driver Support for Cisco Prime Network 3.8* (this document is released when the first DP becomes available; see What Are Device Packages and Independent VNE Drivers?, page 21-1.

Note If the device is not supported, you can add the support using the Prime Network VNE Customization Builder. See *Cisco Prime Network 3.8 Customization User Guide*. Also, this guide contains an extended procedure for finding out which traps and syslogs are not supported and how to troubleshoot them.

2. Make sure you have tried all of the troubleshooting steps provided in these topics:
   - Troubleshooting VNE Communication State Issues, page 20-1
   - Steps to Troubleshoot VNE Communication State Issues, page 20-3
   - Troubleshooting VNE Investigation State (Discovery) Issues, page 20-14
3. Provide all of the necessary details for the bug report (reproduce the problem if necessary).

Information You Must Provide

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

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