CHAPTER 6

Managing AVMs and VNEs

This chapter describes defining and managing autonomous virtual machines (AVM) and virtual network elements (VNE).

- Creating AVMs—Describes how to define an AVM for a Cisco ANA unit server.
- AVM Status—Describes the status of AVMs when they are created and loaded.
- Viewing and Editing an AVM's Properties—Describes how to view and edit an AVM's properties.
- Deleting an AVM—Describes how to delete AVMs.
- Starting and Stopping AVMs—Describes how to stop and start AVMs, and the changes in AVM status.
- Moving AVMs—Describes how to manage AVMs before you move them, and their status after a move.
- Finding an AVM or VNE—Describes how to locate AVMs and VNEs among all Cisco ANA Servers.
- Overview Of VNEs—Provides an overview of assigning VNE IP addresses, the VNE relationship to an AVM, and how to add a VNE to an AVM.
- Defining VNEs—Describes how to open the New VNE dialog box and provides a description of property options you may define in each tab.
- Viewing and Editing a VNE's Properties—Describes how to view and edit the properties of a VNE.
- Deleting a VNE—Describes how to delete a VNE from an AVM.
- Changing the VNE's State—Describes how to start or stop a VNE or move a VNE to maintenance mode.
- Moving Multiple and Single VNEs—Describes how to move VNEs between AVMs.

Creating AVMs

Cisco ANA Manage enables the user to define AVMs for Cisco ANA unit servers. Every AVM in the Cisco ANA fabric is by default managed by the watchdog protocol. Cisco ANA Manage enables the administrator to define AVMs for units, and enable or disable the watchdog protocol on the AVM.

In order to define an AVM:

- The unit must be installed.
- The unit must be connected to the transport network.
- The default AVMs (AVM 0 (the switch AVM); AVM 99 (the management AVM); AVM 100 (the trap management AVM)) must be running.

Note For more information on the status of AVMs, see AVM Status, page 6-3.

- The new AVM must have a unique ID within the unit.

Note AVM ID numbers 0-100 are reserved, and cannot be used. In addition, there may be other reserved AVM ID numbers. The user will be unable to enter a reserved number.

To create an AVM:

Step 1 Select the ANA Servers branch in the Cisco ANA Manage window's tree pane.

Step 2 Expand the ANA Servers branch and select the required ANA Servers Entity sub-branch.

Step 3 Right-click on the required unit to display the menu and choose **New AVM**, or on the toolbar click **New AVM**, or from the File menu, choose **New AVM**. The New AVM dialog box is displayed.

The following fields are displayed in the New AVM dialog box:

- **ANA Unit—**The IP address of the selected unit.

Note The unit does not have to be **Up** to create a new AVM.

- **ID—**The name of the AVM as defined in Cisco ANA Manage, and unique to the unit, for example, AVM 18.

Note The AVM numbers 0-100 are reserved and cannot be used. The user will be unable to enter a reserved number. A message is displayed in the New AVM dialog box informing the user that the number is reserved.

- **Key—**The key is a string that uniquely identifies an AVM in the system, across all units, thus enabling a transparent failover scenario in the system. If the user does not enter a key the default key is used, "ID + timestamp".
- **Allocated Memory—**The maximum memory allocated to the AVM.

The following checkboxes are displayed in the New AVM dialog box:

- **Activate on creation—**Loads the AVM into the bootstrap of the unit. This changes the administrative status of the AVM to **Up** and ensures that the AVM is loaded on subsequent restarts of the unit. By default this option is unchecked, and the newly created AVM has an administrative status of **Down**.
- **Enable AVM Protection—**By default this option is selected enabling the watchdog protocol on the AVM when high availability is enabled. For more information, refer to the *Cisco Active Network Abstraction High Availability User Guide*.

Note It is highly recommended that the user does not disable this option if high availability is enabled.
If this option is selected or unchecked when the AVM is up then you will need to restart the AVM in order for this change to take affect.

Step 4 Define the properties of the AVM.

Step 5 Click **OK**. The new AVM is added to the selected unit, is displayed in the workspace, and is activated.

Creating the new AVM results in Cisco ANA providing the registry information of the new AVM in the specified unit. The AVM can now host VNEs. For more information, see Defining VNEs, page 6-9.

AVM Status

The status of AVMs and VNEs is affected by Admin and Oper modes. Admin mode is the administrative instructions that are sent to the AVM. Oper mode is the actual status of the AVM, for example, Up. See Admin and Oper Mode AVM Status, page 6-3.

When moving an AVM (file), its status, for example, Up or Down, has a bearing on whether the file is reloaded (Up) or not (Down). For more information about moving AVMs, see Moving AVMs, page 6-6. For more information about starting and stopping AVMs, see Starting and Stopping AVMs, page 6-5.

An AVM can have only one of the following statuses at a time:

- **Up—**The file (process) is reachable, and was loaded and started. When a **Start** (command) option is issued, and no problems are encountered, such as an overloaded server, the AVM is running (has been loaded and started), and its status is **Up**.
- **Down—**The file (process) is reachable, and was stopped. When a **Stop** (command) option is issued, Cisco ANA issues instructions to shutdown all the processes. When all the processes have been stopped, the status of the AVM is **Down**.
- **Starting Up—**When a **Start** or upload (command) option is issued, and for example, the server cannot run it as it is busy or overloaded, the status of the AVM is **Starting Up**.
- **Shutting Down—**When a **Stop** (command) option is issued, and while the command is being run (some processes may still be running), the status of the AVM is **Shutting Down**.

Admin and Oper Mode AVM Status

The AVM status table describes the status of an AVM depending on the Admin and Oper modes, as displayed in the **Status** column of the AVMs table. The Admin mode is the administrative instructions that are sent to the VNE. The Oper mode is the actual status of the VNE, for example, Up.

Table 6-1 AVM Status

Status	Admin Mode	Oper Mode
Up	Up	Up
Shutting Down	Down	Up

Table 6-1 AVM Status (continued)

Status	Admin Mode	Oper Mode
Down	Down	Down
Starting Up	Up	Down

Viewing and Editing an AVM's Properties

Cisco ANA Manage enables the user to view and edit the properties of an AVM, for example, the key, and the allocated memory.

To view and edit an AVM's properties:

Step 1 Select the ANA Servers branch in the Cisco ANA Manage window's tree pane.

Step 2 Expand the ANA Servers branch and choose the required AVM sub-branch in the tree pane.

Step 3 Right-click to display the shortcut menu and choose **Properties**, or from the File menu, choose **Properties**, or on the toolbar click **Properties**.

The AVM Properties dialog box is displayed with the details of the selected AVM, including the IP address or key of the unit.

The following field is displayed in the AVM Properties dialog box:

- **Status—**The status of the AVM, namely, Up, Down, or Unreachable. See Admin and Oper Mode AVM Status, page 6-3.

Step 4 Edit the details of the AVM as required.

Note For more information on the other fields displayed in the AVM Properties dialog box, see Creating AVMs, page 6-1.

Step 5 Click **OK**. The AVM's new properties are displayed in the workspace.

Deleting an AVM

The user can remove an AVM. If the AVM is running it will be stopped before removal. This procedure deletes the registry information of the AVM in the specified unit. If there are VNEs running in the AVM, then an error message will be displayed, and the user will be unable to delete the AVM.

Warning **You must remove all the VNEs before removing their hosting AVM.**

For more information, see Deleting a VNE, page 6-27.

Note Reserved AVMs 0-100 cannot be deleted.

To delete an AVM:

Step 1 Select the ANA Servers branch in the Cisco ANA Manage window's tree pane.

Step 2 Expand the ANA Servers branch, and select the required AVM sub-branch in the tree pane.

Step 3 Right-click to display the menu and select **Delete**. A warning message is displayed.

Step 4 Click **Yes**. A confirmation message is displayed.

Step 5 Click **OK**. The selected AVM is deleted from the selected unit.

Note Multiple rows can be selected for deletion.

Starting and Stopping AVMs

Cisco ANA Manage enables the user to start or stop an AVM.

Note Stopping the AVM process stops all the VNEs in the AVM. You should be aware that any change in status of the AVMs may take some time to be applied. For example, when running the **Stop** command, it may take several minutes before the status changes from **Shutting Down** to **Down**.

To start or stop an AVM:

Step 1 Select the ANA Servers branch in the Cisco ANA Manage window's tree pane.

Step 2 Expand the ANA Servers branch, and select the required AVM sub-branch.

Step 3 Right-click to display the shortcut menu and select **Actions | Start** or **Actions | Stop**, or on the toolbar click **Start** or **Stop**.

The AVM is started or stopped, and the appropriate status is displayed in the workspace as follows:

- **Starting Up—**An AVM is started.
- **Up**—The AVM has started.
- **Shutting Down—**The AVM is stopped.
- **Down**—The AVM has stopped.

Note When the AVM status is displayed as **Down**, the status remains **Down** and no-reload will occur.

Moving AVMs

Cisco ANA Manage enables the administrator to move an entire AVM between units.

Note Reserved AVMs 0-100 cannot be moved.

Cisco ANA Manage automatically checks the status of the AVM and VNE before it is moved. This information is maintained in the memory.

If the AVM is **Up** it is stopped, and then it is moved to the target unit. After the move is completed, the AVM is reloaded according to its status prior to the move, namely, the status of the AVM as it was before the move is maintained. For example, if it was **Up** before the move it will remain **Up**, if it was **Down** it will remain **Down**.

To move an AVM:

Step 1 Select the ANA Servers branch in the Cisco ANA Manage window.

Step 2 Expand the ANA Servers branch and select the required AVM sub-branch.

Step 3 Right-click to display the menu and select **Move AVM**. The Move To dialog box is displayed.

The Move To dialog box displays a tree-and-branch representation of the selected Cisco ANA server and its units, excluding the unit in which the AVM is currently located. The highest level of the tree displays the Cisco ANA server. The branches can be expanded and collapsed in order to display and hide information.

Step 4 Browse to and select the unit (branch) where you want to move the AVMs.

Step 5 Click **OK**. The AVMs is moved and now appears beneath the selected unit.

For information about moving VNEs, see Moving Multiple and Single VNEs, page 6-29.

Finding an AVM or VNE

A single search in Cisco ANA Manage can locate AVMs and VNEs among all Cisco ANA servers according to specifically defined search criteria.

To find an AVM or VNE:

Step 1 In the Cisco ANA Manage window tree pane, select the unit sub-branch or any sub-branch.

Step 2 Click **Find**. The Find dialog box is displayed.

The **Find** field enables the user to enter specific search criteria in order to find the required AVM or VNE. For example, the user can search for an AVM using the ID number, or search for a VNE using an IP address.

The **Types** list enables the user to specify whether the user is searching for an AVM or VNE by selecting an option from the list. When an option is selected from the list, then the **Property** area is enabled, displaying the properties for the selected option. For example, if AVM is selected from the **Types** list, then the AVM's properties are displayed in the **Property** area, and the user can select a specific property for the search.

The **Up** and **Down** radio buttons enable the user to search up and down (you can also use the F3 key).

The following buttons are displayed in the Find dialog box:

- **Find—**Searches for the AVM or VNE from the selected point in the tree pane, either up or down.
- **Cancel—**Cancels the search, and clears the Find dialog box.

Step 3 Enter the search criteria in the **Find** field.

When searching for an AVM the following search criteria are displayed:

- ID
- Status
- Key
- Loaded patches

When searching for a VNE the following search criteria are displayed:

- Key
- IP address
- Status
- Element type
- Maintenance
- Polling group

Step 4 From the **Types** dropdown list select AVM or VNE (optional).

Step 5 From the **Property** area select a specific property (optional).

Step 6 Select a direction, namely, **Up** or **Down**.

Step 7 Click **Find**. The AVM or VNE matching the search criteria is highlighted in Cisco ANA Manage.

Note Click **F3** to view the next AVM or VNE matching the search criteria.

Overview Of VNEs

A VNE is designated by its leading IP address and corresponds to a single network element (NE). Typically an NE has only one IP address that is used for management. For such devices, the leading IP address is the single IP address configured for this device.

In cases where an NE has multiple IP addresses, the user must choose one of these IP addresses to be used as a leading IP address. The leading IP address serves as an identifier of the VNE that corresponds to the NE and is displayed wherever the IP address of the NE is required.

Note Two VNEs cannot monitor the same NE.

Cisco ANA Manage enables the user to create VNEs (replicas of devices), for example, by entering the IP address, SNMP and polling rate information and so on. This is called Element Management.

After Cisco ANA Manage installs and runs the process, samples the device and collects the data, a VNE (managed element) is created. The VNE includes tables and physical inventory, and this managed element can be accessed using Cisco ANA NetworkVision.

VNE Status

The status of VNEs is affected by the Admin and Oper modes. Admin mode is the administrative instructions that are sent to the VNE. Oper mode is the actual status of the VNE, for example, Up. For more information about Admin and Oper modes, see Admin and Oper Mode VNE Status, page 6-9.

When moving a VNE, its status, for example, Up or Down, has a bearing on whether the VNE is reloaded (Up) or not (Down). For more information about moving VNEs, see Moving Multiple and Single VNEs, page 6-29. For more information about starting and stopping VNEs, see Changing the VNE's State, page 6-28.

A VNE can have only one of the following statuses at a time:

- **Up—**The VNE (process) is reachable, and was loaded and started. When a **Start** (command) option is issued, and no problems are encountered, such as an overloaded server, the VNE is running (has been loaded and started), and its status is **Up**.
- **Down—**The VNE (process) is reachable and was stopped. When a **Stop** (command) option is issued, Cisco ANA issues instructions to shutdown all the processes. When all the processes have been stopped, the status of the VNE is **Down**.
- **Unreachable—**The VNE cannot be managed by Cisco ANA and its status is defined as Unreachable. When an option (command) is issued that cannot be run by Cisco ANA, the status of the VNE is **Unreachable**.
- **Starting Up—**When a **Start** or upload (command) option is issued, and for example, when the server cannot run it due to the fact that it is busy or overloaded, the status of the VNE is **Starting Up**.
- **Shutting Down—**When a **Stop** (command) option is issued, and while the command is being run (some processes may still be running), the status of the VNE is **Shutting Down**.

In addition to the statuses described, the VNE can be placed in maintenance mode, for example, a VNE's status can be **Up** and in maintenance mode. NEs often undergo maintenance operations and planned outages. The Cisco ANA platform supports such maintenance operations without affecting the overall functionality of the active network.

While in maintenance mode (temporary state) a VNE:

- Does not change state on its own, unless the user explicitly (manually) switches the VNE back to active state.
- Never polls the device.
- Is capable of sending alarms, but it does not poll the device, and therefore service alarms are not supposed to be sent, except for those that are negotiated between adjacent ports, for example, a link-down alarm is still sent. Syslogs and traps are sent, and the flows are active.
- Maintains any existing links.
- Does not fail on verification requests.

For more information about maintenance mode, see Changing the VNE's State, page 6-28.

Admin and Oper Mode VNE Status

The VNE status table describes the status of a VNE depending on the Admin and Oper modes, as displayed in the Status column of the VNE table. The Admin mode is the administrative instructions that are sent to the VNE. The Oper mode is the actual status of the VNE, for example, Up.

Table 6-2 VNE Status

Status	Admin Mode	Oper Mode
Up	Up	Up
Shutting Down	Down	Up
Down	Down	Down
Starting Up	Up	Down
Unreachable	Up	Unreachable

For example, if the user starts the VNE, the Admin status is **Up** but the Oper status is **Down** and has not started yet (because the server is busy), the status is **Starting Up**. If the VNE is **Up** and running and the user stops the VNE, the Admin status is **Down** but the process is not terminated immediately, the status is **Shutting Down**.

Defining VNEs

When the user adds and defines a new VNE, it corresponds to an NE and should only be added to the system once. As the VNE loads, Cisco ANA starts investigating the NE and automatically builds a live model of it, including its physical and logical inventory, its configuration, and its status.

When adding a new VNE, Cisco ANA creates the registry information of the new VNE in the unit. The newly created VNE has an administrative status of Down, and uses the default community strings and polling rates. The VNE inherits these properties from the configuration record that corresponds to the device type.

A VNE must be loaded into the bootstrap of the unit before it starts monitoring its underlying NE. This changes the administrative status of the VNE to Up, and ensures that the VNE is loaded on subsequent restarts of the unit. Loading the VNE also starts the VNE immediately. For more information about the status of VNEs, see Admin and Oper Mode VNE Status, page 6-9.

Before adding a new VNE using Cisco ANA Manage, the user must first determine which unit and AVM the new VNE should be added to.

The user can define and manage SNMP, Telnet/SHH, ICMP, and polling information for the appropriate VNEs in the New VNE dialog box.

Note A new VNE cannot be added to the reserved AVMs 0-100.

The user can create VNEs that perform reachability testing only through ICMP. This can be done by creating the VNE, selecting the type ICMP, and then defining the details in the ICMP tab. See ICMP Tab, page 6-21.

For information on defining VNE properties in the respective VNE tabs, refer to the following:

- General Tab, page 6-12
- SNMP Tab, page 6-13
- Telnet/SSH Tab, page 6-16
- SSHv2 Protocol, page 6-18
- ICMP Tab, page 6-21
- Polling Tab, page 6-23

For details on viewing and editing VNE properties,
see Viewing and Editing a VNE's Properties, page 6-26.

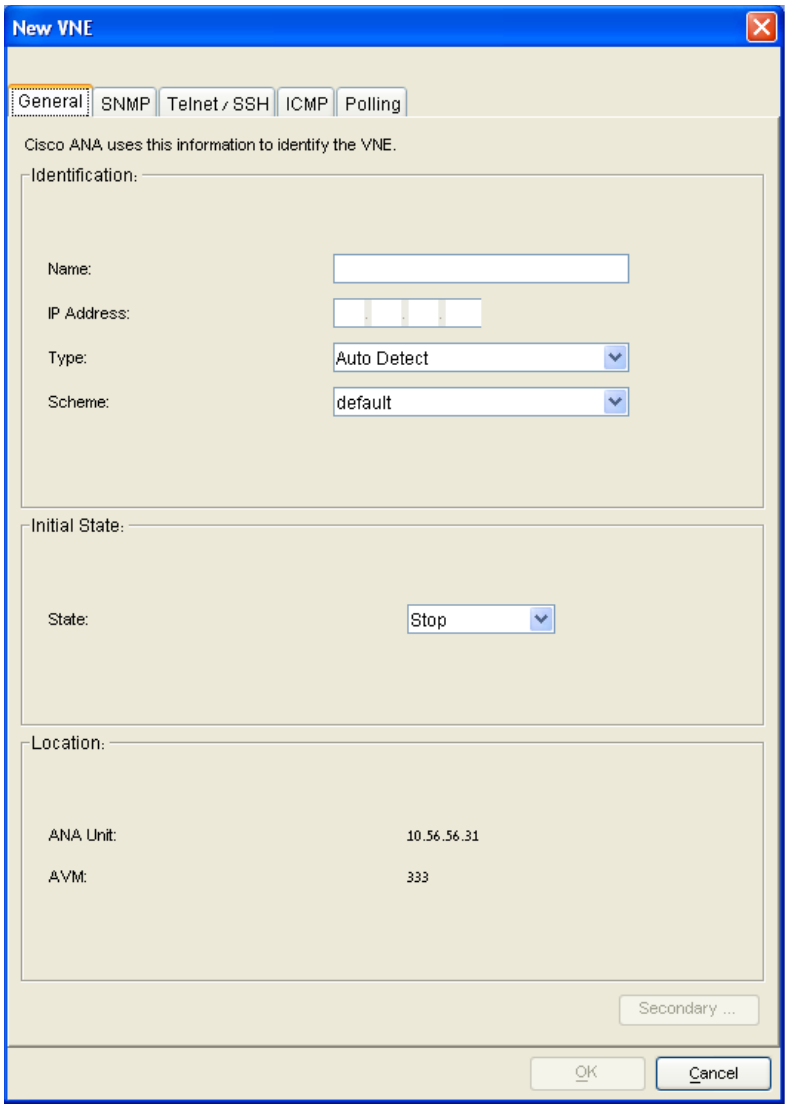
To define the properties of a new VNE:

Step 1 Select the ANA Servers branch in the Cisco ANA Manage window's tree pane.

Step 2 Select the required AVM sub-branch in the tree pane.

Step 3 Right-click in the tree pane to display the shortcut menu and choose **New VNE**, or from the File menu, choose **New VNE**, or on the toolbar, click **New VNE**. The New VNE dialog box is displayed.

Figure 6-1 New VNE Dialog Box



The New VNE dialog box contains the following tabs:

- General Tab—Used to manage VNE information in the connected Cisco ANA (mandatory name and IP fields).
- SNMP Tab—Used to support polling and accessing devices using SNMPv1, SNMPv2c and SNMPv3.
- Telnet/SSH Tab—Used to choose Telnet or SSH for device access and configure the login sequence.
- ICMP Tab—Used to verify that devices are reachable by sending repetitive ICMP request packets, and testing reachability by defining the polling rate.
- Polling Tab—Used to associate a VNE in the Cisco ANA with a polling group, or define an instance.

Note The **OK** button in the New VNE dialog box is enabled only when the user has typed in the VNE name and IP address in the General tab (Mandatory Fields).

General Tab

The **General** tab enables the user to manage VNE information in the connected Cisco ANA.

The following VNE identification fields are displayed in the Identification area:

- **VNE Name—**The name of the VNE that is used as a unique key in NetworkVision, Cisco ANA Manage, and EventVision.

  Note This name is also used for VNE manipulation commands.

- **IP Address—**The IP address of the device.
- **Type—**Select the VNE Type from the list:
  - **Auto Detect—**Automatically detects the device type and loads the relevant VNE.

    Note SNMP cannot be disabled if the **AutoDetect** option is selected.
    See SNMP Tab, page 6-13.

  - **Generic SNMP**—Loads a generic VNE. For more information about defining a generic VNE, see Defining a Generic SNMP VNE, page 6-25.
  - **Cloud—**Loads an unmanaged network segment. Specific cloud configuration is provided on a per project basis.
  - **ICMP—**The VNE uses this ICMP-based reachability test to validate communication with the managed device by continuously sending ICMP packets.

    Note When this option is selected the ICMP tab is enabled (the SNMP, Telnet/SSH and Polling tabs are disabled).

- **Scheme—**Defines the VNE modeling components investigated during the discovery process. This enables the administrator to define different behavior for some devices, for example, some devices poll only with SNMP, other devices poll with Telnet. Soft properties and activation scripts are also attached to a specific scheme. Two schemes are currently available, namely, **default** and **product**. 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.

Note It is recommended that the user select the **product** scheme.

The following VNE state fields are displayed in the initial state area:

- **State—**The initial state of the VNE:
  - **Stop—**The VNE is not loaded. This is the default state.
  - **Start—**The VNE is loaded and starts collecting data.
  - **Maintenance—**The VNE is started and moved to maintenance mode. See VNE Status, page 6-8.

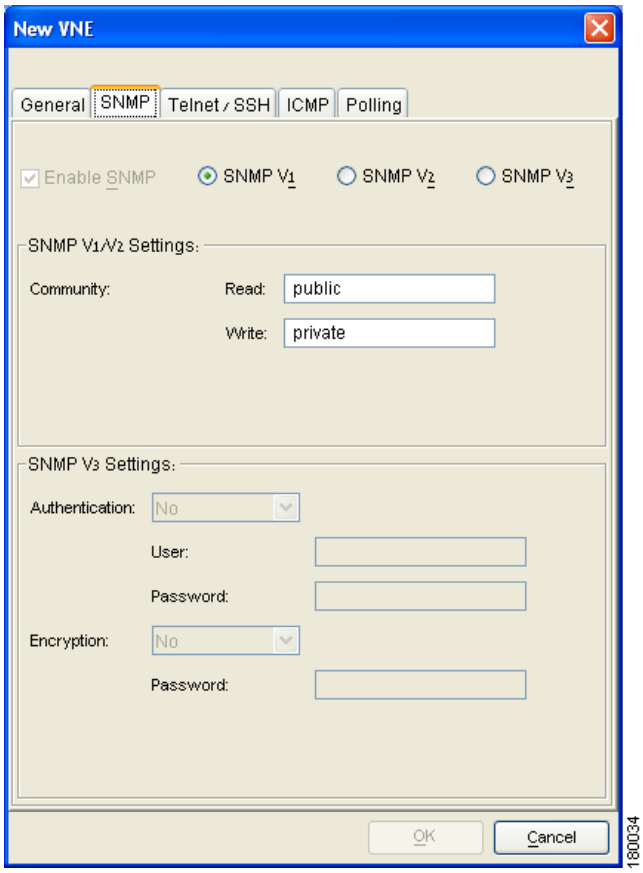
The following fields are displayed in the Location area of the General tab:

- **ANA Unit—**The IP address of the unit that hosts the VNE's AVM.
- **AVM—**The AVM on the unit that hosts the VNE.

SNMP Tab

The SNMP tab enables the user to support polling and accessing devices using SNMPv1, SNMPv2 and SNMPv3. Selecting the SNMP tab displays the following dialog box:

Figure 6-2 SNMP Tab



The following checkbox and radio buttons are displayed in the SNMP tab of the New VNE dialog box:

- **Enable SNMP—**Check this option to enable the SNMP communication protocol so that the user can work with it.

Note A VNE can be SNMP enabled or disabled at any time, however, when the Auto Detect option is selected in the General tab, it cannot be disabled. (For more information, see General Tab, page 6-12).

- **SNMP V1—**Select SNMP version 1
- **SNMP V2—**Select SNMP version 2
- **SNMP V3—**Select SNMP version 3

Note The SNMP V3 settings area is only enabled when SNMP V3 is selected.

The following fields are displayed in the SNMP V1/V2 Settings area:

- **Read—**The SNMP Read Community status, Public or Private, as defined by the user.
- **Write—**The SNMP Write Community status, Public or Private, as defined by the user.

Note The SNMP V3 Settings area is only enabled when SNMP V3 is selected.

The following fields are displayed in the SNMP V3 settings area:

- **Authentication—**Select one of the following:
  - **No—**No authentication is required.
  - md5
  - sha

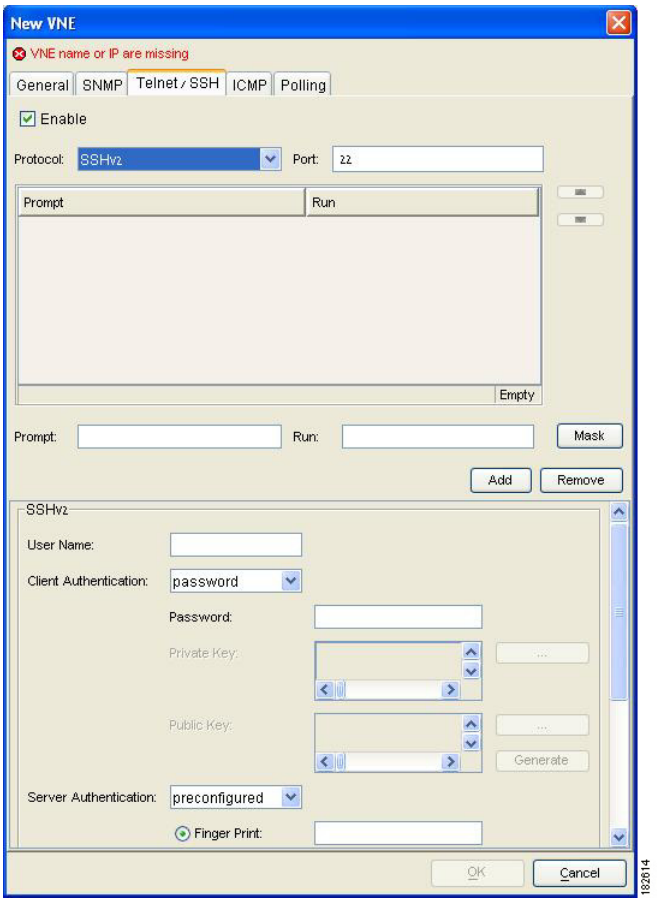
  If MD5 or SHA is selected, enter the required information in the following fields:
  - User
  - Password
- **Encryption—**Select one of the following:
  - **No**—No encryption is required.
  - DES
  - AES-128
  - AES-192
  - AES-256

  If one of the security options is selected, enter the required information in the following field:
  - Password

Telnet/SSH Tab

The Telnet/SSH tab enables the user to define the Telnet command sequence and support SSH for device access (reachability) and investigation. See SSHv2 Protocol, page 6-18 for more information about the SSH protocol. Selecting the Telnet/SSH tab displays the following tabbed dialog box:

Figure 6-3 Telnet/SSH Tab



Note The fields in the lower part of the Telnet/SSH tab change according to the selected protocol. If Telnet is chosen, the lower part of the tab will be empty. If SSHv1 or SSHv2 is chosen then the related fields will be displayed.

There is no more enable/disable of fields.

The following checkbox is displayed in the Telnet/SSH tab of the New VNE dialog box:

- **Enable—**Check this option to enable the Telnet/SSHv1/SSHv2 communication protocol to be used by the VNE to investigate the reachability of the device by activating the **Prompt** and **Run** fields, and the **Add** and **Remove** buttons.

Note A VNE can be Telnet/SSH enabled or disabled at any time.

The following fields are displayed in the Telnet/SSH tab of the New VNE dialog box:

- **Protocol—**A dropdown list of the available protocols, namely:
  - **Telnet—**By default this option is set to Telnet. When Telnet is selected the port field automatically displays 23.
  - **SSHv1—**When SSHv1 is selected the port field automatically displays 22. In addition, the SSH information fields are enabled in the tabbed dialog box.
  - **SSHv2—**When SSHv2 is selected the port field automatically displays 22. In addition, the SSH information fields are enabled in the tabbed dialog box.
- **Port—**When Telnet is selected this field automatically displays 23. When SSHv1 is selected this field automatically displays 22. You can edit the port number displayed.

  Device credentials in the GUI can be masked with asterisks. Click **Mask**. A Password Controller window opens, enter the password and confirm it. An error message is shown if one of the fields is missing, or the password and confirm strings are not identical. Click **OK**. The Password Controller window closes, and the password is inserted in the Run text field as asterisks. The Run text field will stay masked until you add the prompt to the sequence.

  If you do not click Mask, the password is entered as regular text.

  The Run column in theTelnet sequence table displays the data in regular text or as asterisks depending on the chosen option.
- **Prompt—**The expected Telnet/SSH string. This information is displayed in the table (in the relevant column) after clicking **Add**.
- **Run—**The Telnet/SSH string to be sent to the device when the expected prompt is detected. This information is displayed in the table (in the relevant column) after clicking **Add**.

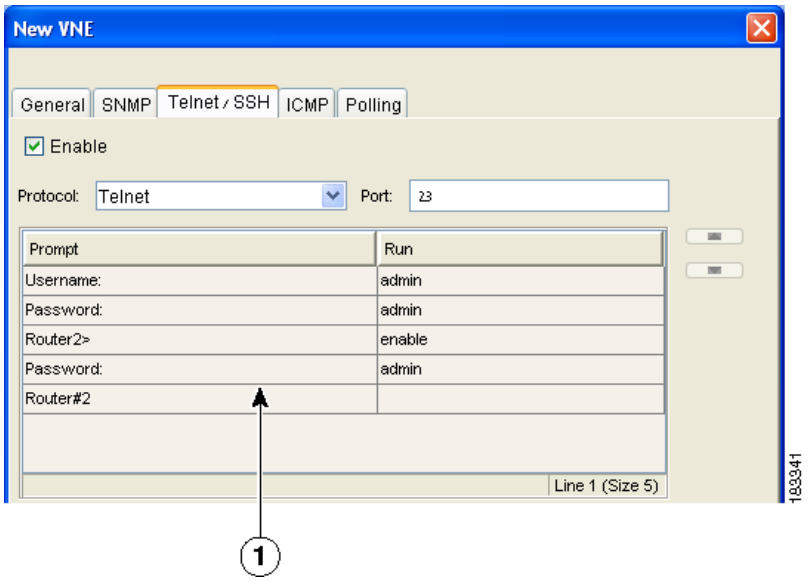
The following buttons are displayed in the Telnet/SSH tab of the New VNE dialog box:

- **Add—**Adds the Prompt and Run fields to the list in the table.
- **Remove—**Removes the selected row from the list in the table.

Use the Up and Down arrows to change the order of the commands in the list.

Note The Telnet sequence (the order of the commands) must end with a line that includes only the prompt field.

Figure 6-4 Telnet Sequence Ending With Prompt Field



SSHv1 Protocol

If the SSHv1 protocol is selected, enter the required information and properties in the following fields:

- Username
- Password
- **Cipher—**Cisco ANA supports polling devices using the SSH protocol, which defines a set of encryption algorithms that may be used to encrypt data. This field provides a list of the available cipher options, namely, 3DES (default), DES, AES-128, AES-192, AES-256 and Blowfish.
- **Authentication—**Displays the Password option.

SSH Login Sequence

After an SSH session is established between the VNE and the device, the VNE will start the login sequence. This sequence is usually shorter than the corresponding Telnet login sequence, as the user name and/or the password may already be sent as part of establishing the SSH session.

It is recommended to first use any SSH client application, for example unix-ssh or openSSH, to see what is the device valid SSH login sequence and then fill the sequence into the VNE configuration.

SSHv2 Protocol

Secure Shell (SSH) is a protocol that provides a secure session using standard cryptographic mechanisms.

SSH Login Sequence

For information on the SSH login sequence see SSH Login Sequence.

Client-Authentication

You need to enter your username and either a password or a private key according to the configured authentication option on the device.

Public key client authentication 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.

You must enter a private key. You can copy and paste it, or upload it from a file, click **Browse for file ...**.

Entering the matching public key is optional. If it is completed, the application will verify that the public and private key are a part of the pair. You may also click **Generate** to generate the matching public key using the private key information.

Supported Algorithms

At least one algorithm must be selected in each subject (key-exchange, MAC, cipher, host-key). 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.

Note Encryption algorithms may have multiple known versions, for example 3DES has: 3des-cbc, 3des-ecb, 3des-cfb, 3des-ofb, 3des-ctr.

Cisco ANA supports the algorithms which are commonly used in network devices as follows:

- MAC:
  - HMAC-SHA-1
  - HMAC-MD5
  - HMAC-SHA1-96
  - HMAC-MD5-96
- Cipher:
  - 3DES-CBC
  - AES128-CBC
  - AES192-CBC
  - AES256-CBC
- Host key algorithm (upto 2048-bit keys officially supported):
  - DSA
  - RSA
- Key Exchange:
  - diffie-hellman-group1-sha1
  - diffie-hellman-group1-exchange-sha1

Server Authentication

Most of the devices which support SSH have a means of identifying themselves to the clients, so the clients are sure that the server is not an imposter.

The server will have a permanent server public key and it will pass it in each session negotiation. The client will compare this public key to the known public key of the server. If they match, the client can be sure of the authenticity of the server.

There are several methods that the VNE supports to do this authentication:

- none—The server identity is never verified. Note that this method does not do any authentication and is not recommended as it poses a security risk for "man-in-the-middle" attacks.
- save-first-auth—On the first connection attempt with the server, the connection will be established and the public key will be saved.

  For all the later connections, authentication will be done against the data saved in the first connection. This method assumes the first connection was legitimate and compares all later connections to it . Note that a security risk still exists if the first connection was compromised.

  After the first connection, this option will automatically be changed into "pre-configured" and the public key data of the session will be inserted as the pre-configured data.
- pre-configured—The server public key or fingerprint is configured in the application event before the first connection was attempted.

  If the server fails to authenticate itself using the pre-configured data, the connection will fail. This is the default behaviour and is the recommended security option.

  The pre-configured data can be of one of two types:

  - Public key for server public key in one of the permitted formats. See Public Key and Private Key File Formats.
  - Fingerprint—Short checksum of the server public key. Serves the same purpose, but is much shorter.

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 which format 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 will 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 `show crypto key mypubkey ...`. 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 using a script.

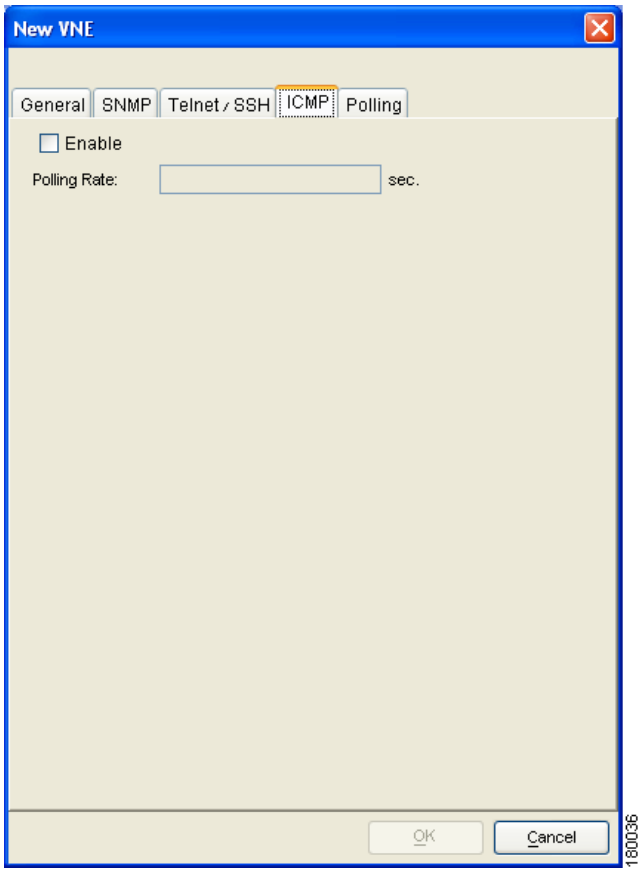
Examples of Valid File Formats

```
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
```

ICMP Tab

The ICMP tab enables repetitive sending of packets to a device to verify that the device is reachable. The user can define the polling rate in seconds for the VNE. Select the ICMP tab to display the ICMP tab in the New VNE dialog box.

Figure 6-5 ICMP Tab



The following checkbox is displayed in the ICMP tab of the New VNE dialog box:

- **Enable—**Check this option to enable the use of the ICMP communication protocol to verify that the device is reachable.

Note The ICMP enable option can be enabled or disabled at any time. If this option is enabled, the user must type in a polling rate in seconds.

Polling Tab

When customizing polling rates, special consideration should be given to the following:

- Fast polling rates (30 sec) provide high data accuracy
- Fast change tracking (VC table, profile changes) and accurate flows

or

- Constant polling generating high NE CPU utilization, high network traffic, polling overlaps, and starvation for scheduled polling
- Slow polling rates (30 min) will affect data accuracy
- Slow change tracking, stuck flows, invalid information

or

- Low NE and network utilization, complete polling cycles

Warning **Changing polling rates may result in excess traffic and cause the NE to crash.**

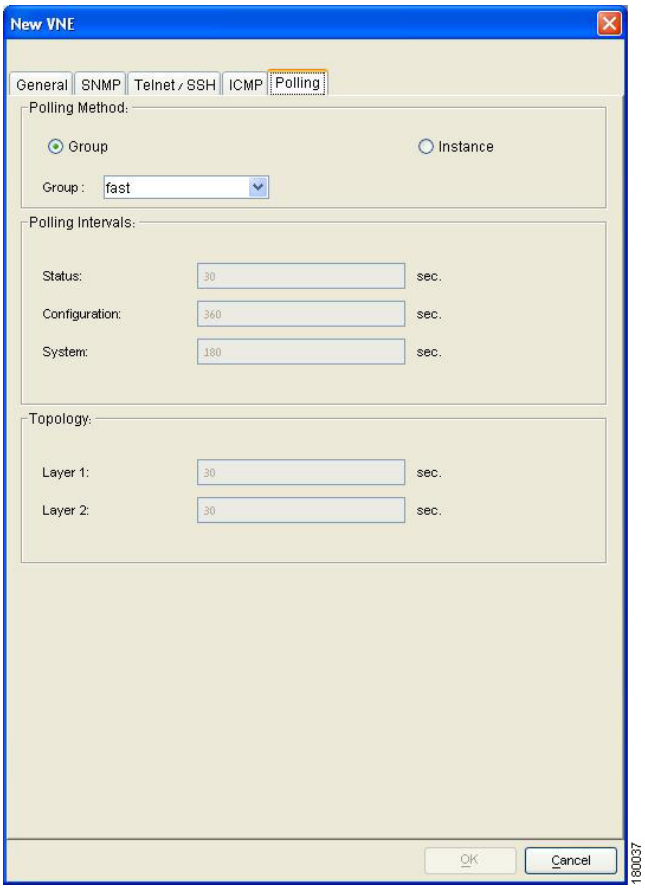
The Polling tab enables the administrator to:

- Associate a VNE with a previously created polling group.
- Customize polling intervals for a VNE. Different polling intervals can be defined:
  - **Status—**Typically the most frequently polled information reflecting the current operational state of the element and its components.
  - **Configuration—**Reflects more dynamic element configuration such as forwarding, routing and switching tables.
  - **System—**Reflects element configuration that is less dynamic in nature.
  - **Topology—**Reflects topology connections at different layers.

In addition, a polling interval can be configured for a class of devices, for example, for all Cisco routers.

Select the Polling tab to display the following dialog box:

Figure 6-6 Polling Tab



The following radio buttons are displayed in the Polling Method area:

- **Group—**The VNE inherits the polling rates from the polling group selected in the list. By default, the VNE inherits the polling rates from the default polling group.

  For more information about creating customized polling groups, see Chapter 7, "Managing Global Settings".

  Note The Polling Intervals and Topology areas are disabled when Group is selected.

- **Instance—**Enables the user to change the polling rates of any one of the built-in polling intervals currently displayed in the dialog box tab.

  Note A polling rate that is not changed inherits its settings from the group specified in the Group dropdown list.

  Note The Polling Intervals and Topology areas are enabled when Instance is selected.

The following polling interval fields are displayed in the Polling Intervals area:

- **Status—**Sets the polling rate for status-related information, such as device status (up or down), port status, admin status and so on. The information is related to the operational and administrative status of the NE. The default setting is 60 seconds.
- **Configuration—**Sets the polling rate for configuration-related information, such as VC tables, scrambling and so on. The default setting is 360 seconds.
- **System—**Sets the polling rate for system-related information, such as device name, device location and so on. The default setting is 900 seconds.

The following fields are displayed in the Topology area:

- **Layer 1—**Sets the polling rate of the topology process as an interval for the Layer 1 counter. This is an ongoing process. The default setting is 60 seconds.
- **Layer 2—**Sets the polling rate of the topology process as an interval for the Layer 2 counter. This process is available on demand. The default setting is 60 seconds.

Defining a Generic SNMP VNE

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

The generic VNE provides basic management capabilities for a device with the following technologies:

- IP
- Ethernet switching
- 802.q

Note IP support is restricted to basic IP only. It does not does include modeling of IPsec, MPLS and routing protocols.

The generic SNMP VNE supports the following inventory items:

- Physical inventory (specific port types only)
- Routing table
- ARP table
- Default bridge
- IP interfaces

There are two different scenarios that can occur when loading the generic SNMP VNE:

1. The VNE is loaded as a generic SNMP VNE (the user defines the VNE type).

   Cisco ANA Manage enables the user to load a VNE as a generic SNMP VNE. The user does this by selecting the Generic SNMP option in the Type field of the New VNE dialog box. For more information about how to define a generic SNMP VNE, see Defining VNEs, page 6-9.

2. The VNE is loaded as a generic SNMP VNE when its type is not supported (the device type is not recognized).

   If the device is not found in the "deviceTypes" list, it is currently unsupported and the user can load the VNE as:

   – An unsupported VNE

   – A generic SNMP VNE

   Every VNE in "agentdefaults/da" has the entry "load generic agent for unsupported device type", where the user can set the value as "true" or "false" (the default is "false"). 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's software versions and builds the VNE (generic SNMP) from the default version.

Polling System Configuration

The sysoid command and the software version command are used to poll the system configuration. The following parameters are available:

- interval—This parameter states the time in milliseconds required to wait before each poll. The default value is 30000 (30 seconds).
- retries—This parameter states how many retries are required to be performed before discontinuing the poll. The default is -1 which means that the retry is unlimited (always). If a positive value is defined, for example, 10 then this is the number of retries that will occur before the VNE discontinues retrying.

Note There is an option to override the default settings, if required. Changing these settings must be done with the support of Cisco Professional Services.

Viewing and Editing a VNE's Properties

Cisco ANA Manage enables the user to view and edit the properties of a VNE in a unit, for example, the status and Telnet settings. See Defining VNEs, page 6-9.

To edit a VNE's properties:

Step 1 Select the ANA Servers branch in the Cisco ANA Manage tabbed dialog box.

Step 2 Expand the ANA Servers branch, and select the required AVM sub-branch in the tree pane.

Step 3 Right-click on the required VNE in the VNEs Properties table to display the shortcut menu. Select **Properties**, or from the File menu, choose **Properties**, or on the toolbar click **Properties**. The VNE Properties dialog box is displayed with the details of the selected VNE.

For more details about the fields displayed in the VNE Properties dialog box, see Defining VNEs, page 6-9. In addition to the fields displayed when adding a new VNE, the following fields and buttons are displayed:

- **VNE Status—**The operational status, Up, Down, Shutting Down, Starting Up, or Unreachable. For more information on the status of VNEs, see VNE Status, page 6-8.
- **Start—**Start the VNE if it has been stopped or is in maintenance mode. See Changing the VNE's State, page 6-28.
- **Stop—**Stop the VNE if it is running or is in maintenance mode.
- **Maintenance—**Move the VNE to maintenance mode. If this is done when the VNE has been stopped, this has no meaning for the VNE.
- **ANA Unit**—The current unit that hosts the VNE.
- **AVM—**The current AVM number, which changes according to the unit selected to show one of the available AVMs on that unit.

Step 4 Edit the details of the VNE as required.

Step 5 Click **Apply**.

Step 6 Click **OK**. The VNE's properties are edited.

Deleting a VNE

Cisco ANA Manage enables the user to delete a VNE from a unit and AVM. This process stops the VNE if it is running, and deletes all VNE references from the system and Golden Source. This includes the registry information of the VNE in the specified unit. A VNE that has been removed no longer appears in any future system reports.

Since all VNE information is deleted, adding the VNE again requires the user to enter all the VNE information.

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

To delete a VNE:

Step 1 Select the ANA Servers branch in the Cisco ANA Manage window.

Step 2 Expand the ANA Servers branch and choose the required AVM sub-branch in the tree pane.

Step 3 Right-click on the required VNE in the VNEs Properties table to display the shortcut menu, and select **Delete**. A warning message is displayed.

Step 4 Click **Yes**. A confirmation message is displayed.

Step 5 Click **OK**. The selected VNE is deleted from the AVM, and is not displayed in the VNEs Properties table.

Changing the VNE's State

Cisco ANA Manage enables the user to start or stop a VNE, or move a VNE to maintenance mode. Starting the VNE adds the VNE to the server bootstrap. Stopping the VNE removes the VNE from the server bootstrap.

During normal operation, NEs often undergo maintenance operations and planned outages such as software upgrades, hardware modifications, cold reboots and so on. The Cisco ANA platform supports such maintenance operations without affecting the overall functionality of the active network. Neighboring VNEs do not generate alarms that are related to links to or from the maintained VNE.

While in maintenance state (temporary state) a VNE:

- Does not change state on its own unless the user explicitly (manually) switches the VNE back to active state.
- Never polls the device.
- Is capable of sending alarms but does not poll the device. therefore service alarms are not supposed to be sent except for those that are negotiated between adjacent ports. For example, a link-down alarm is still sent. Syslogs and traps are sent, and the flows are active.
- Maintains any existing links.
- Does not fail on verification requests.

The VNE blocks all provisioning flows that run through the VNE. A device in maintenance state can be disconnected and restarted, and this does not result in link-down alarms. Upon restart, the VNE receives only persistent information and returns to its latest known configuration. The topology links are renewed automatically.

	This icon indicates a VNE in maintenance state in NetworkVision.

To change the VNE's state:

Step 1 Select the ANA Servers branch in the Cisco ANA Manage window.

Step 2 Expand the ANA Servers branch, and select the required AVM sub-branch in the tree pane.

Step 3 Select the required VNE in the in the VNEs Properties table.

Step 4 Right-click to display the shortcut menu and select one of the following:

- **Actions | Start**, or on the toolbar, click **Start**.
- **Actions | Stop**, or on the toolbar, click **Stop**.
- **Actions | Maintenance**, or on the toolbar, click **Maintenance**.

Step 5 The state of the VNE changes based on your selection:

- If the VNE is started a confirmation message is displayed. Click **OK**. An Up status will eventually be displayed in the VNEs Properties table. You may see a Starting Up status, when, for example, the Server is overloaded, or the VNE is still being loaded.

  In cases where the AVM hosting the VNE is still in a Down status, the VNE status will remain as Starting Up until the AVM is brought up.

- If the VNE is stopped a confirmation message is displayed. Click **OK**. A Down status will eventually be displayed in the VNEs Properties table. You may see a Shutting Down status while various processes are closing down.
- If the VNE is moved to maintenance mode a confirmation message is displayed. Click **OK**. A Maintenance status is displayed in the VNEs Properties table.

Moving Multiple and Single VNEs

Cisco ANA Manage enables the administrator to move single and multiple VNEs between AVMs. The VNEs that are moved are unloaded. The status of the VNEs is maintained after they are reloaded.

To move a single VNE or multiple VNEs:

Step 1 Select the ANA Servers branch in the Cisco ANA Manage window.

Step 2 Expand the ANA Servers branch, and select the required AVM sub-branch in the tree pane. The VNEs are displayed in the workspace.

Step 3 Select a VNE or select multiple VNEs using the mouse or keyboard, then right-click on the required VNEs to display the shortcut menu.

Step 4 Select **Move VNEs** from the shortcut menu. The Move To dialog box is displayed:

The Move To dialog box displays a tree-and-branch representation of the selected Cisco ANA server, its units and AVMs, excluding the AVM in which the VNE is currently located. The highest level of the tree displays the Cisco ANA server. The branches can be expanded and collapsed in order to display and hide information.

Step 5 In the Move To dialog box, browse to and select the AVM (branch) where you want to move the VNEs.

Step 6 Click **OK**. The VNE is moved to its new location, and now appears beneath the selected AVM (branch) in the VNEs Properties table.

Note The user can view the “moved” VNE by selecting the appropriate AVM in the tree pane of the Cisco ANA Manage window (such as AVM 500-930000) and view the “moved” VNE in the VNEs Properties table.

Note The VNE that is moved is automatically unloaded and reloaded, and its status is maintained.