

CHAPTER 2

Adding and Managing VNEs, AVMs, Units, and the Gateway Server

These topics describe how to add, delete, and maintain network elements in Cisco ANA. They also describe the various states and statuses that are displayed in the Cisco ANA GUI client.

- [Managing the Gateway, page 2-1](#), describes how to use the **cmptcl** command to manage and get information on the gateway server.
- [Managing Units \(and High Availability\), page 2-4](#), describes how to add and manage units on the gateway server, and how to configure unit and AVM failover using the high availability feature.
- [Managing AVMs, page 2-9](#), describes how to add and manage AVMs on units, describes AVM status (admin and operational), and lists the default AVMs that are part of Cisco ANA.
- [Managing VNEs, page 2-16](#), describes how to add VNEs to AVMs in bulk using network discovery, how to add VNEs individually, and how to manage VNEs; it also describes VNE status (operational and admin) and VNE states (investigation and communication).

You must have Administrator privileges to use these functions, unless otherwise noted.

The following topics describe how to perform basic management tasks. Refer to these topics for administration information:

- [Cisco ANA Administration, page 13-1](#), explains how to manage polling groups and high availability protection groups for AVMs (for unit and AVM high availability); how to add users and scopes; and how to back up and restore data on the Solaris gateway server. It also contains information on system security.
- [Cisco ANA System Health and Diagnostics, page 14-1](#), provides procedures for checking basic system (CPU, memory) health, creating traffic graphs, running diagnostic jobs, getting database information, gathering logs, and checking connectivity.

Managing the Gateway

As described in [Cisco ANA Architecture, page 1-5](#), the gateway enforces access control and security for all connections and manages client sessions. It maintains a repository of system settings, topological data, and snapshots of active alarms and events. The gateway also maps network resources to the business context, which enables Cisco ANA to contain information that is not directly contained in the network (such as VPNs and subscribers) and display it to northbound applications.

These topics provide more information on how to manage the gateway server, and the roles required:

- [Getting Information on Configured Gateway Servers Using the GUI Client](#)

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL

- [Managing the Gateway Server Using the `cmpctl` Command](#)
- [Roles Required to Stop or Start the Gateway](#)

To connect to a gateway, download and install the client software on your client machine. Installing the gateway and client software is described in [Cisco Active Network Abstraction 4.0.2 Installation and Setup Guide](#), along with other basic setup information.

Getting Information on Configured Gateway Servers Using the GUI Client**Before You Begin**

Be sure to configure Network Time Protocol (NTP) on the gateway so that all network elements are synchronized to a common time base (UTC).

To get information about configured gateways:

- Step 1** In the Administration perspective, click the **Objects** tab in the navigation pane and click the **ANA Servers** drawer. (If you click the Servers tree, Cisco ANA displays the gateway and units that are configured on the system.)
- Step 2** Click the Servers tree and click a gateway. The gateway workspace (above the tabular list) displays the following information about all gateway servers on the system. (If you do not have any separate units, and instead all of your AVMs are on the gateway, the gateway acts as both a gateway and a unit and may display additional information. See [Viewing and Editing Unit Properties](#), page 2-6.)

Field	Description
IP Address	The IP address of the gateway.
Up Since	The date and time that the gateway was started.
Used Memory	The maximum memory used by the gateway. (Used memory is the sum of the memory used by all the AVMs that are up.)
Status	The administration status of the gateway (Up or Down, similar to the status for units, AVMs, and VNEs).
Physical Memory	The physical memory of the gateway.
Allocated Memory	The amount of memory allocated to the gateway. Allocated memory is the sum of all the memory settings for all the AVMs.

The table below the workspace provides information about the units or AVMs installed on the gateway. These are described in [Viewing and Editing Unit Properties](#), page 2-6, and [Viewing and Editing AVM Properties](#), page 2-12.

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL

The log for the gateway server process is stored in *ANAHOME/Main/logs/11.log*.

Managing the Gateway Server Using the **cmpctl** Command

You can use the **cmpctl** command to start and stop the gateway and all component processes (including AVMs you created), or just perform a general check of the system status. The **cmpctl** command is located in *ANAHOME/Main* (*ANAHOME* is the installation directory, normally */export/home/ana41*). It takes the following arguments:

cmpctl [*options*] [**start** | **stop** | **status** | **restart**]

start	Starts the gateway process. With no options, this command starts the gateway server and all component processes.	
stop	Stops the gateway process. With no options, this command stops the gateway server and all component processes.	
restart	Stops and starts the gateway processes. With no options, this command stops and restarts the gateway server and all component processes.	
status	Displays the status of the gateway processes.	
<i>options</i>	-avm <i>avm_id,avm_id,...</i>	Performs the action on the AVM specified by <i>avm_id</i> (for example, AVM111 , AVM112). For all AVMs, use * .
	-unit <i>unit_ip,unit_ip,...</i>	Performs the action on the unit specified by <i>unit_ip</i> (for example, 192.168.01.01). For all units, use * .
	-jboss	Performs the action on the JBoss process.

You must be logged in as *anauser* to use this command. The following is an example.

```
# cd /export/home/ana41/Main
# ./cmpctl status
.-= Welcome to anaserver, running Cisco ANA gateway =-.
+ Checking for services integrity:
- Checking if host's time server is up and running [OK]
- Checking if blood test webserver daemon is up and running [OK]
- Checking if secured connectivity daemon is up and running [OK]
- Checking if license server is up and running [OK]
+ Detected AVM99 is up, checking AVMs
- Checking for AVM112's status [OK]
- Checking for AVM113's status [OK]
- Checking for AVM66's status [OK]
- Checking for JBoss status [OK]
- Checking for AVM11's status [OK]
- Checking for AVM55's status [OK]
- Checking for AVM100's status [OK]
- Checking for AVM0's status [OK]
Note Checking if host's time server is up and running is the only item that can safely
have a status of DOWN. Everything else must display OK.
```

cmpctl could display any of the following status indicators:

OK	Service or AVM is up and running.
DOWN	Service or AVM is down.
LOADED	Service is down, but the system is trying to start (load) it.
EVAL	License service is running with an evaluation license.
DISABLED	AVM has been stopped.

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL

If you would like to configure gateway high availability, contact ask-ana@cisco.com.

See these topics for more information on managing and administering the gateway server:

- [Cisco ANA Administration, page 13-1](#), explains how to manage polling groups, high availability protection groups for AVMs, (for unit and AVM high availability); how to add users and scopes; backing up and restoring data. It also contains information on system security.
- [Cisco ANA System Health and Diagnostics, page 14-1](#), provides procedures for checking basic system health (CPU, memory), creating traffic graphs, running diagnostic jobs, getting database information, gathering logs, and checking connectivity.

Roles Required to Stop or Start the Gateway

[Table 2-1](#) lists the roles that are required to stop or start the gateway. For more information on roles, see [Creating and Managing Users, Passwords, and Scopes, page 13-34](#).

Table 2-1 Roles Required to Stop or Start the Gateway

Task	Role Required
Stopping or starting the gateway using <code>cmptcl</code>	Administrator

Related Topics

- [Managing Units \(and High Availability\), page 2-4](#)
- [Managing AVMs, page 2-9](#)
- [Managing VNEs, page 2-16](#)

Managing Units (and High Availability)

As described in [Cisco ANA Architecture, page 1-5](#), the interconnected fabric of units comprises the lowest level of the Cisco ANA architecture. Each unit manages a group of network elements. Units host the autonomous VNEs. This creates a fabric of interconnected VNEs which can intercommunicate with other VNEs (regardless of which unit they are running on). Cisco ANA also provides a high ability mechanism to protect the system in case a unit malfunctions. If the unit is configured for high availability, Cisco ANA switches over to the redundant standby unit, with no loss of information accumulated to that point.

For more information on high availability, see [Managing Protection Groups and High Availability, page 13-9](#).

To check the basic system health of a unit, see [Cisco ANA System Health and Diagnostics, page 14-1](#).

See these topics for more information:

- [Adding a New Unit \(and Setting Up High Availability\), page 2-5](#)
- [Viewing and Editing Unit Properties, page 2-6](#)
- [Removing a Unit, page 2-7](#)

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL**Roles Required to Manage Units**

Table 2-2 lists the roles that are required to manage units. For more information on roles, see [Creating and Managing Users, Passwords, and Scopes](#), page 13-34.

Table 2-2 Roles Required to Manage Units

Task	Role Required
Adding a unit	Administrator
Viewing unit properties	Administrator
Editing unit properties	Administrator
Finding units	Administrator
Removing units	Administrator

Related Topics

- [Managing Protection Groups and High Availability](#), page 13-9
- [Managing the Gateway](#), page 2-1
- [Managing AVMs](#), page 2-9
- [Managing VNEs](#), page 2-16

Adding a New Unit (and Setting Up High Availability)

After you install the Cisco ANA software on a unit, you can add it to the Cisco ANA fabric. Cisco ANA automatically registers the unit in the registry. The units are linked to the gateway in a star topology.

In addition, administrators can enable or disable high availability for a unit. These settings enable the administrator to define to which protection group a unit is assigned, and whether it is enabled for high availability. For more information on high availability, see:

- [Configuring High Availability for Units](#), page 13-17
- [High Availability Events and Default Settings for Failover](#), page 13-21

Before You Begin

- Before adding a unit, you must install the Cisco ANA software on the unit as described in the [Cisco Active Network Abstraction 4.1.2 Installation and Setup Guide](#).
- If you want to configure unit high availability, verify that the unit's protection group has been configured. See [Managing Protection Groups and High Availability](#), page 13-9.

To add a new unit:

- Step 1** In the Administration perspective, click the **Objects** tab and click the **ANA Servers** drawer.
- Step 2** Right-click the Servers tree and choose **New ANA Unit**. The New ANA unit dialog box is displayed.
- Step 3** Enter the following information:
 - a. Unit IP Address—Enter the unique IP address of the unit.
 - b. Gateway IP Address—IP address of the gateway server for the unit.

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL

- c. Unit Protection—Click the appropriate radio button to indicate the unit’s high availability configuration:
- Protected—Enable high availability for the unit (the default).
 - Unprotected—Do not enable high availability for the unit.
 - Standby—Designate the unit to be a standby for a protection group.



Note It is highly recommended that you do not select Unprotected. For more information about configuring standby units, see [Configuring High Availability for Units, page 13-17](#).

- d. Protection Group—If you selected Protected or Standby for unit protection, choose a protection group from the drop-down list of available groups. (Protection groups are described in [Managing Protection Groups and High Availability, page 13-9](#).)

Step 4 Click **OK**. The new unit is displayed in the tree pane and the workspace.

Step 5 If the unit is configured for high availability and you have configured devices to forward traps to a unit, you should also configure the devices to send traps to the standby unit. (If the unit goes down, when the standby unit comes up, AVM 100 on the standby unit broadcasts to the VNEs, and the VNEs register to it to start receiving traps from the new AVM 100.) See [Trap Forwarding, page 13-23](#).

If the new unit is installed and reachable it starts automatically. The active unit is registered with the gateway. Specifically, the command creates the configuration registry for the new unit in the registry.

Related Topics

- [Roles Required to Manage Units, page 2-5](#)
- [Cisco ANA System Health and Diagnostics, page 14-1](#)
- [Managing Protection Groups and High Availability, page 13-9](#)
- [Viewing and Editing Unit Properties, page 2-6](#)
- [Removing a Unit, page 2-7](#)

Viewing and Editing Unit Properties

To view or edit a unit’s properties:

Step 1 In the Administration perspective, click the **Objects** tab and click the **ANA Servers** drawer.

Step 2 Open the Servers tree and click any unit.

Step 3 The unit workspace (above the tabular list) displays the following information. If the unit is inactive, some of the following information is not displayed.

Field	Description
IP Address	The IP address of the unit.
Up Since	The date and time that the unit was started.
Used Memory	The maximum memory used by the unit. (Used memory is the sum of the memory used by all the AVMs that are up.)

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL

Field	Description
Protection Group	The protection group to which the unit is assigned.
Status	The administration status of the unit (Up or Down, similar to the status for gateways, AVMs, and VNEs).
Physical Memory	The physical memory of the unit.
Allocated Memory	The amount of memory allocated to the unit. Allocated memory is the sum of all the memory settings for all the AVMs.
AVM HA	Indicates whether the AVM watchdog protocol is enabled. (See Managing the Watchdog Protocol on AVMs, page 13-20.)

The table below the workspace provides information about the AVMs installed on the gateway. These are described in [Viewing and Editing AVM Properties, page 2-12.](#)

- Step 4** You can change the assigned unit protection group, as required, by choosing an option from the list.
- The AVM HA check box defines whether the watchdog protocol is enabled. This should be checked. (See [Managing the Watchdog Protocol on AVMs, page 13-20.](#))
- When you change (disable or enable) the Enable Unit Protection option (high availability), changes are effective after a delay of about 15 minutes.
- Step 5** Exit the window. If you made any changes, you are prompted to confirm them.

Related Topics

- [Roles Required to Manage Units, page 2-5](#)
- [Cisco ANA System Health and Diagnostics, page 14-1](#)
- [Managing Protection Groups and High Availability, page 13-9](#)
- [Adding a New Unit \(and Setting Up High Availability\), page 2-5](#)
- [Removing a Unit, page 2-7](#)

Removing a Unit

Before You Begin

Delete all the VNEs and unreserved AVMs before deleting a unit; see [Deleting an AVM, page 2-15.](#) The reserved AVMs cannot be deleted.

Use this procedure to remove a unit:

- Step 1** In the Administration perspective, click the **Objects** tab and click the **ANA Servers** drawer.
- Step 2** Open the Servers tree, right-click the unit you want to delete and choose **Delete**. A warning message is displayed.
- Step 3** Click **Yes** to proceed or **No** to cancel the operation. A confirmation message is displayed.
- Step 4** Click **OK**. The unit is deleted and is no longer displayed in the navigation area or workspace.

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL |**Related Topics**

- [Roles Required to Manage Units, page 2-5](#)
- [Cisco ANA System Health and Diagnostics, page 14-1](#)
- [Managing Protection Groups and High Availability, page 13-9](#)
- [Adding a New Unit \(and Setting Up High Availability\), page 2-5](#)
- [Viewing and Editing Unit Properties, page 2-6](#)

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL

Managing AVMs

As described in [Cisco ANA Architecture, page 1-5](#), AVMs are Java processes that provide the necessary distribution support platform for executing and monitoring multiple VNEs. AVMs and VNEs commonly reside on Cisco ANA units but some also reside on a Cisco ANA gateway. The following AVMs are always created on the gateway; some are also created on units. These cannot be edited or deleted.

Reviewers: Please confirm that these are all the AVMs that users need to know about. I heard that AVM 66 might not be in the GUI anymore. Also, please give an update on AMV 199 (whether it is in or out, what it is for, etc.) Nicola suggested adding Jboss to this list, but Jboss is not an AVM, correct? (We do have a process list in the install guide that lists Jboss.)

AVM #	Purpose	Is installed on...	Can be checked using...
AVM 0	High Availability/Switch AVM—Enables communication between the unit with other units, as well as the gateway.	Gateway	cmpctl status
AVM 11	Gateway server AVM—???(Definition)	Gateway	cmpctl status
AVM 55	Inventory service AVM—Provides modeling information.	Gateway	cmpctl status
AVM 66	Workflow engine AVM—Defines rules and dependencies to activate business and network processes.	Gateway	GUI client and cmpctl status
AVM 99	Management AVM—Manages the unit and the other AVMs running on the unit (or gateway, if there are no separate units).	Gateway and units	cmpctl status
AVM 100	Trap management AVM—Processes syslogs and traps. Note Only one AVM 100 should be running, and all traps and syslogs should be forwarded to the gateway or unit containing the running AVM.	Gateway and units	GUI client and cmpctl status
AVM 199	???	??	??

You can add AVMs to units or directly to a gateway. Each of these AVMs has its own log.

The Cisco ANA Watchdog Protocol monitors the AVM processes to make sure any AVMs that have stopped are restarted. For information on the Watchdog Protocol, see [Configuring AVMs for High Availability, page 13-20](#).

To check the basic system health of AVMs, see [Cisco ANA System Health and Diagnostics, page 14-1](#).

See these topics for more information:

- [Understanding AVM Status, page 2-10](#)
- [Creating an AVM, page 2-11](#)
- [Viewing and Editing AVM Properties, page 2-12](#)
- [Changing AVM Status \(Start or Stop\), page 2-13](#)

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL

- [Moving an AVM, page 2-14](#)
- [Deleting an AVM, page 2-15](#)

Roles Required to Manage AVMs

Table 2-3 lists the roles that are required to manage AVMs. For more information on roles, see [Creating and Managing Users, Passwords, and Scopes, page 13-34](#).

Table 2-3 Roles Required to Manage AVMs

Task	Role Required
Adding an AVM	Administrator
Viewing AVM properties	Administrator
Editing AVM properties	Administrator
Starting or stopping an AVM	Administrator
Finding an AVM	Administrator
Moving an AVM	Administrator
Deleting an AVM	Administrator

Related Topics

- [Managing the Gateway, page 2-1](#)
- [Managing Units \(and High Availability\), page 2-4](#)
- [Managing VNEs, page 2-16](#)

Understanding AVM Status

AVM *status* describes the administrative condition of the AVM process on the unit or gateway. AVM status is determined by a combination of the AVM's admin status and operational status:

- AVM *admin status* is a user-directed status that signifies if the AVM should be up or down. If you stop an AVM using the Administration perspective, the admin status is changed to Disabled. If you start the AVM, the admin status is changed to Enabled.
- AVM *operational status* describes the condition of the AVM as seen by the gateway server.

Table 2-4 describes how the combination of AVM admin and operational status determines the overall AVM status.

Table 2-4 AVM Status

AVM Status	Admin Status	Operational Status	Description
Up	Enabled	Up	The AVM process is reachable, was loaded, and has started. This is the status when the AVM is created (and you selected Activate Upon Creation), and no problems are encountered.
Down	Disabled	Down	The AVM process is reachable, but was stopped. This is the status when a Stop command is issued.

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL

When moving an AVM, its status has a bearing on whether the process is automatically reloaded. If its status is Up, it is reloaded; if its status is down, it is not reloaded. For more information about moving AVMs, see [Moving an AVM, page 2-14](#). For more information about starting and stopping AVMs, see [Changing AVM Status \(Start or Stop\), page 2-13](#).

Related Topics

- [Changing AVM Status \(Start or Stop\), page 2-13](#)
- [High Availability Events and Default Settings for Failover, page 13-21](#)
- [Configuring AVMs for High Availability, page 14-22](#)
- [Roles Required to Manage AVMs, page 2-10](#)
- [Creating an AVM, page 2-11](#)
- [Cisco ANA System Health and Diagnostics, page 14-1](#)

Creating an AVM

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

Before You Begin

- Decide which unit you want to use to install the AVM. See [Creating an AVM, page 2-11](#).
- The unit must be installed.
- The unit must be connected to the transport network.
- The default AVMs (AVM 0, AVM 99, AVM 100) must be running. For more information on the status of AVMs, see [Understanding AVM Status, page 2-10](#).
- The new AVM must have a unique ID within the unit.

**Note**

AVMs 0-100 and AVM 199 are reserved, and cannot be used. Do not enter a reserved number.

- Step 1** In the Administration perspective, click the **Objects** tab and click the **ANA Servers** drawer.
- Step 2** Open the Servers tree, right-click the unit and choose **New AVM**.
- Step 3** Enter the following information. The ANA Unit field is prepopulated with the parent unit's IP address. The unit does not have to be up to create the AVM.

Field	Description
ID	The name of the AVM as defined in Cisco ANA, unique to the unit (for example, AVM 18). AVMs 0-100 and AVM 199 are reserved and cannot be used. Do not enter a reserved number. If you do, a message is displayed in the New AVM dialog box, informing you that the number is reserved.
Key	A string that uniquely identifies an AVM in the system, across all units, thus enabling a transparent failover scenario in the system. If you do not enter a key, the default key, ID + time stamp, is used.

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL

Field	Description
Allocated Memory	The maximum memory allocated to the AVM, in megabytes. For information on the amount of memory to allocate to an AVM, depending on network element types, see COOKBOOK .
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 check box is checked, enabling the watchdog protocol on the AVM when high availability is enabled (you have a standby unit). For more information, see Configuring AVMs for High Availability, page 13-20 . Note It is highly recommended that you do not disable this option if high availability is enabled. If you change the option when the AVM is up, you must restart the AVM for the change to take effect.

- Step 4** Click **OK**. The new AVM is added to the selected unit, displayed in the workspace, and activated. Verify that the Admin Status is Enabled and the Operational Status is Up.

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 and Creating Individual VNEs, page 2-35](#).

Related Topics

- [Understanding AVM Status, page 2-10](#)
- [Changing AVM Status \(Start or Stop\), page 2-13](#)
- [Configuring AVMs for High Availability, page 14-22](#)
- [Watchdog Protocol and Process Monitoring, page 13-11](#)
- [Roles Required to Manage AVMs, page 2-10](#)
- [Cisco ANA System Health and Diagnostics, page 14-1](#)

Viewing and Editing AVM Properties

To view and edit an AVM's properties:

- Step 1** In the Administration perspective, click the **Objects** tab and click the **ANA Servers** drawer.
- Step 2** Open the Servers tree, and click the AVM in which you are interested. (several of the internal Cisco ANA system AVMs are not listed.)
- Step 3** Click the AVM you want to view or edit. The AVM workspace (above the tabular list) displays the following information:

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL

Field	Description
AVM Protection Enabled	If checked, the watchdog protocol is enabled on the AVM (available only when high availability is enabled). For more information, see Managing the Watchdog Protocol on AVMs , page 13-20.
Operational Status	The status of the relationship between the AVM and its child VNEs (see VNE Status (Operational and Admin Status) , page 2-17).
Up Since	When the AVM process was last started.
Key	A string that uniquely identifies an AVM in the system, across all units, thus enabling a transparent failover scenario in the system. The default key, ID + time stamp, is used.
ID	The name of the AVM as defined in Cisco ANA, unique to the unit. Note AVMs 0-100 and AVM 199 and cannot be used. Do not enter a reserved number. If you do, a message is displayed in the New AVM dialog box, informing you that the number is reserved.
Admin Status	The status of the relationship between the AVM and its parent gateway/unit (see VNE Status (Operational and Admin Status) , page 2-17).
Max. Memory	The maximum memory, in megabytes, allocated to the AVM.

The table below the workspace provides information about the VNEs installed on the AVM. These are described in [Viewing and Editing VNE Properties and Schemes](#), page 2-43.

Step 4 Edit the details of the AVM as required.

For more information on the other fields displayed in the AVM Properties dialog box, see [Creating an AVM](#), page 2-11.

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

Related Topics

- [Changing AVM Status \(Start or Stop\)](#), page 2-13
- [Understanding AVM Status](#), page 2-10
- [Watchdog Protocol and Process Monitoring](#), page 13-11
- [High Availability Events and Default Settings for Failover](#), page 13-21
- [Creating an AVM](#), page 2-11
- [Roles Required to Manage AVMs](#), page 2-10

Changing AVM Status (Start or Stop)**Note**

Stopping the AVM 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.

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL

To start or stop an AVM:

-
- Step 1** In the Administration perspective, click the **Objects** tab and click the **ANA Servers** drawer.
- Step 2** Open the Servers tree, and click the unit that contains the AVM you are interested in.
- Step 3** Right-click the AVM and choose **Start** or **Stop**.

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

- Up—The AVM is running.
 - Down—The AVM is stopped.
-

Related Topics

- [Understanding AVM Status, page 2-10](#)
- [High Availability Events and Default Settings for Failover, page 13-21](#)
- [Configuring AVMs for High Availability, page 14-22](#)
- [VNE Persistency Mechanism, page F-1](#)
- [Cisco ANA System Health and Diagnostics, page 14-1](#)
- [Deleting an AVM, page 2-15](#)

Moving an AVM

You can move an entire AVM between units.

**Note**

AVMs 0-100 and AVM 199 are reserved and cannot be moved.

Cisco ANA 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, maintaining the status it was in before the move. For example, if it was up before the move, it remains up; if it was down, it remains down.

To move an AVM:

-
- Step 1** In the Administration perspective, click the **Objects** tab and click the **ANA Servers** drawer.
- Step 2** Open the Servers tree, and click the unit that contains the AVM in which you are interested.
- Step 3** Right-click the AVM and choose **Move**.

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 to display and hide information.

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL

- Step 4** In the servers tree, select the unit (branch) where you want to move the AVMs.
- Step 5** Click **OK**. The AVM is moved and now appears beneath the selected unit.
-

For information about moving VNEs, see [Moving One or More VNEs, page 2-45](#).

Related Topics

- [Understanding AVM Status, page 2-10](#)
- [Changing AVM Status \(Start or Stop\), page 2-13](#)
- [Configuring AVMs for High Availability, page 14-22](#)
- [Viewing and Editing AVM Properties, page 2-12](#)
- [Roles Required to Manage AVMs, page 2-10](#)
- [Cisco ANA System Health and Diagnostics, page 14-1](#)

Deleting an AVM

If an AVM that you want to delete is running, it is stopped before being removed. 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 is displayed, and you cannot delete the AVM.

For more information, see [Deleting a VNE, page 2-46](#).

**Note**

AVMs 0-100 and AVM 199 are reserved and cannot be deleted.

Before You Begin

Remove all VNEs from the AVM, or the deletion fails. See [Deleting a VNE, page 2-46](#).

- Step 1** In the Administration perspective, click the **Objects** tab and click the **ANA Servers** drawer.
- Step 2** Open the Servers tree, and click the unit that contains the AVM in which you are interested.
- Step 3** Right-click the AVM and choose **Delete**. A warning message is displayed.
- Step 4** Click **Yes**. A confirmation message is displayed and the selected AVM is deleted from the selected unit.
-

Related Topics

- [Understanding AVM Status, page 2-10](#)
- [Changing AVM Status \(Start or Stop\), page 2-13](#)
- [Configuring AVMs for High Availability, page 14-22](#)
- [Viewing and Editing AVM Properties, page 2-12](#)
- [Roles Required to Manage AVMs, page 2-10](#)
- [Moving an AVM, page 2-14](#)
- [Cisco ANA System Health and Diagnostics, page 14-1](#)

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL

Managing VNEs

Each Virtual Network Element (VNE) is assigned to manage a single network element instance and contains a replica of that element. The VNEs maintain a live model of each network element and of the entire network. As the VNE loads, Cisco ANA starts investigating the network element and automatically builds a live model of it, including its physical and logical inventory, its configuration, and its status. Cisco ANA also creates the registry information of the new VNE in the unit. The newly created VNE uses the default community strings and polling rates. The VNE inherits these properties from the configuration record that corresponds to the network element type.

Reviewers: Regarding the following paragraph --

(1)if using Network Discovery, how is the VNE type and scheme determined?

(2) Should I say they can only specify a type and scheme if adding individually (right-click AVM and choose New VNE)?

The information collected by a VNE depends on the VNE type and scheme. You should choose a scheme based on the device family and on the technologies you want Cisco ANA to manage (see [Choosing a Scheme when Adding Individual VNEs, page 2-25](#)). The VNE uses whatever southbound management interfaces the network element implements (for example, SNMP or Telnet). Cisco ANA uses the CISCO-ENTITY-MIB, CISCO-STACK-MIB, and OLD-CISCO-CHASSIS-MIB to model Cisco devices.

Reviewers: Does the following note correctly represent the telnet disconnect functionality? I have repeated this note in several places.



Note

By default, when a VNE opens a Telnet session with a network element in order to model and monitor the element, the Telnet session remains open as long as the VNE is up. The VNE does not close the session due to timeouts. If you would like to configure a timeout, contact ask-ana@cisco.com for assistance.

A VNE must be loaded into the bootstrap of the unit before it starts monitoring its underlying network element. This changes the administrative status of the VNE to Enabled, 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 [Understanding VNE Status and VNE States, page 2-17](#).

Each VNE should be added to the system only once. You can add VNEs to Cisco ANA in two ways:

- Add VNEs in bulk based on the devices in your current network.
- Add individual VNEs.

These procedures and all prerequisites are outlined in [Table 2-8 on page 2-21](#).

See these topics for more information:

- [Prerequisites for Adding VNEs to AVMs, page 2-21](#)
- [Using Network Discovery to Add Bulk VNEs, page 2-27](#)
- [Defining and Creating Individual VNEs, page 2-35](#)
- [Viewing and Editing VNE Properties and Schemes, page 2-43](#)
- [Changing VNE Status \(Start, Stop, Maintenance\), page 2-44](#)
- [Moving One or More VNEs, page 2-45](#)
- [Deleting a VNE, page 2-46](#)

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL**Roles Required to Manage VNEs**

Table 2-3 lists the roles that are required to manage VNEs. For more information on roles, see [Creating and Managing Users, Passwords, and Scopes](#), page 13-34.

Table 2-5 Roles Required to Manage VNEs

Task	Role Required
Configuring network discovery settings and performing network discovery	Administrator
Importing VNEs in bulk using a seed file generated using network discovery	Administrator
Creating an individual VNE	Administrator
Viewing VNE properties	Administrator
Editing VNE properties	Administrator
Changing a VNE's status	Administrator
Finding a VNE	Administrator
Moving a VNE	Administrator
Deleting a VNE	Administrator

Related Topics

- [Understanding AVM Status](#), page 2-10
- [Cisco ANA System Health and Diagnostics](#), page 14-1

Understanding VNE Status and VNE States

VNE status describes the administrative condition of the VNE process on the AVM. *VNE state* describes the condition of the VNE as it tries to model and monitor the real network element it represents. (These states are also different from the network element *management states* (Managed, Maintenance, Unmanaged, Unsupported). For information on management states, see [Understanding Network Element Management States](#), page 3-8.)

These topics provide detailed information about VNE status and VNE states:

- [VNE Status \(Operational and Admin Status\)](#), page 2-17
- [VNE States \(Investigation and Communication States\)](#), page 2-18

VNE Status (Operational and Admin Status)

VNE status describes the administrative condition of the VNE process on the unit or gateway. VNE status is determined by a combination of the VNE's admin status and operational status:

- *VNE admin status* is a user-directed status that signifies if the VNE should be up or down. If you stop a VNE using the Administration perspective, the admin status is changed to Disabled. If you start the VNE, the admin status is changed to Enabled. (If you change a VNE to Maintenance mode, its admin status remains Enabled, but its Maintenance mode is displayed as True.)
- *VNE operational status* describes the actual state of the VNE as seen by the gateway server.

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL

Table 2-6 describes how the combination of VNE admin and operational status determines the overall VNE status.

Table 2-6 VNE Status

VNE Status	Admin Status	Operational Status	Description
Up	Enabled	Up	The VNE process is reachable, was loaded, and has started. This is the status when a Start command is issued (or when you create a VNE and choose Start as its initial status), and no problems are encountered (such as an overloaded server). When a VNE is changed to Maintenance mode, it retains its Up status. In the VNE properties table, Maintenance is changed from false to true.
Down	Disabled	Down	The VNE process is reachable, but was stopped. This is the status when a Stop command is issued.
Unreachable	Enabled	Unreachable	The VNE cannot be reached by the gateway, so the VNE cannot be managed.

The admin and operational statuses are displayed in the VNEs table when you select an AVM.

When moving a VNE, its status has a bearing on whether the process is automatically reloaded. If its status is Up, it is reloaded; if its status is down, it is not reloaded. For more information about moving VNEs, see [Moving One or More VNEs](#), page 2-45. For more information about starting and stopping VNEs, see [Changing VNE Status \(Start, Stop, Maintenance\)](#), page 2-44.

You can also place a VNE in Maintenance mode. The VNE status remains Up, but the Maintenance mode (displayed in the UI) changes to true. This allows you to perform maintenance operations without affecting the overall functionality of the active network. Maintenance mode is described in more detail in [VNE States \(Investigation and Communication States\)](#), page 2-18. For information on what a VNE can do when it is in Maintenance mode, see [Understanding Network Element Management States](#), page 3-8.

VNE States (Investigation and Communication States)

A VNE's *state* describes the relationship between the VNE and the real network element it represents, and the VNE's ability to model and inventory the network element. There are two types of VNE states: the investigation and communication states. These important indicators are displayed both as icons (in the device browser and topology maps), and in text format (in the VNE properties area).

- The *investigation state* represents the level of network element discovery that has been performed, or is being performed, by the VNE. There are a number of investigation states, and they are listed in [Table 2-7](#).
- The *communication state* tells you whether the VNE can reach the network element, according to the health of the real device. The communication state can cause a change in the investigation state. There are two communication states: Reachable and Unreachable. *Reachable* means that all of the enabled protocols on the network element are responding; *Unreachable* means that at least one of the enabled protocols is not responding.

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL

Table 2-7 describes the VNE investigation states and the possible communication states for each.

Table 2-7 VNE Investigation States

Investigation State	Description	Communication State
Unknown	The VNE has not been created. (This investigation state is not displayed in the UI.)	N/A
Initializing	The VNE is discovering basic information about the network element (vendor, network element type, hardware and software versions, scheme). This is a transitional state.	Reachable
Modeling in progress	The VNE is discovering the network element and building the model. This is a transitional state. If a reachable network element becomes unreachable, or vice versa, the investigation state does not change. The VNE investigation state remains in Modeling in progress.	Reachable or Unreachable
Normal	The VNE is managing the network element. All investigation commands have successfully completed. If a reachable network element becomes unreachable, the VNE investigation state changes to Sync in progress. When the network element becomes reachable, the VNE investigation state remains at Sync in progress until modeling is complete.	Reachable
Preparing for maintenance	The VNE is changing to Maintenance mode (specifically, its status is changing) and no longer polls the network element. This is a transitional state.	Reachable
Maintenance	The VNE is capable of sending alarms and maintains existing links, but does not poll the network element. (See Understanding Network Element Management States , page 3-8 for information on the Maintenance <i>management</i> state.)	Reachable
Sync in progress	The VNE is synchronizing its model with the network element. (For example, the network element was unreachable but becomes reachable, or a user changes the management state from Maintenance to Managed.) This is a transitional state. If a reachable network element becomes unreachable, or vice versa, the investigation state does not change. The VNE investigation state remains in Sync in progress.	Reachable or Unreachable
Shutting down	The VNE is changing to Down status and is not managing the network element. (For example, a user has selected Stop in the UI.) This is a transitional state.	Reachable
Incomplete	The VNE investigation encountered an issue. For example, a command expired, threw an exception, or has not yet run; or a module is unsupported. However, the VNE can still be managed. If a reachable network element becomes unreachable, the VNE investigation state changes to Sync in progress. When the network element becomes reachable, the VNE investigation state remains at Sync in progress until modeling is complete.	Reachable
Unsupported	The entire network element is not supported.	Reachable

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL

Figure 2-1 illustrates the normal flow of VNE investigation states when a network element is added to Cisco ANA.

Figure 2-1 *VNE Investigation State Sequence when NE is Successfully Added to Cisco ANA*



A network element can also be changed to the Maintenance state, either manually or automatically. You may want to do this manually if you need to perform a maintenance activity, such as a software upgrade, so that Cisco ANA will ignore alarms during the activity. Cisco ANA automatically changes a network element to the Maintenance state when the network element's CPU usage reaches a certain configured level. This behavior prevents the VNE from using too much of the network element's resources. When the network element is ready to be changed back to Normal state, Cisco ANA synchronizes the VNE network model with the element, as shown in Figure 2-2.

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL**Figure 2-2 State Sequence when Attempting to Change VNE from Maintenance to Normal****Related Topics**

- [Understanding Network Element Management States, page 3-8](#)
- [Prerequisites for Adding VNEs to AVMs, page 2-21](#)
- [Defining and Creating Individual VNEs, page 2-35](#)
- [Viewing and Editing VNE Properties and Schemes, page 2-43](#)
- [Deleting a VNE, page 2-46](#)

Prerequisites for Adding VNEs to AVMs

[Table 2-8](#) lists the tasks you must perform before adding VNEs, to ensure that Cisco ANA can fully manage your network elements.

Table 2-8 Steps to Add VNEs to AVMs

	To Perform this Task...	See...
Step 1	If you are concerned about the that is consumed by VNEs, contact ask-ana@cisco.com for help with installing VNEs on AVMs in a way that does not adversely impact system performance.	N/A

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL**Table 2-8 Steps to Add VNEs to AVMs (continued)**

	To Perform this Task...	See...
Step 2	<p>Perform the prerequisites for adding any VNEs, regardless of the method:</p> <ol style="list-style-type: none"> Perform all mandatory configurations on the network element so Cisco ANA can properly manage the element (for example, configuring devices to forward traps to a unit). Gather all prerequisite information (such as IP addresses, credentials, and protocol details) about the network elements you want to add. Decide which scheme to specify when you add the VNE. The scheme determines what information is collected by a VNE and populated in its model. It depends on the device type and the device technologies you want to manage. 	<p>Device Configuration Tasks to Perform Before Adding VNEs, page 2-22</p> <p>Device Information to Gather Before Adding VNEs, page 2-24</p> <p>Choosing a Scheme when Adding Individual VNEs, page 2-25</p>
Step 3	To add individual VNEs, create the VNE and add it to Cisco ANA using the Servers drawer in the Administration perspective.	Defining and Creating Individual VNEs, page 2-35
Step 4	<p>To add VNEs in bulk based on the devices in your current network:</p> <ol style="list-style-type: none"> Use the Network Discovery feature to find all devices in the network. Create the seed file and import the devices using Bulk VNE Import. 	<p>Using Network Discovery to Add Bulk VNEs, page 2-27</p> <ul style="list-style-type: none"> Configuring and Performing Network Discovery, page 2-28 Importing Network Elements from a Seed File, page 2-33

Device Configuration Tasks to Perform Before Adding VNEs

For Cisco ANA to manage a network element, the element must have the proper configuration settings. For example, you might want to configure a device to forward traps to its identified unit (and to the standby unit, if the unit is configured for failover). If a unit goes down, when the standby unit comes up, AVM 100 on the standby unit broadcasts to the VNEs, and the VNEs register to it to start receiving traps from the new AVM 100.

The settings you must apply depend on the network element device family, and are shown in [Table 2-9](#).

**Note**

A forward slash at the end of a line means the command continues on the next line.

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL**Table 2-9 Prerequisite Device Configuration Tasks**

Device Family	Required Settings	Recommended Settings
Cisco IOS and Cisco Cat OS	<pre>snmp-server community public RO snmp-server community private RW snmp-server host gateway_IP public service timestamps debug datetime msec localtime service timestamps log datetime msec localtime logging buffered 64000 informational logging trap informational logging source-interface Loopback0 logging on logging gateway_IP</pre>	<pre>snmp-server enable traps snmp \ authentication linkdown linkup coldstart \ warmstart snmp-server enable traps chassis snmp-server enable traps module snmp-server enable traps bgp snmp-server enable traps ospf state-change snmp-server enable traps ospf errors snmp-server enable traps ospf retransmit snmp-server enable traps ospf lsa snmp-server enable traps ospf \ cisco-specific state-change snmp-server enable traps ospf \ cisco-specific errors snmp-server enable traps ospf \ cisco-specific retransmit snmp-server enable traps ospf \ cisco-specific lsa snmp-server enable traps config snmp-server enable traps ipmulticast snmp-server enable traps syslog snmp-server enable traps entity snmp-server enable traps flash insertion \ removal snmp-server enable traps envmon fan shutdown supply temperature status snmp-server enable traps rtr snmp-server enable traps mpls ldp</pre>
Cisco IOS XR	<pre>logging on logging events level informational logging console debugging logging monitor informational logging buffered 100000 logging buffered debugging domain ipv4 host gateway_name gateway_IP telnet ipv4 server max-servers no-limit snmp-server community public RO snmp-server community private RW snmp-server traps snmp-server host gateway_IP traps version \ [1 2c 3] community vty-pool default 0 99 xml agent tty</pre>	<pre>hostname gateway_name snmp-server location location snmp-server contact contact line default exec-timeout 0 0</pre>
	<p>Additional Requirements for Cisco IOS XR:</p> <ul style="list-style-type: none"> • Install the Cisco IOS XR Manageability Package on top of the Cisco IOS XR version. You can get information on this package from the release notes for your Cisco IOS XR version. • Cisco ANA should use the device login user which is a member of group root-system and cisco-support. • To correctly model logical routers, the Cisco ANA user should use the unique login <i>user@admin</i> (and also be a member of groups root-system and cisco-support). 	
Redback	<pre>snmp community public local¹</pre>	None
UTStarcom	<pre>snmp-server community public RO snmp-server community public RW</pre>	None

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL

1. To check the current settings on the Redback network element, use the **show snmp communities** command.

Device Information to Gather Before Adding VNEs

Before adding a VNE, make sure you have the device information that is listed in [Table 2-10](#). You should also be prepared to enter information about private or public keys, if you plan to use them; see [Public Key and Private Key File Formats](#), page 2-24.


Note

For Cisco IOS and Cisco IOS XR elements, you must know the Telnet login sequence.

Table 2-10 Prerequisite Device Information

Information Required	Verify the following:	
IP address	Network element IP address.	
Name	Network element name.	
Protocol and Credential Details	SNMP	<ul style="list-style-type: none"> • SNMP is running on the network element • Supported version (V1, V2, V3) • For SNMPV1/V2: The SNMP read and write community strings • For SNMP V3: The username, and optionally the authentication or privacy configuration
	Telnet	<ul style="list-style-type: none"> • Telnet is supported on the network element • Port number • Telnet login sequence: Username, password, and prompt <p>Note The Telnet login sequence is required for Cisco IOS and Cisco IOS XR network elements.</p>
	SSH	<ul style="list-style-type: none"> • SSH is supported on the network element • Supported version (V1 or V2) • SSH username and password and any other configuration information (cipher, authentication, key exchange (V2), MAC (V2)). <p>Note Cisco recommends that you first use any SSH client application (such as UNIX SSH or OpenSSH) to determine the device SSH login sequence.</p>

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.

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL

For example, when working with Cisco IOS software, 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 to the supported version.

The easiest solution is to use public key scan, offered 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.

The following are examples of valid file formats.

```
RSA- private key
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgQDvdPw8ItfbSp/hTbWZJqCPmjRyh9S+EpTJ0Aq3fnGpFPTR+
.....
TiOfhiuX5+MlcTaE/if8sScj6jE9A0MpShBrnDU/0A==
-----END RSA PRIVATE KEY-----

DSA private key
-----BEGIN DSA PRIVATE KEY-----
MIIBuwIBAAKBgQDNGO+l2XW+W+YtVnWSYbKXr6qkrH9nO1+
.....
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
```

Choosing a Scheme when Adding Individual VNEs

When you create the VNE, you are prompted to choose a scheme. The VNE scheme determines what network element information is collected by a VNE and populated in its model. You should choose a scheme based on the device family, and on the technologies you want Cisco ANA to manage.

Table 2-11 lists the scheme you should use, depending on the device family.

Table 2-11 VNE Schemes

VNE Scheme	Description
Foundation	Used for all Cisco devices and other vendor devices. <ul style="list-style-type: none"> Cisco IOS, depending on the technologies you want Cisco ANA to manage (see Table 2-12). Cisco CatOS. Non-Cisco.
MPLS	Supports all the technologies available in Foundation scheme; in addition, it supports technologies related to MPLS and Carrier Ethernet. The MPLS scheme, however, does not support other vendor devices. <p>Cisco IOS, depending on the technologies you want Cisco ANA to manage (see Table 2-12).</p> <p>Cisco IOS-XR. For example, Cisco XR 12000 series and Cisco CRS-1.</p>

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL

Technology support for each scheme is listed in [Table 2-12](#). Choosing the correct scheme is important if your devices are running the Cisco IOS operating system, because those network elements can use either scheme. If you need support for technologies related to MPLS and Carrier Ethernet, you should use the MPLS scheme. See [Table 2-12](#) for more information.

Reviewers: Please review this list carefully and let me know which schemes support each new technology. And how about these? They are from MTD. Sonet, SDH, PPP, HDLC, Metro Ethernet.

Table 2-12 Technology Support Based on Schemes

Technology	Foundation	MPLS
ARP	Yes	Yes
ATM		
ATM-IMA		
BGP	Yes	Yes
Bridge Domain	No	Yes
Bridging	Yes	Yes
Carrier Ethernet		
CDP	Yes	Yes
CFM (part of E-OAM)	Yes	Yes
COD	No	Yes
ELMI		
EoMPLS	No	Yes
Ethernet	Yes	Yes
Ethernet Channel	Yes	Yes
Frame Relay		
GRE		
IEEE dot1q	Yes	Yes
IP	Yes	Yes
IPTV Multicast		
IPTV Multiplex over TDM		
IPTV Video Monitor		
ISIS	Yes	Yes
LAG	Yes	Yes
Link-OAM		
OSPF	Yes	Yes
MP-BGP	No	Yes
MPLS	Yes	Yes
MPLS TE-Tunnel	No	Yes
MPLS Layer 3 VPN	No	Yes
Pseudowire	No	Yes

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL**Table 2-12 Technology Support Based on Schemes (continued)**

Technology	Foundation	MPLS
Q-in-Q	Yes	Yes
Layer 2 Tunneling Protocol (L2TP)		
RTPM		
Service Instance (part of Flex UNI)	No	Yes
STP/MSTP	Yes	Yes
SVI/VPLS/H-VPLS	No	Yes
TDM-IMA		
VLAN/S-VLAN	Yes	Yes
VRF	No	Yes
VTP (VLAN Trunk and Tunneling)	Yes	Yes

Related Topics

- [Managing VNEs, page 2-16](#)
- [Roles Required to Manage VNEs, page 2-17](#)

Using Network Discovery to Add Bulk VNEs

The network discovery process creates a list of elements that are present in your network. From the output of that process, you create a seed file, which specifies the elements you want Cisco ANA to manage. Finally, you import the network elements into Cisco ANA, which discovers each element and creates a VNE for it. The result is a living model of all the network elements you want to manage.

If you want to import a small number of network elements, use the procedure that is described in [Defining and Creating Individual VNEs, page 2-35](#).

These are the basic steps of the network discovery and bulkVNE import process.

1. Use Network Discovery to find existing devices in your network.
 - a. Configure the settings that Cisco ANA will use to guide the network discovery process. You specify the discovery methods, seed device IP addresses, and hop counts for the discovery process. You can also specify dependent discovery methods, so the output from the dependent method is used as the input to another method, and further refine the list with filters.
 - b. Run the network discovery process from the GUI, to create the list of elements in your network.
2. Use Bulk VNE Import to create a seed file and import the devices into Cisco ANA.
 - a. From the list of devices found during the discovery process, select the devices that you want Cisco ANA to manage, and specify their credentials, polling settings, and scheme. This information is saved as the seed file.
 - b. Import the seed file to create the VNEs. Cisco ANA discovers the network element details, and uses this information to create a model of all network elements you want to manage.

To use these functions, you must have sufficient privileges. See [Roles Required to Manage VNEs, page 2-17](#).

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL**Understanding the Network Discovery User Interface**

The Network Discovery user interface is where you configure the criteria you want Cisco ANA to use to create the seed file, as described in [Configuring and Performing Network Discovery](#), page 2-28.

Figure 2-3 **Network Discovery User Interface**

**Related Topics**

- [Configuring and Performing Network Discovery](#), page 2-28
- [Importing Network Elements from a Seed File](#), page 2-33
- [Prerequisites for Adding VNEs to AVMs](#), page 2-21

Configuring and Performing Network Discovery

To perform network discovery, you must first configure the settings that will guide the network discovery process. Once that is done, you can start the network discovery process from the GUI, to create the list of elements in your network.

To perform network discovery, follow the procedures in these sections:

- [Creating the Network Discovery Configuration File](#), page 2-28
- [Running Network Discovery to Create a List of Network Elements](#), page 2-32

Creating the Network Discovery Configuration File

Cisco ANA discovers the elements in your network based on parameters that you provide, such as discovery method, seed devices, hop counts, and filters. Cisco ANA uses the loopback address to discover a network element. (If you do not want Cisco ANA to use the loopback address, you can disable this setting; see [Step 10](#) of the following procedure.) For your reference, a sample discovery configuration file is stored in *ANAHOME/Third_Party*.

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL

Use this procedure to create or edit a discovery configuration file.

Before You Begin

Make sure you have performed all prerequisites:

- [Device Configuration Tasks to Perform Before Adding VNEs, page 2-22](#)
- [Device Information to Gather Before Adding VNEs, page 2-24](#)

At a minimum, SNMP should be running on all devices and the devices should be reachable; otherwise, network discovery may fail or be incomplete.

-
- Step 1** In the Administration perspective, click the **Tasks** tab in the navigation pane and click the **NE Discovery and VNE Import** drawer.
- Step 2** Click **Network Discovery** (see [Figure 2-3 on page 2-28](#)).
- Step 3** If you have a saved configuration file that you want to use, perform these steps (otherwise, proceed to [Step 4](#)):
- Click **Import**. The Configuration List dialog box lists all configuration files that are stored in the *ANAHOME/Third_Party* directory (where *ANAHOME* is normally */export/home/ana41*). By default, two sample files are provided, and you should select *User-specific_settings.ad.xml* (the other file is not currently used).
 - Select the file and click **OK**. The Discovery Configuration Settings tree is populated with the file information.
 - If desired, you can rename the file by clicking **Edit** and entering the name in the Discovery Configuration Settings dialog box, and clicking **OK**.
- Step 4** (Mandatory) Modify (or verify) your basic discovery methods to be used to locate devices, starting with one or more devices (called the *seed devices*). You must configure a discovery method.
- In the Discovery Configuration Settings area, choose **Discovery Methods** from the tree. The configured discovery methods are displayed, based on the configuration file you imported in [Step 3](#).
 - Click **Add**. The Discovery Method Settings dialog box opens.
 - Choose a discovery method from the drop-down list. Make sure you meet the requirements for your chosen methods, or the results of the network discovery will be incomplete.

Table 2-13 **Discovery Methods Used by Network Discovery**

Discovery Method ¹	Description	Requirements
Neighbor	Uses the Cisco Discovery Protocol (CDP) to learn about the device type and SNMP agent address of network elements that are neighbors to the elements being queried.	CDP must be enabled.
Cluster	Processes the command switches in a DSBU cluster. The Cluster method queries the <i>ciscoClusterMIB</i> for all members of the cluster, then adds the members to the list.	CISCO-CLUSTER-MIB must be enabled.
Credential	Queries devices based on the supplied SNMP and enable credentials, and verifies the credentials for discovered devices.	Must have at least one dependent method from this table.

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL**Table 2-13** *Discovery Methods Used by Network Discovery (continued)*

Discovery Method ¹	Description	Requirements
PingSweep	Pings all devices in a given IP address range. You can also limit the sweep using subnets.	Device must be reachable. If dependent, must have the same seed IP address and hop counts as its parent method.
PingWithHop	Pings all IP addresses in the seed device ipTable, along with the next-hop router of those IP addresses, and adds the members to the list.	Device must be reachable.
RouterPeer	Queries the OSPF, BGP, or HSRP MIB. <i>Reviewers: Is HSRP correct? Someone said this was removed in 3.6.2.</i>	OSPF MIB must be enabled.
RoutingTable	Queries and analyzes the routing table of the seed routers to find all subnets and next-hop routers in the network. Cisco ANA traverses the routers to find their directly connected subnets, known networks, and next-hop routers as clues. Eventually Cisco ANA finds a router for every known subnet.	IP MIB must be enabled.
ARP	Queries and analyzes the seed routers' ARP table.	IP MIB must be enabled. Must have RoutingTable as a dependent method.

1. If you specify a hop count of 0, or do not specify a hop count at all, the entire network will be discovered if the devices are reachable with the given SNMP credentials.

- d. Enter an IP address and (optionally) the hop count. The hop count value limits discovery to the specified maximum hop count from the given seed device.

**Note**

If you specify a hop count of 0, or do not specify a hop count at all, the entire network will be discovered if the devices are reachable with the given SNMP credentials.

- e. Click **OK**. The information is added to the Discovery Configuration tree.

- f. Add additional discovery methods, as desired.

Step 5 For the discovery methods you configured in [Step 4](#), configure their dependent discovery methods. (All discovery methods use the System method as a dependent; the System method drives the entire discovery process.)

**Note**

This step is mandatory if you are using the Credential or ARP methods. See the requirements listed in [Table 2-13](#).

To configure dependent methods (so that the output from the dependent method is used as the input to the selected discovery method):

- a. Ensure that any dependent methods you plan to use are already configured, as described in [Step 4](#).

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL

- b. Choose **Discovery Methods** and click **Edit**. The Discovery Method Settings dialog box opens.
- c. Choose the discovery method to which you want to add a dependent method from the Choose a Discovery Method drop-down list.
- d. From the Choose Dependent Discovery Methods field, choose dependent methods by checking the appropriate check boxes. (All discovery methods depend on the System method; it drives the entire discovery process.)



Note The Credential method must have at least one dependent method, other than System. The ARP method must have RoutingTable as a dependent method. The dependent method PingSweep must have the same seed IP address and hop counts as its parent method.

- e. Click **Update**.
 - f. Configure additional dependent methods, as desired. (You can configure multiple dependents for any of the methods you configured in [Step 4.](#))
- Step 6** Verify your discovery settings in the Discovery Methods and Dependencies area by choosing the configured methods from the drop-down list and checking the settings. If you chose PingSweep as a dependent method, click the **Ping Settings** link and verify the submask settings.
- Step 7** (Mandatory) Specify the SNMP credentials you want the network discovery process to use when querying devices.
- a. Choose **SNMP Credentials** and click **Add**.
 - b. In the SNMP Credentials Settings dialog box, enter the credentials you want the Network Discovery process to use, and click **OK**.
- Step 8** (Optional) To refine the discovery methods by setting filters to determine whether a device should be included or excluded, choose a discovery method and click **Add**. The optional discovery settings are described in [Table 2-14](#).



Note If both exclude and include filters of the same type are used, the exclude filter is applied first.

Table 2-14 *Optional Network Discovery Settings and Filters*

Optional Discovery Setting	Description
Telnet Credentials	Uses the specified credentials when querying the discovered devices. (If the credentials match the discovered devices, the credentials are listed in the seed file; if they do not match, the credentials fields for those devices are left empty.)
IP Addresses Included	Includes the device if any of its IP addresses match the specified IP address.
IP Addresses Excluded	Excludes the device if any of its IP addresses match the specified IP address.
System OIDs Included	Includes the device if the system OID matches the specified OID.
System OIDs Excluded	Excludes the device if the system OID matches the specified OID.

DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL**Table 2-14 Optional Network Discovery Settings and Filters (continued)**

Optional Discovery Setting	Description
System Locations Included	Excludes the device if the sysLocation in MIB2 system table matches the specified system location.
System Locations Excluded	Excludes the device if the sysLocation in MIB2 system table matches the specified system location.
Domain Names Included	Includes the device if the domain name resolved by a DNS lookup on the IP address matches the specified domain name.
Domain Names Excluded	Excludes the device if the domain name resolved by a DNS lookup on the IP address matches the specified domain name.

- Step 9** To save the configuration file, click **Generate Configuration Files**. This does not start the discovery process that generates the seed file; it simply saves your criteria. By default, the file is saved on the gateway in *ANAHOME/Third_Party/User-Specific* settings.ad_xml (where *ANAHOME* is normally /export/home/ana41).
- Step 10** If you do not want to use the loopback address to discover network elements—for example, if you are using an out-of-band VLAN—edit the *ANAHOME/_Discovery_system_settings.ad_xml* file (where *ANAHOME* is normally /export/home/ana41) as follows:
- ```
PreferredMgmtIPMethod="None"
```
- Step 11** To schedule the discovery (or perform it immediately), proceed to [Running Network Discovery to Create a List of Network Elements](#), page 2-32.

**Running Network Discovery to Create a List of Network Elements**

Once you have set your discovery settings as described in [Configuring and Performing Network Discovery](#), page 2-28, you can perform (or schedule) the network discovery using the following procedure. You can then tailor the resulting list of network elements to create the seed file to add network elements to Cisco ANA.

The network discovery process creates a list of network elements in the network in *ANAHOME/Main/sfresources/deviceOut.xml* (where *ANAHOME* is normally /export/home/ana41). This file is used to populate the Bulk VNE Import page, as described in [Importing Network Elements from a Seed File](#), page 2-33.

- Step 1** In the Administration perspective, click the **Tasks** tab in the navigation pane and click the **NE Discovery and VNE Import** drawer.
- Step 2** Click **Network Discovery** and **Discovery Configuration Schedule**.
- Step 3** Set your schedule:
- To perform the discovery immediately, choose **Immediate** from the Run Type drop-down list, and click **Schedule Discovery Now**. Cisco ANA prompts you for confirmation and then provides job information. You can use this information to check on the status of the job using Job Management (see [Browsing and Controlling Jobs](#), page 13-3).



**DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL**

- To perform the discovery at a later time, choose **Schedule** from the Run Type drop-down list, set your criteria, and click **Schedule Discovery Now**. If desired, you can set the discovery to run at regular intervals, to add new network elements.

The length of the Network Discovery process depends on the discovery methods used and the number of devices found. When the discovery process is done, the Job Management browser displays it as having a Completed state. See [Browsing and Controlling Jobs, page 13-3](#) for more information.

**Related Topics**

- [Roles Required to Manage VNEs, page 2-17](#)
- [Importing Network Elements from a Seed File, page 2-33](#)
- [Understanding VNE Status and VNE States, page 2-17](#)
- [Defining and Creating Individual VNEs, page 2-35](#)
- [Prerequisites for Adding VNEs to AVMs, page 2-21](#)

**Importing Network Elements from a Seed File**

Once the network discovery process has found the elements in the network according to your discovery criteria, you can list the elements on the Bulk VNE Import page. From this list, you can specify which elements you want to add to Cisco ANA, and save the modified list. This modified list is your seed file. Finally, you import the network elements listed in the seed file (by clicking **Import Devices**). After the network elements are imported, you must start the VNEs.

When the network elements are imported and VNEs are created, Cisco ANA traverses the network to fully discover the network elements and uses this information to create the model of the network. Cisco ANA uses internal algorithms (from the Cisco ANA *cookbook*) to allocate the VNEs among AVMs, based on the i and bandwidth required by the various network elements. (By default, Cisco ANA uses the cookbook located in *ANAHOME/Main/sfresources/cookbooksample.xml*. For information on adding single VNEs and allocating them to AVMs, see [Defining and Creating Individual VNEs, page 2-35](#).)

Cisco ANA does not automatically start the VNEs because, in large-scale deployments, this could negatively impact system performance. If you want to change Cisco ANA's default behavior so that VNEs are started after being added, contact ask-ana@cisco.com for instructions.

When you create your seed file, it is saved in the *ANAHOME/Main/sfresources* directory. By default, the file is named *SeedOutput-date-hhmmss.xml*.


**Before You Begin**

- Make sure the Network Discovery job has completed before importing any VNEs (see [Browsing and Controlling Jobs, page 13-3](#)).
- Make sure you have the credentials and scheme information required. See [Device Information to Gather Before Adding VNEs, page 2-24](#) and [Choosing a Scheme when Adding Individual VNEs, page 2-25](#).

Use this procedure to

- 
- Step 1** In the Administration perspective, click the **Tasks** tab in the navigation pane and click the **NE Discovery and VNE Import** drawer.
- Step 2** Click **Bulk VNE Import**. The page is automatically populated with the devices that Cisco ANA found during the network discovery process (*ANAHOME/Main/sfresources/deviceOut.xml*).

**DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL**

- Step 3** Select the devices you want Cisco ANA to manage, and enter their credentials. If desired, you can use the filter above the device list to narrow the list.
- a. On the left side of the workspace, right-click the devices which can have identical credentials and polling settings, and enter the settings. The instructions for entering VNE credentials and polling settings are described in [Defining and Creating Individual VNEs, page 2-35](#), [Step 4](#) through [Step 7](#). (That section includes some settings you will not see when using Bulk VNE Import, such as entering a Type in the Identification Area; the VNE type is discovered by the network discovery process.)
-  **Note** If you enter the wrong credential information when adding the VNE, the VNE will not be successfully added and managed. In this case, you will have to correct the credentials and restart the VNE (see [Changing VNE Status \(Start, Stop, Maintenance\), page 2-44](#)). However, Telnet credentials can be changed in runtime, without having to restart the VNE.
- b. Use the various Add and Remove buttons to move your seed devices to the right side of the workspace.
- Step 4** Enter a seed file name in the Enter Seed File Name field. The file is saved in the *ANAHOME/Main/sfresources* directory. By default, the file is named *SeedOutput-date-hhmmss.xml*; for example, *SeedOutput-Jul02-041442.xml*. If you entered *MySeedFile* as the name, the filename would be *MySeedFile-Jul02-041442.xml*.
- Step 5** Click **Import Devices**. In the back end, the seed file is converted into a format that the VNE creator can recognize, and the VNEs are created and added to AVMs.
- Step 6** Verify that the import job has completed. See [Browsing and Controlling Jobs, page 13-3](#).
- Step 7** When the import is complete, start the VNEs (you can do this in a bulk operation):
- a. Click the **Objects** tab and click the **ANA Servers** drawer.
  - b. Open the Servers tree, and click the AVM that contains the VNEs which you want to start.
  - c. Right-click the VNEs and choose **Start**. The page is updated as the VNEs are started; each VNE should list:
    - Admin Status: Enabled
    - Operational Status: Up
  - d. To verify that the network element has been completely modeled, go to the Inventory perspective. In the device browser, icons indicate if there are any problems (see the network element management state icons, which are described in [Icon Reference, page G-1](#)).

---

To check the results of the VNE import, view the log file at *ANAHOME/Main/logs/SeedFile.log* (where *ANAHOME* is the installation directory, normally */export/home/ana40*).

*Reviewers: (1) Since there is no log file, if user does not have console open, how can they check results to see if it was successful (apart from checking job)?*

**Related Topics**

- [Roles Required to Manage VNEs, page 2-17](#)
- [Configuring and Performing Network Discovery, page 2-28](#)
- [Understanding VNE Status and VNE States, page 2-17](#)
- [Defining and Creating Individual VNEs, page 2-35](#)

**DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL**

- [Prerequisites for Adding VNEs to AVMs, page 2-21](#)

## Defining and Creating Individual VNEs

**Note**

A new VNE cannot be added to AVMs 0-100 and AVM 199 because those AVMs are reserved.

This topic explains how to add individual VNEs to Cisco ANA. You can define and manage SNMP, Telnet/SSH, ICMP, and polling information for the appropriate VNEs in the New VNE dialog box. If desired, you can create VNEs that perform reachability testing, through ICMP only. Do this by creating the VNE, choosing ICMP for the VNE type, and defining the details in the ICMP area.

**Note**

By default, when a VNE opens a Telnet session with a network element in order to model and monitor the element, the Telnet session remains open as long as the VNE is up. The VNE will not close the session due to any timeouts. If you would like to configure a timeout, contact [ask-ana@cisco.com](mailto:ask-ana@cisco.com) for assistance.

To add VNEs in bulk based on the devices in your current network, use the procedure described in [Using Network Discovery to Add Bulk VNEs, page 2-27](#).

### Before You Begin

Make sure you have performed all prerequisite activities:

- [Device Configuration Tasks to Perform Before Adding VNEs, page 2-22](#)
- [Device Information to Gather Before Adding VNEs, page 2-24](#)
- [Choosing a Scheme when Adding Individual VNEs, page 2-25](#)

If you do not perform these prerequisite activities, the VNEs may not be correctly discovered and managed.

**Step 1** In the Administration perspective, click the **Objects** tab and click the **ANA Servers** drawer.

*Reviewers: If user has multiple user-defined AVMs, how do they know which AVM they should add the VNE to? For autodiscovery/import, ANA takes care of this. Can we give any guidance to user?*

**Step 2** Open the Servers tree and find the AVM to which you want to add the VNE. Right-click the AVM and choose **New VNE**. The New VNE dialog box opens.

**Step 3** Enter the VNE general information. At a minimum, you must enter the VNE name and IP address.

| Field                      | Description                                                                                                                 |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>Identification Area</b> |                                                                                                                             |
| Name                       | The name of the VNE, which will be used as a unique key in Cisco ANA. It is also used for commands that manipulate the VNE. |
| IP Address                 | The IP address of the network element.                                                                                      |

**DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL**

| Field  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type   | Defines the protocol Cisco ANA will use to model the element, and the extent to which you want the element to be modeled. (If you are using network discovery, the network discovery process will automatically recognize the type. For more information on network discovery, see <a href="#">Using Network Discovery to Add Bulk VNEs, page 2-27</a> .)                                                                                                                                                                                               |
|        | Auto Detect Use this type if SNMP is enabled on the element. Cisco ANA will use SNMP to gather all available inventory information.                                                                                                                                                                                                                                                                                                                                                                                                                     |
|        | Generic SNMP Use this type if SNMP is enabled on the element, and either Cisco ANA does not support the element, or Cisco ANA does support the element but you only want basic information to be modeled. Cisco ANA will use SNMP to gather the most basic inventory information that is normally provided by all network elements.                                                                                                                                                                                                                     |
|        | ICMP Use this type if ICMP is enabled on the element, and either Cisco ANA does not support the element, or Cisco ANA does support the element but you only want basic information to be modeled. Cisco ANA will use ICMP to gather the most basic inventory information that is normally provided by all network elements, and will perform reachability testing only.                                                                                                                                                                                 |
| Scheme | Defines the VNE modeling components investigated during the discovery process and then populated in the VNE model. This enables the administrator to define different behavior for some network elements; for example, some network elements poll only with SNMP, and other network elements poll with Telnet. Soft properties and activation scripts are also attached to a specific scheme. By default, the VNE inherits the VNE scheme from the default scheme. Where more than one scheme exists in the network, the VNE loads the selected scheme. |
|        | For Cisco IOS devices, you can use the Foundation or MPLS scheme, depending on the technologies you want to manage. For information on supported technologies, schemes, and device types, see <a href="#">Cisco Active Network Abstraction VNE Reference</a> .                                                                                                                                                                                                                                                                                          |
|        | <b>Note</b> If desired, you can change the VNE scheme in runtime. See <a href="#">Viewing and Editing VNE Properties and Schemes, page 2-43</a> .                                                                                                                                                                                                                                                                                                                                                                                                       |
|        | Foundation <ul style="list-style-type: none"> <li>• Cisco CatOS device family.</li> <li>• Cisco IOS device family, when you do not need to support technologies related to MPLS and Carrier Ethernet (see <a href="#">Using Network Discovery to Add Bulk VNEs, page 2-27</a>).</li> <li>• Other vendor device families.</li> </ul>                                                                                                                                                                                                                     |
|        | MPLS <ul style="list-style-type: none"> <li>• Cisco IOS device family, when supporting technologies related to MPLS and Carrier Ethernet (see <a href="#">Using Network Discovery to Add Bulk VNEs, page 2-27</a>).</li> <li>• Cisco IOS XR device family.</li> </ul>                                                                                                                                                                                                                                                                                   |
|        | <del>MPLSIOSXR</del> <ul style="list-style-type: none"> <li>• <del>Cisco IOS XR device family.</del></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                         |

**DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL**

| Field                          | Description                                                                                                                                                                                                                                                                                          |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Context                        | Specifies the default context for devices that support multiple contexts . ( <i>Context</i> is the term that some vendors use to signify a virtual router). The key name ensures that the proper community settings are not overwritten, so that Cisco ANA can discover and investigate the devices. |
| local                          | <ul style="list-style-type: none"> <li>Redback device family</li> </ul>                                                                                                                                                                                                                              |
| default                        | <ul style="list-style-type: none"> <li>Juniper device family</li> </ul> <p><i>Are we supporting context for Juniper devices in 4.1?</i></p>                                                                                                                                                          |
| generic                        | <ul style="list-style-type: none"> <li>All other device families (this is the default)</li> </ul>                                                                                                                                                                                                    |
| <b>Initial/VNE Status Area</b> |                                                                                                                                                                                                                                                                                                      |
| Status                         | Sets the initial disposition of the VNE. Normally you should set it to Start. You may not want to do this if you want to verify the VNE configuration, or if you know the VNE is very complex and might need extra processing to complete the loading procedure.                                     |
| Stop                           | Do not load the VNE (default).                                                                                                                                                                                                                                                                       |
| Start                          | Load the VNE and start collecting data.                                                                                                                                                                                                                                                              |
| Maintenance                    | Start the VNE but change it to the Maintenance investigation state.                                                                                                                                                                                                                                  |
| <b>Location Area</b>           |                                                                                                                                                                                                                                                                                                      |
| ANA Unit                       | The IP address of the unit that hosts the VNE's AVM. This information is prepopulated.                                                                                                                                                                                                               |
| AVM                            | The AVM on the unit that hosts the VNE. This information is prepopulated.                                                                                                                                                                                                                            |

**Step 4** Enter the VNE SNMP information to support polling and network element access:



**Note** For Cisco IOS XR devices, use the default settings.



**Note** If you enter the wrong credential information when adding the VNE, the VNE will not be successfully added and managed. In this case, you will have to correct the credentials and restart the VNE (see [Changing VNE Status \(Start, Stop, Maintenance\)](#), page 2-44). However, Telnet credentials can be changed in runtime, without having to restart the VNE.

| Field                      | Description                                                                                                                                                                                                                                            |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SNMP Version Area</b>   |                                                                                                                                                                                                                                                        |
| Enable SNMP                | Check this check box to enable the SNMP communication protocol so that the user can work with it. A VNE can have SNMP enabled or disabled at any time; however, when the Auto Detect check box is checked (in the General tab), it cannot be disabled. |
| ( <i>SNMP version</i> )    | Click the radio button for the SNMP version you plan to use: SNMP V1, SNMP V2, or SNMP V3.                                                                                                                                                             |
| <b>SNMP V1/V2 Settings</b> |                                                                                                                                                                                                                                                        |

**DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL**

| Field                                                     | Description                                                                                                                                                                                            |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Community String                                          | The SNMP community string settings. These are enabled only when SNMP V1 or V2 is selected:                                                                                                             |
|                                                           | Read<br>The SNMP read community status, public (default) or private, as defined by the user.                                                                                                           |
|                                                           | Write<br>The SNMP write community status, public or private (default), as defined by the user.                                                                                                         |
| <b>SNMP V3 Settings</b>                                   |                                                                                                                                                                                                        |
| These settings are enabled only when SNMP V3 is selected. |                                                                                                                                                                                                        |
| Authentication                                            | Choose one of the following authentication methods. The default is No authentication. <ul style="list-style-type: none"> <li>No</li> <li>md5</li> <li>sha</li> </ul>                                   |
|                                                           | User<br>This field is enabled if you choose any method other than No authentication. Enter the authentication username.                                                                                |
|                                                           | Password<br>This field is enabled if you choose any method other than No authentication. Enter the authentication password.                                                                            |
| Encryption                                                | Choose one of the following encryption methods. The default is No encryption. <ul style="list-style-type: none"> <li>No</li> <li>des</li> <li>aes128</li> <li>aes192</li> <li>aes256</li> </ul>        |
|                                                           | Password<br>This field is enabled if you choose any method other than No encryption. Enter the encryption password.                                                                                    |
| Auto Discover                                             | Instructs Cisco ANA to automatically discovery the device's unique engine ID. We recommend that you check this box.                                                                                    |
| Engine ID                                                 | Unique engine ID for the device. Leave this blank if you checked Auto Discover; the Engine ID will be discovered using the discovery protocol. (The Engine ID is required for the SNMP V3 connection.) |

**Step 5** Enter the VNE Telnet/SSH information to define the Telnet command sequence and to enable SSH for network element access (reachability) and investigation.

| Field                         | Description                                                                                                                                                                                                                               |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Protocol Settings Area</b> |                                                                                                                                                                                                                                           |
| Enable                        | Check this check box to enable the communication protocol so Cisco ANA will investigate the network element. Checking this check box activates the Login Sequence area. You can enable or disable the communication protocol at any time. |

**DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL**

| Field                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |        |     |                  |                  |                  |                 |          |            |                |                      |        |     |                  |                 |                       |               |                  |                 |                    |               |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|-----|------------------|------------------|------------------|-----------------|----------|------------|----------------|----------------------|--------|-----|------------------|-----------------|-----------------------|---------------|------------------|-----------------|--------------------|---------------|
| Protocol                        | <p>Choose one protocol from the drop-down list (the default is Telnet):</p> <ul style="list-style-type: none"> <li>Telnet</li> <li>SSHv1</li> <li>SSHv2</li> </ul> <p><b>Note</b> By default, when a VNE opens a Telnet session with a network element in order to model and monitor the element, the Telnet session remains open as long as the VNE is up. The VNE will not close the session due to any timeouts. If you would like to configure a timeout, contact ask-ana@cisco.com for assistance.</p>                                                                                                                                                                                                                                                                                                                                                                                                                           |        |     |                  |                  |                  |                 |          |            |                |                      |        |     |                  |                 |                       |               |                  |                 |                    |               |
| Port                            | <p>This field is prepopulated, depending on your protocol choice:</p> <ul style="list-style-type: none"> <li>23—Default port for Telnet.</li> <li>22—Default port for SSHv1 or SSHv2.</li> </ul> <p>You can also edit the port number displayed.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |        |     |                  |                  |                  |                 |          |            |                |                      |        |     |                  |                 |                       |               |                  |                 |                    |               |
| <b>Login Sequence Area</b>      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |        |     |                  |                  |                  |                 |          |            |                |                      |        |     |                  |                 |                       |               |                  |                 |                    |               |
| Prompt and Run                  | <p>The network element's expected prompt, and the string Cisco ANA should send to the network element (when the expected prompt is detected). Entering a string in the Prompt field activates the Run field. After making your entries in the Prompt and Run fields, click <b>Add</b> to add them to the login sequence. Click <b>Remove</b> to remove any lines.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |        |     |                  |                  |                  |                 |          |            |                |                      |        |     |                  |                 |                       |               |                  |                 |                    |               |
| Telnet                          | <p>Enter the Telnet information. The sequence (the order of the commands) must end with a line that includes only the prompt field. (You can also change these credentials in runtime.)</p> <ul style="list-style-type: none"> <li>For Cisco IOS XR devices (to go to XML mode): <table> <tr> <td>Prompt</td><td>Run</td></tr> <tr> <td><b>Username:</b></td><td><i>user name</i></td></tr> <tr> <td><b>Password:</b></td><td><i>password</i></td></tr> <tr> <td><b>#</b></td><td><b>xml</b></td></tr> <tr> <td><b>XML&gt;</b></td><td><i>(leave blank)</i></td></tr> </table> </li> <li>For Cisco IOS devices: <table> <tr> <td>Prompt</td><td>Run</td></tr> <tr> <td><b>Password:</b></td><td><i>password</i></td></tr> <tr> <td><i>devicename&gt;</i></td><td><b>enable</b></td></tr> <tr> <td><b>Password:</b></td><td><i>password</i></td></tr> <tr> <td><i>devicename#</i></td><td><b>enable</b></td></tr> </table> </li> </ul> | Prompt | Run | <b>Username:</b> | <i>user name</i> | <b>Password:</b> | <i>password</i> | <b>#</b> | <b>xml</b> | <b>XML&gt;</b> | <i>(leave blank)</i> | Prompt | Run | <b>Password:</b> | <i>password</i> | <i>devicename&gt;</i> | <b>enable</b> | <b>Password:</b> | <i>password</i> | <i>devicename#</i> | <b>enable</b> |
| Prompt                          | Run                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |        |     |                  |                  |                  |                 |          |            |                |                      |        |     |                  |                 |                       |               |                  |                 |                    |               |
| <b>Username:</b>                | <i>user name</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |        |     |                  |                  |                  |                 |          |            |                |                      |        |     |                  |                 |                       |               |                  |                 |                    |               |
| <b>Password:</b>                | <i>password</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |        |     |                  |                  |                  |                 |          |            |                |                      |        |     |                  |                 |                       |               |                  |                 |                    |               |
| <b>#</b>                        | <b>xml</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |        |     |                  |                  |                  |                 |          |            |                |                      |        |     |                  |                 |                       |               |                  |                 |                    |               |
| <b>XML&gt;</b>                  | <i>(leave blank)</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |        |     |                  |                  |                  |                 |          |            |                |                      |        |     |                  |                 |                       |               |                  |                 |                    |               |
| Prompt                          | Run                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |        |     |                  |                  |                  |                 |          |            |                |                      |        |     |                  |                 |                       |               |                  |                 |                    |               |
| <b>Password:</b>                | <i>password</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |        |     |                  |                  |                  |                 |          |            |                |                      |        |     |                  |                 |                       |               |                  |                 |                    |               |
| <i>devicename&gt;</i>           | <b>enable</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |        |     |                  |                  |                  |                 |          |            |                |                      |        |     |                  |                 |                       |               |                  |                 |                    |               |
| <b>Password:</b>                | <i>password</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |        |     |                  |                  |                  |                 |          |            |                |                      |        |     |                  |                 |                       |               |                  |                 |                    |               |
| <i>devicename#</i>              | <b>enable</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |        |     |                  |                  |                  |                 |          |            |                |                      |        |     |                  |                 |                       |               |                  |                 |                    |               |
| SSH V1 and V2                   | <p>Enter the SSH information. This sequence is usually shorter than the corresponding Telnet login sequence, because the username or password may already be sent during the process of establishing the SSH session. Cisco recommends that you first use any SSH client application (such as UNIX SSH or OpenSSH) to determine the device SSH login sequence, and then enter that information.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |        |     |                  |                  |                  |                 |          |            |                |                      |        |     |                  |                 |                       |               |                  |                 |                    |               |
| Hide the Run value while typing | <p>Check this check box if you do not want the Run string displayed as clear text while you enter it in the field.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |        |     |                  |                  |                  |                 |          |            |                |                      |        |     |                  |                 |                       |               |                  |                 |                    |               |

**DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL**

| Field                 | Description                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Confirm               | This field is activated if you checked the Hide the Run value while typing check box. Re-enter the Run string.                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Add and Remove        | Use these buttons to add or remove the prompt and run strings.                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| SSHv1 Area            |                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Username              | Enter the device name.                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Password              | Enter the device password.                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Cipher                | Choose the data encryption algorithm. By default, all methods are used. <ul style="list-style-type: none"><li>• DES—Use the Data Encryption Standard algorithms.</li><li>• 3DES—Use the Triple Data Encryption Standard algorithm.</li><li>• Blowfish—Use the blowfish algorithms.</li></ul> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| SSHv2 Area            |                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Username              | Enter the SSHv2 username.                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Client Authentication | Choose the client-driven authentication method from the drop-down list.                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                       | Password                                                                                                                                                                                                                                                                                     | Use a password to authenticate the client. Enter the password in the Password field.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|                       | public-key                                                                                                                                                                                                                                                                                   | Optionally, use public key authentication, which uses a key pair system in which the client application is configured with the secret private key, and the device is configured with the public nonsecret key (of this pair). <ul style="list-style-type: none"><li>• Private Key—Enter the private key, click <b>Import</b> to import the private key, or click <b>Generate</b> to generate the key.</li><li>• Public Key—Optionally, enter the public key or click <b>Import</b> to import the public key. The application will verify that the public and private keys are part of a pair.</li></ul> |



**DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL**

| Field                             | Description                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server Authentication             | Choose a server authentication method from the drop-down list.                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                                   | none                                                                                                                                                                                                                                                                                                             | No server authentication. (This method does not do any authentication and is not recommended, because it poses a security risk for “man-in-the-middle” attacks.)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|                                   | pre-configured                                                                                                                                                                                                                                                                                                   | <p>Use the server public key or fingerprint that was configured in the application event before the first connection was attempted. This is the default and is the recommended method. Selecting this method activates the Finger Print or Public Key field.</p> <p>Select one of the following (and be sure to read the information in the Host Key Algorithm section):</p> <ul style="list-style-type: none"> <li>Finger Print—Click to use a short checksum of the server public key (this serves the same purpose, but is much shorter).</li> <li>Public Key—Click to use the public key in one of the permitted formats (see <a href="#">Public Key and Private Key File Formats</a>, page 2-24). Enter the public key or click <b>Import</b> to import the key.</li> </ul> |
|                                   | save-first-auth                                                                                                                                                                                                                                                                                                  | <p>Use the public key that was used for the first connection attempt with the server. This method assumes the first connection was legitimate. (A security risk exists if the connection was compromised.)</p> <p>After the first connection, the server authentication method is changed to preconfigured, and the public key data is inserted as the preconfigured data.</p>                                                                                                                                                                                                                                                                                                                                                                                                   |
| Key Exchange <sup>1</sup>         | <p>Choose a key exchange algorithm. The default is none.</p> <ul style="list-style-type: none"> <li>diffie-hellman-group1-sha1</li> <li>diffie-hellman-group1-exchange-sha1</li> </ul>                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| MAC <sup>1</sup>                  | <p>Choose a MAC algorithm for key generation. The default is none.</p> <ul style="list-style-type: none"> <li>sha1</li> <li>md5</li> <li>sha1-96</li> </ul>                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Cipher <sup>1</sup>               | <p>Choose a cipher:</p> <ul style="list-style-type: none"> <li>3des—Use the Triple Data Encryption Standard algorithms.</li> <li>aes-128—Use the Advanced Encryption Standard 128.</li> <li>aes-192—Use the Advanced Encryption Standard 192.</li> </ul>                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Host Key Algorithm <sup>1,2</sup> | <p>Choose a host key algorithm (up to 2048-bit keys are officially supported). See <a href="#">Public Key and Private Key File Formats</a>, page 2-24 for valid file formats.</p> <ul style="list-style-type: none"> <li>dsa—Use the Digital Signature Algorithm.</li> <li>rsa—Use the RSA algorithm.</li> </ul> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

1. You can select multiple algorithms by pressing Ctrl while choosing a method. If more than one is selected, the application will try to use all of the algorithms until one is accepted by the server. There is no priority in the way the algorithms are tried. Also, encryption algorithms may have multiple known versions (for example, 3DES has 3des-cbc, 3des-ecb, 3des-cfb, 3des-ofb, 3des-ctr).
2. There are several file formats for public and private RSA and DSA keys. Cisco ANA officially supports the OpenSSH format (see <http://www.openssh.com/manual.html>).

**DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL**

- Step 6** If you chose ICMP as the VNE type in [Step 3](#), enter the ICMP polling rate you want Cisco ANA to use to verify reachability. You can define the polling rate in seconds for the VNE.

| Field        | Description                                                                                                                                                                            |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable       | Check this check box to instruct Cisco ANA to use the ICMP communication protocol to verify that the network element is reachable. You can enable or disable ICMP polling at any time. |
| Polling Rate | Enter an ICMP polling rate (in seconds).                                                                                                                                               |

- Step 7** Enter the VNE Polling Information to associate a VNE with a previously created polling group, or customize different polling settings according to the type of VNE information you want (status, configuration, and so forth). For information on the settings in the default and slow polling groups, see [Table 13-2 on page 13-5](#).)



**Note** Increasing polling rates may result in excess traffic and cause the network element to crash.

| Field                         | Description                                                                                                                                                                                                                              |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Polling Group Area</b>     |                                                                                                                                                                                                                                          |
| Group                         | Select Group if you want to use polling rates from one of the polling groups listed in the drop-down list. If you do not select a group in the list, Cisco ANA will use the default polling group.                                       |
| Instance                      | Select Instance to change the polling rates of any one of the built-in polling intervals displayed in the dialog box. When you select Instance, the Polling Intervals and Topology areas are activated.                                  |
| <b>Polling Intervals Area</b> |                                                                                                                                                                                                                                          |
| Status                        | Sets the polling rate for status-related information, such as network element status (up or down), port status, admin status, and so on. The information is related to the operational and administrative status of the network element. |
| Configuration                 | Sets the polling rate for configuration-related information, such as VC tables, scrambling, and so on.                                                                                                                                   |
| System                        | Sets the polling rate for system-related information, such as network element name, network element location, and so on.                                                                                                                 |
| Routing Forwarding            | Sets the polling rate for routing-table related information, such as VRF and IGP/BGP routes.                                                                                                                                             |
| <b>Topology Area</b>          |                                                                                                                                                                                                                                          |
| Layer 1                       | Sets the polling rate of the topology process as an interval for the Layer 1 counter. This is an ongoing process.                                                                                                                        |
| Layer 2                       | Sets the polling rate of the topology process as an interval for the Layer 2 counter. This process is available on demand.                                                                                                               |

- Step 8** To create the VNE, click **OK**. (The **OK** button in the New VNE dialog box is enabled only when you enter the VNE name and IP address (mandatory fields) in the General tab.)

**DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL**

The VNE is loaded into the bootstrap of its unit, and Cisco ANA starts investigating the network element. Cisco ANA builds a live model of the network element, including its physical and logical inventory, its configuration, and its status. Cisco ANA also creates the registry information of the new VNE in the unit. After a few minutes, verify that the Admin Status is Enabled and the Operational Status is Up.

**Related Topics**

- [Public Key and Private Key File Formats](#), page 2-24
- [Understanding VNE Status and VNE States](#), page 2-17
- [Changing VNE Status \(Start, Stop, Maintenance\)](#), page 2-44
- [Viewing and Editing VNE Properties and Schemes](#), page 2-43
- [Moving One or More VNEs](#), page 2-45
- [Deleting a VNE](#), page 2-46
- [Roles Required to Manage VNEs](#), page 2-17

**Viewing and Editing VNE Properties and Schemes**

After a VNE is added, you can view and edit its properties , such as the status and Telnet settings. Use this procedure to view and edit a VNE's properties.

**Note**

If you change the Telnet credentials, you do not have to restart the VNE. However, for all other changes, you must restart the VNE.

**Step 1** In the Administration perspective, click the **Objects** tab and click the **ANA Servers** drawer.

**Step 2** Open the Servers tree, and locate and click the AVM that contains the VNE in which you are interested. All VNEs in that AVM are displayed in a table below the AVM workspace.

The various fields displayed in the table are described in detail in [Defining and Creating Individual VNEs](#), page 2-35; however, the following is a summary of what is provided in the table:

| Field              | Description                                                                                                                                                             |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Key                | A string that uniquely identifies a VNE in the system, across all units and AVMs.                                                                                       |
| Admin Status       | The status of the relationship between the VNE and its parent AVM (see <a href="#">VNE Status (Operational and Admin Status)</a> , page 2-17).                          |
| Operational Status | The status of the relationship between the VNE and the real network element it is managing (see <a href="#">VNE Status (Operational and Admin Status)</a> , page 2-17). |
| IP Address         | The IP address of the network element.                                                                                                                                  |
| Maintenance        | Whether the network element is in the Maintenance network element management state.                                                                                     |
| Up Since           | When the VNE was last started.                                                                                                                                          |
| SNMP               | Whether the VNE is using SNMP for investigation and reachability.                                                                                                       |
| Telnet             | Whether the VNE is using Telnet for investigation and reachability.                                                                                                     |

**DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL**

| Field         | Description                                                      |
|---------------|------------------------------------------------------------------|
| Element Class | The VNE type, defined when the VNE was added.                    |
| Element Type  | The network element family to which the network element belongs. |
| Polling Group | The polling group to which the parent AVM/unit belongs.          |

**Step 3** To edit a VNE, or for more details about a VNE, right-click the VNE and choose **Edit**. You can edit the following fields:

- VNE schemes
- VNE SNMP version and settings
- All VNE ICMP settings
- All VNE Telnet/SSH settings
- All VNE Polling settings

For more details about the fields displayed in the VNE Properties dialog box, see [Defining and Creating Individual VNEs, page 2-35](#).

**Step 4** Close the VNE workspace and save your changes.

**Step 5** If you changed anything other than the Telnet credentials, you must restart the VNE for the changes to take effect. (Changing Telnet credentials does not require a VNE restart.)

#### Related Topics

- [Understanding VNE Status and VNE States, page 2-17](#)
- [Changing VNE Status \(Start, Stop, Maintenance\), page 2-44](#)
- [Viewing and Editing VNE Properties and Schemes, page 2-43](#)
- [Moving One or More VNEs, page 2-45](#)
- [Deleting a VNE, page 2-46](#)
- [Roles Required to Manage VNEs, page 2-17](#)

## Changing VNE Status (Start, Stop, Maintenance)

VNE status represents the existing condition of the VNE process, including whether the VNE is communicating with the real device it represents. You can start or stop a VNE, or change it to the Maintenance investigation state.

When you restart a VNE, Cisco ANA builds the VNE model using stored persistency information, and then starts receiving information from the network element. This saves time by enabling quick loading. For information on VNE persistency, see [Appendix F, “VNE Persistency Mechanism.”](#)

To change the VNE’s status:

**Step 1** In the Administration perspective, click the **Objects** tab and click the **ANA Servers** drawer.

**Step 2** Open the Servers tree, and click the AVM that contains the VNE in which you are interested. All VNEs in that AVM are displayed in a table in the workspace.

**Step 3** Right-click the VNE and choose **Start**, **Stop**, or **Maintain**.

**DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL**

- Step 4** The status of the VNE changes based on your selection:
- If the VNE is started, a confirmation message is displayed. Click **OK**. An Up status is eventually displayed in the VNE properties table. (You may see a Starting Up status when, for example, the Server is overloaded or the VNE is still being loaded.)
  - If the VNE is stopped, a confirmation message is displayed. Click **OK**. A Down status is eventually displayed in the VNE properties table. You may see a Shutting Down status while various processes are closing down.
  - If the VNE is changed to Maintenance mode, a confirmation message is displayed. Click **OK**. A Maintenance status is displayed in the VNE properties table.

For information about VNE data that is persisted (saved on the unit), see [VNE Persistency Mechanism](#), page F-1.

**Related Topics**

- [Understanding VNE Status and VNE States](#), page 2-17
- [Defining and Creating Individual VNEs](#), page 2-35
- [Viewing and Editing VNE Properties and Schemes](#), page 2-43
- [Moving One or More VNEs](#), page 2-45
- [Deleting a VNE](#), page 2-46
- [Roles Required to Manage VNEs](#), page 2-17

## Moving One or More VNEs

You can move single and multiple VNEs between AVMs. The VNEs that are moved are unloaded from the old unit, and after they are reloaded on the new unit, their original status is maintained.

To move a single VNE or multiple VNEs:

- Step 1** In the Administration perspective, click the **Objects** tab and click the **ANA Servers** drawer.
- Step 2** Open the Servers tree, and locate and click the AVM that contains the VNE in which you are interested. All VNEs in that AVM are displayed in a table in the workspace.
- Step 3** Right-click one or more VNEs and choose **Move VNEs**.  
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 to display and hide information.
- Step 4** In the Move To dialog box, browse to and choose the AVM (branch) where you want to move the VNEs.
- Step 5** Click **OK**. The VNE is moved to its new location, and now appears beneath the selected AVM (branch) in the VNE properties table.

**Related Topics**

- [Understanding VNE Status and VNE States](#), page 2-17

**DRAFT - 23 JULY 2008 - CISCO CONFIDENTIAL**

- [Defining and Creating Individual VNEs, page 2-35](#)
- [Viewing and Editing VNE Properties and Schemes, page 2-43](#)
- [Changing VNE Status \(Start, Stop, Maintenance\), page 2-44](#)
- [Deleting a VNE, page 2-46](#)
- [Roles Required to Manage VNEs, page 2-17](#)

## Deleting a VNE

You can delete a VNE from an AVM (and its unit). When you delete a VNE, Cisco ANA stops the VNE and deletes all VNE references from the system and golden source, which 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. If the VNE has any static links, you must remove them before removing the VNE (dynamic links are automatically removed).

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

### Before You Begin

If the VNE you plan to delete has any static links, remove them. Dynamic links are automatically removed.

- 
- |               |                                                                                                                                                                        |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the Administration perspective, click the <b>Objects</b> tab and click the <b>ANA Servers</b> drawer.                                                               |
| <b>Step 2</b> | Open the Servers tree, and locate and click the AVM that contains the VNE in which you are interested. All VNEs in that AVM are displayed in a table in the workspace. |
| <b>Step 3</b> | Right-click the VNE and choose <b>Delete</b> . A warning message is displayed.                                                                                         |
| <b>Step 4</b> | Click <b>Yes</b> . A confirmation message is displayed.                                                                                                                |
| <b>Step 5</b> | Click <b>OK</b> . The selected VNE is deleted from the AVM, and is no longer displayed in the VNE properties table.                                                    |
- 

### Related Topics

- [Understanding VNE Status and VNE States, page 2-17](#)
- [Defining and Creating Individual VNEs, page 2-35](#)
- [Viewing and Editing VNE Properties and Schemes, page 2-43](#)
- [Changing VNE Status \(Start, Stop, Maintenance\), page 2-44](#)
- [Moving One or More VNEs, page 2-45](#)
- [Roles Required to Manage VNEs, page 2-17](#)