Using Discovery

Open the Discovery application by clicking **Discovery** in the Task Bar, selecting **Discovery** from the **Applications** menu, or by clicking the Discovery icon in the Topology Toolbar. The Discovery application provides a wizard-like interface that enables you to easily discover the following:

- Alcatel devices in the network.
- The links between devices in the network. This information is used to display network links in graphical maps of network regions.
- Additional link information required by OmniVista's Locator application.
- VLAN information required by OmniVista's VLAN application.
- Third-party devices built by Cisco, 3Com, and Extreme.
- Any additional third-party devices for which support has been added via the Third Party Device Support Preferences window in the Preferences application.

SNMP Setups

The Discovery Wizard now provides the ability to create SNMP Setups that can be selected for individual discoveries. An SNMP Setup specifies:

- The version of SNMP to be used for the discovery (SNMPv1, SNMPv2, or SNMPv3) and the parameters the selected version of SNMP requires.
- Information about the switches to be discovered. This information includes the switch Telnet/FTP user name and password, Trap Station User Name, Shell Preference (Telnet or SSH), and the manner in which the switch's associated links should be discovered. In previous releases of OmniVista, this information had to be specified via a separate, additional "editing" operation after the discovery was complete.

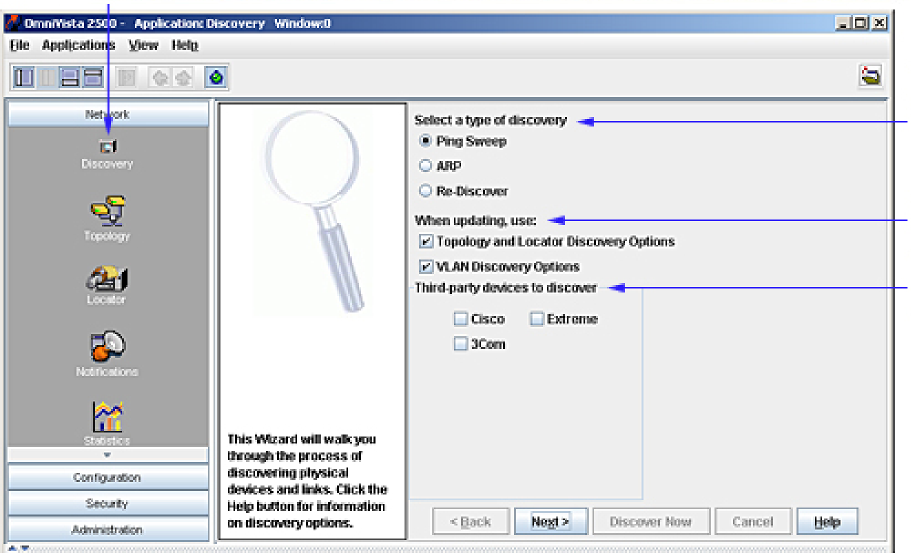
The second page of the Discovery Wizard, SNMP Setups, enables you to create SNMP Setups. The SNMP Setups you create will be available for your selection in subsequent pages of the Discovery Wizard. Click here for more information on SNMP Setups.

Discovery Options

The opening window of the Discovery Wizard enables you to specify the type of discovery you want to perform and optional information you want to discover, as explained below.

The Discovery Application

To open the application, click on Discovery or select Discovery from the Applications Menu.



This Wizard will walk you through the process of discovering physical devices and links. Click the Help button for information on discovery options.

Select a type of discovery

● Ping Sweep

○ ARP

○ Re-Discover

When updating, use:

☑ Topology and Locator Discovery Options

☑ VLAN Discovery Options

Third-party devices to discover

□ Cisco □ Extreme

□ 3Com

Specifies the type of discovery you want to perform.

Specifies optional info you want to discover.

Specifies third-party devices you want to discover.

Specifying the Type of Discovery

Enable one of the following buttons to select the type of discovery you want to perform:

Ping Sweep. A Ping Sweep discovery enables you to discover all switches with an IP address that falls within user-specified ranges of IP addresses.

ARP. An ARP (Address Resolution Protocol) discovery enables you to connect to one or more gateway devices, which then use ARP to return a list of subnets known to each gateway. Each subnet is then discovered.

Re-Discover. This button enables you to select one or more devices that you wish to rediscover. For example, you might wish to rediscover a device to learn VLAN information that was not gathered during the first discovery. You might also wish to rediscover a device if that device was reconfigured outside of OmniVista. If you enable this button, the Discovery Wizard will display a window that enables you to select the devices you wish to rediscover.

Specifying Discovery Options

Select the following checkboxes if you wish to learn additional information during the discovery:

Topology and Locator Discovery Options. Enable this checkbox if you wish to learn information about network links. Link information is maintained by adjacency protocols - such as PNNI for ATM, or AMAP and XMAP for Ethernet - which are active by default in devices that support such protocols. Information about network links is necessary to display the links between devices when the network and its regions are displayed. If you enable this checkbox, the Discovery Wizard will later display a window that allows you to specify the link information you want learned.

> **Note:** As stated, link information is discovered via adjacency protocols, which are supported by all AOS switches, XOS switches, and 61xx devices. However, OmniCore 5xxx devices, the OmniPCX, and most third-party devices do not support such adjacency protocols. You can specify that you want link information gathered for these devices using an alternative method - functionality from OmniVista's Locator application - by creating and using an SNMP Setup that has the **Discover Links** combo box set to **As OEM Device**. (Click here for more information on SNMP Setups.) You can also specify this after the devices themselves are discovered, by editing the devices to enable the **Handle as an OEM Device** checkbox on the Edit Discovery Manager Entry window. When this checkbox is enabled, link information will be gathered for the device during each subsequent polling cycle, using logic from the Locator application.

VLAN Discovery Options. Enable this checkbox if you wish to learn VLAN information required by the VLAN application. If you enable this checkbox, the Discovery Wizard will later display a window that allows you to specify the precise VLAN information you want learned.

Specifying Third-Party Devices for Discovery

By default, OmniVista provides support for third-party devices built by Cisco, 3Com, and Extreme. Support for additional third-party devices can be added via the Third Party Device Support Preferences window in the Preferences application. To discover third-party devices, ensure that the device's checkbox is enabled on the opening window of the Discovery Wizard, as shown above.

Click the **Next** button when you have made your selections.

Creating SNMP Setups

Creating SNMP Setups is **not** required unless you wish to change OmniVista's default behavior (which is described below). If you accept the default behavior, click the **Next** button to display the next page of the Discovery Wizard. If you do create SNMP Setups, they will display for your selection in subsequent windows of the Discovery Wizard.

Overview

By default, OmniVista uses SNMP Version 1 to discover switches. If OmniVista discovers an AOS device, it sets the default to SNMP Version 2 automatically (that is, any further communication between OmniVista and the AOS device will be performed using SNMP Version 2). The SNMP Setups window of the Discovery Wizard enables you to change this default operation and perform the discovery using SNMP Version 1, Version 2, or Version 3.

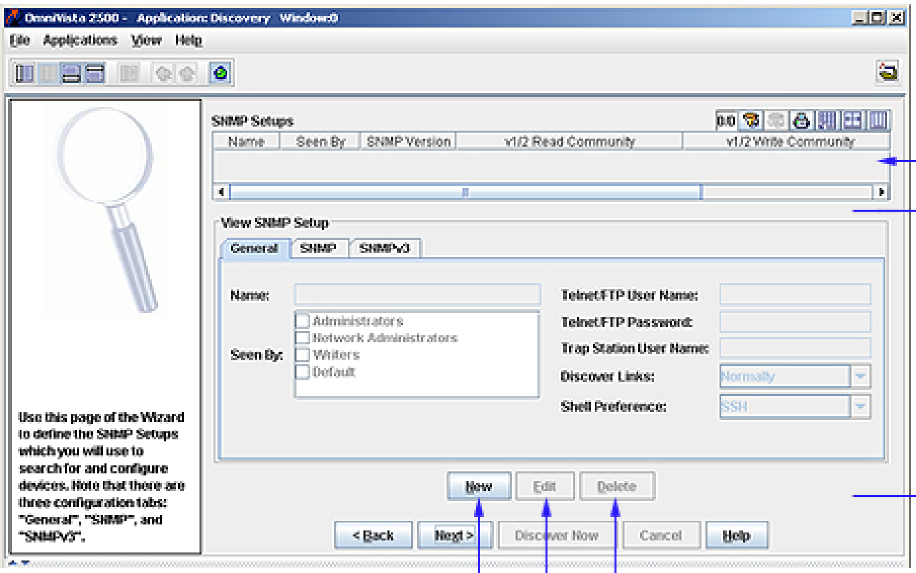
> **Note:** For AOS switches, you can only change the SNMP version after Discovery is complete.

The SNMP Setups window also enables you to inform OmniVista of certain information about the switches to be discovered BEFORE the discovery takes place. This information includes the switch Telnet/FTP user name and password, Trap Station user name, Shell Preference (Telnet or SSH), and the manner in which the switch's associated links should be discovered. In previous releases of OmniVista, this information had to be specified via a separate, additional "editing" operation after the discovery was complete. This additional editing operation will still be required if you do not use the SNMP Setups window to specify this information to OmniVista before the discovery.

The SNMP Setups window enables you to create SNMP "Setups" that specify the SNMP functionality and switch information described above. You can then associate selected SNMP Setups with an individual ping sweep range (if you are using Ping Sweep Discovery) or an individual gateway device (if you are using ARP Discovery). The SNMP Setups will apply to all switches discovered in the ping sweep range or all switches discovered via the gateway device.

> **Note for Previously Discovered Switches**. If a switch was discovered previously, and a new discovery is then performed using an SNMP Setup that specifies General parameters (such the Telnet/FTP user name and password, etc.), the General parameter values specified in the SNMP Setup will NOT overwrite the General parameter values already specified to OmniVista for that switch. The General parameter values specified in the SNMP Setup will apply to newly-discovered switches only.

The SNMP Setup Window



Name	Seen By	SNMP Version	v1/2 Read Community	v1/2 Write Community

Name:

Seen By: □ Administrators
□ Network Administrators
□ Writers
□ Default

Telnet/FTP User Name:

Telnet/FTP Password:

Trap Station User Name:

Discover Links: Normally

Shell Preference: SSH

Use this page of the Wizard to define the SNMP Setups which you will use to search for and configure devices. Note that there are three configuration tabs: "General", "SNMP", and "SNMPv3".

Existing SNMP setups are listed here.

Fields are used to create a new SNMP setup or edit an existing one.

Click **Delete** to delete a selected SNMP setup.

Click Edit to edit a selected SNMP setup.

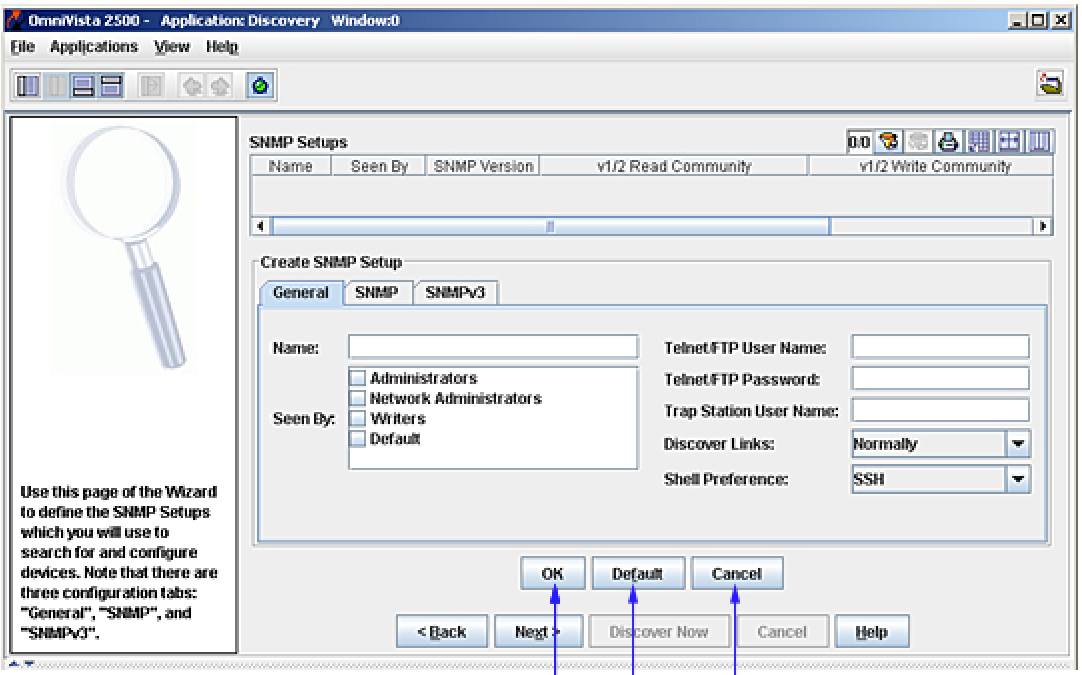
Click **New** to create a new SNMP setup.

Creating a New SNMP Setup - General Tab

Follow the steps below to create a new SNMP Setup.

1. Click the **New** button. The Create SNMP Setup panel activates, as shown below. If you select an existing SNMP Setup and then click **New**, the parameters of the selected Setup will display in the Create SNMP Setup panel for your convenience. You can then edit fields as desired.

Creating a New SNMP Setup



Use this page of the Wizard to define the SNMP Setups which you will use to search for and configure devices. Note that there are three configuration tabs: "General", "SNMP", and "SNMPv3".

Seen By: □ Administrators □ Network Administrators □ Writers □ Default

Discover Links: Normally

Shell Preference: SSH

Click Cancel to cancel the create operation.

Click Default to return the fields to the default settings.

Click OK to create the setup as entered.

2. If it is not already displayed, click the General tab. The General tab of the SNMP Setups window enables you to specify a name for the new SNMP Setup and to specify information about the devices to be discovered.

3. Enter a name for the new SNMP Setup in the **Name** field.

4. The **Seen By** field defines the security permissions that will be required for viewing the switches in the list of All Discovered devices AFTER they are discovered. OmniVista is shipped with four pre-defined user groups -- Administrators, Network Administrators, Writers, and Default -- that have different security permissions. (The Security application *Users and Groups* enables you to view and configure security permissions.) Click the checkboxes in the **Seen By** field to define who will be able to view the switches after they are discovered. Alternatively, if you do not click any checkbox, the switches will be viewable by everyone.

> **Administrators** checkbox. This group has all administrative access rights granted to the Network Administrators group AND full administrative rights to edit the groups and users defined in the Security application *Users and Groups*.

Network Administrators checkbox. This group has full administrative access rights to all switches on the network. Members of this group can run discovery and can manually add, delete, and modify entries in the list of All Discovered Devices. Members of this group also have full read and right access to entries in the *Audit* and *Control Panel* applications. Members of this group can do everything EXCEPT edit the groups and users defined in the Security application *Users and Groups*.

Writers checkbox. This group has both read and write access to switches in the list of All Discovered Devices that are configured to grant access to this group. However, members of this group cannot run discovery nor can they manually add, delete, or modify entries in the list of All Discovered Devices.

Default checkbox. This group has read-only access to switches in the list of All Discovered Devices that are configured to grant access to this group.

5. In the **Telnet/FTP User Name** and **Telnet/FTP Password** fields, enter the user name and password that OmniVista will use to establish FTP and Telnet sessions with the discovered devices. The user name and password specified will be used to auto-login to devices when Telnet sessions are established. They will also be used to perform FTP with the device when configuration files are saved and restored, as explained below.

Firmware configuration files for XOS and AOS devices can be saved to the OmniVista server and restored when desired. When files are saved, they are FTPed from the switch to the OmniVista server. When files are restored, they are FTPed from the server to the switch. New configuration files can also be installed via FTP. In order to FTP files, OmniVista must know the FTP login name and password that is defined on the switch. The **Telnet/FTP User Name** and **Password** fields enable you to specify this information to OmniVista.

Please Note:

- If you do not define the Telnet/FTP login name and password, and you attempt to save, restore, or upgrade configuration files for XOS or AOS devices, you will be individually queried for the FTP login name and password of each individual switch for which configuration files are being saved, restored, or upgraded.
- If you do not define the Telnet/FTP login name and password, OmniVista will be unable to auto-login to the device when establishing Telnet sessions.
- For OmniCore devices, the login name and password specified in these fields will be used to establish Telnet sessions and will be passed to the TrackView Element Manager automatically whenever TrackView is invoked.

6. (AOS Devices only) In the **Trap Station User Name** field, enter the switch user name that will be used when an AOS device is configured to send traps to OmniVista. AOS devices require that a valid switch user name be specified with the trap station configuration entry. If this field is left blank, the following switch user names will be used by default for trap station configuration entries:

- If OmniVista is configured to use SNMP version 3 with this device, the SNMP version 3 user name entered for the device will be used as the switch user name in the trap station configuration entry.
- If OmniVista is configured to use SNMP version 1 or SNMP version 2 with this device, the read community string for the device will be used as the switch user name in the trap station configuration entry.

When using SNMP version 1 or 2, switch user names are interchangeable with community strings AS LONG AS community string mapping is not in use on the switch. If community string mapping is not in use, and an AOS switch is discovered using SNMP version 1 or 2 with a default read community string of "public", or even with a non-default read community string such as "thomas", these community strings are valid switch user names for trap station configuration entries. In this case, no further configuration is required and this field can be left blank.

However, if community string mapping is enabled on the switch, the community string with which the switch is discovered is not guaranteed to be a valid switch user name, and thus is not guaranteed to be a valid switch user name for a trap station configuration entry. In this case, you should enter a valid switch user name in the **Trap Station User Name** field.

7. Set the **Discover Links** combo box to **Normally** or **As OEM Device** to specify how OmniVista should discover the physical links associated with the discovered devices. Links to other switches are displayed graphically on OmniVista's Topology maps. Set the **Discover Links** combo box to **Normally** for devices that support adjacency protocols, such as XOS devices, AOS devices, 61xx, and 6300-24 devices. Adjacency protocols (such as XMAP and AMAP) enable OmniVista to discover the physical links associated with specific devices. In previous releases of OmniVista, devices that did not support adjacency protocols -- such as the OmniPCX, OmniCore 5xxx switches, and third party devices -- were discovered and displayed on Topology maps, but links from these devices to other switches had to be added manually.

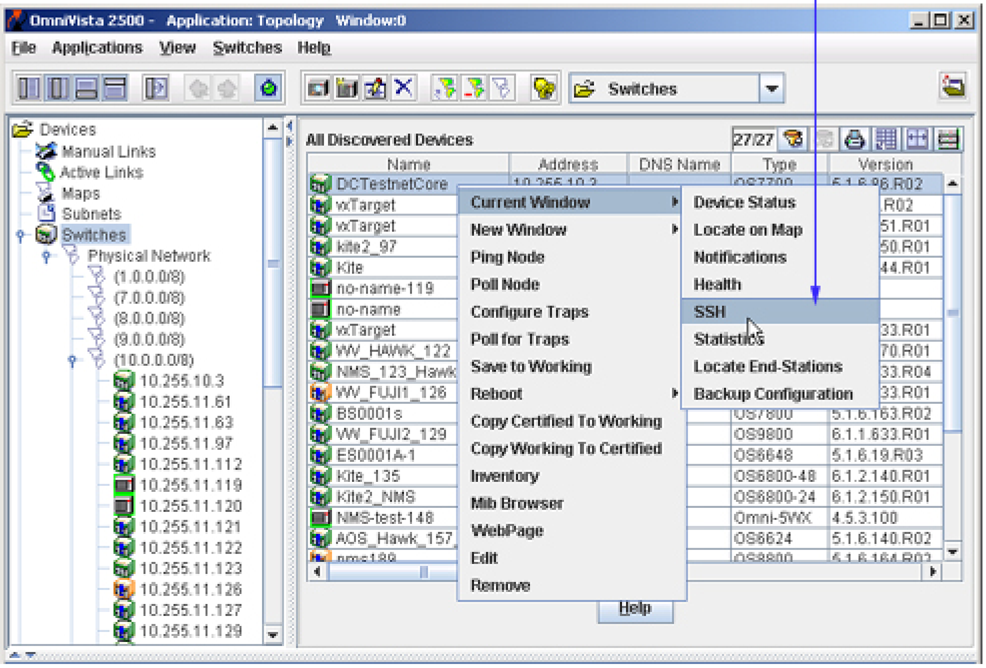
The **Discover Links** combo box's **As OEM Device** setting enables you to use the new "end station search" functionality from the Locator application to automatically discover links for devices that do not support adjacency protocols. When the **Discover Links** combo box is set to **As OEM Device**, and the device does not support an adjacency protocol that enables OmniVista to discover physical links, the end station search algorithms used by the Locator application are invoked at each polling cycle to discover the device's links. All links discovered are displayed on Topology maps automatically.

> **Note**. This approach works well for switches located at the edge of the network that do not support adjacency protocols. However, when a series of such switches are interconnected at the core of a network, this approach may "discover" more links than are meaningful. As an example, consider a series of such switches connected in a chain. Use of the Locator end station search algorithms, without benefit of any actual knowledge of how the switches are connected, will result in showing links between all the switches as a "cloud" instead of a chain. Such situations can be corrected by adding explicit manual links. For example, in the situation described, adding manual links for the actual connections will solve the problem by giving OmniVista the knowledge it needs to show the connections accurately.

8. Set the **Shell Preference** combo box to **Telnet** or **SSH** to specify the default command line interface to be used for the discovered devices. OmniVista's Telnet application supports both the Telnet and SSH command line interfaces. SSH (Secure Shell) is a Telnet-like utility that provides encryption and is far more secure than Telnet. When the **SSH** setting is used, SSH will be used as the default command line interface for the device. If the **Telnet** setting is used, Telnet will be used as the default command line interface for the device. OmniVista pop-up menus, such as the one shown below, will automatically display the default command line interface for the device: **Telnet** or **SSH**. When selected, the Telnet application will open and a connection of the configured type will be established automatically.

> **Note**. Ensure that devices are capable of SSH before you use the **SSH** setting. OmniVista does not verify devices' SSH capabilities. All AOS devices are SSH-capable. XOS devices, OmniCore devices, and OmniStack 6124/6148 devices are not SSH-capable.

When the SSH setting is used, OmniVista pop-up menus display an SSH option instead of the default Telnet option.

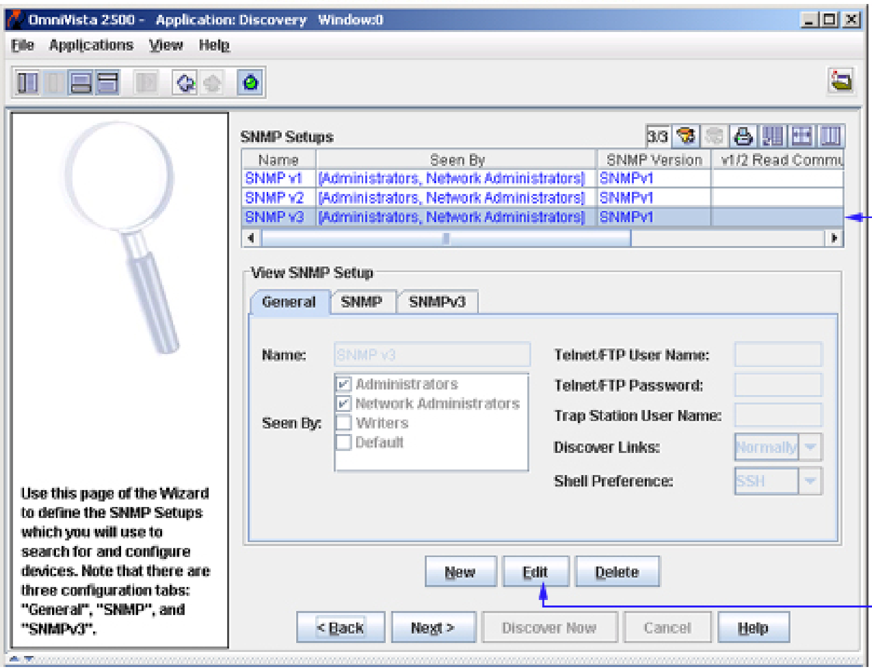


Name	Address	DNS Name	Type	Version
DCTestnetCore	10.255.10.3		OS7700	5.1.6.96.R02
vxTarget				R02
vxTarget				51.R01
kite2_97				50.R01
Kite				44.R01
no-name-119				
no-name				
vxTarget				33.R01
WV_HAWK_122				70.R01
NMS_123_Hawk				33.R04
WV_FUJI1_126				33.R01
BS0001s			OS7800	5.1.6.163.R02
WV_FUJI2_129			OS9800	6.1.1.633.R01
ES0001A-1			OS6648	5.1.6.19.R03
Kite_135			OS6800-48	6.1.2.140.R01
Kite2_NMS			OS6800-24	6.1.2.150.R01
NMS-test-148			Omni-5WX	4.5.3.100
AOS_Hawk_157			OS6624	5.1.6.140.R02
nms189			OS8800	5.1.6.164.R02

Editing a Single SNMP Setup Row

To edit an existing SNMP setup, select the desired setup and click the **Edit** button. You can edit any field. Click **OK** when your changes are complete.

Editing a Single SNMP Setup



Name	Seen By	SNMP Version	v1/2 Read Commu
SNMP v1	[Administrators, Network Administrators]	SNMPv1	
SNMP v2	[Administrators, Network Administrators]	SNMPv1	
SNMP v3	[Administrators, Network Administrators]	SNMPv1	

Name: SNMP v3

Seen By:
☑ Administrators
☑ Network Administrators
☐ Writers
☐ Default

Telnet/FTP User Name:

Telnet/FTP Password:

Trap Station User Name:

Discover Links: Normally

Shell Preference: SSH

Use this page of the Wizard to define the SNMP Setups which you will use to search for and configure devices. Note that there are three configuration tabs: "General", "SNMP", and "SNMPv3".

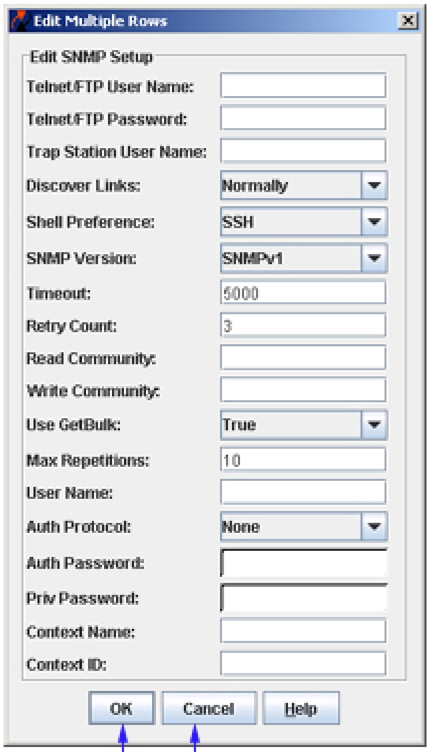
Select the SNMP setup you want to edit.

Click the Edit Button.

Editing Multiple SNMP Setup Rows

To edit multiple existing SNMP setups, select the desired setups and click the **Edit** button. The Edit Multiple Rows panel displays, as shown below. You can edit any field (where appropriate). Click here for more information on these fields. Click **OK** when your changes are complete.

The Edit Multiple SNMP Rows Window



Edit Multiple Rows

Edit SNMP Setup

Telnet/FTP User Name:	
Telnet/FTP Password:	
Trap Station User Name:	
Discover Links:	Normally
Shell Preference:	SSH
SNMP Version:	SNMPv1
Timeout:	5000
Retry Count:	3
Read Community:	
Write Community:	
Use GetBulk:	True
Max Repetitions:	10
User Name:	
Auth Protocol:	None
Auth Password:	
Priv Password:	
Context Name:	
Context ID:	

Click **Cancel** to cancel the edit operation.

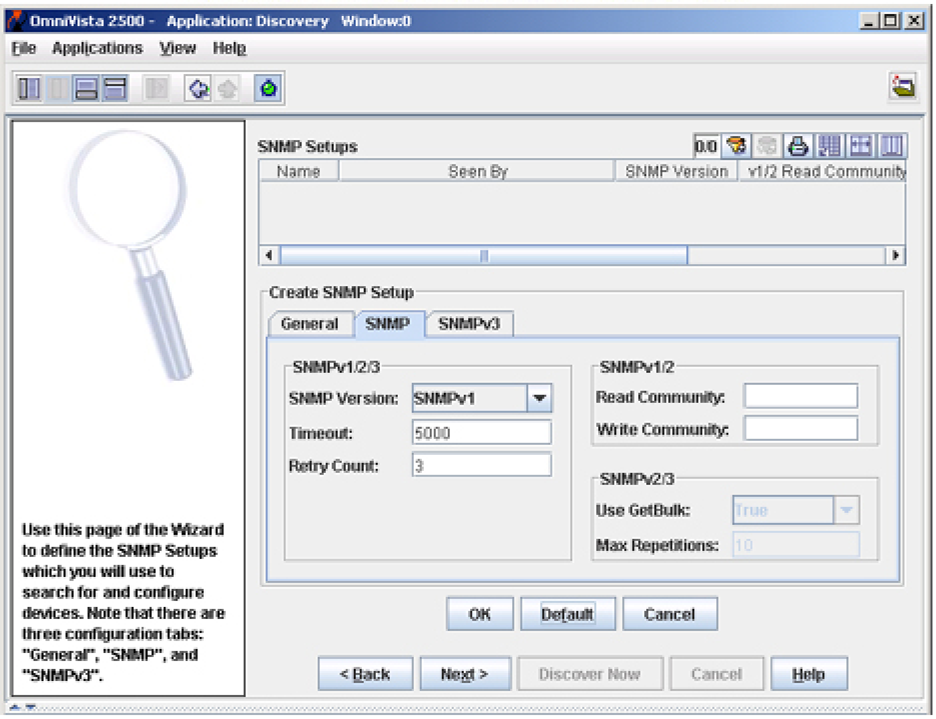
Click **OK** to accept all edits.

When all fields on the SNMP Setups window's General tab are complete, click the SNMP tab. The SNMP tab enables you to configure the SNMP version that will be used for the discovery. Click the **Help** button on the SNMP tab to continue.

Creating a New SNMP Setup - SNMP Tab

The SNMP Setup window's SNMP tab enables you to specify the version of SNMP you want used for this SNMP Setup. It also enables you to configure parameters for the specified version of SNMP. Click on the **SNMP** tab, click the **New** button, and follow the steps below to complete the fields in the SNMP tab.

Creating a New SNMP Setup - SNMP Tab



SNMP Version: SNMPv1

Timeout: 5000

Retry Count: 3

Read Community:

Write Community:

Use GetBulk: True

Max Repetitions: 10

Use this page of the Wizard to define the SNMP Setups which you will use to search for and configure devices. Note that there are three configuration tabs: "General", "SNMP", and "SNMPv3".

1. Set the **SNMP Version** combo box to **SNMPv1**, **SNMPv2**, or **SNMPv3** to specify the version of SNMP you want used for this SNMP Setup. Note that XOS devices support SNMP version 1 only. AOS devices support SNMP version 1, SNMP version 2, or SNMP version 3.

The SNMP version that you select determines the SNMP parameters that need to be configured. SNMP parameters are cumulative in that SNMP version 1 supports only version 1 parameters, SNMP version 2 supports version 1 and version 2 parameters, and SNMP version 3 supports version 1, version 2, and version 3 parameters. Only those parameters that are supported by the selected version of SNMP will activate in the SNMP tab.

2. (SNMPv1, SNMPv2, SNMPv3) In the **Timeout** field, enter the desired time period, in milliseconds, that OmniVista will wait for a switch to respond to a connection request before assuming that the request has timed-out.

3. (SNMPv1, SNMPv2, SNMPv3) In the **Retry Count** field, enter the number of times that you want OmniVista to attempt to connect to a switch.

4. (SNMPv1, SNMPv2) In the **Read Community** field, enter the switch's get community name. The get community name enables you to read information from the switch. In the **Write Community** field, enter the switch's set community name. The set community name enables you to write information to the switch. If the switch's get and set community names are **public**, the default, you can leave these fields blank (OmniVista uses the default name, **public,** when the field is blank.)

Please Note:

- Get and set community names are not configurable from OmniVista. Get and set community names can only be configured by logging onto the switch.
- When you use SNMP Version 3, get and set community names are ignored.

5. (SNMPv2, SNMPv3) Set the **Use GetBulk** combo box to **True** or **False**. When enabled, the Get Bulk operation is used for retrieving large amounts of data, particularly from large tables. The Get Bulk operation performs continuous Get Next operations, each time requesting the number of table rows specified by the value in the **Max Repetitions** field (described below). For example, if the value in the **Max Repetitions** field is ten, each Get Next operation will request 10 rows of table data. Note that the number of rows of data actually returned by the switch will be determined by the amount of memory the switch has available at that time.

6. (SNMPv2, SNMPv3) Enter the desired value in the **Max Repetitions** field. The value in the **Max Repetitions** field determines the number of rows of table data that the Get Bulk operation will request in each Get Next operation.

7. If you specified SNMPv1 or SNMPv2 for this SNMP Setup, the SNMP Setup is now complete. Click the **OK** button to create the SNMP Setup as specified. All SNMP Setups that you create will display for your selection in subsequent windows of the Discovery Wizard.

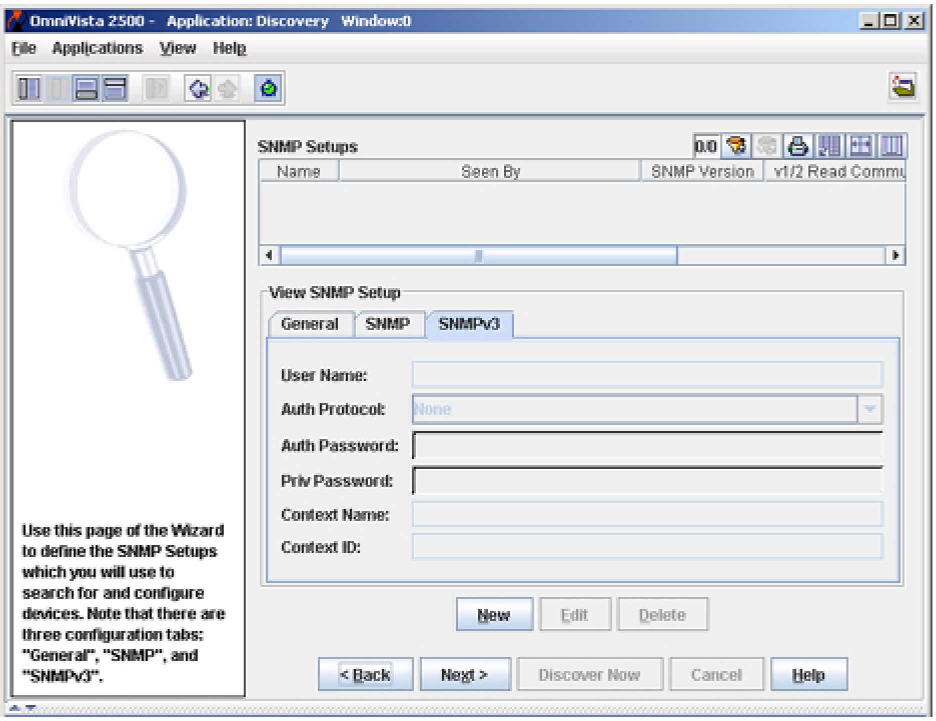
If you clicked **OK** to create an SNMP Setup that specifies SNMPv1 or SNMPv2, click the **Next** button to display the next page of the Discovery Wizard.

If you specified SNMPv3 for this SNMP Setup, click the SNMPv3 tab to specify parameters used for SNMPv3 only. Click the **Help** button on the SNMPv3 tab to continue.

Creating a New SNMP Setup - SNMPv3 Tab

The SNMP Setup window's SNMPv3 tab enables you to configure parameters specific to SNMP Version 3. After completing the SNMP tab for SNMPv3, click on the **SNMPv3 tab**, click on the **New** button, and follow the steps below to complete the fields in the SNMPv3 tab.

Creating a New SNMP Setup - SNMPv3 Tab



Use this page of the Wizard to define the SNMP Setups which you will use to search for and configure devices. Note that there are three configuration tabs: "General", "SNMP", and "SNMPv3".

1. Enter the SNMP version 3 user name in the **User Name** field.

2. Set the **Auth Protocol** combo box to **None**, **MD5**, or **SHA** to specify the authentication protocol OmniVista will use for SNMP communications with the discovered switches. **MD5** (or HMAC-MD5-96) and **SHA** (or HMAC-SHA-96) are the two authentication protocols that have been defined for SNMP version 3.

Authentication uses a secret key to produce a "fingerprint" of the message. The fingerprint is included within the message. The device that receives the message uses the same secret key to validate that the fingerprint is correct. If it is, and if the message was received in a timely manner, then the message is considered authenticated. Otherwise, the message is discarded. The fingerprint is called a Message Authentication Code, or MAC. The MD5 and SHA authentication protocols produce the MAC in a similar, but not an identical, manner.

Note that the **Auth Password** and **Priv Password** fields activate when the authentication protocol is set to something other than **None**. The **Auth Password** field activates because the authentication password is used as the "secret key" mentioned above. For MD5 the secret key should be 16 octets; for SHA the secret key should be 20 octets. Note that this implies that stronger authentication is provided by the SHA protocol, and SHA should be used instead of MD5 when possible. The **Priv Password** field activates because privacy encryption can only be used when authentication is also used. SNMP version 3 uses the CBC-DES Symmetric Encryption Protocol for privacy.

3. In the **Auth Password** field, enter the password (in hex) that OmniVista will use for the MD5 or SHA authentication protocol. This must be the same password that is defined on the switch for MD5 or SHA. If no authentication password is entered, neither authentication nor privacy encryption will be used.

4. In the **Priv Password** field, enter the password (in hex) that will be used as the secret key. This must be the same password that is defined on the switch for the CBC-DES Symmetric Encryption Protocol. If an authentication password is entered, but no privacy password is entered, authentication will be used without privacy encryption.

> **Important Note**. The switch uses a single password as both the **Auth Password** and the **Priv Password**. This means that the same password should be entered in these two fields. You can identify the password to enter by using the switch CLI command **configuration snapshot aaa**. This command will show the "authkey" for each switch user. The authkey is a hex value computed from the user's password. (The user's password is established with the CLI command **user**.) If you want both authentication and privacy encryption, enter the authkey in both the **Auth Password** and the **Priv Password** fields.

5. In the **Context Name** field, enter a unique context name for this context. An SNMP context is a collection of management information accessible by an SNMP entity, in this case OmniVista. A context identifies a subset of management information, in this case the management information OmniVista has about the individual device. OmniVista, as an SNMP entity, has access to many SNMP contexts: one for each device it manages. Each context must be identified by a unique context name and a unique context ID. Note that an item of management information may exist in more than one context.

Technically, the context name and context ID provide a means of distinguishing specific instances of information in the MIB modules from the set of all instances of that information within the management domain.

6. In the **Context ID** field, enter a unique context ID for this context. As explained above, each context must be identified by a unique context name and a unique context ID.

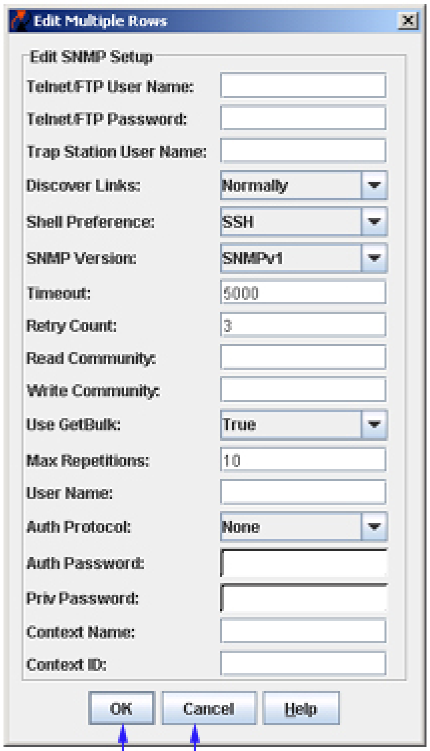
> **Important Note**. Neither the **Context Name** nor the **Context ID** are required for AOS, XOS, or default third-party devices supported by OmniVista. Leave these fields blank unless you are using a non-default third-party device that requires definition of a Context Name and Context ID.

7. The SNMP Setup is now complete. Click the **OK** button to create the SNMP Setup as specified.

> Click the **Next** button to display the next page of the Discovery Wizard.

Editing Multiple SNMP Setups

The Edit Multiple SNMP Rows Window



Edit SNMP Setup

Telnet/FTP User Name:

Telnet/FTP Password:

Trap Station User Name:

Discover Links: Normally

Shell Preference: SSH

SNMP Version: SNMPv1

Timeout: 5000

Retry Count: 3

Read Community:

Write Community:

Use GetBulk: True

Max Repetitions: 10

User Name:

Auth Protocol: None

Auth Password:

Priv Password:

Context Name:

Context ID:

Click **Cancel** to cancel the edit operation.

Click **OK** to accept all edits.

The fields you can modify in the Edit Multiple Rows window for SNMP setups are describe below. After you have made of all your changes click **OK** to enter all of your changes or **Cancel** to discard your changes and exit this edit operation.

Seen By
The security permissions that will be required for viewing the switches in the list of All Discovered devices AFTER they are discovered. OmniVista is shipped with four pre-defined user groups -- Administrators, Network Administrators, Writers, and Default -- that have different security permissions. Click the checkboxes in the **Seen By** field to define who will be able to view the switches after they are discovered. Click here for more information on these user groups.

Telnet FTP/User Name
The user name that OmniVista will use to establish FTP and Telnet sessions with the discovered devices. The user name specified will be used to auto-login to devices when Telnet sessions are established. It will also be used to perform FTP with the device when configuration files are saved and restored.

Telnet/FTP Password
The password that OmniVista will use to establish FTP and Telnet sessions with the discovered devices. The password specified will be used to auto-login to devices when Telnet sessions are established. It will also be used to perform FTP with the device when configuration files are saved and restored.

Trap Station User Name (AOS Devices Only)
The switch user name that will be used when an AOS device is configured to send traps to OmniVista. AOS devices require that a valid switch user name be specified with the trap station configuration entry. Click here for more information on these user names.

Discover Links
How OmniVista should discover the physical links associated with the discovered devices. Click here for more information.

Shell Preference
The default command line interface (Telnet or SSH) to be used for the discovered devices. Click here for more information.

> **Note**. Ensure that devices are capable of SSH before you use the **SSH** setting. OmniVista does not verify devices' SSH capabilities.

SNMP Version
The version of SNMP you want used for all the SNMP Setups you have selected. Click here for more information on SNMP versions.

Timeout (SNMPv1, SNMPv2, SNMPv3)
The desired time period, in milliseconds, that OmniVista will wait for a switch to respond to a connection request before assuming that the request has timed-out. Click here for more information.

Retry Count (SNMPv1, SNMPv2, SNMPv3)
The number of times that you want OmniVista to attempt to connect to a switch. Click here for more information.

Read Community (SNMPv1, SNMPv2)
The switch's get community name, which enables you to read information from the switch. Click here for more information.

Write Community (SNMPv1, SNMPv2)
The switch's set community name, which enables you to write information to the switch. Click here for more information.

Use GetBulk (SNMPv2, SNMPv3)
The Get Bulk operation is used for retrieving large amounts of data, particularly from large tables. The Get Bulk operation performs continuous Get Next operations, each time requesting the number of table rows specified by the value in the **Max Repetitions** field (described below). Click here for more information.

Max Repetitions (SNMPv2, SNMPv3)
The value in the **Max Repetitions** field determines the number of rows of table data that the Get Bulk operation (described above) will request in each Get Next operation. Click here for more information.

User Name (SNMPv3)
The SNMP version 3 user name.

Auth Protocol (SNMPv3)
The authentication protocol OmniVista will use for SNMP communications with the discovered switches, which can be **None**, **MD5**, or **SHA**. Click here for more information.

Auth Password (SNMPv3)
The password (in hex) that OmniVista will use for the MD5 or SHA authentication protocol. Click here for more information.

Priv Password (SNMPv3)
The password (in hex) that will be used as the secret key. Click here for more information.

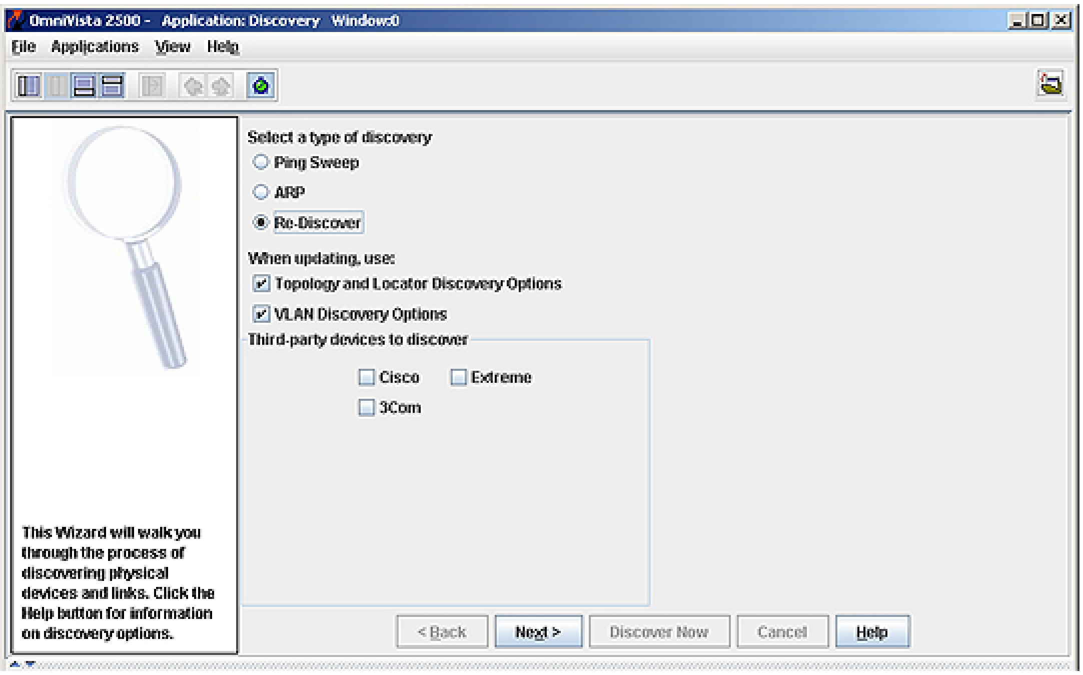
Context Name (SNMPv3)
The unique context name for this context. (An SNMP context is a collection of management information accessible by an SNMP entity, in this case OmniVista.) Click here for more information.

Context ID (SNMPv3)
The unique context ID for this context. Each context must be identified by a unique context name and a unique context ID. Click here for more information.

Selecting Devices for Rediscovery

To rediscover switches, select **Re-Discover** as the Type of Discovery on the first page of the Discovery Wizard and click the **Next** button.

Rediscovering Switches



Select a type of discovery

○ Ping Sweep

○ ARP

● Re-Discover

When updating, use:

☑ Topology and Locator Discovery Options

☑ VLAN Discovery Options

Third-party devices to discover

□ Cisco □ Extreme

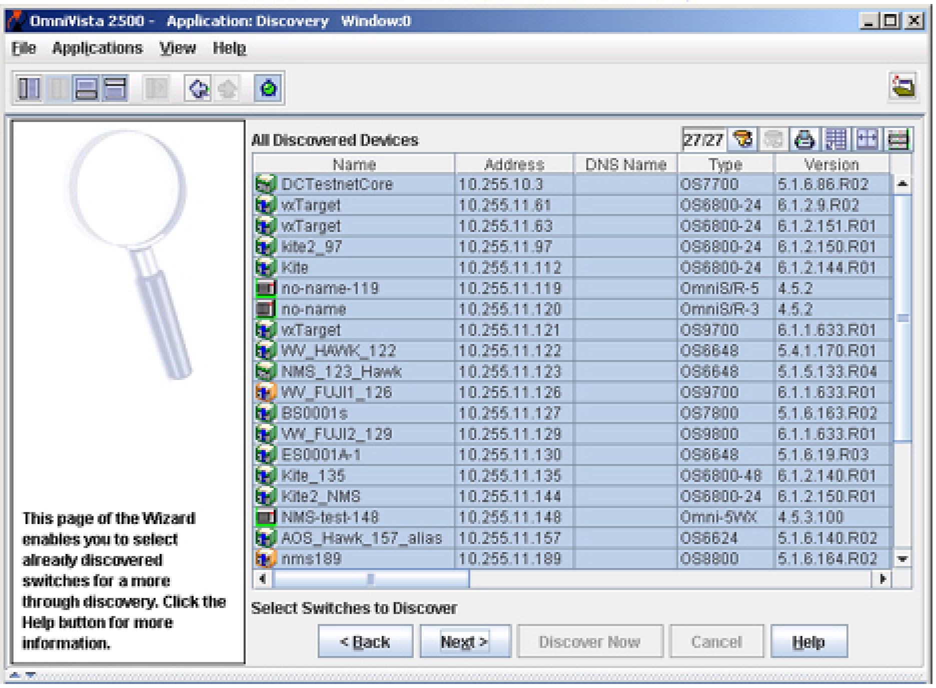
□ 3Com

This Wizard will walk you through the process of discovering physical devices and links. Click the Help button for information on discovery options.

The All Discovered Devices window of the Discovery Wizard appears. This window enables you to select devices that you wish to rediscover. The entire list of All Discovered Devices is displayed for your selection. As shown below, initially all devices are selected. To select an individual device in the list, click on it. You can select multiple contiguous devices by **Shift**-clicking, and multiple non-contiguous devices by **Ctrl**-clicking.

> **Note:** If the VLAN application has prompted you to discover VLAN information for specific devices, those devices will be automatically pre-selected.

Selecting Devices for Rediscovery


OmniVista 2500 - Application: Discovery Window:0
File Applications View Help
27/27
< Back
Next >
Discover Now
Cancel
Help

All Discovered Devices

Name	Address	DNS Name	Type	Version
DCTestnetCore	10.255.10.3		OS7700	5.1.6.86.R02
vxTarget	10.255.11.61		OS6800-24	6.1.2.9.R02
vxTarget	10.255.11.63		OS6800-24	6.1.2.151.R01
kite2_97	10.255.11.97		OS6800-24	6.1.2.150.R01
Kite	10.255.11.112		OS6800-24	6.1.2.144.R01
no-name-119	10.255.11.119		OmniS/R-5	4.5.2
no-name	10.255.11.120		OmniS/R-3	4.5.2
vxTarget	10.255.11.121		OS9700	6.1.1.633.R01
WV_HAWK_122	10.255.11.122		OS6648	5.4.1.170.R01
NMS_123_Hawk	10.255.11.123		OS6648	5.1.5.133.R04
WV_FUJI1_126	10.255.11.126		OS9700	6.1.1.633.R01
BS0001s	10.255.11.127		OS7800	5.1.6.163.R02
WV_FUJI2_129	10.255.11.129		OS9800	6.1.1.633.R01
ES0001A-1	10.255.11.130		OS6648	5.1.6.19.R03
Kite_135	10.255.11.135		OS6800-48	6.1.2.140.R01
Kite2_NMS	10.255.11.144		OS6800-24	6.1.2.150.R01
NMS-test-148	10.255.11.148		Omni-5WX	4.5.3.100
AOS_Hawk_157_alias	10.255.11.157		OS6624	5.1.6.140.R02
nms189	10.255.11.189		OS8800	5.1.6.164.R02

Select Switches to Discover

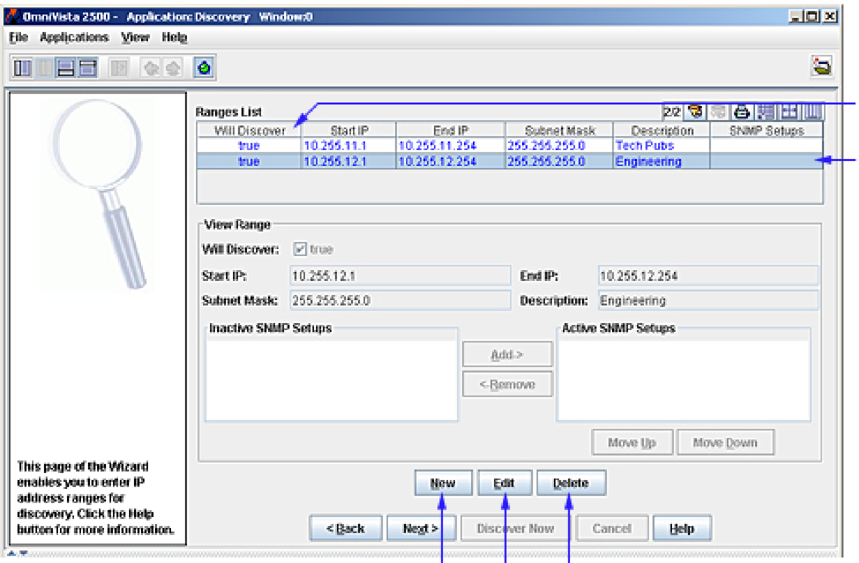
This page of the Wizard enables you to select already discovered switches for a more through discovery. Click the Help button for more information.

Click the **Next** button when you have made your selections.

Discovery by Ping Sweep

A ping sweep discovery enables you to discover all switches within a specified range of IP addresses. Each IP address within the specified range is pinged to discover if a device exists at that address. The Ping Sweep window of the Discovery Wizard, shown below, enables you to enter the ranges of IP addresses that you want discovered, edit ranges that were previously entered, and delete ranges. You can specify the SNMP Setups you want used to discovery each individual range, and you can specify which ranges you want discovered when the next discovery is performed.

The Ping Sweep Window



Ranges List 2/2

Will Discover	Start IP	End IP	Subnet Mask	Description	SNMP Setups
true	10.255.11.1	10.255.11.254	255.255.255.0	Tech Pubs	
true	10.255.12.1	10.255.12.254	255.255.255.0	Engineering	

View Range

Will Discover: ☑ true

Start IP: 10.255.12.1 End IP: 10.255.12.254

Subnet Mask: 255.255.255.0 Description: Engineering

Inactive SNMP Setups

Active SNMP Setups

This page of the Wizard enables you to enter IP address ranges for discovery. Click the Help button for more information.

When Will Discover is true, the range will be discovered when the next discovery is performed.

Ranges are listed here after entry.

Fields are used to enter a new range or edit and existing range.

Click Delete to delete a selected range.

Click Edit to edit a selected range.

Click New to enter a new range.

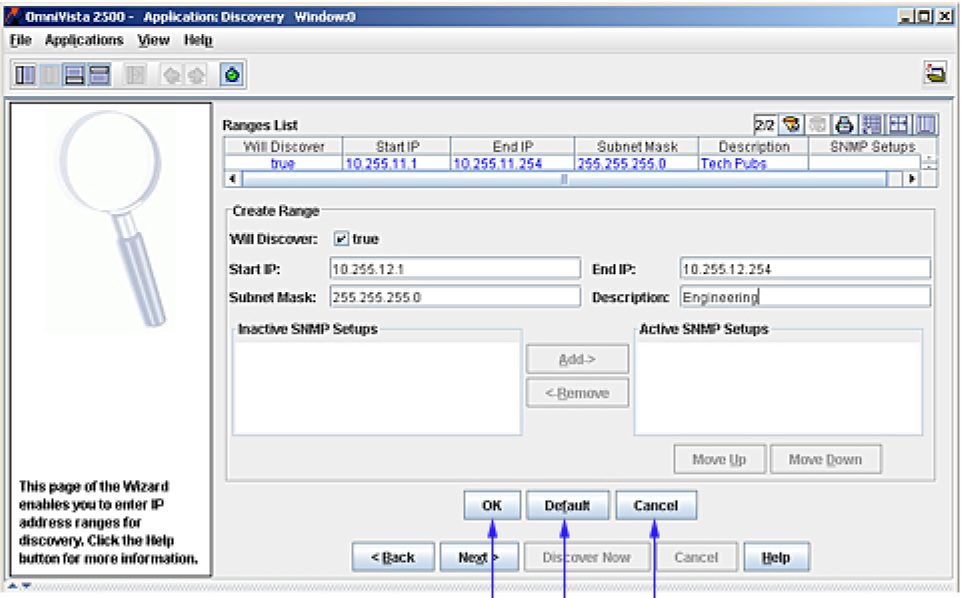
Entering a New Range of IP Addresses

Follow the steps below to enter a new range of IP addresses for discovery. Please note the following:

- You can enter overlapping subnet ranges for discovery, as long as the overlapping ranges are not enabled for discovery at the same time (that is, only one of the overlapping ranges should have its **Will Discover** checkbox set to **true** during any one discovery process).
- You can enter a single IP address to discover a single switch if desired.

1. Click the **New** button. The Create Range panel activates, as shown below. If you select an existing range and then click **New**, the parameters of the selected range will display in the Create Range panel for your convenience. You can then edit fields as desired.

Creating a New Range for Discovery



Ranges List

Will Discover	Start IP	End IP	Subnet Mask	Description	SNMP Setups
true	10.255.11.1	10.255.11.254	255.255.255.0	Tech Pubs	

Create Range

Will Discover: ☑ true

Start IP: 10.255.12.1

End IP: 10.255.12.254

Subnet Mask: 255.255.255.0

Description: Engineering

This page of the Wizard enables you to enter IP address ranges for discovery. Click the Help button for more information.

Click Cancel to cancel the create operation.

Click Default to return the fields to the default settings.

Click OK to create the range as entered.

2. When you enter a new range for discovery, the **Will Discover** checkbox is set to **true** by default. This means that the range will be discovered when the next discovery is performed. If you do not want the new range discovered when the next discovery is performed, uncheck the **Will Discover** checkbox.

3. Enter the starting IP address of the range in the **Start IP** field and enter the ending IP address of the range in the **End IP** field. Note that wildcard characters are not allowed in these IP addresses.

4. Enter the desired subnet mask in the **Subnet Mask** field or accept the default subnet mask of 255.255.255.0.

5. Enter a description of the range in the **Description** field.

6. If you want to apply one or more SNMP Setups to the discovery of the new range, move the desired SNMP Setups from the "Inactive SNMP Setups" window to the "Active SNMP Setups" window. To move an SNMP Setup from one window to the other, merely select it and click the **Add->** or **<-Remove** button.

7. Use the **Move Up** and **Move Down** buttons to arrange the SNMP Setups in the desired priority order. OmniVista will first attempt to discover each switch using the first (highest) SNMP Setup listed in the "Active SNMP Setups" window. If OmniVista cannot communicate with a switch using the first SNMP Setup listed, it will try the next SNMP Setup listed in the "Active SNMP Setups" window, and so on. If OmniVista cannot communicate with a switch using any of the SNMP Setups listed in the "Active SNMP Setups" window, it will attempt to communicate with the switch using default behavior.

If OmniVista finds that it can successfully use an SNMP Setup to communicate with and discover a switch, it will use that SNMP Setup for all future communications with that switch (unless you edit the switch to change the SNMP definition). In addition, if OmniVista can successfully use an SNMP Setup to communicate with a switch, it will apply the General parameters specified in that SNMP Setup to its definition of that switch. For example, if OmniVista can communicate with a switch using an SNMP Setup that specifies a Telnet/FTP User Name of Joe, OmniVista will update its definition of that switch to specify that its Telnet/FTP User Name is Joe.

> **Note:** OmniVista will NOT apply the General parameters specified in an SNMP Setup -- the **Telnet/FTP User Name** and **Password**, the **Trap Station User Name**, the **Discover Links** setting, and the **Shell Preference** setting -- unless it can successfully communicate with the switch using that SNMP Setup. OmniVista will apply the General parameters specified in the first SNMP Setup that results in successful communications.

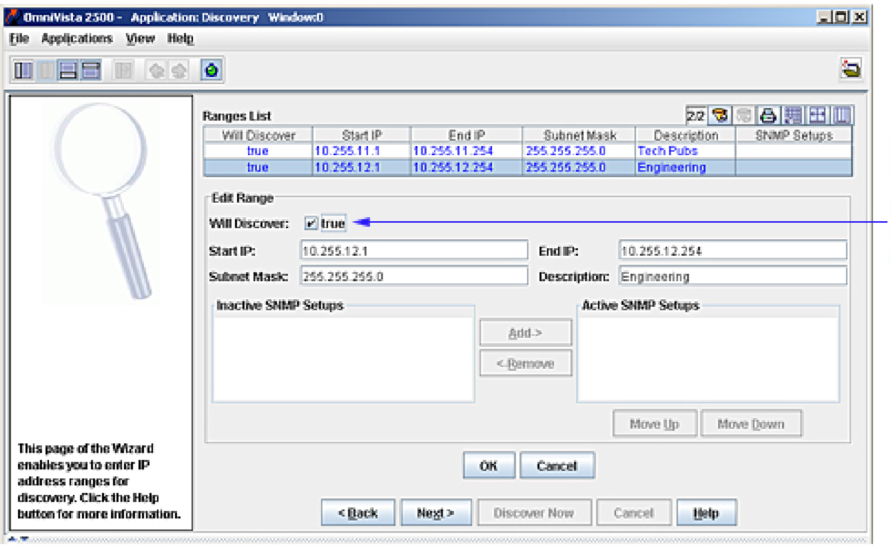
8. Click the **OK** button to create the range. The new range displays in the Ranges List. The new range displays in blue until the discovery is performed.

> **Note:** If a switch has a large number of MAC entries (more than 10K), it can take up to 3 minutes to discover the switch.

Editing a Single Range of IP Addresses

To edit an existing range of IP addresses, merely select the desired range and click the **Edit** button. The selected range displays in the Edit Range panel, as shown below. You can edit any field. Click **OK** when your changes are complete. Note that you can edit a range to change its **Will Discover** checkbox to **true** or **false**, which means that the range will, or will not be, discovered when the next discovery is performed.

Editing a Single Range



Ranges List

Will Discover	Start IP	End IP	Subnet Mask	Description	SNMP Setups
true	10.255.11.1	10.255.11.254	255.255.255.0	Tech Pubs	
true	10.255.12.1	10.255.12.254	255.255.255.0	Engineering	

Edit Range

Will Discover: ☑ true

Start IP: 10.255.12.1

End IP: 10.255.12.254

Subnet Mask: 255.255.255.0

Description: Engineering

Inactive SNMP Setups

Active SNMP Setups

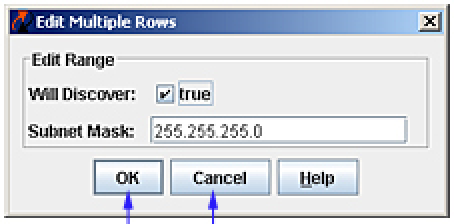
This page of the Wizard enables you to enter IP address ranges for discovery. Click the Help button for more information.

If you want a range discovered during the next discovery, edit it and set its Will Discover checkbox to true.

Editing Multiple Ranges of IP Addresses

To edit multiple existing ranges of IP addresses, select the desired ranges and click the **Edit** button. The Edit Multiple Rows panel displays, as shown below. You can edit the **Will Discover** and/or **Subnet Mask** for all ranges. Click **OK** when your changes are complete. Note that you can edit ranges to change their **Will Discover** checkboxes to **true** or **false**, which means that the ranges will, or will not be, discovered when the next discovery is performed.

Editing Multiple IP Adress Ranges



Will Discover: ☑ true

Subnet Mask: 255.255.255.0

Click Cancel to cancel the edit operation.

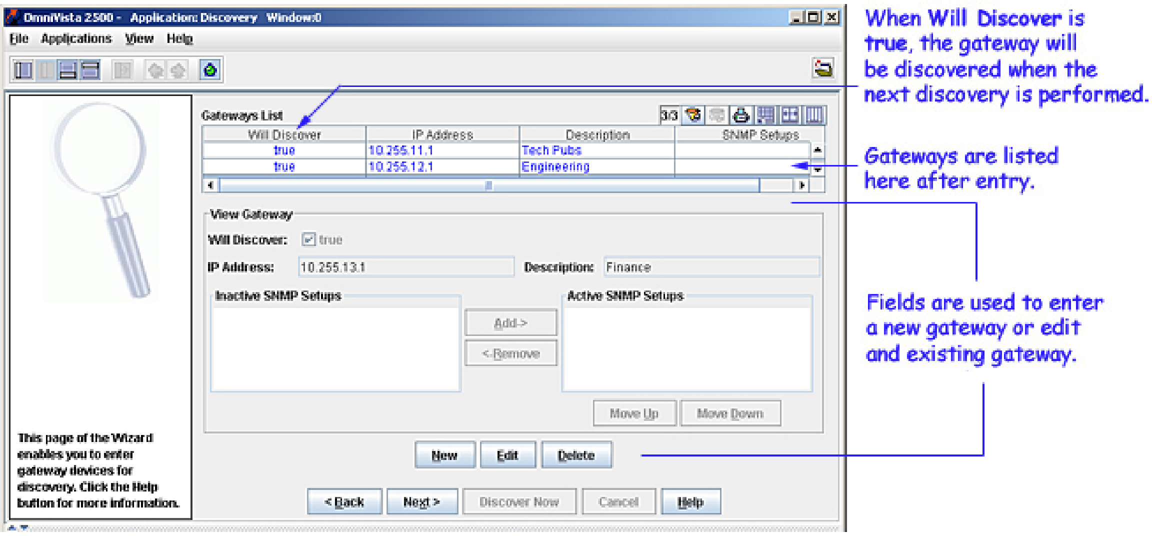
Click OK to accept all edits.

Click the **Next** button when the Ping Sweep window displays the desired ranges.

Discovery by ARP

An ARP (Address Resolution Protocol) discovery requires you to specify one or more gateway devices. When the discovery is performed, ARP is used to retrieve a list of the subnets known to each gateway. Each subnet is then discovered. (For best results it is recommended that you specify gateway devices that have extensive knowledge of the network.) The ARP window of the Discovery Wizard, shown below, enables you to specify gateway devices for discovery, to edit existing gateways, and to delete gateways. You can specify the SNMP Setups you want used to discovery each individual gateway, and you can specify which gateways you want discovered when the next discovery is performed.

The ARP Window



Gateways List

Will Discover	IP Address	Description	SNMP Setups
true	10.255.11.1	Tech Pubs	
true	10.255.12.1	Engineering	

View Gateway

Will Discover: ☑ true

IP Address: 10.255.13.1

Description: Finance

Inactive SNMP Setups

Active SNMP Setups

This page of the Wizard enables you to enter gateway devices for discovery. Click the Help button for more information.

When Will Discover is true, the gateway will be discovered when the next discovery is performed.

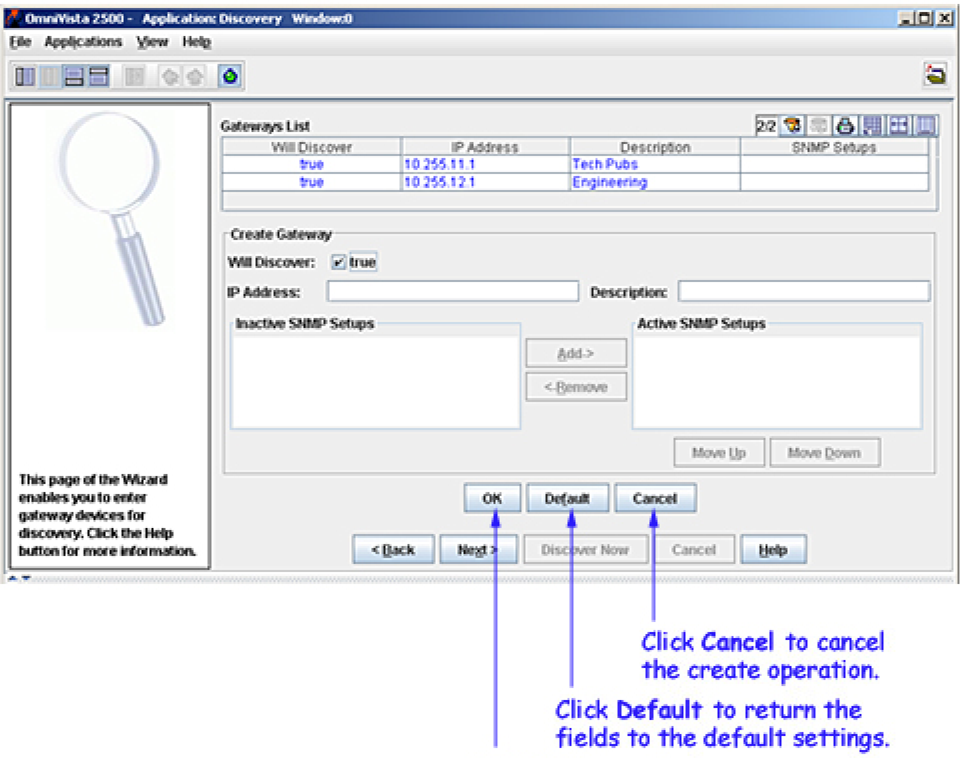
Gateways are listed here after entry.

Fields are used to enter a new gateway or edit and existing gateway.

Adding a New Gateway

1. Click the **New** button. The Create Gateway panel activates, as shown below. If you select an existing gateway and then click **New**, the parameters of the selected gateway will display in the Create Gateway panel for your convenience. You can then edit fields as desired.

Creating a New Gateway for Discovery



Gateways List

Will Discover	IP Address	Description	SNMP Setups
true	10.255.11.1	Tech Pubs	
true	10.255.12.1	Engineering	

Create Gateway

Will Discover: ☑ true

IP Address:

Description:

Inactive SNMP Setups

Active SNMP Setups

This page of the Wizard enables you to enter gateway devices for discovery. Click the Help button for more information.

Click Cancel to cancel the create operation.

Click Default to return the fields to the default settings.

Click OK to create the gateway as entered.

2. When you enter a new gateway for discovery, the **Will Discover** checkbox is set to **true** by default. This means that the gateway will be discovered when the next discovery is performed. If you do not want the new gateway discovered when the next discovery is performed, uncheck the **Will Discover** checkbox.

3. Enter the IP address of the gateway in the **IP Address** field.

4. Enter a description of the gateway in the **Description** field.

5. If you want to apply one or more SNMP Setups to the discovery of the new gateway, move the desired SNMP Setups from the "Inactive SNMP Setups" window to the "Active SNMP Setups" window. To move an SNMP Setup from one window to the other, select it and click the **Add->** or **<-Remove** button.

6. Use the **Move Up** and **Move Down** buttons to arrange the SNMP Setups in the desired priority order. OmniVista will first attempt to discover each switch using the first (highest) SNMP Setup listed in the "Active SNMP Setups" window. If OmniVista cannot communicate with a switch using the first SNMP Setup listed, it will try the next SNMP Setup listed in the "Active SNMP Setups" window, and so on. If OmniVista cannot communicate with a switch using any of the SNMP Setups listed in the "Active SNMP Setups" window, it will attempt to communicate with the switch using default behavior.

If OmniVista finds that it can successfully use an SNMP Setup to communicate with and discover a switch, it will use that SNMP Setup for all future communications with that switch (unless you edit the switch to change the SNMP definition). In addition, if OmniVista can successfully use an SNMP Setup to communicate with a switch, it will apply the General parameters specified in that SNMP Setup to its definition of that switch. For example, if OmniVista can communicate with a switch using an SNMP Setup that specifies a Telnet/FTP User Name of Joe, OmniVista will update its definition of that switch to specify that its Telnet/FTP User Name is Joe.

> **Note**. OmniVista will NOT apply the General parameters specified in an SNMP Setup -- the **Telnet/FTP User Name** and **Password**, the **Trap Station User Name**, the **Discover Links** setting, and the **Shell Preference** setting -- unless it can successfully communicate with the switch using that SNMP Setup. OmniVista will apply the General parameters specified in the first SNMP Setup that results in successful communications.

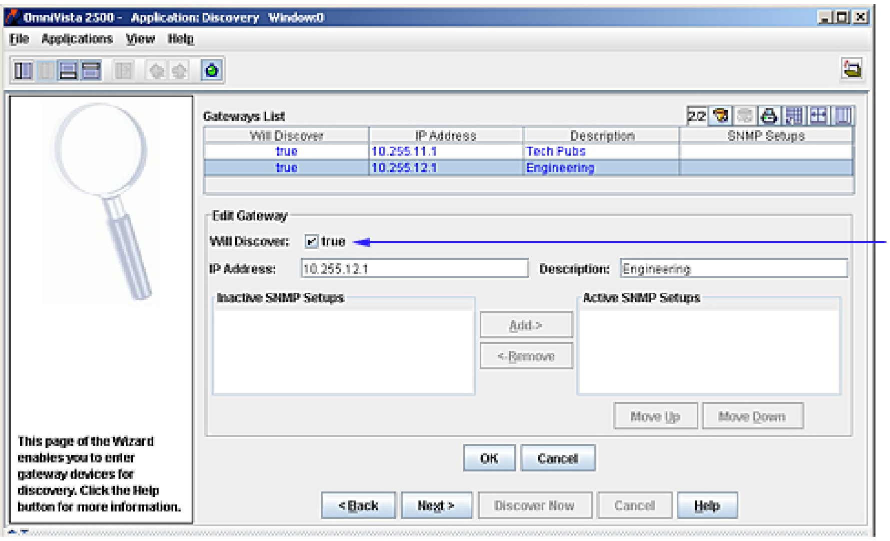
7. Click the **OK** button to create the new gateway. It then displays in the Gateways List. The new gateway displays in blue until the discovery is performed.

> **Note:** If a switch has a large number of MAC entries (more than 10K), it can take up to 3 minutes to discover the switch.

Editing a Single Existing Gateway

To edit a single existing gateway, select the desired gateway and click the **Edit** button. The selected gateway displays in the Edit Gateway panel, as shown below. You can edit any field. Click **OK** when your changes are complete. Note that you can edit a gateway to change its **Will Discover** checkbox to **true** or **false**, which means that the gateway will, or will not be, discovered when the next discovery is performed.

Editing a Gateway


OmniVista 2500 - Application: Discovery Window0
File Applications View Help
2/2
Add->
<-Remove
Move Up
Move Down
OK
Cancel
< Back
Next >
Discover Now
Cancel
Help

Gateways List

Will Discover	IP Address	Description	SNMP Setups
true	10.255.11.1	Tech Pubs	
true	10.255.12.1	Engineering	

Edit Gateway

Will Discover: ☑ true

IP Address: 10.255.12.1

Description: Engineering

Inactive SNMP Setups

Active SNMP Setups

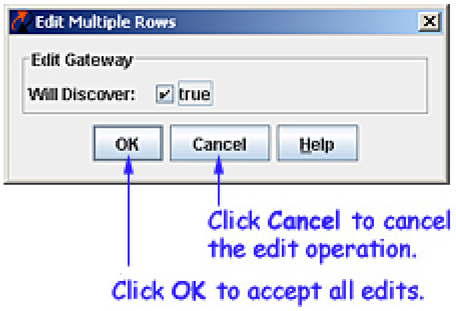
This page of the Wizard enables you to enter gateway devices for discovery. Click the Help button for more information.

If you want a range discovered during the next discovery, edit it and set its Will Discover checkbox to true.

Editing Multiple Existing Gateways

To edit multiple existing gateways, select the desired gateways and click the **Edit** button. The Edit Multiple Rows panel displays, as shown below. You can edit the **Will Discover** to **true** or **false** for all gateways, which means that the gateways will, or will not be, discovered when the next discovery is performed.

The Edit Multiple Gateway Rows Window



Edit Multiple Rows

Edit Gateway

Will Discover: ☑ true

Click Cancel to cancel the edit operation.

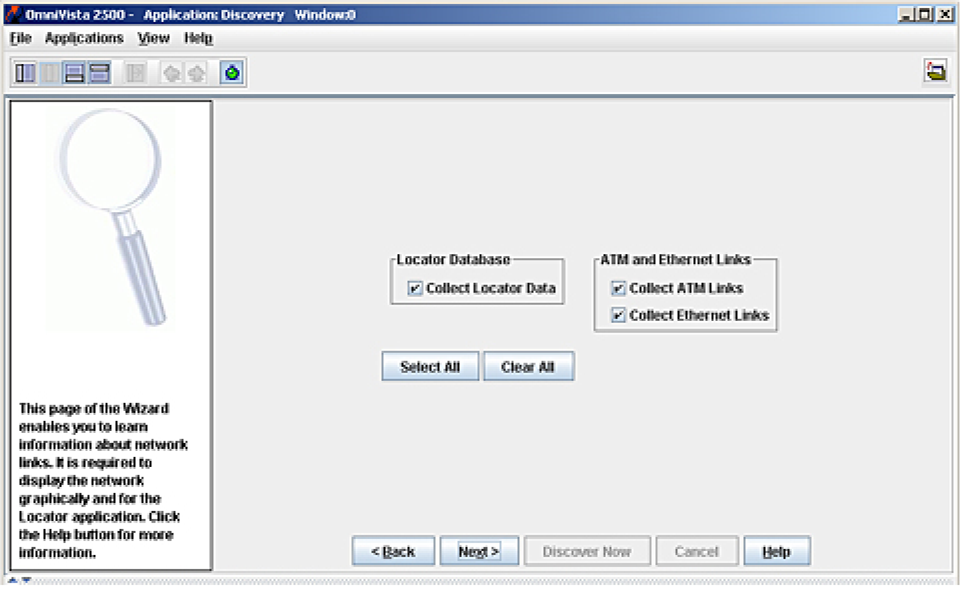
Click OK to accept all edits.

Click the **Next** button when the ARP window displays the desired gateways.

Link Discovery Options

The Link Discovery Options window enables you to specify the link information that you wish to learn during the discovery, as explained below.

Link Discovery Options



Locator Database

☑ Collect Locator Data

ATM and Ethernet Links

☑ Collect ATM Links

☑ Collect Ethernet Links

This page of the Wizard enables you to learn information about network links. It is required to display the network graphically and for the Locator application. Click the Help button for more information.

ATM and Ethernet Links

Click the **Collect ATM Links** checkbox if you want to learn the ATM links that exist in the network during the discovery. When enabled, SNMP gets are used to retrieve information on ATM links. The information is learned via PNNI (Private Network to Network Interface), an ATM protocol.

Click the **Collect Ethernet Links** checkbox if you wish to learn the physical links that exist in network devices that support adjacency protocols. When enabled, SNMP gets are used to retrieve information on existing physical links. Link information is maintained for XOS devices via the proprietary XMAP adjacency protocol. Link information is maintained for AOS devices via the proprietary AMAP adjacency protocol.

> **Note:** As stated, link information is discovered via adjacency protocols, which are supported by all AOS switches, XOS switches, and 61xx devices. However, OmniCore 5xxx devices, the OmniPCX, and most third-party devices do not support such adjacency protocols. You can specify that you want link information gathered for these devices using an alternative method - functionality from OmniVista's Locator application - by creating and using an SNMP Setup that has the **Discover Links** combo box set to **As OEM Device**. (Click here for more information on SNMP Setups.) You can also specify this after the devices themselves are discovered, by editing the devices to enable the **Handle as an OEM Device** checkbox on the Edit Discovery Manager Entry window. When this checkbox is enabled, link information will be gathered for the device during each subsequent polling cycle, using logic from the Locator application.

Locator Database

Click the **Collect Locator Data** checkbox to collect information required by the Locator application.

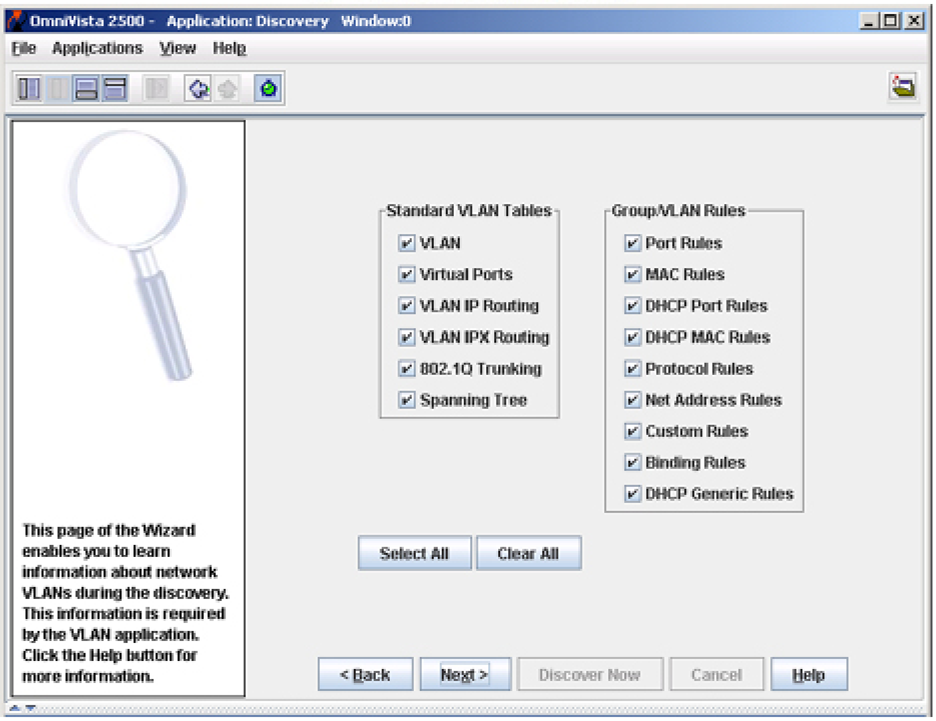
Click the **Next** button when your selections are complete.

VLAN Discovery Options

The VLAN Discovery Options window, shown below, enables you to specify the VLAN information that you want to learn during the discovery. Enable (check) checkboxes to learn the respective VLAN information.

> **Note:** When a checkbox in the window below is checked, each discovered switch will be queried for the respective information. This will make the discovery take longer, so it is not advisable to check all boxes indiscriminately. For example, if your network does not include VLAN port rules, do not check the **Port Rules** checkbox.

VLAN Discovery Options



Standard VLAN Tables
- ☑ VLAN
- ☑ Virtual Ports
- ☑ VLAN IP Routing
- ☑ VLAN IPX Routing
- ☑ 802.1Q Trunking
- ☑ Spanning Tree

Group/VLAN Rules
- ☑ Port Rules
- ☑ MAC Rules
- ☑ DHCP Port Rules
- ☑ DHCP MAC Rules
- ☑ Protocol Rules
- ☑ Net Address Rules
- ☑ Custom Rules
- ☑ Binding Rules
- ☑ DHCP Generic Rules

This page of the Wizard enables you to learn information about network VLANs during the discovery. This information is required by the VLAN application. Click the Help button for more information.

Standard VLAN Tables

VLAN
Enable this checkbox to learn the VLAN instances in each discovered switch and the ports associated with each VLAN.

Virtual Ports
Enable this checkbox to learn the virtual ports in each discovered switch.

VLAN IP Routing
Enable this checkbox to learn the IP Virtual Router instances associated with each VLAN in each discovered switch.

VLAN IPX Routing
Enable this checkbox to learn the IPX Virtual Router instances associated with each VLAN in each discovered switch.

802.1q Trunking
Enable this checkbox to learn the 802.1q trunks associated with each VLAN in each discovered switch.

Spanning Tree
Enable this checkbox to learn Spanning Tree information for each discovered AOS switch.

> **Note:** Enabling this checkbox will not cause Spanning Tree information for XOS devices to be learned. Spanning Tree information for XOS devices must be gathered "manually". The VLAN application will notify the user when the application needs to gather XOS Spanning Tree information for display. The VLAN application also allows users to initiate the gathering of XOS Spanning Tree information.

Group/VLAN Rules

Port Rules
Enable this checkbox to learn any port rules that exist in Groups or VLANs in each discovered switch.

MAC Rules
Enable this checkbox to learn any MAC rules that exist in Groups or VLANs in each discovered switch.

DHCP Port Rules
Enable this checkbox to learn any DHCP Port rules that exist in Groups or VLANs in each discovered switch.

DHCP MAC Rules
Enable this checkbox to learn any DHCP MAC rules that exist in Groups or VLANs in each discovered switch.

Protocol Rules
Enable this checkbox to learn any Protocol rules that exist in Groups or VLANs in each discovered switch.

Net Address Rules
Enable this checkbox to learn any IP and IPX Network Address rules that exist in Groups or VLANs in each discovered switch.

Custom Rules
Enable this checkbox to learn any Custom rules that exist in Groups or VLANs in each discovered switch.

Binding Rules
Enable this checkbox to learn any Binding rules that exist in Groups or VLANs in each discovered switch.

DHCP Generic Rules
Enable this checkbox to learn any DHCP Generic rules that exist in Groups or VLANs in each discovered switch.

Click the **Next** button when your selections are complete.

Periodic Discoveries

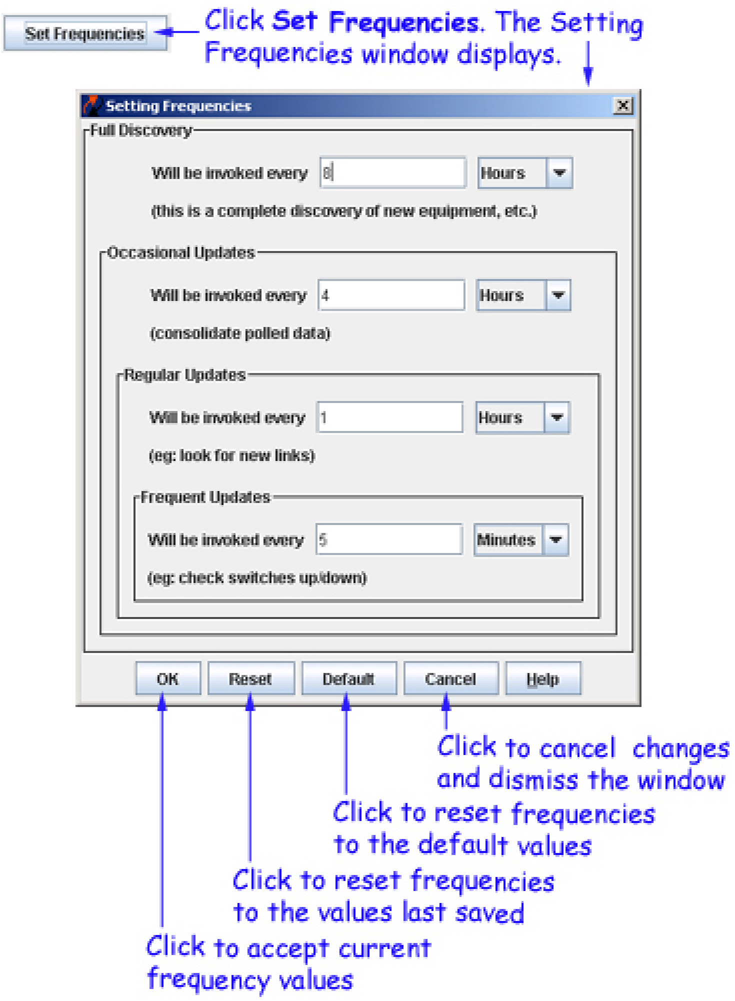
Once the first discovery is complete, OmniVista performs automatic periodic discoveries to keep its information about the network updated. By default, OmniVista performs:

- A full discovery every eight hours
- "Occasional updates" every four hours
- "Regular updates" every hour
- "Frequent updates" every five minutes
- "Down switch" polling once every minute

A detailed description of each type of automatic discovery polling is found in the sections that follow.

The Setting Frequencies Window

The Setting Frequencies window, shown below, enables you to redefine the frequency of each periodic discovery listed above. The Setting Frequencies window is displayed when the **Set Frequencies** button on the last page of the Discovery Wizard is clicked, as shown below. To use the Setting Frequencies window, enter the desired values, set the combo boxes to **Minutes**, **Hours**, or **Days**, as desired, and then click the **OK** button.



Click **Set Frequencies**. The Setting Frequencies window displays.

Full Discovery

Will be invoked every 8 Hours

(this is a complete discovery of new equipment, etc.)

Occasional Updates

Will be invoked every 4 Hours

(consolidate polled data)

Regular Updates

Will be invoked every 1 Hours

(eg: look for new links)

Frequent Updates

Will be invoked every 5 Minutes

(eg: check switches up/down)

Click to cancel changes and dismiss the window

Click to reset frequencies to the default values

Click to reset frequencies to the values last saved

Click to accept current frequency values

Automatic Periodic Discovery Polling

OmniVista performs the following polling during each type of automatic periodic discovery.

Down Switch Polling (once each minute)

Once each minute, OmniVista polls those switches known to be down. Polling is limited to reading a single scalar variable, sysObjectID. The frequency of down switch polling is not configurable.

> **Note:** The Switch Monitoring Preferences setting determines whether Down Switch Polling occurs all the time, or only when system-wide polling is enabled. (The Switch Monitoring Preferences setting is part of the Preferences application.)

Frequent Updates (by default, every five minutes)

By default, OmniVista makes Frequent Updates every five minutes. The frequency of Frequent Updates is user-configurable. Frequent Updates include:

- Down switch polling as described above
- Polling the standard MIB-II scalar variables sysName and sysDescr
- For AOS devices, polling for:
    - The running directory (certified or working), the certification status, and the administrative status of all CMMs.
    - The configuration change status; i.e., has the configuration changed since the last save of memory.
- Polling the state of all known ATM (i.e., PNNI) and Ethernet links
- For SecureView, checking to see if switch is using an Authentication Server.

Regular Updates (by default, once each hour)

By default, OmniVista makes Regular Updates once each hour. The frequency of Regular Updates is user-configurable. Regular Updates include:

- Down switch polling as described above
- Frequent Update polling as described above.
- Additional polling for:
    - Detailed chassis, module, and port information
    - VLAN information
    - LDAP configuration for QoS
    - Health MIB
    - Link Aggregation
    - ATM accounting
    - ATM (i.e., PNNI) link discovery
    - Ethernet link discovery (i.e., polling AMAP tables)
    - Locator:
        - MAC address column from the ARP table
        - Bridge forwarding table
        - IP-MAC table for XOS devices

Occasional Updates (by default, every four hours)

By default, OmniVista makes Occasional Updates once every four hours. The frequency of Occasional Updates is user-configurable. Occasional Updates include:

- Down switch polling as described above
- Frequent Update polling as described above
- Regular Update polling as described above.

Note: Currently, no additional polling is performed for Occasional Updates.

Full Discovery (by default, every eight hours)

By default, OmniVista makes a Full Discovery once every eight hours. The frequency of Full Discoveries is user-configurable. Full Discoveries include:

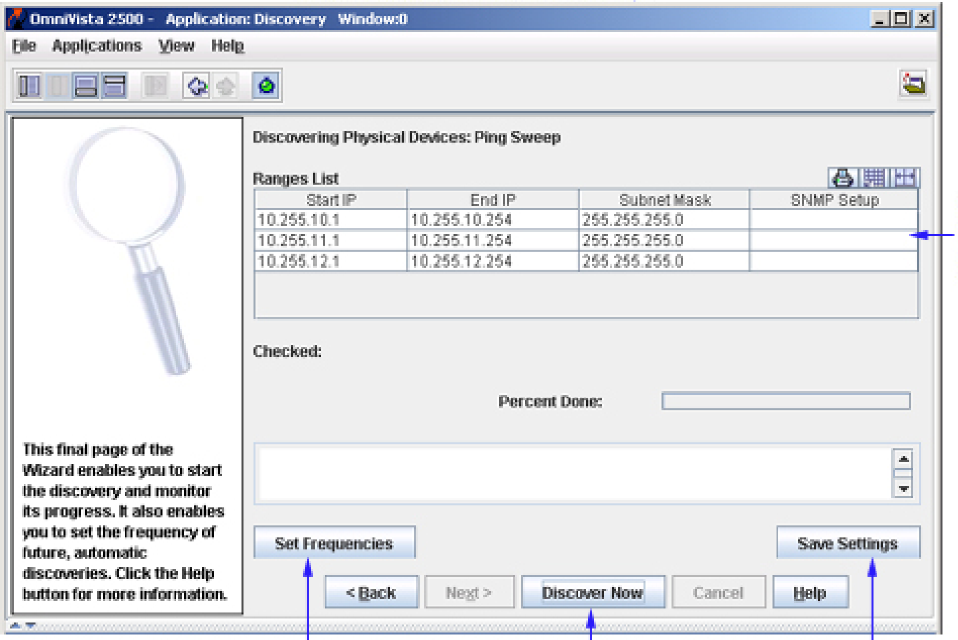
- Down switch polling as described above
- Frequent Update polling as described above
- Regular Update polling as described above
- Autodiscovery of network switches via Ping Sweep discovery or ARP discovery, as specified in the Discovery application.

  Note: If Ping Sweep and ARP discoveries are configured, then both the discoveries will run in the background. However, the final Discovery Wizard screen will display the last discovered information only.

Performing the Discovery

The last window in the Discovery Wizard enables you to perform the actual discovery. It also enables you to save all current settings in the Discovery application and to set the frequency of future, automatic discovery polling, as explained below. (The window shown below displays for a ping sweep discovery; a slightly different version of the window displays for an ARP discovery.)

Performing the Discovery



Discovering Physical Devices: Ping Sweep

Ranges List

Start IP	End IP	Subnet Mask	SNMP Setup
10.255.10.1	10.255.10.254	255.255.255.0	
10.255.11.1	10.255.11.254	255.255.255.0	
10.255.12.1	10.255.12.254	255.255.255.0	

Checked:

Percent Done:

This final page of the Wizard enables you to start the discovery and monitor its progress. It also enables you to set the frequency of future, automatic discoveries. Click the Help button for more information.

The ranges (or gateways) to be discovered.

Click **Set Frequencies** to display the Setting Frequencies window, which enables you to specify the frequency of future, automatic discovery polling.

Click **Save Settings** to save all current settings in the Discovery application without performing a discovery. The settings will persist and be used for future, automatic discovery polling.

Click **Discover Now** to start the discovery. Note that settings will not be saved unless **Save Settings** is clicked.

Saving Discovery Settings

Click the **Save Settings** button to save all current settings in the Discovery application without performing a discovery. The settings will persist in the Discovery application and will be used during future, automatic discovery polling.

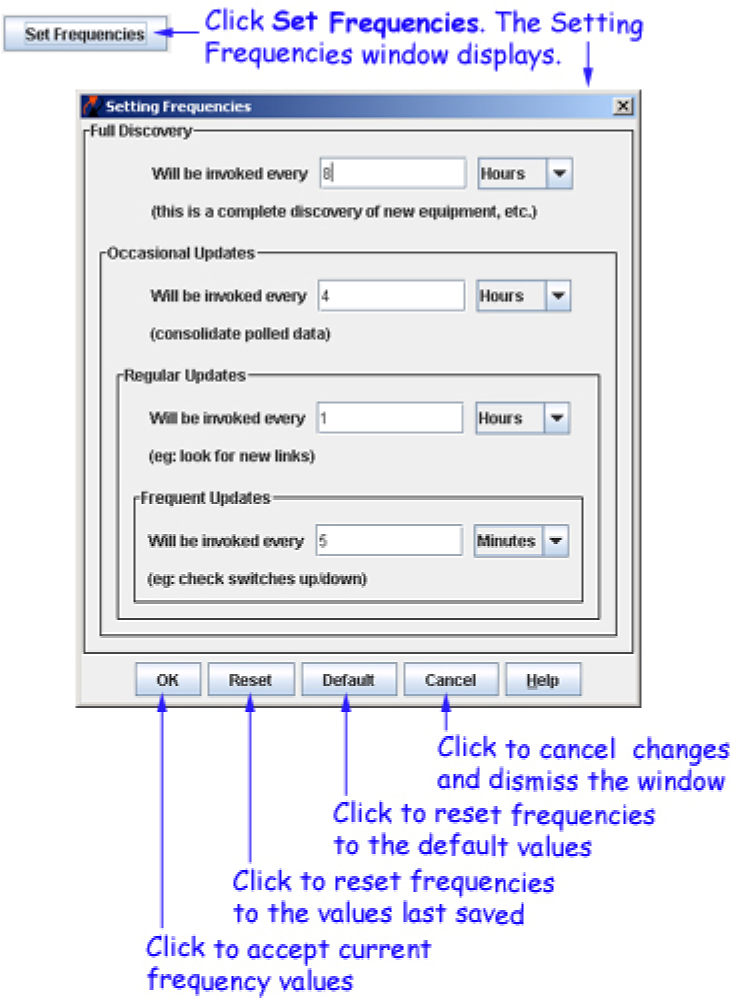
Setting the Frequency of Future Discovery Polling

Once the first discovery is complete, OmniVista performs automatic periodic discovery polling to keep its information about the network updated. By default, OmniVista performs:

- A full discovery every eight hours
- "Occasional updates" every four hours

- "Regular updates" every hour
- "Frequent updates" every five minutes
- "Down switch" polling once every minute

You can change these default values by clicking the **Set Frequencies** button to display the Setting Frequencies window, which enables you to define the frequency of the periodic discovery polling. To use the Setting Frequencies window, enter the desired values, set the combo boxes to **Minutes**, **Hours**, or **Days**, as desired, and then click the **OK** button. Click here for specific information on the types of polling performed.



Click **Set Frequencies**. The Setting Frequencies window displays.

Setting Frequencies

Full Discovery

Will be invoked every 8 Hours

(this is a complete discovery of new equipment, etc.)

Occasional Updates

Will be invoked every 4 Hours

(consolidate polled data)

Regular Updates

Will be invoked every 1 Hours

(eg: look for new links)

Frequent Updates

Will be invoked every 5 Minutes

(eg: check switches up/down)

Click to cancel changes and dismiss the window

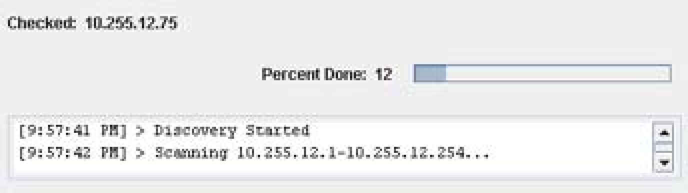
Click to reset frequencies to the default values

Click to reset frequencies to the values last saved

Click to accept current frequency values

Performing the Discovery

To perform the discovery, click the **Discover Now** button on the last page of the Discovery Wizard. The discovery begins immediately and its progress is reported as shown below.



Checked: 10.255.12.75

Percent Done: 12

```
[9:57:41 PM] > Discovery Started
[9:57:42 PM] > Scanning 10.255.12.1-10.255.12.254...
```

After Discovery Completes

When the discovery completes, all discovered switches display in the Topology application's list of All Discovered Devices and the Topology Tree, which open automatically for your convenience. OmniVista arranges the switches it discovers into subnets by default, according to the class of the switch IP address. OmniVista's default subnet creation can be overridden by the creation of manual (i.e., user-defined) subnets. If manual subnets are specified before the discovery is performed, OmniVista will place the discovered switches into the manual subnets as appropriate. Refer to the *Managing Subnets* section of the Topology help for further information on default subnet creation, subnet naming conventions, and manual subnets.

> **Note:** If Ping Sweep and ARP discoveries are configured, then both the discoveries will run in the background. However, the final Discovery Wizard screen will display the last discovered information only.

Preparing AOS Switches for Discovery

Security is a key feature on OmniSwitch 6000s/7000s/8000s. For security reasons, OmniVista cannot discover AOS switches that have the factory-default configuration. You must explicitly reconfigure an AOS switch so that OmniVista can discover it. Reconfiguring a switch so that it can be discovered consists of three basic tasks:

- Unlocking SNMP management sessions
- Setting the SNMP security level
- Creating switch users.

Unlocking SNMP Management Sessions

When you access an AOS switch the first time, you must use a direct console port connection. All other management methods such as Telnet, FTP, HTTP (WebView), and SNMP (OmniVista) are "locked out" until they are manually unlocked by the user. The CLI command used to unlock management session types is **aaa authentication**.

When you unlock management session types, you are granting switch access to non-local sessions (e.g., Telnet, FTP, HTTP, SNMP). As a result, users who know the correct user login and password will have remote access to the switch. For more information on switch security, refer to the "Managing Switch Security" chapter of your *Switch Management Guide*.

Unlocking All Management Sessions

To unlock all session types, including SNMP, enter the following command syntax at the CLI prompt:

```
-> aaa authentication default local
```

This command unlocks all management session types and specifies that users are to be authenticated through the local database. If you want to use a server other than the local database for authentication, refer to the "Managing Switch Security" chapter of your *Switch Management Guide*. Note that SNMP can only use LDAP servers or the local database for authentication.

Unlocking Individual Management Sessions

You can also unlock management session types on a one-by-one basis. To unlock SNMP management sessions only, enter the following command:

```
-> aaa authentication snmp local
```

To unlock HTTP (WebView) sessions only, enter the following command:

```
-> aaa authentication http local
```

You cannot specify more than one session type in a single command line. However, you can still unlock multiple session types by using the **aaa authentication** command in succession. For example:

```
-> aaa authentication snmp local
-> aaa authentication http local
-> aaa authentication ftp local
```

Authentication Servers

All examples of the **aaa authentication** command shown above specify that users are to be authenticated through the local database. As stated, SNMP can only use LDAP servers or the local database for authentication. (Other management session types can use RADIUS servers, ACE/Servers, LDAP servers, or the local database for user authentication.)

A total of four servers can be specified for each management session type, including SNMP sessions. The first server specified is polled first for user information; if that server is unavailable the next server specified is polled, and so on. LDAP servers are specified by their server name. For example:

```
-> aaa authentication snmp ldap1 ldap2 local
```

This command unlocks SNMP management sessions and specifies that users are to be authenticated through the server named ldap1. If server ldap1 is unavailable, the server named ldap2 will be used. If both servers are unavailable the local database will be used for authentication.

Refer to the "Managing Switch Security" chapter of your *Switch Management Guide* for further information on management sessions, authentication servers, and the **aaa authentication** command.

Setting the SNMP Security Level

OmniVista can discover switches using SNMP Version 1, Version 2, or Version 3. SNMP Version 3 provides authentication and encryption, and is the most secure version of SNMP. SNMP Version 3 can use SHA or MD5 authentication, with or without DES encryption.

An AOS switch must be configured to accept the version and type of SNMP queries that OmniVista sends. The CLI command **snmp security** enables you configure a switch to accept the desired version and type of SNMP. By default, **snmp security** is set to **privacy all**, which means the switch accepts only authenticated and encrypted SNMP Version 3 Sets, Gets, and Get-Nexts. To configure a switch to accept different versions and types of SNMP, enter the command **snmp security** followed by the appropriate command parameter from the table below. For example:

```
-> snmp security authentication all
```

snmp security Command Parameters	**SNMP Queries Accepted by the Switch**
no security	All SNMP queries are accepted
authentication set	SNMPv1, SNMPv2 Gets Non-authenticated v3 Gets and Get-Nexts Authenticated v3 Sets, Gets, and Get-Nexts Encrypted v3 Sets, Gets, and Get-Nexts

authentication all	Authenticated v3 Sets, Gets, and Get-Nexts Encrypted v3 Sets, Gets, and Get-Nexts
privacy set	Authenticated v3 Gets and Get-Nexts Encrypted v3 Sets, Gets, and Get-Nexts
privacy all	Encrypted v3 Sets, Gets, and Get-Nexts
traps only	All SNMP requests are rejected

For further information on configuring SNMP, refer to the "Using SNMP" chapter of your *Switch Management Guide*

Creating Switch Users

OmniVista cannot be used to create switch users. For security reasons, switch users must be created from the CLI (or from WebView). Note that when you first boot a new AOS switch, the default user available, **admin**, does NOT have SNMP access.

As previously stated, OmniVista can discover switches using SNMP Version 1, 2, or 3. If Discovery is using SNMP Version 1 or 2, switch users must exist that correlate with get community strings known to OmniVista. If Discovery is using SNMP Version 3, get community strings are ignored; however, switch users must exist that correlate with SNMP Version 3 parameters defined to OmniVista. The sections below provide more details.

If Using SNMP Version 1 or 2

For OmniVista to discover an AOS switch, at least one appropriate user must first be created on the switch. This is accomplished by logging directly into the switch and using the CLI command **user**. The user name created on the switch must be identical to the SNMP get community name known to OmniVista. For example, if only the default get community name **public** is known to OmniVista, a user named **public** must exist on the switch in order for it to be discovered. Alternatively, you can create a user with any name and use the CLI command **snmp community map** to "map" the user to the get community name **public** (or any known get community name). Get community names can be made known to OmniVista before discovery is performed by entering them in the **Passwords** field of either the ARP window or the Ping Sweep window (as determined by the type of discovery you are performing).

Refer to the "Managing Switch User Accounts" chapter of your *Switch Management Guide* for more information on creating users, configuring privileges for users, and mapping users to Get Community Strings.

If Using SNMP Version 3

In order for OmniVista to discover an AOS switch using SNMP Version 3, at least one appropriate user must first be created on the switch. This is accomplished by logging directly into the switch and using the CLI command **user**. The user name created on the switch must be identical to the SNMP Version 3 user name known to OmniVista. The switch user must also be configured for the same type of SNMP Version 3 authentication and encryption (if any) that OmniVista is configured to use. SNMP Version 3 can use either MD5 or SHA authentication, with or without DES encryption.

Authentication uses a secret key to produce a "fingerprint" of the message. The fingerprint is included within the message. The device that receives the message uses the same secret key to validate that the fingerprint is correct. If it is, and if the message was received in a timely manner, then the message is considered authenticated. Otherwise, the message is discarded. The fingerprint is called a Message Authentication Code, or MAC. The MAC is computed by the switch from the user's password. The MD5 and SHA authentication protocols produce the MAC in a similar, but not an identical, manner. Both MD5 and SHA can also use DES encryption.

You can configure a switch user for the following types of SNMP Version 3 authentication and encryption:

- SHA. The SHA authentication algorithm is used for authenticating SNMP queries.
- MD5. The MD5 authentication algorithm is used for authenticating SNMP queries.
- SHA and DES. The SHA authentication algorithm and DES encryption is used for authenticating and encrypting SNMP queries.
- MD5 and DES. The MD5 authentication algorithm and DES encryption is used for authenticating and encrypting SNMP queries.

The **user** command enables you to specify the type of authentication and encryption desired for the user (**sha**, **md5**, **sha+des**, **md5+des**). As an example, to configure a user named "jennifer" with a password of "secret99", SHA authentication and DES encryption, enter the **user** command as follows:

```
-> user jennifer password secret99 sha+des
```

When SNMP authentication is specified, as in the example above, an SNMP secret key is computed from the user password based on the authentication/encryption setting. In this example, the switch would use the SHA authentication algorithm and DES encryption on the secret99 password to compute the SNMP secret key for user jennifer. The key is computed in hexadecimal form. The key is not displayed in the CLI. You can view the secret key in an ASCII configuration file, in hexadecimal, by using the switch CLI command **configuration snapshot aaa**. The secret key for each switch user is indicated in the file by the syntax "authkey."

> **Important Note:** If you are using authentication, the secret key that the switch computes must be specified to OmniVista, in hexadecimal form, as the **Auth Password** for the SNMP Version 3 user name. If you are using encryption in addition to authentication, that same secret key, in hexadecimal form, must also be entered in OmniVista as the **Priv Password** for the SNMP Version 3 user name.

For more information:

- Refer to the "Managing Switch User Accounts" chapter of your *Switch Management Guide* for more information on the **user** command, creating users, and configuring privileges for users.
- Refer to your *CLI Reference Guide* for complete information on all command syntax and usage guidelines.