

Getting Started with VLANs

One of the main benefits of using VLANs to segment network traffic, is that VLAN configuration and port assignment is handled through software. This eliminates the need to physically change a network device connection or location when adding or removing devices from the VLAN broadcast domain. The OmniVista VLANs application software handles the following VLAN configuration tasks performed on XOS, AOS, and OmniStack devices:

- Creating or removing VLANs.
- Modifying VLAN parameters, such as description, administrative status, Spanning Tree status, mobility status (XOS devices only), authentication status, and router interface definitions.
- Changing default VLAN port assignments.
- Creating 802.1Q tagged VLAN port assignments.
- Configuring VLAN Spanning Tree bridge and port parameters.
- Defining VLAN IP and IPX router interfaces to allow Layer 3 routing of VLAN traffic. (IPX routing is not supported on OmniSwitch 6600 series switches.)
- Defining VLAN rules to classify mobile port traffic and trigger dynamic VLAN port assignment.
- Displaying a logical view of the VLAN network configuration.
- Displaying a physical view of the VLAN network on a device by device basis.

Note: The term "OmniStack" refers only to OmniStack models 6024, 6048, 6124, 6148, 6300-24, and 8088. The term "XOS" includes all other OmniStack devices that run XOS software.

The initial configuration for all Alcatel switches consists of a default VLAN 1 and all switch ports are initially assigned to this VLAN. When a switching module is added to the switch, the physical ports on that module are also assigned to VLAN 1. If additional VLANs are not configured on the switch, then the entire switch is treated as one large broadcast domain. All ports will receive all traffic from all other ports.

In compliance with the IEEE 802.1Q standard, each VLAN is identified by a unique number, referred to as the VLAN ID. The user specifies a VLAN ID to create, modify or remove a VLAN and to assign switch ports to a VLAN. When a packet is received on a port, the VLAN ID for that port is inserted into the packet. The packet is then bridged to other ports that are assigned to the same VLAN ID. In essence, the VLAN broadcast domain is defined by a collection of ports and packets assigned to its VLAN ID.

The operational status of a VLAN remains inactive until at least one active switch port is assigned to the VLAN. This means that VLAN properties, such as Spanning Tree and/or router interfaces, also remain inactive. Ports are considered active if they are connected to an active network device. Non-active port assignments are allowed, but do not change the VLAN's operational state.

Note: On the XOS switch platform the term "Group" refers to a VLAN.

When using the OmniVista VLANs application to configure VLANs in your network, consider the following:

- There is no staging of VLAN configuration changes. When you click the **Apply** button, changes are sent directly to the device (switch) and are processed in real time.
- If an error occurs when changes are applied to the switch, any changes successfully made to that point are maintained and not backed out of the switch configuration.
- The parameter values displayed in the VLAN Table, except for the VLAN ID field, is the value obtained from the switch polled that has the lowest IP host address. For example, if VLAN 9 exists on three different switches with IP addresses of 10.0.0.1, 10.0.0.2, and 10.0.0.3 and each

instance of the VLAN has a different description, the VLAN 9 description from switch 10.0.0.1 is displayed in this window.

- When you modify VLAN parameters using the VLAN Table, however, the changes are applied across all switches in the topology that have this VLAN configured. For example, if you selected VLAN 18 and changed the description to "Marketing Department", all switches that contain VLAN 18 would receive this new description value.
- This release of OmniVista VLANs does not support AutoTracker VLANs. You must telnet (or use other available means of access) directly to the switch to configure AutoTracker VLANs.
- If you encounter problems when attempting to delete a Group from an XOS switch configuration, try removing any AutoTracker VLANs and/or switch ports assigned to the Group before attempting to delete the VLAN again.

Note that when you open the OmniVista VLANs application, the following warning message displays if the application detects that it does not have current VLAN information for one or more devices.

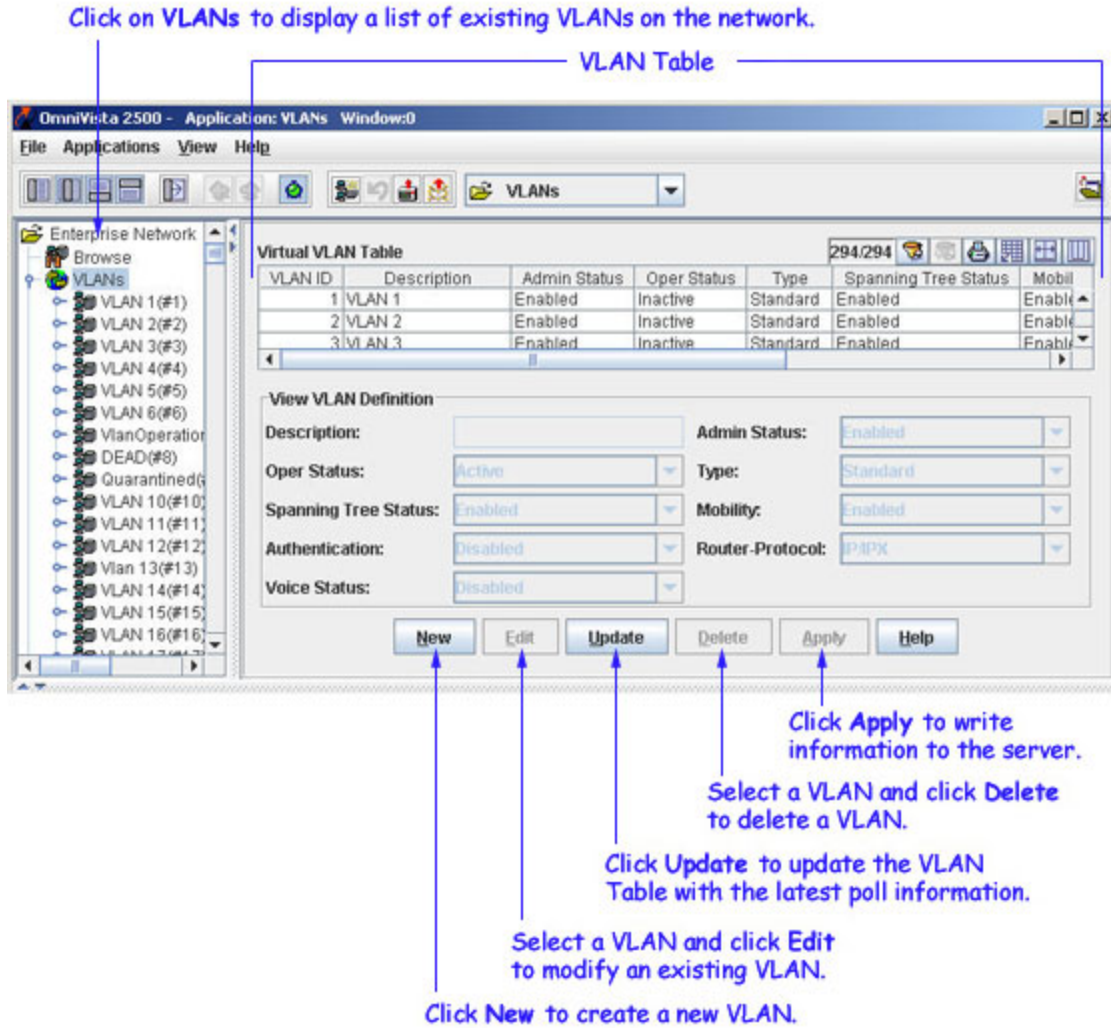


The warning message window contains a list of management IP addresses for those devices that require discovery of VLAN information. Click on **Discover Devices** in this window to activate the Discovery application. Refer to Discovery help for more information about discovering devices. If you click on **Cancel**, the VLANs application database may not contain the latest VLAN configuration for the devices listed in the warning message window.

Using the VLANs Tree

The VLANs portion of the Tree provides a list of all VLANs configured in your network. To display this list, select **VLANs** in the Tree. This displays the VLAN Table, as shown below. The VLAN Table contains a list of all VLANs configured across one or more switches in your network topology.

The VLANs Tree also enables you to create, modify, and delete VLANs. Click [here](#) for more information on configuring VLANs.

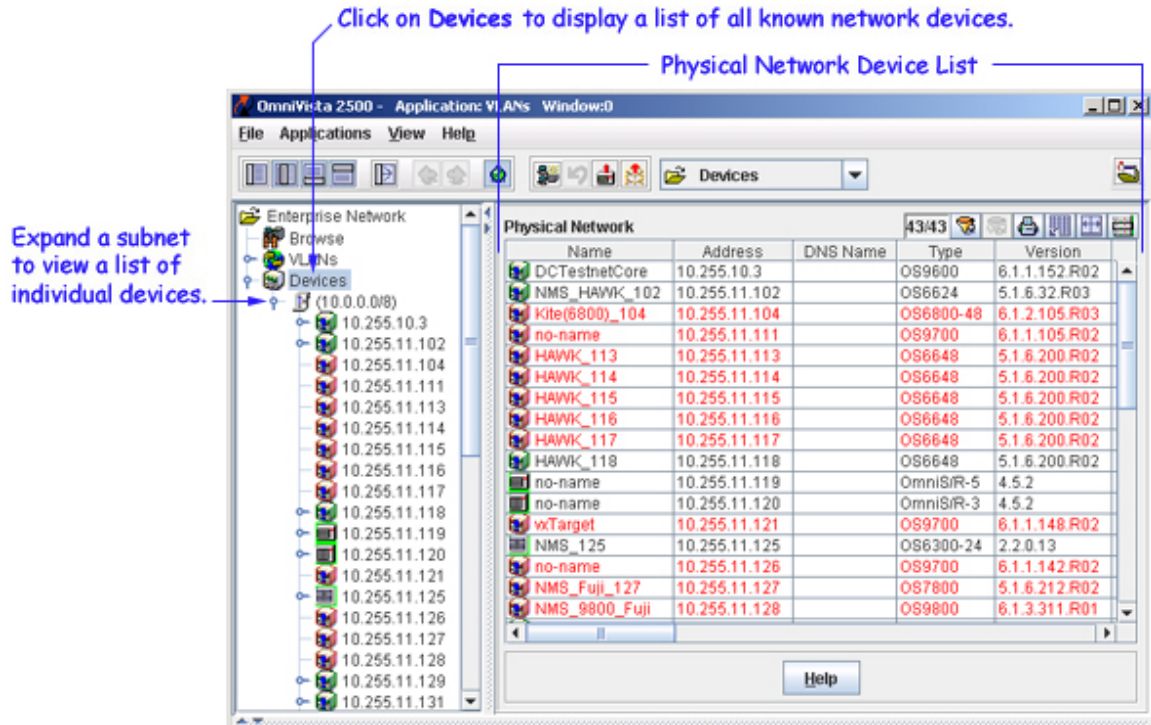


Note: Throughout the VLAN application, prior to applying a configuration, you can use the **Update** button to return all fields to their original values.

Using the Devices Tree

The Devices portion of the Tree provides a list of all AOS, XOS, and OmniStack devices known to the VLANs application. To display the Physical Network list, select **Devices** in the Tree, as shown below. Each device entry in this list contains fields that display related system parameter values, such as device name, management IP address, etc. Click here for information about the fields in Physical Network list.

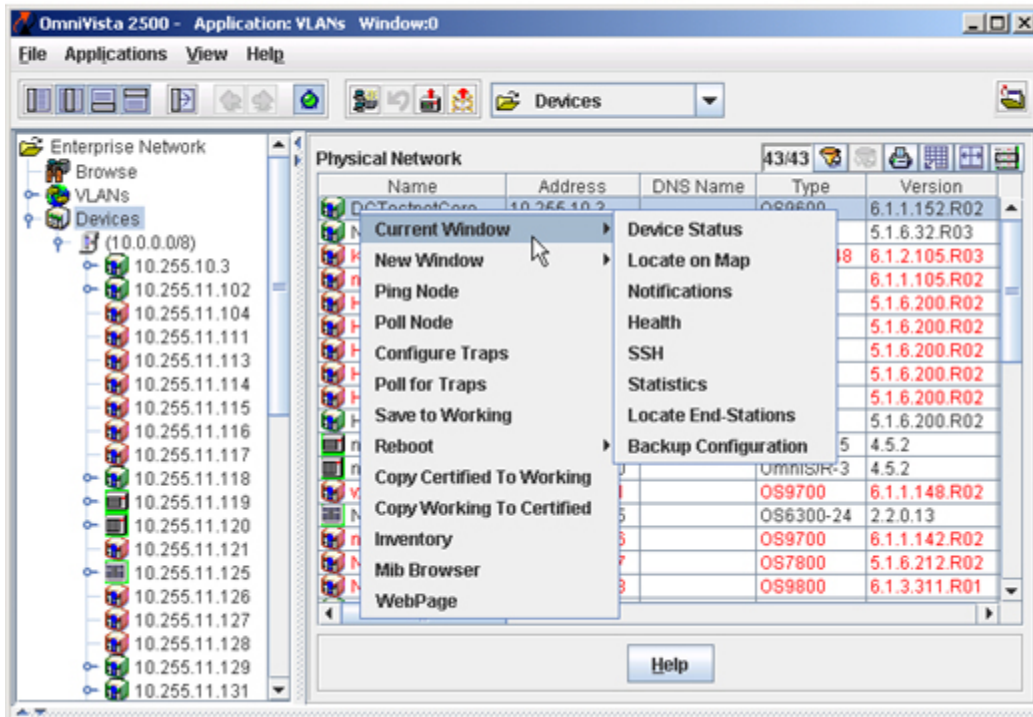
To view individual devices in the physical network, click open **Devices** to view a list of known subnets. You can then click open a subnet in the Tree to view a list of individual devices that belong to that subnet. Each device in the subnet is listed by its management IP address.



Pop-Up Menu Functionality

Click right on one or more devices in the Devices Physical Network list to display a pop-up menu. Somewhat different versions of the pop-up menu display for various devices. The pop-up menu for AOS devices is shown below. Each menu item allows you to launch additional applications and/or tasks to access, manage, or configure the selected device. For more information about these menu items, refer to the Topology application help.

Pop-Up Menu for AOS Devices
(Right-click on an AOS device to display the menu.)



Right-click right on any one device in the Devices Tree to display the Tree Pop-Up menu. This menu is the same menu displayed when you click on any device in the Devices Physical Network list.

Displaying the VLAN Configuration for a Device

The Devices portion of the Tree allows you to view VLAN information on an individual device basis. This provides you with a physical network view of your VLAN configuration, instead of a logical view of your network provided by the VLANs portion of the Tree.

To view all VLANs configured on an individual device, click on the device management IP address displayed in the subnet list. This activates the VLAN Definitions window for the selected device. For example, the VLAN Definitions window shown below is for an AOS device. This same window is displayed for XOS devices. However, a different VLAN Definitions window is displayed if an OmniStack device is selected (click here for more information about the OmniStack VLAN Definitions window).

In addition to displaying the VLAN configuration for an individual device, the VLAN Definitions window enables you to modify one or more VLAN definitions and configure port mobility parameters. For more information,

- Click here for help on configuring VLANs on AOS and XOS devices.
- Click here for help on configuring VLANs on OmniStack devices.
- Click here for help on configuring the mobility feature (only supported on AOS and XOS devices).

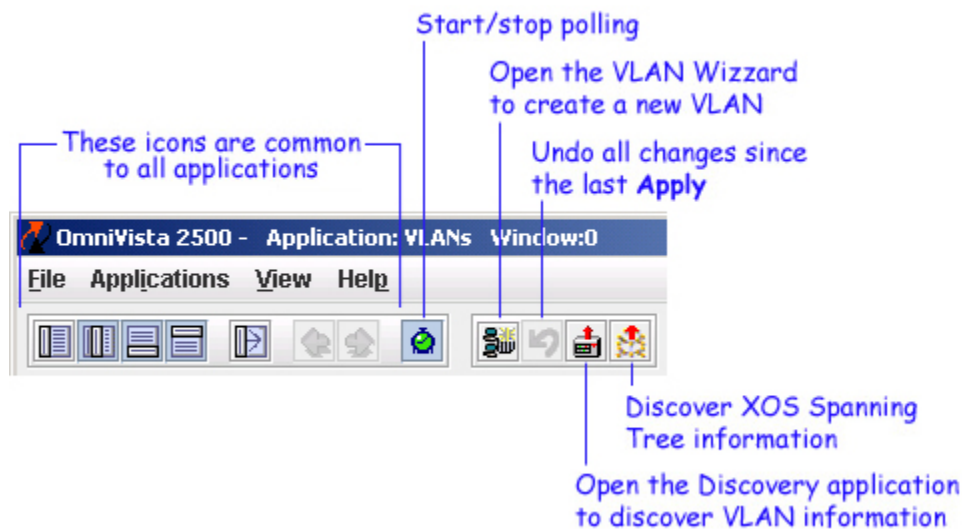
Color Coding

Entries in the VLANs list of devices, the Devices Physical Network list and device icons in the Tree can display green, red, or orange. Devices displayed in green are up (responding to OmniVista's polls). Devices displayed in red are down (not responding to OmniVista's polls). Devices displayed in orange are in the warning state (the switch has sent at least one warning or critical trap).

In addition, icons for AOS devices display a blue exclamation mark when the switch configuration is in the Unsaved state (changes have been made to the running configuration of the switch that have not been saved to the working directory) or the Uncertified state (the working directory has changes that are not in the certified directory). Click here for more information.

The VLANs Application Toolbar

The toolbar that displays when the VLANs application opens contains icons that enable you to perform certain tasks quickly, as shown and explained below.



Assigning Ports to VLANs

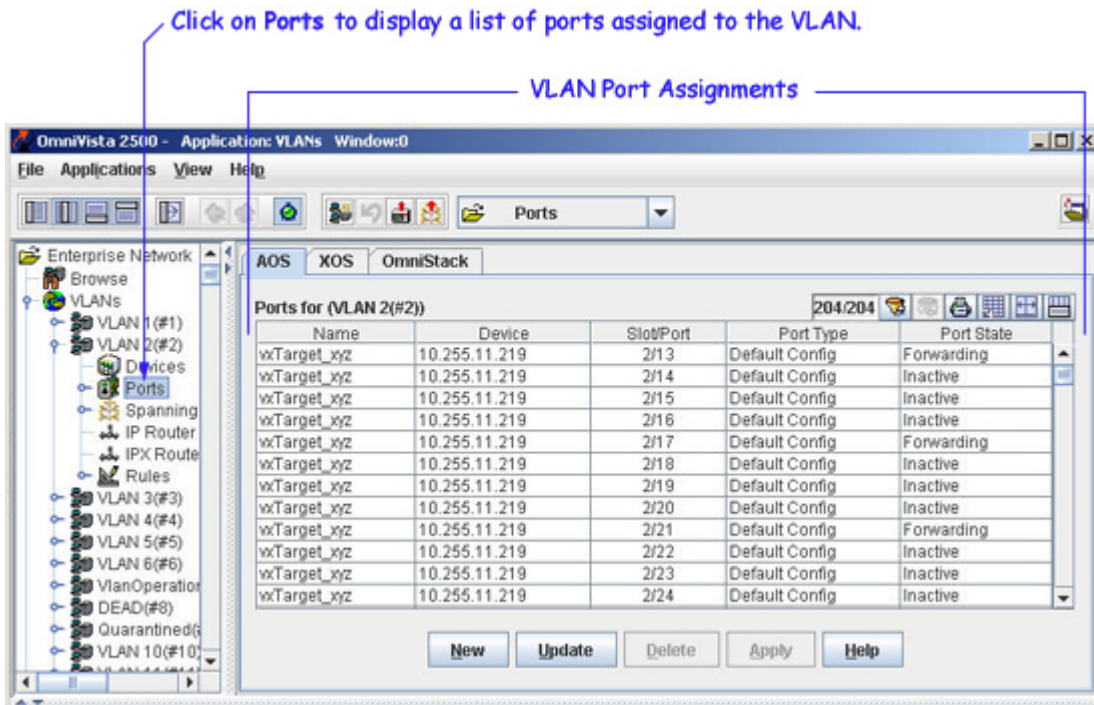
Initially all switch ports are assigned to VLAN 1, which is also their *configured default* VLAN. When additional VLANs are created on the switch, ports are assigned to the VLANs so that traffic from devices connected to these ports is bridged within the VLAN domain.

Switch ports are either statically or dynamically assigned to VLANs. Methods for accessing and configuring static port assignments include the following:

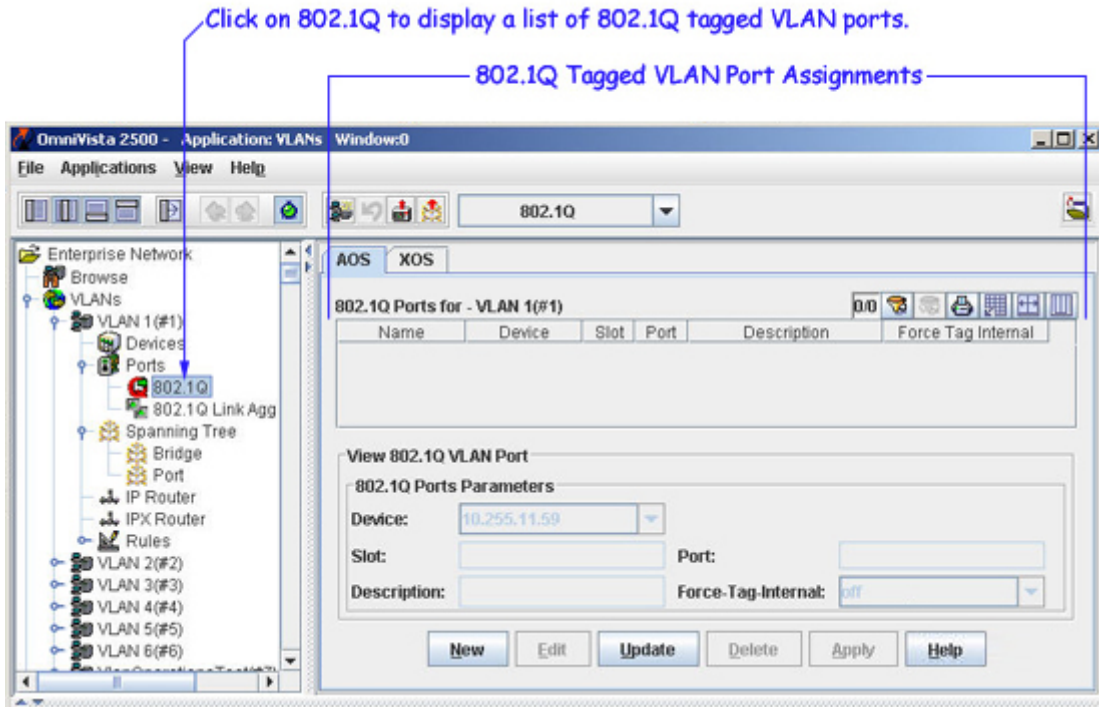
- Configuring a new default VLAN for both fixed and mobile ports.
- Using 802.1Q tagging to configure multiple VLANs on one physical port connection.
- Configuring a new default VLAN for a link aggregate of ports.

Dynamic assignment only applies to mobile ports and requires the additional configuration of VLAN rules. When traffic is received on a mobile port, the packets are examined to determine if their content matches any VLAN rules configured on the switch. If a match occurs, the mobile port is automatically assigned to the VLAN without user intervention. Click here for information about dynamically assigning ports to VLANs.

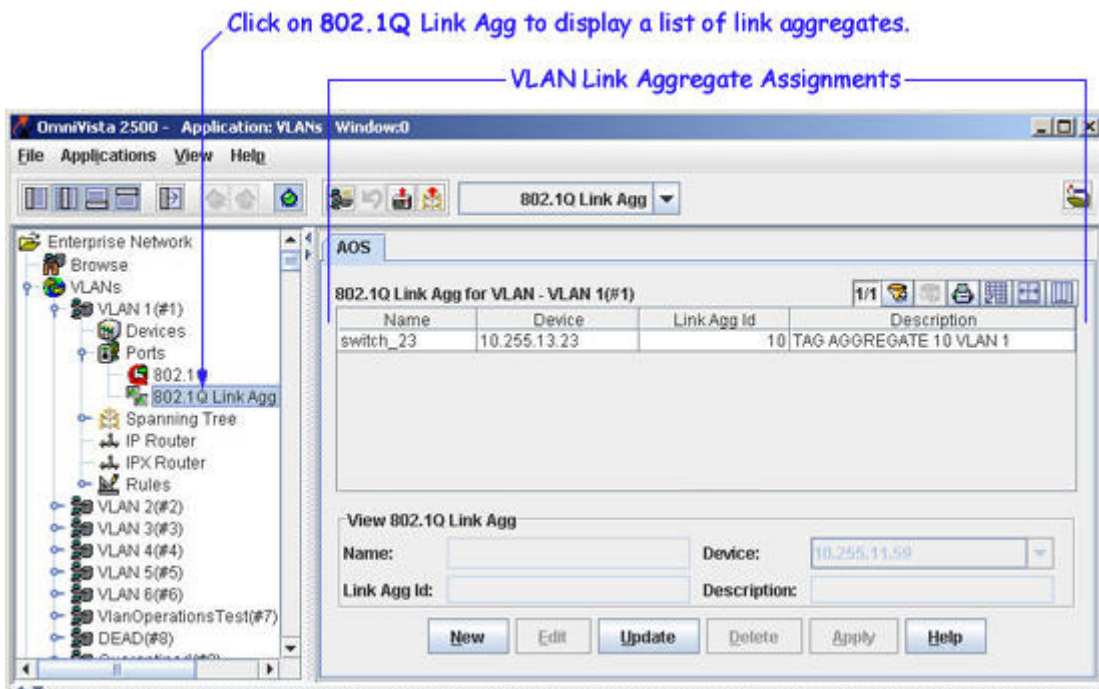
To access a list of ports currently assigned to a VLAN, click on the **Ports** icon underneath the desired VLAN in the Tree. If the selected VLAN contains AOS, XOS, and OmniStack devices, then AOS, XOS, and OmniStack Tabs are available for selection, as shown below. Each tab contains a list of ports on those devices that are currently assigned to the selected VLAN. Click on the appropriate tab to manage and configure VLAN port assignments.



To access a list of 802.1Q tagged port assignments for a VLAN, click open the **Ports** icon and click on the **802.1Q** icon. If the current VLAN contains both AOS and XOS devices, then both AOS and XOS 802.1Q Ports Tabs are available for selection, as shown below. (Note that an OmniStack tab is not available for this feature at this time.) Click on the appropriate tab to manage and configure 802.1Q VLAN port assignments.



To access a list of link aggregate assignments for a VLAN, click open the **Ports** icon and click on the **802.1Q Link Agg** icon. An AOS 802.1Q Link Agg Tab displays, as shown below. If the tab list is empty, there are no link aggregates assigned to this VLAN. (Note that XOS and OmniStack tabs are not available for this feature at this time). Use the AOS 802.1Q Link Agg Tab to assign the link aggregate to a new default VLAN.



Configuring Spanning Tree Parameters

The Spanning Tree Algorithm and Protocol (STP) is a self-configuring algorithm that maintains a loop-free topology while providing data path redundancy and network scalability. STP software is active on all switches by default. As a result, a loop-free network topology is automatically calculated based on default Spanning Tree switch, VLAN (bridge), and port parameter values. It is only necessary to configure Spanning Tree parameters to change how the topology is calculated and maintained.

To access the current STP information for AOS and XOS devices assigned to the VLAN, click on the **Spanning Tree** icon underneath the desired VLAN in the Tree. The Spanning Tree List View window, shown below, displays a list of all devices that contain the selected VLAN in their configuration and provides the current Spanning Tree topology information for each instance of the VLAN. Each entry in the list represents a single device and includes Spanning Tree parameter values. Click here for more information about Spanning Tree parameter fields.

To configure Spanning Tree bridge or port parameters, click open **Spanning Tree** in the Tree and then click on either **Bridge** or **Port**. Note that changing these parameter values will impact your Spanning Tree calculations and may trigger a topology change in your network.

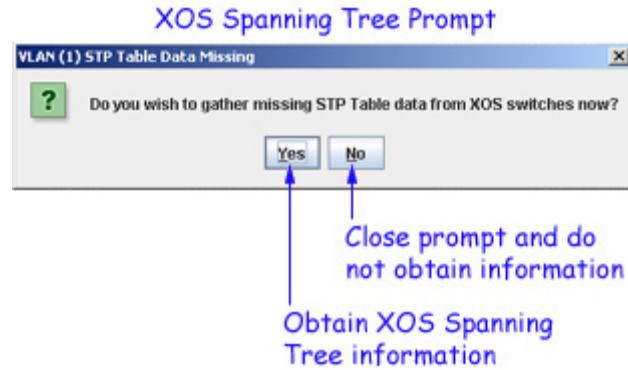
Click on Spanning Tree to display Spanning Tree information for each VLAN device.

Expand Spanning Tree and select Bridge or Port to configure Spanning Tree parameters.

VLAN Spanning Tree Information

Name	Address	Protocol	Priority	Maximum Age	Hello Time	Forward Delay
demo6850	10.1.1.43	RSTP(802.1W)	32768	20	2	15
Kite_59	10.255.11.59	RSTP(802.1W)	32768	20	2	15
wTarget	10.255.11.60	RSTP(802.1W)	32768	20	2	15
Kite2_NMS	10.255.11.61	RSTP(802.1W)	32768	20	2	15
wTarget	10.255.11.63	RSTP(802.1W)	32768	20	2	15
kite2_97_1	10.255.11.97	RSTP(802.1W)	32768	20	2	15
falconCmm	10.255.11.100	STP(802.1D)	32768	20	2	15
Kite_Fiber_U24	10.255.11.101	STP(802.1D)	32768	20	2	15
NMS_HAWK_102_1	10.255.11.102	STP(802.1D)	32768	20	2	15
wTarget	10.255.11.104	STP(802.1D)	32768	20	2	15
wTarget	10.255.11.109	RSTP(802.1W)	32768	20	2	15
wTarget	10.255.11.111	STP(802.1D)	32768	20	2	15
Kite	10.255.11.112	RSTP(802.1W)	32768	20	2	15
no-name	10.255.11.121	RSTP(802.1W)	32768	20	2	15
VW_HAWK_122-Test	10.255.11.122	STP(802.1D)	32768	20	2	15
NMS_123_Hawk_1	10.255.11.123	STP(802.1D)	32768	20	2	15
VW_FUJ1_126x	10.255.11.126	RSTP(802.1W)	32768	8	5	15
BS0001s-to	10.255.11.127	STP(802.1D)	32768	20	2	15
VW_FUJ2_129	10.255.11.129	RSTP(802.1W)	32768	8	5	15
ES0001A-1	10.255.11.130	STP(802.1D)	32768	20	2	15

Note that when you click on the Spanning Tree icon for a VLAN that contains XOS devices, the following prompt displays asking if you want to obtain XOS Spanning Tree information from these devices.



Configuring VLAN Router Interfaces

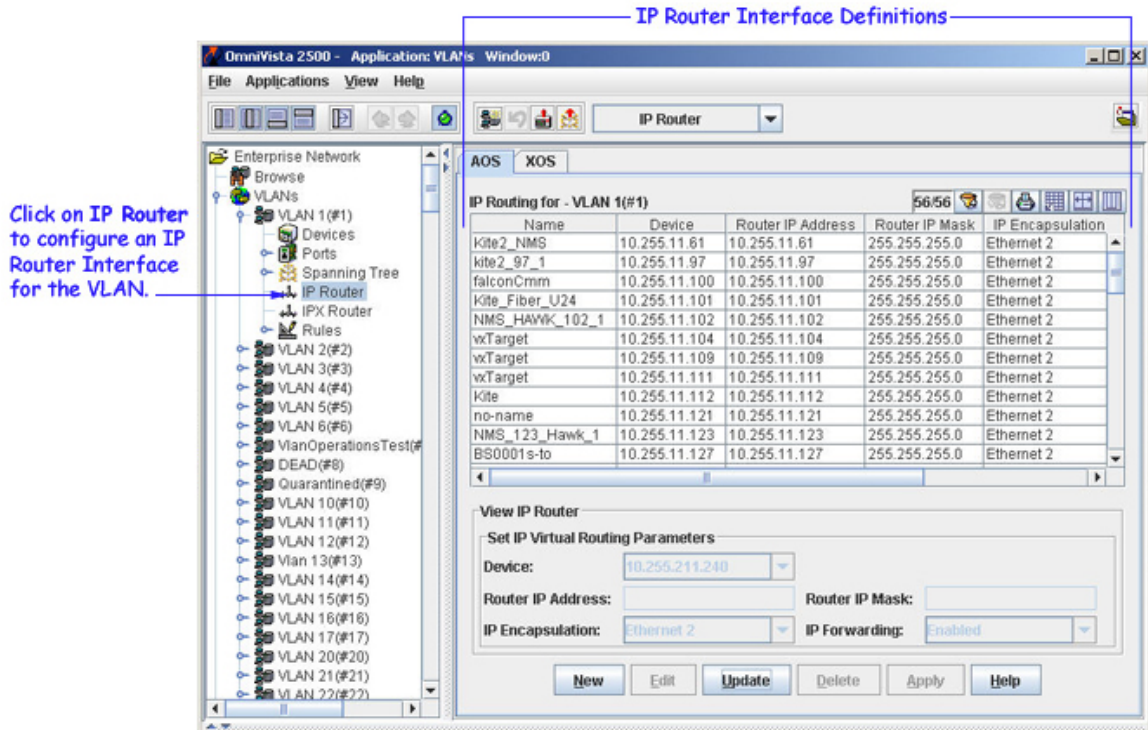
Network device traffic is bridged (switched) at the Layer 2 level between ports that are assigned to the same VLAN. However, if a device needs to communicate with another device that belongs to a different VLAN, then Layer 3 routing is necessary to transmit traffic between the VLANs. Bridging makes the decision on where to forward packets based on the packet's destination MAC address; routing makes the decision on where to forward packets based on the packet's IP or IPX network address (e.g., IP - 21.0.0.10, IPX - 210A).

Alcatel switches support routing of IP and IPX traffic on a per VLAN basis. A VLAN is available for routing when a router interface is defined for that VLAN and at least one active port has joined the VLAN. If a VLAN does not have a router interface configured, its ports are in essence firewalled from other VLANs.

To access a list of AOS or XOS devices that have router interfaces defined for a VLAN, click on the **IP Router** icon underneath the desired VLAN in the Tree, as shown below. If the selected VLAN contains both AOS and XOS devices, then both an AOS and XOS IP Routing Tab is available for selection.

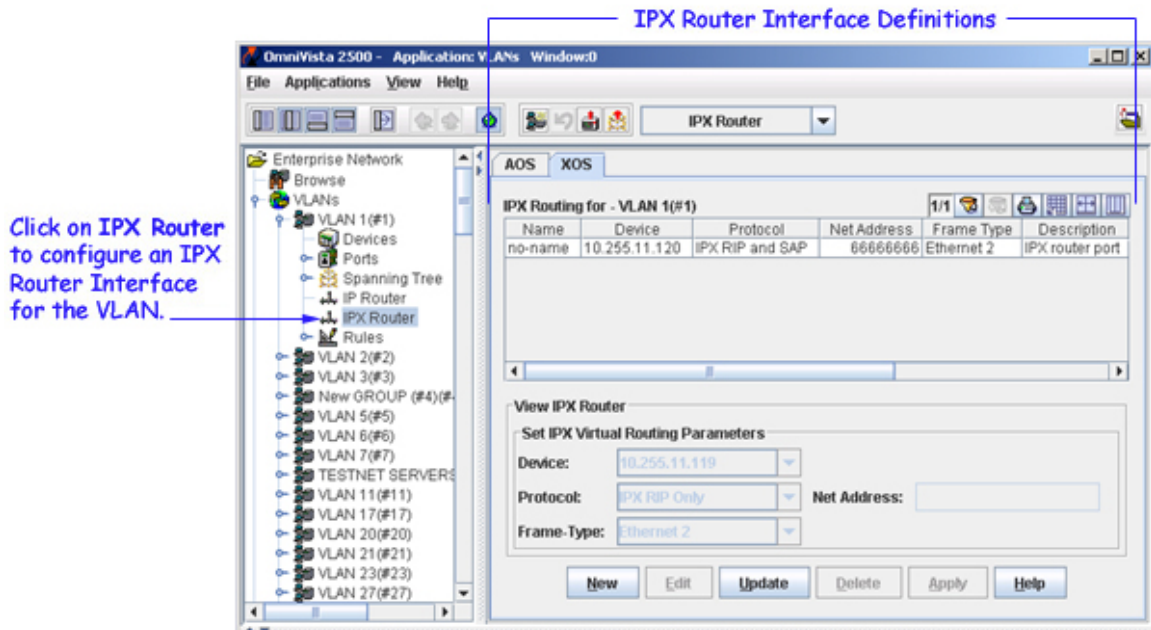
Note: On 7000/8000 (Release 5.1.6) and 9000 (Release 6.1.1) series switches, you can configure up to eight (8) IP router interfaces and one (1) IPX router interface per switch per VLAN.

Click [here](#) for information about using the AOS IP Routing Tab to manage and configure a VLAN router interface for an AOS device. Click [here](#) for information about using the XOS IP Routing Tab to manage and configure a VLAN router interface for an XOS device.



To access a list of AOS or XOS devices that have IPX router interfaces defined for a VLAN, click on the **IPX Router** icon underneath the desired VLAN in the Tree, as shown below. If the selected VLAN contains both AOS and XOS devices, then both an AOS and XOS IPX Routing Tab is available for selection.

Click here for information about using the AOS IPX Routing Tab to manage and configure a VLAN router interface for an AOS device. Click here for information about using the XOS IPX Routing Tab to manage and configure a VLAN router interface for an XOS device.



Defining VLAN Rules

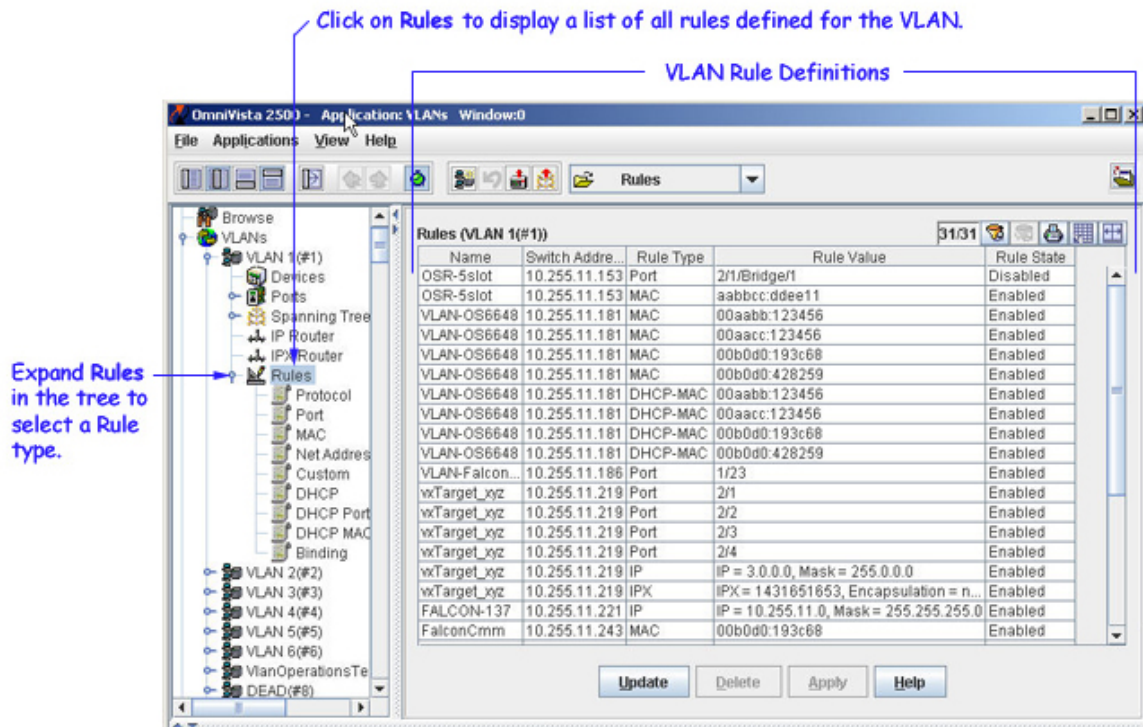
VLAN rules are used to classify mobile port traffic for dynamic VLAN port assignment. Rules are defined by specifying a port, MAC address, protocol, network address, custom (user-defined), DHCP generic, DHCP port, DHCP MAC address, or binding rule criteria to capture certain types of network device traffic. It is possible to define multiple rules for the same VLAN. A mobile port is assigned to a VLAN if its traffic matches any one of the rules defined for that VLAN.

In addition, there is a rule precedence that is followed if traffic received on a mobile port matches multiple rules defined on different VLANs. For example, if VLAN 10 has a MAC address rule and VLAN 20 has an IP address rule and a frame received on a mobile port contains a source MAC address and source IP address that matches both rules, the port is dynamically assigned to VLAN 10 because MAC address rules have a higher precedence over IP network address rules. [Click here for more information about rule precedence.](#)

On XOS platforms, ports become mobile when they are statically assigned to a VLAN that has mobility enabled. Rules to capture mobile port traffic are only defined on mobile VLANs. In addition to enabling mobility on the VLAN and defining VLAN rules, you must also enable the Group Mobility feature for the entire switch. [Click here for more information about configuring mobility on XOS devices.](#)

On AOS platforms, mobility is enabled on individual switch ports. VLANs do not have a mobile or non-mobile distinction and there is no overall switch setting to invoke the mobile port feature. As a result, you can define rules to capture mobile port traffic on any VLAN. [Click here for more information about configuring mobility on AOS devices.](#)

To access a list of all rules defined for a specific VLAN, click on the **Rules** icon underneath the desired VLAN in the Tree. This opens the VLAN Rules window, shown below, which contains a list of all devices that have rules defined for this VLAN in their configuration file. The VLAN Rules window list includes the type of rule defined, the value for that rule, and if the rule is administratively enabled or disabled (applies only to XOS devices). [Click here for more information about the fields in the VLAN Rules window.](#)



To view, create, and/or delete an individual rule definition for a VLAN, click open the **Rules** icon underneath the desired VLAN and then click one of the rule type icons. This opens a VLAN Rules window, similar to the one shown above, that only displays any existing rule definitions for the selected rule type.

Using Port Mobility

Port mobility (also referred to as Group Mobility) allows dynamic VLAN port assignment based on VLAN rules that are applied to port traffic. By default, all switch ports are non-mobile ports that are manually assigned to a specific VLAN and can only belong to one VLAN at a time. When a port is defined as a mobile port, switch software compares traffic coming in on the port with configured VLAN rules. If any of the mobile port traffic matches any of the VLAN rules, the port and the matching traffic become a member of that VLAN. It is also possible for mobile ports to belong to more than one VLAN, when the port carries multiple traffic types that match different rules on different VLANs.

On AOS platforms, VLANs do not have a mobile or non-mobile distinction and there is no overall switch setting to invoke the mobile port feature. Instead, mobility is enabled on individual switch ports and rules are defined for individual VLANs to capture mobile port traffic. Click here for information about configuring mobility on AOS devices.

On XOS platforms, ports become mobile when they are statically assigned to a VLAN that has mobility enabled. Rules to capture mobile port traffic are only defined on mobile VLANs. In addition to enabling mobility on the VLAN and defining VLAN rules, you must also enable the Group Mobility feature for the entire switch. Click here for information about configuring mobility on XOS devices.

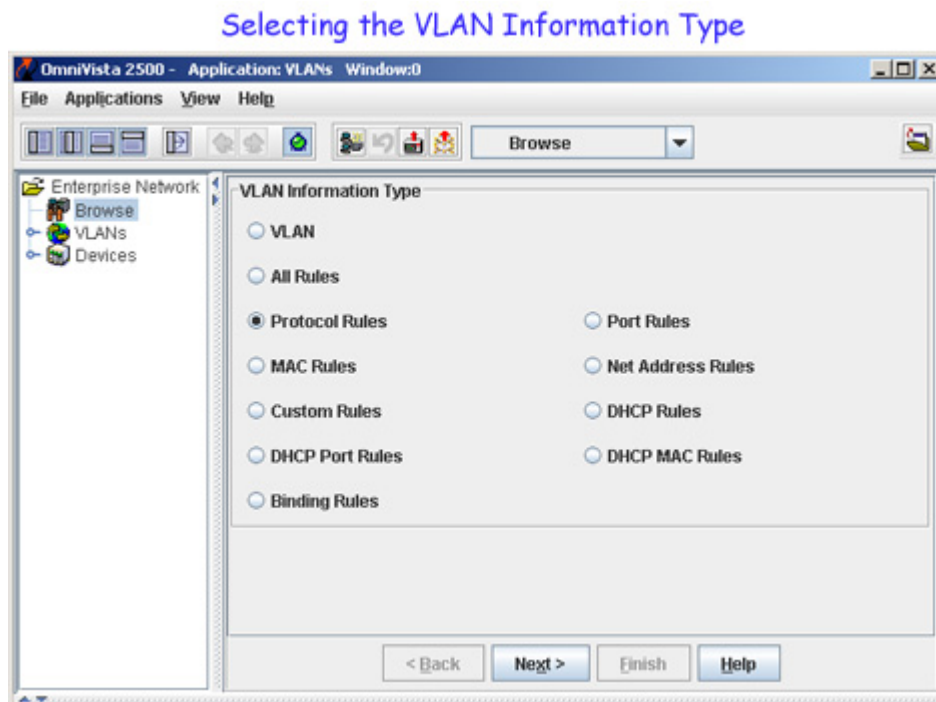
Using the Browse Option

The Browse option of the tree enables you to locate and sort switches by the VLAN rules configured on the switch. When you click the **Browse** node, the VLAN Information Browser wizard is displayed. The first screen of the wizard (shown below) enables you to select the rule type you want to sort on. The second screen enables you to select devices that you want to search. The final screen displays the search results. The results can then be sorted or filtered to further refine your search.

Note: A minimal of read-level permission is required to use this feature.

Selecting the VLAN Information Type

The **VLAN Information Type** panel is the first screen of the VLAN Information Browser wizard. It contains a list of VLAN Rule types to sort on, as well as an option to view all VLANs and/or all rules configured on each switch in the VLAN. Select the information that you want to sort on (e.g., Protocol Rules) and click the **Next** button. You can only sort on one type at a time.



The different VLAN information types are defined below.

VLAN

The "VLAN" information type provides VLAN and switch configuration information for all of the devices you searched on.

All Rules

The "All Rules" information type provides VLAN Rule information for all of the switches you searched on.

Protocol Rules

The "Protocol Rules" information type provides Protocol Rule information for all of the switches you searched on. Only those switches on which a Protocol Rule has been configured will appear in the final Protocol Rule list. Protocol rules determine VLAN assignment based on the protocol a device uses to communicate.

Port Rules

The "Port Rules" information type provides Port Rule information for all of the switches you searched on. Only those switches on which a Port Rule has been configured will appear in the final Port Rule list. Port rules are fundamentally different from all the other supported rule types, in that traffic is not required to trigger dynamic assignment of the mobile port to a VLAN.

MAC Rules

The "MAC Rules" information type provides MAC Rule information for all of the switches you searched on. Only those switches on which a MAC Rule has been configured will appear in the final MAC Rule list. MAC address rules capture frames that contain a source MAC address that matches the MAC address specified in the rule.

Net Address Rules

The "Net Address Rules" information type provides Net Address Rule information for all of the switches you searched on. Only those switches on which a Net Address Rule has been configured will appear in the final Net Address Rule list.

There are two types of network address rules - IP and IPX. An IP network address rule determines VLAN mobile port assignment based on a device's source IP address. An IPX network address rule determines VLAN mobile port assignment based on a device's IPX network and encapsulation.

Custom Rules

The "Custom Rules" information type provides Custom Rule information for all of the switches you searched on. Only those switches on which a Custom Rule has been configured will appear in the final Custom Rule list. Custom rules determine VLAN assignment based on criteria defined by the user.

DHCP Rules

The "DHCP Rules" information type provides DHCP Rule information for all of the switches you searched on. Only those switches on which a DHCP Rule has been configured will appear in the final DHCP Rule list. DHCP rules capture all of the mobile port DHCP frames that do not match any other DHCP rules already defined for other VLANs.

DHCP Port Rules

The "DHCP Port Rules" information type provides DHCP Port Rule information for all of the switches you searched on. Only those switches on which a DHCP Port Rule has been configured will appear in the final DHCP Port Rule list. DHCP port rules capture DHCP frames that are received on a mobile port that matches the port specified in the rule.

DHCP MAC Rules

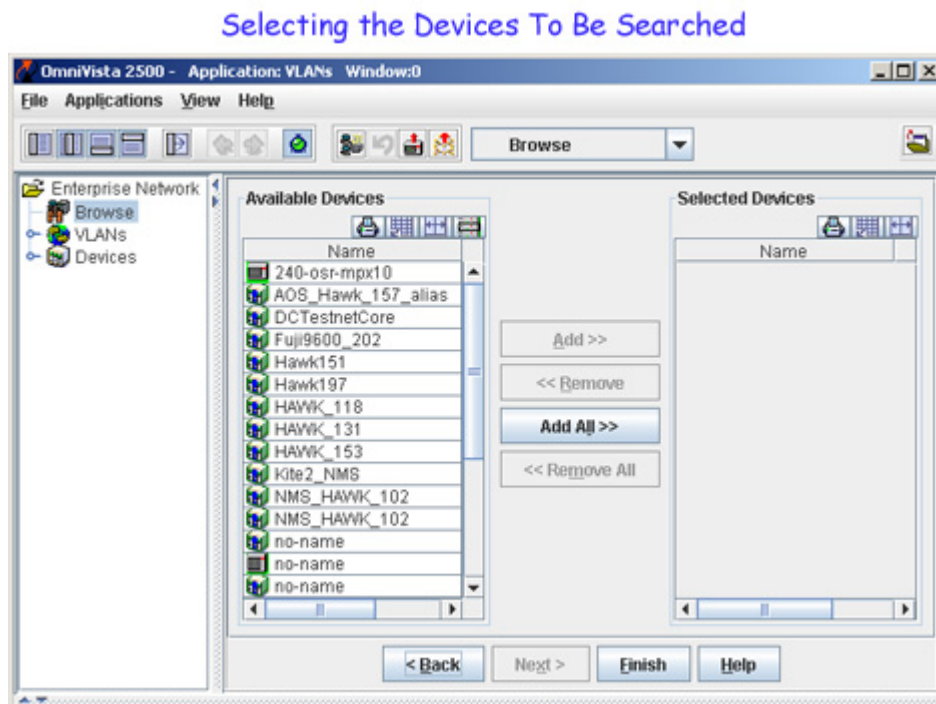
The "DHCP MAC Rules" information type provides DHCP MAC Rule information for all of the switches you searched on. Only those switches on which a DHCP MAC Rule has been configured will appear in the final DHCP MAC Rule list. DHCP MAC rules capture mobile port DHCP frames that contain a source MAC address that matches the MAC address specified in the rule.

Binding Rules

The "Binding Rules" information type provides Binding Rule information for all of the switches you searched on. Only those switches on which a Binding Rule has been configured will appear in the final Binding Rule list. Binding rules restrict VLAN assignment to specific devices by demanding that device traffic match all criteria specified in the rule.

Selecting the Devices to be Assigned

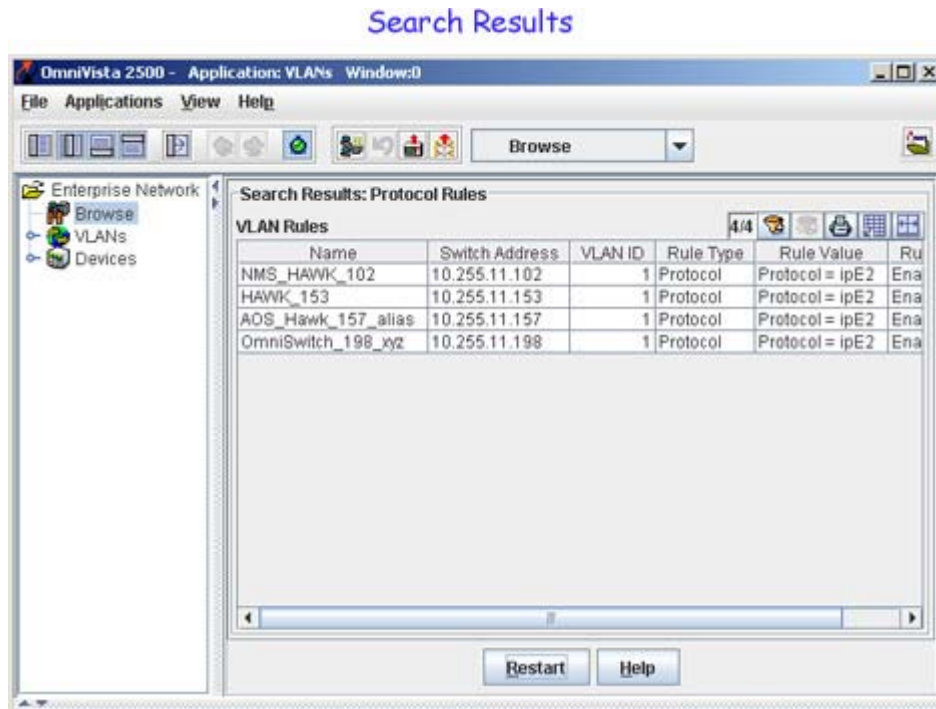
The second screen allows you to select the devices you want to include in your search. To select a device(s), select the device(s) from the **Available Devices** column and move the device(s) to the **Selected Devices** column. You can select multiple contiguous devices by **Shift**-clicking, or multiple non-contiguous devices by **Ctrl**-clicking.



Click the **Finish** button when you have selected the devices.

Viewing the Search Results

The final screen displays the search results in a tabular form. The list contains all of the devices on which the selected rule is configured. For example, the results below display all switches on which a Protocol Rule is configured.



When you right-click on a displayed row, the **Find in Tree** popup is displayed. When you click the **Find in Tree** option, OmniVista will select and display the corresponding VLAN under the **VLANs** node.

Note: The **Search Results** table supports the standard tool buttons, such as **Select Filter**, **Cancel Filter**, **Print Table**, and **Export Table**, as well as sorting columns in ascending/descending order.

Configuring VLANs

The VLANs window, shown below, displays when **VLANs** is selected in the tree. This window contains a list of all VLANs configured across one or more switches in your network topology. In addition to the VLAN ID, each list entry contains fields that display the current values for related VLAN parameters.

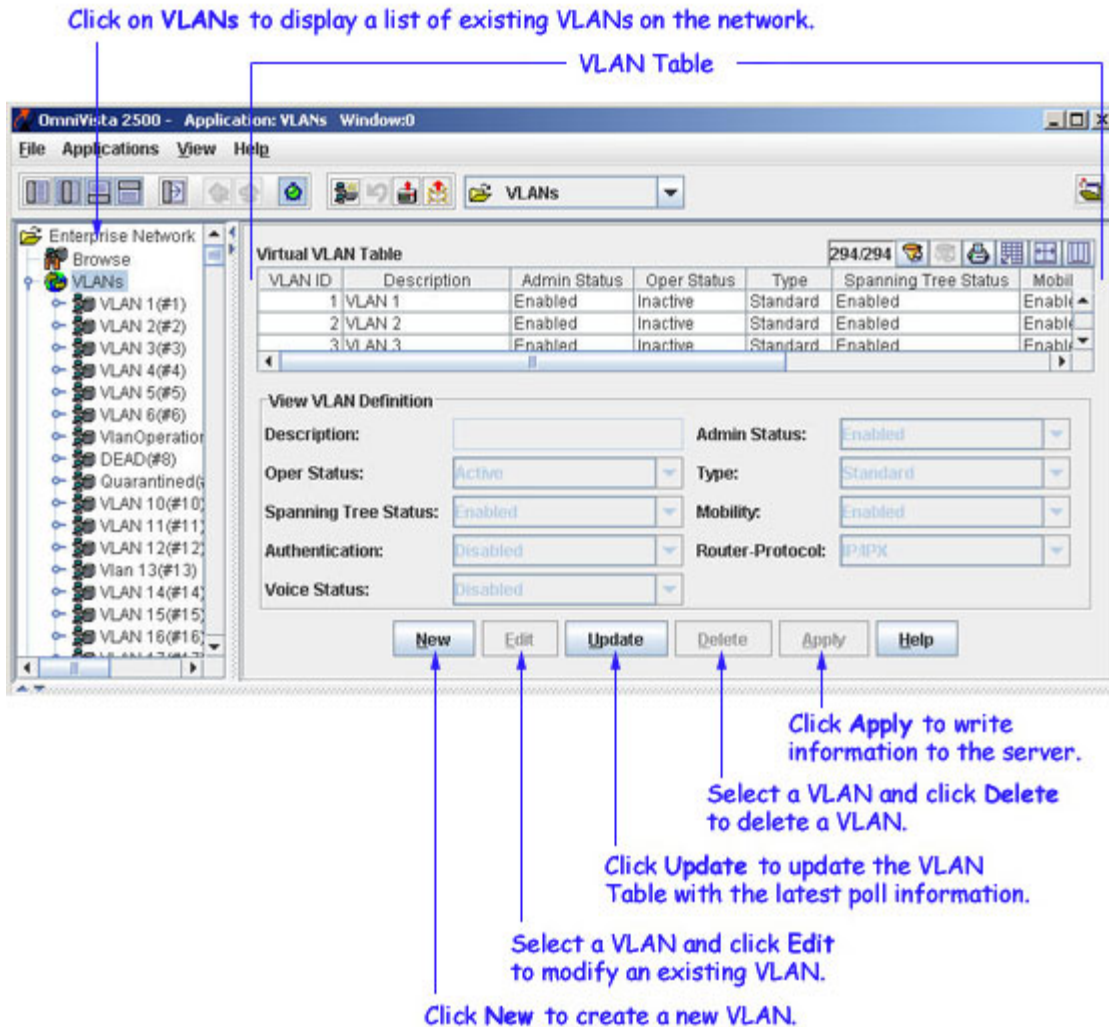
The VLAN parameter value displayed in each field, except for the VLAN ID field, is the value obtained from the switch polled that has the lowest IP host address. For example, if VLAN 9 exists on three different switches with IP addresses of 10.0.0.1, 10.0.0.2, and 10.0.0.3 and each instance of the VLAN has a different description, the VLAN 9 description from switch 10.0.0.1 is displayed in this window.

Note: On the XOS switch platform the term "Group" refers to a VLAN.

The VLANs tree lists all known VLANs in ascending numerical order and includes the corresponding description for each VLAN. Following the description text, the VLAN ID appears in parenthesis next to a number sign (#10). If a description was not specified at the time a VLAN was created, the VLAN ID is used by default. You can click on an individual VLAN in the Tree to view a list of devices that contain the selected VLAN in the switch configuration.

In addition to displaying VLAN configurations, the VLANs window also enables you to add, modify, or remove VLANs. These tasks and VLAN parameters are described below.

When you modify VLAN parameters using this window, however, the changes are applied across all switches in the topology that have this VLAN configured. For example, if you selected VLAN 18 and changed the description to "Marketing Department", all switches that contain VLAN 18 would receive this new description value.



Note: Throughout the VLAN application, prior to applying a configuration, you can use the **Update** button to return all fields to their original values.

Adding a VLAN

Alcatel switches support up to 4094 VLANs on one switch (1024 VLANs on XOS switches, 256 VLANs on OmniStack switches), including default VLAN 1. To add a new VLAN to the configuration of one or more switches, click the **New** button. The VLAN Wizard activates and takes you step by step through the process of creating a new VLAN.

The initial configuration for all Alcatel switches consists of a default VLAN 1 and all switch ports are initially assigned to this VLAN. When a switching module is added to the switch, the module's physical ports are also assigned to VLAN 1. If additional VLANs are not configured on the switch, then the entire switch is treated as one large broadcast domain. All ports will receive all traffic from all other ports.

Copying a VLAN

You can copy the definition of an existing VLAN and add additional switches to this VLAN. To add an additional switch(es) to the same VLAN, right-click the desired VLAN in the VLAN pane, and then select the **Copy VLAN** option from the popup menu. This will launch the **VLAN Wizard**. In the **VLAN Wizard** window, for selecting devices. When you select new switch(es) in the devices panel, all the existing definitions of the copied VLAN will be reused for the selected switch(es).

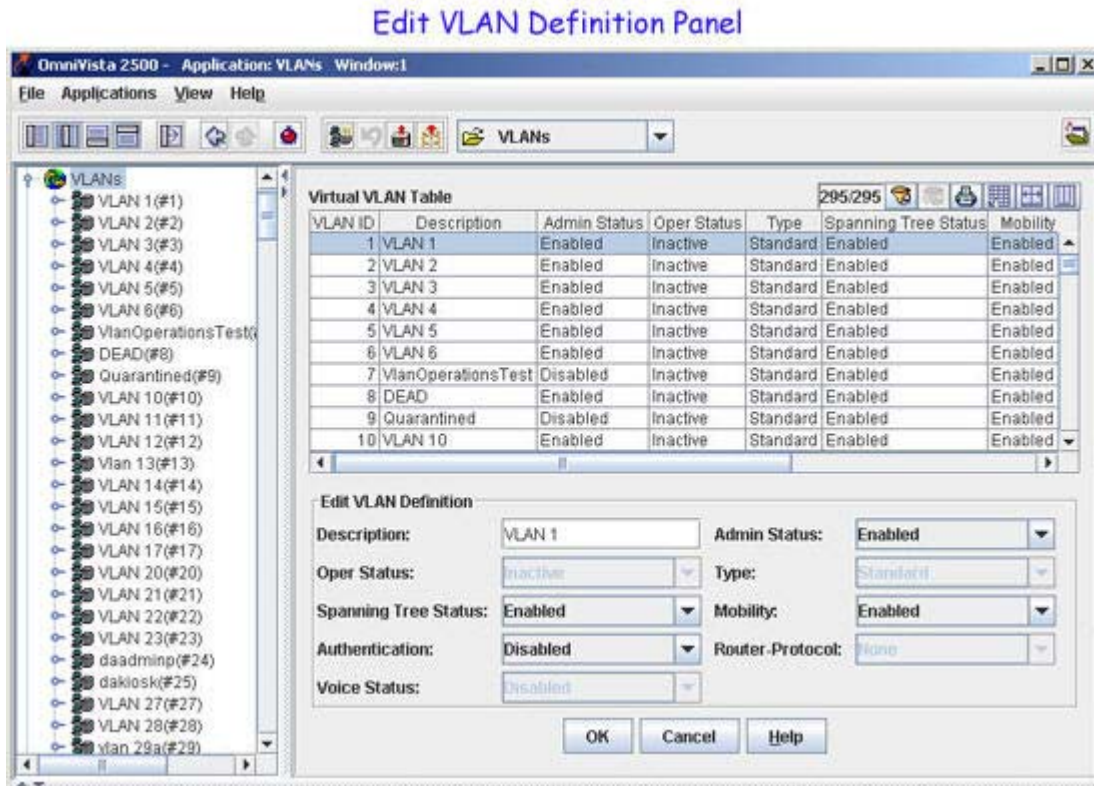
Note: The following definitions will not be copied:

1. IP/IPX routing parameters.
2. VLAN features that are not supported on the target devices. For example, in OS 6800, the Mobility rules like Custom Rules, IP-MAC Binding Rules, IP-Port Binding Rules, and MAC-Port-Protocol are not supported.
3. The VLAN definitions involving slots/ports that do not exist in the target devices.

Modifying a VLAN

By default, the administrative status and Spanning Tree status are enabled and authentication and mobility are disabled when a VLAN is created. In addition, the VLAN ID is used for the description if one is not specified. It is only necessary, therefore, to modify these parameters if you want to change the default values. See VLAN Parameter Definitions below for more information. Follow the steps below to modify VLAN parameter values.

1. Select a single VLAN entry from the list in the VLANs window, shown above, and click the **Edit** button. This activates the Edit VLAN Definition panel, as shown below. Note that parameters that are not modifiable or are not supported in this release are grayed out on the panel.



2. Make the desired changes and click the **OK** button to accept the changes or the **Cancel** button to clear the changes. The Edit VLAN Definition window will close, returning you to the window where you selected the VLAN to modify.

3. If you clicked the **OK** button in the Edit VLAN Definition window, a modify icon now appears next to the VLAN ID. To save the changes to the appropriate switch configurations, click the **Apply** button in the current window.

Note that when you use the VLANs window to modify VLAN parameters, your changes are applied across all switches. For example, if you change the Spanning Tree status for VLAN 10 and VLAN 10 exists on three switches, the status is changed for VLAN 10 on all three switches.

Removing a VLAN

To delete an existing VLAN from the switch configuration, select a single VLAN from the VLANs window list and click the **Delete** button. A delete icon appears in the VLAN ID field for this VLAN. The VLAN is not removed from the appropriate switch configurations until you click the **Apply** button.

If you encounter problems when attempting to delete a Group from an XOS switch configuration, try removing any AutoTracker VLANs and/or switch ports assigned to the Group before attempting to delete the VLAN again. Note that OmniVista VLANs does not support AutoTracker VLANs at this time, so you must telnet (or use other available means of access) directly to the switch to configure AutoTracker VLANs.

When you delete a VLAN it is deleted from all switch configurations that contain that VLAN. For example, if you delete VLAN 15 and VLAN 15 exists on five switches, VLAN 15 is deleted from the configuration on all five of these switches.

VLAN Parameter Definitions

Note: The term "OmniStack" refers only to OmniStack models 6024, 6048, 6124, 6148, 6300-24, and 8088. The term "XOS" includes all other OmniStack devices that run XOS software.

VLAN ID

In compliance with the IEEE 802.1Q standard, each VLAN is identified by a unique number, referred to as the VLAN ID. This number is assigned by the user at the time the VLAN is created and is not a modifiable parameter. When a network device packet is received on a port, the port's VLAN ID is inserted into the packet. The packet is then bridged to other ports that are assigned to the same VLAN ID. In essence, the VLAN broadcast domain is defined by a collection of ports and packets assigned to its VLAN ID.

Valid VLAN ID ranges for the supported devices are as follows:

AOS (range = 1-4094)
 XOS (range = 1-5000)
 OmniStack (range = 1-2048)

Note that these VLAN ID values do not indicate the number of VLANs supported on XOS and OmniStack devices. For example, XOS devices support up to 1024 VLANs, but a VLAN ID number between 1 and 5000 is allowed. OmniStack devices support up to 256 VLANs, but a VLAN ID number between 1 and 2048 is allowed. However, on AOS devices, there is a one-to-one correlation between the number of VLANs supported (4094) and the valid VLAN ID range (1-4094).

Description

A text string up to 32 characters (30 characters for XOS and OmniStack VLANs). This parameter defaults to the VLAN ID number (e.g., VLAN #10) if a description was not specified at the time the VLAN was created.

Admin Status

The administrative status (Enabled/Disabled) for the VLAN. By default, the administrative status is enabled when a VLAN is created.

When a VLAN is administratively disabled, static port and dynamic mobile port assignments are retained but traffic on these ports is not forwarded. However, VLAN rules remain active and continue to classify mobile port traffic for VLAN membership.

Oper Status

The VLAN operational status (Active/Inactive). This parameter is not modifiable; switch software determines if the VLAN is operationally active or inactive and sets the appropriate field value.

A VLAN's operational status remains inactive until at least one active switch port is assigned to the VLAN and the VLAN's administrative status is enabled. This means that VLAN properties, such as Spanning Tree or router ports, also remain inactive. Ports are considered active if they are connected to an active network device. Non-active port assignments are allowed, but do not change the VLAN's operational state.

Type

The type of VLAN is determined at the time the VLAN is created. This field may contain one of the following values:

Standard

ATM CIP (supports Classical IP routing over ATM)*

Frame Relay Router (WAN routing VLAN that contains only WAN ports)*

MPLS RT (supports Multi-Protocol Label Switching routing over ATM)*

MPLS BR (supports Multi-Protocol Label Switching bridging over ATM)*

PTOP Routed (supports RFC 1483 routing over ATM)*

*Feature not supported on all switch platforms.

Parameter not supported on all OmniStack models.

Spanning Tree Status

The Spanning Tree Status (Enabled/Disabled) for the VLAN. When a VLAN is created, an 802.1D standard Spanning Tree Algorithm and Protocol (STP) instance is enabled for the VLAN by default.

STP evaluates VLAN port connections to determine if there are redundant data paths between the same VLAN on other switches. If a redundant path does exist, STP determines which path to block in order to provide a loop-free network topology. In this manner, STP ensures that there is always only one active data path between any two switches (VLANs). When a change occurs, such as a path is disconnected or a path cost change, the Spanning Tree Algorithm activates the blocked path to restore the network connection.

Parameter not supported on all OmniStack models.

Mobility

The mobile status (Enabled/Disabled) for the VLAN. On AOS switches, mobility is not enabled or disabled at the VLAN level. Instead, switch ports are designated as mobile or non-mobile. This parameter, however, displays "Enabled" for all AOS VLANs.

Parameter not supported on all OmniStack models.

Authentication

The authentication status (Enabled/Disabled) for the VLAN. By default, authentication is disabled when a VLAN is created. Once authentication is enabled on a VLAN, however, then only authenticated mobile port devices can join the VLAN after completing the appropriate log-in process.

Layer 2 authentication uses VLAN membership to grant access to network resources. Authenticated VLANs control membership through a log-in process; this is sometimes called user authentication. A VLAN must have authentication enabled before it can participate in the Layer 2 authentication process.

Parameter not supported on all OmniStack models.

Router Protocol

The protocol for the VLAN virtual router port (IP or IPX). If no router port is configured for the VLAN, then "none" appears in this field.

Alcatel switches support routing of IP and IPX traffic on a per VLAN basis. A VLAN is available for routing when a virtual router port is defined for that VLAN and at least one active port has joined the VLAN. If a VLAN does not have a router port, its ports are in essence firewalled from other VLANs.

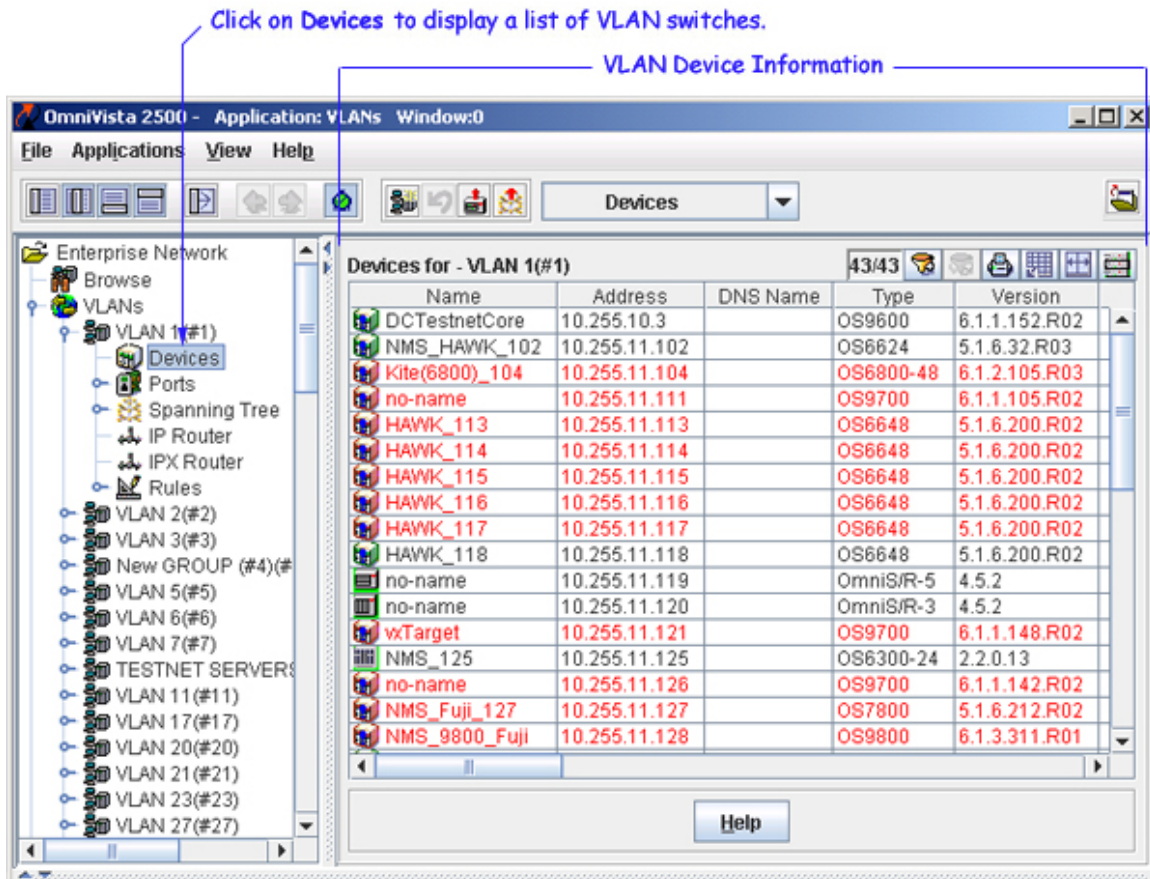
Parameter not supported on all OmniStack models.

Voice Status

Not supported for this release.

VLAN Device Information

The Device Information window displays when you click on **Devices** in the VLANs Tree, as shown below. This window contains a list of all switches in your topology that are configured with the current VLAN. Each device entry contains fields that display related system parameter values.



Device Parameter Definitions

The information contained in the following parameter fields is for reference only and is not modifiable from the VLAN Device Information window. Use the OmniVista Topology application to configure system parameters.

Name

The user-defined name for the device.

Address

The IP host address that identifies the device within the management IP network. It is not the same IP host address defined as a virtual IP router port for the selected VLAN, unless the VLAN is part of the management network. In addition, an IP host address appears in this field even if an IP virtual router port does not exist for the VLAN on that particular switch.

Type

The device chassis type.

Version

The version number of the device firmware.

Backup Date

The date the configuration and/or images files for the device were last backed up to the OmniVista server.

Backup Version

The version number of the configuration and/or images files that were last backed up.

History

The date and time the Locator database was last polled.

Description

A description of the device, usually the vendor name and model.

Status

This field displays the operational status of the device. **Up** displays if the device is up and responding to polls. (When a device is up, it displays green in both the Devices Physical Network list and the Tree.) **Down** displays if the device is down and not responding to polls. (When a device is down, it displays red in both the Devices Physical Network list and the Tree.) **Warning** displays if the switch has sent at least one warning or critical trap and is thus in the warning state. (When a device is in the warning state, it displays orange in both the Devices Physical Network list and the Tree.)

Traps

This field indicates the status of trap configuration for the device. **On** displays if traps are enabled. **Off** displays if traps are disabled. **Not Configurable** displays if traps from this device are not configurable from OmniVista (traps were configured using some other method or device is not an XOS or AOS device). **Unknown** displays if OmniVista does not know the status of trap configuration on this device.

Seen By

This field lists the Security Groups that are allowed to view the device. The default Security Groups shipped with OmniVista are as follows:

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

- **Network Administrators** group. This group has full administrative access rights to all switches on the network. Members of this group can run autodiscovery and can manually add, delete, and modify entries in the All Discovered Devices list. Members of this group also have full read and write access to entries in the Audit application and the Control Panel application. Members of this group can do everything EXCEPT make changes to the Security Groups.
- **Administrators** group. This group has all administrative access rights granted to the Network Administrators group AND full administrative rights to make changes to the Security Groups.

Note that other Security Group names may display in this field if custom Security Groups were created. Refer to help for the Security application *Users and Groups* for further information on Security Groups.

Running From

For AOS devices, this field indicates whether the switch is running from the **certified** directory or from the **working** directory. This field is blank for all other devices. For AOS devices, the directory structure that stores the switch's image and configuration files in flash memory is divided into two parts:

- The certified directory contains files that have been certified by an authorized user as the default configuration files for the switch. When the switch reboots, it will automatically load its configuration files from the certified directory if the switch detects a difference between the certified directory and the working directory. (Note that you can specifically command a switch to load from either directory.)
- The working directory contains files that may -- or may not -- have been altered from those in the certified directory. The working directory is a holding place for new files to be tested before committing the files to the certified directory. You can save configuration changes to the working directory. You cannot save configuration changes directly to the certified directory.

Note that the files in the certified directory and in the working directory may be different from the running configuration of the switch, which is contained in RAM memory. The running configuration is the current operating parameters of the switch, which are originally loaded from the certified or working directory but may have been modified through CLI commands, WebView commands, or OmniVista. Modifications made to the running configuration must be saved to the working directory (or lost). The working directory can then be copied to the certified directory if and when desired.

Changes

For AOS devices, this field indicates the state of changes made to the switch's configuration. This field is blank for all other devices. This field can display the following values:

- **Unsaved.** Changes have been made to the running configuration of the switch that have not been saved to the working directory.
- **Uncertified.** Changes have been saved to the working directory, but the working directory hasn't been copied to the certified directory. The working directory and the certified directory are thus different.
- **Blank.** When this field is blank for an AOS device, the implication is that OmniVista knows of no unsaved configuration changes and thinks that the working and certified directories in flash memory are identical. However, note that configuration changes can be made outside of OmniVista, through CLI commands or WebView, and OmniVista will not be aware of these changes.

Note that it is possible that a switch could be in a state where it is both Unsaved and Uncertified. In this situation, **Unsaved** displays in this field. Whenever an AOS device is in the Unsaved or Uncertified state, a blue exclamation mark displays on its icon.

Assigning Ports to VLANs

Initially all switch ports are assigned to VLAN 1, which is also their *configured default* VLAN. When additional VLANs are created on the switch, ports are assigned to the VLANs so that traffic from devices connected to these ports is bridged within the VLAN domain.

Switch ports are either statically or dynamically assigned to VLANs. Methods for accessing and configuring static port assignments include the following:

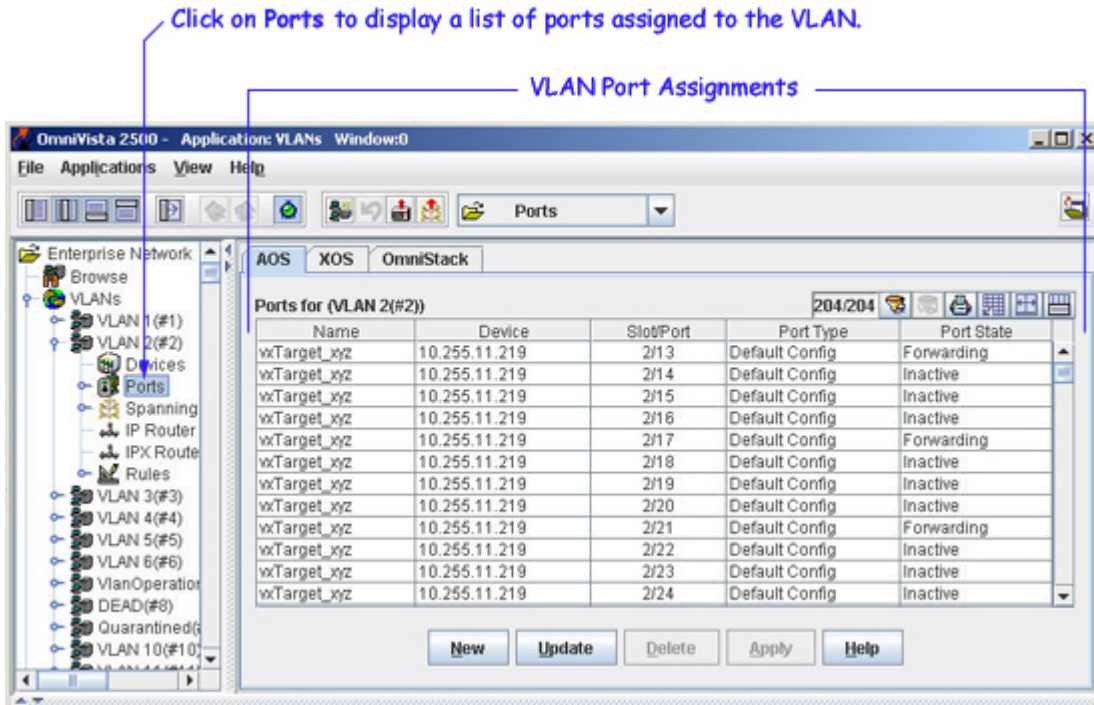
- Configuring a new default VLAN for both fixed and mobile ports.
- Using 802.1Q tagging to configure multiple VLANs on one physical port connection.
- Configuring a new default VLAN for a link aggregate of ports.

Dynamic assignment only applies to mobile ports and requires the additional configuration of VLAN rules. When traffic is received on a mobile port, the packets are examined to determine if their content matches any VLAN rules configured on the switch. If a match occurs, the mobile port is automatically assigned to the VLAN without user intervention. [Click here](#) for information about dynamically assigning ports to VLANs.

Configuring a New Default VLAN for a Port

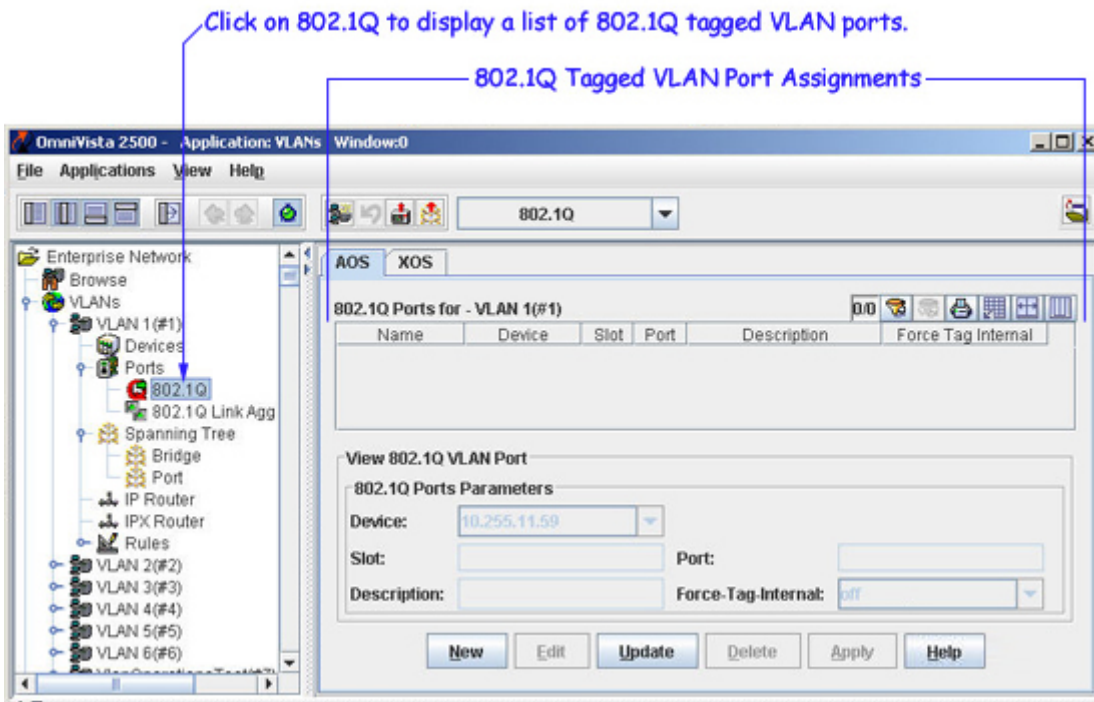
To access a list of ports currently assigned to a VLAN, click on the Ports icon underneath the desired VLAN in the Tree. If the selected VLAN contains AOS, XOS, and OmniStack devices, then AOS, XOS, and OmniStack Tabs are available for selection, as shown below. Each tab contains a list of ports on those devices that are currently assigned to the selected VLAN. Click on the appropriate tab to manage and configure VLAN port assignments.

Note: The term "OmniStack" refers only to OmniStack models 6024, 6048, 6124, 6148, and 8088. The term "XOS" includes all other OmniStack devices that run XOS software.



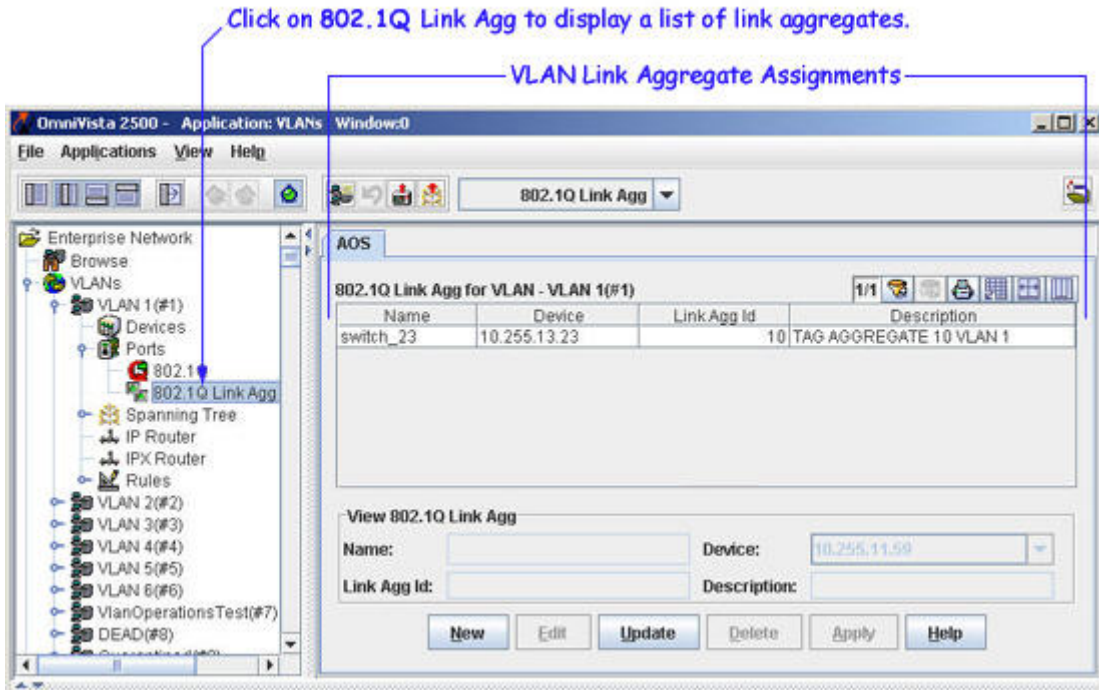
Configuring 802.1Q Tagged VLANs

To access a list of 802.1Q tagged port assignments for a VLAN, click open the Ports icon and click on the 802.1Q icon. If the current VLAN contains both AOS and XOS devices, then both AOS and XOS 802.1Q Ports Tabs are available for selection, as shown below. (Note that an OmniStack tab is not available for this feature at this time.) Click on the appropriate tab to manage and configure 802.1Q VLAN port assignments.



Configuring a New Default VLAN for a Link Aggregate

To access a list of link aggregate assignments for a VLAN, click open the **Ports** icon and click on the **802.1Q Link Agg** icon. An AOS 802.1Q Link Agg Tab displays, as shown below. If the tab list is empty, there are no link aggregates assigned to this VLAN. (Note that XOS and OmniStack tabs are not available for this feature at this time). Use the AOS 802.1Q Link Agg Tab to assign the link aggregate to a new default VLAN.



AOS Ports Tab

The AOS Ports Tab provides a list of all AOS device ports that are assigned to the current VLAN. In addition to the slot and port number, each list entry contains fields that display the current values of related port parameters. The AOS Ports Tab also enables you to add or delete VLAN port assignments. These tasks and port parameter definitions are described below.

AOS VLAN Port Assignments

Name	Device	Slot/Port	Port Type	Port State
Kite_59	10.255.11.59	1/5	Default Config	Inactive
Kite_59	10.255.11.59	1/6	Default Config	Inactive
Kite_59	10.255.11.59	1/7	Default Config	Inactive
Kite_59	10.255.11.59	1/8	Default Config	Inactive
Kite_59	10.255.11.59	1/9	Default Config	Inactive
Kite_59	10.255.11.59	1/10	Default Config	Inactive
Kite_59	10.255.11.59	1/11	Default Config	Inactive
Kite_59	10.255.11.59	1/12	Default Config	Inactive
Kite_59	10.255.11.59	1/13	Default Config	Inactive
Kite_59	10.255.11.59	1/14	Default Config	Inactive
Kite_59	10.255.11.59	1/15	Default Config	Inactive
Kite_59	10.255.11.59	1/16	Default Config	Inactive
Kite_59	10.255.11.59	1/17	Default Config	Inactive
Kite_59	10.255.11.59	1/18	Default Config	Inactive
Kite_59	10.255.11.59	1/19	Default Config	Inactive
Kite_59	10.255.11.59	1/20	Default Config	Inactive
Kite_59	10.255.11.59	1/21	Default Config	Inactive
Kite_59	10.255.11.59	1/22	Default Config	Inactive
Kite_59	10.255.11.59	1/23	Default Config	Inactive

Creating a new VLAN Port Assignment

To assign a port to the current VLAN, click the **New** button found at the bottom of the AOS Ports Tab. This activates the Add Ports pop-up window. Click here for information about how to assign ports to a VLAN using this window.

Removing a VLAN Port Assignment

To remove a VLAN port assignment, select one or more port entries from the AOS Ports Tab list and click the **Delete** button. A delete icon appears in the Name field of the selected entry. Click the **Apply** button to drop the port assignment from the VLAN. When this occurs, the port is returned to the switch default VLAN, which is VLAN 1. *Note that you can not delete a VLAN port assignment from VLAN 1.*

Note: Using the AOS Ports Tab to remove VLAN port assignments is only possible if the VLAN is the configured default VLAN for the port. If the Port Type field contains "Default Config", then the VLAN is the configured default VLAN for the port.

Port Parameter Definitions

Note that the following port parameters are not modifiable. They provide information about the type and status of the VLAN port assignment that is helpful for managing VLAN traffic.

Name

The user-defined name for the switch.

Device

The IP host address that identifies the switch within the management IP network. It is not the same IP host address defined as a virtual IP router port for the selected VLAN, unless the VLAN is part of the management network. In addition, an IP host address appears in this field even if an IP virtual router port does not exist for the VLAN on that particular switch.

Slot/Port

Slot--The slot number of the switch module. Identifies the position of the module in the switch chassis (or the position within a stack of switches, such as with the OmniSwitch 6624/6648 stackable units).

Port--The port number on that module (e.g. 3/1 specifies port 1 on slot 3).

Port Type

The Port Type parameter indicates how the port assignment to the current VLAN was made. This field will contain one of the following values:

Default Config--The port is a fixed port that was statically assigned to the VLAN, which is now the configured default VLAN for the port.

Q Tagged--The port is a fixed port that was statically assigned to the VLAN using the 802.1Q tagging feature. The VLAN is a *static secondary* VLAN assignment for the 802.1Q tagged port.

Mobile--The port is a mobile port that was dynamically assigned to the VLAN when traffic received on the port match traffic rules defined for the VLAN. The VLAN is a *dynamic secondary* VLAN assignment for the mobile port.

Note that only ports with a default config port type are assigned and removed using the AOS Tab. All other port types are managed using the application that created the VLAN port assignment for that type.

Port State

The Port State indicates the status of the VLAN port assignment. This field will contain one of the following values:

Inactive--Port is not active (administratively disabled, down, or nothing is connected to the port).

Blocking--Port is active, but not forwarding any traffic on this VLAN.

Forwarding--Port is active and forwarding traffic on this VLAN.

Filtering--Mobile port traffic is filtered for the VLAN; only traffic received on the port that matches VLAN rules is forwarded. Occurs when a mobile port's VLAN is administratively disabled or the port's default VLAN status is disabled. Does not apply to fixed ports.

XOS Ports Tab

The XOS Ports Tab provides a list of all XOS device ports that are assigned to the current VLAN. In addition to the slot and port number, each list entry contains fields that display the current values of related port parameters. The XOS Ports Tab also enables you to add or delete VLAN port assignments and modify port parameters. These tasks and port parameter definitions are described below.

XOS VLAN Port Assignments

Name	Device	Slot	Port	Function Type	Instance	MAC
no-name-119	10.255.11.119	2	1	Bridge	1	00d0
no-name-119	10.255.11.119	2	2	Bridge	1	00d0
no-name-119	10.255.11.119	2	3	Bridge	1	00d0
no-name-119	10.255.11.119	2	4	Bridge	1	00d0
no-name-119	10.255.11.119	2	5	Bridge	1	00d0
no-name-119	10.255.11.119	2	6	Bridge	1	00d0
no-name-119	10.255.11.119	2	7	Bridge	1	00d0
no-name-119	10.255.11.119	2	8	Bridge	1	00d0
no-name-119	10.255.11.119	2	9	Bridge	1	00d0
no-name-119	10.255.11.119	2	10	Bridge	1	00d0
no-name-119	10.255.11.119	2	11	Bridge	1	00d0
no-name-119	10.255.11.119	2	12	Bridge	1	00d0
no-name-119	10.255.11.119	2	13	Bridge	1	00d0
no-name-119	10.255.11.119	2	14	Bridge	1	00d0
no-name-119	10.255.11.119	2	15	Bridge	1	00d0
no-name-119	10.255.11.119	2	16	Bridge	1	00d0
no-name-119	10.255.11.119	2	17	Bridge	1	00d0
no-name-119	10.255.11.119	2	18	Bridge	1	00d0

Creating a new VLAN Port Assignment

To assign a port to the current VLAN, click the **New** button found at the bottom of the XOS Ports Tab. This activates the Add Ports pop-up window. Click here for more information about how to assign ports to a VLAN using this window.

Removing a VLAN Port Assignment

To remove a VLAN port assignment, select one or more port entries from the XOS Ports Tab list and click the **Delete** button. A delete icon appears in the Name field of the selected entry. Click the **Apply** button to drop the port assignment from the VLAN. When this occurs, the port is returned to the switch default VLAN, which is VLAN 1. Note that you can not delete a VLAN port assignment from VLAN 1.

Note: Using the XOS Ports Tab to remove VLAN port assignments is only possible if the VLAN is the configured default VLAN for the port. If the Function Type field contains "Bridge", then the VLAN is the configured default VLAN for the port.

Modifying Port Parameters

Only the port MAC address and flood limit parameters are modifiable. Additional parameters displayed in the XOS Ports Tab list provide information about the type and status of the VLAN port assignment that is helpful for managing VLAN traffic.

To modify the port MAC address or flood limit, select one or more port entries in the XOS Ports Tab list and click the **Edit** button. This activates the Edit VLAN Ports pop-up window. Note that if you select more than one port to modify, you can only modify the flood limit. Changing the port MAC address is only available on a port by port basis. Click here for information about how to modify XOS port parameters using the Edit VLAN Ports window.

Port Parameter Definitions

Name

The user-defined name for the switch.

Device

The IP host address that identifies the switch within the management IP network. It is not the same IP host address defined as a virtual IP router port for the selected VLAN, unless the VLAN is part of the management network. In addition, an IP host address appears in this field even if an IP virtual router port does not exist for the VLAN on that particular switch.

Slot

The slot number of the switch module. Identifies the position of the module in the switch chassis (or the position within a stack of switches, such as with the OmniSwitch 6624/6648 stackable units).

Port

The physical port number on a module.

Function Type

The Function Type parameter identifies the type of port or type of virtual service port for each VLAN port assignment. Some examples of the port/service types this field may contain are as follows:

Bridge--Virtual bridge port.
VLMP 802.1Q--Virtual 802.1Q tagged port.
Trunk--Virtual trunk port (ATM, FDDI, and WAN service port)
ATM LANE--LANE emulation service port.
CIP--Classical IP service port.

Note that only bridge ports are assigned, removed, or modified using the XOS Tab. All other service port types are managed using the application that created the service port VLAN assignment.

Instance

The Instance is an identifier of this type of service within the switch. Each instance of a service port is given a different number. The number contained in this field is the instance of the virtual service port that was assigned to the VLAN when the service was created.

MAC Address

The MAC address allocated for the port. Each physical and virtual service port instance is allocated a unique MAC address. This is a modifiable parameter.

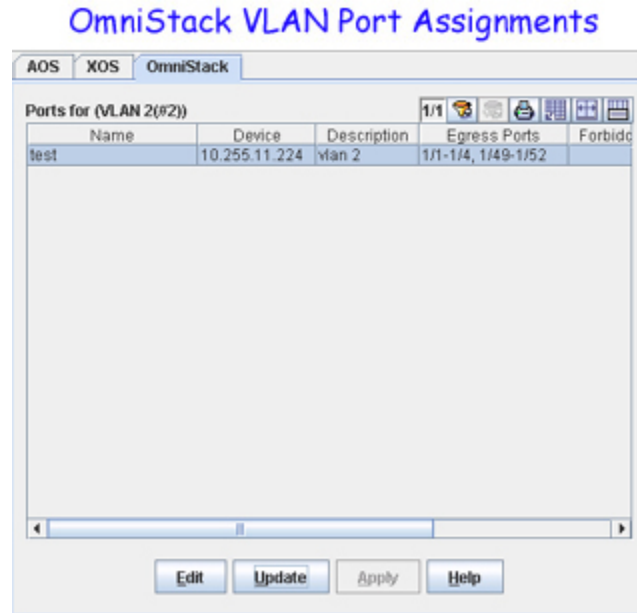
Flood Limit

The flood limit (**0-1000000**) allows you to tune a virtual port to limit the flooding of broadcast, multicast, and unknown destination packets. This feature is useful for controlling broadcast storms on your network. While each network is different, in general the amount of flooded traffic represents a relatively small percentage of network traffic. By default, this parameter is set to **192,000**.

OmniStack Ports Tab

The OmniStack Ports Tab provides a list of OmniStack devices and ports on each device that are assigned to the current VLAN and enables you to add or delete VLAN port assignments. These tasks and port parameter definitions are described below.

Note: The term "OmniStack" refers only to OmniStack models 6024, 6048, 6124, 6148, 6300-24, and 8088. The term "XOS" includes all other OmniStack devices that run XOS software.



Assigning Ports to a VLAN

To assign a port to the current VLAN, select one of the devices in the OmniStack Ports Tab list and click the **Edit** button found at the bottom of the OmniStack Ports Tab. This activates the Assign Ports pop-up window. Click here for information about how to assign ports to a VLAN using this window.

Removing Ports from a VLAN

To remove a VLAN port assignment, select one of the devices in the OmniStack Ports Tab list and click the **Edit** button found at the bottom of the OmniStack Ports Tab. This activates the Assign Ports pop-up window. Click here for information about how to remove ports from a VLAN using this window.

Port Parameter Definitions

Note that the following port parameters are not modifiable. They provide information about the type and status of the VLAN port assignment that is helpful for managing VLAN traffic.

Name

The user-defined name for the switch.

Device

The IP host address that identifies the switch within the management IP network. It is not the same IP host address defined as a virtual IP router port for the selected VLAN, unless the VLAN is part of the management network. In addition, an IP host address appears in this field even if an IP virtual router port does not exist for the VLAN on that particular switch.

Description

A text string up to 32 characters (30 characters for XOS VLANs). This parameter defaults to the VLAN ID number (e.g., VLAN #10) if a description was not specified at the time the VLAN was created.

Egress Ports

Ports that are associated to the VLAN (tagged or untagged) for forwarding VLAN traffic.

Forbidden Egress Ports

Ports that are blocked from automatic assignment to the VLAN by a GVRP operation. Note that GVRP is not supported on all OmniStack platforms.

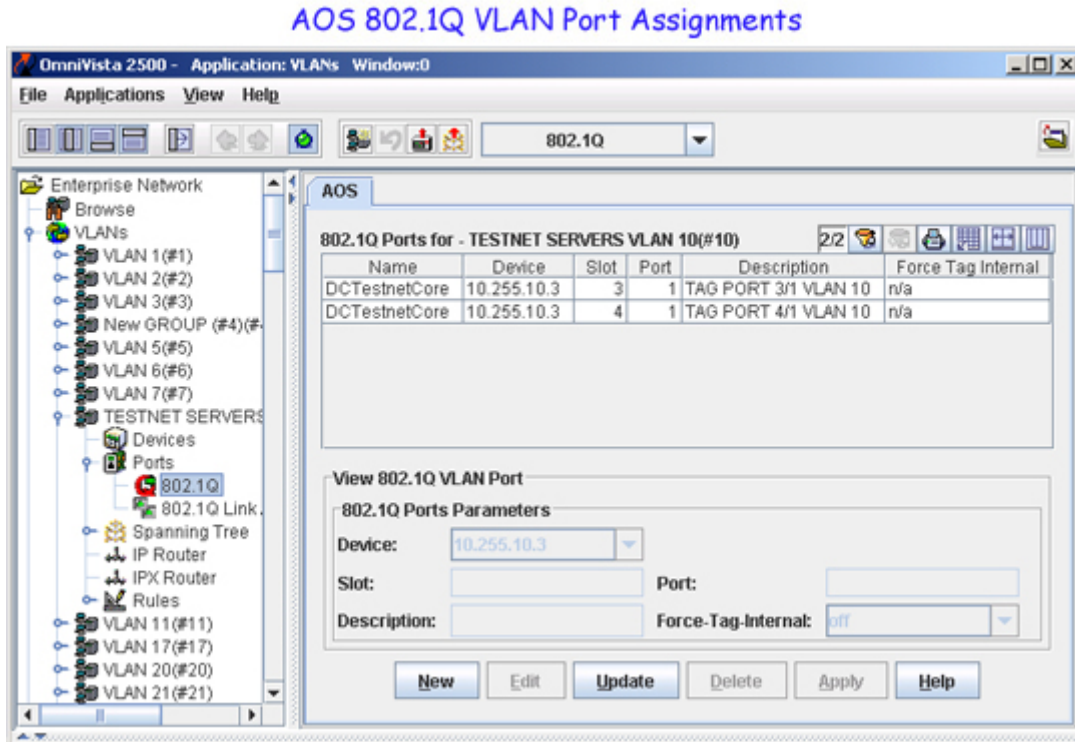
Untagged Ports

Egress ports that are assigned as untagged ports to the VLAN. The VLAN is the default VLAN for these ports. Note that these ports must already have an egress port association with the VLAN. If egress ports do not appear in the untagged ports list, then they have a tagged association with the VLAN.

AOS 802.1Q Ports Tab

The AOS 802.1Q Ports Tab provides a list of all AOS device ports that are tagged to forward traffic on the current VLAN. In addition to the slot and port number, each list entry contains fields that display the current values for related 802.1Q port parameters. This tab also enables you to add or delete 802.1Q tagged port assignments. These tasks and port parameter definitions are described below.

Note: The force tag internal parameter is not available on OmniSwitch 6600, 6800, 6850, or 9000 series switches.



Creating a new 802.1Q Tagged VLAN Port Assignment

To tag a port with the current VLAN, click the **New** button found at the bottom of the AOS 802.1Q Ports Tab. This activates the Add Ports window. Click here for information about how to configure an 802.1Q tagged VLAN port assignment.

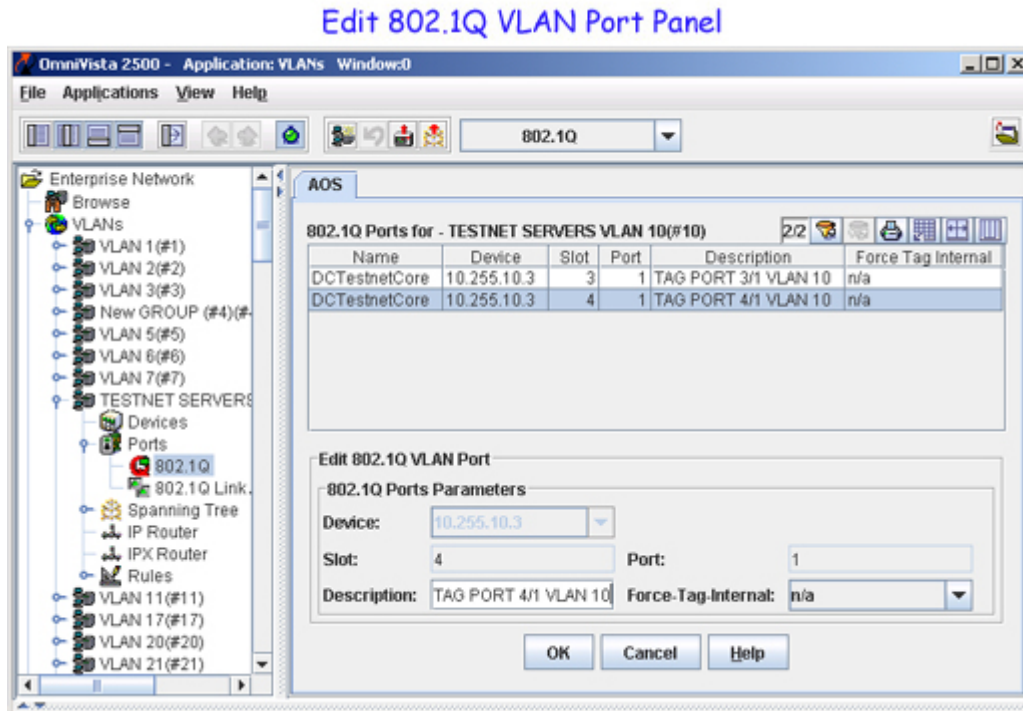
Removing an 802.1Q Port Assignment

To remove an 802.1Q tagged VLAN port assignment, select one or more port entries from the AOS 802.1Q Ports Tab list and click the **Delete** button. A delete icon appears in the Name field of the selected entry. Click the **Apply** button to drop the 802.1Q tagged assignment from the VLAN.

Modifying 802.1Q Port Parameters

Only the description and force tag internal parameter (if applicable) are modifiable. To change these values, select one or more port entries in the AOS 802.1Q Ports Tab list and click the **Edit** button. This activates the Edit 802.1Q VLAN Port panel, as shown below. Parameters that are not modifiable are grayed out on this panel.

Note that if you select multiple ports to modify, an Edit 802.1Q VLAN Ports pop-up window opens that contains only the modifiable parameters.



Using either the Edit 802.1Q VLAN Port(s) panel or pop-up window, make the desired parameter changes and click the **OK** button to return to the AOS 802.1Q Ports Tab list. A modify icon appears in the Name field for the modified port. Click the **Apply** button to apply the changes to the appropriate switch configurations.

802.1Q Tagged Port Parameter Definitions

Note that only the description and force tag internal parameters are modifiable.

Name

The user-defined name for the switch.

Device

The IP host address that identifies the switch within the management IP network. It is not the same IP host address defined as a virtual IP router port for the selected VLAN, unless the VLAN is part of the management network. In addition, an IP host address appears in this field even if an IP virtual router port does not exist for the VLAN on that particular switch.

Slot/Port

Slot--The slot number of the switch module. Identifies the position of the module in the switch chassis (or the position within a stack of switches, such as with the OmniSwitch 6624/6648 stackable units).

Port--The port number on that module (e.g. 3/1 specifies port 1 on slot 3).

Description

An optional textual description (up to 32 characters) for the 802.1Q tagged port assignment. This parameter defaults to the slot/port designation for the tagged port and the VLAN ID (e.g., TAG PORT 2/1 VLAN 110) of the tagged VLAN. If the 802.1Q tagged port assignment is for a link aggregate of ports, the description defaults to the tagged aggregate ID and the VLAN ID of the tagged VLAN (e.g. TAG AGGREGATE 12 VLAN 455).

Force Tag Internal

Indicates if the force tag internal parameter is on or off for the 802.1Q tagged port assignment. By default, this parameter is set to on, which indicates that 802.1Q tagged packets received on untagged ports are updated with the untagged port's VLAN ID when they are forwarded out of the VLAN on the 802.1Q tagged port. If force tag internal is set to off, these same types of packets are not updated; their original Q tag VLAN ID is retained when they are forwarded out of the VLAN on the 802.1Q tagged port.

For example, if force tag internal is set to **on** for an 802.1Q tagged port assigned to VLAN 10, tagged packets forwarded out this port that were received on untagged ports also assigned to VLAN 10 are updated with VLAN 10 as their VLAN ID before they are forwarded out the tagged port. If force tag internal was set to **off**, then these same types of tagged packets would retain their original tagged VLAN ID when they are forwarded out the tagged port.

The exception to this is if the untagged port's VLAN ID is also the 802.1Q tagged port's default VLAN ID, then the packet is forwarded with its original tagged VLAN ID. In this case, the force tag internal parameter is ignored.

Note: The force tag internal parameter is not available on OmniSwitch 6600, 6800, 6850, and 9000 series switches.

XOS 802.1Q Ports Tab

The XOS 802.1Q Ports Tab provides a list of all XOS device ports that are tagged to forward traffic on the current VLAN. In addition to the slot and port number, each list entry contains fields that display the current values for related 802.1Q port parameters. This tab also enables you to add or delete 802.1Q tagged port assignments. These tasks and port parameter definitions are described below.

XOS 802.1Q VLAN Port Assignments

802.1Q Ports for - VLAN 2(#2)

Name	Device	Slot	Port	Spanning Tree	VLAN Tag	Priority
167	10.255.13.167	4	1	IEEE - GigaBit	500	0
167	10.255.13.167	4	2	IEEE - GigaBit	500	0
no-name	10.255.13.193	3	11	Multiple (10/100) - Ethernet	2	0

View 802.1Q VLAN Port

802.1Q Ports Parameters

Device:

Slot: Port:

Spanning Tree: VLAN Tag:

Priority:

Creating a new 802.1Q Tagged VLAN Port Assignment

To tag a port with the current VLAN, click the **New** button found at the bottom of the XOS 802.1Q Ports Tab. This activates the Add 802.1Q Ports pop-up window. Click here for information about how to configure an 802.1Q tagged VLAN port assignment.

Removing an 802.1Q Port Assignment

To remove an 802.1Q VLAN port assignment, select one or more port entries from the XOS 802.1Q Ports Tab list and click the **Delete** button. A delete icon appears in the Name field of the selected entry. Click the **Apply** button to drop the 802.1Q tagged assignment from the VLAN.

Modifying 802.1Q Port Parameters

Only the spanning tree, VLAN tag, and priority parameters are modifiable. To change these parameter values, select one or more port entries in the XOS 802.1Q Ports Tab list and click the **Edit** button. This activates the Edit 802.1Q VLAN Port panel. Parameters that are not modifiable are grayed out on this panel.

Note: If you select multiple ports to modify, an Edit 802.1Q VLAN Ports pop-up window opens that contains only the modifiable parameters.

Edit 802.1Q VLAN Port Panel

Name	Device	Slot	Port	Spanning Tree	VLAN Tag	Priority
167	10.255.13.167	4	1	IEEE - GigaBit	500	0
167	10.255.13.167	4	2	IEEE - GigaBit	500	0
no-name	10.255.13.193	3	11	Multiple (10/100) - Ethernet	2	0

Edit 802.1Q VLAN Port

802.1Q Ports Parameters

Device:

Slot: Port:

Spanning Tree: VLAN Tag:

Priority:

OK Cancel Help

Using either the Edit 802.1Q VLAN Port(s) panel or pop-up window, make the desired parameter changes and click the **OK** button to return to the XOS 802.1Q Ports Tab list. A modify icon appears in the Name field for the modified port. Click the **Apply** button to apply the changes to the appropriate switch configurations.

802.1Q Tagged Port Parameter Definitions

Note that only the spanning tree, VLAN tag, and priority parameters are modifiable.

Name

The user-defined name for the switch.

Device

The IP host address that identifies the switch within the management IP network. It is not the same IP host address defined as a virtual IP router port for the selected VLAN, unless the VLAN is part of the management network. In addition, an IP host address appears in this field even if an IP virtual router port does not exist for the VLAN on that particular switch.

Slot/Port

Slot--The slot number of the switch module. Identifies the position of the module in the switch chassis (or the position within a stack of switches, such as with the OmniSwitch 6624/6648 stackable units).

Port--The port number on that module (e.g. 3/1 specifies port 1 on slot 3).

Spanning Tree

The spanning tree mode for the 802.1Q port assignment; multiple or single. These two modes are only available on 10/100 Ethernet ports. If you are tagging a port that resides on a Kodiak 10/100 Ethernet module, however, this parameter defaults to multiple spanning tree and is not modifiable. On Gigabit Ethernet 802.1Q tagged ports, the spanning tree parameter value defaults to IEEE - Gigabit (also multiple spanning tree) and is not modifiable.

Once you select a type of spanning tree for a port, the port automatically retains the spanning tree selection for any other group it is added to. For example, suppose that Port 3/1 is assigned to Group 2 using the single spanning tree mode. If another 802.1Q tag is created on this port for another group, the mode is automatically set for single spanning tree for the new group.

Since an 802.1Q tagged assignment is a trunked service, and Alcatel switches have a 16 (10/100) or 15 (Gigabit) services per port limit, you can only tag 15 or 14 802.1Q groups to the same port. In both cases, a default bridge service occupies one of the service slots. For Kodiak ASIC-based Fast Ethernet and Gigabit Ethernet modules, up to 64 groups are supported using multiple spanning tree on an 802.1Q link.

VLAN Tag

A simple identifier that is added to 802.1Q packets for identification. This value can be any number between 1 and 4094.

Priority

The priority number assigned to packets from this 802.1Q trunking service.

ESX-K and GSX-K Kodiak ASIC-based modules support 802.1p traffic prioritization. For chassis configurations that include only ESX-K, GSX-K and/or WSX series modules, 802.1p priority bits can be carried inbound on a tagged port (configured with multiple spanning tree 802.1Q) across the backplane. This priority information is used at the egress port to queue the packet, and is sent out in the packet whether the egress port is tagged or not.

The ESX-K and GSX-K modules can also remap incoming priority on an ingress port. If priority remapping has been configured, the new priority will be carried across the backplane. The priority information is used to queue the packet, and is sent out in the packet if the egress port is tagged.

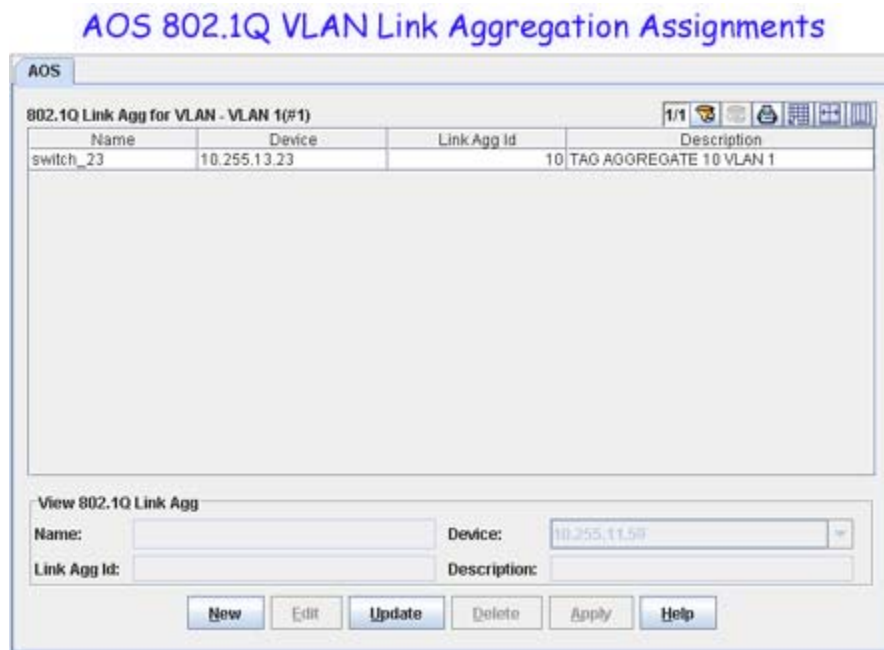
AOS 802.1Q Link Agg Tab

Link aggregation is a way of combining multiple physical links between two switches into one logical link. The aggregate group operates within Spanning Tree as one virtual port and can provide more bandwidth than a single link. It also provides redundancy. If one physical link in the aggregate group goes down, link integrity is maintained.

There are two types of aggregate groups: static and dynamic. Static aggregate groups are manually configured on the switch with static links. Dynamic groups are set up on the switch but they aggregate links as necessary according to the Link Aggregation Control Protocol (LACP).

The AOS 802.1Q Link Agg Tab provides a list of all link aggregates that are assigned to the current VLAN. Each list entry contains fields that display the current values for related link aggregate parameters. This tab also enables you to add or delete link aggregate assignments to the VLAN. These tasks and port parameter definitions are described below.

Note that the Link Agg Tab is used only to view existing link aggregates and to configure a new default VLAN assignment for a link aggregate.



Assigning a Link Aggregate to the VLAN

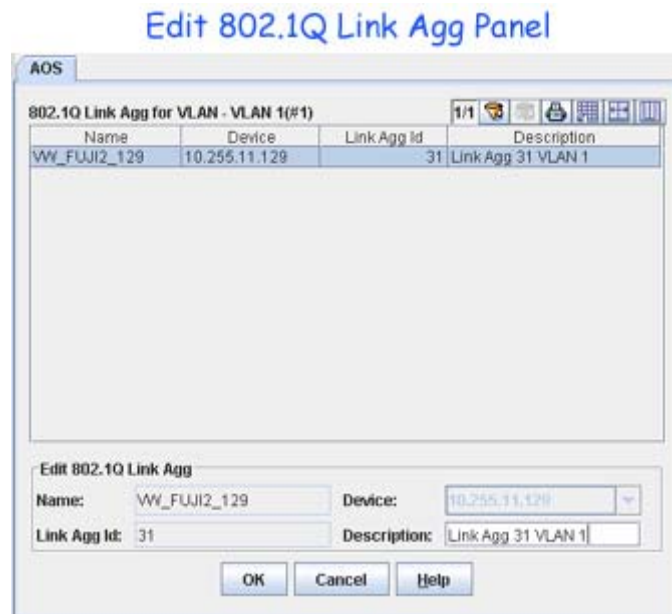
To assign a link aggregate to the current VLAN, click the **New** button found at the bottom of the AOS 802.1Q Link Agg Tab. This activates the Add 802.1Q Link Aggregation window. Click here for information about how to configure an 802.1Q link aggregate VLAN assignment.

Removing a Link Aggregate Assignment from the VLAN

To remove a link aggregate assignment from the current VLAN, select one or more aggregate entries from the AOS 802.1Q Link Agg Tab list and click the **Delete** button. A delete icon appears in the Name field of the selected entry. Click the **Apply** button to drop the link aggregate assignment from the VLAN.

Modifying Link Aggregate Parameters

Only the description parameter is modifiable. To change the description value, select a single link aggregate entry in the AOS 802.1Q Link Agg Tab list and click the **Edit** button. This activates the Edit 802.1Q Link Agg panel, as shown below. Parameters that are not modifiable are grayed out on this panel.



Make the desired description parameter changes and click the **OK** button to return to the AOS 802.1Q Link Agg Tab list. A modify icon appears in the Name field for the modified aggregate. Click the **Apply** button to apply the changes to the appropriate switch configurations.

802.1Q Link Aggregate Parameter Definitions

Note that only the description parameter is modifiable.

Name

The user-defined name for the switch.

Device

The IP host address that identifies the switch within the management IP network. It is not the same IP host address defined as a virtual IP router port for the selected VLAN, unless the VLAN is part of the management network. In addition, an IP host address appears in this field even if an IP virtual router port does not exist for the VLAN on that particular switch.

Link Agg ID

The ID of the link aggregate group of ports. This number was assigned when the aggregate was created. This is a unique integer in the range 0 - 31 on OmniSwitch 6800/6850/7000/9000 switches, 0 - 29 on OmniSwitch 6624 and 6648 switches, and 0 - 15 on OmniSwitch 8800 switches.

Description

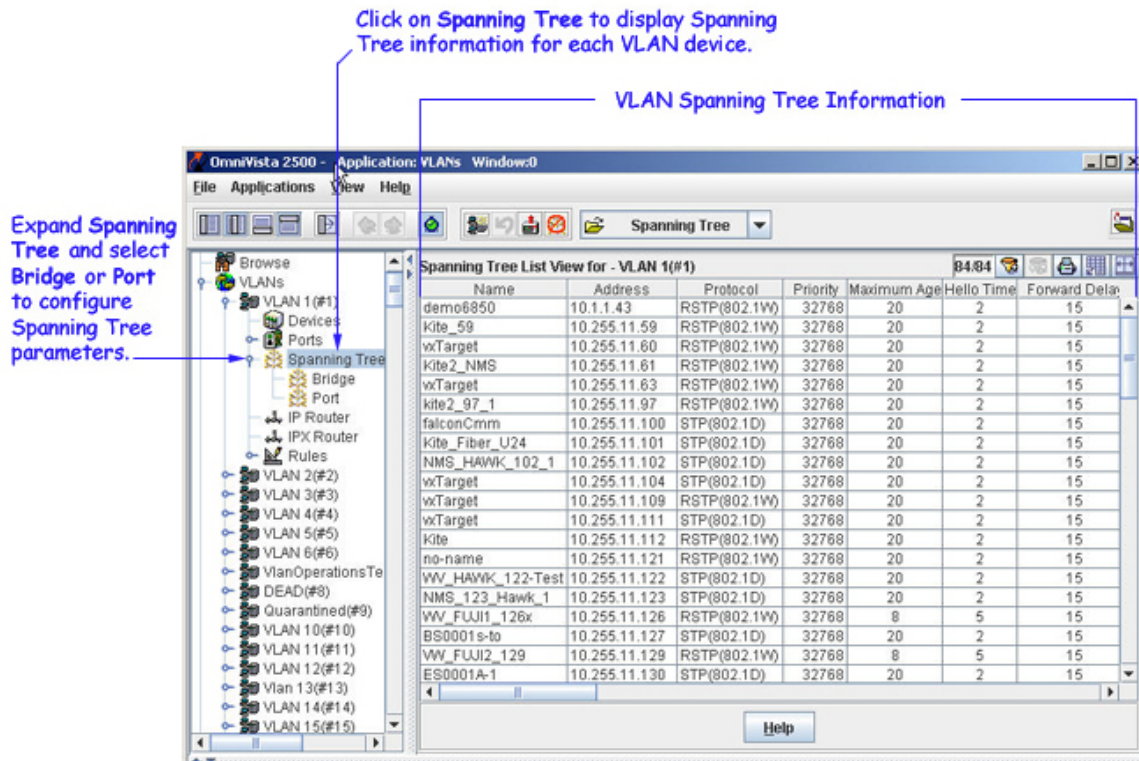
An optional textual description (up to 32 characters) for the link aggregate. If a description was not specified when the link aggregate was created, then the link aggregate ID and the default VLAN ID assigned to the aggregate are used for the description (e.g., Link Agg 30 VLAN 10).

Configuring Spanning Tree Parameters

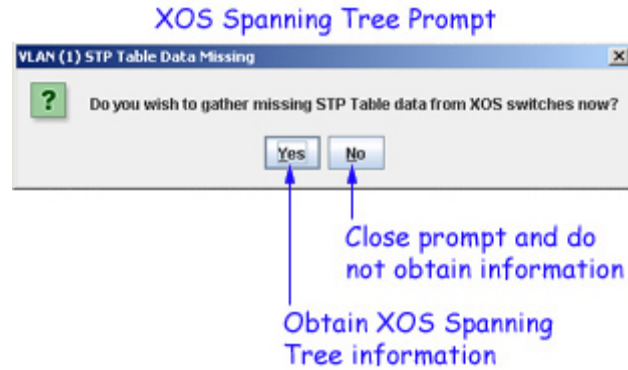
The Spanning Tree Algorithm and Protocol (STP) is a self-configuring algorithm that maintains a loop-free topology while providing data path redundancy and network scalability. STP software is active on all switches by default. As a result, a loop-free network topology is automatically calculated based on default Spanning Tree switch, VLAN (bridge), and port parameter values. It is only necessary to configure Spanning Tree parameters to change how the topology is calculated and maintained.

To access the current STP information for AOS and XOS devices assigned to the VLAN, click on the **Spanning Tree** icon underneath the desired VLAN in the Tree. The Spanning Tree List View window, shown below, displays a list of all devices that contain the selected VLAN in their configuration and provides the current Spanning Tree topology information for each instance of the VLAN. Each entry in the list represents a single device and includes Spanning Tree parameter values described below.

To configure Spanning Tree bridge or port parameters, click open **Spanning Tree** in the Tree and then click on either **Bridge** or **Port**. Note that changing these parameter values will impact your Spanning Tree calculations and may trigger a topology change in your network.



Note that when you click on the Spanning Tree icon for a VLAN that contains XOS devices, the following prompt displays asking if you want to obtain XOS Spanning Tree information from these devices.



Spanning Tree Parameter Definitions

In addition to the device name and management IP address, each entry in the Spanning Tree List View window contains fields that show the current values of Spanning Tree parameters, described below, that apply to the VLAN on the named device.

Name

The user-defined name for the switch.

Address

The IP host address that identifies the switch within the management IP network. It is not the same IP host address defined as a virtual IP router port for the selected VLAN, unless the VLAN is part of the management network. In addition, an IP host address appears in this field even if an IP virtual router port does not exist for the VLAN on that particular switch.

Protocol

The VLAN spanning tree algorithm protocol; **802.1D** (standard) or **802.1w** (rapid reconfiguration). The algorithm determines the state and role of a port within the spanning tree topology. Rapid reconfiguration is based on the 802.1D standard algorithm and is designed to provide quick recovery in the event of a link, port or device failure. By default, this parameter is set to **802.1D**.

Priority

The bridge priority value (**0-65535**) for the VLAN. The lower the number, the higher the priority value. The bridge priority value is used by the spanning tree algorithm to determine which VLAN should serve as the root of the spanning tree. By default, this parameter is set to **32768**.

Maximum Age

The amount of time (**6-40** seconds) that spanning tree information learned from BPDUs received on VLAN ports is retained. When this information has aged beyond the maximum age value, the information is discarded. By default, this parameter is set to **20** seconds.

Hello Time

The amount of time (**1-10** seconds) to wait between each transmission of Configuration Bridge Protocol Data Units (BPDU) on any forwarding VLAN port. BPDUs are transmitted when the VLAN is operating as the spanning tree root or is attempting to become the root. By default, this parameter is set to **2** seconds.

Forward Delay

The amount of time (**4-30** seconds) a VLAN port remains in the listening and learning states while it is transitioning to a forwarding state. In addition, when a topology change occurs, the forward delay time value is used to age all dynamically learned MAC address in the MAC address forwarding table. By default, this parameter is set to **15** seconds.

Path Cost

The cost of the path to the root for this Spanning Tree instance.

Mode

The Spanning Tree operating mode for the switch; **One Spanning Tree Per VLAN** or **Single Spanning Tree** (available only on AOS switch platforms).

If **Single Spanning Tree** mode is selected, the Spanning Tree Algorithm is applied across all VLANs. For example, if a port belonging to VLAN 10 and a port belonging to VLAN 20 both connect to the same switch, then Spanning Tree Algorithm will block one of these ports.

In **One Spanning Tree Per VLAN** mode is selected, a single Spanning Tree instance is enabled for each VLAN configured on the switch. For example, if there are five VLANs configured on the switch, then there are five separate Spanning Tree instances. In essence, a VLAN is a virtual bridge in that it will have its own bridge ID and configurable STP parameters, such as protocol, priority, hello time, max age and forward delay.

By default, the Spanning Tree operating mode is set to **One Spanning Tree Per VLAN**.

Bridge ID

The bridge identifier for this Spanning Tree instance. Consists of the bridge priority value (in hex) concatenated with the bridge MAC address.

Root ID

The bridge identifier of the root of the spanning tree as determined by the Spanning Tree Algorithm and Protocol.

Time Since Last Topology Change

The amount of time, in hundredths of a second, since the last topology change was detected by this spanning tree instance.

Total Topology Changes

The number of topology changes detected by this spanning tree instance since the management entity was last reset or initialized.

Root Port Number

The port that offers the lowest cost path from this bridge to the root bridge for this Spanning Tree instance.

Next Best Root Cost

The cost of the next best root port for this Spanning Tree instance.

Next Best Root Port

The port that offers the next best (second lowest) cost path to the root bridge for this Spanning Tree instance.

Network Maximum Age

The Maximum Age time value for the root bridge.

Network Hello Time

The Hello Time value for the root bridge.

Network Hold Time

The amount of time, in hundredths of a second, in which this spanning tree instance can transmit no more than two Configuration Bridge Protocol Data Units (BPDU).

Network Forward Delay

The Forward Delay time value for the root bridge.

AOS Spanning Tree Bridge Parameters

The AOS Spanning Tree Bridge Parameters window provides a list of all AOS devices that contain the selected VLAN in their configuration. In addition, to the device name and management IP address, each list entry contains fields that show the current values of Spanning Tree bridge parameters that apply to the VLAN on the named device. This tab also enables you to modify Spanning Tree Bridge Parameter values for this instance of the VLAN.

Note: Spanning Tree Mode parameters are configured using the CLI or WebView, and are shown for display purposes only.

AOS Spanning Tree Bridge Parameters

Name	Device	STP Mode	Protocol	Priority	Bridge ID
Kite_59	10.255.11.59	1X1(One STP Per VLAN)	RSTP(802.1W)	32768	80 00 00 d0 95 a3
wxTarget	10.255.11.60	1X1(One STP Per VLAN)	RSTP(802.1W)	32768	80 00 00 d0 95 b2
Kite2_NMS	10.255.11.61	1X1(One STP Per VLAN)	RSTP(802.1W)	32768	80 00 00 d0 95 e0
wxTarget	10.255.11.63	1X1(One STP Per VLAN)	RSTP(802.1W)	32768	80 00 00 d0 95 d5
kite2_97_1	10.255.11.97	1X1(One STP Per VLAN)	RSTP(802.1W)	32768	80 00 00 d0 95 c8
falconCmm	10.255.11.1...	1X1(One STP Per VLAN)	STP(802.1D)	32768	80 00 00 d0 95 6b
Kite_Fiber_U24	10.255.11.1...	1X1(One STP Per VLAN)	STP(802.1D)	32768	80 00 00 d0 95 bd

View Spanning Tree Parameters

Device Spanning Tree Mode
 Device: STP Mode:

Bridge Parameters
 Protocol: Priority:
 Maximum Age: Hello Time:
 Forward Delay:

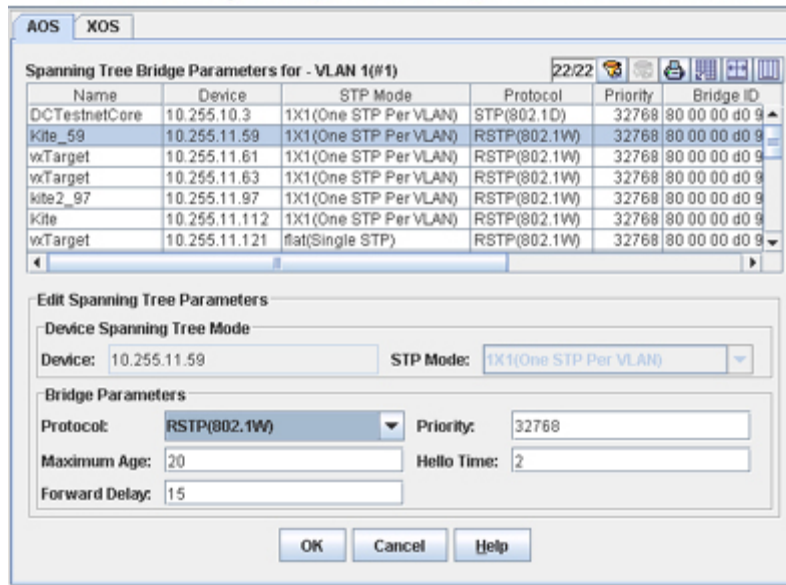
Modifying Spanning Tree Bridge Parameters

The following sections provide instructions for modifying Spanning Tree Bridge Parameters for a single device or multiple devices. Note that Spanning Tree software is active on all switches by default. As a result, a loop-free network topology is automatically calculated based on default Spanning Tree switch, VLAN (bridge), and port parameter values. It is only necessary to configure Spanning Tree bridge parameters to change how the topology is calculated and maintained.

Modifying Parameters on a Single Device

To edit parameters on a single device, select the device and click the **Edit** button. The Edit Spanning Tree Bridge Parameters panel will appear, as shown below.

Edit AOS Spanning Tree Bridge Parameters Panel

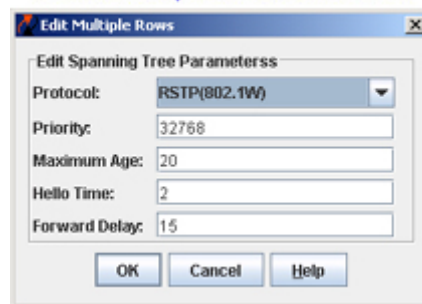


Edit the applicable fields, click the **OK** button, then click the **Apply** button. Click here for Spanning Tree Bridge Parameter definitions.

Modifying Parameters on Multiple Devices

To edit parameters on multiple devices, select the devices using the **SHIFT** or **CTRL** keys and click the **Edit** button. The Edit Multiple Rows window will appear, as shown below.

Edit Multiple Rows Window



Edit the applicable fields, click the **OK** button, then click the **Apply** button. Click here for Spanning Tree Bridge Parameter definitions.

Spanning Tree Bridge Parameter Definitions

Note that changing any of the following bridge parameter values may impact Spanning Tree calculations for this instance of the VLAN and trigger a topology change in your network.

Name

The user-defined name for the switch.

Device

The IP host address that identifies the switch within the management IP network. It is not the same IP host address defined as a virtual IP router port for the selected VLAN, unless the VLAN is part of the management network. In addition, an IP host address appears in this field even if an IP virtual router port does not exist for the VLAN on that particular switch.

STP Mode

The Spanning Tree operating mode for the switch:

- **1x1 Mode** (One Spanning Tree instance per VLAN) - This is the default mode. In this mode, each VLAN behaves as a virtual bridge in that the VLAN has its own configurable bridge parameters that apply only to that VLAN. A single Spanning Tree instance is enabled for each VLAN configured on the switch. For example, if there are five VLANs configured on the switch, then there are five separate Spanning Tree instances.
- **Flat Mode** (Single STP Mode) - There is one Spanning Tree instance for the entire switch; port states are determined across all VLANs. For example, if a port belonging to VLAN 10 and a port belonging to VLAN 20 both connect to the same switch, then the Spanning Tree Algorithm will block one of these ports.

Protocol

The VLAN spanning tree algorithm protocol. The algorithm determines the state and role of a port within the spanning tree topology.

- **STP (802.1D)** - Standard Spanning Tree Algorithm and Protocol (Default).
- **RSTP (802.1W)** - Rapid Spanning Tree Algorithm and Protocol. RSTP is based on the 802.1D standard algorithm and is designed to provide quick recovery in the event of a link, port or device failure.
- **MSTP (802.1S)** - Multiple Spanning Tree Protocol. MSTP is an enhancement to 802.1Q Common Spanning Tree Instance (CST). When the switch is running in Flat Mode, a single Spanning Tree instance is applied across all VLAN port connections. MSTP allows the configuration of Multiple Spanning Tree Instances (MSTI) in addition to the CST instance. Each MSTI is mapped to a set of VLANs. As a result, Flat Mode can now support the forwarding of VLAN traffic over separate data paths.

Priority

The bridge priority value (**0-65535**) for the VLAN. The lower the number, the higher the priority value. The bridge priority value is used by the spanning tree algorithm to determine which VLAN should serve as the root of the spanning tree. By default, this parameter is set to **32768**.

Bridge ID

The bridge identifier for this spanning tree instance. Consists of the bridge priority value (in hex), concatenated with the dedicated bridge MAC address.

Maximum Age

The amount of time (**6-40** seconds) that spanning tree information learned from BPDUs received on VLAN ports is retained. When this information has aged beyond the maximum age value, the information is discarded. By default, this parameter is set to **20** seconds.

Hello Time

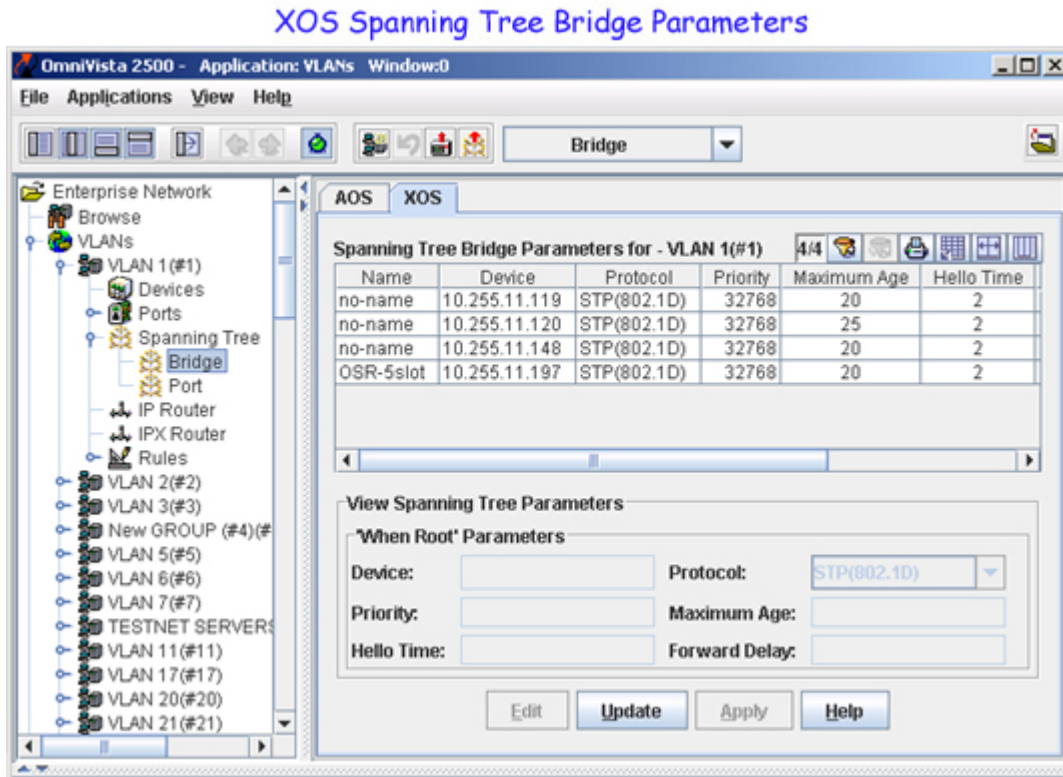
The amount of time (**1-10** seconds) to wait between each transmission of Configuration Bridge Protocol Data Units (BPDU) on any forwarding VLAN port. BPDUs are transmitted when the VLAN is operating as the spanning tree root or is attempting to become the root. By default, this parameter is set to **2** seconds.

Forward Delay

The amount of time (**4-30** seconds) a VLAN port remains in the listening and learning states while it is transitioning to a forwarding state. In addition, when a topology change occurs, the forward delay time value is used to age all dynamically learned MAC address in the MAC address forwarding table. By default, this parameter is set to **15** seconds.

XOS Spanning Tree Bridge Parameters

The XOS Spanning Tree Bridge Parameters window provides a list of all XOS devices that contain the selected VLAN in their configuration. In addition, to the device name and management IP address, each list entry contains fields that show the current values of Spanning Tree bridge parameters that apply to the VLAN on the named device. This tab also enables you to modify Spanning Tree bridge Parameter values for this instance of the VLAN.



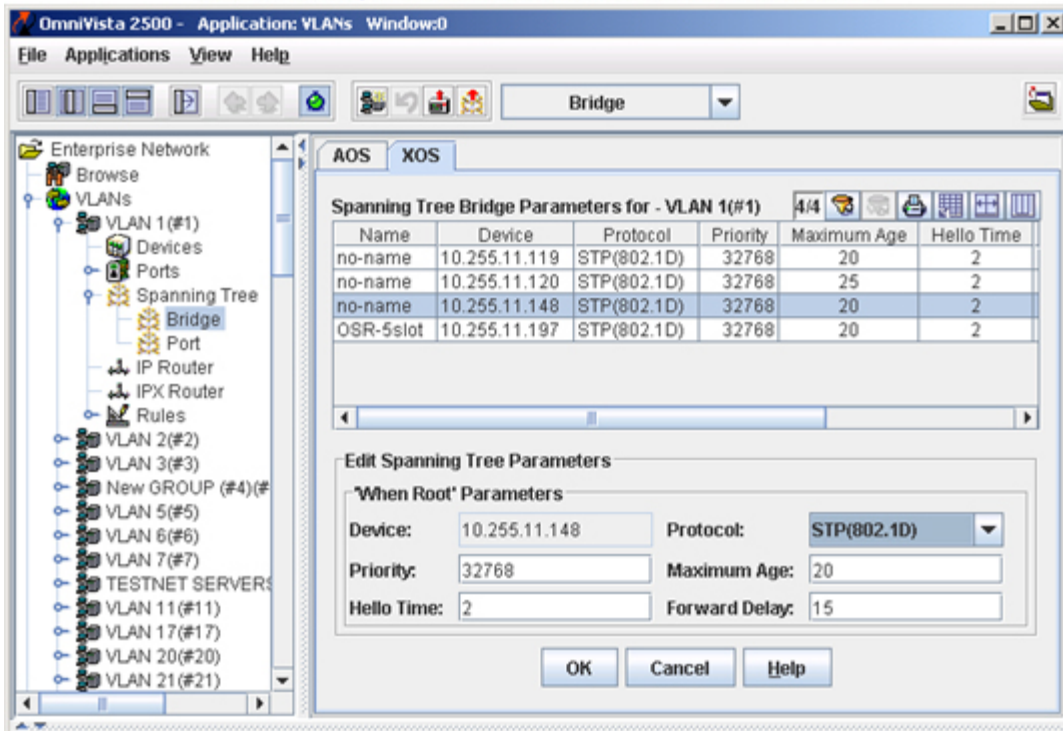
Modifying Spanning Tree Bridge Parameters

The following sections provide instructions for modifying Spanning Tree Bridge Parameters for a single device or multiple devices. Note that Spanning Tree software is active on all switches by default. As a result, a loop-free network topology is automatically calculated based on default Spanning Tree switch, VLAN (bridge), and port parameter values. It is only necessary to configure Spanning Tree bridge parameters to change how the topology is calculated and maintained.

Modifying Parameters on a Single Device

To edit parameters on a single device, select the device and click the **Edit** button. The Edit Spanning Tree Bridge Parameters panel will appear, as shown below.

Edit XOS Spanning Tree Bridge Parameters Panel

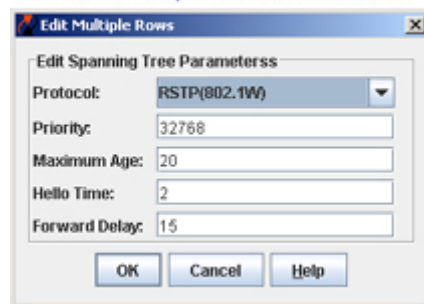


Edit the applicable fields, click the **OK** button, then click the **Apply** button. Click here for Spanning Tree Bridge Parameter definitions.

Modifying Parameters on Multiple Devices

To edit parameters on multiple devices, select the devices using the **SHIFT** or **CTRL** keys and click the **Edit** button. The Edit Multiple Rows window will appear, as shown below.

Edit Multiple Rows Window



Edit the applicable fields, click the **OK** button, then click the **Apply** button. Click here for Spanning Tree Bridge Parameter definitions.

Spanning Tree Bridge Parameter Definitions

Note that changing any of the following bridge parameter values may impact Spanning Tree calculations for this instance of the VLAN and trigger a topology change in your network.

Name

The user-defined name for the switch.

Device

The IP host address that identifies the switch within the management IP network. It is not the same IP host address defined as a virtual IP router port for the selected VLAN, unless the VLAN is part of the management network. In addition, an IP host address appears in this field even if an IP virtual router port does not exist for the VLAN on that particular switch.

Protocol

The VLAN spanning tree algorithm protocol; **802.1D** (standard) or **802.1w** (rapid reconfiguration). The algorithm determines the state and role of a port within the spanning tree topology. Rapid reconfiguration is based on the 802.1D standard algorithm and is designed to provide quick recovery in the event of a link, port or device failure. By default, this parameter is set to **802.1D**.

Priority

The bridge priority value (**0-65535**) for the VLAN. The lower the number, the higher the priority value. The bridge priority value is used by the spanning tree algorithm to determine which VLAN should serve as the root of the spanning tree. By default, this parameter is set to **32768**.

Maximum Age

The amount of time (**6-40** seconds) that spanning tree information learned from BPDUs received on VLAN ports is retained. When this information has aged beyond the maximum age value, the information is discarded. By default, this parameter is set to **20** seconds.

Hello Time

The amount of time (**1-10** seconds) to wait between each transmission of Configuration Bridge Protocol Data Units (BPDU) on any forwarding VLAN port. BPDUs are transmitted when the VLAN is operating as the spanning tree root or is attempting to become the root. By default, this parameter is set to **2** seconds.

Forward Delay

The amount of time (**4-30** seconds) a VLAN port remains in the listening and learning states while it is transitioning to a forwarding state. In addition, when a topology change occurs, the forward delay time value is used to age all dynamically learned MAC address in the MAC address forwarding table. By default, this parameter is set to **15** seconds.

Mode

The Spanning Tree version selected for the VLAN; **IEEE** (IEEE 802.1D) or **IBM** (IBM Spanning Tree).

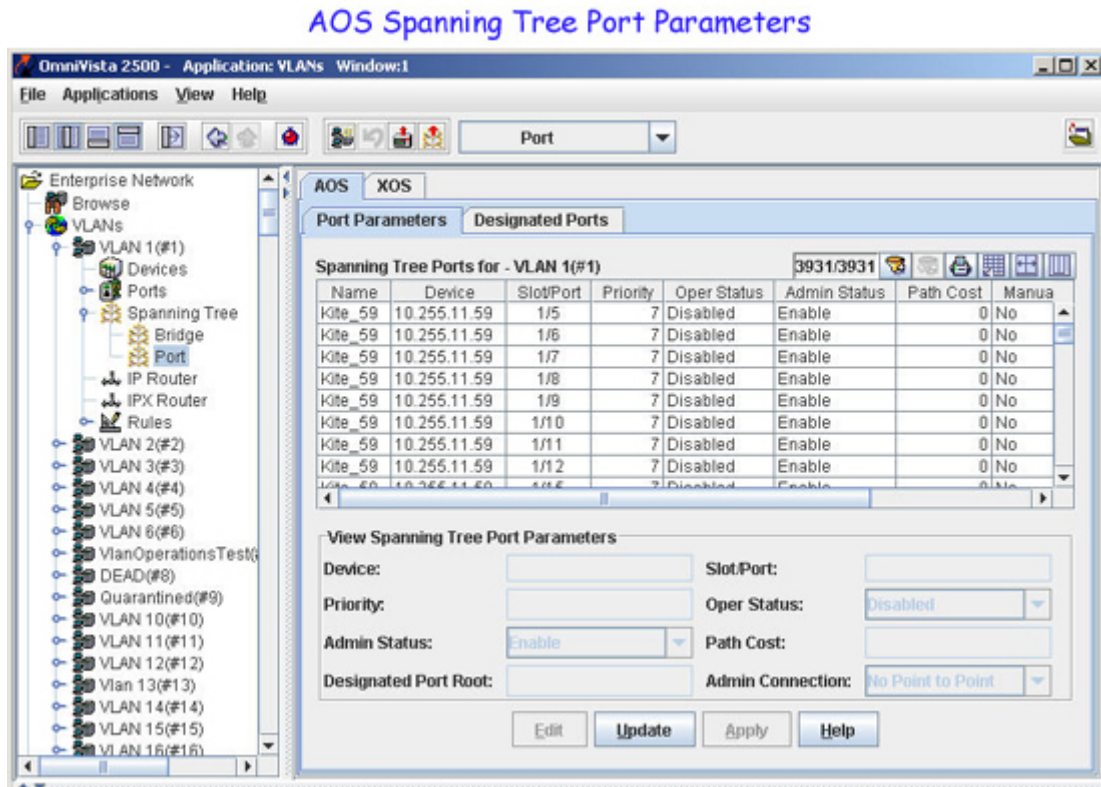
The IBM Spanning Tree protocol is only supported by IBM Token Ring environments that make use of functional addresses for the transmission of Bridge Protocol Data Units (BPDUs). By default, the Spanning Tree version is set to **IEEE 802.1D** when a VLAN is created.

Status

Indicates the VLAN Spanning Tree status; **Enable** or **Disable**. If disabled, then the VLAN does not participate in the Spanning Tree algorithm.

AOS Spanning Tree Port Parameters Tab

The AOS Spanning Tree Port Parameters Tab provides a list of all AOS device ports that are assigned to the VLAN. In addition to the device name and management IP address, each list entry contains fields that show the current values of Spanning Tree port parameters. This tab also enables you to modify Spanning Tree Port Parameter values for this instance of the VLAN. These tasks and port parameter values are described below.



Modifying Spanning Tree Port Parameters

Spanning Tree software is active on all switches by default. As a result, a loop-free network topology is automatically calculated based on default Spanning Tree switch, VLAN (bridge), and port parameter values. It is only necessary to configure Spanning Tree port parameters to change how the topology is calculated and maintained.

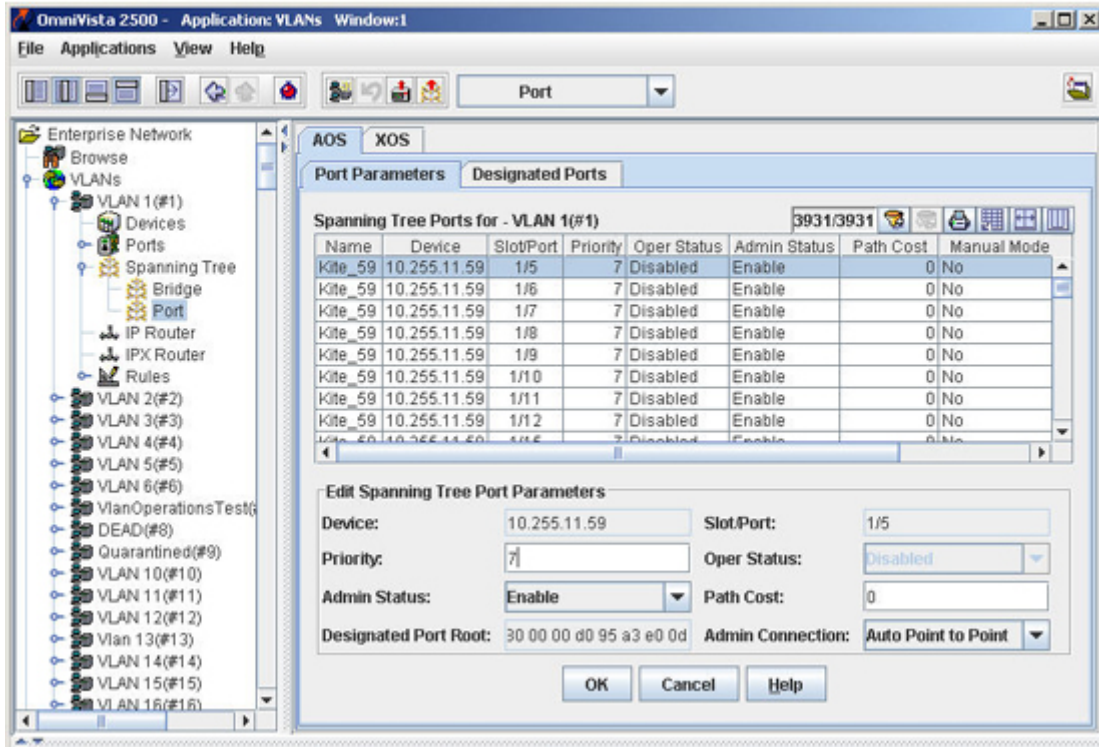
Note that only bridged ports participate in the Spanning Tree Algorithm. A port is considered bridged if it meets all the following criteria:

- Port is either a fixed (non-mobile) port, an 802.1Q tagged port or a link aggregate logical port.
- Spanning tree is enabled on the port.
- Port is assigned to a VLAN that has Spanning Tree enabled.
- Port state (forwarding or blocking) is dynamically determined by the Spanning Tree Algorithm, not manually set.

Modifying Parameters on a Single Device

To edit parameters on a single device, select the device and click the **Edit** button. The Edit AOS Spanning Tree Port Parameters panel will appear, as shown below.

Edit AOS Spanning Tree Port Parameters Panel

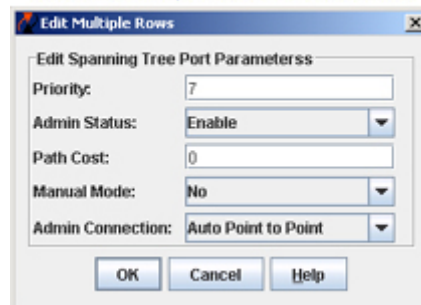


Edit the applicable fields, click the **OK** button, then click the **Apply** button. Click here for AOS Spanning Tree Port Parameter definitions.

Modifying Parameters on Multiple Devices

To edit parameters on multiple devices, select the devices using the **SHIFT** or **CTRL** keys and click the **Edit** button. The Edit Multiple Rows window will appear, as shown below.

Edit Multiple Rows Window



Edit the applicable fields, click the **OK** button, then click the **Apply** button. Click here for AOS Spanning Tree Port Parameter definitions.

Spanning Tree Port Parameter Definitions

Note that changing any of the following port parameter values may impact Spanning Tree calculations that could affect port behavior for this Spanning Tree instance and possibly trigger a topology change in your network.

Name

The user-defined name for the switch.

Device

The IP host address that identifies the switch within the management IP network. It is not the same IP host address defined as a virtual IP router port for the selected VLAN, unless the VLAN is part of the management network. In addition, an IP host address appears in this field even if an IP virtual router port does not exist for the VLAN on that particular switch.

Slot/Port

The slot/port designation that identifies the corresponding slot number for the port's module and the corresponding port number on that module. (e.g., 3/1 specifies port 1 on slot 3).

Priority

The port priority value (**0-15**) for the VLAN. The lower the number, the higher the priority value. The port priority is used to determine which port offers the best path to the root when multiple paths have the same path cost. If the priority values are the same for all ports in the path, then the port with the lowest physical switch port number is selected. By default, this parameter is set to **7**.

Oper Status

The operational state of the port as determined by the spanning tree algorithm. One of the following values will appear in this field:

- Disabled - Physical port is down or administratively disabled.
- Blocking or Discarding - Port does not transmit or receive data to prevent a network loop.
- Listening - Port is preparing to transmit data.
- Learning - Port is learning MAC addresses seen on the port.
- Forwarding - Port is transmitting and receiving data.

Note that this field displays the current operational state value for the port and is not a configurable Spanning Tree parameter.

Admin Status

The Spanning Tree status for the port; **Enable** or **Disable**. If disabled, the port state is set to forwarding for the VLAN spanning tree instance. This status value, however, is ignored if spanning tree is disabled for the associated VLAN. By default, Spanning Tree is enabled on all switch ports.

Path Cost

The path cost value (**0-65535**) for the port. This value specifies the contribution of a port to the path cost towards the root bridge that includes the port. If the path cost is set to **0**, then a default value based on link speed is used.

Manual Mode

The mode used for managing the port's state: **Blocking** or **Forwarding** (manually set) or **No** (dynamic). If the port state is manually set to Blocking or Forwarding, the port remains in that state until it is changed and does not participate in the spanning tree algorithm. Dynamic mode defers configuration of the port state to the spanning tree algorithm. By default, this parameter is set to **No** (dynamic).

Admin Connection

The port's administratively set connection type. This parameter is used by the 802.1w Rapid Spanning Tree Protocol (RSTP) to determine if a port is eligible for rapid transition to the forwarding state. One of the following connection type values appears in this field:

- No Point to Point (port connects to multiple switches).
- Point to Point (port connects directly to another switch).
- Auto Point to Point (connection type is automatically defined to No Point to Point or Point to Point based on the port's operational status).
- Edge Port (port is at the edge of a bridged LAN, does not receive BPDU, and has only one MAC address learned). Edge ports, however, will operationally revert to a no point to point connection type if a BPDU is received on the port.

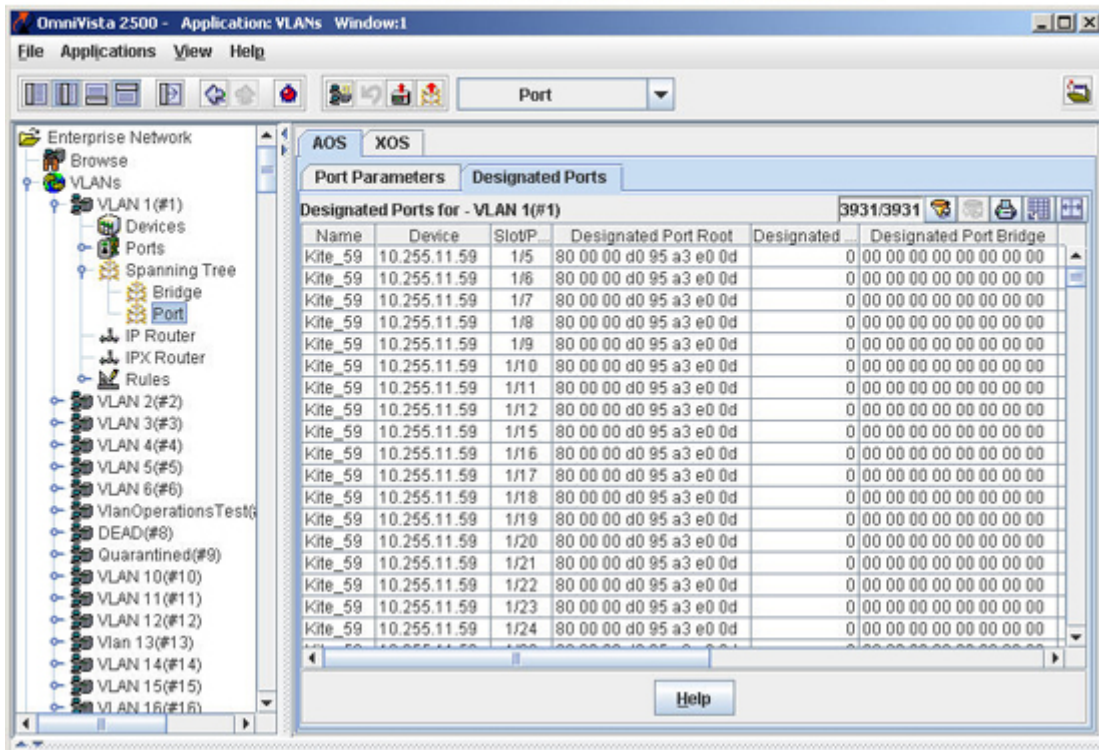
By default, the port connection type is set to **Auto Point to Point**.

Note: Configure ports that will connect to a host (PC, workstation, server, etc.) as **Edge Ports** so that these ports will transition directly to a forwarding state and not trigger an unwanted topology change when a device is connected to the port. If a port is configured as a **Point to Point** or **No Point to Point** connection type, the switch will assume a topology change when this port goes active and will flush and relearn all learned MAC addresses for the port's assigned VLAN.

AOS Spanning Tree Designated Ports Tab

The AOS Spanning Tree Designated Ports Tab provides Spanning Tree statistics for each AOS port assigned to the VLAN. The information provided shows current designated port information calculated by the Spanning Tree algorithm. In addition, the number of times a port has transitioned from the learning state to the forwarding state is also included.

AOS Spanning Tree Designated Port Statistics



Spanning Tree Port and Designated Port Statistics

Spanning Tree port and designated port information is calculated and reported by the Spanning Tree algorithm and is not configurable.

Name

The user-defined name for the switch.

Device

The IP host address that identifies the switch within the management IP network. It is not the same IP host address defined as a virtual IP router port for the selected VLAN, unless the VLAN is part of the management network. In addition, an IP host address appears in this field even if an IP virtual router port does not exist for the VLAN on that particular switch.

Slot/Port

The slot/port designation that identifies the corresponding slot number for the port's module and the corresponding port number on that module. (e.g., 3/1 specifies port 1 on slot 3).

Designated Port Root

The bridge identifier for the root VLAN (bridge) of this port's spanning tree instance.

Designated Port Cost

The path cost of the designated port of the segment connected to this port. If this is the root bridge or the Spanning Tree status of the port is administratively disabled, this value is **0**.

Designated Port Bridge

The bridge identifier for the designated bridge for this port's segment.

Designated Port Priority

The priority value (**0-15**) of the designated port. The lower the number, the higher the priority value.

Designated Port Number

The port identifier of the port on the designated bridge for this port's segment.

Number of Forward Transitions

The number of times this port has transitioned from the learning state to the forwarding state.

XOS Spanning Tree Port Parameters Tab

The XOS Spanning Tree Port Parameters Tab provides a list of all XOS device ports that are assigned to the VLAN. In addition to the device name and management IP address, each list entry contains fields that show the current values of Spanning Tree port parameters. This tab also enables you to modify Spanning Tree Port Parameter values for this instance of the VLAN. These tasks and port parameter values are described below.

XOS Spanning Tree Port Parameters

The screenshot shows the 'XOS Spanning Tree Port Parameters' tab. The table below represents the data shown in the 'Spanning Tree Ports for - VLAN 1(#1)' section.

Name	Device	Slot	Port	Service	Instance	Priority	Oper Status	Admin S
nms-test-103	10.255.11.103	3	1	Bridge	1	128	Forwarding	Enable
nms-test-103	10.255.11.103	3	2	Bridge	1	128	Disabled	Enable
nms-test-103	10.255.11.103	3	3	Bridge	1	128	Disabled	Enable
nms-test-103	10.255.11.103	3	4	Bridge	1	128	Disabled	Enable
nms-test-103	10.255.11.103	3	5	Bridge	1	128	Disabled	Enable
nms-test-103	10.255.11.103	3	6	Bridge	1	128	Disabled	Enable
nms-test-103	10.255.11.103	3	7	Bridge	1	128	Disabled	Enable

The 'View Spanning Tree Port Parameters' form contains the following fields and values:

- Name:
- Device:
- Slot:
- Port:
- Service:
- Instance:
- Priority:
- Oper Status:
- Admin Status:
- Path Cost:

Modifying Spanning Tree Port Parameters

Spanning Tree software is active on all switches by default. As a result, a loop-free network topology is automatically calculated based on default Spanning Tree switch, VLAN (bridge), and port parameter values. It is only necessary to configure Spanning Tree port parameters to change how the topology is calculated and maintained.

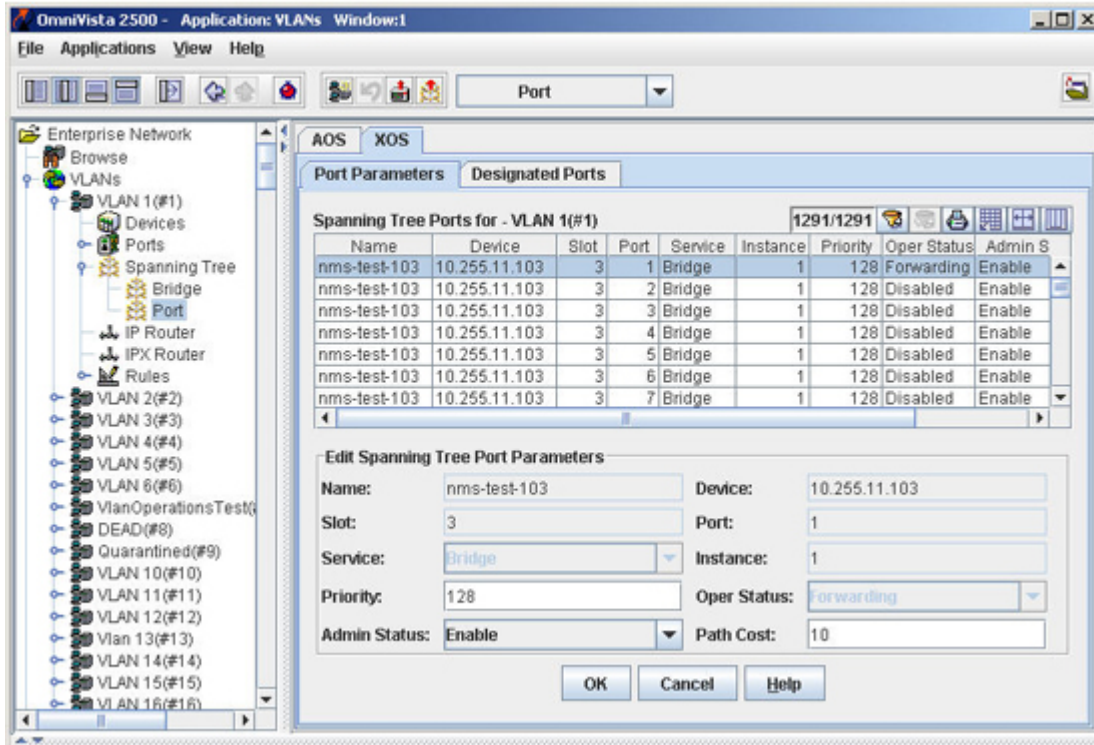
Note that only bridged ports participate in the Spanning Tree Algorithm. A port is considered bridged if it meets all of the following criteria:

- Port is either a fixed (non-mobile) port, an 802.1Q tagged port or a link aggregate logical port.
- Spanning tree is enabled on the port.
- Port is assigned to a VLAN that has Spanning Tree enabled.
- Port state (forwarding or blocking) is dynamically determined by the Spanning Tree Algorithm, not manually set.

Modifying Parameters on a Single Device

To edit parameters on a single device, select the device and click the **Edit** button. The Edit XOS Spanning Tree Port Parameters panel will appear, as shown below.

Edit XOS Spanning Tree Port Parameters

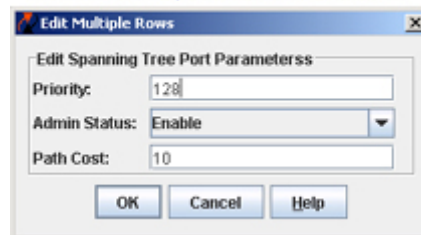


Edit the applicable fields, click the **OK** button, then click **Apply**. Click here for XOS Spanning Tree Port Parameter definitions.

Modifying Parameters on Multiple Devices

To edit parameters on multiple devices, select the devices using the **SHIFT** or **CTRL** keys and click the **Edit** button. The Edit Multiple Rows window will appear, as shown below.

Edit Multiple Rows Window



Edit the applicable fields, click the **OK** button, then click the **Apply** button. Click here for XOS Spanning Tree Port Parameter definitions.

XOS Spanning Tree Port Parameter Definitions

Note that changing any of the following port parameter values may impact Spanning Tree calculations that could affect port behavior for this Spanning Tree instance and possibly trigger a topology change in your network.

Name

The user-defined name for the switch.

Device

The IP host address that identifies the switch within the management IP network. It is not the same IP host address defined as a virtual IP router port for the selected VLAN, unless the VLAN is part of the management network. In addition, an IP host address appears in this field even if an IP virtual router port does not exist for the VLAN on that particular switch.

Slot/Port

The slot/port designation that identifies the corresponding slot number for the port's module and the corresponding port number on that module. (e.g., 3/1 specifies port 1 on slot 3).

Service

The type of virtual service port for this VLAN port assignment. Some examples of the service types this field may contain are as follows:

Bridge--Virtual bridge port.

VLMP 802.1Q--Virtual 802.1Q tagged port.

Trunk--Virtual trunk port (ATM, FDDI, and WAN service port)

ATM LANE--LANE emulation service port.

CIP--Classical IP service port.

Instance

The Instance is an identifier of this type of service within the switch. Each instance of a service port is given a different number. The number contained in this field is the instance of the virtual service port that was assigned to the VLAN when the service was created.

Priority

The port priority value (**0-256**) for the VLAN. The lower the number, the higher the priority value. The port priority is used to determine which port offers the best path to the root when multiple paths have the same path cost. If the priority values are the same for all ports in the path, then the port with the lowest physical switch port number is selected. By default, this parameter is set to **7**.

Oper Status

The operational state of the port as determined by the spanning tree algorithm. One of the following values will appear in this field:

- Disabled - Physical port is down or administratively disabled.
- Blocking or Discarding - Port does not transmit or receive data to prevent a network loop.
- Listening - Port is preparing to transmit data.
- Learning - Port is learning MAC addresses seen on the port.
- Forwarding - Port is transmitting and receiving data.

Note that this field displays the current operational state value for the port and is not a configurable Spanning Tree parameter.

Admin Status

The Spanning Tree status for the port; **Enable** or **Disable**. If disabled, the port state is set to forwarding for the VLAN spanning tree instance. This status value, however, is ignored if spanning tree is disabled for the associated VLAN. By default, Spanning Tree is enabled on all switch ports.

Path Cost

The path cost value (**0-65535**) for the port. This value specifies the contribution of a port to the path cost towards the root bridge that includes the port. If the path cost is set to **0**, then a default value based on link speed is used.

Manual Mode

The mode used for managing the port's state: **Blocking** or **Forwarding** (manually set) or **No** (dynamic). If the port state is manually set to Blocking or Forwarding, the port remains in that state until it is changed and does not participate in the spanning tree algorithm. Dynamic mode defers configuration of the port state to the spanning tree algorithm. By default, this parameter is set to **No** (dynamic).

XOS Spanning Tree Designated Ports Tab

The XOS Spanning Tree Designated Ports Tab provides Spanning Tree statistics for each XOS port assigned to the VLAN. The information provided shows current designated port information calculated by the Spanning Tree algorithm. In addition, the number of times a port has transitioned from the learning state to the forwarding state is also included.

XOS Spanning Tree Designated Port Statistics

Name	Device	Slot	Port	Designated Port Root	Designated Port Cost	De
nms-test-103	10.255.11.103	3	1	00 28 00 d0 95 8a 65 d0	62 00 6	
nms-test-103	10.255.11.103	3	2	00 00 00 00 00 00 00 00	0 00 0	
nms-test-103	10.255.11.103	3	3	00 00 00 00 00 00 00 00	0 00 0	
nms-test-103	10.255.11.103	3	4	00 00 00 00 00 00 00 00	0 00 0	
nms-test-103	10.255.11.103	3	5	00 00 00 00 00 00 00 00	0 00 0	
nms-test-103	10.255.11.103	3	6	00 00 00 00 00 00 00 00	0 00 0	
nms-test-103	10.255.11.103	3	7	00 00 00 00 00 00 00 00	0 00 0	
nms-test-103	10.255.11.103	3	8	00 00 00 00 00 00 00 00	0 00 0	
nms-test-103	10.255.11.103	3	9	00 00 00 00 00 00 00 00	0 00 0	
nms-test-103	10.255.11.103	3	10	00 00 00 00 00 00 00 00	0 00 0	
nms-test-103	10.255.11.103	3	11	00 00 00 00 00 00 00 00	0 00 0	
nms-test-103	10.255.11.103	3	12	00 00 00 00 00 00 00 00	0 00 0	
nms-test-103	10.255.11.103	3	13	00 00 00 00 00 00 00 00	0 00 0	
nms-test-103	10.255.11.103	3	14	00 00 00 00 00 00 00 00	0 00 0	
nms-test-103	10.255.11.103	3	15	00 00 00 00 00 00 00 00	0 00 0	
nms-test-103	10.255.11.103	3	16	00 00 00 00 00 00 00 00	0 00 0	
nms-test-103	10.255.11.103	5	1	00 00 00 00 00 00 00 00	0 00 0	
nms-test-103	10.255.11.103	5	2	00 00 00 00 00 00 00 00	0 00 0	

Spanning Tree Port and Designated Port Statistics

Spanning Tree port and designated port information is calculated and reported by the Spanning Tree algorithm and is not configurable.

Name

The user-defined name for the switch.

Device

The IP host address that identifies the switch within the management IP network. It is not the same IP host address defined as a virtual IP router port for the selected VLAN, unless the VLAN is part of the management network. In addition, an IP host address appears in this field even if an IP virtual router port does not exist for the VLAN on that particular switch.

Slot/Port

The slot/port designation that identifies the corresponding slot number for the port's module and the corresponding port number on that module. (e.g., 3/1 specifies port 1 on slot 3).

Designated Port Root

The bridge identifier for the root VLAN (bridge) of this port's spanning tree instance.

Designated Port Cost

The path cost of the designated port of the segment connected to this port. If this is the root bridge or the Spanning Tree status of the port is administratively disabled, this value is **0**.

Designated Port Bridge

The bridge identifier for the designated bridge for this port's segment.

Designated Port Priority

The priority value (**0-15**) of the designated port. The lower the number, the higher the priority value.

Designated Slot Number

The slot number of the port on the designated bridge for this port's segment.

Designated Interface Number

The port number of the port on the designated bridge for this port's segment.

Designated Port Service

The service port number of the port on the designated bridge for this port's segment.

Designated Service Instance

The service port instance of the port on the designated bridge for this port's segment.

Number of Forward Transitions

The number of times this port has transitioned from the learning state to the forwarding state.

Configuring VLAN Router Interfaces

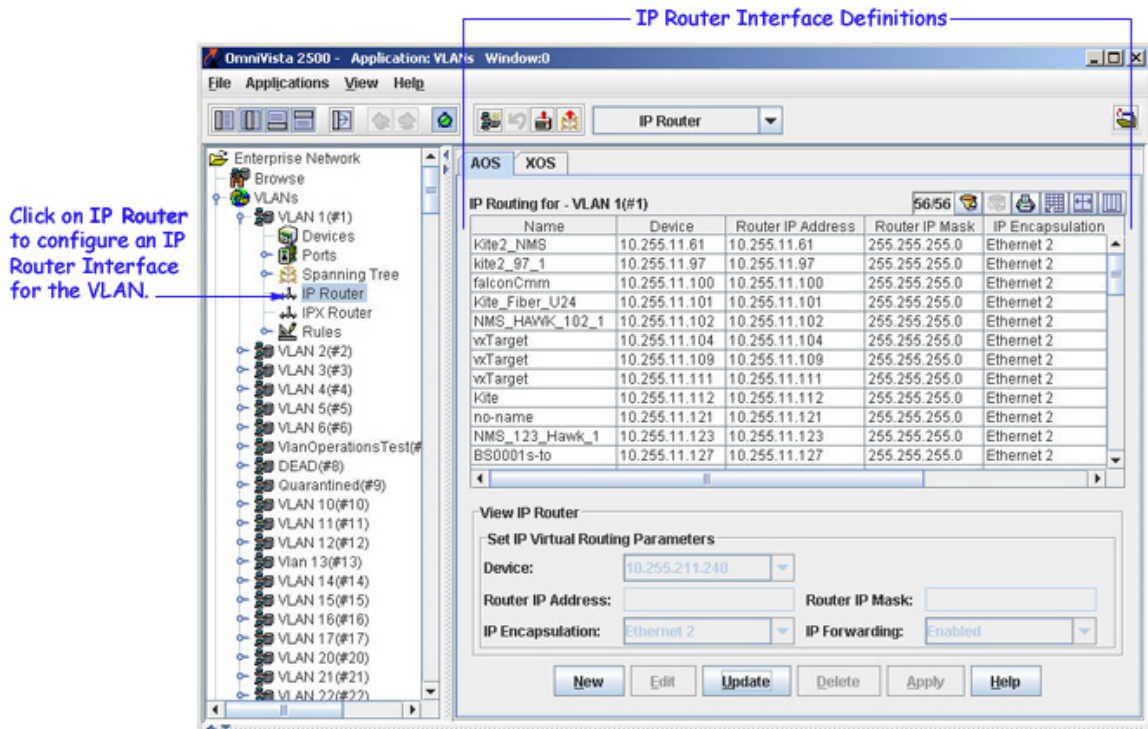
Network device traffic is bridged (switched) at the Layer 2 level between ports that are assigned to the same VLAN. However, if a device needs to communicate with another device that belongs to a different VLAN, then Layer 3 routing is necessary to transmit traffic between the VLANs. Bridging makes the decision on where to forward packets based on the packet's destination MAC address; routing makes the decision on where to forward packets based on the packet's IP or IPX network address (e.g., IP - 21.0.0.10, IPX - 210A).

Alcatel switches support routing of IP and IPX traffic on a per VLAN basis. A VLAN is available for routing when a router interface is defined for that VLAN and at least one active port has joined the VLAN. If a VLAN does not have a router interface configured, its ports are in essence firewalled from other VLANs.

To access a list of AOS or XOS devices that have router interfaces defined for a VLAN, click on the **IP Router** icon underneath the desired VLAN in the Tree, as shown below. If the selected VLAN contains both AOS and XOS devices, then both an AOS and XOS IP Routing Tab is available for selection.

Note: On 7000/8000 (Release 5.1.6) and 9000 (Release 6.1.1) series switches, you can configure up to eight (8) IP router interfaces and one (1) IPX router interface per VLAN.

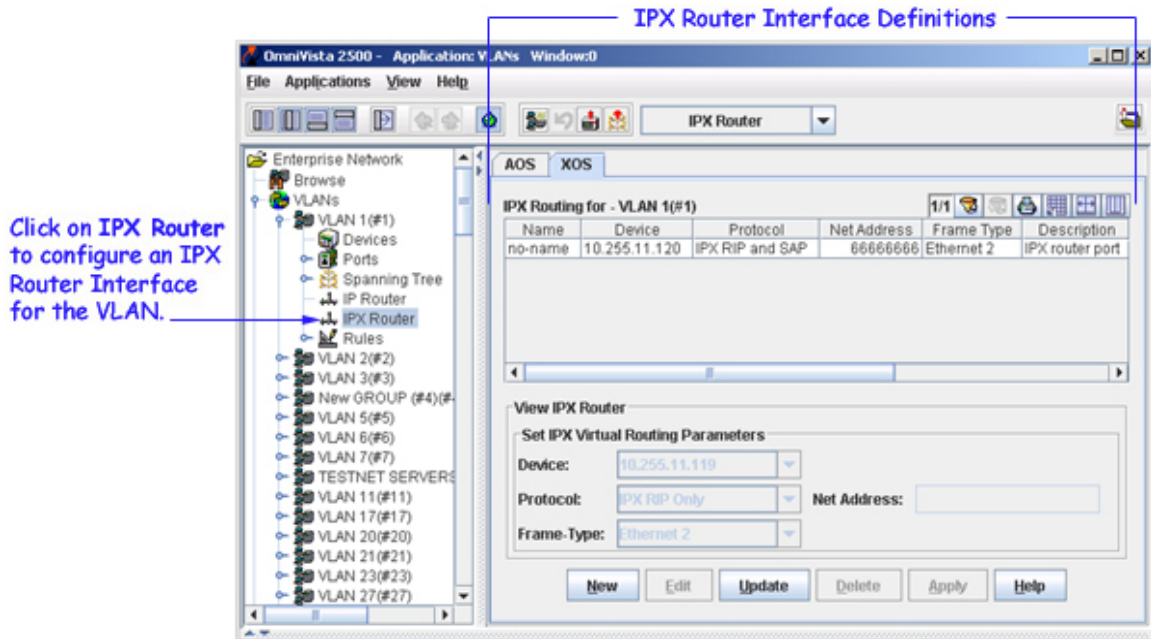
Click [here](#) for information about using the AOS IP Routing Tab to manage and configure an IP router interface for an AOS device. Click [here](#) for information about using the XOS IP Routing Tab to manage and configure an IP router interface for an XOS device.



To access a list of AOS or XOS devices that have IPX router interfaces defined for a VLAN, click on the **IPX Router** icon underneath the desired VLAN in the Tree, as shown below. If the selected VLAN contains both AOS and XOS devices, then both an AOS and XOS IPX Routing Tabs are available for selection.

Note: IPX routing is not supported on OmniSwitch 6600 series switches.

Click [here](#) for information about using the AOS IPX Routing Tab to manage and configure an IPX router interface for an AOS device. Click [here](#) for information about using the XOS IPX Routing Tab to manage and configure an IPX router interface for an XOS device.



AOS IP Routing Tab

The AOS IP Routing tab provides a list of all AOS devices that have an IP router interface defined for the VLAN. In addition to the device name and IP address, each list entry contains fields that display the current values of related IP router interface parameters. The AOS IP Routing Tab also enables you to add, modify, or delete an IP router interface definition for a specific device. These tasks and IP router interface parameter definitions are described below.

Note: On 7000/8000 (Release 5.1.6) and 6800/6850/9000 (Release 6.1.1) series switches, you can configure up to eight (8) IP router interfaces on the switch for each VLAN. On 6600, and XOS devices, you can configure one (1) IP router interface on the switch for each VLAN.

AOS IP Router Interface Definitions

The screenshot shows the 'AOS IP Router Interface Definitions' window. The left pane shows a tree view with 'IP Router' selected under 'VLAN 1 (#1)'. The main pane displays a table of IP router interface definitions for VLAN 1 (#1). Below the table is a 'View IP Router' panel with fields for Device, Router IP Address, Router IP Mask, IP Encapsulation, and IP Forwarding, along with buttons for New, Edit, Update, Delete, Apply, and Help.

Name	Device	Router IP Address	Router IP Mask	IP Encapsulation
NMS_HAWK_102	10.255.11.102	102.102.102.102	255.255.255.0	Ethernet 2
wTarget	10.255.11.104	10.255.11.104	255.255.255.0	Ethernet 2
HAWK_113	10.255.11.113	10.255.11.113	255.255.255.0	Ethernet 2
HAWK_114	10.255.11.114	10.255.11.114	255.255.255.0	Ethernet 2
HAWK_115	10.255.11.115	10.255.11.115	255.255.255.0	Ethernet 2
HAWK_116	10.255.11.116	10.255.11.116	255.255.255.0	Ethernet 2
HAWK_117	10.255.11.117	10.255.11.117	255.255.255.0	Ethernet 2
HAWK_118	10.255.11.118	10.255.11.118	255.255.255.0	Ethernet 2

View IP Router

Set IP Virtual Routing Parameters

Device: 10.255.10.3

Router IP Address: Router IP Mask:

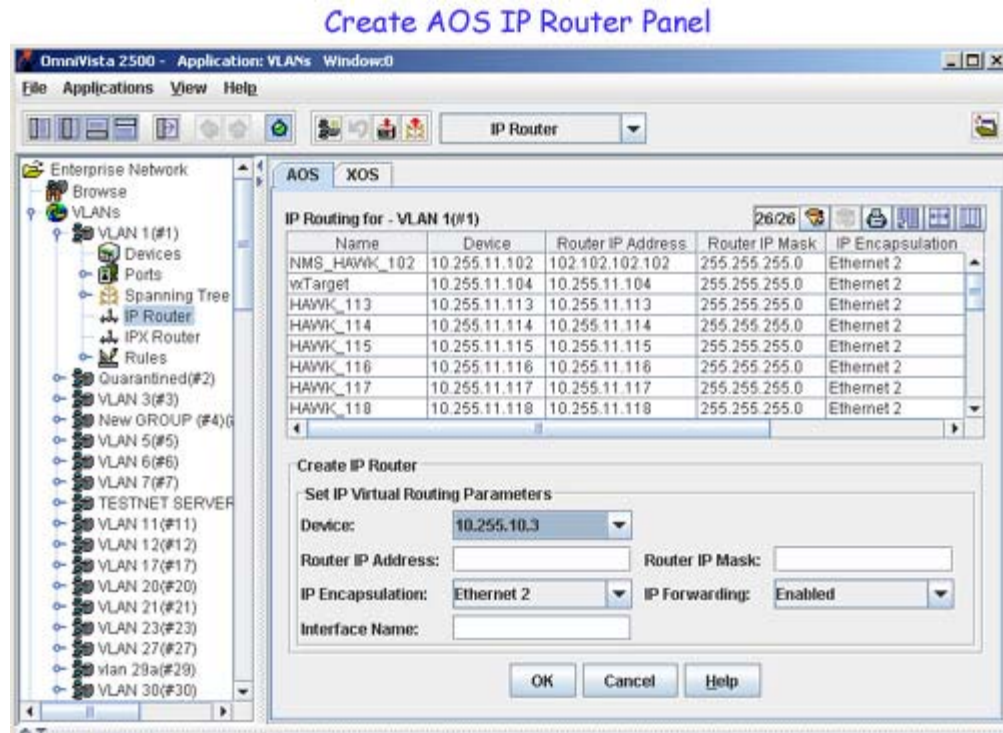
IP Encapsulation: Ethernet 2 IP Forwarding: Enabled

Interface Name:

New Edit Update Delete Apply Help

Defining an IP Router Interface

To define an IP router interface for the VLAN on a specific device, click the **New** button at the bottom of the AOS IP Routing Tab. This activates the Create IP Router panel, as shown below.



Follow the steps below to define an IP router interface using the Create IP Router panel.

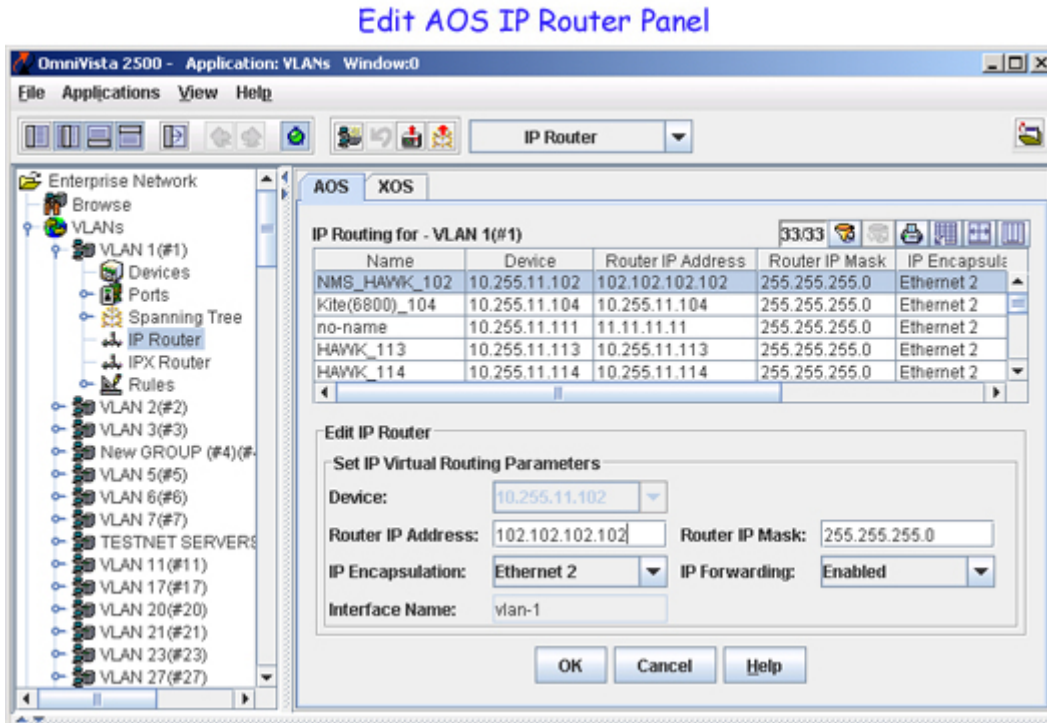
1. Select a device from the **Device** field list (e.g., 242).
2. Enter an IP address in the **Router IP Address** field (e.g., 198.181.10.2). This address is assigned to the IP router interface. The router interface IP address must be unique. You cannot have two router interfaces with the same IP address.
3. Tab to or click on the **Router IP Mask** field and a default subnet mask value for the IP address class is automatically entered in this field. It is only necessary to change this field value if you want to use a different subnet mask.
4. Select the router interface encapsulation from the **IP Encapsulation** field list.
5. Select the router interface forwarding status from the **IP Forwarding** field list.
6. Enter a unique interface name (text string up to 20 characters) in the **Interface Name** field.
7. Click on the **OK** button to accept the parameter values you have defined. The Create IP Router panel will close, returning you to the AOS IP Routing Tab list. A new entry now appears in this list for the IP router interface you just defined for the selected device. This entry contains an add icon in the Name field for the device.

Note: To configure additional router interfaces for the VLAN, click on the **New** button and repeat Steps 1 through 6 before proceeding to Step 7 (Release 5.1.6, 7000 and 8000 devices. Release 6.1.1, 9000 devices).

8. When you are done configuring router interfaces, click on the **Apply** button at the bottom of the AOS IP Routing Tab to update the device with the new IP router interface definition(s).

Modifying IP Router Interface Parameters

To modify IP router interface parameter values, select a router interface entry from the AOS IP Routing Tab list and click the **Edit** button. This activates the Edit IP Router panel, as shown below.



Make the desired parameter changes and click the **OK** button to return to the AOS IP Routing Tab list. A modify icon appears in the Name field for the modified router interface entry. Click the **Apply** button to update the IP router interface device with the new parameter values.

Removing an IP Router Interface

To remove an IP router interface from a VLAN, select a router interface entry from the AOS IP Routing Tab list and click the **Delete** button. A delete icon appears in the Name field of the selected entry. Click the **Apply** button to remove the VLAN router interface from the selected device configuration.

IP Router Interface Parameter Definitions

Note that changing any of the configurable router interface parameters could affect how traffic is routed for this instance of the VLAN on the selected device.

Name

The user-defined name for the switch.

Device

The IP host address that identifies the switch within the management IP network. It is not the same IP host address defined as an IP router interface for the selected VLAN, unless the VLAN is part of the management network. In addition, an IP host address appears in this field even if an IP router interface does not exist for the VLAN on that particular switch.

Router IP Address

The IP host address that identifies the router interface network.

Router IP Mask

The IP subnet mask value. The default value for this field is based on which network class range the IP address falls within; Class A, B, or C. (255.0.0.0, 255.255.0.0, or 255.255.255.0).

IP Encapsulation

The IP router interface frame encapsulation value; Ethernet 2 or SNAP. The frame encapsulation determines the framing type the router interface uses when generating frames that are forwarded out VLAN ports. Select an encapsulation that matches the encapsulation of the majority of IP VLAN traffic. By default, this parameter is set to Ethernet 2.

IP Forwarding

The router interface forwarding status: Enabled or Disabled. A forwarding router interface sends IP frames to other subnets. A "no forwarding" router interface acts as a host only; receives IP frames from other router interfaces. By default, this parameter is set to Enabled.

Interface Name

The user-defined interface name.

XOS IP Routing Tab

The XOS IP Routing Tab provides a list of all XOS devices that have an IP router interface defined for the VLAN. In addition to the device name and IP address, each list entry contains fields that display the current values of related IP router interface parameters. The XOS IP Routing Tab also enables you to add, modify, or delete an IP router interface definition for a specific device. These tasks and IP router interface parameter definitions are described below.

Note: On XOS devices, you can configure one (1) IP router interface on the switch for each VLAN.

XOS IP Router Interface Definitions

IP Routing for - VLAN 1(#1)

Name	Device	Protocol	IP Address	IP Mask	Broadcast Address	D
nms-test-103	10.255.11.103	ipRip	10.255.11.103	255.255.0.0	10.255.255.255	GROUP #
no-name-119x	10.255.11.119	ipRip	10.255.11.119	255.255.255.0	10.255.11.255	GROUP #
no-name	10.255.11.120	ipRip	10.255.11.120	255.255.255.0	10.255.11.255	GROUP #
no-name	10.255.11.124	ipRip	10.255.11.124	255.255.255.0	10.255.11.255	GROUP #
NMS-test-148	10.255.11.148	ipRip	10.255.11.148	255.255.255.0	10.255.11.255	GROUP #
OSR-5slot	10.255.11.153	ipRip	10.255.11.153	255.255.255.0	10.255.11.255	GROUP #
no-name	10.255.11.160	ipRip	10.255.11.160	255.255.255.0	10.255.11.255	GROUP #

View IP Router

Set IP Virtual Routing Parameters

Device:

Protocol: IP Address:

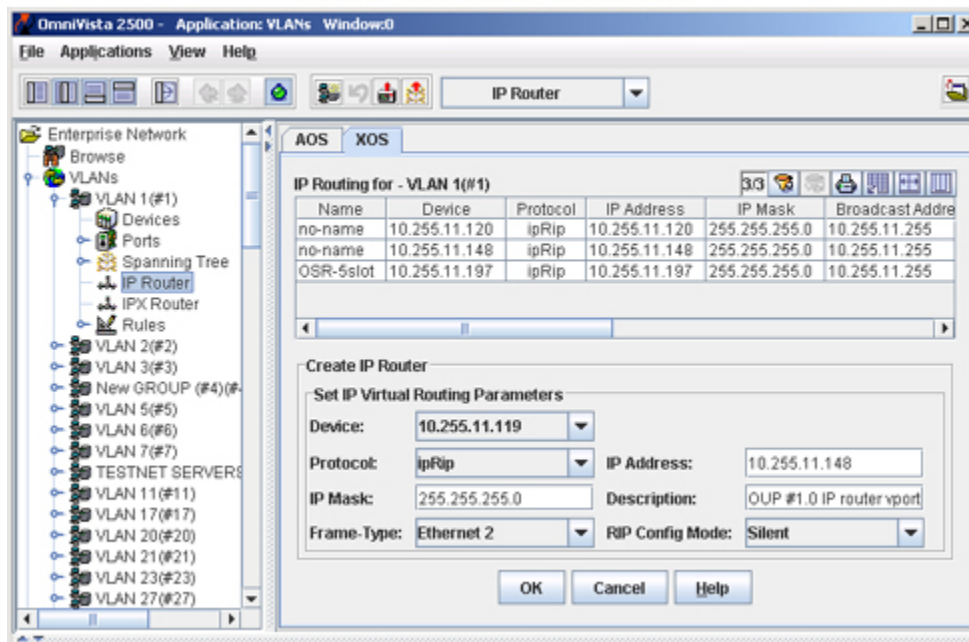
IP Mask: Description:

Frame-Type: RIP Config Mode:

Defining an IP Router Interface

To define an IP router interface for the VLAN on a specific device, click the **New** button found at the bottom of the XOS IP Routing Tab. This activates the Create IP Router panel, as shown below.

Create XOS IP Router Panel

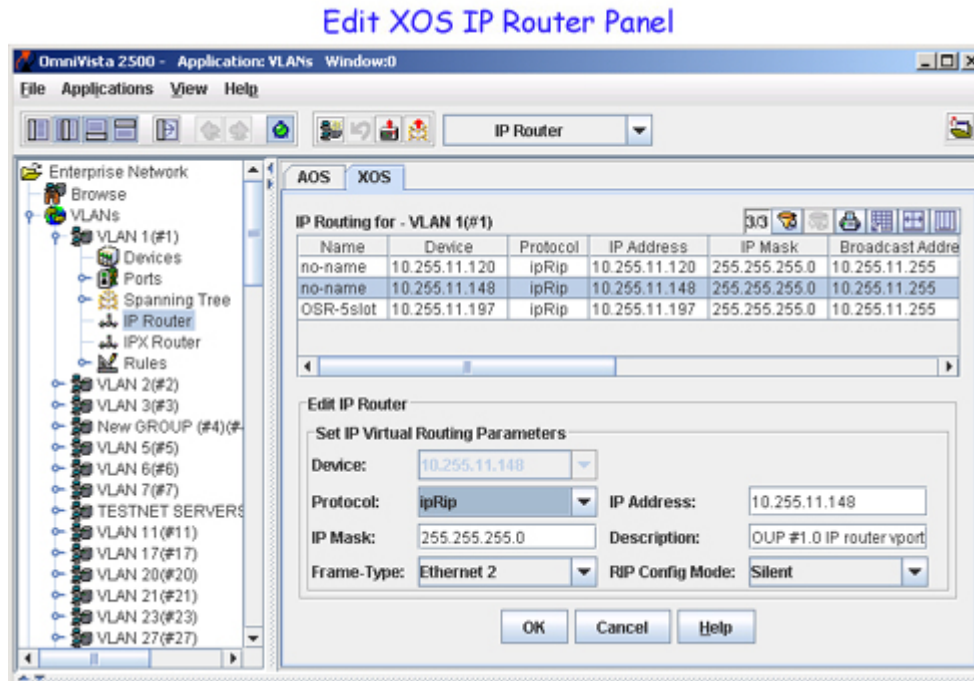


Follow the steps below to define an IP router interface using the Create IP Router panel:

1. Select a device from the **Device** field list. Note that you can only define an IP router interface on a device that does not already have a router interface defined for this VLAN.
2. Select a protocol from the **Protocol** field list. In most cases, the default value of **ipRip** is sufficient.
3. Enter a router IP address in the **IP Address** field (e.g., 198.181.10.2). This address is assigned to the IP router interface and enables routing of VLAN traffic on that device.
4. Tab to or click on the **IP Mask** field and a default subnet mask value for the IP address class is automatically entered in this field. It is only necessary to change this field value if you want to use a different subnet mask.
5. Enter an optional alphanumeric router interface description (up to 30 characters) in the **Description** field.
6. Select the router interface encapsulation from the **Frame Type** field list. By default, the encapsulation is set to Ethernet 2.
7. Select the RIP operational mode from the **RIP Config Mode** field list. By default, the RIP mode is set to Silent (RIP listens for routing updates, but does not send them).
8. Click on the **OK** button to accept the parameter values you have defined. The Create Router IP panel will close, returning you to the XOS IP Routing Tab list. A new entry now appears in this list for the IP router interface you just defined for the selected device. This entry contains an add icon in the Name field for the device.
9. Click on the **Apply** button at the bottom of the XOS IP Routing Tab to update the device with the new IP router interface definition.

Modifying IP Router Interface Parameters

To modify IP router interface parameter values, select a router interface entry from the XOS IP Routing Tab list and click the **Edit** button. This activates the Edit IP Router panel, as shown below.



Make the desired parameter changes and click the **OK** button to return to the XOS IP Routing Tab list. A modify icon appears in the Name field for the modified router interface entry. Click the **Apply** button to update the IP router interface device with the new parameter values.

Removing an IP Router Interface

To remove an IP router interface for the VLAN from a specific device, select a router interface entry from the XOS IP Routing Tab list and click the **Delete** button. A delete icon appears in the Name field of the selected entry. Click the **Apply** button to remove the VLAN router interface from the selected device configuration.

IP Router Interface Parameter Definitions

Note that changing any of the configurable router interface parameters could affect how traffic is routed for this instance of the VLAN on the selected device.

Name

The user-defined name for the switch.

Device

The IP host address that identifies the switch within the management IP network. It is not the same IP host address defined as an IP router interface for the selected VLAN, unless the VLAN is part of the management network. In addition, an IP host address appears in this field even if an IP router interface does not exist for the VLAN on that particular switch.

Protocol

The IP router interface protocol. This parameter value is not configurable on all XOS devices. In most cases, the default value of **IpRip** is sufficient. Consult the IP routing software and configuration you are running before attempting to change this parameter value.

IP Address

The IP host address value that identifies the router interface network.

IP Mask

The IP subnet mask value. The default value for this field is based on the default network class range of the IP address assigned to the router interface; class A, B, or C (255.0.0.0, 255.255.0.0, or 255.255.255.0).

Broadcast Address

The default broadcast address value. The default value for this field is based on the default network class range of the IP address assigned to the router interface. For example, a class A IP address, such as 10.0.0.2, has a default broadcast address of 10.255.255.255. A class C address, such as 198.181.10.2, has a default broadcast address of 198.181.10.255.

Description

An optional alphanumeric description (up to 30 characters) assigned to the router interface instance.

Admin Status

Enabled indicates that an IP router interface has been configured. "Admin Status" is an internal parameter passed to the switch for creating an IP router interface. It is not configurable.

Oper Status

The operational status of the router interface; **Active** or **Inactive**. An IP router interface is not operationally active until at least one active switch port is assigned to the VLAN. This is not a configurable parameter; switch software automatically determines the operational status of the VLAN and router interface.

Frame Type

The IP router interface frame encapsulation value. The frame encapsulation determines the framing type the router interface uses when generating frames that are forwarded out VLAN ports. Select an encapsulation that matches the encapsulation of the majority of IP VLAN traffic. You can set the frame type encapsulation to one of the following values:

- Ethernet 2
- Ethernet 802.3 (SNAP)
- FDDI
- Token Ring (802.5)
- Token Ring Source Routed
- ATM 1483.

By default, this parameter is set to **Ethernet 2** when the router interface is defined. If the encapsulation used by a VLAN device does not match the router interface frame type, then device frames are translated before they are forwarded on by the router interface to the appropriate subnet.

RIP Config Mode

The RIP operational mode for the router interface. You can set the RIP Config Mode to one of the following values:

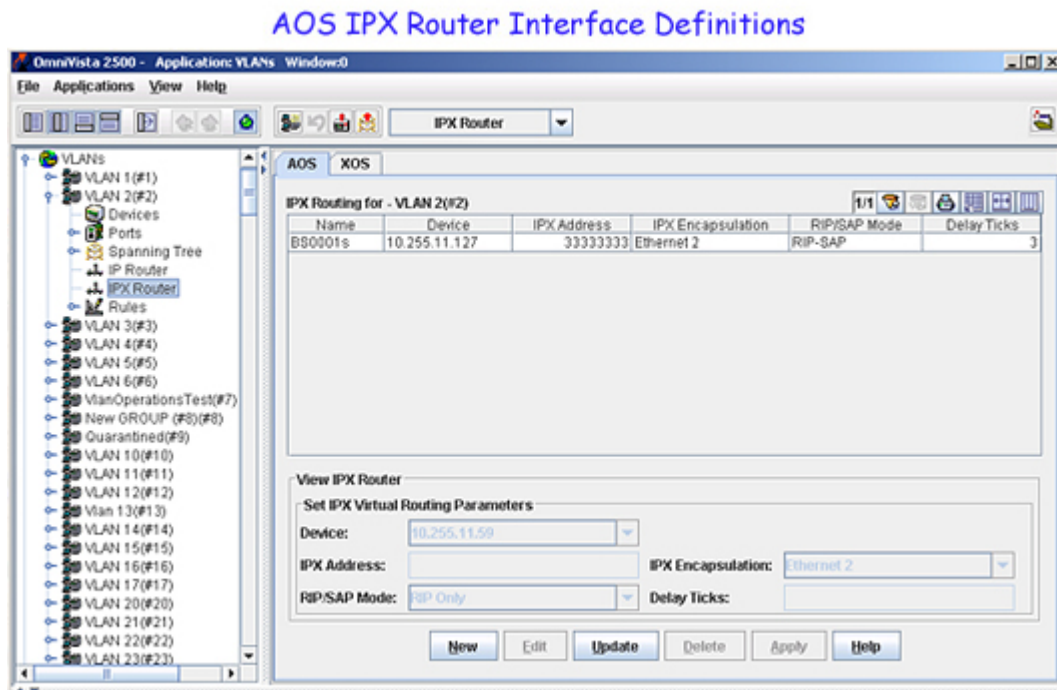
- **Silent.** The default setting shown in parentheses. RIP is active and receives routing information from other VLANs, but does not send out RIP updates. Other VLANs will not receive routing information concerning this VLAN and will not include the VLAN in their routing tables.
- **Deaf.** RIP is active and sends routing information to other VLANs, but does not receive RIP updates from other VLANs. The VLAN will not receive routing information from other VLANs and will not include other VLANs in its routing table.
- **Active.** RIP is active and both sends and receives RIP updates. The VLAN will receive routing information from other VLANs and other VLANs will include this VLAN in their routing tables.
- **Inactive.** RIP is inactive and neither sends nor receives RIP updates. The VLAN will neither send nor receive routing information to/from other VLANs.

By default, this parameter value is set to **Silent** when the router interface is defined.

AOS IPX Routing Tab

The AOS IPX Routing Tab provides a list of all AOS devices that have an IPX router interface defined for the VLAN. In addition to the device name and IP address, each list entry contains fields that display the current values of related IPX router interface parameters. The AOS IPX Routing Tab also enables you to add, modify, or delete an IPX router interface definition for a specific device. These tasks and IPX router interface parameter definitions are described below.

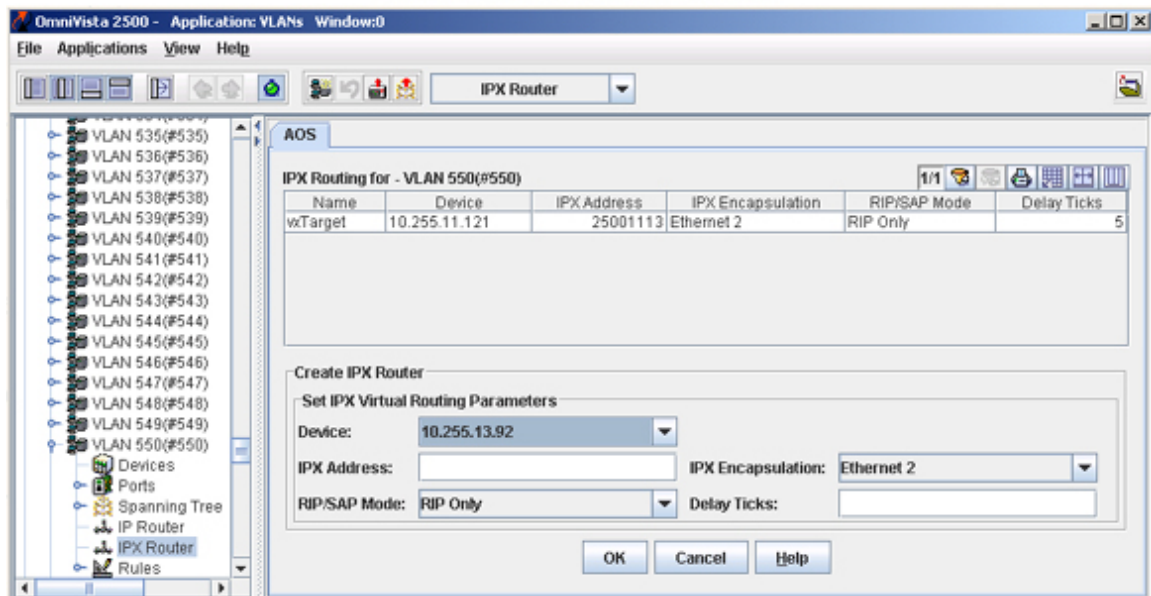
Note: On 6800/6850/7000/8000/9000 series switches, you can configure one (1) IPX router interface on the switch for each VLAN.



Defining an IPX Router Interface

To define an IPX router interface for the VLAN on a specific device, click the **New** button at the bottom of the AOS IPX Routing Tab. This activates the Create IPX Router panel, as shown below.

Create AOS IPX Router Panel



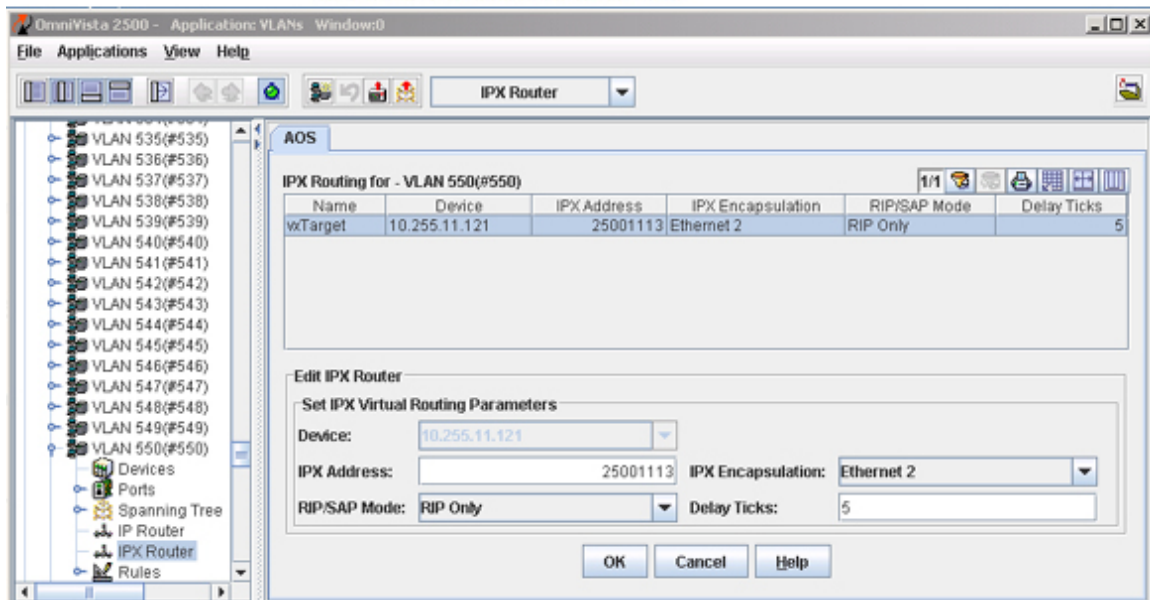
Follow the steps below to define an IPX router interface using the Create IPX Router panel:

1. Select a device from the **Device** field list. Note that you can only define an IPX router on a device that does not already have an IPX router defined for the selected VLAN.
2. Enter an IPX address in the **IPX Address** field. This address is assigned to the IPX router interface and enables routing of VLAN traffic on that device.
3. Select the router interface encapsulation from the **IPX Encapsulation** field list.
4. Select the router interface advertisement mode from the **RIP/SAP Mode** field list.
5. Enter the number of ticks (0-65535) in the **Delay Ticks** field to specify the IPX delay time. A tick is approximately 1/18th of a second.
6. Click on the **OK** button to accept the parameter values you have defined. The Create Router IPX panel will close, returning you to the AOS IPX Routing Tab list. A new entry now appears in this list for the IPX router interface you just defined for the selected device. This entry contains an add icon in the Name field for the device.
7. Click on the **Apply** button at the bottom of the AOS IPX Routing Tab to update the device with the new IPX router interface definition.

Modifying IPX Router Interface Parameters

To modify IPX router interface parameter values, select a router interface entry from the AOS IPX Routing Tab list and click the **Edit** button. This activates the Edit IPX Router panel, as shown below.

Edit AOS IPX Router Panel



Make the desired parameter changes and click the **OK** button to return to the AOS IPX Routing Tab list. A modify icon appears in the Name field for the modified router interface entry. Click the **Apply** button to update the IPX router interface device with the new parameter values.

Removing an IPX Router Interface

To remove an IPX router interface for the VLAN from a specific device, select a router interface entry from the AOS IPX Routing Tab list and click the **Delete** button. A delete icon appears in the Name field of the selected entry. Click the **Apply** button to remove the VLAN router interface from the selected device configuration.

IPX Router Interface Parameter Definitions

Note that changing any of the configurable router interface parameters could affect how traffic is routed for this instance of the VLAN on the selected device.

Name

The user-defined name for the switch.

Device

The IP host address that identifies the switch within the management IP network. It is not the same IP host address defined as an IP router interface for the selected VLAN, unless the VLAN is part of the management network. In addition, an IP host address appears in this field even if an IP router interface does not exist for the VLAN on that particular switch.

IPX Address

The IPX network address that identifies the router interface network. An IPX network address consists of eight hex characters (e.g., 4001690D).

IPX Encapsulation

The IPX router interface frame encapsulation value. The encapsulation determines the framing type the router interface uses when generating frames that are forwarded out VLAN ports. Use an encapsulation value that matches the encapsulation of the majority of IPX VLAN traffic. You can set the frame type encapsulation to one of the following values:

- Ethernet 2
- Novell Raw (802.3)
- LLC (802.2)
- SNAP.

By default, this parameter is set to **Ethernet 2** when the router interface is defined. If the encapsulation used by a VLAN device does not match the router interface frame type, then device frames are translated before they are forwarded on by the router interface to the appropriate subnet.

RIP/SAP Mode

The IPX router interface advertisement mode. You can set this parameter to one of the following values:

- RIP Only (RIP updates are processed). This is the default setting.
- RIP-SAP (RIP and SAP updates are processed)
- Triggered (RIP and SAP updates are broadcast only when updates occur)
- Inactive (RIP and SAP updates are not processed, router interface remains active).

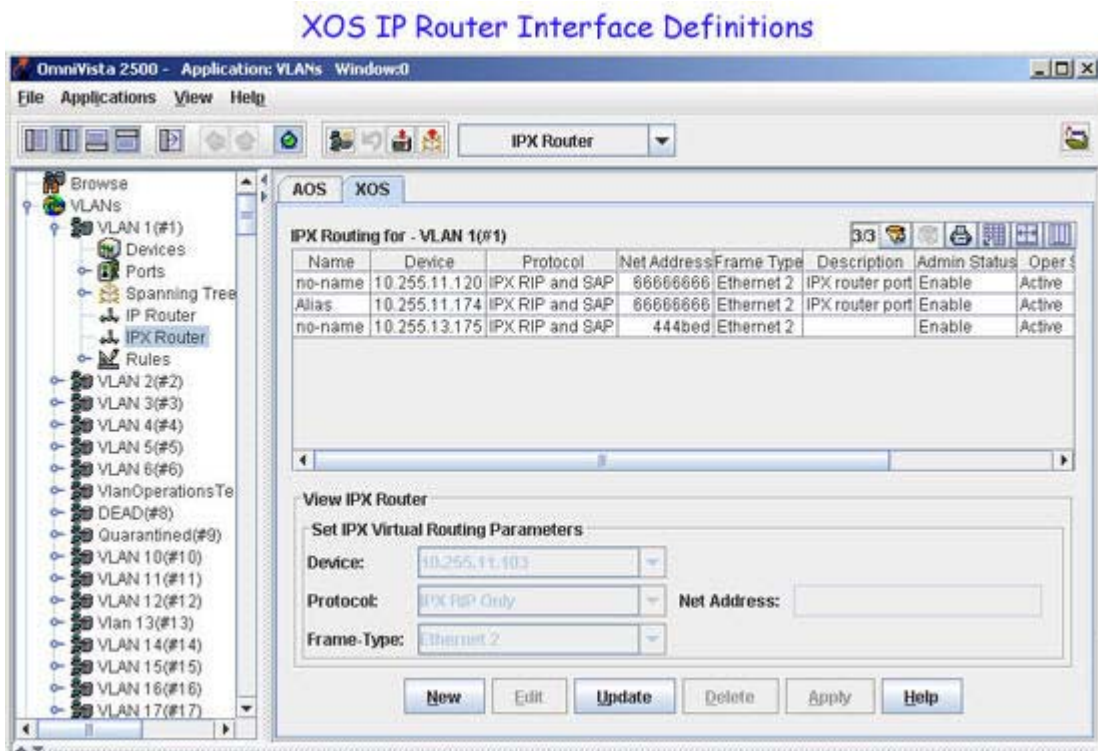
Delay Ticks

A 16-bit value (0-65535) that specifies the number of ticks for IPX delay time. A tick is approximately 1/18th of a second. By default, this parameter is set to **0**.

XOS IPX Routing Tab

The XOS IPX Routing Tab provides a list of all XOS devices that have an IPX router interface defined for the VLAN. In addition to the device name and IP address, each list entry contains fields that display the current values of related IPX router interface parameters. The XOS IPX Routing Tab also enables you to add, modify, or delete an IPX router interface definition for a specific device. These tasks and IPX router interface parameter definitions are described below.

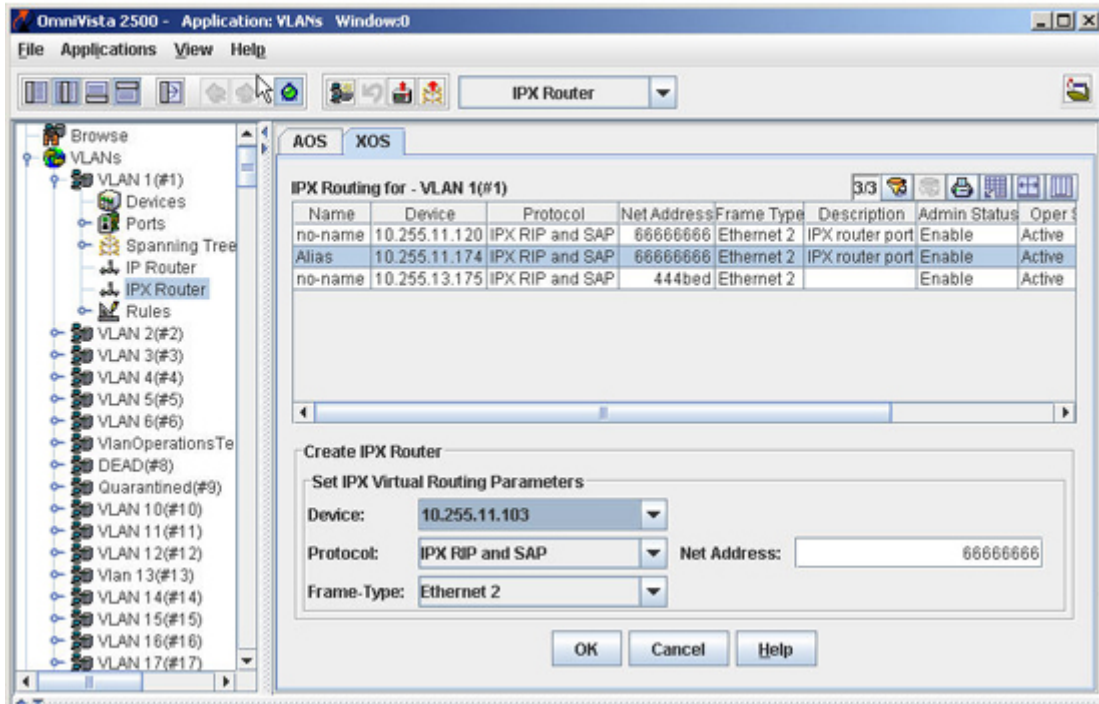
Note: On XOS devices, you can configure one (1) IPX router interface on the switch for each VLAN.



Defining an IPX Router Interface

To define an IPX router interface for the VLAN on a specific device, click the **New** button found at the bottom of the XOS IPX Routing Tab. This activates the Create IPX Router panel, as shown below.

Create XOS IPX Router Panel



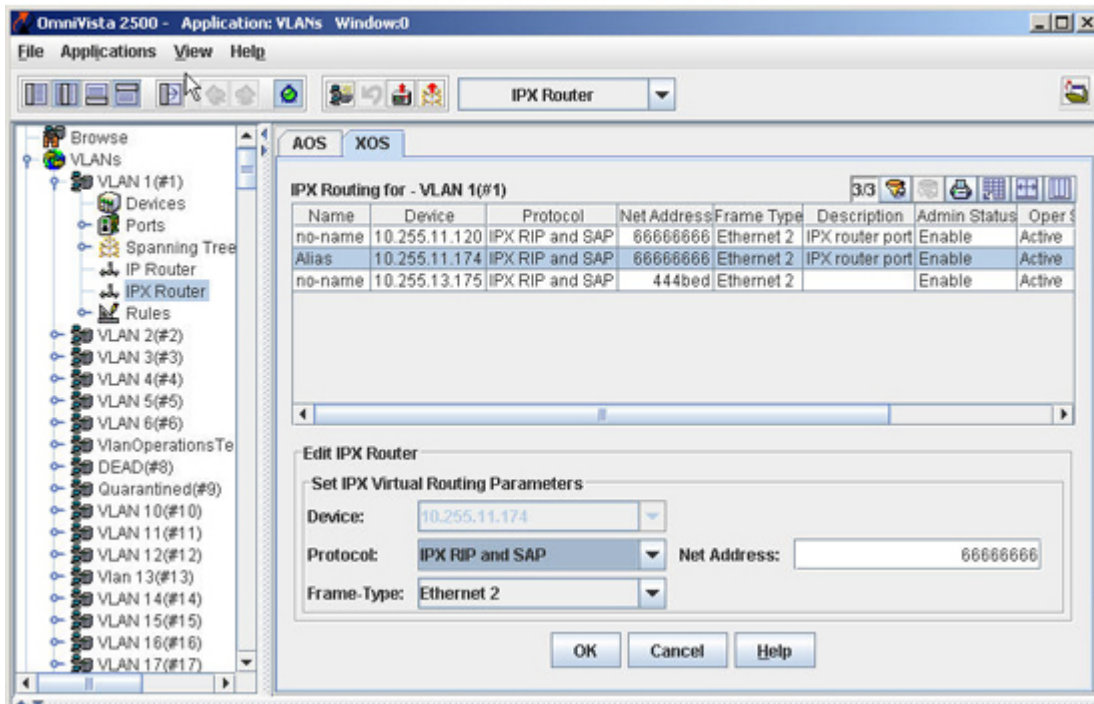
Follow the steps below to define an IPX router interface using the Create XOS IPX Router panel:

1. Select a device from the Device field list. Note that you can only define an IPX router on a device that does not already have an IPX router interface defined for the selected VLAN.
2. Select the router interface advertisement mode from the Protocol field list.
3. Enter an IPX address in the IPX Address field (e.g., 25001113). This address is assigned to the IPX router interface and enables routing of VLAN traffic on that device.
4. Select the router interface encapsulation from the Frame Type field list.
5. Click on the **OK** button to accept the parameter values you have defined. The Create Router IPX panel will close, returning you to the XOS IPX Routing Tab list. A new entry now appears in this list for the IPX router interface you just defined for the selected device. This entry contains an add icon in the Name field for the device.
6. Click on the **Apply** button at the bottom of the XOS IPX Routing Tab to update the device with the new IPX router interface definition.

Modifying IPX Router Interface Parameters

To modify IPX router interface parameter values, select a router interface entry from the XOS IPX Routing Tab list and click the **Edit** button. This activates the Edit IPX Router panel, as shown below.

Edit XOS IPX Router Panel



Make the desired parameter changes and click the **OK** button to return to the XOS IPX Routing Tab list. A modify icon appears in the Name field for the modified router interface entry. Click the **Apply** button to update the IPX router interface device with the new parameter values.

Removing an IPX Router Interface

To remove an IPX router interface for the VLAN from a specific device, select a router interface entry from the XOS IPX Routing Tab list and click the **Delete** button. A delete icon appears in the Name field of the selected entry. Click the **Apply** button to remove the VLAN router interface from the selected device configuration.

IPX Router Interface Parameter Definitions

Note that changing any of the configurable router interface parameters could affect how traffic is routed for this instance of the VLAN on the selected device.

Name

The user-defined name for the switch.

Device

The IP host address that identifies the switch within the management IP network. It is not the same IP host address defined as a IP router interface for the selected VLAN, unless the VLAN is part of the management network. In addition, an IP host address appears in this field even if an IP router interface does not exist for the VLAN on that particular switch.

Protocol

The IPX router interface advertisement mode. You can set this parameter to one of the following values:

- IPX RIP Only (RIP updates are processed)
- IPX RIP-SAP (RIP and SAP updates are processed)
- IPX Triggered (RIP and SAP updates are broadcast only when updates occur).

By default, this parameter is set to **IPX RIP Only**.

Net Address

The IPX network address that identifies the router interface network. An IPX network address consists of eight hex characters (e.g., 4001690D).

Frame Type

The IPX router interface frame encapsulation value. The encapsulation determines the framing type the router interface uses when generating frames that are forwarded out VLAN ports. Use an encapsulation value that matches the encapsulation of the majority of IPX VLAN traffic. You can set the frame type encapsulation to one of the following values:

- Ethernet 2
- Ethernet 802.3 LLC
- Ethernet 802.3 Raw
- FDDI-SNAP
- FDDI-SNAP-Source Routing
- FDDI-LLC
- FDDI-LLC-Source Routing
- Token Ring-SNAP
- Token Ring-SNAP-Source Routing
- Token Ring-LLC
- Token Ring-LLC-Source Routing.

By default, this parameter is set to **Ethernet 2** when the router interface is defined. If the encapsulation used by a VLAN device does not match the router interface frame type, then device frames are translated before they are forwarded on by the router interface to the appropriate subnet.

Description

An optional alphanumeric description (up to 30 characters) assigned to the router interface instance.

Admin Status

The administrative status for the router interface: **Enabled** or **Disabled**. If enabled, the router interface sends IPX frames to other networks. If disabled, the router interface acts as a host only; receives IPX frames from other router interfaces. By default, this parameter is set to **Enabled**.

Oper Status

The operational status of the router interface; **Active** or **Inactive**. An IPX router interface is not operationally active until at least one active switch port is assigned to the VLAN. This is not a configurable parameter; switch software automatically determines the operational status of the VLAN and router interface.

Source Route Type

If a Source Routing frame type was selected for the IPX router interface encapsulation, then this field contains one of the following types of Source Routing broadcasts.

- **ARE broadcasts.** All Routes Explorer. Broadcasts are transmitted over every possible path on inter-connected source-routed rings. This setting maximizes the generality of the broadcast.
- **STE broadcasts.** Spanning Tree Explorer. Broadcasts are transmitted only over Spanning Tree paths on inter-connected source-routed rings. This setting maximizes the efficiency of the broadcast.

Multiple IP Router Interfaces

On 7000/8000 (Release 5.1.6) and 6800/68509000 (Release 6.1.1) series switches, you can configure up to eight (8) IP router interfaces per switch per VLAN. These switches display an IP Interfaces icon in the Device Tree as shown below. On all other devices, you can configure one (1) IP router interface per switch per VLAN. Use the VLAN Tree view to configure IP router interfaces on other devices. Click here for more information on configuring router interfaces using the VLAN Tree view. Click here for information on configuring multiple IP Router Interfaces in the Device Tree view.

Note: You can also use the VLAN Tree to view and configure IP router interfaces on 6800/6850/7000/8000/9000 devices.

The screenshot shows the 'IP Router Interface Definitions' window in the OmniVista 2500 application. The window title is 'OmniVista 2500 - Application: VLANs Window:0'. The interface is divided into several sections:

- Tree View (Left):** Shows a hierarchy starting with 'Enterprise Network', followed by 'Browse', 'VLANs', and 'VLAN 1(#1)'. Under 'VLAN 1(#1)', there are icons for 'Devices', 'Ports', 'Spanning Tree', 'IP Router', and 'IPX Router'. A blue arrow points to the 'IPX Router' icon with the text: "Expand the tree under the device and click on the IP Interfaces Icon to display existing IP router interfaces."
- IP Router Interface Definitions (Top Right):** A blue box highlights this title and the 'IPX Router' dropdown menu.
- IPX Routing for - VLAN 1(#1) Table:**

Name	Device	Protocol	Net Address	Frame Type	Description
no-name	10.255.11.120	IPX RIP and SAP	66666666	Ethernet 2	IPX router port
- View IPX Router (Bottom):** Contains configuration fields:
 - Device: 10.255.11.119
 - Protocol: IPX RIP Only
 - Net Address: (empty field)
 - Frame Type: Ethernet 2
- Buttons (Bottom):** 'New', 'Edit', 'Update', 'Delete', 'Apply', and 'Help'.
 - A blue arrow points to the 'New' button with the text: "Click on New to create a new IP router interface."
 - A blue arrow points to the 'Update' button with the text: "Click on Update to refresh information in the IP Interfaces Table."

Defining VLAN Rules

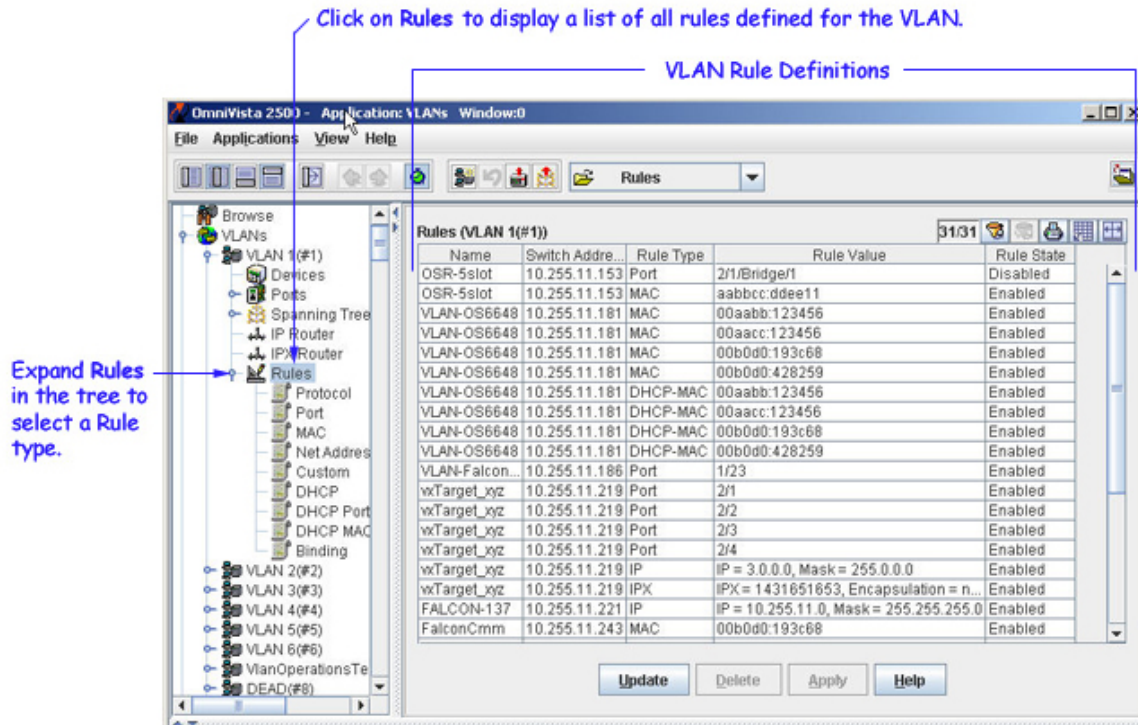
VLAN rules are used to classify mobile port traffic for dynamic VLAN port assignment. Rules are defined by specifying a port, MAC address, protocol, network address, custom (user-defined), DHCP generic, DHCP port, DHCP MAC address, or binding rule criteria to capture certain types of network device traffic. It is possible to define multiple rules for the same VLAN. A mobile port is assigned to a VLAN if its traffic matches any one of the rules defined for that VLAN.

In addition, there is a rule precedence that is followed if traffic received on a mobile port matches multiple rules defined on different VLANs. For example, if VLAN 10 has a MAC address rule and VLAN 20 has an IP address rule and a frame received on a mobile port contains a source MAC address and source IP address that matches both rules, the port is dynamically assigned to VLAN 10 because MAC address rules have a higher precedence over IP network address rules. [Click here for more information about rule precedence.](#)

On XOS platforms, ports become mobile when they are statically assigned to a VLAN that has mobility enabled. Rules to capture mobile port traffic are only defined on mobile VLANs. In addition to enabling mobility on the VLAN and defining VLAN rules, you must also enable the Group Mobility feature for the entire switch. [Click here for more information about configuring mobility on XOS devices.](#)

On AOS platforms, mobility is enabled on individual switch ports. VLANs do not have a mobile or non-mobile distinction and there is no overall switch setting to invoke the mobile port feature. As a result, you can define rules to capture mobile port traffic on any VLAN. [Click here for more information about configuring mobility on AOS devices.](#)

To access a list of all rules defined for a specific VLAN, click on the **Rules** icon underneath the desired VLAN in the Tree. This opens the VLAN Rules window, shown below, which contains a list of all devices that have rules defined for this VLAN in their configuration file. The VLAN Rules window list includes the type of rule defined, the value for that rule, and if the rule is administratively enabled or disabled (applies only to XOS devices).



To view, create, and/or delete an individual rule definition for a VLAN, click open the **Rules** icon underneath the desired VLAN and then click one of the rule type icons. This opens a VLAN Rules window, similar to the one shown above, that only displays any existing rule definitions for the selected rule type.

Copying a VLAN Rule

You can copy the definition of existing VLAN rule(s) from an AOS device and add the selected rule(s) to another AOS device(s) in the same VLAN. To copy the rule(s), right click the desired VLAN rule(s) in the VLAN Rules pane, and then select the **Copy Rule** option from the pop-up menu. This will launch the **Select Devices** dialog. After selecting the new device(s) for which you want to apply the copied VLAN rule(s), click **OK** in the **Select Devices** dialog.

Note: The following definitions of VLAN rules will not be copied:

1. The VLAN rules that are not supported on the target devices. For example, in OS 6800, the VLAN Mobility rules like Custom Rules, IP-MAC Binding Rules, IP-Port Binding Rules, and MAC-Port-Protocol are not supported.
2. The VLAN rules definitions involving slots/ports that do not exist in the target devices.

Note: You cannot copy VLAN rules from an XOS device.

Removing a VLAN Rule

To remove a VLAN rule definition, select one or more rule entries from the VLAN Rules window list and click the **Delete** button. A delete icon appears in the Name field of the selected entry. Click the **Apply** button to remove the VLAN rule from the device in the selected entry.

VLAN Rules Window Information Fields

Name

The user-defined name for the switch.

Switch Address

The IP host address that identifies the switch within the management IP network. It is not the same IP host address defined as a virtual IP router port for the selected VLAN, unless the VLAN is part of the management network. In addition, an IP host address appears in this field even if an IP virtual router port does not exist for the VLAN on that particular switch.

Rule Type

The type of rule defined. There are several types of configurable VLAN rules available for classifying different types of network device traffic and there is no limit to the number of rules allowed per VLAN. The type of rule defined determines the type of traffic that will trigger a dynamic mobile port assignment to the VLAN and the type of traffic the VLAN will forward within its domain.

Rule Value

The rule criteria that is compared to the contents of mobile port traffic. When mobile port traffic matches a VLAN rule, the port and its traffic are dynamically assigned to that VLAN.

Rule State

The administrative status of the rule; Enabled or Disabled. The value of this field only applies to XOS devices. As a result, this field will always display Enabled for AOS devices. If the rule state is set to disabled, then the rule is ignored by the XOS Group Mobility feature and not used to classify mobile port traffic.

Understanding VLAN Rule Precedence

In addition to configurable VLAN rule types, there are two internal rule types for processing mobile port frames. One is referred to as frame type and is used to identify Dynamic Host Configuration Protocol (DHCP) frames. The second internal rule is referred to as default and identifies frames that do not match any VLAN rules.

The VLAN rule precedence table, shown below, provides a list of all VLAN rules, including the two internal rules mentioned above, in the order of precedence switch software applies to classify mobile port frames. The first column lists the rule type names, the second and third columns describe how the switch handles frames that match or don't match rule criteria. The higher the rule is in the list, the higher its level of precedence.

When a frame is received on a mobile port, switch software starts with rule one in the rule precedence table and progresses down the list until there is a successful match between rule criteria and frame contents. The exception to this is if there is a binding rule violation. In this case, the frame is blocked and its source port is not assigned to the rule's VLAN.

Each binding rule type contains criteria that is used to determine if a mobile port frame qualifies for assignment to the binding rule VLAN, violates binding rule criteria, or is simply allowed on the port but not assigned to the rule's VLAN. For example, as indicated in the rule precedence table, a mobile port frame is compared to binding MAC-port rule criteria and processed as follows:

- If the frame's source MAC address matches the rule's MAC address, then the frame's port must also match the rule's port to qualify for assignment to the rule's VLAN.
- If the frame's source MAC matches but the frame's port does not match, then a violation occurs and the frame is blocked and the port is not assigned to the rule's VLAN. There is no further attempt to match this frame to rules of lower precedence.
- If the frame's source MAC does not match but the frame's port does match, the frame is allowed but the port is not assigned to the rule's VLAN. The frame is then compared to other rules of lower precedence in the table or carried on the mobile port's default VLAN (if the mobile port's default VLAN is enabled) if the frame does not match any other VLAN rules.

VLAN Rule Precedence Table

Precedence Step/Rule Type	Condition	Result
1. Frame Type	Frame is a DHCP frame.	Go to Step 2.
	Frame is not a DHCP frame.	Skip Steps 2, 3, 4, and 5.
2. DHCP MAC	DHCP frame contains a matching source MAC address.	Frame source is assigned to the rule's VLAN, but not learned.
3. DHCP MAC Range	DHCP frame contains a source MAC address that falls within a specified range of MAC addresses.	Frame source is assigned to the rule's VLAN, but not learned.
4. DHCP Port	DHCP frame matches the port specified in the rule.	Frame source is assigned to the rule's VLAN, but not learned.
5. DHCP Generic	DHCP frame.	Frame source is assigned to the rule's VLAN, but not learned.
6. MAC-Port-IP Address Binding	Frame contains a matching source MAC address, source port, and source IP subnet address.	Frame source is assigned to the rule's VLAN.
	Frame only contains a matching source MAC address; port and IP address do not match.	Frame is blocked; its source is not assigned to the rule's VLAN.
	Frame only contains a matching IP address; source MAC and port do not match.	Frame is blocked; its source is not assigned to the rule's VLAN.
	Frame only contains a matching port; source MAC and IP address do not match.	Frame is allowed; its source is not assigned to the rule's VLAN.
7. MAC-Port-Protocol Binding	Frame contains a matching source MAC address, source port, and protocol.	Frame source is assigned to the rule's VLAN.
	Frame only contains a matching source MAC address; port and protocol do not match.	Frame is blocked; its source is not assigned to the rule's VLAN.
	Frame only contains a matching port and/or protocol; source MAC address does not match.	Frame is allowed; its source is not assigned to the rule's VLAN.
8. MAC-Port Binding	Frame contains a matching source MAC address and source port.	Frame source is assigned to the rule's VLAN.
	Frame only contains a matching source MAC address; port does not match.	Frame is blocked; its source is not assigned to the rule's VLAN.
	Frame only contains a matching port; source MAC address does not match.	Frame is allowed; its source is not assigned to the rule's VLAN.
9. MAC-IP Address Binding	Frame contains a matching source MAC address and source IP subnet address.	Frame source is assigned to the rule's VLAN.
	Frame only contains a matching source MAC address; IP address does not match.	Frame is blocked; its source is not assigned to the rule's VLAN.
	Frame only contains a matching IP address; source MAC does not match.	Frame is blocked; its source is not assigned to the rule's VLAN.
10. Port-IP Address Binding	Frame contains a matching source port and source IP subnet address.	Frame source is assigned to the rule's VLAN.
	Frame only contains a matching source IP address; port does not match.	Frame is blocked; its source is not assigned to the rule's VLAN.
	Frame only contains a matching port; source IP address does not match.	Frame is allowed; its source is not assigned to the rule's VLAN.
11. Port-Protocol Binding	Frame contains a matching source port and protocol.	Frame source is assigned to the rule's VLAN.
	Frame only contains a matching source port; protocol does not match.	Frame is blocked; its source is not assigned to the rule's VLAN.
	Frame only contains a matching protocol; port does not match.	Frame is allowed; its source is not assigned to the rule's VLAN.
12. MAC Address	Frames contain a matching source MAC address.	Frame source is assigned to the rule's VLAN.
13. MAC Range	Frame contains a source MAC address that falls within a specified range of MAC addresses.	Frame source is assigned to the rule's VLAN.
14. Network Address	Frame contains a matching IP subnet address, or	Frame source is assigned to the rule's VLAN.
	Frame contains a matching IPX network address.	Frame source is assigned to the rule's VLAN.
15. Protocol	Frame contains a matching protocol type.	Frame source is assigned to the rule's VLAN.
16. Custom (User Defined)	Frames contain data that matches customized rule criteria.	Frame source is assigned to the rule's VLAN.
17. Default	Frame does not match any rules.	Frame source is assigned to mobile port's default VLAN.

Defining Protocol Rules

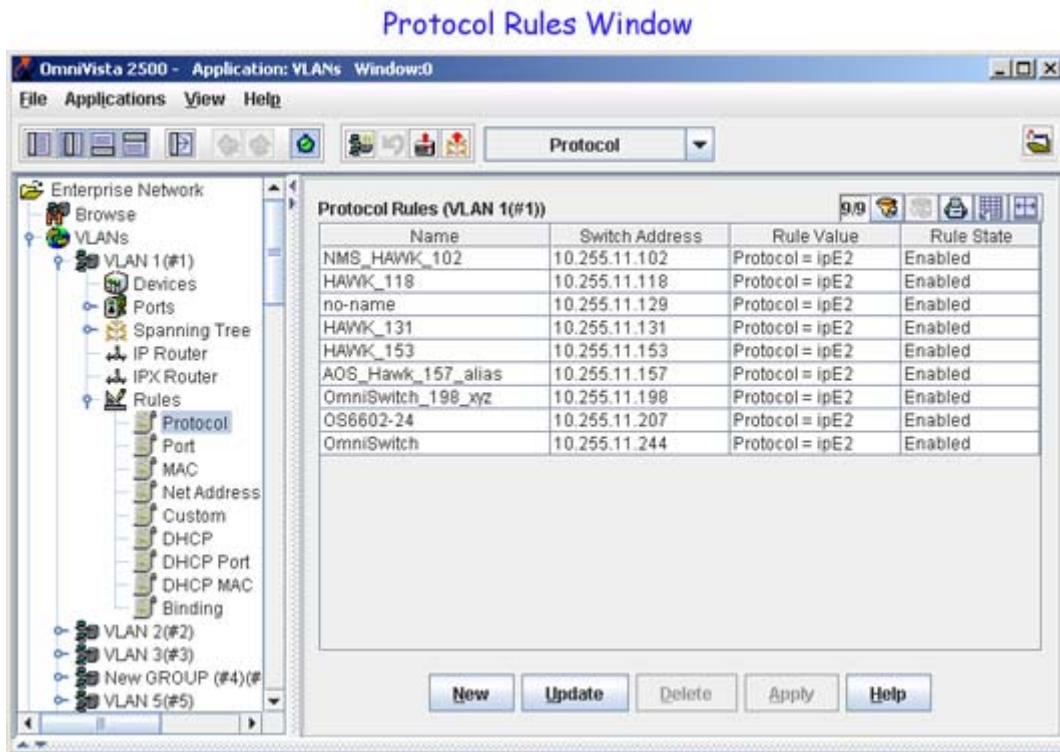
Protocol rules determine VLAN assignment based on the protocol a device uses to communicate. When defining this type of rule, there are several generic protocol values to select from: IP, IPX, AppleTalk, or DECNet. If none of these are sufficient, it is possible to specify an Ethernet type, Destination and Source Service Access Protocol (DSAP/SSAP) header values, or a Sub-network Access Protocol (SNAP) type.

Note: IPX routing is not supported on OmniSwitch 6600 series switches.

Consider the following when defining a VLAN protocol rule:

- IP protocol rules also capture DHCP traffic, if no other DHCP rule exists that would classify the DHCP traffic into another VLAN. Therefore, it is not necessary to combine DHCP rules with IP protocol rules for the same VLAN.
- Specifying a SNAP protocol type restricts classification of mobile port traffic to the ethertype value found in the IEEE 802.2 SNAP LLC frame header.
- If an attempt is made to define an Ethernet type rule with a value equal to a value already captured by one of the generic IP or IPX protocol rules, switch software may detect the duplication and not create the rule. It is recommended that you use the generic IP and/or IPX protocol rules, instead of specifying the same value using the Ethernet type rule.

The Protocol Rules window, shown below, contains a list of existing protocol rule definitions for the current VLAN. If this list is empty, there are no protocol rules defined for this VLAN.



To create a protocol rule definition for the current VLAN, click on the **New** button at the bottom of the Protocol Rules window. This activates the Add Protocol Rules pop-up window. Click here for information on how to define a protocol rule using this window.

Removing a Protocol Rule

To remove a protocol rule definition, select one or more rules from the Protocol Rules window list and click the **Delete** button. A delete icon appears in the Name field of the selected entry. Click the **Apply** button to remove the rule from the device in the selected entry.

Add Protocol Rules Window

The Add Protocol Rules pop-up window, shown below, is used to create a protocol rule definition for the current VLAN. This window displays when you click on the **New** button at the bottom of the Protocol Rules window.

Note: IPX routing is not supported on OmniSwitch 6600 series switches.



Follow the steps below to define a protocol rule using the Add Protocol Rules window:

1. Select one or more devices from the list located in the top half of the Add Protocol Rules window. Note that all devices are selected by default.
2. Click on one of the following protocol types displayed in this window:
 - IP (Ethernet II, ARP, and SNAP)
 - IP-SNAP (AOS only)
 - IPX (Ethernet II, Novell 802.3, LLC 802.2, and SNAP)
 - IPX-LLC (AOS only)
 - IPX-SNAP (AOS only)
 - IPX-Novell (AOS only)
 - AppleTalk (Data Delivery Protocol and AppleTalk ARP)
 - DECNet (DECNet Phase IV--only captures frames with 6003 Ethernet type)
 - Ethernet Type (A two byte hex value between 0x600 and 0xffff that defines an Ethernet type. This value is required for the Ethernet Type field when this protocol type is selected.)
 - SAP Header (A one byte hex value between 0x00 and 0xff that defines DSAP and SSAP header values. These values are required for the DSAP and SSAP fields when this protocol type is selected.)
 - SNAP Type (A two byte hex value between 0x600 and 0xffff that defines a Sub-network Access Protocol. This value is required for the SNAP Type field when this protocol type is selected.)

Note: When you select only XOS devices from the device list, the IPX-LLC, IPX-SNAP, and IPX-Novell buttons are grayed out because these rules are not supported on XOS devices. The IPX protocol rule on XOS devices captures LLC, SNAP, and Novell encapsulations without specifying a separate rule.

3. After selecting the desired protocol type and entering any additional required values, click on the **OK** button. The Add Protocol Rules window closes and a new protocol rule entry appears in the Protocol Rules window list with an add icon in the Name field of the new entry.

Note: When you click on the **OK** button in the Add Protocol Rules window, an error message window displays a list of management IP addresses for all XOS devices that do not have mobility enabled for the VLAN. You cannot configure VLAN rules for non-mobile VLANs on XOS devices.

4. Click the **Apply** button to create the protocol rule on all devices configured with the protocol rule VLAN.

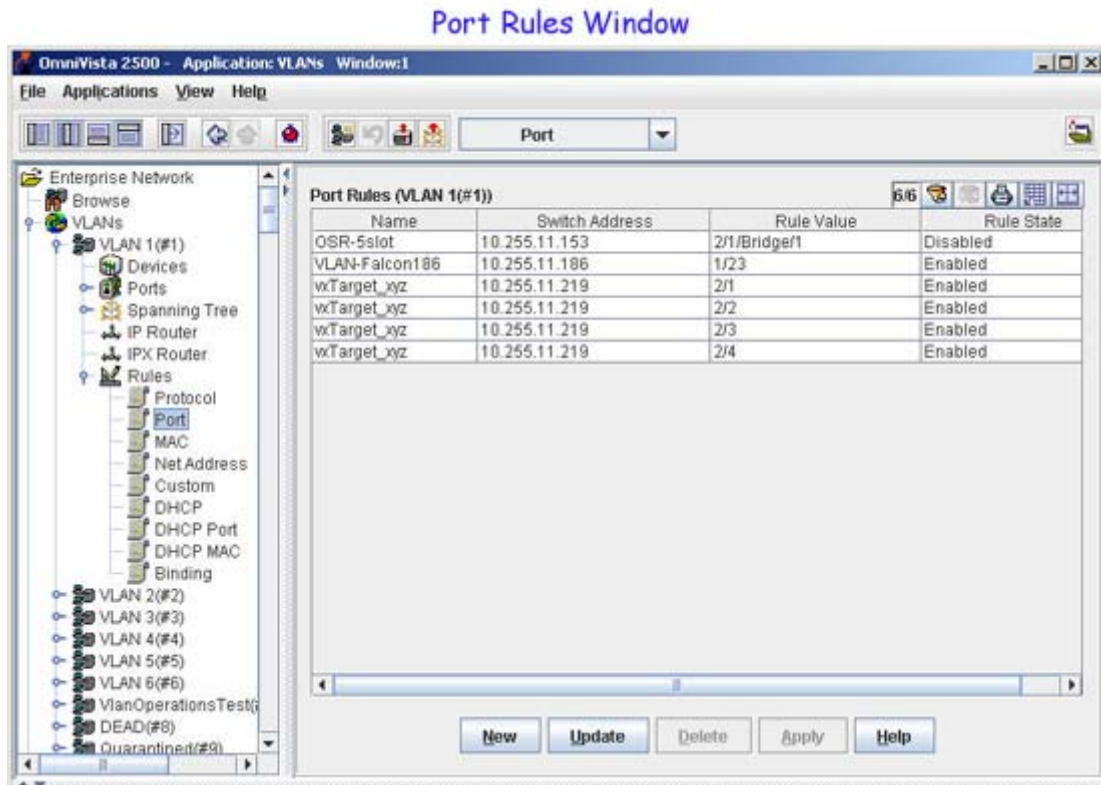
Defining Port Rules

Port rules are fundamentally different from all other supported rule types, in that traffic is not required to trigger dynamic assignment of the mobile port to a VLAN. As soon as this type of rule is created, the specified port is assigned to the VLAN only for the purpose of forwarding broadcast types of VLAN traffic to a device connected to that same port.

Consider the following when defining a VLAN port rule:

- Port rules are mostly used for silent devices, such as printers, that require VLAN membership to receive traffic forwarded from the VLAN. These devices usually do not send traffic, so they do not trigger dynamic assignment of their mobile ports to a VLAN.
- It is possible to specify the same port in more than one port rule defined for different VLANs. The advantage to this is that traffic from multiple VLANs is forwarded out the one mobile port to the silent device. For example, if port 3 on slot 2 is specified in a port rule defined for VLANs 255, 355, and 755, then outgoing traffic from all three of these VLANs is forwarded on port 2/3.
- Port rules only apply to outgoing mobile port traffic and do not classify incoming traffic. If a mobile port is specified in a port rule, its incoming traffic is still classified for VLAN assignment in the same manner as all other mobile port traffic.

The Port Rules window, shown below, contains a list of existing port rule definitions for the current VLAN. If this list is empty, there are no port rules defined for this VLAN.



To create a port rule definition for the current VLAN, click on the **New** button at the bottom of the Port Rules window. This activates the Add Port Rules popup window. Click [here](#) for information about how to define a port rule using this window.

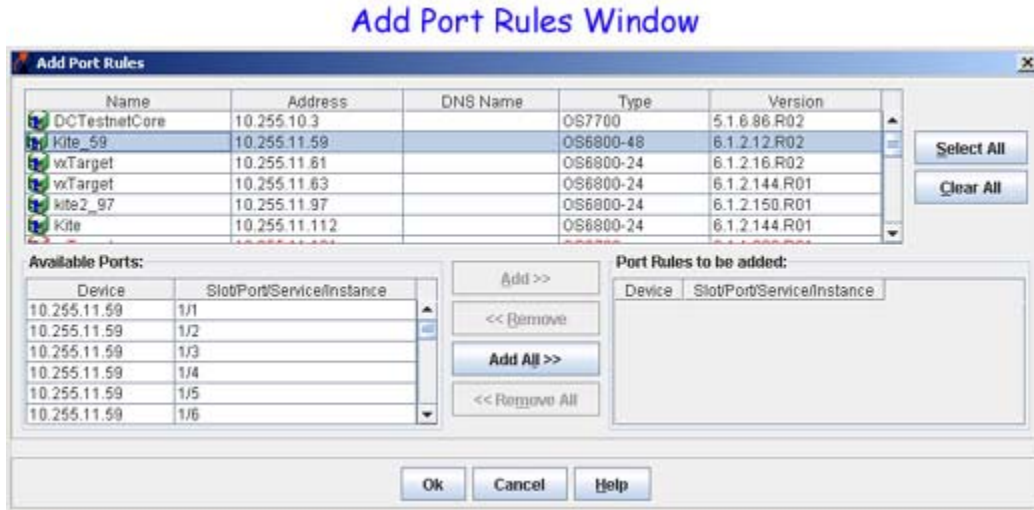
Removing a Port Rule

To remove a Port rule definition, select one or more rules from the Port Rules window list and click the **Delete** button. A delete icon appears in the Name field of the selected entry. Click the **Apply** button to remove the rule from the device in the selected entry.

Add Port Rules Window

The Add Port Rules pop-up window, shown below, is used to create a port rule definition for the current VLAN. This window displays when you click on the **New** button found at the bottom of the Port Rules window.

Note: When the Add Port Rules window opens, an error message window displays a list of management IP addresses for all XOS devices that do not have mobility enabled for the VLAN. You cannot configure VLAN rules for non-mobile VLANs on XOS devices.



The top half of the Add Port Rules window contains a list of VLAN devices. When you select one or more switches from this list, the Available Ports list in the bottom half of this window displays all ports that are eligible for port rule selection. Note that on some platforms (e.g., XOS), you can only specify active switch ports when defining a port rule.

To create a port rule definition for the current VLAN, select one or more switches and then the available ports that you want to specify for the rule and click the **OK** button. The Add Port Rules window closes and a new port rule entry appears in the Port Rules window list with an add icon in the Name field of the new entry. Click the **Apply** button to create the port rule on the selected devices.

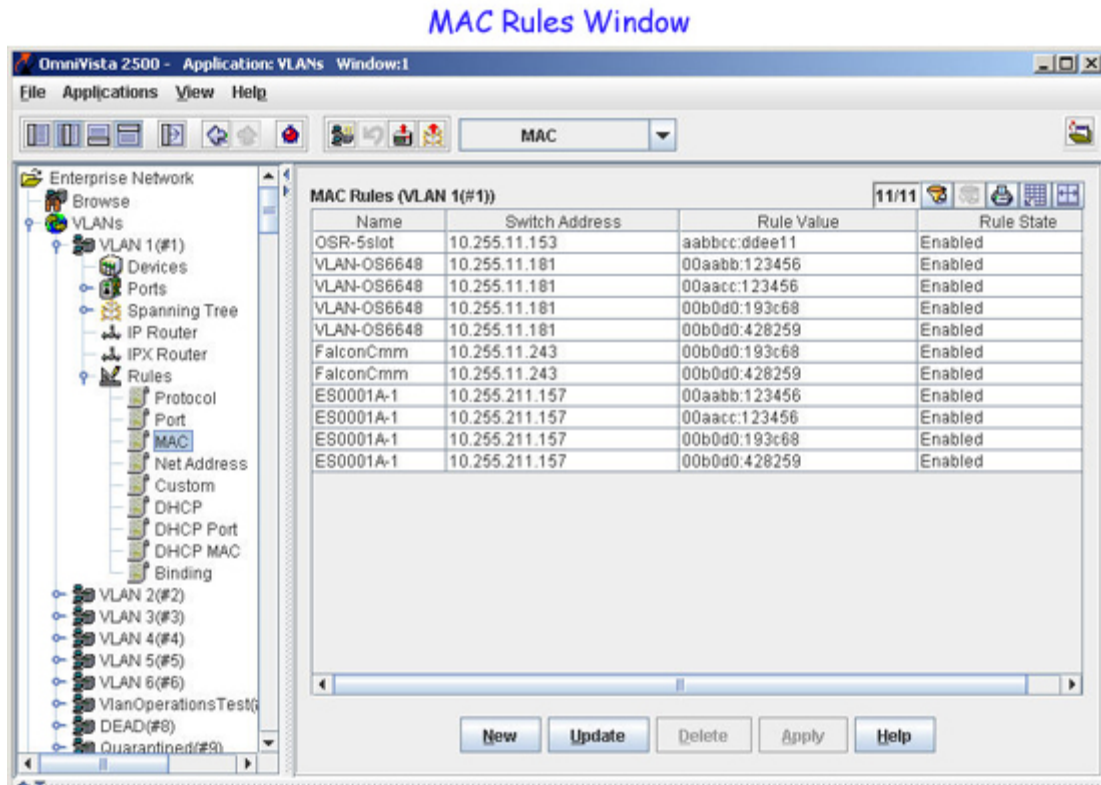
Defining MAC Address Rules

MAC address rules capture frames that contain a source MAC address that matches the MAC address specified in the rule. The mobile port that receives this matching traffic is dynamically assigned to the rule's VLAN.

Consider the following when defining a VLAN MAC address rule:

- A MAC address rule is the simplest type of rule and provides the maximum degree of control and security. Members of the VLAN will consist of devices with specific MAC addresses.
- It is possible to specify a range of MAC addresses, thus creating a MAC address range rule on the device. Frames that contain a source MAC address that matches the low or high end MAC or that falls within the range specified by the low and high end MAC trigger dynamic mobile port assignment to the rule's VLAN.
- Once a device joins a MAC address rule VLAN, it is not eligible to join multiple VLANs even if device traffic matches other VLAN rules.
- MAC address rules also capture DHCP traffic, if no other DHCP rule exists that would classify the DHCP traffic into another VLAN. Therefore, it is not necessary to combine DHCP rules with MAC address rules for the same VLAN.

The MAC Rules window, shown below, contains a list of existing MAC address rule definitions for the current VLAN. If this list is empty, there are no MAC address rules defined for this VLAN.



To create a MAC address rule definition for the current VLAN, click on the **New** button at the bottom of the MAC Rules window. This activates the Add MAC Rules pop-up window. Click [here](#) for information about how to define a MAC address rule using this window.

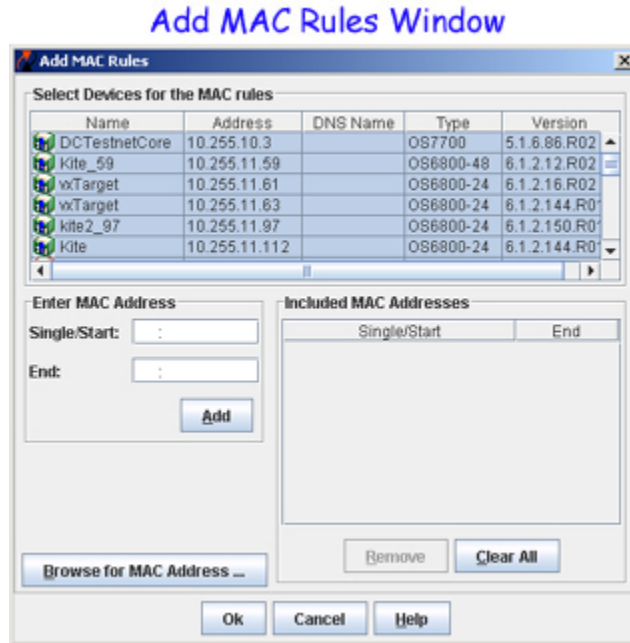
Removing a MAC Address Rule

To remove a MAC address rule definition, select one or more rules from the MAC Rules window list and click the **Delete** button. A delete icon appears in the Name field of the selected entry. Click the **Apply** button to remove the rule from the device in the selected entry.

Add MAC Rules Window

The Add MAC Rules pop-up window, shown below, is used to create a MAC address rule definition for the current VLAN. This window displays when you click on the **New** button at the bottom of the MAC Rules window.

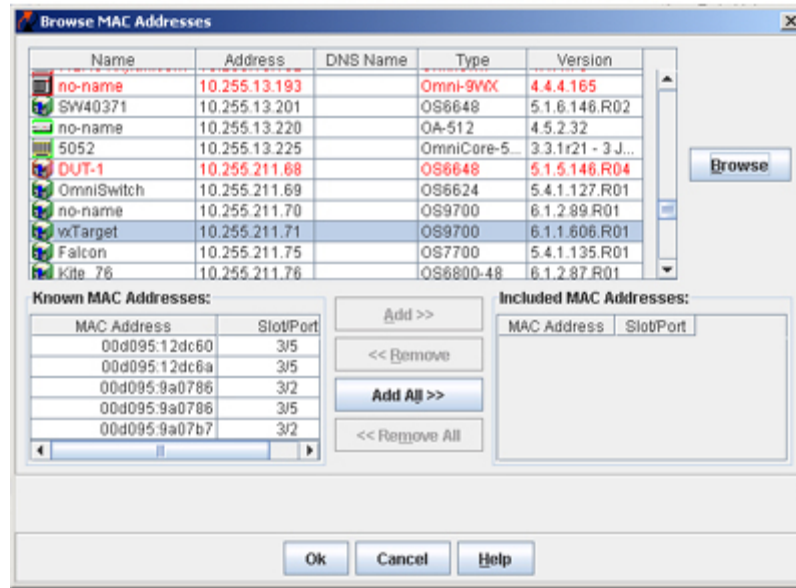
Note: When the Add MAC Rules window opens, an error message window displays a list of management IP addresses for all XOS devices that do not have mobility enabled for the VLAN. You cannot configure VLAN rules for non-mobile VLANs on XOS devices.



Follow the steps below to define a MAC address rule using the Add MAC Rules window:

1. Select one or more devices from the list located in the top half of the Add MAC Rules window.
2. Enter a MAC address in the Single/Start field (note that it is not necessary to use colons when entering a MAC address).
3. Enter a MAC address in the End field to specify a MAC address range, otherwise, leave this field blank.
4. Click on the **Add** button to include the specified MAC address or range of addresses in the rule definition. The MAC addresses entered in the previous steps are moved to the Included MAC Addresses list in the Add MAC Rules window.
5. To select a known MAC address from the source learning MAC Address Table located on each switch, click on the **Browse for MAC Address** button in the Add MAC Rules window. The Browse MAC Addresses window opens, as shown below.

Browse MAC Addresses Window



6. Select one of the devices in the device list located at the top of the Browse MAC Addresses window, then click on the **Browse** button found to the right of the device list. All MAC addresses known to the selected device are displayed in the Known MAC Addresses list.
7. Select one or more MAC addresses from the Known MAC Addresses list or click on the **Add All** button to include the entire list in the rule definition. All MAC addresses selected from the Known MAC Addresses list are moved to the Included MAC Addresses list in the Browse MAC Addresses window.
8. Click on the **OK** button to return to the Add MAC Rules window. The Browse MAC Addresses window closes and the MAC addresses selected in the Browse MAC Addresses window now appear in the Included MAC Addresses list of the Add MAC Rules window.
9. Click on the **OK** button at the bottom of the Add MAC Rules window when you have finished selecting the MAC address(es) for this MAC address rule definition. The Add MAC Rules window closes and a new rule entry appears in the MAC Rules window list with an add icon in the Name field of the new entry.
10. Click the **Apply** button to create the new MAC address rule(s) on the selected device.

Defining Network Address Rules

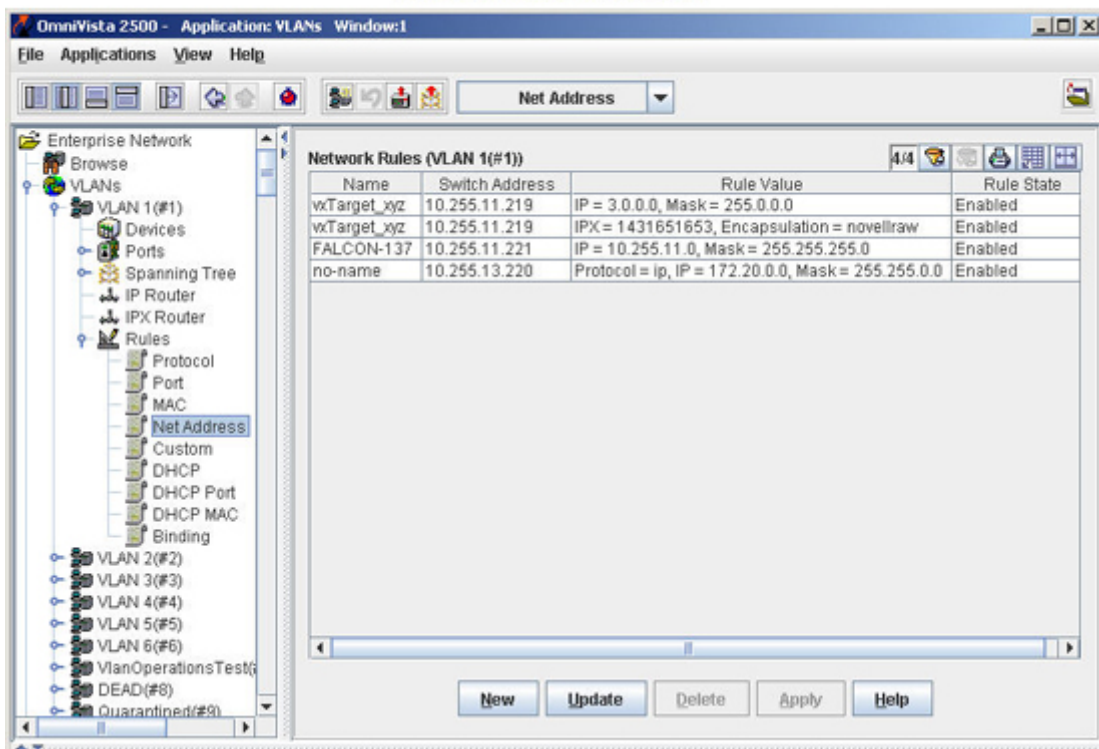
There are two types of network address rules: IP and IPX. An IP network address rule determines VLAN mobile port assignment based on a device's source IP address. An IPX network address rule determines VLAN mobile port assignment based on a device's IPX network and encapsulation.

Consider the following when defining a VLAN network address rule:

- If DHCP is used to provide client workstations with an IP address, you may also need to use one of the DHCP rules in combination with an IP network address rule.
- If the IPX network address rule VLAN is going to route IPX traffic, it is important to specify a rule encapsulation that matches the IPX router port encapsulation. If there is a mismatch, connectivity with other IPX devices may not occur.
- On AOS platforms, IPX network address rules apply only to devices that have already obtained their IPX network address. In addition, frames must match both the IPX network address *and* encapsulation specified in the rule.

The Network Rules window, shown below, contains a list of existing network address rule definitions for the current VLAN. If this list is empty, there are no network address rules defined for this VLAN.

Network Rules Window



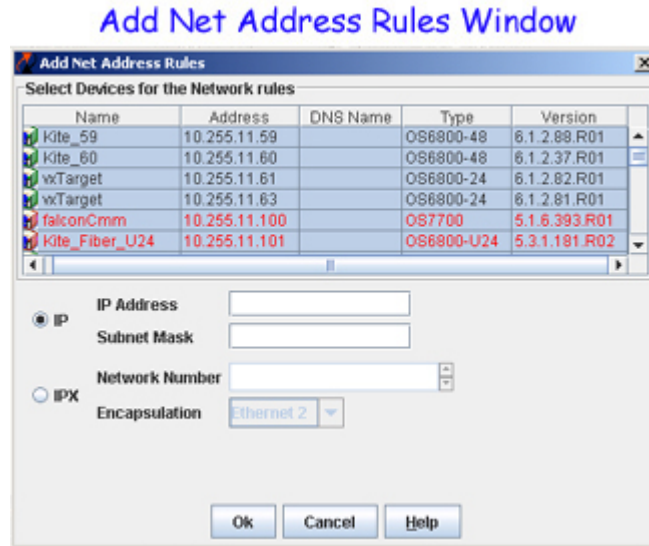
To create a network address rule definition for the current VLAN, click on the **New** button at the bottom of the Network Rules window. This activates the Add Net Address Rules pop-up window. Click [here](#) for information about how to define a network address rule using this window.

Removing a Network Address Rule

To remove a network address rule definition, select one or more rules from the Network Rules window list and click the **Delete** button. A delete icon appears in the Name field of the selected entry. Click the **Apply** button to remove the rule from the device in the selected entry.

Add Net Address Rules Window

The Add Net Address Rules pop-up window, shown below, is used to create a network address rule definition for the current VLAN. This window displays when you click on the **New** button at the bottom of the Network Rules window.



Note: When you click on the **OK** button in the Add Net Address Rules window, an error message window displays a list of management IP addresses for all XOS devices that do not have mobility enabled for the VLAN. You cannot configure VLAN rules for non-mobile VLANs on XOS devices.

Follow the steps below to create an IP network address rule:

1. Select one or more devices from the list located in the top half of the Add Net Address Rules window. Note that all devices are selected by default.
2. Click on **IP** and enter an IP network address (e.g., 172.13.0.0) in the IP Address field and an IP subnet mask (e.g., 255.255.0.0) in the Subnet Mask field.
3. Click the **OK** button at the bottom of the Add Net Address Rules window. The Add Net Address window closes and a new rule entry for each device appears in the Network Rules window list with an add icon in the Name field of the new entry.
4. Click the **Apply** button to create the new IP address rule on each VLAN device.

Follow the steps below to create an IPX network address rule:

1. Select one or more devices from the list located in the top half of the Add Net Address Rules window. Note that all devices are selected by default.
2. Click on **IPX** and enter an IPX network address (e.g., 25040001) in the Network Number field.

3. Select one of the following IPX encapsulation types from the Encapsulation field list:

- Ethernet 2
- Novell Raw (802.3)
- LLC (802.2)
- SNAP

4. Click the **OK** button at the bottom of the Add Net Address Rules window. The Add Net Address window closes and a new rule entry for each device appears in the Network Rules window list with an add icon in the Name field of the new entry.

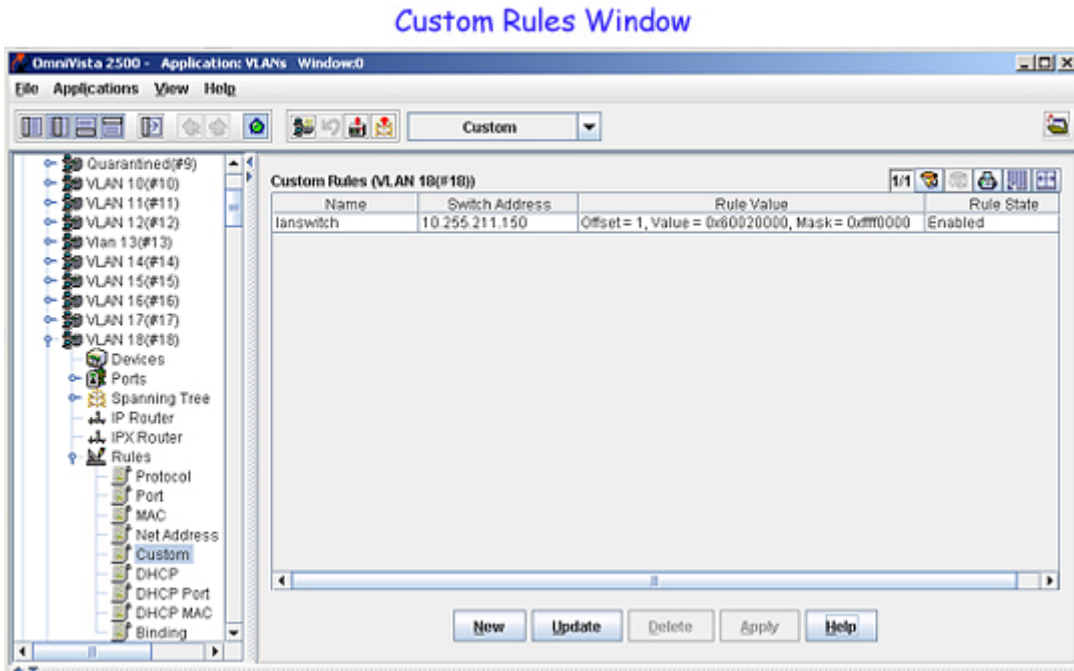
5. Click the **Apply** button to create the new IPX address rule on each VLAN device.

Defining a Custom Rule

Custom rules determine VLAN assignment based on criteria defined by the user. The criteria consists of a specified pattern of data and a location where that data must exist within the frame. Devices originating frames that contain this same data in the required frame location are dynamically assigned to the VLAN.

Note that defining a custom rule is recommended only if none of the other available rules provide the necessary criteria for capturing the desired type of mobile port traffic.

The Custom Rules window, shown below, contains a list of existing custom rule definitions for the current VLAN. If this list is empty, there are no custom rules defined for this VLAN.



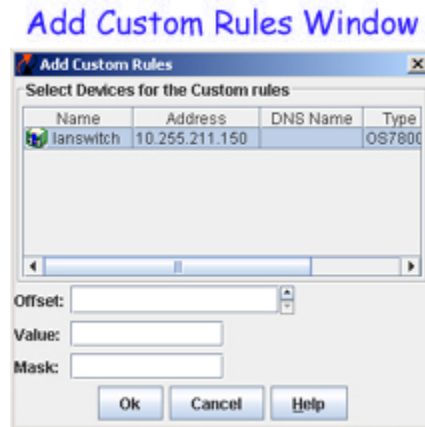
To create a custom rule definition for the current VLAN, click on the **New** button at the bottom of the Custom Rules window. This activates the Add Custom Rule popup window. Click [here](#) for information about how to define a custom rule using this window.

Removing a Custom Rule

To remove a custom rule definition, select one or more rules from the Custom Rules window list and click the **Delete** button. A delete icon appears in the Name field of the selected entry. Click the **Apply** button to remove the rule from the device in the selected entry.

Add Custom Rules Window

The Custom Rules pop-up window, shown below, is used to create a network address rule definition for the current VLAN. This window displays when you click on the **New** button at the bottom of the Custom Rules window.



Follow the steps below to create a custom rule:

1. Select one or more devices from the list located in the top half of the Add Custom Rules window. Note that all devices are selected by default.
2. Enter a number between 0 and 72 in the Offset field to specify the number of bytes into the frame where the pattern (value) is found.
3. Enter a four byte hex value in the Value field to specify a pattern of data (e.g., 60020000).
4. Enter a four byte hex value in the Mask field to identify the bytes in the pattern to compare to the frame contents at the offset location. Use "f" in the mask to mark bytes in the pattern to match and "0" to mark bytes in the pattern to ignore (e.g., ffff0000 is the mask for the 60020000 value pattern).
5. Click the **OK** button at the bottom of the Add Custom Rules window. The Add Custom Rules window closes and a new rule entry for each device appears in the Custom Rules window list with an add icon in the Name field of the new entry.
6. Click the **Apply** button to create the new custom rule on each VLAN device.

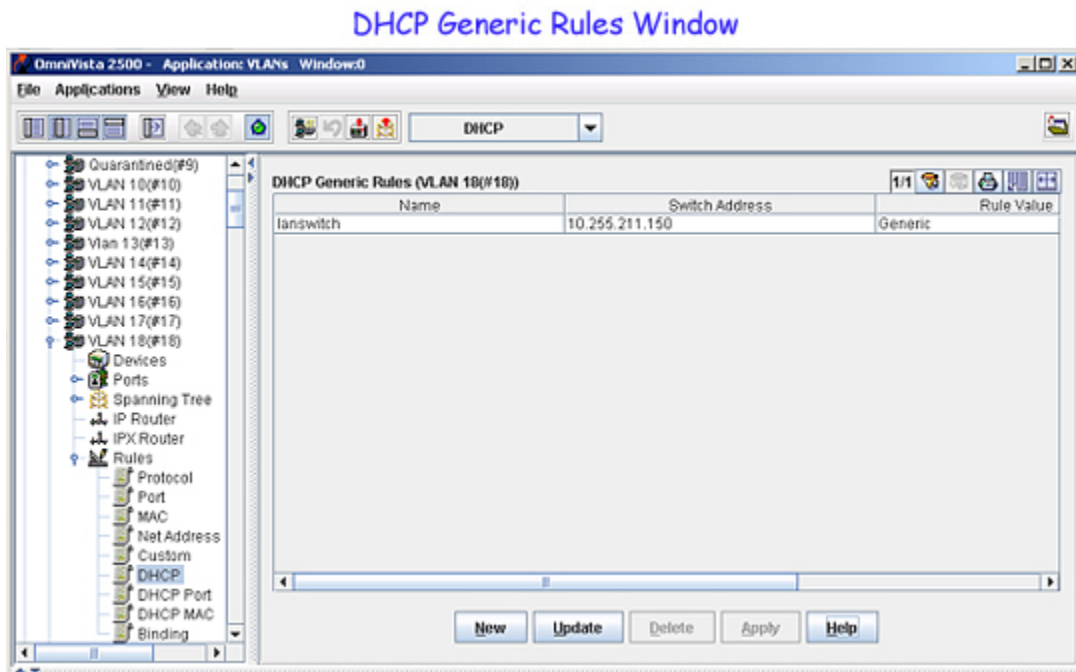
Defining a DHCP Generic Rule

Dynamic Host Configuration Protocol (DHCP) frames are sent from client workstations to request an IP address from a DHCP server. The server responds with the same type of frames, which contain an IP address for the client. If clients are connected to mobile ports, DHCP rules are used to classify this type of traffic for the purposes of transmitting and receiving DHCP frames to and from the server.

A DHCP Generic rule captures all mobile port DHCP frames that do not match any other DHCP rules already defined for other VLANs. For example, if a DHCP frame is received on a mobile port that does *not* match the port specified in any DHCP port rules defined and the frame does *not* contain a source MAC address that matches the MAC address specified in any DHCP MAC address rules defined, then the frame and mobile port are assigned to the DHCP generic rule VLAN.

Note: Only one DHCP generic VLAN rule is allowed per device.

The DHCP Generic Rules window, shown below, contains a list of existing DHCP generic rule definitions for the current VLAN. If this list is empty, there are no DHCP generic rules defined for this VLAN. Since only one generic rule is allowed per device, only one rule appears for each device.



To create a DHCP generic rule definition for the current VLAN, click on the **New** button at the bottom of the DHCP Generic Rule window. This activates the Add DHCP Generic Rule pop-up window. Click [here](#) for information about how to define a DHCP generic rule using this window.

Consider the following when defining a DHCP generic rule:

- When a mobile port receives a DHCP frame that matches a DHCP rule, the port is temporarily assigned to the VLAN long enough to forward the DHCP requests within the VLAN broadcast domain. Note that on AOS platforms, the source MAC address of the DHCP frame is *not* learned for that VLAN port association. As a result, the source MAC address for the DHCP frame does not appear in the source learning MAC address Table on the AOS switch.

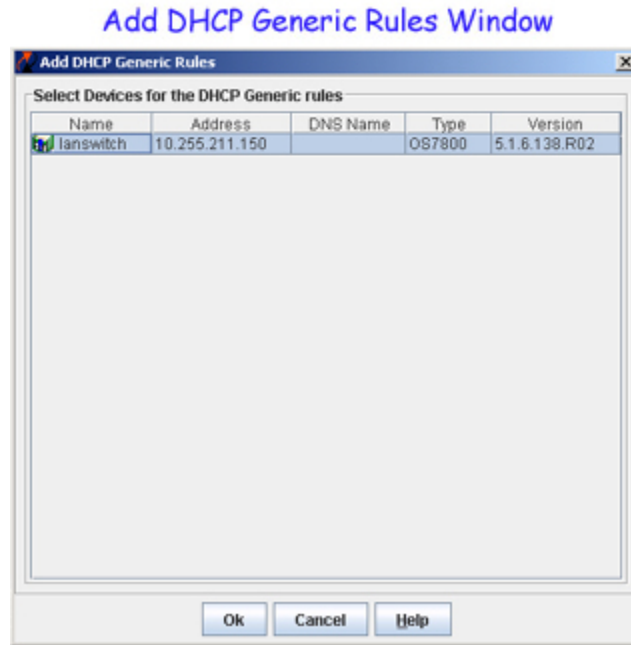
- Once a device connected to a mobile port receives an IP address from the DHCP server, the VLAN port assignment triggered by the device's DHCP frames matching a VLAN DHCP rule is dropped unless regular port traffic matches another rule on that same VLAN. If this match occurs, or the traffic matches a rule on another VLAN, then the source MAC address of the mobile port's frames is learned for that VLAN port association.
- DHCP rules are most often used in combination with IP network address rules. A DHCP client has an IP address of all zeros (0.0.0.0) until it receives an IP address from a DHCP server, so initially it would not match any IP network address rules.
- Binding rules that do *not* specify an IP address, MAC address rules, and protocol rules also capture DHCP traffic for dynamic VLAN assignment. A binding rule that does specify an IP address is similar to a network address rule and will not capture DHCP frames.

Removing a DHCP Generic Address Rule

To remove a DHCP Generic address rule definition, select one or more rules from the DHCP Generic Rules window list and click the **Delete** button. A delete icon appears in the Name field of the selected entry. Click the **Apply** button to remove the rule from the device in the selected entry.

Add DHCP Generic Rules Window

The Add DHCP Generic Rules pop-up window, shown below, is used to create a DHCP generic rule definition for the current VLAN. This window displays when you click on the **New** button at the bottom of the DHCP Generic Rules window.



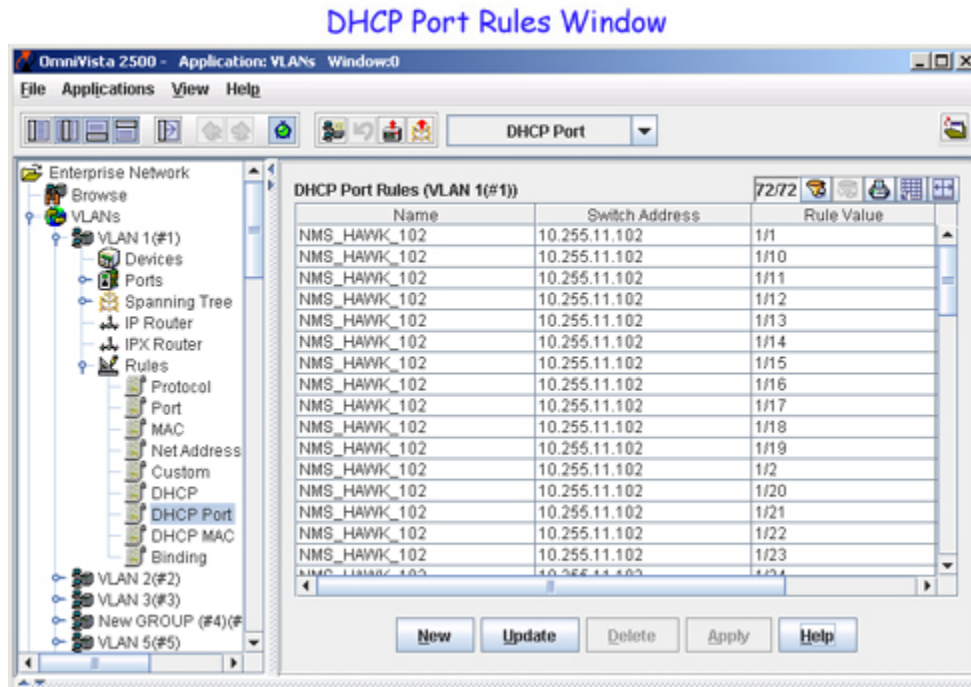
Follow the steps below to define a DHCP generic rule using the Add DHCP Generic Rules window:

1. Select one or more devices from the list located in the top half of the Add Generic Rules window.
2. Click on the **OK** button at the bottom of the Add DHCP Generic Rules window when you have finished selecting the devices for this rule definition. The Add DHCP Generic Rules window closes and a new rule entry appears in the DHCP Generic Rules window list with an add icon in the Name field of the new entry.
3. Click the **Apply** button to create the new DHCP generic address rule on each of the selected devices.

Defining DHCP Port Rules

Dynamic Host Configuration Protocol (DHCP) frames are sent from client workstations to request an IP address from a DHCP server. The server responds with the same type of frames, which contain an IP address for the client. If clients are connected to mobile ports, DHCP rules are used to classify this type of traffic for the purposes of transmitting and receiving DHCP frames to and from the server. DHCP port rules capture DHCP frames that are received on a mobile port that matches the port specified in the rule.

The DHCP Port Rules window, shown below, contains a list of existing DHCP port rule definitions for the current VLAN. If this list is empty, there are no DHCP port rules defined for this VLAN.



To create a DHCP port rule definition for the current VLAN, click on the **New** button at the bottom of the DHCP Port Rules window. This activates the Add DHCP Port Rules pop-up window. Click [here](#) for information about how to define a DHCP port rule using this window.

Consider the following when defining a DHCP port rule:

- When a mobile port receives a DHCP frame that matches a DHCP rule, the port is temporarily assigned to the VLAN long enough to forward the DHCP requests within the VLAN broadcast domain. Note that on AOS platforms, the source MAC address of the DHCP frame is *not* learned for that VLAN port association. As a result, the source MAC address for the DHCP frame does not appear in the source learning MAC address Table on the AOS switch.
- Once a device connected to a mobile port receives an IP address from the DHCP server, the VLAN port assignment triggered by the device's DHCP frames matching a VLAN DHCP rule is dropped unless regular port traffic matches another rule on that same VLAN. If this match occurs, or the traffic matches a rule on another VLAN, then the source MAC address of the mobile port's frames is learned for that VLAN port association.

- DHCP rules are most often used in combination with IP network address rules. A DHCP client has an IP address of all zeros (0.0.0.0) until it receives an IP address from a DHCP server, so initially it would not match any IP network address rules.
- Binding rules that do *not* specify an IP address, MAC address rules, and protocol rules also capture DHCP traffic for dynamic VLAN assignment. A binding rule that does specify an IP address is similar to a network address rule and will not capture DHCP frames.

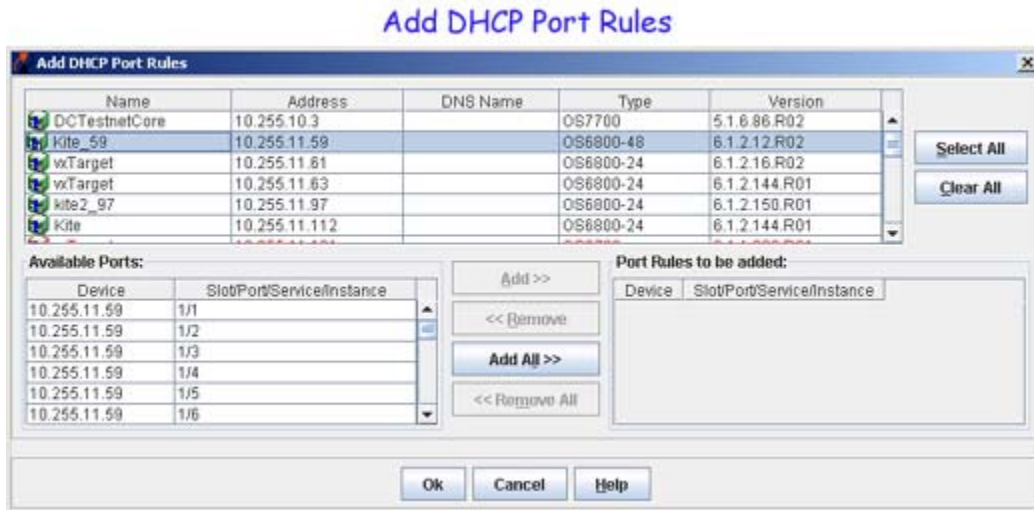
Removing a DHCP Port Rule

To remove a DHCP Port rule definition, select one or more rules from the DHCP Port Rules window list and click the **Delete** button. A delete icon appears in the Name field of the selected entry. Click the **Apply** button to remove the rule from the device in the selected entry.

Add DHCP Port Rules Window

The Add DHCP Port Rules pop-up window, shown below, is used to create a DHCP port rule definition for the current VLAN. This window displays when you click on the **New** button at the bottom of the DHCP Port Rules window.

Note: When the Add Port Rules window opens, an error message window displays a list of management IP addresses for all XOS devices that do not have mobility enabled for the VLAN. You cannot configure VLAN rules for non-mobile VLANs on XOS devices.



The top half of the Add DHCP Port Rules window contains a list of VLAN devices. When you select one or more switches from this list, the Available Ports list in the bottom half of this window displays all ports that are eligible for port rule selection. Note that on XOS platforms you can only specify mobile ports (port assigned to mobile VLANs) when defining a port rule.

To create a DHCP port rule definition for the current VLAN, select one or more switches and then the available ports that you want to specify for the rule and click the **OK** button. The Add DHCP Port Rules window closes and a new DHCP port rule entry appears in the DHCP Port Rules window list with an add icon in the Name field of the new entry. Click the **Apply** button to create the DHCP rule on the selected devices.

Defining DHCP MAC Address Rules

Dynamic Host Configuration Protocol (DHCP) frames are sent from client workstations to request an IP address from a DHCP server. The server responds with the same type of frames, which contain an IP address for the client. If clients are connected to mobile ports, DHCP rules are used to classify this type of traffic for the purposes of transmitting and receiving DHCP frames to and from the server. DHCP MAC address rules capture mobile port DHCP frames that contain a source MAC address that matches the MAC address specified in the rule.

The DHCP MAC Rules window, shown below, contains a list of existing DHCP MAC address rule definitions for the current VLAN. If this list is empty, there are no DHCP MAC address rules defined for this VLAN.

DHCP MAC Rules Panel

Name	Switch Address	Rule Value	Rule State
OmnisR153	10.255.11.153	000abc:def001	Enabled
OmnisR153	10.255.11.153	000abc:def002	Enabled
OmnisR153	10.255.11.153	000abc:def003	Enabled
OmnisR153	10.255.11.153	000abc:def004	Enabled
OmnisR153	10.255.11.153	000abc:def005	Enabled
OmnisR153	10.255.11.153	000abc:def006	Enabled
OmnisR153	10.255.11.153	000abc:def007	Enabled
OmnisR153	10.255.11.153	000abc:def008	Enabled
OmnisR153	10.255.11.153	000abc:def009	Enabled
OmnisR153	10.255.11.153	000abc:def00a	Enabled
OmnisR153	10.255.11.153	000abc:def00b	Enabled
OmnisR153	10.255.11.153	000abc:def00c	Enabled
OmnisR153	10.255.11.153	000abc:def00d	Enabled
OmnisR153	10.255.11.153	000abc:def00e	Enabled
OmnisR153	10.255.11.153	000abc:def00f	Enabled
OmnisR153	10.255.11.153	000abc:def010	Enabled
OmnisR153	10.255.11.153	000abc:def011	Enabled
OmnisR153	10.255.11.153	000abc:def012	Enabled
OmnisR153	10.255.11.153	000abc:def013	Enabled

To create a DHCP MAC address rule definition for the current VLAN, click on the **New** button at the bottom of the DHCP MAC Rules window. This activates the Add DHCP MAC Rules pop-up window. Click [here](#) for information about how to define a DHCP MAC address rule using this window.

Consider the following when defining a DHCP MAC address rule:

- When a mobile port receives a DHCP frame that matches a DHCP rule, the port is temporarily assigned to the VLAN long enough to forward the DHCP requests within the VLAN broadcast domain. Note that on AOS platforms, the source MAC address of the DHCP frame is *not* learned for that VLAN port association. As a result, the source MAC address for the DHCP frame does not appear in the source learning MAC address Table on the AOS switch.
- Once a device connected to a mobile port receives an IP address from the DHCP server, the VLAN port assignment triggered by the device's DHCP frames matching a VLAN DHCP rule is dropped unless regular port traffic matches another rule on that same VLAN. If this match occurs, or the traffic matches a rule on another VLAN, then the source MAC address of the mobile port's frames is learned for that VLAN port association.
- DHCP rules are most often used in combination with IP network address rules. A DHCP client has an IP address of all zeros (0.0.0.0) until it receives an IP address from a DHCP server, so initially it would not match any IP network address rules.

- Binding rules that do *not* specify an IP address, MAC address rules, and protocol rules also capture DHCP traffic for dynamic VLAN assignment. A binding rule that does specify an IP address is similar to a network address rule and will not capture DHCP frames.

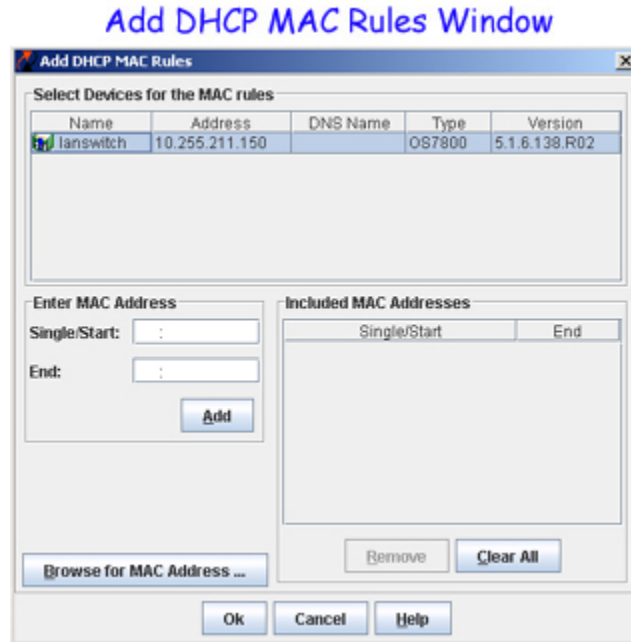
Removing a DHCP MAC Address Rule

To remove a DHCP MAC address rule definition, select one or more rules from the DHCP MAC Rules window list and click the **Delete** button. A delete icon appears in the Name field of the selected entry. Click the **Apply** button to remove the rule from the device in the selected entry.

Add DHCP MAC Rules Window

The Add DHCP MAC Rules pop-up window, shown below, is used to create a DHCP MAC address rule definition for the current VLAN. This window displays when you click on the **New** button at the bottom of the DHCP MAC Rules window.

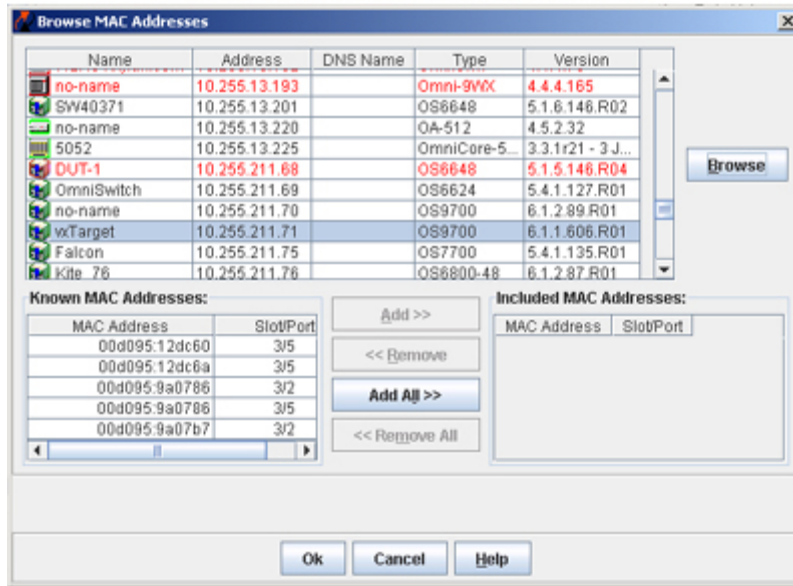
Note: When the Add DHCP MAC Rules window opens, an error message window displays a list of management IP addresses for all XOS devices that do not have mobility enabled for the VLAN. You cannot configure VLAN rules for non-mobile VLANs on XOS devices.



Follow the steps below to define a DHCP MAC address rule using the Add DHCP MAC Rules window:

1. Select one or more devices from the list located in the top half of the Add MAC Rules window.
2. Enter a MAC address in the Single/Start field (note that it is not necessary to use colons when entering a MAC address).
3. Enter a MAC address in the End field to specify a MAC address range, otherwise, leave this field blank.
4. Click on the **Add** button to include the specified MAC address or range of addresses in the rule definition. The MAC addresses entered in the previous steps are moved to the Included MAC Addresses list in the Add DHCP MAC Rules window.
5. To select a known MAC address from the source learning MAC Address Table located on each switch, click on the **Browse for MAC Address** button in the Add DHCP MAC Rules window. The Browse MAC Addresses window opens, as shown below.

Browse MAC Addresses Window



6. Select one of the devices in the device list located at the top of the Browse MAC Addresses window, then click on the **Browse** button found to the right of the device list. All MAC addresses known to the selected device are displayed in the Known MAC Addresses list.
7. Select one or more MAC addresses from the Known MAC Addresses list or click on the **Add All** button to include the entire list in the rule definition. All MAC addresses selected from the Known MAC Addresses list are moved to the Included MAC Addresses list in the Browse MAC Addresses window.
8. Click on the **OK** button to return to the Add DHCP MAC Rules window. The Browse MAC Addresses window closes and the MAC addresses selected in the Browse MAC Addresses window now appear in the Included MAC Addresses list of the Add DHCP MAC Rules window.
9. Click on the **OK** button at the bottom of the Add DHCP MAC Rules window when you have finished selecting the MAC address(es) for this MAC address rule definition. The Add DHCP MAC Rules window closes and a new rule entry appears in the DHCP MAC Rules window list with an add icon in the Name field of the new entry.
10. Click the **Apply** button to create the new DHCP MAC address rule(s) on the selected device.

Defining Binding Rules

Binding rules restrict VLAN assignment to specific devices by requiring that device traffic match all criteria specified in the rule. As a result, a separate binding rule is required for each device. An unlimited number of such rules, however, is allowed per VLAN.

There are six binding rule types available: MAC-Port-IP, MAC-Port-Protocol, MAC-Port, MAC-IP Address, Port-IP Address, and Port-Protocol. The binding rule type name indicates the criteria the rule uses to determine if traffic received on a mobile port qualifies for dynamic VLAN assignment. For example, the MAC-Port-IP address binding rule requires a matching source MAC and IP address in frames received from a device connected to the mobile port specified in the rule.

Although DHCP frames are examined and processed first, binding rules take precedence over all other rules. If frames received on a mobile port do not contain any matching binding rule criteria, they are compared against other existing VLAN rules of lower precedence. However, if a frame violates criteria of any one binding rule, it is discarded. Click [here](#) for more information about rule precedence and binding rule violations.

The Binding Rules window, as shown below, contains a list of existing binding rule definitions for the current VLAN. If this list is empty, there are no binding rules defined for this VLAN.



To create a binding rule definition for the current VLAN, click on the **New** button at the bottom of the Binding Rules window. This activates the Add Binding Rules pop-up window. Click on one of the following binding rule types for more information about how to create that rule:

- IP-MAC
- IP-PORT
- MAC-PORT
- PORT-PROTOCOL
- MAC-IP-PORT
- MAC-PORT-PROTOCOL

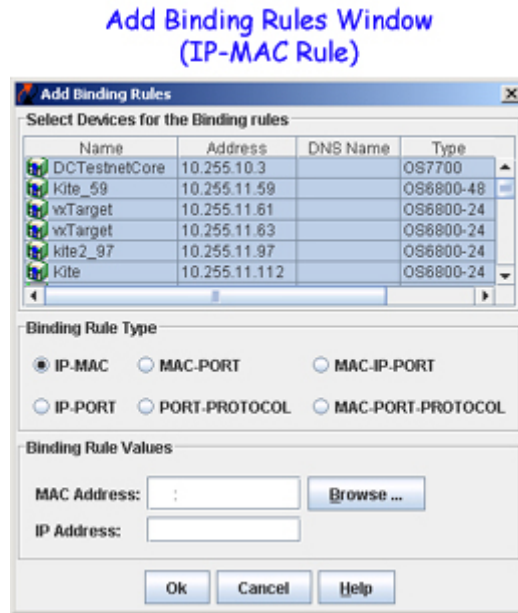
Note: The following Binding Rules are not supported on 6800 series switches: IP-MAC, IP-Port, and MAC-Port-Protocol.

Removing a Binding Rule

To remove a binding rule definition, select one or more rules from the Binding Rules window list and click the **Delete** button. A delete icon appears in the Name field of the selected entry. Click the **Apply** button to remove the rule from the device in the selected entry.

Defining IP-MAC Binding Rule Values

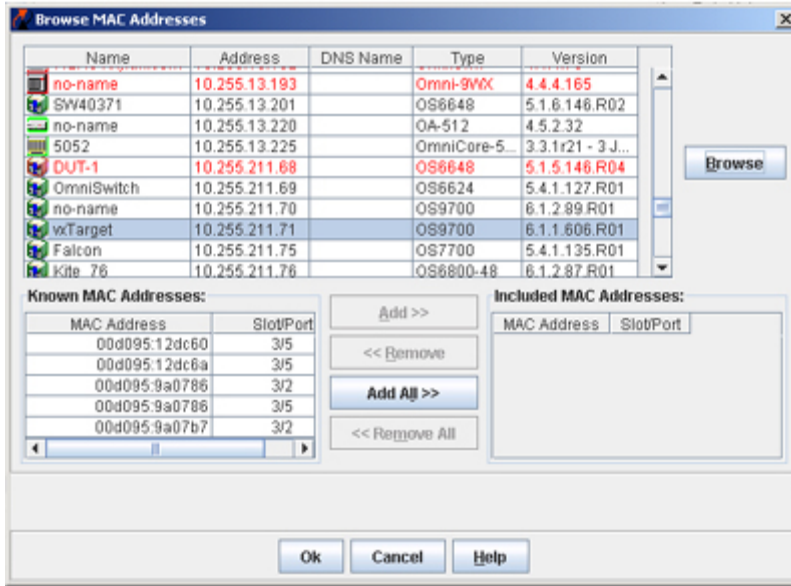
The Add Binding Rules pop-up window displays the IP-MAC binding rule values, shown below, when the IP-MAC rule type is selected.



Follow the steps below to define an IP-MAC binding rule:

1. Select one or more devices from the list located in the top half of the Add Binding Rules window. Note that all devices are selected by default.
2. Select the IP-MAC binding rule type (the default selection). The Binding Rules Values portion of the Add Binding Rules window displays a MAC Address field and an IP Address field. Specifying a value for each field is required to define an IP-MAC binding rule.
3. Enter a MAC address in the MAC Address field. To specify a known MAC address, click on the **Browse** button next to the MAC Address field. The Browse MAC Addresses window opens, as shown below.

Browse MAC Addresses Window



4. Select one of the devices in the device list located at the top of the Browse MAC Addresses window, then click on the **Browse** button found to the right of the device list. All MAC addresses known to the selected device are displayed in the Known MAC Addresses list.

5. Select one MAC address from the Known MAC Addresses list and click on the **Add >>** button. The MAC address selected from the Known MAC Addresses list is moved to the Included MAC Addresses list in the Browse MAC Addresses window.

Note: Only one MAC address is specified for each binding rule, as these types of rules are for restricting VLAN assignment to individual PCs, workstations, etc. If more than one MAC address is selected from the Known MAC Addresses list, only the first address selected is used for the binding rule value.

6. Click on the **OK** button to return to the Add Binding Rules window. The Browse MAC Addresses window closes and the MAC address selected now appears in the MAC Address field of the Add Binding Rules window.

7. Enter an IP network address (e.g., 172.17.10.1) in the IP Address field.

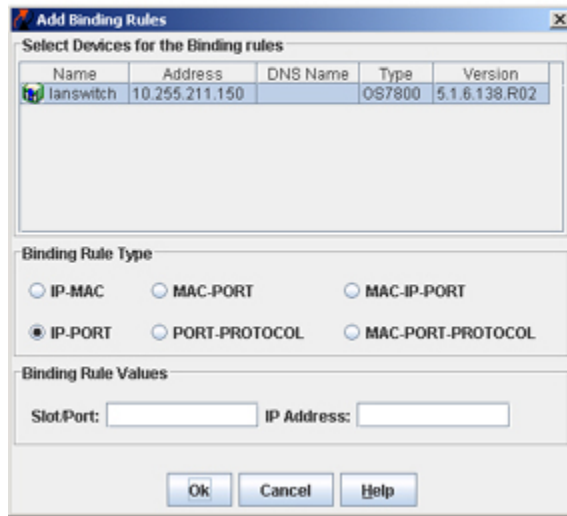
8. Click the **OK** button at the bottom of the Add Binding Rules window. The Add Binding Rules window closes and a new rule entry for each device appears in the Binding Rules window list with an add icon in the Name field of the new entry.

9. Click the **Apply** button to create the new IP-MAC binding rule. The rule is configured for the VLAN on each device that was selected when the rule was defined using the Add Binding Rules window.

Defining IP-Port Binding Rule Values

The Add Binding Rules pop-up window displays the IP-port binding rule values, shown below, when the IP-PORT rule type is selected.

Add Binding Rules Window
(IP-Port Rule)

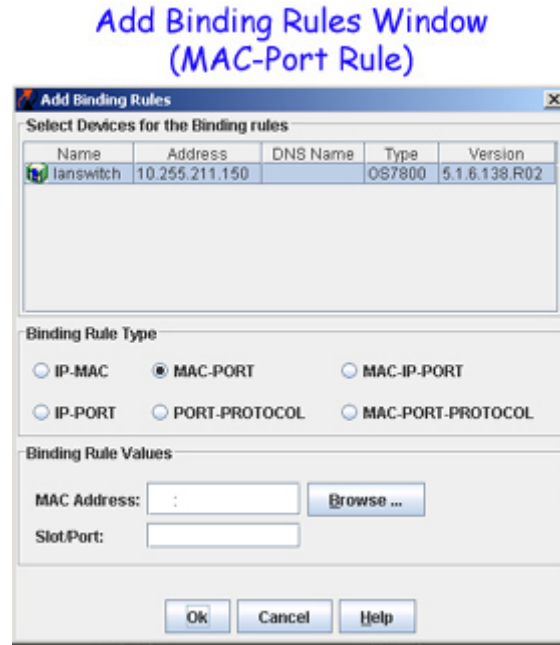


Follow the steps below to define an IP-port binding rule:

1. Select one or more devices from the list located in the top half of the Add Binding Rules window. Note that all devices are selected by default.
2. Select the IP-PORT binding rule type. The Binding Rules Values portion of the Add Binding Rules window displays a Slot/Port field and an IP Address field. Specifying a value for each field is required to define an IP-port binding rule.
3. Enter a valid slot/port designation (e.g., 2/1, 4/8, 5/10) in the Slot/Port field.
4. Enter an IP network address (e.g., 172.17.10.1) in the IP Address field.
5. Click the **OK** button at the bottom of the Add Binding Rules window. The Add Binding Rules window closes and a new rule entry for each device appears in the Binding Rules window list with an add icon in the Name field of the new entry.
6. Click the **Apply** button to create the new IP-Port binding rule. The rule is configured for the VLAN on each device that was selected when the rule was defined using the Add Binding Rules window.

Defining MAC-Port Binding Rule Values

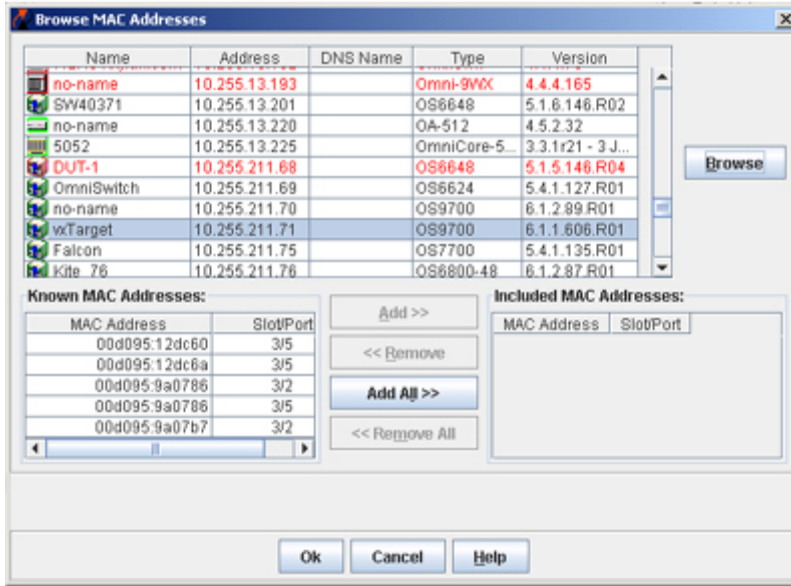
The Add Binding Rules pop-up window displays the MAC-port binding rule values, shown below, when the MAC-PORT rule type is selected.



Follow the steps below to define a MAC-port binding rule:

1. Select one or more devices from the list located in the top half of the Add Binding Rules window. Note that all devices are selected by default.
2. Select the MAC-PORT binding rule type. The Binding Rules Values portion of the Add Binding Rules window displays a MAC Address field and a Slot/Port field. Specifying a value for each field is required to define a MAC-port binding rule.
3. Enter a MAC address in the MAC Address field. To specify a known MAC address, click on the **Browse** button next to the MAC Address field. The Browse MAC Addresses window opens, as shown below.

Browse MAC Addresses Window



4. Select one of the devices in the device list located at the top of the Browse MAC Addresses window, then click on the **Browse** button found to the right of the device list. All MAC addresses known to the selected device are displayed in the Known MAC Addresses list.

5. Select one MAC address from the Known MAC Addresses list and click on the **Add >>** button. The MAC address selected from the Known MAC Addresses list is moved to the Included MAC Addresses list in the Browse MAC Addresses window.

Note: Only one MAC address is specified for each binding rule, as these types of rules are for restricting VLAN assignment to individual PCs, workstations, etc. If more than one MAC address is selected from the Known MAC Addresses list, only the first address selected is used for the binding rule value.

6. Click on the **OK** button to return to the Add Binding Rules window. The Browse MAC Addresses window closes and the MAC address selected now appears in the MAC Address field of the Add Binding Rules window.

7. Enter a valid slot/port designation (e.g., 2/1, 4/8, 5/10) in the Slot/Port field.

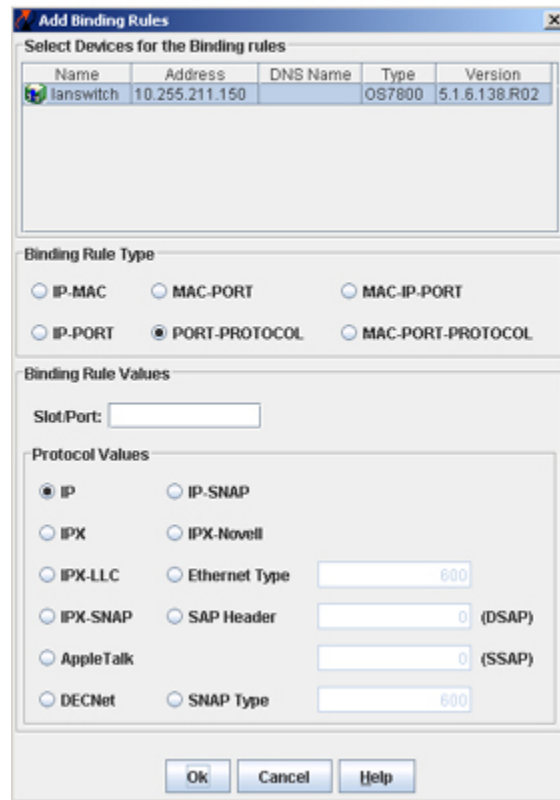
8. Click the **OK** button at the bottom of the Add Binding Rules window. The Add Binding Rules window closes and a new rule entry for each device appears in the Binding Rules window list with an add icon in the Name field of the new entry.

9. Click the **Apply** button to create the new MAC-port binding rule. The rule is configured for the VLAN on each device that was selected when the rule was defined using the Add Binding Rules window.

Defining Port-Protocol Binding Rule Values

The Add Binding Rules pop-up window displays the port-protocol binding rule values, shown below, when the PORT-PROTOCOL rule type is selected.

Add Binding Rules Window
(Port-Protocol Rule)



Follow the steps below to define a port-protocol binding rule:

1. Select one or more devices from the list located in the top half of the Add Binding Rules window. Note that all devices are selected by default.
2. Select the PORT-PROTOCOL binding rule type. The Binding Rules Values portion of the Add Binding Rules window displays a Slot/Port field and a Protocol Values collection of fields. Specifying a value for the Slot/Port field and selecting or specifying a value for one of the protocol fields is required to define a port-protocol binding rule.
3. Enter a valid slot/port designation (e.g., 2/1, 4/8, 5/10) in the Slot/Port field.
4. Click on one of the following protocol types displayed in the Protocol Values portion of the window:
 - IP (Ethernet II, ARP, and SNAP)
 - IP-SNAP (AOS only)
 - IPX (Ethernet II, Novell 802.3, LLC 802.2, and SNAP)

- IPX-LLC (AOS only)
- IPX-SNAP (AOS only)
- IPX-Novell (AOS only)
- AppleTalk (Data Delivery Protocol and AppleTalk ARP)
- DECNet (DECNet Phase IV--only captures frames with 6003 Ethernet type)
- Ethernet Type (A two byte hex value between 0x600 and 0xffff that defines an Ethernet type. This value is required for the Ethernet Type field when this protocol type is selected.)
- SAP Header (A one byte hex value between 0x00 and 0xff that defines DSAP and SSAP header values. These values are required for the DSAP and SSAP fields when this protocol type is selected.)
- SNAP Type (A two byte hex value between 0x600 and 0xffff that defines a Sub-network Access Protocol. This value is required for the SNAP Type field when this protocol type is selected.)

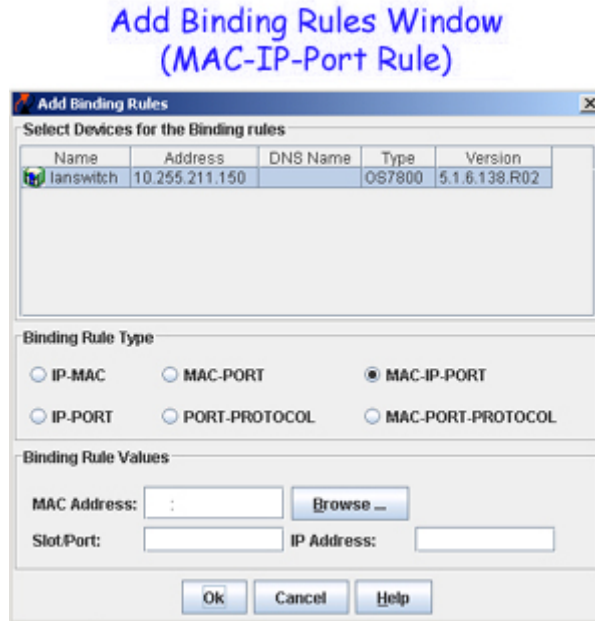
Note: When you select only XOS devices from the device list, the IPX-LLC, IPX-SNAP, and IPX-Novell buttons are grayed out because these rules are not supported on XOS devices. The IPX protocol rule on XOS devices captures LLC, SNAP, and Novell encapsulations without specifying a separate rule.

5. After selecting the desired protocol type and entering any additional required values, click the **OK** button at the bottom of the Add Binding Rules window. The Add Binding Rules window closes and a new rule entry for each device appears in the Binding Rules window list with an add icon in the Name field of the new entry.

6. Click the **Apply** button to create the new port-protocol binding rule. The rule is configured for the VLAN on each device that was selected when the rule was defined using the Add Binding Rules window.

Defining MAC-IP-Port Binding Rule Values

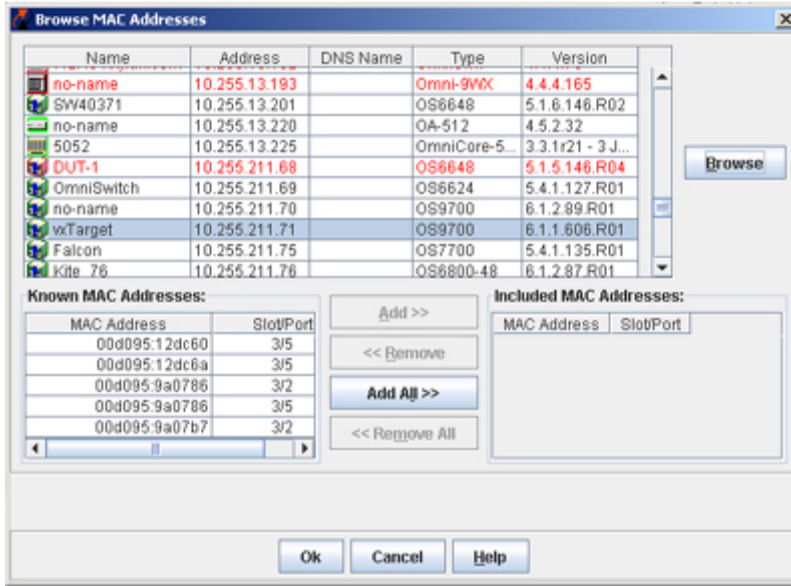
The Add Binding Rules pop-up window displays the MAC-IP-port binding rule values, shown below, when the MAC-IP-PORT rule type is selected.



Follow the steps below to define a MAC-IP-port binding rule:

1. Select one or more devices from the list located in the top half of the Add Binding Rules window. Note that all devices are selected by default.
2. Select the MAC-IP-PORT binding rule type. The Binding Rules Values portion of the Add Binding Rules window displays a MAC Address field, Slot/Port field, and an IP Address field. Specifying a value for all three of these fields is required to define a MAC-IP-port binding rule.
3. Enter a MAC address in the MAC Address field. To specify a known MAC address, click on the **Browse** button next to the MAC Address field. The Browse MAC Addresses window opens, as shown below.

Browse MAC Addresses Window



4. Select one of the devices in the device list located at the top of the Browse MAC Addresses window, then click on the **Browse** button found to the right of the device list. All MAC addresses known to the selected device are displayed in the Known MAC Addresses list.

5. Select one MAC address from the Known MAC Addresses list and click on the **Add >>** button. The MAC address selected from the Known MAC Addresses list is moved to the Included MAC Addresses list in the Browse MAC Addresses window.

Note: Only one MAC address is specified for each binding rule, as these types of rules are for restricting VLAN assignment to individual PCs, workstations, etc. If more than one MAC address is selected from the Known MAC Addresses list, only the first address selected is used for the binding rule value.

6. Click on the **OK** button to return to the Add Binding Rules window. The Browse MAC Addresses window closes and the MAC address selected now appears in the MAC Address field of the Add Binding Rules window.

7. Enter a valid slot/port designation (e.g., 2/1, 4/8, 5/10) in the Slot/Port field.

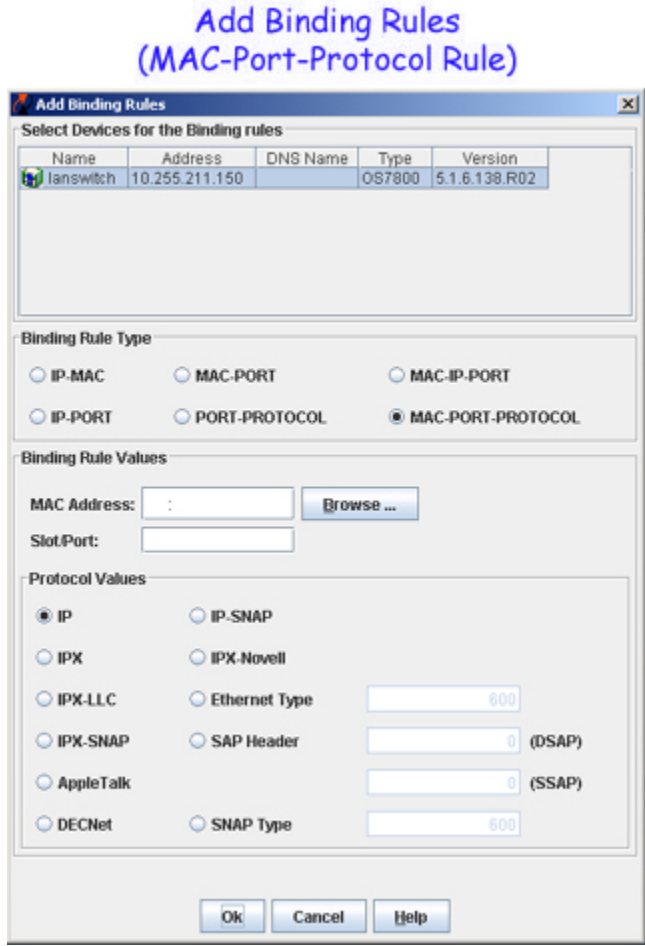
8. Enter an IP network address (e.g., 172.17.10.1) in the IP Address field.

9. Click the **OK** button at the bottom of the Add Binding Rules window. The Add Binding Rules window closes and a new rule entry for each device appears in the Binding Rules window list with an add icon in the Name field of the new entry.

10. Click the **Apply** button to create the new MAC-IP-port binding rule. The rule is configured for the VLAN on each device that was selected when the rule was defined using the Add Binding Rules window.

Defining MAC-Port-Protocol Binding Rule Values

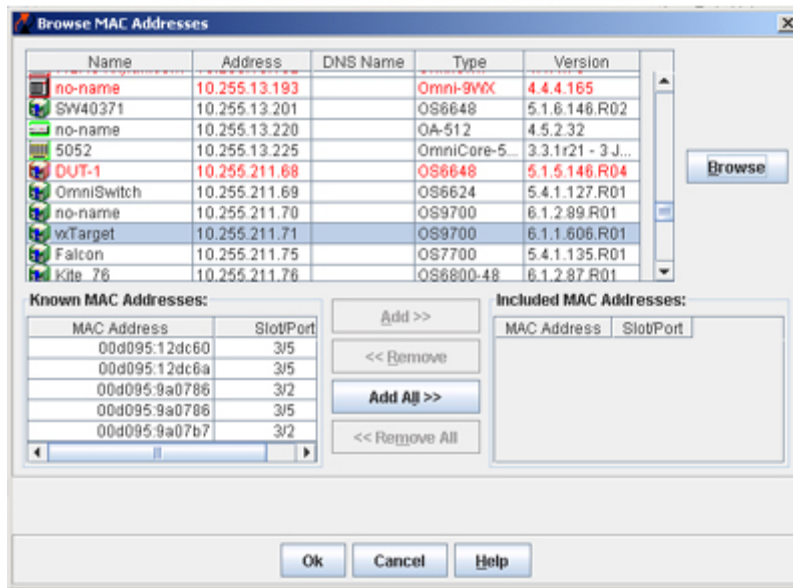
The Add Binding Rules pop-up window displays the MAC-port-protocol binding rule values, shown below, when the MAC-PORT-PROTOCOL rule type is selected.



Follow the steps below to define a MAC-port-protocol binding rule:

1. Select one or more devices from the list located in the top half of the Add Binding Rules window. Note that all devices are selected by default.
2. Select the MAC-PORT-PROTOCOL binding rule type. The Binding Rules Values portion of the Add Binding Rules window displays a MAC Address field, Slot/Port field, and a Protocol Values collection of fields. Specifying a value for all three of these fields is required to define a MAC-port-protocol binding rule.
3. Enter a MAC address in the MAC Address field. To specify a known MAC address, click on the **Browse** button next to the MAC Address field. The Browse MAC Addresses window opens, as shown below.

Browse MAC Addresses Window



4. Select one of the devices in the device list located at the top of the Browse MAC Addresses window, then click on the **Browse** button found to the right of the device list. All MAC addresses known to the selected device are displayed in the Known MAC Addresses list.

5. Select one MAC address from the Known MAC Addresses list and click on the **Add >>** button. The MAC address selected from the Known MAC Addresses list is moved to the Included MAC Addresses list in the Browse MAC Addresses window.

Note: Only one MAC address is specified for each binding rule, as these types of rules are for restricting VLAN assignment to individual PCs, workstations, etc. If more than one MAC address is selected from the Known MAC Addresses list, only the first address selected is used for the binding rule value.

6. Click on the **OK** button to return to the Add Binding Rules window. The Browse MAC Addresses window closes and the MAC address selected now appears in the MAC Address field of the Add Binding Rules window.

7. Enter a valid slot/port designation (e.g., 2/1, 4/8, 5/10) in the Slot/Port field.

8. Click on one of the following protocol types displayed in the Protocol Values portion of the window:

- IP (Ethernet II, ARP, and SNAP)
- IP-SNAP (AOS only)
- IPX (Ethernet II, Novell 802.3, LLC 802.2, and SNAP)
- IPX-LLC (AOS only)
- IPX-SNAP (AOS only)
- IPX-Novell (AOS only)
- AppleTalk (Data Delivery Protocol and AppleTalk ARP)
- DECNet (DECNet Phase IV--only captures frames with 6003 Ethernet type)
- Ethernet Type (A two byte hex value between 0x600 and 0xffff that defines an Ethernet type. This value is required for the Ethernet Type field when this protocol type is selected.)

- SAP Header (A one byte hex value between 0x00 and 0xff that defines DSAP and SSAP header values. These values are required for the DSAP and SSAP fields when this protocol type is selected.)
- SNAP Type (A two byte hex value between 0x600 and 0xffff that defines a Sub-network Access Protocol. This value is required for the SNAP Type field when this protocol type is selected.)

Note: When you select only XOS devices from the device list, the IPX-LLC, IPX-SNAP, and IPX-Novell buttons are grayed out because these rules are not supported on XOS devices. The IPX protocol rule on XOS devices captures LLC, SNAP, and Novell encapsulations without specifying a separate rule.

9. After selecting the desired protocol type and entering any additional required values, click the **OK** button at the bottom of the Add Binding Rules window. The Add Binding Rules window closes and a new rule entry for each device appears in the Binding Rules window list with an add icon in the Name field of the new entry.

10. Click the **Apply** button to create the new MAC-port-protocol binding rule. The rule is configured for the VLAN on each device that was selected when the rule was defined using the Add Binding Rules window.

Using Port Mobility

Port mobility (also referred to as Group Mobility) allows dynamic VLAN port assignment based on VLAN rules that are applied to port traffic. By default, all switch ports are non-mobile ports that are manually assigned to a specific VLAN and can only belong to one VLAN at a time. When a port is defined as a mobile port, switch software compares traffic coming in on the port with configured VLAN rules. If any of the mobile port traffic matches any of the VLAN rules, the port and the matching traffic become a member of that VLAN. It is also possible for mobile ports to belong to more than one VLAN, when the port carries multiple traffic types that match different rules on different VLANs.

On AOS platforms, VLANs do not have a mobile or non-mobile distinction and there is no overall switch setting to invoke the mobile port feature. Instead, mobility is enabled on individual switch ports and rules are defined for individual VLANs to capture mobile port traffic. [Click here for information about configuring mobility on AOS devices.](#)

On XOS platforms, ports become mobile when they are statically assigned to a VLAN that has mobility enabled. Rules to capture mobile port traffic are only defined on mobile VLANs. In addition to enabling mobility on the VLAN and defining VLAN rules, you must also enable the Group Mobility feature for the entire switch. [Click here for information about configuring mobility on XOS devices.](#)

Configuring Mobility on AOS Devices

Follow the steps below to configure the port mobility feature on AOS devices.

1. Enable mobility on the switch ports that you want to designate as mobile ports. When mobility is enabled on a port, the port becomes eligible for dynamic VLAN assignment.
2. Enable or disable mobile port properties, described below, that determine mobile port behavior. Configuring mobility on AOS devices is done on an individual port basis. This step applies only to the selected ports and does not dictate switch-wide behavior of all mobile ports.
3. Create VLANs that will receive and forward mobile port traffic. Note that on AOS devices, VLANs do not have a mobile or non-mobile designation, so you do not have to enable mobility on a VLAN. In essence, all VLANs support the mobility feature.
4. Define rules for the VLANs created in the previous step. These rules will trigger dynamic assignment of mobile ports to these VLANs when mobile ports receive traffic that matches rule criteria.

Enabling/Disabling Port Mobility and Related Parameters

To enable or disable mobility and related port parameters, click open the AOS switch management IP address in the Devices Tree. This displays the Port Mobility Table, as shown below

Click on **Mobility** to display a list of eligible mobile ports

AOS Port Mobility Table

Slot/Port	Mobility	Default VLAN Restore	Default VLAN Enable	Ignore BPDU
1/1	disable	notApplicable	notApplicable	notApplicable
1/2	disable	notApplicable	notApplicable	notApplicable
1/3	disable	notApplicable	notApplicable	notApplicable
1/4	disable	notApplicable	notApplicable	notApplicable
1/5	disable	notApplicable	notApplicable	notApplicable
1/6	disable	notApplicable	notApplicable	notApplicable
1/7	disable	notApplicable	notApplicable	notApplicable
1/8	disable	notApplicable	notApplicable	notApplicable
1/9	disable	notApplicable	notApplicable	notApplicable

View Port Mobility

Slot/Port: Mobility:

Default VLAN Restore: Default VLAN Enable:

Ignore BPDU: Authenticate:

Configured Default VLAN:

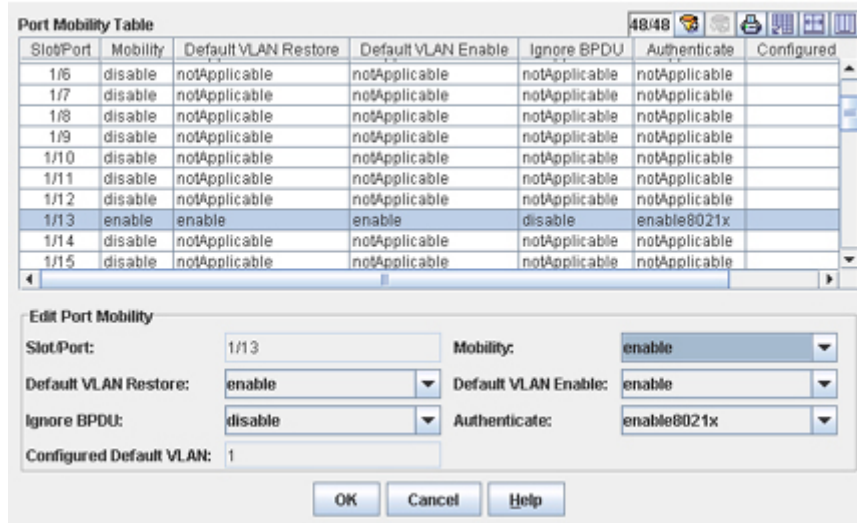
The Port Mobility Table displays a list of all mobile and fixed (non-mobile) Ethernet ports and the status of mobile port properties. The list contains only those ports that are eligible for mobile port status. As a result, 802.1Q tagged ports are not included in the list. This table is also used to enable or disable mobility on a selected port and modify mobile port properties that affect port behavior when it is dynamically assigned.

If mobility is disabled on a port, **notApplicable** displays in each of the mobile port parameter fields for the port. When you enable mobility on the port and do not modify any of the parameter values at the same time, the parameters automatically revert to their default values when you apply the mobility status change for the port to the switch.

Note: If mobility is disabled on a port, and you try to change the **notApplicable** port parameters, then an SNMP error message is generated by that switch.

To modify the mobile status of a port and related mobile port parameters, select one or more ports from the Port Mobility Table list and click the **Edit** button. This activates the Edit Port Mobility panel. If you select more than one port to modify, an Edit Port Mobility popup window opens that contains the configurable port parameters.

Edit Port Mobility Panel



Using either the Edit Port Mobility panel or popup window, make the desired parameter changes and click the **OK** button to return to the Port Mobility Table list. A modify icon appears in the Slot/Port field for the modified port. Click the **Apply** button to apply the changes to the appropriate switch configurations.

Note that enabling mobility on an active connection port that sends or receives Spanning Tree BPDU is not allowed. If mobility is desired on this type of port, enable mobility and the BPDU Ignore flag when the port is not actively carrying any traffic. For example, before anything is even connected to the port.

Port Mobility AOS Parameters

Slot/Port

The slot/port designation that identifies the corresponding slot number for the port's module and the corresponding port number on that module. (e.g., 3/1 specifies port 1 on slot 3).

Mobility

The mobile status of the port; **enabled** or **disabled**. If enabled, then the port is eligible for dynamic VLAN assignment. By default, this parameter is **disabled** on all eligible switch ports.

Default VLAN Restore

Indicates if the mobile port will retain or drop a dynamic VLAN port assignment (VPA) when the qualifying traffic on the port that triggered the VLAN assignment ages out. If this parameter is **enabled**, the VPA is dropped. If this parameter is **disabled**, the VPA is retained. By default, this parameter is **enabled** on mobile ports.

Default VLAN Enable

Indicates if the mobile port will forward or drop its configured default VLAN traffic that does not match any VLAN rules. If this parameter is **enabled**, then non-matching traffic is carried on the configured default VLAN for the port. If this parameter is **disabled**, then non-matching is dropped. By default, this parameter is **enabled** on mobile ports.

Ignore BPDU

Indicates if BPDU ignore active on the mobile port. If **disabled**, switch ports that send or receive spanning tree Bridge Protocol Data Units (BPDU) are not eligible for mobile port dynamic VLAN assignment. If **enabled**, BPDU are ignored on these ports and port traffic is compared to VLAN rules in the same manner as it is for non-BPDU mobile ports. Enabling BPDU ignore is not recommended, however, as it may cause network loops to go undetected or connectivity problems between switches. By default, this parameter is **disabled** on mobile ports.

Authenticate

Indicates if authentication is active on the mobile port. If **enabled**, the port participates in a Layer 2 authentication process that restricts switch access at the VLAN level. At this time, only mobile ports are eligible for authentication status. By default, this parameter is **disabled** on mobile ports.

Configured Default VLAN

The VLAN number of the port's configured default VLAN. All mobile and fixed ports have a configured default VLAN, which initially is the switch default VLAN 1 until the port is statically assigned to another VLAN.

Configuring Mobility on XOS Devices

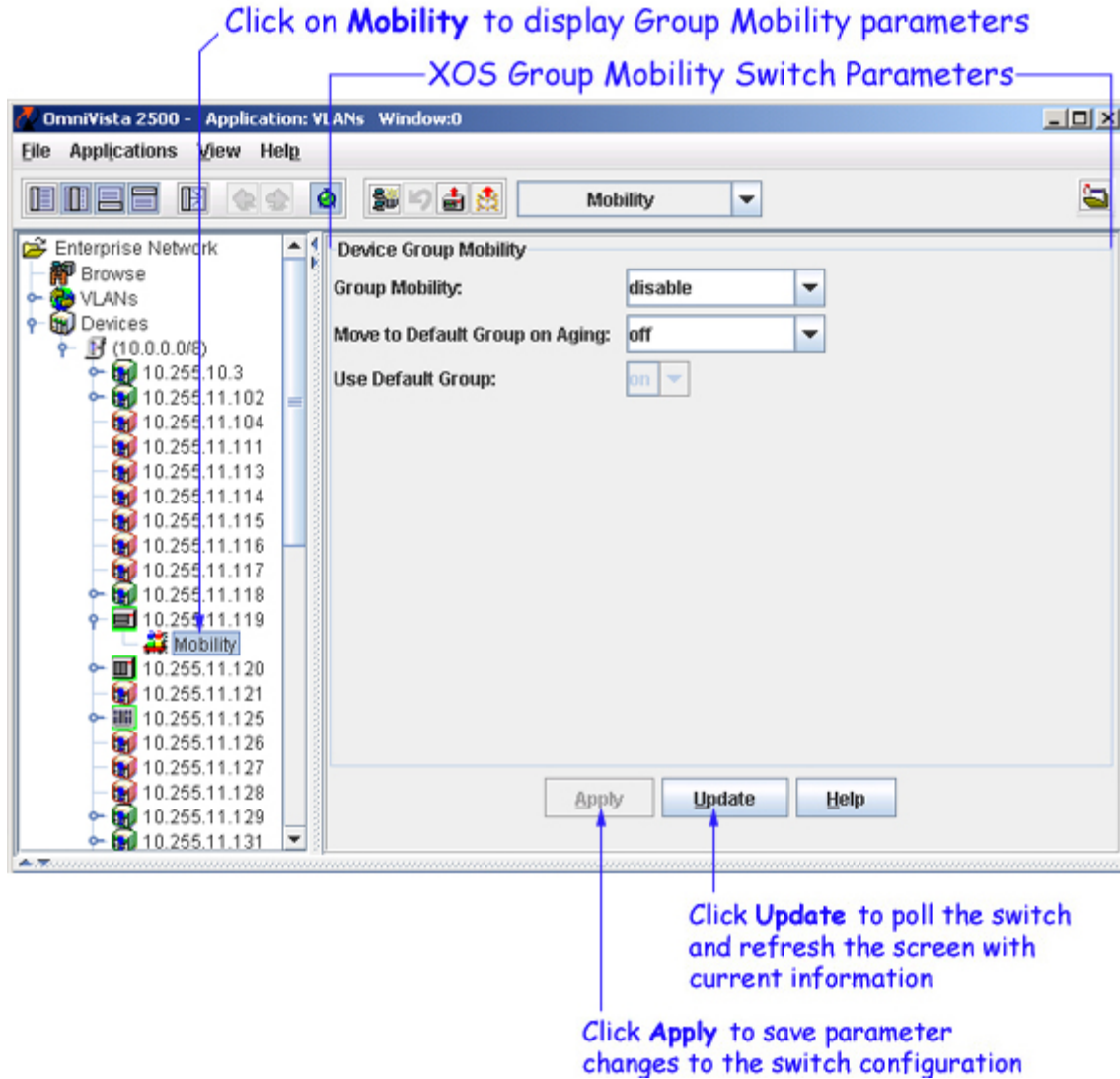
Follow the steps below to configure the port mobility feature on XOS devices.

1. Enable the Group Mobility feature for the switch. Group Mobility is available on every XOS switch, but is disabled by default. When you enable this feature, the default VLAN 1 automatically becomes a mobile VLAN (Group). As a result, all switch ports in VLAN 1 are now considered mobile ports and are eligible for dynamic VLAN assignment.
2. Enable/disable Group Mobility parameters, described below, that globally determine mobile port behavior.
3. Create mobile VLANs that will receive and forward mobile port traffic.
4. Define VLAN rules for the mobile VLANs created in the previous step. These rules will trigger dynamic assignment of mobile ports to these VLANs when mobile ports receive traffic that matches rule criteria.
5. Statically assign switch ports to a mobile VLAN.

XOS switch ports do not become mobile ports until they are assigned to a mobile VLAN. All ports assigned to a standard (non-mobile) VLAN are not eligible for dynamic VLAN assignment using the Group Mobility feature.

Enabling/disabling Group Mobility and Related Parameters

To enable or disable the Group Mobility feature and related parameters, click open the XOS switch management IP address in the Devices Tree. This activates the Device Group Mobility panel, as shown below. Make the desired parameter status changes and click the **Apply** button to make the changes on the device.



Group Mobility XOS Parameters

Note that the following are switch-wide parameters that apply to all mobile VLANs and mobile ports.

Group Mobility

The status of the Group Mobility feature for the switch; **enable** or **disable**. If enabled, switch software compares mobile port traffic to mobile VLAN rules to determine VLAN assignment for the mobile port. If disabled, mobility is inactive regardless of the status of mobility on individual VLANs and/or ports. By default, this parameter is **disabled**.

Move to Default Group on Aging

Determines if a mobile port returns to its default VLAN when port traffic that classified the port into another mobile VLAN ages out. If this parameter is set to **off**, then the port will drop a mobile VLAN port assignment when the qualifying traffic ages out. If this parameter is set to **on**, the port will retain the mobile VLAN port assignment after the qualifying traffic has aged out. By default, this parameter is set to **off**.

Use Default Group

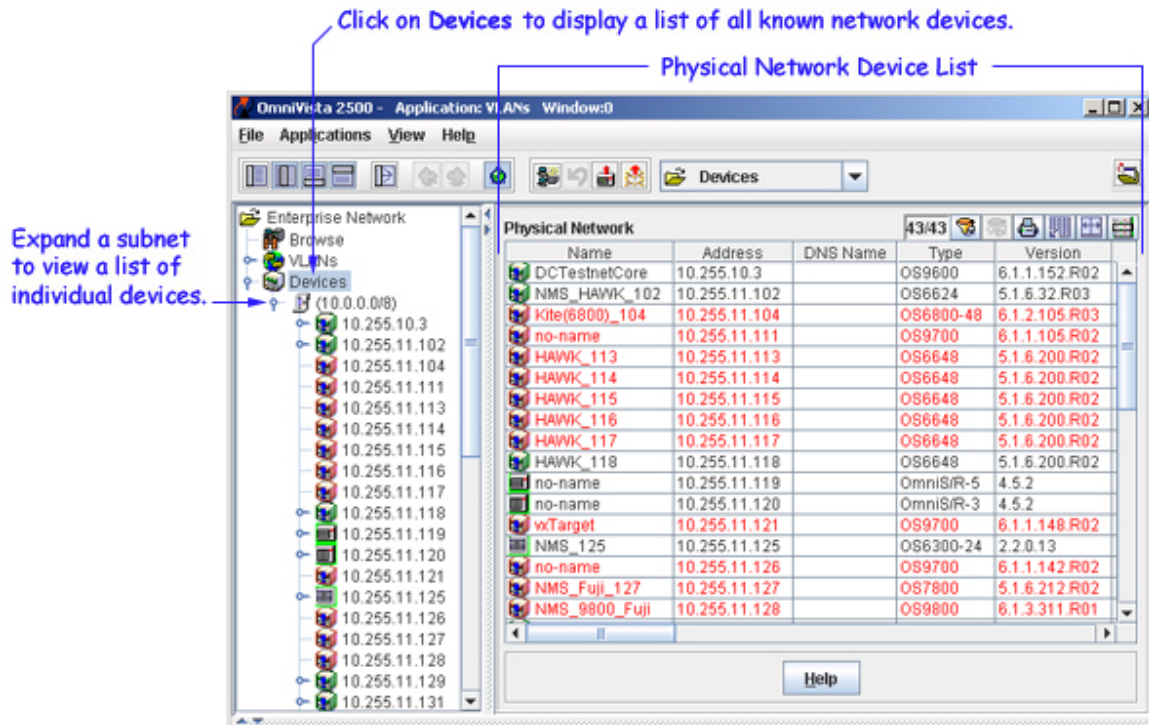
Determines if the default VLAN for a mobile port will carry traffic received on that port that does not match any VLAN rules. If this parameter is set to **on**, then non-matching traffic is forwarded on the default VLAN. If this parameter is set to **off**, then non-matching traffic is discarded and not allowed on the default VLAN. By default, this parameter is set to **on**.

Using the Devices Physical Network List

The Devices portion of the Tree provides a list of all AOS, XOS, and OmniStack devices known to the VLANs application. To display this list, select **Devices** in the Tree, as shown below. Each device entry in this list contains fields that display related system parameter values, such as device name, management IP address, etc.

Note: The term "OmniStack" refers only to OmniStack models 6024, 6048, 6124, 6148, 6300-24, and 8088. The term "XOS" includes all other OmniStack devices that run XOS software.

To view individual devices in the physical network, click open **Devices** to view a list of known subnets. You can then click open a subnet in the Tree to view a list of individual devices that belong to that subnet. Each device in the subnet is listed by its management IP address.



Information Fields in the List

Name

The name of the device.

Address

The address of the device.

DNS Name

The DNS name of the device.

Type

The type of the device chassis.

Version

The version number of the device software. OmniVista may not be able to determine the software version on some third-party devices. In these cases, the field will be blank.

Last Upgrade Status

The status of the last firmware upgrade on the switch.

- "Successful" - Successful BMF and Image upgrade performed.
- "Successful (BMF)" - Successful BMF upgrade performed.
- "Successful (Image)" - Successful Image upgrade is performed.
- "Failed (BMF, Image)" - BMF and Image upgrade failed.
- "Failed (BMF)" - BMF upgrade failed.
- "Failed (Image)" - Image upgrade failed.

In all "Failed" cases, "Reload From Working" will be disabled on the switch until a successful upgrade is performed.

Backup Date

The date that the device's configuration and/or image files were last backed-up to the OmniVista server.

Backup Version

The firmware version of the configuration and/or image files that were last backed-up to the OmniVista server

Last Known Up At

The date and time when the last poll was initiated on the device.

Description

A description of the device, usually the vendor name and model.

Status

This field displays the operational status of the device. It displays **Up** if the device is up and responding to polls. (When a device is up, it displays green in both the List of All Discovered Devices and the tree.) It displays **Down** if the device is down and not responding to polls. (When a device is down, it displays red in both the List of All Discovered Devices and the tree.) This field displays **Warning** if the switch has sent at least one warning or critical trap and is thus in the warning state. (When a device is in the warning state, it displays orange in both the List of All Discovered Devices and the tree.)

Traps

This field indicates the status of trap configuration for the device. **On** means that traps are enabled. **Off** means that traps are disabled. **Not Configurable** means that traps for this device are not configurable from OmniVista. (Note that traps may have been configured for such devices outside of OmniVista.) **Unknown** means that OmniVista does not know the status of trap configuration on this switch. OmniVista will read the switch's trap configuration when traps are configured for the switch via the Configure Traps Wizard.

Seen By

This field lists the Security Groups that are allowed to view the device. (The Security Groups that are allowed to view a device can be defined when devices are autodiscovered, added manually, or edited.) The default Security Groups shipped with OmniVista are as follows:

- **Default** group. This group has read-only access to switches in the list of All Discovered Devices that are configured to grant access to this group.
- **Writers** group. 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 autodiscovery nor can they manually add, delete, or modify entries in the list of All Discovered Devices.
- **Network Administrators** group. This group has full administrative access rights to all switches on the network. Members of this group can run autodiscovery 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 application and the Control Panel application. Members of this group can do everything EXCEPT make changes to Security Groups.
- **Administrators** group. This group has all administrative access rights granted to the Network Administrators group AND full administrative rights to make changes to Security Groups.

Note that other Security Group names may display in this field if custom Security Groups were created. Refer to help for the Security application *Users and Groups* for further information on Security Groups.

Running From

For AOS devices, this field indicates whether the switch is running from the **certified** directory or from the **working** directory. This field is blank for all other devices. For AOS devices, the directory structure that stores the switch's image and configuration files in flash memory is divided into two parts:

- The certified directory contains files that have been certified by an authorized user as the default configuration files for the switch. When the switch reboots, it will automatically load its configuration files from the certified directory if the switch detects a difference between the certified directory and the working directory. (Note that you can specifically command a switch to reboot from either directory -- [click here for information](#).)
- The working directory contains files that may or may not have been altered from those in the certified directory. The working directory is a holding place for new files to be tested before committing the files to the certified directory. You can save configuration changes to the working directory. You cannot save configuration changes directly to the certified directory.

Note that the files in the certified directory and in the working directory may be different from the running configuration of the switch, which is contained in RAM. The running configuration is the current operating parameters of the switch, which are originally loaded from the certified or working directory but may have been modified through CLI commands, WebView commands, or OmniVista. Modifications made to the running configuration must be saved to the working directory (or lost). The working directory can then be copied to the certified directory if and when desired. [Click here for more information](#).

Changes

For AOS devices, this field indicates the state of changes made to the switch's configuration. This field is blank for all other devices. This field can display the following values:

- **Unsaved**. Changes have been made to the running configuration of the switch that have not been saved to the working directory.
- **Uncertified**. Changes have been saved to the working directory, but the working directory hasn't been copied to the certified directory. The working directory and the certified directory are thus different.
- **Blank**. When this field is blank for an AOS device, the implication is that OmniVista knows of no unsaved configuration changes and assumes that the working and certified directories in flash memory are identical.

OmniVista is now capable of tracking AOS configuration changes made through CLI commands or WebView, and so will reflect configuration changes made outside of OmniVista through these two interfaces in the Changes field. Information in the Changes field will be accurate as long as OmniVista has polled the switch since the last change was made (through any interface).

Note that it is possible a switch could be in a state where it is both Unsaved and Uncertified. In this situation **Unsaved** displays in the Changes field. Whenever an AOS device is in the Unsaved or Uncertified state, a blue exclamation mark displays on its icon ().

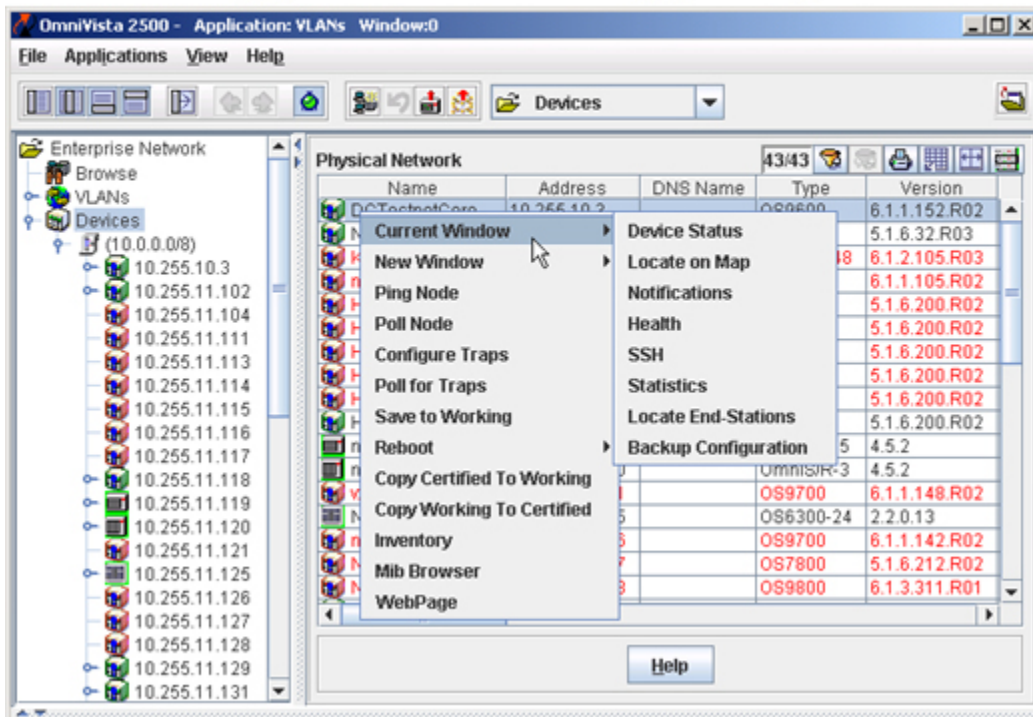
Discovered

This field displays the date and time when OmniVista successfully pings or polls the switch for the first time. This value remains unchanged until the switch entry is deleted. This field will remain blank if OmniVista does not ping or poll the switch at all.

Pop-Up Menu in the List

Click right on one or more devices in the Devices Physical Network list to display a pop-up menu. Somewhat different versions of the pop-up menu display for various devices. The pop-up menu for AOS devices is shown below. Each menu item allows you to launch additional applications and/or tasks to access, manage, or configure the selected device. For more information about these menu items, refer to the Topology application help.

Pop-Up Menu for AOS Devices
(Right-click on an AOS device to display the menu.)



Using the Devices Tree

Displaying the VLAN Configuration for a Device

The Devices portion of the Tree allows you to view VLAN information on an individual device basis. This provides you with a physical network view of your VLAN configuration, instead of a logical view of your network provided by the VLANs portion of the Tree.

To view all VLANs configured on an individual device, click on the device management IP address displayed in the subnet list. This activates the VLAN Definitions window for the selected device. For example, the VLAN Definitions window shown below is for an AOS device. This same window is displayed for XOS devices. However, a different VLAN Definitions window is displayed if an OmniStack device is selected (click here for more information about the OmniStack VLAN Definitions window).

Click on a device to display VLAN configurations.

Click on Mobility to configure port mobility.

Device VLAN Definitions

VLAN ID	Description	Admin Status	Oper Status	Type	Spanning Tree Status
1	VLAN 1	Enabled	Inactive	Standard	Enabled
10	TESTNET SERVERS ...	Enabled	Active	Standard	Enabled
27	VLAN 27	Enabled	Active	Standard	Enabled
50	TESTNET AREA 0 VL...	Enabled	Active	Standard	Enabled
206	STATIC AUTO1 206	Enabled	Active	Standard	Enabled
220	DHCP LABS 220	Enabled	Active	Standard	Enabled
243	CORPNET CONNEC...	Enabled	Active	Standard	Enabled
550	TESTNET AREA 0 D...	Enabled	Active	Standard	Enabled

View VLAN Definition

Description: Admin Status:

Oper Status: Type:

Spanning Tree Status: Mobility:

Authentication: Router-Protocol:

Voice Status:

Edit Update Delete Apply Help

In addition to displaying the VLAN configuration for an individual device, the VLAN Definitions window enables you to modify one or more VLAN definitions and configure port mobility parameters. For more information,

- Click here for help on configuring VLANs on AOS and XOS devices.
- Click here for help on configuring VLANs on OmniStack devices.
- Click here for help on configuring the mobility feature (only supported on AOS and XOS devices).

Pop-Up Menu in the Tree

Click right on any one device in the Tree to display a pop-up menu. This menu is the same pop-up menu displayed when you click on any device in the Devices Physical Network list. [Click here for more information about using the pop-up menu.](#)

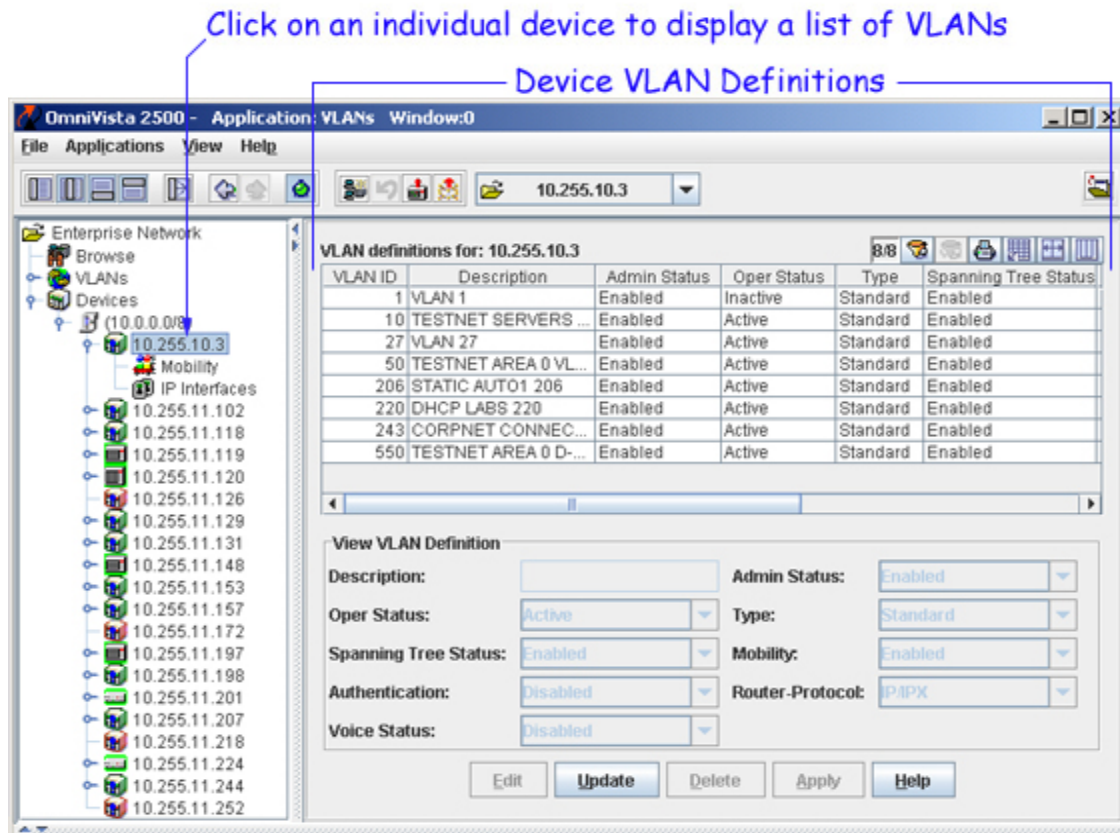
Managing AOS and XOS VLANs by Device

The Devices portion of the Tree allows you to view VLAN information on an individual device basis. This provides you with a physical network view of your VLAN configuration, as opposed to a logical view of your network provided by the VLANs portion of the Tree.

To view all VLANs configured on an individual AOS or XOS device, click on the device management IP address displayed in the subnet list. This activates the VLAN Definitions window, as shown below. Each entry in this table represents a VLAN that exists in the configuration for the selected device. From this window you can also modify parameters for one or more VLANs in the list.

If you click on an OmniStack device, a VLAN Definitions window also displays but contains different fields than those displayed if an AOS or XOS device is selected. Click here for more information about configuring VLANs on OmniStack devices.

Note: The term "OmniStack" refers only to OmniStack models 6024, 6048, 6124, 6148, 6300-24, and 8088. The term "XOS" includes all other OmniStack devices that run XOS software.



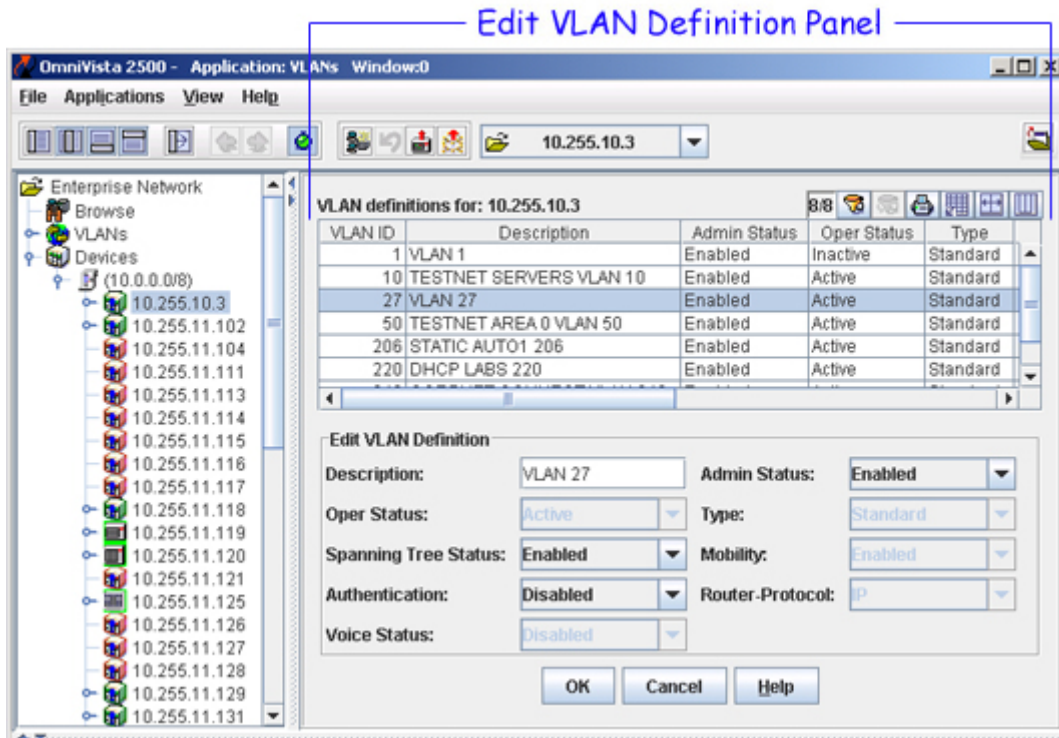
Modifying VLAN Definitions

When a VLAN is created, the administrative status and Spanning Tree status are enabled and authentication and mobility are disabled by default. In addition, the VLAN ID is used for the description if one is not specified. As a result, it is only necessary to modify these parameters if you want to change the default values. See VLAN Parameter Definitions below for more information.

When you modify VLAN parameters using the VLAN Definitions window, the changes are applied only to the selected device configuration. Use the VLANs or the VLAN Device List tables to modify a single VLAN definition across multiple devices.

To modify VLAN definitions for an individual device, select one or more VLANs from the VLAN Definition window and click the **Edit** button. This activates the Edit VLAN Definition panel, shown below. Parameters that are not modifiable from this panel or are not supported in this release are grayed out.

If you select more than one VLAN to modify, an Edit VLAN Definitions popup window opens that contains only the configurable port parameters.



Using either the Edit VLAN Definition panel or popup window, make the desired parameter changes and click the **OK** button to return to the VLAN Definitions window list. A modify icon appears in the VLAN ID field for each of the modified VLANs. Click the **Apply** button to apply the VLAN parameter changes to the selected device configuration.

Removing a VLAN

When you delete a VLAN using the VLAN Definitions window, the VLAN is only removed from the selected device configuration. Use the VLANs or the VLANs Device List tables to remove a single VLAN from multiple devices.

To delete an existing VLAN from an individual device configuration, select one or more VLANs from the VLAN Definitions window list and click the **Delete** button. A delete icon appears in the VLAN ID field for each of the selected VLANs. The VLAN is not removed from the appropriate switch configurations until you click the **Apply** button.

If you encounter problems when attempting to delete a VLAN from an XOS switch configuration, try removing any switch ports that belong to that VLAN before attempting to delete the VLAN again.

VLAN Parameter Definitions

VLAN ID

In compliance with the IEEE 802.1Q standard, each VLAN is identified by a unique number, referred to as the VLAN ID. This number is assigned by the user at the time the VLAN is created and is not a modifiable parameter. When a network device packet is received on a port, the port's VLAN ID is inserted into the packet. The packet is then bridged to other ports that are assigned to the same VLAN ID. In essence, the VLAN broadcast domain is defined by a collection of ports and packets assigned to its VLAN ID.

Valid VLAN ID ranges for the supported devices are as follows:

AOS (range = 1-4094)
XOS (range = 1-5000)
OmniStack (range = 1-2048)

Note that these VLAN ID values do not indicate the number of VLANs supported on XOS and OmniStack devices. For example, XOS devices support up to 1024 VLANs, but a VLAN ID number between 1 and 5000 is allowed. OmniStack devices support up to 256 VLANs, but a VLAN ID number between 1 and 2048 is allowed. However, on AOS devices, there is a one-to-one correlation between the number of VLANs supported (4094) and the valid VLAN ID range (1-4094).

Description

A text string up to 32 characters (30 characters for XOS VLANs). This parameter defaults to the VLAN ID number (e.g., VLAN #10) if a description was not specified at the time the VLAN was created.

Admin Status

The administrative status (Enabled/Disabled) for the VLAN. By default, the administrative status is enabled when a VLAN is created.

When a VLAN is administratively disabled, static port and dynamic mobile port assignments are retained but traffic on these ports is not forwarded. However, VLAN rules remain active and continue to classify mobile port traffic for VLAN membership.

Oper Status

The VLAN operational status (Active/Inactive). This parameter is not modifiable; switch software determines if the VLAN is operationally active or inactive and sets the appropriate field value.

A VLAN's operational status remains inactive until at least one active switch port is assigned to the VLAN and the VLAN's administrative status is enabled. This means that VLAN properties, such as Spanning Tree or router ports, also remain inactive. Ports are considered active if they are connected to an active network device. Non-active port assignments are allowed, but do not change the VLAN's operational state.

Type

The type of VLAN is determined at the time the VLAN is created. This field may contain one of the following values:

Standard

ATM CIP (supports Classical IP routing over ATM)*

Frame Relay Router (WAN routing VLAN that contains only WAN ports)*

MPLS RT (supports Multi-Protocol Label Switching routing over ATM)*

MPLS BR (supports Multi-Protocol Label Switching bridging over ATM)*

PTOP Routed (supports RFC 1483 routing over ATM)*

*Feature not supported on all switch platforms.

Spanning Tree Status

The Spanning Tree Status (Enabled/Disabled) for the VLAN. When a VLAN is created, an 802.1D standard Spanning Tree Algorithm and Protocol (STP) instance is enabled for the VLAN by default.

STP evaluates VLAN port connections to determine if there are redundant data paths between the same VLAN on other switches. If a redundant path does exist, STP determines which path to block in order to provide a loop-free network topology. In this manner, STP ensures that there is always only one active data path between any two switches (VLANs). When a change occurs, such as a path is disconnected or a path cost change, the Spanning Tree Algorithm activates the blocked path to restore the network connection.

Mobility

The mobile status (Enabled/Disabled) for the VLAN. On AOS switches, mobility is not enabled or disabled at the VLAN level. Instead, switch ports are designated as mobile or non-mobile. This parameter, however, displays "Enabled" for all AOS VLANs.

Authentication

The authentication status (Enabled/Disabled) for the VLAN. By default, authentication is disabled when a VLAN is created. Once authentication is enabled on a VLAN, however, then only authenticated mobile port devices can join the VLAN after completing the appropriate log-in process.

Layer 2 authentication uses VLAN membership to grant access to network resources. Authenticated VLANs control membership through a log-in process; this is sometimes called user authentication. A VLAN must have authentication enabled before it can participate in the Layer 2 authentication process.

Router Protocol

The protocol for the VLAN virtual router port (IP or IPX). If no router port is configured for the VLAN, then "none" appears in this field.

Alcatel switches support routing of IP and IPX traffic on a per VLAN basis. A VLAN is available for routing when a virtual router port is defined for that VLAN and at least one active port has joined the VLAN. If a VLAN does not have a router port, its ports are in essence firewalled from other VLANs.

Voice Status

Not supported for this release.

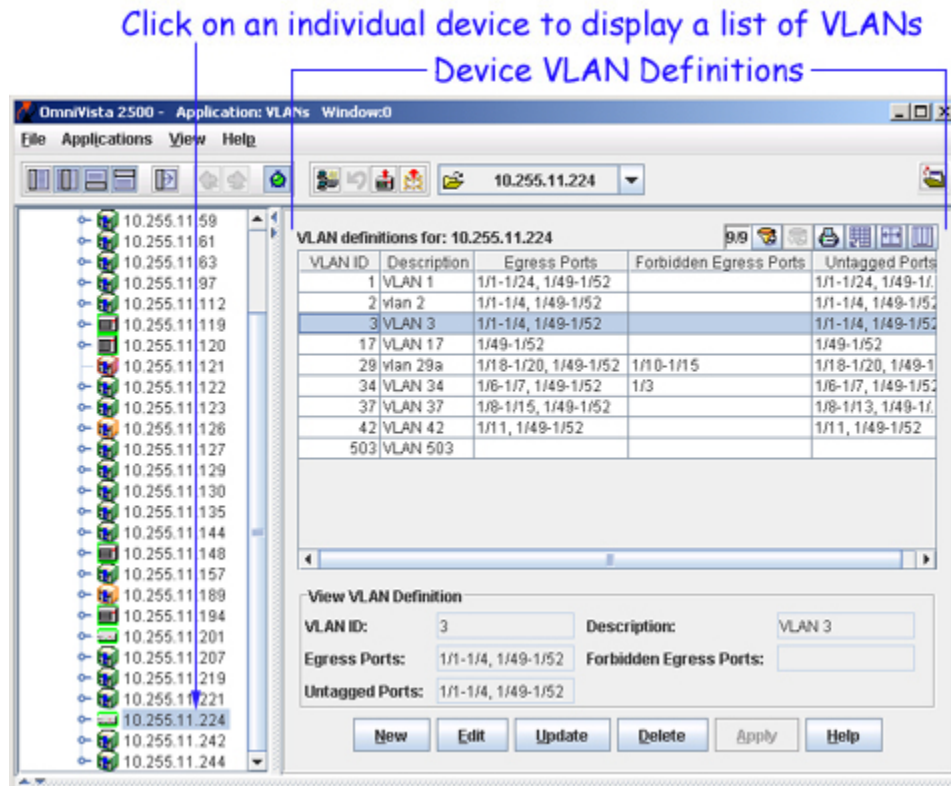
Managing OmniStack VLANs by Device

The Devices portion of the Tree allows you to view VLAN information on an individual device basis. This provides you with a physical network view of your VLAN configuration, as opposed to a logical view of your network provided by the VLANs portion of the Tree.

To view all VLANs configured on an individual OmniStack device, click on the device management IP address displayed in the subnet list. This activates the VLAN Definitions window, as shown below. Each entry in this table represents a VLAN that exists in the configuration for the selected device. From this window you can also add a new VLAN to the switch configuration and/or modify parameters for an existing VLAN.

Note: The term "OmniStack" refers only to OmniStack models 6024, 6048, 6124, 6148, 6300-24, and 8088. The term "XOS" includes all other OmniStack devices that run XOS software.

If you click on an AOS or XOS device management IP address, a VLAN Definitions window also displays but contains different fields than those displayed if an OmniStack device is selected. Click here for more information about configuring VLANs on AOS and XOS devices.



Adding a New VLAN

To add a VLAN to the configuration of the selected OmniStack device, click the **New** button found at the bottom of the VLAN Definitions window. This opens the Create VLAN pop-up window. Click here for information about how to create a VLAN definition using this window.

When you add a VLAN using the Create VLAN window, the new VLAN is only created on the selected device configuration. Use the VLANs table to modify a single VLAN definition across multiple devices.

Modifying VLAN Definitions

When a VLAN is created, the VLAN ID is used for the description if one is not specified and there are no ports assigned to the VLAN. As a result, it is only necessary to modify these parameters if you want to change the default values. See VLAN Parameter Definitions below for more information.

To modify an existing VLAN definition for an individual device, select one VLAN from the VLAN Definitions window and click the **Edit** button. This opens the Edit VLAN pop-up window. Click here for information about how to modify existing VLAN parameters.

When you modify VLAN parameters using the VLAN Definitions window, the changes are applied only to the selected device configuration. Use the VLANs table to modify a single VLAN definition across multiple devices.

Removing a VLAN

When you delete a VLAN using the VLAN Definitions window, the VLAN is only removed from the selected device configuration. Use the VLANs table to remove a single VLAN from multiple devices.

To delete an existing VLAN from an individual device configuration, select one or more VLANs from the VLAN Definitions window list and click the **Delete** button. A delete icon appears in the VLAN ID field for each of the selected VLANs. The VLAN is not removed from the appropriate switch configurations until you click the **Apply** button.

VLAN Parameter Definitions

VLAN ID

In compliance with the IEEE 802.1Q standard, each VLAN is identified by a unique number, referred to as the VLAN ID. This number is assigned by the user at the time the VLAN is created and is not a modifiable parameter. When a network device packet is received on a port, the port's VLAN ID is inserted into the packet. The packet is then bridged to other ports that are assigned to the same VLAN ID. In essence, the VLAN broadcast domain is defined by a collection of ports and packets assigned to its VLAN ID.

Valid VLAN ID ranges for supported devices are as follows:

AOS (range = 1-4094)

XOS (range = 1-5000)

OmniStack (range = 1-2048)

Note that these VLAN ID values do not indicate the number of VLANs supported on XOS and OmniStack devices. For example, XOS devices support up to 1024 VLANs, but a VLAN ID number between 1 and 5000 is allowed. OmniStack devices support up to 256 VLANs, but a VLAN ID number between 1 and 2048 is allowed. However, on AOS devices, there is a one-to-one correlation between the number of VLANs supported (4094) and the valid VLAN ID range (1-4094).

Description

A text string up to 32 characters (30 characters for XOS VLANs). This parameter defaults to the VLAN ID number (e.g., VLAN #10) if a description was not specified at the time the VLAN was created.

Egress Ports

Ports that are associated to the VLAN (tagged or untagged) for forwarding VLAN traffic.

Forbidden Egress Ports

Ports that are blocked from automatic assignment to the VLAN by a GVRP operation. Note that GVRP is not supported on all OmniStack platforms.

Untagged Ports

Egress ports that are assigned as untagged ports to the VLAN. The VLAN is the default VLAN for these ports. Note that these ports must already have an egress port association with the VLAN. If egress ports do not appear in the untagged ports list, then they have a tagged association with the VLAN.

Using the dot1qPortVlan Table

The VLAN Bridge MIB (qBridgeMIB) contains the dot1qPortVlan table that is used to view and configure 802.1Q VLAN attributes for a specific port. As shown below, you can access this table by clicking open an OmniStack switch management IP address in the Devices Tree and then clicking on the Ports node.

Click on Ports to display 802.1Q VLAN Port Attributes

dot1qPort VLAN Table

The screenshot shows the 'Ports' node selected in the Devices Tree. The main window displays the 'dot1qPort VLAN Table' with the following data:

Slot/Port	VLAN ID	Frame Type	Ingress Filtering	GVRP Status	Failed Registrat
1/1	1	admitAll	false	disabled	
1/2	1	admitAll	false	disabled	
1/3	1	admitAll	false	disabled	
1/4	1	admitAll	false	disabled	
1/5	1	admitAll	false	disabled	
1/6	1	admitAll	false	disabled	
1/7	1	admitAll	false	disabled	
1/8	1	admitAll	false	disabled	

Below the table is the 'View dot1qPort VLAN Attributes' panel for the selected port 1/3:

Slot/Port: 1/3 VLAN ID: 1
 Frame Type: admitAll Ingress Filtering: false
 GVRP Status: disabled Failed Registrations: 0
 Last PDU Origin: 000000.000000

Buttons: Edit, Update, Apply, Help

The dot1qPortVlan Table displays a list of all OmniStack ports and the current status and/or value of the 802.1Q VLAN attributes for each port. When you click on one of the ports in this list, the bottom portion of the screen displays the current attribute values for the selected port.

To modify an 802.1Q VLAN attribute for a specific port, select one or more ports from the dot1qPortVlan Table list and click the **Edit** button. This activates the Edit dot1qPortVlan Attributes panel. If you select more than one port to modify, an Edit dot1qPortVlan Attributes pop-up window opens that contains the configurable port parameters.

Edit dot1qPort VLAN Attributes Panel

Slot/Port	VLAN ID	Frame Type	Ingress Filtering	GVRP Status	Failed Registrat
1/1	1	admitAll	false	disabled	
1/2	1	admitAll	false	disabled	
1/3	1	admitAll	false	disabled	
1/4	1	admitAll	false	disabled	
1/5	1	admitAll	false	disabled	
1/6	1	admitAll	false	disabled	
1/7	1	admitAll	false	disabled	
1/8	1	admitAll	false	disabled	

Edit dot1qPort VLAN Attributes					
Slot/Port:	<input type="text" value="1/3"/>	VLAN ID:	<input type="text" value="1"/>		
Frame Type:	<input type="text" value="admitAll"/>	Ingress Filtering:	<input type="text" value="false"/>		
GVRP Status:	<input type="text" value="disabled"/>	Failed Registrations:	<input type="text" value="0"/>		
Last PDU Origin:	<input type="text" value="000000:000000"/>				
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>					

Using either the Edit dot1qPort VLAN Attributes panel or pop-up window, make the desired parameter changes and click the **OK** button to return to the dot1qPortVlan Table list. A modify icon appears in the Slot/Port field for the modified port. Click the **Apply** button to apply the changes to the appropriate switch configuration.

802.1Q VLAN Port Attribute Definitions

Slot/Port

The slot/port designation that identifies the slot number that corresponds to the OmniStack's position within a stack and the port number on that OmniStack device. (e.g., 3/1 specifies port 1 on the third OmniStack from the bottom of the stack).

VLAN ID

The VLAN ID number that is assigned to untagged frames or priority-tagged frames received on the port. Select a VLAN ID number between 1 and 2048. By default, this attribute is set to VLAN ID "1".

Frame Type

Indicates the type of frames that are allowed on the port. If this attribute is set to **admitAll**, then all frames received on the port are accepted. Untagged and priority-tagged frames received are assigned to the VLAN ID for the port. If this attribute is set to **admitOnlyVlanTagged**, then only tagged frames received on the port are accepted. Untagged and priority-tagged frames are discarded. By default, this attribute is set to **admitAll**.

Ingress Filtering

If this attribute is set to **true**, then only frames received on the port that contain a VLAN ID that the port is associated with are accepted. All other frames are discarded. If this attribute is set to **false**, then frames are not qualified by their VLAN ID content and are accepted on the port. By default, this attribute is set to **false**.

Note that this attribute does not affect VLAN independent BPDU frames (i.e. GVRP, STP). VLAN dependent BPDU frames, such as GMRP, are affected by this attribute.

GVRP Status

Indicates if GVRP is **enabled** or **disabled** on the port. If this attribute is set to **enabled**, you must also enable the GVRP feature for the device. If this attribute is set to **disabled**, then GVRP packets are discarded and GVRP registrations are not forwarded from other ports. By default, this attribute is set to **disabled**.


Failed Registrations

Indicates the total number of failed GVRP registrations for this port.

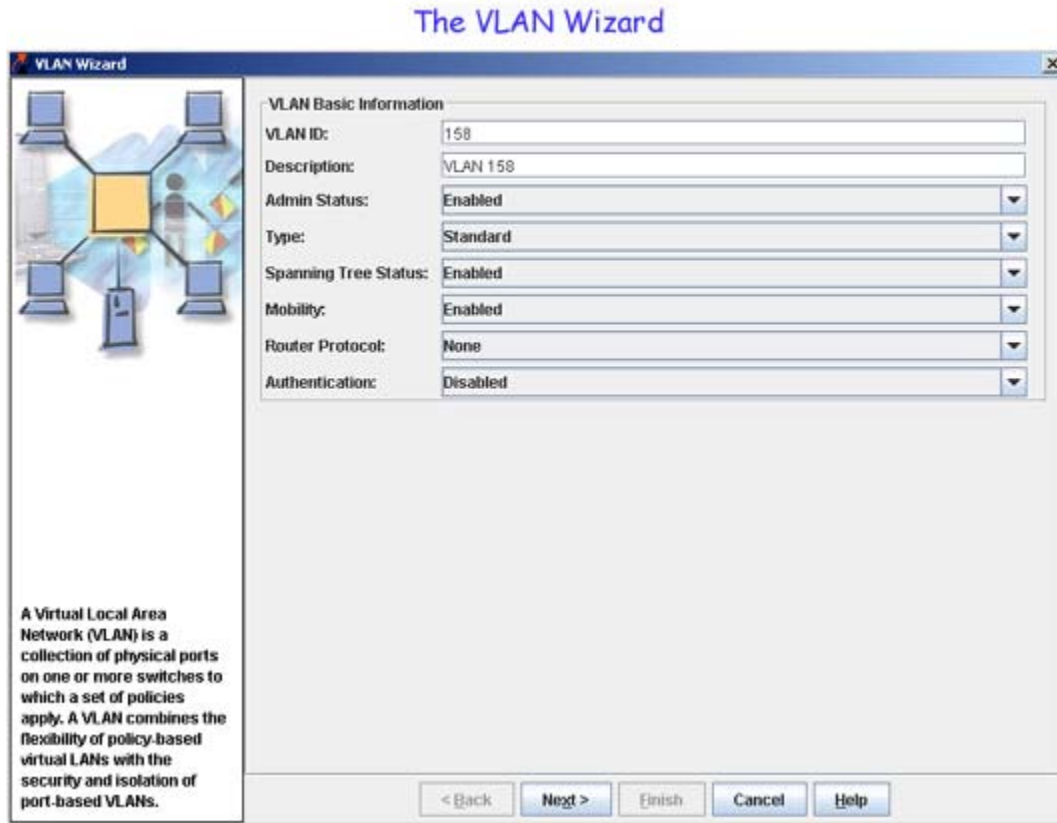
Last PDU Origin

Provides the source MAC address of the last GVRP message received on the port.

Using the VLAN Wizard

To display the VLAN Wizard, click the VLAN Wizard icon . The VLAN Wizard enables you to create new VLANs across multiple XOS, AOS, and OmniStack devices, assign router interfaces to the new VLANs, and define rules for AOS and XOS VLANs. The opening window of the VLAN Wizard, shown below, enables you to define basic information about the new VLAN. Only one VLAN Wizard window can be open at a time.

Note: You can also modify an existing VLAN using the VLAN Wizard by entering the existing **VLAN ID** and clicking the **Next** button to modify the VLAN parameters.



VLAN Basic Information Fields

The VLAN Basic Information page is used to define basic configuration parameters for the new VLAN. The fields are described below.

VLAN ID

Enter the desired VLAN ID or accept the default displayed. This field defaults to the next available VLAN ID that does not already exist on the network. If you enter a VLAN ID greater than 4094 only XOS devices will be allowed in the VLAN. (See valid VLAN ID ranges below for more information.) In addition, if you enter a VLAN ID greater than 2048, OmniStack devices are *not* allowed in the VLAN.

Note: The term "OmniStack" refers only to OmniStack models 6024, 6048, 6124, 6148, and 8088. The term "XOS" includes all other OmniStack devices that run XOS software.

Valid VLAN ID ranges for the supported devices are as follows:

AOS (range = 1-4094)
XOS (range = 1-65535)
OmniStack (range = 1-2048)

Note that these VLAN ID values do not indicate the number of VLANs supported on XOS and OmniStack devices. For example, XOS devices support up to 1024 VLANs, but a VLAN ID number between 1 and 5000 is allowed. OmniStack devices support up to 256 VLANs, but a VLAN ID number between 1 and 2048 is allowed. However, on AOS devices, there is a one-to-one correlation between the number of VLANs supported (4094) and the valid VLAN ID range (1-4094).

Description

Enter the desired description for the new VLAN or accept the default displayed. The description is a text string of up to 32 characters (30 characters for XOS VLANs). If you do not enter a description, this parameter defaults to the VLAN ID number (e.g., VLAN 18).

Admin Status

Set the admin status to **Enabled** or **Disabled** to specify the admin status the VLAN will have when it is created. When a VLAN is administratively disabled, static port and dynamic mobile port assignments are retained but traffic on these ports is not forwarded. However, VLAN rules remain active and continue to classify mobile port traffic for VLAN membership.

Type

This field should be set to **Standard** if the new VLAN will contain AOS devices or a mix of AOS and XOS devices. If this field is set to any value other than **Standard**, only XOS devices may be placed into the VLAN. (When this field is set to any value other than **Standard**, the next page of the Wizard, which enables you to select devices for the VLAN, will display XOS devices only. In addition, Authentication will be defaulted to "off".) If the VLAN is for XOS devices only, you can set this field to:

- **Standard**
- **ATM CIP** (supports Classical IP routing over ATM)
- **Frame Relay Router** (WAN routing VLAN that contains only WAN ports)
- **MPLS RT** (supports Multi-Protocol Label Switching routing over ATM)
- **MPLS BR** (supports Multi-Protocol Label Switching bridging over ATM)
- **PTOP Routed** (supports RFC 1483 routing over ATM)

Note: This parameter not supported on all OmniStack models.

Spanning Tree Status

Set this field to **Enabled** or **Disabled** to specify the state of Spanning Tree when the VLAN is created. When this field is set to **Enabled**, an 802.1D standard Spanning Tree Algorithm and Protocol (STP) instance is enabled for the VLAN.

STP evaluates VLAN port connections to determine if there are redundant data paths between the same VLAN on other switches. If a redundant path does exist, STP determines which path to block in order to provide a loop-free network topology. In this manner, STP ensures that there is always only one active data path between any two switches (VLANs). When a change occurs, such as a path is disconnected or a path cost change, the Spanning Tree Algorithm activates the blocked path to restore the network connection.

Note: This parameter not supported on all OmniStack models.

Mobility

Set this field to **Enabled** or **Disabled** to specify the mobile status for the VLAN. On AOS switches, mobility is not enabled or disabled at the VLAN level. Instead, switch ports are designated as mobile or non-mobile.

Note: This parameter not supported on all OmniStack models.

Router Protocol

Set this field to **None**, **IP**, **IPX**, **IP/IPX** to specify the protocol for the VLAN router interface. When set to **None**, no router interface will be configured for the VLAN. Note that if you set this field to **None**, the VLAN Wizard will not display the IP/IPX configuration page.

Note: You can configure up to eight (8) IP interfaces per VLAN on 7000/8000 (Release 5.1.6) and 6800/6850/9000 (Release 6.1.1) switches. You can only configure one (1) IP interface on 6600 XOS devices.

Alcatel switches support routing of IP and IPX traffic on a per VLAN basis. A VLAN is available for routing when a router interface is defined for that VLAN and at least one active port has joined the VLAN. If a VLAN does not have a router interface, its ports are in essence firewalled from other VLANs.

Note: This parameter not supported on all OmniStack models.

Authentication

Set this field to **Enabled** or **Disabled** to specify the authentication status for the VLAN. When authentication is enabled on a VLAN, only authenticated mobile port devices can join the VLAN after completing the appropriate log-in process.

Layer 2 authentication uses VLAN membership to grant access to network resources. Authenticated VLANs control membership through a log-in process; this is sometimes called user authentication. A VLAN must have authentication enabled before it can participate in the Layer 2 authentication process.

Note: This parameter not supported on all OmniStack models.

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

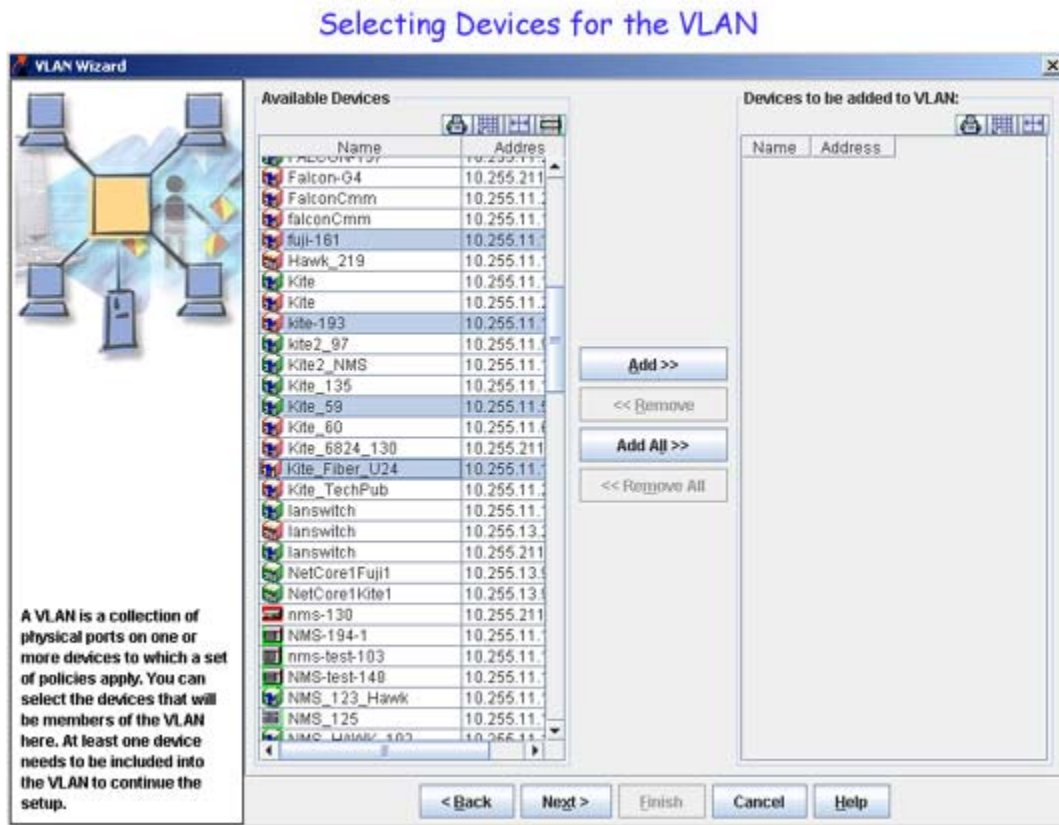
Selecting Devices for the VLAN

The second page of the VLAN Wizard, shown below, enables you to select the devices for the VLAN. (The third page of the VLAN Wizard enables you to select the specific ports that you want in the VLAN.)

The Available Devices area displays all XOS, AOS, and OmniStack devices for your selection. However, if you set the VLAN **Type** field on the previous page to anything other than **Standard**, or if you entered a VLAN ID greater than 4094, only XOS devices are displayed for your selection. In addition, if you entered a VLAN ID greater than 2048, OmniStack devices are *not* displayed for your selection.

Note: The term "OmniStack" refers only to OmniStack models 6024, 6048, 6124, 6148, 6300-24, and 8088. The term "XOS" includes all other OmniStack devices that run XOS software.

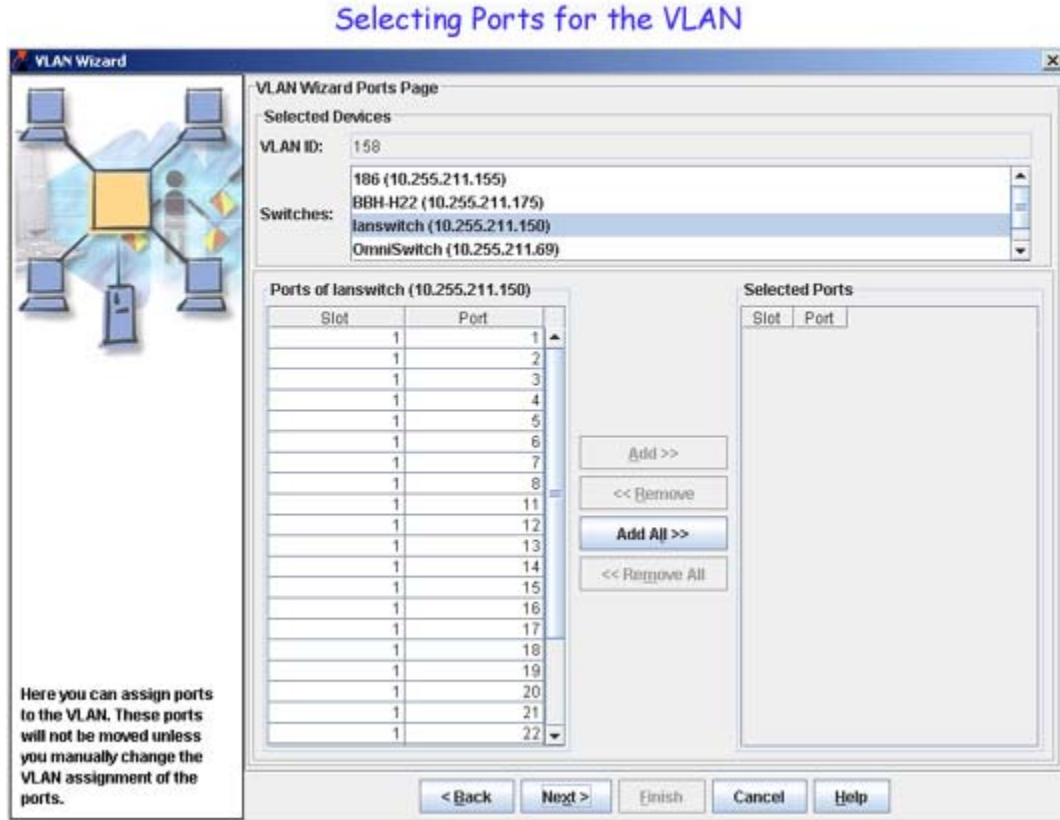
To select devices for the VLAN, select devices in the Available Devices area and move them into the Devices to be Added to VLAN area. To do this, use the **Add >>**, **<< Remove**, **Add All >>**, and **<< Remove All** buttons. Note that you can select multiple contiguous devices by **Shift**-clicking and multiple noncontiguous devices by **Ctrl**-clicking.



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

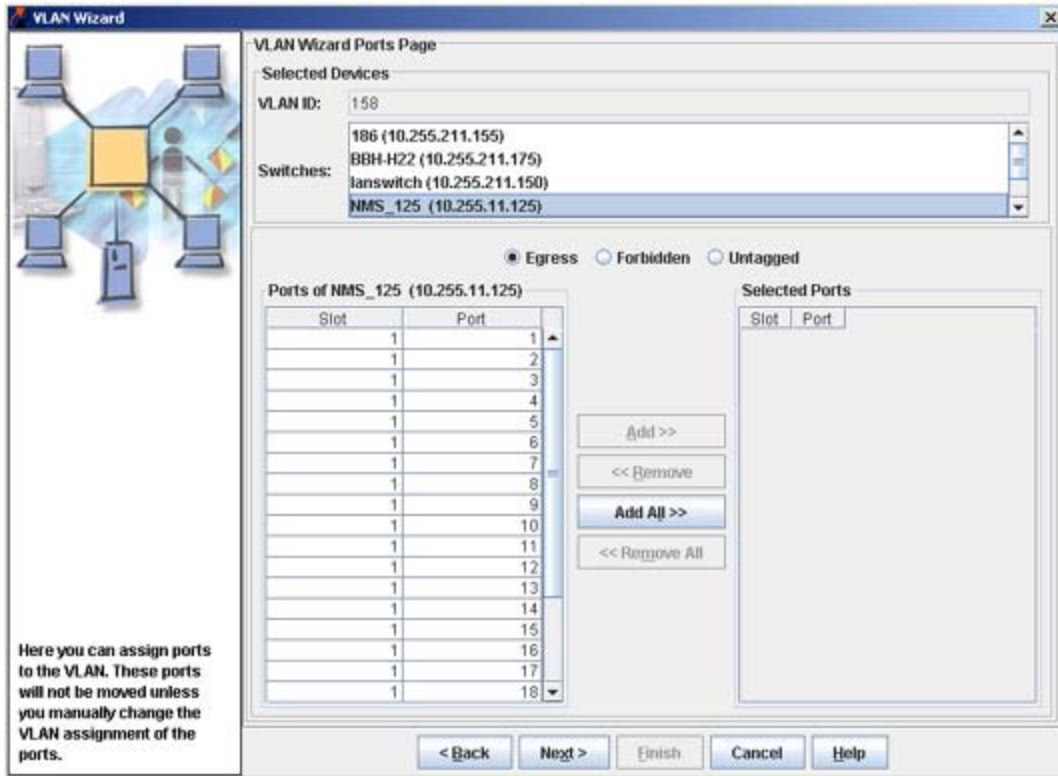
Selecting Ports for the VLAN

The third page of the VLAN Wizard, shown below, enables you to select ports for the VLAN. All of the switches that you selected on the previous page are listed in the Switches area. Click on a switch in the Switches area to display its slots and ports in the Ports of ... area. Move ports from the Ports of ... area to the Selected Ports area using the **Add >>**, **<< Remove**, **Add All >>**, and **<< Remove All** buttons. Note that you can select multiple contiguous ports by **Shift**-clicking and multiple noncontiguous ports by **Ctrl**-clicking. Repeat the procedure for the remaining switches in the Switches area until all desired switch ports are listed in the Selected Ports area.



Note that if you select an OmniStack 6024, 6048, 6124, 6148, 6300-24, or 8008 in the Switches area list, the VLAN Wizard Ports Page displays **Egress**, **Forbidden**, and **Untagged** buttons, as shown below. The **Egress** button is enabled by default and designates a VLAN port assignment (VPA) between the selected ports and the VLAN. Enable the **Forbidden** button to identify ports that you do not want the GVRP protocol to automatically assign to the VLAN (note that GVRP is not supported on all OmniStack platforms). Enable the **Untagged** button to designate this VLAN as the default VLAN for the selected port(s).

Selecting OmniStack Ports for the VLAN

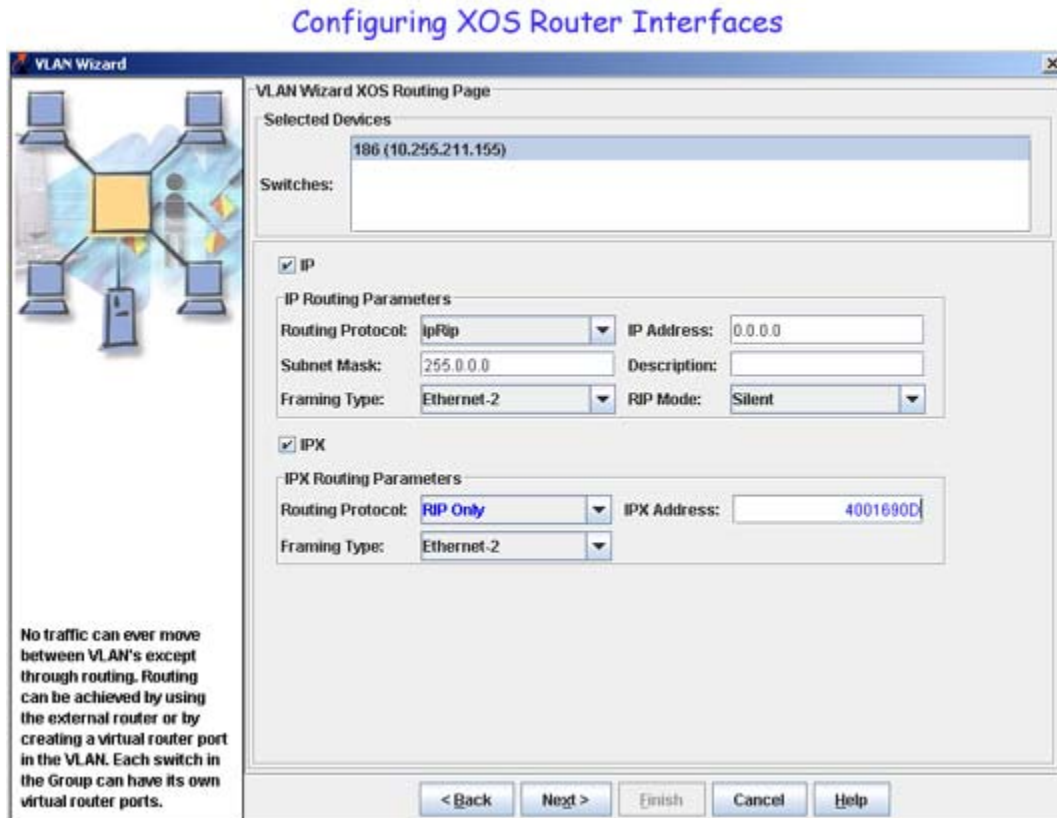


Click the **Next** button when you have made your selections

Configuring XOS Router Interfaces

This page of the VLAN Wizard enables you to configure IP and IPX router interfaces for the XOS devices you added to the VLAN. (If you also added AOS devices to the VLAN, the next page of the Wizard will enable you to configure router interfaces for the AOS devices.) Follow the steps below to configure IP and/or IPX router interfaces for XOS devices in the VLAN.

Note: You can configure one (1) IP and one (1) IPX interface on the switch for each VLAN.



1. Select the switch in the Switches area that you want to configure. The Switches area displays all XOS devices that you added to the VLAN.

2. If you want to configure an IP router interface, click the **IP** checkbox to enable it and perform the following steps:

a. Set the **Routing Protocol** field to the desired routing protocol. This parameter value is not configurable on all XOS devices. In most cases, the default value of **IpRip** is sufficient. Consult the IP routing software and configuration you are running before attempting to change this parameter value.

b. Enter an IP address in the **IP Address** field (e.g., 198.181.10.2). This address is assigned to the IP router interface and enables routing of VLAN traffic on that device.

c. Tab to or click on the **Subnet Mask** field and a default subnet mask value for the IP address class is automatically entered in this field. It is only necessary to change this field value if you want to use a different subnet mask.

d. Enter an optional alphanumeric router interface description (up to 30 characters) in the **Description** field.

e. Select the router interface encapsulation from the **Framing Type** field list. The frame encapsulation determines the framing type the router interface uses when generating frames that are forwarded out VLAN ports. Select an encapsulation that matches the encapsulation of the majority of IP VLAN traffic. You can set the frame type encapsulation to any of the following values:

- **Ethernet 2**
- **Ethernet 802.3** (SNAP)
- **FDDI**
- **Token Ring** (802.5)
- **Token Ring Source Routed**
- **ATM 1483**.

By default, this parameter is set to **Ethernet 2** when the router interface is defined. If the encapsulation used by a VLAN device does not match the router interface type, then device frames are translated before they are forwarded on by the router interface to the appropriate subnet.

f. Select the RIP operational mode from the **RIP Mode** field list. You can set the RIP operational mode to any of the following values:

- **Silent**. RIP is active and receives routing information from other VLANs, but does not send out RIP updates. Other VLANs will not receive routing information concerning this VLAN and will not include the VLAN in their routing tables.
- **Deaf**. RIP is active and sends routing information to other VLANs, but does not receive RIP updates from other VLANs. The VLAN will not receive routing information from other VLANs and will not include other VLANs in its routing table.
- **Active**. RIP is active and both sends and receives RIP updates. The VLAN will receive routing information from other VLANs and other VLANs will include this VLAN in their routing tables.
- **Inactive**. RIP is inactive and neither sends nor receives RIP updates. The VLAN will neither send nor receive routing information to/from other VLANs.

By default, the RIP mode is set to **Silent** (RIP listens for routing updates, but does not send them).

3. If you want to configure an IPX router interface, click the **IPX** checkbox to enable it and perform the following steps:

a. Set the **Routing Protocol** field to one of the following values:

- **RIP Only** (RIP updates are processed)
- **RIP and SAP** (RIP and SAP updates are processed)
- **Triggered** (RIP and SAP updates are broadcast only when updates occur).

b. In the **IPX Address** field, enter the IPX network address that identifies the router interface network. An IPX network address consists of eight hex characters (e.g., 4001690D). If fewer than eight hex digits is specified, the address is prefixed with zeros to equal eight digits.

c. Set the **Framing Type** field to define the type of IPX router interface frame encapsulation. The encapsulation determines the framing type the router interface uses when generating frames that are forwarded out VLAN ports. Use an encapsulation value that matches the encapsulation of the majority of IPX VLAN traffic. You can set the frame type encapsulation to any of the following values:

- Ethernet 2
- Ethernet 802.3 llc
- Ethernet 802.3 snap
- Ethernet 802.3 raw
- FDDI-snap
- FDDI-snap sr (Source Routing)
- FDDI-llc
- FDDI-llc-sr (Source Routing)
- Token Ring-snap
- Token Ring-snap-sr (Source Routing)
- Token Ring-llc
- Token Ring-llc-sr (Source Routing).

By default, this parameter is set to **Ethernet 2**. If the encapsulation used by a VLAN device does not match the router interface frame type, then device frames are translated before they are forwarded on by the router interface to the appropriate subnet.

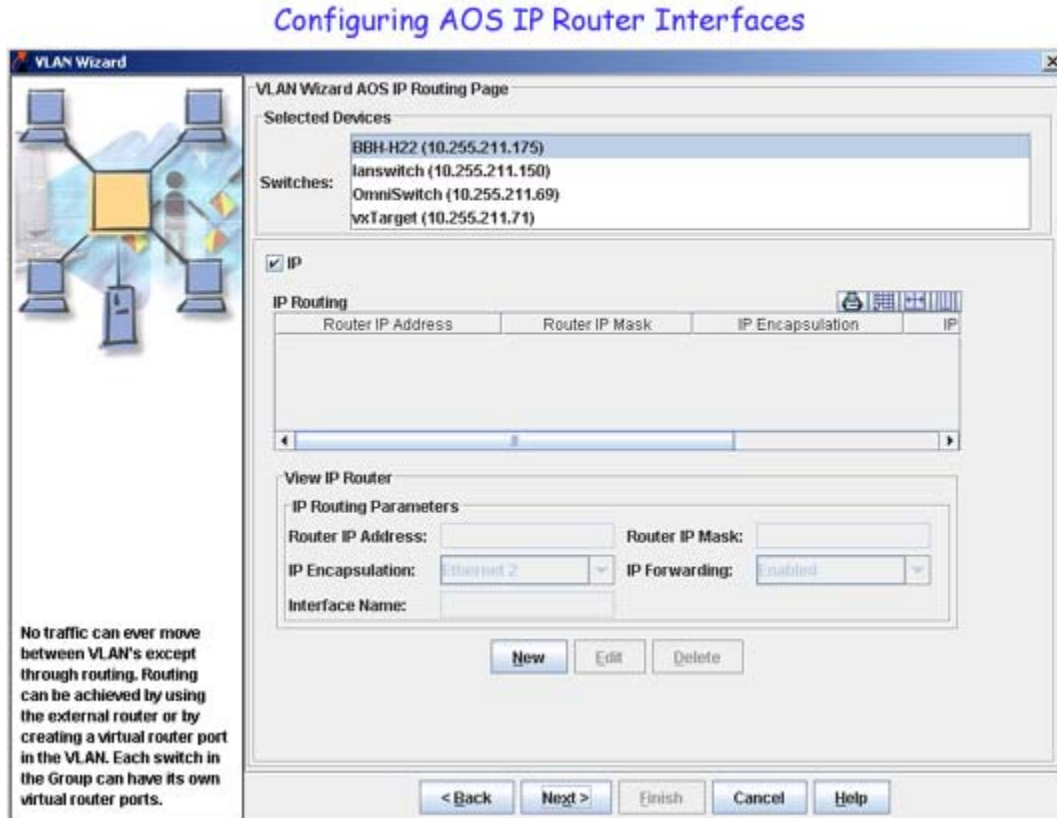
4. Continue to select switches in the Switches area and configure IP and/or IPX routing interfaces as desired.

Click the **Next** button when all desired switches have been configured

Configuring AOS IP Router Interfaces

If you selected **IP** or **IP/IPX** as the Routing Protocol on the VLAN Basic Information page of the VLAN Wizard, the following page will be available. This page enables you to configure IP router interfaces for the AOS devices you added to the VLAN.

Note: You can configure up to eight (8) IP interfaces per VLAN on 7000/8000 (Release 5.1.6) and 6800/6850/9000 (Release 6.1.1) switches. You can only configure one (1) IP interface on 6600 XOS devices.



1. In the Switches area, select the switch that you want to configure. The Switches area displays all AOS devices that you added to the VLAN.

2. Click the **New** button and complete the IP Router Parameters fields.

a. Enter an IP address in the **Router IP Address** field (e.g., 198.181.10.2). This address is assigned to the IP router interface and enables routing of VLAN traffic on that device. The router interface address must be unique. You cannot have two router interfaces with the same address.

b. Tab to or click on the **Router IP Mask** field and a default subnet mask value for the IP address class is automatically entered in this field. It is only necessary to change this field value if you want to use a different subnet mask.

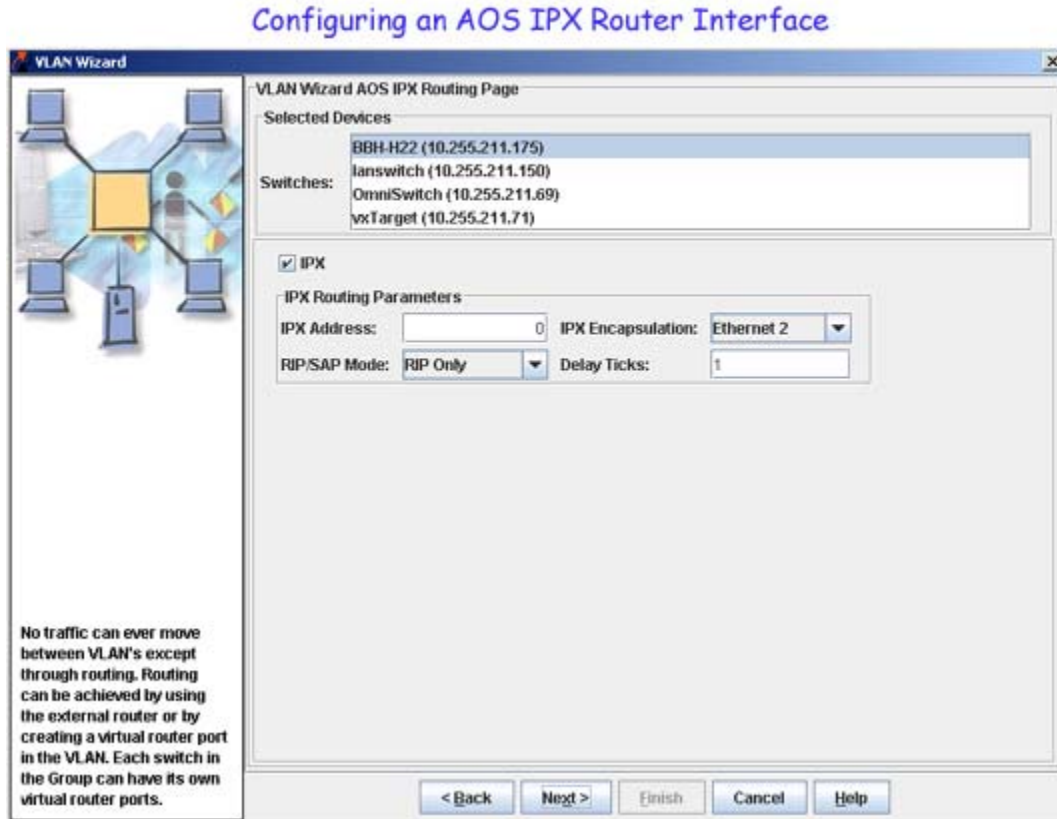
- c.** Select the router interface encapsulation from the **IP Encapsulation** field list. The frame encapsulation determines the framing type the router interface uses when generating frames that are forwarded out VLAN ports. Select an encapsulation that matches the encapsulation of the majority of IP VLAN traffic. You can set the frame type encapsulation to **Ethernet**, **Snap**, or **Not Applicable**.
 - d.** Set the **IP Forwarding** field to **Enable**, **Disable**, or **Not Applicable**. A forwarding router interface sends IP frames to other subnets. A no forwarding router interface acts as a host only; receives IP frames from other router interfaces. By default, this parameter is set to **Enabled**.
 - e.** Enter a unique interface name (text string up to 20 characters) in the **Interface Name** field.
- 3.** Click the **New** button to configure additional router interfaces for the switch; or select additional switches in the Switches area and configure IP router interfaces as desired (7000, 8000 and 9000 switches).

Click the **Next** button when all desired switches have been configured

Configuring AOS IPX Router Interfaces

If you selected **IPX** or **IP/IPX** as the Routing Protocol on the VLAN Basic Information page of the VLAN Wizard, the following page will be available. This page enables you to configure IPX router interfaces for the AOS devices you added to the VLAN.

Note: You can configure one (1) IPX interface on the switch for each VLAN. IPX routing is not supported on OmniSwitch 6600 series switches.



1. In the Switches area, select the switch that you want to configure. The Switches area displays all AOS devices that you added to the VLAN.

2. Complete the IPX Routing Parameters fields.

a. In the **IPX Address** field, enter the IPX network address that identifies the router interface network. An IPX network address consists of eight hex characters (e.g., 4001690D). If fewer than eight hex digits is specified, the address is prefixed with zeros to equal eight digits. The router interface address must be unique. You cannot have two router interfaces with the same address.

b. Set the **IPX Encapsulation** field to define the type of IPX router interface frame encapsulation. The encapsulation determines the framing type the router interface uses when generating frames that are forwarded out VLAN ports. Use an encapsulation value that matches the encapsulation of the majority of IPX VLAN traffic. You can set the frame type encapsulation to any of the following values:

- **Ethernet 2**
- **Novell Raw** (802.3)
- **LLC** (802.2)
- **SNAP**
- **Not Applicable.**

By default, this parameter is set to **Ethernet 2** when the router interface is defined. If the encapsulation used by a VLAN device does not match the router interface frame type, then device frames are translated before they are forwarded on by the router interface to the appropriate subnet.

c. Set the **RIP/SAP Mode** field to one of the following values:

- **RIP Only** (RIP updates are processed)
- **RIP and SAP** (RIP and SAP updates are processed)
- **Triggered** (RIP and SAP updates are broadcast only when updates occur)
- **Inactive** (RIP and SAP updates are not processed, router interface remains active)
- **Not Applicable.**

d. Enter a 16-bit value (**0-65535**) in the **Delay Ticks** field to specify the number of ticks for the IPX delay time. A tick is approximately 1/18th of a second.

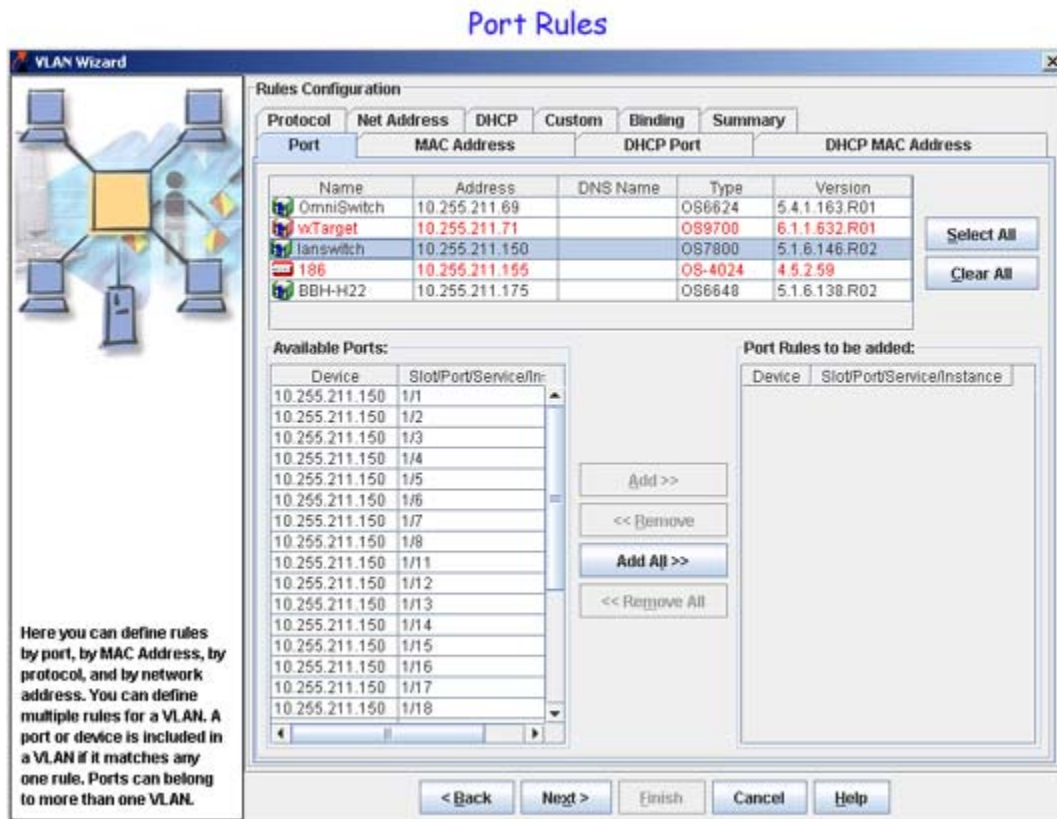
3. Select additional switches in the Switches area and configure IP router interfaces as desired.

Click the **Next** button when all desired switches have been configured

Configuring Port Rules

The Port Tab enables you to configure port rules for the VLAN. Port rules are fundamentally different from all other supported rule types, in that traffic is not required to trigger dynamic assignment of the mobile port to a VLAN. As soon as this type of rule is created, the specified port is assigned to the VLAN only for the purpose of forwarding broadcast types of VLAN traffic to a device connected to that same port. Consider the following when defining a VLAN port rule:

- Port rules are mostly used for silent devices, such as printers, that require VLAN membership to receive traffic forwarded from the VLAN. These devices usually do not send traffic, so they do not trigger dynamic assignment of their mobile ports to a VLAN.
- It is possible to specify the same port in more than one port rule defined for different VLANs. The advantage to this is that traffic from multiple VLANs is forwarded out the one mobile port to the silent device. For example, if port 3 on slot 2 is specified in a port rule defined for VLANs 255, 355, and 755, then outgoing traffic from all three of these VLANs is forwarded on port 2/3.
- Port rules only apply to outgoing mobile port traffic and do not classify incoming traffic. If a mobile port is specified in a port rule, its incoming traffic is still classified for VLAN assignment in the same manner as all other mobile port traffic.



To create port rules for a VLAN, follow the steps below.

1. All switches in the VLAN are listed in the window at the top of the screen. Select a switch in this window and its ports are displayed in the Available Ports window, as shown in the screen above.

2. Move the desired ports from the Available Ports window to the Port Rules to be Added window using the **Add>>**, **<<Remove, Add All>>**, and **<<Remove All** buttons. Note that you can select multiple contiguous ports by **Shift**-clicking and multiple noncontiguous devices by **Ctrl**-clicking. All ports that you add to the Port Rules to be Added window will be part of the VLAN.
3. Continue to select switches and add ports to the Port Rules to be Added window until port rules are configured for all desired switches.

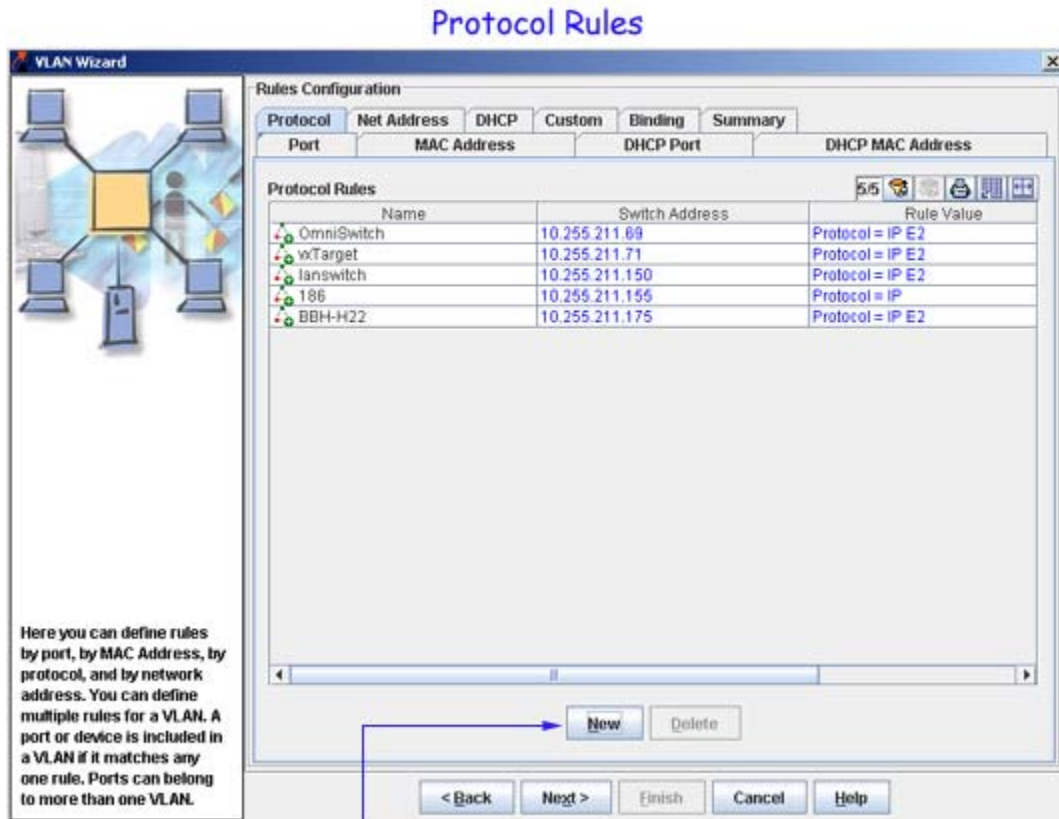
Do not click the **Next** button until all desired rules have been configured.

Configuring Protocol Rules

The Protocol Tab enables you to configure protocol rules for the VLAN. Protocol Rules determine VLAN assignment based on the protocol a device uses to communicate. When defining this type of rule, there are several generic protocol values to select from: IP, IPX, AppleTalk, or DECNet. If none of these are sufficient, it is possible to specify an Ethernet type, Destination and Source Service Access Protocol (DSAP/SSAP) header values, or a Sub-Network Access Protocol (SNAP) type. Consider the following when defining a VLAN protocol rule:

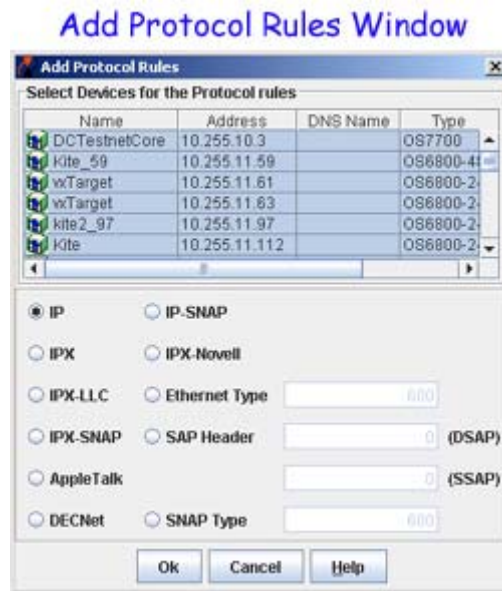
- Protocol rules are defined for all devices listed for the VLAN. For example, if you create an IP protocol rule for VLAN 10 and this VLAN exists on 5 switches, the IP protocol rule is created on VLAN 10 on all 5 switches.
- IP protocol rules also capture DHCP traffic, if no other DHCP rule exists that would classify the DHCP traffic into another VLAN. Therefore, it is not necessary to combine DHCP rules with IP protocol rules for the same VLAN.
- Specifying a SNAP protocol type restricts classification of mobile port traffic to the ethertype value found in the IEEE 802.2 SNAP LLC frame header.
- If an attempt is made to define an Ethernet type rule with a value equal to a value already captured by one of the generic IP or IPX protocol rules, switch software may detect the duplication and not create the rule. It is recommended that you use the generic IP and/or IPX protocol rules, instead of specifying the same value using the Ethernet type rule.

Note: IPX routing is not supported on OmniSwitch 6600 series switches.



Click the **New** button to display the Add Protocol Rules window, shown below.

To create a new protocol rule definition for the VLAN, click on the **New** button at the bottom of the Protocol Rules tab. This activates the Add Protocol Rules pop-up window, shown below.



Click on one of the following protocol types displayed in this window:

- IP (Ethernet II, ARP, and SNAP)
- IPX (Ethernet II, Novell 802.3, LLC 802.2, and SNAP)
- AppleTalk (Data Delivery Protocol and AppleTalk ARP)
- DECNet (DECNet Phase IV--only captures frames with 6003 Ethernet type)
- Ethernet Type (A two byte hex value between 0x600 and 0xffff that defines an Ethernet type. This value is required for the Ethernet Type field when this protocol type is selected.)
- SAP Header (A one byte hex value between 0x00 and 0xff that defines DSAP and SSAP header values. These values are required for the DSAP and SSAP fields when this protocol type is selected.)
- SNAP Type (A two byte hex value between 0x600 and 0xffff that defines a Sub-network Access Protocol. This value is required for the SNAP Type field when this protocol type is selected.)

After selecting the desired protocol type and entering any additional required values, click on the **OK** button. The Add Protocol Rules window closes and a new protocol rule entry appears in the Protocol Rules tab with an add icon in the Name field of the new entry.

Note: When you click on the **OK** button in the Add Protocol Rules window, an error message window displays a list of management IP addresses for all XOS devices that do not have mobility enabled for the VLAN. You cannot configure VLAN rules for non-mobile VLANs on XOS devices.

Removing a Protocol Rule

To remove a protocol rule definition, select one or more rules from the Protocol Rules tab and click the **Delete** button. The selected protocol rules are deleted.

Do not click the **Next button until all desired rules have been configured**

Configuring MAC Address Rules

The MAC Address Tab enables you to configure MAC address rules for the VLAN. MAC Address Rules capture frames that contain a source MAC address that matches the MAC address specified in the rule. The mobile port that receives this matching traffic is dynamically assigned to the rule's VLAN. Consider the following when defining a VLAN MAC Address Rule:

- A MAC address rule is the simplest type of rule and provides the maximum degree of control and security. Members of the VLAN will consist of devices with specific MAC addresses.
- It is possible to specify a range of MAC addresses, thus creating a MAC address range rule on the device. Frames that contain a source MAC address that matches the low or high end MAC or that falls within the range specified by the low and high end MAC trigger dynamic mobile port assignment to the rule's VLAN.
- Once a device joins a MAC address rule VLAN, it is not eligible to join multiple VLANs even if device traffic matches other VLAN rules.
- MAC address rules also capture DHCP traffic, if no other DHCP rule exists that would classify the DHCP traffic into another VLAN. Therefore, it is not necessary to combine DHCP rules with MAC address rules for the same VLAN.

MAC Address Rules

Here you can define rules by port, by MAC Address, by protocol, and by network address. You can define multiple rules for a VLAN. A port or device is included in a VLAN if it matches any one rule. Ports can belong to more than one VLAN.

Name	Switch Address	Rule Value
OmniSwitch	10.255.211.69	00005e:000101
OmniSwitch	10.255.211.69	000bdb:87efd9
OmniSwitch	10.255.211.69	000cf1:89f603
OmniSwitch	10.255.211.69	0010a4:e66d1e
wTarget	10.255.211.71	00005e:000101
wTarget	10.255.211.71	000bdb:87efd9
wTarget	10.255.211.71	000cf1:89f603
wTarget	10.255.211.71	0010a4:e66d1e
lanswitch	10.255.211.150	00005e:000101
lanswitch	10.255.211.150	000bdb:87efd9
lanswitch	10.255.211.150	000cf1:89f603
lanswitch	10.255.211.150	0010a4:e66d1e
186	10.255.211.155	00005e:000101
186	10.255.211.155	000bdb:87efd9
186	10.255.211.155	000cf1:89f603
186	10.255.211.155	0010a4:e66d1e
BBH-H22	10.255.211.175	00005e:000101
BBH-H22	10.255.211.175	000bdb:87efd9
BBH-H22	10.255.211.175	000cf1:89f603
BBH-H22	10.255.211.175	0010a4:e66d1e

Buttons: < Back, Next >, Finish, Cancel, Help

Click the **New** button to display the Add MAC Rules Window, as shown below.

To create a new MAC address rule definition for the VLAN, click the **New** button at the bottom of the screen. This activates the Add MAC Rules pop-up window, shown below.

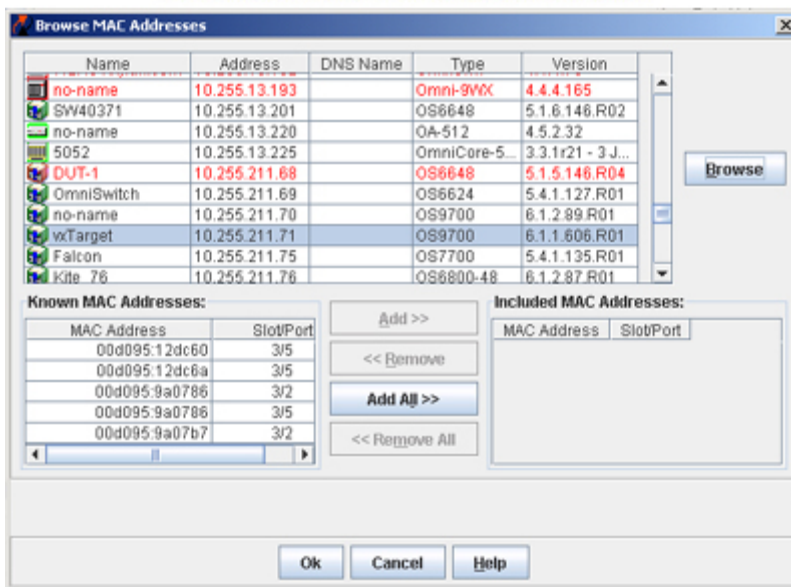
Note: When the Add MAC Rules window opens, an error message window displays a list of management IP addresses for all XOS devices that do not have mobility enabled for the VLAN. You cannot configure VLAN rules for non-mobile VLANs on XOS devices.



Follow the steps below to define a MAC address rule using the Add MAC Rules window:

1. Select one or more devices from the list located in the top half of the Add MAC Rules window.
2. Enter a MAC address in the Single/Start field (note that it is not necessary to use colons when entering a MAC address).
3. Enter a MAC address in the End field to specify a MAC address range, otherwise, leave this field blank.
4. Click on the **Add** button to include the specified MAC address or range of addresses in the rule definition. The MAC addresses entered in the previous steps are moved to the Included MAC Addresses list in the Add MAC Rules window.
5. To select a known MAC address from the source learning MAC Address Table located on each switch, click on the **Browse for MAC Address** button in the Add MAC Rules window. The Browse MAC Addresses window opens, as shown below.

Browse MAC Addresses Window



6. Select one of the devices in the device list located at the top of the Browse MAC Addresses window, then click on the **Browse** button found to the right of the device list. All MAC addresses known to the selected device are displayed in the Known MAC Addresses list.
7. Select one or more MAC addresses from the Known MAC Addresses list or click on the **Add All** button to include the entire list in the rule definition. All MAC addresses selected from the Known MAC Addresses list are moved to the Included MAC Addresses list in the Browse MAC Addresses window.
8. Click on the **OK** button to return to the Add MAC Rules window. The Browse MAC Addresses window closes and the MAC addresses selected in the Browse MAC Addresses window now appear in the Included MAC Addresses list of the Add MAC Rules window.
9. Click on the **OK** button at the bottom of the Add MAC Rules window when you have finished selecting the MAC address(es) for this MAC address rule definition. The Add MAC Rules window closes and a new rule entry appears in the MAC Rules window list with an add icon in the Name field of the new entry.

Removing a MAC Address Rule

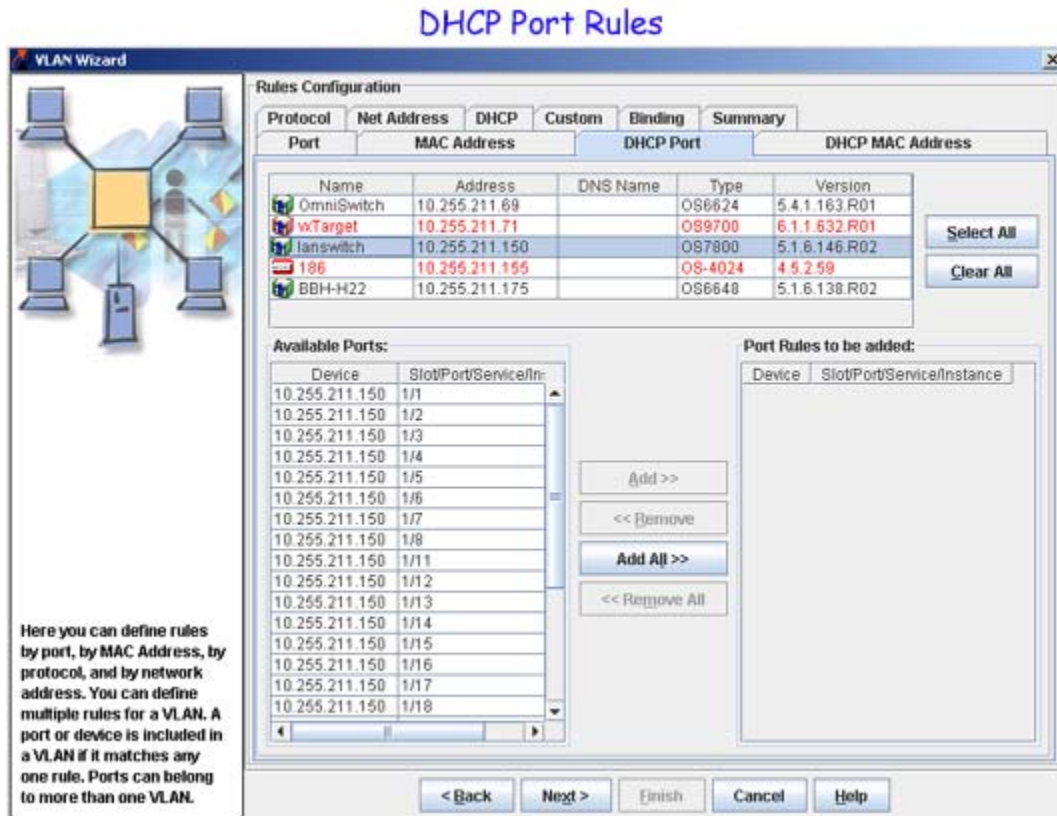
To remove a MAC address rule definition, select one or more rules from the MAC Rules window list and click the **Delete** button. The selected MAC address rules are deleted.

Do not click the **Next** button until all desired rules have been configured

Configuring DHCP Port Rules

The DHCP Port Tab enables you to create DHCP Port Rules for the VLAN. Dynamic Host Configuration Protocol (DHCP) frames are sent from client workstations to request an IP address from a DHCP server. The server responds with the same type of frames, which contain an IP address for the client. If clients are connected to mobile ports, DHCP rules are used to classify this type of traffic for the purposes of transmitting and receiving DHCP frames to and from the server. DHCP Port Rules capture DHCP frames that are received on a mobile port that matches the port specified in the rule. Consider the following when defining a VLAN DHCP Port Rule:

- When a mobile port receives a DHCP frame that matches a DHCP rule, the port is temporarily assigned to the VLAN long enough to forward the DHCP requests within the VLAN broadcast domain. Note that on AOS platforms, the source MAC address of the DHCP frame is *not* learned for that VLAN port association. As a result, the source MAC address for the DHCP frame does not appear in the Source Learning MAC Address Table on the AOS switch.
- Once a device connected to a mobile port receives an IP address from the DHCP server, the VLAN port assignment triggered by the device’s DHCP frames matching a VLAN DHCP rule is dropped unless regular port traffic matches another rule on that same VLAN. If this match occurs, or the traffic matches a rule on another VLAN, then the source MAC address of the mobile port’s frames is learned for that VLAN port association.
- DHCP rules are most often used in combination with IP network address rules. A DHCP client has an IP address of all zeros (0.0.0.0) until it receives an IP address from a DHCP server, so initially it would not match any IP network address rules.



To configure DHCP port rules for the VLAN, follow the steps below:

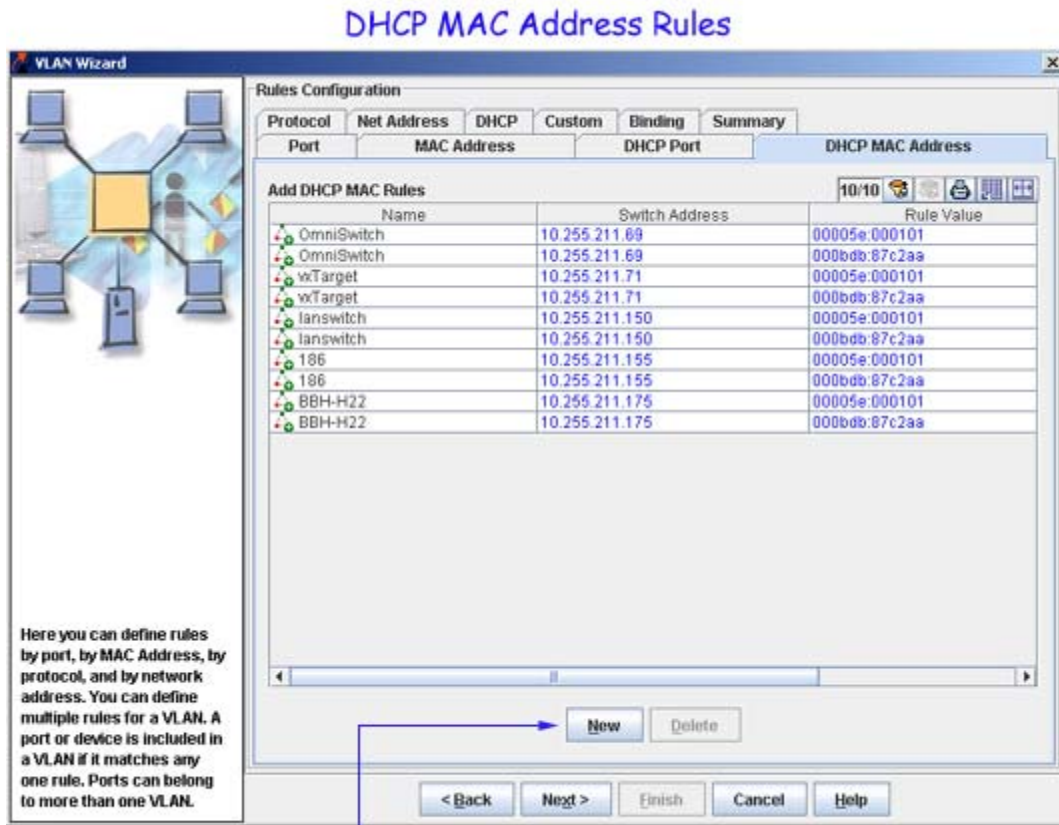
1. All switches in the VLAN are listed in the window at the top of the screen. Select a switch in this window and its ports are displayed in the Available Ports window, as shown in the screen above.
2. Move the desired ports from the Available Ports window to the Port Rules to be Added window using the **Add>>**, **<<Remove, Add All>>**, and **<<Remove All** buttons. Note that you can select multiple contiguous ports by **Shift**-clicking and multiple noncontiguous devices by **Ctrl**-clicking. DHCP port rules will be created for all ports that you add to the Port Rules to be Added window.
3. Continue to select switches and add ports to the Port Rules to be Added window until DHCP port rules are configured for all desired switch ports.

Do not click the **Next button until all desired rules have been configured**

Configuring DHCP MAC Address Rules

The DHCP MAC Address Tab enables you to configure DHCP MAC Address Rules for the VLAN. Dynamic Host Configuration Protocol (DHCP) frames are sent from client workstations to request an IP address from a DHCP server. The server responds with the same type of frames, which contain an IP address for the client. If clients are connected to mobile ports, DHCP rules are used to classify this type of traffic for the purposes of transmitting and receiving DHCP frames to and from the server. DHCP MAC Address Rules capture mobile port DHCP frames that contain a source MAC address that matches the MAC address specified in the rule. Consider the following when defining a VLAN DHCP MAC address rule:

- When a mobile port receives a DHCP frame that matches a DHCP rule, the port is temporarily assigned to the VLAN long enough to forward the DHCP requests within the VLAN broadcast domain. Note that on AOS platforms, the source MAC address of the DHCP frame is *not* learned for that VLAN port association. As a result, the source MAC address for the DHCP frame does not appear in the source learning MAC address Table on the AOS switch.
- Once a device connected to a mobile port receives an IP address from the DHCP server, the VLAN port assignment triggered by the device's DHCP frames matching a VLAN DHCP rule is dropped unless regular port traffic matches another rule on that same VLAN. If this match occurs, or the traffic matches a rule on another VLAN, then the source MAC address of the mobile port's frames is learned for that VLAN port association.
- DHCP rules are most often used in combination with IP network address rules. A DHCP client has an IP address of all zeros (0.0.0.0) until it receives an IP address from a DHCP server, so initially it would not match any IP network address rules.



Click the New button to display the Add DHCP MAC Rules window, as shown below.

To create a new DHCP MAC address rule definition for the VLAN, click on the **New** button at the bottom of the DHCP MAC Rules tab. This activates the Add DHCP MAC Rules pop-up window, as shown below.

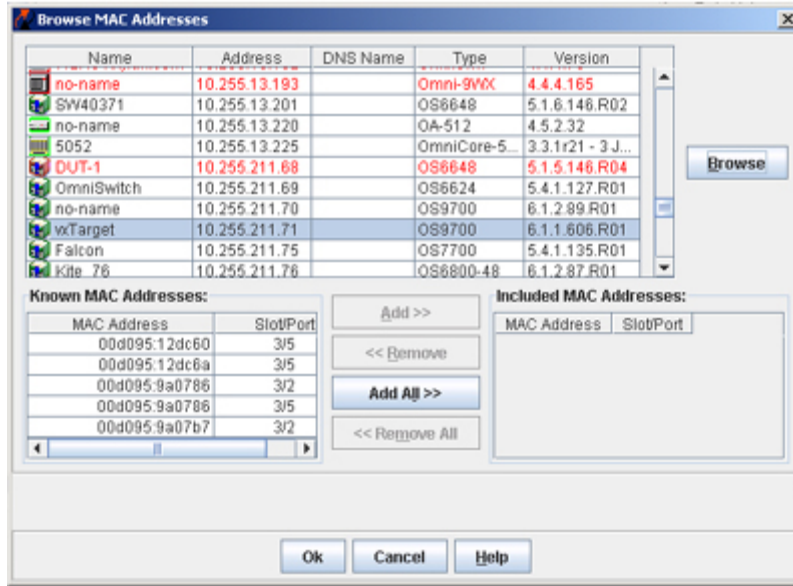
Note: When the Add DHCP MAC Rules window opens, an error message window displays a list of management IP addresses for all XOS devices that do not have mobility enabled for the VLAN. You cannot configure VLAN rules for non-mobile VLANs on XOS devices.



Follow the steps below to define a DHCP MAC Address Rule using the Add DHCP MAC Rules window:

1. Select one or more devices from the list located in the top half of the Add MAC Rules window.
2. Enter a MAC address in the Single/Start field (note that it is not necessary to use colons when entering a MAC address).
3. Enter a MAC address in the End field to specify a MAC address range, otherwise, leave this field blank.
4. Click on the **Add** button to include the specified MAC address or range of addresses in the rule definition. The MAC addresses entered in the previous steps are moved to the Included MAC Addresses list in the Add DHCP MAC Rules window.
5. To select a known MAC address from the source learning MAC Address Table located on each switch, click on the **Browse for MAC Address** button in the Add DHCP MAC Rules window. The Browse MAC Addresses window opens, as shown below.

Browse MAC Addresses Window



6. Select one of the devices in the device list located at the top of the Browse MAC Addresses window, then click on the **Browse** button found to the right of the device list. All MAC addresses known to the selected device are displayed in the Known MAC Addresses list.
7. Select one or more MAC addresses from the Known MAC Addresses list or click on the **Add All** button to include the entire list in the rule definition. All MAC addresses selected from the Known MAC Addresses list are moved to the Included MAC Addresses list in the Browse MAC Addresses window.
8. Click on the **OK** button to return to the Add DHCP MAC Rules window. The Browse MAC Addresses window closes and the MAC addresses selected in the Browse MAC Addresses window now appear in the Included MAC Addresses list of the Add DHCP MAC Rules window.
9. Click on the **OK** button at the bottom of the Add DHCP MAC Rules window when you have finished selecting the MAC address(es) for this MAC address rule definition. The Add DHCP MAC Rules window closes and a new rule entry appears in the DHCP MAC Rules tab with an add icon in the Name field of the new entry.

Removing a DHCP MAC Address Rule

To remove a DHCP MAC Address Rule, select one or more rules listed on the DHCP MAC Rules Tab and click the **Delete** button. The selected DHCP MAC Address Rules are deleted.

Do not click the **Next** button until all desired rules have been configured

Configuring Network Address Rules

The Net Address Tab enables you to configure network address rules for the VLAN. There are two types of Network Address Rules: IP and IPX. An IP Network Address Rule determines VLAN mobile port assignment based on a device's source IP address. An IPX Network Address Rule determines VLAN mobile port assignment based on a device's IPX network and encapsulation. Consider the following when defining a VLAN network address rule:

- Network address rules are defined for all devices listed for the VLAN. For example, if you create an IP network address rule for VLAN 10 and this VLAN exists on 5 switches, the rule is created on VLAN 10 on all 5 switches.
- If DHCP is used to provide client workstations with an IP address, you may need to use one of the DHCP rules in combination with an IP network address rule.
- If the IPX network address rule VLAN is going to route IPX traffic, it is important to specify a rule encapsulation that matches the IPX router port encapsulation. If there is a mismatch, connectivity with other IPX devices may not occur.
- On AOS platforms, IPX network address rules apply only to devices that have already obtained their IPX network address. In addition, frames must match both the IPX network address *and* encapsulation specified in the rule.

Note: IPX routing is not supported on OmniSwitch 6600 series switches.

Network Address Rules

Here you can define rules by port, by MAC Address, by protocol, and by network address. You can define multiple rules for a VLAN. A port or device is included in a VLAN if it matches any one rule. Ports can belong to more than one VLAN.

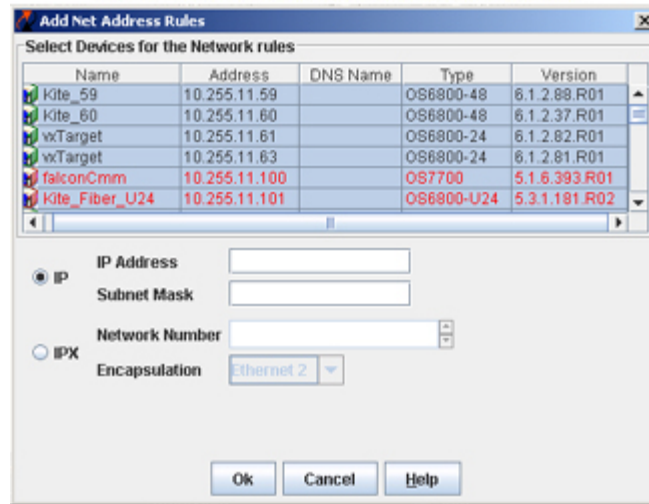
Name	Switch Address	Rule Value	Rule Status
OmniSwitch	10.255.211.69	IP = 10.255.16.172, Mask = 255.0.0.0	Enabled
wTarget	10.255.211.71	IP = 10.255.16.172, Mask = 255.0.0.0	Enabled
lanswitch	10.255.211.150	IP = 10.255.16.172, Mask = 255.0.0.0	Enabled
186	10.255.211.155	Protocol = IP, IP = 10.255.16.172, Mask = 255.0.0.0	Enabled
BBH-H22	10.255.211.175	IP = 10.255.16.172, Mask = 255.0.0.0	Enabled

Buttons: New, Delete, < Back, Next >, Finish, Cancel, Help

Click the **New** button to display the Add Net Address Rules window, shown below.

To create a new network address rule definition for the VLAN, click on the **New** button at the bottom of the Net Address tab. This activates the Add Net Address Rules pop-up window, shown below.

Add Net Address Rules Window



Note: When you click on the **OK** button in the Add Net Address Rules window, an error message window displays a list of management IP addresses for all XOS devices that do not have mobility enabled for the VLAN. You cannot configure VLAN rules for non-mobile VLANs on XOS devices.

Follow the steps below to create an IP network address rule:

1. Click on **IP** and enter an IP network address (e.g., 172.13.0.0) in the IP Address field and an IP subnet mask (e.g., 255.255.0.0) in the Subnet Mask field.
2. Click the **OK** button at the bottom of the Add Net Address Rules window. The Add Net Address window closes and a new rule entry for each device appears in the Net Address tab with an add icon in the Name field of the new entry.

Follow the steps below to create an IPX network address rule:

1. Click on **IPX** and enter an IPX network address (e.g., 25040001) in the Network Number field.
2. Select one of the following IPX encapsulation types from the Encapsulation field list:
 - Ethernet 2
 - Novell Raw (802.3)
 - LLC (802.2)
 - SNAP.
3. Click the **OK** button at the bottom of the Add Net Address Rules window. The Add Net Address window closes and a new rule entry for each device appears in the Net Address tab with an add icon in the Name field of the new entry.

Removing a Network Address Rule

To remove a network address rule definition, select one or more rules from the Net Address tab and click the **Delete** button. The selected network address rules are deleted.

Do not click the **Next** button until all desired rules have been configured

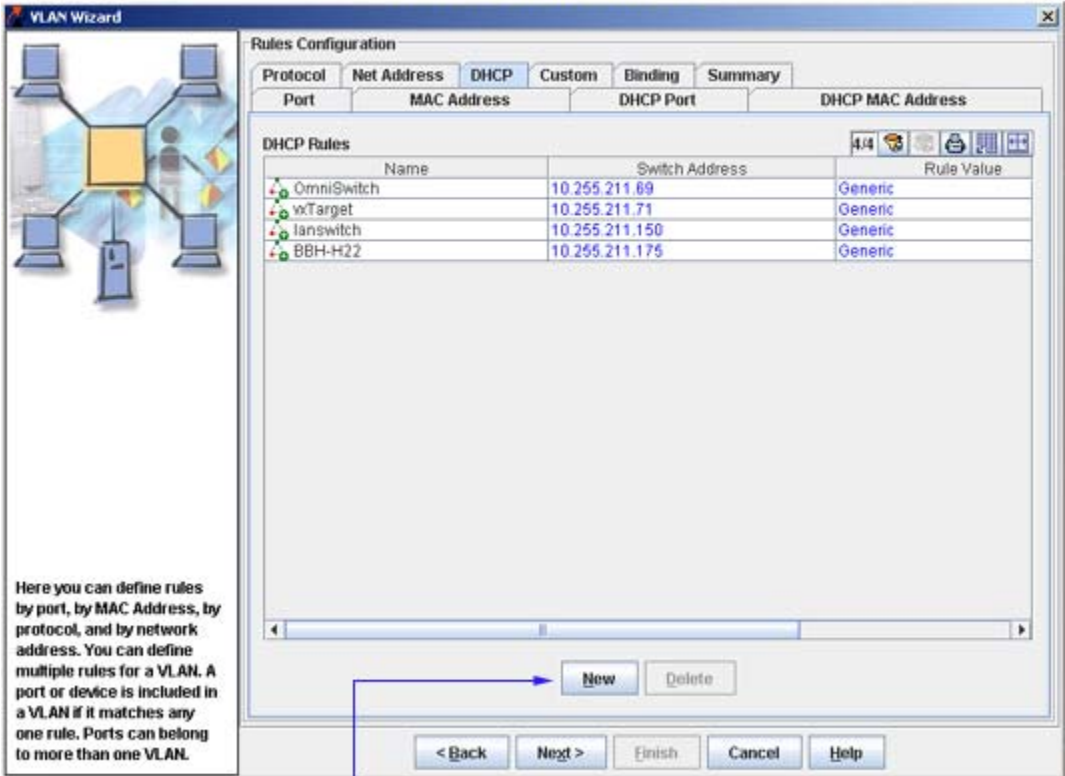
Configuring DHCP Generic Rules

The DHCP Tab enables you to configure DHCP Generic Rules for the VLAN. Dynamic Host Configuration Protocol (DHCP) frames are sent from client workstations to request an IP address from a DHCP server. The server responds with the same type of frames, which contain an IP address for the client. If clients are connected to mobile ports, DHCP rules are used to classify this type of traffic for the purposes of transmitting and receiving DHCP frames to and from the server.

A DHCP Generic Rule captures all mobile port DHCP frames that do not match any other DHCP rules already defined for other VLANs. For example, if a DHCP frame is received on a mobile port that does *not* match the port specified in any DHCP port rules defined and the frame does *not* contain a source MAC address that matches the MAC address specified in any DHCP MAC address rules defined, then the frame and mobile port are assigned to the DHCP generic rule VLAN. Note the following when defining a DHCP Generic Rule:

- Only *one* DHCP Generic rule is allowed per device.
- When a mobile port receives a DHCP frame that matches a DHCP rule, the port is temporarily assigned to the VLAN long enough to forward the DHCP requests within the VLAN broadcast domain. Note that on AOS platforms, the source MAC address of the DHCP frame is *not* learned for that VLAN port association. As a result, the source MAC address for the DHCP frame does not appear in the source learning MAC address Table on the AOS switch.
- Once a device connected to a mobile port receives an IP address from the DHCP server, the VLAN port assignment triggered by the device's DHCP frames matching a VLAN DHCP rule is dropped unless regular port traffic matches another rule on that same VLAN. If this match occurs, or the traffic matches a rule on another VLAN, then the source MAC address of the mobile port's frames is learned for that VLAN port association.
- DHCP Rules are most often used in combination with IP network address rules. A DHCP client has an IP address of all zeros (0.0.0.0) until it receives an IP address from a DHCP server, so initially it would not match any IP network address rules.
- Binding Rules that do *not* specify an IP address, MAC Address Rules, and Protocol Rules also capture DHCP traffic for dynamic VLAN assignment. A Binding Rule that does specify an IP address is similar to a Network Address Rule and will not capture DHCP frames.

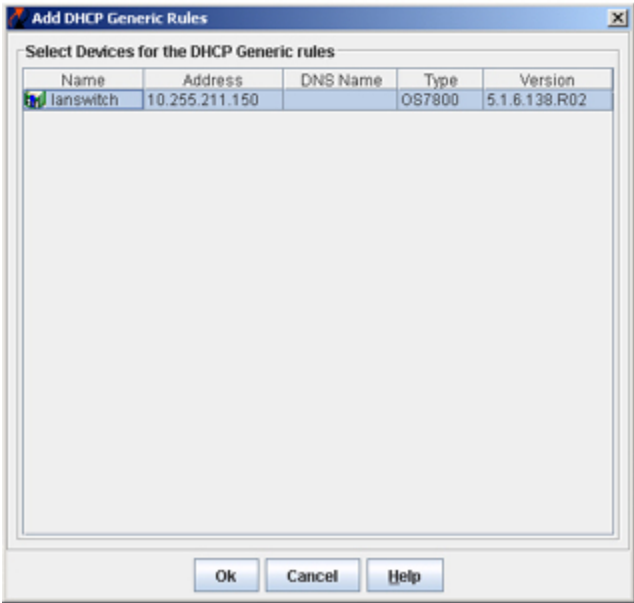
DHCP Generic Rules



Click the New button to display the Add DHCP Generic Rules window, shown below.

To create a DHCP Generic Rule definition for the current VLAN, click on the **New** button at the bottom of the DHCP Generic Rule window. This activates the Add DHCP Generic Rule pop-up window, as shown below.

Add DHCP Generic Rules Window



Follow the steps below to define a DHCP Generic Rule using the Add DHCP Generic Rules window:

1. Select one or more devices from the list located in the top half of the Add Generic Rules window.
2. Click on the **OK** button at the bottom of the Add DHCP Generic Rules window when you have finished selecting the devices for this rule definition. The Add DHCP Generic Rules window closes and a new rule entry appears on the DHCP tab with an add icon in the Name field of the new entry.

Removing a DHCP Generic Rule

To remove a DHCP Generic Rule definition, select one or more rules on the DHCP Tab and click the **Delete** button. The selected DHCP Rules are deleted.

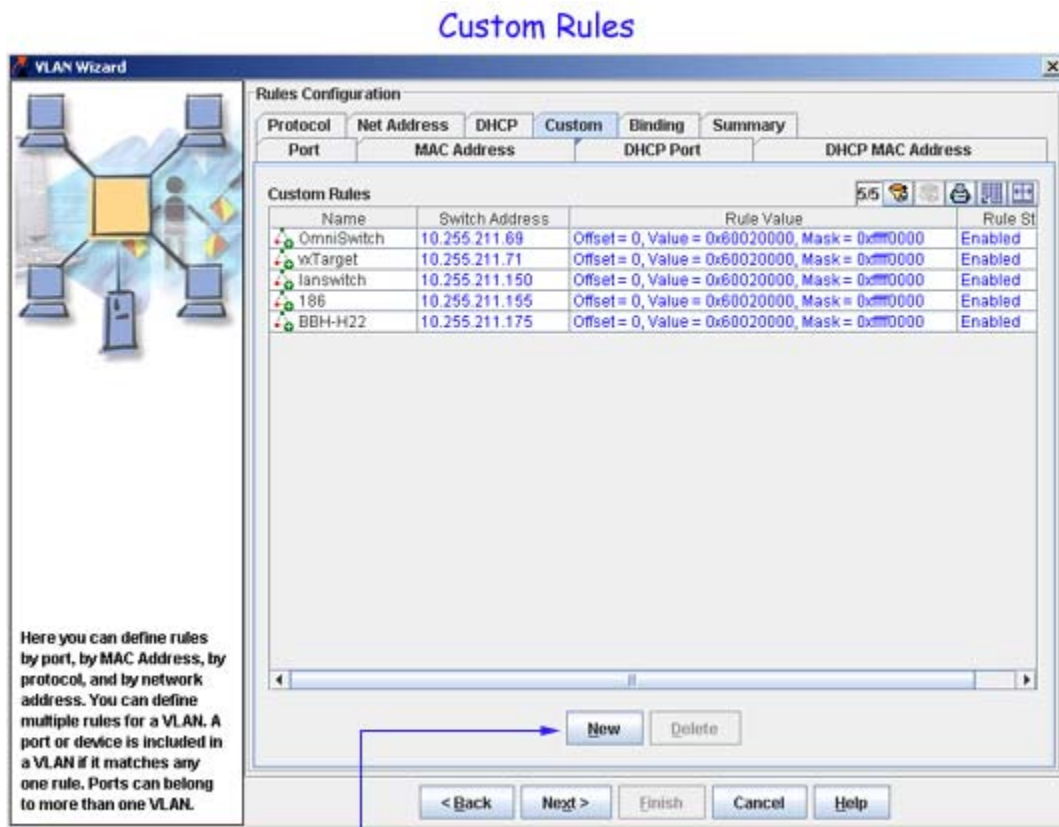
Do not click the **Next** button until all desired rules have been configured

Configuring Custom Rules

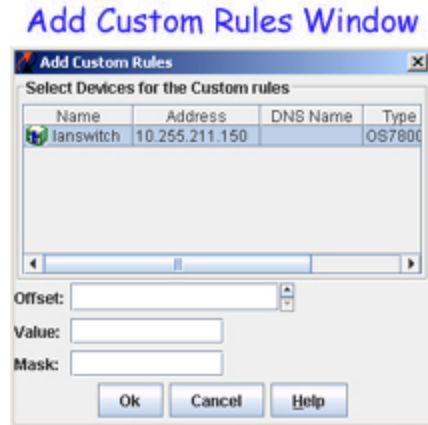
The Custom Tab enables you to configure Custom Rules for the VLAN. Custom Rules determine VLAN assignment based on criteria defined by the user. The criteria consists of a specified pattern of data and a location where that data must exist within the frame. Devices originating frames that contain this same data in the required frame location are dynamically assigned to the VLAN.

Note that defining a custom rule is recommended only if none of the other available rules provide the necessary criteria for capturing the desired type of mobile port traffic.

Note: Custom Rules are not supported on 6800 series switches. When you apply a rule to a group of devices in a VLAN, OmniVista displays a dialog box listing any devices that do not support the rule, if applicable. Those devices that **do** support the rule are updated.



To create a Custom Rule definition for the current VLAN, click on the **New** button at the bottom of the Custom Tab. This activates the Add Custom Rule pop-up window, as shown below.



Follow the steps below to create a custom rule:

1. Select one or more devices from the list located in the top half of the Add Custom Rules window. Note that all devices are selected by default.
2. Enter a number between 0 and 72 in the Offset field to specify the number of bytes into the frame where the pattern (value) is found.
3. Enter a four byte hex value in the Value field to specify a pattern of data (e.g., 60020000).
4. Enter a four byte hex value in the Mask field to identify the bytes in the pattern to compare to the frame contents at the offset location. Use "f" in the mask to mark bytes in the pattern to match and "0" to mark bytes in the pattern to ignore (e.g., ffff0000 is the mask for the 60020000 value pattern).
5. Click the **OK** button at the bottom of the Add Custom Rules window. The Add Custom Rules window closes and a new rule entry for each device appears on the Custom tab with an add icon in the Name field of the new entry.

Removing a Custom Rule

To remove a Custom Rule definition, select one or more rules on the Custom Tab and click the **Delete** button. The selected Custom Rules are deleted.

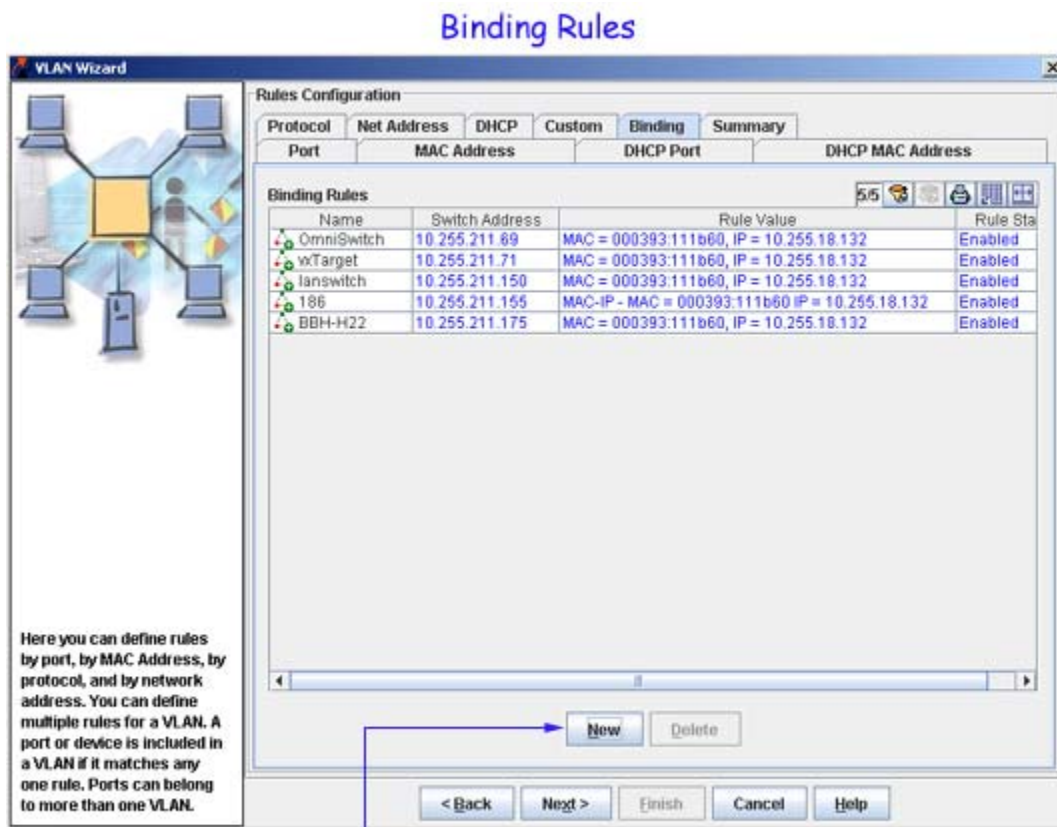
Do not click the **Next** button until all desired rules have been configured

Configuring Binding Rules

The Binding Rules Tab enables you to configure Binding Rules for the VLAN. Binding Rules restrict VLAN assignment to specific devices by requiring that device traffic match all criteria specified in the rule. As a result, a separate Binding Rule is required for each device. An unlimited number of such rules, however, is allowed per VLAN.

There are six binding rule types available: MAC-Port-IP, MAC-Port-Protocol, MAC-Port, MAC-IP Address, Port-IP Address, and Port-Protocol. The Binding Rule type name indicates the criteria the rule uses to determine if traffic received on a mobile port qualifies for dynamic VLAN assignment. For example, the MAC-Port-IP Address Binding Rule requires a matching source MAC and IP address in frames received from a device connected to the mobile port specified in the rule.

Although DHCP frames are examined and processed first, binding rules take precedence over all other rules. If frames received on a mobile port do not contain any matching Binding Rule criteria, they are compared against other existing VLAN rules of lower precedence. However, if a frame violates criteria of any one Binding Rule, it is discarded. Click here for more information about rule precedence and binding rule violations.



Click on the **New** button to display the Add Binding Rules window, shown below.

To create a binding rule definition for the current VLAN, click on the **New** button at the bottom of the Binding Rules tab. This activates the Add Binding Rules pop-up window. Click on one of the following binding rule types for more information about how to create that rule:

- IP-MAC

- IP-PORT
- MAC-PORT
- PORT-PROTOCOL
- MAC-IP-PORT
- MAC-PORT-PROTOCOL

Note: When you apply a rule to a group of devices in a VLAN, OmniVista displays a dialog box listing any devices that do not support the rule, if applicable. Those devices that do support the rule are updated.

Removing a Binding Rule

To remove a Binding Rule definition, select one or more rules on the Binding Rules Tab and click the **Delete** button. The selected Binding Rules are deleted.

Do not click the **Next** button until all desired rules have been configured

Rule Summary Tab

The Summary Tab enables you to view a summary of the rules you have configured for the VLAN. If you wish to change any rule displayed, delete any rules displayed, or add additional rules, merely click on the appropriate tab and make any changes desired. Changes will be reflected in the VLAN rules Summary tab immediately.

VLAN Rules Summary Tab

Here you can define rules by port, by MAC Address, by protocol, and by network address. You can define multiple rules for a VLAN. A port or device is included in a VLAN if it matches any one rule. Ports can belong to more than one VLAN.

Name	Switch Address	Rule Type	Rule Value
OmniSwitch	10.255.211.69	MAC	00005e 000101
OmniSwitch	10.255.211.69	MAC	000bdb.87efd9
OmniSwitch	10.255.211.69	MAC	000cfl.89f603
OmniSwitch	10.255.211.69	MAC	0010a4.e66d1e
OmniSwitch	10.255.211.69	DHCP-MAC	00005e.000101
OmniSwitch	10.255.211.69	DHCP-MAC	000bdb.87c2aa
OmniSwitch	10.255.211.69	Protocol	Protocol = IP E2
OmniSwitch	10.255.211.69	IP	IP = 10.255.16.172, Mask = 255.0.0.0
OmniSwitch	10.255.211.69	DHCP-Generic	Generic
OmniSwitch	10.255.211.69	Custom	Offset = 0, Value = 0x60020000, Mask = 0xffff0000
OmniSwitch	10.255.211.69	MAC-IP	MAC = 000393:111b60, IP = 10.255.18.132
wTarget	10.255.211.71	MAC	00005e 000101
wTarget	10.255.211.71	MAC	000bdb 87efd9
wTarget	10.255.211.71	MAC	000cfl 89f603
wTarget	10.255.211.71	MAC	0010a4.e66d1e
wTarget	10.255.211.71	DHCP-MAC	00005e.000101
wTarget	10.255.211.71	DHCP-MAC	000bdb.87c2aa
wTarget	10.255.211.71	Protocol	Protocol = IP E2
wTarget	10.255.211.71	IP	IP = 10.255.16.172, Mask = 255.0.0.0
wTarget	10.255.211.71	DHCP-Generic	Generic
wTarget	10.255.211.71	Custom	Offset = 0, Value = 0x60020000, Mask = 0xffff0000
wTarget	10.255.211.71	MAC-IP	MAC = 000393:111b60, IP = 10.255.18.132
lanswitch	10.255.211.150	MAC	00005e 000101

Click the **Next** button when all desired rules are configured

Finishing the VLAN

The VLAN Wizard summary page lists all definitions for the new VLAN. If you need to change anything, click the **Back** button and make any desired changes. Changes are reflected in the summary immediately. When the definitions listed in the summary are correct and complete, click the **Finish** button to send the new VLAN definitions to the switches. Errors that occur during this process, if any, are reported in the Status Panel.

VLAN Wizard Summary

The VLAN Wizard Summary lists all definitions for the new VLAN. If you need to change anything, click the **Back** button. If all definitions are correct and complete, click the **Finish** button to send the new VLAN definition(s) to the switch(es).

The screenshot shows the 'VLAN Wizard Summary Page' window. On the left is a network diagram with a central switch and several connected devices. Below the diagram is the text: 'This is a summary of all VLAN configuration information.'

The main content area is titled 'VLAN Wizard Summary Page' and contains the following sections:

VLAN Description

Id :	158	Description :	VLAN 158
Admin Status :	Enabled	Mode :	Standard
Spanning tree :	Enabled	Mobility :	Enabled
Authentication :	Disabled	Router Protocol :	IP

ROUTING

Switch	IP Routing	IPX Routing
186 (10.255.211.155)	Enabled, 0.0.0.0	Enabled, 4001690d
BBH-H22 (10.255.211.175)	5.5.5.1, Engineering	Disabled
lanswitch (10.255.211.150)	5.5.5.16, Accounting	Disabled
OmniSwitch (10.255.211.69)	5.5.5.23, Tech Pubs	Disabled
vxTarget (10.255.211.71)	5.5.5.34, Test	Disabled

At the bottom of the window are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.