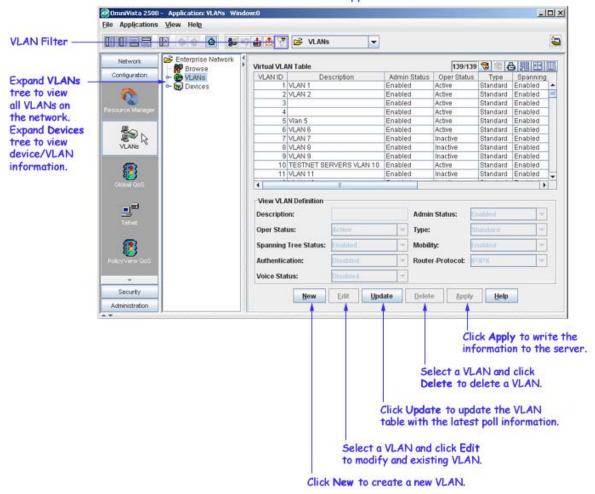
Getting Started with VLANs

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:

- Viewing VLAN information (VLAN View and Device View). You can also filter the VLAN view using the VLAN Filter option.
- 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 VLANs Application

The initial configuration for all Alcatel-Lucent 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.

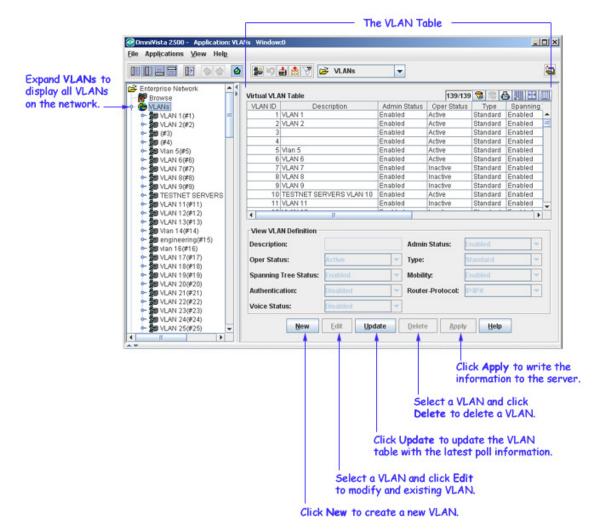
Note that when you open the OmniVista VLANs application, the following warning message displays if the application detects that it does not have current VLAN information for one or more devices.



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.



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.

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.

1			- Physical	Network	Device Lis	ST	(
OmniVista 2500 - Applica	tion: VL	Ns Window:0					
Elle Applications View H	lelp						
	\$ Ø	\$ 9 4 37	🔗 Devices	-			[
Enterprise Network		Physical Network				40/40 🔞 🗐	8
		Name	Address	DNS Name	Type	Version	Last Upgrade :
VLANS		DCTestnetCore	10.255.10.254		OS9600	6.1.5.479.R01	
P CONCES		6200_Stack_of_7	10.255.11.123		OS6200-U24	1.5.0.93	1
		6200_Stand_Alone	10.255.11.124		OS6200-P24	1.5.0.93	
		NMS_125	10.255.11.125		OS6300-24	2.2.0.15	
		🖬 Fuji_9700	10.255.11.129		OS9700	6.3.1.586.R01	S
		🗑 s-dist-5	10.255.11.135		OS6800-48	6.1.5.467.R01	
		OmniStack 6148	10.255.11.155		OS-6148	V3.40.21	(
		Kite2_NMS	10.255.11.194		OS6850-24	6.1.5.479.R01	1
		no-name	10.255.11.198		OS-4024	4.5.3.121	
		OSR5-Slot	10.255.11.197		OmniS/R-5	4.4.4.196	0
		s-core-1	10.255.11.199		OS9800	6.3.1.15.INT	
		🗑 no-name	10.255.11.218		OS9600	6.3.1.15.INT	1
		NMS_HAWK_102	10.255.11.225		OS6624	5.4.1.234.R01	
		HAWK_227	10.255.11.227		OS6624	5.1.6.288.R01	
		Hawk_229	10.255.11.229		OS6648	5.1.6.154.R02	C
		🗑 lanswitch	10.255.11.230		OS6600-P24	5.1.6.143.R02	
		HAWK_231	10.255.11.231	1	OS6648	5.1.6.143.R02	0
		QoS-EP1	10.255.11.232		OS6624	5.1.6.120.R02	
		GoS-H1	10.255.11.233		OS6624	5.1.6.120.R02	
		L2-DUT2	10.255.11.234		OS6648	5.1.5.221.R04	
		L2-DUT1	10.255.11.235		OS6648	5.1.5.221.R04	2
		GoS-HP1	10.255.11.237		OS6624	5.1.6.120.R02	2
10.255.11.235		1					•
► 10.255.11.237				Help			
	Ele Applications View H Image: Second	File Applications Yew Help Image: Second Seco	Image: Section of the sectio	File Applications Yew Help Image: Second Seco	File Applications Yew Help Image: Second Seco	File Applications Yew Help Image: Second Seco	Pie Applications Yew Help Image: Senterp ise Network Image: Senterp is

Expand Devices to view a list of all network subnets.

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 a device to display the menu.)

IIIIII 🕑 🖉 🖉	🐉 i i j 🍰 🕺 🦁	🔗 Devices	-	•		3
Enterprise Network	Physical Network				40/40 🔞	8
Provse Provse ♥ VLNNs ♥ Ul0.0.008) ● ♥ Ul0.0 255.10.254 ● ♥ Ul0.255.11.123 ● ♥ 10.255.11.125 ● ♥ 10.255.11.125 ● ♥ 10.255.11.125 ● ♥ 10.255.11.155 ● ♥ 10.255.11.155 ● ♥ 10.255.11.155 ● ♥ 10.255.11.185 ● ♥ 10.255.11.185 ● ♥ 10.255.11.197 ● ♥ 10.255.11.197 ● ♥ 10.255.11.197 ● ♥ 10.255.11.198	Name DCTestnelCore 6200_Stack_of 7 6200_Stack_of 7 6200_Stack_of 7 Folj_9700 Curr 5-dist-5 Curr 5-dist-5 NMS 125 WinStack 61 NMS Kite2_NMS Poll 0.0875-Slot Corr 5-score1 0.0875-Slot Curr 10.0875-Slot Curr	Address 10.255.10.254 10.255.11.24 10.255.11.124 10.255.11.125 ent Window Window Window Node Node Figure Traps for Traps to Working et Working	ו ע א א א א א א	OS9600 OS6200-U24 OS6200-P24 OS6300-24 evice Status ocate on Map lotifications lealth SH itatistics ocate End-Station	Version 6.1.5.479.R01 1.5.0.93 1.	Last Upgrade :
 → 10.255.11.225 → 10.255.11.227 → 10.255.11.227 → 10.255.11.230 → 10.255.11.231 → 10.255.11.231 → 10.255.11.232 → 10.255.11.232 → 10.255.11.233 → 10.255.11.234 → 10.255.11.235 	Copy Coos-EP1 COOS-EP1 COOS-EP	oot y Certified To Wor y Working To Cert ntory Browser Page	king	ackup Configurati 056600-P24 056648 056624 056624 056648 056648 056648 056648	00 5.154.R02 5.1.6.143.R02 5.1.6.143.R02 5.1.6.120.R02 5.1.6.120.R02 5.1.5.221.R04 5.1.5.221.R04 5.1.6.120.R02	

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.

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,

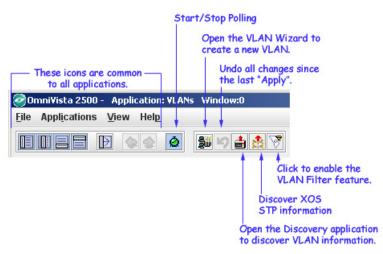
Color Coding

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).

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.

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.

			- T		
nniVista 2500 - Application: VL Applications View Help	JINs Window:0				-
		🕈 🖻 Ports	-		
Enterprise Network	AOS XOS Om	niStack			
VLANS	Ports for (VLAN 2(#	2))		8/8 🐨	
- 🞾 VLAN (#1)	Name	Device	SlotPort	Port Type	Port State
2 20 VLAN 2(#2)	DCTestnetCore	10.255.10.254	1/6	Q Tagged	Inactive
- Divices	DCTestnetCore	10.255.10.254	1/7	Q Tagged	Inactive
← 📴 Ports	DCTestnetCore	10.255.10.254	1/11	Default Config	Forwarding
🗣 👸 Spanning Tree	DCTestnetCore	10.255.10.254	1/14	Default Config	Forwarding
- 4 IP Router	DCTestnetCore	10.255.10.254	1/15	Default Config	Forwarding
- 🞝 IPX Router	DCTestnetCore	10.255.10.254	1/16	Default Config	Forwarding
- Kules	DCTestnetCore	10.255.10.254	3/3	Q Tagged	Inactive
► 📲 (#3)	DCTestnetCore	10.255.10.254	3/4	Q Tagged	Inactive
► 🗿 (#4)					
🗠 🏂 Vlan 5(#5)					
29 VLAN 6(#6)					
 VLAN 7(#7) 					
\$0 VLAN 8(#8)					
► 💏 VLAN 9(#9)					
- STRET SERVERS					
SO VLAN 11(#11)					
VLAN 12(#12)					
🛏 歸 VLAN 13(#13)					
🛏 🌆 Vlan 14(#14)					
 se gineering(#15) se gineering(#16) 					

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 selected VLAN contains AOS and XOS devices, then AOS and XOS tabs are available for selection, as shown below. Click on the appropriate tab to manage and configure 802.1Q VLAN port assignments.

	LANs Window:0					-
Applications View Help						
		😵 802.1Q	-]		
Enterprise Network	AOS XOS					
VLANS	802.1Q Ports for -	VLAN 2(#2)			4.4	***
- 📬 VLAN 1(#1)	Name	Device	Slot	Port	Description	Force Tag Internal
20 VLAN 2(#2)	DCTestnetCore	10.255.10.254	1	6 1		n/a
- Devices	DCTestnetCore	10.255.10.254	1	7 1		n/a
Ports	DCTestnetCore	10.255.10.254	3	3 1		n/a
G 802.10 S Spanning Tree ↓ IP Router ↓ IPX Router Kules	DCTestnetCore DCTestnetCore				2	n/a n/a
	DCTestnetCore	10.255.10.254 10.255.10.254	3	3 1	2	10.4
	DCTestnetCore	10.255.10.254 10.255.10.254	3	3 1	2	10.4
	DCTestnetCore	10.255.10.254 10.255.10.254	3	3 1	2	10.4
	OCTestnetCore	10.255.10.254 10.255.10.254	3	3 1	2	10.4
	View 802.10 VL 802.10 Ports P Device:	10.255.10.254 10.255.10.254 NP Port arameters	3	31	2	10.4
	OCTestnetCore	10.255.10.254 10.255.10.254 NP Port arameters	3	31	2	10.4

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.

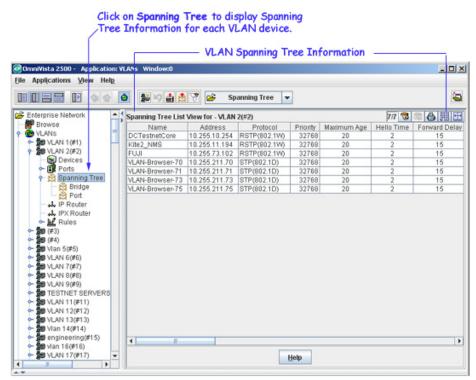
	5FO.	VLAN Link Aggre	guie hasig	in the training the second sec
mniVista 2500 - Application: VLAN	s Window:0			
Applications View Help				
	\$\$ \$\$ \$ \$\$	802.1Q Link Agg	·	1
Enterprise Network	AOS			
2 VLANS	802.1Q Link Agg for V	VLAN - VLAN 2(#2)		11 😒 🕾 🛃 🖽 🗉
BO ACANA L(H1)	Name	Device	Link Agg Id	Description
• 🚰 VLAN 2(#2)	DCTestnetCore	10.255.10.254		1 Link Agg 1 VLAN 2
BO2.10 Link Apg Spanning Tree Ali PR outer Ali PX Router Ali PX				
Spanning Tree A IP Router So (#3) So (#4) So VLAN 6(#5) So VLAN 6(#5) So VLAN 8(#5) So VLAN 9(#9) So VLAN 9(#9) So TESTNET SERVERS VLP So VLAN 1(#11)	∩View 802.1Q Link A	99		
Spanning Tree A IP Router A IP Ro		09	Device	10 255 10 254
Spanning Tree A IP Router So VLAN (#3) So VLAN (#5) So VLAN (#5) So VLAN (#5) So VLAN (#1) So VLAN 11(#11) So VLAN 12(#12) So VLAN 12(#12)	Name:	00	Device:	10.255.10.254
Spanning Tree A IP Router So VLAN 16(#6) So VLAN 16(#6) So VLAN 16(#6) So VLAN 16(#1) So VLAN 12(#12) So VLAN 12(#12) So VLAN 12(#13) So VLAN 14(#14)		99	Device: Description:	10.255.10.254
Spanning Tree A IP Router So VLAN (#3) So VLAN (#5) So VLAN (#5) So VLAN (#5) So VLAN (#1) So VLAN 11(#11) So VLAN 12(#12) So VLAN 12(#12)	Name:	99 Edit Update		10.255.10.254

Configuring Spanning Tree Parameters

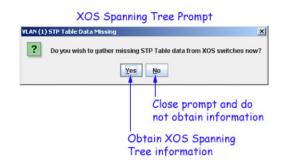
The Spanning Tree Algorithm and Protocol (STP) is a self-configuring algorithm that maintains a loop-free topology while providing data path redundancy and network scalability. STP software is active on all switches by default. As a result, a loop-free network topology is automatically calculated based 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.

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.



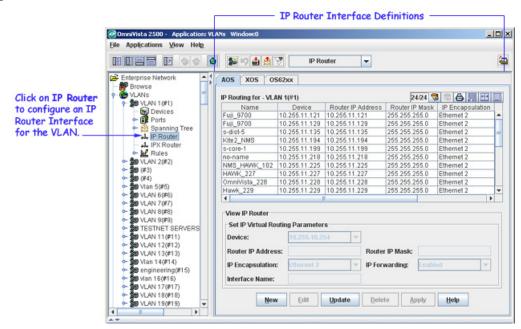
Configuring VLAN Router Interfaces

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).

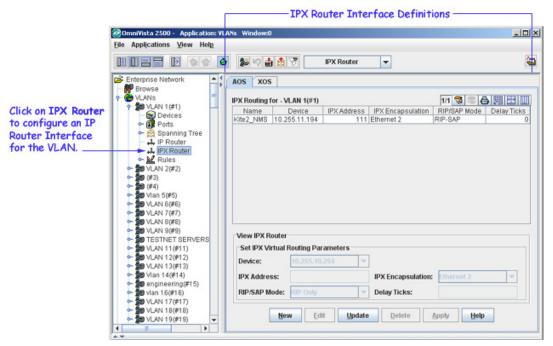
Alcatel-Lucent switches support routing of IP and IPX traffic on a per VLAN basis. A VLAN is available for routing when a router interface is defined for that VLAN and at least one active port has joined the VLAN. If a VLAN does not have a router interface configured, its ports are in essence firewalled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

To access a list of AOS, XOS or OS6200 Series 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. The tabs displayed (e.g., AOS, XOS, OS62xx) vary depending on whether or not those devices are in the selected VLAN.

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.



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.



Defining VLAN Rules

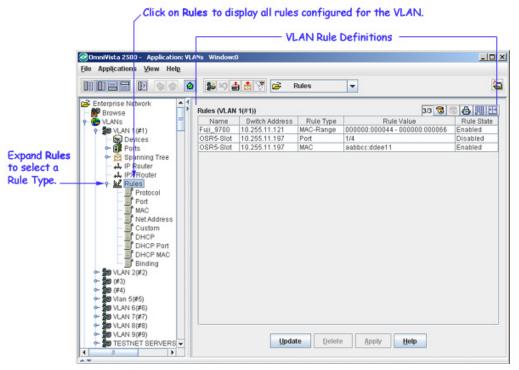
VLAN rules are used to classify mobile port traffic for dynamic VLAN port assignment. Rules are defined by specifying a port, MAC address, protocol, network address, custom (user-defined), DHCP generic, DHCP port, DHCP MAC address, or binding rule criteria to capture certain types of network device traffic. 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.

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.

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.

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.

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.

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.

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.

	o 🛃 🖉 🏦 💐 😵 🛛 Browse	-	-
Enterprise Network	VLAN Information Type VLAN All Rules Protocol Rules Custom Rules DHCP Port Rules Binding Rules 		

Selecting the VLAN Information Type

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.

		Brov 🕅	vse	-		
Enterprise Network	Available Devices				Selected Devices	
Browse VLANs			-			8 JH 1
Devices	Name	Address			Name Address	
Dences	6200 Stack of 7	10.255.11.123				
	6200_Stand_Alone	10.255.11.124				
	DCTestnetCore	10.255.10.254				
	🗑 FUJI	10.255.73.101				
	🗑 FUJI	10.255.73.102				
	Fuji_9700	10.255.11.121				
	🗑 Fuji_9700	10.255.11.129	-	<u>A</u> dd >>		
	HAWK_227	10.255.11.227			1	
	Hawk_229	10.255.11.229	<<	Remove		
	HAWK_231	10.255.11.231			1	
	Kite2_NMS	10.255.11.194	A	dd All >>		
	Kitell-239	10.255.211.239			1	
	L2-DUT1	10.255.11.235	<< F	Remove All		
	L2-DUT1	10.255.11.239				
	L2-DUT2	10.255.11.234				
	L2-DUT4	10.255.11.238				
	😥 lanswitch	10.255.11.230				
	MFE10	10.255.211.242				
	MRFE2	10.255.211.240				
	NMS_125	10.255.11.125				
	NMS_HAWK_102	10.255.11.225				
	📼 no-name	10.255.11.196	+			

Selecting the Devices to Be Searched

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 MAC Rule is configured. To start the search over, click on the **Restart** button.

Dese		0 🛔 👌 🏹 📃	Browse	-		3
Enterprise Network	Search Results: N VLAN Rules	MAC Rules			63.63 🔞	
Devices	Name	Switch Address	VLAN ID	Rule Type	Rule Value	Rule State
Dences	Fuji_9700	10.255.11.121	1	MAC-Range	000000:000044 - 000000:000056	Enabled .
	Fuli 9700	10.255.11.121		MAC	000000:000022	Enabled
	Fuii 9700	10.255.11.121	110	MAC	000000:000033	Enabled
	Fuji 9700	10.255.11.129	99	MAC	0010a4:f95f92	Enabled
	Kite2 NMS	10.255.11.194	53	MAC	0000c0:1e6af9	Enabled
	Kite2 NMS	10.255.11.194	53	MAC	00065b:a3191c	Enabled
	Kite2 NMS	10.255.11.194	53	MAC	000955318454	Enabled
	Kite2 NMS	10.255.11.194	53	MAC	00b0d0:428259	Enabled
	Kite2 NMS	10.255.11.194	53	MAC	aaaaaa;aaaaa3	Enabled
	Kite2 NMS	10.255.11.194	53	MAC	aaaaaa.aaaaa5	Enabled
	OSR5-Slot	10.255.11.197	1	MAC	aabbcc:ddee11	Enabled
	OSR5-Slot	10.255.11.197	53	MAC	000000:010101	Enabled
	OSR5-Slot	10.255.11.197	53	MAC	0000c0:1e6af9	Enabled
	OSR5-Slot	10.255.11.197	53	MAC	00065b:a3191c	Enabled
	OSR5-Slot	10.255.11.197	53	MAC	0010a4:f95f92	Enabled
	OSR5-Slot	10.255.11.197	53	MAC	00b0d0:193c68	Enabled
	OSR5-Slot	10.255.11.197	53	MAC	00b0d0:428259	Enabled
	OSR5-Slot	10.255.11.197	53	MAC	00d0b7 829c5b	Enabled
	OSR5-Slot	10.255.11.197	53	MAC	aaaaaa.aaaaa3	Enabled
	OSR5-Slot	10.255.11.197	53	MAC	aaaaaa aaaaa5	Enabled
	VLAN-Browser-70	10.255.211.70	2	MAC	000000:000015	Enabled .
	4					

Search Results

When you right-click on a displayed row, the **Find in Tree** pop-up 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.

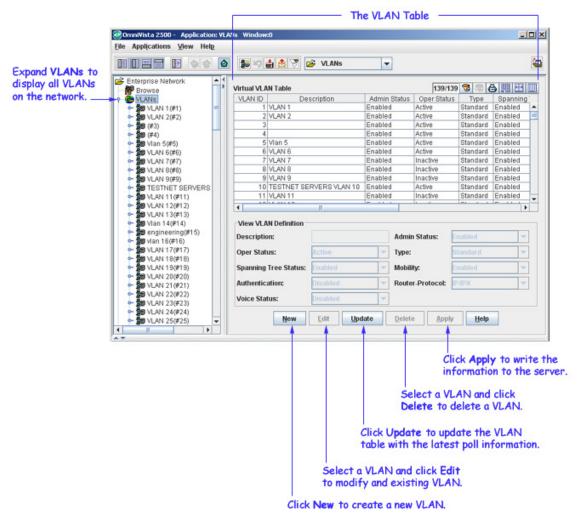
The VLAN parameter value displayed in each field, except for the VLAN ID field, is the value obtained from the switch polled that has the lowest IP host address. For example, if VLAN 9 exists on three different switches with IP addresses of 10.0.0.1, 10.0.0.2, and 10.0.0.3 and each instance of the VLAN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

- IP/IPX routing parameters.
- 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.
- The VLAN definitons 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.

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.

OmniVista 2500 - Application: V Applications View Help	LANs Window:1								- 101
	1	👌 😂 V	LANs	-					-
VLANS ✓ So VLAN 1(#1)	Virtual VLAN 1	l'able				Þ	95/295 🕱 👘	OFE	
- 10 VLAN 2(#2)	VLAN ID	Description	Admin Status	Oper S	Status	Type	Spanning Tree S	tatus Mobi	lity
• 😼 VLAN 3(#3)	1 VLA	N 1	Enabled	inactiv	8	Standard	Enabled	Enabl	ed +
∽ 월 VLAN 4(#4)	2 VLAJ		Enabled	inactiv		Standard		Enable	
VLAN 5(#5)	3 VLAJ		Enabled	Inactiv		Standard		Enabl	-
- 20 VLAN 6(#6)	4 VLA		Enabled	Inactiv		Standard		Enable	Contraction of Contra
- Se VlanOperationsTest(5 VLA		Enabled	Inactiv		Standard		Enabl	
DEAD(#8)	6 VLA	And AN	Enabled	Inactiv		Standard		Enabl	
Quarantined(#9)	7 Vian 8 DEA		est Disabled	Inactiv		Standard		Enabl	
9 VLAN 10(#10)		rantined	Enabled Disabled	Inactiv		Standard		Enabl	
20 VLAN 11(#11) 20 VLAN 12(#12)	10 VLA		Enabled	Inactiv		Standard		Enabl	
20 VLAN 12(#12) 20 Vlan 13(#13)	10 000	N 10:	lenabled	imacuv	e.	stanuaru	Enabled	Enable	P DB
- 20 VLAN 14(#14)	-Edit VLAN De	ofinition							
ULAN 16(#16)	Description:	1	ALAN 1	-	Adn	nin Status:	Enabled		-
VLAN 17(#17)	Oper Status:		nactaar	14	Тур	e:	Standard		51
99 VLAN 21(#21) 99 VLAN 22(#22)	Spanning Tre		Enabled	-		ulity:	Enabled	1	Ŧ
 SE VLAN 22(#22) VLAN 23(#23) 	Authenticatio		Disabled	-		ter-Protoci			51
🗠 🕽 daadminp(#24)	Addioticeout	. <u>.</u>	ладыюч		rapa	iei-Frotoci	a. France		
 daklosk(#25) VLAN 27(#27) 	Voice Status		heabled						
← 20 VLAN 28(#28)	15		ОК	Canc	el	Help			

Edit VLAN Definition 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.

Туре

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.

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.

Commission 2000 Application	VLANs Window:0		
ile Applications View Help			
	🙆 😹 🗐 🋔 🚉 🦁 🛛 Browse	-	
Enterprise Network Rowse Construction Construction Devices	VLAN Information Type VLAN VLAN All Rules Protocol Rules MAC Rules Custom Rules DHCP Port Rules Binding Rules	 Port Rules Net Address Rules DHCP Rules DHCP MAC Rules 	

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.

	k 🙆 🐉 🖬	📩 📝 🛛 Brov	vse	-		
terprise Network	Available Devices		-		Selected Devices	
Browse		8 HH	-			8
VLANs Devices	Name	Address			Name Address	
Devices	6200_Stack_of_7	10.255.11.123				
	6200_Stand_Alone	10.255.11.124				
	DCTestnetCore	10.255.10.254				
	FUJI	10.255.73.101				
	FUJI	10.255.73.102				
	Fuji_9700	10.255.11.121				
	🗑 Fuji_9700	10.255.11.129	=	<u>A</u> dd >>		
	HAWK_227	10.255.11.227				
	Hawk_229	10.255.11.229		<< Bernove		
	HAWK_231	10.255.11.231				
	Kite2_NMS	10.255.11.194		Add All >>		
	kitell-239	10.255.211.239				
	L2-DUT1	10.255.11.235		<< Remove All		
	L2-DUT1	10.255.11.239				
	L2-DUT2	10.255.11.234				
	L2-DUT4	10.255.11.238				
	💓 lanswitch	10.255.11.230				
	MFE10	10.255.211.242				
	MRFE2	10.255.211.240				
	NMS_125	10.255.11.125				
	MMS_HAWK_102	10.255.11.225				
	🔟 no-name	10.255.11.196	-			

Selecting the Devices to Be Searched

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.

le Applications View	Help					
			Browse	-		
Enterprise Network	Search Results: M	AC Rules			63/63 🔞	8 6 [#]
Devices	Name	Switch Address	VLAN ID	Rule Type	Rule Value	Rule State
Conveo	Fuji_9700	10.255.11.121	1	MAC-Range	000000.000044 - 000000.000056	Enabled
	Fuji_9700	10.255.11.121	101	MAC	000000.000022	Enabled
	Fuji_9700	10.255.11.121	110	MAC	000000:000033	Enabled
	Fuji_9700	10.255.11.129	99	MAC	0010a4:f95f92	Enabled
	Kite2_NMS	10.255.11.194	53	MAC	0000c0:1e6af9	Enabled
3	Kite2_NMS	10.255.11.194	53	MAC	00065b:a3191c	Enabled
	Kite2_NMS	10.255.11.194	53	MAC	00095b:318454	Enabled
3	Kite2_NMS	10.255.11.194	53	MAC	00b0d0:428259	Enabled
8	Kite2_NMS	10.255.11.194	53	MAC	888888888888888888888888888888888888888	Enabled
8	Kite2_NMS	10.255.11.194	53	MAC	aaaaaa:aaaaa5	Enabled
	OSR5-Slot	10.255.11.197	1	MAC	aabbcc:ddee11	Enabled
	OSR5-Slot	10.255.11.197	53	MAC	000000.010101	Enabled
8	OSR5-Slot	10.255.11.197	53	MAC	0000c0:1e6af9	Enabled
3	OSR5-Slot	10.255.11.197	53	MAC	00065b;a3191c	Enabled
	OSR5-Slot	10.255.11.197	53	MAC	0010a4:f95f92	Enabled
	OSR5-Slot	10.255.11.197	53	MAC	00b0d0:193c68	Enabled
	OSR5-Slot	10.255.11.197	53	MAC	00b0d0:428259	Enabled
	OSR5-Slot	10.255.11.197	53	MAC	00d0b7:829c5b	Enabled
	OSR5-Slot	10.255.11.197	53	MAC	aaaaaa:aaaaa3	Enabled
8	OSR5-Slot	10.255.11.197	53	MAC	aaaaaa aaaaa5	Enabled
	VLAN-Browser-70	10.255.211.70	2	MAC	000000:000015	Enabled
8	1					

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.

Using the VLAN Device List

The VLAN Device List window, shown below, displays when you select a VLAN from the VLANs Tree. This window provides a list of all devices in your topology that are configured with the selected VLAN. Each list entry contains specific device information and the current VLAN parameter values for that device. In addition, the VLAN Device List window allows you to modify or delete VLANs on a per switch basis. This is different from the VLANs window which enables you to modify or delete VLANs on a per VLAN son a per VLAN basis.

In the VLAN Tree, you can also click open the selected VLAN to view and manage specific device information and VLAN attributes, such as port assignments, Spanning Tree parameters, IP/IPX router ports, and VLAN rules.

	10 d A	VLAN 1	•						
VLANS	VLAN 1(#1)					1	134/134 🔞	8	23
Devices =	Name	Address	Description	17	Admin Status	Oper St	atus Type	Spanning	g Tree
- Ports	Kite_59	10.255.11.59	VLAN 1	E	nabled	Active	Standard		
← B Spanning Tree	Kite_60	10.255.11.60	VLAN 1	E	nabled	Inactive	Standard	Enabled	
J. IP Router	vxTarget	10.255.11.61	VLAN 1	E	nabled	Inactive	Standard	Enabled	
- J. IPX Router	vxTarget	10.255.11.63	VLAN 1		nabled	inactive	Standard		
🗢 🔛 Rules	falconOmm	10.255 11.100	VLAN 1	E	nabled	Active	Standard	Disabled	
- 10 VLAN 2(#2)	Kite_Fiber_U24	10.255.11.101	VLAN 1		nabled	Active	Standard		
50 VLAN 3(#3)	NMS_HAWK_102	10.255.11.102	VLAN 1	E	nabled	Active .	Standard	Enabled	1
- 10 VLAN 4(#4)	nms-test-103	10.255.11.103			nabled	Active	Standard		1
- 50 VLAN 5(#5)	no-name	10.255.11.104	VLAN 1		nabled	Active	Standard		
- 50 VLAN 6(#6)	vxTarget	10.255.11.111	VUAN 1		nabled	Active	Standard		
WanOperationsTest(#7)	Kite	10.255.11.112	VLAN 1	E	nabled	Active	Standard	Enabled	
Se New OROUP (#8)(#8) Se Quarantined(#9)	•		R.	_	1				
 W VLAN 10(#10) 	View VLAN Defini	tion							
- 59 VLAN 11(#11) - 59 VLAN 12(#12)	Description:				Admin State	us: 🔟	bidde		+
10 Vian 13(#13)	Oper Status:	Inscition.		1	Турес	50	andarist.		1
- 59 VLAN 14(#14) - 59 VLAN 15(#15)	Spanning Tree St	atus: Enilbled		4	Mobility:	Cri	obteid		4
- 50 VLAN 16(#16) - 59 VLAN 17(#17)	Authentication:	Otsabled		1	Router-Prot	tocot 🔟	oe.		*
- 50 YLAN 20(#20)	Voice Status:	Omnithed		1					

To modify VLAN parameter values using the VLAN Device List window, follow the steps below:

1. Select one or more devices in the list and click the **Edit**.button. This activates the Edit VLAN Definition panel, as shown below. If you selected more than one switch to modify, however, an Edit VLAN Definitions pop-up window opens.

Edit VLAN Definition Panel

	🛙 🗐 🏥 😫 V	LAN 1	-						1
VLANS	VLAN 1(#1)		-				141/1	41 🔞 🕾 🖨 🛄 🗄	3100
9 VLAN 2(#2)	Name	Address	Description					Spanning Tree Status	3
- 😼 VLAN 3(#3)	Kite_59 10			Enabled	bled Inactive		Standard	Enabled	1.
- 50 VLAN 4(#4)	Kite_60 10	.255.11.60	VLAN 1	Enabled	Inactiv	/8	Standard	Enabled	
- 50 VLAN 5(#5)	vxTarget 10	0.255.11.61	VLAN 1	Enabled	Inactiv	/e	Standard	Enabled	
- 😼 VLAN 6(#6)	vxTarget 10	.255.11.63	VLAN 1	Enabled	Inactiv	18	Standard	Enabled	
VianOperationsTest(#7)	kite2_97 10			Enabled Active			Standard Enabled		
50 DEAD(#8)	falconCmm 10			Enabled	Active		Standard	Disabled	
😼 Quarantined(#9)	Kite_Fiber_U24 10	0.255.11.101	VLAN 1	Enabled	Active		Standard	Enabled	
50 VLAN 10(#10)	NMS_HAWK_102 10	0.255.11.102	VLAN 1	Enabled	Active		Standard	Enabled	
59 VLAN 11(#11)	nms-test-103 10	0.255.11.103	VLAN 1	Enabled	Active		Standard	Enabled	15
- 50 VLAN 12(#12)	•								
- \$9 Vlan 13(#13) - \$9 VLAN 14(#14)	Edit VLAN Definition								
- 20 VLAN 15(#15) - 20 VLAN 16(#16)	Description:	VLAN 1		2	Admin Status:		Enabled		•
- 😼 VLAN 17(#17)	Oper Status:			-	Туре:	Туре:			-
- 39 VLAN 18(#18) - 39 VLAN 19(#19)	Spanning Tree Statu:	s: Enabled	Enabled		Mobility:		Enabled		-
50 VLAN 20(#20)	Authentication:	Disabled							5
- 😼 VLAN 21(#21)	wurnenuc-auon:	Disabled		-	Router-Protocol:		None		
- 50 VLAN 22(#22) - 50 VLAN 23(#23)	Voice Status:	Disabled		-					

2. Make the desired parameter value changes and click the **OK** button to accept the changes or the **Cancel** button to clear the changes. The Edit VLAN Definition panel will close, returning you to the VLAN Device List window.

3. If you clicked the **OK** button on the Edit VLAN Definition panel, a modify icon now appears next in the Name field of each device you selected before clicking the **Edit** button. To save the changes to the appropriate switch configurations, click the **Apply** button in the current window. Note that any modification you make to VLAN parameter values only applies to the device you selected before clicking the **Edit** button.

To delete a VLAN using the VLAN Device List window, follow the steps below:

1. Select one or more devices in the list and click the **Delete** button. A delete icon appears in the Name field of each device you selected, but the VLAN is not removed from the device configuration until you click the **Apply** button.

2. Click the Apply button to permanently remove the VLANs from the selected devices.

VLAN Parameter Definitions

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.

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.

Туре

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.

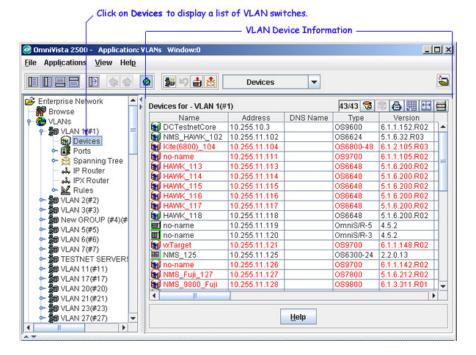
Voice Status

Not supported for this release.

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 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.

Туре

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.

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.

Applications View Help	hNs Window:0				-
	1	Ports	-		
Enterprise Network	AOS XOS On	niStack			
P Browse VLANs	Ports for (VLAN 2(#	2))		8.8 😪	
- 🎦 VLAN 1(#1)	Name	Device	SlotPort	Port Type	Port State
	DCTestnetCore	10.255.10.254	1/6	Q Tagged	Inactive
VLAN 2(#2) Divices Divices	DCTestnetCore	10.255.10.254	1/7	Q Tagged	Inactive
	DCTestnetCore	10.255.10.254	1/11	Default Config	Forwarding
	DCTestnetCore	10.255.10.254	1/14	Default Config	Forwarding
	DCTestnetCore	10.255.10.254	1/15	Default Config	Forwarding
- A IPX Router	DCTestnetCore	10.255.10.254	1/16	Default Config	Forwarding
- Kules	DCTestnetCore	10.255.10.254	3/3	Q Tagged	Inactive
► 30 (#3) ► 30 (#4)	DCTestnetCore	10.255.10.254	3/4	Q Tagged	Inactive

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.

	L/INs Window:0					
pplications yiew Help						
	a 1994	🖉 802.1Q	-			
Enterprise Network	AOS XOS					
VLANS	802.10 Ports for -	VLAN 2(#2)			4.4	3 88 311
🐲 VLAN 1(#1)	Name	Device	Slot	Port	Description	Force Tag Internal
🐲 VLAN 2(#2)	DCTestnetCore	10.255.10.254	1	6		n/a
- Devices	DCTestnetCore	10.255.10.254	1	7		n/a
9 🕄 Ports 🕴	DCTestnetCore	10.255.10.254	3	3	12	n/a
- 6 802.10 % 802.10 Link A	DCTestnetCore	10.255.10.254	3	4		n/a
Spanning Tree Li IP Router Li IPX Router						
II P Router IVX Router Van 5(#5) Van 5(#5) VAN 6(#6) VAN 6(#6) VAN 9(#7) VAN 9(#9) VAN 9(#9) TESTNET SERVERS	-View 802.1Q VLA - 802.1Q Ports Pr Device:					
HP Router Horoter Hit Router Files (#3) VLAN 6(#5) VLAN 6(#5) VLAN 8(#6) VLAN 8(#6) VLAN 8(#6)	802.1Q Ports Pa	arameters				
IP Router IPX Router IP	802.1Q Ports Pa	arameters	Port	t		

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.

OmniVista 2500 - Applica	tion: VI AN:	Windows0		Aggrega					
	ielp	THIDGONIO							-13
	•	10 🛔 🕺 🕻	🖑 802.1Q I	.ink Agg 🔻					
Enterprise Network	AOS							_	
Prowse ♥ VLANs ♥ 500 VLAN 1(#1) ♥ 500 VLAN 2(#2)		802.1Q Link Agg for VLAN - VLAN 2(#2)						AI	
	-	Name	e De	vice	Link Agg li	d	Des	cription	
- Devices		DCTestnetCon	e 10.255.10	254		1 Lir	nk Agg 1 VL	AN Z	_
 B02.10 Lin Spanning Tree IP Router IPX Router IPX Routes IP3 (#3) 		View 302.10 Name:	Link Agg	D	evice:	10.255.	10.254		*
BO2.10 Lin BO2.10 Lin Bo2.10 Lin Bo2.10 Lin Some set to the set of			Link Agg		evice: escription:	10.255.	10.254		¥

Click on 802.1Q Link Agg to display a list of link aggregates.

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.

Ports for (V	LAN 1(#1))		1128/1128	चि 🖪 🖽 🗮 🗄
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	1,17	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. The AOS Add Ports pop-up window, shown below, is used to assign a port to the current VLAN.

	orts									2
		Name	Ad	dress	DNS Name					
	D D	CTestnetCo	ore 10.255	5.10.3		037 -				
	Red Ho	te_59	10 255	5.11.59	14	OSE-	Selec	1.41		
	100 VX	Target	10.255	5.11.61		OSE	Tener			
	1 VX	Target	10.255	5.11.63		OSE	Clea	r All		
	te ki	te2_97	10.255	5.11.97		OSE_				
	-		40.000		-	1000				
Available	Ports:			Ad	d>>	Ports to	be added			
Name	Device	Slot/Port	Port	<u>G</u> u	M.22	Name	Device	Slot/Port	Port Type	
	10.255.11.59	1/25	Default	<< R	emove					
Kite_59	10.255.11.59	1/1	Default		CHHOPE					
Kite_59		1/2	Default	Add	All >>					
Kite_59	10.255.11.59	17.6								
Kite_59 Kite_59 Kite_59	10.255.11.59 10.255.11.59	1/3	Default (3.6915						
Kite_59 Kite_59	10.255.11.59		Default (Default (0.0910	nove All	123				

The top half of the Add Ports 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 assignment to this VLAN. Note that only ports that are not already assigned to this VLAN and that have Default Config as their Port Type appear in the Available Ports list.

To create a new VLAN port assignment, select one or more switches and then the available ports that you want to assign and click the **OK** button. The Add Ports window closes and new list entries appear in the AOS Ports Tab list with the modify icon in the Name field of each entry. Click the **Apply** button to update the appropriate devices with the new VLAN port assignments.

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.

Ports for (VLAN	1(#1))			210/210 🔞	8 🙆 🗐	212 <u>-</u>
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	00d(
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	00d
no-name-119	10.255.11.119	2	17	Bridge	1	00d0
no-name-119	10.255.11.119	2	18	Bridge	1	00d0
4	1					- F

XOS VLAN Port Assignments

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. The XOS Add Ports pop-up window, shown below, is used to assign an XOS port to the current VLAN.



The top half of the Add Ports 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 assignment to this VLAN. Note that only ports that are not already assigned to this VLAN and that have "Bridge" as their Function Type appear in the Available Ports list.

To create a new VLAN port assignment, select one or more switches and then the available ports that you want to assign and click the **OK** button. The Add Ports window closes and new list entries appear in the XOS Ports Tab list with the modify icon in the Name field of each entry. Click the **Apply** button to update the appropriate devices with the new VLAN port assignments.

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.

The Edit VLAN Ports window, shown below, is used to modify XOS port parameter values for multiple ports. This window displays when you select one or more ports from the XOS Ports Tab list and click on the **Edit** button.

Only the port MAC address and flood limit parameters are modifiable. Parameters that are not modifiable do not appear in this window. In addition, if you select more than one port to modify, only the flood limit parameter appears in this window. Changing the port MAC address is only available on a port by port basis. Note that the flood limit parameter field contains a blank vlaue if any of the devices selected were configured with a different flood limit value.

Edit Row		1
Edit VLAN Port	s	
MAC Address:	00d095:46c152	
Flood Limit:	192000	

To modify XOS port parameter(s), make the desired parameter value changes and click the **OK** button or the **Cancel** button to clear the changes. The Edit VLAN Ports window will close, returning you to the XOS Ports Tab list.

If you clicked the OK button in the Edit VLAN Ports window, a modify icon now appears in the Name field of the modified port. Click the **Apply** button to apply the changes to the appropriate switch configurations.

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 (**0-10000000**) 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 to OmniStack 6000, 6100, 6200, and 6300 series switches.

AOS	XOS Om	niStack			
Ports	for (VLAN 2(#2))		1/1 🐄 📾 🛃	
	Name	Device	Description	Egress Ports	Forbid
test		10.255.11.224	vian 2	1/1-1/4, 1/49-1/52	

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 The Assign Ports window, shown below, is used to configure OmniStack port assignments for the current VLAN.

ort Assignme	nts				
	🖲 Eg	ress	🔾 Forbidden 🔾 U	ntagged	
orts of test (10.255.11.22	(4)		Selected Ports	
Slot	Port		Add >>	Slot	Port
1				1	1
1	6 7 8 9		<< Remove	1	
1	7		-	1	8
1	8		Add All >>	1	
1	9				
1	10		<< Remove All		
1	11				

1. Click on **Egress**. Select ports from the available ports list and click on **Add** >> to associate the selected ports with the VLAN or click on **Add All** >> to associate all available ports to the VLAN.

2. Click on **Forbidden** if there are any egress ports that you do not want GVRP to automatically assign to this VLAN. Select ports from the available ports list and click on **Add** >> or click on **Add** All >> to select all ports. Note that GVRP is not supported on all OmniStack platforms.

3. Click on **Untagged** to define port assignments as untagged (the VLAN is the default VLAN for the port). Select ports from the available ports list (only select ports that are already associated as egress ports for the VLAN) and click on **Add** >> or click on **Add All** >> to select all ports.

4. Click on **OK** when you are done to accept the new port assignments for this VLAN or click **Cancel** to cancel this action. The Assign Ports window will close, returning you to the OmniStack Ports Tab.

5. If you clicked the **OK** button in the Assign Ports window, a modify icon appears in the Name field for the selected device. To save the changes to the appropriate switch configurations, click the **Apply** button in the current window.

Removing Ports from a VLAN

To remove a VLAN port assignment using the Assign Ports window, follow the steps below

1. Click on **Egress**. Select ports from the Selected Ports list and click on **<< Remove** to remove the VLAN association from the selected ports or click on **<< Remove All** to remove the VLAN association from all of the ports. Note that when an egress VLAN port association is removed that the port's initial association with default VLAN 1 is restored.

2. Click on **Forbidden** if there are any forbidden egress ports that you want make eligible for GVRP automatic assignment to this VLAN. Select ports from the Selected Ports list and click on << **Remove** to make the selected ports eligible or click on << **Remove All** to make all ports eligible. Note that GVRP is not supported on all OmniStack platforms.

3. Click on **Untagged** to remove an untagged VLAN association (the VLAN is the default VLAN for the port). Select ports from the Selected Ports list and click on **<< Remove** remove the untagged association from the selected ports or click on **<< Remove All** to remove the untagged association from all of the ports.

Note: When an untagged association is removed but the egress association still exists for the port, the egress VLAN port association reverts to tagged.

4. Click on **OK** when you are done to accept the new port assignments for this VLAN or click **Cancel** to cancel this action. The Assign Ports window will close, returning you to the OmniStack Ports Tab.

5. If you clicked the **OK** button in the Assign Ports window, a modify icon appears in the Name field for the selected device. To save the changes to the appropriate switch configurations, click the **Apply** button in the current 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 6400, 6600, 6800, 6850, 6855, 9000, or 9000E series switches.

ag Intern
ag Intern
-

AOS 802.1Q VLAN Port Assignments

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. The Add 802.1Q Ports Window, shown below, is used to tag a port with the current VLAN.



The top half of the Add Ports window contains a list of all 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 802.1Q assignment to this VLAN. This list contains ports that are not already tagged with this VLAN and that have Default Config as their Port Type.

To create a new 802.1Q tagged VLAN port assignment, select one or more switches and then the available ports that you want to assign and click the **OK** button. The Add Ports window closes and new list entries appear in the AOS 802.1Q Ports Tab list with the modify icon in the Name field of each entry. Click the **Apply** button to update the appropriate devices with the new 802.1Q VLAN port assignments.

Note that if you select a port that has this VLAN as its default VLAN assignment, an error occurs when the tag is applied. You cannot tag a port with its own default VLAN, as it is already part of that VLAN's broadcast domain.

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.

Edit 802.1Q VLAN Port Panel

Image: Second	OmniVista 2500 - Application: VL Elle Applications View Help	Ns Window:0	
Browse Boz.10 Ports for - TESTNET SERVERS VLAN 10(#10) 22 3 4 1 1 1 1 1 1 VLAN 2(#2) VLAN 2(#2) DCTestnetCore 10.255.10.3 3 1 1 TAG PORT 31 VLAN 10 n/a VLAN 3(#3) Name Device Stot Port Description VLAN 5(#6) VLAN 5(#6) VLAN 5(#6) VLAN 5(#6) VLAN 7(#7) Fett 802.10 VLAN Port B02.10 B02.10 Link. B02.10 Link. B02.10 VLAN Port B02.10 VLAN 7(#7) B02.10 Link. B02.10 Link. B02.10 VLAN 7(#7) Fetit 802.10 VLAN Port B02.10 Link. B02.10 Link. B02.10 Link. B02.10 VLAN 7(#7) B02.10 Link. B02.10 Link. B02.10 VLAN 7(#7) Fetit 802.10 VLAN Port B02.10 Link. B02.10 Link. B02.10 Link. Forces B02.10 Link. B02.10 Link. B02.10 VLAN 1(#1) Force Tag.Internal B02.10 Link. B02.10 Link. B02.10 VLAN 1(#1) Force Tag.Internal		802.1Q 💌	
Devices Ports Solution Solu	Browse CVLANS CVLANS CVLAN2(#2) CVLAN3(#3) SVLAN3(#3) New GROUP (#4)(#- SVLAN5(#5) VLAN5(#6) VLAN5(#6) VLAN7(#7)	Name Device Slot Port Description DCTestnetCore 10.255.10.3 3 1 TAG PORT 3/1 V	on Force Tag Internal /LAN 10 n/a
	← ←	802.1Q Ports Parameters Device: 10.255.10.3 Y Slot: 4 Port: Description: TAG PORT 4/1 VLAN 10 Force-Tag-Internat:	1

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.

AOS Edit 802.1Q VLAN Ports Window

The Edit 802.1Q VLAN Ports window, shown below, is used to modify 802.1Q tagged port parameters for multiple ports. This window displays when you select more than one port from the AOS 802.1Q Ports Tab list and click the **Edit** button.

Note that only the Description and Force Tag Internal parameters are modifiable. Parameters that are not modifiable do not appear in this window. In addition, a parameter field may appear blank if any of the devices selected are configured with a different parameter value for the same field.

Edit Multiple Rows		×
Edit 802.10 VLAN F	Ports	_
Description:		
Force Tag Internal:	on	-

To modify 802.1Q tagged port parameters, 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 6400, 6600, 6800, 6850, 6855, 9000, or 9000E 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.

02.10 Ports for Name	Device	Slot	Port	Spanning Tree	3.3 😼 🗟 🎒 VLAN Tag	Priority
	1.255.13.167	4		IEEE - GigaBit	500	Phoney
	0.255.13.167	4		IEEE - GigaBit	500	
	0.255.13.193	3		Multiple (10/100) - Ethernet	2	
View 802.1Q VI						
802.1Q Ports I	arameters					
802.1Q Ports I Device:				v		
802.1Q Ports I	arameters			Port:		
802.1Q Ports I Device:	Parameters			<u> </u>		

XOS 802.1Q VLAN Port Assignments

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. The Add 802.1Q Ports window, shown below, is used to tag a port with the current VLAN.

Add Ports	1.2									2
	Name			ddress	DNS Name	Тур				
	no-nam	0	10.25	55.11.120		OmniSi 🔺				
	🔤 no-nam	9	10.25	55.11.124		0A-512=	Selec	IIA to		
	CmniSF	153	10.25	55.11.153		OmniSi	Rena		-	
	🖬 Alias		10.25	\$5.11.174		Omni-3	Clea	r All		
	MMS-19			55.11.194		OmniSt				
	4	nr I	10.00			in rig				
Available Por	ts:			-	100	Port to b	e added:			
Name	Device	Slot	Po		£dd>>	Name	Device	Slot	Port	Function T
OmniSR153	10.255.11.153	2			< Remove	1				
OmniSR153	10.255.11.153	2			< Romove					
OmniSR153	10.255.11.153	2			Add All >>	11				
OmniSR153	10.255.11.153	2	-		ana sii se					
OmniSR153	10.255.11.153	2		• cc	Remove All	1				
			11		rielliore an	4	- 11			

The top half of the Add Ports window contains a list of all VLAN devices. When you select one or more devices from this list, the Available Ports list in the bottom half of this window displays all ports that are eligible for 802.1Q assignment to this VLAN. This list contains ports that are not already tagged with this VLAN and that have Default Config as their Port Type appear in the Available Ports list.

To create a new 802.1Q tagged VLAN port assignment, select one or more switches and then the available ports that you want to assign and click the **OK** button. The Add Ports window closes and new list entries appear in the XOS 802.1Q Ports Tab list with the modify icon in the Name field of each entry. Click the **Apply** button to update the appropriate devices with the new 802.1Q VLAN port assignments.

Note: If you select a port that has this VLAN as its default VLAN assignment, an error occurs when the tag is applied. You cannot tag a port with its own default VLAN, as it is already part of that VLAN's broadcast domain.

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.

OS X	(OS							
02.1Q P	orts for -	VLAN 2(#2)					33 📆 🗟 🖨	
Nam	ie	Device	Slot	Port	Spannin	g Tree	VLAN Tag	Priority
67	10	.255.13.167	4	1 1	EEE - GigaBit	-	500	
67	10	.255.13.167	4	2 1	EEE - GigaBit		500	
10-name	9 10	.255.13.193	3	11 N	lultiple (10/100)	- Ethernet	2	
F-84 002	4018 4	1 Part						
	2.1Q VLA 2 Ports P	N Port arameters						
	Ports P							
802.10	Ports P	arameters			Port:	2		
802.10 Device: Slot:	Ports P	arameters			_	2		

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.

XOS Edit 802.1Q VLAN Ports Window

The Edit 802.1Q VLAN Ports window, shown below, is used to modify 802.1Q tagged port parameters for multiple ports. This window displays when you select more than one port from the XOS 802.1Q Ports Tab list and click the **Edit** button. Note that only the VLAN tag and priority parameters are modifiable. Parameters that are not modifiable do not appear in this window.

Edit Multip		×
Edit 802.10	VLAN Ports	
VLAN Tag:	500	
Priority:	0	

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 seelcted 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.

02.1Q Link Agg fo	r VLAN - VLAN 1(#1)		1/1 🐨 📾 📰 🖽
Name	Device	Link Agg Id	Description
switch_23	10.255.13.23	1	0 TAG AGGREGATE 10 VLAN 1
15 002 40 1 int			
	: Agg		
View 802.1Q Link Name:	. Agg	Device:	10.255.11.59



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. The Add 802.1Q Link Aggregation Window, shown below, is used to assign a link aggregate group of ports to the current VLAN.



The top half of the Add 802.1Q Link Aggregation window contains a list of all VLAN devices. When you select one or more switches from this list, the Available Link Agg list displays all known link aggregates that are eligible for assignment to this VLAN. This list contains aggregates that are not already assigned to this VLAN.

To assign a link aggregate to the current VLAN, select one or more switches and then the available aggregates that you want to assign to the VLAN and click the **OK** button. The Add 802.1Q Link Aggregation window closes and new list entries appear in the AOS 802.1Q Link Agg Tab list with the modify icon in the Name field of each entry. Click the **Apply** button to update the appropriate devices with the new 802.1Q link aggregate assignments.

Note that when you assign a link aggregate to the current VLAN, you are changing the default VLAN for that aggregate. For example, if a link aggregate is assigned to VLAN 20 as its default VLAN and you assign the link aggregate to VLAN 300, then VLAN 300 becomes the new default VLAN for that aggregate. In addition, the link aggregate is no longer assigned to VLAN 20. It is also possible to tag a link aggregate with one or more VLANs using the AOS Add 802.1Q Ports Tab.

Refer to the OmniVista Topology application help for more information about link aggregation parameter definitions.

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.

102 10 Link 4	gg for VLAN - V	AN 4/#4)		11 3 3 8 8 19 11 1
Name		evice	Link Agg Id	Description
WV_FUJI2_1	10.255.1	1.129		Link Agg 31 VLAN 1
Edit 802.1Q	Link Agg			
Edit 802.1Q Name:	.ink Agg WV_FUJI2_12	9	Device:	10.255.11.129

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 of:

- 0 127 on OmniSwitch 9000E Switches
- 0 31 on OmniSwitch 6800/6850/7000/9000 Switches,
- 0 29 on OmniSwitch 6624 and 6648 Switches
- 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

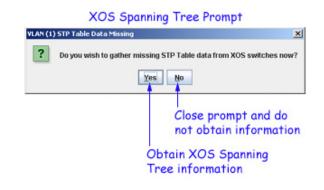
The Spanning Tree Algorithm and Protocol (STP) is a self-configuring algorithm that maintains a loop-free topology while providing data path redundancy and network scalability. STP software is active on all switches by default. As a result, a loop-free network topology is automatically calculated based 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.

JmniVista 2500 - Ap							ormation			
	plication	n: VL	ANs Window:0							
Applications Vie	w Help	2								
des d	**	e) 🔊 🖉 🍰 📩	🔻 🧭 Sp	anning Tree 🔻					4
Enterprise Network		- 1	Spanning Tree List	View for - VLAN	2(#2)			7/7 🔞	88	
🚰 Browse			Name	Address	Protocol	Priority	Maximum Age	Hello Time	Forward I	
🔁 VLANs	1		DCTestnetCore	10.255.10.254	RSTP(802.1W)	32768	20	2	15	
🗠 💏 VLAN 1(#1)		- 3	Kite2_NMS	10.255.11.194		32768	20	2	15	_
🕈 🎥 VLAN 2(#2)		13	FUJI		RSTP(802.1W)	32768	20	2	15	
- 😡 Devices		1	VLAN-Browser-70	10.255.211.70	STP(802.1D)	32768	20	2	15	
🗢 🚺 Ports		1	VLAN-Browser-71	10.255.211.71	STP(802.1D)	32768	20	2	15	_
🕈 💥 Spanning	Tree	13	VLAN-Browser-73			32768	20	2	15	
- 😤 Bridge			VLAN-Browser-75		STP(802.1D)	32768	20	2	15	
→ ↓ PX Route → ↓ Rules ⊕ (#3) ⊕ (#4)	WERS									

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. he 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.

Note: MSTP in VLAN spanning tree view is only displayed for Instance 0 under VLAN 1. None of the other instances will be displayed.

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.
- If **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.

Note: 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.

OmniVista 2500 - Application: VL/ jle Applications View Help	Window:1							
	10 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 -	Brid	lge	-				
🗲 Enterprise Network	AOS XOS							
- M Browse - 😁 VLANs	Spanning Tree Br	idge Paramet	ers for - VL	AN 1(#1)	85	85 🔞	
	Name	Device	STP	Mode	1	Protocol	Priority	
- Devices			1)(1(One S1	TP Per	LAND F			80 00 00 d0 95 a3 4
🗠 🗊 Ports								80 00 00 d0 95 b2
🕈 👸 Spanning Tree								80 00 00 d0 95 e0
Bridge								80 00 00 d0 95 d5
- 🛱 Port								80 00 00 d0 95 c8
IP Router بله						STP(802.1D)		80 00 00 d0 95 6b
IPX Router	Kite Fiber U24					STP(802.1D)	32768	80 00 00 d0 95 bd
← M Rules	1							
	View Spanning Device Spanni Device:			s	TP Mod	le: Nat(Single	STP)	~
- 30 DEAD(#8)	Bridge Parame	ters						
 Guarantined(#9) VLAN 10(#10) 	Protocol:	STP(802.10)	-	Prior	ity:		
← 200 VLAN 11(#11) ← 200 VLAN 12(#12)	Maximum Age: Forward Delay:				Hello	Time:		
	Porwal ti Delay.		dit Up	date	Ap	ply Help		

AOS Spanning Tree Bridge Parameters

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.

panning Tree B	ridge Parameters	for - VLAN 1(A	(1)		22/22	38	878
Name	Device	STP N	Aode	F	rotocol	Priority	Bridge ID
OCTestnetCore	10.255.10.3	1X1(One STP	Per VLAN)	STP(802.1D)	32768	80 00 00 d0 9
<ite_59< td=""><td>10.255.11.59</td><td>1X1(One STP</td><td>Per VLAN)</td><td>RSTR</td><td>P(802.1W)</td><td>32768</td><td>80 00 00 d0 9</td></ite_59<>	10.255.11.59	1X1(One STP	Per VLAN)	RSTR	P(802.1W)	32768	80 00 00 d0 9
xTarget	10.255.11.61	1X1(One STP	Per VLAN)	RSTR	P(802.1W)	32768	80 00 00 d0 9
xTarget	10.255.11.63	1X1(One STP	Per VLAN)	RSTR	P(802.1W)	32768	80 00 00 d0 9
(te2_97	10.255.11.97	1X1(One STP	Per VLAN)	RSTR	P(802.1W)	32768	80 00 00 d0 9
Cite	10.255.11.112	1X1(One STP	Per VLAN)	RSTR	P(802.1W)	32768	80 00 00 d0 9
xTarget (10.255.11.121	flat(Single ST			P(802.1VV)	32768	9 0b 00 00 08
«Target Edit Spanning 1 Device Spann	ree Parameters ing Tree Mode	flat(Single ST	P)	RSTR	P(802.1VV)		•
xTarget Edit Spanning 1 Device Spann Device: 10.2	ree Parameters ing Tree Mode i5.11.59	flat(Single ST		RSTR			
«Target Edit Spanning 1 Device Spann	ree Parameters ing Tree Mode i5.11.59		P)	RSTR	P(802.1VV)		•
Carget	ree Parameters ing Tree Mode 55.11.59 eters RSTP(802.1W)		P) STP Mode:		P(802.1W)		•

Edit the applicable fields, click the **OK** button, then click the **Apply** button.

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 Ro	wis	2
Edit Spanning T	ree Parameterss	
Protocol:	RSTP(802.1W)	
Priority:	32768]
Maximum Age:	20] [
Hello Time:	2]
Forward Delay:	15	

Edit the applicable fields, click the **OK** button, then click the **Apply** button.

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.

	2 200		Bridge	-		
Enterprise Network	AOS XOS	5				
🕐 VLANS	Spanning Tr	ee Bridge Parar	neters for - VL/	AN 1(#1)	4/4 🕱 📾 🚑	
	Name	Device	Protocol	Priority	Maximum Age	Hello Time
Devices	no-name	10.255.11.119	STP(802.1D)		20	2
🗢 🗊 Ports 📃	no-name	10.255.11.120	STP(802.1D)	32768	25	2
🕈 🙀 Spanning Tree	no-name	10.255.11.148	STP(802.1D)		20	2
Bridge Port		10.255.11.197	STP(802.1D)	32768	20	2
- 44 IP Router - 44 IPX Router						
- ↓ IPX Router		ning Tree Parar	neters)
	View Span	ning Tree Parar	neters)
- ↓ IPX Router	View Span			otocol:	STP(802.1D))
	View Span "When Ro	oot Parameters	Pro	otocol: ximum Ago ward Dela	e:	,

XOS Spanning Tree Bridge Parameters

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.

OmniVista 2500 - Application: V le Applications <u>V</u> iew Hel <u>p</u>	LANs Window:	D				
	2 50		Bridge	-		ļ
Enterprise Network	AOS XOS	1				
👶 VLANs	Spanning Tre	e Bridge Paran	neters for - VL	AN 1(#1)	4/4 🔞 📾 🛃	
Y 20 VLAN 1(#1)	Name	Device	Protocol	Priority	Maximum Age	Hello Time
Devices	no-name	10.255.11.119	STP(802.1D)		20	2
🗝 🗊 Ports 📃	no-name	10.255.11.120	STP(802.1D)	32768	25	2
🕈 🙀 Spanning Tree	no-name	10.255.11.148	STP(802.1D)	32768	20	2
- Bridge Port	OSR-5slot	10.255.11.197	STP(802.1D)	32768	20	2
		ng Tree Param ot Parameters 10.255.11.14 32768 : 2	8 Pr	otocol: aximum Age rward Delay		
← 30 VLAN 17(#17) ← 30 VLAN 20(#20) ← 30 VLAN 21(#21)			OK Can		s p	

Edit the applicable fields, click the **OK** button, then click the **Apply** button.

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 Ro	ws	2
Edit Spanning T	ree Parameterss	
Protocol:	RSTP(802.1W)	-
Priority:	32768	
Maximum Age:	20	
Hello Time:	2	
Forward Delay:	15	

Edit the applicable fields, click the **OK** button, then click the **Apply** button.

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.

	20 19	1 A	Port		-				-
Enterprise Network	AOS X	ios							_
Browse VLANs	Port Para	ameters De	signated Por	ts					
• 10 VLAN 1(#1)	Spanning	Tree Ports fo	. M AN 1/#1	n		3931/3931			m
- GR Ports	Name	Device	Slot/Port	Priority	Oper Status	the process of the local division of the loc	Path Cost	and a summer of	
9 Spanning Tree	Kite 59	10.255.11.59	1/5		Disabled	Enable		No	
Bridge	Kite_59	10.255.11.59			Disabled	Enable		No	12
Port	Kite 59	10.255.11.59	1/7		Disabled	Enable		No	-
IP Router	Kite 59	10.255.11.59	1/8		Disabled	Enable		No	-
IPX Router	Kite_59	10.255.11.59	1/9		Disabled	Enable		No	-
- K Rules	Kite 59	10.255.11.59	1/10	7	Disabled	Enable	0	No	-
- SO VLAN 2(#2)	Kite 59	10.255.11.59	1/11		Disabled	Enable		No	-
- 50 VLAN 3(#3)	Kite 59	10.255.11.59	1/12		Disabled	Enable		No	-
- 10 VLAN 4(#4)		10 366 11 60	1/1.5		Diashlad	Enshin	0	1.1m	
← 💏 VLAN 5(#5)	4							,	1
← 20 VLAN 6(#6)	View Sp	panning Tree P	ort Paramet	ers					
SolutionsTest() DEAD(#8)	Device:				Slot.Por	t			
Guarantined(#9)						-		-	
- 10 VLAN 10(#10)	Priority:				Oper St	atus:	ablied	1	
- 59 VLAN 11(#11)	Admin S	A	Enable		Path Co	-			
- 99 VLAN 12(#12)	Aumin S	status.	C. Transition		Path Cu	st.			
- 39 Vlan 13(#13)	Designa	ted Port Root:			Admin (Connection: No	Point to Point	1 7	
								_	

AOS Spanning Tree Port Parameters

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 criterio:

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.

	10	a 🙇 📃	Port		-				3
Enterprise Network	AOS	os							
W Browse	Port Para	ameters De	esignated	Ports					
- ∰ VLAN 1(#1)									
- Devices	Spanning	Tree Ports fo	r - VLAN	1(#1)		3931/3	931 🐯 💿		
🗢 🗊 Ports	Name	Device	Slot/Port			Admin Status	Path Cost	Manual N	lode
👇 🙀 Spanning Tree		10.255.11.59	1/5		Disabled	Enable		No	-
- 🙀 Bridge		10.255.11.59	1/6		Disabled	Enable		No	-
- 🔂 Port		10.255.11.59	1/7		Disabled	Enable		No	
IP Router ولو		10.255.11.59	1/8		Disabled	Enable		No	
IPX Router		10.255.11.59	1/9		Disabled	Enable		No	
🗢 🕍 Rules		10.255.11.59	1/10		Disabled	Enable		No	_
• 🚰 VLAN 2(#2)		10.255.11.59	1/11		Disabled	Enable		No	
🗢 🚰 VLAN 3(#3)		10.255.11.59	1/12		Disabled	Enable		No	-
🗢 🎒 VLAN 4(#4)	1 4	10 365 11 50	AME	710	Dischlad	Enchio		hia	•
- 20 VLAN 5(#5)							_		1.
• 📬 VLAN 6(#6)	Edit Spa	anning Tree P	ort Param	neters					1
← 📬 VlanOperationsTest(Device:		10.255	11 50	SI	ot/Port:	1/5		
• 20 DEAD(#8)	Device.				51	Jur or c	110		_
🗢 🍰 Quarantined(#9)	Priority:		7		Op	er Status:	Disabled		-
← 💏 VLAN 10(#10)			-		_				-
• 90 VLAN 11(#11)	Admin S	status:	Enable		 Pa 	th Cost:	0		
← 🚰 VLAN 12(#12)	Decima	ited Port Root	20.00.0	0 40 05 9	0.0 h0 0.0	min Connection:	Auto Poin	at to Doint	-
🗢 🌆 Vlan 13(#13)	Designa	ited Port Root	. 50 00 0	0 00 95 a.	seu uu Au	min connection.	AUTO NOIL	it to Point	-

Edit AOS Spanning Tree Port Parameters Panel

Edit the applicable fields, click the **OK** button, then click the **Apply** button.

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 Row	5	
Edit Spanning Tre	e Port Parameterss	
Priority:	7	
Admin Status:	Enable	-
Path Cost:	0	
fanual Mode:	No	-
Admin Connection	: Auto Point to Point	-

Edit the applicable fields, click the **OK** button, then click the **Apply** button.

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.

Elle Applications View Help
Port -
Enterprise Network AOS XOS Port Parameters Designated Ports
P ULN1 (#1) 3931/3931 Image: Control of the second sec
IPX Router Kite_59 10.255.11.59 1/10 80.00.00.00.95 a3 e0.0d 0.00.00.00.00.00.00.00 Weiles Kite_59 10.255.11.59 1/11 80.00.00.00.95 a3 e0.0d 0.00.00.00.00.00.00.00 00.00.00.00.00.00 00.00.00.00.00.00 00.00.00.00.00.00 00.00.00.00.00.00 00.00.00.00.00.00 00.00.00.00.00.00 00.00.00.00.00 00.00.00.00.00 00.00.00.00 00.00.00.00.00 00.00.00 00.00.00.00 00.00.00 00.00.00 00.00.00 00.00.00 00.00
• by VLAN 6(#6) Kite_59 10.255.11.59 1/18 80 00 00 d 95 a3 e0 0d 0 00 00 00 00 00 00 00 00 • by VLAN 6(#6) Kite_59 10.255.11.59 1/19 80 00 00 d 95 a3 e0 0d 0 00 00 00 00 00 00 00 00 00 • by DEAD(#8) Kite_59 10.255.11.59 1/19 80 00 00 d 95 a3 e0 0d 0 00 00 00 00 00 00 00 00 • by Quarantined(#9) Kite_59 10.255.11.59 1/20 80 00 00 d 95 a3 e0 0d 0 00 00 00 00 00 00 00 • by VLAN 10(#10) Kite_59 10.255.11.59 1/21 80 00 00 d 95 a3 e0 0d 0 00 00 00 00 00 00 00 • by VLAN 11(#11) Kite_59 10.255.11.59 1/22 80 00 00 d 95 a3 e0 0d 0 00 00 00 00 00 00 00

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.

		Po	rt		-					
Enterprise Network	AOS XOS									
Browse =	Port Paramete	rs Designat	ed Ports							
• 20 VLAN 1(#1)	Spanning Tree	Ports for - VLA	N 1(#1)			10	291/1291	8 8 B		W
🗢 🗊 Ports	Name	Device	Slot	Port	Service	Instance	Priority	Oper Status	Admin	3
💡 👸 Spanning Tree	nms-test-103	10.255.11.103	3	1	Bridge	1	128	Forwarding	Enable	-
- 😤 Bridge	nms-test-103	10.255.11.103	3	2	Bridge	1	128	Disabled	Enable	Ξ
- B Port	nms-test-103	10.255.11.103		3	Bridge		128	Disabled	Enable	
- A IP Router	nms-test-103	10.255.11.103	3	4	Bridge	1	128	Disabled	Enable	1
- A IPX Router	nms-test-103	10.255.11.10	3	5	Bridge	1	128	Disabled	Enable	1
⊷ 🛃 Rules	nms-test-103	10.255.11.10	1 3 1 3 1 3	6	Bridge	1	128	Disabled	Enable	1
← 💏 VLAN 2(#2)	nms-test-103	10.255.11.103	3	7	Bridge	1	128	Disabled	Enable	
∽ 歸 VLAN 3(#3)	4	1		all see)	
► 10 VLAN 4(#4) ► 10 VLAN 5(#5)	View Spannin	g Tree Port Pa	rameters							
- 10 VLAN 6(#6)	Name:				Devic	e:				
 VianOperationsTest(i 	Slot:				Port:					
 ► 100 DEAD(#8) ► 100 Quarantined(#9) 				-	_					
 WLAN 10(#10) 	Service:	Unionover			 Instar 	ice:				
SO VLAN 11(#11)	Delevite				-	C4	Disabled	7	+	1
► SO VLAN 12(#12)	Priority:				Oper	Status:	rulanno			
► 30 Vian 13(#13)	Admin Status:	Enable		- 1	Path	Cost:				
				_		www.				

XOS Spanning Tree Port Parameters

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.

	🐉 in 🛔 👌	Port	2	-	•					
Enterprise Network	AOS XOS									-
BIOWSE	Port Parameter	Designate	Ports	1						
	Spanning Tree	Ports for - VLAN	1(#1)			1	291/1291	8 8 B		Ш
- 🗊 Ports	Name	Device	Slot	Port	Service	Instance	Priority	Oper Status	Admin	3
🕈 👸 Spanning Tree	nms-test-103	10.255.11.103	3	1	Bridge		128	Forwarding	Enable	-
Bridge	nms-test-103	10.255.11.103	3	2	Bridge	1	128	Disabled	Enable	1
- B Port	nms-test-103	10.255.11.103	3	3	Bridge	3	128	Disabled	Enable	Г
- A IP Router	nms-test-103	10.255.11.103	3	4	Bridge	3	1 128	Disabled	Enable	
- J. IPX Router	nms-test-103	10.255.11.103	3	5	Bridge	-	128	Disabled	Enable	1
← M Rules	nms-test-103	10.255.11.103	3	6	Bridge		128	Disabled	Enable	1
← 30 VLAN 2(#2)	nms-test-103	10.255.11.103	3	7	Bridge	1	1 128	Disabled	Enable	
- 50 VLAN 3(#3)	4			1				-	,	T
 ► 50 VLAN 4(#4) ► 50 VLAN 5(#5) ► 50 VLAN 6(#6) 	Edit Spanning Name:	Tree Port Parar	neters		Devic	or.	10.255.1	102		
← Se VlanOperationsTest(Martic.	Timo-tese 105			Devic	6 1	10.200.1	1.103		
- 50 DEAD(#8)	Slot:	3			Port:		1			
Guarantined(#9) VLAN 10(#10)	Service:	Bridge			- Instar	ice:	1			
► 30 VLAN 11(#11) ► 30 VLAN 12(#12)	Priority: 128				Oper Status:		Forwards	-	1	
- 30 Vian 13(#13)	Admin Status:	Enable			 Path (Cost:	10			

Edit XOS Spanning Tree Port Parameters

Edit the applicable fields, click the **OK** button, then click **Apply**.

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 R	lows	×
Edit Spanning	Tree Port Parameterss	
Priority:	128	
Admin Status:	Enable	-
Path Cost:	10	

Edit the applicable fields, click the **OK** button, then click the **Apply** button.

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 seelcted 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.

		Po	rt		•		1
erprise Network	AOS XOS	1					
Browse _	Port Parame	ters Designat	ed Port	s			
9 VLAN 1(#1)	Designated Po	rts for - VLAN 1(A	(1)			1291/1291 🔞 💿 🖨	<u>ا</u> ا
- Devices	Name	Device	Slot	Port	Designated Port Root	Designated Port Cost	
🗠 🛐 Ports	nms-test-103	10.255.11.103	3		00 28 00 d0 95 6a 65 d0		00 6
🕈 💥 Spanning Tree	nms-test-103	10.255.11.103	3		00 00 00 00 00 00 00 00 00	0	00.0
Bridge	nms-test-103	10.255.11.103	3		00 00 00 00 00 00 00 00 00		00.0
- 😤 Port	nms-test-103	10.255.11.103	3		00 00 00 00 00 00 00 00 00		00.0
- 📣 IP Router	nms-test-103	10.255.11.103	3	5	00 00 00 00 00 00 00 00 00	0	000
IPX Router	nms-test-103	10.255.11.103	3	6	00 00 00 00 00 00 00 00 00		00 0
🗠 🕍 Rules	nms-test-103	10.255.11.103	3		00 00 00 00 00 00 00 00 00		00.0
VLAN 2(#2)	nms-test-103	10.255.11.103	3		00 00 00 00 00 00 00 00 00		00.00
🗩 VLAN 3(#3)	nms-test-103	10.255.11.103	3		00 00 00 00 00 00 00 00 00		00 0
9 VLAN 4(#4)	nms-test-103	10.255.11.103	3		00 00 00 00 00 00 00 00 00		00 0
🗩 VLAN 5(#5)	nms-test-103	10.255.11.103	3		00 00 00 00 00 00 00 00 00		00 0
🗩 VLAN 6(#6)	nms-test-103	10.255.11.103	3		00 00 00 00 00 00 00 00 00		00 0
VianOperationsTest(nms-test-103	10.255.11.103	3		00 00 00 00 00 00 00 00 00		00 0
DEAD(#8)	nms-test-103	10.255.11.103	3		00 00 00 00 00 00 00 00 00		00.00
Guarantined(#9)	nms-test-103	10.255.11.103	3		00 00 00 00 00 00 00 00 00		00 0
9 VLAN 10(#10)	nms-test-103	10.255.11.103	3		00 00 00 00 00 00 00 00 00		00 0
VLAN 11(#11)	nms-test-103	10.255.11.103	5		00 00 00 00 00 00 00 00 00		00.00
VLAN 12(#12)	nms-test-103	10.255.11.103	5		00 00 00 00 00 00 00 00 00		00 0
🕽 Vlan 13(#13)	1 1 4 6 6	10.255.11.105			00 00 00 00 00 00 00 00	0	00.0
VLAN 14(#14)	•	E.	_				•

XOS 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 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.

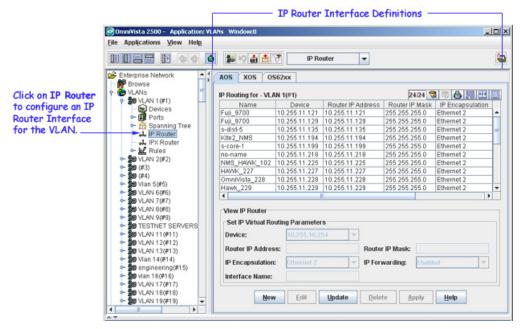
Configuring VLAN Router Interfaces

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.



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.

	ſ	IPX Router Interface Definitions	
	OmniVista 2500 - Application: VLA	ANs Window:0	
		IPX Router 👻	S
Click on IPX Router to configure an IP Router Interface for the VLAN.	Enterprise Network ■ Browse ● WUANN (#1) ● Devices ● Devices	Nos XOS IPX Routing for - VLAN 1(#1) I/1 T T T T T T T T T T T T T T T T T T T	Delay Ticks 0

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 6800/6850/9000/9000E (Release 6.1.1) series switches, you can configure up to eight (8) IP router interfaces on the switch for each VLAN. On 6000 series and XOS devices, you can configure one (1) IP router interface on the switch for each VLAN.

AOS IP Router Interface	Definitions
-------------------------	-------------

		P Ro	uter 💌		
Enterprise Network	AOS XOS OS	562xx			
🙆 VLANS	IP Routing for - VLA	NN 1(#1)		22/22	8 8 8 H H
	Name	Device	Router IP Address	Router IP Mask	IP Encapsulation
Devices Ports	Fuji_9700	10.255.11.129	10.255.11.129	255.255.255.0	Ethernet 2
	s-dist-5	10.255.11.135	10.255.11.135	255.255.255.0	Ethernet 2
← 🛱 Spanning Tree	Kite2_NMS	10.255.11.194	10.255.11.194	255.255.255.0	Ethernet 2
- 4 IP Router	s-core-1	10.255.11.199	10.255.11.199	255.255.255.0	Ethernet 2
Rules	no-name	10.255.11.218	10.255.11.218	255.255.255.0	Ethernet 2
- 10 VLAN 2(#2)	NMS_HAWK_102	10.255.11.225	10.255.11.225	255.255.255.0	Ethernet 2
- 20 Vlan 3(#3)	HAWK_227	10.255.11.227	10.255.11.227	255.255.255.0	Ethernet 2
• 30 Vian 3(#3) • 30 VLAN 4(#4)	Hawk_229	10.255.11.229	10.255.11.229	255.255.255.0	Ethernet 2
- 20 VLAV 4(#4)	lanswitch	10.255.11.230	10.255.11.230	255.255.255.0	Ethernet 2
- St Vian_5(#5)	1		1	1	•
- 10 Vian 7(#7)	View IP Router				
- 30 Vlan 8(#8)					
- 10 Vian 9(#9)	Set IP Virtual Ro	uting Parameter	\$		
- TESTNET SERVERS	Device:	10.255.11.1	29		
- 50 Vlan 11(#11)					
- 20 Vlan 12(#12)	Router IP Addres	is:	Route	r IP Mask:	
- 50 Vlan 13(#13)	IP Encapsulation	Ethernet 2	IP For	warding: Enabl	led 👻
- 50 Vlan 14(#14)	IP Encapsulation	cinemet z	IP For	warding:	eu 🗸
- 50 Vlan 15(#15)	Interface Name:				

Note: If the device supports the Multiple VRF feature, a **VRF ID** field is displayed. If you are creating a new interface, select a VRF from the drop-down menu to assign the interface to a configured VRF instance (by default all interfaces are assigned to the

Default VRF). You can assign a new interface to a VRF; however, you cannot edit the VRF ID of an existing interface.

VRF instances are created on the switch through the CLI or WebView application. This feature is only supported on 9000E Series Switches (Release 6.4.1). For more information on the VRF feature, go to "Multiple Virtual Routing and Forwarding" on page 167. *See the "Configuring Multiple VRF" Chapter in the OmniSwitch AOS Release 6 Network Configuration Guide for detailed instructions on configuring VRF instances.*

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

OmniVista 2500 - Application: V le Applications View Help	LANs Window:0						- 10
		P Ro	uter	•			
Enterprise Network	AOS XOS O	S62xx					
😁 VLANS	IP Routing for - VL	AN 1(#1)			22/22	3 S 🕹 🗐 🖽	IT
	Name	Device	Router IP A	ddress Rou	rter IP Mask		
Devices	Fuji 9700	10.255.11.129	10.255.11.12		255.255.0	Ethernet 2	۰.
- 🗊 Ports	s-dist-5	10.255.11.135	10.255.11.13	35 255.3	255.255.0	Ethernet 2	Т
- 🛱 Spanning Tree	Kite2_NMS	10.255.11.194	10.255.11.19	94 255.3	255.255.0	Ethernet 2	
- A IP Router	s-core-1	10.255.11.199	10.255.11.19	99 255.3	255.255.0	Ethernet 2	
- A IPX Router	no-name	10.255.11.218	10.255.11.21	18 255.3	255.255.0	Ethernet 2	П
- M Rules	NMS_HAWK_102	10.255.11.225	10.255.11.22	25 255.3	255.255.0	Ethernet 2	
← 20 VLAN 2(#2) ← 20 Vlan 3(#3)	HAWK_227	10.255.11.227	10.255.11.22	27 255.3	255.255.0	Ethernet 2	
• 50 VIAN 4(#4)	Hawk_229	10.255.11.229	10.255.11.22	29 255.3	255.255.0	Ethernet 2	
- 50 Vlan_5(#5)	lanswitch	10.255.11.230	10.255.11.23	30 255.3	255.255.0	Ethernet 2	
• \$ Vian_5(#6)	•		1				F
- 10 Vian 7(#7)	Create IP Router						
- 😼 Vlan 8(#8)							
- 50 Vlan 9(#9)	Set IP Virtual Ro	uting Parameter	5				
- DIESTNET SERVERS	Device:	10.255.11.1	29 💌				
🗢 💏 Vlan 11(#11)	0						1
🗢 🍰 Vlan 12(#12)	Router IP Addres	ss: 198.181.10.	2	Router IP M	ask: 255.2	55.255.0	1
🗢 💈 Vlan 13(#13)	IP Encapsulation	: Ethernet 2	-	IP Forwardi	ng: Enabl	led 🔻	
🗢 🎥 Vlan 14(#14)							
• 📬 Vlan 15(#15)	Interface Name:	VLAN 1					
• 😼 Vlan 16(#16)	a state and the second s	· · · · · ·					
• 😼 Vlan 17(#17) • 😼 Vlan 18(#18)		-	K Can	cel Hel	n		

1. Select a device from the **Device** field list (e.g., 10.255.11.129).

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.

	2 10 10 10 10 10 10 10 10 10 10 10 10 10	P Ro	uter 👻		
Enterprise Network	AOS OS62xx				
Browse VLANs	IP Routing for - VLAN	1(#1)		22/22	3 8 8 1 H
• 🐲 VLAN 1(#1) - 🗑 Devices	Name	Device	Router IP Address	Router IP Mask	IP Encapsulation
Ports	WebView_141	10.255.11.141	10.255.11.141	255.255.255.0	Ethernet 2
	WebView_142	10.255.11.142	10.255.11.142	255.255.255.0	Ethernet 2
 Spanning Tree ID Deuter 	OS6850_48X_152	10.255.11.152	10.255.11.152	255.255.255.0	Ethernet 2
- A IP Router	vx:Target	10.255.11.159	10.255.11.159	255.255.255.0	Ethernet 2
- A IPX Router	HAWK_227	10.255.11.227	10.255.11.227	255.255.255.0	Ethernet 2
	OmniVista_228	10.255.11.228	10.255.11.228	255.255.255.0	Ethernet 2
 VLAN 2(#2) 	Hawk_229	10.255.11.229	10.255.11.229	255.255.255.0	Ethernet 2
⊶ 🐲 Vlan 3(#3)	lanswitch_NNNNN	10.255.11.230	10.255.11.230	255.255.255.0	Ethernet 2
• 📁 VLAN 4(#4)	HAWK_231	10.255.11.231	10.255.11.231	255.255.255.0	Ethernet 2
- 50 VLAN 5(#5)	QoS-EP1	10.255.11.232	10.255.11.232	255.255.255.0	Ethernet 2
 SO VLAN 6(#6) SO VLAN 7(#7) 		н.,			•
• 50 VLAN 9(#9)	Edit IP Router				
- 10 VLAN 10(#10)					
- 50 VLAN 11(#11)	Set IP Virtual Routi	ng Parameters			
- 10 VLAN 12(#12)	Device:	10.255.11.14	×		
► 20 VLAN 14(#14) ► 20 vlan 16(#16)	Router IP Address:	10.255.11.14	Porter	IP Mask: 255.2	55.255.0
• 10 VLAN 17(#17)	roomen in Picturess.	10.200.11.14	router	IF INGSN: 200.2	30.200.0
• 50 VLAN 19(#19)	IP Encapsulation:	Ethernet 2	 IP Forv 	varding: Enable	ed 🔻
- 10 VLAN 20(#20)	Interface Name:	VLAN 1			

Edit IP Router Panel

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.

VRF ID

The VRF ID. If multiple VRFs are configured on the device, the VRF ID is displayed. If none are configured, or if the feature is not available on the device, the column will display "Default", indicating that the switch is operating as a single routing instance. (The Multiple VRF feature is available on AOS 6.4.1 only). For more information on the VRF feature, go to "Multiple Virtual Routing and Forwarding" on page 167.

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

		P Rot	ter	-		4
Enterprise Network	AOS XOS OS	562xx				
🕐 VLANS	IP Routing for - VLA	IN 1(#1)			6.6 🐯 🗟 4	9 .
• 🐲 VLAN 1(#1)	Name	Device	Protocol	IP Address	IP Mask	Broadcast Ad
Devices Ports	OSR5-Slot	10.255.11.197	ipRip	10.255.11.197	255.255.255.0	10.255.11.255
	VLAN-Browser-70	10.255.211.70	ipRip	10.255.211.70	255.255.255.192	10.255.211.12
 Spanning Tree 	VLAN-Browser-71	10.255.211.71	ipRip	10.255.211.71	255.255.255.192	10.255.211.12
- A IP Router	VLAN-Browser-73	10.255.211.73	ipRip	10.255.211.73	255.255.255.192	10.255.211.12
- 🕂 IPX Router	VLAN-Browser-74	10.255.211.74	ipRip	10.255.211.74	255.255.255.192	10.255.211.12
• 10 VLAN 2(#2)	VLAN-Browser-75	10.255.211.75	ipRip	10.255.211.75	255.255.255.192	10.255.211.12
\$0 VLAN 4(#4) \$0 Vlan_5(#5) \$0 Vlan 6(#6) \$0 Vlan 7(#7)	View IP Router	1		1		•
• 20 Vian 8(#8)	Set IP Virtual Ro	uting Parameter				
🗢 🎒 Vlan 9(#9)		-				
- SI TESTNET SERVERS	Device: 10	.255.11.196				
• 📁 Vlan 11(#11) • 💆 Vlan 12(#12)	Protocol:	Rip	-	IP Address:		
	IP Mask:		1	Description:		
🗢 🎒 Vlan 13(#13)			_			
• 💼 Vlan 14(#14)					Silent	
	Frame-Type:	hernet 2	T	RIP Config Mode	Stream	

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

OmniVista 2500 - Application: VI a Applications View Help						
) ; ;;;;	💎 🛛 IP Rot	ıter	-		[
Enterprise Network	AOS XOS O	S62xx				
Prowse ULANs	IP Routing for - VL	AN 1(#1)			6.6 📆 🕾 (9
9 🎒 VLAN 1(#1)	Name	Device	Protocol	IP Address	IP Mask	Broadcast A
- Devices	OSR5-Slot	10.255.11.197	ipRip	10.255.11.197	255.255.255.0	10.255.11.25
- B Ports	VLAN-Browser-70		ipRip	10.255.211.70	255.255.255.192	10.255.211.1
🗢 🙀 Spanning Tree	VLAN-Browser-71	10.255.211.71	ipRip	10.255.211.71	255.255.255.192	10.255.211.1
- A IP Router	VLAN-Browser-73		ipRip	10.255.211.73	255.255.255.192	10.255.211.1
- IPX Router	VLAN-Browser-74	10.255.211.74	ipRip	10.255.211.74	255.255.255.192	10.255.211.1
← M Rules ← M VLAN 2(#2)	VLAN-Browser-75	10.255.211.75	ipRip	10.255.211.75	255.255.255.192	10.255.211.1
• \$0 VLAN 4(#4) • \$0 Vlan_5(#5) • \$0 Vlan 6(#6)	•					
• 😼 Vlan 7(#7)	Create IP Router	r				
🗢 💈 Vlan 8(#8)	Set IP Virtual R	outing Parameter	s			
• 📬 Vlan 9(#9)	Device:	0.255.11.196	-			
 TESTNET SERVERS 	Device.	0.200.11.100	-			
• \$9 Vian 11(#11) • \$9 Vian 12(#12)	Protocol:	Rip	-	IP Address:	10.255.11.148	
• 20 Vian 12(#12) • 20 Vian 13(#13)					La martine a	
	IP Mask: 2	55.0.0.0		Description:	VLAN 1 XOS Roo	iter Port
	Frame-Type: E	thernet 2	-	RIP Config Mode:	Silent	-
• 😼 Vian 14(#14)						
• 30 Vian 14(#14) • 30 Vian 15(#15) • 30 Vian 16(#16)	Traine-Type: L					

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., 10.255.11.148). 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.

OmniVista 2500 - Application: V Applications View Help	LANs Window:0					
) 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	IP Rot	ıter	-		
Enterprise Network	AOS XOS	OS62xx				
Prowse ULANS	IP Routing for - V	LAN 1(#1)			6.6 📆 🗟 (
• 🐲 VLAN 1(#1)	Name	Device	Protocol	IP Address	IP Mask	Broadcast A
Devices	OSR5-Slot	10.255.11.197	ipRip	10.255.11.197	255.255.255.0	10.255.11.25
- R Ports	VLAN-Browser-7		ipRip	10.255.211.70	255.255.255.192	10.255.211.1
 Spanning Tree 	VLAN-Browser-7	1 10.255.211.71	ipRip	10.255.211.71	255.255.255.192	10.255.211.1
- A IP Router	VLAN-Browser-7	3 10.255.211.73	ipRip	10.255.211.73	255.255.255.192	10.255.211.1
- A IPX Router	VLAN-Browser-7	4 10.255.211.74	ipRip	10.255.211.74	255.255.255.192	10.255.211.1
• 10 VLAN 2(#2)	VLAN-Browser-7	5 10.255.211.75	ipRip	10.255.211.75	255.255.255.192	10.255.211.1
- \$9 VLAN 4(#4) - \$9 Vlan_5(#5) - \$9 Vlan 6(#6)	•	1				
- 10 vian 0(#0)	Edit IP Router					
- 😼 Vlan 8(#8)	Set ID Virtual	Routing Parameter	e			
- 妇 Vlan 9(#9)			_			
- STRET SERVERS	Device:	10.255.11.197				
•- 🞾 Vian 11(#11) •- 🞾 Vian 12(#12)	Protocol:	ipRip	-	IP Address:	10.255.11.197	
• \$0 Vian 13(#13) • \$0 Vian 14(#14)	IP Mask:	255.255.255.0		Description:	GROUP #1 IP ro	uter vport
- 🚰 Vlan 15(#15)	Frame-Type:	Ethernet 2	-	RIP Config Mode:	Silent	-
∽ 😼 Vian 16(#16) ∽ 😼 Vian 17(#17)					_	

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.

	💕 崎 🏥 🚺 IPX Router	•	
VLANS	AOS XOS		
10 VLAN 2(#2)	IPX Routing for - VLAN 2(#2)	11 🕲 🕾 🖨 🧾	
Devices Ports Spanning Tree	Name Device IPX BS0001s 10.255.11.127	X Address IPX Encapsulation RIP/SAP Mode Delay T 33333333 Ethernet 2 RIP-SAP	
- 1 IP Router - 1 IPX Router			
50 VLAN 3(#3) 50 VLAN 4(#4)			
20 VLAN 5(#5) 20 VLAN 6(#6)			
StanOperationsTest(#7)			
90 New GROUP (#8)(#8) 90 Quarantined(#9)			
10 VLAN 10(#10)	View IPX Router		
The reserves of the rest	Set IPX Virtual Routing Parameters		
19 VLAN 12(#12)			
99 VLAN 12(#12) 99 Vlan 13(#13) 99 VLAN 14(#14)	Device: 10.255.11.59		
Sep VLAN 12(#12) Sep VLAN 13(#13) Sep VLAN 14(#14) Sep VLAN 14(#14) Sep VLAN 15(#15) Sep VLAN 16(#16)	Device: 10.255.11.59 IPX Address:	PX Encapsulation: Ethernet 2	-
SVLAN 12(#12) SVLAN 12(#13) SVLAN 14(#14) SVLAN 14(#14) SVLAN 15(#15)			-

AOS IPX Router Interface Definitions

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.

	Cr	eate AU	S TAX KOU	ter Panel		
OmniVista 2500 - Application:	VLANs Window:0					_ [] ×
ile Applications View Help						
	0 瓣 🕬 🏭 🙆	IPX R	outer 💌			5
- 📾 VLAN 535(#535)	AOS					
 VLAN 536(#536) VLAN 537(#537) 	IPX Routing for -	VLAN 550(#550)			1/1 🔞 🗏	ARED
🗢 🚰 VLAN 538(#538)	Name	Device	IPX Address	IPX Encapsulation	RIP/SAP Mode	Delay Ticks
- 🚰 VLAN 539(#539)	vxTarget 10	.255.11.121	25001113	Ethernet 2	RIP Only	5
∽ 🎥 VLAN 540(#540)						
► 20 VLAN 541(#541)						
► 🞥 VLAN 542(#542)						
► \$# VLAN 543(#543)						
► Se VLAN 544(#544)						
∽ 🎥 VLAN 545(#545)						
► \$\$\$ VLAN 546(#546)	-Create IPX Rout	ter				
► 📬 VLAN 547(#547)						
← 🚰 VLAN 548(#548)	Set IPX Virtual	Routing Parame	eters			
- 🚰 VLAN 549(#549)	Device:	10.255.13.92		-		
🕈 🎥 VLAN 550(#550) 🔚						
Devices	IPX Address:			IPX Encapsulation:	Ethernet 2	-
🗢 🗊 Ports						
🗢 🙀 Spanning Tree	RIP/SAP Mode:	RIP Only		 Delay Ticks: 		
- A IP Router						
- A IPX Router			ОК	Cancel Help		
🗢 🕍 Rules 🛛 👻			On	Concer Dath		

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 A	OS IPX R	outer Pane	el		
🧭 OmniVista 2500 - Application: VL	ANs Window:0					_ 🗆 ×
Eile Applications View Help						
) 🐉 () 🍰 🖗	IPX Ro	uter 💌			a
∽ 🕶 VLAN 535(#535) 🚔	AOS					
 Se VLAN 536(#536) Se VLAN 537(#537) 	IPX Routing for -	VLAN 550(#550)			1/1 🔞 🗐	
- 🕶 VLAN 538(≢538)	Name	Device	IPX Address	IPX Encapsulation	RIP/SAP Mode	Delay Ticks
 VLAN 539(#539) VLAN 540(#540) 	vxTarget 10	.255.11.121	25001113	Ethernet 2	RIP Only	5
VLAN 541(#541)						
- 🖢 VLAN 542(#542)						
🗢 🚰 VLAN 543(#543)						
• 99 VLAN 544(#544)						
 VLAN 545(#545) VLAN 546(#546) 	-					
VLAN 547(#547)	Edit IPX Router					
- SO VLAN 548(#548)	Set IPX Virtual	Routing Parame	ters			
🗢 🎥 VLAN 549(#549)	Device:	10.255.11.121				
• 10 VLAN 550(#550)						
Ports	IPX Address:		25001113	IPX Encapsulation:	Ethernet 2	
🗢 👸 Spanning Tree	RIP/SAP Mode:	RIP Only		Delay Ticks:	5	
- A IP Router				-		
- A IPX Router			ОК	Cancel Help		
Rules V						

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.

OmniVista 2500 - Application ile Applications View Help	VLANs Window:0	
	🙆 🔰 🛃 IPX Router 👻	
Browse	AOS XOS	
9 29 VLAN 1(#1)	IPX Routing for - VLAN 1(#1) 3/3 🐯	
	Name Device Protocol NetAddressFrameType Description no-name 10.255.11.120 IPX RIP and SAP 866666666 Ethernet 2 IPX router port Alias 10.255.11.174 IPX RIP and SAP 66666666 Ethernet 2 IPX router port no-name 10.255.11.174 IPX RIP and SAP 444bed Ethernet 2 IPX router port no-name 10.255.13.175 IPX RIP and SAP 444bed Ethernet 2 IPX router port	
✓ ✓		1
Sep VianOperationsTe Sep UlanOperationsTe Sep DEAD(#3) Sep VLAN 10(#10) Sep VLAN 11(#11) Sep VLAN 12(#12) Sep VLAN 12(#13)	View IPX Router Set IPX Virtual Routing Parameters Device: ID255.11.103 Protocol: IPX RBP Cody Net Address:	

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

and the second se	60 200		IPX Router	-				
Browse VLANs	AOS XOS							
📲 VLAN 1(#1)	IPX Routing for	- VLAN 1(P	#1)			3/3 😒	B	
Devices	Name [Device	Protocol	Net Address	Frame Type	Description	Admin Status	Op
- B Spanning Tree			IPX RIP and SAP			IPX router port		Activ
IP Router			IPX RIP and SAP			IPX router port		Activ
IPX Router	no-name 10.2	55.13.175	IPX RIP and SAP	444bed	Ethernet 2		Enable	Activ
- 50 VLAN 4(#4)	_							
- 30 VLAN 2(#2) - 30 VLAN 3(#3) - 30 VLAN 4(#4) - 30 VLAN 5(#5) - 30 VLAN 5(#6)	4		,					
- \$0 VLAN 2(#2) - \$0 VLAN 3(#3) - \$0 VLAN 4(#4) - \$0 VLAN 5(#5) - \$0 VLAN 5(#5) - \$0 VLAN 5(#5) - \$0 VLAN 5(#5)	Create IPX Ro	and the second	-					
- SU VLAN 2(#2) - SU VLAN 3(#3) - SU VLAN 4(#4) - SU VLAN 5(#5) - SU VLAN 5(#6) - SU VLAN 5(#6) - SU DEAD(#8) - SU Dearantined(#9)	1 Marganeses	and the second	-					
VLAN 2(#2) VLAN 3(#3) VLAN 3(#3) VLAN 4(#4) VLAN 5(#5) VLAN 6(#6) VLAN 6(#6) ULAN 6(#6) ULAN 6(#8) UDEAD(#8) Uuarantined(#9) VLAN 10(#10)	Create IPX Ro	and the second	Parameters					
- SU VLAN 2(#2) - SU VLAN 3(#3) - SU VLAN 4(#4) - SU VLAN 5(#5) - SU VLAN 5(#5) - SU VLAN 5(#6) - SU DEAD(#8) - SU DEAD(#8) - SU VLAN 10(#10) - SU VLAN 11(#11)	Create IPX Ro Set IPX Virtu Device:	al Routing	Parameters		Address		BREFA	866
	Create IPX Ro Set IPX Virtu	al Routing 10.255.1 IPX RIP a	Parameters 1.103 and SAP		Address: [666666	666

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 filed 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.

62xx IP Routing Tab

The 62xx IP Routing tab provides a list of all 6200 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 62xx 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 6000 series devices, you can configure one (1) IP router interface on the switch for each VLAN.

e Applications View Help						
		P Rour	ter 💌			3
Enterprise Network	AOS XOS OS	62жк				
🙆 VLANS	IP Intrfaces for - VL	AN 1(#1)		2	12 🕲 🕾 🖨 🞚	
9-20 VLAN 1(#1)	Name	Device	IP Address	IP Mask	The IP Interface	
Devices	6200_Stack_of_7	10.255.11.123	10.255.11.123	255.255.255.0	static	U
⊷ 🗊 Ports ⊷ 🥸 Spanning Tree	6200_Stand_Alone	10.255.11.124	10.255.11.124	255.255.255.0	static	U
Rules Rules VLAN 2(#2) VLAN 2(#4) VLAN 4(#4) VLAN 4(#4) VLAN 5(#5) Man 6(#6)						
	1		,			
VLAN 2(#2) Vlan 3(#3) VLAN 4(#4) Vlan 5(#6) Vlan 6(#6) Vlan 6(#6) Vlan 7(#7)						
	View IP Interface		1			1
VLAN 2(#2) VLAN 2(#2) VLAN 4(#4) VLAN 4(#4) VLAN 4(#4) VLAN 6(#5) VLAN 5(#5) VLAN 5(#6) VLAN 8(#8) VLAN 8(#8) VLAN 8(#8) VLAN 8(#1) VLAN 1(#11) VLAN 1(#11) VLAN 1(#12)	View IP Interface Set IP Interface P		1			
	View IP Interface Set IP Interface P	arameters .11.123	IP Address			
VLAN 2(#2) Vlan 3(#3) Vlan 3(#3) Vlan 5(#5) Vlan 5(#5) Vlan 5(#6) Vlan 8(#8) Vlan 8(#8) Vlan 8(#8) Vlan 1(#11) Vlan 12(#12) Vlan 12(#13) Vlan 14(#14)	View IP Interface Set IP Interface P Device: 10.255		4			
	View IP Interface Set IP Interface P		IP Address The IP Inter		tie-	
	View IP Interface Set IP Interface P Device: 10.255		The IP Inter			

6200 Series IP Router Interface Definitions

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 62xx Routing Tab to activate the Create IP Router panel. Follow the steps below to define an IP router interface.

Create 6200 IP Ro	uter Panel
-------------------	------------

\$ 9 \$ 7	IP Route	er 🔽			
AOS XOS OS6	2жх				
IP Intrfaces for - VLA	N 1(#1)		2	2 😪 🕾 🗛 🎹 🖽	3100
Name	Device	IP Address			
			255.255.255.0	static	UF
			255,255,255,0	static	U
4		,			
∢ ⊂Create IP Interface		,			•
Create IP Interface	rameters	,		1	
Create IP Interface Set IP Interface Pa		,			
Create IP Interface		■ IP Address:	199	8.181.10.5	•
	IP Intrfaces for - VLA Name 6200_Stack_of_7	IP Intrfaces for - VLAN 1(#1) Name Device 6200_Stack_of_7 10.255.11.123	IP Intrfaces for - VLAN 1(//1) Name Device IIP Address 6200_Stack_of_7 10.255.11.123 10.255.11.123	IP Intrfaces for - VLAN 1(#1) IP Address IP Mask 0200_51ack_of_7 10.255.11.123 10.255.11.123 255.255.255	IP Intrfaces for - VLAN 1(#1) P/Z Image: Constraint of the cons

1. Select a device from the **Device** field list.

2. Enter an IP address in the **Router IP** Address field (e.g., 198.181.10.5). 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 an interface type from the **IP Interface Type** field list.

5. 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.

	0 🐉 🖉 🎍 🕅	IP Rout	ter 💌			4
Enterprise Network	AOS XOS OS	62xx				
P Browse VLANs	IP Intrfaces for - VL/	AN 1(#1)		Đ	2 🕲 🕾 🖨	
9 🐲 VLAN 1(#1)	Name	Device	IP Address	IP Mask	The IP Interfac	e Type Ad
- Devices	6200_Stack_of_7	10.255.11.123	10.255.11.123	255.255.255.0	static	UP
🗢 🗊 Ports 🗢 👸 Spanning Tree	6200_Stand_Alone	10.255.11.124	10.255.11.124	255.255.255.0	static	UP
We Rules VLAN 2(#2) Se VLAN 2(#2) Se VLAN 4(#4) Se VLAN 4(#4) Se VLAN 5(#5) Se VLAN 5(#6) Se VLAN 8(#6)	1		,			•
VLAN 2(#2) VLAN 2(#2) So VLAN 2(#2) So VLAN 2(#4) So VLAN 4(#4) So VLAN 5(#5) So VLAN 5(#6) So VLAN 5(#6) So VLAN 5(#8)	▲ Edit IP Interface —		,			•
VLAN 2(#2) VLAN 2(#2) VLAN 2(#2) VLAN 4(#4) Start VLAN 4(#4) Start VLAN 4(#4) Start VLAN 4(#5) VLAN 5(#6) Start VLAN 5(#6) Start VLAN 5(#6) Start VLAN 5(#8) Start VLAN 5(arameters	7			
VLAN 2(#2) VLAN 2(#2) VLAN 2(#2) VLAN 3(#3) VLAN 4(#4) VLAN 4(#4)	Edit IP Interface		,			•
VLAN 2(#2) VLAN 2(#2) VLAN 2(#2) VLAN 4(#4) VLAN 4(#4) VLAN 4(#4) VLAN 4(#6) VLAN 4(#6) VLAN 7(#7) VLAN 7(#7) VLAN 7(#7) VLAN 7(#7) VLAN 7(#1) VLAN 1(#11) VLAN 2(#2) VLAN 1(#11) VLAN 1(#11) VLAN 1(#12) VLAN 13(#13)	Edit IP Interface		IP Address:	. 10.	255.11.123	•
VLAN 2(#2) VLAN 2(#2) VLAN 2(#2) VLAN 3(#3) VLAN 4(#4) VLAN 4(#4)	Edit IP Interface	11.123	IP Address: The IP Inter			,

Edit 6200 IP Router Panel

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.

IP Address

The IP host address that identifies the router interface network.

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 Interface Type

The IP router interface type: Static or DHCP.

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.

Using the IP Interfaces Node

The **IP Interfaces** Node under 9000 and 6850 devices in the Devices Tree is used to view and configure IP Interfaces for 9000/6850 Series Switches. As shown below, you can access this table by clicking open a 9000/6850 Series switch IP address in the Devices Tree and then clicking on the **IP Interfaces** node.

Applications View Help										
	104		IP Interface	s	-					6
derprise Network	IP Interfaces	Table(10.255.	11,122)				51/5	1 3 8	ame	
VLANs	Name	IP Address	Mask	A	dmin State	Device		VLAN Id	IP Forward	-
Devices	vian-1 1	0.255.11.122	255.255.255.0	en	able	vian		1	enable	-
Ff (10.0.0.0/8)	vlan-50 f	0.50.50.50	255.255.0.0	en	able	unbour	d	0	disable	1
9 9 10.255.11.122	vlan-55 9	9.99.99.99	255.255.255.0	en	able	unboun	d	0	disable	
Mobility	vlan-60 8	0.60.60.60	255.255.255.0	en	able	vian		60	disable	
IP Interfaces	vlan-70 7	0.70.70.70	255.255.255.0	en	able	vian		70	disable	
► E 10.255.11.123	vian-80 0	0.0.0	0.0.0.0	en	able	unbour	d	0	disable	
► 10.255.11.124	vlan 2199 2	.99.80.2	255.255.252.0	en	able	vlan	A.A	2199	disable	
► 10.255.11.135	vlan 3999 2	99.252.2	255.255.255.0	en	able	vian		3999	disable	
10.255.11.155	vlan 2101 2	2.1.80.2	255.255.252.0	en	able	vian		2101	disable	
- 10.255.11.159	vlan 2102 2	2 80 2	255 255 252.0	en	able	vian		2102	disable	•
10.255.11.183	4	- Aller							,	
► 10.255.11.194	Manu ID Inte	rface Attribut								
► 10.255.11.197	view ip inte	riace Attribut	es.							-
► 10.255.11.199	Name:				IP Address	R .				
🗠 🗑 10.255.11.218 🛛 🛁	Mask				Admin Sta	1.0.1	enable		-	
► 10.255.11.227	mask.				Admin Sta	te;	Contraction of the		-	
► 10.255.11.228	Device Type	c hinthound		-	VLAN Id:					
► 10.255.11.229				-			-			
► 10.255.11.230	IP Forward:	enable		1	IP Encaps	ulation:	ethern		-	13
► 10.255.11.231							-		_	43 I.
► 10.255.11.232	MTU:				Local Prov	y Arp:	orsoble		×	
► 10.255.11.233	Prim Cfg:	False	1	-						
► 10.255.11.234	Prim cig:	College.								
- D 10.255.11.235		Distance 11	100000		1000000		10101		1	
► 10.255.11.237		New	Edit Upd	ate	Delet	e	Apply	Help		
10.255.11.238										

The IP Interfaces Table displays a list of all configured IP interfaces for the selected switch. When you click on one of the interfaces in this list, the bottom portion of the screen displays the current attribute values for the selected interface.

To create a new interface, click on the **New** button and complete the fields as described below. To modify an existing interface, select the interface in the table, click on the **Edit** button, and modify the field(s) as described below. When you are done, click on the **OK** button. A modify icon appears in the Slot/Port field of the table for the new/modified interface. Click the **Apply** button to apply the changes.

Note: If the device supports the Multiple VRF feature, a **VRF ID** field is displayed. If you are creating a new interface, select a VRF from the drop-down menu to assign the interface to a configured VRF instance (by default all interfaces are assigned to the Default VRF). You can assign a new interface to a VRF; however, you cannot edit the VRF ID of an existing interface.

VRF instances are created on the switch through the CLI or WebView application. This feature is only supported on 9000E Series Switches (Release 6.4.1). For more information on the VRF feature, go to "Multiple Virtual Routing and Forwarding" on page 167. See the "Configuring Multiple VRF" Chapter in the OmniSwitch AOS Release 6 Network Configuration Guide for detailed instructions on configuring VRF instances.

IP Interface Attribute Definitions

Name

The user-defined name for the interface.

IP Address

The interface IP address.

Mask The IP address mask.

Admin State The administrative state of the interface (Up/Down)

Interface

The VLAN on which the interface is configured.

Device Type

The device on which the interface is configured (e.g., VLAN, GRE Tunnel).

VLAN ID

The VLAN ID number.

IP Forward

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.

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.

MTU

The Maximum Transmission Unit (MTU) value for the interface.

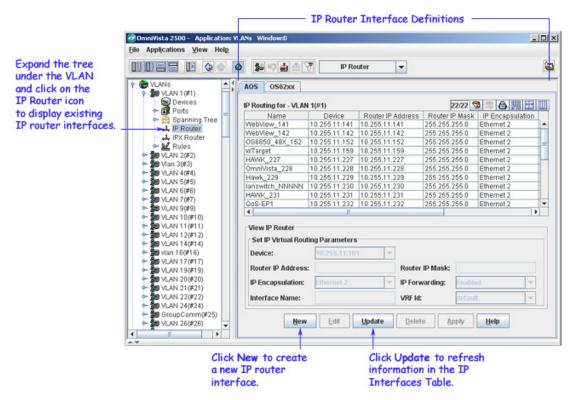
Local Proxy ARP

Enables/Disables Local Proxy ARP on the interface.

Configuring Multiple IP Router Interfaces

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 per switch per VLAN. These switches display an IP Router 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.

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



Creating an IP Router Interface

To create an IP router interface on a device, click on the **New** button at the bottom of the IP Interfaces Page. This activates the Create IP Interface Attributes panel, as shown below.

Note: If the device supports the Multiple VRF feature, a **VRF ID** field is displayed. If you are creating a new interface, select a VRF from the drop-down menu to assign the interface to a configured VRF instance (by default all interfaces are assigned to the Default VRF). You can assign a new interface to a VRF; however, you cannot edit the VRF ID of an existing interface.

VRF instances are created on the switch through the CLI or WebView application. This feature is only supported on 9000E Series Switches (Release 6.4.1). For more information on the VRF feature, go to "Multiple Virtual Routing and Forwarding" on page 167. See the "Configuring Multiple VRF" Chapter in the OmniSwitch AOS Release 6 Network Configuration Guide for detailed instructions on configuring VRF instances.

10.255.11.152	Router IP / 10.255.11.1 10.255.11.1		Router		888	
Device 10.255.11.141 10.255.11.142 10.255.11.152	10.255.11.1		Router			
10.255.11.141 10.255.11.142 10.255.11.152	10.255.11.1		Router			
10.255.11.141 10.255.11.142 10.255.11.152	10.255.11.1					ion
10.255.11.142 10.255.11.152			/00 /00 /	255.0	Ethernet 2	-
10.255.11.152		142	255.255.2		Ethernet 2	_
	10.255.11.1		255.255.2		Ethernet 2	
10.255.11.159	10.255.11.1		255.255.2		Ethernet 2	-17
	10.255.11.2		255.255.2	255.0	Ethernet 2	—µ
10.255.11.228	10.255.11.2	228	255.255.2	255.0	Ethernet 2	
10.255.11.229	10.255.11.2	229	255.255.2	255.0	Ethernet 2	
10.255.11.230	10.255.11.2	230	255.255.2	255.0	Ethernet 2	
10.255.11.231					Ethernet 2	
10.255.11.232	10.255.11.2	232	255.255.2	255.0	Ethernet 2	-
						•
10.255.11.10	-	Router	IP Mask:			
: Ethernet 2	-	IP Forw	arding:	Enable	bd	-
		VRF Id:		defaut	t	-
	10.255.11.229 10.255.11.230 10.255.11.231 10.255.11.232 uting Parameters 10.255.11.10 ss:	10.255.11.229 10.255.11. 10.255.11.230 10.255.11. 10.255.11.231 10.255.11. 10.255.11.231 10.255.11. 10.255.11.232 10.255.11. Uting Parameters 10.255.11.101	10.255.11.229 10.255.11.230 10.255.11.230 10.255.11.231 10.255.11.231 10.255.11.231 10.255.11.232 10.255	10.255.11.229 10.255.11.229 255.255. 10.255.11.230 10.255.11.230 255.255. 10.255.11.231 10.255.11.231 255.255. 10.255.11.232 10.255.11.232 255.255. uting Parameters 10.255.11.101 st: Router IP Mask: c Ethernet 2 IP Forwarding:	10.255.11.229 10.255.11.229 255.255.255.0 10.255.11.230 10.255.11.230 255.255.255.0 10.255.11.231 10.255.11.231 255.255.255.0 10.255.11.232 10.255.11.232 255.255.255.0 10.255.11.232 10.255.11.232 255.255.255.0 10.255.11.101 ss: Router IP Mask: Ethernet 2 IP Forwarding: Enable	10.255.11.229 10.255.11.229 255.255.0 Ethernet 2 10.255.11.230 10.255.11.230 255.255.255.0 Ethernet 2 10.255.11.231 10.255.11.231 255.255.255.0 Ethernet 2 10.255.11.232 10.255.11.232 255.255.25.0 Ethernet 2 10.255.11.232 10.255.11.232 255.255.25.0 Ethernet 2 10.255.11.101 ss: Router IP Mask: c Ethernet 2 IP Forwarding: Enabled

Create IP IP Router Panel

Follow the steps below to create an IP router interface.

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 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.

OmniVista 2500 - Application: Applications View Help	TER S THINGHA							_
	o ≥ 0∎≞®₹	IP Ro	uter	•				
Enterprise Network								
• 30 VLAN 1(#1)	IP Routing for - VLAN	- 4 4					3 8 8 1	
- Devices	Name WebView 141	Device 10.255.11.141	Router IP 10.255.11.		Router I 255.255		IP Encapsul Ethernet 2	ation
- R Ports		10.255.11.141	10.255.11.		255.255.		Ethernet 2	_
🗢 👸 Spanning Tree			10.255.11.		255.255.		Ethernet 2	
- +1+ IP Router		10.255.11.159	10.255.11.		255.255.		Ethernet 2	
- +1, IPX Router		10.255.11.227	10.255.11.		255.255.		Ethernet 2	_
🗢 🕍 Rules		10.255.11.228	10.255.11.		255.255.		Ethernet 2	_
🗢 🍰 VLAN 2(#2)			10.255.11.		255.255.		Ethernet 2	_
🗢 🎒 Vlan 3(#3)		10.255.11.230	10.255.11.		255.255.3		Ethernet 2	
- 10 VLAN 4(#4)		10.255.11.231	10.255.11.		255.255.		Ethernet 2	
🗢 월 VLAN 5(#5)			10.255.11.		255.255.		Ethernet 2	_
• 😼 VLAN 6(#6)	4						In other the second sec	•
Sor VLAN 7(#7) Sor VLAN 9(#9) Sor VLAN 9(#9) Sor VLAN 10(#10) Sor VLAN 11(#11)	Edit IP Router	ng Parameters						
- 10 VLAN 12(#12)	Device:	10.255.11.14						
- 10 VLAN 14(#14)	Router IP Address:	10.255.11.14	1	Porter	IP Mask:	266.2	55.255.0	
- 10 vlan 16(#16)	Pouler IP Address;	10.255.11.14	1	Router	IP mask.	255.23	55.255.0	
 VLAN 17(#17) VLAN 19(#19) 	IP Encapsulation:	Ethernet 2	-	IP Forv	varding:	Enable	ed	-
- 50 VLAN 20(#20) - 50 VLAN 21(#21)	Interface Name:	VLAN 1						
VLAN 22(#22) VLAN 24(#24)		0	K Ca	ncel	Help			

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.

VRF ID

The VRF ID. If multiple VRFs are configured on the device, the VRF ID is displayed. If none are configured, or if the feature is not available on the device, the column will display "Default", indicating that the switch is operating as a single routing instance. (The Multiple VRF feature is available on AOS 6.4.1 only). For more information on the VRF feature, go to "Multiple Virtual Routing and Forwarding" on page 167.

Defining VLAN Rules

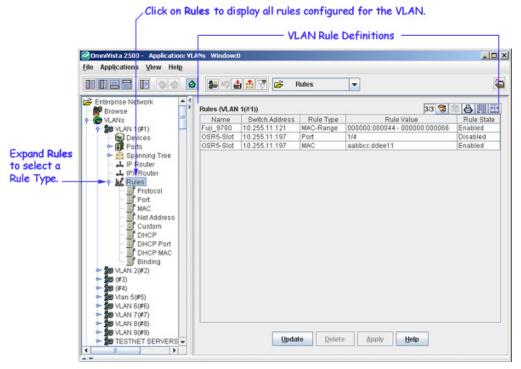
VLAN rules are used to classify mobile port traffic for dynamic VLAN port assignment. Rules are defined by specifying a port, MAC address, protocol, network address, custom (user-defined), DHCP generic, DHCP port, DHCP MAC address, or binding rule criteria to capture certain types of network device traffic. 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.

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:

- 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.
- 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 are 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.

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 pro- tocol 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 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
 Port-IP Address Binding 	Frame contains a matching source port and source IP subnet address.	
	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 sub- net address, or	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 proto- col 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.

VLAN Rule Precedence Table

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.

	0 10 10 10 10	Protocol 💌		
Enterprise Network	Protocol Rules (VLAN 1(#	1))	9/9	3 8 A
VLANs	Name	Switch Address	Rule Value	Rule State
• 50 VLAN 1(#1)	NMS_HAWK_102	10.255.11.102	Protocol = ipE2	Enabled
Devices	HAWK_118	10.255.11.118	Protocol = ipE2	Enabled
- R Ports	no-name	10.255.11.129	Protocol = ipE2	Enabled
► Spanning Tree	HAWK_131	10.255.11.131	Protocol = ipE2	Enabled
IP Router	HAWK_153	10.255.11.153	Protocol = ipE2	Enabled
IPX Router	AOS_Hawk_157_alias	10.255.11.157	Protocol = ipE2	Enabled
Rules	OmniSwitch_198_xyz	10.255.11.198	Protocol = ipE2	Enabled
Protocol	086602-24	10.255.11.207	Protocol = ipE2	Enabled
Port	OmniSwitch	10.255.11.244	Protocol = ipE2	Enabled
Net Address Custom DHCP DHCP Port DHCP Port DHCP MAC Binding VLAN 2(#2) VLAN 3(#3) VLAN 3(#3) Son WGROUP (#4)(#				

Protocol Rules Window

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.

Adding a Protocol Rule

The Add Protocol Rules pop-up window, shown below, is used to create a protocol rule definition for the current VLAN.

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

Name	Address	DNS Name	Type	
DCTestnetCore	10.255.10.3		087700	
Kite_59	10.255.11.59		086800-4	ni
wTarget	10.255.11.61		OS6800-2	-
w/Target	10.255.11.63		OS6800-2	
kite2_97	10.255.11.97		086800-2	
🖬 Kite	18.255.11.112		OS6800-2	-
4	1. S. M. S.			
⊖ IPX	PX-Novell			
	PX-Novell Ethernet Type			
O IPX-LLC O I			000 (DS	AP
O IPX-LLC O I	Ethernet Type			

Add Protocol Rules Window

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.

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.

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.

	Port 💌		3
Port Rules (VLAN 1	#1))	6.6	3 088
Name	Switch Address	Rule Value	Rule State
		2/1/Bridge/1	Disabled
VLAN-Falcon186		1/23	Enabled
vxTarget_xyz	10.255.11.219	2/1	Enabled
vxTarget_xyz	10.255.11.219	2/2	Enabled
vxTarget_xyz	10.255.11.219	2/3	Enabled
vxTarget_xyz	10.255.11.219	2/4	Enabled
	Name OSR-5slot VLAN-Falcon186 w/Target_xyz w/Target_xyz w/Target_xyz	Name Switch Address OSR-5slot 10.255.11.153 VLAN-Falcon186 10.255.11.216 vxTarget_xyz 10.255.11.219 vxTarget_xyz 10.255.11.219	Name Switch Address Rule Value OSR-5slot 10.255.11.153 2/1/Bridge/1 VLAN-Falcon186 10.255.11.186 1/23 vxTarget_xyz 10.255.11.219 2/1 vxTarget_xyz 10.255.11.219 2/2 vxTarget_xyz 10.255.11.219 2/3

Port Rules Window

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.

Adding a Protocol Rule

The Add Port Rules pop-up window, shown below, is used to create a port rule definition for the current VLAN.

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.

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.

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.

	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	MAC		
Enterprise Network	MAC Rules (VLAN	l 1(#1))	F	11/11 🕲 💿 🔠 🧮
VLANS	Name	Switch Address	Rule Value	Rule Stat
• 10 VLAN 1(#1)	OSR-5slot	10.255.11.153	aabbcc:ddee11	Enabled
Devices	VLAN-OS6648	10.255.11.181	00aabb:123456	Enabled
- B Ports	VLAN-OS6648	10.255.11.181	00aacc:123456	Enabled
- Spanning Tree	VLAN-036648	10.255.11.181	00b0d0:193c68	Enabled
- A IP Router	VLAN-036648	10.255.11.181	00b0d0:428259	Enabled
IPX Router	FalconCmm	10.255.11.243	00b0d0:193c68	Enabled
P M Rules	FalconCmm	10.255.11.243	00b0d0:428259	Enabled
Protocol	ES0001A-1	10.255.211.157	00aabb:123456	Enabled
- Port	ES0001A-1	10.255.211.157	00aacc:123456	Enabled
MAC	ES0001A-1	10.255.211.157	00b0d0:193c68	Enabled
Net Address	ES0001A-1	10.255.211.157	00b0d0:428259	Enabled
→ DHCP → DHCP Port → DHCP NAC → Binding → Se VLAN 2(#3) → Se VLAN 3(#3) → Se VLAN 5(#5) → Se VLAN 5(#5) → Se VLAN 5(#5)			*	

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.

Adding a MAC Address Rule

The Add MAC Rules pop-up window, shown below, is used to create a MAC address rule definition for the current VLAN.

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.

Add MAE Rules				
Select Devices for t	he MAC rules			
Name	Address	DNS Name	Type	Version
DCTestnetCore	10.255.10.3		087700	5.1.6.86.R02
Kite_59	10.255.11.59		OS6800-48	6.1.2.12.R02
w/Target	10.255.11.61		OS6800-24	6.1.2.16.R02
w.Target	10.255.11.63		OS6800-24	8.1.2.144.R01
kite2_97	10.255.11.97		OS6800-24	6.1.2.150.R01
💓 Kite	10.255.11.112		OS6800-24	6.1.2.144.R01
4		1		
Enter MAC Address	in the	cluded MAC A	ddresses	
Single/Start:		Single	VStart	End
inde				
ind:				
	Add			
	200			

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.

Name	Address	DNS Name	Туре	Version		
no-name	10.255.13.193		Omni-9V00	4.4.4.165	-	
SW40371	10.255.13.201		OS6648	5.1.6.146.R0	2	
a no-name	10.255.13.220		0A-512	4.5.2.32		
5052	10.255.13.225		OmniCore-	5. 3.3.1r21 - 3 J		
DUT-1	10.255.211.68		OS6648	5.1.5.148.R0	4	Browse
OmniSwitch	10.255.211.69		036624	5.4.1.127.R0	1	1
no-name	10.255.211.70		0\$9700	6.1.2.89.R01		
vxTarget	10.255.211.71		059700	6.1.1.606 R0	1	
Falcon	10.255.211.75		0\$7700	5.4.1.135.R0	1	
Kite 76	10.255.211.76		0\$6800-48	6.1.2.87.R01	-	
(nown MAC Addresse	s:	1		Included MAC Ad	dresses:	
MAC Address	SlotPo	n <u>A</u> dd	>>:	MAC Address	SlotPort	-
00d095:12dc	3/5	1				f
00d095.12dcl	3a 3/5	<< <u>R</u> er	move			
00d095:9a07	3/2	Add A	11 h h			
00d095:9a07	16 3/5	AGUA	ŵ,>>			
00d095:9a071	7 3/2	<< Rem	mm All			
(II	100	- realli	over red			

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.

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.

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.

IIII D Q 0	10 to 1	Net Au	ldress	-		3
Enterprise Network	Network Rules	(VLAN 1(#1))			4/4 🔞	
VLANS	Name	Switch Address	1	Rule Value		Rule State
• 10 VLAN 1(#1)	vxTarget_xyz	10.255.11.219	IP = 3.0.0.), Mask= 255.0.0.0	1	Enabled
Devices	vxTarget_xyz	10.255.11.219	IPX=1431	651653, Encapsulation = novella	raw I	Enabled
- R Ports	FALCON-137	10.255.11.221	IP = 10.25	5.11.0, Mask = 255.255.255.0	1200	Enabled
- Spanning Tree	no-name	10.255.13.220	Protocol =	ip, IP = 172.20.0.0, Mask = 255.2	255.0.0	Enabled
IPX Router IPX Router Protocol Port MAC Net Address						
Areids Protocol Protocol Port Areidadress OHCP Port OHCP Port OHCP Port OHCP Port OHCP Mac Binding VLAN 2(#2) VLAN 4(#4)						
VLAN 2(#2) VLAN 2(#2) VLAN 2(#2) VLAN 3(#3)	4					

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.

Adding a Network Address Rule

The Add Net Address Rules pop-up window, shown below, is used to create a network address rule definition for the current VLAN.

Add Net Address Rules									
Select D	evices for t	he Network rules							
N	lame	Address	DNS Name	Type	Version				
🖌 Kite_5				OS6800-48	6.1.2.88.R01	+			
🖌 Kite_6	50	10.255.11.60		OS6800-48	6.1.2.37.R01	=			
🛿 vxTarg		10.255.11.61		OS6800-24	6.1.2.82.R01				
w.Targ		10.255.11.63		OS6800-24	6.1.2.81.R01				
alcon 🖉		10.255.11.100		087700	5.1.6.393.R01				
Kite_F	iber_U24	10.255.11.101		OS6800-U24	5.3.1.181.R02	Ŧ			
•			- II.		•				
⊛ IP	IP Addres Subnet Ma Network N	ask							

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.

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.

Defining a Custom Rule

Custom rules determine VLAN assignment based on criteria defined by the user. The criteria consist 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.

Custom Rules Window

OmniVista 2500 - Application: VLA	Wis Window:0			_10
e Applications View Help				
1083 D 000 0	🐉 in 🛔 😫	Custom	-	
- 10 Ouarantined(#9)	Custom Rules (VI.A	N 18(#18))		14 S & A III -
\$0 VLAN 11(#11) \$0 VLAN 12(#12) \$0 VLAN 12(#12) \$10 Vlan 13(#13)	Name lanswitch	Switch Address 10.255.211.150	Rule Value Offset = 1, Value = 0x60020000, Mas	Rule State
- 50 VLAN 17(#17) • 50 VLAN 18(#18)				
Devices Ports Spanning Tree				
- A IP Router - A IPX Router - & Rules				
Protocol				
Net Address				
- DHCP	4			
DHCP Port		New	pdate Delete Apply	Help

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.

Adding a Custom Rule

The Custom Rules pop-up window, shown below, is used to create a network address rule definition for the current VLAN.

Add Custon	1 Rules		2
Select Device	s for the Custom r	ules	
Name Name	Address 10.255.211.150	DNS Name	Type OS7800
4	1		
((A)	•
		-	•
• Offset:		A.	•
			•

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.

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.

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 rules is allowed per device, only one rule appears for each device.

	🙆 🐉 Ю 🏭 🚺 ОН	CP 💌	
← 🞾 Quarantined(#9) – ← 🞾 VLAN 10(#10)	DHCP Generic Rules (VLAN 18)	/#18))	11 🕲 🗇 🖨 🛄 🗄
- \$9 VLAN 11(#11)	Name	Switch Address	Rule Valu
 50 VLAN 12(#12) 50 Vlan 13(#13) 	lanswitch	10.255.211.150	Generic
Devices Devices Ports Spanning Tree			
- Devices • 1 Ports			

DHCP Generic Rules Window

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. 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.

Adding a DHCP Generic Address Rule

The Add DHCP Generic Rules pop-up window, shown below, is used to create a DHCP generic rule definition for the current VLAN.

Add DHCP Generic Rules Select Devices for the DHCP Generic rules Name Address DNS Name Type Version Ind lanswitch 10.255.211.150 OS7800 5.1.6.138.R02 Ok Cancel Help

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 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.

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.

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.

		DHCP Port 💌	
Enterprise Network Browse	DHCP Port Rules (VLAN	1(#1))	72/72 🧒 🖷 📇 🖽
VLANS	Name	Switch Address	Rule Value
9 50 VLAN 1(#1)	NMS_HAWK_102	10.255.11.102	1/1
Devices	NMS_HAWK_102	10.255.11.102	1/10
- Ports	NMS_HAWK_102	10.255.11.102	1/11
🗢 👸 Spanning Tree	NMS_HAWK_102	10.255.11.102	1/12
IP Router	NMS_HAWK_102	10.255.11.102	1/13
- J IPX Router	NMS_HAWK_182	10.255.11.102	1/14
P & Rules	NMS_HAWK_102	10.255.11.102	1/15
Protocol	NMS_HAWK_102	10.255.11.102	1/16
- Port	NMS_HAWK_102	10.255.11.102	1/17
- If MAC	NMS_HAWK_102	10.255.11.102	1/18
Net Address	NMS_HAWK_102	10.255.11.102	1/19
- If Custom	NMS HAWK 102	10.255.11.102	1/2
DHCP	NMS_HAWK 102	10.255.11.102	1/20
DHCP Port	NMS HAWK 102	10.255.11.102	1/21
- TO DHCP MAC	NMS HAWK 102	10.255.11.102	1/22
Binding	NMS_HAWK_102	10.255.11.102	1/23
- 20 VLAN 2(#2)	NING LIBING LOD	10 365 11 103	1 ma
- 50 VLAN 3(#3)	4		

DHCP Port Rules Window

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. 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.

Adding a DHCP Port Rule

The Add DHCP Port Rules pop-up window, shown below, is used to create a DHCP port rule definition for the current VLAN.

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.

Name		Address	D	NS Name		Type	Version		
DCTestnetCo	re	10.255.10.3			0677	00	5.1.6.86.R02	-	
Kite_59	×	10.255.11.59			0.968	800-48	6.1.2.12.R02	=	Select Al
w/Target		10.255.11.61			0568	300-24	6.1.2.16.R02		Percet Pri
w Warget		10.255.11.63			0868	800-24	6.1.2.144.R01		Clear All
kite2_97		10.255.11.97			0.568	00-24	6.1.2.150.R01		2000000000
Kite		10.255.11.112			0568	300-24	6.1.2.144.R01	-	
a		18.855.11.151				10.0	0.1.1.000.000	1.	
Available Ports:					_	Port Rule	is to be added:		
Device	SIC	otPort/Service/Instance		Add >>		Device	Slot/Port/Service/Instance		
10.255.11.59	1/1		-	<< Remo	14			_	
10.255.11.59	1/2		-	<< Gauno	WB .				
10.255.11.59	1/3			Add All >	~				
10.255.11.59	1/4			Aug Au	-				
10.255.11.59	1/5			<< Romov	110.0				
10.255.11.59	1/6		-		0.9111				

Add DHCP Port Rules

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.

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.

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.

	19 4 A	MAC	-	
terprise Network	MAC Rules (VLAN	(1(#1))	F	11/11 🕲 🕲 🔠 🛃
VLANS	Name	Switch Address	Rule Value	Rule Sta
30 VLAN 1(#1)	OSR-5slot	10.255.11.153	aabbcc:ddee11	Enabled
Devices	VLAN-OS6648	10.255.11.181	00aabb:123456	Enabled
- Ports	VLAN-OS6648	10.255.11.181	00aacc:123456	Enabled
- Spanning Tree	VLAN-OS6648	10.255.11.181	00b0d0:193c68	Enabled
- IP Router	VLAN-0S6648	10.255.11.181	00b0d0:428259	Enabled
IPX Router	FalconCmm	10.255.11.243	00b0d0:193c68	Enabled
P M Rules	FalconCmm	10.255.11.243	00b0d0:428259	Enabled
Protocol	ES0001A-1	10.255.211.157	00aabb:123456	Enabled
- Port	ES0001A-1	10.255.211.157	00aacc:123456	Enabled
MAC	ES0001A-1	10.255.211.157	00b0d0:193c68	Enabled
- Met Address	ES0001A-1	10.255.211.157	00b0d0:428259	Enabled
DHCP DHCP Port DHCP MAC DHCP MAC DHCP MAC VLAN 2(#2) VLAN 3(#3) VLAN 4(#4) VLAN 5(#5) VLAN 6(#6)	4			

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.

Adding a MAC Address Rule

The Add MAC Rules pop-up window, shown below, is used to create a MAC address rule definition for the current VLAN.

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.

Select Devices for 1		I average and		1
Name	Address	DNS Name	Туре	Version
DCTestnetCore	10.255.10.3		087700	5.1.6.86.R02 -
Kite_59	10.255.11.59		OS6800-48	6.1.2.12.R02
w/Target	10.255.11.61	1	OS6800-24	6.1.2.16.R02
wTarget	10.255.11.63		OS6800-24	6.1.2.144.R01
kite2_97	10.255.11.97		OS6800-24	6.1.2.150.R01
kite	10.255.11.112		OS6800-24	8.1.2.144.R01
1		11		
0.000 C C C C C C C C C C C C C C C C C				
End:	Add			

Add MAC Rules Window

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.

A	ddress	DNS Name	Туре	Version		
10.25	55.13.193		Omni-9W00	4.4.4.165	-	
10.25	55.13.201		OS6648	5.1.6.146.R03	2	
10.25	55.13.220		OA-512	4.5.2.32		
10.25	55 13 225		OmniCore-5	3.3.1r21 - 3 J.		
10.25	55.211.68		056648	5.1.5.148.R04		Browse
10.25	55.211.69		036624	5.4.1.127.R01		1
10.25	55.211.70		0\$9700	6.1.2.89.R01		
10.25	55.211.71		059700	6.1.1.606.R01		
10.25	55.211.75		0\$7700	5.4.1.135.R01		
10.25	55.211.76		036800-48	6.1.2.87.R01	•	
sses:			- Ir	Included MAC Ad	dresses:	
-	Piet/Deut	Add	>>	MAC Address	Plat/Dout	-
		A CONTRACTOR	111111111111	MAC Address	SHUPPOR	1
		<< <u>Re</u>	move			
		Add A	11 >>			
101.01		<< Rem	ove All			
	10.25 10.25 10.25 10.25 10.25 10.25 10.25 10.25 10.25 10.25 10.25 5585:	10.255.13.193 10.255.13.201 10.255.13.225 10.255.13.225 10.255.211.69 10.255.211.69 10.255.211.70 10.255.211.71 10.255.211.75 10.255.211.76 sses: Slot/Port 2dc60 3/5 2dc60 3/	10.255.13.193 10.255.13.201 10.255.13.220 10.255.13.225 10.255.13.225 10.255.211.69 10.255.211.70 10.255.211.75 10.255.211.76 2025.211.76 2025.211.76 2025.211.76 2026.00 3/5 2026.00 3/5 2026.00 3/5 2026.03 3/5 207.06 3/2 Add A 207.0757 3/2	10.255.13.193 Omni-9WX 10.255.13.201 OS6648 10.255.13.221 OS6648 10.255.13.225 OmniCore-5 10.255.211.68 OS6648 10.255.211.69 OS6648 10.255.211.70 OS8700 10.255.211.71 OS8700 10.255.211.75 OS7700 10.255.211.76 OS8800-48 Sses: Add >> 2dc60 3/5 2dc68 3/5 00786 3/2 Add Aji >> So7767 3/2	IO.255.13.193 Omni-9VXX 4.4.4.165 IO.255.13.201 OS6649 51.6.146.R0 IO.255.13.220 OA-512 4.5.2.32 IO.255.13.225 OmniCore-53.11r21 - 3.J. 3.3.1r21 - 3.J. IO.255.211.68 OS6646 51.5146.R0 IO.255.211.69 OS6624 5.4.1.127.R0 IO.255.211.70 OS9700 6.1.2.89.R01 IO.255.211.71 OS9700 6.1.2.89.R01 IO.255.211.75 OS7700 5.4.1.127.R01 IO.255.211.76 OS8200-48 6.1.2.87.R01 IO.255.211.76 OS8200-48 6.1.2.87.R01 IO.255.211.76 OS8200-48 6.1.2.87.R01 IO.255.211.76 OS8200-48 6.1.2.87.R01 Sees: Add >> MAC Address 20766 3/5 << <bernove all<="" td=""> Add All >> Add All >> MAC Address 20786 3/5 <<remove all<="" td=""></remove></bernove>	10.255 13.193 Omni-9WX 4.4.4 165 10.255 13.201 OS6648 5.1.6.146.R02 10.255 13.220 OA-512 4.5.2.32 10.255 13.225 OrmicOre-5 3.3.1721 - 3.J., 10.255 13.225 OrmicOre-5 3.3.1721 - 3.J., 10.255 211.68 OS6648 5.1.6.146 R04 10.255 211.70 OS8700 6.1.2.98 R01 10.255 211.71 OS8700 6.1.2.89 R01 10.255 211.76 OS700 5.4.135 R01 10.255 211.76 OS8800-48 6.1.2.87 R01 \$

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.

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.

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.

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.

Binding Rules Panel

Binding Rules (VLAN 18	8(#18))	1/1 😒 💿 🖨 💹 🖽
Name	Switch Address	Rule Value
lanswitch	10.255.211.150	MAC = 0010a4:e508f8, IP = 10.255.215.1
•		
	New Update D	elete Apply Help

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.

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.

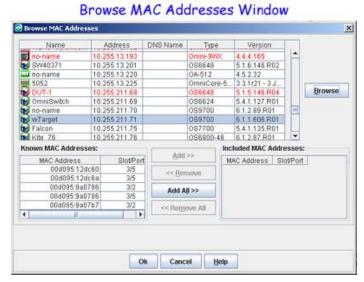
Add Binding Rule:				
Select Devices for 1	the Binding rules			
Name	Address	DNS Name	Type	
DCTestnetCore	10.255.10.3		087700	ŀ
Kite_59	10.255.11.59		OS6800-48	ŀ
🖬 vxTarget	10.255.11.61		0\$6800-24	Γ
w/Target	10.255.11.63		OS6800-24	1
kite2_97	10.255.11.97		OS6800-24	Т
NIEZ_07				
Kite	10.255.11.112		OS6800-24	1
	10.255.11.112	1	086800-24	
¥ Kite ↓ Binding Rule Type ● IP-MAC ○ N	MC-PORT	O MAC-IP-I	•	
¥ Kite ↓ Binding Rule Type ● IP-MAC ○ N	MAC-PORT		PORT	

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.



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

Select Device:	s for the Binding r	ules		
Name	Address	DNS Name	Туре	Version
answitch	10.255.211.150		0\$7800	5.1.6.138.R02
Binding Rule T	O MAC-PORT		MAC-IP-I	PORT
 IP-MAC IP-PORT 	O PORT-PRO	TOCOL	MING-1 CA	

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.

and the second	Rules			
Select Devices	s for the Binding ru	les		
Name Name	Address 10.255.211.150	DNS Name	Type OS7800	Version 5.1.6.138.R02
Binding Rule T	vpe			
○ IP-MAC○ IP-PORT	MAC-PORT PORT-PROTO	OCOL O	MAC-IP-P MAC-POR	ORT RT-PROTOCOL
○ IP-MAC○ IP-PORT	MAC-PORT PORT-PROTO	OCOL O		
O IP-MAC	MAC-PORT PORT-PROTO alues			

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.

Name	A	ddress	DNS Name	Туре	Version		
no-name	10.25	5.13.193		Omni-9W00	4.4.4.165	-	
SW40371	10.25	5.13.201		OS6648	5.1.6.146.R	02	
no-name	10.25	5.13.220		OA-512	4.5.2.32		
5052	10.25	5.13.225		OmniCore-5	5. 3.3.1r21 - 3	J	
DUT-1	10.25	5.211.68		OS6648	51.5148.R	04	Browse
OmniSwitch	10.25	5.211.69		0\$6624	5.4.1.127.R	01	
no-name	10.25	5.211.70		0\$9700	6.1.2.89.R0	1	10
💓 vxTarget	10.25	5.211.71		059700	6.1.1.606 R	01	
Falcon	10.25	5.211.75		0\$7700	5.4.1.135.R	01	
🖬 Kite 76	10.25	5.211.76		056800-48	6.1.2.87.R0	1 .	-
Known MAC Addre	sses:				included MAC A	ddress	es:
MAC Address		Slot/Port	Add	>>	MAC Address	SlotP	ort
00d095:1		3/5			ne to statute as	and a later of the	
00d095.1		3/5	<< <u>R</u> en	110/10			
00d095:9	a0786	3/2	Add A				
00d095:9	a0786	3/5	A00 A	ŵ >>			
00d095:9	a07b7	3/2	<< Rem	com All			
4		- P	- se mette	OVE MI			

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.

elect Devices t	for the Binding ru	lles			
Name	Address	DNS Name	Туре		ersion
answitch 1	0.255.211.150		OS7800	5.1.6	.138.R02
inding Rule Ty	90				
IP-MAC	O MAC-PORT	0	MAC-IP-P	ORT	
IP-PORT	PORT-PROT	OCOL O	MAC-POF	T-PR	DTOCOL
inding Rule Va	lues				
Slot/Port:		j			
Protocol Value	s				
	O IP-SNAP				
⊖ IPX	O IPX-Novel				
O IPX-LLC	O Ethernet 1	Гуре			
O IPX-SNAP	SAP Head	ler			(DSAP)
 AppleTalk 					(SSAP)
· shipse i din	SNAP TWO	e			
O DECNet	O oran iyo				

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.

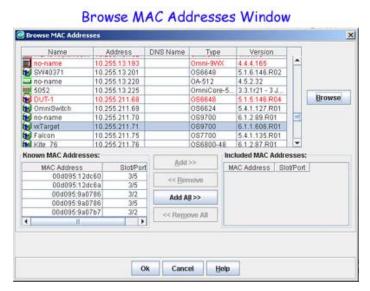
🗟 Add Binding R	ules			
Select Devices	for the Binding r	ules		
Name	Address	DNS Name	Туре	Version
👩 lanswitch 🕆	10.255.211.150		0\$7800	5.1.6.138.R02
O IP-MAC	O MAC-POR		MAC-II	
				P-PORT PORT-PROTOCOL
○ IP-MAC ○ IP-PORT	 MAC-POR PORT-PRO 			
	O MAC-POR O PORT-PRO		○ MAC-F	

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.



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.

	Rules				
Select Devices	for the Binding rul				- 201
Name Ionswitch	Address 10.255.211.150	DNS Name	Type OS7800	Version 516138 R	0.2
Binding Rule Ty	100 mg 200 mg 200 mg		~		
O IP-MAC	MAC-POF	स	O M	AC-IP-PORT	
IP-PORT	O PORT-PR	OTOCOL	M M	AC-PORT-PR	OTOCOL
Binding Rule Va	alues				
	-				
3inding Rule Va MAC Address	-	Brow	wse		
	-	Bron	wse		
MAC Address	¢	Bron	wse		
MAC Address Slot/Port:	¢		wse		
MAC Address Slot/Port: Protocol Value IP	es O IP-SNA	P	wse		
MAC Address Slot/Port: Protocol Value	es	P	WS8		
MAC Address Slot/Port: Protocol Value IP	es O IP-SNA	p	wse		
MAC Address Slot/Port: Protocol Value IP O IPX	es IP-SNA IPX-Nov Etherno	p vell et Type	wse		(DSAP)
MAC Address Slot.Port: Protocol Value IP IPX IPX-LLC IPX-SNAP	es IP-SNA IP-SNA IPX-Nor Etherni SAP He	p vell et Type	wse		(DSAP)
MAC Address Slot.Port: Protocol Value IP IPX IPX IPX-LLC	es IP-SNA IP-SNA IPX-Nor Etherni SAP He	p vell et Type	WSE		(DSAP) (SSAP)

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.

Name	A	ddress	DNS Name	Туре	Version		
no-name	10.2	55.13.193		Omni-9W00	4.4.4.165	-	
SW40371	10.2	55.13.201		OS6648	5.1.6.146.R	02	
no-name	10.2	55.13.220		OA-512	4.5.2.32		
5052	10.2	55.13.225		OmniCore-	5. 3.3.1r21 - 3	J	-
DUT-1	10.2	55.211.68		OS6648	5.1.5.148.R	04	Browse
OmniSwitch	10.2	55.211.69		036624	5.4.1.127.R	01	
no-name	10.2	55.211.70		0\$9700	6.1.2.89.R0	1	
vxTarget	10.2	55.211.71		059700	6.1.1.606.R	01	
Falcon	10.2	55.211.75		0\$7700	5.4.1.135.R	01	
Kite 76	10.2	55.211.76		0\$6800-48	6.1.2.87.R0	1 -	
nown MAC Addres	ses:				Included MAC A	ddresse	s:
MAC Address	1	SlotPort	Add	>>:	MAC Address	SlotPo	1
00d09512	dc60	3/5	1				
00d09512	dc6a	3/5	<< <u>R</u> e	move			
00d095:9a	0786	3/2	0.04	III La			
00d095:9a	0786	3/5	A00 /	ŵ >>			
00d095:9a	07b7	3/2	CC Down	mm All			
(II			really	NA DEC			
		1.00	9				
00d095:9a 00d095:9a	0786		Add /				

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.

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.

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.

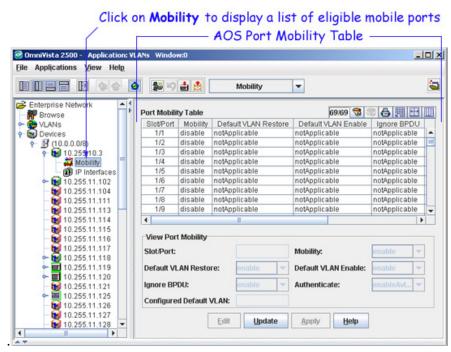
2. Enable or disable mobile port properties, described below, that determine mobile port behavior. Configuring mobility on AOS devices is done on an individual port basis. This step applies only to the selected ports and does not dictate switch-wide behavior of all mobile ports.

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



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 pop-up window opens that contains the configurable port parameters.

Configure	d Default \	AN:	1						
gnore BP	DU:		disable		-	Authenti	cate:	enable8021x	-
Default VI	AN Resto	re:	enable		•	Default \	/LAN Enable:	enable	-
SlotPort:			1/13		_	Mobility:		enable	-
Edit Port	Mobility								
-		_		_	-				1
1/15	disable		plicable	notAppli			notApplicable		
1/14	disable		plicable	notAppli	cabl	8	notApplicable		
1/13	enable	enabl		enable	0.010	<i>y</i>	disable	enable8021x	
1/12	disable		plicable plicable	notAppli			notApplicable notApplicable	notApplicable notApplicable	-
1/10	disable disable		plicable	notAppli			notApplicable		
1/9	disable		plicable	notAppli			notApplicable		
1/8	disable		plicable	notAppli			notApplicable		
1/7	disable	notAp	plicable	notAppli	cabl	0	notApplicable	notApplicable	
1/6	disable	notAp	plicable	notAppli	cabl	8	notApplicable	notApplicable	
SlotPort	Mobility	Defa	ult VLAN Restore	Default	VLA	N Enable	Ignore BPDU	J Authenticate	Configure

Edit Port Mobility Panel

Using either the Edit Port Mobility panel or pop-up 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

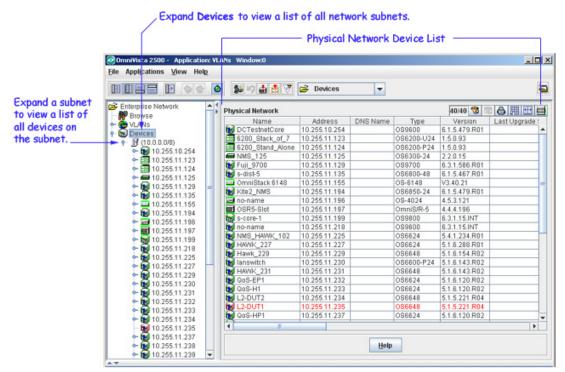
Determines if the default VLAN for a mobile port will carry traffic received on that port that does not match any VLAN rules. If this parameter is set to **on**, then non-matching traffic is forwarded on the default VLAN. If this parameter is set to **off**, then non-matching traffic is discarded and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

Туре

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 auto-discovered, 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.
- 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.

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 a device to display the menu.)

1023 d 44 4	\$ 9 4 37	🖻 Devices		-			3
Enterprise Network	Physical Network					40/40 🔞	8
VLANS	Name	Address	DNSM	lame	Type	Version	Last Upgrade :
Devices	DCTestnetCore	10.255.10.254			OS9600	6.1.5.479.R01	
P B (10.0.0.0/8)	6200_Stack_of_7	10.255.11.123			OS6200-U24	1.5.0.93	
► 10.255.10.254	6200_Stand_Alon				OS6200-P24	1.5.0.93	
· III 10.255.11.123	NMS_125	10.255.11.125			OS6300-24	2.2.0.15	
o- E 10.255.11.124	🙀 Fuji_9700 👘	urrent Window		Desé	e Status	1.586.R01	
►	s-dist-5		· · ·			5.467.R01	
• 10.255.11.129	CILINGTACK 01	ew Window	2 1	Loca	te on Map	0.21	
· · · · · · · · · · · · · · · · · · ·	Kite2_NMS P	ing Node		Notif	cations	5.479.R01	
· II.255.11.155	no-name p	oll Node		Healt	h	3.121	
► 10.255.11.194	COSR5-Slot					4.196	
► 10.255.11.196	and proofer i	onfigure Traps		SSH		1.15.INT	
· II 10.255.11.197	no-name P	oll for Traps		Stati	stics	1.15.INT	
← → 10.255.11.199	NMS_HAWK_ S	ave to Working		Loca	te End-Stations	1.234.R01	
• 10.255.11.218	HAWIK_227	eboot		Dack	up Configuratio	5.288.R01	
► 10.255.11.225	Hawk_229		1	Back		0.154.1902	
► 10.255.11.227	answitch C	opy Certified To Wo	rking		OS6600-P24	5.1.6.143.R02	
• 10.255.11.229	HAWIK_231 C	opy Working To Cer	tified		OS6648	5.1.6.143.R02	
- 10.255.11.230	QoS-EP1	ventory			OS6624	5.1.6.120.R02	
· M 10.255.11.231	Q05-H1	-			OS6624	5.1.6.120.R02	
• 10.255.11.232	CL DOTA	ib Browser			OS6648	5.1.5.221.R04	
• 10.255.11.233		/ebPage			OS6648	5.1.5.221.R04	
• M 10.255.11.234	QoS-HP1	10.200.11.207			OS6624	5.1.6.120.R02	
10.255.11.235	1			-			•
• 10.255.11.237							
► 10.255.11.238				Help			
· 10.255.11.239 ·			_	2 auto	1 m m		

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.

	-			0.000			11973 A		
		n: 17	LANs Window:0						_ 0
	Eile Applications View Help								
		ø	10 🛔 🕺 💕	10.255.	.10.3 💌				
	Enterprise Network	1	VLAN definitions for: 10.	255.10.3			8.8	3 - A .	
	► OTANS		VLAN ID Descri	ption	Admin Status	Oper Status	Type	Spanning Tr	
lick on Mobility	P Devices		1 VLAN 1		Enabled	Inactive	Standard		
configure port			10 TESTNET SE	RVERS	Enabled	Active	Standard		
	9 10.255 10.3	8	27 VLAN 27		Enabled	Active	Standard		
obility	🕨 🚔 Mobility		50 TESTNET AR		Enabled	Active	Standard		
	IP Interfaces		206 STATIC AUTO		Enabled	Active	Standard		
	► 10.255.11.102		220 DHCP LABS 243 CORPNET C		Enabled Enabled	Active	Standard		
	► 10.255.11.118 ► 10.255.11.119		550 TESTNET AR		Enabled	Active		Enabled	
	► ■ 10.255.11.119		000 TED THE FAR	ERO D	Chabled	Pacting	otanuaru	Enabled	
	- 10.255.11.126		•						
	► 10.255.11.129 ► 10.255.11.131		View VLAN Definition						
	► ■ 10.255.11.148 ► ■ 10.255.11.153		Description:			Admin Statu	s: Ena	bled	-
	► B 10.255.11.157		Oper Status:	Active	-	Type:	-		
	10.255.11.172		Oper Status.	errine.	*	type.	510	nuaru	
	· 10.255.11.197		Spanning Tree Status:	Enabled	-	Mobility:	Ena		-
	► 10.255.11.198		Authentication:	Disabled		Router-Proto	cot: PU		1-1
	► == 10.255.11.201	8	warnenacadon:	Disableu	· · · · ·	POULET-PTOL		(A.	_
	► 10.255.11.207 ■ 10.255.11.218	8	Voice Status:	Disabled	-				

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,

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 popup menu displayed when you click on any device in the Devices Physical Network list.

Using the VLAN Wizard

To display the VLAN Wizard, click the VLAN Wizard icon **Solution**. 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.

S VLAN Wizard			×
	VLAN Basic Informatio	n	
AA	VLAN ID:	158	
	Description:	VLAN 158	1
1000	Admin Status:	Enabled	
	Type:	Standard	
TIN	Spanning Tree Status:	Enabled	
日间日	Mobility:	Enabled	
	Router Protocol:	None	
	Authentication:	Disabled	
A Virtual Local Area Network (VLAN) is a collection of physical ports on one or more switches to which a set of policies apply. A VLAN combines the flexibility of policy-based			
virtual LANs with the security and isolation of port-based VLANs.		< Back Negt > Finish Cancel Help	

VLAN Basic Information Fields

The VLAN Basic Information page is used to define basic configuration paratmeters 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.

Туре

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

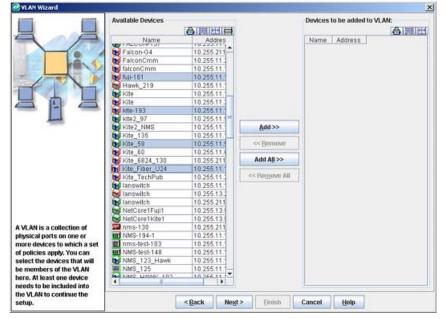
Selecting Devices for the VLAN

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.



Selecting Devices for the VLAN

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.

VLAN Wizard	VLAN Wiza	rd Ports Par	ne			
			ye.			
	Selected I					
	VLAN ID:	158				
		186 (10.2	55.211.155)			-
1000	Switches:	BBH-H22	(10.255.211.175)			_
	Switches:	lanswitch	(10.255.211.150)			
		OmniSwit				
	Ports of I	answitch (1	0.255.211.150)	Selected Ports		
	SI	100 million (100 million)	Port		Slot Port	
		1	1 -			
-2000		1	2			
	-	1	- 3			
		1	4			
		1	5			
		1	5	Add >>		
		1		108brouger		
		1	8	<< Bemove		
	-	1	12	Add All >>		
		1	13			
		1	15	<< Remove All		
		1	16			
		1	17			
		1	18			
		1	19			
ere you can assign ports the VLAN. These ports		1	20			
ill not be moved unless		1	22 -			
u manually change the	here	1	**		1	
LAN assignment of the	1					
orts.			<back next<="" td=""><td>> Finish</td><td>Cancel Help</td><td></td></back>	> Finish	Cancel Help	

Selecting Ports for the VLAN

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).

	VLAN Wiza Selected D		ge					
	VLAN ID:	158						
	Switches:	BBH-H22 lanswitch	55.211.155) (10.255.211.175) (10.255.211.150) (10.255.11.125)					
	Ports of N	IMS_125 (1	Egress 0.255.11.125)	O Forbidden C	Untagged Selected Ports			
	SI	x	Port		Slot Port			
	1 1 2	1	1 🔺					
		1	2					
	-	1	3					
	-	1	4					
	-	1	4 5 6	Add >>				
		1	7					
	-	1	8	<< Bemove				
		1	9		1			
		1	10	Add All >>				
		1	11	<< Remove All	P			
		1	12	s s rue <u>in</u> ore ru				
		1	13					
		1	14					
		1	15					
you can assign ports		1	16					
e VLAN. These ports ot be moved unless		1	17					
		1	18 -					

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.

	VLAN Wizard XOS Ro	uting Page				
Y	186 (10.2 Switches:	255.211.155)				
	IP IP Routing Param	eters		26		
	Routing Protocol:	ipRip	-	IP Address:	0.0.0.0	
-	Subnet Mask:	255.0.0.0		Description:	[
	Framing Type:	Ethernet-2	-	RIP Mode:	Silent	-
	IPX IPX Routing Param Routing Protocol:		-	IPX Address:	400169	oD
	Framing Type:	Ethernet-2				
affic can ever move reen VLAN's except Joh routing, Routing	Framing Type:	Ethernet-2				

Configuring XOS Router Interfaces

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

S VLAN Wizard	
	VLAN Wizard AOS IP Routing Page Selected Devices
	BBH-H22 (10.255.211.175) Ianswitch (10.255.211.150) OmniSwitch (10.255.211.69) vxTarget (10.255.211.71)
	PRouting Router IP Address Router IP Mask IP Encapsulation IP
	View IP Router
	IP Routing Parameters Router IP Address: Router IP Mask: IP Encapsulation: Interface Name:
No traffic can ever move between VLAN's except through routing, Routing can be achieved by using the external router or by creating a virtual router port in the VLAN. Each switch in	New Edit Delote
the Group can have its own virtual router ports.	<back negt=""> Finish Cancel Help</back>

Configuring AOS IP Router Interfaces

Note: If the device supports the Multiple VRF feature, a **VRF ID** field is displayed. If you are creating a new interface, select a VRF from the drop-down menu to assign the interface to a configured VRF instance (by default all interfaces are assigned to the Default VRF).

VRF instances are created on the switch through the CLI or WebView application. This feature is only supported on 9000E Series Switches (Release 6.4.1). For more information on the VRF feature, go to "Multiple Virtual Routing and Forwarding" on page 167. See the "Configuring Multiple VRF" Chapter in the OmniSwitch AOS Release 6 Network Configuration Guide for detailed instructions on configuring VRF instances.

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.

🗟 VLAN Wizard								×
	Selected De	BBH-H lansw Omnis	PX Routing Pa i22 (10.255.21 itch (10.255.21 Switch (10.255 get (10.255.21	1.175) 11.150 .211.6				
	✓ IPX IPX Rout IPX Addr RIP/SAP	ess:	RIP Only	0	IPX Encapsulation: Delay Ticks:	Ethernet 2	•	
No traffic can ever move between VLAN's except through routing. Routing can be achieved by using the external router or by creating a virtual router port in the VLAN. Each switch in the Group can have its own virtual router ports.			< Back		legt>	Cancel	Help	

Configuring an AOS IPX Router Interface

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 VLAN Rules

The next page of the VLAN Wizard, shown below, enables you to configure rules for the VLAN. A separate rule configuration tab enables you to configure each type of rule: Port Rules, MAC Address Rules, DHCP Port Rules, DHCP MAC Address Rules, Protocol Rules, Network Address Rules, DHCP Rules, Custom Rules, and Binding Rules. The Summary Tab displays a summary of the rules you configure.

Protoc	ol Net A	ddress	DHCP	Cus	stom Bindir	g Sum	mary		
Port		MAC A	ddress		DHCP	Port	r	DHCP MAC	Address
	Name		Address	T	DNS Name	Туре		Version	1
In the On	nniSwitch		5.211.69			OS6624	5.4.1	163.R01	
	arget	10.25	5.211.71	_		059700	6.1.1	.632.R01	Select All
by lan		10.25	5.211.150			087800	5.1.6	3.146.R02	Select A
18	6	10.25	5.211.155			08-4024	4.5.1	2.59	Clear All
	H-H22	10.25	5.211.175			OS6648	5.1.0	5.138.R02	
Availa	ble Ports:						Port Rule	es to be addee	4-
								is in the annei	A.
)evice	Slot/Po	rt/Service/I	n:			Device		n. rvice/Instance
		Slot/Po 1/1	rt/Service/I	n:					
10.255			rt/Service/I	1000					
10.255	5.211.150	1/1	rt/Service/I	1000					
10.25 10.25 10.25	5.211.150 5.211.150	1/1 1/2	rt/Service/I	1000					
10.255 10.255 10.255 10.255	5.211.150 5.211.150 5.211.150	1/1 1/2 1/3	rt/Service/I	1000	Add>				
10.255 10.255 10.255 10.255 10.255 10.255	5.211.150 5.211.150 5.211.150 5.211.150	1/1 1/2 1/3 1/4	rt/Service/I	1000	- Add				
10.255 10.255 10.255 10.255 10.255 10.255 10.255	5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150	1/1 1/2 1/3 1/4 1/5	rt/ServiceЛ		Add>				
10.25 10.25 10.25 10.25 10.25 10.25 10.25 10.25 10.25	5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150	1/1 1/2 1/3 1/4 1/5 1/6	d/Service/I						
10.25 10.25 10.25 10.25 10.25 10.25 10.25 10.25 10.25 10.25 10.25 10.25	5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150	1/1 1/2 1/3 1/4 1/5 1/6 1/7	rt/Service/I			>			
10.25 10.25 10.25 10.25 10.25 10.25 10.25 10.25 10.25 10.25 10.25 10.25	5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150	1/1 1/2 1/3 1/4 1/5 1/6 1/7 1/8	rt/Service/I		<< Benn	>			
10.25 10.25 10.25 10.25 10.25 10.25 10.25 10.25 10.25 10.25 10.25 10.25 10.25	5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150	1/1 1/2 1/3 1/4 1/5 1/6 1/7 1/8 1/11	rt/Service/I		<< Benn	> ove >>			
10.25 10.25	5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150	1/1 1/2 1/3 1/4 1/5 1/6 1/7 1/8 1/11 1/12	rt/Service/I		<< Benn	> ove >>			
10.25 10	5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150	1/1 1/2 1/3 1/4 1/5 1/6 1/7 1/8 1/11 1/12 1/13	rt/Service/I		<< Benn	> ove >>			
10.25 10	5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150	1/1 1/2 1/3 1/4 1/5 1/6 1/7 1/8 1/11 1/12 1/13 1/14	rt/Service/		<< Benn	> ove >>			
efine rules Address, by network	5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150	1/1 1/2 1/3 1/4 1/5 1/6 1/7 1/8 1/11 1/12 1/13 1/14 1/15	d/Service/I		<< Benn	> ove >>			
10.25 10.25 </td <td>5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150</td> <td>1/1 1/2 1/3 1/4 1/5 1/6 1/7 1/8 1/11 1/12 1/13 1/14 1/15 1/16</td> <td>d/Service/</td> <td></td> <td><< Benn</td> <td>> ove >></td> <td></td> <td></td> <td></td>	5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150	1/1 1/2 1/3 1/4 1/5 1/6 1/7 1/8 1/11 1/12 1/13 1/14 1/15 1/16	d/Service/		<< Benn	> ove >>			
In 10,25 In 2,25 In	5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150 5.211.150	1/1 1/2 1/3 1/4 1/5 1/6 1/7 1/8 1/11 1/12 1/13 1/14 1/15 1/16 1/17			<< Benn	> ove >>			

VLAN Rules Tabs

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.

	Rules Confi	wration							
		100000 C	nuen la		-				
A	Protocol Port	Net Address MAC Ad		Custom	Binding DHCP Port	Summary	DHCP MAC Address		
Her	Protocol R						55 3 8 A III H		
		Name			Switch Addr	ess	Rule Value		
	Comnis	Partch		0.255.211			Protocol = IP E2		
	 ↓ wTarg 	et		0.255.211			Protocol = IP E2		
	lansw	tch		0.255.211			Protocol = IP E2		
	←0 186			0.255.211			Protocol = IP		
	BBH-	122	1	0.255.211	1/5		Protocol = IP E2		
e you can define rules oort, by MAC Address, by									
oort, by MAC Address, by tocol, and by network	1			1					
ort, by MAC Address, by	4			New	Delo	te			

Protocol Rules

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.

Name	Address	DNS Name	Type	
DCTestnetCore			087700	
Kite_59	10.255.11.59		056800-4	ni
w/Target	10.255.11.61		OS6800-2	
wTarget	10.255.11.63		OS6800-2	
kite2_97	10.255.11.97		086800-2	
Kite	10.255.11.112		OS6800-2	-
4				
	IP-SNAP IPX-Novell			
OIPX O	IPX-Novell Ethernet Type		600	
OIPX O	IPX-Novell		000) (05/	AP)
OIPX O	IPX-Novell Ethernet Type			



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 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.

	Protocol Net	Address D	HCP Cu	istom Bindir	g Sumr	nary	
P	Port	MAC Addr	ess	DHCP	Port	DHCP MAC	Address
	Name	Addr	ess	DNS Name	Type	Version	1
	OmniSwitch	10.255.21	1.69		OS6624	5.4.1.163.R01	
	w/Target	10.255.21	1.71		089700	6.1.1.632.R01	Select A
	lanswitch	10.255.21			087800	5.1.6.146.R02	Pencerra
	186	10.255.21			08-4024	4.5.2.59	Clear All
	BBH-H22	10.255.21	1.175		OS6648	5.1.6.138.R02	
	Available Ports:					Port Rules to be added	-
- II					2		
	Device	SlotPort/Se			1	Device Slot/Port/Ser	vice/Instance
	10.255.211.150	1/1					
	10.255.211.150	1/2					
	10.255.211.150 10.255.211.150	1/2 1/3					
	10.255.211.150 10.255.211.150 10.255.211.150	1/2 1/3 1/4			_		
	10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150	1/2 1/3 1/4 1/5		Add >	>		
	10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150	1/2 1/3 1/4 1/5 1/6	_				
	10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150	1/2 1/3 1/4 1/5 1/6 1/7		Add >			
	10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150	1/2 1/3 1/4 1/5 1/6 1/7 1/8		<< Benn	ove		
	10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150	1/2 1/3 1/4 1/5 1/6 1/7 1/8 1/11			ove		
	10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150	1/2 1/3 1/4 1/5 1/6 1/7 1/8 1/11 1/12		<< Benn	>>		
	10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150	1/2 1/3 1/4 1/5 1/6 1/7 1/8 1/11		<< Berni Add All	>>		
	10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150	1/2 1/3 1/4 1/5 1/6 1/7 1/8 1/11 1/12 1/13		<< Berni Add All	>>		
ress, by	10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150	1/2 1/3 1/4 1/5 1/6 1/7 1/8 1/7 1/8 1/7 1/8 1/1 1/12 1/13 1/14 1/15		<< Berni Add All	>>		
iress, by work	10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150 10.255.211.150	1/2 1/3 1/4 1/5 1/7 1/7 1/8 1/11 1/12 1/13 1/14		<< Berni Add All	>>		
tress, by work efine	$\begin{array}{c} 10.255,211.150\\ 10.255,211.150\\ 10.255,211.150\\ 10.255,211.150\\ 10.255,211.150\\ 10.255,211.150\\ 10.255,211.150\\ 10.255,211.150\\ 10.255,211.150\\ 10.255,211.150\\ 10.255,211.150\\ 10.255,211.150\\ 10.255,211.150\\ \end{array}$	1/2 1/3 1/4 1/5 1/6 1/7 1/8 1/7 1/8 1/7 1/8 1/7 1/1 1/12 1/13 1/14 1/15 1/16		<< Berni Add All	>>		
define rules C Address, by by network can define for a VLAN. A is included in	$\begin{array}{c} 10.255.211.150\\ 10.255.$	1/2 1/3 1/4 1/5 1/6 1/7 1/7 1/8 1/11 1/12 1/14 1/15 1/16 1/17 1/18		<< Berni Add All	>>		

Port Rules

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 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.

Rules Config	juration						
Protocol	Net Address	DHCP	Custom	Binding	Summary		
Port	MAC	Address		DHCP Port		DHCP MAC Address	
MAC Rules	1					20:20 😒 😂 🛃	
Kee A	Name			Switch Add	ress	Rule Value	
Co Omnis	witch		10.255.21	1.69		00005e:000101	
Comnis	witch		10.255.21	1.69		000bdb:87efd9	
Comnis	witch		10.255.21	1.69		000cf1:89f603	
- Omnis	witch		10.255.21	1,69		0010a4:e66d1e	
wTarg	et		10.255.21	1.71		00005e:000101	
4 wTarg			10.255.21	1.71		000bdb:87efd9	
↓ wTarg	et		10.255.21	1.71		000cf1:89f603	
A wTarg	et		10.255.21	1.71		0010a4;e66d1e	
4 lanswi	tch		10.255.21	1,150		00005e:000101	
40 lanswi	tch		10.255.21	1.150		000bdb:87efd9	
ianswi	tch.		10.255.21	1.150		000cf1.89f603	
4 lansw	tch		10.255.21	1.150		0010a4:e66d1e	
4 lanswi 4 186			10.255.21	1.155		00005e:000101	
← 186			10.255.21	1.155		000bdb:87efd9	
4o 186			10.255.21			000cf1:89f603	
186			10.255.21			0010a4:e66d1e	
46 BBH-H	22		10.255.21			00005e:000101	
BBH-H			10.255.21			000bdb:87efd9	
G BBH-H			10.255.21			000cf1:89f603	
les 6 BBH-H	22		10.255.21	1.175		0010a4:e66d1e	
ress, by							
ork			- H.,				
e							
I VLAN. A	-		> Nev	Dele	to		
xled in			Eles.	- Econ			
es any	-						
belong		11			11	1	

MAC Address Rules

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.

Select Devices for t	he MAC rules			
Name	Address	DNS Name	Type	Version
DCTestnetCore	10.255.10.3		087700	5.1.6.86.R02
Kite_59	10.255.11.59		056800-48	6.1.2.12.R02 =
w/Target	10.255.11.61	1	OS6800-24	6.1.2.16.R02
w.Target	10.255.11.63		OS6800-24	8.1.2.144.R01
kite2_97	10.255.11.97		OS6800-24	6.1.2.150.R01
💓 Kite	10.255.11.112		OS6800-24	8.1.2.144.R01
Enter MAC Address Single/Start:		cluded MAC A Single		End
	âdd			

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

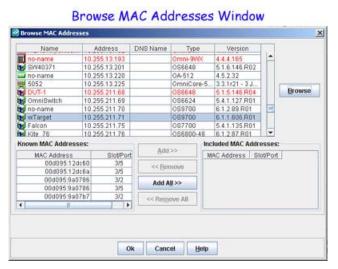
1. Select one or more devices from the list located in the top half of the Add MAC Rules window.

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.



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.

Protocol	Net A	ddress	DHCP	Cus	tom Bindir	g Sun	mary		
Port	T	MAC A	ddress		DHCP	Port	1	DHCP MAG	C Address
Na Na	me	1	Address		DNS Name	Type		Version	1
Omnis Omnis	Switch	10.255	5.211.69			OS6624	5.4	1.163.R01	
W wTarg	jet	10.255	5.211.71			059700	6.1	1.632.R01	Select Al
I lansw	itch	10.255	5.211.150			087800	5.1	6.146.R02	Desective
186		10.255	5.211.155			08-4024	4.5	2.59	Clear All
BBH-	H22	10.255	5.211.175			O\$6648	5.1	6.138.R02	
Available	Dorte:			_			Dort Bu	es to be adde	ut-
MAGINOPAG	L.01104						COLC128		
	Concerne .		1.00 C 10						
Devi			rt/Service/I	1000		1	Device		ervice/Instance
10.255.21	11.150	1/1	rt/Service/I	n:			Device		
10.255.21	11.150 11.150	1/1 1/2	rt/Service/I	1000			Device		
10.255.21 10.255.21 10.255.21	11.150 11.150 11.150	1/1 1/2 1/3	t/Service/I	1000			Device		
10.255.21 10.255.21 10.255.21 10.255.21	11.150 11.150 11.150 11.150	1/1 1/2 1/3 1/4	t/Service/I	1000			Device		
10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21	11.150 11.150 11.150 11.150 11.150 11.150	1/1 1/2 1/3 1/4 1/5	rt/Service/I		- Ådd >	<u> </u>	Device		
10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21	11.150 11.150 11.150 11.150 11.150 11.150 11.150	1/1 1/2 1/3 1/4 1/5 1/6	t/Service/I	1000			Device		
10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21	11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150	1/1 1/2 1/3 1/4 1/5 1/6 1/7	t/Service/I		Add >		Device		
10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21	11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150	1/1 1/2 1/3 1/4 1/5 1/6 1/7 1/8	t/Service/I		<< Benu	ove	Device		
10.265.21 10.265.21 10.265.21 10.265.21 10.265.21 10.265.21 10.265.21 10.265.21 10.265.21 10.265.21	11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150	1/1 1/2 1/3 1/4 1/5 1/6 1/7 1/8 1/11	t/Service/I			ove	Device		
10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21	11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150	1/1 1/2 1/3 1/4 1/5 1/6 1/7 1/8 1/1 1/1 1/12	t/Service/I		<< Berni Add All	ove >>	Device		
10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21	11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150	1/1 1/2 1/3 1/4 1/5 1/6 1/7 1/8 1/1 1/1 1/12 1/13	t/Service/I		<< Benu	ove >>	Device		
10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21	11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150	1/1 1/2 1/3 1/4 1/5 1/6 1/7 1/8 1/11 1/12 1/13 1/14	t/Service/		<< Berni Add All	ove >>	Device		
10.255.2 10.255	11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150	1/1 1/2 1/3 1/4 1/5 1/6 1/7 1/8 1/11 1/12 1/13 1/14 1/15	t/Service/I		<< Berni Add All	ove >>	Device		
10.255.21 10.255.21 <td< td=""><td>11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150</td><td>1/1 1/2 1/3 1/4 1/5 1/6 1/7 1/8 1/11 1/12 1/13 1/14 1/15 1/14 1/15</td><td>t/Service/I</td><td></td><td><< Berni Add All</td><td>ove >></td><td>Device</td><td></td><td></td></td<>	11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150	1/1 1/2 1/3 1/4 1/5 1/6 1/7 1/8 1/11 1/12 1/13 1/14 1/15 1/14 1/15	t/Service/I		<< Berni Add All	ove >>	Device		
10.255.2 10.255	11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150	1/1 1/2 1/3 1/4 1/5 1/6 1/7 1/8 1/11 1/12 1/13 1/14 1/15 1/14 1/15 1/16 1/17	t/Service/I		<< Berni Add All	ove >>	Device		
10.255.21 10.255.21	11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150 11.150	1/1 1/2 1/3 1/4 1/5 1/6 1/7 1/8 1/11 1/12 1/13 1/14 1/15 1/14 1/15			<< Berni Add All	ove >>	Device		

DHCP Port 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.

	Rules Config	2010/01/	-	1			
	Protocol	Net Address	DHCP	Custom	Binding	Summary	
	Port	MAC	Address	- P	DHCP Port		DHCP MAC Address
	Add DHCP	MAC Rules					10/10 😒 🕾 🖨 💹
		Name			Switch Add	ess	Rule Value
A DECK OF THE REAL PROPERTY OF	Comnis	witch		10.255.21	1.69		00005e:000101
	4 Omnis	witch		10.255.21	1.69		000bdb:87c2aa
	4X wTare	et		10.255.21	1.71		00005e:000101
	4 wTarg	et		10.255.21	1.71		000bdb:87c2aa
	46 lanswi	tch		10.255.21	1.150		00005e:000101
	40 lanswi	tch		10,255.21	1.150		000bdb:87c2aa
	40 186 40 186			10.255.21	1.155		00005e:000101
	186			10.255.21	1.155		000bdb:87c2aa
	BBH-H	22		10.255.21	1.175		00005e:000101
	BBH-H	22		10.255.21	1.175		000bdb:07c2aa
you can define rules 1, by MAC Address, by							
	4			П.			1

DHCP MAC 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.

Name	Address	DNS Name	Type	Version
lanswitch	10.255.211.150	Divis reame	OS7800	5 1 6 138 R02
Enter MAC Add	Iress	Included MAC A	ddresses	
Single/Start:	1	Single	e/Start	End
End:	:			
	Add			

Add DHCP MAC Rules Window

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.

Name	A	ddress	DNS Name	Тур	e	Version	_	1
no-name	10.25	55.13.193		Omni-9V	VOC -	4.4.4.165	-	
SW40371	10.25	55.13.201		OS6648		5.1.6.146.R0	2	
no-name	10.25	55.13.220		0A-512		4.5.2.32		
5052	10.25	55 13 225		OmniCo	re-5	3.3.1r21 - 3 J		
DUT-1	10.25	55.211.68		OS6648		51.5146.R0	4	Browse
OmniSwitch	10.25	55.211.69		086624		5.4.1.127.R0	1	
no-name	10.25	55 211.70		0\$9700		6.1.2.89.R01		e .
w Target	10.25	55.211.71		059700		6.1.1.606.R0	1	
Falcon	10.25	55.211.75		087700	S.,	5.4.1.135.R0	1	
Kite 76	10.25	55.211.76		038800	48	6.1.2.87.R01		-
Known MAC Address	es:		1	10.00	Inc	luded MAC Ad	dress	es:
MAC Address	1	SlotPor	1 80	d>>	M	AC Address	SlotP	ort
00d095:12d	c60	3/5	a states	510221 C				2012-1
00d095.12d	c6a	3/5	<< H0	90000				
00d095:9a0	786	3/2						
00d095:9a0	786	3/5	A00	Ali >>				
00d095:9a0	7b7	3/2	ec Bon	In mon				
•	_	RAD	- neg	Robert best				
00d095:9a0			<< Ren	nove All				



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.

	Rules Config	200101000	_	-					
	Protocol	Net Addre	SS	DHCP	Custom	Binding	Summary	1. 	
	Port	M	AC Ad	Idress	and the second	DHCP Por	r	DHCP MAC Add	ress
	Network R	tules						55 🔂 👘	6
PER S	Na	me	Swite	h Addre	SS		Rule Valu	8	Rule St
(and)	Comnis	Switch 1	0.255	211.69	IP = 1	0.255.16.173	, Mask = 255		Enabled
	46 w/Targ	et 1	0.255.	211.71	IP = 1	0.255.16.172	2, Mask= 255	0.0.0	Enabled
	 Ianswi 	itch 1	0.255	211.150	IP = 1	0.255.16.173	2, Mask = 255	0.0.0	Enabled
	40 186	1	0.255.	211.155	Protoc	ol = IP, IP =	10.255.16.17	2, Mask= 255.0.0.0	Enabled
	A BBH-H	122 1	0.255.	211.175	IP = 1	0.255.16.171	2, Mask = 255	0.0.0	Enabled
re you can define rules port, by MAC Address, by									
port, by MAC Address, by stocol, and by network	1					8			
port, by MAC Address, by	4				Net		oto :		

Network Address Rules

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.

Select D	evices for t	he Network rules				
N	ame	Address	DNS Name	Type	Version	Γ
Kite_59		10.255.11.59		OS6800-48	6.1.2.88.R01	ŀ
Kite_60		10.255.11.60		0\$6800-48	6.1.2.37.R01	Ŀ
vxTarg	et	10.255.11.61		OS6800-24	6.1.2.82.R01	L
w.Targ	let	10.255.11.63		086800-24	6.1.2.81.R01	
🛿 falcon		10.255.11.100		087700	5.1.6.393.R01	L
Kite_F	iber_U24	10.255.11.101		OS6800-U24	5.3.1.181.R02	ŀ
IP	IP Address Subnet Ma	ask				
⊖ IPX	Network N	lumber		11		

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.

	Rules Confi	guration					
	Protocol	Net Address	DHCP	Custom	Binding	Summary	
A	Port	MAC A	ddress		DHCP Port	r	DHCP MAC Address
	DHCP Rule						44 3 8 6 1
		Name			Switch A	ddress	Rule Value
	Comnis	Bwitch		10.255.	211.69		Generic
6 VN	46 w/Targ			10.255.3	211.71		Generic
	Iansw	itch		10.255.	211.150		Generic
	+o BBH-H	122		10.255.3	211.175		Generic
you can define rules rt, by MAC Address, by coll and by network				11			
	4			New	N Dele	to	

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.

Name	Address	DNS Name	Type	Version
lanswitch	10.255 211 150	Dire reality	087800	5.1.6.138 R02

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.

	Rules Confi	guration						
	Protocol	Net Address	DHCP	Custom	Binding	Summary		
A	Port	MAC	Address	1	DHCP Por	and the second se	DHCP MAC Add	ress
	Custom R	ules					55 😪 📚	6
	Na	ime S	witch Addre	ss		Rule Value	and the second sec	Rule S
	Comnis		55.211.69		t= 0, Value =		Mask = 0x110000	Enabled
	40 w/Targ		55.211.71	Offse	t= 0, Value =	0x60020000,	Mask = 0x110000	Enabled
	4 lansw	itch 10.3	55.211.150	Offse	t = 0, Value =	0x60020000,	Mask = 0xff0000	Enabled
	← 186		55.211.155	5 Offse	t= 0, Value =	0x60020000.	Mask = 0x110000	Enabled
	40 BBH-H	122 10.1	55.211.175	5 Offse	t= 0, Value =	: 0x60020000.	Mask = 0x110000	Enabled
e you can define rules not by MAC Address by								
oort, by MAC Address, by tocol, and by network	4							Þ
oort, by MAC Address, by	4				11	uto		

Custom Rules

Click the New button to display the Add Custom Rules window, shown below.

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.

Add Custor	n Rules		2
Select Devic	s for the Custom i	rules	
Name Name	Address 10.255.211.150	DNS Name	Type OS7800
4			•
۲ ffset:	1	÷.	•
1		1 1	•

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.

	Rules Configuration	1			
	Protocol Net A	ddress DHCP C	ustom Binding Summ	narv	
AA	Port	MAC Address	DHCP Port	DHCP MAC Add	ress
	Binding Rules			55 3 8	6
E RENT	Name	Switch Address	Rule	Value	Rule Sta
	ComniSwitch	10.255.211.69	MAC = 000393:111b60, IP		Enabled
	46 w/Target	10.255.211.71	MAC = 000393:111860, IP		Enabled
	A lanswitch	10 255 211 150	MAC = 000393:111b60, IP :		Enabled
	40 186	10.255.211.155	MAC-IP - MAC = 000393:11		Enabled
	BBH-H22	10.255.211.175	MAC = 000393:111b60, IP :	= 10.255.18.132	Enabled
re vou can define rules					
port, by MAC Address, by tocol, and by network	4				
Iress. You can define Itiple rules for a VLAN. A t or device is included in LAN if it matches any			New Delete		
e rule. Ports can belong					

Binding Rules

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:

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.

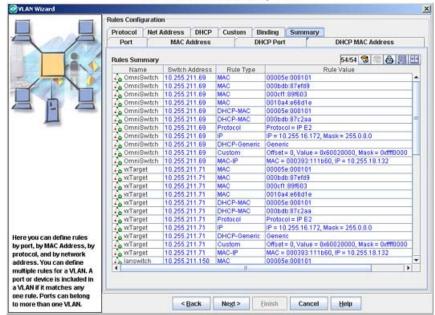
Removing a Binding Rule

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

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).

	VLAN Wizard Summary Pa	ge				
	VLAN Description					
	Id :	Id : 158		Description :		VLAN 158
111	Admin Status :	Enabled	d	Mode :		Standard
- 6 -	Spanning tree :	Enabled	d	Mobility :		Enabled
	Authentication :	Disable	ed	Router Protocol		IP
	ROUTING			1		<u> </u>
	ROUTING Switch		IP Rout	ing	IPX	Routing
			IP Rout Enabled,			Routing led, 4001690d
	Switch	75)	Enabled,			led, 4001690d
	Switch 186 (10.255.211.155)		Enabled,	, 0.0.0.0	Enab	led, 4001690d bled
	Switch 186 (10.255.211.155) BBH-H22 (10.255.211.1	50)	Enabled, 5.5.5.1, 5.5.5.16	, 0.0.0.0 Engineering	Enab Disal	led, 4001690d bled bled
	Switch 186 (10.255.211.155) BBH-H22 (10.255.211.1 lanswitch (10.255.211.1	50) 1.69)	Enabled, 5.5.5.1, 5.5.5.16	, 0.0.0.0 Engineering , Accounting , Tech Pubs	Enab Disal Disal	led, 4001690d bled bled bled
tis is a summary of all AN configuration	Switch 186 (10.255.211.155) BBH-H22 (10.255.211.1 Ianswitch (10.255.211.1 OmniSwitch (10.255.21	50) 1.69)	Enabled, 5.5.5.1, 5.5.5.16 5.5.5.23	, 0.0.0.0 Engineering , Accounting , Tech Pubs	Enab Disal Disal Disal	led, 4001690d bled bled bled

Multiple Virtual Routing and Forwarding

The Multiple Virtual Routing and Forwarding (VRF) feature allows the user to configure separate routing instances on the same switch. Similar to using VLANs to segment Layer 2 traffic, VRF instances are used to segment Layer 3 traffic. Each VRF instance is in essence a virtual LAN for Layer 3 traffic. Some of the benefits of using the Multiple VRF feature include:

- Multiple routing instances within the same physical switch. Each VRF instance is associated with a set of IP interfaces and creates and maintains independent routing tables. Traffic between IP interfaces is only routed and forwarded to those interfaces that belong to the same VRF instance.
- Multiple instances of IP routing protocols, such as static, RIP, IPv4, BGPv4, and OSPFv2 on the same physical switch. An instance of each type of protocol may operate within one or more VRF instances.
- The ability to use duplicate IP addresses across VRF instances. Each VRF instance maintains its own IP address space to avoid any conflict with the service provider network or other customer networks.
- Separate IP routing domains for customer networks. VRF instances configured on the Provider Edge (PE) are used to isolate and carry customer traffic through the shared provider network.

This implementation of VRF functionality does not require a BGP/MPLS configuration in the provider network. Instead, VRF instances can route and forward IP traffic between customer sites using point-to-point Layer 3 protocols, such as IP-IP or GRE tunneling.

Note: The Multiple VRF feature is only available on 9000E Series Switches, Release AOS 6.4.1. SNMPv3 is required to manage VRF instances; SNMPv1 and v2 are not supported. If OmniVista finds Multiple VRFs configured on a device using SNMPv2 during Discovery polling, OmniVista warns the user about presence of Multiple VRFs in the Status Panel and logs the message.

Configuring the Multiple VRF Feature

VRF instances are created using the Command Line Interface (CLI) or WebView application. Configuring the Multiple VRF feature consists of creating a VRF instance, assigning one or more IP interfaces to the instance, and configuring routing protocols to operate within a specific instance.

The initial configuration of an Alcatel-Lucent switch consists of a default VRF instance, which is always active when the switch starts up and is not removable from the switch configuration. Any subsequent configuration of switch applications applies only to the default instance. To provide multiple, independent IP routing domains on the same switch, configuring additional VRF instances is required.

Creating a VRF Instance Using the CLI

Use the CLI **vrf** command to create a VRF instance. A VRF instance is identified by a name, which is specified at the time the instance is configured. For example, the following command creates the IpOne instance:

-> vrf IpOne

Use the **vrf** command to configure additional instances on the switch. Once you configure VRF instances, they will appear in the VRF ID drop-down field on the **View/New IP Router** Panels.

Note: See the "Configuring Multiple VRF" Chapter in the *OmniSwitch AOS Release 6 Network Configuration Guide* for detailed instructions on configuring VRF instances.

Creating a VRF Instance Using the WebView Application

Go to **Networking - IP - VRF** to bring up the Virtual Routing and Forwarding Instances Table. Use this page to create a new VRF instance or select an existing instance for configuration.

G Back • 🤅) - 💌	2 🏠	Search	Favor	tes 🚱 🔓	- 💆 🖾 -	4		
Address 🙆 http:			nt/login.html						💌 🏓 G
Alcatel·Lucent	0				đ	Fuji2 (10.255.11.1	01) Onlines I. Sava	Continuation I	
Physical	VRF: defau	IT IP UDI	P TCP IC	MP ARP	VRRPVRRP2	RIP.RIPV2 OSPF		oution 1515	the second processing the second
Layer 2									
Networking	Made			-					
\$ >	virtu	al Routi	ng and	Forwa	rding Ins	ances			
IP Do	101	index V	name	S					
	Г	0	default	SI					
Pv6	E	1	1						
	Г	2	2						
07	E	3	3						
IP Multicest	F	4	4						
8-8	Г	5	5						
UDP Relay	E	6	6						
	Г	7	7						
U	E	8	8						
Services	Г	9	9						
	E	10	10						
	(ifail								
Policy	Add	Se	lect	Delete	Retresh	Help			
	1000000	-	-			-			

Note: See WebView Help for detailed instructions on configuring VRF instances using the WebView application.