Getting Started with VLANs

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

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

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

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

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

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

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

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

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

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

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

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

VL.	AN Discovery	Warning Message
Warning	¥	X
	The following devices do no 10.255.11.152	t have VLAN discovery information!
	Discover Devices	Cancel

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

Using the VLANs Tree

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

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

mniVista 2500 - Applicat	ion: VLANs Window:0							
Applications View H		B	VLANs	-				
Enterprise Network	Virtual VLAN Table						294/294 🕱 🗟 🛃	
VLANS VLAN 1(#1) S@ VLAN 1(#1) S@ VLAN 2(#2) VLAN 3(#3)	VLAN ID Descript 1 VLAN 1 2 VLAN 2 3 VLAN 3	lion	Admin Status Enabled Enabled Enabled	Oper Inactiv Inactiv Inactiv	Status e e e	Type Standard Standard Standard	Spanning Tree Status Enabled Enabled Fnabled	Mobil Enable Enable Enable
See VLAN 4(#4) See VLAN 5(#5) VLAN 6(#6) VLAN 6(#6)	View VLAN Definition				Admir	n Status:	Enabled	-
DEAD(#8) Quarantined(; VLAN 10(#10) VLAN 11(#11)	Oper Status: Spanning Tree Status:	Active	nd	V Type		ity:	Standard Enabled	*
Set VLAN 12(#12) Set VLAN 13(#13) VLAN 14(#14) VLAN 14(#14)	Authentication: Voice Status:	Disab Disab	ed ed		Route	r-Protocol:	рдрх	*
• SVLAN 16(#16)	New		Edit Upda	te	Delete	e <u>A</u> p	ply <u>H</u> elp	
						Clic	k Apply to write prmation to the s	erver
					Sel to d	lect a Vi delete d	LAN and click De VLAN.	lete
			Cli To	ick U ible w	pdate /ith t	e to upd he lates	late the VLAN st poll information	n.
			Select a Vi to modify a	LAN an ex	and c isting	lick Edi VLAN.	1	
	CI	ick N	ew to creat	te a r	ew V	LAN.		

Click on VLANs to display a list of existing VLANs on the network.

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

Using the Devices Tree

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

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



Pop-Up Menu Functionality

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



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

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

Displaying the VLAN Configuration for a Device

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

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

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

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

Color Coding

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

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

The VLANs Application Toolbar

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



Assigning Ports to VLANs

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

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

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

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

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

niVista 2500 - Annlin	ation: VI ANs Window	u-O			
Annlications View	Holm	*10			
whhicanoi s Aica	neig				
	🔹 🙆 🐉 🖄	💼 🚉 🖙 Ports	-		
nterprise Network	ADE YOE	mmiCtack			
Browse	AUS AUS (AUNISCICK			
VLANs	Ports for (VLAN 2	(#2))		204/204	
10 VLAN 1(#1)	Name	Device	SlotPort	Port Type	Port State
W VLAN 2(#2)	vxTarget_xyz	10.255.11.219	2/13	Default Config	Forwarding
Divices	vxTarget_xyz	10.255.11.219	2/14	Default Config	Inactive
e Brons	vxTarget_xyz	10.255.11.219	2/15	Default Config	Inactive
spanning	vxTarget_xyz	10.255.11.219	2/16	Default Config	Inactive
ede IP Router	vxTarget_xyz	10.255.11.219	2/17	Default Config	Forwarding
ede IPX Route	vxTarget_xyz	10.255.11.219	2/18	Default Config	Inactive
- Kules	vxTarget_xyz	10.255.11.219	2/19	Default Config	Inactive
VLAN 3(#3)	vxTarget_xyz	10.255.11.219	2/20	Default Config	Inactive
20 VLAN 4(#4)	vxTarget_xyz	10.255.11.219	2/21	Default Config	Forwarding
20 VLAN 5(#5)	vxTarget_xvz	10.255.11.219	2/22	Default Config	Inactive
20 VLAN 6(#6)	vxTarget_xyz	10.255.11.219	2/23	Default Config	Inactive
WilanOperation	wTarget wz	10 255 11 219	2/24	Default Config	Inactive

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.

Click on 8	J2.1Q to display a list of 802.1Q tagged VLAN ports. 802.1Q Tagged VLAN Port Assignments
🖉 OmniVista 2500 - Application: VLAN	s Window:0
Elle Applications View Help	
	802.1Q 🔽
Enterprise Network Browse VLANs VLAN 1(#1) Devices VEPorts 802.10 R02.10 Link Agg	AOS XOS 802.1Q Ports for - VLAN 1(#1) Name Device Slot Port Description Force Tag Internal
Spanning Tree Bridge Port Prouter IP Router Rules VLAN 2(#2) VLAN 3(#3) VLAN 4(#4) VLAN 4(#4)	View 802.10 VLAN Port 802.10 Ports Parameters Device: 10.255.11.59 Slot: Port: Description: Force-Tag-Internal: off
	New Edit Update Delete Apply Help

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.

o Applications View	ition: VLAN	s Window:0			
	e 🔕	19	802.1Q Link Ag	g 🕶	
Enterprise Network Browse VLANs	4	AOS 802.1Q Link Agg	for VLAN - VLAN 1(#1)		11 3 8 8 3 3
6 802.1 0 802.1 0 802.1 0 Lin	k Agg				
IP Router IPX Router Rules VLAN 2(#2)		- View 802.1Q Li	nk Agg		

Configuring Spanning Tree Parameters

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

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

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

	Click o Tree i	on Spanning Tre information for	ee to displa each VLAN — VLAN	y Spanning I device. Spanning T	ree In	formation			7
	🖉 OmniVista 2500 - Application	VLANs Window:0						_10	1×
	Eile Applications view Help								
Expand Spanning		0 \$940	🖻 Spann	ing Tree 🔻				3	3
Dridee on Dent	Browse 🔺	Spanning Tree List Vi	ew for - VLAN 1(#1)			84.84 🐯	889	Ŧ
Bridge or Fort	🕈 🧒 VLANS 🔤	Name	Address	Protocol	Priority	Maximum Age	Hello Time	Forward Dela	
to configure	9-20 VLAN 1(#1)	demo6850	10.1.1.43	RSTP(802.1W)	32768	20	2	15	-
Spanning Tree	Devices	Kite_59	10.255.11.59	RSTP(802.1W)	32768	20	2	15	
parameters	Ports	w/Target	10.255.11.60	RSTP(802.1W)	32768	20	2	15	
paramororo.	P St Spanning Tree	Kite2_NMS	10.255.11.61	RSTP(802.1W)	32768	20	2	15	
	Bridge	vxTarget	10.255.11.63	RSTP(802.1W)	32768	20	2	15	
	Port	kite2_97_1	10.255.11.97	RSTP(802.1W)	32768	20	2	15	
	ede IP Rouber	falconCmm	10.255.11.100	STP(802.1D)	32768	20	2	15	
	ady IPX Router	Kite_Fiber_U24	10.255.11.101	STP(802.1D)	32768	20	2	15	
	Rules	NMS_HAWK_102_1	10.255.11.102	STP(802.1D)	32768	20	2	15	
	- 30 VLAN 2(#2)	vxTarget	10.255.11.104	STP(802.1D)	32768	20	2	15	
	- 30 VLAN 3(#3)	vxTarget	10.255.11.109	RSTP(802.1W)	32768	20	2	15	
	- 30 VLAN 4(#4)	vxTarget	10.255.11.111	STP(802.1D)	32768	20	2	15	
	- 30 VLAN 5(#5)	Kite	10.255.11.112	RSTP(802.1W)	32768	20	2	15	
	- 30 VLAN 6(#6)	no-name	10.255.11.121	RSTP(802.1W)	32768	20	2	15	
	C an operations re	WV_HAWK_122-Test	10.255.11.122	STP(802.1D)	32768	20	2	15	
	DEAD(#0)	NMS_123_Hawk_1	10.255.11.123	STP(802.1D)	32768	20	2	15	
	Guaranthed(#9)	WV_FUUI1_126x	10.255.11.126	RSTP(802.1W)	32768	8	5	15	
		BS0001s-to	10.255.11.127	STP(802.1D)	32768	20	2	15	
		VW_FUUI2_129	10.255.11.129	RSTP(802.1W)	32768	8	5	15	
	1/(ap.12/#12)	ES0001A-1	10.255.11.130	STP(802.1D)	32768	20	2	15	-
	← 10 VLAN 14(#14) ← 10 VLAN 15(#15) ▼			He	lp			•	

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



Configuring VLAN Router Interfaces

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

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

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

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

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

			— IP Route	r Interface De	efinitions—	
	🛃 OmniVista 2500 - Application: VLA	is Window:0				
	File Applications View Help					
		10 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	IP Router	•		
	Browse	AOS XOS			nama 🖨	
ick on IP Router	0- \$ VLAN 1(#1)	IP Routing for - VLAN	1(#1)		00/00	
configure on TD	Devices	Name	Device	Router IP Address	Router IP Mask	IP Encapsulation
configure an IP	- E Ports	Kite2_NMS	10.255.11.61	10.255.11.61	255.255.255.0	Ethernet 2
uter Interface	Spanning Tree	kite2_97_1	10.255.11.97	10.255.11.97	255.255.255.0	Ethernet 2
the VLAN	IP Router	falconCmm	10.255.11.100	10.255.11.100	255.255.255.0	Ethernet 2
	- AL IPX Router	Kite_Fiber_U24	10.255.11.101	10.255.11.101	255.255.255.0	Ethernet 2
	- W Rules	NMS_HAWK_102_1	10.255.11.102	10.255.11.102	255.255.255.0	Ethernet 2
	- Se VI AN 2(#2)	vxTarget	10.255.11.104	10.255.11.104	255.255.255.0	Ethernet 2
	VLAN 3(#3)	vxTarget	10.255.11.109	10.255.11.109	255.255.255.0	Ethernet 2
	- 50 VI AN 4(#4)	vxTarget	10.255.11.111	10.255.11.111	255.255.255.0	Ethernet 2
	- 50 VLAN 5(#5)	Kite	10.255.11.112	10.255.11.112	255.255.255.0	Ethernet 2
	- Se VLAN 6(#6)	no-name	10.255.11.121	10.255.11.121	255.255.255.0	Ethernet 2
	- St VianOperationsTest/#	NMS_123_Hawk_1	10.255.11.123	10.255.11.123	255.255.255.0	Ethernet 2
	- SH DEAD(#8)	BS0001s-to	10.255.11.127	10.255.11.127	255.255.255.0	Ethernet 2
	> Se Quarantined(#9)	4	1			•
		View IP Router Set IP Virtual Routi Device: Router IP Address: IP Encapsulation: <u>N</u> ew	ng Parameters 10.255.211.24 Ethernet 2	Router II P Forwa Update Delete	P Mask: arding: Enabled	Feb

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

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

	Г	IPX Router Interface Definitions
	OmniVista 2500 - Application: V. Elle Applications View Help	ANs Window:0
Click on IPX Router to configure an IPX Router Interface for the VI AN		IPX Router IPX Router AOS XOS IPX Routing for - VLAN 1(#1) 1/1 3 2 3 3 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
TOP THE VLAIN.		View IPX Router Set IPX Virtual Routing Parameters Device: 10.255.11.119 Protocot: PX RIP Only Frame-Type: Ethermet 2 New Edit Update Delete Apply Help

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 nonmobile distinction and there is no overall switch setting to invoke the mobile port feature. As a result, you can define rules to capture mobile port traffic on any VLAN. Click here for more information about configuring mobility on AOS devices.

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

				- VLA	N Rule Definitions		
	🖉 OmniVista 250) - Application:	LANs Window:)				
	File Applications View Help	o 500	1 🛎 🖻	Rules	•		4
	Browse VLANs	Rules (VLAN 1(#1))		31/31	3 - A	
	- 🞾 VLAN 1(#1)	Name	Switch Addre	Rule Type	Rule Value	Rule State	
	Devices	OSR-5slot	10.255.11.153	Port	2/1/Bridge/1	Disabled	-
	Pots	OSR-5slot	10.255.11.153	MAC	aabbcc:ddee11	Enabled	
	🗢 💥 Spanning Tree	VLAN-OS6648	10.255.11.181	MAC	00aabb:123456	Enabled	
	+4+ IP Router	VLAN-OS6648	10.255.11.181	MAC	UUaacc:123456	Enabled	
mand Didan	+ IPX Router	VLAN-OS6648	10.255.11.181	MAC	00b0d0:193c68	Enabled	
xpana kules -	P? M Rules	VLAN-OS6648	10.255.11.181	MAC	00b0d0:428259	Enabled	
n the tree to	- Protocol	VLAN-OS6648	10.255.11.181	DHCP-MAC	00aabb:123456	Enabled	
elect a Rule	- Port	VLAN-OS6648	10.255.11.181	DHCP-MAC	000800123456	Enabled	
the	MAC	VLAN-US6648	10.255.11.181	DHCP-MAC	000000193068	Enabled	
ype.	NetAddres	VLAN-US6648	10.255.11.181	DHCP-MAC	4/22	Enabled	
	Custom	VLAR-Parcon	10.255.11.100	Port	1/23	Enabled	
	DHOP	vxTarget_xyz	10.255.11.218	Port	2/1	Enabled	П
	DHCP Pon	wTarget_xyz	10.255.11.218	Port	2/2	Enabled	
	Disding	wTarget_wz	10.255.11.218	Port	2/3	Enabled	
	Sinding	wTarget_wg	10.255.11.218	IP	IP = 2.0.0.0 Mark = 256.0.0.0	Enabled	
		wTarget wz	10 255 11 219	IPX	IPY = 1431651653 Encanculation = n	Enabled	
		FALCON-137	10 255 11 221	IP	IP = 10 255 11 0 Mack = 255 255 255 0	Enabled	
	- Se VI AN 5(#5)	FalconCmm	10 255 11 243	MAC	00b0d0:193c68	Enabled	-
			L	lpdate	Delete Apply Help		

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

Using Port Mobility

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

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

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

Using the Browse Option

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

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

Selecting the VLAN Information Type

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

OmniVista 2500 - Applicatio File Applications View Hel	on: VLANs Window:0		
		Browse	a
Contemprise Network	AN Information Type VLAN All Rules Protocol Rules MAC Rules Custom Rules DHCP Port Rules Binding Rules Kite: Sec.internation: Sec.inte	 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.

	@ 🙆 🧕 😹 🅬 🍓 🧕		Browse	-	1
Enterprise Network	Available Devices	_		Selected Devices	
Frowse Browse	ATHIN	-			
VLANS	Namo			Nome	
Devices	240-ost-mnx10			Indiffe	
	AOS Hawk 157 alias				
	DCTestnetCore				
	Fuji9600 202		Add >>		
	Hawk151				
	Hawk197	171	<< Bemove		
	HAWK_118	1			
	HAWK_131		Add All >>		
	HAWK_153				
	Kite2_NMS		<< Remove All		
	NMS_HAWK_102				
	MMS_HAWK_102				
	📷 no-name				
	📕 no-name				
	no-name	-			(a
				•	

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.

Tarrent Concert Streets (1997		Browse	£	-		04
Enterprise Network	Search Results: Protoc VLAN Rules	ol Rules		4.4		
Devices	Name	Switch Address	VLAN ID	Rule Type	Rule Value	R
	NMS_HAWK_102	10.255.11.102	1	Protocol	Protocol = ipE2	En
	HAWK_153	10.255.11.153	1	Protocol	Protocol = ipE2	En
	AOS_Hawk_157_alias	10.255.11.157	21	Protocol	Protocol = ipE2	En
	OmniSwitch_198_xyz	10.255.11.198	1	Protocol	Protocol = ipE2	En
	2011					

Search Results

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

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

Configuring VLANs

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

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

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

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

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

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

	[- VLA	N Tat	ole -			
OmniVista 2500 - Applica	tion: VLANs Window:0							
le Applications <u>View</u> H	leip							
	0 🗿 🐉 🛛 🏜 😫	🥩 VLAN:	5	-				3
Enterprise Network	Virtual VI AN Table						294/294 3 3 4	
Browse VLANs VLANs VLAN 1(#1) VLAN 2(#2) VLAN 2(#2)	VLAN ID Descript 1 VLAN 1 2 VLAN 2 3 VLAN 3	ion Adm Enab Enab	in Status led led led	Oper Inactive Inactive	Status 9 9	Type Standard Standard Standard	Spanning Tree Status Enabled Enabled Enabled	Mobil Enable Enable
 VLAN 3(#3) VLAN 4(#4) 	1		and a		n	- naunatu.	11 11050110	•
 Set VLAN 5(#5) VLAN 6(#6) VLAN 6(#6) VLAN 6(#6) VLAN 10(#10) VLAN 10(#10) VLAN 10(#11) VLAN 11(#11) VLAN 12(#12) VLAN 13(#13) VLAN 13(#13) VLAN 15(#15) VLAN 18(#16) 	View VLAN Definition – Description: Oper Status: Spanning Tree Status: Authentication: Voice Status:	Activo Enabled Disabled Disabled	Upda		Admir Type: Mobili Route	ty:	Enabled Standard Enabled P/IPX	Y Y Y
	TEN	Eau				Clic	k Apply to write prmation to the s	erver.
					Sel to a	ect a VI delete a	AN and click De	lete
			Cli	ck Uj ible w	date	to upd he lates	ate the VLAN t poll information	n.
		Sele to n	ect a Vi nodify	LAN o	and c isting	lick Edi VLAN.		
	c	ick New 1	o crea	te a n	ew V	LAN.		

Click on VLANs to display a list of existing VLANs on the network.

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

Adding a VLAN

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

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

Copying a VLAN

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

Note: The following definitions will not be copied:

1. IP/IPX routing parameters.

2. VLAN features that are not supported on the target devices. For example, in OS 6800, the Mobility rules like Custom Rules, IP-MAC Binding Rules, IP-Port Binding Rules, and MAC-Port-Protocol are not supported.

3. The VLAN 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. See VLAN Parameter Definitions below for more information. Follow the steps below to modify VLAN parameter values.

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

	1		VLA	Ns	•				
VLANS 4	Virtual VI	LAN Table					295	5/295 🔞 🏾 🔠	
50 VLAN 2(#2)	VLAN ID	Descriptio	n	Admin Status	Oper S	Status Type	Sp	anning Tree Status	Mobilit
🝰 VLAN 3(#3)	-1	VLAN 1		Enabled	Inactiv	e Standar	d En	abled	Enabled
20 VLAN 4(#4)	2	VLAN 2		Enabled	Inactiv	e Standar	dEn	abled	Enabled
20 VLAN 5(#5)	3	VLAN 3		Enabled	Inactiv	e Standar	d En	abled	Enabled
20 VLAN 6(#6)	4	VLAN 4		Enabled	Inactiv	e Standar	d En	labled	Enabled
• 🞾 VlanOperationsTest(5	VLAN 5		Enabled	Inactiv	e Standar	dEn	labled	Enabled
20 DEAD(#8)	6	VLAN 6		Enabled	Inactiv	e Standar	d En	labled	Enabled
Quarantined(#9)	7	VlanOperation:	sTest	Disabled	Inactiv	e Standar	dEn	abled	Enabled
29 VLAN 10(#10)	8	DEAD		Enabled	Inactiv	e Standar	d En	abled	Enabled
20 VLAN 11(#11)	9	Quarantined		Disabled	Inactiv	e Standar	dEn	abled	Enabled
20 VLAN 12(#12)	10	VLAN 10		Enabled	Inactiv	e Standar	dEn	abled	Enabled
10 Vlan 13(≠13)	4			- Non-)
- 200 VLAN 14(#14) - 200 VLAN 15(#15)	Edit VL	AN Definition							
VLAN 16(#16)	Descrip	tion:	VLA	N 1		Admin Statu	is:	Enabled	-
VLAN 20(#20)	Oper St	atus:	in an	tion		Туре:		Standacit:	-
99 VLAN 21(#21) 99 VLAN 22(#22)	Spannin	ng Tree Status:	Ena	bled	-	Mobility:		Enabled	-
VLAN 23(#23)	Authent	ication:	Disa	abled	-	Router-Prote	ocol;	None	-
daklosk(#25)	Voice St	tatus:	Dist	blod	-				

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.

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.

Click on	Devid	ces to display a list	of VLAN swit	tches.			
	_		- VLAN De	vice Inform	ation —		
🙋 Omni¥ista 2500 - Applicatio	on: VL/	ANs Window:0				<u>_</u>	П×
File Applications View Hel	p						_
	٥	10 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Devices	-			5
Enterprise Network		Devices for - VLAN 1(#	1)		43/43 🔞	8 8 H H	<u></u>
- A VI ANIC		Name	Address	DNS Name	Туре	Version	
		😥 DCTestnetCore	10.255.10.3		OS9600	6.1.1.152.R02	-
Devices		💓 NMS_HAWK_102	10.255.11.102		OS6624	5.1.6.32.R03	
- Ports		💓 Kite(6800)_104	10.255.11.104		OS6800-48	6.1.2.105.R03	
Spanning Tree		💓 no-name	10.255.11.111		OS9700	6.1.1.105.R02	
- J. IP Router		🗑 HAWK_113	10.255.11.113		OS6648	5.1.6.200.R02	
- I IPY Pouter		🗑 HAWK_114	10.255.11.114		OS6648	5.1.6.200.R02	
> N Pulse		🗑 HAWK_115	10.255.11.115		OS6648	5.1.6.200.R02	
		🗑 HAWK_116	10.255.11.118		OS6648	5.1.6.200.R02	
		🗑 HAWK_117	10.255.11.117		OS6648	5.1.6.200.R02	
		🗑 HAWK_118	10.255.11.118		OS6648	5.1.6.200.R02	
		🔳 no-name	10.255.11.119		OmniS/R-5	4.5.2	
		🔟 no-name	10.255.11.120		OmniS/R-3	4.5.2	
		🞲 vxTarget	10.255.11.121		OS9700	6.1.1.148.R02	
		III NMS_125	10.255.11.125		OS6300-24	2.2.0.13	
		🗑 no-name	10.255.11.126		OS9700	6.1.1.142.R02	
		NMS_Fuji_127	10.255.11.127		OS7800	5.1.6.212.R02	
200 VLAN 17(#17)	1311	NMS 9800 Fuji	10.255.11.128		OS9800	6.1.3.311.R01	-
		1					
VLAN 21(#21)	3						
₩ 200 VLAN 23(#23)	- 31			Holp			
• 200 VLAN 27(#27)	-			ūeih			
	~~~~~	~~~~~	~~~~~		~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~~~~~	www.

## **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. Click here for information about dynamically assigning ports to VLANs.

# Configuring a New Default VLAN for a Port

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

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

	ation: VLANs Window	e0				-1
Applications View	Help					
		🛔 👲 😅 Ports	-			
Enterprise Network	AOS XOS C	mniStack				
VLANS	Ports for (VLAN 2	(#2))		204/204	388.	Te
VLAN 2(#2)	Name	Device	Slot/Port	Port Type	Port State	4
- D vices	vxTarget_xyz	10.255.11.219	2/13	Default Config	Forwarding	-
- C Ports	vxTarget_xyz	10.255.11.219	2/14	Default Config	Inactive	-
- Spanning	vxTarget_xyz	10.255.11.219	2/15	Default Config	Inactive	-
- A IP Router	vxTarget_xyz	10.255.11.219	2/16	Default Config	Inactive	_
- J. IPY Route	vxTarget_xyz	10.255.11.219	2/17	Default Config	Forwarding	_
Dulas	vxTarget_xyz	10.255.11.219	2/18	Default Config	Inactive	
- Ba VI AN 2000	vxTarget_xyz	10.255.11.219	2/19	Default Config	Inactive	
- Se VLOUV S(#3)	vxTarget_xyz	10.255.11.219	2/20	Default Config	Inactive	
SD AT104 4(6.4)	vxTarget_xyz	10.255.11.219	2/21	Default Config	Forwarding	
- BO 10 ANI E/4E1	vxTarget_xyz	10.255.11.219	2/22	Default Config	Inactive	
VLAN 5(#5)		10 055 11 010	2/22	Default Config	Inactive	
<ul> <li>SØ VLAN 5(#5)</li> <li>SØ VLAN 6(#6)</li> </ul>	vxTarget_xyz	10.255.11.219	212.3	Delaur Coring	III MODIFIE	

Red of a contract of the short of the

## **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.

Click on 80	02.1Q to display a list of 802.1Q 802.1Q Tagged VI	! tagged VLAN ports. LAN Port Assignments
🖉 OmniVista 2500 - Application: VLANs	Window:0	
Eile Applications View Help		
	😸 🕫 🏥 🕺 802.1Q 🔍	
Enterprise Network  Browse  VLANs  VLANs  VLAN 1(#1)  Devices  Constant  Devices  Constant  Co	AOS XOS 802.1Q Ports for - VLAN 1(#1) Name Device Stot Port	Doo 😙 🕾 📰 🖽 🛄
Port Port Protection Port Port Port Port Port Port	View 802.1Q VLAN Port 802.1Q Ports Parameters Device: 10.255.11.59	
← M Rules ← M VLAN 2(#2) ← M VLAN 3(#3) ← M VLAN 4(#4)	Slot: Description:	Port: Force-Tag-Internal:
✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓      ✓	New Edit Update	Delete Apply Help

## 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.

ile Applications <u>V</u> iew H	lelp	Window:0				-10
		<b>\$</b> 9	802.1Q Link Agg	-		
Enterprise Network	A 4	AOS				
VLANs		802.1Q Link Age	for VLAN - VLAN 1(#1)		11 🕲 🕾 🖨 📰 🗄	310
VLAN 1(#1)		Name	Device	Link Agg Id	Description	
Porte		switch_23	10.255.13.23	10	TAG AGGREGATE 10 VLAN 1	
Spanning Tree     Al IP Router     Al IP Router     Al IPX Router		View 802.1Q L	ink Agg		The same of the same	31
<ul> <li>D VLAN 3(#3)</li> <li>D VLAN 4(#4)</li> <li>D VLAN 5(#5)</li> </ul>		Name:		Device:	10.295.11.59	4
<ul> <li>W VLAN 3(#3)</li> <li>VLAN 4(#4)</li> <li>VLAN 5(#5)</li> <li>VLAN 6(#6)</li> </ul>		Name: Link Agg Id:		Device:	10.229.33.59	

# **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	रे 🔊 🕹 📰 🗄	
Name	Device	Slot/Port	Port Type	Port State	
Kite_59	10.255.11.59	1/5	Default Config	Inactive	-
Kite_59	10.255.11.59	1/6	Default Config	Inactive	
Kite_59	10.255.11.59	1/7	Default Config	Inactive	
Kite_59	10.255.11.59	1/8	Default Config	Inactive	
Kite_59	10.255.11.59	1/9	Default Config	Inactive	
Kite_59	10.255.11.59	1/10	Default Config	Inactive	
Kite_59	10.255.11.59	1/11	Default Config	Inactive	
Kite_59	10.255.11.59	1/12	Default Config	Inactive	
Kite_59	10.255.11.59	1/13	Default Config	Inactive	
Kite_59	10.255.11.59	1/14	Default Config	Inactive	
Kite_59	10.255.11.59	1/15	Default Config	Inactive	
Kite_59	10.255.11.59	1/16	Default Config	Inactive	
Kite_59	10.255.11.59	1/17	Default Config	Inactive	
Kite_59	10.255.11.59	1/18	Default Config	Inactive	
Kite_59	10.255.11.59	1/19	Default Config	Inactive	
Kite_59	10.255.11.59	1/20	Default Config	Inactive	
Kite_59	10.255.11.59	1/21	Default Config	Inactive	
Kite_59	10.255.11.59	1/22	Default Config	Inactive	
kite 59	10 255 11 59	1/23	Default Confin	Inactive	-

#### AOS 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 AOS Ports Tab. This activates the Add Ports pop-up window. Click here for information about how to assign ports to a VLAN using this window.

### **Removing a VLAN Port Assignment**

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

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

### **Port Parameter Definitions**

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

#### Name

The user-defined name for the switch.

#### Device

The IP host address that identifies the switch within the management IP network. It is not the same IP host address defined as a virtual IP router port for the 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).

#### 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.

AOS	xos	OmniStack					
Ports 1	for (VLAN	1(#1))			210.210 🔞	88.	EE (***
1	lame	Device	Slot	Port	Function Type	Instance	MAC
no-na	me-119	10.255.11.119	2	1	Bridge	1	00d0 4
no-na	me-119	10.255.11.119	2	2	Bridge	1	00d0
no-nai	me-119	10.255.11.119	2	3	Bridge	1	00d0
no-na	me-119	10.255.11.119	2	4	Bridge	1	00d0
no-na	me-119	10.255.11.119	2	5	Bridge	1	00d0
no-na	me-119	10.255.11.119	2	6	Bridge	1	00d0
no-na	me-119	10.255.11.119	2	7	Bridge	1	00d0
no-na	me-119	10.255.11.119	2	8	Bridge	1	00d0
no-na	me-119	10.255.11.119	2	9	Bridge	1	00d0
no-na	me-119	10.255.11.119	2	10	Bridge	1	00d0
no-na	me-119	10.255.11.119	2	11	Bridge	1	00d0
no-na	me-119	10.255.11.119	2	12	Bridge	1	00d0
no-na	me-119	10.255.11.119	2	13	Bridge	1	00d(
no-na	me-119	10.255.11.119	2	14	Bridge	1	00d0
no-na	me-119	10.255.11.119	2	15	Bridge	1	00d0
no-na	me-119	10.255.11.119	2	16	Bridge	1	00d
no-na	me-119	10.255.11.119	2	17	Bridge	1	00d0
no-na	me-119	10.255.11.119	2	18	Bridge	1	00d0 •
4							•
-							_
	New	Edit Up	date	D	elete Apply	/ Help	

#### **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. Click here for more information about how to assign ports to a VLAN using this window.

### **Removing a VLAN Port Assignment**

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

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

### **Modifying Port Parameters**

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

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

### **Port Parameter Definitions**

#### Name

The user-defined name for the switch.

#### Device

The IP host address that identifies the switch within the management IP network. It is not the same IP host address defined as a virtual IP router port for the 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

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

#### Port

The physical port number on a module.

#### **Function Type**

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

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

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

#### Instance

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

#### MAC Address

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

#### Flood Limit

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

# **OmniStack Ports Tab**

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

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

orts for (VLAN 2(#	(2))		1/1 📆 🕾 🖨 🛃	
Name	Device	Description	Egress Ports	Forbid
est	10.255.11.224	vlan 2	1/1-1/4, 1/49-1/52	

#### **OmniStack VLAN Port Assignments**

### **Assigning Ports to a VLAN**

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

### **Removing Ports from a VLAN**

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

### **Port Parameter Definitions**

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

The user-defined name for the switch.

#### Device

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

#### Description

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

#### **Egress Ports**

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

#### Forbidden Egress Ports

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

#### **Untagged Ports**

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

# AOS 802.1Q Ports Tab

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

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

nivista 2500 - Application: VL	ANs Window:0					_0_×
Eile Applications View Help						
	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	802	.1Q		-	<b>a</b>
Enterprise Network	AOS					
🕈 🥵 VLANs 🔤	802.1Q Ports for	- TESTNET SEE	<b>WERS</b>	VLAN	10(#10) 2/2 🤯	S 🕹 🗒 🎛 🛄
- 300 VLAN 1(#1)	Name	Device	Slot	Port	Description	Force Tag Internal
- 200 VLAN 2(#2)	DCTestnetCore	10.255.10.3	3	1	TAG PORT 3/1 VLAN 10	n/a
	DCTestnetCore	10.255.10.3	4	1	TAG PORT 4/1 VLAN 10	n/a
- 98 VLAN 6(#6)						
- Sn VLAN 7(#7)						
TESTNET SERVERS						
Devices						
Ports						
- <b>G</b> 802.1Q	View 802.10 VL	AN Port				
- 🍢 802.1 Q Link	802.10 Ports F	Parameters				
🗢 👸 Spanning Tree	Dendoor	0.255 40.2	-	7		
- 🕹 IP Router	Device.	10.200.10.0				
- A IPX Router	Slot:			Po	rt:	
🗢 🕍 Rules	Description (					
∽ 📷 VLAN 11(#11)	Description:			FOI	rce-rag-internal:	
- 300 VLAN 17(#17)			_			
VLAN 20(#20)	New	Edit	Upd	ate	Delete Apply	Help
- 200 VLAN 21(#21) ▼	-					

### 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. Click here for information about how to configure an 802.1Q tagged VLAN port assignment.

# **Removing an 802.1Q Port Assignment**

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

# **Modifying 802.1Q Port Parameters**

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

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

🖉 OmniVista 2500 - 🛛 Application: VI	ANs Window:0		
Eile Applications View Help			
	80	2.10 💌	S
	AOS B02.1Q Ports for - TESTNET SE Name Device DCTestnetCore 10.255.10.3 DCTestnetCore 10.255.10.3 Edit 802.1Q VLAN Port 802.1Q Ports Parameters Device: 10.255.10.3 Slot: 4	RVERS VLAN 10(#10) Slot Port De 3 1 TAG POR 4 1 TAG POR	22 3 8 9 9 10 10 10 10 10 10 10 10 10 10 10 10 10
	Description: TAG PORT 4/1	OK Cancel	Help

### Edit 802.1Q VLAN Port Panel

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

# **802.1Q Tagged Port Parameter Definitions**

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

#### Name

The user-defined name for the switch.

#### Device

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

#### Slot/Port

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

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

#### Description

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

#### **Force Tag Internal**

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

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

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

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

# XOS 802.1Q Ports Tab

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

2.10 Ports for	VLAN 2(#2)				3.3 🔞 🗟 🙆	
Name	Device	Slot	Port	Spanning Tree	VLAN Tag	Priority
87 10	.255.13.167	4	1	IEEE - GigaBit	500	
67 10	.255.13.167	4	2	IEEE - GigaBit	500	
o-name 10	.255.13.193	3	11	Multiple (10/100) - Ethernet	2	
fiew 802.1Q VL	AN Port					
/iew 802.1Q VL 802.1Q Ports F	AN Port					
view 802.1Q VL 802.1Q Ports F Device:	AN Port arameters 10.255.11.120			<b>V</b>		
/iew 802.1Q VL 802.1Q Ports P Device: Slot:	AN Port arameters 10.255.11.120			Port:		
/iew 802.1Q VL 802.1Q Ports F Device: Slot: Spanning Tree:	AN Port arameters 10.255.11.120 Proprietary - G	igaBit		Port:       VLAN Tag:		

### 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. Click here for information about how to configure an 802.1Q tagged VLAN port assignment.

### **Removing an 802.1Q Port Assignment**

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

## **Modifying 802.1Q Port Parameters**

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

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

history	Davise	City I	Deat	Octobelle	a Tana	NA ANI TAN	N 121   Solid   Land
Name 44	Device	Slot	Port	Spannin	g tree	VLAN 1ag	Priority
67 10	255.13.167	4	2	IEEE - OigaBit		500	0
0/ 14	255 13 107		- 11	Multiple /10/10/0	Ethomot	200	0
Edit 802.1Q VL/	N Port						
Edit 802.1Q VL/ 802.1Q Ports F	N Port Parameters						
Edit 802.1Q VL/ 802.1Q Ports F Device:	N Port Parameters			*			
Edit 802.10 VL/ 802.10 Ports F Device: Slot:	N Port Parameters 10.255,13,167 4			Port:	2		
Edit 802.1Q VLA 802.1Q Ports F Device: Slot: Spanning Tree:	N Port Parameters 10.255.13.167 4 IEEE - GigaBit			Port:	2		

### Edit 802.1Q VLAN Port Panel

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

### **802.1Q Tagged Port Parameter Definitions**

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

#### Name

The user-defined name for the switch.

#### Device

The IP host address that identifies the switch within the management IP network. It is not the same IP host address defined as a virtual IP router port for the 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	or VLAN - VLAN 1(#1)				1/1 🕲 🕾 🖨 📰	22
Name	Device	1 17	Link Agg Id		Description	
switch_23	10.255.13.23		1	0 TAG AGO	REGATE 10 VLAN 1	
View 802.1Q Link	¢ Agg					
View 802.1Q Link Name:	¢ Agg		Device:	10.255,111		
View 802.1Q Link Name: Link Agg Id:	k Agg		Device: Description:	10.255,114	ат.	

### AOS 802.1Q VLAN Link Aggregation Assignments

### Assigning a Link Aggregate to the VLAN

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

## Removing a Link Aggregate Assignment from the VLAN

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

# **Modifying Link Aggregate Parameters**

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

802.1Q Link A	gg for VLAN - VLAN 10	#1)	1/1 🐨 🕾 🖨 🖽 🖽
Name	Device	Link Agg Id	Description
10012_1	10.200.11.128	31	DURANJY STADAN I
Edit 802 10	ink dan		
Edit 802.1Q	Link Agg		for the state of the
Edit 802.1Q Name:	Link Agg VW_FUJI2_129	Device:	10.255.71.128

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

# 802.1Q Link Aggregate Parameter Definitions

Note that only the description parameter is modifiable.

#### Name

The user-defined name for the switch.

#### Device

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

#### Link Agg ID

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

#### Description

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

# **Configuring Spanning Tree Parameters**

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

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

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

	Click o Tree i	on Spanning Tre nformation for	ee to displa each VLAN — VLAN	y Spanning I device. Spanning T	ree In	formation	ı ——		7
	💋 Omni¥ista 2500 - Application	VLANs Window:0							٦×
	Eile Applications New Help								
Expand Spanning		0 1000	😂 Spann	ning Tree 💌					5
Pridee on Dont	Browse	Spanning Tree List Vi	ew for - VLAN 1	(#1)			84.84 🐯	881	212
Bridge or Port	🕈 😚 VLANS	Name	Address	Protocol	Priority	Maximum Age	Hello Time	Forward Del	an
to configure		demo6850	10.1.1.43	RSTP(802.1W)	32768	20	2	15	-
Spanning Tree	Devices	Kite_59	10.255.11.59	RSTP(802.1W)	32768	20	2	15	
norometers	Ports	vxTarget	10.255.11.60	RSTP(802.1W)	32768	20	2	15	
pur unicitor s.	P Spanning Tree	Kite2_NMS	10.255.11.61	RSTP(802.1W)	32768	20	2	15	
	Bridge	vxTarget	10.255.11.63	RSTP(802.1W)	32768	20	2	15	
	Port	kite2_97_1	10.255.11.97	RSTP(802.1W)	32768	20	2	15	
	ede IP Router	falconCmm	10.255.11.100	STP(802.1D)	32768	20	2	15	
	ade IPX Router	Kite_Fiber_U24	10.255.11.101	STP(802.1D)	32768	20	2	15	
	- M Rules	NMS_HAWK_102_1	10.255.11.102	STP(802.1D)	32768	20	2	15	
	- 30 VLAN 2(#2)	vxTarget	10.255.11.104	STP(802.1D)	32768	20	2	15	
	- 30 VLAN 3(#3)	vxTarget	10.255.11.109	RSTP(802.1W)	32768	20	2	15	
	- 20 VLAN 4(#4)	vxTarget	10.255.11.111	STP(802.1D)	32768	20	2	15	
	- 30 VLAN 5(#5)	Kite	10.255.11.112	RSTP(802.1W)	32768	20	2	15	
	VLAN 0(#0)	no-name	10.255.11.121	RSTP(802.1W)	32768	20	2	15	
	C D VianOperations re	WV_HAWK_122-Test	10.255.11.122	STP(802.1D)	32768	20	2	15	
	DEAD(#8)	NMS_123_Hawk_1	10.255.11.123	STP(802.1D)	32768	20	2	15	
	Guaranthed(#9)	WV_FUUI1_126x	10.255.11.126	RSTP(802.1W)	32768	8	5	15	
		BS0001s-to	10.255.11.127	STP(802.1D)	32768	20	2	15	
		VW_FUUI2_129	10.255.11.129	RSTP(802.1W)	32768	8	5	15	_
		ES0001A-1	10.255.11.130	STP(802.1D)	32768	20	2	15	-
				He	lp				•

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



# **Spanning Tree Parameter Definitions**

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

#### Name

The user-defined name for the switch.

#### Address

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

#### Protocol

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

#### Priority

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

#### Maximum Age

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

#### Hello Time

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

#### **Forward Delay**

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

#### Path Cost

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

#### Mode

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

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

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

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

#### Bridge ID

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

#### Root ID

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

#### Time Since Last Topology Change

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

#### **Total Topology Changes**

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

#### **Root Port Number**

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

#### Next Best Root Cost

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

#### Next Best Root Port

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

#### Network Maximum Age

The Maximum Age time value for the root bridge.

#### **Network Hello Time**

The Hello Time value for the root bridge.

#### **Network Hold Time**

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

#### **Network Forward Delay**

The Forward Delay time value for the root bridge.

# **AOS Spanning Tree Bridge Parameters**

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

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

111 de 1	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Brid	lge 🔻				
nterprise Network	AOS XOS						
VLANS	Spanning Tree E	Bridge Paramet	ers for - VLAN 1	1(#1)	85	85 🔞 📾	AIII
- 📁 VLAN 1(#1)	Name	Device	STP Mor	le	Protocol	Priority	Bridge ID
Devices	Kite 59	10.255.11.59	1X1(One STP P	er VLAN)	RSTP(802.1W)	32768 80 0	00 00 d0 95 a3
• IF Ports	vxTarget	10.255.11.60	1X1(One STP P	er VLAN)	RSTP(802.1W)	32768 80 0	00 00 d0 95 b2
9 55 Spanning Tree	Kite2_NMS	10.255.11.61	1X1(One STP P	er VLAN)	RSTP(802.1W)	32768 80 0	00 00 d0 95 e0
- State Bridge	vxTarget	10.255.11.63	1X1(One STP P	er VLAN)	RSTP(802.1W)	32768 80 0	00 00 d0 95 d5
Port	kite2_97_1	10.255.11.97	1X1(One STP P	er VLAN)	RSTP(802.1W)	32768 80 0	00 00 d0 95 c8
W Router	falconCmm	10.255.11.1	1X1(One STP P	er VLAN)	STP(802.1D)	32768 80 0	0 00 d0 95 6b
Dulas	Kite_Fiber_U24	10.255.11.1	1X1(One STP P	er VLAN)	STP(802.1D)	32768 80 0	00 00 d0 95 bd
A VLAN 2/#2	4		1				•
- 50 VLAN 3(#3) - 50 VLAN 4(#4) - 50 VLAN 5(#5) - 50 VLAN 6(#6) - 50 VLAN 6(#6)	View Spanning Device Spann Device:	g Tree Paramet ning Tree Mode	ers	STP Mo	de: Nat(Single	STP)	*
50 DEAD(#8)	Bridge Paran	neters					
Guarantined(#9)	Protocol:	STP(802.10	)	- Prio	rity:		
20 VLAN 11(#11) 20 VLAN 12(#12)	Maximum Age	8		Hell	o Time:		

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.

Name		Device	OTD	Mada	Droto	col	Dringity	Dri	dae ID
Name	0.000	Lence	51F1	NOGE	PT010	100	20760	00.00 I	oge iD
/do 60	Jore	10.255.10.5	1X1/One STP	Per VLAN)	DOTD/002	2 1100	32768	90.001	0 40 9
VTornot		10.255.11.61	1V1/One STR	Per VLAN)	DOLD (00)	2.1140	22760	90.001	10 40 9
xTarget vTarget		10.255.11.01	1V1/One STE	Per VLAN	DOTD(00)	2 1100	22700	90.001	00400
Magger		10.255.11.05	1V1/One STE	Per VLAN)	PSTP(00	2.199)	32769	90.001	10 40 9
(ite		10.255.11.112	1X1(One STE	Per VLAN	RSTP(80)	2 1100	32768	80.001	P 05 00
216		10.200.11.112	fixing one one	1.61.4674(4)	DOTD(00)	2.1177)	32700	20.001	0 40 0
Target		111 255 11 121	inatizeindie Si	P1	The second se	/ 1991	- AZZ DB		
×Target Edit Spann Device Sp	ning Tro pannin	ee Parameters - g Tree Mode	mat(single si	P)	KolF (ou	2.199)	32700	0000	•
Edit Spann Device Sp Device:	ning Tro pannin 10.255	ee Parameters- g Tree Mode	inationgle of	F)	1X1(0n	e STP P	er VLAN	0000	
Edit Spann Device Sp Device:	ning Tro pannin 10.255 aramet	ee Parameters g Tree Mode .11.59 lers	mati,single s i	P)	1X1(On	e STP P	er VLAN	0000	<b>•</b>
Edit Spann Device Sp Device: Bridge Pa Protocol:	ning Tro pannin 10.255 aramet	ee Parameters g Tree Mode .11.59 lers RSTP(802.1W)	Inati, single s i	STP Mode	: 1X1(0n r 327	e STP P 68	er VLAN)	0000	
Edit Spann Device Sp Device: Bridge Pa Protocol: Maximum	ning Tro pannin 10.255 aramet a Age:	ee Parameters g Tree Mode 	nationgle 5 i	STP Mode Priority Hello T	: 1X1(0n r. 327 ime: 2	e STP P 68	er VLAN)	0000	

Edit AOS Spanning Tree Bridge Parameters Panel

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

### **Modifying Parameters on Multiple Devices**

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

Edit Multiple Ro		×
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. Click here for Spanning Tree Bridge Parameter definitions.

### **Spanning Tree Bridge Parameter Definitions**

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

#### Name

The user-defined name for the switch.

#### Device

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

#### STP Mode

The Spanning Tree operating mode for the switch:

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

#### Protocol

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

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

#### Priority

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

#### Bridge ID

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

#### Maximum Age

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

#### Hello Time

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

#### **Forward Delay**

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

# **XOS Spanning Tree Bridge Parameters**

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

XC	5 Spanni	ng Tree B	ridge Par	amete	rs	
OmniVista 2500 - Application: V	LANs Window	0				_0
jile Applications View Help						
	<b>)</b>		Bridge	-		6
Enterprise Network	AOS XOS	;				
P Browse	Spanning Tr	ee Bridge Parar	neters for - VLA	N 1(#1)	4/4 🔞 🗟 🍓	
9-200 VLAN 1(#1)	Name	Device	Protocol	Priority	Maximum Age	Hello Time
Devices	no-name	10.255.11.119	STP(802.1D)	32768	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
C Bridge	OSR-5slot	10.255.11.197	STP(802.1D)	32768	20	2
- IP Router						
- 🞝 IPX Router						
► M Rules	•		1			· •
🗠 🌆 VLAN 2(#2)						
• 📬 VLAN 3(#3)	View Span	ning Tree Paran	neters			
- 20 New GROUP (#4)(#	₩hen Ro	ot' Parameters				
∽ 📬 VLAN 5(#5)	Davisor		Dro	tocol	CTD/002 4D	
- 20 VLAN 6(#6)	Device.		PIU	1000	STP(602.1D)	
- 200 VLAN 7(#7)	Priority:		Max	ximum Ag	e:	
TESTNET SERVER						
- 10 VLAN 11(#11)	Hello Time	c	For	ward Dela	y:	
• 10 VLAN 17(#17)						
VLAN 20(#20)		Edit	Update	Apply	Help	
• 200 VLAN 21(#21) ▼						
	L					

# **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	LANs Window:0					
Lie Applications Yiew Help	) ;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;		Bridge	-		-
Enterprise Network	AOS XOS	e Bridge Paran	neters for - VLA	N 1(#1)	4/4 🕱 🕽 🚑	
•  •  •  •  •  •  •  •  •  •  •  •  •	Name	Device	Protocol	Priority	Maximum Age	Hello Time
Devices	no-name	10.255.11.119	STP(802.1D)	32768	20	2
Ports	no-name	10.255.11.120	STP(802.1D)	32768	25	2
Pridee	no-name 1	10.255.11.148	STP(802.1D)	32768	20	2
Bluge	OSR-5slot	10.255.11.197	STP(802.1D)	32768	20	2
← ↓ IPX Router ← ₩ Rules ← ₩ VLAN 2(#2) ← ₩ VLAN 3(#3)	Edit Spannir	ng Tree Param	eters			Þ
- 10 New GROUP (#4)(#	When Roo	t' Parameters				
<ul> <li>W VLAN 5(#5)</li> <li>VLAN 6(#6)</li> </ul>	Device:	10.255.11.14	8 Pro	tocol:	STP(802.1D)	-
<ul> <li>SO VLAN 7(#7)</li> <li>SERVERS</li> </ul>	Priority:	32768	Ma	cimum Age	: 20	
<ul> <li>VLAN 11(#11)</li> <li>VLAN 11(#11)</li> </ul>	Hello Time:	2	For	ward Delay	: 15	
			OK Canc	el <u>H</u> e	lp	

#### Edit XOS Spanning Tree Bridge Parameters Panel

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

### **Modifying Parameters on Multiple Devices**

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

Edit Multiple Rows							
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. Click here for Spanning Tree Bridge Parameter definitions.

### **Spanning Tree Bridge Parameter Definitions**

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

#### Name

The user-defined name for the switch.

#### Device

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

#### Protocol

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

#### Priority

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

#### Maximum Age

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

#### **Hello** Time

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

#### **Forward Delay**

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

#### Mode

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

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

#### Status

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

# **AOS Spanning Tree Port Parameters Tab**

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

	19	a 🛔 📃	Port		-		
nterprise Network	AOS X	OS					
VLANs	Port Para	meters Des	ignated Port	IS			
20 VLAN 1(#1)	Spanning	Tree Ports for	- VLAN 1(#1	,		3931/3931	
- B Ports	Name	Device	Slot/Port	Priority	Oper Status	Admin Status	Path Cost Manua
🕈 👸 Spanning Tree	Kite_59	10.255.11.59	1/5	7	Disabled	Enable	0 No
Bridge	Kite_59	10.255.11.59	1/6	7	Disabled	Enable	0 No
- B Port	Kite_59	10.255.11.59	1/7	7	Disabled	Enable	0 No
IP Router	Kite 59	10.255.11.59	1/8	7	Disabled	Enable	0 No
IPX Router	Kite 59	10.255.11.59	1/9	7	Disabled	Enable	0 No
- M Rules	Kite 59	10.255.11.59	1/10	7	Disabled	Enable	0 No
50 VLAN 2(#2)	Kite 59	10.255.11.59	1/11	7	Disabled	Enable	0 No
50 VLAN 3(#3)	Kite 59	10.255.11.59	1/12	7	Disabled	Enable	0 No
1 VLAN 4(#4)	1030 60	10 766 11 60	5/5E	7	Dischlad	Enable	0 10
VLAN 5(#5)	4						•
0 VLAN 6(#6)	View Sp	anning Tree Po	ort Paramete	ers			
DEAD(#8)	Device:				Slot/Port	:	
Guarantined(#9)	Priority:				Oper Sta	itus: Dis	ableti 💌
VLAN 11(#11)	Admin S	tatus:	Enable		Path Cos	st:	
VLAN 12(#12)	Designa	ted Port Root:			Admin C	onnection: No	Point to Point

#### 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 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.

	1	🗄 🏦 📃	Port		-				
Enterprise Network	AOS X	os							
P Browse	Dort Dara	motore De	nimatod	Dorte	1				
VLANS	PUILPala	ineters De	signateu	PUILS					
• 20 VLAN 1(#1)	Conneline	Tree Dorte fo	- 10 -01	4/2/41		2024/2	024 🗨 😁		ana lin
Devices	Spanning	Tree Ports It	I - VLAN	1(#1)		39313	951 99 99	G 200	
Ports	Name	Device	SlotPort	Priority	Oper Statu	s Admin Status	Path Cost	Manual N	lode
Pridae	Kite_59	10.255.11.59	1/5	1	Disabled	Enable	0	NO	
C Bridge	Kite_59	10.255.11.59	1/0	7	Disabled	Enable	0	NO	-
ID Deuter	Kite_09	10.255.11.59	1//	7	Disabled	Enable	0	NO	
I IBV Bouder	Kite_59	10.255.11.59	1/0	7	Disabled	Enable	0	No	-
- Dulae	Vite_09	10.255.11.59	1/19	7	Disabled	Enable	0	No	-
Ba VLAN 2/#2)	Vite_09	10.255.11.59	1/10	7	Disabled	Enable	0	No	-
- Se VI AN 3(#3)	kite_50	10.255.11.59	1/12	7	Disabled	Enshle	0	No	_
VI AN A(#A)	1/ite_00	10.255.11.55	4/4.6	7	Disabled	Enable	. 0	No	_
VI AN 5(#5)	4								•
<ul> <li>VLAN 6(#6)</li> </ul>	-Fall Car	maina Troo D	ort Docom	otoro					
- In VlanOperationsTest()	Eux Spa	nning tree P	ortParam	ieters					
- a DEAD(#8)	Device:		10.255	11.59	S	lot/Port:	1/5		
🗠 🍰 Quarantined(#9)	Driorite		7		0	mor Status	Disabled		
- 🍰 VLAN 10(#10)	Filority.		d.			per status.	Disableu		
• 😼 VLAN 11(#11)	Admin S	Admin Status:			🔻 P	ath Cost:	0		
<ul> <li>SO VLAN 12(#12)</li> <li>SO VLAN 12(#12)</li> </ul>	Designa	ted Port Root	30 00 0	0 d0 95 ;	a3 e0 0d A	dmin Connection	Auto Poin	t to Point	-
Vian 13(#13)	e congred					initiati contriconon			

Edit AOS Spanning Tree Port Parameters Panel

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

### **Modifying Parameters on Multiple Devices**

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

Ealt Multiple Rows	
Edit Spanning Tree	Port Parameterss
Priority:	7
Admin Status:	Enable
Path Cost:	0
Manual Mode:	No
Admin Connection:	Auto Point to Point

# E PARTINE DE LA MARTINE

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

### **Spanning Tree Port Parameter Definitions**

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

#### Name

The user-defined name for the switch.

#### Device

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

#### Slot/Port

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

#### Priority

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

#### **Oper Status**

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

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

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

#### Admin Status

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

#### Path Cost

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

#### Manual Mode

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

#### Admin Connection

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

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

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

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

# **AOS Spanning Tree Designated Ports Tab**

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

			Por	t 🖵			
Entermine Network							_
B Prowno	AOS	xos					
VI ANC	Port Pa	rameters D	esignate	ed Ports			
• 📾 VLAN 1(#1)	Decimate	ul Dorte for	0 AM 4/#	45	20	A	m
Devices	Designati	purforts for - v	Lenn IQ		pa-	11/2921 1 1/2 1/2 1/2 1/2	
- R Ports	Name Vac. 50	Device	SI00P	Designated Port Root	Designated	Designated Port Bridg	e
🕈 👸 Spanning Tree	Kile_59	10.200.11.09	1/3	80 00 00 d0 95 a3 e0 0d	0		0
- 😫 Bridge	1/ite_50	10.255.11.59	1/7	90 00 00 d0 95 a3 e0 00	0	00 00 00 00 00 00 00 00 0	0
- B Port	1/ite_50	10 255 11 59	1/0	90 00 00 d0 95 a3 e0 0d	0	00 00 00 00 00 00 00 00 0	0
- 📣 IP Router	kite 59	10 255 11 59	1/9	80 00 00 d0 95 a3 e0 0d	0	00 00 00 00 00 00 00 00 0	0
IPX Router	kite 59	10 255 11 59	1/10	80 00 00 d0 95 a3 e0 0d	0	00 00 00 00 00 00 00 00 00 00	ň
- M Rules	Kite 59	10.255.11.59	1/11	80 00 00 d0 95 a3 e0 0d	0	00 00 00 00 00 00 00 00 00 00	0
∽ 월 VLAN 2(#2)	Kite 59	10.255.11.59	1/12	80 00 00 d0 95 a3 e0 0d	0	00 00 00 00 00 00 00 00 0	Ō
🗢 🚰 VLAN 3(#3)	Kite 59	10.255.11.59	1/15	80 00 00 d0 95 a3 e0 0d	0	00 00 00 00 00 00 00 00 0	0
← 🚰 VLAN 4(#4)	Kite 59	10.255.11.59	1/16	80 00 00 d0 95 a3 e0 0d	0	00 00 00 00 00 00 00 00 00	0
← 📁 VLAN 5(#5)	Kite_59	10.255.11.59	1/17	80 00 00 d0 95 a3 e0 0d	0	00 00 00 00 00 00 00 00 00	0
<ul> <li>20 VLAN 6(#6)</li> </ul>	Kite_59	10.255.11.59	1/18	80 00 00 d0 95 a3 e0 0d	0	00 00 00 00 00 00 00 00 0	0
<ul> <li>VianOperationsTest()</li> </ul>	Kite_59	10.255.11.59	1/19	80 00 00 d0 95 a3 e0 0d	0	00 00 00 00 00 00 00 00 0	0
- 10 DEAD(#8)	Kite_59	10.255.11.59	1/20	80 00 00 d0 95 a3 e0 0d	0	00 00 00 00 00 00 00 00 0	0
- Guarantined(#9)	Kite_59	10.255.11.59	1/21	80 00 00 d0 95 a3 e0 0d	0	00 00 00 00 00 00 00 00 0	0
<ul> <li>VLAN 10(#10)</li> </ul>	Kite_59	10.255.11.59	1/22	80 00 00 d0 95 a3 e0 0d	0	00 00 00 00 00 00 00 00 0	0
VLAN 11(#11)	Kite_59	10.255.11.59	1/23	80 00 00 d0 95 a3 e0 0d	0	00 00 00 00 00 00 00 00 0	0
• 10 VLAN 12(#12)	Kite_59	10.255.11.59	1/24	80 00 00 d0 95 a3 e0 0d	0	00 00 00 00 00 00 00 00 0	0
🗣 📷 Vian 13(#13)	1.01 00	LOARD IL FO	1.000				9.

### 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.

		S Port		•	•					
nterprise Network	AOS XOS									
VLANs =	Port Paramete	rs Designated	l Ports							
VLAN 1(#1)	Spanning Tree	Ports for - VLAN	1(#1)			12	91/1291	388		10
🗢 🗊 Ports	Name	Device	Slot	Port	Service	Instance	Priority	Oper Status	Admin	S
🕈 👸 Spanning Tree	nms-test-103	10.255.11.103	3	1	Bridge	1	128	Forwarding	Enable	٦
- 😤 Bridge	nms-test-103	10.255.11.103	3	2	Bridge	1	128	Disabled	Enable	
- B Port	nms-test-103	10.255.11.103	3	3	Bridge	1	128	Disabled	Enable	
- 🕹 IP Router	nms-test-103	10.255.11.103	3	4	Bridge	1	128	Disabled	Enable	1
- 🞝 IPX Router	nms-test-103	10.255.11.103	3	5	Bridge	1	128	Disabled	Enable	
► 🛃 Rules	nms-test-103	10.255.11.103	3	6	Bridge	1	128	Disabled	Enable	
WLAN 2(#2)	nms-test-103	10.255.11.103	3	7	Bridge	1	128	Disabled	Enable	
► 🍰 VLAN 3(#3)	4			11					)	•
► 📁 VLAN 4(#4) ► 📁 VLAN 5(#5)	View Spannir	ig Tree Port Para	meters							
- 20 VLAN 6(#6)	Name:				Devic	:90				
<ul> <li>VianOperationsTest()</li> </ul>	Slot				Dort					
- 29 DEAD(#8)	300			_	Purc					
<ul> <li>Quarantined(#9)</li> <li>Quarantined(#10)</li> </ul>	Service:	Unknown			👻 Insta	nce:				
VLAN 11(#11)	Priority:				Oper	Status:	Disabled		-	1
VLAN 12(#12)	Admin Status:	Enable		_	Path	Cost:				1
Vian 13(#13)	Aumin Status	Lindbild			Paul	COSt				

### 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.

		Port			-					
Enterprise Network	AOS XOS									
VLANs	Port Parameter	s Designate	i Ports							
9- 20 VLAN 1(#1)	Spanning Tree	Ports for - VLAN	1(#1)			1	291/1291	3 8 A		
- Ports	Name	Device	Slot	Port	Service	Instance	Priority	Oper Status	Admin	8
9 👸 Spanning Tree	nms-test-103	10.255.11.103	3	1	Bridge	1	128	Forwarding	Enable	ĥ,
Bridge	nms-test-103	10.255.11.103	3	2	Bridge	1	128	Disabled	Enable	T
Port	nms-test-103	10.255.11.103	3	3	Bridge	1	128	Disabled	Enable	1
IP Router	nms-test-103	10.255.11.103	3	4	Bridge	1	128	Disabled	Enable	1
IPX Router	nms-test-103	10.255.11.103	3	5	Bridge	1	128	Disabled	Enable	1
🗢 🕍 Rules	nms-test-103	10.255.11.103	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	1
🗢 🍰 VLAN 3(#3)	4			11				1	•	•
← 20 VLAN 4(#4) ← 20 VLAN 5(#5)	Edit Spanning	Tree Port Parar	neters							
• 📁 VLAN 6(#6)	Name:	nms-test-103			Devie	:e:	10.255.1	1.103		
<ul> <li>WanOperationsTest()</li> </ul>	Slot	2			Dort		4			
- 20 DEAD(#8)	3100	3			Ford		-			
<ul> <li>Guarantined(#9)</li> <li>WLAN 10(#10)</li> </ul>	Service:	Bridge			<ul> <li>Insta</li> </ul>	nce:	1			
• 😏 VLAN 11(#11)	Priority:	128			Oper	Status:	Forward	ng		1
► 30 VLAN 12(#12) ► 30 VLAN 13(#13)	Admin Status:	Enable			▼ Path	Cost:	10			1
- 50 VI AN 14(#14)										4

Edit XOS Spanning Tree Port Parameters

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

### **Modifying Parameters on Multiple Devices**

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

Edit Multiple R	ows	×
Edit Spanning	Tree Port Parameterss	
Priority:	128	
Admin Status:	Enable	

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

### **XOS Spanning Tree Port Parameter Definitions**

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

#### Name

The user-defined name for the switch.

#### Device

The IP host address that identifies the switch within the management IP network. It is not the same IP host address defined as a virtual IP router port for the 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.

	è 🐉 🖗	Po Po	rt	-		
Enterprise Network	AOS XOS	1				
Browse	Port Parame	ters Designat	ed Ports	1		
20 VLAN 1(#1)	Designated Po	ts for - VI AN 10	(1)		1291/1291 🕱 🕾 🗛	
- Devices	blomo	Device	Clot	Port Decispoted Port Post	Decignated Part Cost	D
- B Ports	nme.teet.103	10 255 11 103	3000	1 00 28 00 d0 95 6a 65 d0	Cesignated Port Cost	2 00
🕈 👸 Spanning Tree	nms-test-103	10 255 11 103	3	2 00 00 00 00 00 00 00 00 00		1 00
- 😤 Bridge	nms-test-103	10 255 11 103	3	3 00 00 00 00 00 00 00 00		1 00
- 😤 Port	nms-test-103	10.255.11.103	3	4 00 00 00 00 00 00 00 00 00	1	00 0
- 🕹 IP Router	nms-test-103	10.255.11.103	3	5 00 00 00 00 00 00 00 00 00	1	00 0
IPX Router	nms-test-103	10.255.11.103	3	6 00 00 00 00 00 00 00 00 00		00 0
← M Rules	nms-test-103	10.255.11.103	3	7 00 00 00 00 00 00 00 00 00	(	00 0
VLAN 2(#2)	nms-test-103	10.255.11.103	3	8 00 00 00 00 00 00 00 00 00	(	00 0
VLAN 3(#3)	nms-test-103	10.255.11.103	3	9 00 00 00 00 00 00 00 00 00	(	00 0
► 20 VLAN 4(#4)	nms-test-103	10.255.11.103	3	10 00 00 00 00 00 00 00 00 00	(	00 0
VLAN 5(#5)	nms-test-103	10.255.11.103	3	11 00 00 00 00 00 00 00 00 00	(	00 0
► 30 VLAN 6(#6)	nms-test-103	10.255.11.103	3	12 00 00 00 00 00 00 00 00 00	(	00 0
VianOperationsTest(	nms-test-103	10.255.11.103	3	13 00 00 00 00 00 00 00 00 00	(	00 0
DEAD(#8)	nms-test-103	10.255.11.103	3	14 00 00 00 00 00 00 00 00 00		00 0
Guarantined(#9)	nms-test-103	10.255.11.103	3	15 00 00 00 00 00 00 00 00 00	(	00 0
VLAN 10(#10)	nms-test-103	10.255.11.103	3	16 00 00 00 00 00 00 00 00		00 0
VLAN 11(#11)	nms-test-103	10.255.11.103	5	1 00 00 00 00 00 00 00 00	(	00 0
VLAN 12(#12)	nms-test-103	10.255.11.103	5	2 00 00 00 00 00 00 00 00	(	00 (
Vian 13(#13)	1 1 100	LAARFILLAA	-	alaa aa aa aa aa aa aa aa		-lan

### 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.

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

			- IP Route	r Interface De	efinitions—		1
	🖉 OmniVista 2500 - Application: VLA?	is Window:0				_0	×
	Eile Applications View Help						Г
		19 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	IP Router	-		8	
	Provide Section Sectio	AOS XOS	1(#1)		56/56 😨		
Click on IP Router	• 🕽 VLAN 1(#1)	Name	Device	Router IP Address	Router IP Mack	IP Enconculation	
to configure an IP	Devices	Kite2 NMS	10.255.11.61	10.255.11.61	255 255 255 0	Ethernet 2	
Pouter Interface	🔶 💽 Ports	kite2 97 1	10.255.11.97	10.255.11.97	255 255 255 0	Ethernet 2	
for the VI ANI	🗠 💥 Spanning Tree	falconCmm	10.255.11.100	10.255.11.100	255.255.255.0	Ethernet 2	
TOP THE VLAIN.	1, IP Router	Kite Fiber U24	10.255.11.101	10.255.11.101	255.255.255.0	Ethernet 2	
	- IPX Router	NMS_HAWK_102_1	10.255.11.102	10.255.11.102	255.255.255.0	Ethernet 2	
	Rules	vxTarget	10.255.11.104	10.255.11.104	255.255.255.0	Ethernet 2	
	> 20 VLAN 2(#2)	vxTarget	10.255.11.109	10.255.11.109	255.255.255.0	Ethernet 2	
	- 30 VLAN 3(₹3)	vxTarget	10.255.11.111	10.255.11.111	255.255.255.0	Ethernet 2	
	- 30 VLAN 4(#4)	Kite	10.255.11.112	10.255.11.112	255.255.255.0	Ethernet 2	
		no-name	10.255.11.121	10.255.11.121	255.255.255.0	Ethernet 2	
	Se VianOnerationeTect/d	NMS_123_Hawk_1	10.255.11.123	10.255.11.123	255.255.255.0	Ethernet 2	
		BS0001s-to	10.255.11.127	10.255.11.127	255.255.255.0	Ethernet 2	
	S Quarantined(#9)	•	1			•	
	- 50 VLAN 10(#10)	View IP Router					
	- 😼 VLAN 12(#12)	Set IP Virtual Routi	ng Parameters				
	← 🞾 Vian 13(#13) ← 🍰 VLAN 14(#14)	Device:	10.255.211.24	0 💌			
	← 🞥 VLAN 15(#15)	Router IP Address:		Router I	P Mask:		
	• 30 VLAN 16(#16) • 30 VLAN 17(#17)	IP Encapsulation:	Ethernet 2	IP Forwa	arding: Enabled	-	
		New	Edit	Update Delete	Apply	Help	

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

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

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

	[	IPX Router Interface Definitions	1
	🖉 OmniVista 2500 - Application: V.	ANs Window:0	×
	File Applications View Help		
		IPX Router 💌	Ł
Click on IPX Router to configure an IPX Router Interface for the VLAN.		AOS XOS  IPX Routing for - VLAN 1(#1)  Name Device Protocol Net Address Frame Type Description no-name 10.255.11.120 IPX RiP and SAP 66666666 Ethernet 2 IPX router View IPX Router Set IPX Virtual Routing Parameters Device: 10.255.11.119 View IPX Router Frame-Type: Ethernet 2 V	
	← 20 VLAN 23(#23) ← 20 VLAN 27(#27) ▼	New Edit Update Delete Apply Help	
## **AOS IP Routing Tab**

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

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

		IP Rout	ter 💌		
prise Network	AOS XOS				
ans	IP Routing for - VLA	N 1(#1)		26/26	88 <b>6</b>
N 1(#1)	Name	Device	Router IP Addre	ss Router IP Mask	IP Encapsulation
5	NMS_HAWK_102	10.255.11.102	102.102.102.102	255.255.255.0	Ethernet 2
Tree	vxTarget	10.255.11.104	10.255.11.104	255.255.255.0	Ethernet 2
ig riee	HAWK_113	10.255.11.113	10.255.11.113	255.255.255.0	Ethernet 2
	HAWK_114	10.255.11.114	10.255.11.114	255.255.255.0	Ethernet 2
4	HAWK_115	10.255.11.115	10.255.11.115	255.255.255.0	Ethernet 2
	HAWK_116	10.255.11.116	10.255.11.116	255.255.255.0	Ethernet 2
F4)	HAWK_117	10.255.11.117	10.255.11.117	255.255.255.0	Ethernet 2
	HAWK_118	10.255.11.118	10.255.11.118	255.255.255.0	Ethernet 2
-470	•		10		)
	-View ID Router				
#7)	Contraction of the second seco				
SERVER	Set IP Virtual Ro	uting Parameter	s		
)	Device:	10.255.10.3	-		
0					
7)	Router IP Addres	is:	Ro	uter IP Mask:	
	IP Encapsulation	Ethernet 2	V IP I	Forwarding: Enabl	ed 👻
21)	. Enoupoundation				

AOS 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 AOS IP Routing Tab. This activates the Create IP Router panel, as shown below.

		IP Rout	ter	-				
rprise Network	AOS XOS							
JANS	IP Routing for - VLAN	N 1(#1)			2	6/26 🐄	88	
VLAN 1(#1)	Name	Device	Router IP A	ddress	Router	P Mask	IP Encapsul	ation
is and	NMS_HAWK_102	10.255.11.102	102.102.10	2.102	255.255.3	255.0	Ethernet 2	
	vxTarget	10.255.11.104	10.255.11.1	04	255.255.1	255.0	Ethernet 2	
Liee	HAWK_113	10.255.11.113	10.255.11.1	13	255.255	255.0	Ethernet 2	
	HAWK_114	10.255.11.114	10.255.11.1	14	255.255.3	255.0	Ethernet 2	
	HAWK_115	10.255.11.115	10.255.11.1	15	255.255.2	255.0	Ethernet 2	_
	HAWK_116	10.255.11.116	10.255.11.1	18	255.255	255.0	Ethernet 2	_
	HAWK_117	10.255.11.117	10.255.11.1	17	255.255	255.0	Ethernet 2	
	HAWK_118	10.255.11.118	10.255.11.1	18	255.255	255.0	Ethernet 2	
G E	1	i. (J				· · · · · ·		
12	Create ID Router							
75								
ET SERVER	Set IP Virtual Rou	ting Parameter	s					
11)	Device:	10.255.10.3	-					
).	Design ID Address							
	Router IP Address			Router	IP Mask:	l		
0)	IP Encapsulation:	Ethernet 2		IP Forv	varding:	Enable	d	-
		-	E10					-
3)	Interface Name:	1	-					
<i>n</i>								

Create AOS IP Router Panel

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

1. Select a device from the Device field list (e.g., 242).

**2.** Enter an IP address in the **Router IP Address** field (e.g., 198.181.10.2). This address is assigned to the IP router interface. The router interface IP address must be unique. You cannot have two router interfaces with the same IP address.

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

4. Select the router interface encapsulation from the IP Encapsulation field list.

5. Select the router interface forwarding status from the IP Forwarding field list.

6. Enter a unique interface name (text string up to 20 characters) in the Interface Name field.

7. Click on the **OK** button to accept the parameter values you have defined. The Create IP Router panel will close, returning you to the AOS IP Routing Tab list. A new entry now appears in this list for the IP router interface you just defined for the selected device. This entry contains an add icon in the Name field for the device.

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

**8.** When you 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 😫 🕫 🏥 👲	IP Router	• •		
Enterprise Network	AOS XOS				
Prowse	IP Routing for - VLA	N 1(#1)		33/33	<b>3</b> - <b>8</b>    H
• 对 VLAN 1(#1)	Name	Device	Router IP Add	dress Router I	Mask IP Encapsula
Devices	NMS_HAWK_102	10.255.11.102	102.102.102.1	02 255.255.2	55.0 Ethernet 2
Pons	Kite(6800)_104	10.255.11.104	10.255.11.104	255.255.2	255.0 Ethernet 2
Spanning Tree	no-name	10.255.11.111	11.11.11.11	255.255.2	55.0 Ethernet 2
adv IP Router	HAWK_113	10.255.11.113	10.255.11.113	255.255.2	255.0 Ethernet 2
- adv IPX Router	HAWK_114	10.255.11.114	10.255.11.114	255.255.2	55.0 Ethernet 2
~ Sa 10 AN 2/#21	•				•
- Se VLAN 3(#3)	-Edit ID Poutor				
- Se New GROUP (#4)(#	Ealt IP router				
- 🖬 VLAN 5(#5)	-Set IP Virtual Rou	ting Parameters	s		
- 50 VLAN 6(#6)	Device:	10.255.11.10	2 -		
- 10 VLAN 7(#7)				_	
- STRET SERVERS	Router IP Address	s: 102.102.102	.102 Rot	uter IP Mask: 2	55.255.255.0
- 🍰 VLAN 11(#11)	ID Encansulation:	Ethernet 2	T ID F	orwarding:	nabled
- 50 VLAN 17(#17)	- chcapsuiduon.	ctilemet z		or war unity.	Trainest V
	Interface Name:	vlan-1			
- 🚰 VLAN 20(#20)					
► 20 VLAN 20(#20) ► 20 VLAN 21(#21)					

Edit AOS 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.

## **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.

		IP	Router	-			
Browse	AOS XOS						
• 10 VLAN 1(#1)	IP Routing for -	VLAN 1(#1)				46/46 🕱 🕲 🖨	
Devices	Name	Device	Protocol I	P Address	s IP Mask	Broadcast Address	D
- Ex Ports	nms-test-103	10.255.11.103	ipRip 10	255.11.1	03 255 255 0.0	10.255.255.255	GROUP #
- St spanning Tree	no-name-119x	10.255.11.119	ipRip 10	255.11.1	19 255.255.255.0	10.255.11.255	GROUP
es IP Router	no-name	10.255.11.120	ipRip 10	255.11.1	20 255.255.255.0	10.255.11.255	GROUP
ad IPA Router	no-name	10.255.11.124	ipRip 10	255.11.1	24 255 255 255 0	10.255.11.255	GROUP #
C- M Rules	NMS-test-148	10.255.11.148	IpRip 10	255.11.1	48 255 255 255 0	10.255.11.255	GROUP
- 30 VLAN 2(#2)	OSR-5slot	10.255.11.153	ipRip 10	255.11.1	53 255 255 255 0	10.255.11.255	GROUP #
- 200 VLAN 3(#3)	69.0000	10 265 11 160	inDin 50	266.11.1	0.336 336 336 93	10 266 11 266	GROUP
<ul> <li>SØ VLAN 5(#5)</li> <li>SØ VLAN 6(#6)</li> <li>SØ VIAN 0(#6)</li> </ul>	View IP Route Set IP Virtua	r I Routing Paran	neters				
<ul> <li>20 DEAD(#8)</li> <li>20 Quarantined(#9)</li> </ul>	Device:	10.255.11.103		7			
<ul> <li>SO VLAN 10(#10)</li> <li>SO VLAN 11(#11)</li> </ul>	Protocol:	upilititi -		IP A	Address:		
- 10 VLAN 12(#12)	ID Mask			Des	scription		
- 10 Vian 13(#13)	in mounts			Dus	a a particular		-
	Frame-Type:	Ethernet 2		- RIP	Config Mode:	lient	

**XOS 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 found at the bottom of the XOS IP Routing Tab. This activates the Create IP Router panel, as shown below.

OmniVista 2500 - Application: Vi File Applications View Help	ANs Window:0					
Enterprise Network	AOS XOS IP Routing for - Name no-name 10 OSR-5slot 10	VLAN 1(#1) Device 0.255.11.120 0.255.11.148 0.255.11.197	Protocol ipRip ipRip ipRip	IP Address 10.255.11.120 25 10.255.11.148 25 10.255.11.197 25	3/3 😪 🕅 IP Mask 5.255.255.0 5.255.255.0 5.255.255.0	Broadcast Addre 10.255.11.255 10.255.11.255 10.255.11.255
← Mark Rules ← Mark Rules ← Se VLAN 2(#2) ← Se VLAN 3(#3) ← Se New GROUP (#4)(#- ← Se VLAN 5(#5)	Create IP Rou Set IP Virtua	I Routing Para	meters	1		•
Set VLAN 8(#6)     Set VLAN 7(#7)     Set VLAN 7(#7)     Set VLAN 7(#1)     Set VLAN 11(#11)     Set VLAN 17(#17)     Set VLAN 20(#20)	Protocol: IP Mask: Frame-Type:	10.255.11.1 ipRip 255.255.255 Ethernet 2	19 <b>•</b>	IP Address: Description: RIP Config Mode	10.255.11 OUP #1.0	.148 IP router vport
VLAN 21(#21)     VLAN 23(#23)     VLAN 27(#27)		[	ок	Cancel Help		

Create XOS IP Router Panel

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

**1.** Select a device from the **Device** field list. Note that you can only define an IP router interface on a device that does not already have a router interface defined for this VLAN.

2. Select a protocol from the Protocol field list. In most cases, the default value of IpRip is sufficient.

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

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

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

**6.** Select the router interface encapsulation from the **Frame Type** field list. By default, the encapsulation is set to Ethernet 2.

7. Select the RIP operational mode from the **RIP Config Mode** field list. By default, the RIP mode is set to Silent (RIP listens for routing updates, but does not send them).

**8.** Click on the **OK** button to accept the parameter values you have defined. The Create Router IP panel will close, returning you to the XOS IP Routing Tab list. A new entry now appears in this list for the IP router interface you just defined for the selected device. This entry contains an add icon in the Name field for the device.

**9.** Click on the **Apply** button at the bottom of the XOS IP Routing Tab to update the device with the new IP router interface definition.

## **Modifying IP Router Interface Parameters**

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

OmniVista 2500 - Application: Vi File Applications View Help	LANs Window:0					_0,
		🏥 🛛 IP	Router	-		
Enterprise Network  Browse  VLANs  VLAN1(#1)  Devices     Ports  Ports  Ports  Ports  Ports  Rules  Rules  Rules  Ports  Rules  Ports  Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Ports Por	AOS XOS IP Routing for - Name no-name 10 OSR-5slot 10 4	VLAN 1(#1) Device .255.11.120 .255.11.148 .255.11.197	Protocol ipRip ipRip ipRip	IP Address 10.255.11.120 10.255.11.148 10.255.11.197	0.3 3 0 IP Mask 255.255.255.0 255.255.255.0 255.255.255.0	Broadcast Addre 10.255.11.255 10.255.11.255 10.255.11.255
	Edit IP Router Set IP Virtual Device: Protocol: IP Mask: Frame-Type:	Routing Para 10.255.11.1 ipRip 255.255.255 Ethernet 2	imeters 18 T i.0	IP Address: Description: RIP Config Me	10.255.11 OUP #1.0 ode: Silent	148 IP router vport
		[	ок	Cancel	lelp	

Edit XOS IP Router Panel

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.

OmniVista 2500 - Application: YLAN File Applications View Help	s Windows0	
	AOS XOS  IPX Routing for - VLAN 2(#2)  Name Device IPX Address IPX Encapsulation RiP/SAP Mode D BS0001s 10.255.11.127 33333333 Ethernet 2 RIP-SAP	elayTicks 3
Set VLAN 10(#10)     Set VLAN 11(#11)     Set VLAN 11(#11)     Set VLAN 12(#12)     Set VLAN 13(#13)     Set VLAN 13(#13)     Set VLAN 15(#15)     Set VLAN 15(#15)     Set VLAN 15(#16)     Set VLAN 15(#16)     Set VLAN 12(#20)     Set VLAN 21(#21)	View IPX Router Set IPX Virtual Routing Parameters Device: 10.255.11.59 IPX Address: IPX Encapsulation: Ethernet 2 RIP/SAP Mode: OP Only  Delay Ticks:	
Start VLAN 21(#21)     Start VLAN 22(#22)     Start VLAN 22(#22)     Start VLAN 23(#23)     ▼	New Edit Update Delete Apply Help	

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.

🖉 OmniVista 2500 - Application: VL	ANs Window:0					
Eile Applications View Help						
	) <b>\$</b> 94\$	IPX Rou	ter 💌			2
- WLAN 535(#535)	AOS					
- Se VLAN 536(#536)						
🗠 🍻 VLAN 537(#537)	IPX Routing for - V	LAN 550(#550)			1/1 🔞 🗏	
∽ 🚰 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
← 20 VLAN 540(#540)						
VLAN 541(#541)						
→ SI VLAN 543(#543)						
VLAN 544(#544)						
∽ 🝰 VLAN 545(#545)						
∽ 🐲 VLAN 546(#546)	-Create IDV Route	or				
► 📬 VLAN 547(#547)	Create IFA rout					
► 20 VLAN 548(#548)	Set IPX Virtual	Routing Paramete	ers			
• 10 VLAN 549(#549)	Device:	10.255.13.92	-	·		
Paul Y LAW 550(#550)	IDV Addrosom			IDV Enconculations	Ethornot 2	
Ports	IPA Autoress.			IPA Elicapsulation.	Culernet 2	
🗢 👸 Spanning Tree	RIP/SAP Mode:	RIP Only	-	Delay Ticks:		
IP Router				-	1	
IPX Router			OK	Cancel Help		
🔶 🔛 Rules 🔍 👻			- On	Concer Link		

### 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.

🖉 OmniVista 2500 - Application: VL	ANs Window:0					
Eile Applications View Help						
		IPX Rot	uter 💌			<b>a</b>
- 50 VLAN 535(#535)	AOS					
← 💭 VLAN 536(#536) ← 💭 VLAN 537(#537)	IPX Routing for -	VLAN 550(#550)			1/1 🔞 🕅	
<ul> <li>VLAN 538(#538)</li> </ul>	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
S S VI AN 541(#540)						
VLAN 542(#542)						
∽ 🚰 VLAN 543(#543)						
🗠 🎒 VLAN 544(#544)						
🗠 🞾 VLAN 545(#545)						
VLAN 546(#546)	Edit IPX Router					
- 200 VLAN 54/(#547)	Set IDX Virtual	Routing Paramet	ers			
- Se VI AN 549(#549)	Jet in A Virtue	Turaning F di diffici		1		
- SO VLAN 550(#550)	Device:	10.255.11.121				
Devices 🗧	IPX Address:		25001113	IPX Encapsulation:	Ethernet 2	-
🗠 🗊 Ports						
🕈 🙀 Spanning Tree	RIP/SAP Mode:	RIP Only		Delay Ticks:	5	
- A IP Router						
- Rules			OK	Cancel Help		

Edit AOS IPX Router Panel

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

### **Removing an IPX Router Interface**

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

## **IPX Router Interface Parameter Definitions**

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

#### Name

The user-defined name for the switch.

#### Device

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

#### **IPX Address**

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

#### **IPX Encapsulation**

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

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

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

#### **RIP/SAP Mode**

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

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

#### **Delay Ticks**

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

## **XOS IPX Routing Tab**

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

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

Browse	AOS XOS	
• 🐉 VLAN 1(#1)	IPX Routing for - VLAN 1(#1) 33 3 3 A B	EIII
Devices	Name Device Protocol Net AddressFrame Type Description Admin Status	Ope
- Ex Ports	no-name 10 255 11 120 IPX RIP and SAP 866666666 Ethernet 2 IPX router port Enable A	Active
• Ss spanning free	Alias 10.255.11.174 IPX RIP and SAP 666666666 Ethernet 2 IPX router port Enable A	Active
J IDV Dautar	no-name 10.255.13.175 IPX RIP and SAP 444bed Ethemet 2 Enable A	Active
<ul> <li>► SØ VLAN 2(#2)</li> <li>► SØ VLAN 3(#3)</li> <li>► SØ VLAN 4(#4)</li> <li>► SØ VLAN 5(#5)</li> </ul>		
← 50 VLAN 2(#2) ← 50 VLAN 3(#3) ← 50 VLAN 4(#4) ← 50 VLAN 4(#4) ← 50 VLAN 5(#6) ← 50 VLAN 5(#6) ← 50 VLAN 5(#6)	Mew IDV Porter	
<ul> <li>S0 VLAN 2(#2)</li> <li>S0 VLAN 3(#3)</li> <li>S0 VLAN 4(#4)</li> <li>S0 VLAN 5(#5)</li> <li>S0 VLAN 6(#6)</li> <li>S0 VLAN 6(#6)</li> <li>S0 VLAN 6(#8)</li> </ul>	View IPX Router     Set IDX Vietual Routing Datameters	1
	View IPX Router     Set IPX Virtual Routing Parameters	1
<ul> <li>S0 VLAN 2(#2)</li> <li>S0 VLAN 3(#3)</li> <li>S0 VLAN 4(#4)</li> <li>S0 VLAN 5(#5)</li> <li>S0 VLAN 6(#6)</li> <li>S0 VLAN 6(#6)</li> <li>S0 VLAN 6(#6)</li> <li>S0 Quarantined(#9)</li> <li>VLAN 10(#10)</li> <li>VLAN 11(#11)</li> </ul>	View IPX Router     Set IPX Virtual Routing Parameters     Device: 0.255.11.103	
<ul> <li>SU VLAN 2(#2)</li> <li>VLAN 3(#3)</li> <li>VLAN 4(#4)</li> <li>VLAN 5(#5)</li> <li>VLAN 6(#6)</li> <li>VLAN 6(#6)</li> <li>VLAN 6(#6)</li> <li>VLAN 6(#6)</li> <li>VLAN 10(#10)</li> <li>VLAN 10(#10)</li> <li>VLAN 10(#11)</li> <li>VLAN 12(#12)</li> <li>VLAN 12(#12)</li> <li>VLAN 13(#13)</li> </ul>	View IPX Router       Set IPX Virtual Routing Parameters       Device:     10.255.11.103       Protocol:     IVX PRP Only   Net Address:	
<ul> <li>W VLAN 2(#2)</li> <li>W VLAN 3(#3)</li> <li>W VLAN 4(#4)</li> <li>VLAN 5(#6)</li> <li>W VLAN 6(#6)</li> <li>U VLAN 6(#6)</li> <li>U VLAN 10(#10)</li> <li>VLAN 10(#10)</li> <li>VLAN 12(#12)</li> <li>W VLAN 12(#12)</li> <li>VLAN 14(#14)</li> </ul>	Image: Content of the second secon	

**XOS IP 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 found at the bottom of the XOS IPX Routing Tab. This activates the Create IPX Router panel, as shown below.

	🙆 🐉 🗐 🛔 👲 IPX Router 💌	
Browse VLANs VLANs VLAN 1(#1)  Browces Grows Forts Spanning Tree  KIP Router KIP Router KIPS	AOS         XOS           IPX Routing for - VLAN 1(#1)         3.3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	Active Active Active
<ul> <li>30 VLAN 2(#2)</li> <li>30 VLAN 3(#3)</li> </ul>		
<ul> <li>VLAN 2(#2)</li> <li>VLAN 3(#2)</li> <li>VLAN 4(#4)</li> <li>VLAN 5(#5)</li> <li>VLAN 6(#6)</li> <li>VLAN 6(#6)</li> <li>DEAD(#8)</li> <li>Quarantined(#9)</li> <li>VLAN 10(#10)</li> </ul>	Create IPX Router Set IPX Virtual Routing Parameters Device: 10.255.11.103	

Create XOS IPX Router Panel

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

**1.** Select a device from the Device field list. Note that you can only define an IPX router on a device that does not already have an IPX router interface defined for the selected VLAN.

2. Select the router interface advertisement mode from the Protocol 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.

OmniVista 2500 - Application: le Applications View Help	LANs Window:0	Router	
Browse VLANs VLAN 1 (#1) Devices Spanning Tree A IP Router C VLAN 2(#2) VLAN 3(#3) NLAN 3(#3) NLAN 3(#3)	AOS XOS IPX Routing for - VLAN 1(#1) Name Device Pro no-name 10.255.11.120 IPX RIP Alias 10.255.11.174 IPX RIP no-name 10.255.13.175 IPX RIP	tocol Net Address Frame Type Deso and SAP 66666666 Ethernet 2 IPX ro and SAP 66666666 Ethernet 2 IPX ro and SAP 444bed Ethernet 2	333 😵 🖘 🕹 🏢 🖭 cription Admin Status Oper uter port Enable Active Enable Active
← 50 VLAN 5(#5) ← 50 VLAN 6(#6)	•	1	
300 VianOperationsTe     300 DEAD(#8)     400 Quarantined(#9)     500 VLAN 10(#10)     500 VLAN 11(#11)     500 VLAN 12(#12)     500 Vian 13(#13)	Edit IPX Router Set IPX Virtual Routing Parame Device: 10.255.11.174 Protocol: IPX RIP and SAP Frame-Type: Ethernet 2	eters	66666666

Edit XOS IPX Router Panel

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

### **Removing an IPX Router Interface**

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

## **IPX Router Interface Parameter Definitions**

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

#### Name

The user-defined name for the switch.

#### Device

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

#### Protocol

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

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

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

#### Net Address

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

#### Frame Type

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

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

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

#### Description

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

#### Admin Status

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

#### **Oper Status**

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

#### **Source Route Type**

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

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

# **Multiple IP Router Interfaces**

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

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



# **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 nonmobile distinction and there is no overall switch setting to invoke the mobile port feature. As a result, you can define rules to capture mobile port traffic on any VLAN. Click here for more information about configuring mobility on AOS devices.

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

				- VLA	N Rule Definitions		
	🖉 OmniVista 250) - Application: 1	LANs Window:	)				-0
	File Applications View Help						
		a so:	1 🚔 🖻 F	Rules	-		4
	P Browse	Rules (VLAN 1(	#1))		31/31	388	
	•  •  •  •  •  •  •  •  •  •  •  •  •	Name	Switch Addre	Rule Type	Rule Value	Rule State	
	- Devices	OSR-5slot	10.255.11.153	Port	2/1/Bridge/1	Disabled	-
	- 🖬 Ports	OSR-5slot	10.255.11.153	MAC	aabbcc:ddee11	Enabled	
	🗢 👸 Spanning Tree	VLAN-OS6648	10.255.11.181	MAC	00aabb:123456	Enabled	
	- +1+ IP Router	VLAN-OS6648	10.255.11.181	MAC	00aacc:123456	Enabled	
	- J. IPX Router	VLAN-OS6648	10.255.11.181	MAC	00b0d0:193c68	Enabled	
×pand Rules –	Rules	VLAN-OS6648	10.255.11.181	MAC	00b0d0:428259	Enabled	
the tree to	Protocol	VLAN-OS6648	10.255.11.181	DHCP-MAC	00aabb:123456	Enabled	-
last Dile	- Port	VLAN-0S6648	10.255.11.181	DHCP-MAC	00aacc:123456	Enabled	
elect a Rule	- T MAC	VLAN-0S6648	10.255.11.181	DHCP-MAC	00b0d0:193c68	Enabled	
/pe.	- The Addres	VLAN-0S6648	10.255.11.181	DHCP-MAC	00b0d0:428259	Enabled	
	- Custom	VLAN-Falcon	10.255.11.186	Port	1/23	Enabled	
	- T DHCP	vxTarget_xyz	10.255.11.219	Port	2/1	Enabled	
	- The DHCP Port	vxTarget_xyz	10.255.11.219	Port	2/2	Enabled	
	- TO DHCP MAC	vxTarget_xyz	10.255.11.219	Port	2/3	Enabled	
	Binding	vxTarget_xyz	10.255.11.219	Port	2/4	Enabled	
	- Se VLAN 2(#2)	vxTarget_xyz	10.255.11.219	IP	IP = 3.0.0.0, Mask = 255.0.0.0	Enabled	
	- Se VLAN 3(#3)	vxTarget_xyz	10.255.11.219	IPX .	IPX=1431651653, Encapsulation = n	Enabled	
	- 😼 VLAN 4(#4)	FALCON-137	10.255.11.221	IP	IP = 10.255.11.0, Mask = 255.255.255.0	Enabled	
	- SU VLAN 5(#5)	FalconCmm	10.255.11.243	MAC	00b0d0:193c68	Enabled	-
			U	pdate	Delete Apply Help		

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

## **Copying a VLAN Rule**

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

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

**1.** The VLAN rules that are not supported on the target devices. For example, in OS 6800, the VLAN Mobility rules like Custom Rules, IP-MAC Binding Rules, IP-Port Binding Rules, and MAC-Port-Protocol are not supported.

**2.** The VLAN rules definitions involving slots/ports that do not exist in the target devices.

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

## **Removing a VLAN Rule**

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

## **VLAN Rules Window Information Fields**

#### Name

The user-defined name for the switch.

#### **Switch Address**

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

#### **Rule** Type

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

#### **Rule Value**

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

#### **Rule State**

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

# **Understanding VLAN Rule Precedence**

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

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

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

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

- If the frame's source MAC address matches the rule's MAC address, then the frame's port must also match the rule's port to qualify for assignment to the rule's VLAN.
- If the frame's source MAC matches but the frame's port does not match, then a violation occurs and the frame is blocked and the port is not assigned to the rule's VLAN. There is no further attempt to match this frame to rules of lower precedence.
- If the frame's source MAC does not match but the frame's port does match, the frame is allowed but the port is not assigned to the rule's VLAN. The frame is then compared to other rules of lower precendence 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.
<ol> <li>MAC-IP Address Binding</li> </ol>	Frame contains a matching source MAC address and source IP subnet address.	Frame source is assigned to the rule's VLAN.
	Frame only contains a matching source MAC address; IP address does not match.	Frame is blocked; its source is not assigned to the rule's VLAN.
	Frame only contains a matching IP address; source MAC does not match.	Frame is blocked; its source is not assigned to the rule's VLAN.
10. Port-IP Address Binding	Frame contains a matching source port and source IP subnet address.	Frame source is assigned to the rule's VLAN.
	Frame only contains a matching source IP address; port does not match.	Frame is blocked; its source is not assigned to the rule's VLAN.
	Frame only contains a matching port; source IP address does not match.	Frame is allowed, its source is not assigned to the rule's VLAN.
11. Port-Protocol Binding	Frame contains a matching source port and protocol.	Frame source is assigned to the rule's VLAN.
	Frame only contains a matching source port; protocol does not match.	Frame is blocked; its source is not assigned to the rule's VLAN.
	Frame only contains a matching protocol; port does not match.	Frame is allowed; its source is not assigned to the rule's VLAN.
12. MAC Address	Frames contain a matching source MAC address.	Frame source is assigned to the rule's VLAN.
13. MAC Range	Frame contains a source MAC address that falls within a specified range of MAC addresses.	Frame source is assigned to the rule's VLAN.
<ol> <li>Network Address</li> </ol>	Frame contains a matching IP sub- net address, or	Frame source is assigned to the rule's VLAN.
	Frame contains a matching IPX network address.	Frame source is assigned to the rule's VLAN.
15. Protocol	Frame contains a matching proto- col type.	Frame source is assigned to the rule's VLAN
16. Custom (User Defined)	Frames contain data that matches	Frame source is assigned to the
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.

	50 i 10 i	Protocol 👻		
Enterprise Network	Protocol Rules (VLAN 1(#	1))	9.9 😌	
VLANS	Name	Switch Address	Rule Value	Rule State
Se 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
- L 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 MAC     Binding     VLAN 2(#2)     VLAN 3(#3)				

### 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. Click here for information on how to define a protocol rule using this window.

## **Removing a Protocol Rule**

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

# **Add Protocol Rules Window**

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

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

Add Protoco	Rules			2
Select Devices	s for th	ne Protocol rules	-	
Name		Address	DNS Name	Type
DCTestnet	Core	10.255.10.3		OS7700 -
Kite_59		10.255.11.59		OS6800-41-
w/Target		10.255.11.61		OS6800-2
w/Target		10.255.11.83		OS6800-2-
kite2_97		10.255.11.97		086800-2-
Kite		10.255.11.112		OS6800-2
1	_	and the second se		
● IP ○ IPX	0 #	P.SNAP PX-Novell		
<ul> <li>IP</li> <li>IPX</li> <li>IPX-LLC</li> <li>IPX-SNAP</li> </ul>	0 IF 0 IF 0 E	P-SNAP PX-Novell thernet Type AP Header		000) (DSAP)
<ul> <li>IP</li> <li>IPX</li> <li>IPX-LLC</li> <li>IPX-SNAP</li> <li>AppleTalk</li> </ul>	0 II 0 II 0 E	P-SNAP PX-Novell thernet Type AP Header		(DSAP)

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

**1.** Select one or more devices from the list located in the top half of the Add Protocol Rules window. Note that all devices are selected by default.

2. Click on one of the following protocol types displayed in this window:

- IP (Ethernet II, ARP, and SNAP)
- IP-SNAP (AOS only)
- IPX (Ethernet II, Novell 802.3, LLC 802.2, and SNAP)
- IPX-LLC (AOS only)
- IPX-SNAP (AOS only)
- IPX-Novell (AOS only)
- AppleTalk (Data Delivery Protocol and AppleTalk ARP)
- DECNet (DECNet Phase IV--only captures frames with 6003 Ethernet type)
- Ethernet Type (A two byte hex value between 0x600 and 0xffff that defines an Ethernet type. This value is required for the Ethernet Type field when this protocol type is selected.)
- SAP Header (A one byte hex value between 0x00 and 0xff that defines DSAP and SSAP header values. These values are required for the DSAP and SSAP fields when this protocol type is selected.)
- SNAP Type (A two byte hex value between 0x600 and 0xffff that defines a Sub-network Access Protocol. This value is required for the SNAP Type field when this protocol type is selected.)

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

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

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

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

# **Defining Port Rules**

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

Consider the following when defining a VLAN port rule:

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

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

		Port 💌		
nterprise Network	Port Rules (VLAN 1	(#1))		66 <b>3</b> 8 8 3
VLANS	Name	Switch Address	Rule Value	Rule Stat
30 VLAN 1(#1)	OSR-5slot	10.255.11.153	2/1/Bridge/1	Disabled
Devices	VLAN-Falcon186	10.255.11.186	1/23	Enabled
- Ports	vxTarget_xyz	10.255.11.219	2/1	Enabled
- Spanning Tree	vxTarget_xyz	10.255.11.219	2/2	Enabled
IP Router	vxTarget_xyz	10.255.11.219	2/3	Enabled
IPX Router	vxTarget_xyz	10.255.11.219	2/4	Enabled
- MAC Net Address				
MAC Net Address Custom DHCP DHCP Port DHCP MAC Binding				

### 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. Click here for information about how to define a port rule using this window.

## **Removing a Port Rule**

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

# **Add Port Rules Window**

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

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

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		10.255.11.59			0\$6800-48		6.1.2.12.R02	=	Select All
wTarget 10.255		10.255.11.61			0568	00-24	6.1.2.16.R02		Scient Pill
w/Target		10.255.11.63			0368	00-24	6.1.2.144.R01		Clear All
kite2_97		10.255.11.97		056800-24		6.1.2.150.R01		2000 100	
Kite		10.255.11.112			0568	30-24	6.1.2.144.R01	-	
Available Ports:					- AGE CON	Port Rule	s to be added:		
Device	Sk	tPort/Service/Instance	Port/Service/Instance		Add >> Device		Slot/Port/Service/Instan	ce	
10.255.11.59	1/1		-	22 Donas					
10.255.11.59	1/2			~~ Denno	1952				
10.255.11.59	1/3			Add All	~				
10.255.11.59	1/4			Add Ag	~				
10.255.11.59	1/5			<< Romma	10.0				
10 255 11 59	1/6		-	resilier	o pin				

### Add Port Rules Window

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

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

# **Defining MAC Address Rules**

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

Consider the following when defining a VLAN MAC address rule:

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

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

	🐉 🗠 🍰 😫	MAC	•	
Enterprise Network	MAC Rules (VLAN	l 1(#1))	11/11	388
VLANS	Name	Switch Address	Rule Value	Rule State
- 50 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-0S6648	10.255.11.181	00b0d0:193c68	Enabled
- LIP Router	VLAN-0S6648	10.255.11.181	00b0d0:428259	Enabled
IPX Router بلد	FalconCmm	10.255.11.243	00b0d0:193c68	Enabled
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
- T MAC	ES0001A-1	10.255.211.157	00b0d0:193c68	Enabled
- Net Address	ES0001A-1	10.255.211.157	00b0d0:428259	Enabled
- 😼 VLAN 6(#6)	1		1	
	and the second se			

### MAC Rules Window

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

## **Removing a MAC Address Rule**

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

## **Add MAC Rules Window**

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

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

Add MAC Rules				3
Select Devices for th	e MAC rules			
Name	Address	DNS Name	Type	Version
DCTestnetCore	10.255.10.3		OS7700	5.1.6.86.R02 🔺
💓 Kite_59	10.255.11.59		OS6800-48	6.1.2.12.R02 =
💓 vxTarget	10.255.11.61		OS6800-24	6.1.2.16.R02
💓 vxTarget	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	6.1.2.144.R01
4		1		
Single/Start: :	Add	Single	JStart	End
		Rem	Cle	ar 01

### 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.

Name	Address	DNS Name	Туре		Version	_		
no-name	10.255.13.193		Omni-9W0	C .	4.4.4.165		<b>^</b>	
SW40371	10.255.13.201		OS6648		5.1.6.146.R	02		
no-name	10.255.13.220		0A-512		4.5.2.32			
5052	10.255.13.225		OmniCore	-5	3.3.1r21 - 3	J	l l r	_
DUT-1	10.255.211.68		OS6648		5.1.5.146.R	04		Browse
OmniSwitch	10.255.211.69		OS6624		5.4.1.127.R	01	Ш.	
no-name	10.255.211.70		0S9700		6.1.2.89.R0	1		
vxTarget	10.255.211.71		059700		6.1.1.606.RI	01		
Falcon	10.255.211.75		OS7700		5.4.1.135.R	01		
Kite 76	10.255.211.76		OS6800-4	8	6.1.2.87.R0	1	Ŧ	
nown MAC Addresse	s:			Inc	luded MAC A	ddres	ses:	
MAC Address	Slot/Por	t <u>A</u> dd	>>	E MA	AC Address	Slot	Port	
00d095:12dc8	30 3/5					0.104		1
00d095:12dc8	3a 3/5	<< <u>R</u> er	nove					
00d095:9a078	36 3/2							
00d095:9a078	36 3/5	Add A	Ŵ >>					
00d095:9a078	3/2	C C Dom	II A CLASS					
		- reetti	OA6 WII					
		<u>.</u>						

### Browse MAC Addresses Window

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

7. Select one or more MAC addresses from the Known MAC Addresses list or click on the Add All button to include the entire list in the rule definition. All MAC addresses selected from the Known MAC Addresses list are moved to the Included MAC Addresses list in the Browse MAC Addresses window.

**8.** Click on the **OK** button to return to the Add MAC Rules window. The Browse MAC Addresses window closes and the MAC addresses selected in the Browse MAC Addresses window now appear in the Included MAC Addresses list of the Add MAC Rules window.

**9.** Click on the **OK** button at the bottom of the Add MAC Rules window when you have finished selecting the MAC address(es) for this MAC address rule definition. The Add MAC Rules window closes and a new rule entry appears in the MAC Rules window list with an add icon in the Name field of the new entry.

10. Click the Apply button to create the new MAC address rule(s) on the selected device.

## **Defining Network Address Rules**

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

Consider the following when defining a VLAN network address rule:

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

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

ConniVista 2500 - Application: YLA File Applications View Help	Ns Window:1			
	201	Net Ac	ldress 🔻	<b>a</b>
Enterprise Network	Network Rules	s (VLAN 1(#1))		44 🕲 📾 📰 🎛
9- 🔂 VLANS	Name	Switch Address	Rule Value	Rule State
- 10 VLAN 1(#1)	vxTarget_xyz	10.255.11.219	IP = 3.0.0.0, Mask = 255.0.0.0	Enabled
- Devices	vxTarget_xyz	10.255.11.219	IPX = 1431651653, Encapsulation =	novellraw Enabled
- Ports	FALCON-137	10.255.11.221	IP = 10.255.11.0, Mask = 255.255.25	5.0 Enabled
- Spanning Tree	no-name	10.255.13.220	Protocol = ip. IP = 172.20.0.0. Mask =	255,255.0.0 Enabled
	•		lander Delete	Links
Quarantined/#9)		New	Update Delete Apply	Helb

### Network Rules Window

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

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

## **Add Net Address Rules Window**

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

Kite_59         10.255.11.59         OS6800-48         6.1.2.88.R01           Kite_60         10.255.11.60         OS6800-48         6.1.2.37.R01           wxTarget         10.255.11.61         OS6800-24         6.1.2.82.R01           wxTarget         10.255.11.63         OS6800-24         6.1.2.81.R01           falconCmm         10.255.11.101         OS6800-U24         5.3.1.181.R02           file         Fiber_U24         10.255.11.101         OS6800-U24         5.3.1.181.R02           file         Address         Subnet Mask         Image: Contract	N	lame	Addraee	DNS Name	Type	Varsion
Intersection         Intersection<	kite 6	59	10 255 11 59	Diabitante	056800-48	6 1 2 88 R01
Intervention         Intervention<	Kite P	50	10.255.11.60		086800-48	61237 R01
WTarget         10.255.11.63         OS6800-24         6.1.2.81.R01           falconCmm         10.255.11.100         OS7700         5.1.6.393.R01           Kite_Fiber_U24         10.255.11.101         OS6800-U24         5.3.1.181.R02           IP         Address	wTarc	set.	10.255 11.61		056800-24	61282 R01
fakconCmm         10.255.11.100         087700         5.1.6.393.R01           kite_Fiber_U24         10.255.11.101         086800-U24         5.3.1.181.R02           IP         IP Address	wTare	ret	10.255.11.63		086800-24	6.1.2.81.R01
Kite_Fiber_U24         10.255.11.101         OS6800-U24         5.3.1.181.R02           IP         IP Address	faicon	Cmm	10 255 11 100		087700	516393 R01
IP Address Subnet Mask T	Kite F	iber U24	10.255.11.101		086800-U24	5.3.1.181 R02
		IP Address	8	I		

#### Add Net Address Rules Window

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

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

**1.** Select one or more devices from the list located in the top half of the Add Net Address Rules window. Note that all devices are selected by default.

**2.** Click on **IP** and enter an IP network address (e.g., 172.13.0.0) in the IP Address field and an IP subnet mask (e.g., 255.255.0.0) in the Subnet Mask field.

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

4. Click the Apply button to create the new IP address rule on each VLAN device.

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

**1.** Select one or more devices from the list located in the top half of the Add Net Address Rules window. Note that all devices are selected by default.

2. Click on IPX and enter an IPX network address (e.g., 25040001) in the Network Number field.

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

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

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

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

# **Defining a Custom Rule**

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

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

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



#### Custom Rules Window

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

### **Removing a Custom Rule**

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

# **Add Custom Rules Window**

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

Add Custor	n Rules		2
Select Device	es for the Custom r	ules	
Name	Address	DNS Name	Type
🗑 lanswitch	10.255.211.150		0\$780
4			•

Follow the steps below to create a custom rule:

**1.** Select one or more devices from the list located in the top half of the Add Custom Rules window. Note that all devices are selected by default.

**2.** Enter a number between 0 and 72 in the Offset field to specify the number of bytes into the frame where the pattern (value) is found.

3. Enter a four byte hex value in the Value field to specify a pattern of data (e.g., 60020000).

**4.** Enter a four byte hex value in the Mask field to identify the bytes in the pattern to compare to the frame contents at the offset location. Use "f" in the mask to mark bytes in the pattern to match and "0" to mark bytes in the pattern to ignore (e.g., ffff0000 is the mask for the 60020000 value pattern).

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

6. Click the Apply button to create the new custom rule on each VLAN device.

## **Defining a DHCP Generic Rule**

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

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

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

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

DmniVista 2500 - Application: VL	ANs Window:0		
Eile Applications View Help			
	DHCP	•	<b>a</b>
- 10 Quarantined(#9)	DHCP Generic Rules (VLAN 18(#18))		1/1 🕲 🕾 🛃 🖽
► \$9 VLAN 11(#11)	Name	Switch Address	Rule Value
← 20 VLAN 12(#12)	lanswitch	10.255.211.150	Generic
🗢 월 Vlan 13(#13)			
• \$9 VLAN 14(#14)			
► 20 VLAN 16(#16)			
• 10 VLAN 17(#17)			
9 20 VLAN 18(#18)			
Devices			
- EF Ports			
• Spanning Tree			
- ede IP Houter			
A IPX Router			
Provinces			
Protocol			
E MAC			
That Address			
Cuetara			
E DUCP			
DHCP Port	•		•
- TO DHOP MAC			-
Binding V	New U	pdate Delete Apply Help	
4 P			-

#### 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. Click here for information about how to define a DHCP generic rule using this window.

Consider the following when defining a DHCP generic rule:

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

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

## **Removing a DHCP Generic Address Rule**

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

## **Add DHCP Generic Rules Window**

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

ect Devices	for the DHCP Gener	ic rules		
Name	Address	DNS Name	Type	Version
lanswitch	10.255.211.150		OS7800	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 in the DHCP Generic Rules window list with an add icon in the Name field of the new entry.

3. Click the Apply button to create the new DHCP generic address rule on each of the selected devices.

# **Defining DHCP Port Rules**

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

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

		DHCP Port 🔻	
Enterprise Network	DHCP Port Rules (VLAN	1(#1))	72/72 🔞 🗟 🧮
VLANS	Name	Switch Address	Rule Value
• 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
- 🞝 IPX Router	NMS_HAWK_102	10.255.11.102	1/14
P→ M Rules	NMS_HAWK_102	10.255.11.102	1/15
- S Protocol	NMS_HAWK_102	10.255.11.102	1/16
- 🛒 Port	NMS_HAWK_102	10.255.11.102	1/17
- S MAC	NMS_HAWK_102	10.255.11.102	1/18
- 📑 Net Address	NMS_HAWK_102	10.255.11.102	1/19
- 📑 Custom	NMS_HAWK_102	10.255.11.102	1/2
- B DHCP	NMS_HAWK_102	10.255.11.102	1/20
- Br DHCP Port	NMS_HAWK_102	10.255.11.102	1/21
- B DHCP MAC	NMS_HAWK_102	10.255.11.102	1/22
- Sf Binding	NMS_HAWK_102	10.255.11.102	1/23
- 20 VLAN 2(#2)	AMAG 1144487 100	40.055.44.400	1000
		10	

**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. Click here for information about how to define a DHCP port rule using this window.

Consider the following when defining a DHCP port rule:

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

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

### **Removing a DHCP Port Rule**

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

# **Add DHCP Port Rules Window**

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

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

Name		Address	D	NS Name		Type	Version	_	
DCTestnetCor	8	10.255.10.3			05770	10	5.1.6.86.R02	-	
Kite_59		10.255.11.59			0\$680	10-48	6.1.2.12.R02	-	Select All
💓 w.Target		10.255.11.61			05680	10-24	6.1.2.16.R02		
🛃 vxTarget		10.255.11.63			0\$680	10-24	6.1.2.144.R01		Clear All
kite2_97		10.255.11.97		OSF		10-24	6.1.2.150.R01		
😥 Kite		10.255.11.112			05680	0-24	6.1.2.144.R01	-	
Available Ports:				A.445.5	1	Port Rule	es to be added:		
Device	Sk	tPort/Service/Instance		800 >>		Device	Slot/Port/Service/Instan	ce	
10.255.11.59	1/1			er Donno					
10.255.11.59	1/2			ere Denno	441				
10.255.11.59	1/3			Add All >	0				
10.255.11.59	1/4			Augu Au	-				
10.255.11.59	1/5			<< Roman	10.0				
0.366.11.60	1/6		-	a s i de interne					

### 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.

# **Defining DHCP MAC Address Rules**

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

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

DHCP Mac Rules (V	LAN 2(#2))		81.81 🔞 🥽 🖨 💹 🗄
Name	Switch Address	Rule Value	Rule State
OmniSR153	10.255.11.153	000abc:def001	Enabled
OmniSR153	10.255.11.153	000abc:def002	Enabled
OmniSR153	10.255.11.153	000abc:def003	Enabled
OmniSR153	10.255.11.153	000abc:def004	Enabled
OmniSR153	10.255.11.153	000abc:def005	Enabled
OmniSR153	10.255.11.153	000abc:def006	Enabled
OmniSR153	10.255.11.153	000abc:def007	Enabled
OmniSR153	10.255.11.153	000abc:def008	Enabled
OmniSR153	10.255.11.153	000abc:def009	Enabled
OmniSR153	10.255.11.153	000abc:def00a	Enabled
OmniSR153	10.255.11.153	000abc:def00b	Enabled
OmniSR153	10.255.11.153	000abc:def00c	Enabled
OmniSR153	10.255.11.153	000abc:def00d	Enabled
OmniSR153	10.255.11.153	000abc:def00e	Enabled
OmniSR153	10.255.11.153	000abc:def00f	Enabled
OmniSR153	10.255.11.153	000abc:def010	Enabled
OmniSR153	10.255.11.153	000abc:def011	Enabled
OmniSR153	10.255.11.153	000abc:def012	Enabled
OmniSR153	10.255.11.153	000abc:def013	Enabled
0	40.000 44.400	000-1	Produlant

#### DHCP MAC Rules Panel

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

Consider the following when defining a DHCP MAC address rule:

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

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

## **Removing a DHCP MAC Address Rule**

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

## **Add DHCP MAC Rules Window**

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

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

hlanna		David Minute	<b>T</b>	bite seal and
Name	Address	DNS Name	Type	Version
ter MAC Add	ress	Included MAC A	ddresses	End
d:	: 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	Address	DNS Name	Type	Version		
no-name	10.255.13.193		Omni-9WK	4.4.4.165	-	
SW40371	10.255.13.201		OS6648	5.1.6.146.R	02	
no-name	10.255.13.220		OA-512	4.5.2.32		
5052	10.255.13.225		OmniCore-5	3.3.1r21 - 3	J	_
DUT-1	10.255.211.68		OS6648	5.1.5.146.R	04	Brows
OmniSwitch	10.255.211.69		OS6624	5.4.1.127.R	01	
no-name	10.255.211.70		OS9700	6.1.2.89.R0	1 📃	
w/Target	10.255.211.71		OS9700	6.1.1.606.R	01	
Falcon	10.255.211.75		OS7700	5.4.1.135.R	01	
Kite 76	10.255.211.76		OS6800-48	6.1.2.87.R0	1 -	
wn MAC Addresse	s:		Inc	luded MAC A	ddresses:	
MAC Aridress	SlotiPo	rt <u>A</u> dd	>>	Andress	SintPort	
00d095:12dc8	60 3/5			10 /1001000	0.001 011	
00d095:12dc8	6a 3/5	<< <u>R</u> er	nove			
00d095:9a078	86 3/2					
00d095:9a078	86 3/5	Add A	ή>>			
00d095:9a078	b7 3/2	C Paul	min All			
		rue <u>ini</u>	0/6 //11			
		-	-			

#### Browse MAC Addresses Window

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

7. Select one or more MAC addresses from the Known MAC Addresses list or click on the Add All button to include the entire list in the rule definition. All MAC addresses selected from the Known MAC Addresses list are moved to the Included MAC Addresses list in the Browse MAC Addresses window.

**8.** Click on the **OK** button to return to the Add DHCP MAC Rules window. The Browse MAC Addresses window closes and the MAC addresses selected in the Browse MAC Addresses window now appear in the Included MAC Addresses list of the Add DHCP MAC Rules window.

**9.** Click on the **OK** button at the bottom of the Add DHCP MAC Rules window when you have finished selecting the MAC address(es) for this MAC address rule definition. The Add DHCP MAC Rules window closes and a new rule entry appears in the DHCP MAC Rules window list with an add icon in the Name field of the new entry.

10. Click the Apply button to create the new DHCP MAC address rule(s) on the selected device.

# **Defining Binding Rules**

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

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

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

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

Ninding Rules (VLAN 18	8(#18))	1/1 😒 📼 🖨 💹 🖽
Name	Switch Address	Rule Value
answitch	10.255.211.150	MAC = 0010a4:e508f8, IP = 10.255.215.1
	New Undate	Delete Annh: Heln
	inen Obrace	Scierce White Treeh

### **Binding Rules Panel**

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

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

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

## **Removing a Binding Rule**

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

# **Defining IP-MAC Binding Rule Values**

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

Add Binding Rules Window

and Binding Rules			
Select Devices for the	he Binding rules		
Name	Address	DNS Name	Type
DCTestnetCore	10.255.10.3		087700
🖬 Kite_59	10.255.11.59		OS6800-48
🖬 w.Target	10.255.11.61		OS6800-24
w/Target	10.255.11.63		OS6800-24
kite2_97	10.255.11.97		0\$6800-24
🖌 Kite	10.255.11.112		OS6800-24
∢ Binding Rule Type — ● IP-MAC ○ M	AC-PORT	O MAC-IP-I	PORT
IP-MAC M     IP-MAC M     IP-PORT P Binding Rule Values     MAC Address:	AC-PORT DRT-PROTOCOL	MAC-IP-I MAC-PO Browse.	PORT RT-PROTOCO

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.

Name	Address	DNS Name	Type	Version	
no-name	10.255.13.193		Omni-9WX	4.4.4.165	1 🛋
SW40371	10.255.13.201		OS6648	5.1.6.146.R02	111
no-name	10.255.13.220		0A-512	4.5.2.32	111
5052	10.255.13.225		OmniCore-5	3.3.1r21 - 3 J	
DUT-1	10.255.211.68		OS6648	5.1.5.146.R04	Brows
OmniSwitch	10.255.211.69		OS6624	5.4.1.127.R01	
no-name	10.255.211.70		OS9700	6.1.2.89.R01	
vxTarget	10.255.211.71		0S9700	6.1.1.606.R01	
Falcon	10.255.211.75		OS7700	5.4.1.135.R01	
Kite 76	10.255.211.76		OS6800-48	6.1.2.87.R01	<b>•</b>
own MAC Addresse	s:		Inc	luded MAC Addr	esses:
MAC Address	SlotiPo	d <u>A</u> dd	>>	AC Address SI	ot/Port
00d095:12dcl	60 3/5			No Fiddle of the	
00d095:12dc	6a 3/5	<< <u>Re</u>	move		
00d095:9a07	86 3/2				
00d095:9a07	86 3/5	Add A	ŵ >>		
00d095:9a07	b7 3/2	C Paul	ann All		
1		< ruem	046 101		
		-			

#### Browse MAC Addresses Window

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

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

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

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

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

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

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

# **Defining IP-Port Binding Rule Values**

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

Select Devices	s for the Binding ru	ules		
Name	Address	DNS Name	Туре	Version
📷 lanswitch	10.255.211.150		0\$7800	5.1.6.138.R02
Binding Rule T	ype			
Binding Rule T IP-MAC	VIDE		MAC-IP-F	
Binding Rule T P-MAC P-PORT Binding Rule V	Vpe MAC-PORT PORT-PROT alues	C TOCOL C	MAC-IP-F MAC-POI	PORT RT-PROTOCOL

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.

Select Devices	s for the Binding rul	les		
Name	Address	DNS Name	Туре	Version
lanswitch	10.255.211.150		087800	5.1.6.138.R02
Binding Rule T	ype			
Binding Rule T O IP-MAC	MAC-PORT     ORDER DROTE	0	MAC-IP-P	ORT
Binding Rule Ty O IP-MAC O IP-PORT Binding Rule V	ype MAC-PORT O PORT-PROTO alues	OCOL O	MAC-IP-POR	ORT T-PROTOCOL
Binding Rule Ty P-MAC IP-PORT Binding Rule V MAC Address	NPE MAC-PORT PORT-PROTO alues R :	OCOL O	MAC-IP-P( MAC-POR	ORT T-PROTOCOL

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	Address	DNS Name	Туре	Version		
no-name	10.255.13.193		Omni-9WX	4.4.4.165	-	
SW40371	10.255.13.201		OS6648	5.1.6.146.R	02	
no-name	10.255.13.220		OA-512	4.5.2.32		
5052	10.255.13.225		OmniCore-5	3.3.1r21 - 3	J	_
DUT-1	10.255.211.68		OS6648	5.1.5.146.R	04	Brow
OmniSwitch	10.255.211.69		OS6624	5.4.1.127.R	01	
no-name	10.255.211.70		OS9700	6.1.2.89.R0	1 📃	
w/Target	10.255.211.71		OS9700	6.1.1.606.R	01	
Falcon	10.255.211.75		OS7700	5.4.1.135.R	01	
Kite 76	10.255.211.76		OS6800-48	6.1.2.87.R0	1 💌	
wn MAC Addresse	s:		Inc	luded MAC A	ddresses:	
MAC Address	SlotiPo	d <u>A</u> dd	>>	AC Address	SlotPort	
00d095:12dc8	60 3/5				01001 011	_
00d095:12dc8	6a 3/5	<< <u>Re</u>	nove			
00d095:9a078	3/2	0.44.0				
00d095:9a078	3/5	Add A	ų			
00d095:9a078	b7 3/2	<< Dom	III auto			
11		S TVBIII	046 111			
		-				

#### Browse MAC Addresses Window

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

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

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

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

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

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

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

# **Defining Port-Protocol Binding Rule Values**

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

SIECT DEVICES	for the Binding ru	les			
Name Ianswitch 1	Address 0.255.211.150	DNS Name	Type OS7800	Ve 5.1.6.1	rsion 38.R02
nding Rule Ty	pe				
P-MAC	O MAC-PORT	0	MAC-IP-P	ORT	
P-PORT	PORT-PROT	OCOL O	MAC-POR	T-PRO	TOCOL
nding Rule Va	lues				
Slot/Port:		]			
Protocol Value	s				
• P	O IP-SNAP				
⊖ IPX	O IPX-Novel				
	O Ethernet	Гуре			
O IPX-LLC				0	DSAP)
<ul> <li>IPX-LLC</li> <li>IPX-SNAP</li> </ul>	SAP Head	ler			
<ul> <li>IPX-LLC</li> <li>IPX-SNAP</li> <li>AppleTalk</li> </ul>	SAP Head	ler		0	(SSAP)

### 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.

Name I lanswitch	Address	ules DNS Name	Tyne	
Name Name	Address 0.255.211.150	DNS Name	Type	
			087800	Version 5.1.6.138.R02
3inding Rule Typ	pe			
Binding Rule Typ	O MAC-PORT	r	MAC-I	IP-PORT
Binding Rule Typ O IP-MAC O IP-PORT	O MAC-PORT	T	MAC-I O MAC-I	IP-PORT PORT-PROTOCOL
inding Rule Typ IP-MAC IP-PORT Sinding Rule Val	De O MAC-PORT O PORT-PRO	T DTOCOL	® MAC-I ○ MAC-I	IP-PORT PORT-PROTOCOL
Binding Rule Typ IP-MAC IP-PORT Sinding Rule Val MAC Address:	MAC-PORT PORT-PRO lues	T DTOCOL Brow	MAC-I     MAC-I     MAC-I	IP-PORT PORT-PROTOCOL

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.

Name	Address	DNS Name	Type	Version		
no-name	10.255.13.193		Omni-9WX	4.4.4.165	-	
SW40371	10.255.13.201		OS6648	5.1.6.146.R	02	
no-name	10.255.13.220		OA-512	4.5.2.32		
5052	10.255.13.225		OmniCore-5	3.3.1r21 - 3	J	_
DUT-1	10.255.211.68		OS6648	5.1.5.146.R	04	Brows
OmniSwitch	10.255.211.69		OS6624	5.4.1.127.R	01	
no-name	10.255.211.70		089700	6.1.2.89.R0	1 📃	
vxTarget	10.255.211.71		OS9700	6.1.1.606.R	01	
Falcon	10.255.211.75		087700	5.4.1.135.R	01	
Kite 76	10.255.211.76		OS6800-48	6.1.2.87.R0		
own MAC Addresse	S:		Inc	luded MAC A	ddresses:	
MAC Address	SlotiPo	rt <u>A</u> dd	>>	AC Address	SlotPort	
00d095:12dcf	50 3/5			10 /1001000	0.001 011	
00d095:12dc8	6a 3/5	<< <u>Re</u>	nove			
00d095:9a078	86 3/2					
00d095:9a078	86 3/5	Add A	ή>>			
00d095:9a07t	57 3/2	C Paul	mm All			
1		rue <u>ini</u>	OV8 MII			
		-	-			

#### Browse MAC Addresses Window

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

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

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

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

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

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

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

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

# **Defining MAC-Port-Protocol Binding Rule** Values

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

	Rules				
elect Devices	for the Binding ru	les			
Name	Address 10 255 211 150	DNS Name	Type OS7800	Version	12
inding Rule Ty	/pe				
O IP-MAC	O MAC-POF	स	○ M/	C-IP-PORT	
IP-PORT	O PORT-PR	OTOCOL	M     M	C-PORT-PR	DTOCOL
inding Rule V	alues				
MAC Address	e _ :	Brow	vse		
Slot/Port:		_			
Protocol Valu	es				
● IP	IP-SNA	Р			
🔾 ІРХ	O IPX-No	vell			
	O Ethern	et Type			
○ IPX-LLC	○ SAP He	ader			(DSAP)
IPX-LLC     IPX-SNAP	U DHI H	- Granda			(0.5/11 )
IPX-LLC     IPX-SNAP					(SSAP)
<ul> <li>IPX-LLC</li> <li>IPX-SNAP</li> <li>AppleTalk</li> </ul>	5				

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	Address	DNS Name	Type	Version	
no-name	10.255.13.193		Omni-9WK	4.4.4.165	
SW40371	10.255.13.201		OS6648	5.1.6.146.R0	2
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	5.1.5.146.R0	4 Brow
OmniSwitch	10.255.211.69		OS6624	5.4.1.127.R0	1
no-name	10.255.211.70		OS9700	6.1.2.89.R01	
vxTarget	10.255.211.71		OS9700	6.1.1.606.R0	1
Falcon	10.255.211.75		OS7700	5.4.1.135.R0	1
Kite 76	10.255.211.76		OS6800-48	6.1.2.87.R01	<b>v</b>
wn MAC Addresses	s:	1	Inc	luded MAC Ad	dresses:
MAC Address	SlotiPor	H <u>A</u> dd	>>	Address	SlotPort
00d095:12dc8	30 3/5			01071001000	orour on
00d095:12dc8	3a 3/5	<< <u>R</u> er	move		
00d095:9a078	36 3/2				
00d095:9a078	36 3/5	Add A	ŵ >>		
00d095:9a07t	3/2	C C Dom	ann All		
		- reetti	OVE MIL		
		<u>.</u>	-		

### Browse MAC Addresses Window

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

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

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

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

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

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

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

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

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

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

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

# **Using Port Mobility**

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

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

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

# **Configuring Mobility on AOS Devices**

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

**1.** Enable mobility on the switch ports that you want to designate as mobile ports. When mobility is enabled on a port, the port becomes eligible for dynamic VLAN assignment.

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

**3.** Create VLANs that will receive and forward mobile port traffic. Note that on AOS devices, VLANs do not have a mobile or non-mobile designation, so you do not have to enable mobility on a VLAN. In essence, all VLANs support the mobility feature.

**4.** Define rules for the VLANs created in the previous step. These rules will trigger dynamic assignment of mobile ports to these VLANs when mobile ports receive traffic that matches rule criteria.

### **Enabling/Disabling Port Mobility and Related Parameters**

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

			ACCTOIL M	During Tuble		-
Omni¥ista 2500 - Application: \	LANs Window	N:0			_	
e Applications View Help						
idee D 💿	4 🐉 🕫	<b>å</b>	Mobility	-		4
Enterprise Network	Port Mobili	ty Table		69.69 🐯 🖇	• 8 5 5	
👶 VLANs	Slot/Port	Mobility	Default VLAN Restore	Default VLAN Enable	Ignore BPDU	
Devices	1/1	disable	notApplicable	notApplicable	notApplicable	-
	1/2	disable	notApplicable	notApplicable	notApplicable	
P 10.25910.3	1/3	disable	notApplicable	notApplicable	notApplicable	
🛶 Mobility	1/4	disable	notApplicable	notApplicable	notApplicable	
IP Interfaces	1/5	disable	notApplicable	notApplicable	notApplicable	
🗢 🗑 10.255.11.102	1/6	disable	notApplicable	notApplicable	notApplicable	4
- 🗑 10.255.11.104	1/7	disable	notApplicable	notApplicable	notApplicable	
- 🗑 10.255.11.111	1/8	disable	notApplicable	notApplicable	notApplicable	
- 🗑 10.255.11.113 🔚	1/9	disable	notApplicable	notApplicable	notApplicable	_
- 🗑 10.255.11.114	4					•
	-View Port	Mobility				
10.255.11.110						-
~ 10.255.11.117	Slot/Port:			Mobility:	enable 💌	1
	Dofault M	AN Docto	anabla -	Default M AN Enables	onable -	
	Derault VL	AN RESID	enable	Derduit VLAN Endbie.	enable	
10.255.11.120	lanore BP	DU:	enable 🔻	Authenticate:	enableAvi 🔻	7
	ignore br					
10.255.11.125	Configure	d Default \	/LAN:			
10.255.11.120	-					
2 10.255.11.127			Edit Update	Apply Help		

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

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

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

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

	y ranie							48/48 🐯 🥽	8 7 E
SlotPort	Mobility	Defa	ult VLAN Restore	Default	VLA	N Enable	Ignore BPDU	Authenticate	Configured
1/6	disable	notAp	plicable	notApplic	abl	e	notApplicable	notApplicable	
1/7	disable	notApp	plicable	notApplic	notApplicable notApplicabl		notApplicable	notApplicable	
1/8	disable	notAp	plicable	notApplic	abl	8	notApplicable	notApplicable	
1/9	disable	notAp;	plicable	notApplic	abl	e	notApplicable	notApplicable	
1/10	disable	notAp;	plicable	notApplic	abl	8	notApplicable	notApplicable	
1/11	disable	notAp	plicable	notApplic	abl	е	notApplicable	notApplicable	
1/12	disable	notAp;	plicable	notApplic	abl	e	notApplicable	notApplicable	1
1/13	enable	enabl	8	enable			disable	enable8021x	
1/14	disable	notAp;	plicable	notApplic	abl	е	notApplicable	notApplicable	
1/15	disable	notAp	plicable	notApplic	:abl	8	notApplicable	notApplicable	
• Fdit Port !	Mobility								•
Slot.Port:			1/13			Mobility:		enable	-
Default VL	AN Resto	re:	enable		•	Default \	/LAN Enable:	enable	-
Ignore BPC	DU:		disable			Authenti	cate:	enable8021x	-
Configured	d Default \	VLAN:	1						

#### Edit Port Mobility Panel

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

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

### **Port Mobility AOS Parameters**

#### Slot/Port

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

### Mobility

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

### **Default VLAN Restore**

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

### **Default VLAN Enable**

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

### **Ignore BPDU**

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

### Authenticate

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

### **Configured Default VLAN**

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

# **Configuring Mobility on XOS Devices**

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

1. Enable the Group Mobility feature for the switch. Group Mobility is available on every XOS switch, but is disabled by default. When you enable this feature, the default VLAN 1 automatically becomes a mobile VLAN (Group). As a result, all switch ports in VLAN 1 are now considered mobile ports and are eligible for dynamic VLAN assignment.

**2.** Enable/disable Group Mobility parameters, described below, that globally determine mobile port behavior.

3. Create mobile VLANs that will receive and forward mobile port traffic.

**4.** Define VLAN rules for the mobile VLANs created in the previous step. These rules will trigger dynamic assignment of mobile ports to these VLANs when mobile ports receive traffic that matches rule criteria.

5. Statically assign switch ports to a mobile VLAN.

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

### **Enabling/disabling Group Mobility and Related Parameters**

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



### **Group Mobility XOS Parameters**

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

### **Group Mobility**

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

### Move to Default Group on Aging

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

### **Use Default Group**

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

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

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

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



# **Information Fields in the List**

#### Name

The name of the device.

### Address

The address of the device.

### **DNS Name**

The DNS name of the device.

### 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 autodiscovered, added manually, or edited.) The default Security Groups shipped with OmniVista are as follows:

- **Default** group. This group has read-only access to switches in the list of All Discovered Devices that are configured to grant access to this group.
- Writers group. This group has both read and write access to switches in the list of All Discovered Devices that are configured to grant access to this group. However, members of this group cannot run autodiscovery nor can they manually add, delete, or modify entries in the list of All Discovered Devices.
- Network Administrators group. This group has full administrative access rights to all switches on the network. Members of this group can run autodiscovery and can manually add, delete, and modify entries in the list of All Discovered Devices. Members of this group also have full read and right access to entries in the Audit application and the Control Panel application. Members of this group can do everything EXCEPT make changes to Security Groups.
- Administrators group. This group has all administrative access rights granted to the Network Administrators group AND full administrative rights to make changes to Security Groups.

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

### **Running From**

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

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

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

## Changes

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

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

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

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

### Discovered

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

# **Pop-Up Menu in the List**

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



# Using the Devices Tree

# Displaying the VLAN Configuration for a Device

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

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



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

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

# **Pop-Up Menu in the Tree**

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

# Managing AOS and XOS VLANs by Device

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

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

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

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

Click or	n an individual	device	e to disp	olay a lis	t of V	/LANs	
Í		Device	e VLAN	Definiti	ons -		
🛷 OmniVista 2500 - Application	VLANs Window:0						- [D] X
File Applications View Help							
	10111	10.255.1	0.3 🔻				1
Enterprise Network	VLAN definitions for: 10.3	255.10.3			8/8		
🗢 🙋 VLANs	VLAN ID Descrip	ption	Admin Status	Oper Status	Type	Spanning Tre	e Status
🕈 📆 Devices	1 VLAN 1	1	Enabled	Inactive	Standard	Enabled	
	10 TESTNET SE	RVERS I	Enabled	Active	Standard	Enabled	
	27 VLAN 27		Enabled	Active	Standard	Enabled	
— 🌉 Mobility	50 TESTNET AR	EA 0 VL	Enabled	Active	Standard	Enabled	
IP Interfaces	206 STATIC AUTO	01 206	Enabled	Active	Standard	Enabled	
► ₩ 10.255.11.102	220 DHCP LABS	220	Enabled	Active	Standard	Enabled	
► 10.255.11.118	243 CORPNET C	ONNEC	Enabled	Active	Standard	Enabled	
► ■ 10.255.11.119	550 TESTNET AR	EA 0 D	Enabled	Active	Standard	Enabled	
► 10.255.11.120							
10.255.11.126	•	1					•
► 10.255.11.129							
• 10.255.11.131	View VLAN Definition						
► 10.255.11.148 ► 10.255.11.153	Description:			Admin Status	s: Enab	led	-
10.255.11.157	Oper Status:	Active	-	Туре:	Stan	dard	-
	Spanning Tree Status:	Enabled	-	Mobility:	Enab	oled	-
► ■ 10.255.11.201	Authentication:	Disabled	-	Router-Proto	col: IPAP	х	-
10.255.11.207 10.255.11.218	Voice Status:	Disabled	-				
• 10.255.11.224 • 10.255.11.244 • 10.255.11.252	Ēd	it Up	date Dele	ete Appl	<u>H</u> e	lp	

# **Modifying VLAN Definitions**

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

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

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

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

	Ec	dit VLAN De	efinition	Panel —		
OmniVista 2500 - Application:	VLANs Window:0				-	10
le Applications View Help						
	0 😫 10 🛔 😂	10.255.10.3	-			1
Enterprise Network	1					Tan
P Browse	VLAN definitions for: 10	.255.10.3		8/8 🧟 🗠 🄇		ļļ
🔁 VLANs	VLAN ID D	escription	Admin Status	Oper Status	Type	Ц
Devices	1 VLAN 1		Enabled	Inactive	Standard	4
∲  ∬ (10.0.0.0/8)	10 TESTNET SE	ERVERS VLAN 10	Enabled	Active	Standard	Ц
► 10.255.10.3	27 VLAN 27		Enabled	Active	Standard	Щ
🗢 🚮 10.255.11.102 📑	50 TESTNET AF	REA 0 VLAN 50	Enabled	Active	Standard	Щ
- 💓 10.255.11.104	206 STATIC AUT	01 206	Enabled	Active	Standard	Щ
- 💓 10.255.11.111	220 DHCP LABS	220	Enabled	Active	Standard	4
- 💓 10.255.11.113	4					•
- 💓 10.255.11.114						
- 💓 10.255.11.115	Edit VLAN Definition					
- 10.255.11.116	Description:	VLAN 27	Admin Statu	s: Enabled	-	-
10.255.11.117						5
• M 10.255.11.118	Oper Status:	Active	Type:	Standar	d 🛛 🔻	1
► 10.255.11.119		E				ñ.
• <b>1</b> 0.255.11.120	Spanning Tree Status:	Enabled	MODIIRY:	Enabled	*	
10.255.11.121	Authentication:	Disabled	Router, Prote	ncot:		7
• <u>10.255.11.125</u>		o radinicu	100001-1100			1
10.255.11.126	Voice Status:	Disabled	· ·			
10.255.11.127			_			-
10.255.11.128		OK Can	cel Help			
10.255.11.129			East			
10.255.11.131	5					

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

# **Removing a VLAN**

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

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

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

# **VLAN Parameter Definitions**

## VLAN ID

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

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

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

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

## Description

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

## Admin Status

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

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

### **Oper Status**

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

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

## 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.

### **Spanning Tree Status**

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

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

### Mobility

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

### Authentication

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

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

### **Router Protocol**

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

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

## Voice Status

Not supported for this release.

# Managing OmniStack VLANs by Device

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

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

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

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



# Adding a New VLAN

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

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

# **Modifying VLAN Definitions**

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

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

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

# **Removing a VLAN**

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

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

# VLAN Parameter Definitions

## VLAN ID

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

Valid VLAN ID ranges for supported devices are as follows:

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

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

## Description

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

### **Egress Ports**

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

### **Forbidden Egress Ports**

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

### **Untagged Ports**

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

# Using the dot1qPortVlan Table

The VLAN Bridge MIB (qBridgeMIB) contains the dodt1qPortVlan table that is used to view and configure 802.1Q VLAN attributes for a specific port. As shown below, you can access this table by clicking open an OmniStack switch management IP address in the Devices Tree and then clicking on the Ports node.

		— dot1qP	ort VLAN	Table –	
OmniVista 2500 - Application: VL	ANs Window:0				_10
e Applications View Help					
	10 10 10 10 10 10 10 10 10 10 10 10 10 1	Ports	-		3
► 🙀 10.255 11.61	desta Desta A	Table			
► 10.255 11.63	dot1qPort VLAN	Table		8.8 20 00	O 20 CO U
► ₩ 10.255 11.97	SlotPort VL	4N ID Frame Type	Ingress Filtering	GVRP Status	Failed Registr
• 10.255.11.112	1/1	1 admitAll	false	disabled	
• <b>1</b> 0.25511.119	1/2	1 admitAll	false	disabled	
• 10.25511.120	173	1 adminut	false	disabled	
10.25511.121	1/6	1 admired	folgo	disabled	
10.25511.122	1/8	1 admirAll	false	disabled	
10.255111.123	1/7	1 admitáli	folco	dicabled	
10.255111.120	1/9	1 admital	falea	dicabled	
10.255.11.127	110	1 autorea	laise	ursabled	
- 10.255 11.125					
► D 10 255 11 135					
► 10.255 11.144					
► ■ 10 255 11 148	•				
• M 10.255 11.157	New dot 1 nDo	t VI AN Attributes			
► 10.255 11.189	non nor np o	C TEMTTICI IDUIOD			
► ■ 10.255 11.194	Slot.Port:	1/3	VLAN ID:		1
10.25511.201	Frame Type:	admitAll	- Ingress Filte	ring: false	-
Ports	and the		ange obdit nee		
► 10.255.11.207	GVRP Status:	disabled	<ul> <li>Failed Regis</li> </ul>	trations:	0
► 10.255.11.219	1				
► 10.255.11.221	Last PDU Origi	n: 00000000000000			
► == 10.255.11.224					
• 10,255,11,242		Edit U	pdate Apply	Help	
×					

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

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

origi ori inte	AN Table			8/8	A6 100	
Slot/Port V	'LAN ID	Frame Type	Ingress Filtering	GVRP	Status	Failed Regis
1/1	1	admitAll	false	disable	d	
1/2	1	admitAll	false	disable	d	
1/3	1	admitAll	false	disable	đ	
1/4	1	admitAll	false	disable	d	
1/5	1	admitAll	false	disable	d	
1/6	1	admitAll	false	disable	d	
1/7	1	admitAll	false	disable	d	
171						
1/8	1	admitAll	false	disable	d	
Edit dot1qPo	1 ort VLAN	admitAll II Attributes	false	disable	d	
Edit dot1qPo Slot/Port:	1 ort VLAN 1/	admitAll	faise VLAN ID:	disable	d	1
Edit dot1qPo Slot:Port: Frame Type:	1 ort VLAN 1/ at	admitAll I Attributes 3 ImitAll	false VLAN ID: Tingress Filte	disable	false	1
Edit dot1qPo Slot/Port: Frame Type: GVRP Status	1 ort VLAN 1/ ac c di	admitAll I Attributes 3 ImitAll sabled	false VLAN ID: Ingress Filte Falled Regist	disable	false	1

# Edit dot1qPort VLAN Attributes Panel

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

# **802.1Q VLAN Port Attribute Definitions**

### Slot/Port

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

### VLAN ID

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

#### Frame Type

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

#### **Ingress Filtering**

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

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

### **GVRP Status**

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

### **Failed Registrations**

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

### Last PDU Origin

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

# Using the VLAN Wizard

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

	VLAN Basic Informatio	n -	
	VLAN ID:	158	
	Description:	VLAN 158	
12 10 0	Admin Status:	Enabled	•
	Туре:	Standard	-
P T	Spanning Tree Status:	Enabled	-
	Mobility:	Enabled	-
	Router Protocol:	None	-
	Authentication:	Disabled	-

The VLAN Wizard

# 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.

	100				
VLANID	158				
	186 (10.25	55.211.155)			1
Switche	s: BBH-HZZ	(10.255.211.175)			-
	lanswitch	(10.255.211.150)			5
	OmniSwit	ch (10.255.211.69)			
Ports of	f lanswitch (1	0.255.211.150)		Selected Ports	
	Slot	Port		Slot Port	
	1	1 +			
	1	2			
	1	3			
	1	4			
	1	5			
	1	0	Add>>		
	1	0			
	1	11	<< Bemove		
	1	12		i l	
	1	13	Add All >>		
	1	14	or Domon & All		
	1	15	<< LINITIOAG MIL	1,-	
	1	16			
	1	.17			
	1	18			
	1	19			
e you can assign ports	1	20			
he VLAN. These ports	1	21			
not be moved unless	1	22 💌		2	

## 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 Wizard					×
	VLAN Wizard Ports Selected Devices VLAN ID: 158 186 (1 Switches: NMS	Page 10.255.211.155) 122 (10.255.211.175) ritch (10.255.211.150) 125 (10.255.11.125)			
	Ports of NMS_12	Egress     (10.255.11.125)     Port     1	i 🔾 Forbidden 🤇	Untagged Selected Ports	
		1 2 1 3 1 4 1 5 1 6 1 6	Add>>		
		1 8 1 9 1 10 1 11 1 12	<< Bemove Add All >>    Add All >>    << Remove All		
Here you can assign ports to the VLAN. These ports will not be moved unless you manually change the VLAN assignment of the ports.		1 13 1 14 1 15 1 16 1 17 1 18 ▼ <back next<="" td=""><td>&gt; Einish</td><td>Cancel Help</td><td></td></back>	> Einish	Cancel Help	

# Selecting OmniStack Ports for the VLAN

Click the Next button when you have made your selections

# **Configuring XOS Router Interfaces**

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

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

	VLAN Wizard XOS Ro Selected Devices 186 (10.) Switches:	uting Page 255.211.155)				
	IP IP Routing Param	eters			0000	
	Subnet Mask:	255.0.0.0	14	Description:	0.00	-
	Framing Type:	Ethernet-2	-	RIP Mode:	Silent	-
	PX Routing Parar Routing Protocol:	RIP Only	•	IPX Address:	400169	
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 is the NA Each exists in						

## 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)
- o 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
- o Ethernet 802.3 snap
- Ethernet 802.3 raw
- o FDDI-snap
- FDDI-snap sr (Source Routing)
- o FDDI-llc
- FDDI-llc-sr (Source Routing)
- o 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 (Release 6.1.1) switches. You can only configure one (1) IP interface on 6600 XOS devices.

VLAN Wizard	
	VLAN Wizard AOS IP Routing Page Selected Devices BBH-H22 (10.255.211.175) lanswitch (10.255.211.150) OmniSwitch (10.255.211.69) vxTarget (10.255.211.71)
	P     P     P     Routing     Router IP Address     Router IP Mask     IP Encapsulation     IP
	View IP Router  IP Routing Parameters  Router IP Mask:  IP Encapsulation:  Interface Name:  IP Forwarding:  IP Forwarding:  IP Forwarding:  IP Forwarding:  IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding: IP Forwarding:
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.	New Edit Delete

## Configuring AOS IP Router Interfaces

**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 AOS I Selected Devices BBH-H lansw OmniS vxTar	IPX Routing Page 122 (10.255.211.175 ritch (10.255.211.15 Switch (10.255.211.3 get (10.255.211.71)	) D) 59)		
	-IPX Routing Par IPX Address: RIP/SAP Mode:	RIP Only	IPX Encapsulation: Delay Ticks:	Ethernet 2	
o traffic can ever move stween VLAN's except rough routing. Routing on be achieved by using e external router or by eating a virtual router port the VLAN. Each switch in e Group can have its own					

## 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)
- o LLC (802.2)
- o SNAP
- Not Applicable.

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

c. Set the RIP/SAP Mode field to one of the following values:

- **RIP Only** (RIP updates are processed)
- **RIP** and **SAP** (RIP and SAP updates are processed)
- Triggered (RIP and SAP updates are broadcast only when updates occur)
- Inactive( RIP and SAP updates are not processed, router interface remains active)
- Not Applicable.

**d.** Enter a 16-bit value (**0-65535**) in the **Delay Ticks** field to specify the number of ticks for the IPX delay time. A tick is approximately 1/18th of a second.

3. Select additional switches in the Switches area and configure IP router interfaces as desired.

Click the **Next** button when all desired switches have been configured

# **Configuring Port Rules**

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

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

	Protocol	Net A	ddress	DHCP	Cu	istom	Bindin	g Sum	mary		
	Port		MAC A	ddress	diantes	r	DHCPI	Port	r	DHCP MAC	Address
	Nan	ne		Address		DNS	Name	Туре	100	Version	1
	OmniS	witch	10.25	5.211.69	-			OS6624	5.4	1.1.163.R01	
	by wTarge	et	10.25	5.211.71				089700	6.1	1.632.R01	Select All
	In lanswit	tch	10.25	5.211.150	r i			087800	5.1	.6.146.R02	Delect Ma
	186		10.25	5.211.155				08-4024	4.5	2.59	Clear All
	BBH-H	22	10.25	5.211.175				OS6648	5.1	.6.138.R02	
	Available I	Ports:				1		1	Port Ru	des to be adde	d:
	Devic	- 0	SlotiPo	rtiRonica	ln-	1		1	Device	SlotiPortige	nicalnotonca
	10 255 21	1.150	1/1	100citiec					Dence	01000101000	TAILENINGTON
	10.255.21	1.150	1/2								
	10 266 21	1 160	1/2		- 1						
	1 10 2 2 2 3 3 . 2										
	10.255.21	1,150	1/4								
	10.255.21	1.150	1/4			-	Add>:				
	10.255.21 10.255.21 10.255.21 10.255.21	1.150 1.150 1.150	1/4 1/5 1/6				Add >:				
	10.255.21 10.255.21 10.255.21 10.255.21 10.255.21	1.150 1.150 1.150 1.150 1.150	1/4 1/5 1/6 1/7		_		Add >: << Renu	>			
	10 255 21 10 255 21 10 255 21 10 255 21 10 255 21 10 255 21	1.150 1.150 1.150 1.150 1.150 1.150	1/4 1/5 1/6 1/7 1/8		-		Add >: << Berno	>			
	10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21 10.255.21	1.150 1.150 1.150 1.150 1.150 1.150 1.150	1/4 1/5 1/6 1/7 1/8 1/11		_		Add >: << Benn Add All	> 7/10			
	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	1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150	1/4 1/5 1/6 1/7 1/8 1/11 1/12				Add >: << Benn Add All :	>>>			
	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	1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150	1/4 1/5 1/6 1/7 1/8 1/11 1/12 1/13				Add >: << Berno Add All : Remov	>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>			
	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	1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150	1/4 1/5 1/6 1/7 1/8 1/11 1/12 1/13 1/14				Add >: << Berno Add All : Remov	> we >>			
you can define rules	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	1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150	1/4 1/5 1/6 1/7 1/8 1/11 1/12 1/13 1/14 1/15				Add >: << Benn Add All < Remov	> we >>			
you can define rules rt, by MAC Address, by	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	1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150	1/4 1/5 1/6 1/7 1/8 1/11 1/12 1/13 1/14 1/15 1/16				Add >: << Berno Add All : Remov	> >ve >> ve All			
you can define rules rt, by MAC Address, by col, and by network	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	1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150	1/4 1/5 1/6 1/7 1/7 1/8 1/11 1/12 1/13 1/14 1/15 1/16 1/17				Add >: << Berno Add All : Remov	> >ve >> ve All			
you can define rules rt, by MAC Address, by col, and by network ess. You can define pla outer for a VI AN A	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	1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150	1/4 1/4 1/5 1/6 1/7 1/8 1/11 1/12 1/13 1/14 1/15 1/16 1/17 1/18			¢	Add >: << Berno Add All : Remov	> ove >> re All			
you can define rules rt, by MAC Address, by icol, and by network ess. You can define ple rules for a VLAN. A se device is included in	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	1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150 1.150	1/4 1/4 1/5 1/6 1/7 1/8 1/11 1/12 1/13 1/14 1/15 1/16 1/17 1/18			Č	Add >: << Berno Add All : Remov	>>> ve 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 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.

VLAN Wizard	and the second se						
	Rules Config	guration					
	Protocol	Net Address	DHCP	Custom	Binding	Summary	1
AP	Port	MACA	Address		DHCP Port	- P	DHCP MAC Address
	Protocol R	ules					55 🐨 🖨 💷 🗄
Ker ()		Name			Switch Addr	ess	Rule Value
	Comnis	Pwitch		10.255.21	1.69		Protocol = IP E2
	to wTarg	et		10.255.21	1.71		Protocol = IP E2
	4 lanswi	tch		10.255.21	1.150		Protocol = IP E2
	Lo 186			10.255.21	1.155		Protocol = IP
	BBH-H	22		10.255.21	1.175		Protocol = IP E2
ere you can define rules y port, by MAC Address, by							
ere you can define rules y port, by MAC Address, by otocol, and by network birnes. You can define	4						,
ere you can define rules / port, by MAC Address, by otocol, and by network ldress. You can define utiple rules for a VLAN. A /rt or device is included in VLAN if it matches any worke. Refere				Nev	<b>D</b> ole	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.

Add Protocol Rul	25		2
Select Devices for	the Protocol rules	-	
Name	Address	DNS Name	Type
DCTestnetCore	10.255.10.3		OS7700 -
Kite_59	10.255.11.59		OS6800-41-
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		r de dus
● IP ○ ○ IPX ○ ○ IPX-LLC ○	IP-SNAP IPX-Novell Ethernet Type		
• IP 0 0 IPX 0 0 IPX-LLC 0 0 IPX-SNAP 0	IP-SNAP IPX-Novell Ethernet Type SAP Header		Tano (DSAP)
<ul> <li>IP</li> <li>IPX</li> <li>IPX-LLC</li> <li>IPX-SNAP</li> <li>AppleTalk</li> </ul>	IP-SNAP IPX-Novell Ethernet Type SAP Header		0 (DSAP)

Click on one of the following protocol types displayed in this window:

- IP (Ethernet II, ARP, and SNAP)
- IPX (Ethernet II, Novell 802.3, LLC 802.2, and SNAP)
- AppleTalk (Data Delivery Protocol and AppleTalk ARP)
- DECNet (DECNet Phase IV--only captures frames with 6003 Ethernet type)
- Ethernet Type (A two byte hex value between 0x600 and 0xffff that defines an Ethernet type. This value is required for the Ethernet Type field when this protocol type is selected.)
- SAP Header (A one byte hex value between 0x00 and 0xff that defines DSAP and SSAP header values. These values are required for the DSAP and SSAP fields when this protocol type is selected.)
- SNAP Type (A two byte hex value between 0x600 and 0xffff that defines a Sub-network Access Protocol. This value is required for the SNAP Type field when this protocol type is selected.)

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

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

# **Removing a Protocol Rule**

To remove a protocol rule definition, select one or more rules from the Protocol Rules tab and click the **Delete** button. The selected protocol rules are deleted.

Do not click the Next button until all desired rules have been configured

# **Configuring MAC Address Rules**

The MAC Address Tab enables you to configure MAC address rules for the VLAN. MAC Address Rules capture frames that contain a source MAC address that matches the MAC address specified in the rule. The mobile port that receives this matching traffic is dynamically assigned to the rule's VLAN. Consider the following when defining a VLAN MAC Address Rule:

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

Protocol	Net Address DHCP	Custom Binding Summary	
Port	MAC Address	DHCP Port	DHCP MAC Address
MAC Rule			20:20 😪 🛸 🖨
Ker S	Name	Switch Address	Rule Value
🕹 Omni	Switch	10.255.211.69	00005e:000101
Comni	Switch	10.255.211.69	000bdb:87efd9
Comni	Switch	10.255.211.69	000cf1:89f603
Comni	Switch	10.255.211.69	0010a4:e66d1e
- wTan	et	10.255.211.71	00005e:000101
40 wTar	et	10.255.211.71	000bdb:87efd9
↓o wTar	et	10.255.211.71	000cf1:89f603
⊷ wTar	et	10.255.211.71	0010a4:e66d1e
+o lansw	tch	10.255.211.150	00005e:000101
<ul> <li>Jansw</li> </ul>	tch	10.255.211.150	000bdb:87efd9
40 lansw	tch	10.255.211.150	000cf1:89f603
4 lansw	tch	10.255.211.150	0010a4:e66d1e
186		10.255.211.155	00005e:000101
↓ 186		10.255.211.155	000bdb:87efd9
Lo 186		10.255.211.155	E03168: 11000
Lo 186		10.255.211.155	0010a4:e66d1e
40 BBH-	122	10.255.211.175	00005e:000101
A BBH-	122	10.255 211.175	000bdb:87efd9
Co BBH-	122	10.255.211.175	000cf1:89f603
BBH-I	122	10.255.211.175	0010a4:e66d1e
ess, by			
k 4		-12	
ine			
AN. A		> New Delete	
ted in		Tour Francis	
any			

# 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 th	te MAC rules			
Name	Address	DNS Name	Type	Version
DCTestnetCore	10.255.10.3		OS7700	5.1.6.86.R02 A
😿 Kite_59	10.255.11.59		OS6800-48	6.1.2.12.R02 =
💓 vxTarget	10.255.11.61		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	6.1.2.144.R0
ĩ		1		•
ind: :	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.
Name	Ad	dress	DNS Name	Туре		Version			
no-name	10.255	613.193		Omni-9W	x	4.4.4.165		<b>_</b>	
SW40371	10.255	5.13.201		OS6648		5.1.6.146.R	02		
no-name	10.255	5.13.220		0A-512		4.5.2.32			
5052	10.255	5.13.225		OmniCore	3-5	3.3.1r21 - 3	J	l l r	_
DUT-1	10.255	5.211.68		OS6648		5.1.5.146.R	04		Brows
OmniSwitch	10.255	5.211.69		OS6624		5.4.1.127.R	01	Ш.	
no-name	10.255	5.211.70		OS9700		6.1.2.89.R0	1		
vxTarget	10.255	5.211.71		0S9700		6.1.1.606.R	01		
Falcon	10.255	5.211.75		OS7700		5.4.1.135.R	01	Ц.	
Kite 76	10.255	211.76		OS6800-4	8	6.1.2.87.R0	1	Ŧ	
own MAC Address	es:				Inc	luded MAC A	ddres	ses:	
MAC Address	_	SlotiPort	Add	>>	M	AC Address	Sint	Port	
00d095:12d	c60	3/5				10 /1001000	0.100	1 011	1
00d095:12d	c6a	3/5	<< <u>R</u> er	nove					
00d095:9a0	786	3/2							
00d095:9a0	786	3/5	Add A	ή>>					
00d095:9a0	7b7	3/2	C Pana	II de cuero					
		•	- ruetti	0/6 //11					

#### Browse MAC Addresses Window

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

7. Select one or more MAC addresses from the Known MAC Addresses list or click on the Add All button to include the entire list in the rule definition. All MAC addresses selected from the Known MAC Addresses list are moved to the Included MAC Addresses list in the Browse MAC Addresses window.

**8.** Click on the **OK** button to return to the Add MAC Rules window. The Browse MAC Addresses window closes and the MAC addresses selected in the Browse MAC Addresses window now appear in the Included MAC Addresses list of the Add MAC Rules window.

**9.** Click on the **OK** button at the bottom of the Add MAC Rules window when you have finished selecting the MAC address(es) for this MAC address rule definition. The Add MAC Rules window closes and a new rule entry appears in the MAC Rules window list with an add icon in the Name field of the new entry.

## **Removing a MAC Address Rule**

To remove a MAC address rule definition, select one or more rules from the MAC Rules window list and click the **Delete** button. The selected MAC address rules are deleted.

# **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.

	Rules Configura	ation							
	Protocol N	et Addre	ss Di	ICP	Custom	Bindir	g Sumn	nary	
P	Port	M	AC Addr	ess		DHCP	Port	DHCP MA	C Address
	Name		Addr	ess	DN	S Name	Type	Version	1
	OmniSwib	ch 10	0.255.21	1.69			OS6624	5.4.1.163.R01	1.0
	w/Target	10	0.255.21	1.71			089700	6.1.1.632.R01	Select All
	lanswitch	10	0.255.21	1.150			OS7800	5.1.6.146.R02	Descerva
	186	10	0.255.21	1.155			08-4024	4.5.2.59	Clear All
百月	BBH-H22	10.255.211.175			08		5.1.6.138.R02		
	Available Dec	4.00			-			art Dular to be add	Indt
	Available Por	ts:			_		1	ort rules to be add	ea:
	Device	Slo	ot/Port/Se	rvice/In			1	Device Slot/Port/S	Service/Instance
	10.255.211.1	50 1/1	2503.000	000003	*				
	10.255.211.1	50 1/2	_						
	10.255.211.1	50 1/3							
	10.255.211.1	50 1/4							
	10.255.211.1	50 1/5	_			Add>:			
	10.255.211.1	50 1/6							
	10.255.211.1	50 1/7				<< Benn	We Sve		
	10.255.211.1	50 1/8							
	10.255.211.1	50 1/11				Add All	>>		
	10.255.211.1	50 1/12	2						
	10.255.211.1	50 1/13	}			<< Remov	e All		
unu can define rules	10.255.211.1	50 1/14	1						
the MAC Address Inc	10.255.211.1	50 1/15	5		1				
n, by mac address, by	10.255.211.1	50 1/16	5		1				
col, and by network	10.255.211.1	50 1/17	7						
ess. Tou can deline	10.255.211.1	50 1/18	3		1				
derdes for a VLAN. A			- 1		-				
device is included in	1		_		laid)				
IN I II ITLATITUES AND	-								
and a Render cone balance	0.1								

### **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.

# **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.

	runea coning						
	Protocol	Net Address	DHCP	Custom	Binding	Summary	n An an an Anna Anna Anna Anna Anna Anna
P	Port	MACA	Address	r	DHCP Port		DHCP MAC Address
	Add DHCP	MAC Rules					10/10 🐨 🖨 🛃
Ker S		Name			Switch Add	ress	Rule Value
and the first	ComniS	witch		10.255.21	1.69		00005e:000101
N. N. P.	Comnis	witch		10.255.21	1.69		000bdb:87c2aa
28 18	40 wTarge	et		10.255.21	1.71		00005e:000101
	4 wTarge	ət		10.255.21	1.71		000bdb:87c2aa
	4 lanswit	tch		10.255.21	1.150		00005e:000101
11	40 lanswit	tch		10,255.21	1.150		000bdb:87c2aa
	Lo 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:87c2aa
can define rules / MAC Address, by and by network	BBH-H	22		10.255.21	1.175		000bdb:87c2aa

#### 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.

select Devices	TOT the MAC fulles			
Name	Address	DNS Name	Type	Version
Ianswitch	10.255.211.150		087800	5.1.6.138.R02
Enter MAC Add	iress	Included MAC A Single	ddresses -	End
nd: [	: 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	Address	DNS Name	Type	Version	
no-name	10.255.13.193		Omni-9WK	4.4.4.165	-
SW40371	10.255.13.201		OS6648	5.1.6.146.R02	111
no-name	10.255.13.220		OA-512	4.5.2.32	
5052	10.255.13.225		OmniCore-5	3.3.1r21 - 3 J	
DUT-1	10.255.211.68		OS6648	5.1.5.146.R04	Brows
OmniSwitch	10.255.211.69		OS6624	5.4.1.127.R01	
no-name	10.255.211.70		OS9700	6.1.2.89.R01	
vxTarget	10.255.211.71		059700	6.1.1.606.R01	
Falcon	10.255.211.75		OS7700	5.4.1.135.R01	
Kite 76	10.255.211.76		OS6800-48	6.1.2.87.R01	<b>v</b>
own MAC Addresse	s:	_	Inc	luded MAC Add	resses:
MAC Address	SlotiPo	et <u>A</u> dd	>>	AC Address S	IntPort
00d095:12dcf	60 3/5			1071001000	
00d095:12dc8	6a 3/5	<< <u>R</u> er	nove		
00d095:9a078	86 3/2				
00d095:9a078	86 3/5	Add A	ή>>		
00d095:9a078	57 3/2	Ce Dam	min All		
		> restriction	0/6 //11		
		-	-		

#### Browse MAC Addresses Window

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

7. Select one or more MAC addresses from the Known MAC Addresses list or click on the Add All button to include the entire list in the rule definition. All MAC addresses selected from the Known MAC Addresses list are moved to the Included MAC Addresses list in the Browse MAC Addresses window.

**8.** Click on the **OK** button to return to the Add DHCP MAC Rules window. The Browse MAC Addresses window closes and the MAC addresses selected in the Browse MAC Addresses window now appear in the Included MAC Addresses list of the Add DHCP MAC Rules window.

**9.** Click on the **OK** button at the bottom of the Add DHCP MAC Rules window when you have finished selecting the MAC address(es) for this MAC address rule definition. The Add DHCP MAC Rules window closes and a new rule entry appears in the DHCP MAC Rules tab with an add icon in the Name field of the new entry.

# **Removing a DHCP MAC Address Rule**

To remove a DHCP MAC Address Rule, select one or more rules listed on the DHCP MAC Rules Tab and click the **Delete** button. The selected DHCP MAC Address Rules are deleted.

# **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.

Certificaru								
	Rules Configu	uration						
	Protocol	Net Address	DHCP	Custom	Binding	Summary		
4 1	Port	MACA	ddress		DHCP Port		DHCP MAC Addr	ess
	Network Ru	les					5.5 🔞 💿	8
	Nam	ne Swi	tch Addre:	88		Rule Value		Rule Sta
	🖧 OmniSv	witch 10.25	5.211.69	IP = 10	.255.16.172	, Mask = 255.0	0.0.0	Enabled
	👍 vxTarge	t 10.25	5.211.71	IP = 10	.255.16.172	, Mask= 255.0	0.0.0	Enabled
	💫 lanswite	ch 10.25	5.211.150	IP = 10	.255.16.172	, Mask = 255.0	0.0.0	Enabled
	🖧 186	10.25	5.211.155	Protoc	ol = IP, IP = 1	0.255.16.172,	Mask= 255.0.0.0	Enabled
	BBH-H2	22 10.25	5.211.175	IP = 10	.255.16.172	Mask = 255.0	0.0.0	Enabled
Here you can define rules by port, by MAC Address, by profeced and by network								
address. You can define						_		
port or device is included in a VLAN if it matches any				Nev	Dele	te		
one rule. Ports can belong to more than one VLAN.		< 8	ack	Ne <u>x</u> t >	Einish	Cancel	Help	

### 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.

				-	
N	ame	Address	DNS Name	Туре	Version
kite_5	9	10.255.11.59		OS6800-48	6.1.2.88.R01
<ite_6< td=""><td>0</td><td>10.255.11.60</td><td></td><td>086800-48</td><td>6.1.2.37.R01</td></ite_6<>	0	10.255.11.60		086800-48	6.1.2.37.R01
<b>x</b> Targ	et	10.255.11.61		OS6800-24	6.1.2.82.R01
o:Targ	et	10.255.11.63		086800-24	6.1.2.81.R01
alcon	Cmm	10.255.11.100		087700	5.1.6.393.R01
kite_Fi	iber_U24	10.255.11.101		OS6800-U24	5.3.1.181.R02
IP .					
IP	Subnet Ma	lumber			
IP	Subnet Ma Network N Encapsula	ask lumber ition	2 💌	A. T	

#### Add Net Address Rules Window

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

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

**1.** Click on **IP** and enter an IP network address (e.g., 172.13.0.0) in the IP Address field and an IP subnet mask (e.g., 255.255.0.0) in the Subnet Mask field.

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

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

1. Click on IPX and enter an IPX network address (e.g., 25040001) in the Network Number field.

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

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

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

# **Removing a Network Address Rule**

To remove a network address rule definition, select one or more rules from the Net Address tab and click the **Delete** button. The selected network address rules are deleted.

# **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.) 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 Config	juration						
	Protocol	Net Address	DHCP	Custom	Binding	Summary		
RA	Port	MAC	Address		DHCP Port	- P	DHCP MAC Address	
	DHCP Rule	s					44 3 8 8 9	
		Name			Switch A	ddress	Rule Value	
	Comnis	Switch		10.255.2	211.69		Generic	
1 N	wTarg	et		10.255.2	211.71	Generic		
	<li>lanswi</li>	ch 10.255.211.150				Generic		
	BBH-H	122		10.255.3	211.175		Generic	
port, by MAC Address, by								
port, by MAC Address, by tocol, and by network fress. You can define ftiple rules for a VLAN. A t or device is included in	•			Nev	V Dele	rto	Þ	

### 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.

rules DNS Name	OS7800	Version 5.1.6.138.R02
DNS Name	OS7800	Version 5.1.6.138.R02
	OS7800	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.

# **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 Coning	guración						
	Protocol	Net Address	s DHCP	Custom	Binding	Summary		
	Port	MA	C Address		DHCP Port		DHCP MAC Add	ress
	Custom R	ules					55 😪 👘	A
	Na	me !	Switch Addra	ess		Rule Value	2	Rule S
	Comnis	Switch 10.	255.211.69	Offse	t= 0, Value =	0x60020000.	Mask = 0xfm0000	Enabled
	46 w/Targ	et 10.	255.211.71	Offse	t= 0, Value =	0x60020000	Mask = 0x110000	Enabled
	answ	itch 10.	255.211.15	0 Offse	t= 0, Value =	0x60020000,	Mask= 0xff0000	Enabled
	Lo 186	10.	255.211.15	5 Offse	t=0, Value=	0x60020000,	Mask = 0x1110000	Enabled
	A BBH-H	122 10.	255.211.17	5 Offse	t=0, Value=	0x60020000,	Mask = 0x110000	Enabled
re you can define rules port, by MAC Address, by								
re you can define rules port, by MAC Address, by tlocol, and by network tress. You can define	4							Þ
e you can define rules port, by MAC Address, by tocol, and by network lress. You can define tiple rules for a VLAN. A t or device is included in LAN if it matches any	4			Ne	W Dele	te		

## 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 Cus	stom	Rules		2
Select De	vices	s for the Custom r	ules	
Name		Address	DNS Name	Туре
🗑 lansw	itch	10.255.211.150		0\$7800
1		п		•
۲ Mīset:		I	÷	•
Iffset:			A V	•

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.

# **Configuring Binding Rules**

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

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

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

VLAN Wizard								
	Rules Confi	guration						
	Protocol	Net Addre	SS DHCP	Custor	Binding	Summary		
AP	Port	M	C Address	r	DHCP Por	1	DHCP MAC Add	ress
	Binding B	des					55 3 3	AUUR
KEN 1	Na	me	Switch &ddro	0 C		Rule Volue	Provi de Line	Rule Sta
	Comnis	Switch 10	255,211,69	MAC	= 000393:111	b60, IP = 10.25	5.18.132	Enabled
	4% w/Taro	iet 10	255,211,71	MAC	= 000393:111	b60, IP = 10.25	5.18.132	Enabled
	4 lansw	itch 10	255.211.150	MAC	= 000393:111	b60, IP = 10.25	5.18.132	Enabled
	40 186	10	255.211.155	MAC	IP - MAC = 00	0393:111660	e = 10.255.18.132	Enabled
	46 BBH-H	122 10	255.211.175	MAC	= 000393:111	b60, IP = 10.25	5.18.132	Enabled
lere you can define rules								
ly port, by MAC Address, by vrotocol, and by network	4							1.1.1
ddress. You can define nultiple rules for a VLAN. A ort or device is included in VLAN if it matches any				- 1	ew De	ete		
one rule. Ports can belong to more than one VLAN.			< Back	Ne <u>x</u> t >	Einish	Cancel	Help	

## **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:

• IP-MAC

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

**Note:** When you apply a rule to a group of devices in a VLAN, OmniVista displays a dialog box listing any devices that do not support the rule, if applicable. Those devices that do support the rule are updated.

# **Removing a Binding Rule**

To remove a Binding Rule definition, select one or more rules on the Binding Rules Tab and click the **Delete** button. The selected Binding Rules are deleted.

# **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.

	Rules Configuratio	n			
	Protocol Net	Address DHCP	Custom B	nding Summary	
A	Port	MAC Address	DH	ICP Port	DHCP MAC Address
	Rules Summary				54/54 🥵 🕾 🖨 🛄
	Name	Switch Address	Rule Type	R	ule Value
	ComniSwitch	10 255 211 89	MAC	00005e 000101	
	42 OmniSwitch	10.255.211.69	MAC	000bdb:87efd9	
	ComniSwitch	10.255.211.69	MAC	000cft 89f603	
	42 OmniSwitch	10.255.211.69	MAC	0010a4;e66d1e	
	4) OmniSwitch	10.255.211.69	DHCP-MAC	00005e:000101	
	ComniSwitch	10.255.211.69	DHCP-MAC	000bdb:87c2aa	
	ComniSwitch	10.255.211.69	Protocol	Protocol = IP E2	
	ComniSwitch	10.255.211.69	IP	IP = 10.255.16.172, M	ask = 255.0.0.0
	ComniSwitch	10.255.211.69	DHCP-Generic	Generic	
	ComniSwitch	10.255.211.69	Custom	Offset = 0, Value = 0x	0020000, Mask = 0xm0000
	ComniSwitch	10.255.211.89	MAC-IP	MAC = 000393:111b6	0, IP = 10.255.18.132
	↓ wTarget	10.255.211.71	MAC	00005e:000101	
	WTarget	10.255.211.71	MAC	000bdb:87efd9	
	io wTarget	10.255.211.71	MAC	000cf1:89f603	
	↓ wTarget	10.255.211.71	MAC	0010a4:e66d1e	
	↓ wTarget	10.255.211.71	DHCP-MAC	00005e:000101	
	↓ wTarget	10.255.211.71	DHCP-MAC	000bdb:87c2aa	
	WTarget	10.255.211.71	Protocol	Protocol = IP E2	
	↓ wTarget	10.255.211.71	IP	IP = 10.255.16.172, M	ask = 255.0.0.0
you can define rules	A voltarget	10.255.211.71	DHCP-Generic	Generic	
rt, by MAC Address, by	A wTarget	10.255.211.71	Custom	Offset = 0, Value = 0x	0020000, Mask = 0xfff0000
col, and by network	↓ w(Target	10.255.211.71	MAC-IP	MAC = 000393:111b6	0, IP = 10.255.18.132
ss. You can define	<ul> <li>Ianswitch</li> </ul>	10.255.211.150	MAC	00005e:000101	
A MA BLE THE THE THE					•

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 Page VLAN Description						
	Id :	158	Description :	VLAN 158	-1		
1 Th	Admin Status :	Enabled	Mode :	Standard			
<u> </u>	Spanning tree :	Enabled	Mobility :	Enabled			
-100	Authentication :	Disabled	Router Protocol :	IP			
	Switch	r	P Routing	IPX Routing			
	186 (10.255.211.155)		nabled, 0.0.0.0	Enabled, 4001690d			
	BBH-H22 (10.255.211.175)		.5.5.1, Engineering	Disabled			
	,						
	lanswitch (10.255.211.15	50) 5	5.5.16, Accounting	Disabled	_		
	lanswitch (10.255.211.15 OmniSwitch (10.255.211	50) 5 69) 5	5.5.16, Accounting 5.5.23, Tech Pubs	Disabled Disabled			
	lanswitch (10.255.211.1) OmniSwitch (10.255.211 vxTarget (10.255.211.7)	50) 5 1.69) 5 ) 5	5.5.16, Accounting 5.5.23, Tech Pubs 5.5.34, Test	Disabled Disabled Disabled			