

InterVLAN Routing

Establishing Communication Between VLANs

This Configuration Guide explains the concepts behind interVLAN routing using your ProCurve Secure Router Operating System (SROS) product. For detailed information regarding specific command syntax, refer to the *SROS Command Line Interface Reference Guide* on your *ProCurve SROS Documentation CD*.

This guide consists of the following sections:

- *Understanding VLANs* on page 2
- *Understanding InterVLAN Routing* on page 3
- *Configuring InterVLAN Routing* on page 4

Understanding VLANs

A VLAN (virtual local area network) allows creation of logical subnetworks, broadening your ability to segment your network in ways independent of the physical setup. VLANs have all the same attributes as traditional physical LANs, but allow network devices to be grouped together based on organizational function and application rather than be constrained by geographical or physical location. By creating VLANs, your switched network can consist of multiple segments, each with its own separate broadcast and multicast domains. You can set up VLANs either statically (where each switch interface is assigned specifically to a VLAN) or dynamically (based on MAC addresses).

Incorporating VLANs into a typical network provides benefits including security, broadcast or congestion control, and management. Through the use of VLANs, users can be isolated from one another; that is, a user in one VLAN cannot access data in a different VLAN. Also, just as switches isolate collision domains, VLANs isolate broadcast (messages sent to all users) and multicast (messages sent to some users) domains. By preventing broadcast and multicast traffic from traversing the entire network, network performance improves. Additionally, VLANs can be thought of as a limited broadcast domain. This means that all members of a VLAN receive broadcast packets that are sent by members of the same VLAN. This logical grouping of users allows easier network management. A network administrator can easily move an individual from one group to another without having to recable the network.

VLANs can span multiple switches. For example, you could have Ports 1 through 10 of Switch A assigned to VLAN 100, and Ports 11 through 20 of Switch A assigned to VLAN 200. If Switch A and Switch B share a high-speed link, then Switch B could also have ports assigned to the same VLANs as Switch A. See Figure 1 for a graphical depiction of this concept.

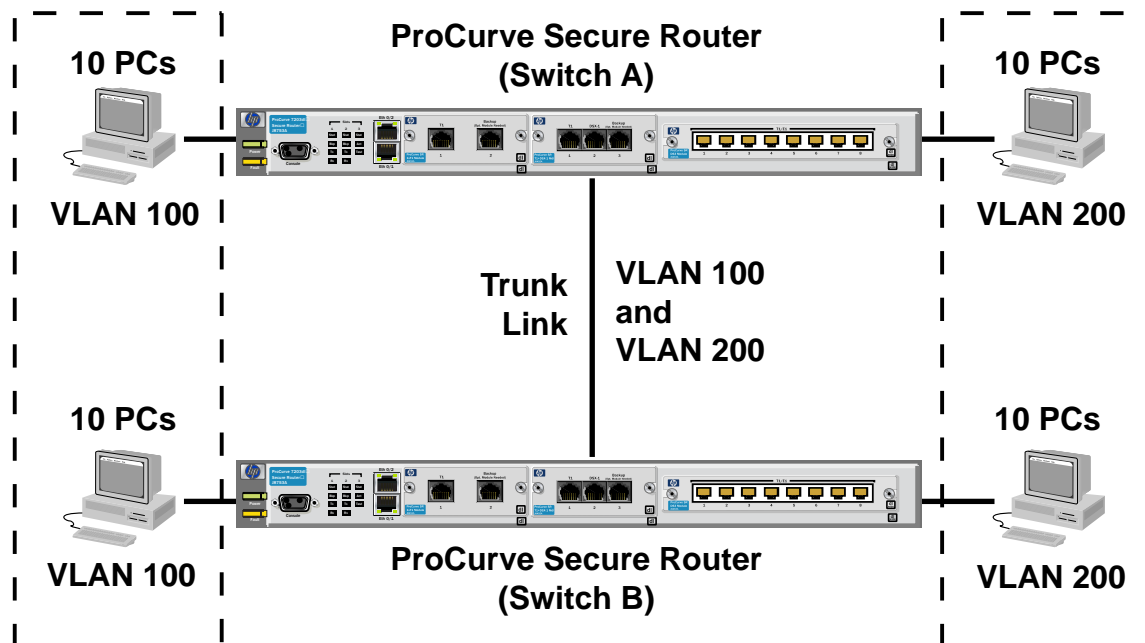


Figure 1. Basic VLAN Configuration

Understanding InterVLAN Routing

In order for network devices in different VLANs to communicate, a router must be used to route traffic between the VLANs. While VLANs help to control local traffic, if a device in one VLAN needs to communicate with a device in another VLAN one or more routers must be used for interVLAN communication.

Figure 1 shows a topology where interVLAN routing would be necessary for PCs in one VLAN to communicate with PCs in other VLANs. The router has two interfaces with 802.1Q encapsulation enabled and multiple VLANs configured on each. For PC1 in VLAN2 to communicate with PC2 in the same VLAN, PC1 simply sends a packet addressed to PC2. The switch will forward the packet directly to the destination PC without going through the router. However, for PC1 to send a packet to PC5, the switch will have to place a VLAN2 tag on the packet and forward the packet on Trunk A to the router. The router will remove the VLAN2 tag, determine the appropriate outgoing interface based on the IP route table, place a VLAN4 tag on the packet, and send it out on Trunk B. The switch in VLAN4 that receives the packet will forward it directly to PC5.

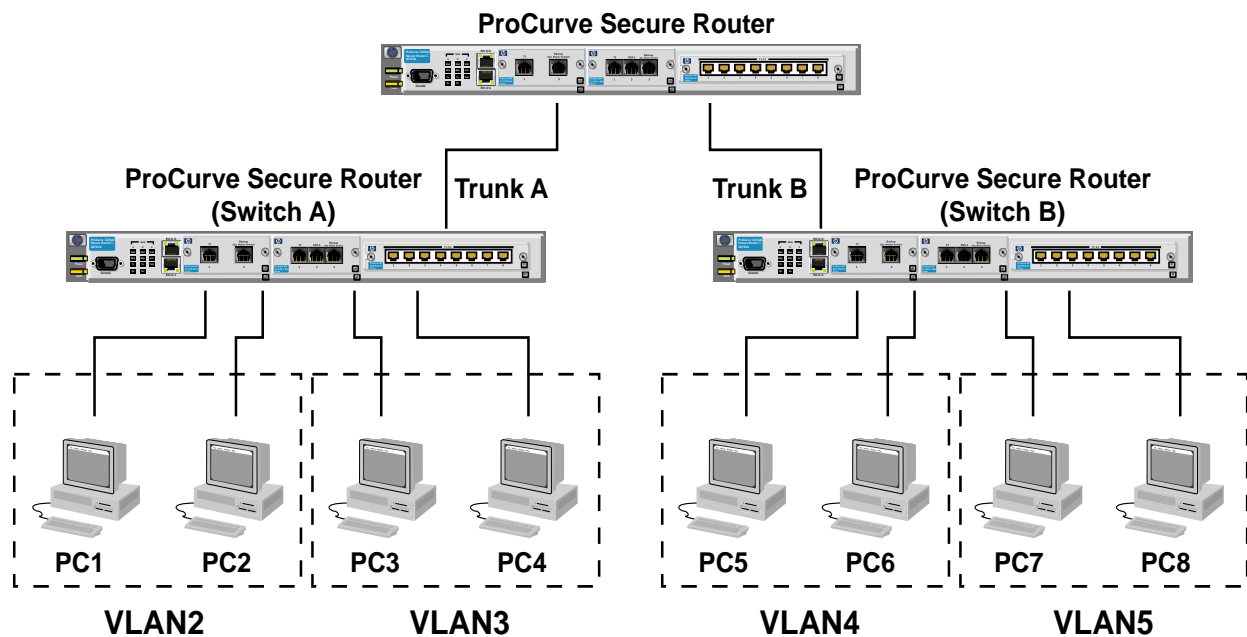


Figure 2. InterVLAN Routing Topology

Configuring InterVLAN Routing

Enabling 802.1Q Encapsulation

To accomplish interVLAN routing, 802.1Q encapsulation must be enabled. Enabling this option adds a 32-bit header for VLAN tagging. This tag sits in the Ethernet frame between the source address field and the media access control (MAC) client type/length field. Table 1 shows the commands necessary to enable 802.1Q encapsulation.

Table 1. Step-by-Step Configuration: Enabling 802.1Q Encapsulation

Step	Action	Command
1	Enter Enable Security mode.	>enable
2	Enter Global Configuration mode.	#configure terminal
3	Enter Ethernet Configuration mode.	 #(config)interface ethernet 0/2
4	Enable 802.1Q encapsulation.	(config-eth 0/2)#encapsulation 802.1q

Creating a Sub-Interface

After enabling 802.1Q encapsulation, the VLAN sub-interface will need to be created. Currently, Ethernet is the only media type that supports VLANs. Table 2 shows the steps necessary to create an Ethernet sub-interface. The description command can be used to help identify the newly-created interface. This comment line can contain up to 80 alphanumeric characters.

Table 2. Step-by-Step Configuration: Creating VLAN Sub-Interface

Step	Action	Command
1	Enter Ethernet Configuration mode.	 #(config)interface ethernet 0/2
2	Create sub-interface for VLAN use.	(config-eth 0/2)#interface ethernet 0/2.1
3	<i>(Optional)</i> Add comment line to help identify new interface.	(config-eth 0/2.1)#description lab1

Assigning a VLAN ID and an IP Address

The next step in configuring interVLAN routing is to assign a VLAN ID to the sub-interface. Valid VLAN IDs are in the range of 1 to 4094. Use the **native** option for the VLAN that will be used as the management VLAN (see optional Step 1 in Table 3). This option specifies that the data for this VLAN will go out untagged.

The final step necessary for interVLAN routing is to assign an IP address to the sub-interface. Each sub-interface will have its own subnet. Step 2 shows the command needed to assign an IP address from this subnet to the sub-interface. This IP address will be the default gateway IP for the VLAN.

After the VLAN ID and the IP address are set, the sub-interface can be activated using the **no shutdown** command. Step 3 shows the necessary steps for assigning the ID and enabling the port.

Table 3. Step-by-Step Configuration: Assigning VLAN Identification and IP Address

Step	Action	Command
1	Assign VLAN identification.	(config-eth 0/2.1)# vlan-id 3
2	<i>(Optional)</i> Assign VLAN identification to the management VLAN.	(config-eth 0/2.1)# vlan-id 3 native
3	Assign IP address to the VLAN sub-interface.	(config-eth 0/2.1#) ip address 10.15.1.254 255.555.255.0
4	Activate new interface.	(config-eth 0/2.1)# no shutdown