802.1Q VLAN
User's Guide

9032599-03

ENTERASYS NETWORKS™

NOTICE

Enterasys Networks reserves the right to make changes in specifications and other information contained in this document and its web site without prior notice. The reader should in all cases consult Enterasys Networks to determine whether any such changes have been made.

The hardware, firmware, or software described in this document is subject to change without notice.

IN NO EVENT SHALL ENTERASYS NETWORKS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS DOCUMENT, WEB SITE, OR THE INFORMATION CONTAINED IN THEM, EVEN IF ENTERASYS NETWORKS HAS BEEN ADVISED OF, KNEW OF, OR SHOULD HAVE KNOWN OF, THE POSSIBILITY OF SUCH DAMAGES.

Enterasys Networks, Inc.
35 Industrial Way
Rochester, NH 03867

Order Number: 9032599-03 December 2002

Version:	Information in this guide refers to firmware version 3.x and 4.x only. It does not refer to firmware version 5.x. This guide applies to 2X2XX, 6X2XX, and 6X3XX Ethernet switch devices only.

Contents

Figures

Tables

Preface

Welcome to the Enterasys Networks *802.1Q VLAN User's Guide*. This guide introduces and describes Enterasys Networks' implementation of the IEEE 802.1Q standard for 802.1Q Virtual Local Area Network (VLAN) technology, and the VLAN Local Management screens used to configure Enterasys Networks products used in 802.1Q VLAN environments.

IMPORTANT NOTICE

Information in this guide refers to firmware version 3.x and 4.x only. It does not refer to firmware version 5.x.

This guide applies to 2X2XX, 6X2XX, and 6X3XX Ethernet switch devices only.

USING THIS GUIDE

This guide serves as a supplement to the Local Management chapter of the Enterasys Networks user's guides for devices that support 802.1Q VLANs. Read Chapter 1 and Chapter 2 first to gain an understanding of VLANs, the associated terminology, and the process for configuring VLANs on a switch. Look at the examples in Chapter 4 to see how VLANs can be created and changed using the existing network infrastructure in a building and how the switch handles the frames while they make their way through the networks shown in the examples. Chapter 3 describes the VLAN Local Management screens and provides a quick walkthrough on how to use them to configure VLANs in a switch.

STRUCTURE OF THIS GUIDE

This guide is organized as follows:

Chapter 1, **Virtual Local Area Networks**, presents the basic concepts of VLANs, including their benefits and uses. This chapter also provides information about how to obtain additional help if needed.

Chapter 2, **VLAN Operation**, describes the operation of an 802.1Q VLAN, the steps necessary to prepare an 802.1Q VLAN aware switch for VLAN operation, and examines the operation of an 802.1Q VLAN switch.

Chapter 3, **VLAN Configuration**, describes how to set up the switch for local and remote management, shows the Local Management screens used in 802.1Q VLAN configuration and explains their use.

Chapter 4, **Examples**, offers examples of 802.1Q VLANs and explains how network transmissions are treated by the components of each VLAN.

RELATED DOCUMENTS

Other Enterasys Networks documents that may be useful for understanding some of the concepts introduced or discussed in this guide are listed below:

The SmartSwitch user's guide of any Enterasys Networks 802.1Q VLAN aware SmartSwitch device.

The manual can be obtained from the World Wide Web in Adobe Acrobat Portable Document Format (PDF) at the following site:

http://www.enterasys.com/

DOCUMENT CONVENTIONS

The following conventions are used throughout this document:

Note symbol. Calls the reader's attention to any item of information that may be of special importance.

In Local Management sections, **Bold type** indicates fields, field values, and commands that can be highlighted or selected by the user.

In Local Management sections, keystrokes are shown in UPPERCASE.

Italic type denotes complete book titles.

1

Virtual Local Area Networks

This chapter introduces the concepts of Virtual Local Area Networks (VLANs) and discusses the central concepts of IEEE 802.1Q VLANs. This chapter also contains information on how to contact Enterasys Networks for additional support related to VLANs.

1.1 DEFINING VLANs

A Virtual Local Area Network is a group of devices that function as a single Local Area Network segment (broadcast domain). The devices that make up a particular VLAN may be widely separated, both by geography and location in the network.

The creation of VLANs allows users located in separate areas or connected to separate ports to belong to a single VLAN group. Users that are assigned to such a group will send and receive broadcast and multicast traffic as though they were all connected to a common network. VLAN aware switches isolate broadcast, multicast, and unknown traffic received from VLAN groups, so that traffic from stations in a VLAN are confined to that VLAN.

When stations are assigned to a VLAN, the performance of their network connection is not changed. Stations connected to switched ports do not sacrifice the performance of the dedicated switched link to participate in the VLAN. As a VLAN is not a physical location, but a membership, the network switches determine VLAN membership by associating a VLAN with a particular port or frame type.

Figure 1-1 shows a simple example of a port based VLAN. Two buildings house the Sales and Finance departments of a single company, and each building has its own internal network. The stations in each building connect to a SmartSwitch in the basement. The two SmartSwitches are connected to one another with a high speed link.

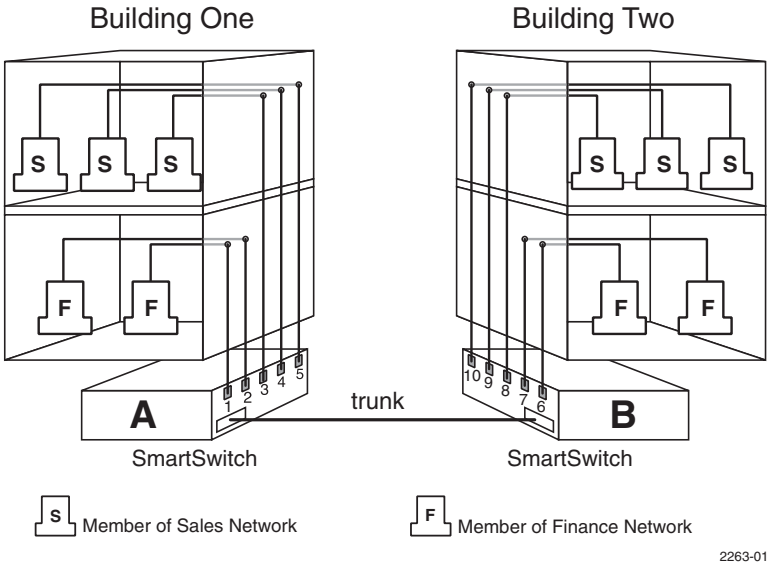


Figure 1-1 Example of a VLAN

In this example, the Sales and Finance workstations have been placed on two separate VLANs. In a plain Ethernet environment, the entire network is a broadcast domain, and the SmartSwitches follow the IEEE 802.1D bridging specification to send data between stations. A broadcast or multicast transmission from a Sales workstation in Building One would propagate to all the switch ports on SmartSwitch A, cross the high speed link to SmartSwitch B, and then propagated out all switch ports on SmartSwitch B. The SmartSwitches treat each port as being equivalent to any other port, and have no understanding of the departmental memberships of each workstation.

In a VLAN environment, each SmartSwitch understands that certain individual ports or frames are members of separate workgroups. In this environment, a broadcast or multicast data transmission from one of the Sales stations in Building One would reach SmartSwitch A, be sent to the ports connected to other local members of the Sales VLAN, cross the high speed link to SmartSwitch B, and then be sent to any other ports and workstations on SmartSwitch B that are members of the Sales VLAN.

1.2 TYPES OF VLANs

There are a number of different strategies for creating Virtual Local Area Networks, each with their own approaches to defining a station's membership in a particular VLAN.

1.2.1 802.1Q VLANs

An 802.1Q VLAN switch determines the VLAN membership of a data frame by its Tag Header, described later in this chapter. If the frame received is not tagged, the switch classifies the frame into the VLAN that is assigned as the default VLAN of the switch.

Some or all ports on the switch may be configured to operate as GARP VLAN Registration Protocol (GVRP) ports. If a frame received is tagged, the frame is forwarded to the GVRP ports that are configured to transmit frames associated with the frame VLAN ID and protocol. If the received frame is not tagged, the frame is examined and tagged as belonging to the default VLAN. Then the frame is forwarded to the GVRP ports that are configured to transmit frames associated with the default VLAN and the frame protocol.

1.2.2 SecureFast VLANs

Enterasys Networks' SecureFast VLAN strategy takes a different approach to creating virtual LANs. In a SecureFast VLAN environment, the switches in the network recognize Network Layer routing requests and translate them. Based on this translation, the switches set up a connection between the end devices in the network.

1.2.3 Other VLAN Strategies

VLANs may also be created by a variety of addressing schemes, including the recognition of groups of MAC addresses or types of traffic. One of the best-known VLAN-like schemes is the use of IP Subnets to divide networks into smaller subnetworks.

1.3 BENEFITS AND RESTRICTIONS

The primary benefit of the 802.1Q VLAN technology is that it provides localization of traffic. This function also offers improvements in security and performance to stations assigned to a VLAN.

While the localization of traffic to VLANs can improve security and performance, it imposes some restrictions on network devices that participate in the VLAN. Through the use of Filtering Database ID's (FIDs) security can be implemented to enable or prevent users from one or more VLANs from communicating with each other.

One or more VLANs can be assigned to a FID so that all the users that share a common FID can communicate with each other regardless of their VLAN affiliation. However, for the sake of security, the members of one FID cannot communicate with the members of another FID.

To set up a VLAN, all the network switch devices that are assigned to the VLAN must support the IEEE 802.1Q specification for VLANs. Before you attempt to implement a VLAN strategy, ensure that the switches under consideration support the IEEE 802.1Q specification.

1.4 VLAN TERMS

To fully understand the operation and configuration of port based VLANs, it is essential to understand the definitions of several key terms.

VLAN ID

A unique number (between 1 and 4094) that identifies a particular VLAN.

VLAN Name

A 32-character alphanumeric name associated with a VLAN ID. The VLAN Name is intended to make user-defined VLANs easier to identify and remember.

Filtering Database Identifier (FID)

Addressing information that the device learns about a VLAN is stored in the filtering database assigned to that VLAN. Several VLANs can be assigned to the same FID to allow those VLANs to share addressing information. This enables the devices in the different VLANs to communicate with each other when the individual ports have been configured to allow communication to occur.

The configuration is accomplished using the Local Management VLAN Forwarding Configuration screen. By default a VLAN is assigned to the FID that matches its VLAN ID.

Tag Header (VLAN Tag)

Four bytes of data inserted in a frame that identifies the VLAN/frame classification. The Tag Header is inserted into the frame directly after the Source MAC address field. Twelve bits of the Tag Header represent the VLAN ID. The remaining bits are other control information.

Tagged Frame

A data frame that contains a Tag Header. A VLAN aware device can add the Tag Header to any frame it transmits.

Untagged Frame

A data frame that does not have a Tag Header.

Default VLAN

The VLAN to which all ports are assigned upon initialization. The Default VLAN has a VLAN ID of 1 and cannot be deleted or renamed.

Forwarding List

A list of the ports on a particular device that are eligible to transmit frames for a selected VLAN.

Port VLAN List
A per port list of all eligible VLANs whose frames can be forwarded out one specific port and the frame format (tagged or untagged) of transmissions for that port. The Port VLAN List specifies what VLANs are associated with a single port for frame transmission purposes.

Filtering Database
A database structure within the switch that keeps track of the associations between MAC addresses, VLANs, and interface (port) numbers. The Filtering Database is referred to when a switch makes a forwarding decision on a frame.

1Q Trunk
A connection between 802.1Q switches that passes only traffic with a VLAN Tag Header inserted in the frame. By default, a port designated as a 1Q Trunk port has all VLANs in its Port VLAN List and is configured to transmit all frames as tagged frames. A 1Q Trunk drops all incoming frames that do not have a VLAN tag.

1D Trunk
A connection from a switch that passes only untagged traffic. By default, a port designated as a 1D Trunk port has all VLANs on its Port VLAN List and is configured to transmit all frames as untagged frames.

Generic Attribute Registration Protocol (GARP)
GARP is a protocol used to propagate state information throughout a switched network.

GARP VLAN Registration Protocol (GVRP)
A GARP application used to dynamically create VLANs across a switched network.

GARP Multicast Registration Protocol (GMRP)
A GARP application that functions in a similar fashion as GVRP, except that GMRP registers multicast addresses on ports to control the flooding of multicast frames.

1.5 GETTING HELP

For additional support related to this document, contact Enterasys Networks using one of the following methods:

World Wide Web	http://www.enterasys.com
Phone	(603) 332-9400
Internet mail	support@enterasys.com
FTP	ftp://ftp.enterasys.com
Login	*anonymous*
Password	*your email address*

To send comments or suggestions concerning this document, contact the Technical Writing Department via the following email address: **TechWriting@enterasys.com**

Make sure to include the document Part Number in the email message.

Before contacting Enterasys Networks for technical support, have the following information ready:

- Your Enterasys Networks service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (e.g., changing mode switches, rebooting the unit, etc.)
- The serial and revision numbers of all involved Enterasys Networks products in the network
- A description of your network environment (layout, cable type, etc.)
- Network load and frame size at the time of trouble (if known)
- The device history (i.e., have you returned the device before, is this a recurring problem, etc.)
- Any previous Return Material Authorization (RMA) numbers

2

VLAN Operation

This chapter describes the operation of a VLAN switch and discusses the operations that a VLAN switch performs in response to both normal and VLAN-originated network traffic.

2.1 DESCRIPTION

The 802.1Q VLAN operation is slightly different than the operation of traditional switched networking systems. These differences are due to the importance of keeping track of each frame and its VLAN association as it passes from switch to switch or from port to port within a switch.

2.2 VLAN COMPONENTS

Before describing the operation of an 802.1Q VLAN, it is important to understand the basic elements that are combined to make up an 802.1Q VLAN.

Stations

A station is any end unit that belongs to a network. In the vast majority of cases, stations are the computers through which the users access the network.

Switches

In order to configure a group of stations into a VLAN, the stations must be connected to VLAN aware switches. It is the job of the switch to classify received frames into VLAN memberships and transmit frames, according to VLAN membership, with or without a VLAN Tag Header.

2.3 CONFIGURATION PROCESS

Before a VLAN can operate, steps must be performed to configure the switch to establish and configure a VLAN. Enterasys Networks VLAN aware SmartSwitches default to operate in the 802.1Q VLAN mode. However, further configuration is necessary to establish multiple logical networks.

NOTE: The actual steps involved in VLAN configuration using Local Management are presented in Chapter 3, **VLAN Configuration**.This brief section describes the actions that must be taken in very general terms, and is intended only to aid in the Administrator's understanding of VLAN switch operation.

2.3.1 Defining a VLAN

A VLAN must exist and have a unique identity before any ports or rules can be assigned to it. The Administrator defines a VLAN by assigning it a unique identification number (the VLAN ID), a filter database association, and an optional name. The VLAN ID is the number that will identify data frames originating from, and intended for, the ports that will belong to this new VLAN.

2.3.2 Classifying Frames to a VLAN

Now that a VLAN has been created, rules are defined to classify all frames in a VLAN. This is accomplished through management by associating a VLAN ID with each port on the switch. Optionally, frames can be classified according to a protocol identifier contained within the frame. The order of frame classification priority is by VLAN Tag, a protocol match, and lastly the PVID. This combination of the switch port's identification and the VLAN ID becomes the Port VLAN ID (PVID).

At the same time, the Administrator configures the trunk ports that need to consider themselves members of every VLAN. The configuration of trunk ports is very important in multiswitch VLAN configurations where a frame's VLAN membership needs to be maintained across several switches.

2.3.3 Customizing the VLAN Forwarding List

Each port on a VLAN aware switch has a VLAN forwarding list that contains, as a minimum, the PVID of the VLAN configured. Additionally, the Port VLAN Forwarding List of each port can be configured to allow any number of VLANs to be added to its list. In the case of GMRP (dynamic VLANs), the list can have VLANs added and deleted by the switch as directed by the protocol.

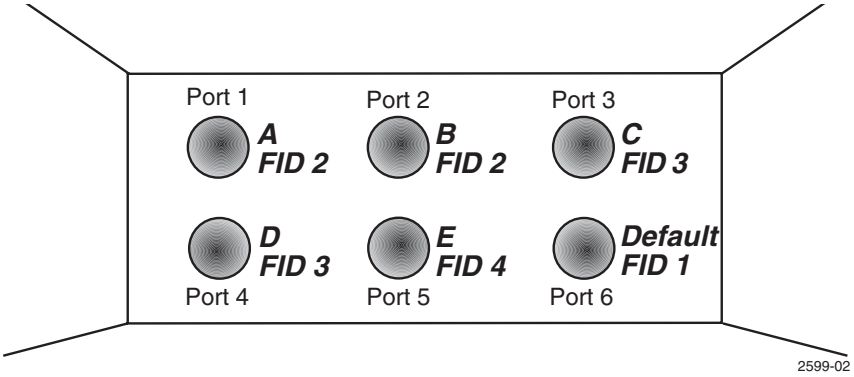
2.4 VLAN SWITCH OPERATION

IEEE 802.1Q VLAN switches act on the classification of frames into VLANs. Sometimes, VLAN classification is based on tags in the headers of data frames. These VLAN tags are added to data frames by the switch as the frames are transmitted out certain ports, and are later used to make forwarding decisions by the switch and other VLAN aware switches. In the absence of a VLAN tag header, the classification of a frame into a particular VLAN depends upon the configuration of the switch port that received the frame.

The operation of an 802.1Q VLAN switch is best understood from a point of view *of* the switch itself. To illustrate this concept, the examples that follow view the switch operations from *inside* the switch.

Figure 2-1 depicts the inside of a switch with six ports, numbered one through six. The switch has been configured to associate VLAN A and B with FID 2, VLAN C and D with FID 3, and VLAN E with FID 4. Port 6 has been classified as a 1Q Trunk Port. This classification establishes that all VLANs are members of the Port VLAN List for Port 6 and the frames transmitted for all VLANs will contain a tag header. Also the PVID for Port 6 is set to the default VLAN with its corresponding relationship to FID 1. Although untagged frames are not usually present on a 1Q Trunk Port, any untagged frames received would need to be classified if the port has not been configured to drop all untagged frames.

Figure 2-1 Inside the Switch



2.4.1 Receiving Frames from VLAN Ports

When a switch is placed in 802.1Q Operational Mode, every frame received by the switch must belong, or be assigned, to a VLAN.

Untagged Frames

The switch receives a frame from Port 1 and examines the frame. The switch notices that this frame does not currently have a VLAN tag. The switch recognizes that Port 1 is a member of VLAN A and classifies the frame as such. In this fashion, all untagged frames entering a VLAN switch assume membership in a VLAN.

NOTE: A VLAN ID is always assigned to a port. By default, it is the Default VLAN (VLAN ID = 1).

The switch will now make a forwarding decision on the frame, as described in Section 2.4.2.

Tagged Frames

In this example, the switch receives a tagged frame from Port 4. The switch examines the frame and notices the frame is tagged for VLAN C. This frame may have already been through a VLAN aware switch, or originated from a station capable of specifying a VLAN membership. If a switch receives a frame containing a tag, the switch will classify the frame in regard to its tag rather than the PVID for its port.

The switch will now make a forwarding decision on the frame, as described in Section 2.4.2.

2.4.2 Forwarding Decisions

The type of frame under consideration and the filter setting of a VLAN switch determines how it forwards VLAN frames.

2.4.2.1 Broadcasts, Multicasts, and Unknown Unicasts

If a frame with a broadcast, multicast, or other unknown address is received by an 802.1Q VLAN aware switch, the switch checks the VLAN classification of the frame. The switch then forwards the frame out all ports that are identified in the Forwarding List for that VLAN. For example, if Port 3, shown in Figure 2-1, received the frame, the frame would then be sent to all ports that had VLAN C in their Port VLAN List.

2.4.2.2 Known Unicasts

When a VLAN switch receives a frame with a known MAC address as its destination address, the action taken by the switch to determine how the frame is transmitted depends on the VLAN, the VLAN associated FID, and if the port identified to send the frame is enabled to do so.

When a frame is received it is classified into a VLAN. The destination address is looked up in the FID associated with the VLAN. If a match is found, it is forwarded out the port identified in the lookup if, and only if, that port is allowed to transmit frames for that VLAN. If a match is not found, then the frame is flooded out all ports that are allowed to transmit frames belonging to that VLAN.

For example, assume that a frame is received by the switch depicted in Figure 2-1. This frame is a unicast untagged frame received on Port 3. The frame is then classified for VLAN C. The switch then makes its forwarding decision by comparing the destination MAC address to its filtering database. In this case, the MAC address is looked up in the filtering database FID 3, which is associated with VLAN C and VLAN D. The switch recognizes the destination MAC address of the frame as being located out Port 4.

Having made the forwarding decision, the switch now examines the Port VLAN List of Port 4 to determine if it may transmit a frame belonging to VLAN C. If so, the frame is transmitted out Port 4. If Port 4 has not been configured to transmit frames belonging to VLAN C, the frame is discarded.

2.5 GARP SWITCH OPERATION

Some or all ports on the switch may be activated to operate under the Generic Attribute Registration Protocol (GARP) applications, GVRP and/or GMRP. For a description of the protocols and how the frames are handled, refer to the user's guide of your SmartSwitch device.

3

VLAN Configuration

This chapter describes how to set up the switch for local or remote management, and the VLAN Local Management screens used to create and configure VLANs in a SmartSwitch.

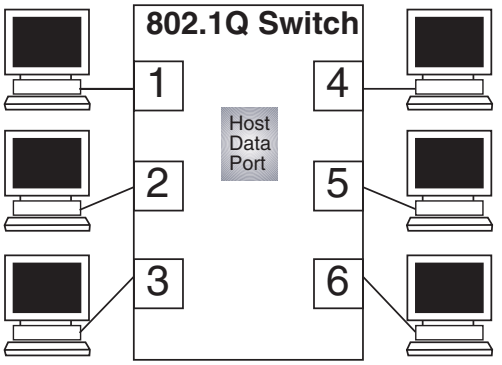
3.1 MANAGING THE SWITCH

The switch may be managed locally via a terminal connected to the COM port, or remotely (SNMP or Telnet sessions) from a management station connected to a switch port that is a member of the same VLAN as the switch's Host Data Port. (By default, this is the default VLAN.) When the switch is configured with VLANs, special precautions must be taken to use remote management.

3.1.1 Switch Without VLANs

When the switch is powered up, the switch uses its default settings to switch frames like an 802.1D switch. In this default configuration, all ports are a member of the default VLAN (VLAN 1) including the virtual Host Data Port of the switch, so any port can be used to manage the device as shown in Figure 3-1.

Figure 3-1 Switch Management with Only Default VLAN



NOTE: All ports, including the virtual Host Data Port, are members of the default VLAN. Therefore, any station shown may be used as the management station.

2599_14

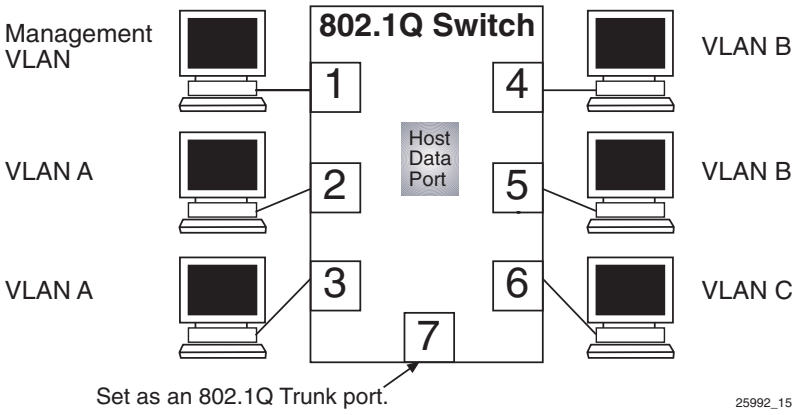
3.1.2 Switch with VLANs

If the switch is to be configured for multiple VLANs, it may be desirable to configure a management-only VLAN. This allows a management station connected to the management VLAN to manage all ports on the switch and make management secure by preventing management via ports assigned to other VLANs.

NOTE: The switch's virtual Host Data Port, like any other port, has configurable VLAN membership. For manageability of the device to be maintained, this port must be a member of the same VLAN as the port to which the management station is connected.

Figure 3-2 shows an example of a switch configured with port 1 on the Management VLAN port and the other users belonging to VLANs A, B, and C.

Figure 3-2 Switch Management with VLANs



To set up the switch shown in Figure 3-2 to establish a management VLAN on port 1, use the process described below:

1. Use the Device VLAN Configuration screen for the following:
   a. Define a new VLAN named "Management VLAN" (or other suitable name) and its VLAN ID. In this example, the VLAN ID is set to 2.
   b. Set the FID so the Management VLAN has its own number to make the VLAN secure. In this example, the FID is 3 and no other VLAN should be assigned to this FID. This keeps the new VLAN from sharing its filtering database with other VLANs in the switch. For details on defining a VLAN, refer to Section 3.4.1.
2. Use the Port Assignment Configuration screen for the following:
   a. Assign the VLAN ID, 2, of the new Management VLAN to a port. In this example, it is port 1. Leave the Port Mode setting in the default value of HYBRID.

NOTE: It is not necessary to configure a physical port for management on each switch. Only those switches that will have a management station attached to it need a physical port assigned to the Management VLAN.

   b. Assign the VLAN ID, 2, of the new Management VLAN to the Host Data Port. The port number will depend on the device. This port is not a physical port and will usually be one number above the maximum number physical ports on the device, including the ports on any optional interfaces installed. In this example, it will be port 8. Leave the Port Mode setting in the default value of HYBRID. For details on assigning a VLAN ID, refer to Section 3.4.2.

This process would be repeated on every switch that is connected in the network to ensure that each switch has a secure Management VLAN for switch management.

If the switch was connected to another switch via port 7, which was set as a 1Q Trunk port, then the management station connected to the Management VLAN port of either switch could manage both switches.

NOTE: The management stations at each switch must be on the same Management VLAN.

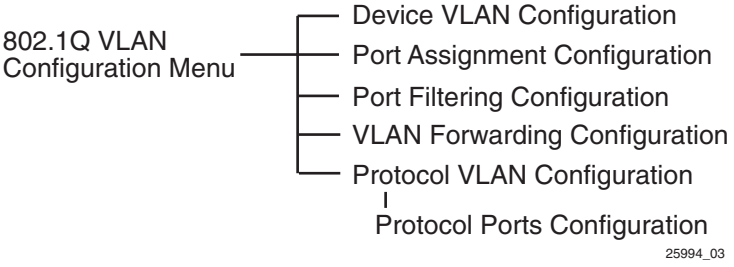
No matter how many switches are connected, a management station connected to any port on the same Management VLAN can be used to remotely manage any Enterasys Networks 802.1Q switch in the network as long as the Host Data Port of all the switches are members of the same Management VLAN.

3.2 SUMMARY OF VLAN LOCAL MANAGEMENT

The VLAN configuration process is an extension of normal Local Management operations. A series of Local Management screens provides access to the functions and commands necessary to add, change, or delete VLANs and to assign ports to those VLANs.

A switch supporting 802.1Q VLANs provides the VLAN Configuration screens as a standard part of its Local Management hierarchy when the switch is configured to operate in 802.1Q Mode. The hierarchy of the Local Management screens pertaining to 802.1Q VLAN configuration is shown in Figure 3-3.

Figure 3-3 802.1Q VLAN Screen Hierarchy



Preparing for VLAN Configuration

A little forethought and planning is essential to a good VLAN implementation. Before attempting to configure a single switch for VLAN operation, consider the following:

- How many VLANs will be required
- What stations will belong to them
- What ports are connected to those stations
- What ports will be configured as GARP-aware ports

It may also be helpful to sketch out a diagram of your VLAN strategy. The examples provided in Chapter 4 may be useful for a depiction of the planning process.

Access Local Management as described in your device user's guide. Perform all required initial setup operations. Navigate to the 802.1Q VLAN Configuration Menu screen to begin the VLAN configuration process for the device.

3.3 802.1Q VLAN CONFIGURATION MENU SCREEN

When to Use

To select screens to assign switched network ports to VLANs, define new VLANs, and configure port filtering according to a VLAN list or untagged frames. Network users can be logically grouped into VLANs even if they span long physical distances over a vast, intricate physical network. The VLAN Local Management menu items listed on the 802.1Q VLAN Configuration Menu allow such VLANs to be configured on a network at the switched port of the device or SmartSwitch chassis. Also, some or all of the ports on the switch can be configured as GVRP ports, which enable frames received with a particular VLAN ID and protocol to be transmitted on a limited number of ports. This keeps the traffic associated with a particular VLAN and protocol to be isolated from the other parts of the network.

Before attempting the VLAN configuration, ensure that the device to be configured has been set for 802.1Q SWITCHING mode. The mode selection is a Local Management operation that is accessible through the General Configuration screen of the device.

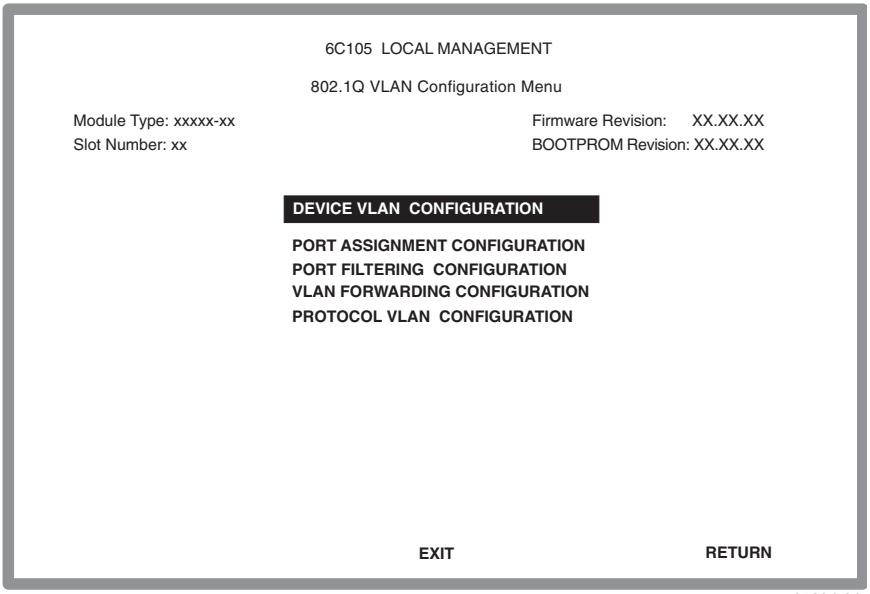
CAUTION: The device resets when changing operational modes.

How to Access

Use the arrow keys to highlight the **802.1Q VLAN CONFIGURATION MENU** item from the module, device, or chassis specific Configuration Menu screen and press ENTER. The 802.1Q VLAN Configuration Menu screen displays.

Screen Example

Figure 3-4 802.1Q VLAN Configuration Menu Screen



25994-04

Menu Definitions

Table 3-1 802.1Q VLAN Configuration Menu Screen Menu Items

Menu Item	Screen Function
DEVICE VLAN CONFIGURATION	Used to view, add, name, enable, or disable VLANs within the device, and also associate the VLANs to a Filter Database ID (FID). It also enables the user to configure attributes that apply to the entire switch and/or VLANs. Refer to Section 3.4 for additional information.

Table 3-1 802.1Q VLAN Configuration Menu Screen Menu Items (Continued)

Menu Item	Screen Function
PORT ASSIGNMENT CONFIGURATION	Displays a list of ports and enables the user to assign a Port VLAN ID (PVID) to each port. The screen also allows the user to change the operational mode of a port. Refer to Section 3.5 for additional information.
PORT FILTERING CONFIGURATION	Used to set the switch to filter out inbound frames to prevent them from being forwarded by the switch out a particular port. This screen also lists the VLANs whose frames are eligible to be transmitted out that port. Refer to Section 3.6 for additional information.
VLAN FORWARDING CONFIGURATION	Used to view which ports are included in the VLAN's Forwarding List and whether to include a Tag Header in a frame being transmitted. Refer to Section 3.7 for additional information.
PROTOCOL VLAN CONFIGURATION	Used to assign VLAN IDs to protocol types of received frames and to access the Protocol Port Configuration screen to add or delete transmitting ports associated with a specific VLAN ID and protocol type. Refer to Section 3.6 for additional information.

3.4 DEVICE VLAN CONFIGURATION SCREEN

When to Use

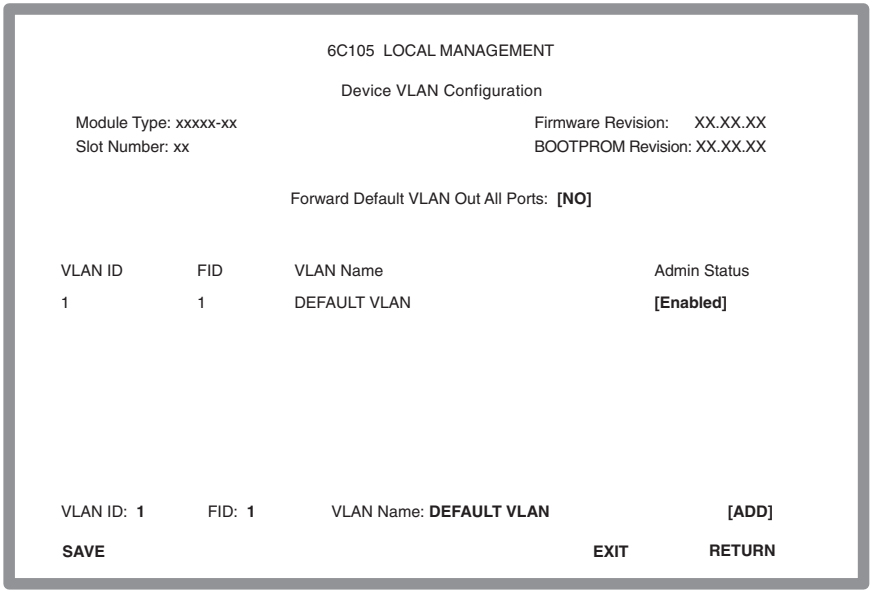
To define the operating characteristics of the switch to add, name, delete, enable, and disable VLANs, and assign VLANs to FIDs. The screen can display up to eight VLANs simultaneously.

How to Access

Use the arrow keys to highlight the **DEVICE VLAN CONFIGURATION** menu item on the 802.1Q VLAN Configuration Menu screen and press ENTER. The Device VLAN Configuration screen displays.

Screen Example

Figure 3-5 Device VLAN Configuration Screen



25993-05

Field Definitions

Table 3-2 Device VLAN Configuration Screen Field Definitions

Use this field …	To …
Forward Default VLAN Out All Ports (Toggle)	Assign or remove the default VLAN from the Port VLAN List for all ports. When set to YES, the default VLAN is added to the Port VLAN List of all ports that do not already include it. When set to NO, the default VLAN is removed from the Port VLAN List of any port that does not have the default VLAN as its PVID. The default is NO.
VLAN ID - *upper part of screen* (Read-Only)	Display the assigned VLAN IDs that are configured in the module. Initially, only the Default VLAN (VLAN ID: 1) is listed.
FID - *upper part of screen* (Read-Only)	Display the names assigned to the corresponding VLAN IDs. If a name has not been assigned to a VLAN, the VLAN Name field displays, “Not Defined”.
Admin Status (Toggle)	Set the current state of the associated VLAN. This field toggles between Enabled and Disabled. An enabled VLAN is operational and a disabled VLAN is not operational. If a VLAN is disabled, all ports assigned to that VLAN will assume a PVID of the default VLAN.

Table 3-2 Device VLAN Configuration Screen Field Definitions (Continued) (Continued)

Use this field …	To …
VLAN ID - *lower part of screen* (Modifiable)	Enter input to select or define a new VLAN ID.
FID - *lower part of screen* (Modifiable)	Display the FID currently associated with the VLAN typed in the VLAN ID field. A new number can be typed into the FID field to reassign the VLAN to a different filtering database. Each VLAN will default to a FID that matches its VLAN ID and can be changed to a FID from 1 to 1094.
VLAN Name - *lower part of screen* (Modifiable)	Assign or change names of VLANs. The VLAN Name (with up to 32 characters) is an optional attribute of a VLAN, and is not required for VLAN operation.
ADD/DEL (Toggle)	Toggle the action taken between adding the entered VLAN to the switch or deleting the selected VLAN from the switch.

3.4.1 Defining a VLAN

To define a VLAN, proceed as follows:

1. Use the arrow keys to highlight the **VLAN ID** field.
2. Enter the VLAN ID using a unique number between 2 and 4094. The VLAN IDs of 0, 1, and 4095 may not be used for user-defined VLANs.

   If an illegal number is entered, the Event Message Line will display: ”PERMISSIBLE RANGE FOR VLAN IDS: 2 to 4094” and the field will refresh with the previous value.

NOTE: Each VLAN ID must be unique. If a duplicate VLAN ID is entered, the switch assumes that the Administrator intends to modify the existing VLAN.

3. If the VLAN is to be assigned to a different filtering database, use the arrow keys to highlight the **FID** field. If the VLAN is not going to be assigned to a different FID, go to Step 5.
4. Type in the ID number of the FID.
5. Use the arrow keys to highlight the **VLAN Name** field.

6. Type a name of up to 32 ASCII characters in the VLAN Name field. This is an optional attribute of a VLAN, and is not required for VLAN operation.
7. Use the arrow keys to highlight the **ADD/DEL** field.
8. Press the SPACE bar to select **ADD** for a defined VLAN. Press ENTER. The new VLAN will be added to the VLAN list. The message "VLAN ADDED" displays in the Event Message Line in the upper left-hand corner of the screen.

   The VLAN will not be saved to the switch until the configuration is saved.
9. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen. Press ENTER. The message "SAVED OK" displays.

3.4.2 Changing the VLAN to FID Association

To change the association of a VLAN to a FID, proceed as follows:

1. Use the arrow keys to highlight the **VLAN ID** field.
2. Enter the VLAN ID of the VLAN of which the FID association is to be changed.

   If an illegal number is entered, the Event Message Line will display: "PERMISSIBLE RANGE FOR VLAN IDS: 2 to 4094" and the field will refresh with the previous value.
3. Use the arrow keys to highlight the **FID** field.
4. Type in the ID number of the FID. If the ID number is valid, the Event Message Line in the upper left hand corner of the screen displays "VLAN # UPDATED", where # represents the entered ID number.
5. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen. Press ENTER. The message "SAVED OK" displays.

3.4.3 Renaming a VLAN

To change the name of an existing VLAN, proceed as follows:

1. Enter the VLAN ID. The **VLAN Name** field will automatically update to display the VLAN's current name.
2. Use the arrow keys to highlight the **VLAN Name** field.
3. Type a name of up to 32 ASCII characters in the VLAN Name field. Press ENTER. If the name is valid, the Event Message Line in the upper left hand corner of the screen displays "VLAN # UPDATED", where # represents the entered VLAN name.

4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen. Press ENTER. The message "SAVED OK" displays.

3.4.4 Deleting a VLAN

To delete a VLAN from the current VLAN list, proceed as follows:

1. Enter the VLAN ID. The **VLAN Name** field will automatically update to display the VLAN's name if that VLAN has been previously configured.
2. Use the arrow keys to highlight the **ADD/DEL** field.
3. Press the SPACE bar to select **DEL**. Press ENTER. The VLAN is removed from the list. The message "VLAN DELETED" displays in the Event Message Line in the upper left-hand corner of the screen.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen. Press ENTER. The message "SAVED OK" displays.

NOTE: The default VLAN cannot be deleted from the list.

3.4.5 Enabling VLANs

To enable a VLAN, proceed as follows:

1. Use the arrow keys to highlight the **Admin Status** field of the selected VLAN.
2. Press the SPACE bar to toggle the field to display **Enabled**.
3. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message "SAVED OK" displays.

3.4.6 Disabling VLANs

To disable a VLAN, proceed as follows:

1. Use the arrow keys to highlight the **Admin Status** field of the selected VLAN.
2. Press the SPACE bar to toggle the field to display **Disabled**.

3. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message “SAVED OK” displays.

NOTE: The default VLAN cannot be disabled.

3.4.7 Changing the Forwarding Mode

To change the forwarding mode of the switch, proceed as follows:

1. Use the arrow keys to highlight the **Forward Default VLAN Out All Ports** field.
2. Press the SPACE bar or BACKSPACE to toggle between **YES** and **NO**. The YES selection places the default VLAN (VLAN ID=1) in the Port VLAN Lists of all ports on the switch. The NO selection removes the default VLAN from the Port VLAN Lists of all ports, unless those ports have a PVID of 1 (those belonging to only the Default VLAN).
3. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message “SAVED OK” displays.

3.4.8 Paging Through the VLAN List

To display additional VLANs that do not display in the current VLAN List as shown on the screen, use the **NEXT** or **PREVIOUS** commands located at the bottom of the screen, as follows:

NOTE: The NEXT and PREVIOUS fields will only display if there are further VLAN List entries to page through.

1. To display the next screen, use the arrow keys to highlight **NEXT**. Press ENTER to view the entries on the next screen.
2. To display the previous screen, use the arrow keys to highlight **PREVIOUS**. Press ENTER to view the entries on the previous screen.

3.5 PORT ASSIGNMENT CONFIGURATION SCREEN

When to Use

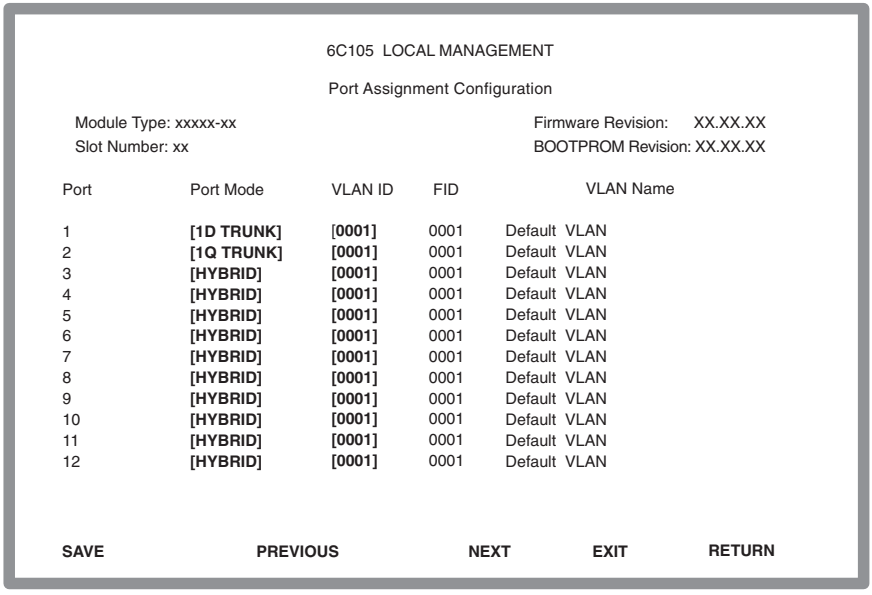
To select a mode of operation for each port and to assign a Port VLAN Identification (PVID) to each port.

How to Access

Use the arrow keys to highlight the **PORT ASSIGNMENT CONFIGURATION** menu item on the 802.1Q VLAN Configuration Menu screen and press ENTER. The Port Assignment Configuration screen displays.

Screen Example

Figure 3-6 Port Assignment Configuration Screen



25992-06

Field Definitions

Table 3-3 Port Assignment Configuration Screen Field Definitions

Use this field …	To …
Port (Read-Only)	See the port numbers of the interfaces of the current module.
Port Mode (Selectable)	Display the current operational mode for the corresponding port and select one of three modes: HYBRID, 1Q TRUNK, or ID TRUNK. The default is HYBRID.
VLAN ID (Selectable)	Select the ID number of the VLAN that is associated with the current port (Port VLAN ID). This is the VLAN ID into which any untagged frame will be classified. The default PVID is 0001.
FID (Read-Only)	Display the FID associated with the VLAN ID. This field updates as the associated VLAN ID field is changed.
VLAN Name (Read-Only)	Display the name that is associated with the current VLAN ID. If a name was not assigned to a VLAN, "NOT DEFINED" displays as the VLAN name.

3.5.1 Changing the Port Mode

To change the operational mode of a port, proceed as follows.

1. Use the arrow keys to highlight the **PORT MODE** field for the module and port combination you wish to change.
2. Use the SPACE bar or BACKSPACE key to step through the available selections. A port may be configured for any of the following modes:
   - **HYBRID** – This is the default mode for all ports on the switch. The initial Port VLAN List includes the PVID with a frame format of untagged. Any other VLANs desired for the Port VLAN List need to be manually configured. By changing the default mode to 1Q Trunk or 1D Trunk, the Port VLAN List and the associated frame type are automatically configured.
   - **1Q TRUNK** – This mode sets the port for transmitting to another 802.1Q aware device. In this mode, all frames are transmitted with a tag header included in the frame (excluding BPDUs). The switch will drop all untagged frames it receives on the 1Q Trunk port. The Port VLAN List for the port includes all VLANs.

- **1D TRUNK –** This mode sets the port for transmitting to a legacy 802.1D switch fabric. In this mode, all incoming frames are classified into the default VLAN and all frames are transmitted untagged. The switch expects to receive only untagged frames through the 1D Trunk port. This mode also updates the Port VLAN List and makes the port eligible to transmit frames for all VLANs. The 1D Trunk mode can be used in conjunction with the "Forward Default VLAN Out All Ports" parameter and the Default VLAN to allow all stations on a legacy portion of the network to access all stations or servers in the 802.1Q portion of the network.

3. When the desired operational mode for the port is displayed, use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message "SAVED OK" displays.

3.5.2 Assigning a VLAN ID

The Port Assignment Configuration screen also enables the user to set each port's VLAN ID (PVID) by stepping through a list of all configured VLANs. To assign a VLAN ID to a port in this manner, perform the following steps:

NOTE: It may be necessary to use the NEXT and PREVIOUS commands to page through the available ports. For instructions, refer to Section 3.5.3.

1. Use the arrow keys to highlight the **VLAN ID** field for the port combination you wish to change.
2. Use the SPACE bar or BACKSPACE key to step sequentially through the previously configured VLAN ID numbers. Only existing VLAN IDs will be displayed.

NOTE: New VLAN IDs must be created with the functions available on the Device VLAN Configuration screen, discussed in Section 3.4.

3. When the desired VLAN ID is displayed, use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message "SAVED OK" displays.

3.5.3 Paging Through the Port List

To display additional ports that do not display in the current screen, use the **NEXT** or **PREVIOUS** commands at the bottom of the screen, as follows:

NOTE: The NEXT and PREVIOUS fields will only display if there are further Port List entries to page through.

1. To display the next screen, use the arrow keys to highlight **NEXT**. Press ENTER to view the entries on the next screen.
2. To display the previous screen, use the arrow keys to highlight **PREVIOUS**. Press ENTER to view the entries on the previous screen.

3.6 PORT FILTERING CONFIGURATION SCREEN

When to Use

To perform the following functions:

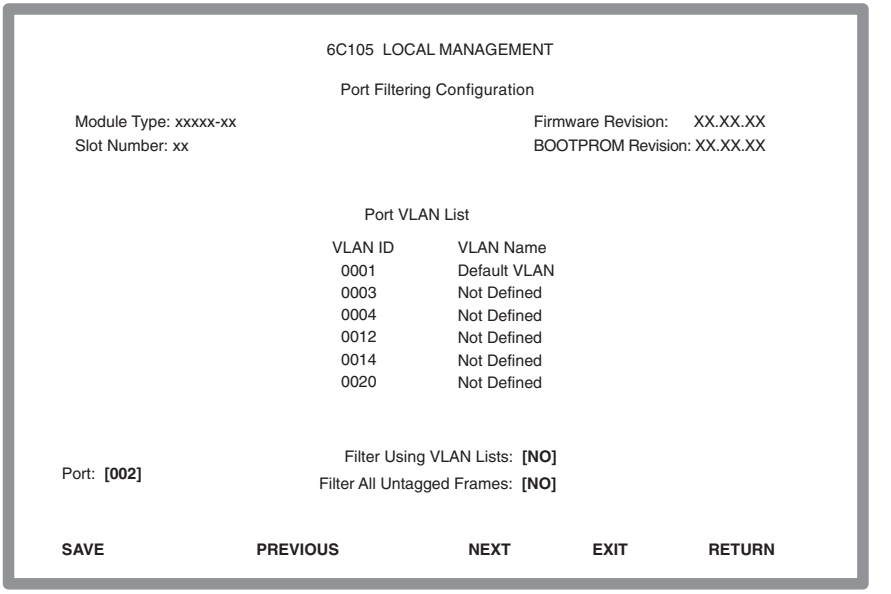
- Select a port and view a list of VLANs that are configured to have their frames transmitted out that port.
- Filter out certain incoming frames according to the VLAN List and prevent them from being switched and transmitted out another port.
- Filter out of all incoming untagged frames so they will not be transmitted out another port.

How to Access

Use the arrow keys to highlight the **PORT FILTERING CONFIGURATION** menu item on the 802.1Q VLAN Configuration Menu screen and press ENTER. The Port Filtering Configuration screen displays.

Screen Example

Figure 3-7 Port Filtering Configuration Screen



25992-07

Field Definitions

Table 3-4 Port Filtering Configuration Screen Field Definitions

Use this field …	To …
VLAN ID (Read-Only)	See the VLAN ID of the VLANs that are configured to have their frames transmitted out the port selected in the Port # field.
VLAN Name (Read-Only)	See the names of the VLANs associated with the VLAN ID. If a VLAN does not have a name, “Not Defined” is displayed.
Port (Selectable)	To step to the port number of the interface being configured including the selection of ALL ports.

Table 3-4 Port Filtering Configuration Screen Field Definitions (Continued)

Use this field …	To …
Filter Using VLAN Lists (Toggle)	Filter out (drop) frames that are classified, via their VLAN tag, as belonging to a VLAN that is not on the Port VLAN List and prevent them from being forwarded by the switch. This field toggles between YES and NO. YES enables filtering according to the Port VLAN List. NO allows the switch to forward the frames. The default is NO.
Filter All Untagged Frames (Toggle)	To filter out all incoming untagged frames so they will not be forwarded by the switch. This field toggles between YES and NO. YES enables the filtering of untagged frames. NO allows the switch to forward untagged frames. The default is NO.

3.6.1 Displaying VLAN IDs Associated with a Port

To display the VLAN IDs and VLAN Names of the VLANs associated with a particular port, proceed as follows:

1. Use the arrow keys to highlight the **Port** field.
2. Use the SPACE bar or BACKSPACE key to step through the available port selections. The screen displays the Port VLAN List of the selected Port. If ALL is selected, no VLAN ID or VLAN Name information is displayed under Port VLAN List.
3. To display additional VLANs that do not display in the current screen display, use the **NEXT** or **PREVIOUS** commands located at the bottom of the screen, as follows:

NOTE: The NEXT and PREVIOUS fields will only display if there are further VLANs in the list to page through.

4. To display the next screen, use the arrow keys to highlight **NEXT**. Press ENTER to view the entries on the next screen.
5. To display the previous screen, use the arrow keys to highlight **PREVIOUS**. Press ENTER to view the entries on the previous screen.

3.6.2 Selecting the Type of Filtering for a Port

A port can be set to filter out received frames according to its Port VLAN List. This keeps them from being transmitted and drops all untagged frames from being transmitted. To set this type of filtering, proceed as follows:

1. Use the arrow keys to highlight the **Port #** field.
2. Use the SPACE bar or BACKSPACE key to step through the available port selections.
3. Use the arrow keys to highlight the **Filter Using VLAN List** field.
4. Use the SPACE bar or BACKSPACE key to toggle between **YES** and **NO**. When set to YES, the switch will drop all incoming frames that are classified with a VLAN tag of a VLAN that does not appear on the Port VLAN List. The default is NO.
5. Use the arrow keys to highlight the **Filter All Untagged Frames** field.
6. Use the SPACE bar or BACKSPACE key to toggle between **YES** or **NO**. When set to YES, the switch will drop all incoming frames that do not have a VLAN tag header. The default is NO.
7. To save the settings, Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
8. Press ENTER. The message “SAVED OK” displays. The settings are saved.

3.7 VLAN FORWARDING CONFIGURATION SCREEN

When to Use

To perform the following functions:

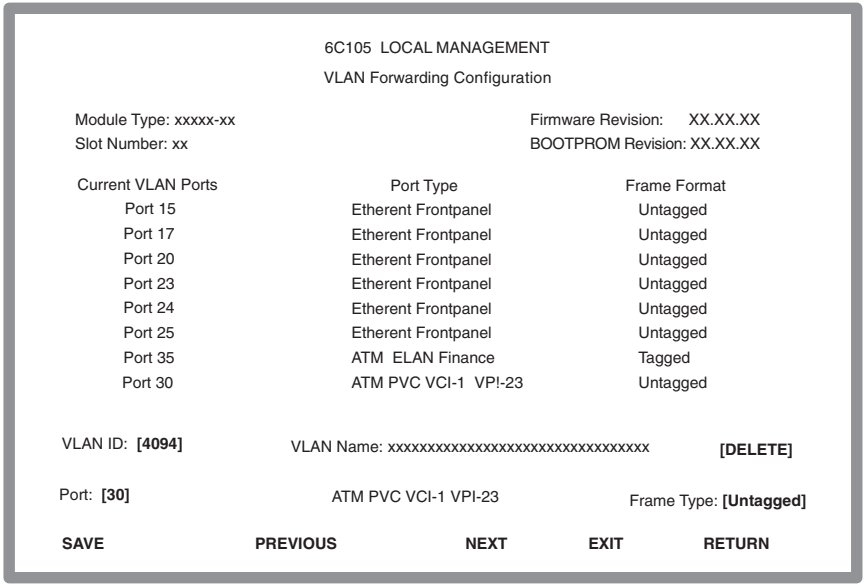
- View the ports included in a VLAN’s Forwarding List.
- Define which ports to include in the VLAN’s Forwarding List.
- Specify the formats of the frames (Tagged or Untagged) that a VLAN port will forward.

How to Access

Use the arrow keys to highlight the **VLAN FORWARDING CONFIGURATION** menu item on the 802.1Q VLAN Configuration Menu screen and press ENTER. The VLAN Forwarding Configuration screen displays.

Screen Example

Figure 3-8 VLAN Forwarding Configuration Screen



25991-08

Field Definitions

Table 3-5 VLAN Forwarding Configuration Screen Field Definitions

Use this field …	To …
Current VLAN Ports (Read-Only)	See the ports that are currently configured to transmit frames classified to the selected VLAN.
Port Type (Read-Only)	See the MIB2 interface description for the selected switch port.
Frame Format (Read-Only)	See the frame format (Tagged or Untagged) for the frames of the selected VLAN that the port will transmit.
VLAN ID (Selectable)	Select the identification of the VLAN under examination. This screen displays the list of ports currently configured to transmit frames for the VLAN ID in this field.

Table 3-5 VLAN Forwarding Configuration Screen Field Definitions (Continued)

Use this field …	To …
VLAN Name (Read-Only)	See the name associated with the VLAN ID.
ADD/DELETE (Toggle)	Swap the action taken to add or delete a port from the VLAN Forwarding List.
Port (Selectable)	Select the port number of the interface being configured. The MIB2 interface description of the port appears to the right of the Port field. In Section 3-8, ATM PVC VCI-1 VPI-23 is the Port Type for Port 30.
Frame Type (Toggle)	Select the format of frames (Tagged or Untagged) that will be transmitted by the selected port for this VLAN. The default is Untagged.

3.7.1 Viewing Current VLAN Ports

To display the VLAN Forwarding List for a particular VLAN, proceed as follows:

1. Use the arrow keys to highlight the **VLAN ID** field. Use the SPACE bar or BACKSPACE to step to the desired VLAN ID and VLAN Name.
2. Press ENTER. The screen updates to display the VLAN Forwarding List for the selected VLAN.

3.7.2 Paging Through VLAN Forwarding List Entries

To display additional entries in the VLAN Forwarding List that do not appear on the screen, use the **NEXT** or **PREVIOUS** commands located at the bottom of the screen, as follows:

1. To display the next screen, use the arrow keys to highlight **NEXT**. Press ENTER to view the entries on the next screen.
2. To display the previous screen, use the arrow keys to highlight **PREVIOUS**. Press ENTER to view the entries on the previous screen.

3.7.3 Adding Forwarding List Entries

To add a port to the VLAN Forwarding List, proceed as follows:

1. Use the arrow keys to highlight the **VLAN ID** field. Use the SPACE bar or BACKSPACE to step to the desired VLAN ID and VLAN Name. Press ENTER.

2. Use the arrow keys to highlight the **Port** field. Step through the available ports on the module with the SPACE bar or BACKSPACE.
3. Use the arrow keys to highlight the **ADD/DELETE** field. Press the SPACE bar to select ADD **or** DELETE. Press ENTER.

   The Forwarding List entry will be added to the list of current VLANs once the configuration is saved.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
5. Press ENTER. The message “SAVED OK” displays.

   The port is added to the VLAN Forwarding List of the selected VLAN.

3.7.4 Deleting Forwarding List Entries

To remove a port from the currently displayed VLAN Forwarding List, proceed as follows:

1. Use the arrow keys to highlight the **VLAN ID** field. Use the SPACE bar or BACKSPACE to step to the desired VLAN ID and VLAN Name. Press ENTER.
2. Use the arrow keys to highlight the **Port** field. Step through the available ports on the module with the SPACE bar or BACKSPACE.
3. Use the arrow keys to highlight the **ADD/DELETE** field. Press the SPACE bar to select **DEL**. Press ENTER.

   The Forwarding List entry will be deleted from the list of current VLANs once the configuration is saved.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
5. Press ENTER. The message “SAVED OK” displays and the port is deleted from the VLAN Forwarding List of the selected VLAN.

3.7.5 Changing the Frame Format

To change the frame format for a port, proceed as follows:

1. Use the arrow keys to highlight the **Port** field. Step through the available ports by pressing the SPACE bar or BACKSPACE.
2. Using the arrow keys, select the **Frame Type** field. Use the SPACE bar or BACKSPACE to toggle between **Tagged** or **Untagged**.
3. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message “SAVED OK” displays.

3.8 PROTOCOL VLAN CONFIGURATION SCREEN

When to Use

To assign a protocol to a VLAN ID on one or more ports on the switch. This enables the switch to add a particular VLAN identifier with the specified protocol to each frame that arrives on a configured port.þ Other switches receiving the frame will classify the frame according to the VLAN identifier within the frame. Entries may also be deleted or modified.

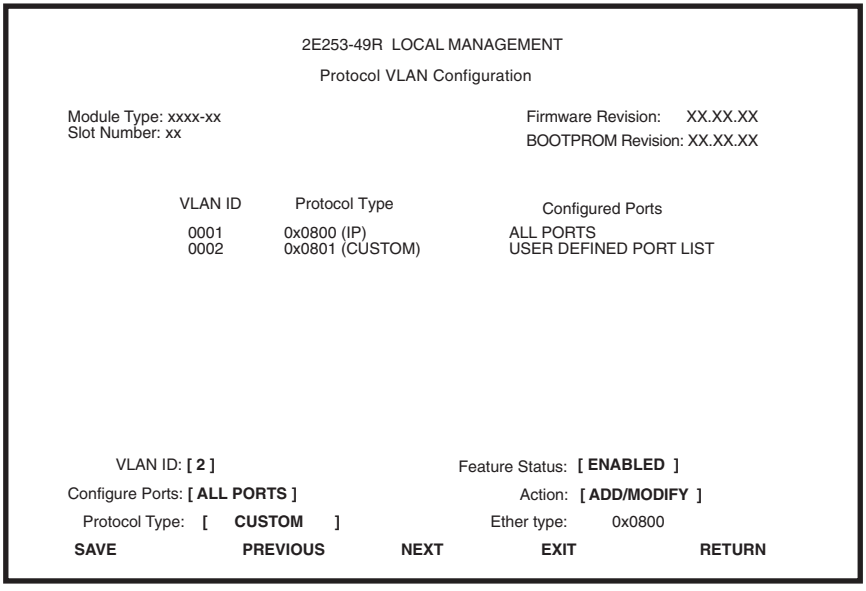
When the frame is transmitted, it is sent to the ports associated with the VLAN ID as established using the Protocol Port Configuration screen.

How to Access

Use the arrow keys to highlight the **PROTOCOL VLAN CONFIGURATION** menu item on the 802.1Q VLAN Configuration Menu screen and press ENTER. The Protocol VLAN Configuration screen displays.

Screen Example

Figure 3-9 Protocol VLAN Configuration Screen



25991_23

Field Definitions

Table 3-6 Protocol VLAN Configuration Screen Field Definitions

Use this field …	To …
VLAN ID - upper part of screen (Selectable)	Display the VLAN IDs currently configured and may be selected after the screen is saved to call up the Protocol Ports Configuration screen using the ENTER key.
Protocol Type - **upper part of screen** (Selectable)	Display the protocol type associated with the VLAN ID in the VLAN ID column. This field may be selected after the screen is saved to call up the Protocol Ports Configuration screen.
Configured Ports (Selectable)	Indicate if a VLAN ID and Protocol Type applies to all configurable ports or only those listed in the Protocol Ports Configuration screen for that Priority and Protocol Type. Configurable ports are all the physical ports and existing virtual interfaces (such as for ATM).
VLAN ID (Modifiable)	Enter the VLAN ID which will be assigned to a protocol. The VLAN ID may be one already created or a new one. If a new VLAN ID is entered, it will be added to the VLAN Configuration with a FID of the same value as the VLAN ID and a VLAN name of PROTOCOL VLAN. To enter the VLAN IDs, refer to Section 3.8.2.
Configure Ports (Toggle)	Apply the priority and protocol type to all or none of the configurable ports. The choices are: ALL PORTS NO PORTS **NOTE:** If ports are added or removed from the port list in the Priority Ports Configuration screen described in Section 3.9, the Configured Ports for the particular VLAN ID and Protocol Type will change from ALL PORTS or NO PORTS to USER DEFINED PORT LIST in the Protocol Priority Configuration screen.

Table 3-6 Protocol VLAN Configuration Screen Field Definitions (Continued)

Use this field …	To …
Protocol Type (Selectable)	Select one of the following protocol types: IP – pertains to all IP associated Ether Types (i.e., 0x0x0800, 0x0806, and, 0x8035). IPX – pertains to all IPX associated Ether Types (i.e., 0x8137, 0x8138, and special cases, 0x0100 [LLC Type 1 Encapsulation] and 0x0101 [LLC Type 2 Encapsulation]). Appletalk – pertains to all Appletalk associated Ether Types (i.e., 0x809B and 0x80F3). Netbios – pertains to all Netbios associated Ether Types (i.e. 0x0102). Banyan Vines – pertains to all Banyan Vines associated Ether Types (i.e., 0x0103 and 0x0BAD). DECNET – pertains to all DECNET associated Ether Types. CUSTOM – when this field is chosen, Ether Type "0x0" displays so the user can input a particular Ether Type. **NOTE:** Any Ether type selected or entered in the Ether type field and saved will become part of the selection in the protocol field. For details, refer to Section 3.8.1.
Feature Status (Toggle)	Enables or disables the entries. The entries can be made but are not affective until this field is set to ENABLED. The choices for this field are: ENABLED DISABLED
Action (Toggle)	Used to add or delete an entry (Priority) and its protocol. This field toggles between [ADD/MODIFY] and [DELETE]. ADD/MODIFY– adds the new Priority and Protocol Type entries (for example, Priority [0] and Protocol Type [Banyan Vines]). DELETE – deletes an existing entry with the associated priority (for example, Priority [0] and Protocol Type [Banyan Vines]).

Table 3-6 Protocol VLAN Configuration Screen Field Definitions (Continued)

Use this field …	To …
Ether type (Modifiable)	Enter the values of a new Ether type when CUSTOM is selected in the Protocol Type field.The value 0x0 will display, which can be modified. A protocol may have more that one Ether Type. Any Ether Type greater than 05dc (hex) and less than ffff (hex) may be entered.þ The maximum number of Ether Types configured per switch is 32. If an attempt is made to enter more that 32, an error message, “ETHER TYPE TABLE FULL” displays. To enter values of a particular Ether Type, refer to Section 3.8.2.

3.8.1 Displaying the Current Protocol, VLAN ID, and Port Assignments

In some instances it may be desirable to see which VLAN IDs and the associated ports that are currently assigned to a particular protocol. To display this information, proceed as follows:

1. Use the arrow keys to highlight the **Protocol** field at the bottom of the screen.
2. Press the SPACE bar to step to the appropriate protocol.
3. Press ENTER. The screen displays all VLAN IDs and associated ports currently assigned to the selected protocol.
4. If there is more information than the screen can display, use the NEXT and PREVIOUS command at the bottom of the screen to display the information.

3.8.2 Assigning a Protocol Family to a VLAN ID

To assign all Ether Types associated with a Protocol Family to a VLAN ID, proceed as follows:

NOTE: The list of Ether Type configurations is searched prior to the list of “Protocol Family” configurations when a frame is received on a switch.þ This means that if Ether Type of 0x0800 is configured on port 10 with VID of 5 and IP is configured on port 10 with VID of 6, the incoming frame will receive the VID 5 as Ether Types have priority over “Protocol Family”.

1. Use the arrow keys to highlight the **VLAN ID** field at the bottom of the screen.

2. Enter the VLAN ID. If a new VLAN ID is entered that has not been created on the switch, use a unique number between 2 and 4094. The VLAN IDs of 0, 1, and 4095 may not be used for user-defined VLANs.
   A FID will automatically be assigned to the new VLAN ID. The FID assigned will have the same value.

   If an illegal number is entered, the Event Message Line will display: ”PERMISSIBLE RANGE FOR VLAN IDS: 2 to 4094” and the field will refresh with the previous value.

NOTE: Each VLAN ID must be unique. If a duplicate VLAN ID is entered, the switch assumes that the Administrator intends to modify the existing VLAN.

3. Use the arrow keys to highlight the **Protocol** field at the bottom of the screen.
4. Use the SPACE bar to step to the appropriate protocol type; IP, IPX, Appletalk, Netbios, Banyan Vines, DECNET, or CUSTOM. If CUSTOM is selected, Ether Type 0x0 displays. The user’s own Ether Type can then be entered if necessary.

NOTE: Any Ether Type entered in the Ether Type field and saved will become part of the selection in the Protocol field.

TIP: To see if there are VLANs currently assigned to the Protocol displayed in the Protocol field, press ENTER.

5. Use the arrow keys to highlight the **Configure Ports** field near the bottom of the screen.
6. Press the SPACE bar to toggle the field to apply the VLAN ID and Protocol Type entries to either ALL PORTS or NO PORTS.
7. If CUSTOM was selected in the Protocol Type field, use the arrow keys to highlight the **Ether type** field. Otherwise, go to step 9.
8. Enter your particular protocol type in the Ether type field.
9. Use the arrow keys to highlight the **Action** field.
10. Press the SPACE bar to toggle the field to either ADD/MODIFY or DELETE the settings selected in the VLAN ID and Protocol Type fields.

11. Press ENTER and the new settings are displayed under the VLAN ID, Protocol Type, and Configured Ports values.
12. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
13. Press ENTER. The message "SAVED OK" displays and the settings are saved. A particular line of data displayed may now be highlighted to display the Protocol Ports Configuration screen, as described in Section 3.8.3, to view, add, or delete ports from the priority in the highlighted line.

3.8.3 Displaying the Protocol Types on Current Ports

To display the current ports and port types associated with a VLAN ID, the Protocol Ports Configuration screen must be displayed. While in that screen, ports and their port type may be added to, or current ones deleted from, the VLAN ID. To access the Protocol Ports Configuration screen, proceed as follows:

1. Highlight the **line of information** containing the VLAN ID of interest to display the current ports and port types associated with that VLAN ID. The entries in the line of information must have been saved before you can select it to display the Protocol Ports Configuration screen.
2. Press ENTER. The Protocol Ports Configuration screen displays, showing all current ports and port types associated with that VLAN ID. For more information about the Protocol Ports Configuration screen and how to use it, refer to Section 3.9.

3.9 PROTOCOL PORTS CONFIGURATION SCREEN

When to Use

To display the current ports and port types associated with a VLAN and protocol selected in the Protocol VLAN Configuration screen described in Section 3.8.

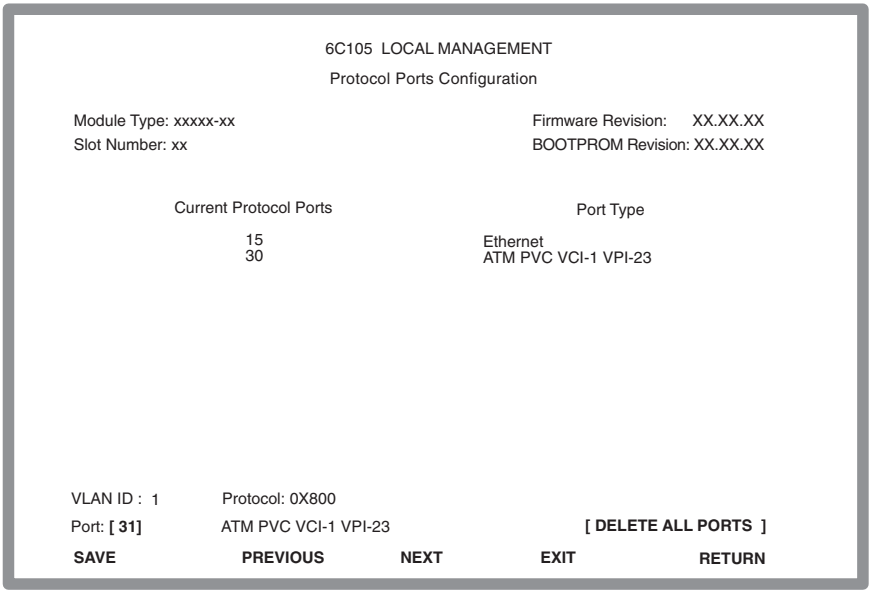
NOTE: The line of information selected must have been saved before it can be used to access the Protocol Ports Configuration screen as described below.

How to Access

Use the arrow keys to highlight a line of information under the VLAN ID/Protocol Type/Configured Ports BitMap columns in the Protocol Priority Configuration screen and press ENTER. The Protocol Ports Configuration screen displays.

Screen Example

Figure 3-10 Protocol Ports Configuration Screen



2599_24

Field Definitions

Table 3-7 Protocol Ports Configuration Screen Field Definitions

Use this field …	To …
Current Protocol Ports (Read-Only)	Display the current ports associated with the VLAN ID.
Port Type (Read-Only)	Display the Port Type associated with the port in the Current Ports column.
VLAN ID (Read-Only)	Display the VLAN ID that is in the line of information highlighted in the Protocol VLAN Configuration screen.
Protocol (Read-Only)	Display the protocol in the line of information highlighted in the Protocol VLAN Configuration screen.

Table 3-7 Protocol Ports Configuration Screen Field Definitions (Continued)

Use this field …	To …
Port (Selectable)þ	Step through the ports to select a port to add of deleted from the VLAN ID shown in the VLAN ID field. When a port is displayed the associated port type is displayed to the right of the port number. In Figure 3-10, the port is 31 and the associated port type is, ATM PVC VCI-1 VPI-23.
DELETE ALL PORTS (Selectable)	Add or delete a port selected in the Port field of the VLAN ID displayed, or add all ports to, or deleted all ports that are configurable on the device. All ports includes, all physical and virtual ports such as ATM ports if supported. In Figure 3-10, the priority is "0". The selections are as follows: ADD PORT – adds the port selected in the Port field. ADD ALL PORTS – adds ALL PORTS that are configurable to the VLAN ID shown in the VLAN ID field. DELETE PORT – deletes the port selected in the Port field. DELETE ALL PORTS – deletes ALL PORTS that are configurable from the VLAN ID shown in the VLAN ID field.

3.9.1 Adding/Deleting Ports Associated with a VLAN ID

To add or delete ports from a VLAN, proceed as follows:

1. Use the arrow keys to highlight the **Port** field.
2. Press the SPACE bar to step to the appropriate port number. The associated protocol is displayed for that port.
3. Use the arrow keys to highlight the **DELETE ALL PORTS** field.
4. Press the SPACE bar to step to the appropriate selection to ADD PORT, ADD ALL PORTS, DELETE PORT, or DELETE ALL PORTS from the VLAN ID shown in the VLAN ID field.
5. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
6. Press ENTER. The message "SAVED OK" displays and the settings are saved.

3.10 QUICK VLAN WALKTHROUGH

The procedures below provide a short tutorial walkthrough that presents each of the steps necessary to configure a new VLAN, assign a port to it, and check the Port VLAN List of the port. You may wish to follow this walkthrough from start to finish before attempting to configure your own VLANs.

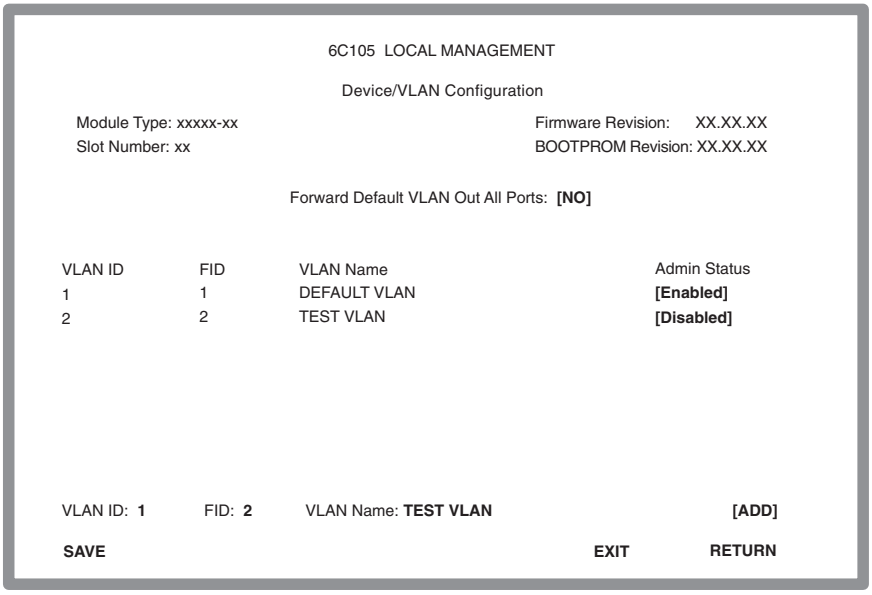
This walkthrough begins at the 802.1Q VLAN Configuration Menu screen for a 6C105 chassis. Follow the instructions in your device user's guide to navigate to this Local Management screen.

NOTE: The screens displayed by your devices may be marginally different from those shown in the illustrations for this walkthrough.

1. On the 802.1Q VLAN Configuration Menu screen, use the arrow keys to highlight the **DEVICE VLAN CONFIGURATION** menu item. Press ENTER. The Device VLAN Configuration screen displays.
2. In this walkthrough, we will not change the setting of the Forward Default VLAN Out All Ports fields from their default setting of NO.
3. Use the arrow keys to highlight the **VLAN ID** field. Assign a number to a new VLAN by typing the number "**2**" in the **VLAN ID** field.
4. Use the arrow keys to highlight the **FID** field. In this example we will assign the new VLAN to FID 2 by typing the number "**2**" in the FID field.
5. Use the arrow keys to highlight the **VLAN Name** field. Type "**TEST VLAN**" in the VLAN Name field. Press ENTER.
6. Use the arrow keys to highlight the **ADD/DEL** field.
7. Press the SPACE bar to toggle the field to **ADD**. Press ENTER. The VLAN is added to the list.
8. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen. Press ENTER. The message "SAVED OK" displays. The screen refreshes and VLAN **2**, the **TEST VLAN** has been added to the Device VLAN Configuration screen and all learning of MAC addresses will be updated in FID 2. The screen should now look like Figure 3-11.

NOTE: This new VLAN is currently disabled, as the DISABLED field to the far right shows. When all the rules and settings for the VLAN are in place, it will be necessary to return to this screen and enable the VLAN.

Figure 3-11 Walkthrough Stage One



25993-09

It is now time to assign a port to this new VLAN.

9. Use the arrow keys to highlight the **RETURN** command at the bottom of the screen. Press ENTER. The 802.1Q VLAN Configuration Menu screen displays. Use the arrow keys to select the **PORT ASSIGNMENT CONFIGURATION** menu item and press ENTER. The Port Assignment Configuration screen displays.

NOTE: For the purposes of this walkthrough, port 3 will be configured.

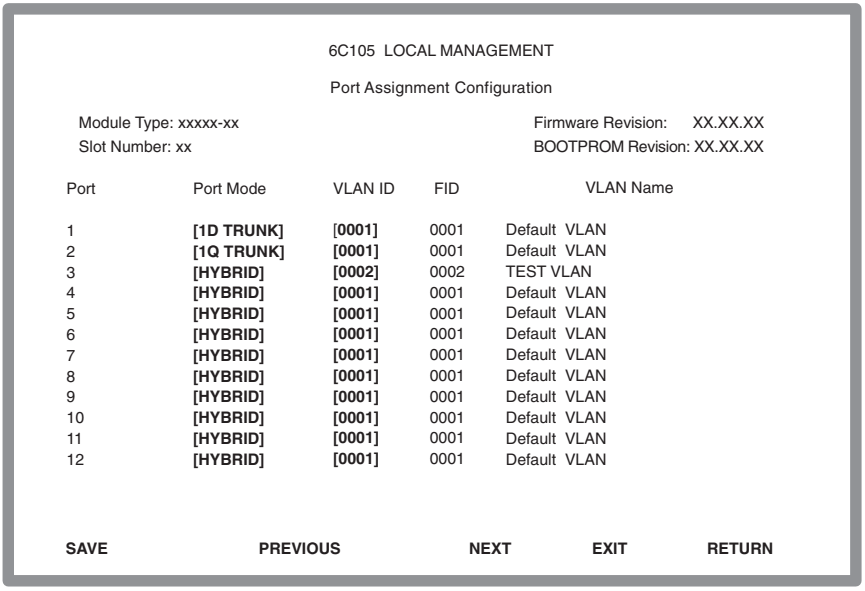
10. Use the arrow keys to highlight the **VLAN ID** field for the module and port combination you wish to change.

NOTE: As this port will connect to a single workstation, and is not to be used for switch-to-switch communications, it is not necessary to change the PORT MODE from the default setting of HYBRID.

11. Use the SPACE bar to step sequentially through the previously configured VLAN ID numbers. When the number **0002** (the new VLAN ID) is displayed, the FID field updates to **0002,** and the **VLAN Name** field updates showing the name assigned to this VLAN, **TEST VLAN**.

12. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen. Press ENTER. The PVID for Port 3 is now configured to the TEST VLAN. The TEST VLAN is also added to the Port VLAN List for Port 3 with a frame format of Untagged. The screen should now look like Figure 3-12.

Figure 3-12 Walkthrough Stage Two



25992-10

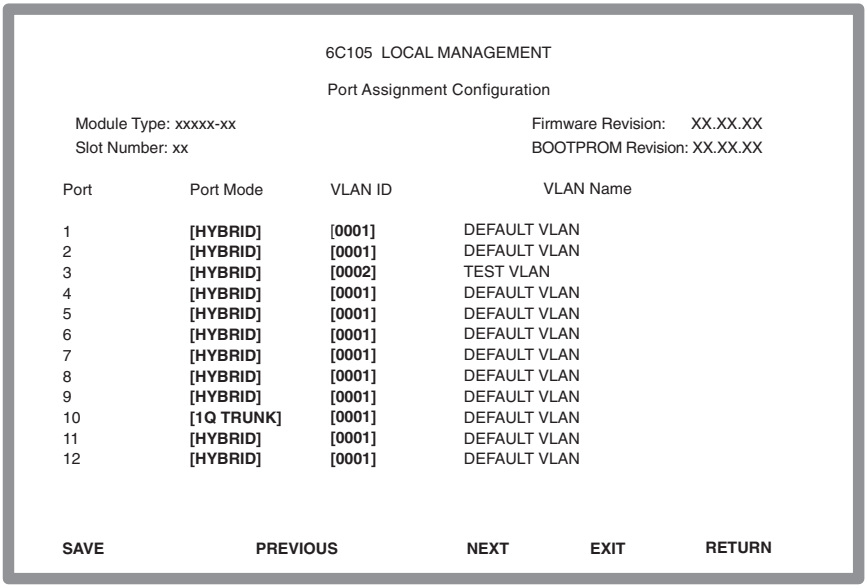
Now that port 3 belongs to the TEST VLAN, we will designate one port as a 1Q Trunk port for a connection to another VLAN aware switch. This 1Q Trunk port will carry traffic from all VLANs, allowing VLAN frames to maintain their VLAN ID across multiple switches.

NOTE: For the purposes of this walkthrough, port 10 will be configured as the trunk port.

13. Use the arrow keys to highlight the **Port Mode** field for port 10. Use the SPACE bar or BACKSPACE key to step sequentially through the possible settings of the port until **1Q TRUNK** is displayed.

14. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen. Press ENTER. Port 10 is now acting as a 1Q Trunk port and every VLAN is in its Port VLAN List. The frame format for every VLAN is also set to tagged. The screen should now look like Figure 3-13.

Figure 3-13 Walkthrough Stage Three

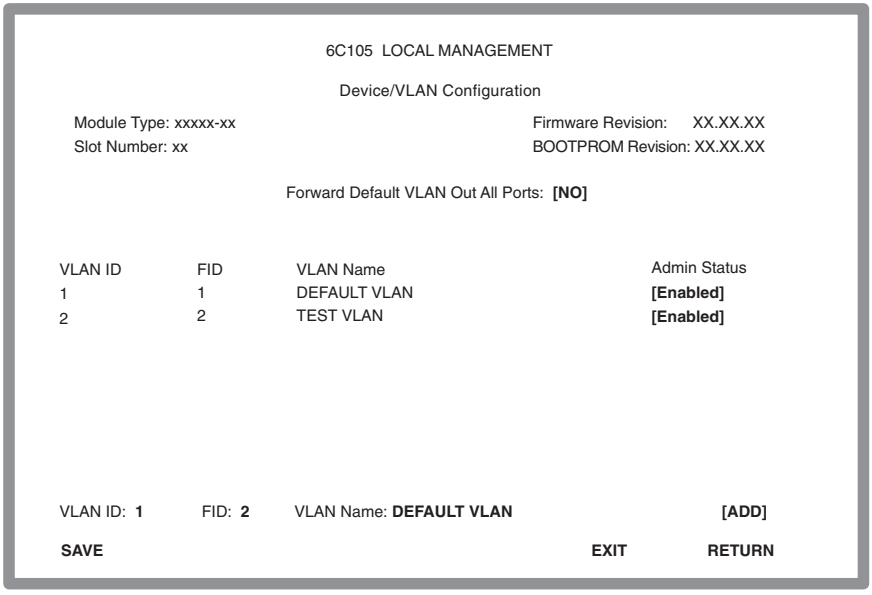


25991-11

Now that the TEST VLAN and the 1Q Trunk connection are set up, we can proceed to activate the TEST VLAN.

15. On the 802.1Q VLAN Main Menu screen, use the arrow keys to highlight the **DEVICE VLAN CONFIGURATION** menu item. Press ENTER. The Device VLAN Configuration screen, Figure 3-14, displays.

Figure 3-14 Walkthrough Stage Four



25993-12

16. Use the arrow keys to highlight the **Admin Status** field of VLAN ID 2, the TEST VLAN.

17. Press the SPACE bar to toggle the field to display Enabled.

18. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.

19. Press ENTER. The message "SAVED OK" displays. The switch activates the new VLAN.

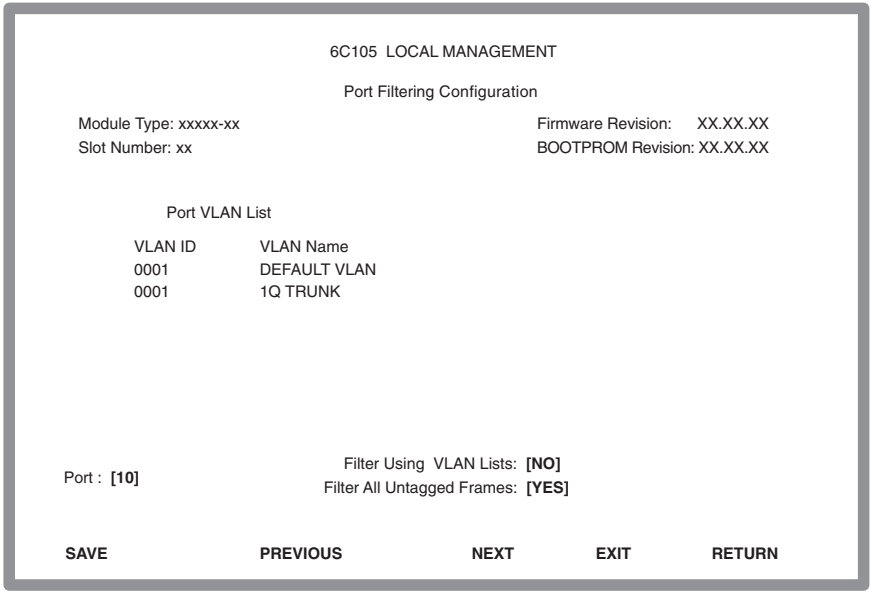
This effectively completes the configuration of a single VLAN, assigning it to a port, and configuring the switch to forward the frames received on that port to be forwarded with the VLAN information included in the frame.

The Port VLAN List of any port on the device can also be checked at any time using the Port Filtering Configuration screen. A list of all ports eligible to transmit frames for a given VLAN will also be listed on the VLAN Forwarding Configuration screen. Each port can also be set to filter out (drop) incoming frames that have VLAN tags that do not match with any of those in its Port VLAN List, and also filter out all untagged frames received by the port. As a default neither function is activated.

In this walkthrough, we will show how to display the Port VLAN List of port 10 and set the port to filter out all untagged frames that it receives.

20. On the 802.1Q VLAN Main Menu screen, use the arrow keys to highlight the **PORT FILTERING CONFIGURATION** menu item. Press ENTER. The Port Filtering Configuration screen displays.
21. Use the arrow keys to highlight the **Port** field.
22. Press the SPACE bar to step the field to display **2**.
23. Use the arrow keys to highlight the **Filter All Untagged Frames** field.
24. Press the SPACE bar to toggle the field to display **YES**.
25. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
26. Press ENTER. The message "SAVED OK" displays. The Port Filtering Configuration screen displays the Port VLAN List for port 2 and the Filtering All Untagged Names field is set to YES as shown in Figure 3-15.

Figure 3-15 Final Walkthrough Stage



25992-20

This effectively completes the displaying of the Port VLAN List and the setting of the port filtering of all untagged frames.

4

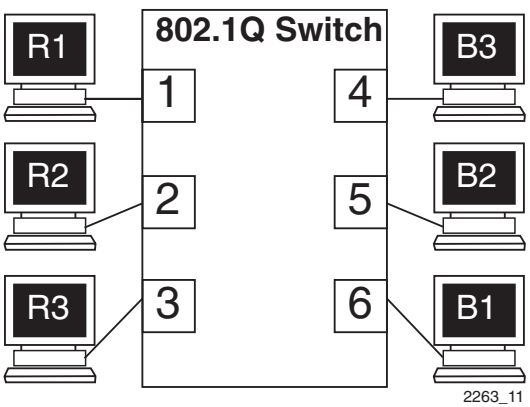
Examples

This chapter provides examples of how VLAN aware SmartSwitches can be configured to group users at the port level to create VLANs in existing networks. Each example presents a problem and shows how it is solved by configuring the switches using the VLAN Local Management screens. The actual procedures and screens used to configure a VLAN aware switch are covered in Chapter 3, **VLAN Configuration**. Also provided in the discussion of each example is a description of how the frames transmitted from one user would traverse the network to its target device.

4.1 EXAMPLE 1, SINGLE SWITCH OPERATION

This first example looks at the configuration of a single Ethernet switch for VLAN operation. In this example, two groups of three users are to be assigned to two VLANs to isolate them from one another. The blue users (B1, B2, B3) are to be kept completely separate from the red users (R1, R2, R3). Figure 4-1 shows the initial state of the switch.

Figure 4-1 Example 1, Single Switch Operation

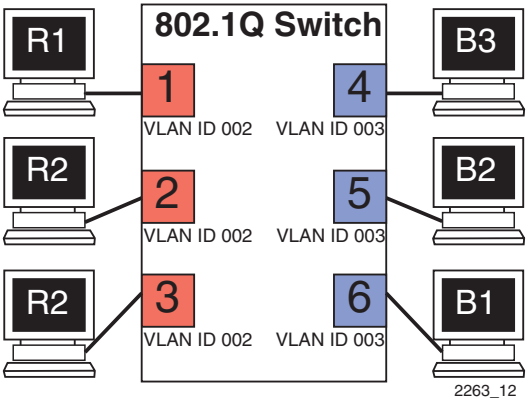


4.1.1 Solving the Problem

To set up this switch, users will be assigned to two new VLANs, red stations to the Red VLAN, and blue stations to the Blue VLAN. The information below describes how the switch is configured to create these two VLANs and how users are assigned to them.

1. First, the switch is set for 802.1Q operation. Since traffic isolation is to be based on VLAN membership alone, the switch is set so the Red VLAN is a member of FID 2 and the Blue VLAN is a member of FID 3 from the Device/VLAN Configuration screen.
2. The Administrator uses the Device/VLAN Configuration screen to define the two VLANs for this switch; the Red VLAN, with a VLAN ID of 002, and the Blue VLAN, with a VLAN ID of 003.
3. The Administrator brings up the Port Assignment Configuration screen and assigns the ports to the VLANs.
   - Ports 1, 2, and 3: VLAN ID 002 (Red VLAN)
   - Ports 4, 5, and 6: VLAN ID 003 (Blue VLAN)
4. Now that the ports have been assigned, the VLANs are enabled from the Device/VLAN Configuration screen.

Figure 4-2 Switch Configured for VLANs



The switch will now classify each frame received as belonging to either the Red or Blue VLANs. Traffic from one VLAN will not be forwarded to the members of the other VLAN, and all frames transmitted by the switch will be normal, untagged Ethernet frames.

4.1.2 Frame Handling

This section describes the operations of the switch when two frames are received. The first frame is a broadcast sent by station R1.

1. Station R1 transmits the broadcast frame. The switch receives this frame on Port 1. As the frame is received, the switch classifies it. The frame is untagged, so the switch classifies it as belonging to the VLAN that Port 1 is assigned to, the Red VLAN.
2. At the same time, the switch adds the source MAC address of the frame and the VLAN associated with port 1 to its Source Address Table in FID 2. In this fashion it learns that station R1 is located out Port 1.
3. Once the frame is classified, its destination MAC address is examined. The switch discovers that the frame is a broadcast, and treats it as it would any other unknown destination MAC address. The switch forwards the frame out all ports in the Red VLAN's Forwarding List except for the one that received the frame. In this case, the frame is sent to Ports 2 and 3.

The second frame is a unicast, where station R2 responds to station R1's broadcast.

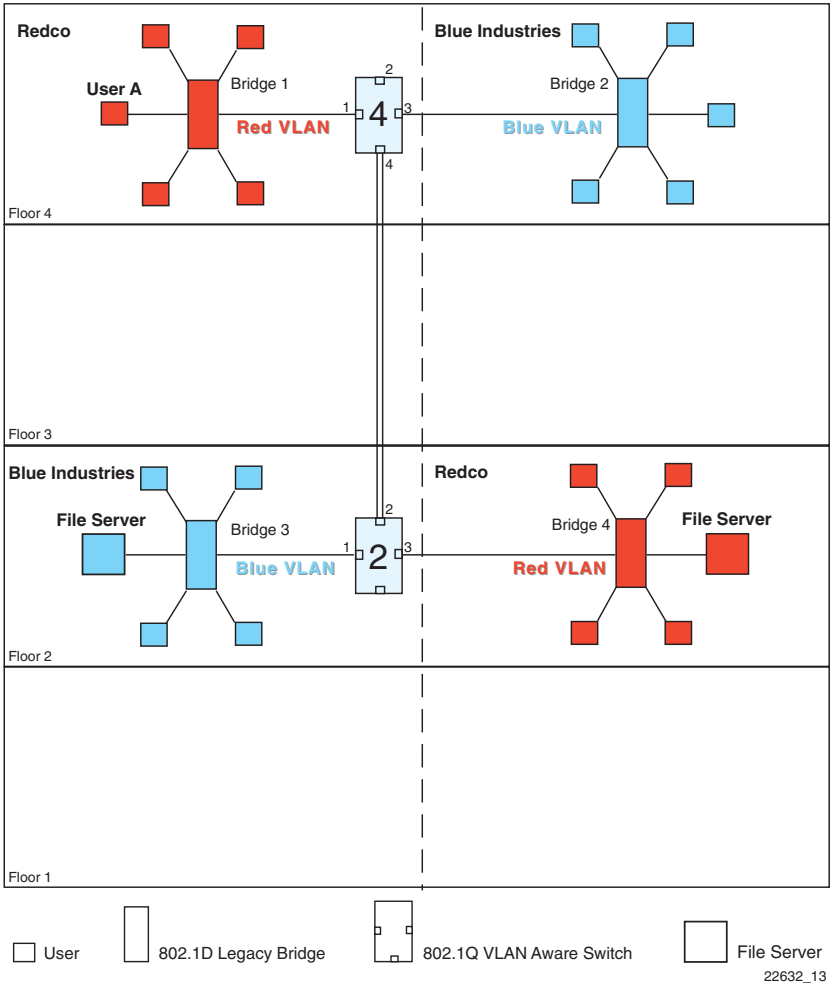
4. Station R2, having received and recognized the broadcast from R1, transmits a unicast frame as a response. The switch receives this frame on Port 2. The switch classifies this new untagged frame as belonging to the Red VLAN.
5. The switch adds the source MAC address and VLAN for station R2 to its Source Address Table in FID 2, and checks the Source Address Table for the destination MAC address given in the frame. The switch finds the MAC address and VLAN in this table, and recognizes that the MAC address and VLAN match for R1 is located out Port 1.
6. The switch examines its VLAN configuration information and determines that the frame for Red VLAN is allowed to be forwarded out Port 1 and that it must be sent in an untagged format.
7. The switch forwards the frame out Port 1. Any other unicast transmissions between stations R1 and R2 will be handled identically.

4.2 EXAMPLE 2, VLANs ACROSS MULTIPLE SWITCHES

This second example investigates the steps that must be taken to set up VLANs across multiple 802.1Q VLAN switches. This includes the configuration and operation of 1Q Trunks between 802.1Q VLAN switches.

As shown in Figure 4-3, two companies, "Redco" and "Blue Industries", share floors 2 and 4 in a building where the network infrastructure is supplied by the building owner. The objective is to completely isolate the network traffic of the two companies by limiting the user's traffic through the ports of two switches, thus maintaining security and shielding the network traffic from each company. This example will show the use and configuration of a 1Q Trunk connection and the creation of VLANs across multiple switches.

Figure 4-3 Example 2, VLANs Across Multiple Switches



4.2.1 Solving the Problem

To solve the problem in this example, the users are assigned to VLANs using Switch 4 and Switch 2 as shown in Figure 4-3. Redco users are assigned to the Red VLAN and Blue Industries users to the Blue VLAN. The following information shows how Switch 4 and Switch 2 are configured to create the two VLANs to isolate the users of the two companies from one another on the network using the existing infrastructure.

Switch 4

Switch 4 is set as follows:

1. Two VLANs are added to the list of VLANs in the Device/VLAN Configuration screen and assigned to a FID. In this example they are as follows:
   - VLAN ID 2, FID 2, with a VLAN Name of Red
   - VLAN ID 3, FID 3, with a VLAN Name of Blue

   Because the VLANs are assigned to two separate FIDs, the users on VLAN ID 2 and VLAN ID 3 cannot communicate with each other.
2. Ports 1 and 3 are assigned to the Port VLAN ID (PVID) as follows using the Port Assignment Configuration screen:
   - Port 1, VLAN ID: 2 for the Red VLAN
   - Port 3, VLAN ID: 3 for the Blue VLAN

   This causes the switch to classify all untagged frames received as belonging to the VLAN specified by each port PVID and to replace the previous PVID information in the port VLAN List with the new PVID information. This makes Port 1 part of the Red VLAN, Port 3 part of the Blue VLAN, and both are set as VLAN frame format of untagged.
3. Port 4 is configured as a 1Q Trunk port as follows using the Port Assignment Configuration screen:
   - Port Mode: 1Q Trunk

   Port 4 is set as an 802.1Q Trunk port, which makes the port eligible to transmit to all VLANs, and all frames forwarded out this port are forwarded as tagged frames. By default there is no PVID associated with the trunk port and the port remains as a member of the Default VLAN. With the original classification information inserted in the frame Tag Header, the receiving switch will maintain the original frame classification.

Switch 2

Switch 2 is set as follows:

1. Two VLANs are added to the list of VLANs using the Device/VLAN Configuration screen and assigned to a FID. In this example they are as follows:
   - VLAN ID 2, FID 2, with a VLAN Name of Red
   - VLAN ID 3, FID 3, with a VLAN Name of Blue

2. A Port VLAN ID is assigned to each port (1 and 3) as follows using the Port Assignment screen:
   - Port 1, VLAN ID: 223 for the Blue VLAN
   - Port 3, VLAN ID: 222 for the Red VLAN

   These settings change the configuration of the switch, so that Port 1 is part of Blue VLAN, Port 3 is part of Red VLAN, and both are set as frame type of untagged.
3. Port 2 is configured as a 1Q Trunk port as follows using the Port Assignment Configuration screen:
   - Port 2, Port Mode: 1Q Trunk

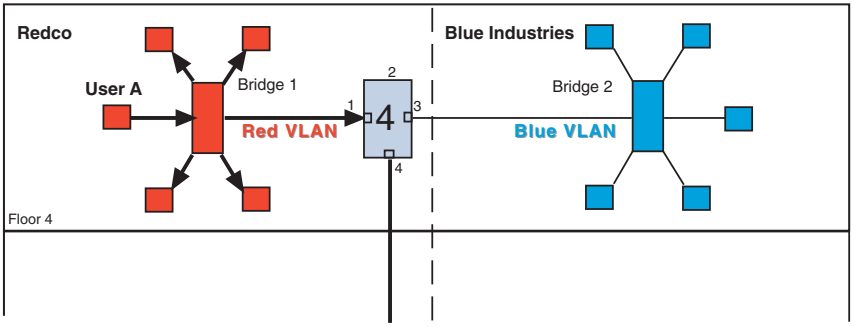
   Port 2 is set as an 802.1Q Trunk port, which makes its Port VLAN List contain all VLANs and sets all frames forwarded out this port as tagged frames. This completes the transmission path between Switch 4 and Switch 2.

4.2.2 Frame Handling

The following describes how, when User A attempts to log on to the File Server on Bridge 4, the frames from User A are classified on Switch 4 and traverse the network. In this example, the MAC address of User A is “Y” and the MAC address for the File Server is “Z”. The following description includes illustrations to help understand how the frames flow through the network.

1. User A sends a frame with a Broadcast Destination Address in an attempt to locate the File Server. The frame is received on User A’s port of Bridge 1 and, because the frame is a broadcast frame, it is transmitted out all ports of Bridge 1 as shown in Figure 4-4.

Figure 4-4 Bridge 1 Broadcasts Frames



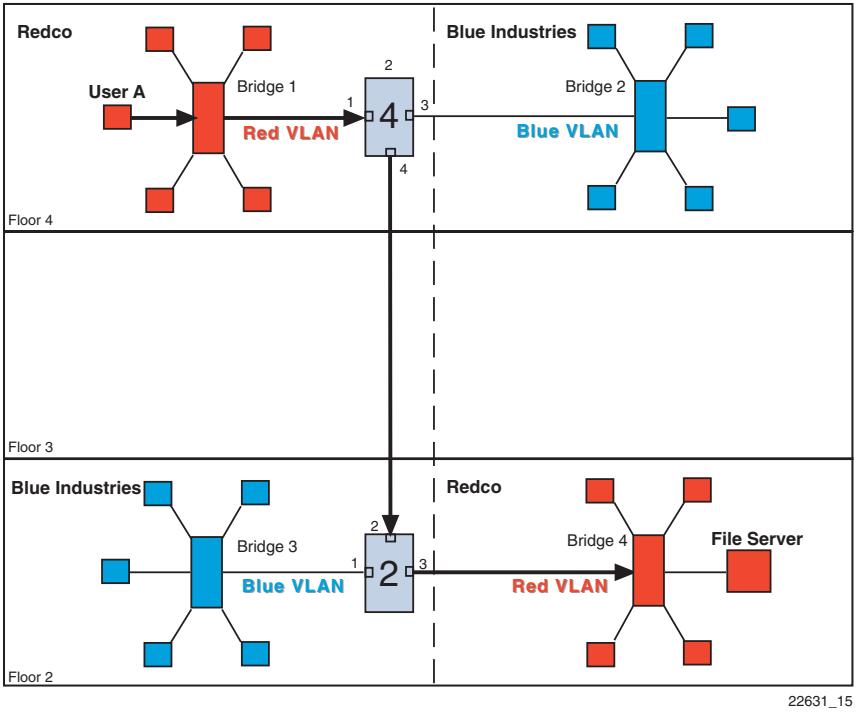
2. Switch 4 receives the frame from Bridge 1 and immediately classifies it as belonging to the Red VLAN. After the frame is classified, Switch 4 checks the Destination Address and, upon discovering that it is a Broadcast Destination Address, forwards the frame out all ports in the Red VLAN Forwarding List excluding Port 1, which received the frame. In this example, it is only Port 4.

Switch 4 updates its Source Address Table in FID 2 if it didn't already have a dynamic entry for MAC address "Y" in FID 2. Because Switch 4 received the frame on Port 1, it does not forward the frame out that port, but does forward the frame to Port 4.

The frame is transmitted to Switch 2 with a VLAN Tag Header inserted in the frame. The VLAN Tag Header indicates that the frame is classified as belonging to the Red VLAN. Figure 4-5 shows the path taken to this point to reach Switch 2.

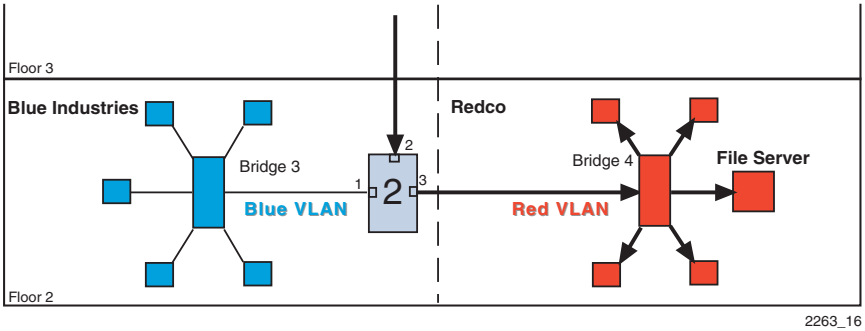
The VLAN Tag Header is inserted because Switch 4, Port 4 is designated as an 802.1Q Trunk port. In this case, the Port Mode setting for Port 4 is 802.1Q Trunk and the VLAN Frame format for that VLAN is tagged.

Figure 4-5 Transmitting to Switch 4



3. When Switch 2 receives the tagged frame on its Port 2, it checks the frame's VLAN Tag Header and determines that the frame is classified as belonging to the Red VLAN, and that the frame is a broadcast frame. Switch 2 forwards the frame to all ports in the Red VLAN Forwarding List excluding Port 2, which received the frame. In this example, the only eligible port is Port 3, which connects to Bridge 4. Switch 2 checks its Forwarding List, which specifies that the VLAN frame type for that port is untagged. Switch 2 then updates its Source Address Table in FID 3 for MAC address "Y" if necessary. The untagged frame is then transmitted out Port 3 to Bridge 4. Bridge 4 forwards the frame out all its ports because it is a broadcast frame, and the server receives it as shown in Figure 4-6.

Figure 4-6 Transmitting to Bridge 4



4. The File Server responds with a unicast frame to User A. All switches between the File Server and User A have an entry in their respective Source Address Tables identifying which port to use for forwarding the frame to User A, MAC address "Y" in FID 3. All switches update their Source Address Tables for the File Server's MAC address "Z" as the frame is forwarded through the switch fabric to User A. The 802.1D switches update their Source Address Tables based on the source MAC address and receive port and the 802.1Q switches update their databases based on the source MAC address, VLAN, and receive port.

5. The frame from the File Server is received on Switch 2, and forwarded to Switch 1 as a tagged frame classified as belonging to the Red VLAN. Switch 1 removes the tag and forwards the frame to Bridge 1, which in turn forwards the frame out of the port attached to User A. All subsequent frames between User A and the File Server are forwarded through the switch fabric in the same manner.

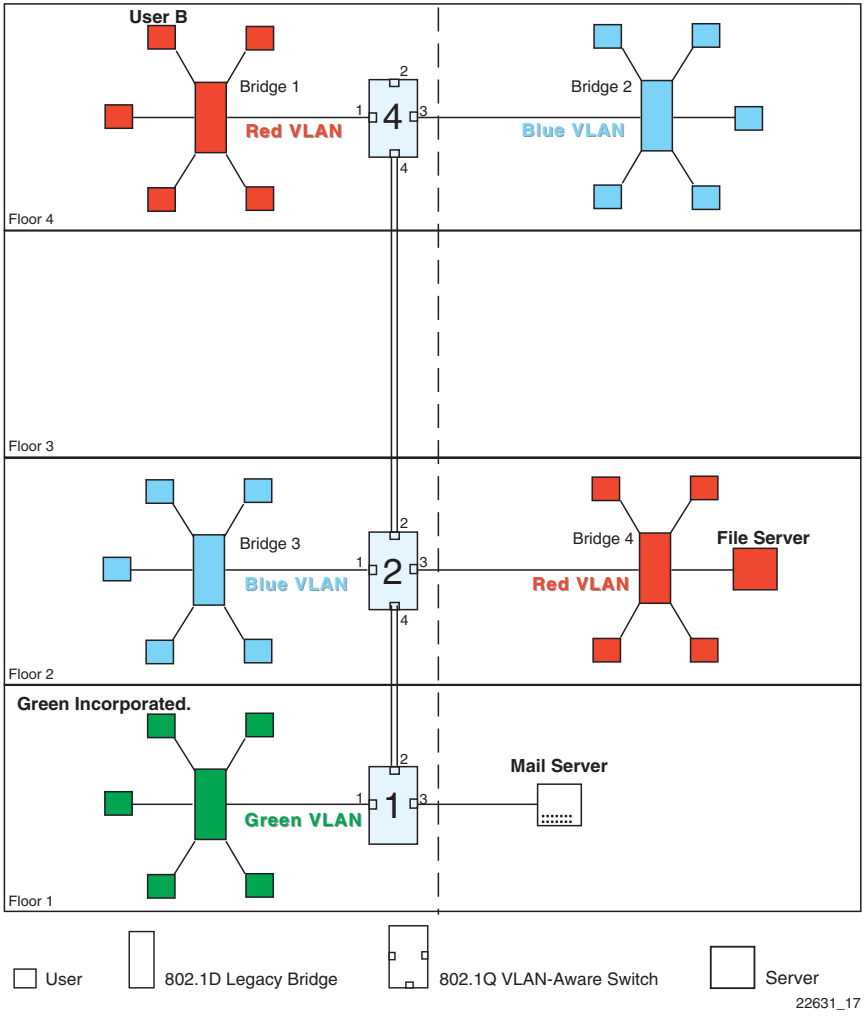
4.3 EXAMPLE 3, 1D TRUNK CONNECTION TO 802.1Q VLAN NETWORK

This example illustrates the use of a 1D Trunk to connect a device to a network of 802.1Q VLAN switches.

In this example, a merger has taken place between the companies in the previous example, Redco and Blue Industries. The two companies have become divisions within a single corporation, Green Incorporated.

As illustrated in Figure 4-7, a third group of stations, the Green Incorporated staff, is added to the facility. Also, the Green Incorporated Network Administrators want to add a Mail Server to the network on the first floor.

Figure 4-7 Example 3, 1D Trunk Connection to 802.1Q VLAN Network



The Green Incorporated Network Administrators want to continue to separate normal network traffic between the Blue and Red VLANs, and create a new isolated VLAN for Green, Incorporated users. All divisions in the facility are to have equal access to the Mail Server on the first floor.

4.3.1 Solving the Problem

Much of the existing network configuration can remain as it was for Example 2, VLANs Across Multiple Switches. However, the Forward Default VLAN Out All Ports must be set to YES on Switch 4 and 2, and a new 1Q Trunk port must be activated and configured on Switch 2. There are no other real changes to the network above the first floor.

Switch 4

Switch 4 is set as follows:

1. The Forward Default VLAN Out All Ports is set to YES using the Device/VLAN Configuration screen. This adds the Default VLAN to the Port VLAN List of every switch port and all VLANs become members of FID 1. This allows all traffic received from the mail server via Switch 2 and Switch 1 to be received and classified to the Default VLAN of Switch 4.

Switch 2

Switch 2 is set as follows:

1. The Forward Default VLAN Out All Ports is set to YES using the Device/VLAN Configuration screen. This adds the Default VLAN to the Port VLAN List of every switch port and all VLANs become members of FID 1.
2. The port mode of Port 4 is set using the Port Assignment screen:

   - Port 4, Port Mode: 1Q Trunk

   This causes Port 4 to be set as an additional 802.1Q Trunk port, which makes its Port VLAN List contain all VLANs, and all frames forwarded out this port are forwarded as tagged frames.

Switch 1

Switch 1 needs to be added to the network backbone to handle traffic from the Green Incorporated network and the mail server. To accomplish this Switch 1 is configured as follows:

1. One VLAN is added to the list of VLANs in the Device/VLAN Configuration screen. In this example, Switch 1 is set as follows:

   - VLAN ID 4, FID 4, with a VLAN Name of Green

2. The Forward Default VLAN Out All Ports is set to YES using the Device/VLAN Configuration screen. This adds the Default VLAN to the Port VLAN List of every switch port and all VLANs become members of FID 1.

3. A Port VLAN ID is assigned to Port 1 using the Port Assignment screen, as follows:

- Port 1, VLAN ID: 224 for the Green VLAN

  This setting changes the configuration of the switch, so that Port 1 is part of the Green VLAN and is set to transmit a frame type of untagged.

4. The port mode of Ports 2 and 3 are set using the Port Assignment screen:

   - Port 2, Port Mode: 1Q Trunk
   - Port 3, Port Mode: 1D Trunk

   Port 2 is set as an 802.1Q Trunk port, which makes the port eligible to transmit frames of all VLANs, and sets all frames forwarded out this port as tagged frames.

   Port 3 is set as a 1D Trunk port, where frames classified as belonging to any VLAN are forwarded untagged, and received frames are classified as belonging to the Default VLAN. This allows the Mail Server to send/receive mail traffic to/from all VLAN users on the network backbone,

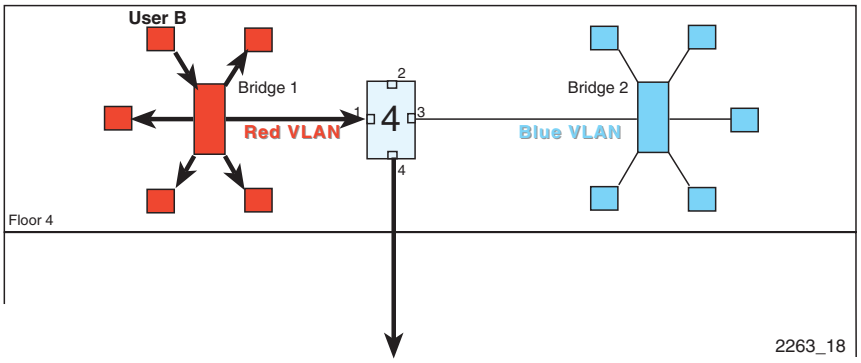
4.3.2 Frame Handling

The following describes how, when User B attempts to contact the Mail Server on Switch 1, the frames are classified on Switch 4 and traverse the network.

1. User B sends a broadcast frame in an attempt to contact the Mail Server. The frame enters Bridge 1 and, being a broadcast, is forwarded to all ports. Bridge 1 learns User B's MAC address from the Source Address field of the frame and adds it to its Source Address Table in FID 1.
2. Switch 4 receives the frame and classifies this new untagged frame as belonging to the Red VLAN. Since the frame is a broadcast, it is forwarded to any ports that are classified as eligible to receive Red VLAN frames. Switch 4 also updates its Source Address Table for FID 1, identifying User B as being located out Port 1.

   On Switch 4, the only port eligible to receive Red VLAN frames is Port 4, the 1Q Trunk. The frame is forwarded out Port 4 with the Red VLAN Tag header being added, as shown in Figure 4-8.

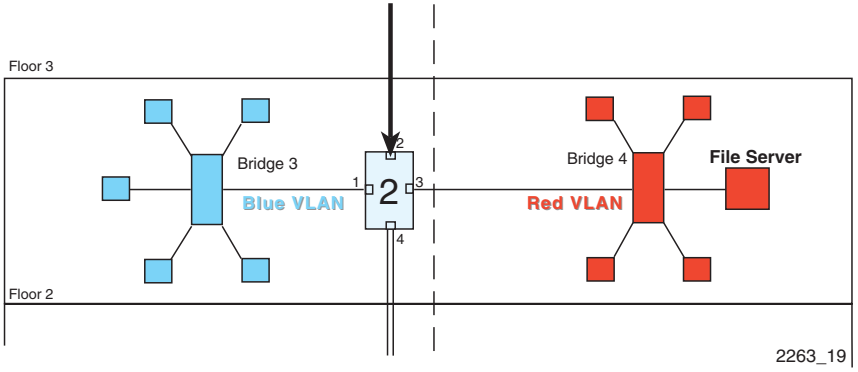
Figure 4-8 Bridge 1 Broadcasts Frames



3. Switch 2 receives the tagged Red VLAN frame on Port 2, as shown in Figure 4-9. The VLAN Tag in the frame is maintained, classifying the frame as belonging to the Red VLAN. The switch forwards the broadcast frame out all the eligible ports, Ports 3 and 4. Switch 2 simultaneously updates its Source Address Table for FID 1 to reflect the location of User B (Port 2).

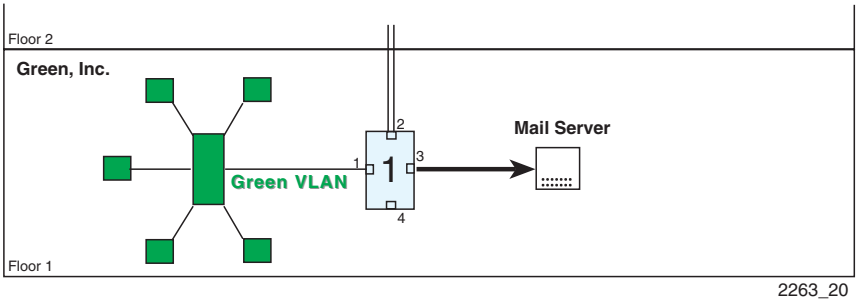
The frame forwarded out Port 3 has its VLAN Tag stripped before transmission, and it is passed to Bridge 4 as a normal broadcast frame. The frame that is transmitted out Port 4, the 1Q Trunk, retains its VLAN tag.

Figure 4-9 Switch 2 Forwards to 1Q Trunk



4. When Switch 1 receives the tagged broadcast frame, it also examines the tag and classifies the frame as belonging to the Red VLAN. This broadcast frame is then sent to all ports eligible to receive Red VLAN frames. In this case only the 1D trunk, Port 3, is eligible, as it is considered a member of all VLANs for forwarding purposes. The VLAN Tag is stripped from the frame and the frame is transmitted out Port 3 as shown in Figure 4-10. The Source Address Table, FID 1 for Switch 1 is updated to contain User B.

Figure 4-10 Switch 1 Forwards to 1D Trunk



5. The Mail Server receives the broadcast frame and recognizes it. The Mail Server responds with a unicast frame to User B. This frame crosses the 1D Trunk and is received by Switch 1. Switch 1 classifies the unicast frame as belonging to the Default VLAN (the only membership for the 1D Trunk port).

   Switch 1 checks the Filtering Database for the MAC address of User B. User B's MAC address is located, and Port 2 is identified as User B's location. The frame is then checked for eligibility and frame format for Port 2. Since Port 2 is a 1Q Trunk port, it is eligible to transmit frames for all VLANs. The frame is tagged and transmitted out Port 2.

   The switch also recognizes the MAC address of User B in its Source Address Table, FID 1, and updates that table to contain the MAC address and port combination of the Mail Server.

6. This tagged unicast frame is received by Switch 2. The frame is already tagged as belonging to the Default VLAN, so no classification needs to be done. The switch recognizes User B's MAC address in its Source Address Table, FID 1, and updates that table to contain the Mail Server's MAC address and port combination.

   The switch checks the Filtering Database for the MAC address of User B. User B's MAC address is located, and Port 2 is identified as the location of User B. The frame is checked for eligibility and frame format for Port 2. Since Port 2 is a 1Q Trunk port, it is eligible to transmit frames for all VLANs. The frame is tagged and transmitted out port 2.

7. Switch 4 receives the frame on its 1Q Trunk port, Port 4, and examines the frame's Tag. The frame maintains its Default VLAN classification. The switch also refers to its Source Address Table, FID 1, to see if it can locate an entry for User B. User B is found to be located on Port 1. The switch also updates its Source Address Table, FID 1, with the port and MAC address combination for the Mail Server.

   The switch examines the Filtering Database and locates the MAC address entry for User B and Port 1. The frame is then checked for eligibility and frame format for Port 1. As Port 1 is considered eligible to transmit to the Default VLAN, the frame is transmitted out Port 1 without a VLAN Tag.

8. Bridge 1 receives the frame and recognizes User B's MAC address. The frame is forwarded to the correct port and the bridge's Source Address Table is updated with an entry for the Mail Server's MAC address. User B receives the Mail Server's response. Any further unicast traffic between the Mail Server and User B will be handled in the same fashion by the switches in the network.

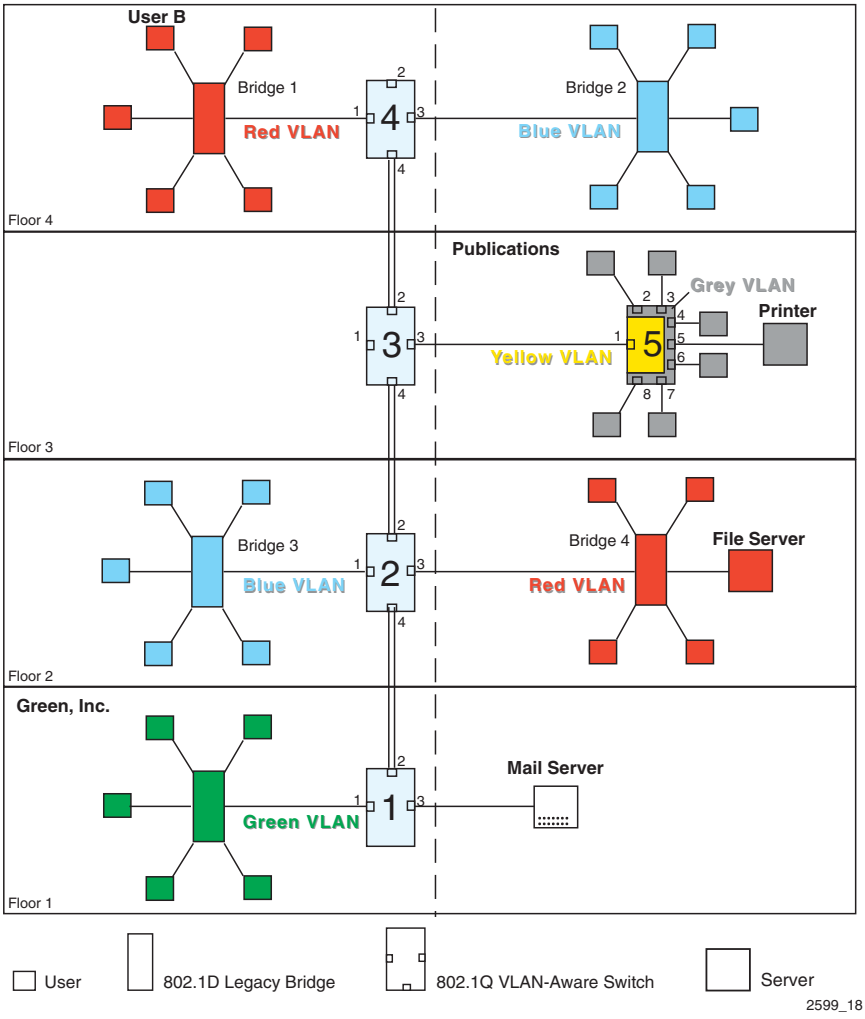
4.4 EXAMPLE 4, ISOLATING NETWORK TRAFFIC ACCORDING TO PROTOCOL

This final example illustrates how to restrict AppleTalk protocol traffic of a network to prevent unwanted multicast frames from slowing down the whole network and yet be able to send and receive frames associated with other protocols.

In this example, illustrated in Figure 4-7, the Publications Department is relocating from another site to the third floor. This network will consist of six computers and a printer using several protocols including the AppleTalk protocol. A characteristic of the AppleTalk protocol is to send all frames as multicast frames. These multicast frames will be isolated to a VLAN (Grey VLAN) to prevent them from slowing down the other networks.

A second VLAN (Yellow VLAN) will be established to handle traffic of other protocols. The Publications Department users will have access to the mail server on the first floor along with the Red, Blue, and Green VLANs.

Figure 4-11 Example 4, Isolating Traffic According to Protocol



4.4.1 Solving the Problem

Much of the existing network configuration can remain as it was for Example 3, 1D Trunk Connection to 802.1Q VLAN Network. However, Switch 3, Switch 5, and the devices that will make up Publication's Grey VLAN have been added.

Switch 5 will be configured to isolate all AppleTalk protocol frame traffic to the devices in the Grey VLAN and all other protocol traffic to the Yellow VLAN. Switch 3 will link the traffic from Switch 5 to the buildings network backbone.

Two 1Q Trunk ports must be activated and configured on Switch 3, and one 1Q Trunk port must be activated and configured on Switch 4.

Ports 2, 3, 4, 5, 6, 7, and 8 of Switch 5 are connected to the Publication Department devices. These ports will be configured to classify all AppleTalk frames into the AppleTalk VLAN (Grey). The same ports will also be configured to classify all other protocol frames into a second VLAN (Yellow). Port 1 will be assigned to the Yellow VLAN to handle the traffic between Switch 3 and 5.

Switch 3

Switch 3 is set as follows:

1. One VLAN is added to the list of VLANs in the Device/VLAN Configuration screen. In this example, Switch 3 is set as follows:
   - VLAN ID 5, FID 5, with a VLAN Name of Yellow
2. The Forward Default VLAN Out All Ports is set to YES using the Device/VLAN Configuration screen. This adds the Default VLAN to the Port VLAN List of every switch port and all VLANs become members of FID 1.
3. A Port VLAN ID is assigned to Port 3 using the Port Assignment screen, as follows:
   - Port 3, VLAN ID: 5, FID 5
4. The port mode of Ports 2 and 4 are set using the Port Assignment screen:
   - Port 2, Port Mode: 1Q Trunk
   - Port 4, Port Mode: 1Q Trunk

   Ports 2, and 4 are set as 802.1Q Trunk ports, which makes these ports eligible to transmit frames of all VLANs, and sets all frames forwarded out these ports as tagged frames. This allows traffic from Switch 4 to reach Switch 2 on the network backbone.

Switch 5

Switch 5 is set as follows:

1. Two VLANs are added to the list of VLANs in the Device/VLAN Configuration screen. In this example, it is set as follows:
   - VLAN ID 5, FID 5, with a VLAN Name of Yellow
   - VLAN ID 6, FID 6, with a VLAN Name of Grey
2. The Forward Default VLAN Out All Ports is set to YES using the Device/VLAN Configuration screen. This adds the Default VLAN to the Port VLAN List of every switch port.

3. To allow all frames (except the AppleTalk frames, which will be prevented in steps 4 and 5) from being transmitted out Port 1 to Switch 3 and the network backbone, Port VLAN IDs are assigned to all switch ports using the Port Assignment screen, as follows:

- Port 1, VLAN ID: 5 for the Yellow VLAN
- Port 2, VLAN ID: 5 for the Yellow VLAN
- Port 3, VLAN ID: 5 for the Yellow VLAN
- Port 4, VLAN ID: 5 for the Yellow VLAN
- Port 5, VLAN ID: 5 for the Yellow VLAN
- Port 6, VLAN ID: 5 for the Yellow VLAN
- Port 7, VLAN ID: 5 for the Yellow VLAN
- Port 8, VLAN ID: 5 for the Yellow VLAN

4. On the Protocol VLAN Configuration screen, the VLAN ID 6 of the Grey VLAN is assigned to the AppleTalk protocol.

- VLAN ID 6, Protocol Type: AppleTalk, Status: ADD

This creates the protocol VLAN ID 6 that will handle only AppleTalk frames and enables ports to be assigned the this VLAN.

5. The AppleTalk frames must now be restricted to Ports 2 through 8 of the Yellow VLAN. On the Protocol Ports Configuration screen, All ports except Port 1 are assigned to the AppleTalk protocol, as follows:

- Port 2, VLAN ID: 6, Protocol: AppleTalk
- Port 3, VLAN ID: 6, Protocol: AppleTalk
- Port 4, VLAN ID: 6, Protocol: AppleTalk
- Port 5, VLAN ID: 6, Protocol: AppleTalk
- Port 6, VLAN ID: 6, Protocol: AppleTalk
- Port 7, VLAN ID: 6, Protocol: AppleTalk
- Port 8, VLAN ID: 6, Protocol: AppleTalk

Any AppleTalk frame received on ports 2 through 8 will be broadcast to all other ports on Switch 5 associated with the AppleTalk protocol. For example, if Port 2 received a frame with the AppleTalk protocol, Switch 5 would only transmit the frame to Ports 2, 3, 4, 6, 7, and 8.

6. Use the VLAN Forwarding Configuration screen to assign Port 1 to the Yellow VLAN and set the frame type to tagged. With this configuration, the frames transmitted on Port 1 are tagged as being from the Yellow VLAN.

If a frame associated with any protocol other than AppleTalk (for example, for the mail server) is received on any of the Ports 2 through 8, the frame would be part of the Yellow VLAN and transmitted out Port 1 as a tagged frame to Switch 3 and handled in the same manner as previously described in the previous examples to route the frame to the Mail Server on the first floor.

Any unicast frames received via Port 1 that are destined for a device in the Yellow VLAN are transmitted to the correct device. Any broadcast frames received via Port 1 are transmitted to all the devices in the Yellow VLAN and handled in a similar manner as previously described in Example 2.

Index

Numerics

C

D

E

F

H

I

L

M

N

O

P

R

S

T

U

V