



DIGITAL MultiSwitch 700

Port Based VLAN User's Guide

DIGITAL MultiSwitch 700

Port Based VLAN User's Guide

Part Number: 9032619

September 1998

This guide provides a general overview of the DIGITAL MultiSwitch 700 Port Based VLAN.

Revision/Update Information:

This is a new document.

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

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

IN NO EVENT SHALL CABLETRON SYSTEMS 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 MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF CABLETRON SYSTEMS HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

© Copyright 1998 by Cabletron Systems, Inc., P.O. Box 5005, Rochester, NH 03866-5005

All Rights Reserved

Printed in the United States of America

Cabletron Systems is a registered trademarks of Cabletron Systems, Inc.

DIGITAL and the DIGITAL logo are trademarks of Digital Equipment Corporation.

All other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies.

PREFACE

Structure of This Guide	V
Document Conventions	V
Related Documentation	vi
Correspondence	vi
Documentation Comments	vi
World Wide Web	vi
Getting Help	vii

CHAPTER 1 VIRTUAL LOCAL AREA NETWORKS

1.1	Defining VLANs	1-1
1.2	Types of VLANs	1-3
1.2.1	Port Based VLANs	1-3
1.2.2	Other VLAN Strategies	1-3
1.3	Benefits and Restrictions	1-3
1.4	VLAN Terms	1-4

CHAPTER 2 VLAN OPERATION

2.1	Description	2-1
2.2	VLAN Components	2-1
2.3	Configuration Process	2-2
2.3.1	Defining a VLAN	2-2
2.3.2	Assigning Ports to a VLAN	2-2
2.3.3	Customizing the VLAN's Forwarding List	2-2
2.3.4	Customizing the Port's Egress List	2-3
2.3.5	Setting the Operational Mode	2-3
2.4	VLAN Switch Operation	2-3
2.4.1	Receiving Frames from VLAN Ports	2-4
2.4.2	Forwarding Decisions	2-5

CHAPTER 3 VLAN CONFIGURATION

3.1	Summary of VLAN Local Management	3-1
3.1.1	Preparing for VLAN Configuration	3-1
3.2	VLAN Main Menu Screen	3-2
3.3	Device/VLAN Configuration Screen	3-4
3.3.1	Defining a VLAN	3-6
3.3.2	Renaming a VLAN	3-7
3.3.3	Deleting a VLAN	3-7
3.3.4	Enabling VLANs	3-8
3.3.5	Disabling VLANs	3-8
3.3.6	Changing the VLAN Operation Mode	3-8

Contents

3.3.7	Changing the Forwarding Mode	3-9
3.3.8	Paging Through the VLAN List.....	3-9
3.4	Port Assignment Screen	3-10
3.4.1	Changing the Port Mode	3-11
3.4.2	Assigning a VLAN ID.....	3-12
3.4.3	Paging Through the Port List.....	3-13
3.5	VLAN Forwarding Configuration Screen	3-14
3.5.1	Viewing Current VLAN Ports	3-15
3.5.2	Paging Through VLAN Forwarding List Entries.....	3-16
3.5.3	Adding Forwarding List Entries	3-16
3.5.4	Deleting Forwarding List Entries	3-17
3.5.5	Changing the Frame Format	3-17
3.6	Quick VLAN Walkthrough	3-17

CHAPTER 4 EXAMPLES

4.1	Example 1	4-1
4.1.1	Solving the Problem	4-2
4.1.2	Frame Handling.....	4-3
4.2	Example 2	4-4
4.2.1	Solving the Problem	4-6
4.2.2	Frame Handling.....	4-7
4.3	Example 3.....	4-11
4.3.1	Solving the Problem	4-13
4.3.2	Frame Handling.....	4-14

INDEX

PREFACE

Welcome to the **DIGITAL Port Based VLAN User's Guide**. This guide introduces and describes port based Virtual Local Area Network (VLAN) technology and the VLAN Local Management screens used to configure the MultiSwitch 700 product used in port based VLAN environments.



The term “port based VLAN” will be used throughout this document to refer to prestandard IEEE 802.1Q Virtual Local Area Networks.

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 the organization of this guide and references to available assistance and related documents.

Chapter 2, **VLAN Operation**, describes the operation of a port based VLAN, describes the steps necessary to prepare a port based VLAN aware switch for VLAN operation, and examines the operation of a port based VLAN switch.

Chapter 3, **VLAN Configuration**, presents the Local Management screens used in port based VLAN configuration and explains their use.

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

DOCUMENT CONVENTIONS

Throughout this guide, the following symbols are used to call attention to important information.



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

RELATED DOCUMENTATION

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

- The *DIGITAL MultiSwitch 700 Overview and Setup Guide*.
- This manual can be obtained from the World Wide Web in Adobe Acrobat Portable Document Format (PDF) at the following site:
<http://www.networks.digital.com>

CORRESPONDENCE

Documentation Comments

If you have comments or suggestions about this manual, send them to DIGITAL Network Products:

Attn.:	Documentation Project Manager
E-MAIL:	doc_quality@lkg.mts.dec.com

World Wide Web

To locate product-specific information, refer to the DIGITAL Network products Home Page on the World Wide Web at the following locations:

North America:	http://www.networks.digital.com
Europe:	http://www.networks.europe.digital.com
Asia Pacific:	http://www.networks.digital.com.au

GETTING HELP

Contact your DIGITAL representative for technical support. Before calling, have the following information ready:

- 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.)
- 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.)

CHAPTER 1

VIRTUAL LOCAL AREA NETWORKS

This chapter introduces the concepts of Virtual Local Area Networks (VLANs) and discusses the central concepts of prestandard IEEE 802.1Q VLANs.

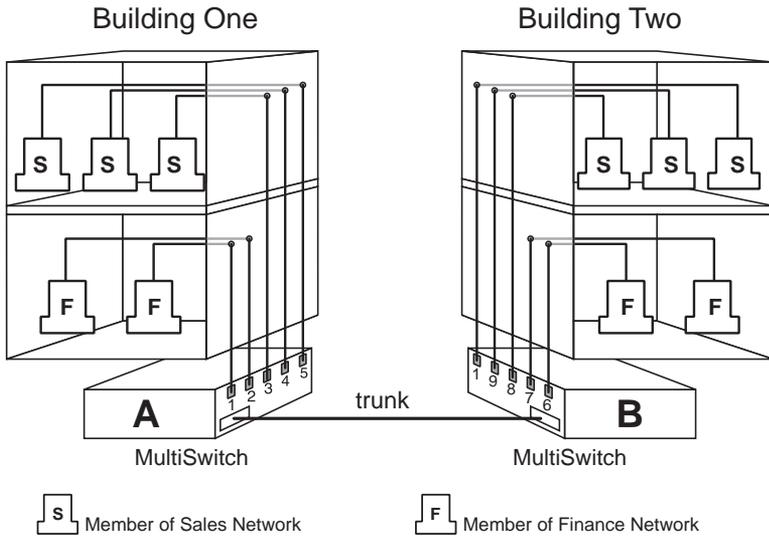
1.1 DEFINING VLANS

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 single network segment. VLAN aware switches isolate broadcast and multicast traffic received from VLAN groups, keeping broadcasts from stations in a VLAN 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.

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 MultiSwitch 700 in the basement. The two switches are connected to one another with a high speed link.



2263-01

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 two switches 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 MultiSwitch A, cross the high speed link to MultiSwitch B, and be propagated to all the switch ports on MultiSwitch B. The switches treat each port as being equivalent to any other port, and have no understanding of the departmental memberships of each workstation.

In a port based VLAN environment, each MultiSwitch 700 understands that certain individual ports 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 MultiSwitch A, be sent to the ports connected to other local members of the Sales VLAN, cross the high speed link to MultiSwitch B, and then be sent to any other ports and workstations on MultiSwitch 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 Port Based VLANs

A port based VLAN switch determines the membership of a data frame by examining the configuration of the port that received the transmission or reading a portion of the data frame's tag header. A four-byte field in the header is used to identify the VLAN. This VLAN identification indicates what VLAN the frame belongs to. If the frame has no tag header, the switch checks the VLAN setting of the port that received the frame. If the switch has been configured for port based VLAN support, it assigns the port's VLAN identification to the new frame.

1.2.2 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. These other VLAN types offer performance advantages and disadvantages that can be quite different from those available with the port based VLAN strategy.

1.3 BENEFITS AND RESTRICTIONS

The primary benefit of the port based VLAN technology is the localization of traffic that it provides. This function can offer 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. If a switch is operating in the "secure mode," a

group of users assigned to a single VLAN can communicate with one another freely, but cannot communicate with users on other VLANs without the services of a Network Layer (OSI Layer 3) routing device to make the connection between the VLANs. In the “open” mode, this restriction does not apply.

In order to set up a VLAN, all the network switch devices that are assigned to the VLAN must support the prestandard IEEE 802.1Q specification for port based 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 meanings of several key terms.

VLAN ID

A unique number (between 1 and 4095) 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.

Tag Header (VLAN Tag)

A field within a frame that identifies the VLAN the frame has been classified into. The Tag Header is inserted into the frame directly after the Source MAC address field. Twelve bits of the Tag Header are the VLAN ID. The remaining bits are other control information.

Tagged Frame

A data frame that contains a Tag Header. The Tag Header can be added to the data frame by a VLAN aware switch to any frame received from a port that is a member of a VLAN.

Untagged Frame

A data frame that does not have a Tag Header inserted into it.

Port VLAN ID (PVID)

An identification that encompasses a particular switch port's identification (port 6, module 2) and that port's VLAN membership. This identification is used to classify incoming untagged frames when they are received.

Default VLAN

The VLAN to which all ports are assigned upon initialization. The Default VLAN has a VLAN ID of 1.

Forwarding List

A list of the ports on a particular device that are eligible to transmit frames for a selected VLAN. The Forwarding List identifies what ports are associated with a single VLAN for frame transmission purposes.

Egress List

A per port list of all eligible VLANs that can be forwarded out one specific port and the frame format of transmissions for that port. The Egress 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, VLAN eligibilities, and interface (port) numbers. The Filtering Database is referred to when a VLAN aware 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.

1d Trunk

A connection from a switch that passes only untagged traffic.

CHAPTER 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

Port based 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 transmission's VLAN membership as it passes from switch to switch or from port to port within a switch.

2.2 VLAN COMPONENTS

Before describing the operation of a port based 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

A VLAN requires a series of configuration steps in order to begin operating. Digital MultiSwitch 700 does not default to VLAN mode. The VLAN operation must be configured and activated through software management.



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) 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 Assigning Ports to a VLAN

Now that a VLAN has been created, individual ports are given membership in the VLAN. This is accomplished through software management by associating a VLAN ID with each port on the VLAN aware switch. 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 any needed trunk ports to consider themselves members of every VLAN. The configuration of trunk ports is very important in MultiSwitch 700 VLAN configurations where VLAN membership applies to users across several switches.

2.3.3 Customizing the VLAN's Forwarding List

Once the ports that will participate in the VLAN have been associated with a VLAN ID, the VLAN Forwarding List can be customized. The information in the Forwarding List tells the VLAN aware switch what ports are eligible to forward traffic for that particular VLAN.

2.3.4 Customizing the Port's Egress List

When the VLAN Forwarding List is fully configured, the Egress List for each port may be customized if needed. The entries in the Egress List allow traffic classified into specific VLANs to be transmitted out the port.

2.3.5 Setting the Operational Mode

Once the VLANs are in place, the operation of the switch is dependent upon the method of operation specified by the Administrator. All port based VLAN switches can be set to one of two operational modes: Open and Secure. The mode configuration of a switch determines how the switch handles the frames that it receives. The differences between the two modes are discussed in Section 2.4, VLAN Switch Operation, below.

2.4 VLAN SWITCH OPERATION

Prestandard 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 interfaces, 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 a port based 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 four interfaces, numbered one through four. The switch knows that interfaces 1 and 2 belong to VLAN A. Interface 3 belongs to VLAN B. Interface 4 is a trunk port belonging to all VLANs. At intervals, frames come in to the switch through these interfaces and are examined.

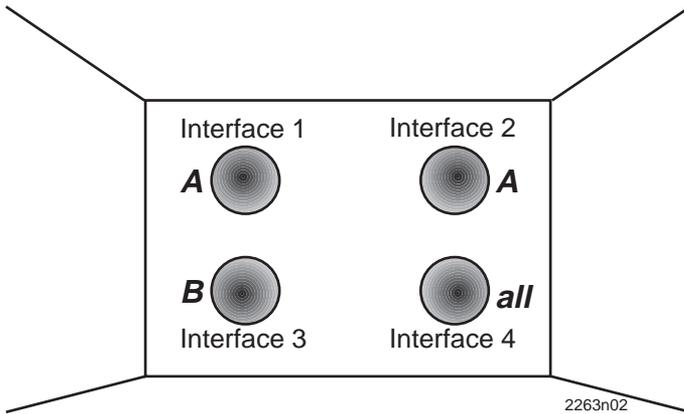


Figure 2-1 Inside the Switch

2.4.1 Receiving Frames from VLAN Ports

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

Untagged Frames

The switch receives a frame from Interface 1 and examines the frame. The switch notices that this frame does not currently have a VLAN tag. The switch recognizes that Interface 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.



If a VLAN ID has not been assigned to a port by the Administrator, the switch will classify frames received from that port as belonging to the Default VLAN (VLAN ID = 1)

The switch will now make a forwarding decision on the frame based on its mode of operation, as described in Section 2.4.2, Forwarding Decisions.

Tagged Frames

In this example, the switch receives a tagged frame from Interface 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 this frame based on its mode of operation, as described in Section 2.4.2, Forwarding Decisions.

2.4.2 Forwarding Decisions

The type of frame under consideration and the operational mode 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 a 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.

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 whether the frame is transmitted depends on the operational mode of the switch.

Open Mode

A switch operating in the Open mode examines a known unicast VLAN frame and makes its forwarding decision based on the destination MAC address of the frame. This decision only determines if the switch can identify a single output interface for the destination MAC address of the frame. If such an interface is identified, the switch will then compare the VLAN tag of the frame with the VLAN eligibilities in that interface's Egress List.

In Open mode, the forwarding decision is based only on the destination MAC address of the frame. As an example, assume that a frame is received by the switch depicted in Figure 2-1. This frame is a unicast untagged frame received from Interface 3. The frame is classified for VLAN B. The switch makes its forwarding decision by comparing the destination MAC address to its filtering database. The switch recognizes the destination MAC address of the frame as being located out Interface 1.

Having made the forwarding decision, the switch now examines the Egress List of Interface 1 to determine if it may transmit the frame. If Interface 1 was only a member of VLAN A, the frame would be discarded. Because the Egress List for Interface 1 does not contain an eligibility for VLAN B, the frame is discarded.

Secure Mode

If the switch is operating in Secure mode, it makes its forwarding decision based on different criteria. While Open mode bases the forwarding decision on only one item in the Filtering Database (the MAC address), Secure mode makes the decision based on the combination of MAC address and VLAN match.

For example, the switch shown in Figure 2-1 receives an untagged frame from Interface 1, and the frame is a unicast intended for a MAC address that the switch Source Address Table recognizes as being located out Interface 3. Immediately upon reception, this untagged frame is classified into a VLAN, VLAN A.

The forwarding decision for the frame is made by examining the Filtering Database for a match of the destination MAC address and membership in VLAN A. The switch examines the Filtering Database and finds no matches for this combination of MAC address and VLAN.

Since no matches were found containing both the destination MAC address and the desired VLAN, the frame will be forwarded to all ports in the Forwarding List for VLAN A.

CHAPTER 3

VLAN CONFIGURATION

This chapter describes the VLAN Local Management screens used to create and configure VLANs in a MultiSwitch 700.

3.1 SUMMARY OF VLAN LOCAL MANAGEMENT

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

Switches supporting port based VLANs will provide the VLAN Configuration screens as a standard part of their Local Management hierarchy, if that switch has been configured to operate in 802.1Q Mode. The hierarchy of the Local Management screens that pertain to port based VLAN configuration is shown in Figure 3-1.

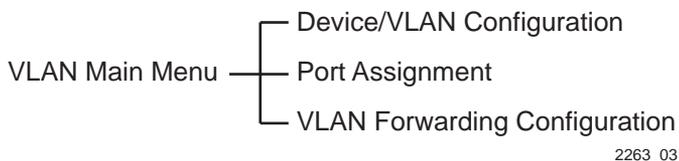


Figure 3-1 VLAN Screen Hierarchy

3.1.1 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 those stations are connected to

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's user's guide. Perform all required initial setup operations. Navigate to the VLAN Main Menu screen to begin VLAN configuration for the device.

3.2 VLAN MAIN MENU SCREEN

The VLAN Main Menu screen enables the user to select screens to assign switched network ports to VLANs, configure switch operation, and define new VLANs. 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 VLAN Main Menu allow such VLANs to be configured on a network at the switched port of the device or MultiSwitch 700 chassis.

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

To access the VLAN Main Menu screen from the module, device, or chassis specific Configuration Menu screen, use the arrow keys to highlight the **802.1Q VLAN CONFIGURATION** menu item and press ENTER. The VLAN Main Menu screen, Figure 3-2, displays.

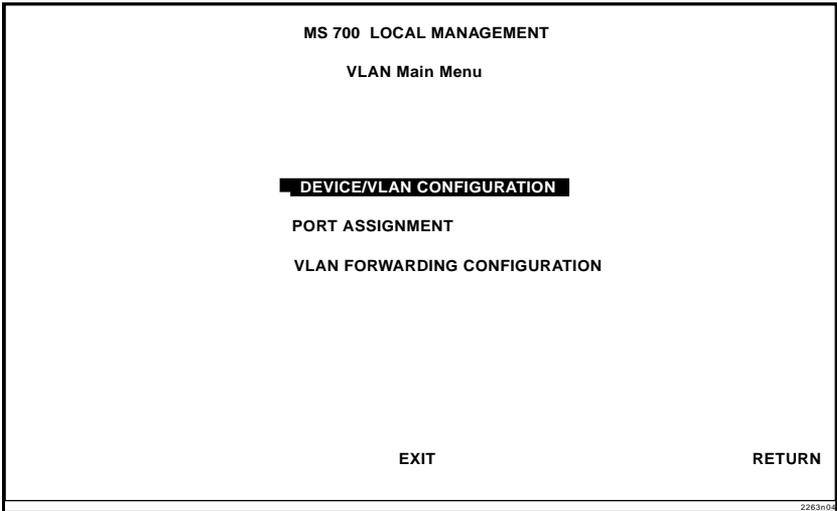


Figure 3-2 VLAN Main Menu Screen

The following describes each menu item on the VLAN Main Menu screen:

DEVICE/VLAN CONFIGURATION

The Device/VLAN Configuration screen enables the user to view, add, enable, or disable VLANs within a network switch device. It also enables the user to configure attributes that apply to the entire switch and/or VLANs. Refer to Section 3.3 for additional information.

PORT ASSIGNMENT

The Port Assignment screen displays a list of ports and enables the user to assign a Port VLAN ID (PVID) to each port. The Port Assignment screen also allows the user to change the operational mode of a port. Refer to Section 3.4 for additional information.

VLAN FORWARDING CONFIGURATION

The VLAN Forwarding Configuration screen enables the user to define or 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 3.5 for additional information.

3.3 DEVICE/VLAN CONFIGURATION SCREEN

The Device/VLAN Configuration screen enables the user to define operating characteristics for the switch and enables the user to add, delete, enable, and disable VLANs. The screen will display up to six VLANs simultaneously.

To access the Device/VLAN Configuration screen from the VLAN Main Menu, use the arrow keys to highlight the **DEVICE/VLAN CONFIGURATION** menu item and press ENTER. The Device/VLAN Configuration screen, Figure 3-3, displays.

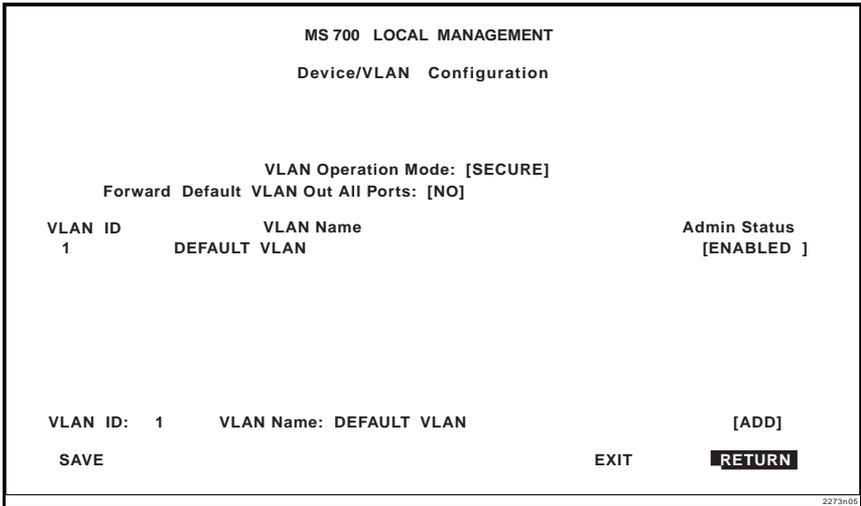


Figure 3-3 Device/VLAN Configuration Screen

The following defines each field of the Device/VLAN Configuration Screen:

VLAN Operation Mode (Toggle)

Displays the security mode used by the VLAN switch. This field toggles between OPEN or SECURE. The Secure mode classifies frames as known if a MAC address and VLAN combination in the Filtering Database is found. Open mode classifies a frame as known if a MAC address match is located.

Forward Default VLAN Out All Ports (Toggle)

Allows the Administrator to assign or remove the default VLAN from the Egress List for all ports. When set to YES, the default VLAN is added to the Egress List of all ports that do not already include it. When set to NO, the default VLAN is removed from the Egress List of any port that does not have the default VLAN as its PVID.

VLAN ID - upper part of screen (Read-Only)

A list of the assigned VLAN IDs that are configured in the module. Initially, only the Default VLAN (VLAN ID: 1) is listed.

VLAN Name - upper part of screen (Read-Only)

A list of the names assigned to the corresponding VLAN IDs.

Admin Status (Toggle)

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.

VLAN ID - lower part of screen (Input)

Accepts input from the user to define new VLAN IDs, modify VLAN Names or to select existing VLAN IDs for deletion.

VLAN Name - lower part of screen (Input)

Accepts input from the user to assign names to new VLANs. The VLAN Name is an optional attribute of a VLAN, and is not required for VLAN operation.

ADD/DEL (Toggle)

Toggles the action taken between adding the named VLAN to the switch or deleting the named VLAN from the switch.

3.3.1 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 are reserved and 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 4095" and the field will refresh with the previous value.

3. Use the arrow keys to highlight the **VLAN Name** field.



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.

4. Type a name of up to 32 ASCII characters in the VLAN Name field (optional).
5. Use the arrow keys to highlight the **[ADD/DEL]** field.
6. 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.

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

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

3.3.3 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.



The default VLAN cannot be deleted from the list.

3.3.4 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.

3.3.5 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.



The default VLAN cannot be disabled.

3.3.6 Changing the VLAN Operation Mode

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

1. Use the arrow keys to highlight the **VLAN Operation Mode** field.
2. Press the SPACE bar or BACKSPACE to toggle between **SECURE** and **OPEN**.
3. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message “SAVED OK” displays.

3.3.7 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 Egress Lists of all ports on the switch. The NO selection removes the default VLAN from the Egress 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.

3.3.8 Paging Through the VLAN List

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



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.

3.4 PORT ASSIGNMENT SCREEN

The Port Assignment screen enables the user to select a mode of operation for each port and to assign a Port VLAN Identification (PVID) to each port.

To access the Port Assignment screen from the VLAN Main Menu, use the arrow keys to highlight the **PORT ASSIGNMENT** menu item and press ENTER. The Port Assignment screen, Figure 3-4, displays.

Module	Port	Port Mode	VLAN ID	VLAN Name
2	1	[HYBRID]	[0001]	DEFAULT VLAN
2	2	[HYBRID]	[0001]	DEFAULT VLAN
2	3	[HYBRID]	[0001]	DEFAULT VLAN
2	4	[HYBRID]	[0001]	DEFAULT VLAN
2	5	[HYBRID]	[0001]	DEFAULT VLAN
2	6	[HYBRID]	[0001]	DEFAULT VLAN
2	7	[HYBRID]	[0001]	DEFAULT VLAN
2	8	[HYBRID]	[0001]	DEFAULT VLAN
2	9	[HYBRID]	[0001]	DEFAULT VLAN
2	10	[HYBRID]	[0001]	DEFAULT VLAN
2	11	[HYBRID]	[0001]	DEFAULT VLAN
2	12	[HYBRID]	[0001]	DEFAULT VLAN

SAVE Module [2] NEXT EXIT **RETURN**

2263n01

Figure 3-4 Port Assignment Screen

The following defines each field of the Port Assignment screen:

Module (Read-Only)

Indicates the module number (slot number in the chassis) of the device being configured.

Port (Read-Only)

Lists the port numbers of the interfaces of the current module.

Port Mode (Selectable)

Displays the current operational mode for the corresponding port.

VLAN ID (Selectable)

The ID number of the VLAN that is associated with the current port. This is the VLAN ID that any untagged frame will be classified into.

VLAN Name (Read-Only)

The name that is associated with the current VLAN ID.

3.4.1 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:
 - a. **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's Egress List includes all VLANs.
 - b. **1d TRUNK**: This mode sets the port for transmitting to a legacy 802.1d switch fabric and allows multiple VLANs to share services. In this mode, all frames are transmitted untagged, and the switch expects to receive only untagged frames through the 1d Trunk port. This mode also updates the Egress List for the port to be eligible for all VLANs. The 1d Trunk mode can be used in conjunction with the Open Mode (see Section 2.3.5, Setting the Operational Mode) and the Default VLAN to share a connection among multiple VLANs, for example, making a server available to two or more separate VLANs.
 - c. **HYBRID**: This mode assigns the PVID and the forwarding list of the Default VLAN to the port. If the PVID changes, the result is the replacement of the previous PVID with the new PVID in the Egress List. The exception to this is that the Default PVID does remain on the list if the switch is configured to forward the Default VLAN out all ports. The forwarding list always has an untagged frame format for the entry that matches the PVID. A Hybrid port will receive and allow both tagged and untagged frames.

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.

3.4.2 Assigning a VLAN ID

The Port Assignment 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:

1. Use the arrow keys to highlight the **MODULE** field number at the bottom of the screen. Use the **SPACE** bar or **BACKSPACE** key to step sequentially through the available module numbers.
2. When the desired module is selected, press ENTER.



It may be necessary to use the **NEXT** and **PREVIOUS** commands to page through the available ports on the selected module. For instructions, refer to Section 3.4.3, *Paging Through the Port List*.

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



New VLAN IDs must be created with the functions available on the Device/VLAN Configuration screen, discussed in Section 3.3.

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

3.4.3 Paging Through the Port List

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



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.

3.5 VLAN FORWARDING CONFIGURATION SCREEN

The VLAN Forwarding Configuration screen enables the user to view the ports included in a VLAN's Forwarding List. The user can also define which ports to include in the VLAN's Forwarding List. The formats of the frames (Tagged or Untagged) that a VLAN port will forward can also be specified with this screen.

To access the VLAN Forwarding Configuration screen from the VLAN Main Menu screen, use the arrow keys to highlight the **VLAN FORWARDING CONFIGURATION** menu item and press ENTER. The VLAN Forwarding Configuration screen, Figure 3-5, displays.

MS 700 LOCAL MANAGEMENT			
VLAN Forwarding Configuration			
Current VLAN Ports	Port	Type	Frame Format
Module 2 Port 2	Ethernet	Frontpanel	Untagged
Module 2 Port 3	Ethernet	Frontpanel	Untagged
Module 2 Port 4	Ethernet	Frontpanel	Untagged
Module 2 Port 5	Ethernet	Frontpanel	Untagged
Module 2 Port 6	Ethernet	Frontpanel	Untagged
Module 2 Port 7	Ethernet	Frontpanel	Untagged
Module 2 Port 8	Ethernet	Frontpanel	Untagged
Module 2 Port 9	Ethernet	Frontpanel	Untagged
VLAN ID: [1] VLAN NAME: DEFAULT VLAN			[ADD]
Module: [3]	Port: [1]	Ethernet Frontpanel	Frame Format: [UNTAGGED]
SAVE	NEXT	EXIT	RETURN

Figure 3-5 VLAN Forwarding Configuration Screen

The following defines each field of the VLAN Forwarding Configuration screen:

Current VLAN Ports (Read-Only)

Lists the ports of the module that are members of the selected VLAN.

Port Type (Read-Only)

The MIB2 interface description for the selected switch port.

Frame Format- *upper part of screen* (Read-Only)

The format of frames (TAGGED or UNTAGGED) that the port is currently forwarding.

VLAN ID (Selectable)

The number of the VLAN under examination. This screen displays the Forwarding List for the VLAN ID in this field.

VLAN Name (Read-Only)

The name associated with the VLAN ID.

ADD/DEL (Toggle)

Swaps the action taken between adding a port to the Forwarding List or removing the port from the Forwarding List.

Module (Selectable)

The module number (slot number in the chassis) of the device being configured. This field is not selectable if the device being configured is a standalone switch.

Port (Selectable)

The port number of the interface being configured.

Frame Format- *lower part of screen* (Toggle)

Selects the format of frames (TAGGED or UNTAGGED) that will be transmitted by the selected port for this VLAN.

3.5.1 Viewing Current VLAN Ports

To display the 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 Forwarding List for the selected VLAN.

3.5.2 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.

3.5.3 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 **Module** field. Step through the available modules by pressing the **SPACE** bar or **BACKSPACE**.
3. Use the arrow keys to highlight the **Port** field. Step through the available ports on the module with the **SPACE** bar or **BACKSPACE**.
4. Use the arrow keys to highlight the **[ADD/DEL]** field. Press the **SPACE** bar to select **[ADD]**. Press **ENTER**.

The Forwarding List entry will be added to the list of current VLANs once the configuration is saved.

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

The port is added to the Forwarding List for the selected VLAN. At the same time, the Egress List for the port so assigned is updated to contain the new VLAN and Frame Format.

3.5.4 Deleting Forwarding List Entries

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

1. Enter the VLAN ID.
2. Enter the VLAN name.
3. Use the arrow keys to highlight the **[ADD/DEL]** field.
4. Press the SPACE bar to select **[DEL]**. Press ENTER.
5. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
6. Press ENTER. The message “SAVED OK” displays. The port has been removed from the VLAN list.

3.5.5 Changing the Frame Format

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

1. Use the arrow keys to highlight the **Module** field. Use the SPACE bar or BACKSPACE to step to the desired module and port combination. Press ENTER.
2. Use the arrow keys to highlight the **Port** field. Step through the available ports by pressing the SPACE bar or BACKSPACE.
3. Using the arrow keys, select the **Frame Format** field. Use the SPACE bar or BACKSPACE to toggle between **TAGGED** or **UNTAGGED**.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
5. Press ENTER. The message “SAVED OK” displays.

3.6 QUICK VLAN WALKTHROUGH

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

This walkthrough begins at the VLAN Main Menu screen for a DLM6C-AA chassis. Follow the instructions in your device user's guide to navigate to this Local Management screen.



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

1. On the VLAN Main Menu screen, use the arrow keys to highlight the **DEVICE/VLAN CONFIGURATION** menu item. Press ENTER. The Device/VLAN Configuration screen displays.
2. Verify the current VLAN Operation Mode (SECURE) and Forwarding Mode (NO). If these fields display values other than those given here, follow the instructions in Section 3.3.6 and Section 3.3.7.
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 **VLAN Name** field. Type “**TEST VLAN**” in the VLAN Name field. Press ENTER.
5. Use the arrow keys to highlight the [ADD/DEL] field.
6. Press the SPACE bar to toggle the field to [ADD]. Press ENTER. The VLAN is added to the list.
7. 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. The screen should now look like Figure 3-6.
 - 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, we will return to this screen and enable the VLAN.

```

MS 700 LOCAL MANAGEMENT
Device/VLAN Configuration

VLAN Operation Mode: [SECURE]
Forward Default Vlan Out ALL Ports: [NO]

VLAN ID      VLAN Name      Admin Status
 1          DEFAUL VLAN  [ENABLED ]
 2          TEST VLAN  [DISABLED]

VLAN ID: 2      VLAN NAME: TEST VLAN      [ADD]
[SAVE]                               EXIT      RETURN

```

Figure 3-6 Walkthrough Stage One

We can now proceed to assign a port to this new VLAN.

8. Use the arrow keys to highlight the **RETURN** command at the bottom of the screen. Press ENTER. The VLAN Main Menu screen displays. Use the arrow keys to select the **PORT ASSIGNMENT** menu item and press ENTER. The Port Assignment screen displays.
9. Use the arrow keys to highlight the **MODULE** field number at the bottom of the screen. Use the SPACE bar or BACKSPACE key to step sequentially through the available module numbers. The ports and configuration of the module will be automatically updated.
 - For the purposes of this walkthrough, we have elected to configure port 3 on module 2.
10. Use the arrow keys to highlight the **VLAN ID** field for the module and port combination you wish to change.
 - 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 **2** (the new VLAN ID) is displayed, the **VLAN Name** field updates and displays 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 on module 2 is now configured to the TEST VLAN. The TEST VLAN is also added to the Egress List for Port 3 on Module 2 with a frame format of Untagged. The screen should now look like Figure 3-7.

MS 700 LOCAL MANAGEMENT				
Port Assignment				
Module	Port	Port Mode	VLAN ID	VLAN Name
2	1	[HYBRID]	[0001]	DEFAULT VLAN
2	2	[HYBRID]	[0001]	DEFAULT VLAN
2	3	[HYBRID]	[0002]	TEST VLAN
2	4	[HYBRID]	[0001]	DEFAULT VLAN
2	5	[HYBRID]	[0001]	DEFAULT VLAN
2	6	[HYBRID]	[0001]	DEFAULT VLAN
2	7	[HYBRID]	[0001]	DEFAULT VLAN
2	8	[HYBRID]	[0001]	DEFAULT VLAN
2	9	[HYBRID]	[0001]	DEFAULT VLAN
2	10	[HYBRID]	[0001]	DEFAULT VLAN
2	11	[HYBRID]	[0001]	DEFAULT VLAN
2	12	[HYBRID]	[0001]	DEFAULT VLAN

SAVE Module: [2] NEXT EXIT RETURN

Figure 3-7 Walkthrough Stage Two

Now that port 3 on module 2 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.

- For the purposes of this walkthrough, port 10 on module 2 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 Egress List. All frame formats for this new 1Q Trunk port are set to tagged. The screen should now look like Figure 3-8.

MS 700 LOCAL MANAGEMENT				
Port Assignment				
Module	Port	Port Mode	VLAN ID	VLAN Name
2	1	[HYBRID]	[0001]	DEFAULT VLAN
2	2	[HYBRID]	[0001]	DEFAULT VLAN
2	3	[HYBRID]	[0002]	TEST VLAN
2	4	[HYBRID]	[0001]	DEFAULT VLAN
2	5	[HYBRID]	[0001]	DEFAULT VLAN
2	6	[HYBRID]	[0001]	DEFAULT VLAN
2	7	[HYBRID]	[0001]	DEFAULT VLAN
2	8	[HYBRID]	[0001]	DEFAULT VLAN
2	9	[HYBRID]	[0001]	DEFAULT VLAN
2	10	[1Q TRUNK]	[0001]	DEFAULT VLAN
2	11	[HYBRID]	[0001]	DEFAULT VLAN
2	12	[HYBRID]	[0001]	DEFAULT VLAN
2				
SAVE		Module: [2]	NEXT	EXIT RETURN

Figure 3-8 Walkthrough Stage Three

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

15. On the VLAN Main Menu screen, use the arrow keys to highlight the **DEVICE/VLAN CONFIGURATION** menu item. Press ENTER. The Device/VLAN Configuration screen, shown in Figure 3-9, displays.

```
MS 700 LOCAL MANAGEMENT
Device/VLAN Configuratyion

VLAN Operation Mode: [ SECURE ]
Forward Default VLAN Out ALL Ports: [ NO ]

VLAN ID      VLAN Name      Admin Status
 1          DEFAULT VLAN  [ ENABLED ]
 2          TEST VALN  [ ENABLED ]

VLAN ID : 1      VLAN Name : DEFAULT VLAN

SAVE          EXIT          RETURN
```

Figure 3-9 Final Walkthrough Stage

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, a VLAN port, and a 1Q Trunk port.

CHAPTER 4

EXAMPLES

This chapter provides examples of how VLAN aware MultiSwitch 700 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

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.

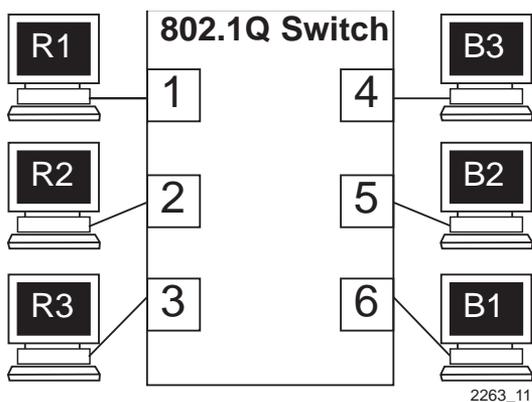


Figure 4-1 Initial Switch State

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 and the operational mode is set. Since traffic isolation is to be based on VLAN membership alone, the switch is set to SECURE mode from the 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 Administration screen and assigns the interfaces to the VLANs.
 - Interfaces 1, 2, and 3: VLAN ID 002 (Red VLAN)
 - Interfaces 4, 5, and 6: VLAN ID 003 (Blue VLAN)

- Now that the ports have been assigned, the VLANs are enabled from the Device/VLAN Configuration screen. The switch automatically updates the Forwarding Lists for the Red and Blue VLANs and updates the Egress Lists for all the ports on the switch.

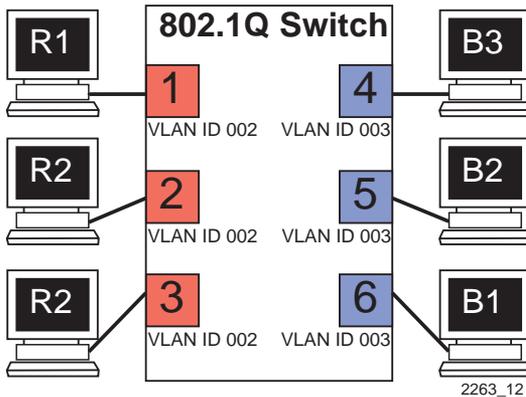


Figure 4-2 Switch Configured for VLANs

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.

- Station R1 transmits the broadcast frame. The switch receives this frame on Interface 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 Interface 1 is assigned to, the Red VLAN.
- At the same time, the switch adds the source MAC address of the frame and VLAN it was learned from to its Source Address Table. In this fashion it learns that station R1 is located out Interface 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. In this case, the frame is sent to Interfaces 2 and 3.

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

4. Station R2, having received the broadcast from R1 and recognized it, transmits a unicast frame as a response. The switch receives this frame on Interface 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, 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 Interface 1.
6. The switch examines the Egress List for interface 1 and determines that the port is configured to forward untagged frames classified into the Red VLAN. The switch transmits the frame with no VLAN tag header.
7. The switch forwards the frame out Interface 1. Any other unicast transmissions between stations R1 and R2 will be handled identically.

4.2 EXAMPLE 2

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

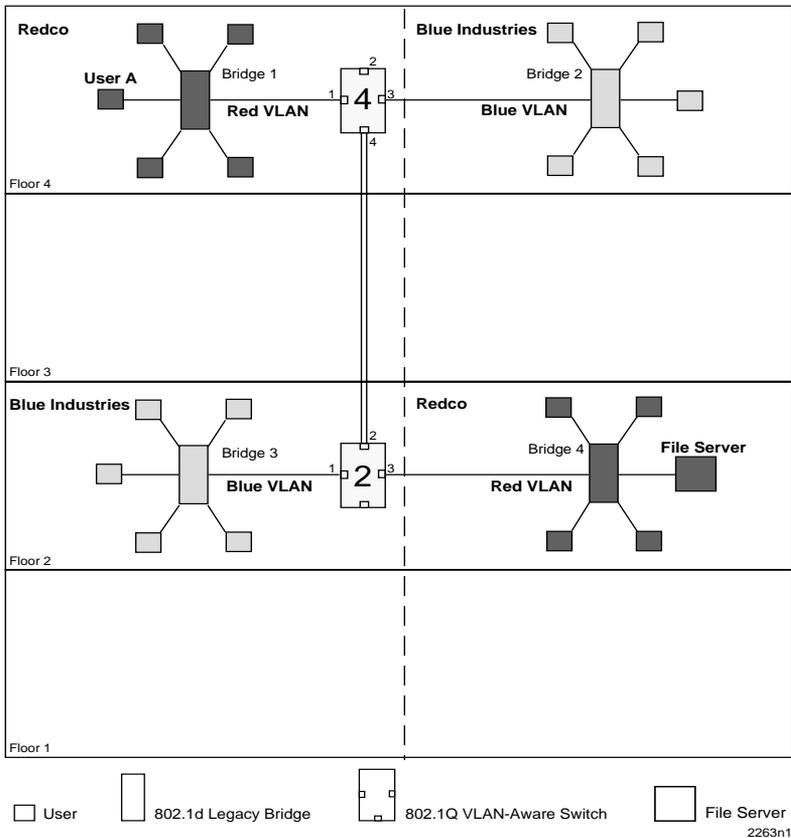


Figure 4-3 Example 2

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. The VLAN Operational Mode is set to SECURE using the Device/VLAN Configuration screen.
2. Two VLANs are added to the list of VLANs in the Device/VLAN Configuration screen. In this example they are as follows:
 - VLAN ID 222 with a VLAN Name of Red
 - VLAN ID 223 with a VLAN Name of Blue
3. A Port VLAN ID is assigned to each port (1, 3, and 4) as follows using the Port Assignment screen:
 - Port 1, VLAN ID: 222 for the Red VLAN
 - Port 3, VLAN ID: 223 for the Blue VLAN
 - Port 4, Port Mode: 1Q Trunk

This causes the switch to classify all frames received as belonging to the VLAN specified and to replace the current Default VLAN settings in the Egress List with these settings, so that port 1 is part of the Red VLAN, port 3 is part of the Blue VLAN, and both are set as VLAN frame format of untagged. Port 4 is set as an 802.1Q Trunk port, which makes the port Egress List contain all VLANs, and all frames forwarded out this port are forwarded as tagged frames. This tag allows the receiving switch to maintain the original frame classification.

Switch 2

Switch 2 is set as follows:

1. The VLAN Operational Mode is set to SECURE using the Device/VLAN Configuration screen.
2. Two VLANs are added to the list of VLANs in the Device/VLAN Configuration screen. In this example they are as follows:
 - VLAN ID 222 with a VLAN Name of Red
 - VLAN ID 223 with a VLAN Name of Blue
3. A Port VLAN ID is assigned to each port (1, 2, and 3) as follows using the Port Assignment screen:
 - Port 1, VLAN ID: 223 for the Blue VLAN
 - Port 2, Port Mode: 1Q Trunk
 - 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. Port 2 is set as an 802.1Q Trunk port, which makes the port Egress List contain all VLANs and sets all frames forwarded out this port to be tagged frames.

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.

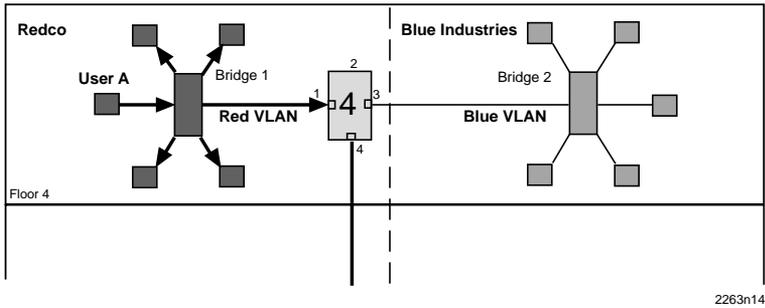


Figure 4-4 Bridge 1 Broadcasts Frames

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. In this example, it is only port 4.

Switch 4 updates its Source Address Table if it didn't already have a dynamic entry for MAC address "Y" and VLAN "Red". Because Switch 4 received the frame on port 1 it does not forward the packet 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 tag 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.

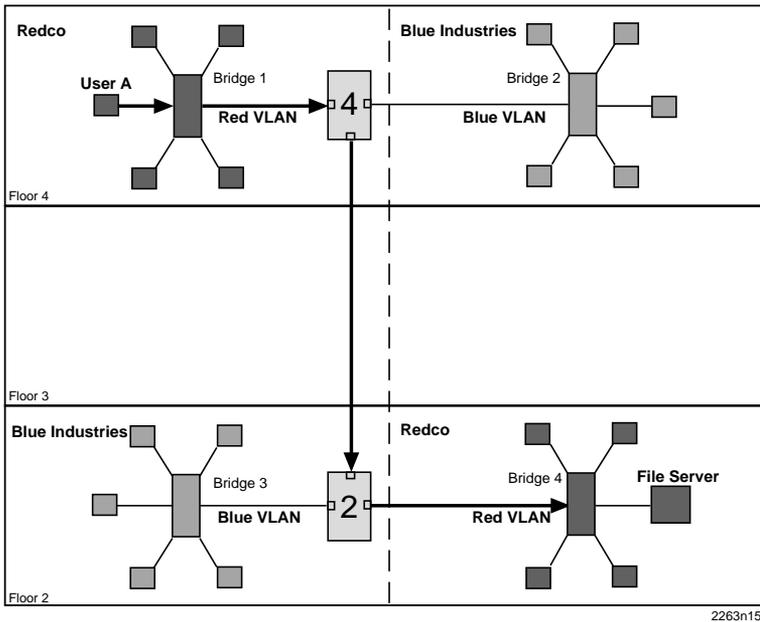


Figure 4-5 Transmitting to Switch 4

- 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 for MAC address "Y" and VLAN Red 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.

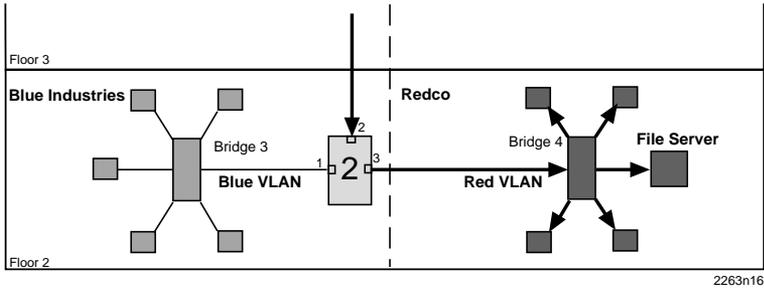


Figure 4-6 Transmitting to Bridge 4

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”, VLAN Red. All switches update their Source Address Tables for the File Server’s MAC address “Z”, VLAN Red combination as the frame is forwarded through the switch fabric to User A. The 802.1d bridge update their Source Address Tables based on the source MAC address and receive port and the 802.Q 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 4 as a tagged frame classified as belonging to the Red VLAN. Switch 4 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

This final example illustrates the use of a 1d Trunk to connect a device to a network of port based VLAN switches. It also covers the uses of the Open mode of switch operation.

In this example, illustrated in Figure 4-7, a merger has taken place between Redco and Blue Industries, the companies in the previous example. The two companies have become divisions within a single corporation, Green, Inc. A third group of stations, the Green, Inc. staff, is added to the facility. Also, the Green, Inc. Network Administrators add a Mail Server to the network on the first floor.

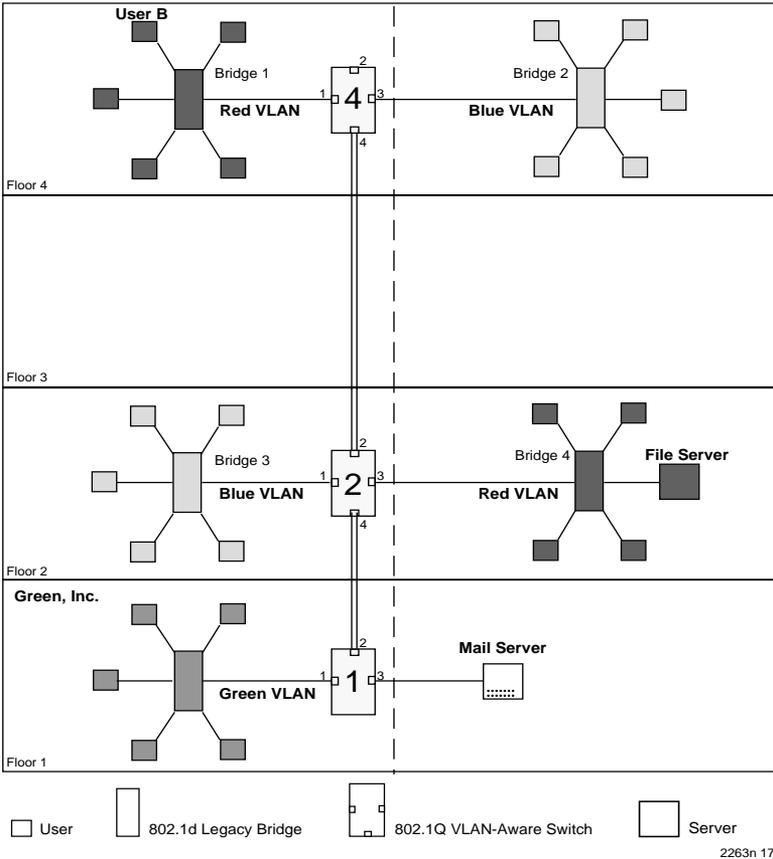


Figure 4-7 Example 3

The Green, Inc. Network Administrators want to continue to separate normal network traffic between the Blue and Red VLANs, and create a new isolated VLAN for Green, Inc. 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. While a new 1Q Trunk port must be activated and configured on Switch 2, and the operational modes of the switches must be changed, there are no other real changes to the network above the first floor.

Switch 4

Switch 4 is set as follows:

1. The VLAN Operational Mode is set to OPEN using the Device/VLAN Configuration screen.
2. The Forward Mode for the switch is set to YES, adding the Default VLAN to the Egress List of every switch port.

Switch 2

Switch 2 is set as follows:

1. The VLAN Operational Mode is set to OPEN using the Device/VLAN Configuration screen.
2. The Forward Mode for the switch is set to YES, adding the Default VLAN to the Egress List of every switch port.
3. 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 Egress List contain all VLANs, and all frames forwarded out this port are forwarded as tagged frames.

Switch 1

Switch 1 is set as follows:

1. The VLAN Operational Mode is set to OPEN using the Device/VLAN Configuration screen.
2. The Forward Mode for the switch is set to YES, adding the Default VLAN to the Egress List of every switch port.

3. One VLAN is added to the list of VLANs in the Device/VLAN Configuration screen. In this example is set as follows:
 - VLAN ID 224 with a VLAN Name of Green
4. A Port VLAN ID is assigned to the switch ports as follows using the Port Assignment screen:
 - Port 1, VLAN ID: 224 for the Green VLAN
 - Port 2, Port Mode: 1Q Trunk
 - Port 3, Port Mode: 1d Trunk

These settings change 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. Port 2 is set as an 802.1Q Trunk port, which makes the port Egress List contain all VLANs and sets all frames forwarded out this port to be 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.

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.
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, identifying User B and 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.

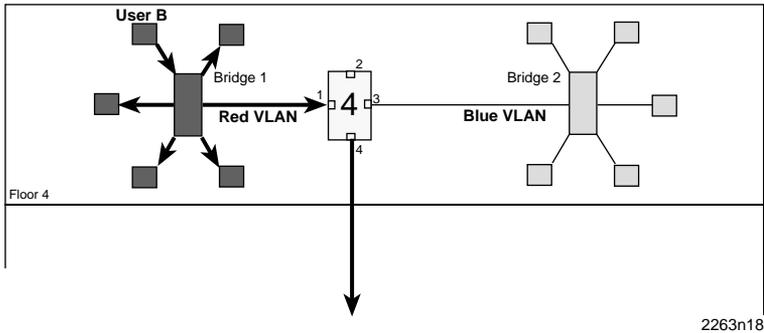


Figure 4-8 Bridge 1 Broadcasts Frames

- Switch 2 receives the tagged Red VLAN frame on port 2, as shown in Figure 4-9. The 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 to reflect the location of User B (port 2).

The frame forwarded out port 3 has its 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.

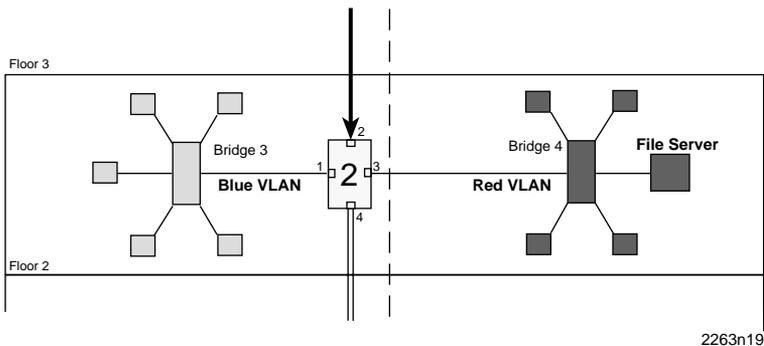


Figure 4-9 Switch 2 Forwards to 1Q Trunk

- 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 Tag is stripped from the frame and the frame is transmitted out port 3 as shown in Figure 4-10. The Source Address Table for Switch 1 is updated to contain User B.

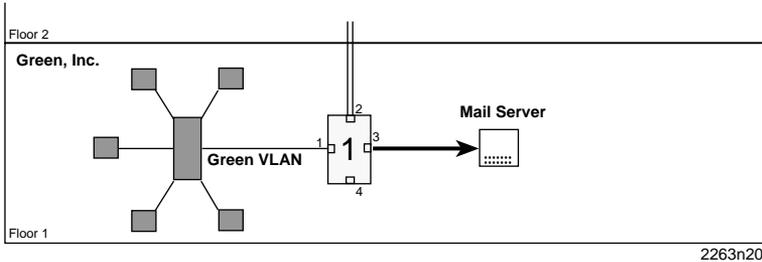


Figure 4-10 Switch 1 Forwards to 1d Trunk

- 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 against the Egress List for port 2. Since port 2 is a 1Q Trunk port, its Egress List contains 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 and updates that table to contain the MAC address and port combination of the Mail Server.

- 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 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 against the Egress List for port 2. Port 2's Egress List contains all VLANs, and is a 1Q Trunk port, so the frame is transmitted, tagged, out port 2.

7. Switch 4 receives the frame on its 1Q port and examines the frame's Tag. The frame maintains its Default VLAN classification. The switch also refers to its Source Address Table 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 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 against the Egress List for port 1. As port 1 is considered eligible to transmit to the Default VLAN and the switch is in the open mode, the frame is forwarded out port 1 and the tag is removed.

8. Bridge 1 receives the frame and recognizes User B's MAC address. The frame is forwarded to the correct interface 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.

Numerics

1D Trunk 3-11, 4-11

1Q Trunk 3-11, 4-4

C

Configuration 2-2

D

Default VLAN 1-5

Device/VLAN Configuration screen 3-4

E

Egress list 1-5

F

Filtering Database 1-5

Forwarding list 1-5

- adding entries 3-16

- customizing 2-2

- deleting entries 3-17

- viewing 3-15

Forwarding mode

- changing 3-9

Frame format

- changing 3-17

Frames

- tagged 1-4, 2-5

- untagged 1-4, 2-4

H

Hybrid 3-11

L

Lists

- Egress 1-5

- Forwarding 1-5

Local Management 3-1

O

Operational mode 2-3

 changing 3-8

 open 2-5

 secure 2-6

P

Port Assignment screen 3-10

Port mode

 1D Trunk 3-11

 1Q Trunk 3-11

 changing 3-11

 Hybrid 3-11

PVID 1-5

S

Screens

 Device/VLAN Configuration 3-4

 Port Assignment 3-10

 VLAN Forwarding Configuration 3-14

 VLAN Main Menu 3-2

Station 2-1

Switch 2-1

T

Tag 1-4

Tag Header 1-4

Tagged frame 1-4, 2-5

Trunk 1-5

U

Untagged frame 1-4, 2-4

V

VLAN

 assigning ports 2-2

 components 2-1

 configuration 2-2

- default VLAN 1-5
- defining 2-2
- definition 1-1–1-4
- operation 2-3
- terms 1-4
- types 1-3
- VLAN Configuration
 - deleting 3-7
 - disabling 3-8
 - enabling 3-8
- VLAN Forwarding Configuration screen 3-14
- VLAN ID 1-4
 - assigning 3-12
- VLAN Main Menu screen 3-2
- VLAN name 1-4

digital