Creating VLANs with the DIGITAL MultiSwitch 700 and GIGAswitch/Router Network Modules

March 1999

Prepared by Douglas Bonner, NAC Product Management

Special Contributions by Fraser Murphy, NAC Engineering

Abstract: This white paper describes the capabilities and uses of IEEE 802.1Q virtual local area networks (VLANs) with the DIGITAL MultiSwitch 700 and DIGITAL GIGAswitch/Router network modules.

Notice

The information in this publication is subject to change without notice and is provided “AS IS” WITHOUT WARRANTY OF ANY KIND. THE ENTIRE RISK ARISING OUT OF THE USE OF THIS INFORMATION REMAINS WITH RECIPIENT. IN NO EVENT SHALL COMPAQ BE LIABLE FOR ANY DIRECT, CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE OR OTHER DAMAGES WHATSOEVER (INCLUDING WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION OR LOSS OF BUSINESS INFORMATION), EVEN IF COMPAQ HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The limited warranties for Compaq products are exclusively set forth in the documentation accompanying such products. Nothing herein should be construed as constituting a further or additional warranty.

This publication does not constitute an endorsement of the product or products that were tested. The configuration or configurations tested or described may or may not be the only available solution. This test is not a determination or product quality or correctness, nor does it ensure compliance with any federal state or local requirements.

Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Compaq, Contura, Deskpro, Fastart, Compaq Insight Manager, LTE, PageMarq, Systempro, Systempro/LT, ProLiant, TwinTray, ROMPaq, LicensePaq, QVision, SLT, ProLinea, SmartStart, NetFlex, DirectPlus, QuickFind, RemotePaq, BackPaq, TechPaq, SpeedPaq, QuickBack, PaqFax, Presario, SilentCool, CompaqCare (design), Aero, SmartStation, MiniStation, and PaqRap, registered United States Patent and Trademark Office.

Netelligent, Armada, Cruiser, Concerto, QuickChoice, ProSignia, Systempro/XL, Net1, LTE Elite, Vocalyst, PageMate, SoftPaq, FirstPaq, SolutionPaq, EasyPoint, EZ Help, MaxLight, MultiLock, QuickBlank, QuickLock, UltraView, Innovate logo, Wonder Tools logo in black/white and color, and Compaq PC Card Solution logo are trademarks and/or service marks of Compaq Computer Corporation.

DIGITAL and the DIGITAL logo are trademarks of Compaq Computer Corporation.

Cabletron and GIGAswitch are trademarks of Cabletron Systems Inc.

Microsoft, Windows, Windows NT, Windows NT Server and Workstation, Microsoft SQL Server for Windows NT are trademarks and/or registered trademarks of Microsoft Corporation.

NetWare and Novell are registered trademarks and intraNetWare, NDS, and Novell Directory Services are trademarks of Novell, Inc.

Pentium is a registered trademark of Intel Corporation.

Contents

VLAN Overview

Virtual LANs (VLANs) are a means of dividing a physical network into several logical (virtual) LANs. The division can be done on the basis of various criteria, giving rise to different types of VLANs. For example, the simplest type of VLAN is the port-based VLAN. Port-based VLANs divide a network into a number of VLANs by assigning a VLAN to each port of a switching device. Then, any traffic received on a given port of a switch *belongs* to the VLAN associated with that port.

Figure 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.

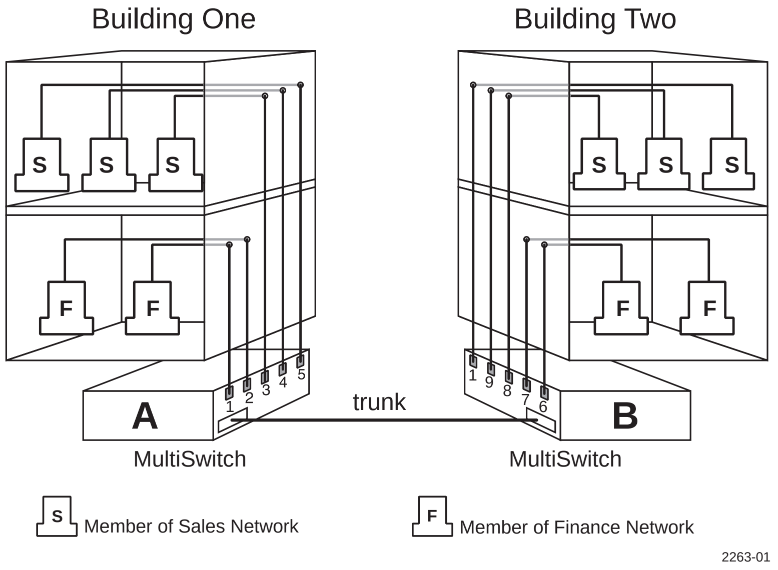


Figure 1. Example of a VLAN

In this example, the Sales and Finance workstations are 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 propagates to all switch ports on MultiSwitch A, crosses the high speed link to MultiSwitch B, and propagates to all switch ports on MultiSwitch B. The switches treat each port as equivalent to any other port, and have no understanding of the departmental memberships of each workstation.

In a port-based VLAN environment, each switch 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 reaches MultiSwitch A, is sent to the ports connected to other local members of the Sales VLAN, crosses the high-speed link to MultiSwitch B, and is sent to any other ports and workstations on MultiSwitch B that are members of the Sales VLAN.

VLANs are primarily used for broadcast containment. A layer-2 (L2) broadcast frame is normally transmitted all over a bridged network. By dividing the network into VLANs, the *range* of a broadcast is limited, that is, the broadcast frame is transmitted only to the VLAN to which it belongs. This reduces the broadcast traffic on a network by an appreciable factor.

Types of VLANs

The type of VLAN depends upon one criterion — how a received frame is classified as belonging to a particular VLAN. VLANs can be categorized into the following types:

- Port based
- MAC address based
- Protocol based
- Subnet based
- Multicast based
- Policy based

Port-Based VLANs

Ports of L2 devices (switches, bridges) are assigned to VLANs. Any traffic received by a port is classified as belonging to the VLAN to which the port belongs. For example, if ports 1, 2, and 3 belong to the VLAN named “Marketing,” then a broadcast frame received by port 1 is transmitted on ports 2 and 3. It is not transmitted on any other port. Also see Figure 1 on page 1 for an example of port-based VLANs.

MAC-Address-Based VLANs

In this type of VLAN, each switch (or a central VLAN information server) keeps track of all MAC addresses in a network and maps them to VLANs based on information configured by the network administrator. When a frame is received at a port, its destination MAC address is looked up in the VLAN database. The VLAN database returns the name of the VLAN to which this frame belongs.

This type of VLAN is powerful in the sense that network devices such as printers and workstations can be moved anywhere in the network without the need for network reconfiguration. However, the administration is intensive because all MAC addresses on the network need to be known and configured.

Protocol-Based VLANs

Protocol-based VLANs divide the physical network into logical VLANs based on protocol. When a frame is received at a port, its VLAN is determined by the protocol of the packet. For example, there could be separate VLANs for IP, IPX, and AppleTalk. An IP broadcast frame will be sent to all ports in the IP VLAN only.

Subnet-Based VLANs

Subnet-based VLANs are a subset of protocol-based VLANs and determine the VLAN of a frame based on the subnet to which the frame belongs. To do this, the switch must look into the network layer header of the incoming frame. This type of VLAN behaves similarly to a router by segregating different subnets into different broadcast domains.

Multicast-Based VLANs

Multicast-based VLANs are created dynamically for multicast groups. Typically, each multicast group corresponds to a different VLAN. This ensures that multicast frames are received only by those ports that are connected to members of the appropriate multicast group.

Policy-Based VLANs

Policy-based VLANs are the most general definition of VLANs. Each incoming (untagged) frame is looked up in a policy database, which determines the VLAN to which the frame belongs. For example, you could set up a policy that creates a special VLAN for all email traffic between the management officers of a company, so that this traffic will not be seen anywhere else.

MultiSwitch 700 Port-Based VLAN Operation

The DIGITAL MultiSwitch 700 firmware version 4.00.08 supports the prestandard IEEE 802.1Q specification for port-based VLANs. Currently, if 802.1Q is to be utilized, all modules in the chassis must be configured to operate in 802.1Q mode.

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.

The basic elements that combine to make up an 802.1Q VLAN are:

- Stations — any end unit that belongs to a network. In most cases, stations are the computers through which users access the network.
- Switches — VLAN-aware switches to which the stations are connected. The switch classifies received frames into VLAN memberships and transfers frames according to VLAN membership, with or without a VLAN tag header.

Preparing for MultiSwitch 700 VLAN Configuration

Planning is essential to 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
- To which ports those stations are connected

It may also be helpful to sketch out a diagram of your VLAN strategy. The examples provided in "Configuration Examples" may be useful in the planning process.

Refer to your device's user's guide for information on how to access Local Management. Perform all required initial setup operations. Navigate to the VLAN Main Menu screen to begin VLAN configuration for the device (see navigation information in "Example 1: Setting Up Two Shared VLANs" on page 27).

Configuration Process

The MultiSwitch 700 does not default to VLAN mode. You must configure and activate VLAN operation through software management. To perform the series of configuration steps required for VLAN operation, use the device's Local Management or clearVISN MultiSwitch 700 Manager screens. You will need to perform the following:

- Define a VLAN (with a unique identification number and optional name).
- Set the operational or security mode: open or secure.
- Assign ports to the VLAN.
- Configure any needed trunk ports.
- Customize the VLAN's forwarding list.
- Customize the port's egress list.
- Enable the VLAN.

Refer to the *DIGITAL MultiSwitch 700 Port Based VLAN User's Guide* for information on the steps required for VLAN configuration and management using the MultiSwitch 700 device's Local Management screens. To configure VLANs for the MultiSWitch 700 using the MultiSwitch 700 Manager, refer to the *DIGITAL MultiSwitch 700 Manager Tools Guide*.

Configuration Examples

This section provides examples of how a 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 the *DIGITAL MultiSwitch 700 Port Based VLAN User's Guide*. Each example also includes a description of how the frames transmitted from one user would traverse the network to its target device.

Example 1: Setting Up a VLAN on an Ethernet Switch

This first example looks at the configuration of a single Ethernet switch for VLAN operation. Two groups of three users — the blue users (B1, B2, B3) and the red users (R1, R2, R3) — are assigned to two VLANs to isolate them from one another. Figure 2 shows the initial state of the switch.

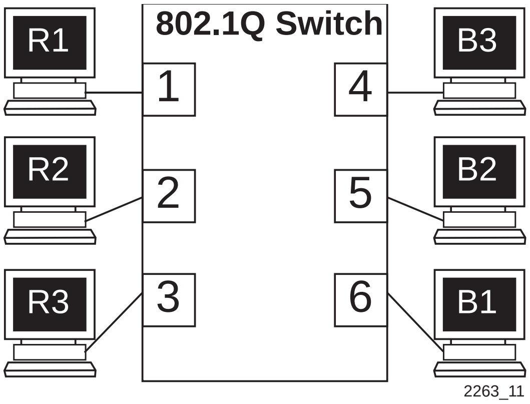


Figure 2. Initial Switch State

Solving the Problem

To set up this switch, users are 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)
4. With the ports 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 ports on the switch.

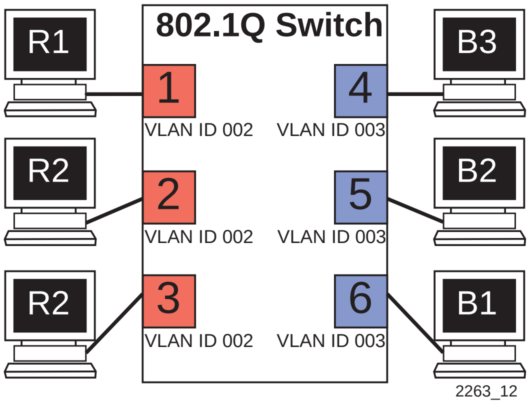


Figure 3. Switch Configured for VLANs

The switch now classifies each frame received as belonging to either the red or blue VLANs. Traffic from one VLAN is not forwarded to the members of the other VLAN, and all frames transmitted by the switch are normal, untagged Ethernet frames.

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 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 to which interface 1 is assigned, the red VLAN.

2. At the same time, the switch adds the source MAC address of the frame and VLAN where it was learned to its source address table. Thus, the switch learns that station R1 is located out of 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 of 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.

1. Station R2, receiving the broadcast from R1 and recognizing 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.
2. 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 of interface 1.
3. 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.
4. The switch forwards the frame out of interface 1. Any other unicast transmissions between stations R1 and R2 are handled identically.

Example 2: Setting Up VLANs Across Multiple Switches

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 802.1Q trunks between port-based VLAN switches.

As shown in Figure 4 on page 10, 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.

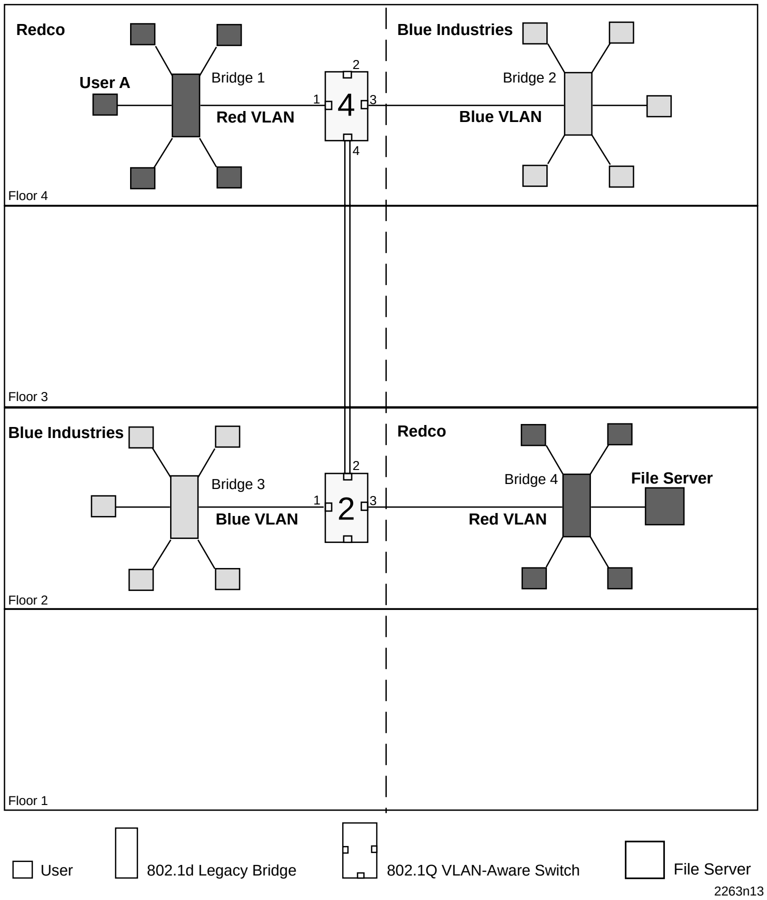


Figure 4. Example 2

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. 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 with a 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 of 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 the blue VLAN, port 3 is part of the red VLAN, and both are set with 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 of this port to be tagged frames.

Frame Handling

The following describes how the frames from user A are classified on switch 4 and traverse the network when user A attempts to log on to the file server on bridge 4. In this example, the MAC address of user A is *Y* and the MAC address for the file server is *Z*. The illustrations show 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 of all ports of bridge 1 as shown in Figure 5.

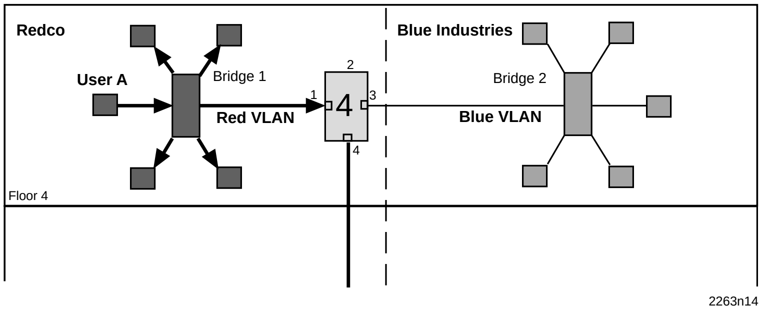


Figure 5. Bridge 1 Broadcast Frames

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 of 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 did not already contain 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 6 on page 13 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.

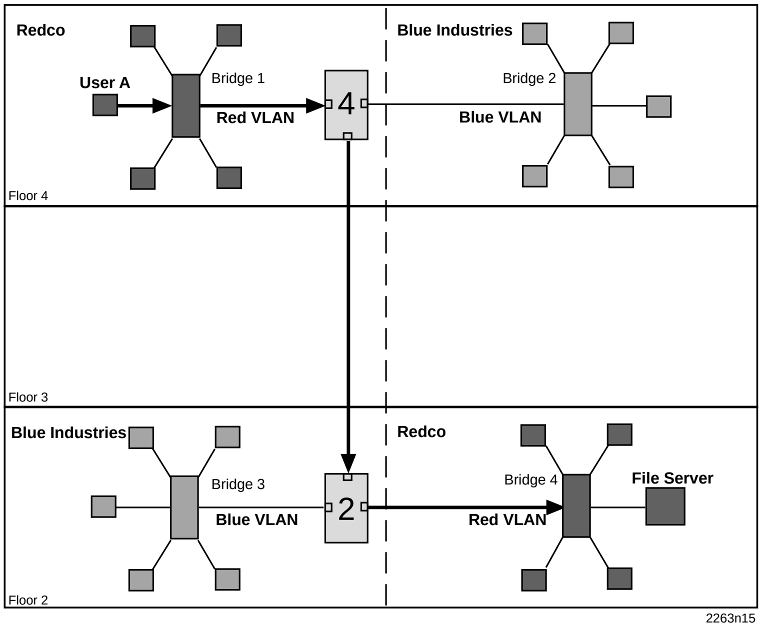


Figure 6. Transmitting to Switch 4

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's 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 the VLAN red, if necessary. The untagged frame is then transmitted out of port 3 to bridge 4. Bridge 4 forwards the frame out of all its ports because it is a broadcast frame, and the server receives it as shown in Figure 7.

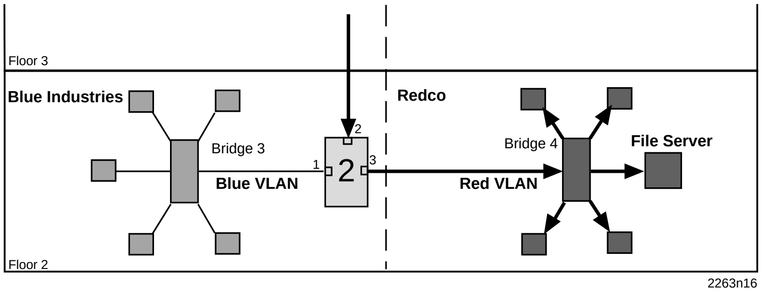


Figure 7. Transmitting to Bridge 4

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 the red VLAN. All switches update their source address tables for the file server's MAC address *Z*, red VLAN combination as the frame is forwarded through the switch fabric to user A. The 802.1d bridges 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 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.

Example 3: Connecting VLAN Switches to a Device Using a 1d Trunk

This final example illustrates the use of a 802.1d trunk to connect a device to a network of port-based VLAN switches. The example also covers the uses of the open mode of switch operation.

In this example, illustrated in Figure 8, 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.

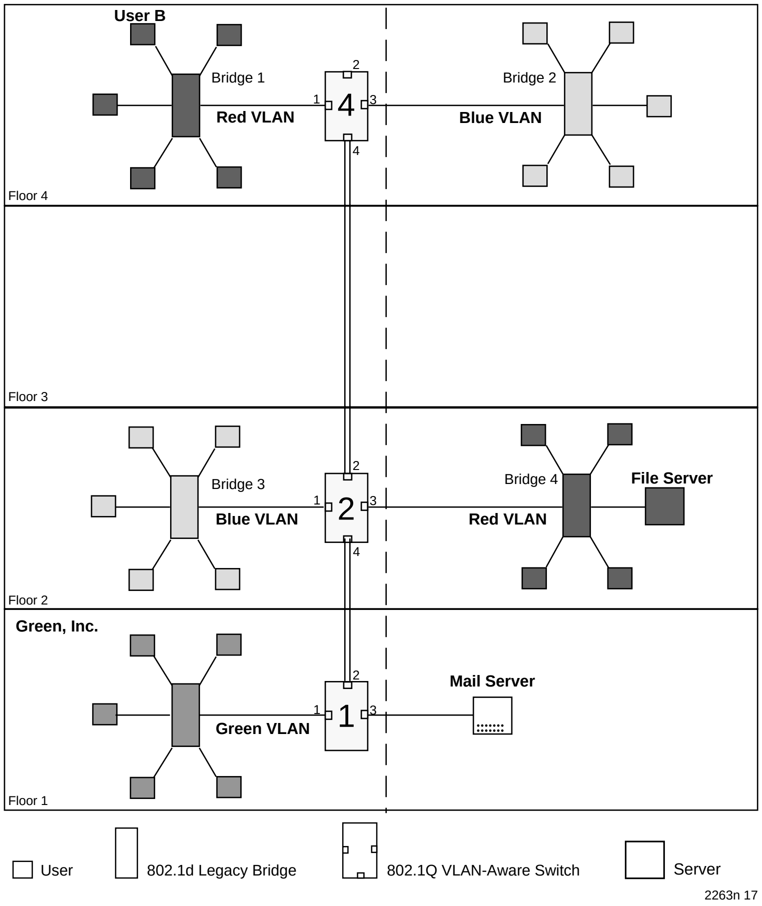


Figure 8. Example 3

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.

Solving the Problem

Much of the existing network configuration can remain as it was for "Example 2: Setting Up VLANs Across Multiple Switches" on page 9. While a new 1Q trunk port must be activated and configured on switch 2, and the operational modes of the switches must be changed, no other real changes are required 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 of 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, it 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.

Frame Handling

The following describes how the frames are classified on switch 4 and traverse the network when user B attempts to contact the mail server on switch 1.

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 location out of 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 of port 4 with the red VLAN tag header added, as shown in Figure 9.

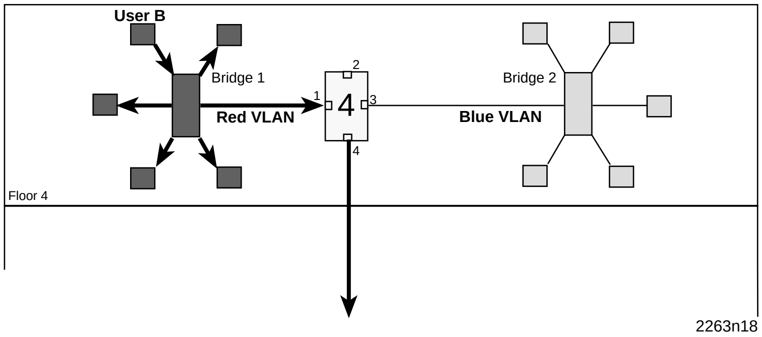


Figure 9. Bridge 1 Broadcasts Frames

3. Switch 2 receives the tagged red VLAN frame on port 2, as shown in Figure 10 on page 18. The Tag in the frame is maintained, classifying the frame as belonging to the red VLAN. The switch forwards the broadcast frame out of 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 of 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 of port 4, the 1Q trunk, retains its VLAN tag.

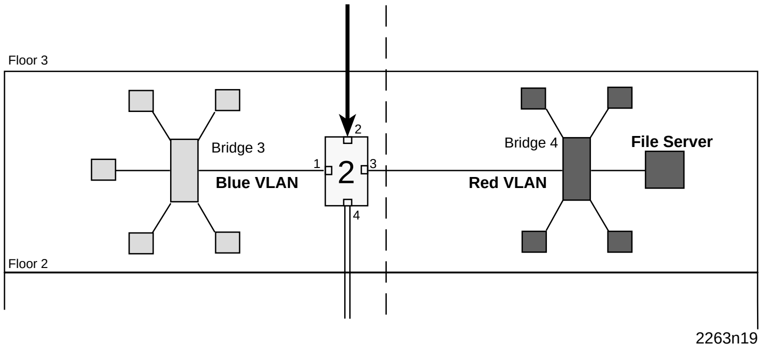


Figure 10. Switch 2 Forwards to 1Q Trunk

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 tag is stripped from the frame and the frame is transmitted out of port 3 as shown in Figure 11. The source address table for switch 1 is updated to contain user B.

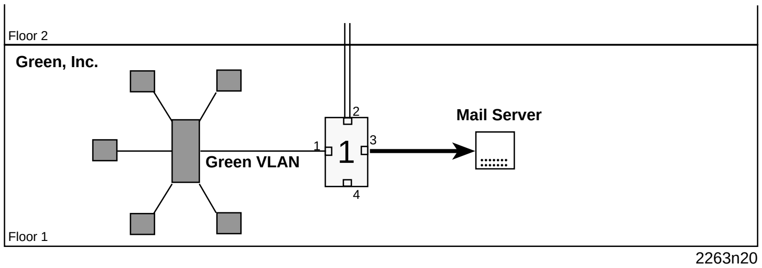


Figure 11. Switch 1 Forwards to 1d Trunk

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 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.

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 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, and tagged, out of 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 is handled in the same way by the switches in the network.

GIGAswitch/Router VLAN Support

VLANs contain layer 2 broadcast and multicast traffic. No traffic is allowed to cross VLAN boundaries unless it passes through routers. Once connected by routers, VLANs are equivalent to subnets.

VLANs are created by grouping a set of bridged ports together as part of one bridged network. Broadcasts from one of the ports in a VLAN are received by other ports in the group, but not by any ports outside of the group. Similarly, unicast traffic is bridged only between ports in a group, but not to ports outside of the group. Thus, traffic is not allowed to cross the group boundary. A bridge may have multiple VLANs defined, appearing as multiple virtual bridges on the DIGITAL GIGAswitch/Router (GSR).

The GSR supports the following types of VLANs. The VLAN type determines the type of traffic the GSR will forward on the VLAN.

- Protocol-based VLAN, which divides the physical network into logical VLANs based on one or more of the following protocols:
  - IP VLAN, which is a VLAN used for IP traffic.
  - IPX VLAN, which is a VLAN used for IPX traffic.
  - Bridged-protocol VLAN, which is a VLAN used for bridged protocols (such as AppleTalk).
- Port-based VLAN, which is a VLAN that is independent of the traffic type. Port-based VLANs treat IP, IPX, and bridged protocols alike.

The ports in a VLAN can be configured as one of the following:

- Access ports

  Access ports can belong to only one VLAN per protocol (IP, IPX, or a bridged protocol). This is the default for all ports.

  On access ports, traffic is sent out without 802.1Q frame format.

- Trunk ports

  Trunk ports can belong to any number of VLANs. Use trunk ports when you want to connect GSR routers together and send traffic for multiple VLANs on a single network segment connecting the routers.

  On trunk ports, traffic is always sent out with 802.1Q frame format.

When using the GSR as an L2 bridge/switch, use the port-based and protocol-based VLAN types. When using the GSR as a combined switch and router, use the subnet-based VLANs in addition to port-based and protocol-based VLANs. You do not need to remember the types of VLANs in order to configure the GSR, as seen in the section “Configuring VLANs Using the Command Line Interface” on page 24.

VLANs and the GSR

VLANs are an integral part of the GSR family of switching routers. The GSR switching routers can function as layer-2 (L2) switches, as well as fully functional, layer-3 (L3) routers. Hence, they can be viewed as a switch and a router in one box. To provide maximum performance and functionality, the L2 and L3 aspects of the GSR switching routers are tightly coupled.

The GSR can be used purely as an L2 switch. Frames arriving at any port are bridged and not routed. In this case, setting up VLANs and associating ports with VLANs is all that is required. You can set up the GSR switching router to use port-based VLANs, protocol-based VLANs, or a mixture of the two types.

The GSR can also be used purely as a router, that is, each physical port of the GSR is a separate routing interface. Packets received at any interface are routed and not bridged. In this case, no VLAN configuration is required. Note that VLANs are still created implicitly by the GSR as a result of creating L3 interfaces for IP and/or IPX. However, these implicit VLANs do not need to be created or configured manually. The implicit VLANs created by the GSR are subnet-based VLANs.

Most commonly, a GSR is used as a combined switch and router. For example, it may be connected to two subnets S1 and S2. Ports 1 through 8 belong to S1 and ports 9 through 16 belong to S2. The required behavior of the GSR is that intra-subnet frames be bridged and inter-subnet packets be routed. In other words, traffic between two workstations that belong to the same subnet should be bridged, and traffic between two workstations that belong to different subnets should be routed.

The GSR switching routers use VLANs to achieve this behavior. This means that an L3 subnet (that is, an IP or IPX subnet) is mapped to a VLAN. A given subnet maps to exactly one and only one VLAN. With this definition, the terms *VLAN* and *subnet* are almost interchangeable.

To configure a GSR as a combined switch and router, the administrator must create VLANs whenever multiple ports of the GSR are to belong to a particular VLAN/subnet. Then the VLAN must be *bound to* an L3 (IP/IPX) interface so that the GSR knows which VLAN maps to which IP/IPX subnet.

Ports, VLANs, and L3 Interfaces

The term *port* refers to a physical connector on the GSR, such as an Ethernet port. Each port must belong to at least one VLAN. When the GSR is unconfigured, each port belongs to a VLAN called the “default VLAN.” By creating VLANs and adding ports to the created VLANs, the ports are moved from the default VLAN to the newly created VLANs.

Unlike traditional routers, the GSR has the concept of logical interfaces rather than physical interfaces. An L3 interface is a logical entity created by the administrator. It can contain more than one physical port. When an L3 interface contains exactly one physical port, it is equivalent to an interface on a traditional router. When an L3 interface contains several ports, it is equivalent to an interface of a traditional router that is connected to an L2 device such as a switch or bridge.

Access Ports and Trunk Ports (802.1Q Support)

The ports of a GSR can be classified into two types, based on VLAN functionality: **access ports** and **trunk ports**. By default, a port is an access port. An access port can belong to at most one VLAN of the following types: IP, IPX, or bridged protocols. The GSR can automatically determine whether a received frame is an IP frame, an IPX frame, or neither. Based on this, it selects a VLAN for the frame. Frames transmitted out of an access port are *untagged*, meaning that they contain no special information about the VLAN to which they belong. Untagged frames are classified as belonging to a particular VLAN based on the protocol of the frame and the VLAN configured on the receiving port for that protocol.

For example, if port 1 belongs to VLAN *IPX_VLAN* for IPX, VLAN *IP_VLAN* for IP and VLAN *OTHER_VLAN* for any other protocol, then an IP frame received by port 1 is classified as belonging to VLAN *IP_VLAN*.

Trunk ports (802.1Q) are usually used to connect one VLAN-aware switch to another. They carry traffic belonging to several VLANs. For example, suppose that GSR A and B are both configured with VLANs V1 and V2.

A frame arriving at a port on GSR A must be sent to GSR B, if the frame belongs to VLAN V1 or to VLAN V2. Thus the ports on GSR A and B that connect the two GSRs must belong to both VLAN V1 and VLAN V2. Also, when these ports receive a frame, they must be able to determine whether the frame belongs to V1 or to V2. This is accomplished by “tagging” the frames, that is, by prepending information to the frame in order to identify the VLAN to which the frame belongs. In the GSR switching routers, trunk ports always transmit and receive tagged frames only. The format of the tag is specified by the IEEE 802.1Q standard. The only exception to this is Spanning Tree Protocol frames, which are transmitted as untagged frames.

Explicit and Implicit VLANs

As mentioned earlier, VLANs can either be created explicitly by the administrator (explicit VLANs) or are created implicitly by the GSR when L3 interfaces are created (implicit VLANs).

Configuring VLANs Using the Command Line Interface

You can use the DIGITAL GIGAswitch/Router Command Line Interface (CLI) to perform the following tasks when configuring VLANs for the GSR:

- Create VLANs.
- List VLANs.
- Add ports to VLANs.
- Change the port membership of VLANs.
- Make a VLAN port either a trunk or access port.

Refer to the *DIGITAL GIGAswitch/Router User Reference Manual* for more information on configuring VLANs.

Configuring a Port- or Protocol-Based VLAN

To create a port- or protocol-based VLAN, perform the following steps in the CLI Configure mode:

1. Create a port- or protocol-based VLAN:

```
gs/r(config)# vlan create <vlan-name> <type> id <num>
```

2. Add physical ports to a VLAN:

```
gs/r(config)# vlan add ports <port-list> to <vlan-name>
```

Configuring VLAN Trunk Ports

The GSR supports standards-based VLAN trunking between multiple GSRs as defined by IEEE 802.1Q. The standard adds a header to a standard Ethernet frame that includes a unique VLAN ID per trunk between two GSRs. These VLAN IDs extend the VLAN broadcast domain to more than one GSR.

To configure a VLAN trunk, perform the following command in the Configure mode:

```
gs/r(config)# vlan make <port-type> <port-list>
```

Suppose you have two VLANs/subnetworks of IP users on separate GSRs and those VLANs need to belong to the same layer broadcast domain. You could trunk two GSRs together as shown in the Figure 12 on page 25.

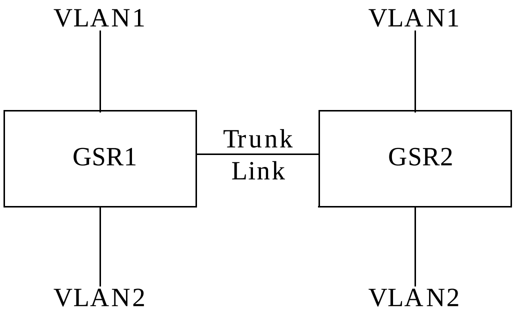


Figure 12. Connecting GSRs

Configuration Examples

Creating an IP or IPX VLAN

VLANs are used to associate physical ports on the GSR with connected hosts that may be physically separated but need to participate in the same broadcast domain. To associate ports to a VLAN, you must first create an IP or IPX VLAN and then assign ports to the VLAN.

For example, servers connected to port gi.1.(1-2) on the GSR need to communicate with clients connected to et.4.(1-8). You can associate all the ports containing the clients and servers to an IP VLAN called BLUE.

First, create an IP VLAN named BLUE:

```
gs/r(config)# vlan create BLUE ip
```

Next, assign ports to the BLUE VLAN:

```
gs/r(config)# vlan add ports et.1.(1-8),gi.1.(1-2) to BLUE
```

Configuring GSR VLANs with DIGITAL clearVISN CoreWatch

DIGITAL clearVISN CoreWatch is a comprehensive, easy-to-use, network management and device configuration application for GSRs. Based on Java, clearVISN CoreWatch provides configuration, monitoring, and reporting capabilities with the assistance of wizards and drag-and-drop operations. DIGITAL clearVISN CoreWatch simplifies the task of configuring VLANs, as well as configuring routers and security filters, and setting up application-level QoS policies.

Using clearVISN CoreWatch Configuration Expert and the VLAN Wizard, you can perform the following tasks:

- Define access ports and trunk ports.
- Use the VLAN Wizard to create a protocol-based or port-based VLAN and add ports to the VLAN.
- Change a port-based VLAN’s name or ID.
- Change a protocol-based VLAN’s name, ID, or protocol binding.
- Replace an interface’s VLAN.
- Add ports to a VLAN.
- Remove ports from a VLAN.

Refer to the *DIGITAL clearVISN CoreWatch User’s Guide* for specific information on using DIGITAL clearVISN CoreWatch to set up IEEE 802.1Q VLANs for the GSR.

MultiSwitch 700s and GSRs: Shared VLANs

You can establish a shared 802.1Q port-based VLAN between DIGITAL MultiSwitch 700, Generation 2, modules and DIGITAL GIGAswitch/Router, Version 2.1, modules. All switches under consideration for a shared port-based VLAN must support the IEEE 802.1Q specifications.

Configuring a Shared VLAN

No common firmware or software application exists to configure VLANs for both the MultiSwitch 700 and the GIGAswitch/Router (GSR) modules. VLANs for each device family needs to be configured separately using an application specific to the module.

- To configure the MultiSwitch 700 module, use the device's Local Management or the DIGITAL clearVISN MultiSwitch 700 Manager (MS 700 Manager) software.

  Certain restrictions apply when configuring an 802.1Q VLAN using the MS 700 Manager. Refer to the *DIGITAL clearVISN MultiSwitch 700 Manager Tools Guide* for detailed information.

- To configure the GIGAswitch/Router module, use the GSR Command Line Interface (CLI) or DIGITAL clearVISN CoreWatch.

Shared VLAN Configuration Examples

The following examples show how to configure two VLANs in an existing network so that users on a MultiSwitch 700 module and a GIGAswitch/Router module (line card) can function as a single local area network segment (broadcast domain). Each example shows how to configure shared VLANs using a module-specific VLAN application.

The actual procedures and screens used to configure a MultiSwitch 700 VLAN-aware switch are covered in the *DIGITAL MultiSwitch 700 Port Based VLAN User's Guide*. CLI commands for setting up VLANs for the GIGAswitch/Router are covered in the *DIGITAL GIGAswitch/Router Command Line Interface Reference Manual*.

Example 1: Setting Up Two Shared VLANs

The following example shows how to configure two shared VLANs, (green 0011 and yellow 0012) between ports on the following modules:

- DIGITAL MultiSwitch 700EX (DLE52-MA) module with sixteen (16) RJ45 10/100 Ethernet ports and one optional High Speed Interface Module (HSIM) or Very High Speed Interface module (VHSIM) slot.

- DIGITAL GIGAswitch/Router 10/100BASE-TX Line Card (DGSRT-AA) with eight (8) independent Ethernet ports. Each port automatically configures itself as a 10Base-T or 100Base-TX port.

The green VLAN will contain the users to Port 1 in the 10/100BASE-TX line card in slot 2 of the GSR and Port 7 of the DLE52-MA module in slot 2 of the MultiSwitch 700.

The yellow VLAN will contain users attached to Port 2 in the 10/100BASE-TX line card in slot 2 of the GSR and Port 8 of the DLE52-MA module in slot 2 of the MultiSwitch 700.

1Q trunk ports will be configured for Port 3 of the 10/100BASE-TX line card and Port 10 of the DLE52-MA module.

Configuring the MultiSwitch 700EX DLE52-MA

The following procedure presents the necessary steps to configure two new VLANs (green 0011 and yellow 0012) on the DLE52-MA (in slot 2), assign a port to each VLAN (port 7 to green VLAN and port 8 to yellow VLAN), and set up a 1Q trunk port for the DLE52-MA (port 10).

1. Locate the Device/VLAN Configuration screen. Use arrow keys to move to and highlight menu items.

   a. At the MS 700 Local Management screen, use arrow keys to highlight MODULE and press Enter.

   b. Highlight Module Configuration Menu on the Module Menu and press Enter.

   c. Highlight 802.1 VLAN Configuration Menu on the Module Configuration Menu and press Enter.

   d. Highlight 802.1Q VLAN Configuration Menu (VLAN Main Menu) on the 802.1 Configuration Menu and press Enter.

   e. Highlight Module / VLAN Configuration and press Enter.

2. Create two shared VLANs. (Refer to Figure 13 on page 29 for a sample Device/VLAN Configuration screen. Items on the your screen may not match exactly those in the sample.)

   a. At the bottom of the Module / VLAN Configuration screen:

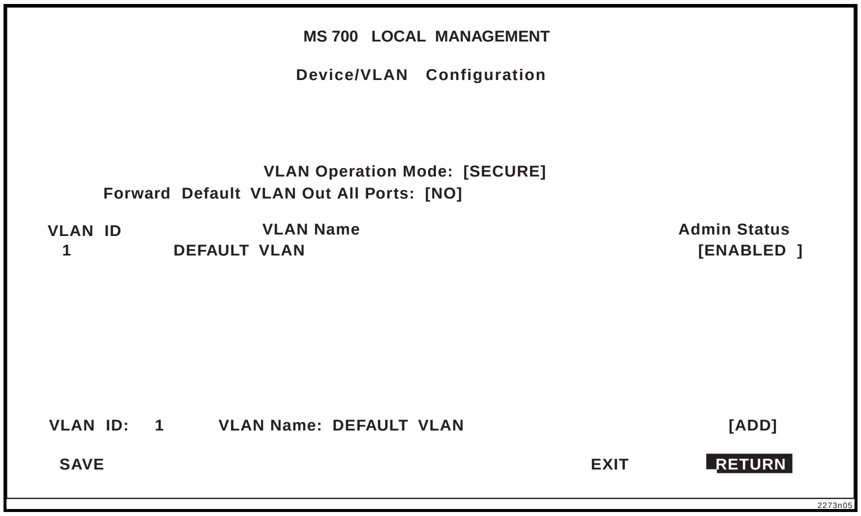
      For the one VLAN — highlight the VLAN ID field and enter **10,** then highlight the VLAN Name field and enter **green**.

      For the second VLAN — highlight the VLAN ID: field and enter **11,** then highlight the VLAN Name: field and enter **yellow**.

   b. After adding each new VLAN, toggle to ADD using space bar.

c. Highlight Admin Status of the new VLANS and toggle to ENABLED.

d. Use arrows to highlight SAVE and press Enter.



```
                              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            DEFAULT  VLAN                                      [ENABLED  ]





   VLAN  ID:    1        VLAN Name:  DEFAULT  VLAN                         [ADD]

    SAVE                                               EXIT           RETURN
                                                                               2273n05
```

Figure 13. Device/VLAN Configuration Screen

3. Assign port 7 to the green VLAN and port 8 to the yellow VLAN. (Refer to Figure 14 on page 30 for a sample Port Assignment screen. Items on the your screen may not match exactly those in the sample.)

   a. Return to the 802.1QVLAN Configuration Menu (VLAN Main Menu). Use the arrow keys to highlight the Port Assignment option and press Enter.

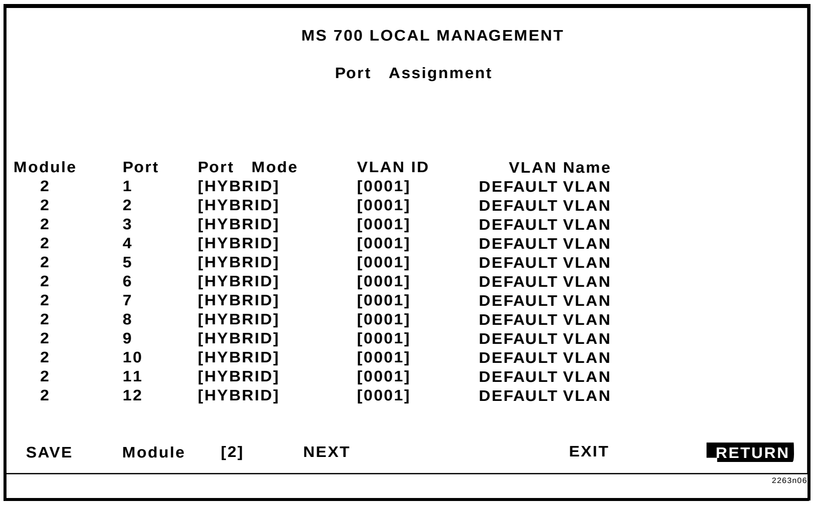
   b. Use arrow keys to highlight the VLAN ID field for module 2, port 7 and toggle the number until **0010** is displayed. Highlight the VLAN Name field and toggle until **green** is displayed.

   c. Use arrow keys to highlight the VLAN ID field for module 2, port 8 and toggle the number until **0011** is displayed. Highlight the VLAN Name field and toggle until **yellow** is displayed.

   d. Highlight SAVE and press Enter.

4. Define port 10 as an 1Q trunk.

   a. On the same Port Assignment screen, use arrow keys to highlight the Port Mode field of module 2, port 10. Toggle this field until **1Q TRUNK** is displayed.



```
                          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]        [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
```

Figure 14. Port Assignment Screen

VLAN configuration for the MultiSwitch 700EX module is complete.

Configuring the GIGAswitch/Router 10/100BASE-TX Line Card

The following example shows the necessary steps to configure two new VLANs (green 0011 and yellow 0012) on the 10/100BASE-TX line card (in slot 2), assign a port to each VLAN (port 1 to green VLAN and port 1 to yellow VLAN), and set up a 1Q trunk port for the 10/100BASE-TX line card (port 3).

VLAN configuration is accomplished in GSR CLI’s Configure mode.To enter Configure mode, first enter Enable mode (**enable** command), then enter the **configure** command from the Enable command prompt.

1. Create two shared VLANS. Enter the following commands in Configure mode:

```
gs/r(config)# vlan create green port-based id 10

gs/r(config)# vlan create yellow port-based id 11
```

2. Associate port 1 with green VLAN and port 2 with yellow VLAN. Enter the following commands in Configure mode:

```
gs/r(config)# vlan add port et.2.1 to green

gs/r(config)# vlan add port et.2.2 to yellow
```

3. Define port 3 as a 1Q trunk. Enter the following command in Configure mode:

```
      gs/r(config)# vlan make trunk port et.2.3
```

4. Associate the 1Q trunk port with both the green and yellow VLANs. Enter the following commands in Configure mode:

```
      gs/r(config)# vlan add ports et.2.3 to green

      gs/r(config)# vlan add ports et.2.3 to yellow
```

5. Save the VLAN configuration in the Startup configuration. Enter the following commands in Configure mode:

```
      gs/r(config)# save active

      gs/r(config)# save startup
```

VLAN configuration for the GSR 10/100BASE-TX line card is now complete.

Two port-based shared VLANs are in operation between the MultiSwitch 700 DLE52-MA module and the GIGAswitch/Router 10/100BASE-TX line card module.

Example 2: Setting Up a Gigabit 802.1Q Trunk

This example shows how to set up a Gigabit IQ trunk for use in a VLAN shared by Gigabit ports on the MultiSwitch 700EX DLE52-MA and ports on a GIGAswitch/Router 1000BASE-SX Line Card (DGSRS-AA). The DGSRS-AA contains two independent Gigabit (1000Mbps) Ethernet ports.

Port 17 of the DLE52-MA (Slot 2) will be defined as the Gigabit 1Q trunk for the MultiSwitch 700EX. port 1 of the DGSRS-AA (Slot 3) will be defined as the Gigabit 1Q trunk for the GSR.

Configuring the MultiSwitch 700EX DLE52-MA

The following procedure presents the necessary steps to set up a Gibabit 1Q trunk port for the DLE52-MA on port 17 (the HSIM/VHSIM slot).

1. Locate the 802.1QVLAN Configuration Menu (VLAN Main Menu).

   a. Use the arrow keys to highlight the Port Assignment option and press Enter.

b. Highlight Next and press Enter to show further port entries.

2. Use arrow keys to highlight the Port Mode field of module 2, port 17. Toggle this field until **1Q TRUNK** is displayed.

A Gigabit 1Q trunk is set up for the MultiSwitch 700EX DLE52-MA.

Configuring the GIGAswitch/Router 1000BASE-SX Line Card

The following procedure shows the necessary steps to set up a Gibabit 1Q trunk port (port 1) for the GIGAswitch/Router1000BASE-SX line card (DGSRS-AA) in slot 3.

VLAN trunk ports are defined in the GSR CLI's Configure mode. To enter Configure mode, first enter Enable mode (**enable** command), then enter the **configure** command from the Enable command prompt.

1. Define port 1as a 1Q trunk. Enter the following command in Configure mode:

```
        gs/r(config)# vlan make trunk port gi.3.1
```

2. Associate the 1Q trunk port with both the green and yellow VLANs. Enter the following commands in Configure mode:

```
        gs/r(config)# vlan add ports gi.3.1 to green

        gs/r(config)# vlan add ports gi.3.1 to yellow
```

3. Save the VLAN configuration in the Startup configuration. Enter the following commands in Configure mode:

```
        gs/r(config)# save active

        gs/r(config)# save startup
```

A Gigabit 1Q trunk is set up for the GIGAswitch/Router1000BASE-SX line card and a Gigabit 1Q trunk is available for the green and yellow VLANs shared between a MultiSwitch 700 and a GIGAswitch/Router.

VLAN Terms

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

1d trunk
A connection from a switch that passes only untagged traffic.

1Q trunk
A connection between 802.1Q switches that passes only traffic with a VLAN tag header inserted in the frame.

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

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.

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.

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

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.

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.

untagged frame
A data frame that does not have a tag header inserted into it.

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.

References

Information for this white paper was taken from the following manuals:

DIGITAL clearVISN CoreWatch User’s Guide, 9032685-02, Cabletron Systems, Inc., February 1999.

DIGITAL clearVISN MultiSwitch 700 Manager Tools Guide, 9032780-E, Cabletron Systems, Inc., January 1999.

DIGITAL GIGAswitch/Router Command Line Interface Reference Manual, 9032682-01, Cabletron Systems, Inc., February 1999.

DIGITAL GIGAswitch/Router User Reference Manual, 9032684-01, Cabletron Systems, Inc., February 1999.

DIGITAL MultiSwitch 700 Port Based VLAN User’s Guide, 9032619, Cabletron Systems, Inc., September 1998.