Lesson 4: Implementing Switch Technology

At a Glance



Virtual LANs (VLANs) offer flexibility in designing networks and in modifying existing networks. Using a VLAN, workstations can be grouped together as a segment even when they are not physically near one another. Segments can be created and reorganized without having to change the network physically. VLANs offer the advantages of a routed network with separate broadcast domains while still transmitting data at the speed of switches.

What You Will Learn

After completing this lesson, you will be able to:

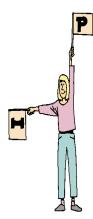
- Describe VLANs and explain why they are important
- Give an example of when a network manager would implement a VLAN
- Explain the role of VLANs and Broadcast Domains
- Describe Port based, MAC based, and Protocol/IP based VLANs
- Explain how VLANs function
- Tell why 802.lq is important



Student Notes:

Tech Talk

• **802.1q**—The IEEE standard that defines VLAN configuration and management.



- **Latency**—The difference between the time it would take data to transmit if it were traveling at wire speed and the time it actually takes.
- Quality of Service (QoS)—Quality of Service (QoS) refers to the ability of a network to provide better and more consistent service to selected packets and network traffic based on pre-established criteria.
- **Tagging**—The bits added to a frame header that identify the VLAN destination of the frame.
- **VLAN**—A virtual network segment defined by software rather than by physical connections.



VLAN Overview

Over time, as networks grow, congestion becomes a problem and causes network slowdowns and crashes. Virtual networks were established to solve these problems. A virtual local area network (virtual network), or VLAN, is a physical network that can be divided into logically independent broadcast domains. VLANs are created at the box level (the hardware device). They are software based and can be created using either Layer 2 or Layer 3 protocols. The first VLANs allowed network managers to separate broadcast domains by configuring the ports on switches.

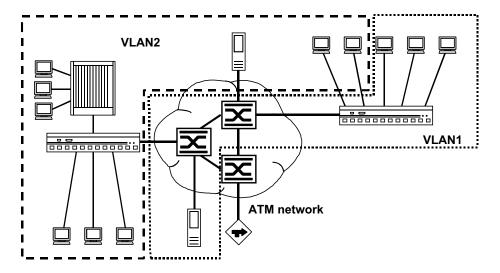
Today's VLANs provide low-latency, segmented, wire-speed communication among VLAN members. Since they are software based, networks are not limited by physical location. An individual who is a member of a VLAN can plug in at the office, at home, at school, or at a friend's and still be a member of the VLAN defined broadcast domain.

VLANs offer the following advantages:

- VLANs offer functions that traditionally only routers could perform.
 The advantage is that they perform at the greater transmission speeds offered by switches.
- VLANs create separate broadcast domains thus limiting broadcast traffic that causes congestion and slows down a network.
- Network managers can create VLANs (broadcast domains) for specific groups of users regardless of their geographic location.
- VLANs can be based on several different criteria, such as MAC address VLANs, IP address VLANs, or Multicast VLANs.
- Creating Layer 3 LANs involves routing, which can now be performed by Layer 3 switches. This increases network speed since the router's store-and-forward method of data transfer is not necessary.
- VLANs allow greater mobility in today's very mobile society. A user can remain part of a group regardless of protocol being used or location.
- Since VLANs can be created and/or modified by network managers through the use of software, the need to physically re-cable networks for user additions, moves, and changes is virtually eliminated.
- Although VLANs software is often proprietary, standards based on 802.1p (VLAN tagging protocol) and 802.1q (VLAN trunking protocol) are being used to create interoperable networks.

The purpose of bridges and Layer 2 switches is to segment broadcast domains into separate collision domains, therefore limiting problems with congestion. The purpose of VLANs is to segment broadcast domains to limit congestion caused by broadcast transmissions such as ARP requests.

Typical VLAN Network



There is no one correct VLAN set-up. The traffic of most corporate intranets varies widely depending upon the user requirements. As a result of this unpredictability, it is nearly impossible to devise an optimal scheme of VLANs to satisfy all users. Therefore, VLANs are designed for a specific network scheme.



Check Your Understanding

- ♦ What are VLANs and why are they important in networks?
- Give an example of a situation where using a VLAN network would be a useful.

A VLAN Example

In an architectural firm whose office occupies three floors of a building, the network may be set up with a LAN segment for each floor. Each LAN segment is connected to a switch on that floor, and those three switches are connected to a main backbone switch. Suppose some of the architects and engineers work on the third floor and some work on the second floor. Most of the time, architects talk to other architects and engineers talk to other engineers. It would improve network performance if the engineers and the architects were each on their own subnetwork. To do this a network manager has several choices. He or she can:

- Physically rewire the building to connect all the engineers to one segment and all the architects to another.
- Set up subnetworks by assigning IP addresses and adding a router that forwards packets based on Layer 3 IP protocols.
- Have all the architects and engineers move their offices so they are on the same segment.
- Create VLANs so that the architects are on one VLAN and the engineers are on another.

A network manager would always opt for the last solution since it is the easiest and least expensive of the choices.



Check Your Understanding

- Why would a network manager want to set up a VLAN?
- Give an example of a time when it would make sense to set up a VLAN.
- ◆ Suppose an architectural firm wins the commission to design a hospital. A dozen architects and several engineers are assigned to the project. Creating a new VLAN, the network administrator puts the architects working on the hospital onto their own VLAN and does the same for the engineers. He or she adds a server on which all the hospital drawings will be stored. This arrangement has several advantages. List some of the advantages.

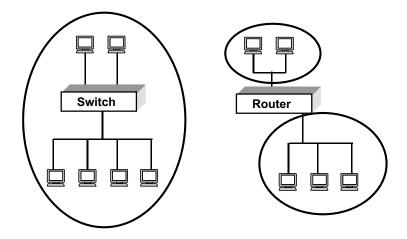
network

VLANs and Broadcast Domains

VLANs offer network designers a way to create separate broadcast domains using switches. In general, switches transfer data faster than routers, and they are usually less expensive. Network designers try to use switches instead of routers whenever possible. Because they are Layer 3 devices, routers have been able to do some things that switches could not. One of those things is to physically connect LAN segments while keeping each segment in its own broadcast domain. VLANs have made it possible to use switches to do this job.

Maintaining separate broadcast domains is important for security. A flat network with switches but no routers allows any machine on the network to communicate with all other devices on the network. Switches forward broadcast frames to all segments, which means that all devices connected to the switch are in the same broadcast domain. This can create congestion problems and slow the network. Isolating broadcast domains through the use of VLANs limits congestion caused by broadcast packets. It also prevents unauthorized people from accessing those segments.

Routers Create Separate Collision Domains





A VLAN gives a network manager the ability to create individually designed VLANs with the speed advantage of switching and the advantage of a router's ability to segment broadcast domains. A single intelligent switch can have multiple VLANs. Because each VLAN has its own broadcast domain, a single switch with multiple VLANs will "virtually" have segments with separate broadcast domains.

Routers do not forward broadcast messages. Routers only forward packets that are addressed to a specific device. Because broadcast messages are not addressed to a specific device, routers drop them. When routers interconnect LANs, the LANs remain in independent broadcast domains.

Check Your Understanding

- Why might a network manager want to design a network with VLANs?
- ♦ What is a benefit that results when a network manager sets up a VLAN?

VLAN Configuration

Virtual LANs are not connected physically; rather they are connected (virtually) logically. VLANs can be configured in a variety of ways. There are both Layer 2 and Layer 3 VLAN configurations.

Three common VLAN configurations include the following:

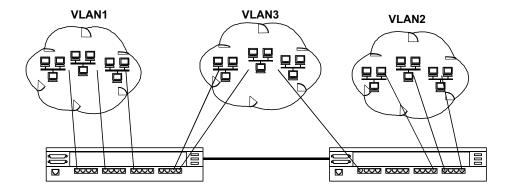
- Port-based VLANs
- MAC-based VLANs
- Protocol/IP-based VLANs

Port-Based VLANs

To create a port-based VLAN, the network administrator assigns specific ports on a switch to the VLAN. A port based VLAN can include one port or many ports on one or more switches. The VLAN configuration blocks broadcast traffic among VLANs even if they are connected to ports on the same switch.

The network manager must manually configure the ports. They are easy to configure and maintain, but as networks grow, the time involved in manually configuring ports becomes a problem. Also, when a VLAN is created at the port level, a device can only be a member of the VLAN group if it is connected to the port. This presents a problem if a user moves from location to location. So, in networks where individual users frequently change locations, port based VLANs are not necessarily a good choice. Another drawback is that in port based VLANs, the user can only be assigned to one VLAN since it is based on the port that the device is physically connected to. Port based VLANs do, however, do offer a high degree of security since only the network manager can change the configurations. Although they have disadvantages, port based VLANs, offer the highest degree of security and control since all assignment changes must be set manually.

Port-based VLAN





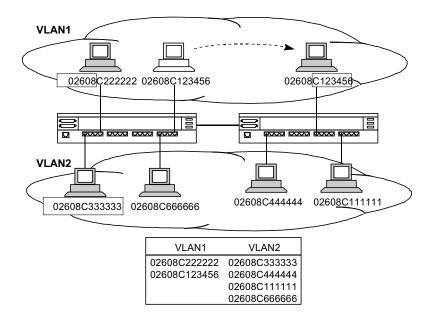
MAC-Based VLANs

As you know, every NIC has a unique MAC address. VLANs can be configured based on a device's MAC address. To create a MAC-based VLAN, the network manager manually programs into the switch a list of MAC addresses for each particular VLAN.

Unlike a port based VLAN, a MAC based VLAN is not dependent on the port connection. This means that a user can remain a member of the VLAN even if his/her office location changes. Once the switch knows which VLAN the MAC address belongs to, the switch can learn the new location of the workstation and reconnect it to the correct VLAN. Additionally, with MAC based VLANs, it is possible to belong to more than one VLAN.

Both MAC and port based VLANs are Layer 2 LANs. This can be a problem for remote MAC based VLAN users. If the remote user goes to a location that is not on the same network, Layer 2 protocols will not allow network layer data transfer. This type of VLAN also becomes a management problem in large networks because of the need to manually configure the MAC address data.

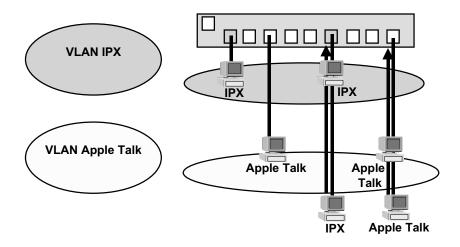
GMAC-based VLANs



Protocol/IP-Based VLANs

Protocol/IP-based VLANs can be configured based on specific protocols. For example, IPX users can be assigned to one VLAN, NetBEUI users to another VLAN, IP users to another, and so on. Note that this type of VLAN can be either a Layer 2 or Layer 3 scheme. In a protocol/IP based VLAN, the switch looks at the protocol type field of the frame header and uses that information to determine which VLAN a frame is destined for. This means, for example, that if a network manager wants, he or she can keep all Macintosh users in one VLAN and all the IPX users in another.

Protocol-based VLAN



Since this VLAN is based on the protocol associated with the frame being transmitted, it is not necessary for the network manager to manually configure each user. The manager need only configure the switch with the specifications for the VLAN types. The main advantage to this type of VLAN is that in IPX networks, it can keep the Service Advertisement Protocol broadcasts manageable.

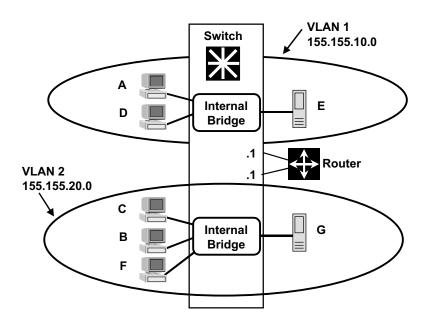
VLAN Tagged Frames Indicate Protocol Type

6 Bytes	6 Bytes	4 Bytes	2 Bytes	46-1500 Bytes
Destination MAC Address	Source MAC Address	802 TAG	Protocol Type	Data



A network administrator can also create a VLAN using the IP addresses (Layer 3 addresses) of the devices. In this kind of VLAN the switch must be able to look at Layer 3 addresses as a router does. Although it routes transmissions over networks, it is not true routing and should not be mistaken for a routing function.

IP-based VLAN



Check Your Understanding

- List and describe four different types of VLANs.
- ♦ With MAC-based VLANs, a user can become a member of all of the VLANs on a network. Give an example of a how this can be of benefit to a network manager.
- ♦ List two advantages and two disadvantages for a port-based, MAC-based, and protocol-based VLAN.



How VLANs Function

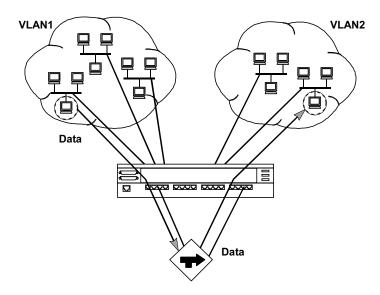
So far you have learned that transmission speed is the major advantage to setting up VLANs with switches instead of connecting LAN segments with routers. Switches move data faster than routers. But once VLANs are created, how does data get from a device on one VLAN to a device on another VLAN? The two devices exist in separate broadcast domains, so a broadcast from one VLAN device will not be received by a device on another VLAN.

When a switch receives a VLAN frame, it looks for the following information:

- Does the frame's header include a tag that directs it to a particular VLAN?
- Does the frame belong to a MAC based VLAN?
- Does the frame belong to a protocol/IP based VLAN?
- If the answer to all of the above is no, then the frame belongs to the port-based VLAN configured on the received port.

Layer 2 switches use Layer 2 protocols for switching in VLAN environments. Layer 3 VLANs, such as IP VLANs need to be routed since they use higher level protocols.

Messages Between VLANs Must Be Routed First

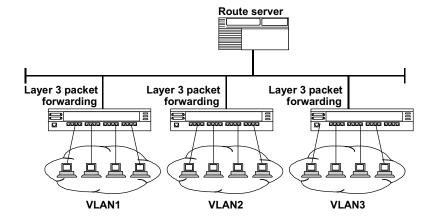


Integrating Router Functions

A router is a Layer 3 device that performs two main tasks, route calculation and packet forwarding. In addition, routers can function as firewalls and security devices. Routing is necessary for Layer 3 VLANs. There are three strategies for integrating the functions of a router in a VLAN network.

The first is to connect all the VLAN switches to a single router. This requires that one port on each switch be used to connect the switch to the router rather than for connecting a LAN segment. All traffic must pass through one router. This makes it easy to manage but can cause latency since the router must process more data than Layer 2 devices.

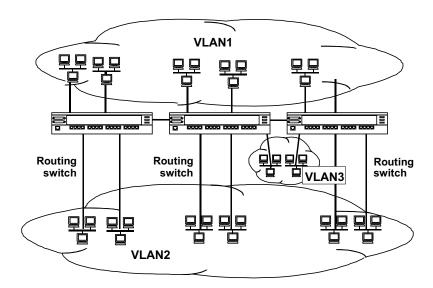
Single Router Switching





A second design strategy is to have the switches themselves take on the job of the router. Switches that can do routing are called Layer 3 switches and are much more expensive than standard switches. By doing the routing at each switch, traffic between devices on different VLANs may be kept off the backbone if the two devices are attached to the same switch.

Distributing Routing Functionality



A third strategy is actually a combination of the first two. It gives the switch only the packet forwarding portion of the router's function and leaves the route calculation to a single central router.

Route First, Then Switch

Although routers are more expensive than switches, they are not as fast as switches when transmitting data. Routers take the frames, examine them for errors, filter data, and perform algorithms to determine the best route for the data to take. Using a router in a VLAN may seem to defeat the purpose of using a switch to increase transmission speed. However, there is a need for routers in Layer 3 environments. Without the router, Layer 3 protocols cannot be used to determine the best route to the destination device.

When a switch knows the Layer 2 MAC address of both the source and destination devices, data can be transmitted even if the network manager has created IP-based (Layer 3) VLANs. This is done through the use of routers. In a network where VLANs are connected by switches as well as by routers, the router only needs to be used to establish the connection between two devices. That is, the router finds the destination device, ensures that the source and destination devices are allowed to communicate, and sets up the connection. The router is only used until the connection is established and the two devices learn one another's MAC (Layer 2) addresses. Data can then be transmitted between the two devices by way of switches instead of through the router.

The following is a list of steps that occur when data is transmitted in a router/switched VLAN environment.

- 1. A device on VLAN 1 sends a message to a device on VLAN 2.
- 2. All devices on VLAN 1 as well as the router connecting VLAN 1 and VLAN 2 receive packet.
- 3. All other devices on VLAN 1 discard the packet because the layer 2 address does not belong to them. The router looks at the layer 3 address in the packet and determines that the address is that of a device on VLAN 2.
- 4. The router then forwards the packet to VLAN 2.
- 5. The destination device receives the packet that contains, in its header, the MAC address of the sending device.
- 6. The destination device sends acknowledgement of packet receipt back to the source device. The acknowledgement message includes in its header the MAC address of the destination device.
- 7. Since both the source and destination devices are connected by switches and now know the MAC addresses, the remaining packets can be transmitted through switches using layer 2 protocols. This enables the devices to bypass the router for subsequent data transmissions.



Check Your Understanding

- ◆ Explain why IP-based VLANs need to be routed and not just switched.
- Why would a network administrator want to use switches rather than routers?
- Explain how a router/switched environment transmits data.

802.1q and Multiple Switch VLANs

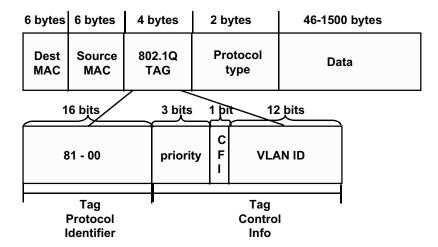
VLANs can extend across multiple switches. One way to include multiple switches in a VLAN is to use port-based or MAC-based VLANs and simply configure all of the switches as needed. This is also knows as a proprietary VLAN. When proprietary VLANs are used, the switch decides which VLAN a frame should go to. All switches must understand the configuration.

When using switches from various vendors, it is necessary to have to a standard for communicating that allows information to be transmitted among the switches. The IEEE 802.1q standard allows a computer transmitting a frame to add a tag to the frame header. This tag is 4 bytes long and immediately follows the destination and source MAC addresses. Part of this tag contains the VLAN Identifier (called the tag control information or TCI field) which indicates the VLAN that the frame is headed for.

802.1q rules classify received frames to appropriate VLANs, define port-based tagging rules, prioritize, and determine where to forward frames. In addition, they map frames for transmission, detail the frame format for VLANs.

The significant difference between 802.1q and proprietary VLANs is that all devices know about the existence of 802.1q VLANs and can attach tags to the headers of frames which direct those frames to particular VLANs.

802.1q Frame



LAN emulation (LANE), which you will learn about in the cell-switching lesson 3-2, is another way that switches can communicate VLAN membership information.

Check Your Understanding

- ♦ What is 802.1q and why is it important?
- Could adding a tag to a frame cause transmission problems? Why or why not?



Try It Out

Materials Needed:

- BayStack 350T Switch and owner's manual
- HyperTerminal software
- Three (3) workstations



Port Based VLAN Configuration

In this lab, you will configure two VLANs. Keep notes during this activity about your experiences. Write a one-page report that documents your observations and participation in this activity and include it in your portfolio.

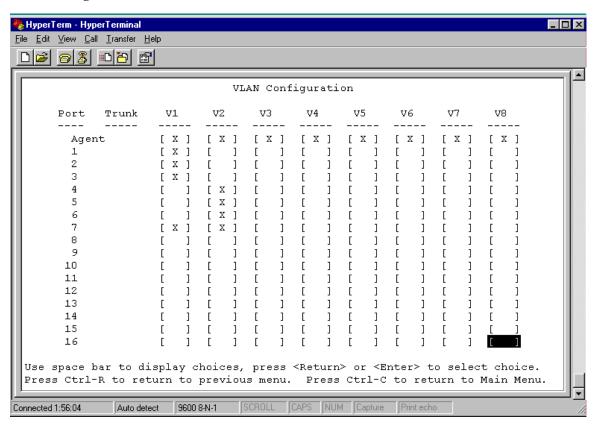
- 1. Open HyperTerminal and access the VLAN window via the Switch Configuration window.
 - ♦ How many VLANs are there for the 350 Switch?
- 2. Configure two VLANs: V1 and V2. Assign ports 1, 2, and 3 to V1. This is one group of users.

To group switch ports into logical workgroups, select the port number [1, 2, 3, ...] beneath the VLAN name [V1, V2, V3,...]. To allow users on different VLANs to share a port, select that port under the VLAN name.

- 3. Assign the second group of users to V2, which should include ports 4, 5, and 6.
 - How many broadcast domains does you network now have?
 Explain.
 - How many collision domains have you configured? Describe them.
 - Why might a network manager want to segment the network into different collision domains? Give an example of this type of situation.

- 4. Both groups will share a common server. If your network does not have a server device, you should create a server first. Configure the server device for both VLANs VI and V2. Use port 7 for the server device.
 - Has the broadcast domain changed? Explain.
 - ♦ Have the collision domains changed? Explain.

The configuration should look like the window below.



You have now configured two port-based VLANs.

• If a multicast transmission is sent to V1, which ports will receive the data? Explain.



- ♦ How might this be useful to a network manager?
- ◆ If a broadcast transmission is sent to V1, which ports will receive the data? Explain.
- If a unicast message is sent to port 1 who will receive the transmission? Explain.
- With the above configuration, which device will receive all multicast and broadcast transmissions? Explain.
- 5. Connect workstations to the switch. Use at least three workstations. Connect one workstations to port 1, connect the second workstation to port 4, and connect the third workstation to port 7.
 - Predict what will happen and defend your answer.
- 6. Test your prediction by trying to communicate with each of the devices.

Rubric: Suggested Evaluation Criteria and Weightings:

Criteria	%	Your Score
Active participation in lab activity	25	
Complete, accurate answers to questions that indicate a thorough understanding of key concepts	60	
Portfolio entries complete	15	
Other		
TOTAL	100	



Stretch Yourself

Materials Needed:

• Classroom Network



Configure VLANs Spanning Multiple Switches and Share Resource Device

In this activity, you are going to design and implement a LAN with two switches and several different VLANs that all share some of the same resources.

- 1. Obtain specifications for the LAN you will design from your instructor.
- 2. Keep records at each step along the way. Your records should include the reasoning behind your choices.
- 3. Create a computer-generated diagram of your network that indicates VLANs; port numbers, devices, cable types, etc.
- 4. Obtain instructor approval of your design.
- 5. Implement and test your design. If you are unsuccessful, troubleshoot until your design is functioning efficiently.

Rubric: Suggested Evaluation Criteria and Weightings:

Criteria	%	Your Score
Efficient use of time and resources	25	
Complete record keeping and documentation of all steps in the process	25	
Professional quality computer generated network diagram	25	
Network design implemented and up and running	25	
Other		
TOTAL	100	

Network Wizards

Materials Needed:

- Classroom Network
- Optivity software



Monitoring Network Activity - Nodes and Ports

Part 1: Monitor network activity for network nodes.

- 1. Start Optivity.
- 2. In the CCC Folders panel, select the LANs folder.
- 3. Select your team's segment or ring and click the Monitor button. The NodalView for the selected LAN appears. NodalView takes a period of time to populate all the available statistics. Allow 2–3 minutes to fully display statistics.
- 4. Double—click on the % column in the middle of the display.

 The NodalView is displayed sorted by nodes with the highest activity at the top of the window.
- 5. Double-click on the Segment Utilization bar above the graph. Close the window.
- 6. Double-click on the small button to the right of the Segment Utilization bar.
 - What changes on the graph?
- 7. Using the statistics graphs and pie charts at the top of NodalView answer the following questions:
 - What is the most common frame size on this network?
 - What percentage of total traffic is broadcast?



- What is the current utilization of the segment?
- ♦ What options are available?
- 8. Select Location.
 - What is the location of the first PC listed for the segment?
- 9. Change the selection for Properties back to Net Address.
- 10. Move to the section to the right of Properties and use the right mouse button to display the available selections. Select Performance.
 - ♦ What is the Frames count?
 - ♦ What is the Coll (collision) count?
- 11. Use the right mouse button again at the same location and select RMON Performance.
 - ♦ What is the highest count for OutPkts?
 - What is the IP address of the device with the most OutPkts?
- 12. Close the NodalView.

Part 2: Monitor network activity for slots and ports.

- 1. In the CCC Folders panel, select the Hubs folder.
- 2. Select your team's hub and click the Monitor button.

The Expanded View for the selected hub is displayed.

3. Click the right mouse button on a port or module and choose Activity from the Performance menu.

The Activity window opens for the selected port or module.

- ♦ What is the GoodPkt count for this port?
- 4. Close the Activity window.
- 5. Click the right mouse button on a hub and choose Recorder from the Performance menu.

The **Recorder** window opens for the selected port or module. This window shows utilization and error rates over a period of time.

- 6. Close the Recorder window.
- 7. Close the Expanded View.

Rubric: Suggested Evaluation Criteria and Weighting

Criteria	%	Your Score
Successful completion of activity	15	
Accurately follows directions	15	
Complete, accurate responses to lab activity questions	15	
Complete summary of experiences and an insightful analysis of how a network manager might use this software to help improve network performance.	20	
Summary included in portfolio	15	
Participation and cooperative teamwork during activity	20	
Other		
TOTAL	100	



Summary

Lesson 4: Implementing Switch Technology

In this lesson, you learned the following:

- Describe VLANs and explain why they are important
- Give an example of when a network manager would implement a VLAN
- Explain the role of VLANs and Broadcast Domains
- Describe Port-based, MAC-based, and Protocol/IP-based VLANs
- Explain how VLANs function
- Tell why 802.lq is important

Unit 2 Review Questions

Review Questions

Lesson 4: Implementing Switch Technology

Multiple Choice: Select the best answer.

- 1. When three LAN segments are connected by a switch on a traditional network., how many broadcast domains are there?
 - a. One
 - b. Two
 - c. Three
 - d. Cannot tell
- 2. When a router on a traditional network connects two LANs, how many broadcast domains are there?
 - a. One
 - b. Two
 - c. Unknown
- 3. Which one of the following statements about VLANs is false?
 - a. VLANs improve network performance through creating separate broadcast domains.
 - b. VLAN switches are cheaper than routers
 - c. A VLAN switch is a level 3 switch.
- 4. Members of a VLAN can be specified by:
 - a. Port
 - b. MAC address
 - c. IP address
 - d. All of the above



- 5. Which one of the following statements about VLANs is false?
 - a. A VLAN gives a network designer the speed advantage of switching.
 - b. A VLAN gives a network designer the ability to create separate broadcast domains.
 - c. A single level 3 switch can have multiple VLANs.
 - d. A VLAN has devices that are physically connected.
- 6. Which one of the following list of advantages of VLANs is false?
 - a. VLANs are flexible software-defined groups of devices.
 - b. VLANs handle the changing traffic of today's networks better than older methods.
 - c. VLANs involve routing which can only be performed by routers.
- 7. Which VLAN configuration would you use to build a VLAN for salesmen who often take their PC with them on the road?
 - a. Port-based
 - b. MAC-based
 - c. Policy-based
- 8. Which VLAN configuration would you have a network that consists of an AppleTalk section and PC section
 - a. Port-based
 - b. MAC-based
 - c. Policy-based

Unit 2 Review Questions

9. Which router strategy would you use for your VLAN if you find you have an extra router, but limited switches and money?

- a. Use switches that can do routing
- b. Connect all VLAN switches to a single router
- c. Give the switches only the packet-forwarding portion of the router's function, and use a router for route calculation.
- 10. Which one of the following statements about multiple Switch VLANs is false?
 - a. A proprietary VLAN uses port-based or MAC-based VLANs and configures all switches as needed.
 - b. In proprietary VLANs a switch decides which VLAN a frame should go to.
 - c. Both 802.1Q and proprietary VLANs can attach a tag to a frame header with a VLAN address.



Scoring

Criteria	Points	Your Score
Check Your Understanding		
Describe VLANs and explain why they are important	18	
Give an example of when a network manager would implement a VLAN	15	
Explain the role of VLANs and Broadcast Domains	17	
Describe Port based, MAC based, and Protocol/IP based VLANs	18	
Explain how VLANs function	17	
Tell why 802.lq is important	15	
Total	100	
Try It Out: Port Based VLAN Configuration	100	
Stretch Yourself:: Configure VLANs Spanning Multiple Switches and Share Resource Device	100	
Network Wizards: Monitoring Network Activities : Nodes and Ports	100	
Review	100	
TOTAL	500	

Unit 2 Resources:

Resources:

Bay Networks, Inc. (1999). Accelar Fundamental Technologies Instructor Student Guide, Bay Networks, Inc., Billerica, Massachusetts.

BayNetworks (1998). Using the BayStack 350 Series 10/100 Autosense Switch. BayNetworks, Inc. Billerica, Massachusetts.

Black, Darryl P. (1999). Building Switched Networks: Multilayer Switching, QoS, IP Multicast, Network Policy, and Service Level Agreements. Addison-Wesley, Reading, Massachusetts.

Keshav, S., *Switching: an Engineering Approach to Computer Networking* http://www.cs.cornell.edu/home/skeshav/book/slides/switching/ppframe.htm

Layer 3 Switching: An Introduction, by Robert Ciampa http://www.3com.com/technology/tech_net/white_papers/500660.html#A

Metzler, J., DeNoia, L. (1999) Layer 3 Switching: A Guide for IT Professionals. Prentice Hall PTR, Upper Saddle River, New Jersey.

Nortel Networks (1999). *NetKnowledge: Routing*. Nortel Networks, Billerica, Massachusetts.

Nortel Networks (1995). *Introduction to Internetworking*. BayNetworks, Inc. Billerica, Massachusetts.

Sheldon, Tom (1998). LANTIMES Encyclopedia of Networking, Electronic Edition. Osborne/McGraw-Hill, Berkeley, California.

Smith, Marina (1997). Virtual LANs: A Guide to Construction, Operation, and Utilization. McGraw-Hill, New York, New York.

