Save 10% on Exam Voucher

See Inside

EXAM CRAM

CompTIA®

Network+

N10-008

Cram Sheet

Flash Cards

Practice Tests

EMMETT DULANEY

EXAM CRAM

CompTIA® Network+ N10-008 Exam Cram

Emmett Dulaney

Pearson

by which data can be moved between two networks or systems, such as transport protocols, which in the case of TCP/IP is IP.

Although VLAN membership may be based on Layer 3 information, this has nothing to do with routing or routing functions. The IP numbers are used only to determine the membership in a particular VLAN, not to determine routing.

- **Port-based VLANs:** Port-based VLANs require that specific ports on a network switch be assigned to a VLAN. For example, ports 1 through 4 may be assigned to marketing, ports 5 through 7 may be assigned to sales, and so on. Using this method, a switch determines VLAN membership by taking note of the port used by a particular packet. Figure 3.7 shows how the ports on a server could be used for port-based VLAN membership.

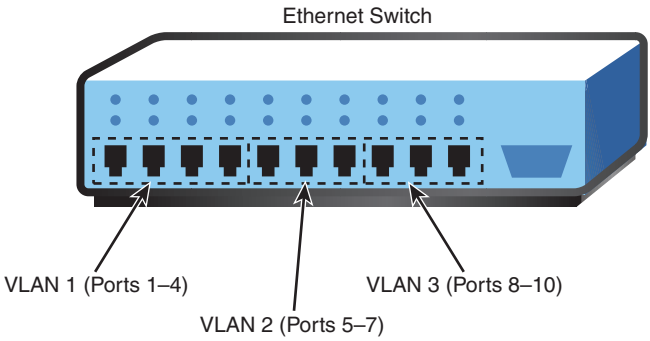

FIGURE 3.7 **Port-based VLAN membership**

- **MAC address-based VLANs:** The *Media Access Control (MAC)* address is a unique 12-digit hexadecimal number that is stamped into every network interface card. Every device used on a network has this unique address built in to it. It cannot be modified in any way. As you may have guessed, the MAC address type of a VLAN assigns membership according to the workstation's MAC address. To do this, the switch must keep track of the MAC addresses that belong to each VLAN. The advantage of this method is that a workstation computer can be moved anywhere in an office without needing to be reconfigured. Because the MAC address does not change, the workstation remains a member of a particular VLAN. Table 3.9 provides examples of the membership of MAC address-based VLANs.

TABLE 3.9 **MAC Address-Based VLANs**

MAC Address	VLAN	Description
44-45-53-54-00-00	1	Sales
44-45-53-54-13-12	2	Marketing
44-45-53-54-D3-01	3	Administration
44-45-53-54-F5-17	1	Sales

VLAN Segmentation

The capability to logically segment a LAN provides a level of administrative flexibility, organization, and security. Whether the LAN is segmented using the protocol, MAC address, or port, the result is the same: the network is segmented. The segmentation is used for several reasons, including security, organization, and performance. To give you a better idea of how this works, Figure 3.8 shows a network that doesn't use a VLAN.

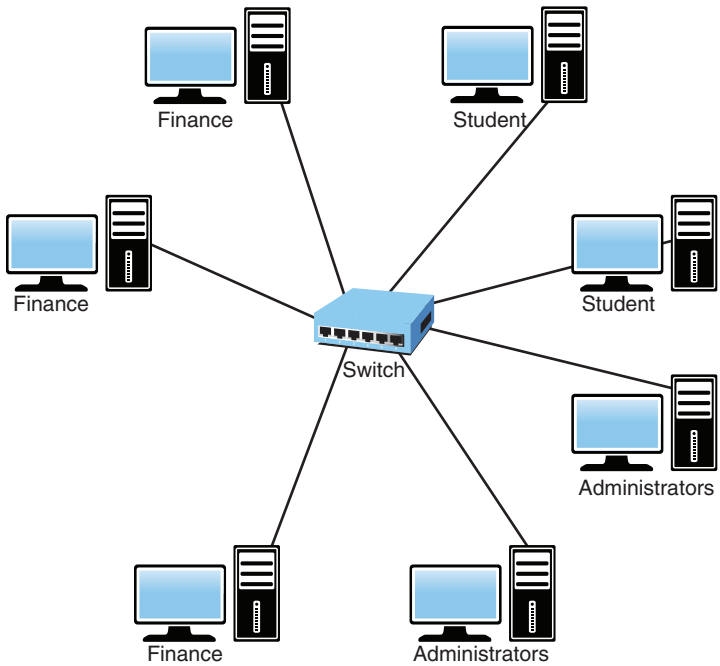

FIGURE 3.8 **Network configuration without using a VLAN**

In Figure 3.8, all systems on the network can see each other. That is, the students can see the finance and administrator computers. Figure 3.9 shows how this network may look using a VLAN.

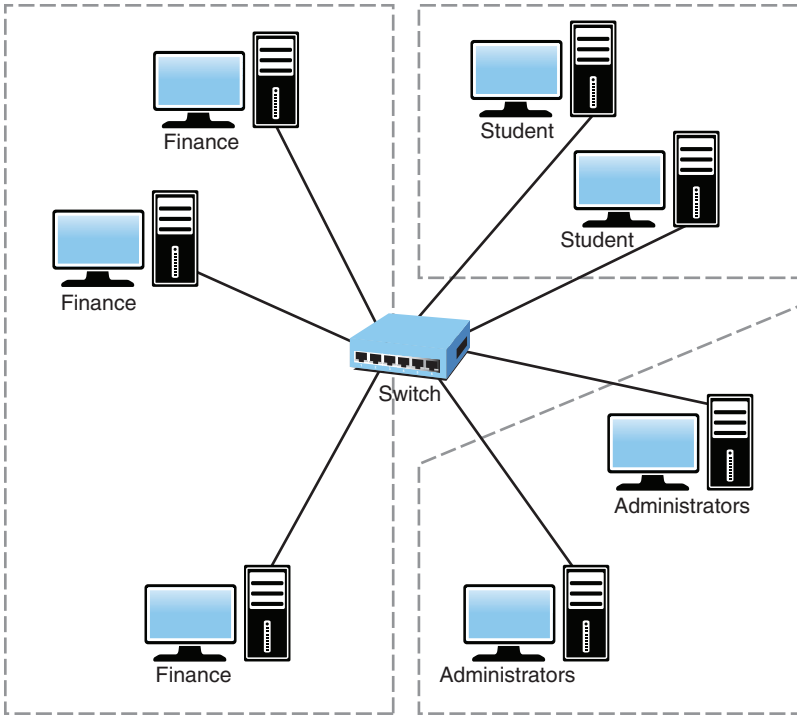

FIGURE 3.9 **Network configuration using a VLAN**

ExamAlert

Remember that one of the primary purposes of segmentation is to protect sensitive information from other hosts or the rest of the network in general.

The Spanning Tree Protocol

An Ethernet network can have only a single active path between devices on a network. When multiple active paths are available, switching loops can occur. Switching loops are the result of having more than one path between two switches in a network. *Spanning Tree Protocol (STP)* is designed to prevent these loops from occurring.

STP is used with network bridges and switches. With the help of *Spanning Tree Algorithm (STA)*, STP avoids or eliminates loops on a Layer 2 bridge.

> **Note**
>
> As a heads up, talking about STP refers to Layer 2 of the OSI model. Both bridges and most switches work at Layer 2; routers work at Layer 3, as do Layer 3 switches.

STA enables a bridge or switch to dynamically work around loops in a network's topology. Both STA and STP were developed to prevent loops in the network and provide a way to route around any failed network bridge or ports. If the network topology changes, or if a switch port or bridge fails, STA creates a new spanning tree, notifies the other bridges of the problem, and routes around it. STP is the protocol, and STA is the algorithm STP uses to correct loops.

If a particular port has a problem, STP can perform a number of actions, including blocking the port, disabling the port, or forwarding data destined for that port to another port. It does this to ensure that no redundant links or paths are found in the spanning tree and that only a single active path exists between any two network nodes.

STP uses *bridge protocol data units (BPDUs)* to identify the status of ports and bridges across the network. BPDUs are simple data messages exchanged between switches. BPDUs contain information on ports and provide the status of those ports to other switches. If a BPDU message finds a loop in the network, it is managed by shutting down a particular port or bridge interface.

Redundant paths and potential loops can be avoided within ports in several ways:

- **Blocking:** A blocked port accepts BPDU messages but does not forward them.
- **Disabled:** The port is offline and does not accept BPDU messages.
- **Forwarding:** The port is part of the active spanning tree topology and forwards BPDU messages to other switches.
- **Learning:** In a learning state, the port is not part of the active spanning tree topology but can take over if another port fails. Learning ports receive BPDUs and identify changes to the topology when made.
- **Listening:** A listening port receives BPDU messages and monitors for changes to the network topology.

Most of the time, ports are in either a forwarding or blocked state. When a disruption to the topology occurs or a bridge or switch fails for some reason, listening and learning states are used.

ExamAlert

STP actively monitors the network, searching for redundant links. When it finds some, it shuts them down to prevent switching loops. STP uses STA to create a topology database to find and then remove the redundant links. With STP operating from the switch, data is forwarded on approved paths, which limits the potential for loops.

Interface Configuration and Switch Management

Aside from VLAN trunking (802.1Q), binding, and a number of other possibilities previously discussed in this chapter, when you configure a switch interface, there are often other options that you can choose or tweak. They include the following:

- **Tag versus untag VLANs:** Tagging should be used if you are trunking. Because trunking combines VLANs, you need a way to identify which packet belongs to which VLAN; this is easily accomplished by placing a VLAN header (a *tag*) in the data packet. The only VLAN that is not tagged in a trunk is the *native VLAN*, and frames are transmitted to it unchanged.
- **Default VLAN:** The *default VLAN* is mandatory (cannot be deleted) and is used for communication between switches (such as configuring STP). In the Cisco world, the default VLAN is VLAN 1.
- **Flow control:** Ethernet provides a means of temporarily stopping the transmission of data to ensure zero packet loss in the presence of network congestion. This is accomplished using *flow control* and the pause frame. First appearing as a part of the IEEE 802.3x standard, it was further expanded upon in the IEEE 802.1Qbb standard.
- **Port mirroring:** Also known as port spanning, port mirroring is covered in more detail later in this chapter.
- **Port security:** Port security works at Layer 2 of the OSI model and allows an administrator to configure switch ports so that only certain MAC addresses can use the port. This essentially differentiates so-called

dumb switches from managed (or intelligent) switches. Three main areas of port security are (1) MAC limiting and filtering (limit access to the network to MAC addresses that are known, and filter out those that are not); (2) 802.1X (adding port authentication to MAC filtering takes security for the network down to the switch port level and increases your security exponentially); and (3) blocking unused ports (all ports not in use should be disabled).

- **Authentication, accounting, and authorization (AAA):** AAA overrides can also be configured for network security parameters as needed. AAA is the primary method for access control and often uses RADIUS, TACACS+, or Kerberos to accomplish integrated security.
- **Usernames/passwords:** It is possible to configure, without AAA, local username authentication using a configured username and password. This does not provide the same level of access control as AAA does and is not recommended.
- **Virtual consoles and terminals:** The console port (often called the *virtual console* or *VC*) is often a serial or parallel port, and it is possible for virtual ports to connect to physical ports. The *virtual terminal* (vt or vty) is a remote port connected to through Telnet or a similar utility and, as an administrator, you will want to configure an access list to limit who can use it.

ExamAlert

Know that the simplest way to protect a virtual terminal interface is to configure a username and password for it and prevent unauthorized logins.

- **Jumbo Frames:** One of the biggest issues with networking is that data of various sizes is crammed into packets and sent across the medium. Each time this is done, headers are created (more data to process), along with any filler needed, creating additional overhead. To get around this, the concept of *jumbo frames* is used to allow for very large Ethernet frames; by sending a lot of data at once, the number of packets is reduced, and the data sent is less processor intensive.
- **Other:** Other common configuration parameters include the speed, whether duplexing will be used or not, IP addressing, and the default gateway. Duplexing determines the direction in which data can flow through the network media and is discussed in Chapter 5, "Cabling Solutions and Issues."