CHAPTER 26

Chapter Goals

- Understand the relationship of LAN switching to legacy internetworking devices such as bridges and routers.
- Understand the advantages of VLANs.
- Know the difference between access and trunk links.
- Know the purpose of a trunk protocol.
- Understand Layer 3 switching concepts.

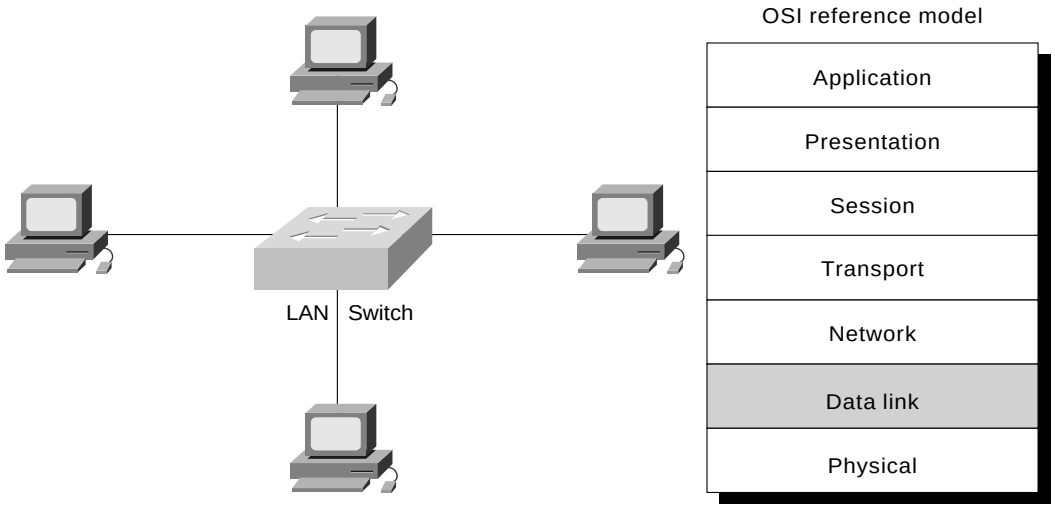
LAN Switching and VLANs

A *LAN switch* is a device that provides much higher port density at a lower cost than traditional bridges. For this reason, LAN switches can accommodate network designs featuring fewer users per segment, thereby increasing the average available bandwidth per user. This chapter provides a summary of general LAN switch operation and maps LAN switching to the OSI reference model.

The trend toward fewer users per segment is known as *microsegmentation*. Micro-segmentation allows the creation of private or dedicated segments—that is, one user per segment. Each user receives instant access to the full bandwidth and does not have to contend for available bandwidth with other users. As a result, collisions (a normal phenomenon in shared-medium networks employing hubs) do not occur, as long as the equipment operates in full-duplex mode. A LAN switch forwards frames based on either the frame's Layer 2 address (Layer 2 LAN switch) or, in some cases, the frame's Layer 3 address (multilayer LAN switch). A LAN switch is also called a frame switch because it forwards Layer 2 frames, whereas an ATM switch forwards cells.

Figure 26-1 illustrates a LAN switch providing dedicated bandwidth to devices and illustrates the relationship of Layer 2 LAN switching to the OSI data link layer.

Figure 26-1 A LAN Switch Is a Data Link Layer Device



History

The earliest LAN switches were developed in 1990. They were Layer 2 devices (bridges) dedicated to solving desktop bandwidth issues. Recent LAN switches evolved to multilayer devices capable of handling protocol issues involved in high-bandwidth applications that historically have been solved by routers. Today, LAN switches are used to replace hubs in the wiring closet because user applications demand greater bandwidth.

LAN Switch Operation

LAN switches are similar to transparent bridges in functions such as learning the topology, forwarding, and filtering. These switches also support several new and unique features, such as dedicated communication between devices through full-duplex operations, multiple simultaneous conversations, and media-rate adaption.

Full-duplex communication between network devices increases file-transfer throughput. Multiple simultaneous conversations can occur by forwarding, or switching, several packets at the same time, thereby increasing network capacity by the number of conversations supported. Full-duplex communication effectively doubles the throughput, while with media-rate adaption, the LAN switch can translate between 10 and 100 Mbps, allowing bandwidth to be allocated as needed.

Deploying LAN switches requires no change to existing hubs, network interface cards (NICs), or cabling.

VLANs Defined

A VLAN is defined as a *broadcast domain* within a switched network. Broadcast domains describe the extent that a network propagates a broadcast frame generated by a station. Some switches may be configured to support a single or multiple VLANs. Whenever a switch supports multiple VLANs,

broadcasts within one VLAN never appear in another VLAN. Switch ports configured as a member of one VLAN belong to a different broadcast domain, as compared to switch ports configured as members of a different VLAN.

Creating VLANs enables administrators to build broadcast domains with fewer users in each broadcast domain. This increases the bandwidth available to users because fewer users will contend for the bandwidth.

Routers also maintain broadcast domain isolation by blocking broadcast frames. Therefore, traffic can pass from one VLAN to another only through a router.

Normally, each subnet belongs to a different VLAN. Therefore, a network with many subnets will probably have many VLANs. Switches and VLANs enable a network administrator to assign users to broadcast domains based upon the user's job need. This provides a high level of deployment flexibility for a network administrator.

Advantages of VLANs include the following:

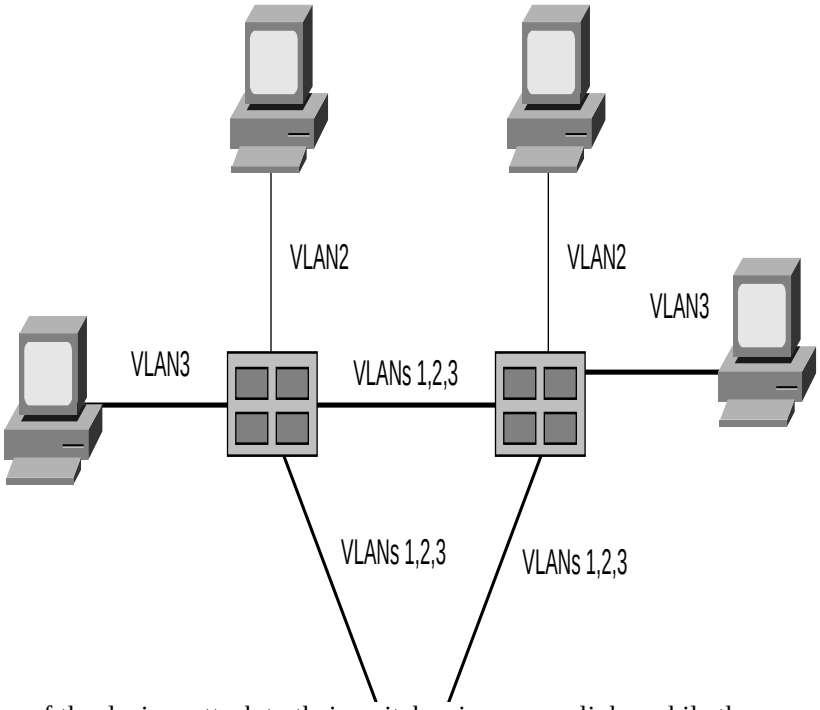
- Segmentation of broadcast domains to create more bandwidth
- Additional security by isolating users with bridge technologies
- Deployment flexibility based upon job function rather than physical placement

Switch Port Modes

Switch ports run in either access or trunk mode. In access mode, the interface belongs to one and only one VLAN. Normally a switch port in access mode attaches to an end user device or a server. The frames transmitted on an access link look like any other Ethernet frame.

Trunks, on the other hand, multiplex traffic for multiple VLANs over the same physical link. Trunk links usually interconnect switches, as shown in Figure 26-2. However, they may also attach end devices such as servers that have special adapter cards that participate in the multiplexing protocol.

Figure 26-2 Switches Interconnected with Trunk Links



Note that some of the devices attach to their switch using access links, while the connections between the switches utilize trunk links.

To multiplex VLAN traffic, special protocols exist that encapsulate or tag (mark) the frames so that the receiving device knows to which VLAN the frame belongs. Trunk protocols are either proprietary or based upon IEEE 802.1Q. For example, a proprietary trunk protocol may be like Cisco's proprietary Inter-Switch Link (ISL), which enables Cisco devices to multiplex VLANs in a manner optimized for Cisco components. Or, an intervendor solution may be implemented, such as 802.1Q, which enables products from more than one vendor to multiplex VLANs on a trunk link.

Without trunk links, multiple access links must be installed to support multiple VLANs between switches. This is not cost-effective and does not scale well, so trunks are preferable for interconnecting switches in most cases.

LAN Switching Forwarding

LAN switches can be characterized by the forwarding method that they support. In the store-and-forward switching method, error checking is performed and erroneous frames are discarded. With the cut-through switching method, latency is reduced by eliminating error checking.

With the store-and-forward switching method, the LAN switch copies the entire frame into its onboard buffers and computes the cyclic redundancy check (CRC). The frame is discarded if it contains a CRC error or if it is a *runt* (less than 64 bytes, including the CRC) or a *giant* (more than 1518 bytes, including the CRC). If the frame does not contain any errors, the LAN switch looks up the destination address in its forwarding, or switching, table and determines the outgoing interface. It then forwards the frame toward its destination.

With the cut-through switching method, the LAN switch copies only the destination address (the first 6 bytes following the preamble) into its onboard buffers. It then looks up the destination address in its switching table, determines the outgoing interface, and forwards the frame toward its destination. A cut-through switch provides reduced latency because it begins to forward the frame as soon as it reads the destination address and determines the outgoing interface.

Some switches can be configured to perform cut-through switching on a per-port basis until a user-defined error threshold is reached, when they automatically change to store-and-forward mode. When the error rate falls below the threshold, the port automatically changes back to store-and-forward mode.

LAN switches must use store-and-forward techniques to support multilayer switching. The switch must receive the entire frame before it performs any protocol-layer operations. For this reason, advanced switches that perform Layer 3 switching are store-and-forward devices.

LAN Switching Bandwidth

LAN switches also can be characterized according to the proportion of bandwidth allocated to each port. Symmetric switching provides evenly distributed bandwidth to each port, while asymmetric switching provides unlike, or unequal, bandwidth between some ports.

An *asymmetric LAN switch* provides switched connections between ports of unlike bandwidths, such as a combination of 10BaseT and 100BaseT. This type of switching is also called *10/100 switching*. Asymmetric switching is optimized for client/server traffic flows in which multiple clients simultaneously communicate with a server, requiring more bandwidth dedicated to the server port to prevent a bottleneck at that port.

A *symmetric switch* provides switched connections between ports with the same bandwidth, such as all 10BaseT or all 100BaseT. Symmetric switching is optimized for a reasonably distributed traffic load, such as in a peer-to-peer desktop environment.

A network manager must evaluate the needed amount of bandwidth for connections between devices to accommodate the data flow of network-based applications when deciding to select an asymmetric or symmetric switch.

LAN Switch and the OSI Model

LAN switches can be categorized according to the OSI layer at which they filter and forward, or switch, frames. These categories are: Layer 2, Layer 2 with Layer 3 features, or multilayer.

A Layer 2 LAN switch is operationally similar to a multiport bridge but has a much higher capacity and supports many new features, such as full-duplex operation. A Layer 2 LAN switch performs switching and filtering based on the OSI data link layer (Layer 2) MAC address. As with bridges, it is completely transparent to network protocols and user applications.

A Layer 2 LAN switch with Layer 3 features can make switching decisions based on more information than just the Layer 2 MAC address. Such a switch might incorporate some Layer 3 traffic-control features, such as broadcast and multicast traffic management, security through access lists, and IP fragmentation.

A multilayer switch makes switching and filtering decisions based on OSI data link layer (Layer 2) and OSI network layer (Layer 3) addresses. This type of switch dynamically decides whether to switch (Layer 2) or route (Layer 3) incoming traffic. A multilayer LAN switch switches within a workgroup and routes between different workgroups.

Layer 3 switching allows data flows to bypass routers. The first frame passes through the router as normal to ensure that all security policies are observed. The switches watch the way that the router treats the frame and then replicate the process for subsequent frames. For example, if a series of FTP frames flows from a 10.0.0.1 to 192.168.1.1, the frames normally pass through a router. Multilayer switching observes how the router changes the Layer 2 and Layer 3 headers and imitates the router for the rest of the frames. This reduces the load on the router and the latency through the network.

Review Questions

Q—*A multilayer switch mimics the actions of a router when an initial frame passes through a router. What things does the multilayer switch do to the Layer 2 and Layer 3 headers to thoroughly imitate the router?*

A—The switch must modify the source and destination MAC addresses in the Layer 2 header so that the frame appears to come from/to the router/workstation. Furthermore, the switch must change things in the Layer 3 header such as the IP time-to-live value.

Q—*A LAN switch most closely resembles what type of internetworking device?*

A—A LAN switch behaves like a multiport bridge.

Q—*Two trunk protocols were described. For what situation would you use the IEEE 802.1Q mode?*

A—Whenever you deploy a hybrid of switches from multiple vendors and need to trunk between them. All other trunk protocols work within specific vendor equipment environments.

Q—*Which switching method protects network segment bandwidth from errored frames?*

Store-and-forward transmits frames only if the frame's integrity is assured. If the switch receives an errored frame, then the switch discards it.

Q—*How does a store-and-forward switch know if a frame is errored?*

A—The switch uses the CRC to determine whether any changes occurred to the frame since the source generated it. The switch calculates CRC for the received frame and compares it with the CRC transmitted with the frame. If they differ, the frame changed during transit and will be discarded in a store-and-forward switch.

Q—*Do VLAN borders cross routers?*

A—No. VLANs are broadcast domains and describe the extent that broadcast frames transit the network. Routers do not pass broadcasts. Therefore, the same VLAN cannot exist on two ports of a router.

Q—*How does a trunk link differ from an access link?*

A—An access link carries traffic for a single VLAN. The traffic on an access link looks like any other Ethernet frame. A trunk link transports traffic for multiple VLANs across a single physical link. Trunks encapsulate Ethernet frames with other information to support the multiplexing technology employed.

Q—*Before switches and VLANs, administrators assigned users to a network based not on the user's needs, but on something else. What determined the user network assignment?*

A—Administrators previously assigned users to a network based upon the user's physical proximity to a network device or cable.

For More Information

Breyer, Robert, and Sean Riley. *Switched and Fast Ethernet*. New York: Ziff-Davis Press, 1997.

Clark, Kennedy, and Kevin Hamilton. *CCIE Professional Development: Cisco LAN Switching.* Indianapolis: Cisco Press, 1999.

Hein, Mathias, and David Griffiths. *Switching Technology in the Local Network*. New York: International Thomson Publishing, 1997.

Perlman, Radia. *Interconnections*, Second Edition: *Bridges, Routers, Switches, and Internetworking Protocols.* Boston: Addison Wesley, 1999.