Today's local-area networks (LANs) are becoming increasingly congested and overburdened. In addition to an ever-growing population of network users, several factors have combined to stress the capabilities of traditional LANs:

- Faster CPUs-In the mid-1980s, the most common desktop workstation was a PC. At the time, most PCs could execute 1 million instructions per second (MIPS). Today, workstations with 50 to 75 MIPS of processing power are common, and I/O speeds have increased accordingly. Two modern engineering workstations on the same LAN can easily saturate it.
- Faster operating systems-Until recently, operating system design had constrained network access. Of the three most common desktop operating systems (DOS/Windows, the UNIX operating system, and the Mac OS), only the UNIX operating system could multitask. Multitasking allows users to initiate simultaneous network transactions. With the release of Windows 95, which reflected a redesign of DOS/Windows that included multitasking, PC users could increase their demands for network resources.
- Network-intensive applications-Use of client-server applications, such as Network File System (NFS), LAN Manager, NetWare, and World Wide Web is increasing. Client-server applications allow administrators to centralize information, thus making it easy to maintain and protect. Client-server applications free users from the burden of maintaining information and the cost of providing enough hard disk space to store it. Given the cost benefit of client-server applications, such applications are likely to become even more widely used in the future.

Switching is a technology that alleviates congestion in Ethernet, Token Ring, and Fiber Distributed Data Interface (FDDI) LANs by reducing traffic and increasing bandwidth. Such switches, known as LAN switches, are designed to work with existing cable infrastructures so that they can be installed with minimal disruption of existing networks. Often, they replace shared hubs. This case study describes how LAN switching works, how virtual LANs work, and how to configure virtual LANs (VLANs) in a topology that consists of Catalyst 5000 LAN switches.

Guide Contents
Internetworking Design Basics
Designing various internetworks
Network Enhancements
IP Routing Concepts
UDP Broadcast Flooding
Large-Scale H.323 Network Design for Service Providers
LAN Switching
Subnetting an IP Address Space
IBM Serial Link Implementation Notes
References and Recommended Reading

Contents

Understanding Switching Basics

The term switching was originally used to describe packet-switch technologies, such as Link Access Procedure, Balanced (LAPB), Frame Relay, Switched Multimegabit Data Service (SMDS), and X.25. Today, switching refers to a technology that is similar to a bridge in many ways.

The term bridging refers to a technology in which a device (known as a bridge) connects two or more LAN segments. A bridge transmits datagrams from one segment to their destinations on other segments. When a bridge is powered and begins to operate, it examines the Media Access Control (MAC) address of the datagrams that flow through it to build a table of known destinations. If the bridge knows that the destination of a datagram is on the same segment as the source of the datagram, it drops the datagram because there is no need to transmit it. If the bridge knows that the destination is on another segment, it transmits the datagram on that segment only. If the bridge does not know the destination segment, the bridge transmits the datagram on all segments except the source segment (a technique known as flooding). The primary benefit of bridging is that it limits traffic to certain network segments.

Like bridges, switches connect LAN segments, use a table of MAC addresses to determine the segment on which a datagram needs to be transmitted, and reduce traffic. Switches operate at much higher speeds than bridges, and can support new functionality, such as virtual LANs.

Switching in the Ethernet Environment

The most common LAN media is traditional Ethernet, which has a maximum bandwidth of 10 Mbps. Traditional Ethernet is a half-duplex technology. Each Ethernet host checks the network to determine whether data is being transmitted before it transmits and defers transmission if the network is in use. In spite of transmission deferral, two or more Ethernet hosts can transmit at the same time, which results in a collision. When a collision occurs, the hosts enter a back-off phase and retransmit later. As more hosts are added to the network, hosts must wait more often before they can begin transmitting, and collisions are more likely to occur because more hosts are trying to transmit. Today, throughput on traditional Ethernet LANs suffers even more because users are running network-intensive software, such as client-server applications, which cause hosts to transmit more often and for longer periods of time.

An Ethernet LAN switch improves bandwidth by separating collision domains and selectively forwarding traffic to the appropriate segments. Figure: Ethernet switching shows the topology of a typical Ethernet network in which a LAN switch has been installed.

Figure: Ethernet switching
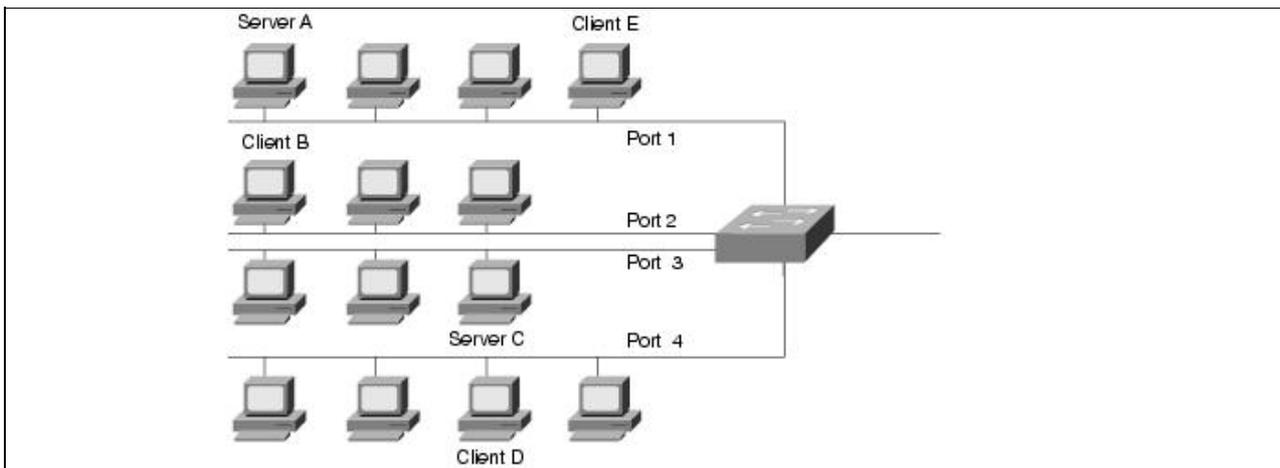
In <u>Figure: Ethernet switching</u>, each Ethernet segment is connected to a port on the LAN switch. If Server A on port 1 needs to transmit to Client B on port 2, the LAN switch forwards Ethernet frames from port 1 to port 2, thus sparing port 3 and port 4 from frames destined for Client B. If Server C needs to send data to Client D at the same time that Server A sends data to Client B, it can do so because the LAN switch can forward frames from port 3 to port 4 at the same time it is forwarding frames from port 1 to port 2. If Server A needs to send data to Client E, which also resides on port 1, the LAN switch does not need to forward any frames.

Performance improves in LANs in which LAN switches are installed because the LAN switch creates isolated collision domains. By spreading users over several collision domains, collisions are avoided and performance improves. Many LAN switch installations assign just one user per port, which gives that user an effective bandwidth of 10 Mbps.

Understanding Virtual LANs

A virtual LAN (VLAN) is a group of hosts or network devices, such as routers (running transparent bridging) and bridges, that forms a single bridging domain. Layer 2 bridging protocols, such as IEEE 802.10 and Inter-Switch Link (ISL), allow a VLAN to exist across a variety of equipment, including LAN switches.

VLANs are formed to group related users regardless of the physical connections of their hosts to the network. The users can be spread across a campus network or even across geographically dispersed locations. A variety of strategies can be used to group users. For example, the users might be grouped according to their department or functional team. In general, the goal is to group users into VLANs so that most of their traffic stays within the VLAN. When you configure VLANs, the network can take advantage of the following benefits:

- Broadcast control-Just as switches physically isolate collision domains for attached hosts and only forward traffic out a particular port, VLANs provide logical collision domains that confine broadcast and multicast traffic to the bridging domain.
- Security-If you do not include a router in a VLAN, no users outside of that VLAN can communicate with the users in the VLAN and vice versa. This extreme level of security can be highly desirable for certain projects and applications.
- Performance-You can assign users that require high-performance networking to their own VLANs. You might, for example, assign an engineer who is testing a multicast application and the servers the engineer uses to a single VLAN. The engineer experiences improved network performance by being on a "dedicated LAN," and the rest of the engineering group experiences improved network performance because the traffic generated by the network-intensive application is isolated to another VLAN.

Figure: Ethernet switching   3

- Network management-Software on the switch allows you to assign users to VLANs and, later, reassign them to another VLAN. Recabling to change connectivity is no longer necessary in the switched LAN environment because network management tools allow you to reconfigure the LAN logically in seconds.

Figure: Typical VLAN topology shows an example of a switched LAN topology in which VLANs are configured.

Figure: Typical VLAN topology
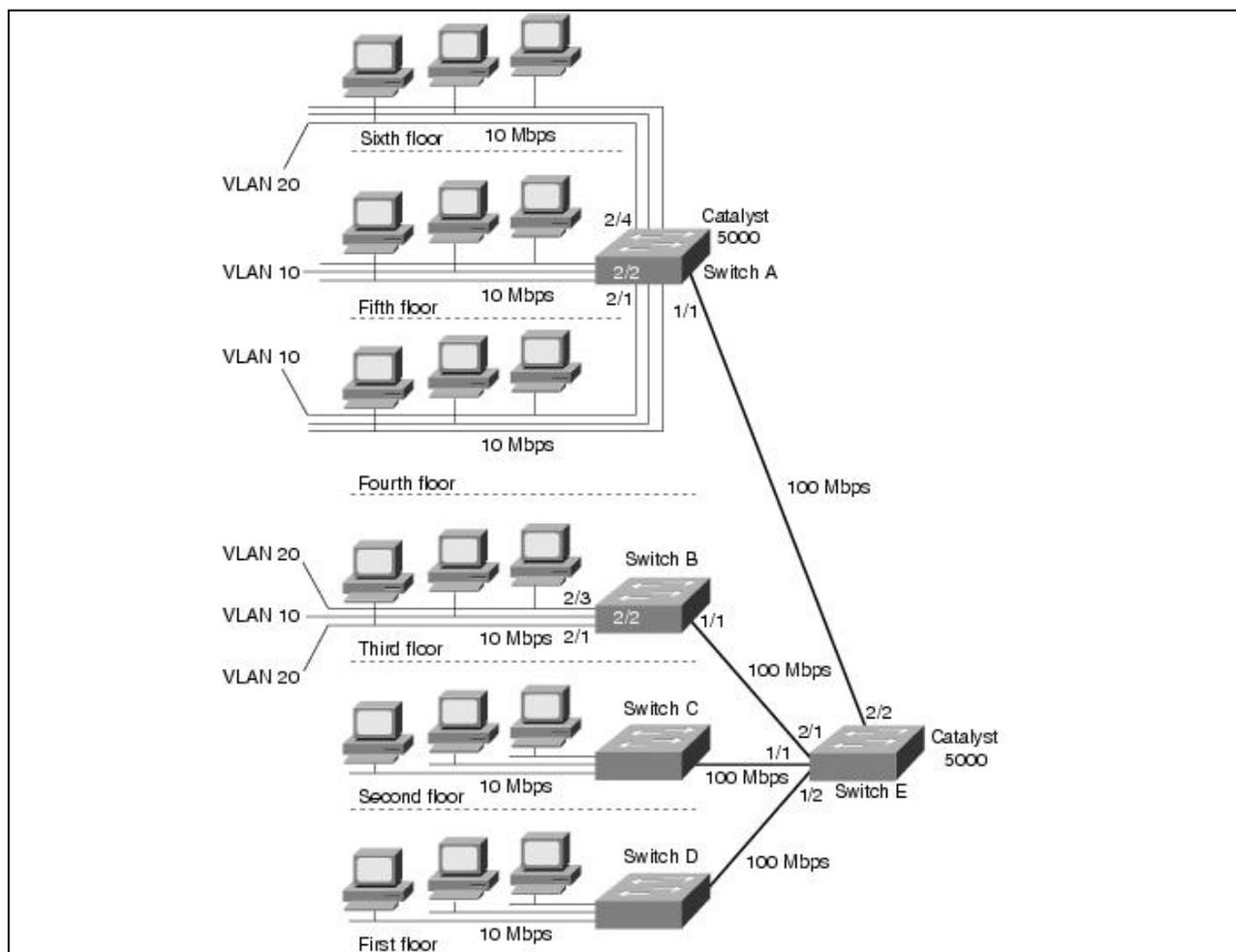
In Figure: Typical VLAN topology, a 10-Mbps Ethernet connects the hosts on each floor to Catalyst 5000 LAN switches. 100-Mbps Fast Ethernet connects switches A, B, C, and D to Switch E.

Note: The Catalyst 5000 has five slots in which modules can be installed. The supervisor engine module is always installed in slot 1. The supervisor engine module is the main system processor switch; it provides a console port and two 100-Mbps Fast Ethernet ports. A variety of other modules providing 10-Mbps Ethernet and Fast Ethernet interfaces can be installed in slots 2 through 5. Ports are identified by their slot number and their position, from left to right, on the module. For example, port 2/2 is the second port from the left on the module in slot 2.

The switches in Figure: Typical VLAN topology communicate with each other using ISL, which is a protocol that maintains VLAN information as traffic flows between the switches. With ISL, an Ethernet

Understanding Virtual LANs   4

frame is encapsulated with a 30-byte header that contains a two-byte VLAN ID.

Figure: Typical VLAN topology shows that VLAN 20 consists of port 4 in slot 2 on Switch A and ports 1 and 3 in slot 4 on Switch B. Frames exchanged between ports 1/4 and 3/4 are switched by Switch B as normal. On Switch B, any frame generated by ports 1/4 and 3/4 that is not destined for ports 1/4 and 3/4 is encapsulated in an ISL header that includes a VLAN 20 identifier and is sent to Switch E. Switch E examines the ISL header and determines that the frame is intended for VLAN 20 and sends the frame out on port 2/2 to Switch A. Switch A examines the ISL header to determine the VLAN for which the frame is destined, removes the header, and switches it to all ports in VLAN 20 (if the frame is broadcast or multicast) or to port 2/4 if the frame is a unicast.

Configuring the Switches

When a Catalyst 5000 switch first starts up, the following defaults are set:

- The console port is set to 9600 baud, 8 data bits, no parity, and 1 stop bit. If you want to change the baud rate, use the **set system baud** command.
- The Cisco Discovery Protocol (CDP) is enabled on every port to send a CDP message every 60 seconds. If you want to disable CDP on ports that do not have a Cisco device, use the **set cdp disable** command.
- The following Simple Network Management Protocol (SNMP) community strings are defined:
  - ♦ "public" for the read-only access type
  - ♦ "private" for the read-write access type
  - ♦ "secret" for the read-write-all access type

  If you want to set other SNMP community strings, use the **set snmp community** command.

- All modules and all ports are enabled. To disable a module, use the **set module disable** command, and to disable a port, use the **set port disable** command.
- All 10-Mbps Ethernet ports are set to half duplex. Use the **set port duplex** command to set a port to full duplex.

When you first start up a switch, you should set some values that apply to the switch as a whole. For example, you might enter the following commands at the console port of Switch A:

```
set system contact Terry Moran
set system location Norwich
set system name SwitchA
set time fri 9/15/95 14:08:34
set prompt SwitchA>
set password
set enablepass
set interface sc0 131.108.40.1
```

The **set system contact** command establishes "Terry Moran" as the person to contact for system administration. The **set system name** establishes "SwitchA" as the name of this switch. The **set time** command sets the current time, using a 24-hour clock format. The **set prompt** command sets the prompt to "SwitchA>". The default prompt is "Console".

The **set password** command sets password protection for the administrative interface in normal mode. When you enter the **set password** command, the switch prompts you to enter a password and then prompts you to reenter the password.

The **set enablepass** command sets password protection for the administrative interface in privileged mode. When you enter the **set enablepass** command, the switch prompts you to enter a password and then prompts you to reenter the password.

The **set interface** command assigns an IP address and netmask to interface sc0. After you make this assignment, you can Telnet to the switch to perform administrative tasks. The switch supports up to eight simultaneous Telnet connections. Alternatively, you can use the **set interface** command to enable a Serial Line Interface Protocol (SLIP) connection on the console interface (sl0).

Configuring VLANs on Switch A

The following commands configure VLANs 10 and 20 on Switch A:

```
set vlan 10 2/1,2/2
set vlan 20 2/4
set trunk 1/1 10,20
```

The first **set vlan** command creates VLAN 10 and assigns ports 1 and 2 in slot 2 to it. The second **set vlan** command creates VLAN 20 and assigns port 4 in slot 2 to it.

The **set trunk** command configures port 1 in slot 1 as a trunk and adds VLANs 10 and 20 to it. Trunks are used for Fast Ethernet connections between switches. When a port is configured as a trunk, it runs in ISL mode. To detect and break loops, trunks use the spanning-tree protocol on all VLANs that are carried across the trunk.

Configuring VLANs on Switch B

The following commands configure VLANs 10 and 20 on Switch B:

```
set vlan 10 2/2
set vlan 20 2/1,2/3
set trunk 1/1 10,20
```

The first **set vlan** command creates VLAN 10 and assigns port 2 in slot 2 to it. The second **set vlan** command creates VLAN 20 and assigns ports 1 and 3 in slot 2 to it. The **set trunk** command configures port 1 in slot 1 as a trunk and adds VLANs 10 and 20 to it.

Configuring VLANs on Switch E

The following commands configure VLANs 10 and 20 on Switch E:

```
set trunk 2/1 10,20
set trunk 2/2 10,20
```

The first **set trunk** command configures port 1 in slot 2 as a trunk and adds VLANs 10 and 20 to it. This trunk is used to communicate with Switch B. The second **set trunk** command configures port 2 in slot 2 as a trunk and adds VLANs 10 and 20 to it. This trunk is used to communicate with Switch A.

Summary

LAN switching technology improves the performance of traditional Ethernet, FDDI, and Token Ring technologies without requiring costly wiring upgrades or time-consuming host reconfiguration. The low price per port allows the deployment of LAN switches so that they decrease segment size and increase available

bandwidth. VLANs make it possible to extend the benefit of switching over a network of LAN switches and other switching devices.