Networking Course. Lesson 1. Networking Basis

Document version 0.1
This document was created, but not reviewed yet.
You should use it very carefully.

Theory

- Networking Basics
  - What Is a Network?
  - Logical Networks
  - Data Transmission Modes
  - Types of Networks
- Network Models and Standards
  - OSI Model
  - Moving Through the OSI Model
  - Hierarchical Design Model
  - Network Standards
- Local-Area Networking Introduction
  - Comparing LANs to WANs
  - OSI Model (As It Applies to LANs and the Interrelation Between Layers)
  - Summary
- Traditional LAN Architecture
  - Components of a LAN
  - LAN Topologies
  - Local-Area Networks (LANs)
- Ethernet LANs
  - Media Access Control (MAC) Addressing
  - Carrier Sense Multiple Access with Collision Detect (CSMA/CD)
  - Ethernet LAN Equipment
- How a Switch Works
  - Frames Revisited
  - Transmission Methods
  - Frame Size
  - Layer 2 Switching Methods
  - Layer 3 Switching

Networking Basics

What Is a Network?

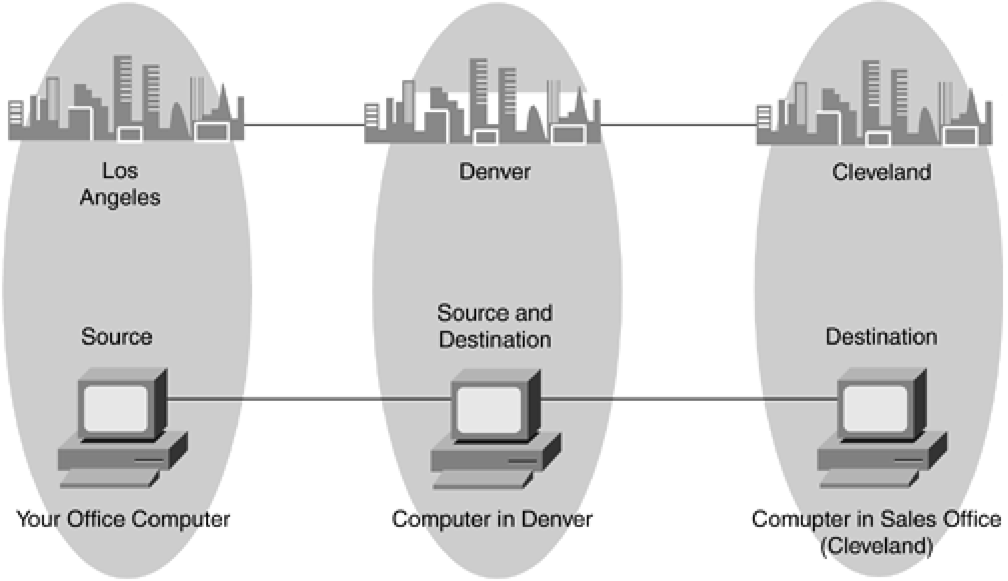
A network is a system of interconnecting lines, such as telephone lines for communication or subway tracks for transportation. We use transportation networks during the course of an average day for a number of different purposes: the train or subway for daily expeditions, the roads for commuting to and from work, and the airlines for longer trips. In the computer and Information Technology (IT) environment, a network is just defined as a group of computers and connecting circuitry functioning in a specific manner. A transportation network is defined as a system of crossing or interconnecting routes, such as roads or subway tracks.

Transportation and Computer Networks

A transportation network connects two or more points, enabling the exchange of resources, such as people, goods, or information. These points might be cities connected by railroad lines, buildings within a city connected by streets, or desks within a building connected by hallways and stairwells. The common denominator here is that there is some sort of connection, or path, between these pointsrailroad tracks, city streets, or office hallways. These paths provide a way for people or goods to get from one point to another. This originating point, or starting point, is called the sender, originator, or source; the second point, or arrival point, is called the receiver, or destination.

In transportation networks, an originating (source) and ending point (destination) are two distinct locations in a journey. In addition, the ending point can become the originating point for another part of a journey. Think of a flight from Los Angeles to Cleveland with a two-hour layover in Denver, as shown in Figure 1-1. Denver, in this case, is both a destination and an end point of one trip and the starting point of another trip. Computer networks function in a similar way. Data can be sent to a destination (endpoint) that in turn becomes the originating point for another transmission to the final destination. These sources and destinations are not fixed points, but change depending on the direction of message (data) flow.

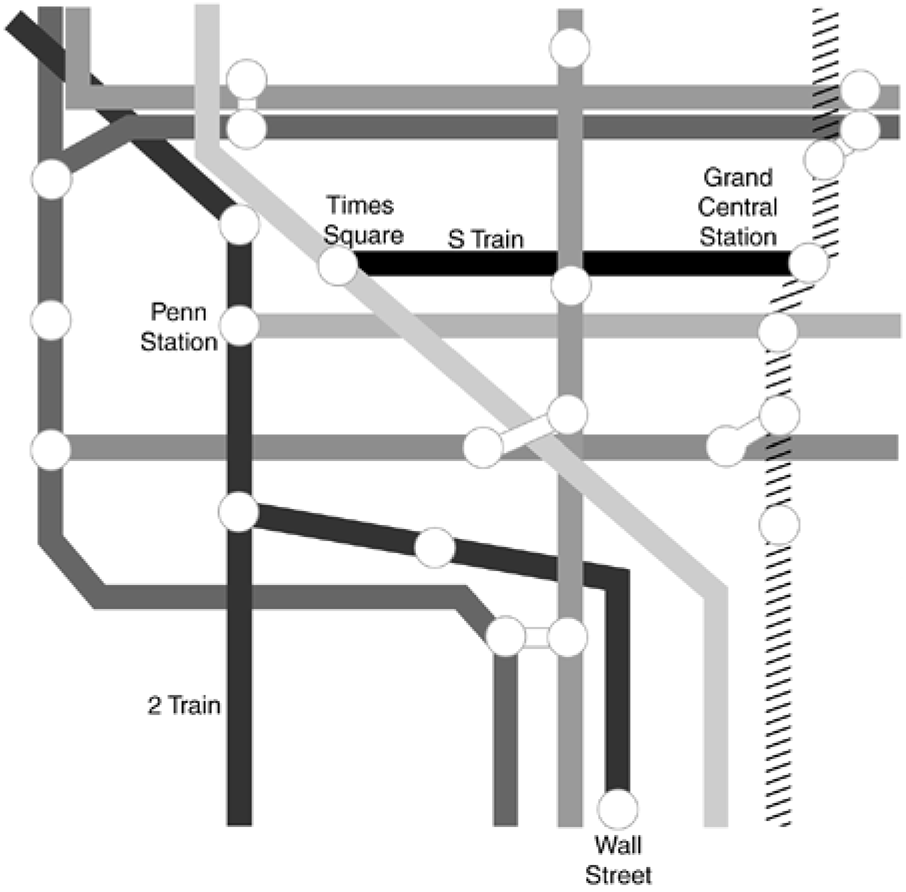
Figure 1-1. Source and Destination Relationships



To better understand IT networks, such as data (computer or Internet) or voice (telephone) networks, and the concept of switching within these networks, let's look first at the networks we use daily, such as the subway, railroad, and airline routes.

As described previously, these are transportation networks that effect the moving of resources (people) from one point to another across an established path. Take, for example, the New York City subway. Figure 1-2 shows a few stops.

Figure 1-2. New York City Subway Stops



If you are on Wall Street and want to go to Grand Central Station, you cannot take a direct route between these two points. As illustrated in Figure 1-2, you might take the number 2 train to Times Square and the S train from Times Square to Grand Central.

It is the connection of Wall Street to Times Square to Grand Central that enables you to move from Wall Street to Grand Central, and it is the network of these subway connections that enables you to move throughout the city.

The airline and the subway networks connect different points and connect them in differing fashions. In the case of the airlines, cities are connected via preplanned routes in the sky. In the case of the subway, various city points (stations) are connected via subway tracks. A key point here is that just because a network path passes through a city block, in the case of the subway, or over a city, in the case of an airline, that pass-through point cannot be used to get on or off the network. The only way you can join a network is at an origination (starting) or termination (ending) point of the network connection.

While walking along the streets of New York City, for example, you can hear, and sometimes see, the subway trains running under the city sidewalk, but you can't get on the train from that point (unless you happen to be in a Hollywood movie chase scene). To get on that train, you must get to a station on that train's route, a demarcation point. A demarcation point is the boundary between two entities; in this case, the demarcation point is the boundary between the street and the train station. This demarcation point is both the point whereby passengers get on the train (originating or source point) or get off the train (terminating or destination point).

It is important to understand that the origination point and the termination point are interconnected, meaning they are connected to each other in some fashion. In the New York City subway, Wall Street and Times Square are interconnected via one set of tracks, Times Square and Grand Central Station are interconnected via another set of tracks, and Wall Street and Grand Central Station are interconnected via yet another set of tracks. Times Square is the switching point for passengers between Wall Street and Grand Central, because subway passengers need to disembark the number 2 train (Wall StreetTimes Square) in order to board the S train (Times SquareGrand Central).

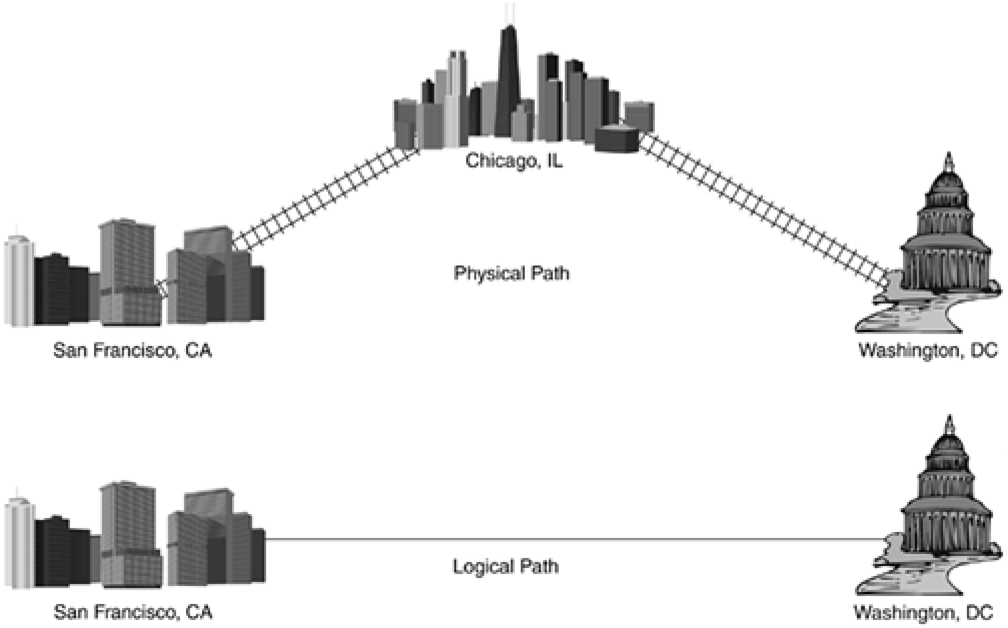
Each track segment and station is a leg in the subway network. Legs of the network are joined at key locations, where other major arteries carry you to other key locations. These key locations are "distribution" or "hub" points on the network. This is true of airlines, roads, and telephone calls.

Logical Networks

Transportation networks are made up of physical objects that you can hold or touch with your hand, such as railroad ties and subway rails. Logical network elements do not have these same physical properties as physical networks. Just as virtual reality in video games gives you the illusion of driving a tank or firing a weapon (even though you are not really in a tank or pulling the trigger), logical networks are based on elements that you can't really see or hold, but nonetheless they are there.

A network is made up of several pieces and parts that connect the source and destination. These pieces and parts are grouped into two categories: physical and logical components. It is these physical and logical components that make up the infrastructure and end-user pieces of a network, enabling you to communicate with someone else on the network. Suppose, for example, that you are taking the train from Washington, D.C., to San Francisco. There is a physical and logical component to your trip, as illustrated in Figure 1-3.

Figure 1-3. Physical and Logical Journey from Washington, D.C., to San Francisco



View full size image

The physical path of your journey takes you from Washington, D.C., to Chicago, where you switch trains to continue to San Francisco. In your mind, however, your trip is logically from Washington, D.C., to San Francisco because you are not staying over in Chicago, merely changing trains. The physical component here are the tracks between the three cities, but the logical component is the starting and ending point of the two cities because you are most concerned with where you start your trip and where your trip ends.

This same physical and logical concept applies to networking and networking components. A brief introduction to these physical and logical components follows.

Network Physical Components

The physical component of a network is a network hardware device, such as a switch and the cabling. This collection of devices and cables, carrying the data from source to destination, makes up the complete physical network.

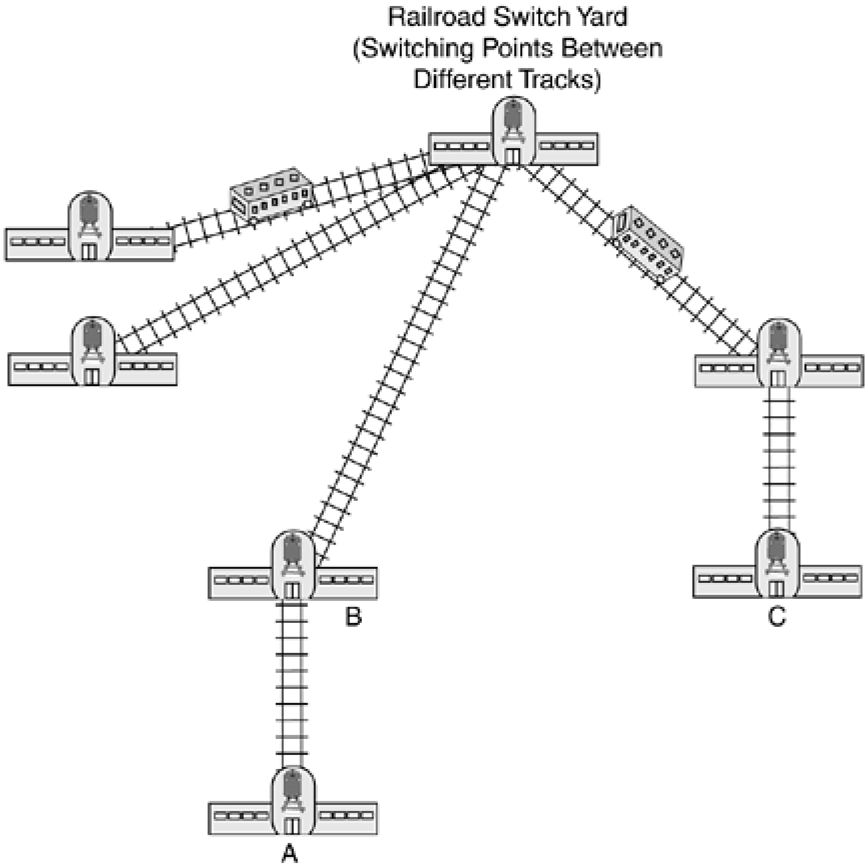
Switches

If there isn't a straight route from one city to the next, either the train passengers have to disembark from one train and board another, at a demarcation point (train station), or the trains themselves have to change paths at rail switching stations along the way. Network switches work in a similar fashion by connecting network paths together, providing a route for the frame from source to destination. A switch can also connect one machine to another in a straight path and might be the only path that exists, such as for two PCs connected together in the same room, or for a PC and a networked printer.

Figure 1-4 illustrates the function of a switchyard in a railroad network. A train starting at a distant-end station must go through a railroad switchyard that will change the train's route so that the train can reach its destination train station. In networking, the distant end can be either of the following, depending on the context of the conversation you are having with someone when discussing your network:

- The terminating point of the attached network connection
- The entire path

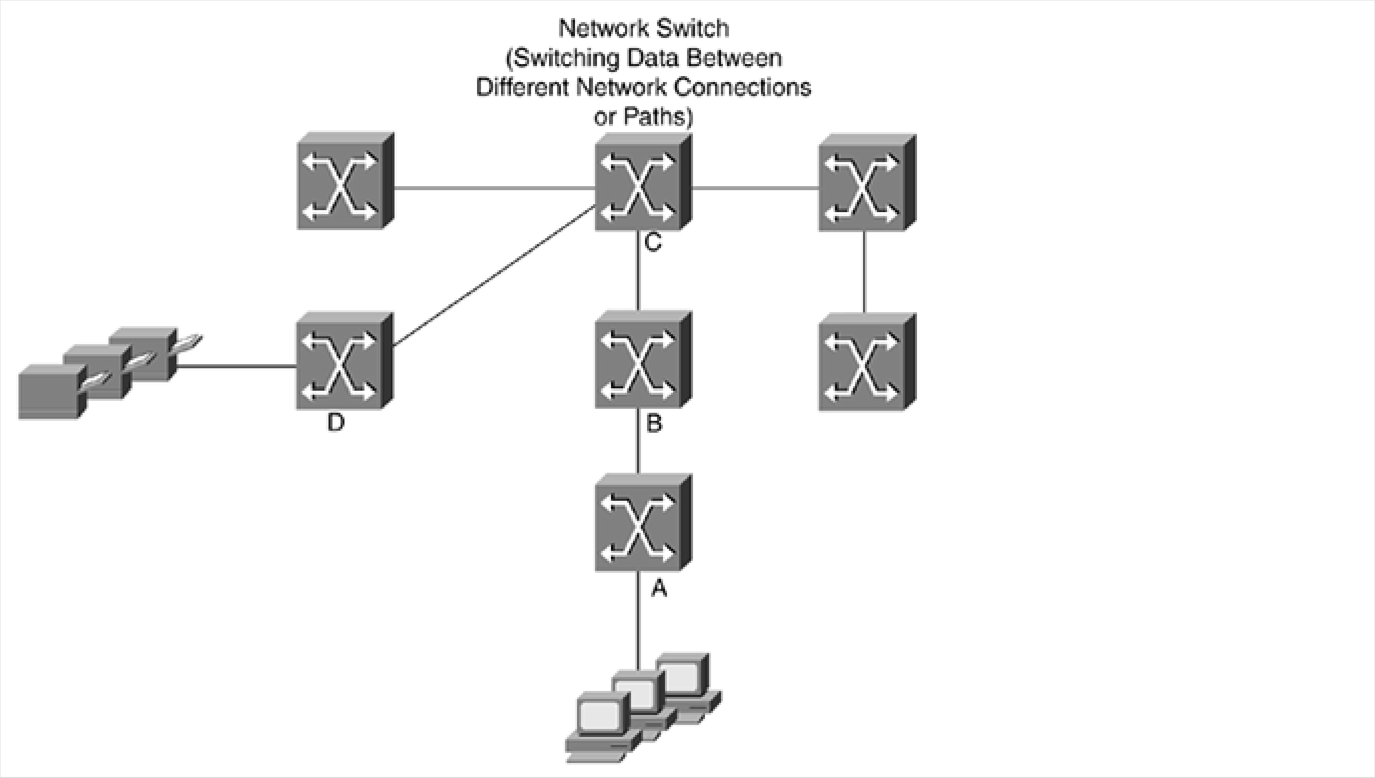
Figure 1-4. Railroad Switching Point Between Different Tracks



In Figure 1-4, for example, a train leaves from station A, the distant end of the track is station B, and the distant end of the path (ultimate destination of the passengers) is station C. It is important to establish the context when discussing network origination and termination points: Are you discussing the physical connection between two points or the entire path from source to destination?

Figure 1-5 illustrates this same switching concept in a data network, such as you might find in a corporate office.

Figure 1-5. Network Switching Between Paths



For example, user computers are connected to this network by switch A. To print documents from their computers, the users instruct the application to print. The application then sends the document across the network to the printers connected to switch D. The document to be printed is packaged in a frame and sent out on to the network, where it passes through switch B and switch C and terminates at switch D. Switch D then passes the frame(s) to the printer for the users to retrieve. All this switching, which is transparent to the user, occurs as a result of the user pressing Ctrl-P in a word processor program.

Cabling

To interconnect two or more points, there must be some sort of medium to carry the information from one point to the other, like the railroad tracks between train stations. A medium is defined as the physical substance through which something else is transmitted or carried. Different types of media are used today for network communication, such as copper cable, fiber-optic cable, and the air.

Copper cabling carries electrical signals, such as those generated by computer modems and telephone handsets. Fiber-optic cabling carries light signals, which are transmitted as pulses of light. Imagine turning a flashlight on and off in Morse code. Fiber-optic transmission works in a fashion similar to Morse code, but is much faster and uses a different code. The air carries radio and voice signals, such as the words we speak and the radio broadcasts to which we listen. Simply stated, when people talk, the air between the speaker and the listener is changed, or modulated. The listener's eardrum converts the changes, or demodulates the signal (in this case the voice), so that the listener can understand the signal.

Network cabling connects network devices, such as computers, much as the railroad tracks connect stations within a city or between cities. Without these tracks, the railroad engines and cars would have no way to go from city to city. Without cabling, network devices would not be able to exchange information. If you are deploying a wireless network, however, the communication principles are the same in that each network device must be connected to a wireless transmitter/receiver, or transceiver, for communication to occur.

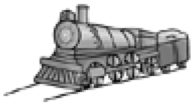
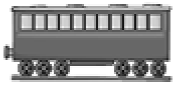
Network Logical Components

The logical component of a network is the information being carried from source to destination. The user information, which is called data, is carried inside a frame across the network.

Frames

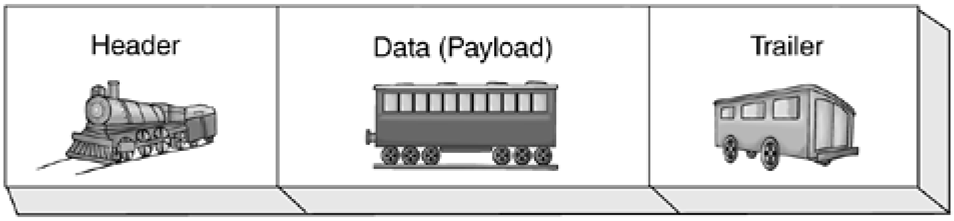
Frames carry the data across the network and are made up of three parts: the header, the data itself, and the trailer. It is these frames that carry user data, just as railroad cars carry passengers. Whereas railroad passengers have tickets specifying their destinations, frames have destination addresses.

Let's look at the functions of the three components of a frameheader, payload, and trailerby comparing them to railroads:

- Frame header 
    - Train engine carrying source and destination information, such as the source and destination address (identifies the sender of the data and as well as the intended recipient)
- Frame data 
    - Train car carrying passengers (user data)
- Frame trailer
    - Train caboose signifying the end of the train (frame)

These components combine to make up a complete frame, as illustrated in Figure 1-6.

Figure 1-6. Complete FrameHeader, Data (Payload), Trailer



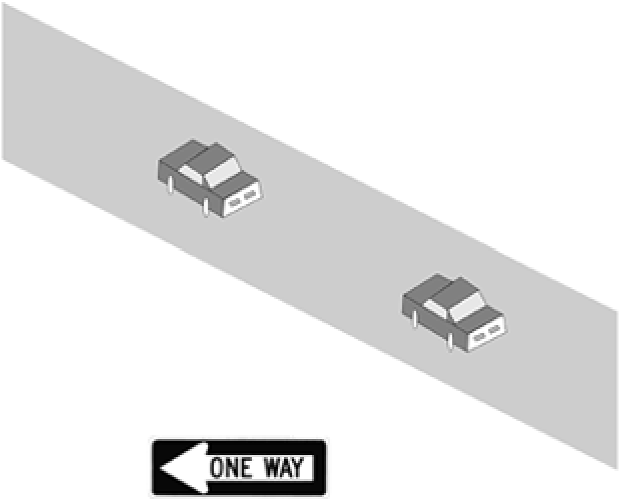
User data moves like passengers on a trainthey ride the train to reach a destination. Whereas railroad cars carry passengers, network frames carry data. The physical network moves these frames carrying the data from source to destination across the network.

Data Transmission Modes

Network devices use three transmission modes (methods) to exchange data, or "talk" to each other, as follows: simplex, half duplex, and full duplex.

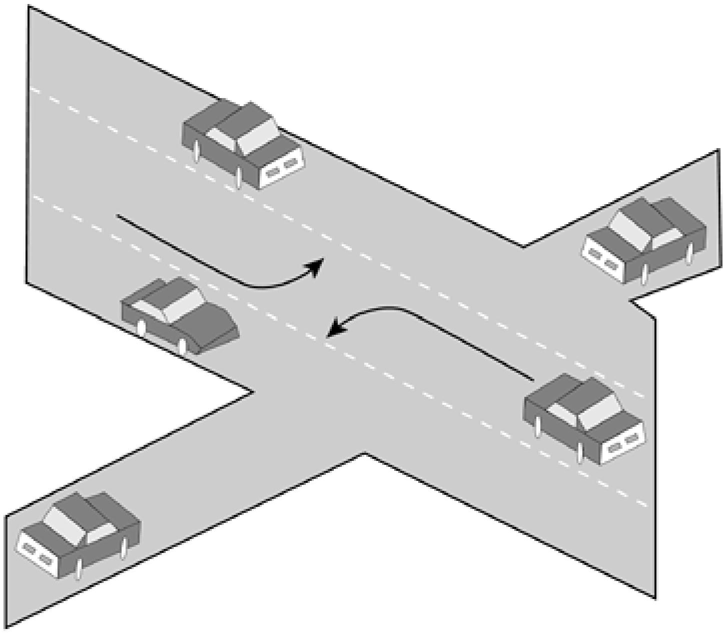
- Simplex transmission is like a one-way street where traffic moves in only one direction. Simplex mode is a one-way-only transmission, which means that data can flow only in one direction from the sending device to the receiving device. Figure 1-7 illustrates simplex transmission.

  Figure 1-7. Simplex (One-Way Street)

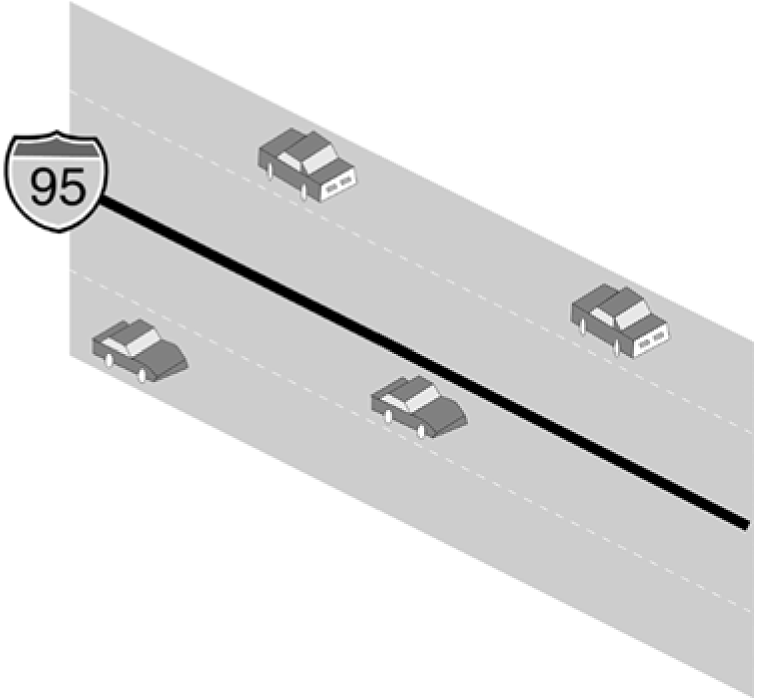
- Half-duplex transmission is like the center lane on some three-lane roads. It is a single lane in which traffic can move in one direction or the other, but not in both directions at the same time. Half-duplex mode limits data transmission because each device must take turns using the line. Therefore, data can flow from A to B and from B to A, but not at the same time. Figure 1-8 illustrates half-duplex transmission.

Figure 1-8. Half Duplex (Center Turn Lane)



- Full-duplex transmission is like a major highway with two lanes of traffic, each lane accommodating traffic going in opposite directions. Full-duplex mode accommodates two-way simultaneous transmission, which means that both sides can send and receive at the same time. In full-duplex mode, data can flow from A to B and B to A at the same time. Figure 1-9 illustrates full-duplex transmission.

Figure 1-9. Full Duplex (Interstate Highway)



Full-duplex transmission is, in fact, two simplex connections: One connection has traffic flowing in only one direction; the other connection has traffic flowing in the opposite direction of the first connection.

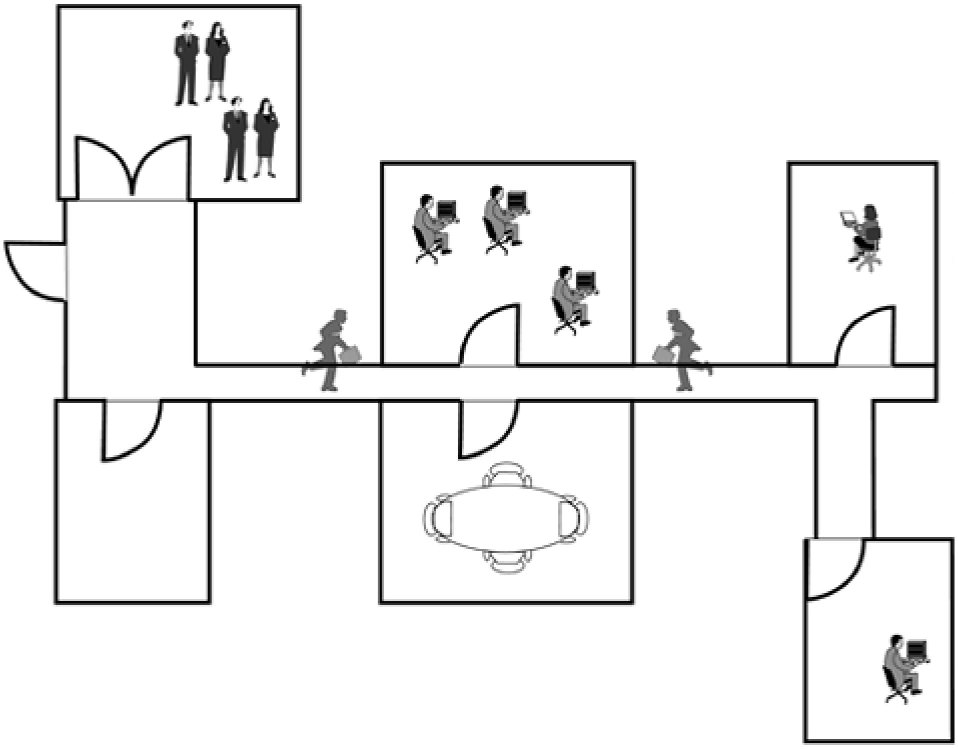
Types of Networks

Three primary types of information networks are in use today:

- Local-area networks (LANs) are found in small geographic areas, such as the floor of an office building.
- Metropolitan-area networks (MANs) are found in medium-sized geographic areas, such one or several city blocks.
- Wide-area networks (WANs) are found in large geographic areas, such as expanses that cross a state or country.

Figure 1-10 illustrates the concept of a LAN covering a small geographic area (in this case, the floor of an office building). For these employees to walk between rooms, they must use one or more of the hallways in the building. In this case, the network of hallways provides the connection between each room, enabling each person to move locally on the floor of this building. You would be hard pressed to find a hallway that stretches across several city blocks (MANs) or several states (WANs).

Figure 1-10. Office Building Floor



The following characteristics differentiate one network from another:

- Topology - The physical or logical geometric arrangement of devices on the network. For example, devices, such as computers, routers, or switches, can be arranged in a ring (Token Ring and Fiber Distributed Data Interface (FDDI)) or in a straight line (Ethernet).
- Protocols - The rules and specifications for communication between two devices, similar to grammar in a spoken or written language. For two people to be able to understand each other, for instance, they must both use not only the same language, but also the same syntax and grammar. Network protocols use these same rules of syntax and grammar to determine the following: how the devices talk with each other; whether the network is a peer-to-peer network, such as for file sharing; whether the network has a client/server architecture, such as used with a corporate database for inventory lookup in a retail store or warehouse.
- Media - The physical media carrying the signal between the two network points (source and destination). Examples of media include twisted-pair wire (shielded or unshielded), coaxial cables, fiber-optic cables connecting network devices, and the air. Some networks, such as wireless LANs (WLANs) and radio use the air as their communication media.

LANs

A local-area network (LAN) is a computer network spanning a small geographic area, such as a single building or floor within a building. One LAN can be connected to other LANs over any distance through media, such as telephone lines or radio waves. A system of LANs connected in this fashion is called a wide-area network (WAN).

There are many different types of LANs, and Ethernet is the most common LAN type used today. Some other common LAN types include Token Ring and FDDI.

Most LANs connect workstations, personal computers, and network printers to each other, often for the purpose of resource sharing. Each individual device on a LAN is called a node. Most LAN workstations have their own central processing unit (CPU) with which they execute programs, such as a spreadsheet or word processor program. LAN workstations are also capable of accessing data and devices anywhere on the same LAN. This means that many users can share devices, such as printers, as well as data, either through direct file sharing, or through another LAN node called a file server. Users can also use the LAN to communicate with each other, by sending e-mail or engaging in chat sessions, such as those provided by instant messenger applications.

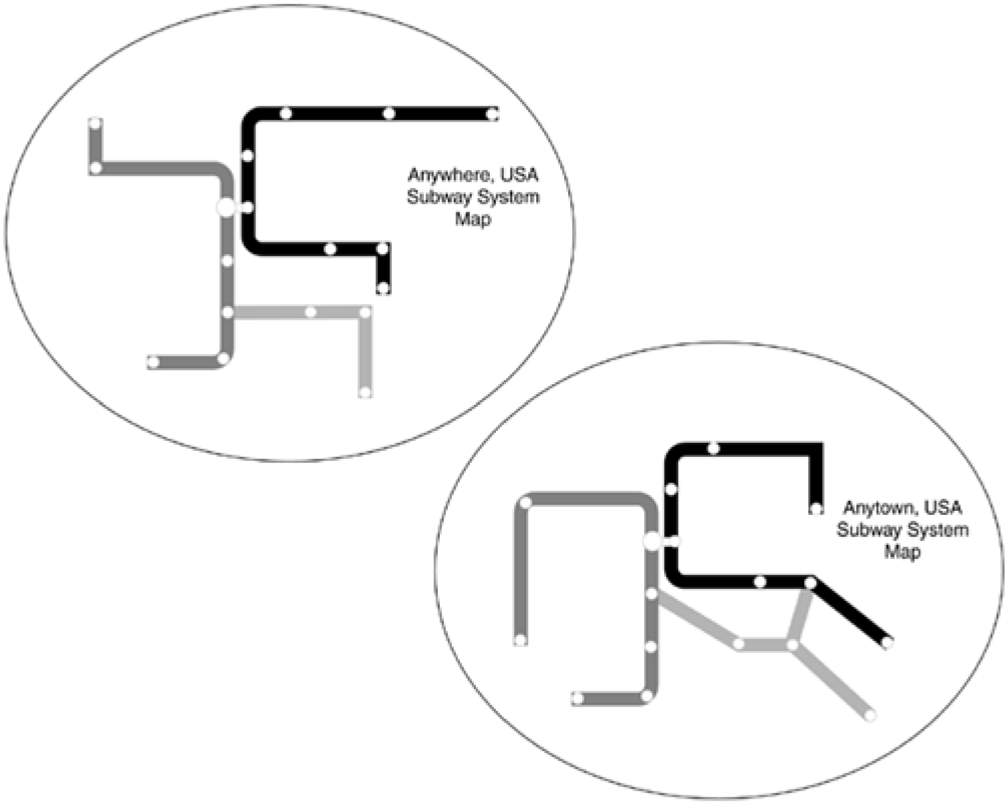
A file server is a central repository for file storage. Instead of several people in an office e-mailing the same file to each other, for example, the file can be kept in a central location and each person can access the file directly to read or write updates. A print server is a computer that manages print requests from multiple users and provides printer status information that is available to end users and network administrators.

MANs

A metropolitan-area network (MAN) is a data network designed for a town or city. A MAN can either be built as service provider and leased among multiple customers or a company can build its own private MAN. In terms of geographic breadth, MANs are larger than LANs, but smaller than WANs. MANs are usually characterized by high-speed connections using fiber-optic cable or other digital media and are often used by companies with several offices located within the same city. A corporation can extend the LAN services in each building across a metropolitan region by deploying a MAN to interconnect each corporate office.

An example of a noncomputer MAN in today's world is a city subway system. The subway routes interconnect different points within a metropolitan area, such as a city, as illustrated in Figure 1-11.

Figure 1-11. Subway System Map for Anywhere, USA



View full size image

WANs

A wide-area network, or WAN, is a computer network that spans a relatively large geographic area, such as an expanse that crosses several states or countries. Computers connected to a WAN are often connected through public networks, such as the telephone system (through a network service provider). Computers can also be connected through leased lines or satellites, also from a network service provider.

An example of a noncomputer WAN in today's world is the routes flown by various airlines between cities. These routes span a broad geographic area. Figure 1-12 shows an airline route map; in this case, the geographic area is North America.

Figure 1-12. Airline Route Map

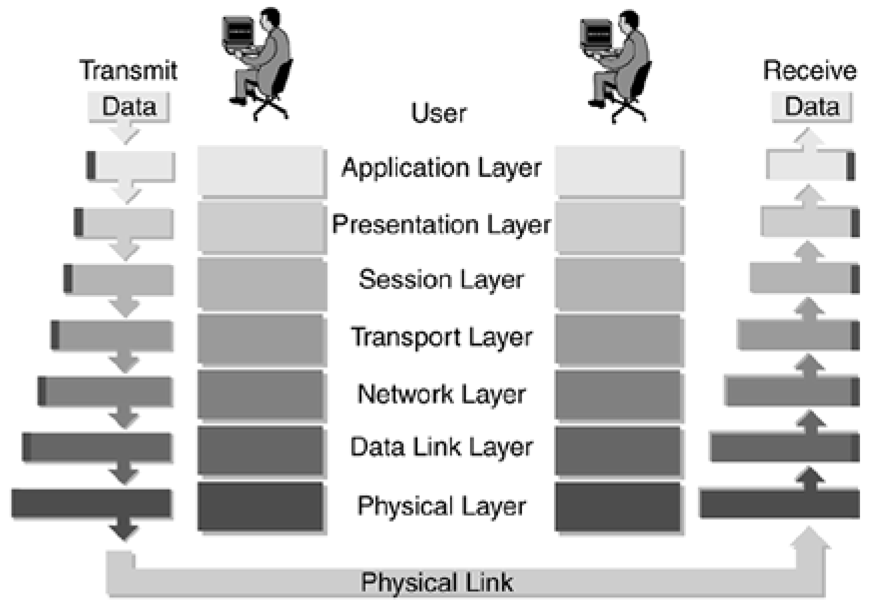
View full size image

Network Models and Standards

OSI Model

This general overview of the Open System Interconnection (OSI) model lays the foundation for the rest of this book, but do not consider it exhaustive. The OSI model defines a networking framework in seven layers. Control of the data passes from one layer to the next, starting at the sending station's application layer, and then working down through the model, to the bottom layer. Control of the data then passes across the physical connection between each station along the path and then back up the model layers to the top layer at the receiving (destination) station. Figure 2-1 shows this process.

Figure 2-1. OSI Model Sending and Receiving



In the networking environment, the OSI is the universal model and is made up of seven layers, each layer providing a service to the layer above it and dependent on the layer below. These seven layers are as follows:

- Layer 7 - Application
- Layer 6 - Presentation
- Layer 5 - Session
- Layer 4 - Transport
- Layer 3 - Network
- Layer 2 - Data link
- Layer 1 - Physical

Layers 1 through 4 are referred to as the lower layers, and Layers 5 through 7 are referred to as the upper layers. Each layer performs a specific function in itself and provides a service to the layer above it. For example, Layer 2 (data link) depends on services provided to it by Layer 1 (physical) and provides services to the layer above it, Layer 3 (network).

Layer 7 - Application Layer

The application layer is the user-interaction layer, enabling the software and end-user processes. Everything at this layer is application specific. For example, a web browser application for surfing the Internet would user this layer. The application layer provides application services for file transfers, e-mail, and other network-based software services, such as your web browser or e-mail software.

Layer 6 - Presentation Layer

The presentation layer provides for data representation to the user, such as a document (.doc) or spreadsheet (.xls). The presentation layer also "translates" the user data into a format that can be carried by the network, such as the segments and packets required at the lower layers. The presentation layer converts your data into a form that the application layer can accept, such as converting a string of data into a recognizable file format, such as .doc (word processing document) or .jpeg (graphics format). The presentation layer formats and encrypts data (when required by the user's application) to be sent across the network.

Layer 5 - Session Layer

The session layer establishes, manages, and terminates virtual communications connections between applications. In other words, the session layer starts and stops communication sessions between network devices. When you place a telephone call, for example, you are establishing a communication session with another person. When you are finished with the call, you hang up the telephone, which terminates the session.

Layer 4 - Transport Layer

The transport layer provides data transfer between end systems and is responsible for end-to-end error recovery and flow control. Flow control ensures complete data transfer and provides transparent checking for data that might have been dropped along the way from sender to receiver. Error recovery retrieves lost data if it is dropped or suffers from errors while in transit from source to destination.

Layer 3 - Network Layer

The network layer provides the routing technologies, creating a forwarding table or a logical path between the source and destination. These logical paths are known as virtual circuits and are considered to be point-to-point network connections. Routing and forwarding are functions of the network layer. Network addressing, error handling, congestion control, and packet sequencing are all functions of the network layer.

Note: Error handling is the response to an error that advises either the user or another process that an error has occurred. Error correction is the action taken to correct the error. Examples of error correction methods include resending the data or the application, or "figuring out" the corrupted data by the use of a checksum (a mathematical operation based on the number of 1s and 0s in the data).

Layer 2 - Data Link Layer

At the data link layer, data packets are placed into frames for subsequent transmission across the network. The data link layer provides the transmission protocol knowledge and management and handles physical layer errors, flow control, and frame synchronization.

The data link layer is divided into two smaller sublayers: the Media Access Control (MAC) layer and the logical link control (LLC) layer. The MAC sublayer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control, and error checking.

Think of the MAC and LLC sublayers as the pilot and copilot of an aircraft. The MAC sublayer prepares the frame for physical transmission, much as the pilot focuses on the physical aspects of flying the aircraft. The LLC sublayer is concerned with the logical aspects of the transmission, not with the physical aspects of the transmission. The LLC layer acts like the copilot, who focuses on navigation, leaving the physical aspects of flying to the pilot.

Layer 1 - Physical Layer

The physical layer carries the bit stream through the network. The bit stream can be carried as an electrical, light, or radio signal. This layer provides the hardware means of sending and receiving data on a carrier, including defining the cables, cards, and physical aspects. Gigabit Ethernet, wireless, dense wavelength-division multiplexing (DWDM), Synchronous Optical Network (SONET), Electronic Industries Alliance/Telecommunications Industry Alliance 232 (EIA/TIA-232; formerly RS-232), and Asynchronous Transfer Mode (ATM) are all protocols with physical layer components.

Table 2-1 outlines the signal type carried by each medium.

Table 2-1. Physical Media Used by Different Signal Types

Medium	Signal Type
Fiber optic	Light
Copper	Electrical
Air	Wireless, radio

Moving Through the OSI Model

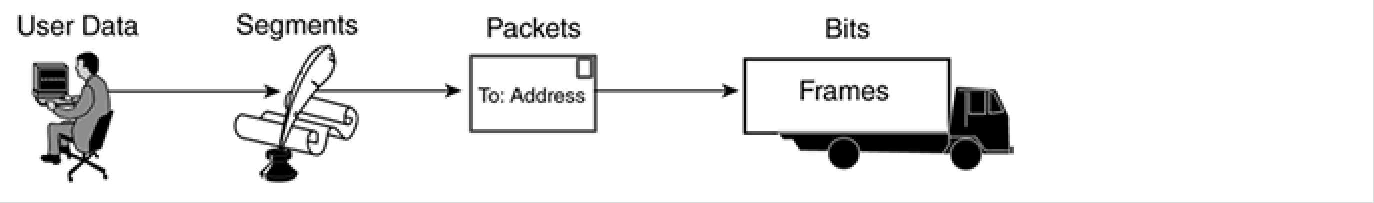
To better understand how network switching works, it is vital to understand how the OSI model works and how data moves through the OSI model. How you move through the OSI model depends on whether you are the sender or the receiver. The sending side wraps, or encapsulates, the data, much as you enclose a letter in an envelope. The receiving side unwraps, or decapsulates, the data, much as the receiver opens an envelope to remove the contents.

Sending, or encapsulating, data requires five steps, as follows:

- Step 1. User data (Layers 5-7 - application, presentation, session)
- Step 2. Segments (Layer 4 - transport)
- Step 3. Packets (Layer 3 - network)
- Step 4. Frames (Layer 2 - data link)
- Step 5. Bits (Layer 1 - physical)

To demonstrate the encapsulation of data, let's look at what happens when you write and send a letter (a real, old-fashioned letter, not e-mail), as illustrated in Figure 2-2.

Figure 2-2. Data Encapsulation



View full size image

As shown in Figure 2-2, data (in this case, old-fashioned mail) is sent (or encapsulated) as follows:

- User data (Layers 5-7) - You write your words using a specific style, such as Roman characters or script, on a piece of paper, in a certain language, such as English.
- Segments (Layer 4) - You fold the paper and place it into an envelope. If your letter is made up of multiple pages, each page, or "segment," is numbered so the letter is reassembled in the correct order by the receiver.
- Packets (Layer 3) - You write the sender's and receiver's postal address on the envelope. Like an envelope, a packet contains user information and identifies the sending and receiving address.
- Frames (Layer 2) - Your letter is put into a mailbag with other letters to be carried to the same destination. The mailbag here is the frame carrying multiple packets. These frames are put onto a mail truck, in which a truck driver carries the envelope to its destination.
- Bits (Layer 1) - The truck is driven across the highways and other roads to reach the receiver.

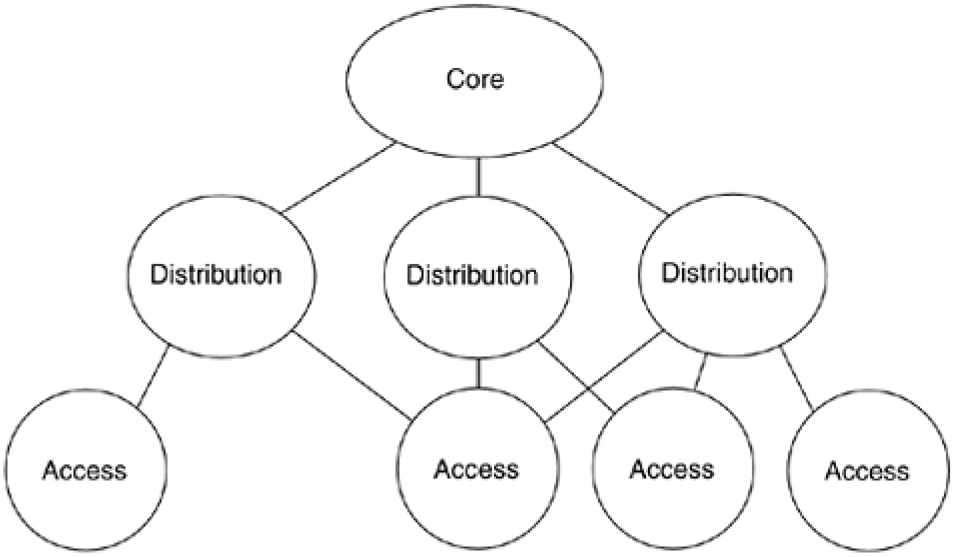
The following steps demonstrate what happens to the data on the receiving end, where it is opened (decapsulated):

1. The mail truck arrives at its destination, carrying the envelope.
2. The receiving station examines the destination address on the envelope and delivers it to that address.
3. Someone at the receiving address opens the envelope and extracts the paper.
4. The paper's recipient then reads the contents, the words and paragraphs, of the letter.

Hierarchical Design Model

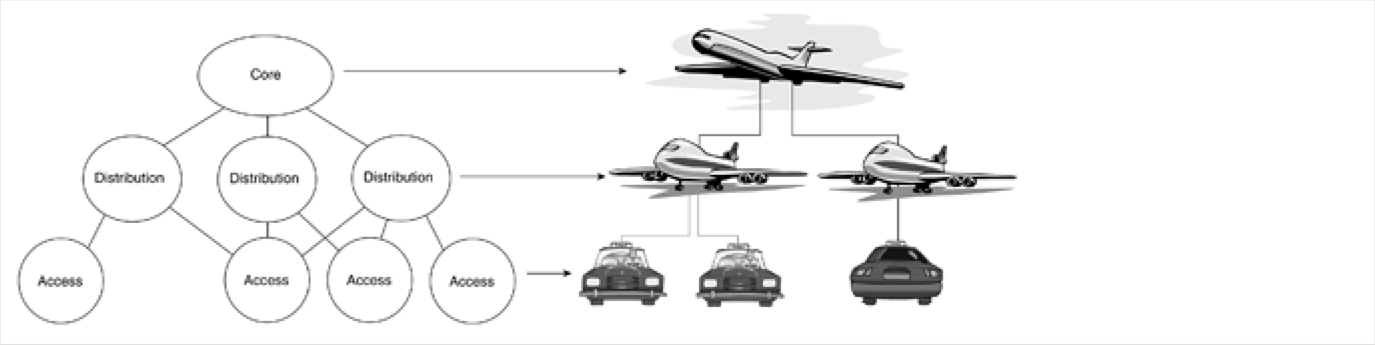
The Cisco Hierarchical Design Model is another network model that is used to design and engineer data communication networks. The Hierarchical Design Model is a three-tiered, or layered, model with a core, distribution, and access layer, as illustrated in Figure 2-3.

Figure 2-3. Three-Tiered Design Model



The Hierarchical Design Model is used by network designers, architects, and engineers when designing and implementing scalable and efficient networks. As stated previously, the three tiers of this model (illustrated in Figure 2-4) are the core, distribution, and access layers. The core layer provides high-speed switching between sites and is considered the backbone of the network. The distribution layer provides policy-based connectivity, such as what type of data can and cannot transit across the network. The access layer enables users to access the network and its resources.

Figure 2-4. Three-Tiered Model



View full size image

Hierarchical design models can also be found in travel. The taxi you take from home to the airport is working at the access layer because the taxi is providing access to the airport resources (in this case, the airplane). At the airport, your ticket determines through which gate you enter. Your ticket provides the routing - that is, it tells you which gate to use to board your airplane.

Network Standards

If the different network standards in place today were in print, they would fill volumes upon volumes of text. These network standards serve specific purposes, as defined by the standard itself. For example, there is a standard for you to communicate across the Internet and a different standard for you to talk across the telephone network

Standards dictate almost everything that surrounds us during the course of a day. The television signal of your TV follows a standard, as does the lid on your "to-go" coffee cup. Some standards, such as the television signal, are regulated by an administering body such as the National Television System Committee (NTSC) or the new High-Definition Television (HDTV) standard developed in part by the Advanced Television System Committee (ATSV), whereas other standards are nonregulated.

These nonregulated standards are known as de facto standards and become standardized over time by their use. For example, no regulating authority is responsible for "to-go" coffee cup lids, but the sizes of cups used are static, meaning that a "to-go" coffee cup from one coffee shop doesn't usually differ from a "to-go" coffee cup from another shop. Hence it is logical that the lids for these cups will be the same, regardless of the manufacturer.

Standards in the network world work the same way. There are regulated standards such as those published by the International Telecommunication Union (ITU), the American National Standards Institute (ANSI), and the Institute of Electrical and Electronics Engineers (IEEE). There are also de facto standards, such as those put forth by network vendors, such as Cisco, and adopted over time by everyone else.

ITU (International Telecommunication Union)

The International Telecommunication Union (ITU) is made up of telecommunication policy makers and regulators, network operators, equipment manufacturers, hardware and software developers, regional standards-making organizations, and financing institutions. The activities, policies, and strategic direction of the ITU are determined and shaped by the industry it serves.

The three sectors of the ITU are Radiocommunication (ITU-R), Telecommunication Standardization (ITU-T), and Telecommunication Development (ITU-D).

- ITU-R draws up the technical characteristics of terrestrial and space-based wireless services and systems, and develops operational procedures. It also undertakes the important technical studies, which serve as a basis for the regulatory decisions made at radio communication conferences.
- ITU-T experts prepare the technical specifications for telecommunication systems, networks, and services, including their operation, performance, and maintenance. Their work also covers the tariff principles and accounting methods used to provide international service.
- ITU-D experts focus their work on the preparation and development of recommendations, opinions, guidelines, handbooks, manuals and reports. These documents provide decision makers with "best business practices" relating to a host of issues ranging from development strategies and policies to network management.

Each of the three ITU sectors works through conferences and meetings at which members negotiate the agreements that serve as the basis for the operation of global telecommunication services. The activities of the ITU cover all aspects of telecommunication: setting standards that facilitate seamless interworking of equipment and systems on a global basis; adopting operational procedures for the vast and growing array of wireless services; and designing programs to improve telecommunication infrastructure in the developing world.

ANSI (American National Standards Institute)

American National Standards Institute (ANSI) serves as administrator and coordinator of the United States private-sector voluntary standardization system. ANSI was founded in 1918 by five engineering societies and three governmental agencies, and is a private, nonprofit membership organization. ANSI ensures each foot-long ruler is accurate in its dimensions, for instance, essentially using a ruler to measure a ruler. ANSI ensures that each inch on the ruler is in fact 1 inch, and that the foot-long ruler is in fact made up of 12 of these inches.

ANSI, like the ITU, regulates telecommunications standards; unlike the ITU, however, ANSI regulates standards in North America, whereas the ITU regulates standards in Europe. For example, ANSI regulates the T1 telecommunications standard, whereas the ITU regulates the E1 telecommunications standard in Europe.

IEEE 802 Group

The Institute of Electrical and Electronics Engineers (IEEE, pronounced "eye-triple-E") is a nonprofit, technical professional association in 150 countries. The IEEE is a leading authority in technical areas ranging from computer engineering, to biomedical technology, to telecommunications, to electric power, to aerospace and consumer electronics. The IEEE produces 30 percent of the world's published literature in electrical engineering, computers, and control technology and has nearly 900 active standards with 700 under development.

Some of the best-known IEEE standards are as follows:

- IEEE 802.1 (LAN/MAN)
- IEEE 802.3 (Ethernet)
- IEEE 802.5 (Token Ring)
- IEEE 802.11 (Wireless LAN)

IEEE 802.1 LAN/MAN Standards

The IEEE 802.1 group defined internetworking standards, with IEEE 802.1d and IEEE 802.1q used in the local-area networking environment. The standards are as follows:

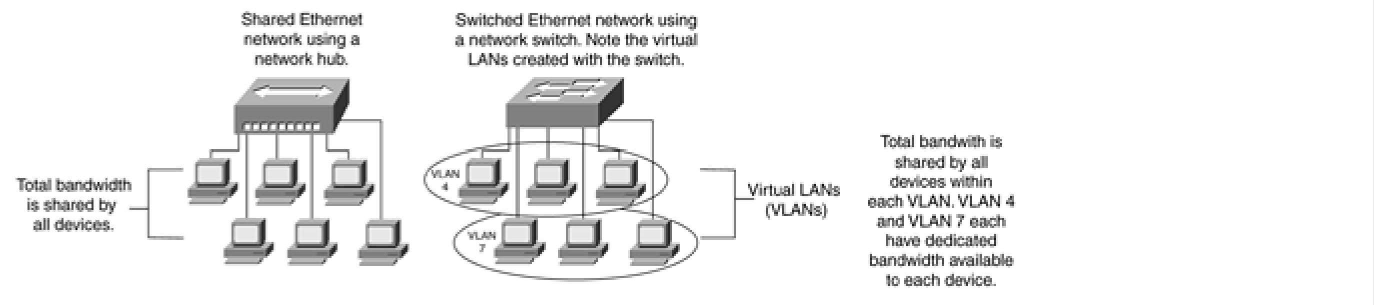
- IEEE 802.1d - Spanning Tree Protocol (STP) - STP is a link-management protocol that is part of the IEEE 802.1 standard for Media Access Control bridges and is used for Layer 2 redundancy. Using the spanning-tree algorithm, STP provides redundant paths through the LAN while preventing loops in the LAN that are created by multiple active paths between stations. These multiple paths, or loops, occur when there are alternative routes between hosts. To establish path redundancy, STP creates a tree that spans all the switches in an extended network, forcing redundant paths into a standby, or blocked, state. STP allows for one active path at a time between any two network devices, preventing loops, but establishing the redundant links as a backup (in case the primary link fails). If a change occurs in the LAN, such as a network segment becoming unreachable, the spanning-tree algorithm reconfigures the tree topology and reestablishes the link by activating the standby path. Without STP in place, both primary and redundant connections might be simultaneously live, resulting in an endless loop of traffic on the LAN.
- IEEE 802.1q - virtual LANs (VLANs) - A VLAN is a network of computers that behaves as if the computers are connected to the same physical network segment, even though these computers might be physically located on different segments of a LAN. VLANs are configured in software and are not limited by physical location or to specific switch ports. This makes VLANS flexible to use within a network. One of the advantages of VLANs is that when a computer is physically moved to another location, it can stay on the same VLAN without any end-device or protocol reconfiguration.

IEEE 802.3 Ethernet Standards

Several Ethernet standards are used in today's network environment. Some of these standards dictate the bandwidth and operation of the Ethernet LAN, such as Ethernet and Fast Ethernet, whereas other standards dictate how these Ethernet networks function, such as the STP.

Ethernet is a half-duplex shared-media LAN in which each station on the segment uses part of the total bandwidth. The total LAN bandwidth for Ethernet is 10 megabits per second (Mbps - Ethernet) or 100 Mbps (Fast Ethernet). Ethernet and Fast Ethernet can operate in either half-duplex or full-duplex mode; half-duplex Ethernet shares the LAN media, whereas full-duplex mode has separate LAN media dedicated to the sending and receiving side of the network interface card (NIC). The 1000 Mbps (Gigabit Ethernet) is not a shared-media LAN implementation because Gigabit Ethernet operates in full-duplex mode only. Hubs enable shared-media LANs, and switches enable dedicated-media LANs. With switched Ethernet, each sender and receiver pair has the full bandwidth available for use, as illustrated in Figure 2-5.

Figure 2-5. Switched and Shared Ethernet Networks


Shared Ethernet network using a network hub.
Switched Ethernet network using a network switch. Note the virtual LANs created with the switch.
Total bandwidth is shared by all devices.
VLAN 4
VLAN 7
Virtual LANs (VLANs)
Total bandwith is shared by all devices within each VLAN. VLAN 4 and VLAN 7 each have dedicated bandwidth available to each device.

View full size image

The IEEE 802.3 standards define how the Ethernet standard is used in the networking environment. These 802.3 standards are as follows:

- IEEE 802.3 (Ethernet) - 10-Mbps Ethernet specification developed by Xerox, served as the basis for the IEEE 802.3 standard. This specification describes the use of carrier sense multiple access collision detect (CSMA/CD) in handling the simultaneous demands for network access. Often used in LAN environments.
- IEEE 802.3u (Fast Ethernet) - 100-Mbps Ethernet specification working at 10 times the speed of 10-Mbps Ethernet. Often used in LAN environments.
- IEEE 802.3z (Gigabit Ethernet) - 1000-Mbps/1-Gbps Ethernet specification that transfers data at 1 gigabit per second (1000 Mbps). Often used in large LAN environments at the core layer.
- IEEE 802.3ae (10Gigabit Ethernet) - 10,000-Mbps/10-Gbps Ethernet specification that transfers data at 10 gigabits per second (10,000 Mbps). Often used in metropolitan-area networks (MANs).

Note: CSMA/CD is a standard enabling Ethernet hosts to detect a collision. In a half-duplex Ethernet environment, collisions occur when two nodes begin sending traffic at the same time. Collisions do not occur in full-duplex Ethernet environments. After detecting a collision, the host waits a random amount of time and then tries retransmitting the message. If the sending host detects a collision again when trying to send the same frame, the host waits an exponentially increasing amount of time after each transmission attempt before resending.

IEEE 802.5 Token Ring Standards

With Ethernet, any host on the network can send data at any time, as long as no one else is on the line. In contrast, the Token Ring works by passing a token around the network, almost like a relay-race runner passing the baton to the next runner. When a host has possession of this token, it has the right to send data across the network, just as the relay runner can run only when in possession of the baton. If a host has nothing to send, it passes the token to the next host down the line in the network.

IEEE 802.5 is a related specification and compatible with the Token Ring standard developed by IBM. Token Ring refers to both IBM Token Ring and IEEE 802.5 network implementations. IBM originally developed the Token Ring network in the 1970s; however, IBM gave up on Token Ring in favor of Ethernet several years ago.

Token Ring is a LAN in which all the hosts are arranged in a logical circle. A special frame, called the token, travels around the circle. To send a message, a host catches the token, attaches its data, and then lets it continue to travel around the network. Token Ring is not found in many LANs nowadays because of its slow speed as compared to Ethernet LANs.

IEEE 802.11 Wireless LAN (WLAN) Standards

The IEEE 802.11 standard refers to a family of specifications developed for wireless LAN technology. IEEE 802.11 specifies an over-the-air interface between a wireless client and a base station, such as a wireless laptop and a wireless base unit or between two wireless clients, such as between two wireless laptops.

Figure 2-6 illustrates a wireless LAN between a laptop and a base unit, with the base unit connected to the Internet, either in the home or the office. The base unit can enable multiple users to share the same Internet connection as long as each user has a wireless-LAN-capable device. The benefit here is straightforward: no wires to get tangled or cables to be hidden. Wireless LANs raise other issues - the most notable is the broadcast of your data into the open air. Wireless LANs should not be implemented without some sort of encryption to protect your data from being stolen out of the air.

Figure 2-6. Wireless LAN Between a Laptop and a Base Unit

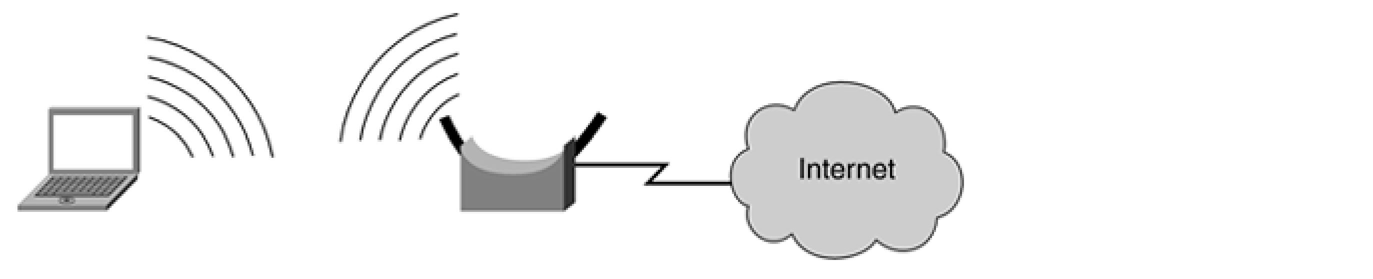


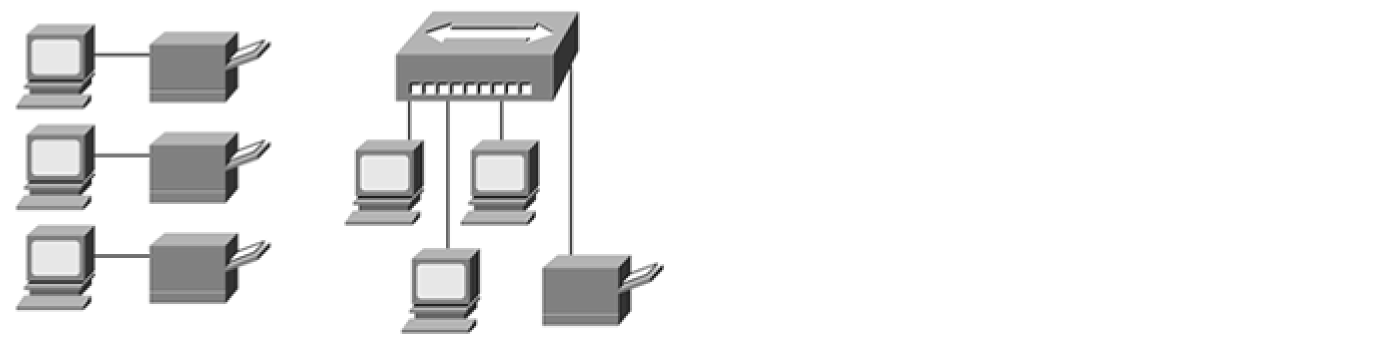
Figure 2-7 illustrates a wireless LAN that might also be found in a home or office. This configuration demonstrates the same sharing concept of the previous example, but this time users are sharing a wireless printer. The benefit here is the same: no wires.

Figure 2-7. Wireless LAN Between a Laptop and a Printer

Local-Area Networking Introduction

Local-area networks (LANs) send and receive data at rates much faster than can be transmitted over a telephone line; but the distances are limited, often to a few hundred feet maximum without using costly, long-range technologies, such as Long Reach Ethernet (LRE) or wave-division multiplexing (WDM). Because of distance limitations, LANs are found in small areas such as a floor in your office building or a home network. LANs are used to connect personal computers (PCs), network workstations, routers to the Internet, and other network devices, such as network-capable printers, as illustrated in Figure 3-1.

Figure 3-1. Desktop/Printer Implementation Without a LAN and with a LAN, Respectively



Users connected via a LAN can chat and share files, Internet access, and printer access. The alternative to a LAN is for each user to have his own printer and Internet access.

Three characteristics differentiate one LAN from another:

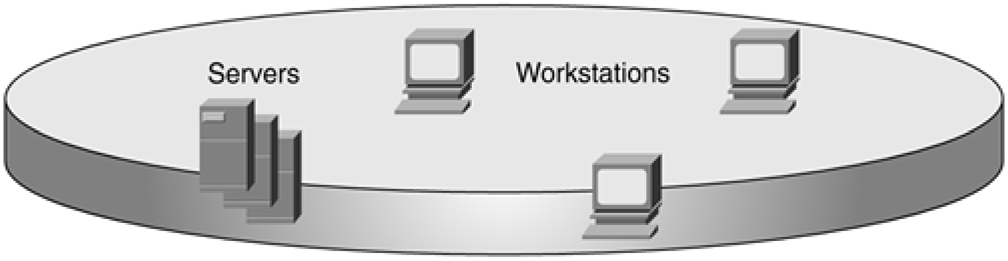
- LANs can be configured in different topologies. Topology is the geometric arrangement of devices on the network. For example, devices can be arranged in a continuous ring, where each computer is a link in the chain, or in a star, where each computer is connected to the same central device.
- LANs follow different protocols, which are the rules and specifications for sending and receiving data.
- LANs are connected through different media. For example, with LANs, the media through which a signal is transmitted among devices is twisted-pair wire, coaxial cable, fiber-optic cable, or wireless.

Several small LANs can be connected together to create a single larger LAN within a building. If your LANs are in offices across the country, these LANs use connections provided by a network service provider to create a wide-area network (WAN).

Comparing LANs to WANs

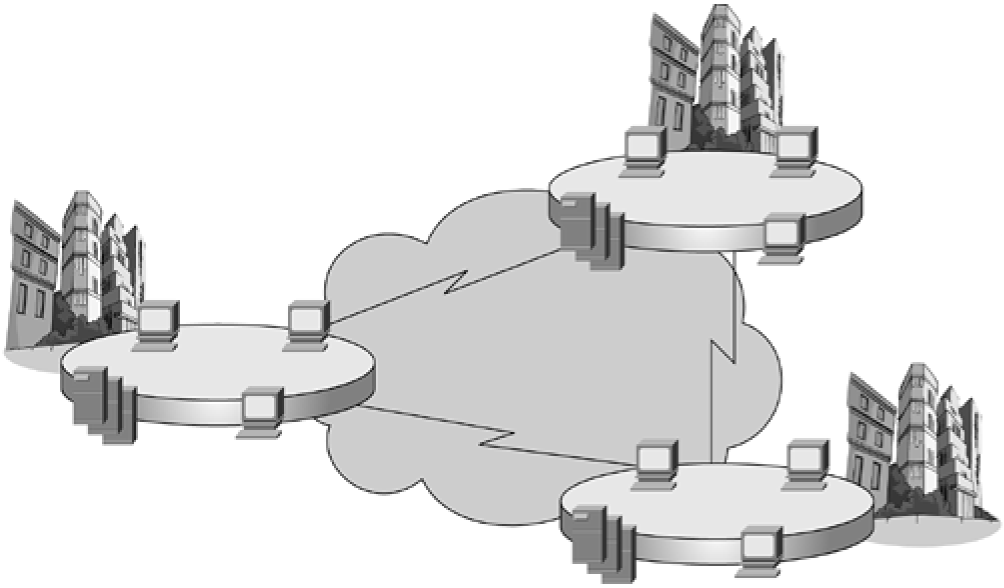
As previously stated, a LAN is just what the name implies - a network that is confined to a local geographic area, such as a single office building, a small office in a commercial building, or even a network in your own home. As shown in Figure 3-2, LANs enable you to share resources, such as Internet access or laser printing, with other users on the same network.

Figure 3-2. Local-Area Network (LAN)



In contrast, WANs cover a much broader geographic range than LANs, as shown in Figure 3-3. WANs are often used to connect LANs across a public network, such as the Public Switched Telephone Network (PSTN). LANs can also be connected through leased lines or satellites to create a WAN.

Figure 3-3. Wide-Area Network (WAN)



Not all WANs require a public network. A WAN can use privately owned connections, such as "dark fiber," to create a wholly owned and dedicated network.

As the name implies, WANs are networks that cover a broad geographic area, such as multiple cities, states, or even countries. The largest WAN in existence is the Internet; it spans the globe.

OSI Model (As It Applies to LANs and the Interrelation Between Layers)

The upper layers of the Open System Interconnection (OSI) model, where user data is found, need the lower layers, like a train needs tracks to get from point A to B. It is these lower layers - physical, data link, and network - that provide the "railroad tracks" for the user data. They allow the data to ride across the network, such as when sending an e-mail or surfing the Internet.

Layer 1 - Physical Layer

The physical layer moves the bit stream (signal) from one point to another across a carrier, such as a network cable, originating from the transmitter (device sending the signal) and terminating at the receiver (device receiving the signal). For example, when you have a telephone conversation with someone, your mouthpiece is the transmitter and the other person's earpiece is the receiver. The signal is either an electrical impulse when carried over copper, light when carried over fiber-optic cabling, or a radio signal when carried through the air.

The physical layer is made up of the following:

- Signal - The data being carried in the form of bits (1s and 0s), which are converted into electrical impulses (sine wave), radio signals, or pulses of light
- Hardware - A transmitter, receiver, repeater, regenerator, or a hub
- Media - Coaxial (coax), fiber-optic, or copper (shielded and unshielded twisted-pair) cabling; and air for wireless signals

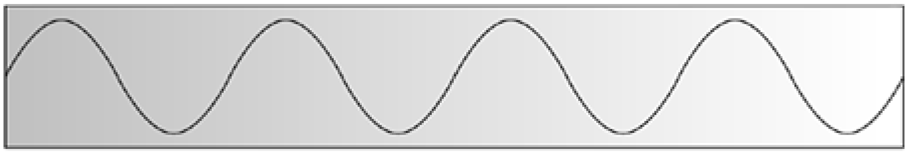
In a LAN environment, the physical layer components are the network interface card (NIC) in your computer, the cable connecting your computer to the network, and the signal being sent by your NIC across the cable.

Signal

The signal, with respect to cabling, is the information being sent across the medium in an electronic or optical (light) fashion.

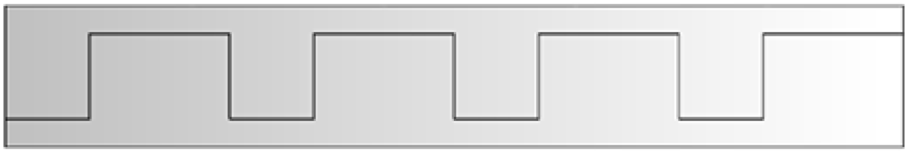
There are two types of electronic signals: analog and digital. Analog signals are represented as continuous waves, as illustrated in Figure 3-4.

Figure 3-4. Analog Signal Wave



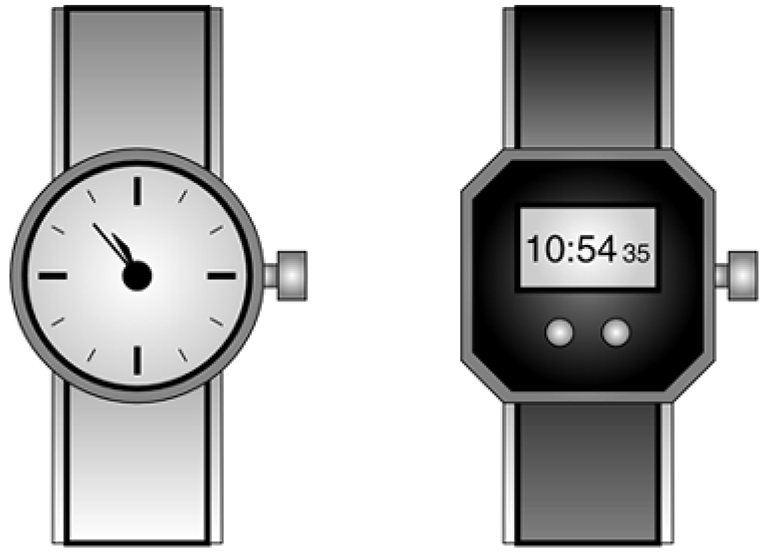
In contrast to the continuous wave of an analog signal, digital signals consist of values measured at discrete intervals, or square waves, as illustrated in Figure 3-5.

Figure 3-5. Digital Signal Wave



The difference between analog and digital can be best demonstrated by looking at both an analog and a digital watch, as illustrated in Figure 3-6.

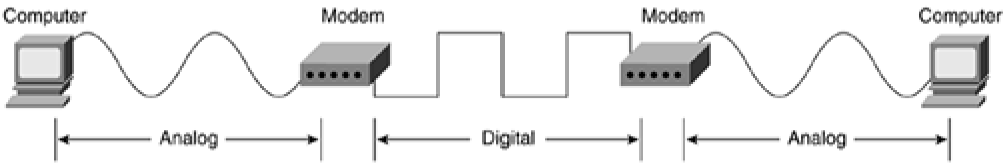
Figure 3-6. Analog and Digital Watches



Digital watches display one value (10:54) and then the next (10:55) without showing all the intermediate values between the two. Digital watches, therefore, display only a finite number of times of the day, such as every minute. In contrast, the hands of analog watches move continuously around the clock face. As the minute hand goes around, it not only touches the numbers 1 through 12, but also the infinite number of points in between, indicating every possible time of day.

We experience the world in an analog fashion; vision is analog because we perceive infinitely smooth gradations of shapes and colors. Speech is analog because there are infinite variances in tone and pitch that make up the sounds we hear. Most analog events, however, can be simulated digitally (the photographs in newspapers, for instance). Although these photos are made up of arrays of discrete black or white dots (digital form), when we look at the photographs we perceive lines and shading that appear to flow into each other to form images. In this way, we perceive a digital image as an analog picture. Although digital representations are approximations of analog events, they are useful because they are relatively easy to store and manipulate electronically. As shown in Figure 3-7, the idea here is that analog is free flowing, whereas digital is exact.

Figure 3-7. Analog-to-Digital Conversion



View full size image

This same principle of digital information being presented as analog is the principle behind compact discs (CDs). The music exists in an analog form as waves in the air, but these sounds are then translated into a digital form that is encoded onto the disc as 1s and 0s. When you play a compact disc, the CD player reads this digital data, translating the 1s and 0s back into a form of music (audio vibrations) that we hear from our stereo giving the perception of the original analog music.

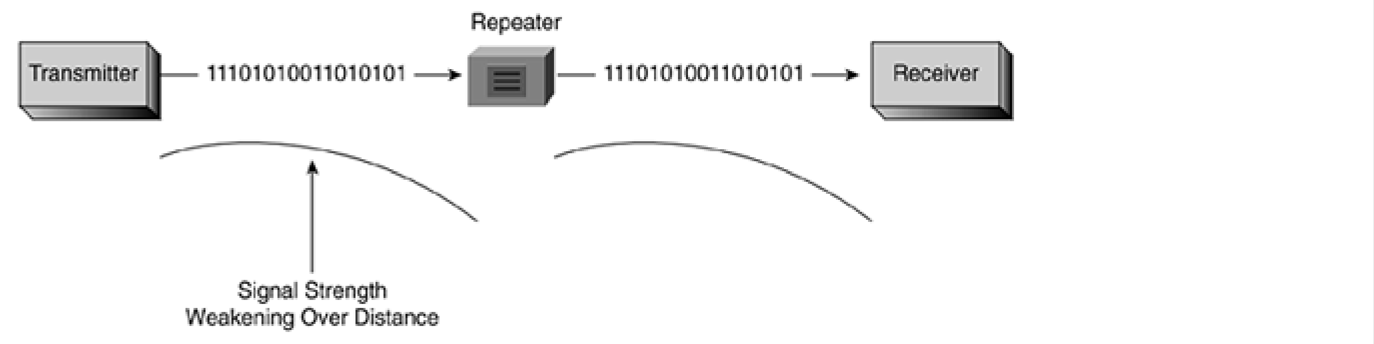
The term bit (short for binary digit) was first used in 1946 by John Tukey (1915 - 2000), a leading statistician and adviser to five U.S. presidents. (If you win money in a trivia contest for knowing this, please contact me and we can split the winnings.)

To send and receive these signals across a medium, we need network hardware.

Hardware

A transmitter is the device sending the signal, a receiver is the device receiving the signal, and a repeater is a network device used to copy or boost a signal on the path between the transmitter and receiver. Repeaters are used in transmission systems to regenerate analog or digital signals distorted by transmission loss. Analog repeaters amplify the signal, whereas digital repeaters reconstruct the signal to its near-original quality, as shown in Figure 3-8. Analog and digital repeaters amplify any noise on the line as well as the signal. Regenerators amplify the signal but not the noise. However, regenerators are often more costly to implement than repeaters. Repeaters and regenerators can be used for electronic, optical, and wireless signals, and are used extensively in long-distance transmission. Repeaters are used to tie two LANs of the same type together, such as two Ethernet LANs.

Figure 3-8. Repeater



View full size image

Hubs are often used to connect small LAN segments where the number of devices generally is 24 or fewer. Hubs are multiport repeaters, and when a frame arrives on one port, it is repeated to the other ports so that all segments of the LAN can see all frames, as illustrated in Figure 3-9.

Figure 3-9. Hub

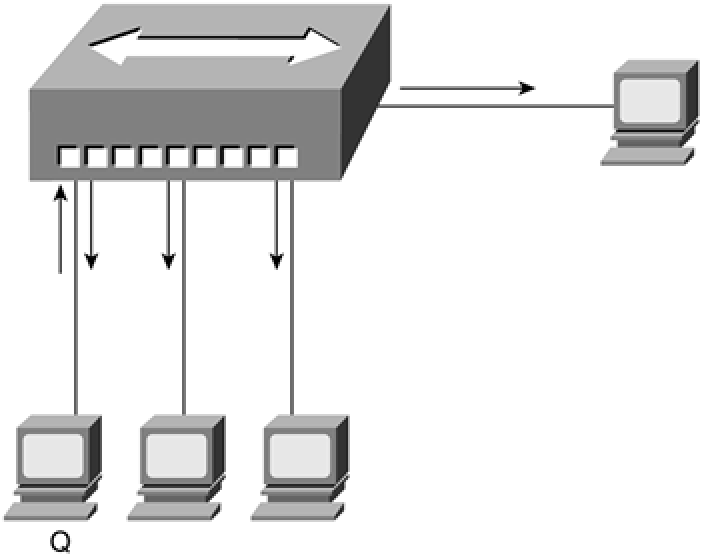


Figure 3-9 shows Host Q sending traffic, in the form of frames, out to the network via a port on the hub. These frames are received by the hosts connected to the same hub, including the host that sent the traffic to begin with, Host Q. Host Q, knowing what it sent, ignores what comes back. The other hosts, however, must read each frame to determine whether they are the intended recipients. If it helps you to understand the process shown in Figure 3-9, you can think of it as being similar to mail arriving for everyone in your office in separate envelopes. Each person receiving an envelope reads the name and address to determine whether the mail is in fact for him. To return to the electronic example - if you are in a small office, with a few people, this is not so bad; in a larger office, however, the process becomes cumbersome because it slows the network down with all the additional traffic.

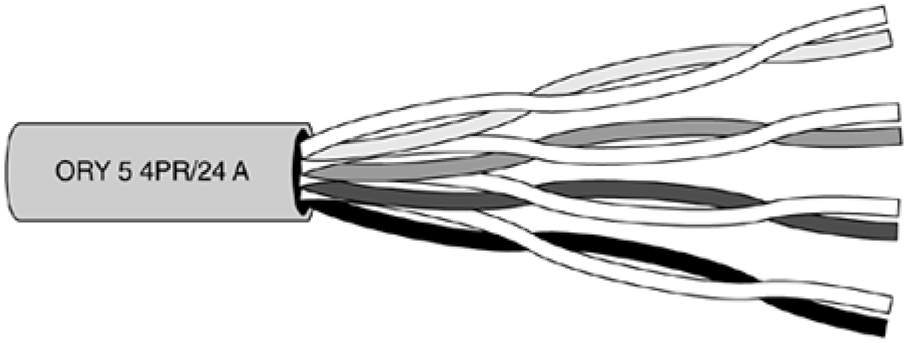
Each host connects to a network device, be it a hub, bridge, or switch, via some sort of medium, as discussed in the next section.

Media

The network medium provides the physical connection between the sender and the receiver. Air is the medium used for wireless communications, and cabling is the medium used in wireline (nonwireless) communications. The three types of network cabling in use today are as follows:

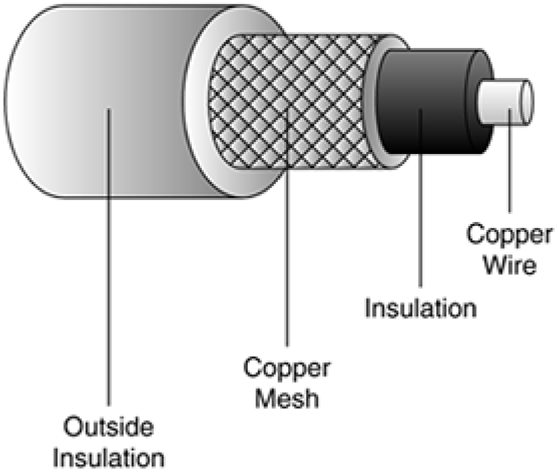
- Twisted-pair cable, which is illustrated in Figure 3-10, comes in two cabling options - unshielded twisted-pair (UTP) and shielded twisted-pair (STP).

  Figure 3-10. Twisted-Pair Cable



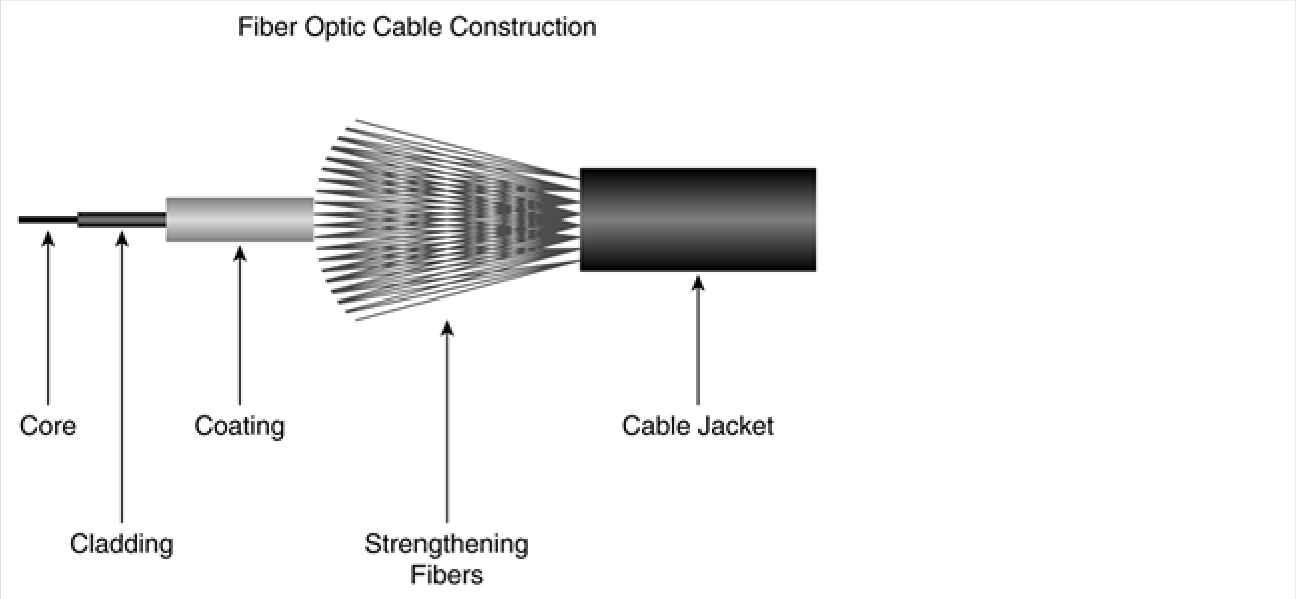
  - UTP is a popular type of cable made up of two unshielded wires twisted around each other. Due to its low cost, UTP cabling is used for LAN and telephone connections. UTP cabling does not provide for high bandwidth or good protection from electromagnetic interference (EMI) such as coaxial or fiber-optic cabling provides. EMI is an electrical disturbance caused natural phenomena (such as lightning), low-frequency waves from electromechanical devices, such as disk drives and printers, or high-frequency waves (radio frequency interference, RFI) from chips and other electronic devices, such as central processing units (CPUs).
  - STP is a type of copper telephone wiring in which each of the two copper wires is twisted together and coated with an insulating coating functioning as a ground for the wires. The extra covering in STP wiring protects the transmission line from EMI leaking into or out of the cable, resulting in signal degradation or loss.
- Coaxial cable, illustrated in Figure 3-11, is a type of wire carrying electrical impulses that consists of a center wire surrounded by insulation and then a grounded shield of braided wire. The shield minimizes EMI and RFI and is the primary cabling type used in the cable television (CATV) industry.

Figure 3-11. Coaxial Cable



- Fiber-optic cable is a type of cable using glass or plastic threads (fibers) to transmit data. As illustrated in Figure 3-12, fiber-optic cable consists of a bundle of glass threads, each of which transmits messages via light waves. This glass is encased in cladding and coating, reinforced by strengthening fibers and further wrapped within a cable jacket.

Figure 3-12. Fiber-Optic Cable



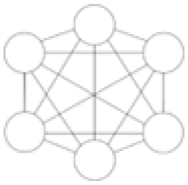
Layer 2 - Data Link

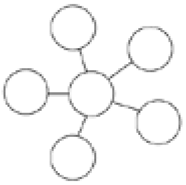
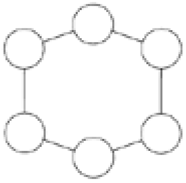
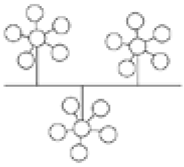
So far, this chapter has discussed the types of signal and media that are found at Layer 1 of the OSI model, but you might be asking yourself, "What are these signals carrying?" The signals are carrying user data in the form of frames. Frames are found at Layer 2 and move data around the network. It is the network topology that determines which devices these frames can be exchanged among.

Have you ever bought a "one size fits all" hat that you couldn't squeeze onto your head? The arrangement, or topology, of a network is much the same; there is no "one size fits all." Each topology serves its own purpose, and it is this purpose that determines what size fits. For example, let's revisit the railroad from Chapter 2, "Networking Models and Standards," for a moment. If all the cities needed to be directly connected with one another, a full mesh topology might be used because a direct path between each city would be available. A star topology might also be used in which each city would directly connect to a central place where the trains would switch tracks.

This same connectivity concept applies to data networks. If hosts on the network need to communicate directly with each other, a full-mesh topology is the answer. (For a description of full-mesh topology, see Table 3-1.) However, this is not often the case; instead, it is more common to see each host communicate through a central point, as in a star topology.

Table 3-1. LAN and WAN Topologies

Topology	Description	Figure	When to Use
Full mesh	Devices are connected with many redundant interconnections between network nodes. In a true mesh topology, every node has a connection to every other node in the network.		Hosts need to talk directly with each other. This topology might be used in a peer-to-peer environment where frequent file sharing is required. The challenge here is the number of connections each host has to maintain. A formula used to determine the number of links required in a full-mesh network: (n * (n - 1))/2 or $(n^{2} - n)/2$ n is number of nodes. In a WAN environment, a full-mesh topology might be used in virtual private network (VPN) environments where it is easy to configure multiple sites connected to each other.

Star	All devices are connected to a central hub. Nodes communicate across the network by passing data through the hub.		This is a common LAN topology. In a star topology, all LAN devices connect to a centralized point, such as a hub or a switch. This central point enables each host to talk to the other hosts but not in the direct fashion afforded in the full-mesh topology. The advantage of the star over the full-mesh is that each host has one connection to maintain, not several. One drawback to this topology is that the central point is a single point of failure; if this point fails, all connected devices are also down. A formula used to determine the number of links required in a star network: n - 1, where n is the number of nodes. In a WAN environment, a star topology might be used to provide connectivity to multiple remote locations, such as remote offices in a corporate network.
Ring	All devices are connected to one another in the shape of a closed loop, so that each device is connected directly to two other devices, one on either side of it.		The ring topology is often used when there is a redundancy requirement. Therefore, if a network segment fails, each network device can continue to communicate with the others around the ring. A ring topology might be used to provide metropolitanarea network (MAN) connectivity, possibly using WDM.
Tree	A hybrid topology. Groups of star-configured networks are connected to a linear bus backbone.		The tree topology is used when a hierarchical network is desired to group users together, such as by geographic location or by function, such as accounting or sales. This topology is often seen in WAN environments.

Remember the OSI model? We're never very far from it during any network discussion, and topology discussions are no different. Each layer of the OSI model could have its own topology. For example, each network device could be physically connected in a star topology to a central device but logically work as a ring topology. This type of Token Ring implementation is illustrated in Figure 3-13 and Figure 3-14.

Figure 3-13. Token Ring Physical Topology

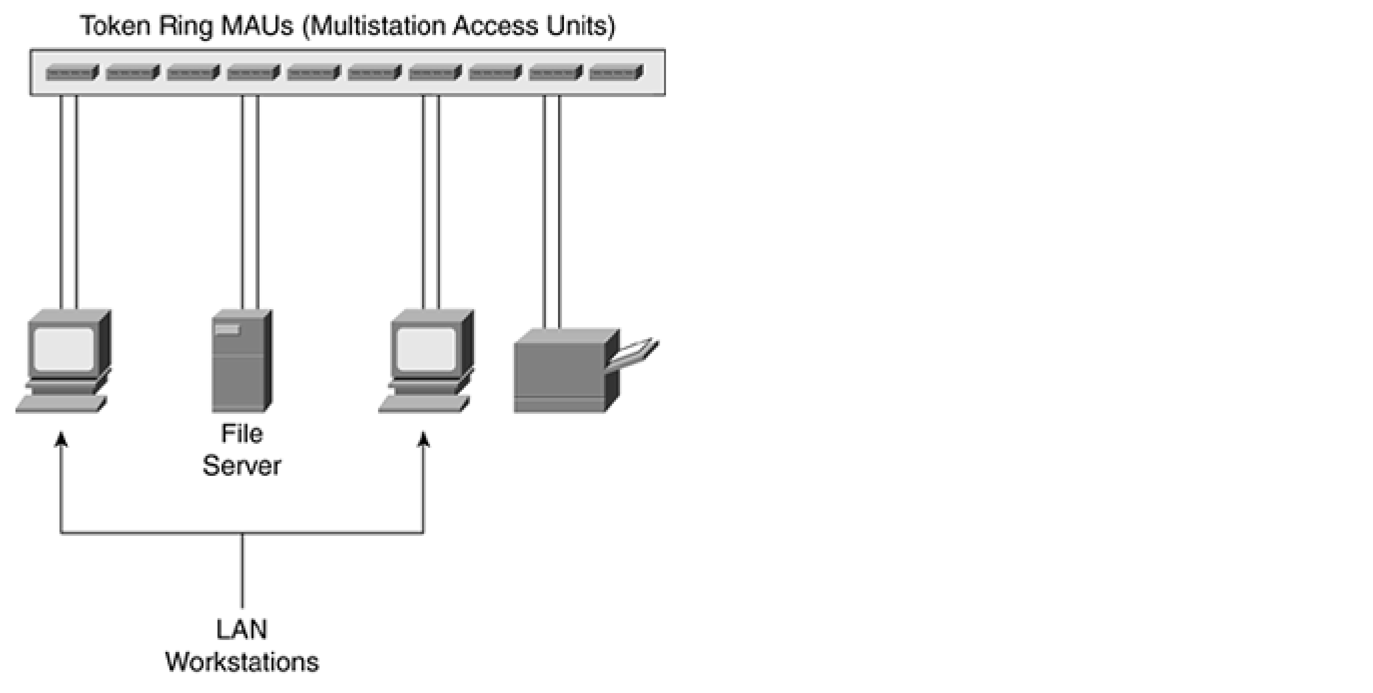
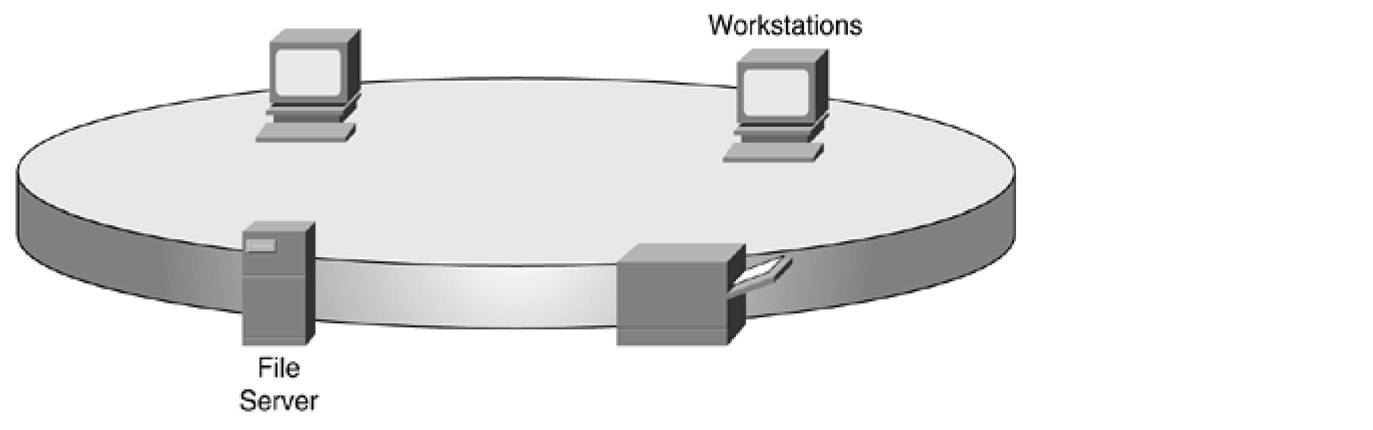


Figure 3-14. Token Ring Logical Topology



Frames

Recall the discussion of frames from Chapter 1, "Networking Basics." Frames carry data across the network and are made up of three parts: the header, the payload itself, and the trailer. It is these frames that carry user data (packets) just as railroad cars carry passengers. Whereas railroad passengers have tickets that specify their destinations, data-link frames have destination addresses specifying where the frame should go. The following table outlines the three components of a frame and their respective functions.

Table 3-2. Frame Components and Functions

Frame Component	Function
Header	Signifies the start of the frame and carries Layer 2 source and destination address information
Payload	Carries data from Layer 3, such as packets from the network layer containing user data
Trailer	Signifies the end of the frame and carries error-detection information in the form of a cyclic redundancy check (CRC)

The three frame components - header, payload, and trailer - combine in making up a complete frame, as was illustrated in Figure 1-6.

Much as a train consists of the engine, passenger/cargo car, and caboose, the frame is made up of a header, payload, and trailer. Whereas the train engine determines which track, or path, the train takes, the frame header determines which path through the network the frame follows. The data (payload) carries the information just as the passengers are carried by the train. The trailer identifies the end of the frame, just as the caboose identifies the end of the train.

Just as the railroad train moves around the country, so too do frames move around the network across the tracks. These tracks are often interconnected with bridges, connecting track segments to form longer rail lines; and railroad switches provide a way for each train to change tracks, or direction. Network bridges and switches work in much the same fashion as the bridges and switches in the railroad and are discussed in more detail in the next section.

Hardware

As mentioned earlier in this chapter, repeaters work at Layer 1 (physical) by repeating the signal received from the transmitting side out to the receiver and vice versa. This type of repeater has two ports - one for each direction.

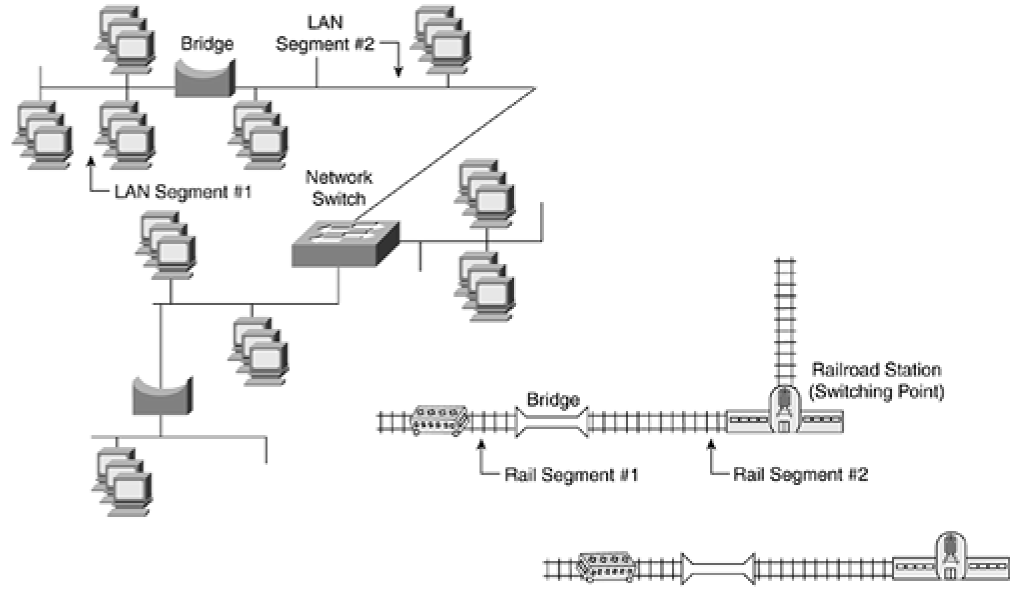
If multiple devices need the benefits of a repeater, however, a hub is used because a hub is a multiport repeater. Recall that with a hub, a signal received on one port is repeated out all ports. Much as a hub is a multiport repeater, a bridge is a multiport hub. Bridges connect two LANs or two segments of the same LAN using the same protocol, such as Ethernet. Bridges learn from experience and build and maintain address tables of the nodes on the network, called Media Access Control (MAC) tables. By monitoring the LAN, the bridge learns which hosts belong to which segment and builds a table using the source MAC address of the frames, as they come in to the bridge.

Bridges work at the data link layer (OSI Layer 2) and are protocol independent. Bridges with more than two ports (multiport bridges) perform switching functions. Switches also work at the data link layer and, like bridges, are protocol independent.

A bridge is considered a multiport hub, whereas a switch is considered to be a multiport bridge with multiple network segments that might, or might not, communicate with each other. Switches also build tables based on the MAC address received on each switch port and forward frames based on these tables.

Figure 3-15 illustrates the use of bridges and switches in a data network and in a railroad network.

Figure 3-15. Network Bridges and Switches



View full size image

In a railroad network, bridges connect separate track segments to create a single "network" of tracks from the smaller track segments. Sometimes these trains change tracks at a railroad switchyard or station, with the passengers still on board. Other times the trains go back and forth between stations with the passengers switching between trains. If the passengers are not at their intended destination and need to continue their journey, they do not stay on the same train and try to convince the engineer to keep going. They change trains at the train station.

The train stations provide a switching point for the passengers riding these trains and sometimes the trains themselves. If a passenger needs to ride several trains to get from the originating (starting) point to the terminating (ending) point, the passenger switches trains at the railroad station. How does the passenger know which train to board at the railroad station? The answer is found in the train ticket, which states the originating and terminating points (start and destination).

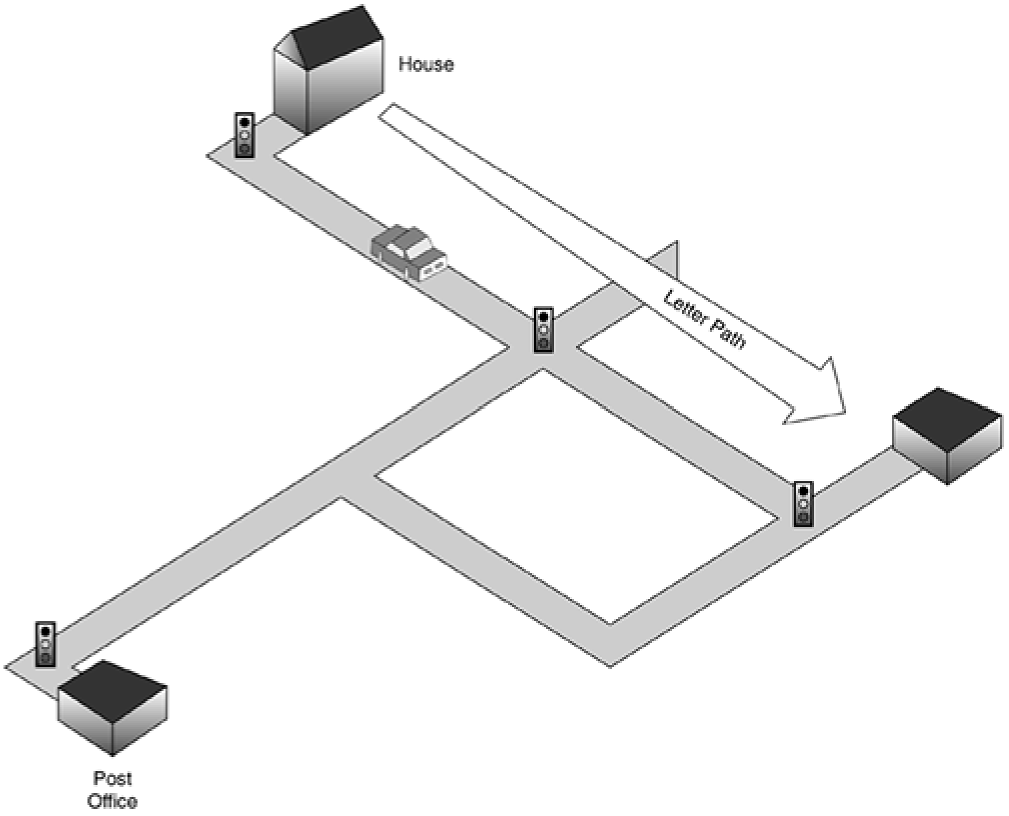
When you arrive at the train station, with ticket in hand telling you where you are going (in case you forgot), you look at the train departure board to determine from which track your train is departing. When you know which track, you go to the gate, board the train, and continue your journey, repeating these steps until you arrive at your intended destination.

A train switching tracks with the passengers still aboard is similar to frames being switched between LAN segments (Layer 2 switching). When the passengers disembark and board another train at the train station, with ticket in hand telling them where to go, this is similar to packets being routed between network segments (Layer 3 routing).

Layer 3 and Above

The logical topology at Layer 3 (network) is made possible by the logical topology at Layer 2 (data link) and the physical topology at Layer 1 (physical) underneath it all. A packet has to and from addresses (destination and origination), much as a letter has sending (return) and receiving addresses. The letter does not concern itself (as much as a letter is "concerned") with how it gets from sender to receiver because it has a logical "straight line." The letter, or packet, is not aware of the lower logical and physical layers that comprise the line of direction, just that the letter has a path to get to its intended destination, as illustrated in Figure 3-16.

Figure 3-16. Logical and Physical Topology of a Letter's Travels



View full size image

The physical topology is illustrated by the roads between the house and the post offices. This physical topology is broken down into segments by the traffic lights at various points along the way. The logical topology here is the straight line from the house to the post office, unaffected by the roads traveled or the traffic signals along the way. The letter's transmission from house to post office is affected here when there is no physical path at all, such as all available roads closed or blocked.

Packets

Because packets and frames work at different layers (Layer 3 and Layer 2 respectively), they involve different aspects of the network. Think of a frame as a train engineer - he needs to know where to go and how to get there and is not concerned with where the train has just left. A packet needs to know where it is going and from where it came, much as a letter needs to have the recipient's address and the sender's address. The recipient in turn uses the return address to send a reply.

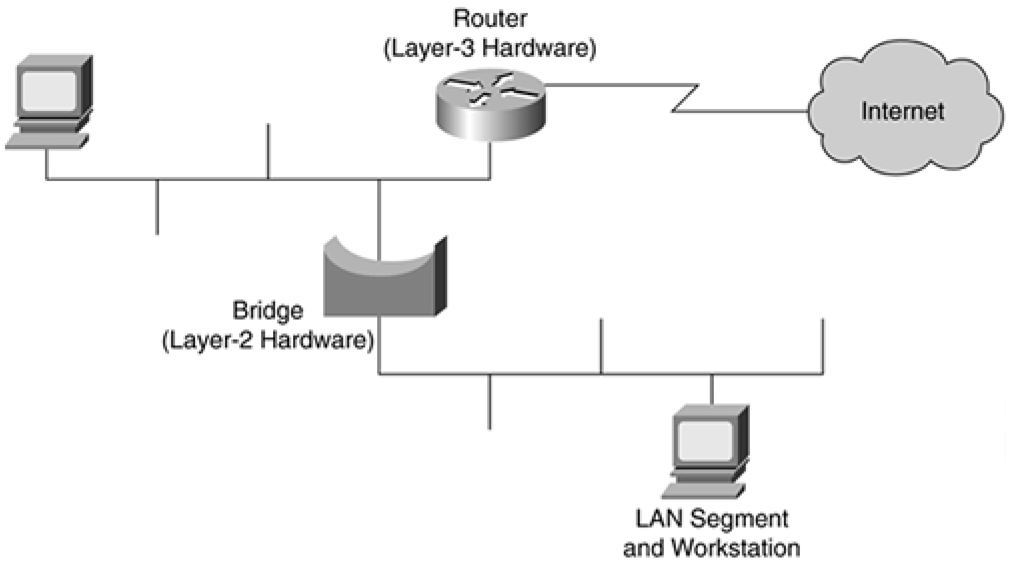
A packet is a fixed block of data sent as a single entity across a network. Commonly when LANs are discussed, the terms frame and packet are used synonymously. However, packets are found in the network layer (Layer 3 of the OSI model), and frames are at the data link layer (Layer 2 of the OSI model).

Packets are only affected by the underlying physical and logical topology if a failure results in the path being broken. For example, suppose you have three roads between home and work and at any time you can take any one of those roads. One morning one of those roads is closed for construction; the physical path is unavailable for use. The physical topology for your drive has changed because now two roads are available rather than the original three. You are not concerned here because you still have a way to get from home to work. Your logical path has not changed; it is still home to work, but the physical topology has changed in that now you have to take a different road. Network packets work in the same way. It is the routers and Layer 3 switches that decide over which path the packets move, making the decisions just as you would behind the wheel of the car.

Hardware

Hubs and repeaters are found at Layer 1, bridges and switches and found at Layer 2, and routers are found at Layer 3. A router is a network device that receives and forwards data packets along a network. A router connects two or more networks together; often these are WANs, but routers can also be used to connect two or more LANs. The most common placement of a router is between a LAN and a WAN, such as the Internet, as illustrated in Figure 3-17.

Figure 3-17. Router Connecting a LAN and the Internet



Routers work at Layer 3 of the OSI model to examine the header of each packet. From the header the router determines the path on which the packet must be forwarded. This is similar to the decision you make when you look at an arrival and departure board in the train station to determine on which track your train departs. Routers determine pathways for packets based on routing tables.

The common theme here is that you make a determination based on a table of information, and routers make a determination based on a similar table of information, called a routing table.

Summary

Local-area networks (LANs) are confined to small geographic areas, such as your home or office building. Wide-area networks (WANs) span broad geographic areas, such sections of a country or continents. WANs interconnect LANs and create what appears to users as a single network.

Information sent across media is called a signal and is in electronic (analog or digital), optical (light), or radio (wireless or cellular) form. Analog signals are measured as continuous waves with a certain frequency, whereas digital signals are measured as square waves with discrete values: 1 or 0. Optical signals are light pulses and are also measured as square waves with the same values as digital signals. Radio signals are measured like analog signals, in continuous waves with a specified frequency.

Recall the physical topology of a network is its layout; the logical topology determines where the devices are placed in the network and how these devices communicate with each other. It is the topology that also determines how network devices talk with each other, either in a direct path or through another device. A full-mesh topology enables every network device to talk with every other device - each device has a direct path to every other device. A star topology provides a central point in the network for communication from each device to pass through.

The physical (OSI model Layer 1) topology of a network represents how each device is interconnected by media or equipment. The logical (OSI model Layers 2 and 3) topology of a network represents the conceptual view of how devices are interconnected, often, but not always, bearing a resemblance to the physical topology.

Hubs carry bits, switches carry frames, and routers carry packets. They all connect physical segments together to create a larger network. Frames are moved around the network by Layer 2 hardware, such as bridges or switches. Bridges and switches use the frame header to determine to which network segment the frame must be forwarded. Bridges and switches determine forwarding decisions for frame movement based on a forwarding table in a MAC table.

The packet, a Layer 3 data unit, is carried by the frame inside its payload section. Packets are the concern of Layer 3 hardware, such as routers. The difference is that whereas a bridge or switch just forwards the frame out a specified port, routers decide the disposition of the packet, such as through which port to forward the packet and if the router is to forward the packet at all. A router can make a more intelligent decision because it knows the source and destination and has capacity to make a decision about paths that are several hops downstream from the router.

Traditional LAN Architecture

Components of a LAN

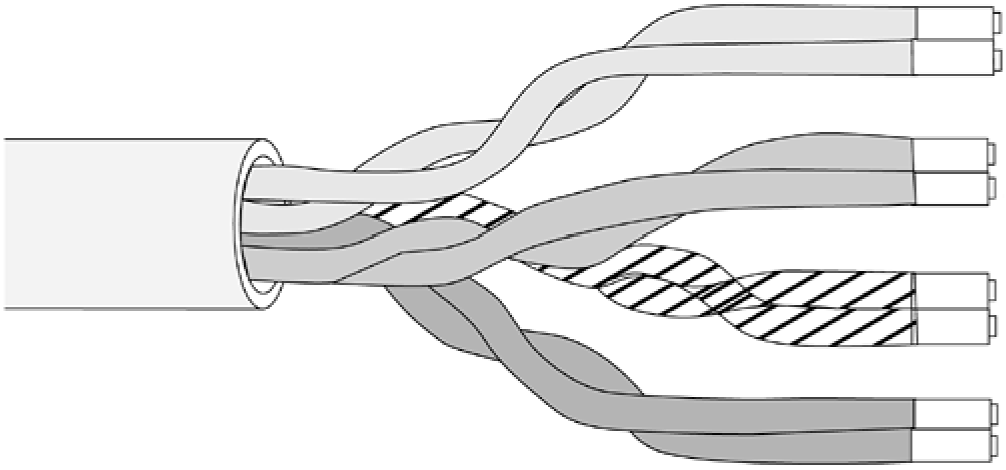
By simple definition, a LAN is two or more devices connected to each other by some type of medium, such as a cable. With the exception of wireless LANs, which are beyond the scope of this book, if there is no cable connection between devices, no connection can occur. These network cables attach to LAN devices via the network interface card (NIC) or network interface port, such as found on a switch.

Cabling

Twisted-Pair Cabling

Twisted-pair cable is a thin-diameter copper wire used for voice and data network cabling. The wires are twisted around each other to minimize interference from other twisted pairs in the cable. Twisted-pair cabling, illustrated in Figure 4-1, enables the use of less bandwidth than required for coaxial cable or optical fiber.

Figure 4-1. Twisted-Pair Cable



Two types of twisted-pair cabling are found in LANs: shielded twisted-pair (STP) and unshielded twisted-pair (UTP).

Shielded Twisted-Pair (STP)

Shielded twisted-pair (STP) is a type of copper wiring in which each of the two copper wires is twisted together and coated with an insulating coating that functions as a ground for the wires. The extra covering in STP wiring protects the transmission line from electromagnetic interference (EMI) leaking into or out of the cable that could result in signal degradation or loss.

STP is used for most Ethernet cabling requirements, especially Fast Ethernet connections, such as 100 megabits per second (Mbps). STP cabling is also used when emission security concerns exist, such as with a classified network (protecting national security information, for instance).

Unshielded Twisted-Pair (UTP)

Unshielded twisted-pair (UTP) is a popular cable type made up of two unshielded wires twisted around each other. Because UTP is not expensive, it is the prevailing choice for LAN and telephone connections. UTP cabling differs from STP in that UTP does not provide the high bandwidth and good protection from EMI that coaxial and fiber-optic cabling provides.

UTP cabling is available in seven standard categories defined by the Telecommunications Industry Association 568 (ANSI/EIA/TIA-568) and are listed in Table 4-1.

Table 4-1. UTP Cable Categories

Category	Number of Wires	Transmission Rate
1	Two	Voice (telephone cable)
2	Four	Up to 4 Mpbs
3	Four	Up to 10 Mbps
4	Four	Up to 16 Mbps
5	Four	Up to 1 gigabit per second (Gbps)
5e	Four	Up to 1 Gbps
6	Four	Up to 10 Gbps

The cable category indicates the number of twists per inch. The more twists in the cabling, the more immune the cable from interference, the faster the cable can transmit, and the greater the bandwidth.

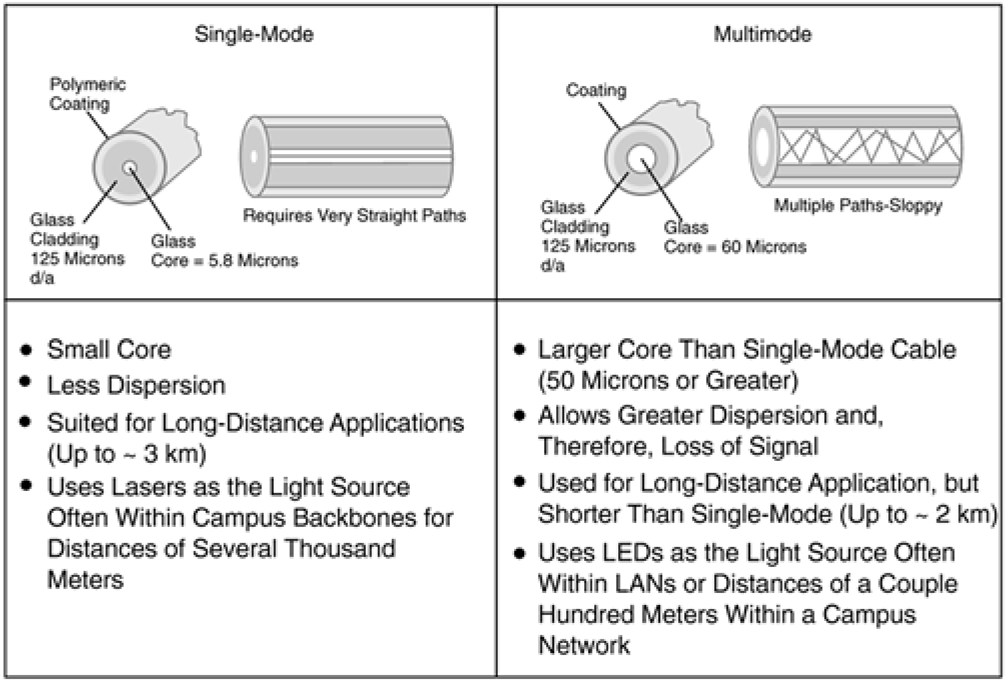
Fiber-Optic Cabling

An optical fiber is a thin glass or plastic strand designed for light transmission and capable of transmitting trillions of bits per second. Optical fiber offers many advantages over copper wire because the light pulses carried by fiber are not affected by random radiation in the environment, and its error rate is significantly lower. Fiber enables longer distances to be spanned before the signal has to be regenerated by repeaters, as required for the electrical signal carried by copper wire. Fiber is also more secure than copper because wire taps in the fiber line can be detected.

A fiber-optic cable is essentially a glass or plastic strand encased in a metal and plastic sheath. Light is transmitted across the fiber strands via lasers. To understand how the laser light moves down the strand, imagine shining a flashlight down a poster tube. The tube prevents the light from spreading in all directions; instead, the tube contains the light and provides a path for the light to travel across. The laser is sent from a laser diode at the sending end of the fiber and travels down the strand to the receiver; and no, you cannot set the laser to stun in the laser diode.

Figure 4-2 illustrates the two primary types, or modes, of fiber used in optic transmission: multimode and single mode.

Figure 4-2. Multimode and Single-Mode Fiber



Single-Mode	Multimode
• Small Core • Less Dispersion • Suited for Long-Distance Applications (Up to ~ 3 km) • Uses Lasers as the Light Source Often Within Campus Backbones for Distances of Several Thousand Meters	• Larger Core Than Single-Mode Cable (50 Microns or Greater) • Allows Greater Dispersion and, Therefore, Loss of Signal • Used for Long-Distance Application, but Shorter Than Single-Mode (Up to ~ 2 km) • Uses LEDs as the Light Source Often Within LANs or Distances of a Couple Hundred Meters Within a Campus Network

View full size image

Single-mode fiber is used to span longer distances, and multimode fiber is common for short distances.

Single-mode fiber (SMF) is an optical fiber used for high-speed transmission over long distances. SMF provides a higher-quality cable that allows for a cleaner, stronger signal, and therefore provides more bandwidth than multimode. However, the smaller core of SMF makes it more difficult to align the light source at the receiver.

Multimode fiber (MMF) is an optical fiber with a larger core than single-mode fiber and is the most common fiber used for short distances, such as for LANs. Light can enter the core at different angles, making it easier to transmit light from the source to a broader receiver. This broader scope permits the use of a light emitting diode (LED) rather than the precise laser required by single-mode fiber. This is comparable to the difference between using a flashlight and a laser pointer as a pointing device during a lecture; the flashlight is somewhat broad in its coverage, whereas the laser pointer is more precise.

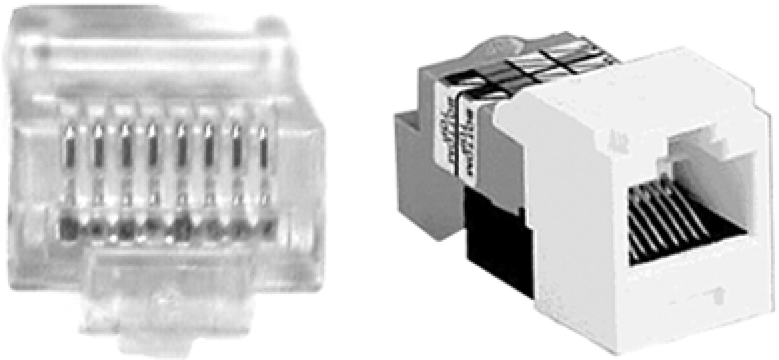
Cable Termination

Cabling between two devices serves no purpose if there is no way to attach the two together - and although duct tape certainly has its purposes in this world, this is not one of them. Cables, whether copper or fiber optic, are clamped at the ends with a jack connection, known as a registered jack, or RJ.

Several types of RJ connectors are used in networking today, and each type is identified by a number. For example, most telephone handset and wall ports use RJ-11 connectors. Ethernet uses RJ-21 and RJ-45 jack types, and T1 lines use RJ-48.

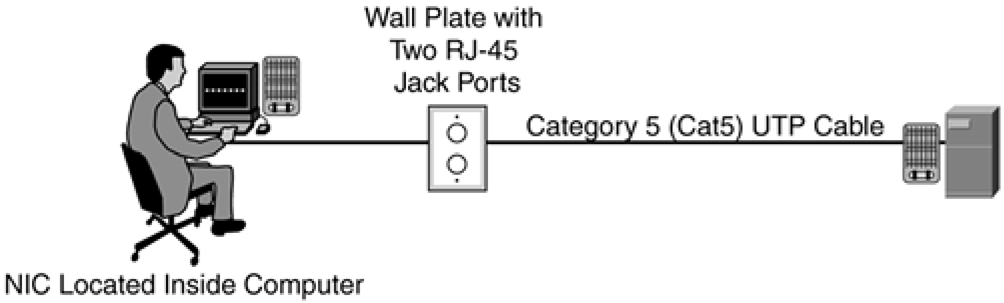
The RJ-21 (Registered Jack-21) is an Ethernet cable using a 50-pin telco connector on one end. On the other end, the cable branches out to 12 RJ-45 (Registered Jack-45) connectors. The RJ-45 is a connector that holds up to eight wires, as illustrated in Figure 4-3.

Figure 4-3. RJ-45 Plug and Socket (Jack)



These RJ-45 plugs and sockets (jacks) are used in Ethernet and Token Ring devices, as illustrated in Figure 4-4.

Figure 4-4. LAN User Cable Termination Points



The NIC found inside the user's desktop computer or other network device, such as a mail server or network printer, is connected via the network cable to the network interface jack.

Wall Plates and Wall Boxes

Wall plates and wall boxes serve the aesthetic purpose of hiding holes in the wall and visible wires. Wall plates and wall boxes help protect the cable from being pulled out, cut, or damaged. They also help with providing a place to label cables. Further, a box can be organized to centralize multiple services for a user in a single location (for example, phone and data together). Figure 4-5 and Figure 4-6 illustrate a wall plate and a wall box that are often used in LAN implementations.

Figure 4-5. Wall Plates

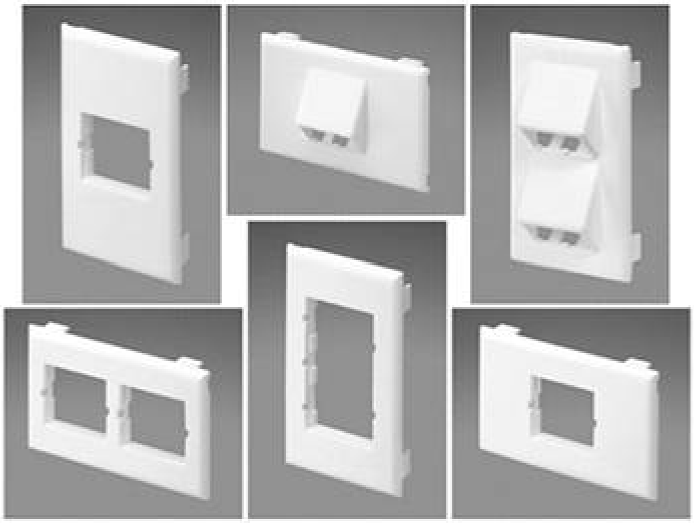
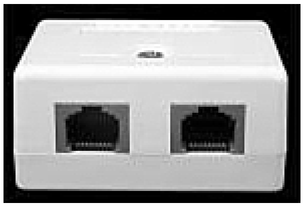


Figure 4-6. Wall Box



The wall plate is mounted onto the wall with an opening for the RJ connection, and a wall box is a freestanding box that can be, but is not always, mounted to a wall. Behind these wall plates and wall boxes is the cabling that runs back to the LAN switch, often sitting in a communications closet somewhere within the building.

Network Interface Card (NIC)

Much as your driveway is an interface to the main road, the network interface card is your interface to the network. With one end of the network cable connected to a port in the wall, the other end needs to connect to a device to complete the circuit. This device is the network interface card, or NIC. NICs are circuit boards that plug into your desktop, laptop, or network servers, such as a web or e-mail server. The NIC controls the sending and receiving of data across the physical Open System Interconnection (OSI) model Layer 1 and data link OSI model Layer 2.

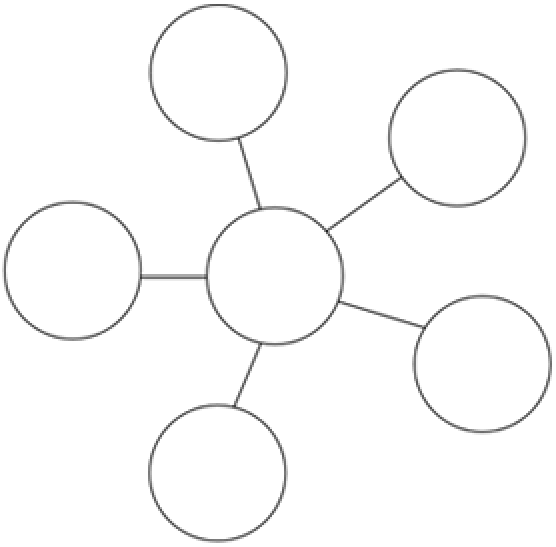
LAN Topologies

There are differences between physical and logical topologies, just as there are differences between physical and logical networks. A physical topology is determined by the cabling that connects the network devices together, whereas a logical topology is determined by the traffic flow across the network.

Star Topology

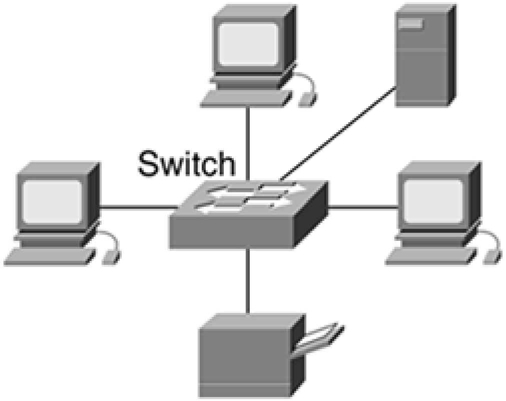
The defining aspect of the star or hub-and-spoke topology is that all network devices are connected to a central point, such as a hub or a switch. The topology resembles a star, as illustrated in Figure 4-7. Star topologies best reflect the difference between a physical and logical topology in that the star topology is wired in a physical star, but your data, such as a print request, moves around the network in a circle.

Figure 4-7. Star or Hub-and-Spoke Topology



The central point of a star topology plays the role of traffic cop in that it directs traffic to its intended destination rather than to everyone on the network. In a LAN implementation, the traffic cop is often the switch. A star topology with a single switch at its central point might look something like the illustration in Figure 4-8.

Figure 4-8. Single-Switch LAN

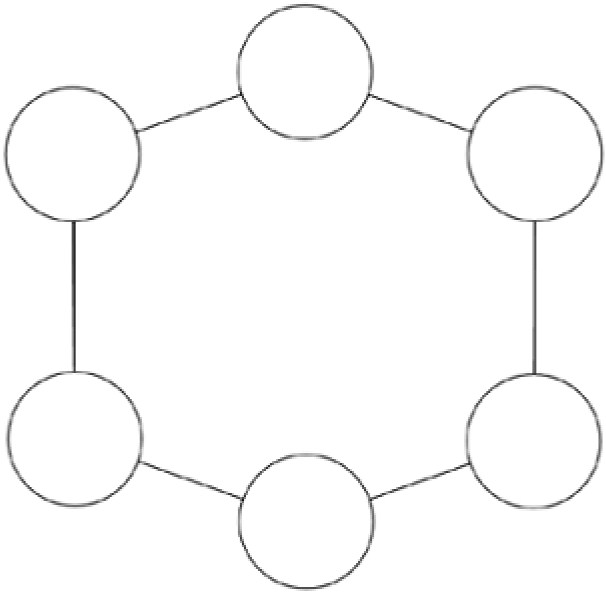


This topology might be found in small office/home office (SOHO) networks or small-to medium-sized corporate networks. A switch is central to the LAN, providing a connection between all devices, such as desktop workstations, servers for file sharing or e-mail, or network-attached shared printers.

Ring Topology

In a physical ring topology, all devices are connected to one another in a closed loop, so that each device is connected to two other devices, one on either side of it. Ring topologies are used in Token Ring and Fiber Distributed Data Interface (FDDI) LANs because of the inherent redundancy in a ring network. For example, if the connection on one side of your machine goes down, the connection on the other side of your machine remains up so you are still connected to network resources.

Figure 4-9. Ring Topology

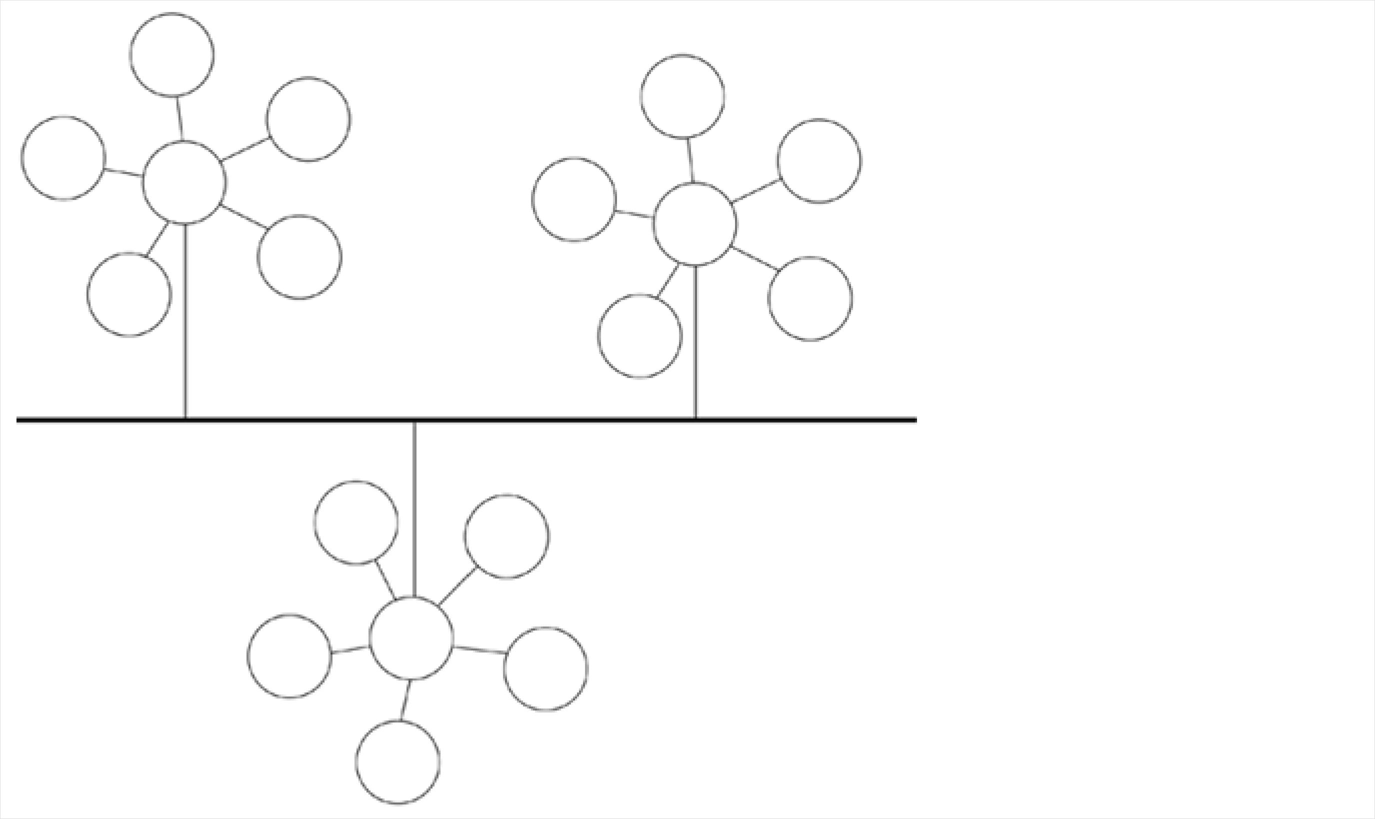


Ring topologies do not use switches but rather multistation access units, or MAUs, enabling connection from each device to the LAN. These MAUs enable your data to travel around the ring in either a clockwise or counterclockwise fashion with each device connected to the ring acting as a repeater.

Tree Topology

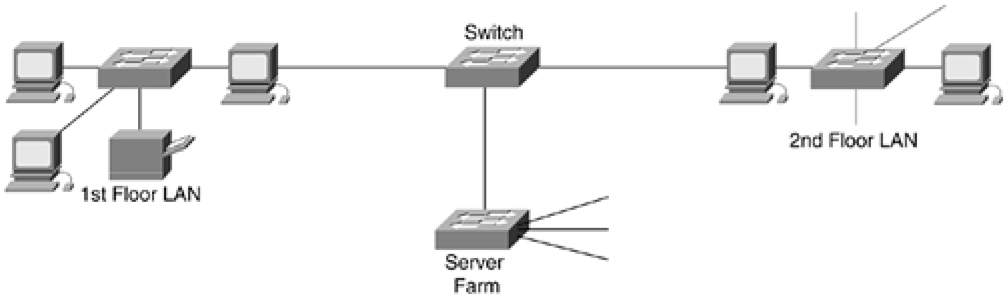
The tree topology is a multitiered hierarchical star topology, in which the endpoint of one spoke in a star is the hub of another, as illustrated in Figure 4-10.

Figure 4-10. Tree Topology



This physical topology is made possible with multiple switches and might be used in an office building where each floor has its own switch, or branch off the tree, connecting to a backbone switch, which provides connectivity between floors, as illustrated in Figure 4-11.

Figure 4-11. Multiswitch LAN



View full size image

Figure 4-11 shows that the users on the first or second floor LAN can use the server farm resources by the connection provided by the backbone switch. These server farm resources might be web servers, e-mail servers, file servers, network printer servers, or any other server on which multiple users need to share information. For example, compare these two methods for sharing files with someone else in your office: E-mail the file back and forth until all changes are complete; or share and edit the file as it sits on a shared file server. You will likely choose the latter, because editing a shared file is easier to manage than multiple e-mails and revisions. In a medium or large LAN, these servers might be grouped together in one place or distributed across the LAN. For example, each floor could have its own shared file and print server.

Local-Area Networks (LANs)

The topology of the LAN is determined by the technology. (For example, a ring topology is implemented by Token Ring or FDDI, and a star or tree topology is implemented by Ethernet.)

Token Ring

Token Ringis a technology developed by IBM and standardized by the Institute of Electrical and Electronics Engineers (IEEE) 802.5 committee for implementation in a LAN environment. Token Ring uses a special frame, called a token, to designate the authoritative speaker for that LAN segment. This technology can connect up to 255 nodes in a physical star or ring connection that can sustain 4 or 16 Mbps. Each node on a Token Ring LAN connects to a central wiring hub called the multistation access unit (MAU) using a twisted wire cable, such as UTP.

Token Ring is more deterministic than Ethernet, which means that it ensures that all users get regular turns at transmitting their data. With Ethernet, all users have to compete for network access to get on to the network. In a Token Ring network, a token is passed around the network from one workstation to the next, giving each workstation equal access to the network. Unlike an Ethernet workstation, which can send data if the line is idle, a Token Ring workstation cannot send data across the network unless it is in possession of the token.

FDDI

Fiber Distributed Data Interface, or FDDI (pronounced "fiddy"), is a LAN and metropolitan-area network (MAN) access method. It is a token-passing network, similar to Token Ring, and uses optical fiber cabling to transmit at 100 Mbps up to 10 kilometers. FDDI provides network services at the same OSI model layers as Ethernet and Token Ring (Layer 1 and Layer 2).

FDDI provides the option of a dual counter-rotating ring topology. This dual-ring topology is used for redundancy so that if one ring fails the other ring carries the traffic. Traffic on these rings travels in opposite directions: The traffic on one ring travels clockwise, whereas the traffic on the other ring travels counterclockwise.

Ethernet

Ethernet is the most widely deployed LAN access method, defined by the IEEE as the 802.3 standard. Ethernet has become popular such that a specification for a LAN connection or network card implies the use of Ethernet even if not explicitly stated. A 10/100 Ethernet port supports both 10BASE-T at 10 Mbps and 100BASE-T at 100 Mbps.

Ethernet is often considered to be a shared-media LAN, which means that all stations on the segment share the total bandwidth - 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet), or 1000 Mbps (Gigabit Ethernet). When Ethernet is deployed in a switched environment, it is no longer considered to be shared. Therefore, each sender and receiver pair has the full Ethernet bandwidth available for use.

Ethernet uses carrier sense multiple access collision detect (CSMA/CD) technology, broadcasting each frame onto the physical medium (wire, fiber, and so on). All stations attached to the Ethernet listen to the line for traffic, and the station with the matching destination MAC address accepts the frame and checks for errors before doing anything further with the frame. If the frame is error free, it is handed to the network layer (Layer 3) of the OSI model and ultimately the data is presented to the user, such as an e-mail. If the frame has errors, however, it is discarded.

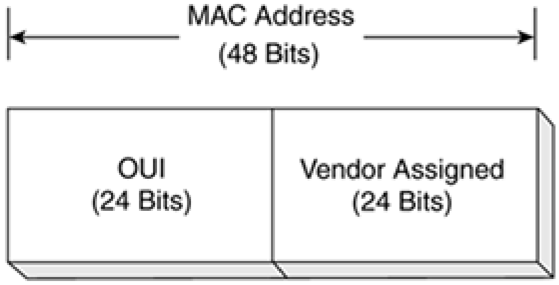
Ethernet LANs

Media Access Control (MAC) Addressing

The MAC address is the unique serial number burned into each network adapter that differentiates the network card from all others, just as your house number is unique on your street and identifies your home from all others. To be a part of any network, you must have an address so that others can reach you. Two types of addresses are found in a network: the logical (OSI model Layer 3, network) and the physical (OSI model Layer 2, data link). For this discussion of LAN environments, the physical address (also known as the Media Access Control (MAC) address) is relevant.

A MAC address is the physical address of the device. It is 48 bits (6 bytes) long and is made up of two parts: the organizational unique identifier (OUI) and the vendor-assigned address, as illustrated in Figure 5-1.

Figure 5-1. MAC Address



The MAC address on a computer might look like this: 00-08-a1-08-c8-13. This MAC address is used for the Fast Ethernet adapter on the computer in question. The OUI is 00-08-a1, and the vendor-assigned number is 08-c8-13.

The OUI is administered by the IEEE and identifies the vendor of the network adapter. The vendor-assigned portion of the MAC address is just that, the alphanumeric identifier assigned by the vendor. It is the combination of the OUI and the vendor-assigned number that ensures that no two network adapters have the same MAC address.

MAC addresses are represented as hexadecimal (hex) numbers.

With the hexadecimal numbering system, each half byte (4 bits) is assigned a hex digit, which is listed in Table 5-1, with its decimal and binary equivalents. Hex values are identified with an h or dollar sign, so $3E0, 3E0h, and 3E0H all stand for the hex number 3E0.

Table 5-1. Hexadecimal, Decimal, and Binary Conversion Table

Hexadecimal (Base 16)	Decimal (Base 10)	Binary (Base 2)
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
A	10	1010
B	11	1011
C	12	1100
D	13	1101
E	14	1110
F	15	1111

Carrier Sense Multiple Access with Collision Detect (CSMA/CD)

Have you been in a meeting in which everyone has had something to say? It's difficult to get anything done when everyone is talking at the same time. When this happens, everyone eventually stops talking and lets one person talk. Ethernet works much the same way when using CSMA/CD.

With CSMA/CD, when an Ethernet device attempts to access the network to send data, the network interface on the workstation or server checks to see if the network is quiet. When the network is clear, the network interface knows that transmission can begin. If it does not sense a carrier, the interface waits a random amount of time before retrying. If the network is quiet and two devices try sending data at the same time, their signals collide. When this collision is detected, both devices back off and wait a random amount of time before retrying, much like two people starting to talk at the same time - both stop and wait a random amount of time before trying to speak again.

CSMA/CD Operation

In a half-duplex environment, Ethernet operates with CSMA/CD, such as found in 10BASE-T (10 Mbps) Ethernet LANs. Half-duplex Ethernet operation means that each device can send and receive data, but not at the same time.

In the framework of CSMA/CD, the computers on a network operate as follows.

- Carrier sense - Each computer on the LAN is always listening for traffic on the wire to determine when gaps between frame transmissions occur.
- Multiple access - Any computer can begin sending data whenever it detects that the network is quiet. (There is no traffic.)
- Collision detect - If two or more computers in the same CSMA/CD network collision domain begin sending at the same time, the bit streams from each sending computer interfere, or collide, with each other, making each transmission unreadable. If this collision occurs, each sending computer must be able to detect that a collision has occurred before it has finished sending its frame.Each computer must stop sending its traffic as soon as it has detected the collision and then wait some random length of time, called the back-off algorithm, before attempting to retransmit the frame.

Collisions

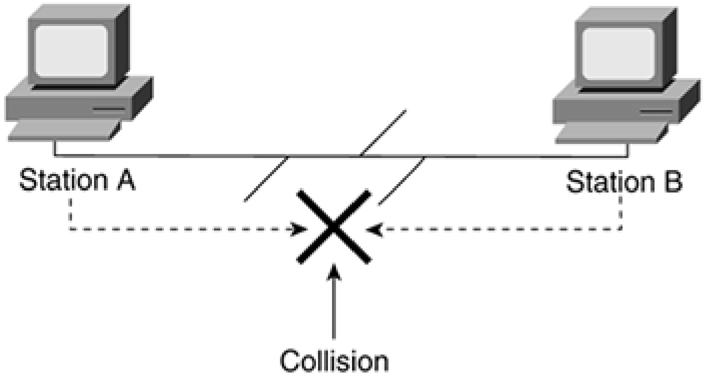
Collisions are used by Ethernet to control network access and shared bandwidth among connected stations that are trying to transmit at the same time on a shared medium, such as the network segment. Because the network medium is shared, a mechanism must exist whereby the network stations can detect network availability so that they do not transmit at the same time; this mechanism is collision detection.

Collisions occur when two frames try to use the same network segment at the same time and both frames are lost, not unlike two people trying to talk at the same time. As you might suspect, collisions in networks and conversations are best avoided. However, collisions in a shared environment cannot be avoided, whether that shared environment is a network segment or the air of a conversation.

Figure 5-2 illustrates what happens when a collision occurs on a network segment.

- Station A attempts to send a frame across the network. First, Station A checks to see if the network is available (carrier sense). If the network is not available, Station A waits until the current sender on the medium has finished.
- Let's suppose that Station A believes the network is available and tries sending a frame. Because the network is shared (multiple access), other stations on the same network segment might also attempt to send at the same time (Station B, for instance).
- Shortly after Station B attempts to send traffic across the line, both Station A and Station B realize that another device is attempting to send a frame (collision detection). Each station waits a random amount of time before sending again. The time after the collision is divided into time slots; Station A and Station B each pick a random slot for attempting a retransmission.
- Should Station A and Station B attempt to retransmit at the same time, they extend the amount of time each waits before trying again, decreasing the chance of resending data in the same time slot.

Figure 5-2. Ethernet Collision



The maximum number of retransmissions for the same data frame is 16; if the transmission fails 16 consecutive times, the network is considered unavailable.

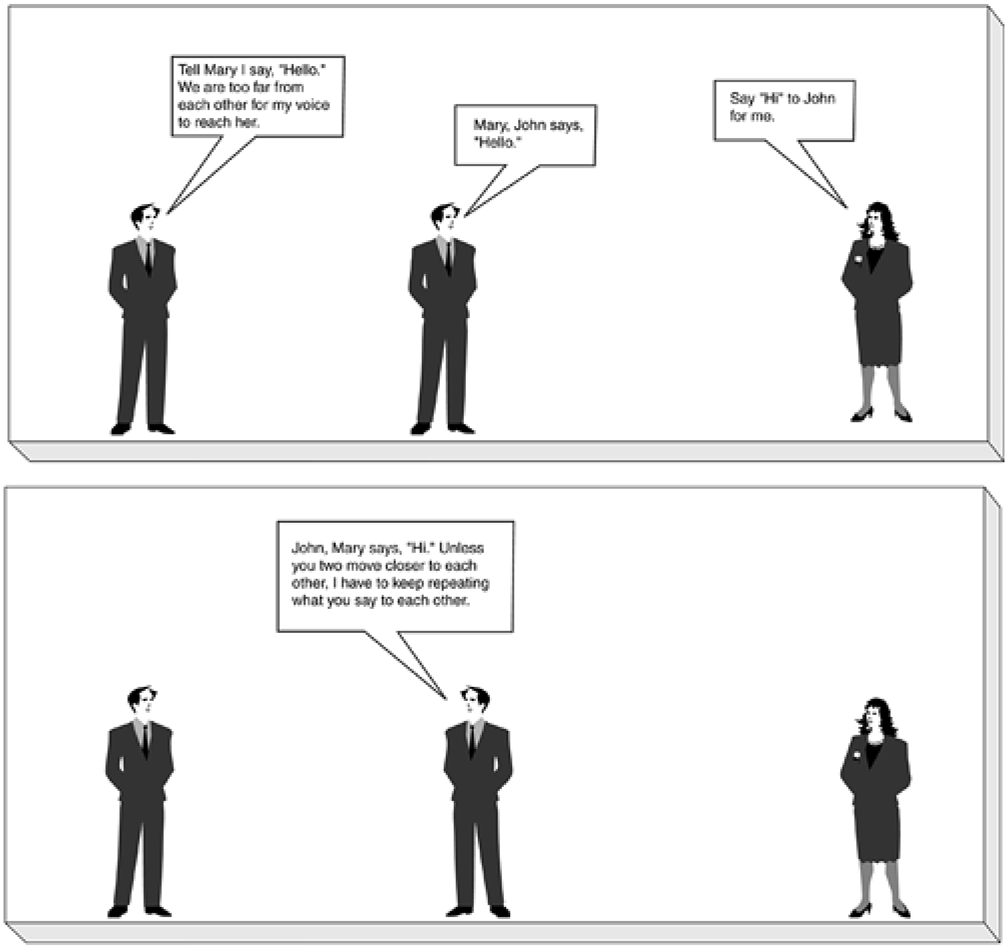
Reducing the number of collisions in a LAN is essential to the design and operation of the network just as reducing the amount of traffic in the city is crucial to reducing delays. Increased collisions result from too many users and devices on the network contending for network bandwidth. This contention slows the performance of the network from the user's point of view, yielding the most frequent call to the help desk: "The network is slow today." Breaking up, or segmenting, the network is the common way of reducing this network contention. Network segmentation occurs when a network is divided into different pieces joined together logically with a bridge, switch, or router.

Ethernet LAN Equipment

Repeaters - Layer 1 Devices

To begin this discussion, it is useful to review the definition presented in Chapter 3: A repeater is a network device used to regenerate or replicate a signal. Repeaters are used in transmission systems to regenerate analog or digital signals distorted by transmission loss. Repeaters are used in both local-and wide-area networking environments to extend the distance a signal can reach. For example, you might use a third person repeating your words to carry your message across a large room, as shown in the Figure 5-3.

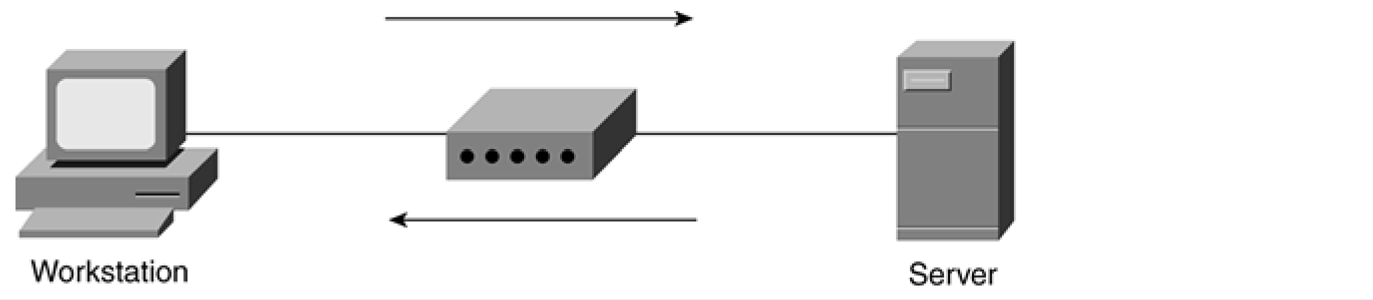
Figure 5-3. Two-Person Conversation with a Third Person Repeating


Tell Mary I say, "Hello." We are too far from each other for my voice to reach her.
Mary, John says, "Hello."
Say "Hi" to John for me.
John, Mary says, "Hi." Unless you two move closer to each other, I have to keep repeating what you say to each other.

View full size image

In the LAN environment, you would use a repeater to extend the distance a data signal can travel on a cable, as illustrated in Figure 5-4.

Figure 5-4. Repeater Operation



If you are in a large building and you are connecting two network devices that are several hundred feet apart (a server and a workstation, for example), a single 25-or 50-foot cable segment is obviously not going to be long enough. You can use a repeater to connect multiple cables together to make a single cable length long enough for your requirement.

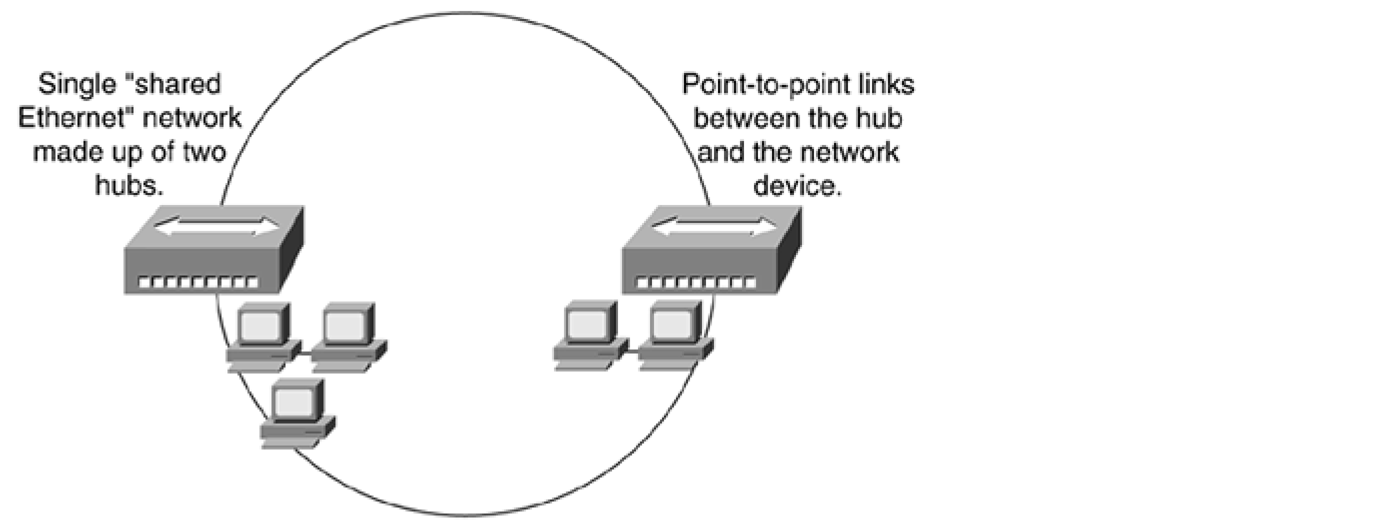
Hubs - Layer 1 Devices

A hub is often used to connect small LAN segments in which the number of devices is generally 24 or fewer, and hubs are multiport repeaters. Hubs are used to create collision domains, in which all devices on the network can see each other. In larger designs, signal quality begins to deteriorate as segments exceed their maximum length, often a couple hundred feet. Hubs provide the signal amplification required to allow a segment to be extended a greater distance. A hub takes an incoming signal on any one port and repeats it out all ports to enable users to share the Ethernet network resources.

Ethernet hubs create star topologies in 10-Mbps or 100-Mbps half-duplex Ethernet LANs. It is the hub that enables several point-to-point segments to be joined together into one single network, and it is this network of hubs that makes up a shared Ethernet, just as several point-to-point roads join together into the single large network of roads you use to get around town.

A shared Ethernet LAN means that all members of the network are contending for transmission of data onto a single network (collision domain); individual members of a shared network get only a percentage of the available network bandwidth, as illustrated in Figure 5-5.

Figure 5-5. Shared Ethernet (Total Bandwidth Shared Among Attached Hosts)


Single "shared Ethernet" network made up of two hubs.
Point-to-point links between the hub and the network device.

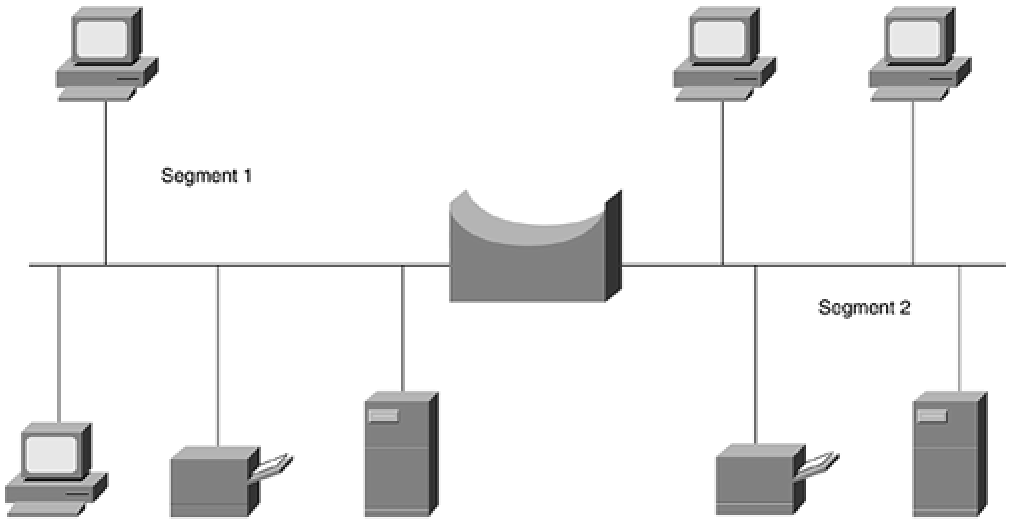
One end of the point-to-point link is attached to the hub, and the other is attached to the network device, such as a computer or printer. Connecting multiple hubs together expands the shared Ethernet segment but puts more stress on the line's bandwidth because now more users are trying to use the same bandwidth. This is similar to building a new neighborhood without adding roads and thus putting stress on existing roads. As you and your car sit stuck in traffic, so might your data suffer in network congestion.

Network bridges are one way to prevent this congestion. Network bridges function like hubs in that bridges provide a network connection; however, bridges preserve the separation of these network segments by keeping network traffic local to its respective segment instead of repeating it all to the world. Bridge operation is discussed in detail in the following section.

Bridges - Layer 2 Devices

Repeaters and hubs have no intelligence; they just repeat whatever signal is received from one port out all ports without looking at what is being sent or received. Bridges add a level of intelligence to the network by using the MAC address to build a table of hosts, mapping these hosts to a network segment and containing traffic within these network segments. For example, Figure 5-6 illustrates a bridged network with two network segments.

Figure 5-6. Bridge Connecting Two Ethernet Segments



View full size image

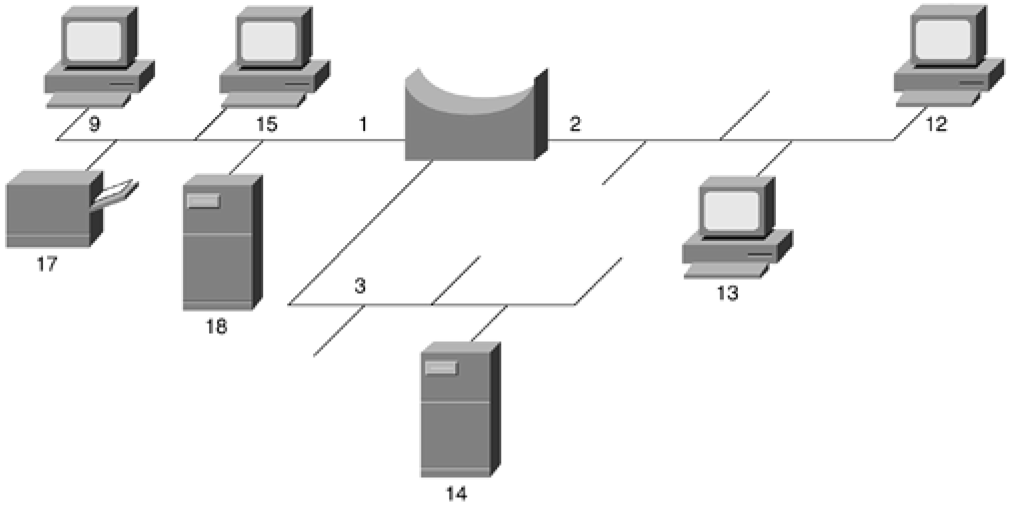
Segments 1 and 2 contain two workstations each, a file server (for file sharing) and a network printer. Suppose that your engineering and financial teams share a floor in an office building and that Segment 1 is made up of your engineering team and Segment 2 is made up of your financial team. If a hub were used to connect these teams to your corporate network, each team would be contending for the total network bandwidth, causing slowdowns on the network. The engineering team might be using all the bandwidth at the moment that someone in finance is trying to process the payroll.

As you might surmise, using a hub in this scenario is not the preferred method because of the contention for the network bandwidth. In this scenario, a bridge is a better choice than a hub because the bridge segments the network into two smaller parts - an engineering team segment and a financial team segment - keeping traffic local to its respective segment.

Ethernet bridges map the MAC addresses of the network devices, or nodes, residing on each network segment. Bridges allow only necessary traffic to pass through the bridge, such as traffic destined for a segment other than the source. When a frame is received by the bridge, the bridge looks at the frame header and reads the source and destination MAC addresses, determining the frame sender and destination. If the frame's source and destination segments are the same, the frame is dropped, or filtered by the bridge; if the segments differ, the bridge forwards the frame to the correct segment.

Figure 5-7 illustrates a small bridged network with three network segments.

Figure 5-7. Bridge Connecting Three LAN Segments



If the bridge sees a frame arrive on port 1 from Host 9, the bridge concludes that Host 9 can be reached through the segment connected to port 1. If the same bridge sees a frame arrive on port 2 from Host 12, the bridge concludes that Host 12 can be reached through the network segment connected to port 2, as illustrated in Figure 5-8. Through this learning process, bridges build a table, such as shown in Table 5-2.

Figure 5-8. Bridge Connecting Two LAN Segments (A and B)

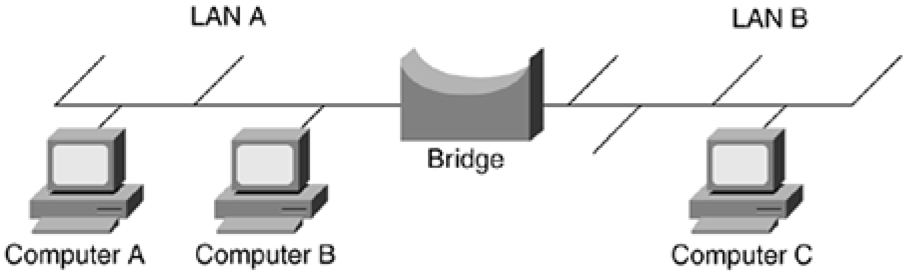


Table 5-2. Bridge Table

Host Address	Network Segment
15	1
17	1
12	2
13	2
18	1
9	1
14	3

This filtering or forwarding function is similar to what an organization's mailroom does on receipt of an envelope; if the destination of the envelope is the same as the source (within the building), the mailroom attendant filters this envelope from any outgoing mail being forwarded to the post office. If this envelope is for a destination outside of the building, the mailroom attendant forwards it to the network, and in this case, the network is the post office.

Bridge Operation

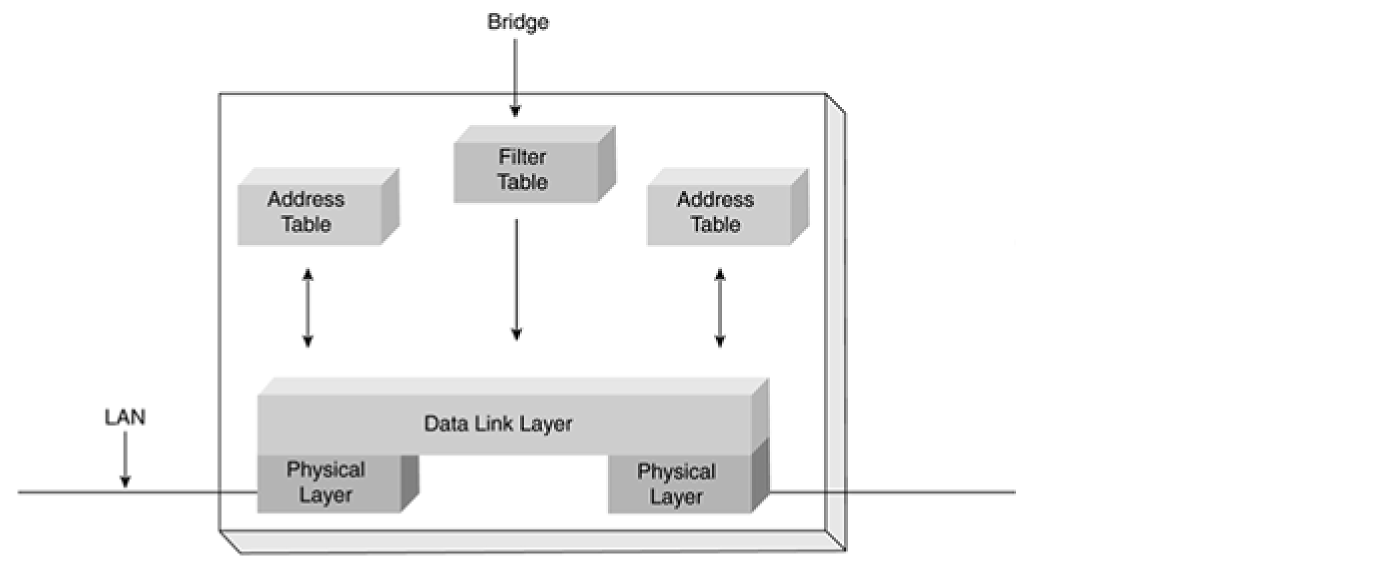
The most frequently used bridge in Ethernet LANs is the transparent bridge. The bridge is called "transparent" because the computers using a bridge are unaware of its presence in the network, and traffic passes "transparently" over the bridge. Think how often you barely notice a small bridge you drive across; if it weren't for the view, you would not know you passed over a bridge because the road continued onward.

LAN bridges forward frames from one LAN to another. For example, as illustrated in Figure 5-8, the bridge forwards all traffic originating from LAN A to destinations found in LAN B, such as Computer C.

The bridge could forward all frames it receives but in doing so it acts as a repeater, not a bridge. The desired operation is for the bridge to forward only frames that need to travel from one LAN to another, such as from LAN A to LAN B and vice versa (as shown in Figure 5-8). In forwarding traffic between LAN segments the bridge learns the following: which computers are connected to which LANs, which addresses to use when forwarding traffic on to another LAN segment, and which addresses to filter or not forward.

To learn which addresses are used and by which ports, the bridge examines the headers of received Ethernet frames on each port in use. The bridge is looking specifically at the source MAC address of each received frame and recording the port on which it was received. A bridge stores the hardware addresses observed from frames received by each interface and uses this information to learn which frames need to be forwarded by the bridge. Figure 5-9 shows this bridge-learning process.

Figure 5-9. Operation of a Bridge Filter Table



View full size image

The learned addresses are stored in the interface address table associated with each port (interface). As this table is being built, the bridge examines the destination MAC address of all received frames. As it examines the frames, the bridge searches the interface table to see whether a frame has been previously received from the same address, such as a frame with a source address matching the current destination address.

The bridge's search of the interface table can encounter the following circumstances:

- If the address is not found, no frames have been received from the source.
- The source may not exist, or it may not have sent any frames using this address. (The address may also have been deleted by the bridge because the bridge was restarted or ran short of address entries in the interface table or the address was too old.)

Because the bridge does not know which port to use to forward the frame, it sends the frame out all ports, except that port from which the frame was received; this is called flooding.

It is unnecessary to send the frame back to the same cable segment from which it was received, because any other computer/bridges on this cable will already have received the frame.

- If the address is found in the interface table and is associated with the port on which it was received, the frame is discarded because it is considered to already have been received by the destination.
- If the address is found in the interface table and is not associated with the port from which it was received, the bridge forwards the frame to the port associated with the address.

Interface Table Management

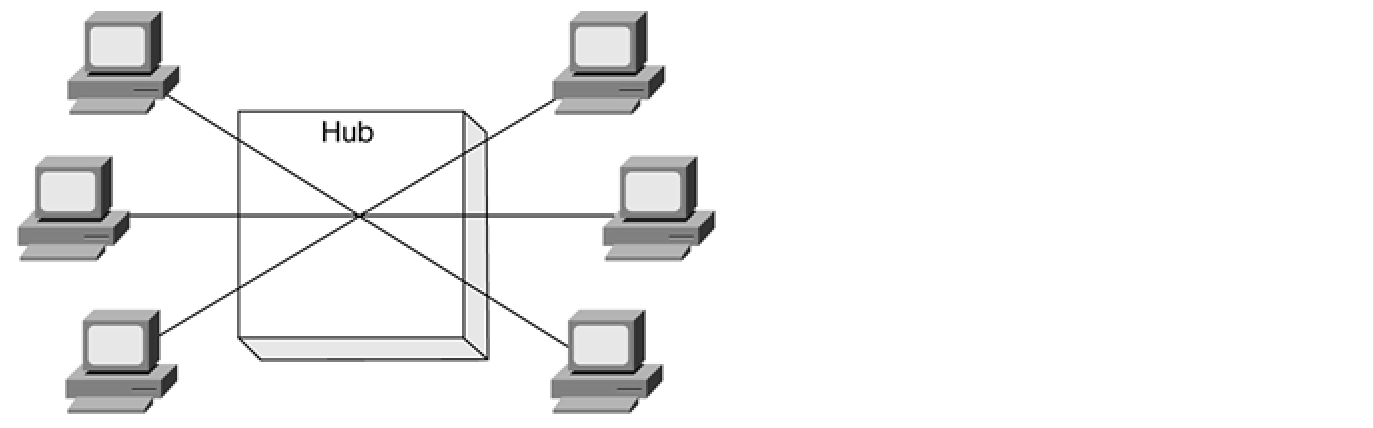
A bridge might implement an interface table using a software data structure or use a content-addressable memory (CAM) chip. In either case, the size of the table is finite. In a large LAN, this limit might be a problem in that there could be more hosts and addresses than there is space in the table. To help keep the table small, most bridges maintain a check of how recently each address was used. Addresses that have not been used for a long period of time (minutes) are deleted. This has the effect of removing unused entries; if the address is used again, however, before a frame is received from the same source, it requires the frame to be flooded to all ports.

A useful side effect of deleting old addresses is that the bridge interface table records only working MAC addresses. If a network interface card (NIC) stops sending, its address is deleted from the table. If the NIC is subsequently reconnected, the entry is restored; if the connection is made to another port (the cable is changed), however, a different (updated) entry is inserted that corresponds to the actual port associated with the address. (The bridge always updates the interface table for each source address in a received MAC frame. Therefore, even if a computer changes the point at which it is connected without first having the interface table entry removed, the bridge still updates the table entry.)

Switches - Layer 2 Devices

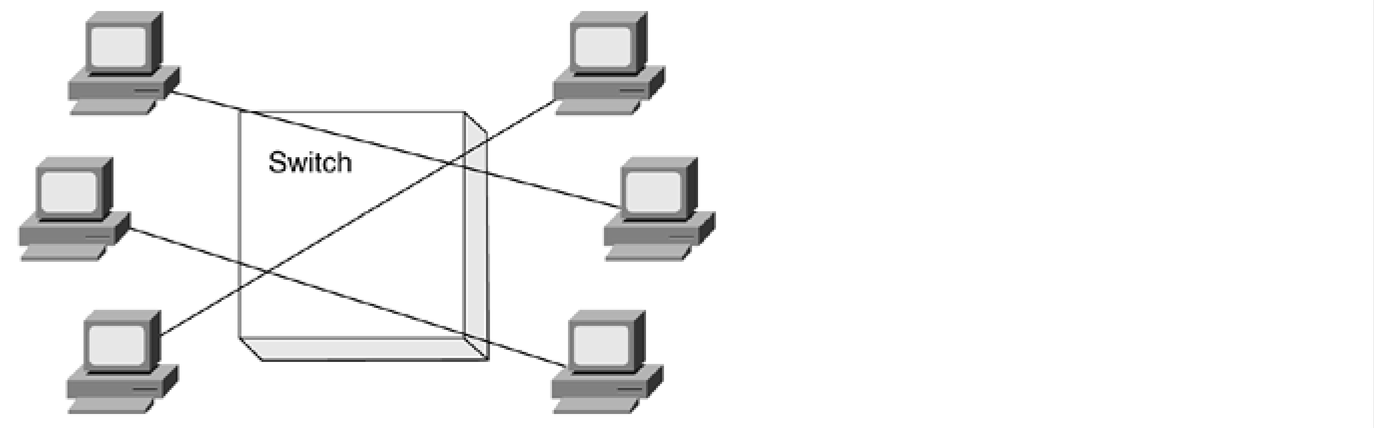
Hubs create a network environment in which each connected device shares the available network bandwidth with other devices contending for the same network resources, as illustrated in Figure 5-10.

Figure 5-10. Shared Network



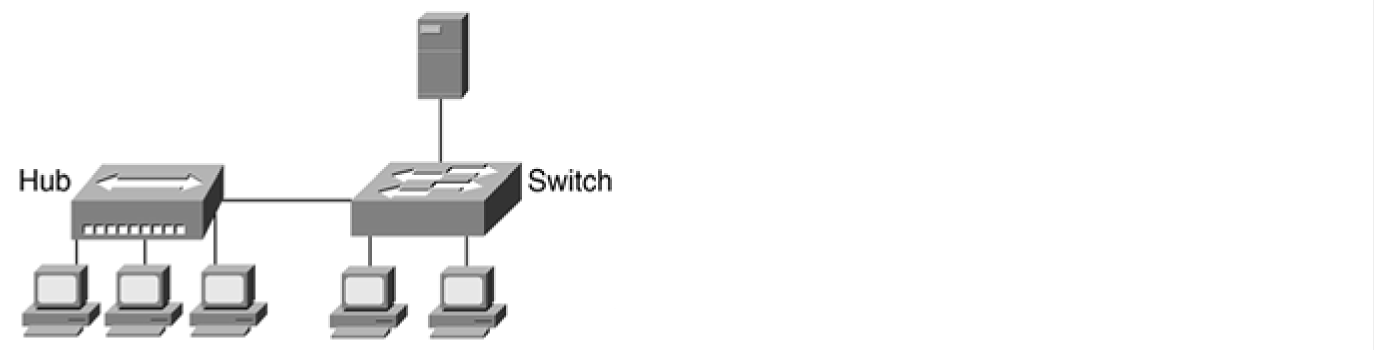
The hub is connecting six workstations together, each sharing the network bandwidth. A finite amount of network bandwidth is available. For example, 10BASE-T Ethernet provides 10 Mbps, and the more workstations added to this network, the less bandwidth available for each. Switches address the shared bandwidth issue and eliminate contention by dedicating a path between the source and the destination, as illustrated in the Figure 5-11.

Figure 5-11. Dedicated Network



Network switches replace shared-media hubs, increasing network bandwidth. For example, a 16-port 100BASE-T hub shares the total 100-Mbps bandwidth with all 16 attached nodes. By replacing this hub with a switch, each source (sender) and destination (receiver) pair has access to the full 100-Mbps capacity of the network. Each port on the switch can give full bandwidth to a single server or client station or each can be connected to a hub with several stations, as illustrated in Figure 5-12.

Figure 5-12. Switch with Dedicated and Hubbed Nodes



Dedicating ports on Ethernet switches to individual nodes is another way to speed access for critical computers. Servers and power users can take advantage of a full segment for one node, so some networks connect high-traffic nodes to a dedicated switch port.

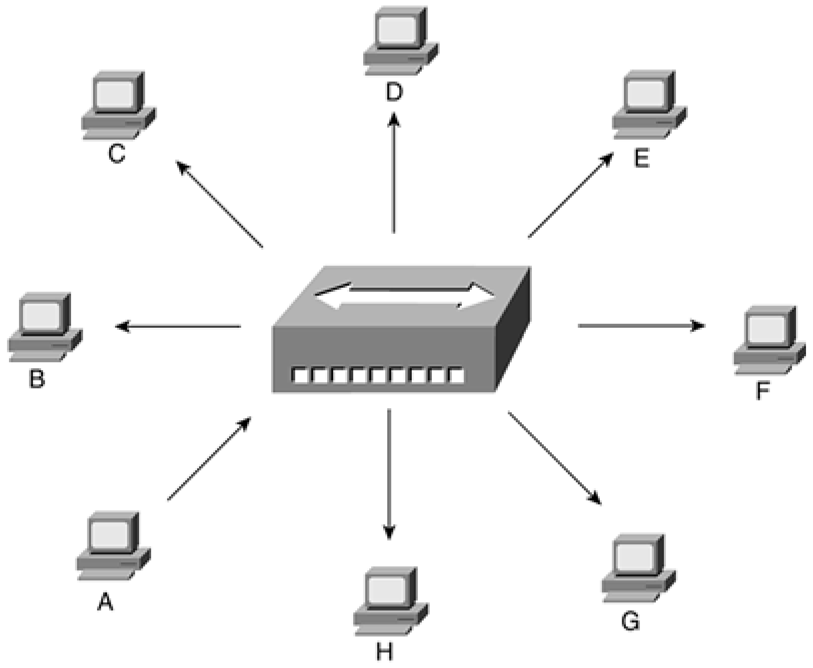
Switches sit in the same place in the network as hubs. Unlike hubs, however, switches examine each frame and process the frame accordingly instead of just repeating the signal to all ports. Switches map the MAC addresses of the nodes residing on each network segment and then allow only the necessary traffic to pass through the switch. A switch performs the same functions as a bridge; so when the switch receives a frame, it examines the destination and source MAC addresses and compares them to a table of network segments and addresses. If the segments are the same, the frame is dropped, or filtered; if the segments differ, the frame is forwarded to the proper segment.

The filtering of frames and regeneration of forwarded frames enables switches to split a network into separate collision domains. Frame regeneration enables greater distances and more network devices, or nodes, to be used in the total network design, and lowers the overall collision rates. In switched networks, each segment is an independent collision domain, whereas in shared networks all nodes reside in one, big, shared collision domain.

Switch Operation

Remember that a bridge with more than two ports can also be called a switch. The difference between a hub and a bridge/switch is the number of frames they forward. Figure 5-13 illustrates how a hub forwards a frame received from Node A that is destined for Node F.

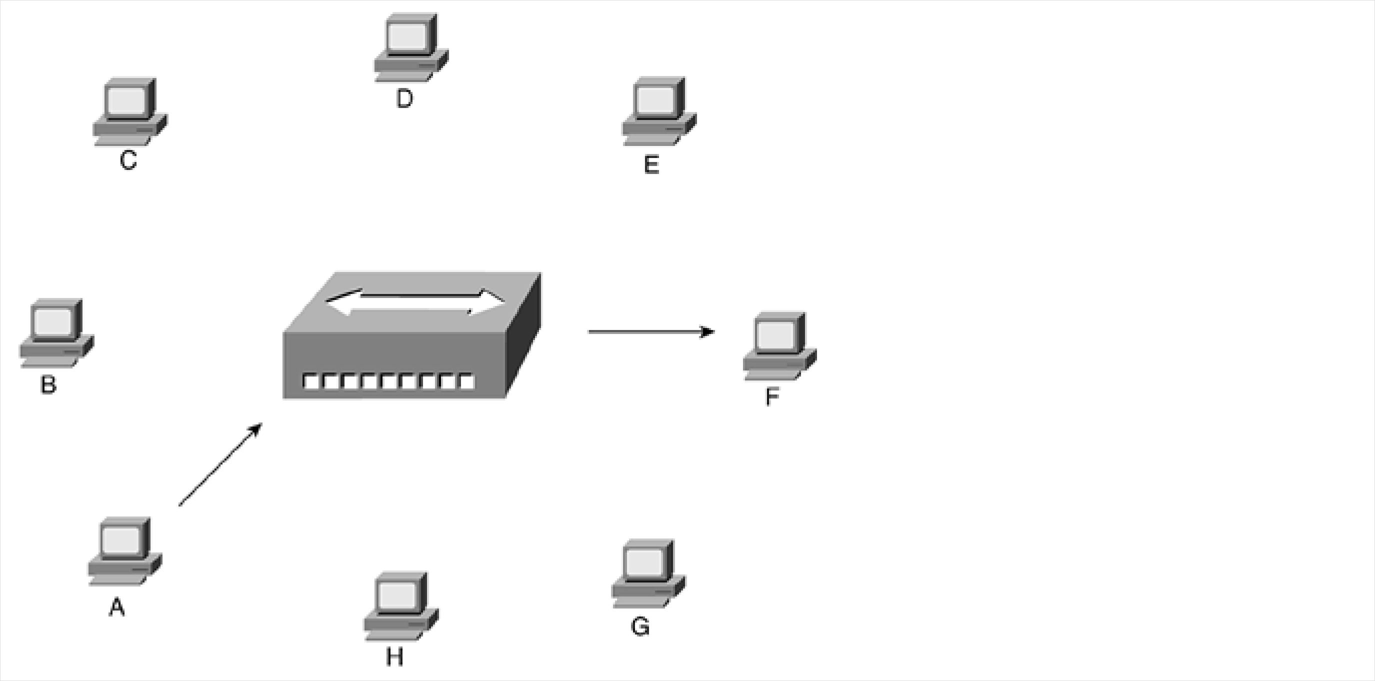
Figure 5-13. A Hub Repeating a Frame from A to F



Recall that a hub is a multiport repeater and repeats any signal received on one port out all ports. When the hub receives a signal from Node A, it repeats, or forwards, this received frame out all the ports, so that the frame reaches all connected equipment, even though the frame might be destined for a device connected to one specific port interface (Node F, for example, in the case of Figure 5-13).

Instead of repeating the frame out every port, the switch forwards the frame to only the required interface, as illustrated in Figure 5-14.

Figure 5-14. Switch Forwarding a Frame from A to F



The switch learns the association between the node's MAC address and the interface port in the same way a bridge learns - by listening to which MAC addresses enter the switch and from which port. By sending the frame only where it needs to go, the switch reduces the number of frames on the other LAN segments, in turn reducing the load on these segments and increasing the performance of the connected LANs.

If the switch does not have an entry in its forwarding table and forwards a frame out every port, this is known as a broadcast. This scenario makes it possible to have a flood that is similar to a flood in a hub-based environment. A switch will perform a directed transmission, if it knows the port, and therefore does reduce broadcasts, but a switch does not remove all broadcasts. Because a switch does not remove all broadcasts, a router is used in network designs because a router breaks up broadcast domains and reduces broadcast storms.

Switching Methods

Ethernet switches are an expansion of Ethernet bridging in that switches can link several LANs together. In linking several LANs together, switches forward frames between these LAN segments using one of two basic methods: "cut through" and "store and forward".

Cut-through switches examine only the frame's destination MAC address before forwarding it on to its destination segment. Cut-through switching is comparable to the postmen taking each piece of mail received at a post office, looking at the address, and then sending the mail on to its destination.

Store-and-forward switches accept the entire frame, analyze it for errors, look at the destination MAC address, and then forward the frame on to its destination. Store-and-forward switching is comparable to postmen taking each piece of mail received at the post office, opening it, checking the contents for spelling, grammar, and ensuring no contents are missing, before sending the mail on to its destination. It takes more time to examine the entire frame, but store-and-forward switching enables the switch to catch certain frame errors and keep them from propagating through the network.

Both cut-through and store-and-forward switches separate networks into collision domains, allowing network design rules to be extended. Each of the segments attached to a switch has a full bandwidth shared by fewer users, resulting in better performance, in contrast to the bandwidth sharing that is characteristic of a hub-based environment. A network composed of a number of switches linked together is called a collapsed backbone network.

Connecting Bridges and Switches Together

A special rule controls bridge and switch interconnection. The rule says that a bridge/switch/hub LAN must form a tree, and not a ring. This means there must be only one path between any two computers. If more than one parallel path exists, a loop would be formed, resulting in endless circulation of frames over the loop. This network loop would result in network overload. To prevent this from happening, the IEEE has defined the spanning-tree algorithm (STA) in IEEE 802.1d, which detects loops and disables one of the parallel paths. The STA might also be used to build fault-tolerant networks, because if the chosen path becomes invalid due to a cable/bridge/switch fault and an alternative path exists, the alternative path is enabled automatically.

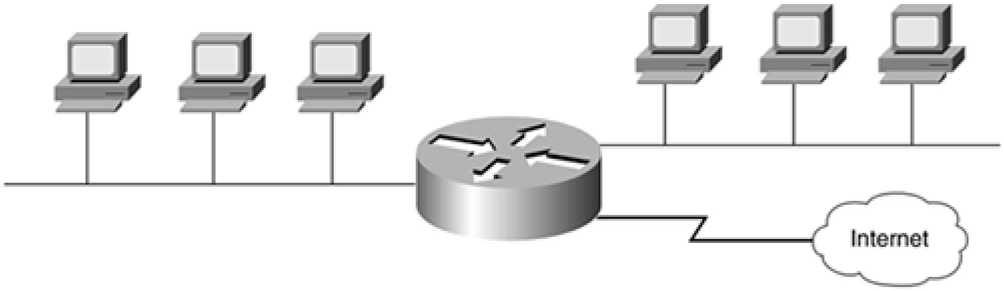
Switches address OSI model Layer 2 (data link) networks, moving frames around based on the hardware, or MAC, address, but switches are limited in their use in that they are LAN devices. Switches do not provide wide-area network (WAN) connectivity. To connect your LAN to another LAN through some outside network, such as the Internet or corporate WAN, a router is needed.

Routers - Layer 3 Devices

Routers are devices that forward data packets from one LAN or WAN to another. Based on routing tables and routing protocols, routers read the network address in the packet contained within each transmitted frame. Routers then select a sending method for the packet based on the most expedient route. This most expedient route is determined by factors such as traffic load, line quality, and available bandwidth. Routers work at Layer 3 (network) in the protocol stack, whereas bridges and switches work at Layer 2 (data link).

Routers segment LANs to balance traffic within workgroups and to filter traffic for security purposes and policy management. Routers also can be used at the edge of the network to connect remote offices, across WANs or the Internet, as illustrated in Figure 5-15.

Figure 5-15. Router Connecting Two LANs to the Internet



View full size image

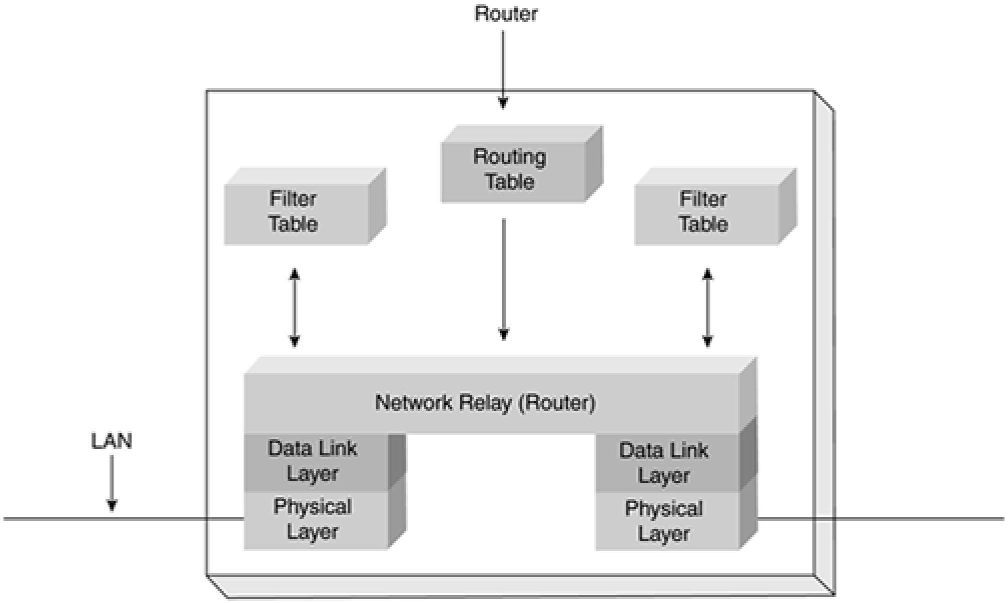
Because routers must examine the network address in the packet, they do more processing and add more overhead than bridges and switches, which both work at the data link (MAC) layer.

Router Operation

A router is essentially a computer with two or more NICs supporting a network protocol, such as the Internet Protocol (IP). The router receives packets from each network interface and forwards these received packets to an appropriate output network interface. Received packets have all data link layer (OSI Layer 2) protocol headers removed, and transmitted packets have a new link protocol header added before transmission.

The router uses the information held in the network layer header, such as an IP address, to decide whether to forward each received packet, and which network interface to use to send the packet. Most packets are forwarded based on the packet's network destination address, along with routing information held within the router in a routing table, as illustrated in Figure 5-16.

Figure 5-16. Router Architecture



View full size image

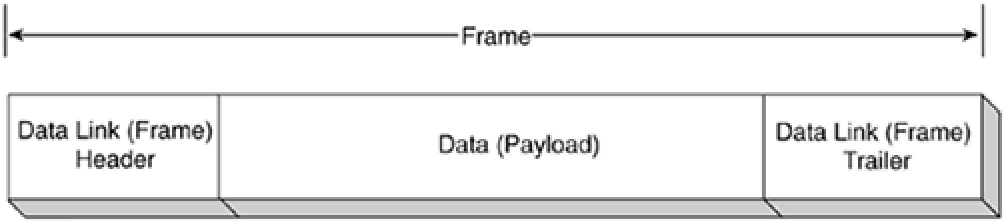
The routing and filter tables found in a router are similar to the tables used by bridges and switches. The difference between routing and switching tables is that instead of specifying link hardware (MAC) addresses, the router table specifies network addresses. The routing table lists known IP destination addresses with the appropriate network interface used to reach that destination. A default entry is used for all addresses not explicitly defined in the table, such as packets destined for the Internet. It's more manageable to have a single entry in the table for the Internet than to have an entry for each Internet site you might visit.

How a Switch Works

Frames Revisited

Frames carry data across the network and are made up of three parts: the header, the data itself (payload), and the trailer, as illustrated in the Figure 6-1.

Figure 6-1. Complete Frame (Header, Data/Payload, Trailer)



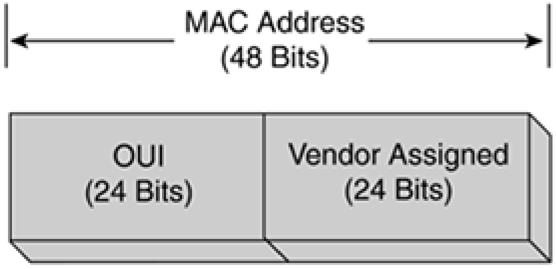
View full size image

These three frame components - the header, data, and trailer - combine in making up a complete frame. The header identifies the destination data-link address of the frame, the payload is data from upper-layer protocols (such as packets from the network layer), and the trailer signifies the end of the frame.

MAC address (Media Access Control address or physical address) is the unique serial number burned into network adapters that differentiates that network card from all others on the network. To be a part of any network, you must have an address so that others can reach you. There are two types of addresses found in a network: the logical network address and the physical data-link address. In LAN bridging and switching environments, you are concerned with the physical address (MAC address), and the MAC address is found in the frame header.

A MAC address is the physical address of the device and is 48 bits (6 bytes) long. It is made up of two parts: the organizational unique identifier (OUI) and the vendor-assigned address, as illustrated in Figure 6-2.

Figure 6-2. MAC Address



Recall that the MAC address on a computer might look like this: 00-06-0f-08-b4-12. This MAC address is used for the Fast Ethernet adapter on the computer in question - the OUI is 00-06-0f, and the vendor-assigned number is 08-b4-12.

Transmission Methods

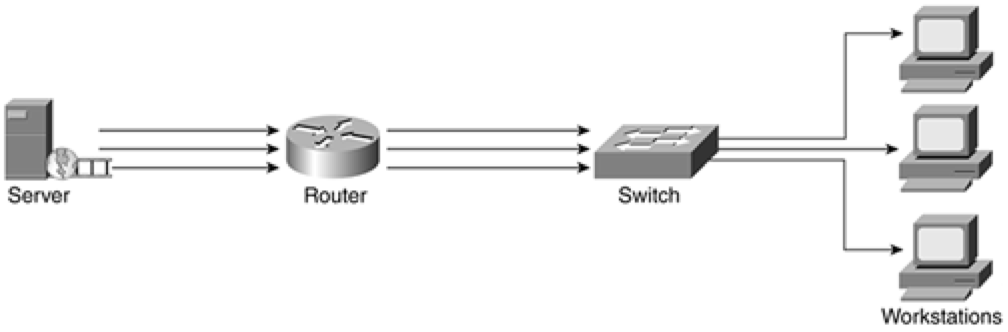
LAN data transmissions at Layer 2 fall into three classifications: unicast, multicast, and broadcast. In each type of transmission, a single frame is sent to one node on the network. If the frame is to be sent to more than one node on the network, the sender must send individual unicast data streams to each node.

In a unicast transmission, a single frame or packet is sent from a single source to a single destination on a network. In a multicast transmission environment, a single data frame or a single source to multiple destinations packet is copied and sent to a specific subset of nodes on the network. In a broadcast transmission environment from a single source to all nodes, a single data frame or packet is copied and sent to all nodes on the network.

Unicast

Unicast is a one-to-one transmission method in which the network carries a message to one receiver, such as from a server to a LAN workstation. In a unicast environment, even though multiple users might ask for the same information from the same server at the same time, such as a video clip, duplicate data streams are sent. One stream is sent to each user, as illustrated in the Figure 6-3.

Figure 6-3. Unicast Operation



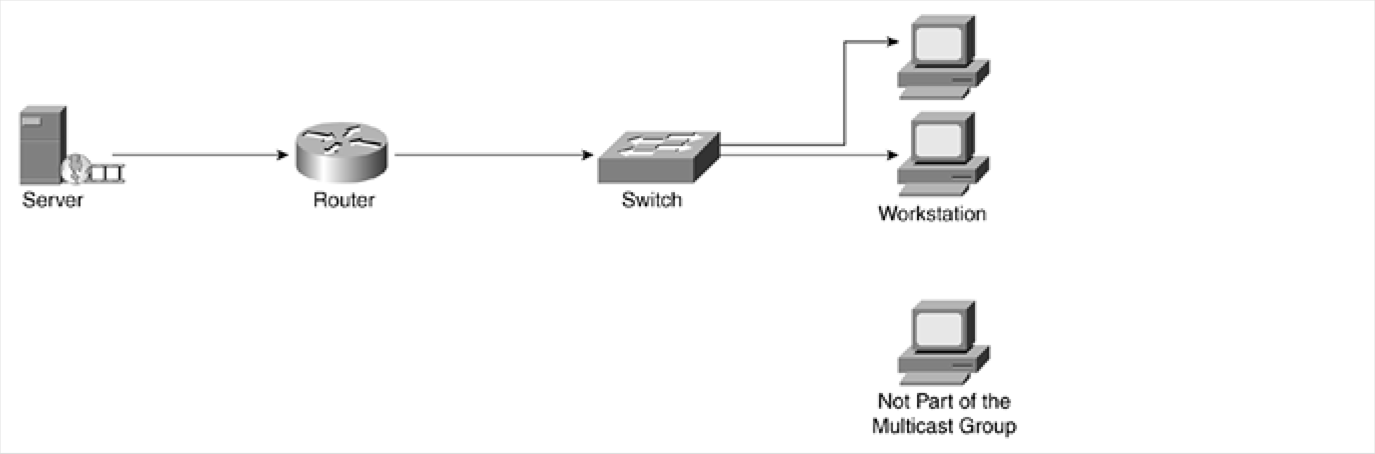
View full size image

Unicast sends separate data streams to each computer requesting the data, in turn flooding the network with traffic. Unicast might be compared to an after-work gathering. You and several of your co-workers might be going to the same destination, but each taking his own vehicle, flooding the streets with cars. (So the next time you go to an after-work gathering, and each person drives his own car, tell them you're "unicasting.")

Multicast

Multicast is a one-to-many transmission method in which the network carries a message to multiple receivers at the same time. Multicast is similar to broadcasting, except that multicasting means sending to a specific group, whereas broadcasting implies sending to everybody, whether they want the traffic or not. When sending large amounts of data, multicast saves considerable network bandwidth because the bulk of the data is sent only once. The data travels from its source through major backbones and is then multiplied, or distributed out, at switching points closer to the end users (see Figure 6-4) . This is more efficient than a unicast system, in which the data is copied and forwarded to each recipient.

Figure 6-4. Multicast Operation



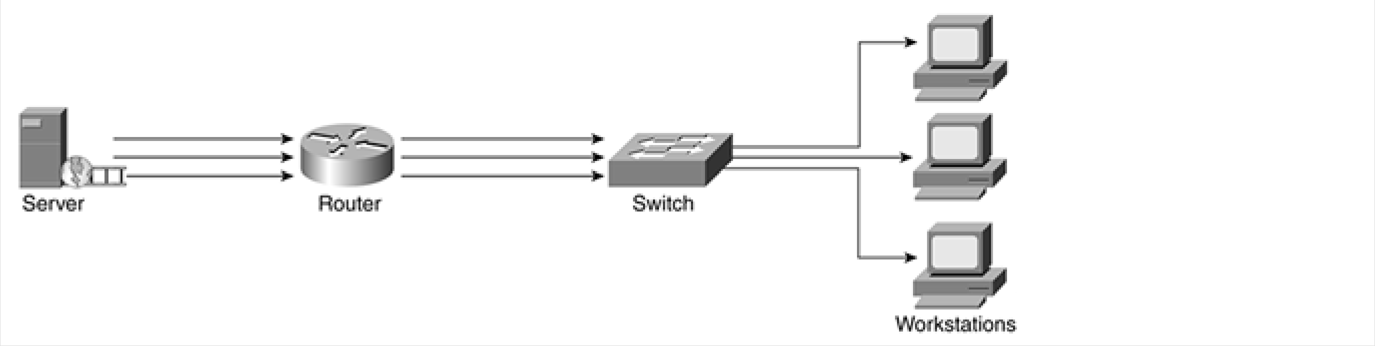
View full size image

Multicast conserves network bandwidth by sending a single data stream across the network, much as you and others might carpool to and from work, thereby reducing the traffic on the roads. For example, a few of you might ride together to some point, such as a drop-off point in the city, and then disperse from there. Multicasting works in the same way by using the concept of shared transmission across a network. Multicasting sends the data to a predetermined endpoint, such as a switch, where the traffic is sent to each intended recipient, instead of each traffic stream being sent from start to finish across the network, independent of others.

Broadcast

Broadcast is a one-to-all transmission method in which the network carries a message to all devices at the same time, as illustrated in Figure 6-5.

Figure 6-5. Broadcast Operation



View full size image

Broadcast message traffic is sent out to every node on the network where the broadcast is not filtered or blocked by a router. Broadcasts are issued by the Address Resolution Protocol (ARP) for address resolution when the location of a user or server is not known. For example, the location could be unknown when a network client or server first joins the network and identifies itself. Sometimes broadcasts are a result of network devices continually announcing their presence in the network, so that other devices don't forget who is still a part of the network. Regardless of the reason for a broadcast, the broadcast must reach all possible stations that might potentially respond.

Frame Size

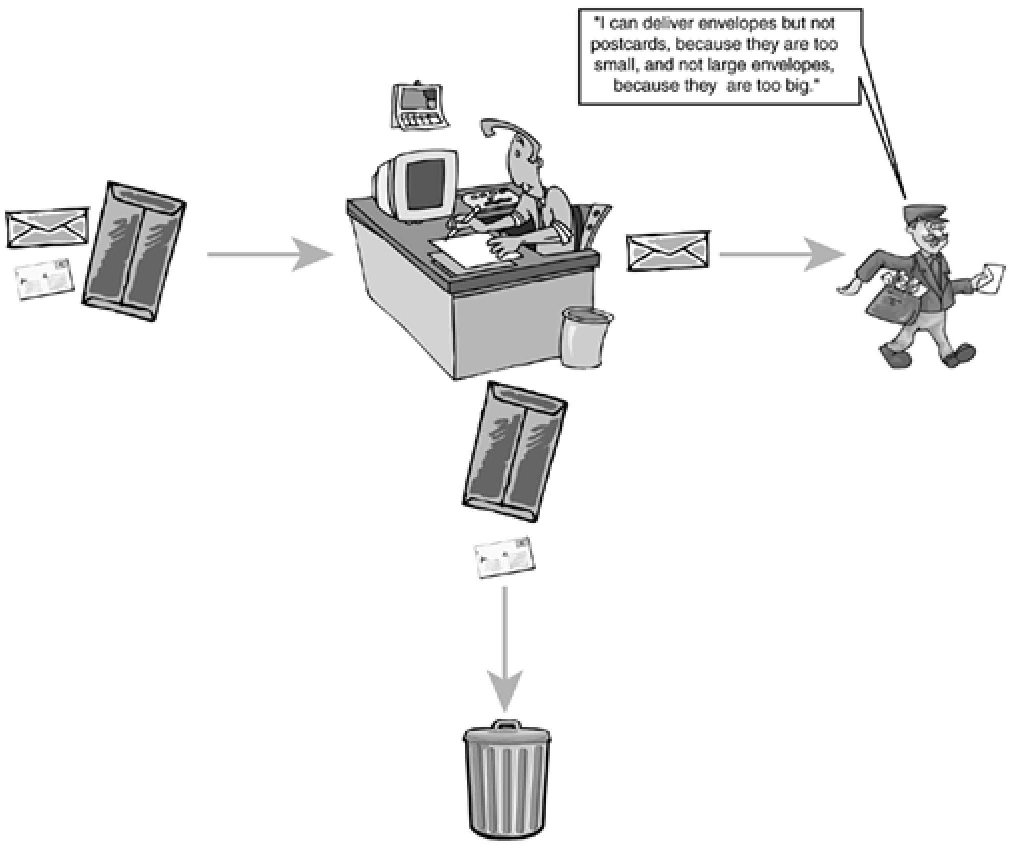
Frame size is measured in bytes and has a minimum and maximum length, depending on the implemented technology. For example, the minimum frame size for an Ethernet LAN is 64 bytes with a 4-byte cyclic redundancy check (CRC), and the maximum frame size is 1518 bytes. The minimum/maximum for a Token Ring LAN is 32 bytes/16 kilobytes (KB), respectively.

Why is it important to know the minimum and maximum frame sizes your network can support? Knowing the sizes enables you to ensure that your users' message traffic gets to where it needs to go quickly and accurately.

Suppose your corporate mailroom is equipped only to handle letter- and business-sized envelopes and is not equipped to handle postcards or larger legal-sized envelopes. The letter-sized envelope is the minimum size, and the business-sized envelope is the maximum sized "frame" allowed by your mailroom. Anything smaller than the letter-sized envelope, such as a postcard, might be considered a runt, and anything larger than the business-sized envelope might be considered a giant.

Figure 6-6 illustrates the concept of a minimum and maximum frame size, and the result, in a corporate mailroom. (Let's hope this doesn't really happen, although it might explain a few missing pieces of mail.)

Figure 6-6. Mailroom in Action


"I can deliver envelopes but not postcards, because they are too small, and not large envelopes, because they are too big."

View full size image

In this mailroom (switch) scenario, both the postcards (runts) and legal-sized envelopes (giants) would not be accepted by the mailroom (the switch) and therefore would be dropped into the trash.

The maximum frame size is also known as the maximum transmission unit, or MTU. When a frame is larger than the MTU, it is broken down, or fragmented, into smaller pieces by the Layer 3 protocol to accommodate the MTU of the network.

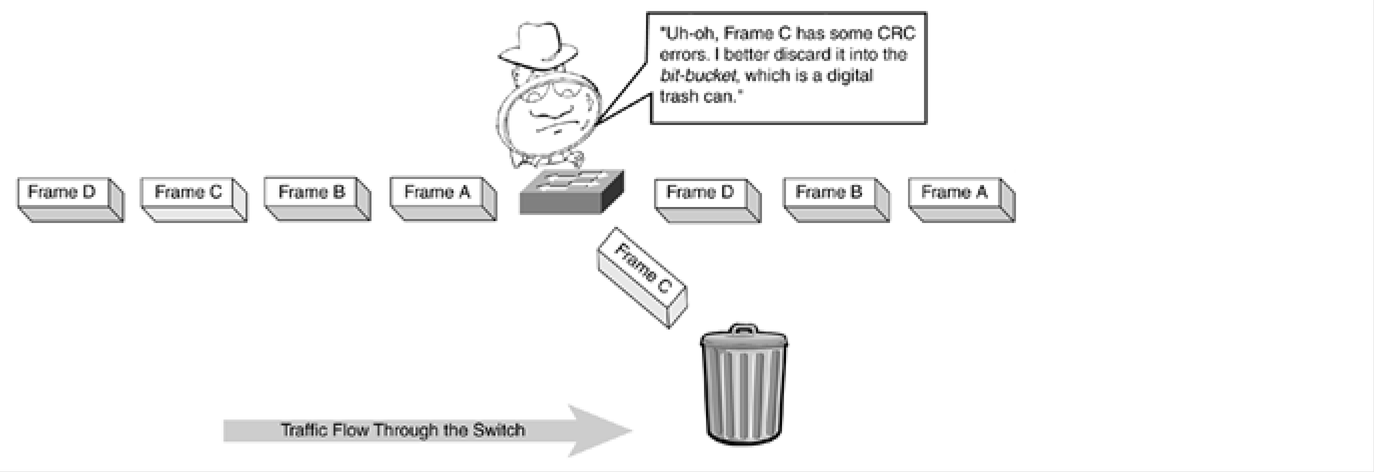
Layer 2 Switching Methods

LAN switches are characterized by the forwarding method that they support, such as a store-and-forward switch, cut-through switch, or fragment-free switch. In the store-and-forward switching method, error checking is performed against the frame, and any frame with errors is discarded. With the cut-through switching method, no error checking is performed against the frame, which makes forwarding the frame through the switch faster than store-and-forward switches.

Store-and-Forward Switching

Store-and-forward switching means that the LAN switch copies each complete frame into the switch memory buffers and computes a cyclic redundancy check (CRC) for errors. CRC is an error-checking method that uses a mathematical formula, based on the number of bits (1s) in the frame, to determine whether the received frame is errored. If a CRC error is found, the frame is discarded. If the frame is error free, the switch forwards the frame out the appropriate interface port, as illustrated in Figure 6-7.

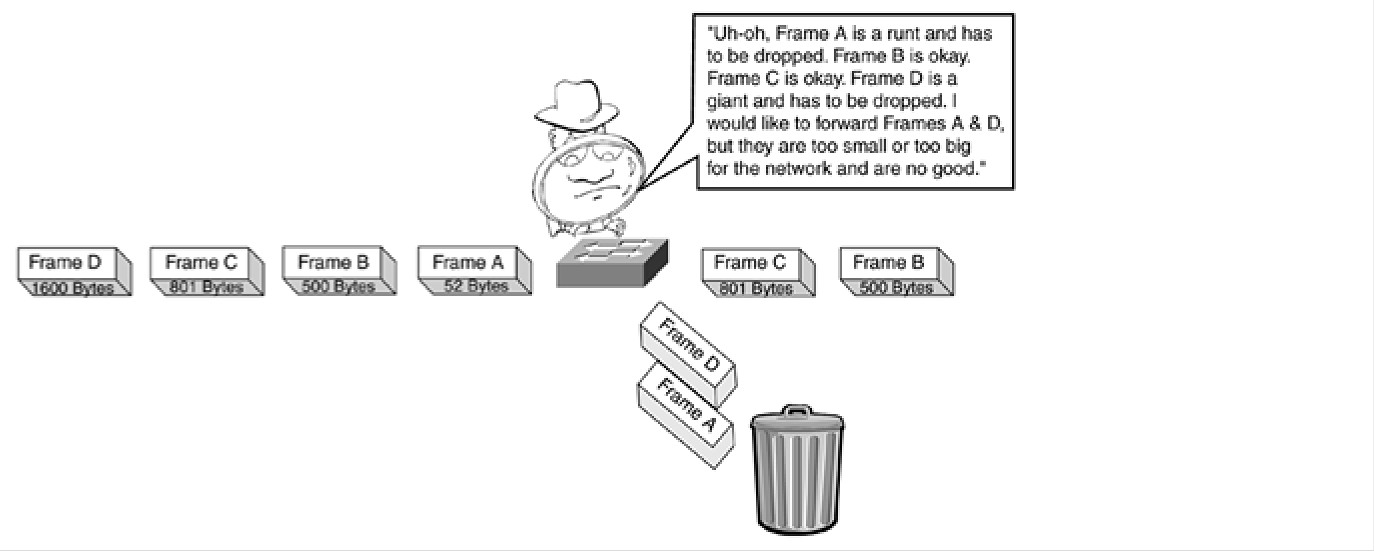
Figure 6-7. Store-and-Forward Switch Discarding a Frame with a Bad CRC


"Uh-oh, Frame C has some CRC errors. I better discard it into the *bit-bucket*, which is a digital trash can."
Frame D
Frame C
Frame B
Frame A
Frame D
Frame B
Frame A
Frame C
Traffic Flow Through the Switch

View full size image

An Ethernet frame is discarded if it is smaller than 64 bytes in length, a runt, or if the frame is larger than 1518 bytes in length, a giant, as illustrated in Figure 6-8.

Figure 6-8. Runts and Giants in the Switch


"Uh-oh, Frame A is a runt and has to be dropped. Frame B is okay. Frame C is okay. Frame D is a giant and has to be dropped. I would like to forward Frames A & D, but they are too small or too big for the network and are no good."
Frame D 1600 Bytes
Frame C 801 Bytes
Frame B 500 Bytes
Frame A 52 Bytes
Frame C 801 Bytes
Frame B 500 Bytes
Frame D
Frame A

View full size image

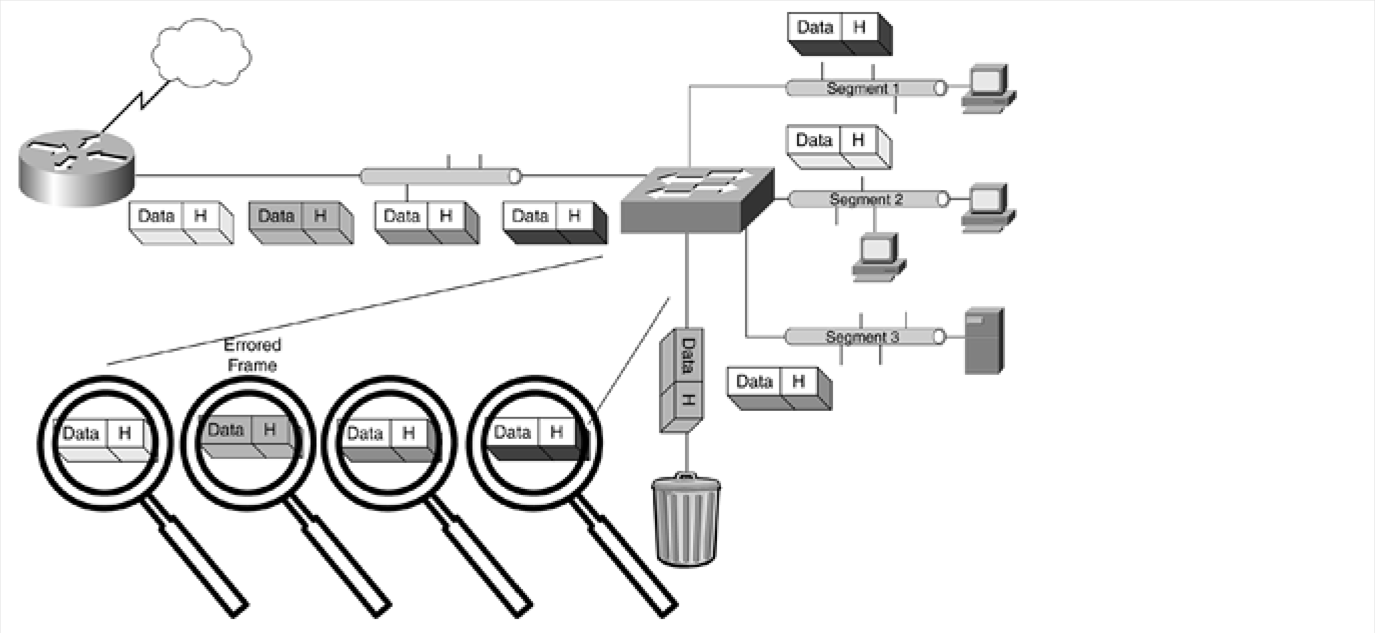
Some switches can be configured to carry giant, or jumbo, frames.

If the frame does not contain any errors, and is not a runt or a giant, 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 intended destination.

Store-and-Forward Switching Operation

Store-and-forward switches store the entire frame in internal memory and check the frame for errors before forwarding the frame to its destination. Store-and-forward switch operation ensures a high level of error-free network traffic, because bad data frames are discarded rather than forwarded across the network, as illustrated in Figure 6-9.

Figure 6-9. Store-and-Forward Switch Examining Each Frame for Errors Before Forwarding to Destination Network Segment



View full size image

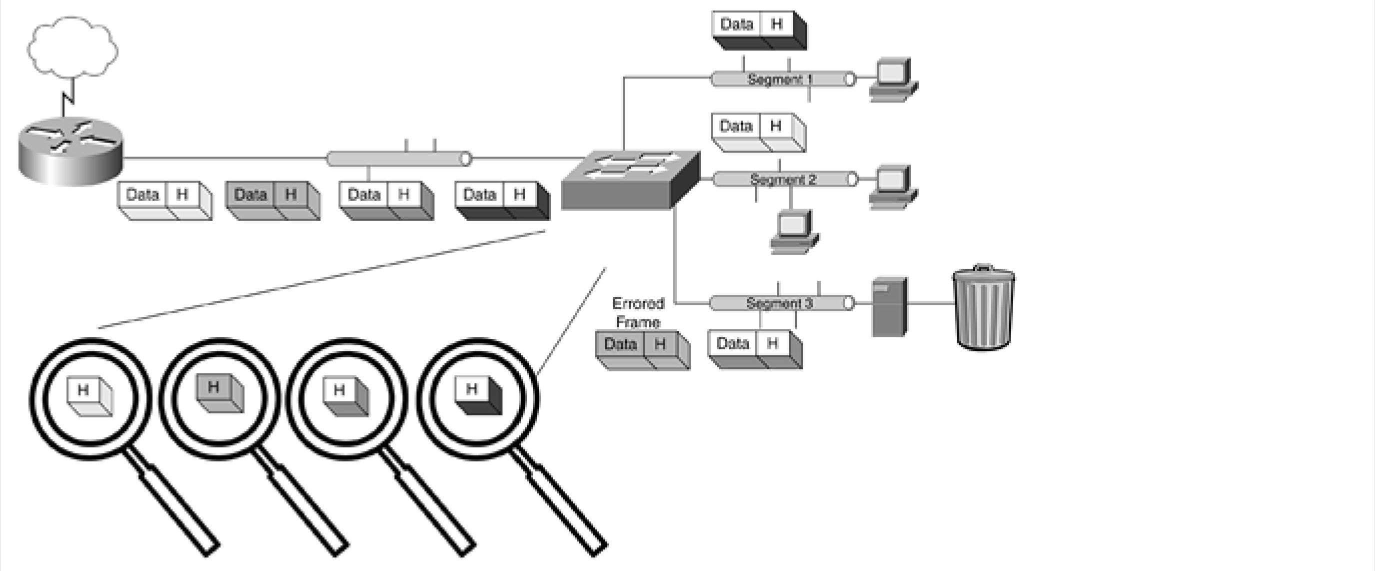
The store-and-forward switch shown in Figure 6-9 inspects each received frame for errors before forwarding it on to the frame's destination network segment. If a frame fails this inspection, the switch drops the frame from its buffers, and the frame is thrown in to the proverbial bit bucket.

A drawback to the store-and-forward switching method is one of performance, because the switch has to store the entire data frame before checking for errors and forwarding. This error checking results in high switch latency (delay). If multiple switches are connected, with the data being checked at each switch point, total network performance can suffer as a result. Another drawback to store-and-forward switching is that the switch requires more memory and processor (central processing unit, CPU) cycles to perform the detailed inspection of each frame than that of cut-through or fragment-free switching.

Cut-Through Switching

With cut-through switching, the LAN switch copies into its memory only the destination MAC address, which is located in the first 6 bytes of the frame following the preamble. The switch looks up the destination MAC address in its switching table, determines the outgoing interface port, and forwards the frame on to its destination through the designated switch port. A cut-through switch reduces delay because the switch begins to forward the frame as soon as it reads the destination MAC address and determines the outgoing switch port, as illustrated in Figure 6-10.

Figure 6-10. Cut-Through Switch Examining Each Frame Header Before Forwarding to Destination Network Segment



View full size image

The cut-through switch shown in Figure 6-10 inspects each received frame's header to determine the destination before forwarding on to the frame's destination network segment. Frames with and without errors are forwarded in cut-through switching operations, leaving the error detection of the frame to the intended recipient. If the receiving switch determines the frame is errored, the frame is thrown out to the bit bucket where the frame is subsequently discarded from the network.

Cut-through switching was developed to reduce the delay in the switch processing frames as they arrive at the switch and are forwarded on to the destination switch port. The switch pulls the frame header into its port buffer. When the destination MAC address is determined by the switch, the switch forwards the frame out the correct interface port to the frame's intended destination.

Cut-through switching reduces latency inside the switch. If the frame was corrupted in transit, however, the switch still forwards the bad frame. The destination receives this bad frame, checks the frame's CRC, and discards it, forcing the source to resend the frame. This process wastes bandwidth and, if it occurs too often, network users experience a significant slowdown on the network. In contrast, store-and-forward switching prevents errored frames from being forwarded across the network and provides for quality of service (QoS) managing network traffic flow.

Cut-Through Switching Operation

Cut-through switches do not perform any error checking of the frame because the switch looks only for the frame's destination MAC address and forwards the frame out the appropriate switch port. Cut-through switching results in low switch latency. The drawback, however, is that bad data frames, as well as good frames, are sent to their destinations. At first blush, this might not sound bad because most network cards do their own frame checking by default to ensure good data is received. You might find that if your network is broken down into workgroups, the likelihood of bad frames or collisions might be minimized, in turn making cut-through switching a good choice for your network.

Fragment-Free Switching

Fragment-free switching is also known as runtless switching and is a hybrid of cut-through and store-and-forward switching. Fragment-free switching was developed to solve the late-collision problem.

When two systems' transmissions occur at the same time, the result is a collision. Collisions are a part of Ethernet communications and do not imply any error condition. A late collision is similar to an Ethernet collision, except that it occurs after all hosts on the network should have been able to notice that a host was already transmitting.

A late collision indicates that another system attempted to transmit after a host has transmitted at least the first 60 bytes of its frame. Late collisions are often caused by an Ethernet LAN being too large and therefore needing to be segmented. Late collisions can also be caused by faulty network devices on the segment and duplex (for example, half-duplex/full-duplex) mismatches between connected devices.

Fragment-Free Switching Operation

Fragment-free switching works like cut-through switching with the exception that a switch in fragment-free mode stores the first 64 bytes of the frame before forwarding. Fragment-free switching can be viewed as a compromise between store-and-forward switching and cut-through switching. The reason fragment-free switching stores only the first 64 bytes of the frame is that most network errors and collisions occur during the first 64 bytes of a frame.

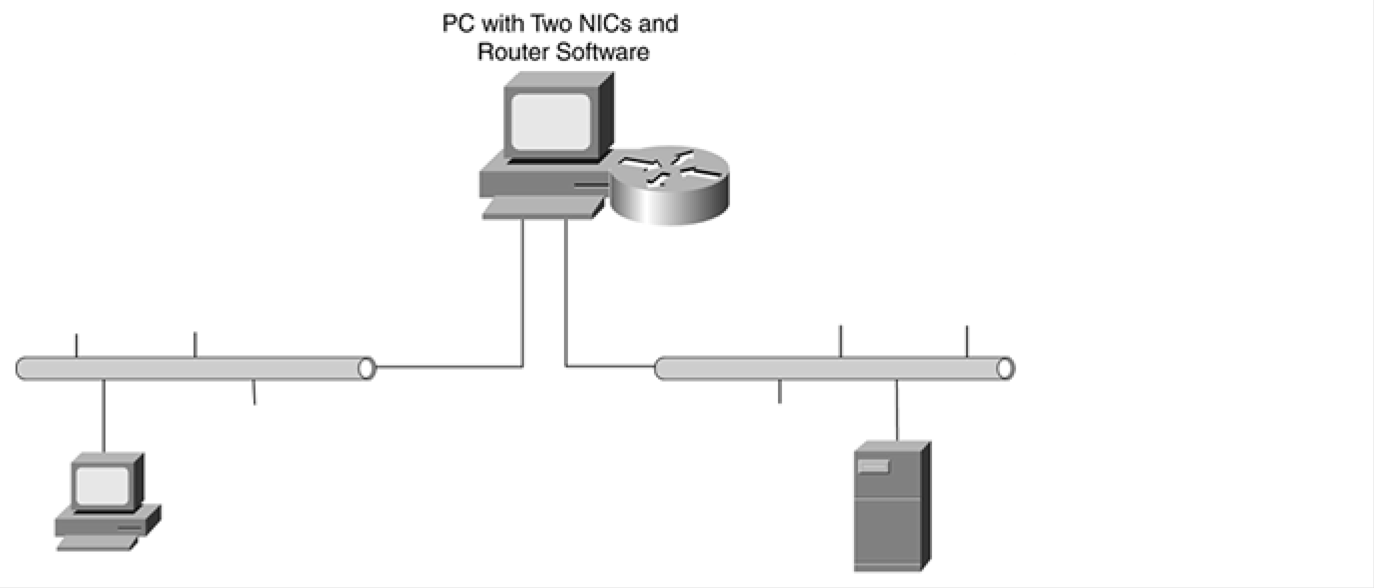
Different methods work better at different points in the network. For example, cut-through switching is best for the network core where errors are fewer, and speed is of utmost importance. Store-and-forward is best at the network access layer where most network problems and users are located.

Layer 3 Switching

Layer 3 switching is another example of fragment-free switching. Up to now, this discussion has concentrated on switching and bridging at the data link layer (Layer 2) of the Open System Interconnection (OSI) model. When bridge technology was first developed, it was not practical to build wire-speed bridges with large numbers of high-speed ports because of the manufacturing cost involved. With improved technology, many functions previously implemented in software were moved into the hardware, increasing performance and enabling manufacturers to build reasonably priced wire-speed switches.

Whereas bridges and switches work at the data link layer (OSI Layer 2), routers work at the network layer (OSI Layer 3). Routers provide functionality beyond that offered by bridges or switches. As a result, however, routers entail greater complexity. Like early bridges, routers were often implemented in software, running on a special-purpose processing platform, such as a personal computer (PC) with two network interface cards (NICs) and software to route data between each NIC, as illustrated in Figure 6-11.

Figure 6-11. PC Routing with Two NICs



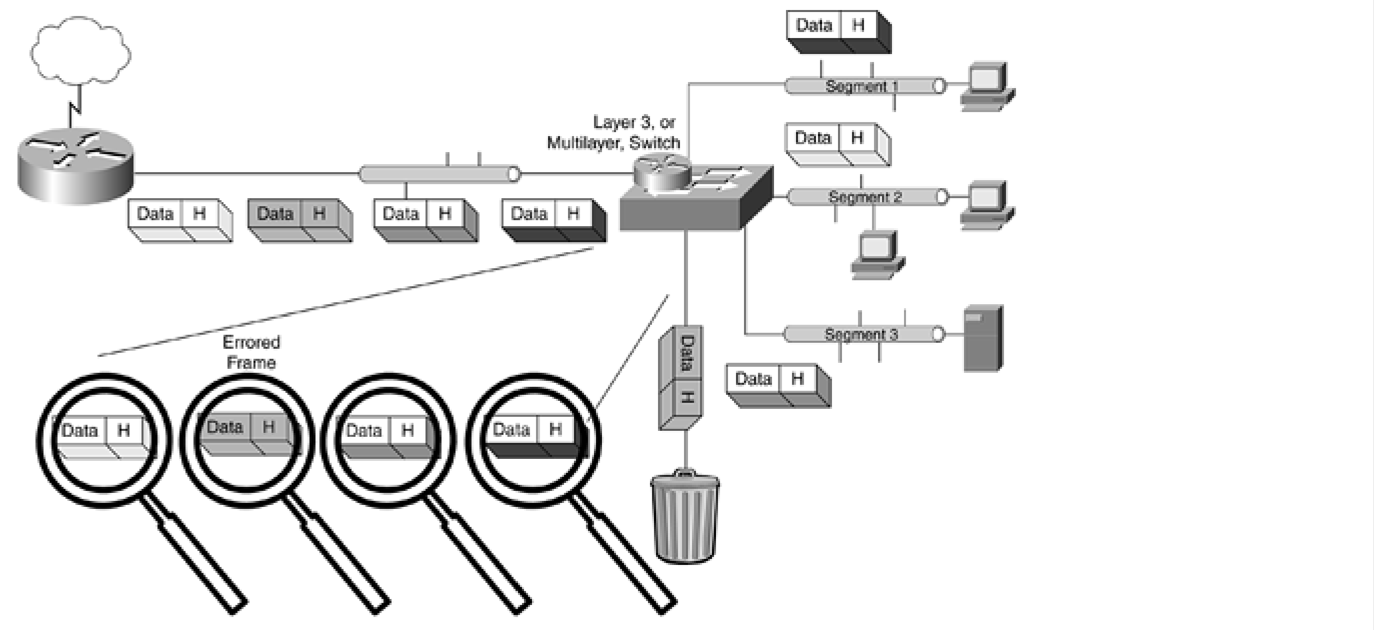
View full size image

The early days of routing involved a computer and two NIC cards, not unlike two people having a conversation, but having to go through a third person to do so. The workstation would send its traffic across the wire, and the routing computer would receive it on one NIC, determine that the traffic would have to be sent out the other NIC, and then resend the traffic out this other NIC.

In the same way that a Layer 2 switch is another name for a bridge, a Layer 3 switch is another name for a router. This is not to say that a Layer 3 switch and a router operate the same way. Layer 3 switches make decisions based on the port-level Internet Protocol (IP) addresses, whereas routers make decisions based on a map of the Layer 3 network (maintained in a routing table).

Multilayer switching is a switching technique that switches at both the data link (OSI Layer 2) and network (OSI Layer 3) layers. To enable multilayer switching, LAN switches must use store-and-forward techniques because the switch must receive the entire frame before it performs any protocol layer operations, as illustrated in Figure 6-12.

Figure 6-12. Layer 3 (Multilayer) Switch Examining Each Frame for Error Before Determining the Destination Network Segment (Based on the Network Address)



View full size image

Similar to a store-and-forward switch, with multilayer switching the switch pulls the entire received frame into its memory and calculates its CRC. It then determines whether the frame is good or bad. If the CRC calculated on the packet matches the CRC calculated by the switch, the destination address is read and the frame is forwarded out the correct switch port. If the CRC does not match the frame, the frame is discarded. Because this type of switching waits for the entire frame to be received before forwarding, port latency times can become high, which can result in some latency, or delay, of network traffic.

Layer 3 Switching Operation

You might be asking yourself, "What's the difference between a Layer 3 switch and a router?" The fundamental difference between a Layer 3 switch and a router is that Layer 3 switches have optimized hardware passing data traffic as fast as Layer 2 switches. However, Layer 3 switches make decisions regarding how to transmit traffic at Layer 3, just as a router does.

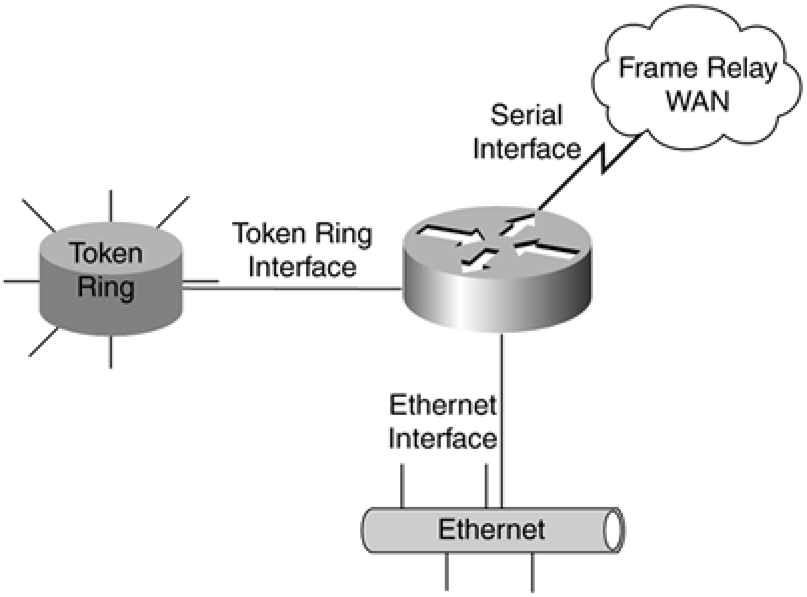
Within the LAN environment, a Layer 3 switch is usually faster than a router because it is built on switching hardware. Bear in mind that the Layer 3 switch is not as versatile as a router, so do not discount the use of a router in your LAN without first examining your LAN requirements, such as the use of network address translation (NAT).

Before going forward with this discussion, recall the following points:

- A switch is a Layer 2 (data link) device with physical ports and that the switch communicates via frames that are placed on to the wire at Layer 1 (physical).
- A router is a Layer 3 (network) device that communicates with other routers with the use of packets, which in turn are encapsulated inside frames.

Routers have interfaces for connection into the network medium. For a router to route data over the Ethernet, for instance, the router requires an Ethernet interface, as illustrated in Figure 6-13.

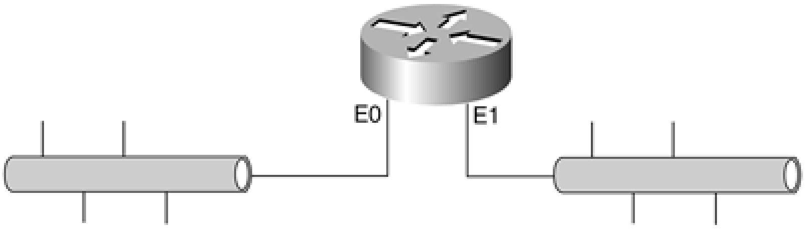
Figure 6-13. Router Interfaces



A serial interface is required for the router connecting to a wide-area network (WAN), and a Token Ring interface is required for the router connecting to a Token Ring network.

A simple network made up of two network segments and an internetworking device (in this case, a router) is shown in Figure 6-14.

Figure 6-14. Two-Segment Network with a Layer 3 Router



The router in Figure 6-14 has two Ethernet interfaces, labeled E0 and E1. The primary function of the router is determining the best network path in a complex network. A router has three ways to learn about networks and make the determination regarding the best path: through locally connected ports, static route entries, and dynamic routing protocols. The router uses this learned information to make a determination by using routing protocols. Some of the more common routing protocols used include Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Interior Gateway Routing Protocol (IGRP), and Border Gateway Protocol (BGP).

Routing protocols are used by routers to share information about the network. Routers receive and use the routing protocol information from other routers to learn about the state of the network. Routers can modify information received from one router by adding their own information along with the original information, and then forward that on to other routers. In this way, each router can share its version of the network.

Packet Switching

Layer 3 information is carried through the network in packets, and the transport method of carrying these packets is called packet switching, as illustrated in Figure 6-15.

Figure 6-15. Packet Switching Between Ethernet and Token Ring Network Segments

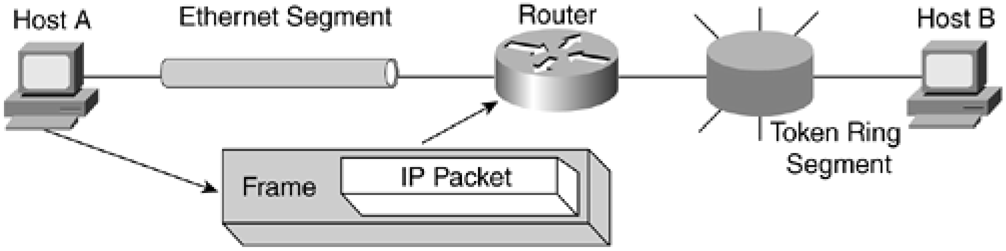


Figure 6-15 shows how a packet is delivered across multiple networks. Host A is on an Ethernet segment, and Host B on a Token Ring segment. Host A places an Ethernet frame, encapsulating an Internet Protocol (IP) packet, on to the wire for transmission across the network.

The Ethernet frame contains a source data link layer MAC address and a destination data link layer MAC address. The IP packet within the frame contains a source network layer IP address (TCP/IP network layer address) and a destination network layer IP address. The router maintains a routing table of network paths it has learned, and the router examines the network layer destination IP address of the packet. When the router has determined the destination network from the destination IP address, the router examines the routing table and determines whether a path exists to that network.

In the case illustrated in Figure 6-15, Host B is on a Token Ring network segment directly connected to the router. The router peels off the Layer 2 Ethernet encapsulation, forwards the Layer 3 data packet, and then re-encapsulates the packet inside a new Token Ring frame. The router sends this frame out its Token Ring interface on to the segment where Host B will see a Token Ring frame containing its MAC address and process it.

Note the original frame was Ethernet, and the final frame is Token Ring encapsulating an IP packet. This is called media transition and is one of the features of a network router. When the packet arrives on one interface and is forwarded to another, it is called Layer 3 switching or routing.

Routing Table Lookup

Routers (and Layer 3 switches) perform table lookups determining the next hop (next router or Layer 3 switch) along the route, which in turn determines the output port over which to forward the packet or frame. The router or Layer 3 switch makes this decision based on the network portion of the destination address in the received packet.

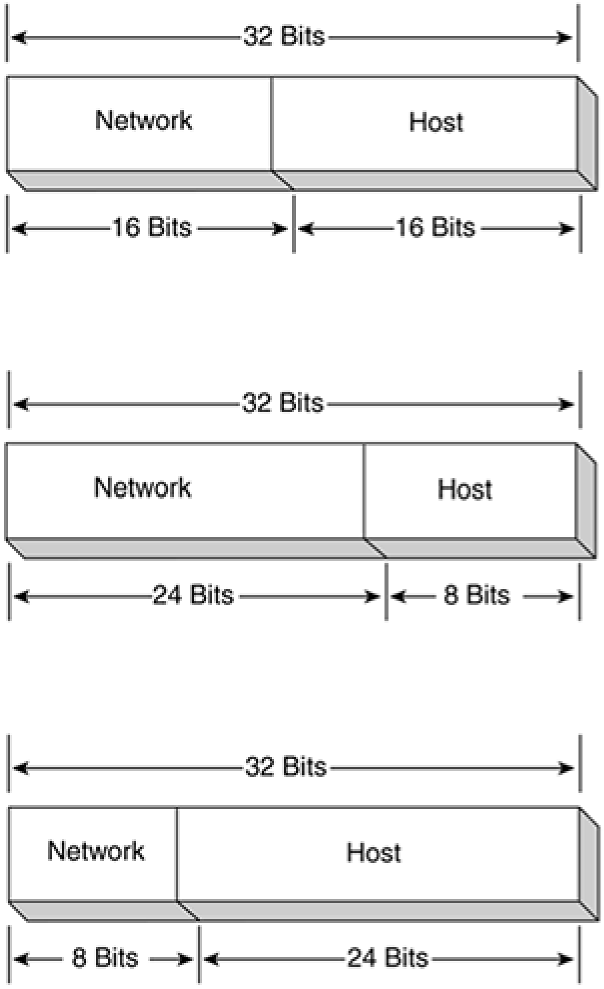
This lookup results in one of three actions:

- The destination network is not reachable - There is no path to the destination network and no default network. In this case, the packet is discarded.
- The destination network is reachable by forwarding the packet to another router - There is a match of the destination network against a known table entry, or to a default route if a method for reaching the destination network is unknown. The first lookup tells the next hop. Then a second lookup is performed to determine how to get to the next hop. Then a final determination of the exit port is reached. The first lookup can return multiple paths, so the port is not known until after the determination of how to get there is made. In either case, the lookup returns the network (Layer 3) address of the next-hop router, and the port through which that router can be reached.
- The destination network is known to be directly attached to the router - The port is directly attached to the network and reachable. For directly attached networks, the next step maps the host portion of the destination network address to the data link (MAC) address for the next hop or end node using the ARP table (for IP). It does not map the destination network address to the router interface. It needs to use the MAC of the final end node so that the node picks up the frame from the medium. Also, you are assuming IP when stating that the router uses the ARP table. Other Layer 3 protocols, such as Internetwork Packet Exchange (IPX), do not use ARP to map their addresses to MAC addresses.

Routing table lookup in an IP router might be considered more complex than a MAC address lookup for a bridge, because at the data link layer addresses are 48-bits in length, with fixed-length fields - the OUI and ID. Additionally, data-link address space is flat, meaning there is no hierarchy or dividing of addresses into smaller and distinct segments. MAC address lookup in a bridge entails searching for an exact match on a fixed-length field, whereas address lookup in a router looks for variable-length fields identifying the destination network.

IP addresses are 32 bits in length and are made up of two fields: the network identifier and the host identifier, as illustrated in Figure 6-16.

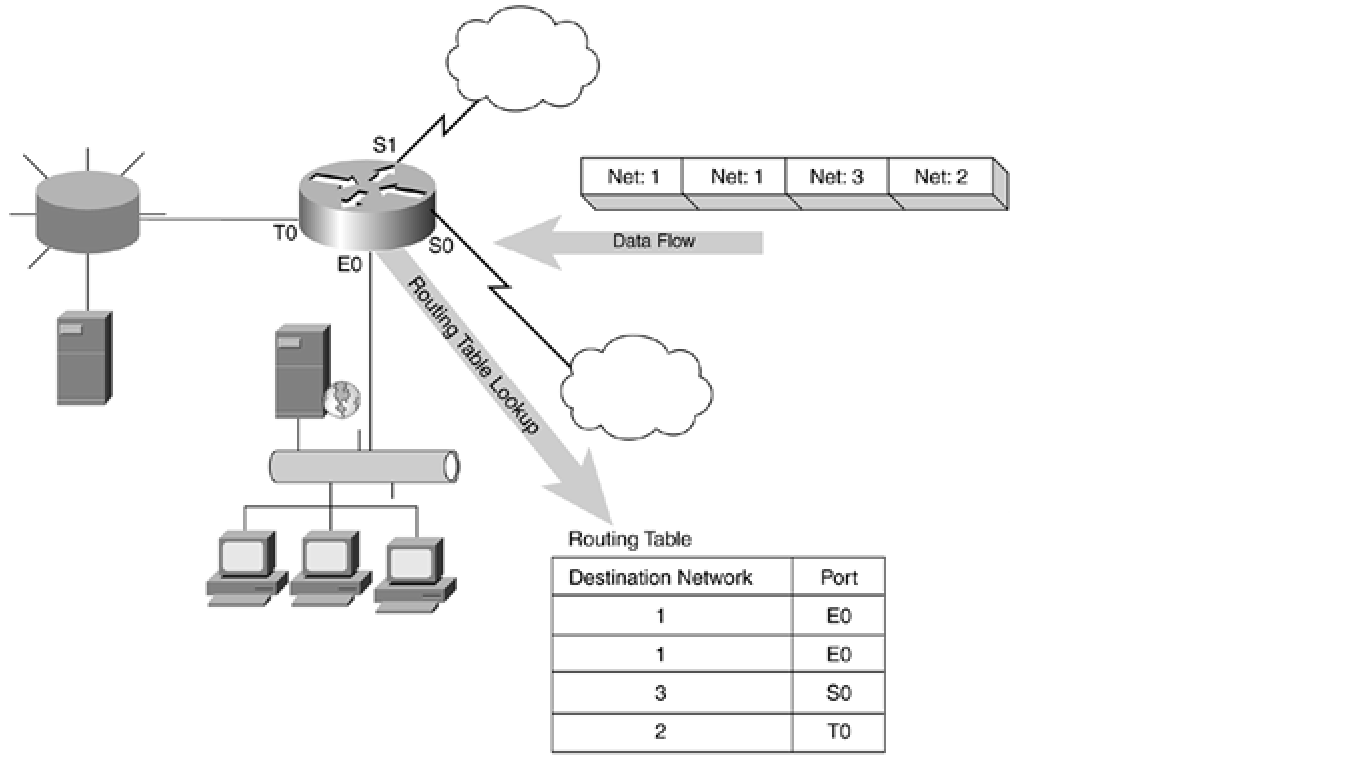
Figure 6-16. IP Address Space



Both the network and host portions of the IP address can be of a variable or fixed length, depending on the hierarchical network address scheme used. Discussion of this hierarchical, or subnetting, scheme is beyond the scope of this book, but suffice to say you are concerned with the fact that each IP address has a network and host identifier.

The routing table lookup in an IP router determines the next hop by examining the network portion of the IP address. After it determines the best match for the next hop, the router looks up the interface port to forward the packets across, as illustrated in Figure 6-17.

Figure 6-17. Routing Table Lookup Operation



Routing Table

Destination Network	Port
1	E0
1	E0
3	S0
2	T0

View full size image

Figure 6-17 shows that the router receives the traffic from Serial Port 1 (S1) and performs a routing table lookup determining from which port to forward out the traffic. Traffic destined for Network 1 is forwarded out the Ethernet 0 (E0) port. Traffic destined for Network 2 is forwarded out the Token Ring 0 (T0) port, and traffic destined for Network 3 is forwarded out Serial Port 0 (S0).

The host identifier portion of the network address is examined only if the network lookup indicates that the destination is on a locally attached network. Unlike data-link addresses, the dividing line between the network identifier and the host identifier is not in a fixed position throughout the network. Routing table entries can exist for network identifiers of various lengths, from 0 bits in length, specifying a default route, to 32 bits in length for host-specific routes. According to IP routing procedures, the lookup result returned should be the one corresponding to the entry that matches the maximum number of bits in the network identifier. Therefore, unlike a bridge, where the lookup is for an exact match against a fixed-length field, IP routing lookups imply a search for the longest match against a variable-length field.

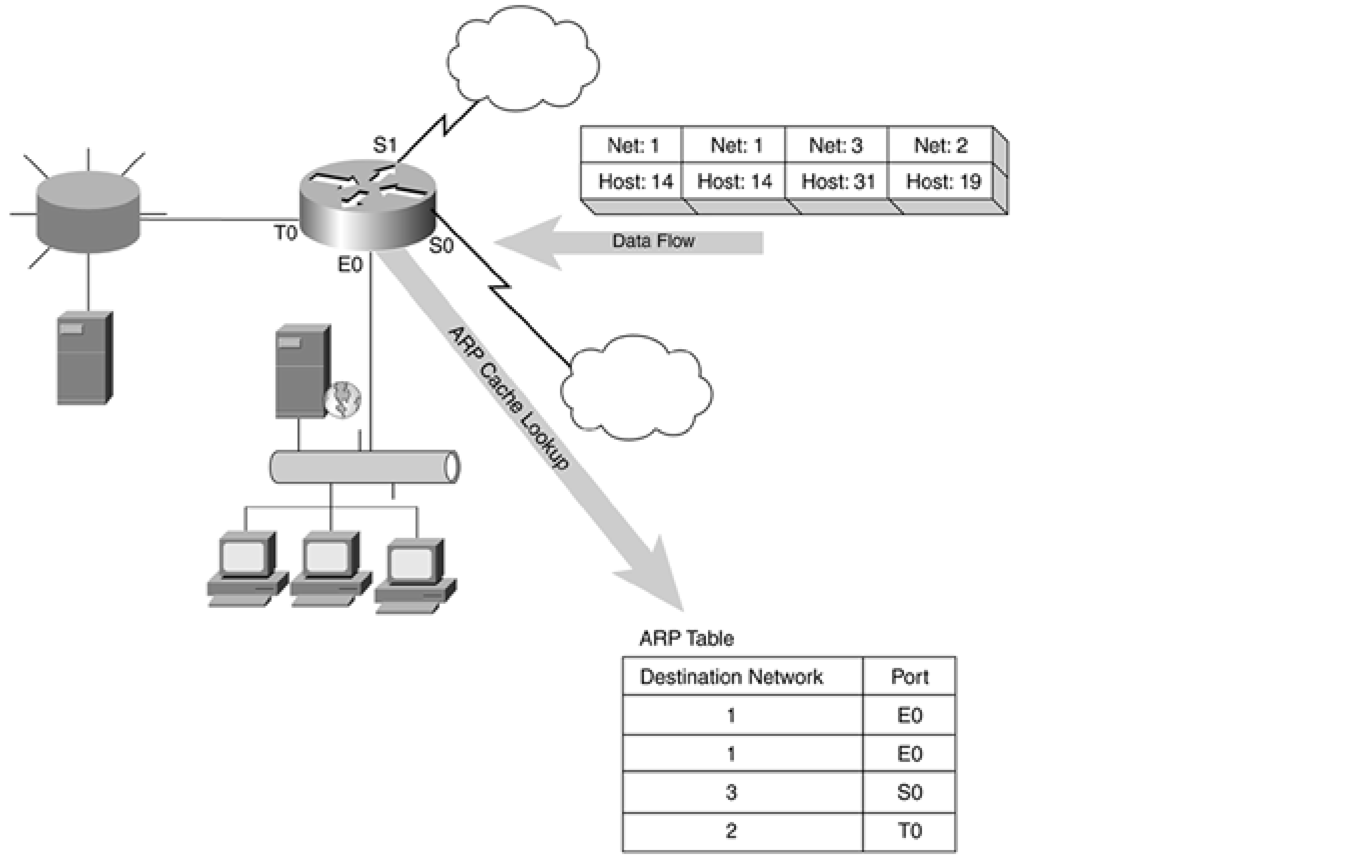
For example, a network host might have both the IP address of 68.98.134.209 and a MAC address of 00-0c-41-53-40-d3. The router makes decisions based on the IP address (68.98.134.209), whereas the switch makes decisions based on the MAC address (00-0c-41-53-40-d3). Both addresses identify the same host on the network, but are used by different network devices when forwarding traffic to this host.

ARP Mapping

Address Resolution Protocol (ARP) is a network layer protocol used in IP to convert IP addresses into MAC addresses. A network device looking to learn a MAC address broadcasts an ARP request onto the network. The host on the network that has the IP address in the request replies with its MAC (hardware) address. This is called ARP mapping, the mapping of a Layer 3 (network) address to a Layer 2 (data link) address.

Because the network layer address structure in IP does not provide for a simple mapping to data-link addresses, IP addresses use 32 bits, and data-link addresses use 48 bits. It is not possible to determine the 48-bit data-link address for a host from the host portion of the IP address. For packets destined for a host not on a locally attached network, the router performs a lookup for the next-hop router's MAC address. For packets destined for hosts on a locally attached network, the router performs a second lookup operation to find the destination address to use in the data-link header of the forwarded packet's frame, as illustrated in Figure 6-18.

Figure 6-18. Router ARP Cache Lookup



Destination Network	Port
1	E0
1	E0
3	S0
2	T0

View full size image

After determining for which directly attached network the packet is destined, the router looks up the destination MAC address in its ARP cache. Recall that ARP enables the router to determine the corresponding MAC address when it knows the network (IP) address. The router then forwards the packet across the local network in a frame with the MAC address of the local host, or next-hop router.

Note in Figure 6-18 that Net 3, Host: 31 is not part of the ARP cache, because during the routing table lookup, the router determined that this packet is to be forwarded to another, remote (nonlocally attached) network.

The result of this final lookup falls into one of the three following categories:

- The packet is destined for the router itself - The IP destination address (network and station portion combined) corresponds to one of the IP addresses of the router. In this case, the packet must be passed to the appropriate higher-layer entity within the router and not forwarded to any external port.
- The packet is destined for a known host on the directly attached network - This is the most common situation encountered by a network router. The router determines the mapping from the ARP table and forwards the packet out the appropriate interface port to the local network.
- The ARP mapping for the specified host is unknown - The router initiates a discovery procedure by sending an ARP request determining the mapping of network to hardware address. Because this discovery procedure takes time, albeit measured in milliseconds, the router might drop the packet that resulted in the discovery procedure in the first place. Under steady-state conditions, the router already has ARP mappings available for all communicating hosts. The address discovery procedure is necessary when a previously unheard-from host establishes a new communication session.

Fragmentation

Each output port on a network device has an associated maximum transmission unit (MTU). Recall from earlier in this chapter that the MTU indicates the largest frame size (measured in bytes) that can be carried on the interface. The MTU is often a function of the networking technology in use, such as Ethernet, Token Ring, or Point-to-Point Protocol (PPP). PPP is used with Internet connections. If the frame being forwarded is larger than the available space, as indicated by the MTU, the frame is fragmented into smaller pieces for transmission on the particular network.

Bridges cannot fragment frames when forwarding between LANs of differing MTU sizes because data-link connections rarely have a mechanism for fragment reassembly at the receiver. The mechanism is at the network layer implementation, such as with IP, which is capable of overcoming this limitation. Network layer packets can be broken down into smaller pieces if necessary so that these packets can travel across a link with a smaller MTU.

Fragmentation is similar to taking a picture and cutting it into pieces so that each piece will fit into differently sized envelopes for mailing. It is up to the sender to determine the size of the largest piece that can be sent, and it is up to the receiver to reassemble these pieces. Fragmentation is a mixed blessing; although it provides the means of communication across different link technologies, the processing accomplishing the fragmentation is significant and could be a burden on each device having to fragment and reassemble the data. Further, pieces for reassembly can be received out of order and may be dropped by the switch or router.

As a rule, it is best to avoid fragmentation in your network if at all possible. It is more efficient for the sending station to send packets not requiring fragmentation anywhere along the path to the destination, instead of sending large packets requiring intermediate routers to perform fragmentation.

Hosts and routers can learn the maximum MTU available along a network path through the use of MTU discovery. MTU discovery is a process by which each device in a network path learns the MTU size that the network path can support.