Introduction to Networking

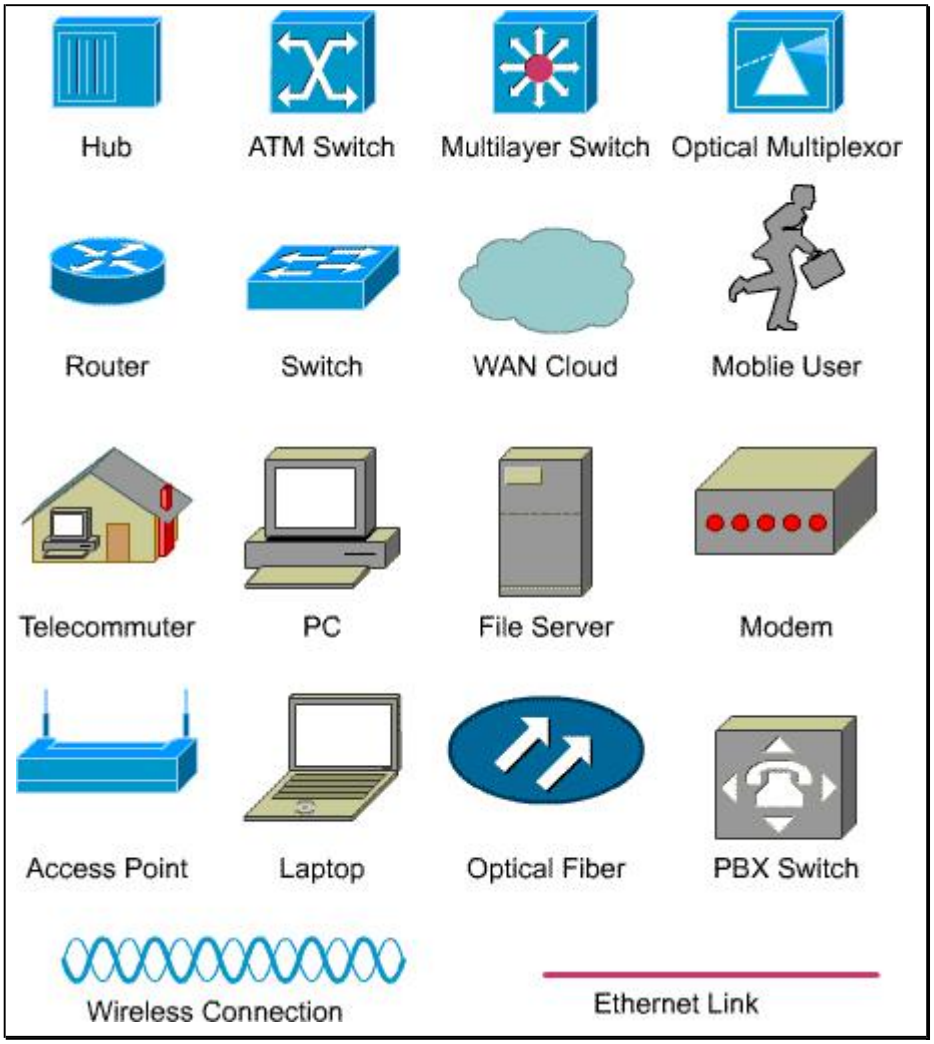
COMPUTER NETWORKING

Computer networking may be considered a branch of electrical engineering, electronics engineering, telecommunications, computer science, information technology or computer engineering, since it relies upon the theoretical and practical application of the related disciplines.

A computer network facilitates interpersonal communications allowing users to communicate efficiently and easily via various means: email, instant messaging, online chat, telephone, video telephone calls, and video conferencing. A network allows sharing of network and computing resources. Users may access and use resources provided by devices on the network, such as printing a document on a shared network printer or use of a shared storage device. A network allows sharing of files, data, and other types of information giving authorized users the ability to access information stored on other computers on the network.

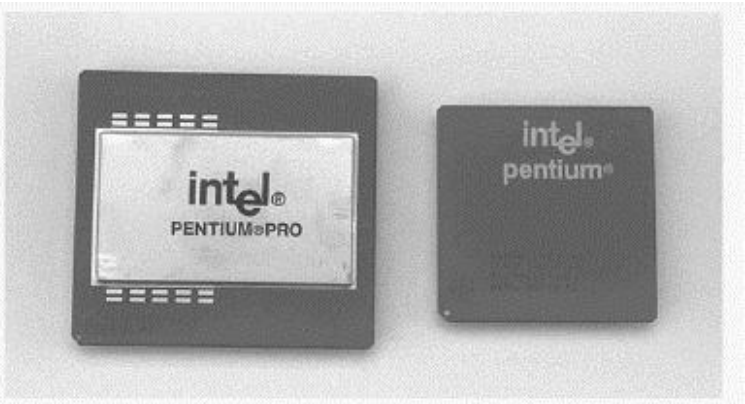
1. Icons andSymbols

Figure 1: Icons and Symbols



1.1 PCComponents

Figure 1: CPU



The CPU is a silicon-based microprocessor.

Figure 2: Expansion Slot

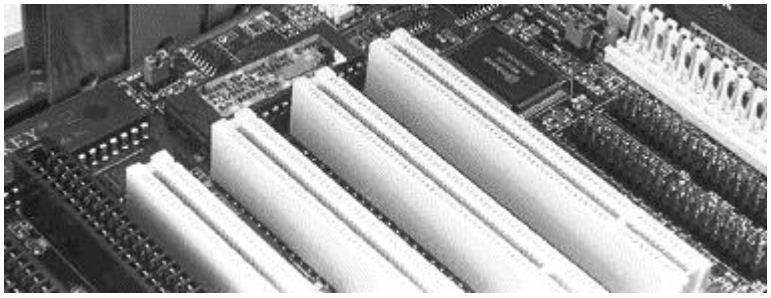
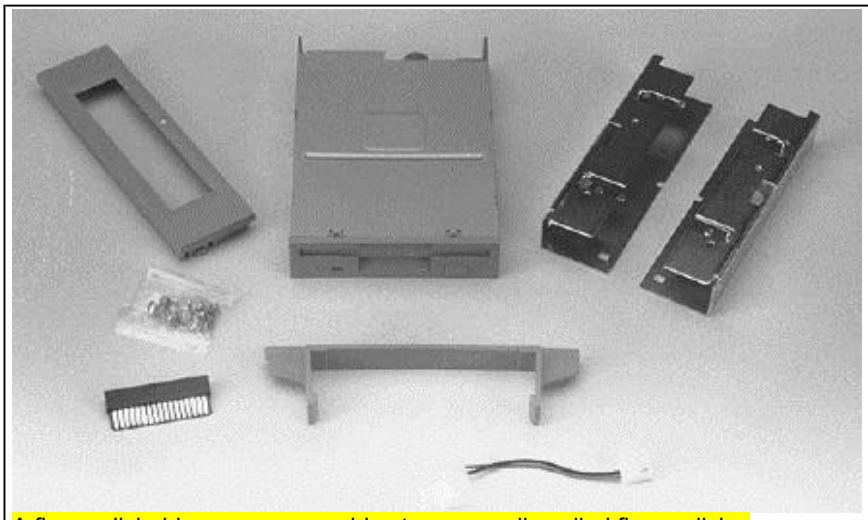
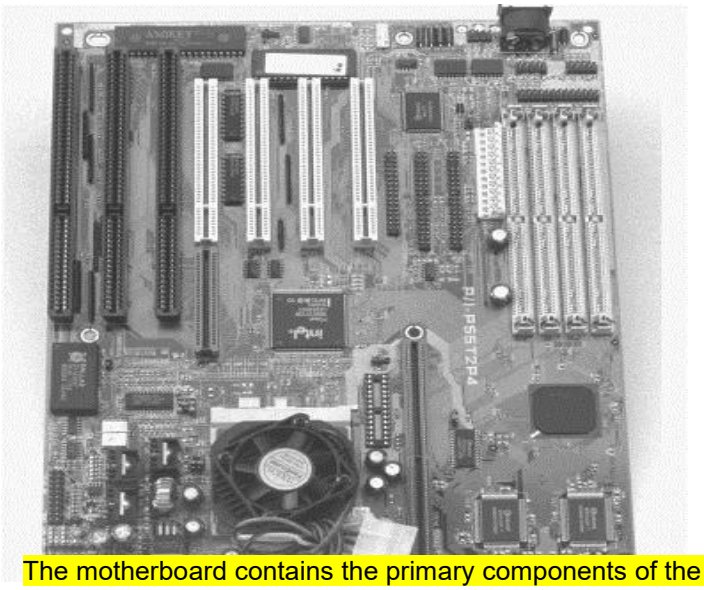


Figure 3: Floppy disk drive



A floppy disk drive uses removable storage media called floppy disks.

Figure 4: Motherboard



The motherboard contains the primary components of the computer system.

Because computers are important building blocks in a network, it is important to be able to recognize and name the major components of a *personal computer* (PC).

Many networking devices are special-purpose computers and have many of the same parts as “normal” PCs. To use your computer as a reliable means of obtaining information, your computer must be in good working order. You might occasionally need to troubleshoot a simple hardware or software problem.

You should be able to recognize, name, and state the purpose of the following PC components:

■ **Bus**—A bus is a collection of wires through which data is transmitted from one part of a computer to another. It connects all the internal computer components to the CPU. The Industry-Standard Architecture (ISA) and the peripheral component interconnect (PCI) are two types of buses.

■ **CD-ROM drive**—The CD-ROM drive is a compact disk read-only memory drive, a device that can read information from a CD-ROM.

■ **Central processing unit (CPU***)*—The CPU is the brains of the computer, where most calculations take place (see Figure **[1]**).

■ **Expansion card**—The expansion card is a printed circuit board you can insert into a computer to give it added capabilities.

■ **Expansion slot**—The expansion slot is an opening in a computer where a circuit board can be inserted to add new capabilities to the computer (see Figure **[2]**).

■ **Floppy disk drive**—This disk drive can read and write to floppy disks (see Figure **[3]**).

■ **Hard disk drive**—This device reads and writes data on a hard disk.

■ **Microprocessor**—A microprocessor is a silicon chip that contains a CPU.

■ **Motherboard**—The motherboard is the main circuit board of a microcomputer (see Figure **[4]**).

■ **Power supply**—This component supplies power to a computer.

■ **Printed circuit board (PCB***)*—The PCB is a thin plate on which chips (integrated circuits) and other electronic components are placed.

■ **Random-access memory (RAM***)*—Also known as read-write memory, RAM can have new data written into it as well as stored data read from it. A drawback of RAM is that it requires electrical power to maintain data storage. If the computer is turned off or looses power, all data stored in RAM is lost, unless the data was saved to disk.

■ **Read-only memory (ROM***)*—ROM is computer memory on which data has been prerecorded.

■ **System unit**—The system unit is the main part of a PC; it includes the chassis, microprocessor, main memory, bus, and ports, but does not include the keyboard or monitor, or any external devices connected to the computer.

Backplane Components

external devices, such as printers.

■ **Power cord**—The power cord is used to connect an electrical device to an electrical outlet in order to provide power to the device.

■ **Serial port**—This interface can be used The following
items are backplane components of a PC: 289

■ **Backplane**—The backplane is a large circuit board that contains sockets for expansion cards.

■ **Interface**—The interface is a piece of hardware, such as a modem connector, that allows two devices to be connected.

■ **Mouse port**—This port is designed for connecting a mouse to a PC.

■**Network card**—The network card is an expansion board inserted into a computer so that the computer can be connected to a network.

■ **Parallel port**—The parallel port is an interface capable of transferring

more than one bit simultaneously. It is used to connectfor serial communication in which
only one bit is transmitted at a time.

■ **Sound card**—A sound card is an expansion board that handles all sound functions.

■ **Video card**—The video card is a board that plugs into a PC to give it display capabilities

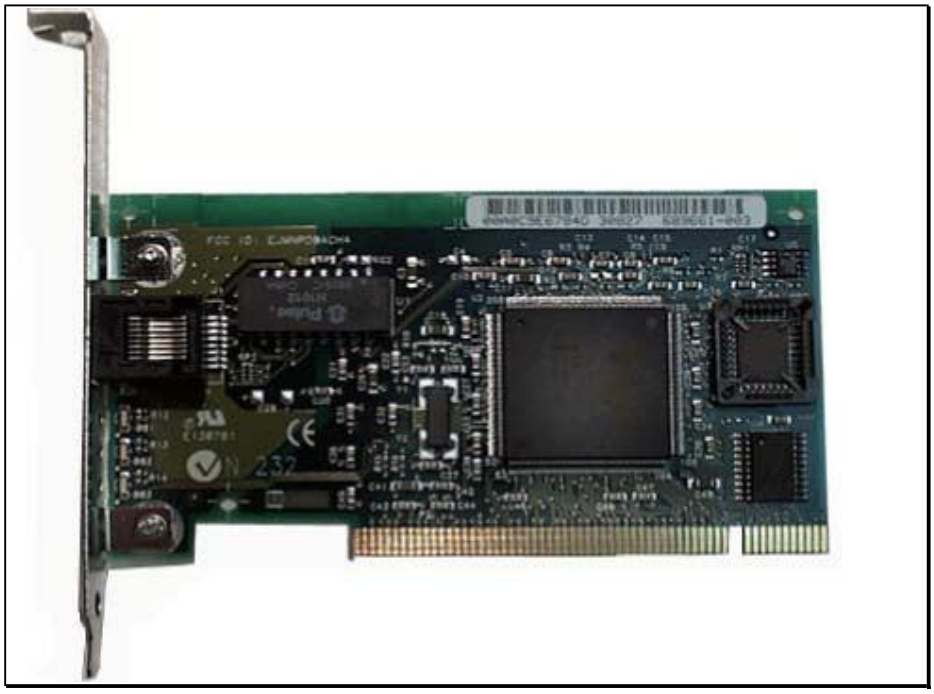
1.2 PC vs.Laptop

Figure 1: PCMCIA Card

Laptop computers and notebook computers are becoming increasingly popular, as
are palmtop computers, personal digital assistants, and other small computing
devices. The information described in the previous sections also pertains to laptops.
The main difference is that components in a laptop are smaller—the expansion slots
become PCMCIA slots or PC slots, where network interface cards (NICs), modems,
hard drives, and other useful devices (usually the size of a thick credit card) can be
inserted into the PCMCIA slots along the perimeter, as shown in
the figure.

Network InterfaceCard

Figure 1: Network Interface Card



As shown in Figure **[1]**, a *network interface card* (NIC) is a printed circuit board that provides network communication capabilities to and from a personal computer. Also called a *LAN adapter*, a NIC plugs into a motherboard and provides a port for connecting to the network. It constitutes the computer interface with the LAN.
347

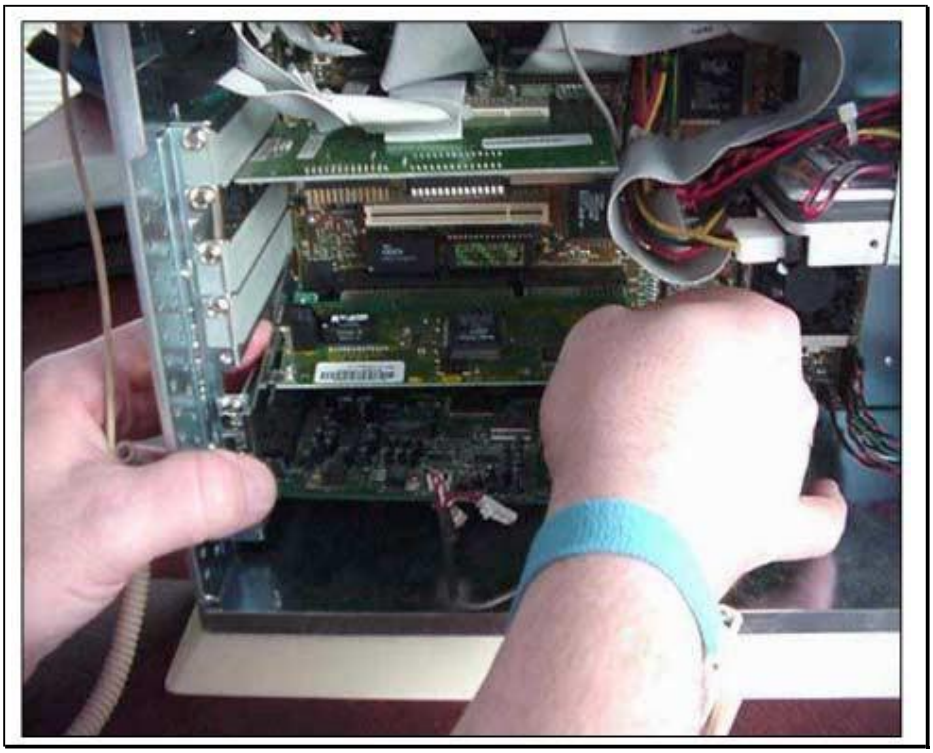
The NIC communicates with the network through a serial connection, and with the computer through a parallel connection. When a NIC is installed in a computer, it requires an *interrupt request line* (IRQ), an input/output (I/O) address, and a memory space for the operating systems (such as DOS or Windows 95/98/XP/NT/2000) drivers in order to perform its function. An IRQ is a signal that informs a CPU that an event that needs its attention has occurred. An IRQ is sent over a hardware line to the microprocessor. An example of an interrupt being issued would be when a key is pressed on a keyboard; the CPU must move the character

from the keyboard to RAM. An I/O address is a location in memory used to enter data or retrieve data from a computer by an auxiliary device. In DOS-based systems, upper memory refers to the memory area between the first 640 kilobytes (KB) and 1 megabyte (MB) of RAM. 360
The following important considerations should be made when selecting a NIC to use on a network:

1. **Type of network**— Ethernet NICs are designed for Ethernet LANs.
2. **Type of media**—The type of port or connector that the NIC provides for network connection is for specific media types such as twisted-pair, coaxial, fiber-optic, or wireless.
3. **Type of system bus**—The PCI slots are faster than ISA.

NIC Installation

Figure 1: Installing NIC



The NIC enables hosts to connect to the network and is, therefore, considered a key component.
To install a NIC, you need to have the following resources:

■ Knowledge of how the network card is configured, including jumpers, plug-and-play" software, and erasable programmable read-only memory

■ Use of network card diagnostics, including the vendor-supplied diagnostics and loopback test (see the documentation for the card)

■ Ability to resolve hardware resource conflicts, including IRQ, I/O base address, and direct memory address (DMA) (used to transfer data from RAM to a device without going through the CPU)

1.3 Bit, Bytes, and Measurement Terms

Figure 1: Units of Information

Unit	Bytes*	Bits*
bit (b)	1 bit	1 bit
byte (B)	1 byte	8 bits
Kilobyte (KB)	1000 bytes	8000 bits
Megabyte (MB)	1 million bytes	8 million bits
Gigabyte (GB)	1 billion bytes	8 billion bits

* Common or approximate bytes or bits.

Computers are electronic devices made up of electronic switches. At the lowest levels of computation, computers depend on these electronic switches to make decisions. As such, computers react only to electrical impulses. These impulses are understood by the computer as either “on” or “off” states, or as 1s or 0s.

Computers can understand and process only data that is in a binary format, which is represented by 0s and 1s. These 0s and 1s represent the two possible states of an electronic component and are referred to as binary digits (*bits*).

Most computer coding schemes use 8 bits to represent each number, letter, or symbol. A serial of 8 bits is referred to as a *byte*. One byte represents a single addressable storage location. The following are commonly used computer measurement terminology.

bit—The smallest unit of data in a computer. A bit equals 1 or 0, and it is the binary format in which data is processed by computers.

byte—A byte is a unit of measure used to describe the size of a data file, the amount of space on a disk or other storage medium, or the amount of data being sent over a network. One byte equals 8 bits of data.

Kb (kilobit)—A kilobit is approximately 1000 bit s. It can be abbreviated as "k."

KB (kilobyte)—A kilobyte is approximately 1000 bytes (actually, it is 1024 bytes). It can be abbreviated as "k."

kbps (kilobits per second)—This is a standard measurement of the amount of data transferred over a network connection.

kBps (kilobytes per second)—This is a standard measurement of the amount of data transferred over a network connection.

Decimal-to-BinaryConversion

Figure 1: Decimal-to-Binary Conversion Algorithm

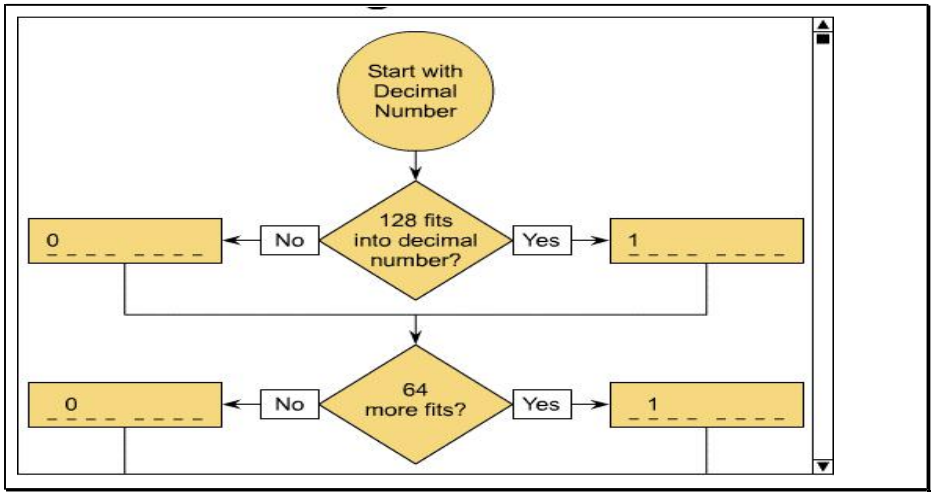


Figure 2: Base 2 Number System

Computers recognize and process data using the binary, or Base 2, numbering system. The binary number system uses only two symbols (0 and 1) instead of the ten symbols used in the decimal numbering system. The position, or place, of each digit represents the number 2 (the base number) raised to a power (exponent), based on its position (2^0, 2^1, 2^2, 2^3, 2^4, and so on)

Converting a decimal number to a binary number is one of the most common procedures performed while working with IP addresses. IP addresses identify a device on a network and the network to which it is attached. To make them easy to remember, IP addresses are usually written in dotted-decimal notation. Therefore, IP addresses are four decimal numbers separated by dots. An example of this is the address 166.122.23.130. Keep in mind that a decimal number is a base 10 number.

To convert a decimal number to binary, the idea is to first find the biggest power of 2 that will "fit" into the decimal number. The flowchart in Figure **[1]** describes the converting process. Consider the decimal number 35. Looking at Figure **[2]**, what is the greatest power of 2 that is less or equal to 35? Starting with the largest number, 2^5, or 32, is smaller than 35. You would place a "1" in that column. Now, you need to calculate how much is left over by subtracting 32 from 35. The result is 3.

Next, ask yourself if 16 (the next lower power of 2) fits into 3. Because it does not, a "0" is placed in that column.

The value of the next number is 8, which is larger than 3, so a "0" is placed in that column too.

The next value is 4, which is still larger than 3, so it too receives a "0." The next value is 2, which is smaller than 3. Because 3 fits into 2, place a "1" in that column. Now subtract 2 from 3, which results in 1. The value of the last number is 1, which fits in the remaining number left. Thus, place a "1" in the last column.

You now have the binary equivalent of the decimal number 35, which is 100011.

Binary-to-Decimal Conversion

Figure 1: Binary-to-Decimal Conversion Algorithm

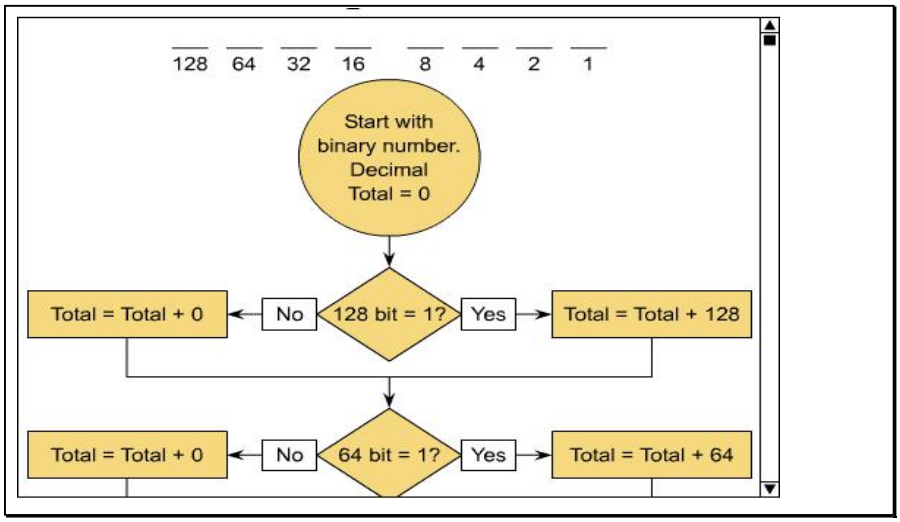


Figure 2: Base 2 Number System

As with binary-to-decimal conversion, there is usually more than one way to solve the conversion; you can use any method that you find easiest. The flowchart in Figure **[1]** shows the process for one of the conversion methods.

Example:

Convert the binary number 10111001 to a decimal number.

As shown in Figure **[2]**, the number in the 2^7 (128) column is 1, so the decimal totalis 128. Next, there is a 0 in the 2^6 (64) column. The decimal total is128 + 0 = 128. Now, there is a 1 in the 2^5 (32) column. The decimal total becomes128 + 32 = 160. Next, there is a 1 in the 2^4 (16) column. You will have to add the value to the decimal total, so you now have 160 + 16 = 176. The next column, 2^3, has a 1, so you need to add the value 8 to the decimal total 176 + 8 = 184. Next, there are 0s in the 2^2 and 2^1 columns. You will add 0s to the decimal total 184 + 0 +0 = 184. Finally, there is a 1 in the 2^0 (1) column. Now add 1 to 184. The result is

.

You now have the decimal equivalent of the binary number 10111001, which is 185.

Hex-to-Binary Conversion

Figure 1: Binary and Hexadecimal Number Systems

Decimal	Binary	Hexadecimal
0	00000000	00
1	00000001	01
2	00000010	02
3	00000011	03
4	00000100	04
5	00000101	05
6	00000110	06
7	00000111	07
8	00001000	08
9	00001001	09
10	00001010	0A
11	00001011	0B
12	00001100	0C
13	00001101	0D
14	00001110	0E
15	00001111	0F
16	00010000	10
32	00100000	20
64	01000000	40
128	10000000	80
255	11111111	FF

Converting from hexadecimal to binary works in exactly the opposite way as that in the previous section. Convert every one hex digit into four binary digits (bits). For example, convert hex AC to binary. First convert hex A, which is 1010 binary, and then convert hex C, which is 1100 binary. So the conversion of hex AC is 10101100 binary (see Figure [1]).

Figure [2] shows another example of converting a hexadecimal number to a binary number.

Be especially careful to include four binary digits for each hexadecimal character, adding zeros to the left of the number when necessary.

Binary-to-Hex Conversion

Figure 1: Binary and Hexadecimal Number Systems

Decimal	Binary	Hexadecimal
0	00000000	00
1	00000001	01
2	00000010	02
3	00000011	03
4	00000100	04
5	00000101	05
6	00000110	06
7	00000111	07
8	00001000	08
9	00001001	09
10	00001010	0A
11	00001011	0B
12	00001100	0C
13	00001101	0D
14	00001110	0E
15	00001111	0F
16	00010000	10
32	00100000	20
64	01000000	40
128	10000000	80
255	11111111	FF

Figure 2: Binary and Hexadecimal Number Systems

Binary Conversions

10010010000101111101111101110011001

converts to:

0001 0010 0100 0101 1111 0111 1101 1100 1001

converts to:

1 2 4 5 F 7 D C 9

so:

10010010000101111101111101110011001 Binary = 1245F7DC9 hexadecimal

The Base 16, or hexadecimal (or hex), number system is used frequently when working with computers, because it can be used to represent binary numbers in a more readable form. The computer performs computations in binary, but there are several instances when the binary output of a computer is expressed in hexadecimal to make it easier to read.

The primary uses of hex numbering are in config-register settings and in addressing schemes. You use a hex number as the argument for the config-register register command in order to change a

configuration setting. You use hex numbering in addressing schemes to provide a shorthand method of writing binary octets. Layer two Media Access Control (MAC) addresses are typically written in hex form Ethernet and Token Ring, these addresses are 48 bits, or six octets. Because these addresses consist of six distinct octets, they can be expressed as six hex numbers instead. of writing 10101010.11110000.11000001.11100010.01110111.01010001, you can write the much shorter hex equivalent: AA.F0.C1.E2.77.51. To make handling hex versions of MAC addresses even easier, the dots are placed only after each four digits, as in AAF0.C1E2.7751.

The most common way for computers and software to express hexadecimal output is using “0x” in front of the hexadecimal number. Thus, whenever you see “0x,” you know that the number that follows is a hexadecimal number. For example, 0x1234 means 1234 in Base 16.

It is referred to as Base 16 because it uses sixteen symbols; combinations of these symbols can then represent all possible numbers. Because there are only ten symbols that represent digits (0, 1, 2, 3, 4, 5, 6, 7, 8, 9), and the Base 16 requires six more symbols, the extra symbols are the letters A, B, C, D, E, and F. The “A” represents the decimal number 10, “B” represents 11, “C” represents 12, “D” represents 13, “E” represents 14, and “F” represents 15.

The position of each symbol, or digit, in a hex number represents the base number 16 raised to a power, or exponent, based on its position. Moving from right to left, the first position represents 16^0 (or 1), the second position represents 16^1 (or 16), the third position, 16^2 (or 256), and so on.

Converting hexadecimal to binary is an easy conversion because Base16 (hexadecimal) is a power of Base 2 (binary). **[1]** Every four binary digits (bits) are equal to one hexadecimal digit (see Figure **[2]**). The conversion looks like the following:

Binary	Hexadecimal	Binary	Hexadecimal
0000 = 0		1000 = 8	
		0001 = 1	1001 = 9
		0010 = 2	1010 = A
		0011 = 3	1011 = B
		0100 = 4	1100 = C
		0101 = 5	1101 = D
		0110 = 6	1110 = E
		0111 = 7	1111 = F

So if there is a binary number that looks like 01011011, it can be broken into two groups of four bits. These groups look like the following: 0101 and 1011. When converting these two groups to hex, they look like 5 and B. So, the hexadecimal equivalent of the binary 01011011 is 5B.

No matter how large the binary number, you always apply the same conversion. Start from the *right* of the binary number and break the number into groups of four. If the number of numbers is not divisible by four, add zeros to the left end until there are four digits (bits) in every group. Then convert each group of four to its hex equivalent.

1.4 Basic NetworkingTerminology

Computer networking, like most professions, has its own jargon, such as technical terms, abbreviations, and acronyms, that can, at first glance, look as foreign to the uninitiated as does the alphabet of a country halfway around the world.

Without a good grasp of the terminology, you will have difficulty understanding the concepts and processes

in this course. This lesson gives you a head start on deciphering some of the terminology used in this course. Please note that this is not intended to be a comprehensive glossary of networking terms, but a quick reference that defines and briefly discusses some of the most important and most basic words,
phrases, and acronyms that enable you to navigate through the next few modules. Each definition is expanded on in the modules that follow. Please refer to the course glossary for a more comprehensive list of definitions.

NIC—Pronounced "nick," NIC refers to the network interface card, also called the LAN adapter, or just the network interface. This card typically goes into an Industry-Standard Architecture (ISA), peripheral component interconnect (PCI), or PCMCIA (PC card) slot in a computer and connects to the network medium, which in turn is connected to other computers on the network.

Media—Media refers to the various physical environments through which transmission signals pass. Common network media include twisted-pair, coaxial, and fiber-optic cable, and the atmosphere (through which wireless transmission occurs).

Protocol—A network protocol is a set of rules by which computers communicate.Protocols are sometimes compared to languages, but a better analogy is that the protocol is like the syntax of a language, which is the order in which processes occur. There are many different types of computer protocols. The term protocol suite describes a set of several protocols that perform different functions related to different aspects of the communication process.

IOS—IOS, internetworking operating system, is Cisco system software that provides common functionality, scalability, and security for all products under the CiscoFusion architecture. Cisco IOS Software allows centralized, integrated, and automated installation and management of internetworks, while ensuring support for a wide variety of protocols, media, services, and platforms. Properly abbreviated Cisco IOS Software.

NOS—NOS, which stands for network operating system, usually refers to server software, such as Windows NT, Windows 2000 Server, Novell NetWare, and UNIX. The term sometimes refers to the networking components of a client operating system such as Windows 95 or the Macintosh OS.

Connectivity devices—This term refers to several different device types, all of which are used to connect cable segments, connect two or more smaller networks (or subnets) into a larger network, or divide a large network into smaller ones. The term encompasses repeaters, hubs, switches, bridges, and routers.

LAN—A local-area network (LAN) is a network that is confined to a limited geographic area. This can be a room, a floor, a building, or even an entire campus.

MAN—A metropolitan-area network (MAN) is a network that is between the LAN and the WAN in size. This is a network that covers approximately the area of a large city or metropolitan area.

WAN—A wide-area network (WAN) is made up of interconnected LANs. It spans wide geographic areas by using WAN links such as telephone lines or satellite technology to connect computers in different cities, countries, or even different continents.

Physical topology—This refers to the layout or physical shape of the network, whether the computers are arranged so that cabling goes from one to another in a linear fashion (linear bus topology), the last connects back to the first to form a ring (ring topology), the systems "meet in the middle" by connecting to a central hub (star topology), or multiple redundant connections make pathways (mesh topology).

Logical topology—The logical topology is the path that signals take from one computer to another. This topology can correspond to the physical topology. For instance, a network can be a physical star, in which each computer connects to a central hub, but inside the hub, the data can travel in a circle, making it a logical ring.

Network Applications

Figure 1: WWW Request-Response

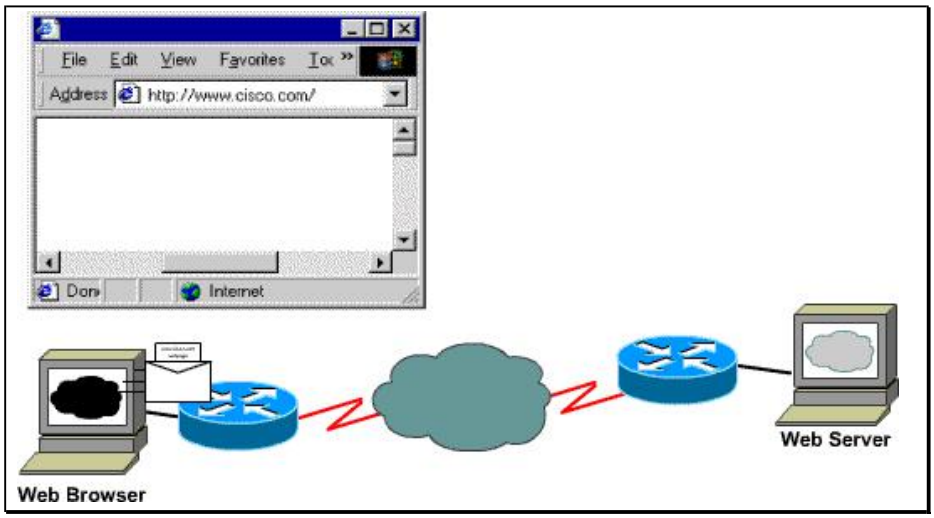
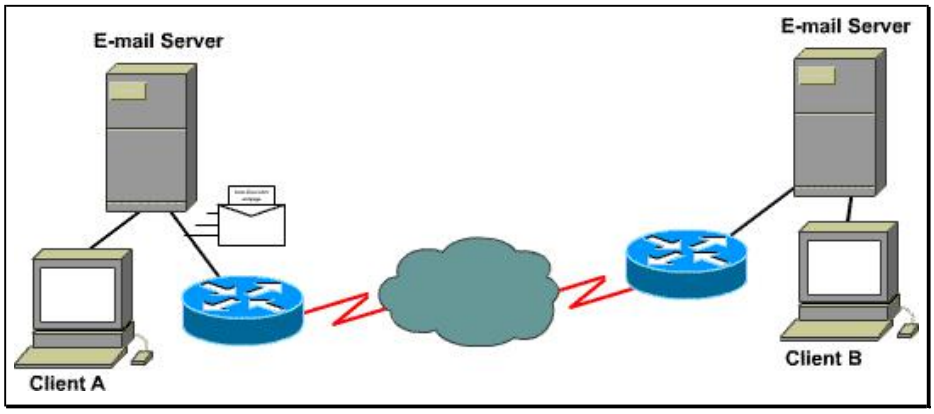


Figure 2: Sending Email



You select network applications based on the type of work you need to accomplish. A complete set of application layer programs is available to interface with the Internet. Each application program type is associated with its own application protocol. Here are some examples.

- The World Wide Web (WWW) uses the HTTP protocol (see Figure [1]).
- Remote access programs use the Telnet protocol for directly connecting to remote resources.
- E-mail programs support the POP3 application layer protocol f

or electronic mail.

- File utility programs use the FTP protocol for copying and moving files between remote sites.
- Network data gathering and monitoring use the SNMP protocol.

It is important to re-emphasize the fact that the application layer is just another protocol layer in the OSI or TCP/IP models. The programs interface with application layer protocols. E-mail client applications (i.e. Eudora, Microsoft Mail, Pegasus, and Netscape Mail) work with the POP3 protocol. The same is true with Web browsers. The two most popular Web browsers are Microsoft Internet Explorer and Netscape Communicator. The appearance and operation of these two programs is very different, but they both work with the application layer HTTP protocol.

Electronic mail (e-mail) enables you to send messages between connected computers. The procedure for sending an e-mail document involves two separate processes. The first is to send the e-mail to the user's post office, and the second is to deliver the e-mail from that post office to the user's e-mail client—the recipient (see Figure [2]).

WhyNetwork Computers?

Figure 1: Defining Components of the Network

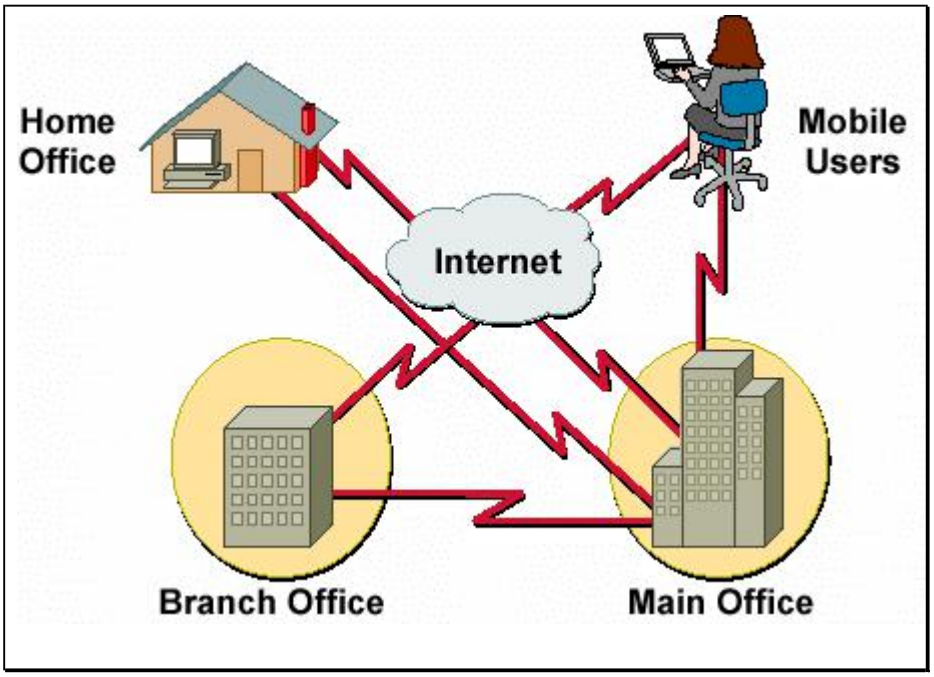
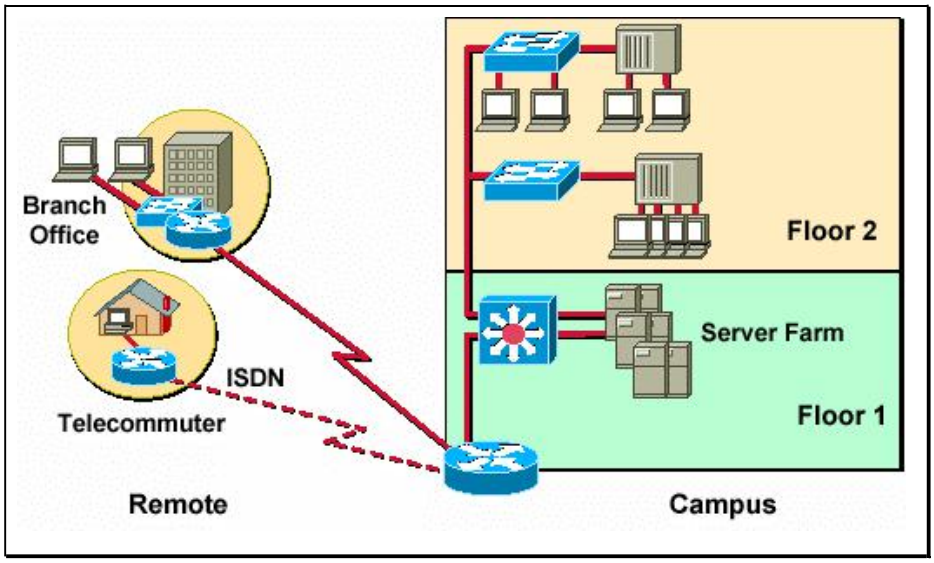


Figure 2: Defining Components of the Network



One of the primary purposes of networks is to increase productivity by linking computers and computer networks so that people have easy access to information regardless of differences in time, place, or type of computer system. Because companies have adopted their networks as part of their business strategy, it is typical to subdivide and map corporate networks to the corporate business structure. In Figure [1], the network is defined based on the grouping of employees (users) in the following ways:

■ A *main office* is where everyone is connected via a local-area network (LAN) and where the bulk of corporate information is located. A main office can have hundreds or even thousands of people who depend on network access to do their jobs. It may have several LANs or be a campus that contains several buildings. Because everyone needs access to central resources and information, it is common to see a high-speed backbone LAN as well as a legacy data center with mainframe computers and applications.

■ A variety of remote access locations that connect to the main office or each other using WAN services:

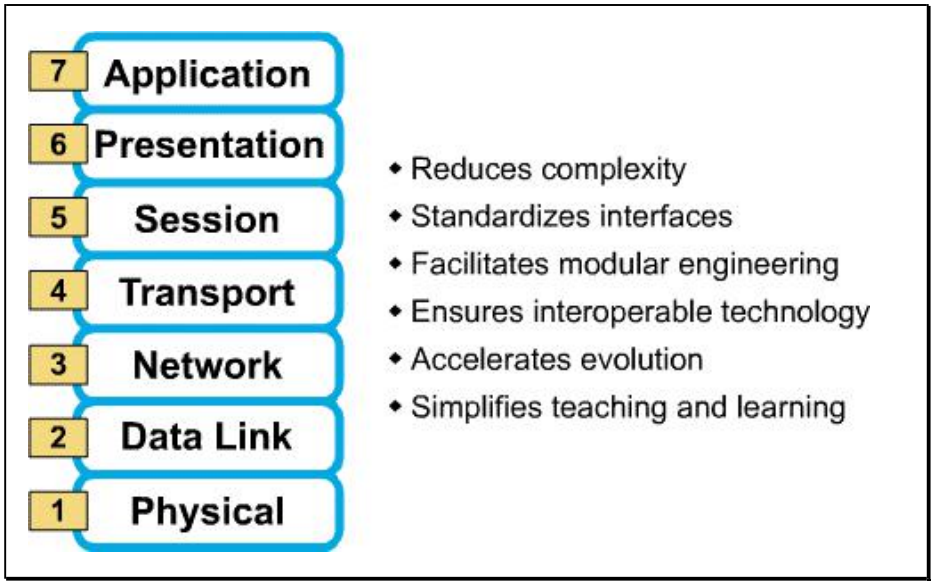
– **Branch offices**: Where smaller groups of people work and connect to each other via a LAN. To connect to the main office, these users have to use wide-area network (WAN) services. Although some corporate information may be stored at a branch office, it is more likely that they will have user resources, such as printers, but will have to access information directly from the main office. The frequency of accessing the main office determines whether the WAN will be based on permanent or dialup connections.

– **Home offices**: Where individuals work out of their homes. They will most likely require on-demand connections to the main office or the branch office to access information or use network resources such as file servers.

– **Mobile users**: These individuals connect to the main office LAN when they are at the main office, at the branch office, or on the road. Their network access needs are based on where they are located at a given point in time.In order to understand what types of equipment and services to deploy and when inyour n twork, it is important to understand the business and user needs. Figure [2] shows how you can map an organization's business or user requirements to a network.

1.5 The OSIModel

Figure 1: Why a Layered Network Model?



The early development of local-area networks (LANs), metropolitan-area networks (MANs), and wide-area networks (WANs) was chaotic in many ways. The early 1980s saw tremendous increases in the numbers and sizes of networks. As companies realized the money they could save and the productivity they could gain by using networking technology, they added networks and expanded existing networks almost as rapidly as new network technologies and products could be Introduced

By the mid-1980s, these companies began to experience growing pains from all the expansions they had made. It became more difficult for networks that used different specifications and implementations to communicate with each other. They realized that they needed to move away from proprietary networking systems. Proprietary systems are privately developed, owned, and controlled. In the computer industry,proprietary is the opposite of open. Proprietary means that one or a small group of companies controls all usage of the technology. Open means that free usage of the technology is available to the public. To address the problem of networks being incompatible and unable to communicate with each other, the International Organization for Standardization (ISO) researched network schemes. As a result of this research, the ISO created a network model that would help vendors create networks that would be compatible with, and operate with, other networks.

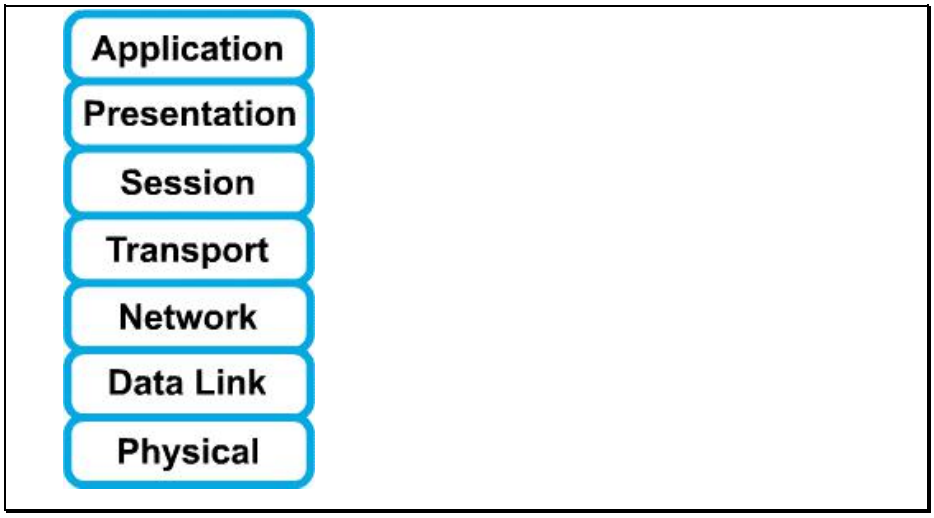
The Open System Interconnection (OSI) reference model, released in 1984, was the descriptive scheme the OSI created. It provided vendors with a set of standards that ensured greater compatibility and interoperability between the various types of network technologies that were produced by the many companies around the world. The OSI reference model is the primary model for network communications. Although other models exist, most network vendors today relate their products to the OSI reference model, especially when they want to educate users on the use of their products. They consider it the best tool available for teaching people about sending and receiving data on a network. The OSI reference model allows you to view the network functions that occur at each layer. More importantly, the OSI reference model is a framework that you can use to understand how information travels throughout a network. In addition, you can use the OSI reference model to visualize how information, or data packets, travel from application programs (for example, spreadsheets, documents, and so on), through a network medium (for example, wires, and so on), to another application program that is located in another computer on a network, even if the sender and receiver have different types of network media.

The OSI reference model has seven numbered layers, each of which illustrates a particular network function. This separation of networking functions is called layering. Dividing the network into these seven layers provides the following advantages:

- It breaks network communication into smaller, simpler parts.
- It standardizes network components to allow multiple-vendor development and support.
- It allows different types of network hardware and software to communicate with each other.
- It prevents changes in one layer from affecting the other layers, so that they can develop more quickly.
- It breaks network communication into smaller parts to make it easier to learn.

The OSI Layers and Functions

Figure 1: The Seven Layers of the OSI Model



The problem of moving information between computers is divided into seven smaller and more manageable problems in the OSI reference model. Each of the seven smaller problems is represented by its own layer in the model. The seven layers of the OSI reference model follow:

- Layer 7: The application layer
- Layer 6: The presentation layer
- Layer 5: The session layer
- Layer 4: The transport layer
- Layer 3: The network layer
- Layer 2: The data link layer
- Layer 1: The physical layer

Each individual OSI layer has a set of functions that it must perform in order for data packets to travel from a source to a destination on a network. Below is a brief description of each layer in the OSI reference model as shown in the Figures **[1] – [7]**.

Layer 7: The Application Layer
The application layer is the OSI layer that is closest to the user; it provides network services to the user's applications. It differs from the other layers in that it does not provide services to any other OSI layer, but rather, only to applications outside the OSI model. Examples of such applications are spreadsheet programs and word- processing programs. The application layer establishes the availability of intended communication partners, and synchronizes and establishes agreement on procedures for error recovery and control of data integrity.

Layer 6: The Presentation Layer
The presentation layer ensures that the information that the application layer of one system sends out is readable by the application layer of another system. If necessary, the presentation layer translates between multiple data formats by using a common format.

Layer 5: The Session Layer
As its name implies, the session layer establishes, manages, and terminates sessions between two communicating hosts. The session layer provides its services to the presentation layer. It also synchronizes dialogue between the two hosts' presentation layers and manages their data exchange. In addition to session regulation, the session layer offers provisions for efficient data transfer, class of service, and exception reporting of session layer, presentation layer, and application layer problems.

Layer 4: The Transport Layer
The transport layer segments data from the sending host's system and reassembles the data into a data stream on the receiving host's system. The boundary between the transport layer and the session layer can be thought of as the boundary between application protocols and data-flow protocols. Whereas the application, presentation, and session layers are concerned with application issues, the lower four layers are concerned with data-transport issues.

The transport layer attempts to provide a data-transport service that shields the upper layers from transport implementation details. Specifically, issues such as reliability of transport between two hosts are the concern of the transport layer. In providing communication service, the transport layer establishes, maintains, and properly terminates virtual circuits. In providing reliable service, transport error detection and recovery and information flow control are used.

Layer 3: The Network Layer
The network layer is a complex layer that provides connectivity and path selection between two host systems that may be located on geographically separated networks.

Layer 2: The Data Link Layer
The data link layer provides reliable transit of data across a physical link. In so doing, the data link layer is concerned with physical (as opposed to logical) addressing, network topology, network access, error notification, ordered delivery of frames, and flow control.

Layer 1: The Physical Layer
The physical layer defines the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between end systems. Such characteristics as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, physical connectors, and other, similar attributes are defined by physical layer specifications.

Data Communication

Figure 1: Data Encapsulation

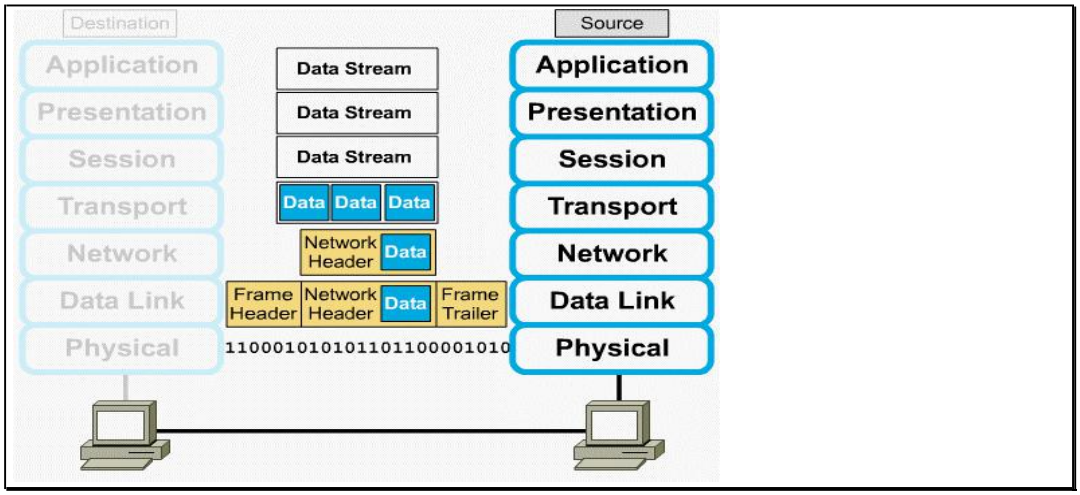


Figure 2: Data Encapsulation Example

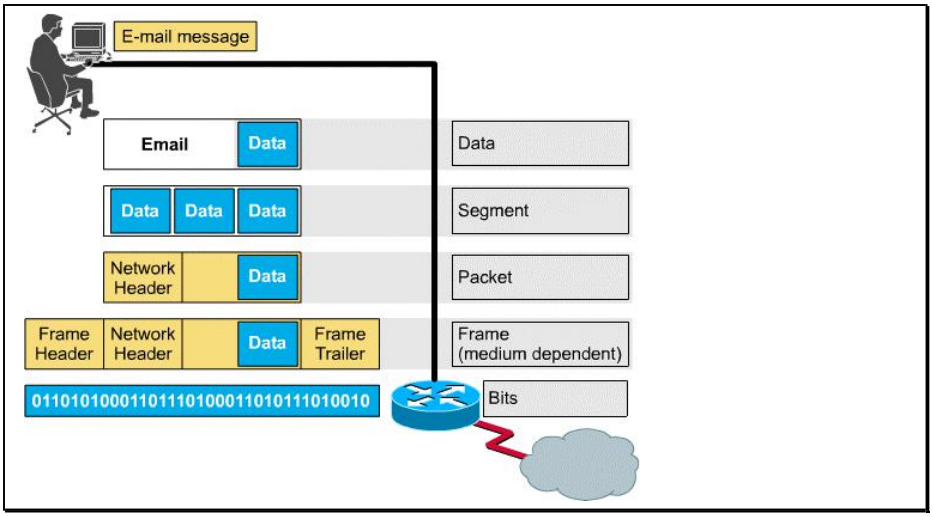


Figure 3: De-Encapsulation

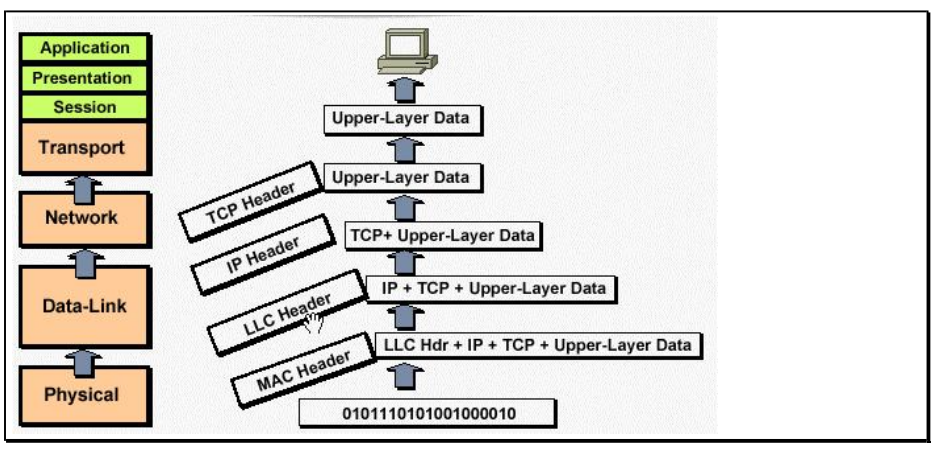


Figure 4: Peer-to-Peer Communications

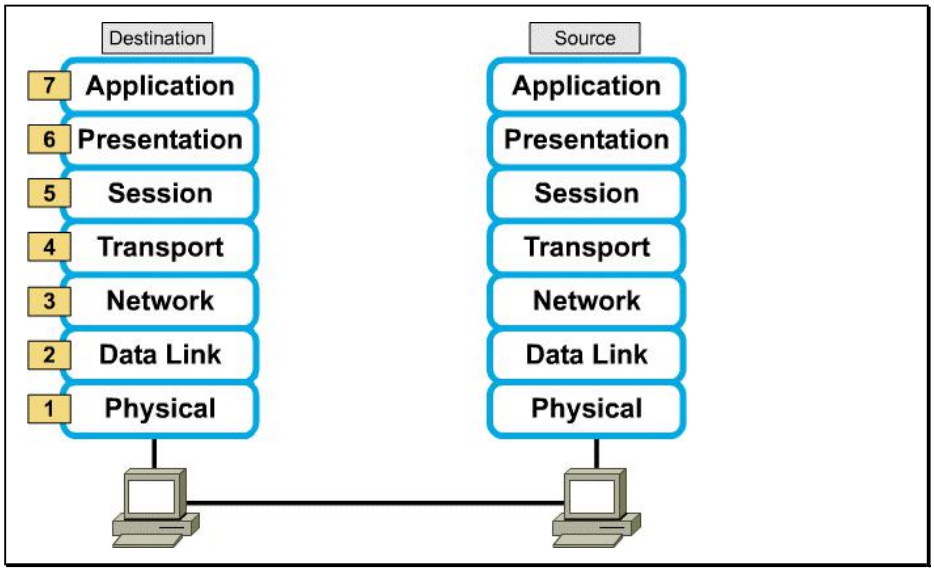
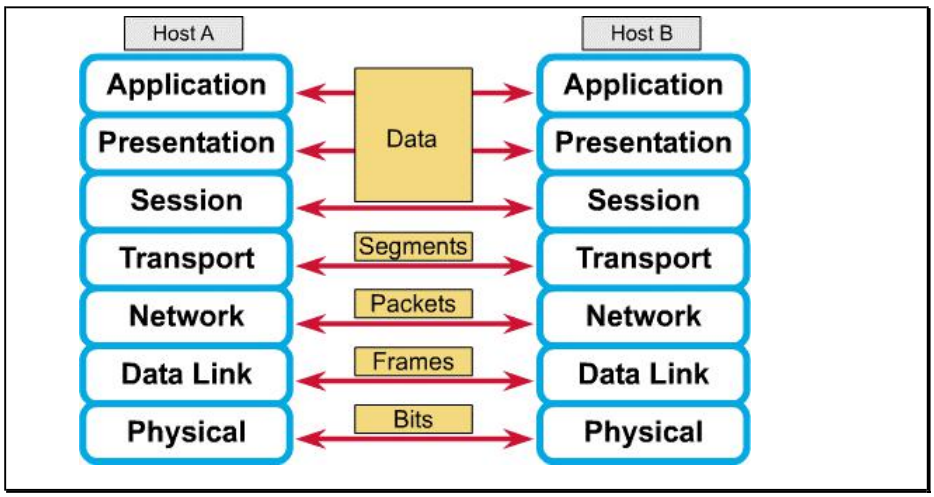


Figure 5: Peer-to-Peer Communications



All communications on a network originate at a source and are sent to a destination. The information that is sent on a network is referred to as data or data packets. If one computer (host A) wants to send data to another computer (host B), the data must first be packaged by a process called *encapsulation*.

Encapsulation

Encapsulation wraps data with the necessary protocol information before network transit. Therefore, as the data packet moves down through the layers of the OSI model, it receives headers, trailers, and other information.

To see how encapsulation occurs, let's examine the manner in which data travelsthrough the layers, as illustrated in the Figure **[1]**. After the data is sent from the source, as depicted in Figure **[1]**, it travels through the application layer down through the other layers. As you can see, the packaging and flow of the data that is exchanged goes through changes as the networks perform their services for end users. As illustrated in the Figures **[2]**, networks must perform the following five conversion steps in order to encapsulate data

1. **Build the data.**
   As a user sends an e-mail message, its alphanumeric characters are converted to data that can travel across the internetwork.
2. **Package the data for end-to-end transport.**
   The data is packaged for internetwork transport. By using segments, the transport function ensures that the message hosts at both ends of the e-mail system can reliably communicate.
3. **Append (add) the network address to the header.**
   The data is put into a packet or datagram that contains a network header with source and destination logical addresses. These addresses help network devices send the packets across the network along a chosen path.
4. **Append (add) the local address to the data link header.**
   Each network device must put the packet into a frame. The frame allows connection to the next directly connected network device on the link. Each device in the chosen network path requires framing in order for it to connect to the next device.
5. **Convert to bits for transmission.**
   The frame must be converted into a pattern of 1s and 0s (bits) for transmission on the medium (usually a wire). A clocking function enables the devices to distinguish these bits as they travel across the medium. The medium on the physical internetwork can vary along the path used. For example, the e-mail message can originate on a LAN, cross a campus backbone, and go out a WAN link until it reaches its destination on another remote LAN. Headers and trailers are added as data moves down through the layers of the OSI model.

De-Encapsulation [3]

When the remote device receives a sequence of bits, it passes them to the data link layer for frame manipulation. When the data link layer receives the frame it does the following:

1. It reads the physical address and other control information provided by the directly connected peer data link layer.
2. It strips the control information from the frame, thereby creating a datagram.
3. It passes the datagram up to the next layer, following the instructions that appeared in the control portion of the frame.

This process is referred to as *de-encapsulation*. Each subsequent layer performs a similar de-encapsulation process.

Peer-to-Peer Communication

In order for data packets to travel from the source to the destination, each layer of the OSI model at the source must communicate with its peer layer at the destination. This form of communication is referred to as *peer-to-peer communications*. During this process, the protocols at each layer exchange information, called *protocol data units (PDUs)*, between peer layers. Each layer of communication on the source

The TCP/IPModel

Figure 1: TCP/IP Model

Although the OSI reference model is universally recognized, the historical and technical open standard of the Internet is Transmission Control Protocol/Internet Protocol (TCP/IP). The TCP/IP reference model and the TCP/IP protocol stack make data communication possible between any two computers, anywhere in the world, at nearly the speed of light. The TCP/IP model has historical importance, just like the standards that allowed the telephone, electrical power, railroad, television, and videotape industries to flourish.

The U.S. Department of Defense (DoD) created the TCP/IP reference model because it wanted a network that could survive any conditions, even a nuclear war. To illustrate further, imagine a world at war, criss-crossed by different kinds of connections—wires, microwaves, optical fibers, and satellite links. Then imagine that you need information/data (in the form of packets) to flow, regardless of the condition of any particular node or network on the internetwork (which in this case may have been destroyed by the war). The DoD wants its packets to get through every time, under any conditions, from any one point to any other point. It was this very difficult design problem that brought about the creation of the TCP/IP model, and which has since become the standard on which the Internet has grown.

As you read about the TCP/IP model layers, remember the original intent of the Internet. It will help explain why certain things are as they are. The TCP/IP model has four layers: the application layer, the transport layer, the Internet layer, and the network access layer. It is important to note that some of the layers in the TCP/IP model have the same name as layers in the OSI model. However, do not confuse the layers of the two models. Even with the same name, the layers have different functions in each model.

Application Layer
The designers of TCP/IP felt that the higher-level protocols should include the session and presentation layer details. They simply created an application layer that handles high-level protocols, issues of representation, encoding, and dialog control. The TCP/IP combines all application-related issues into one layer, and ensures that this data is properly packaged for the next layer.

Transport Layer
The transport layer deals with the quality-of-service issues of reliability, flow control, and error correction. One of its protocols, the Transmission Control Protocol (TCP), provides excellent and flexible ways to create reliable, well- flowing, low-error network communications.

Internet Layer

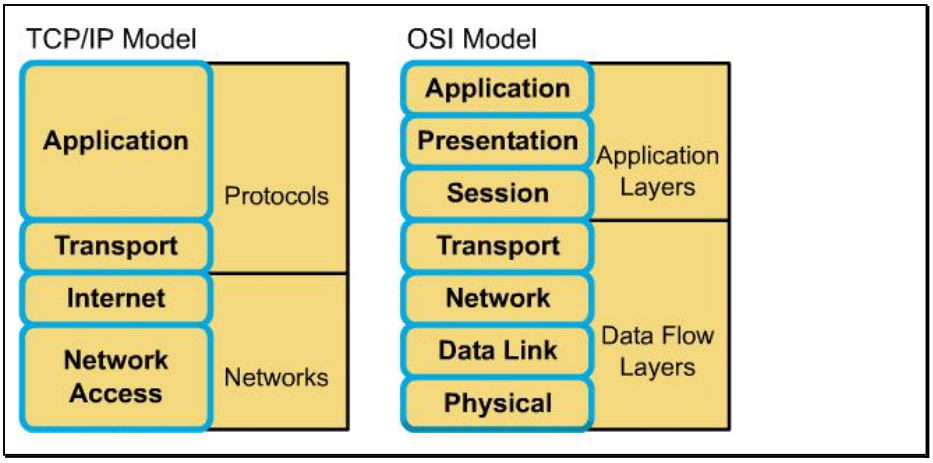
The purpose of the Internet layer is to send source packets from any network on the internetwork and have them arrive at the destination independent of the path and networks they took to get there.

Network Access Layer

The name of this layer is very broad and somewhat confusing. It is also called the host-to-network layer. It is the layer that is concerned with all the issues that an IP packet requires to actually make a physical link, and then to make another physical link. It includes the LAN and WAN technology details, and all the details in the OSI physical and data link layers.

OSI Model vs. TCP/IP Model

Figure 1: OSI Model vs. TCP/IP Model



If you compare the OSI model and the TCP/IP model, you will notice that they have similarities and differences. Examples include:

Similarities

- Both models have layers.
- Both models have application layers, though they include very different services.
- Both models have comparable transport and network layers.
- Packet-switched (not circuit-switched) technology is assumed in both models.
- Networking professionals need to know both models.

Differences

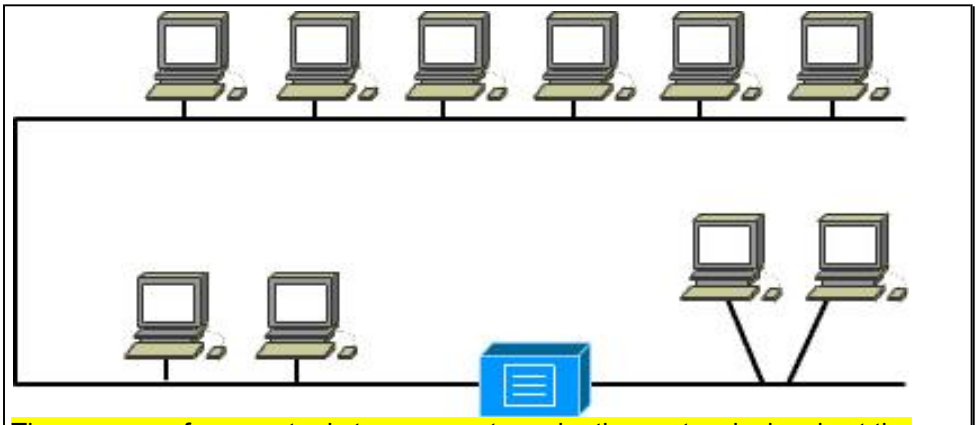
- TCP/IP combines the presentation and session layer issues into its application layer.
- TCP/IP combines the OSI data link and physical layers into one layer— network access layer.

- TCP/IP appears simpler because it has fewer layers.
- TCP/IP protocols are the standards around which the Internet developed, so the TCP/IP model gains credibility just because of its protocols. In contrast, typically networks are not built on the OSI protocol, even though the OSI model is used as a guide.

1.6 Network Devices

Layer 1 Devices

Figure 1: Repeater



The purpose of a repeater is to regenerate and retime network signals at the bit level to allow them to travel a longer distance on the media.

Figure 2: Hub (Multiport Repeater)

This course introduces three LAN technologies: Ethernet, Token Ring, and Fiber Distributed Data Interface (FDDI). All three have a wide variety of Layer 1 components and devices.

The common Layer 1 devices follow:

- Repeaters
- Hubs

Repeater [1]
Repeaters are networking devices that exist at Layer 1, the physical layer, of the OSI reference model. To begin understanding how a repeater works, it is important to understand first that as data leaves a source and goes out over the network, it is transformed into either electrical or light pulses that pass along the networking media. These pulses are referred to as signals. When signals first leave a

transmitting station, they are clean and easily recognizable. However, the longer the cable length, the weaker and more deteriorated the signals become as they pass along the networking media. The purpose of a repeater is to regenerate and retime network signals at the bit level to allow them to travel a longer distance on the media.

The term repeater originally meant a single port “in” and a single port “out” device. But today, multiple-port repeaters also exist. Repeaters are classified as Layer 1 devices in the OSI model, because they act only on the bit level and look at no other information.

Hub [2]
The purpose of a hub is to regenerate and retime network signals. You might notice the characteristics of a hub are similar to those of the repeater; thus a hub is also known as a *multiport repeater*. The difference between a repeater and a hub is the number of cables that connect to the device. Whereas a repeater typically has only 2 ports, a hub generally has from 4 to 20 or more ports, as shown in Figure **[2]**.
Whereas a repeater receives on one port and repeats on the other, a hub receives on one port and transmits on all other ports.

The following are the most important properties of hubs:

- Hubs amplify signals.
- Hubs propagate signals through the network.
- Hubs do not require filtering.
- Hubs do not require path determination or switching.
- Hubs are used as network concentration points.

Hubs are used most commonly in Ethernet 10BASE-T or 100BASE-T networks. A *media attachment unit* (MAU) plays the role of a hub in a Token Ring network. Physically, it resembles a hub, but Token Ring technology is very different, as you will learn in Module 3. In FDDI, the connecting device is called a *concentrator*.

MAUs and concentrators are also Layer 1 devices. Two reasons to use hubs are to create a central connection point for the wiring media and to increase the reliability of the network. Allowing any single cable to fail without disrupting the entire network increases the reliability of the network. This feature differs from the bus topology where having one cable fail disrupts the entire network. (Network topology is discussed later in this module.) Hubs are considered Layer 1 devices because they only regenerate the signal and repeat it out all of their ports (network connections).

Layer 2 Devices

Figure 1: Network Interface Card

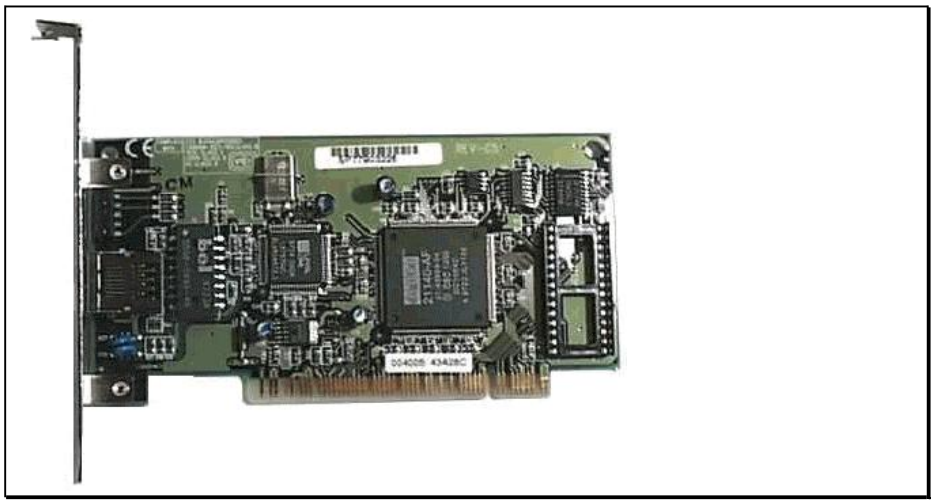


Figure 2: Bridge

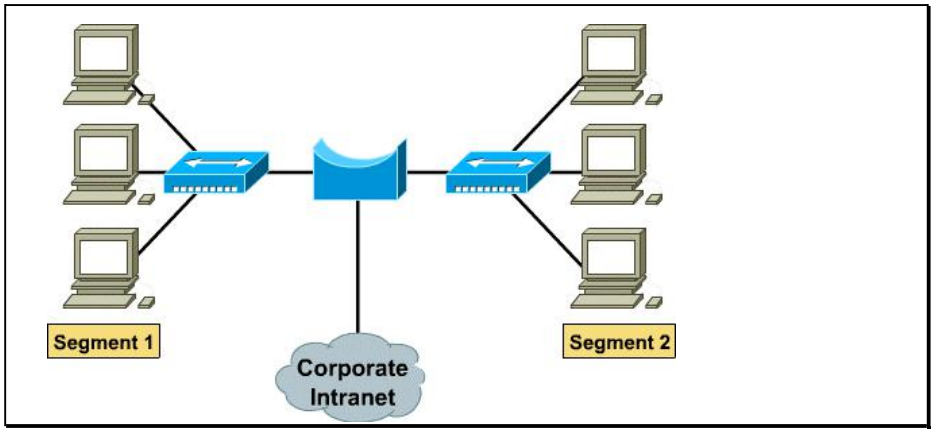
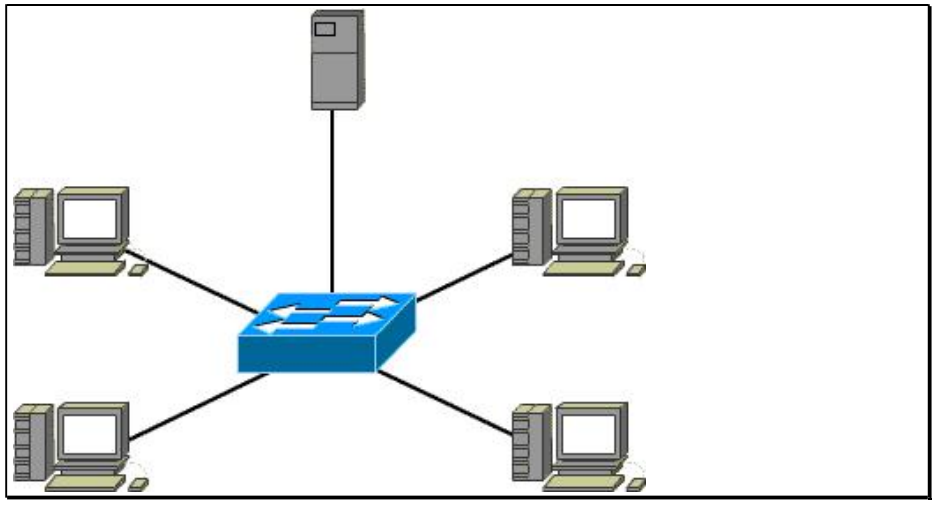


Figure 3: Switches



Network Interface Cards [1]
So far in this module, we have dealt with Layer 1 devices and concepts. Starting with the network interface card (NIC), the discussion moves to Layer 2, the data link layer of the OSI model.

NICs are considered Layer 2 devices because each individual NIC throughout the world carries a unique code, called a Media Access Control (MAC) address. This address is used to control data communication for the host on the network. You will learn more about the MAC address later. The NIC controls the access of the host to the medium.

Bridges [2]
A bridge is a Layer 2 device designed to create two or more LAN segments, each of which is a separate collision domain. That is, they were designed to create more useable bandwidth. The purpose of a bridge is to filter traffic on a LAN—to keep local traffic local—yet allow connectivity to other parts (segments) of the LAN for traffic that is directed there. You might wonder, then, how the bridge knows which traffic is local and which is not. The answer is the same one the postal service uses when asked how it knows which mail is local. It looks at the local address. Every networking device has a unique MAC address on the NIC. The bridge keeps track of which MAC addresses are on each side of the bridge and makes its decisions based on this MAC address list.

Bridges filter network traffic by looking only at the MAC address. Therefore, they can rapidly forward traffic representing any network layer protocol. Because bridges look only at MAC addresses, they are not concerned with network layer protocols. Consequently, bridges are concerned only with passing or not passing frames, based on their destination MAC addresses. The following are the important properties of bridges:

- Bridges are more intelligent than hubs—that is, they can analyze incoming frames and forward (or drop) them based on addressing information.
- Bridges collect and pass packets between two or more LAN segments.
- Bridges create more collision domains, allowing more than one device to transmit simultaneously without causing a collision.
- Bridges maintain address tables.

Figure **[2]** shows an example of how a bridge is used. The appearance of bridges varies greatly, depending on the type.

What really defines a bridge is its Layer 2 filtering of frames and how this is actually accomplished. Just as was the case of the repeater/hub combination, another device, called a switch (which you learn about next in this section), is used for multiple bridge connections.

In order to filter or selectively deliver network traffic, bridges build tables of all MAC addresses located on a network and other networks and map them.

- If data comes along the network media, a bridge compares the destination MAC address carried by the data to MAC addresses contained in its tables.

- If the bridge determines that the destination MAC address of the data is from the same network segment as the source, it does not forward the data to other segments of the network.
- If the bridge determines that the destination MAC address of the data is not from the same network segment as the source, it forwards the data to the appropriate segment.
- By performing this process, bridges can significantly reduce the amount of traffic between network segments by eliminating unnecessary traffic.

Layer 2 Switches

Switches, also referred to as LAN switches (see Figure **[3]**), often replace shared hubs and work with existing cable infrastructures to ensure that they are installed with minimal disruption of existing networks.

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

Switches are data link layer devices that, like bridges, enable multiple physical LAN segments to be interconnected into single larger network. Similar to bridges, switches forward and flood traffic based on MAC addresses. Because switching is performed in hardware instead of in software, it is significantly faster. You can think of each switch port as a microbridge; this process is called *microsegmentation*. Thus each switch port acts as a separate bridge and gives the full bandwidth of the medium to each host.

Layer 3 Devices

Figure 1: Cisco 2600 Series Router

Router [1]
Networking has two addressing schemes: one uses the MAC address, a data link (Layer 2) address; the other uses an address located at the network layer (Layer 3) of the OSI model. An example of a Layer 3 address is an IP address. A router is a type of internetworking device that passes data packets between networks, based on Layer 3 addresses. A router can make intelligent decisions regarding the best path for delivery of data on the network.

Working at Layer 3 allows the router to make decisions based on network addresses as opposed to individual Layer 2 MAC addresses. Routers also can connect different Layer 2 technologies, such as Ethernet, Token Ring, and FDDI. However, because of their capability to route packets based on Layer 3 information, routers have become the backbone of the Internet, running the IP protocol.

The purpose of a router is to examine incoming packets (Layer 3 data), choose the best path for them through the network, and then switch them to the proper outgoing port. Routers are the most important traffic-regulating devices on large networks.
They enable virtually any type of computer to communicate with any other computer anywhere in the world.

Multilayer Switches
A multilayer switch works very much the same as a Layer 2 switch. In addition to switching using Layer 2 MAC addresses, a multilayer switch also uses Layer 3 network addresses (IP).

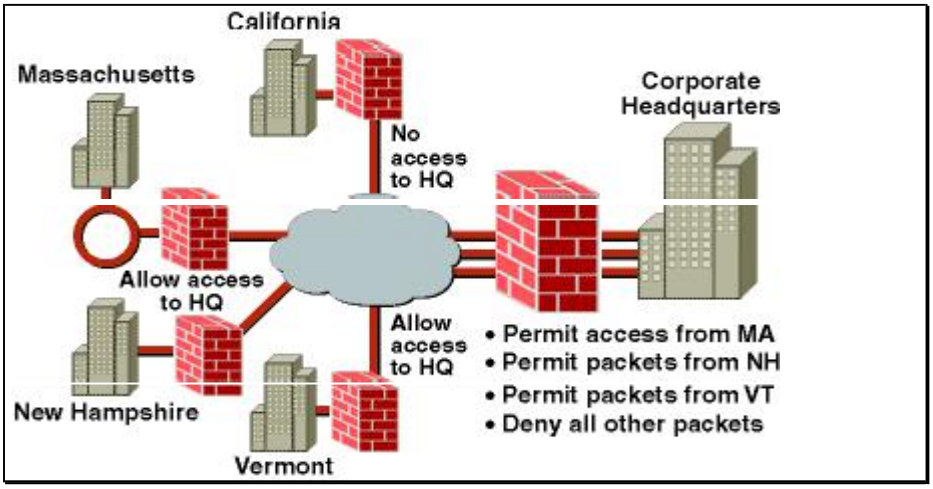
Traditionally, Layer 3 functions have occurred only within routers, but over the past few years, improved hardware has allowed many Layer 3 routing functions to occur in hardware. Layer 3 routing has traditionally been a software-bound process that creates network bottlenecks. With the advent of high-speed, hardware-based multilayer switches, Layer 3 functions can be performed as quickly as Layer 2 functions. Layer 3 no longer is a bottleneck.

These Layer 3 functions include added capability for quality of service (QoS) and for security. Packets can be prioritized based on the network (IP) that they are coming from or to which they are being sent. Traffic from specific networks can be barred from entering your network.

A multilayer switch can also examine Layer 4 information, including TCP headers that can help identify the type of application from which the packet came or to which the packet is directed.

Firewalls and AAA Servers

Figure 1: Firewalls



Firewalls

The term *firewall* refers to either a firewall program(s) running on a router or server or a special standalone hardware component of a network.

A firewall protects the resources of a private network from users in other networks.

Working closely with a router program, a firewall examines each network packet to determine whether to forward it toward its destination. A firewall also includes or can work with a proxy server that makes network requests on behalf of workstation users.

AAA Servers

An AAA server is a server program that handles user requests for access to computer resources and, for an enterprise, provides Authentication, Authorization, and Accounting (AAA) services. The AAA server ensures that only authentic users can get in the network (authentication), that the users are allowed access only to the resources they need (authorization), and records everything they do after they are let in (accounting).

1.7 Network Topologies

Physical vs. Logical

Figure 1: Physical Topologies

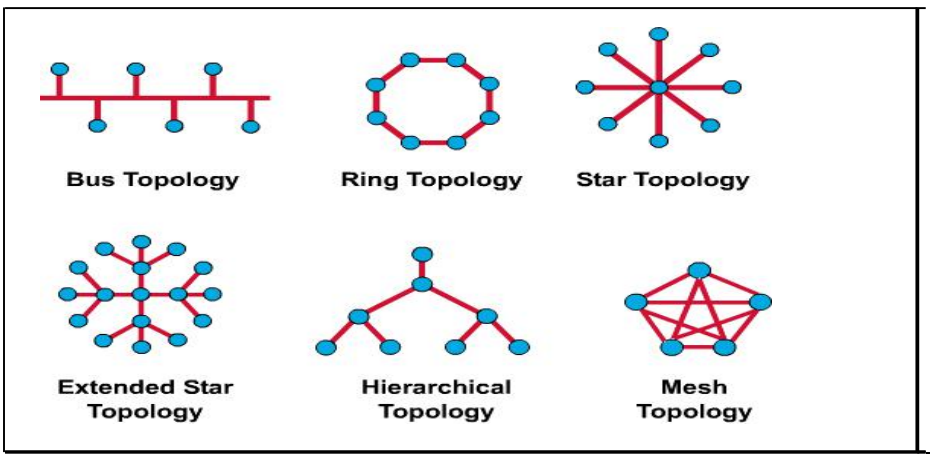
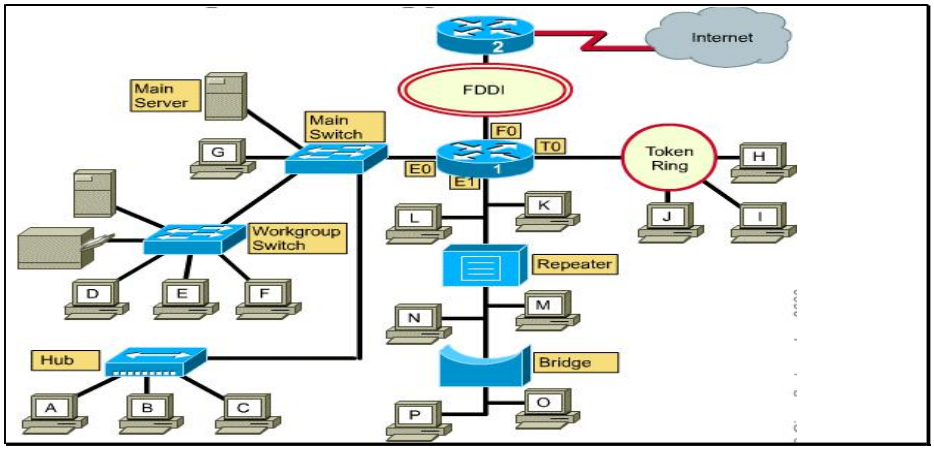


Figure 2: Teaching Topologies



The network topology defines the way in which the computers, printers, and other devices are connected. In other words, the topology of a network describes the layout of the wire and devices as well as the paths used by data transmissions. The topology greatly influences the way the network works.

Networks can have both a physical and a logical topology (see Figures **[1]** and **[2]**).

- **Physical topology**: Refers to the layout of the devices and media.

- **Logical topology**: Refers to the paths that signals travel from one point on the network to another (that is, the way in which data accesses media and transmits packets across it).

The physical and logical topologies of a network can be the same. For instance, in a network physically shaped as a linear bus, the data travels in a straight line from one computer to the next. Hence, it has both a bus physical topology and a bus logical topology.

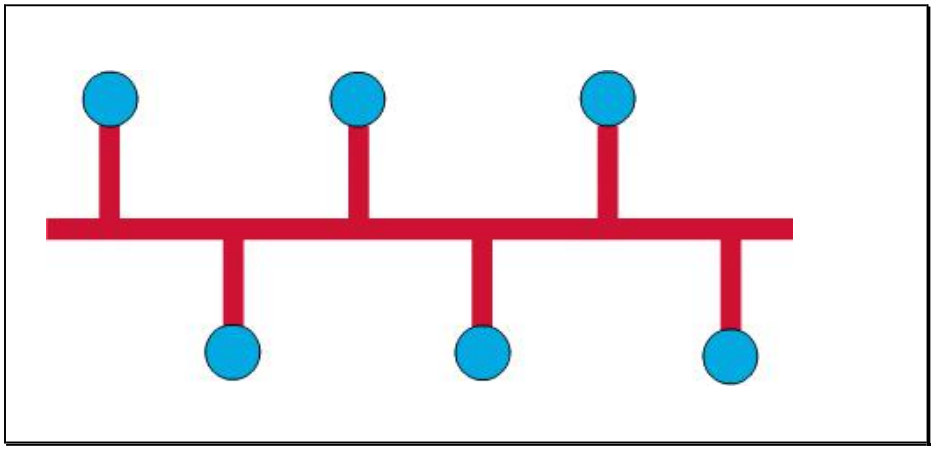
A network can also have physical and logical topologies that are quite different. For example, a physical topology in the shape of a star, where cable segments can connect all computers to a central hub, can, in fact, have a logical ring topology. Remember that in a ring, the data travels from one computer to the next. That is because inside the hub, the wiring connections are such that the signal actually travels around in a circle from one port to the next, creating a logical ring. Therefore, you cannot always predict how data travels in a network by simply observing its physical layout.

As for Ethernet and Token Ring, Token Ring uses a logical ring topology in either a physical ring or physical star, whereas Ethernet uses a logical bus topology in either a physical bus or physical star.

In the following sections, you will learn about the different types of topologies, including bus, star, ring, and mesh.

Bus

Figure 1: Bus Topology



Commonly referred to as a linear bus, all the devices on a bus topology are connected by one single cable, which proceeds from one computer to the next like a bus line going through a city. The main cable segment must end with a terminator that absorbs the signal when it reaches the end of the line or wire. If there is no terminator, the electrical signal representing the data bounces back at the end of the wire, causing errors in the network. Only one packet of data can be transmitted at a time. If more than one packet is transmitted, they collide and have to be resent. A bus topology with many hosts can be very slow because of the collisions.

Star and Extended Star

Figure 1: Star Topology

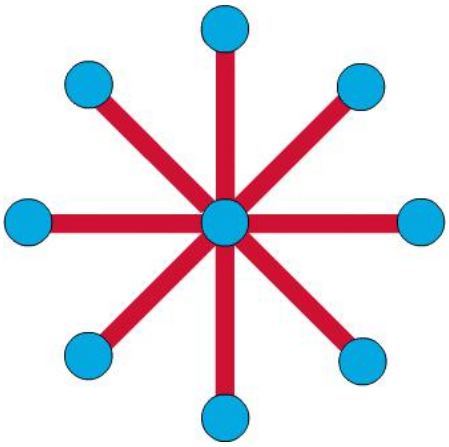
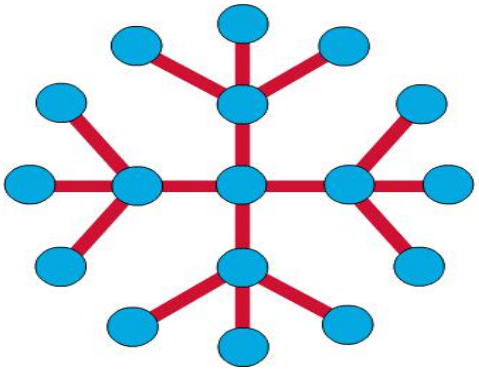


Figure 2: Extended-Star Topology



Star Topology [1]

The star topology is the most commonly used architecture in Ethernet LANs. When installed, the star topology resembles spokes in a bicycle wheel. It is made up of a central connection point that is a device, such as a hub, switch, or router, where all the cabling segments actually meet. Each host in the network is connected to the central device with its own cable.

Although a star topology costs more to implement than the bus topology because more cable is used and a central device such as a hub, switch, or router is needed, the advantages of a star topology are worth the additional costs. Because each host is connected to the central device with its own wire, when there is a problem with that cable, only that host is affected. The rest of the network is operational. This benefit is extremely important and the reason why virtually every newly designed network has this topology.

Extended-Star Topology [2]

When a star network is expanded to include an additional networking device connected to the main networking device, it is called an extended-star topology.
Most larger networks, such as those for corporations or schools, use the extended-star topology. This topology when used with network devices that filter data packets, such as switches and routers, significantly reduces the traffic on the wires by sending packets only to the wires of the destination host.

Ring

Figure 1: Ring Topology

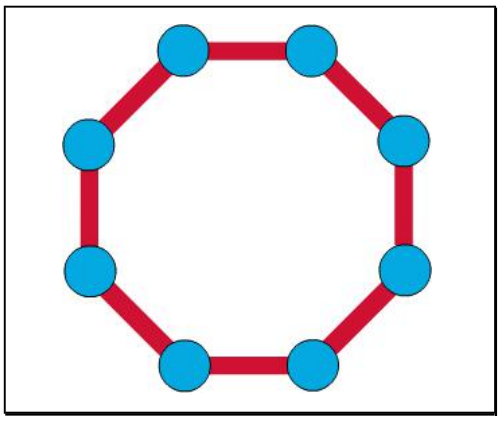
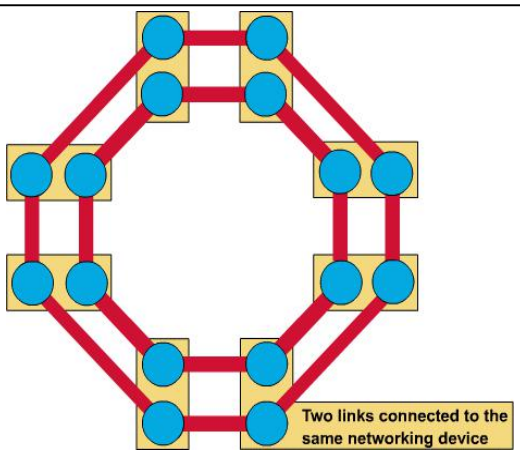


Figure 2: Dual-Ring Topology



The ring topology is another important topology in LAN connectivity. As the name implies, hosts are connected in the form of a ring or circle. Unlike the bus topology, it has no beginning or end that needs to be terminated. Data is transmitted in a way unlike either the bus or the star topology. A frame travels around the ring, stopping at each node. If a node wants to transmit data, it adds that data as well as the destination address to the frame. The frame then continues around the ring until it finds the destination node, which takes the data out of the frame. The advantage of using this type of method is that there are no collisions of data packets.

There are two types of rings:

Single ring: All the devices on the network share a single cable, and the data travels in one direction only (see Figure **[1]**). Each device waits its turn to send data over the network.

Dual ring: Two rings allow data to be sent in both directions (see Figure **[2]**). This setup creates redundancy (fault tolerance), meaning that if one ring fails, data can be transmitted on the other ring.

The most common implementation of the ring topology is in Token Ring networks. The IEEE 802.5 standard is the Token Ring access method used. Fiber Distributed Data Interface (FDDI) technology is a similar to Token Ring, but it uses light instead of electricity to transmit data. It uses the dual ring.

Mesh and PartialMesh

Figure 1: Full-Mesh Topology

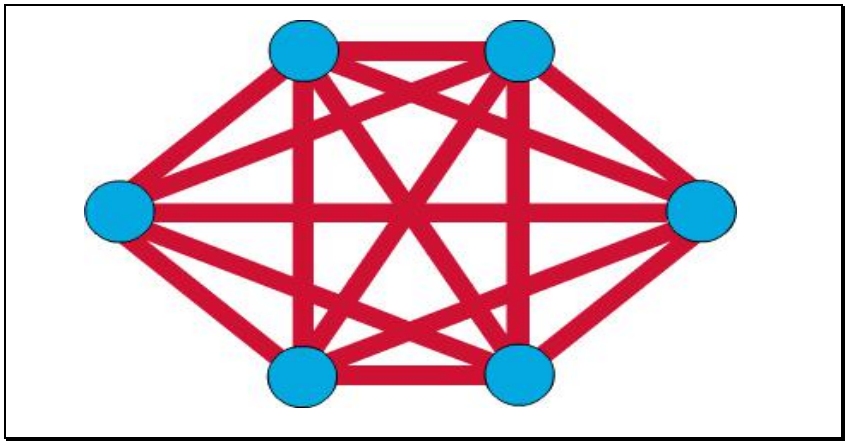
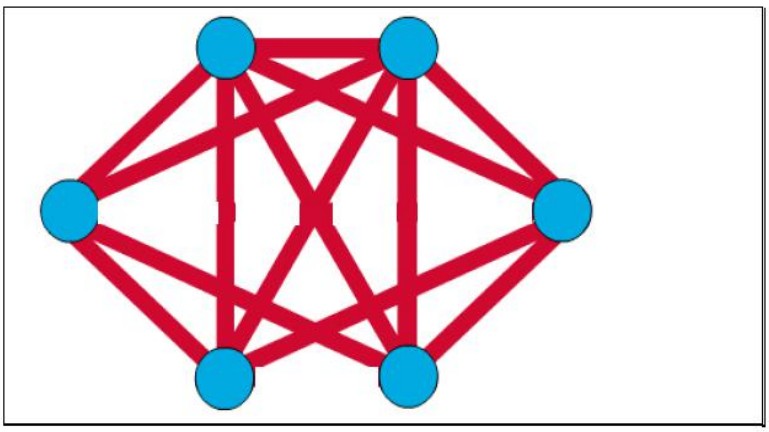


Figure 2: Partial-Mesh Topology



Full-Mesh Topology [1]

The full-mesh topology connects all devices (nodes) to each other for redundancy and fault tolerance. Implementing the full-mesh topology is expensive and difficult.

Partial-Mesh Topology [2]

In a partial-mesh topology, at least one device maintains multiple connections to others, without being fully meshed.

DATA COMMUNICATION

The term telecommunication means communication at a distance. The word data refers to information presented in whatever form is agreed upon by the parties creating and using the data. Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable

A data communication system is made up of five components .

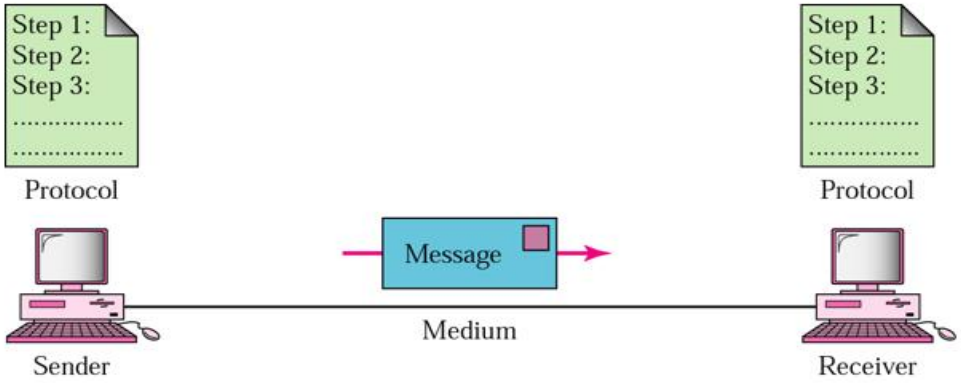
Message. The message is the information (data) to be communicated. It can con-sists of text, numbers, pictures, sound, or video or any combination of these.

Sender. The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

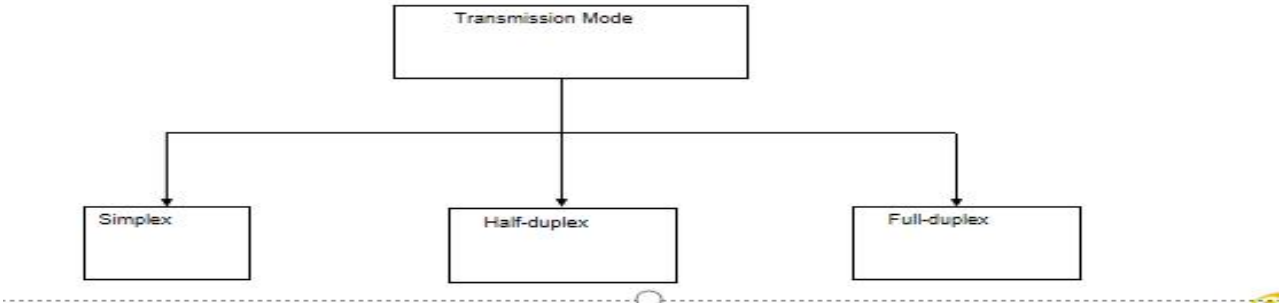
Receiver. The receiver is the device that receives the message. It can be a com-puter, workstation, telephone handset, television, and so on.

Medium. The transmission medium is the physical path by which a message travels from sender to receiver**.** It can consist of twisted pair wire, coaxial cable, fiber-optic cable, laser, or radio waves (terrestrial or satellite microwave).

Protocol. A protocol is a set of rules that govern data communication. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

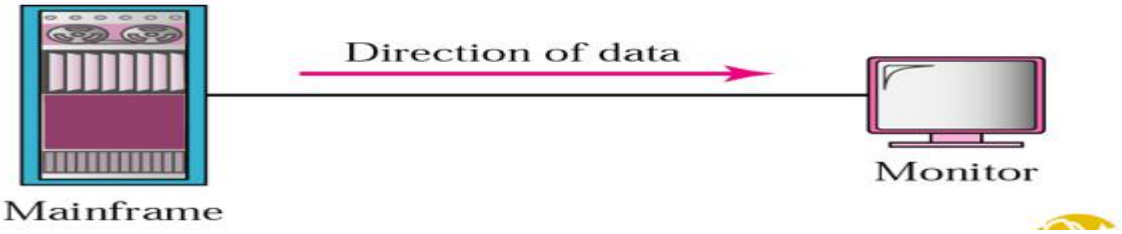


- The term *transmission mode* is used to define the direction of signal flow between two linked devices.



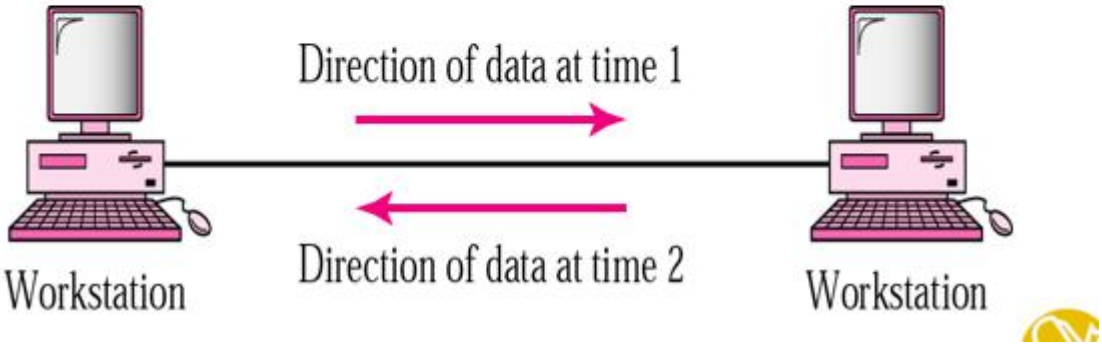
SIMPLEX

- In simplex mode, the communication is unidirectional, as on a one-way Street. Only one of the two stations on a link can transmit; the other can only receive



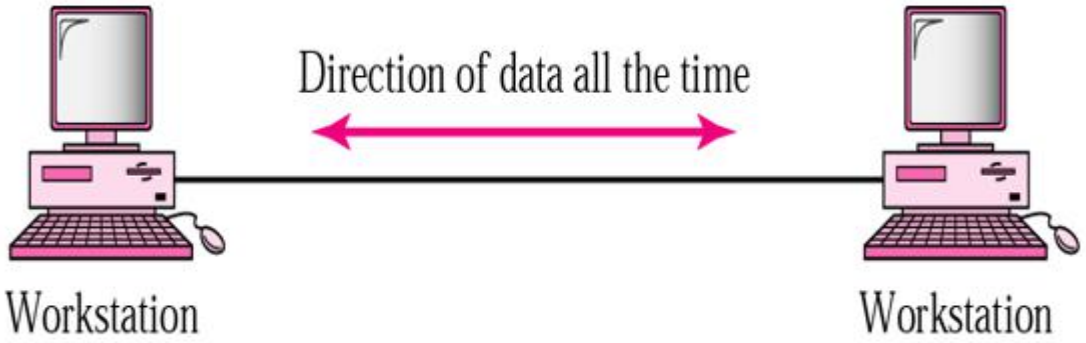
HALF-DUPLEX

- In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa.

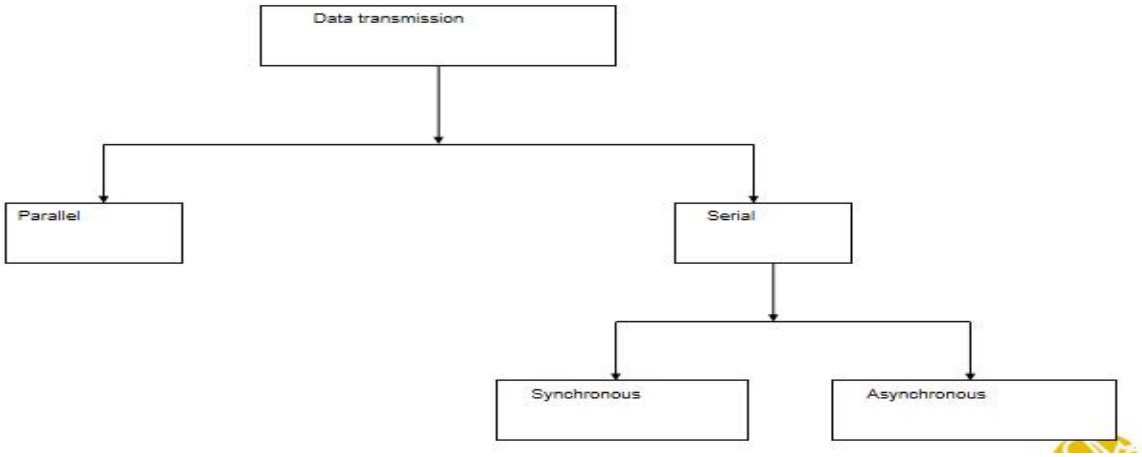


FULL-DUPLEX

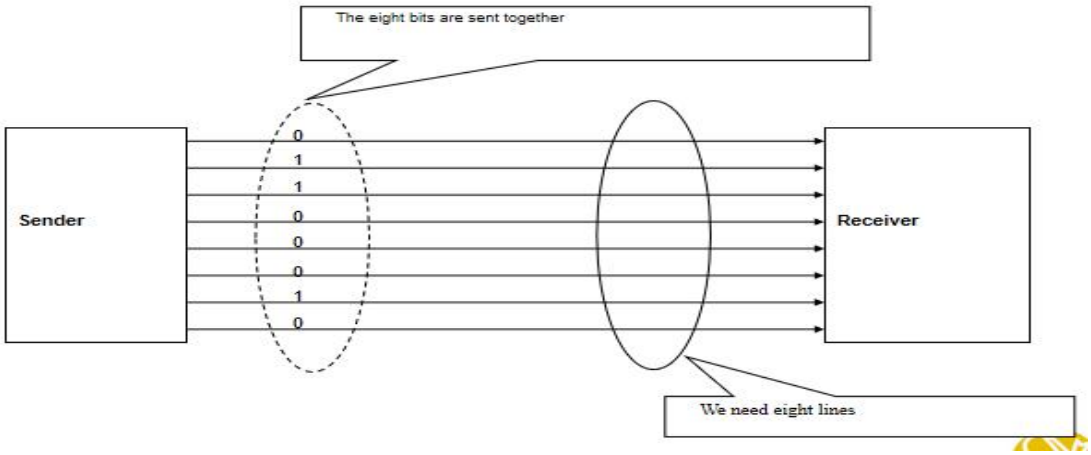
- In full-duplex mode (also called duplex), both stations can transmit and receive simultaneously.



DATA TRANSMISSION



PARALLEL TRANSMISSION



In parallel data transmission, multiple bits are sent simultaneously down different wires (channels) within the same cable.

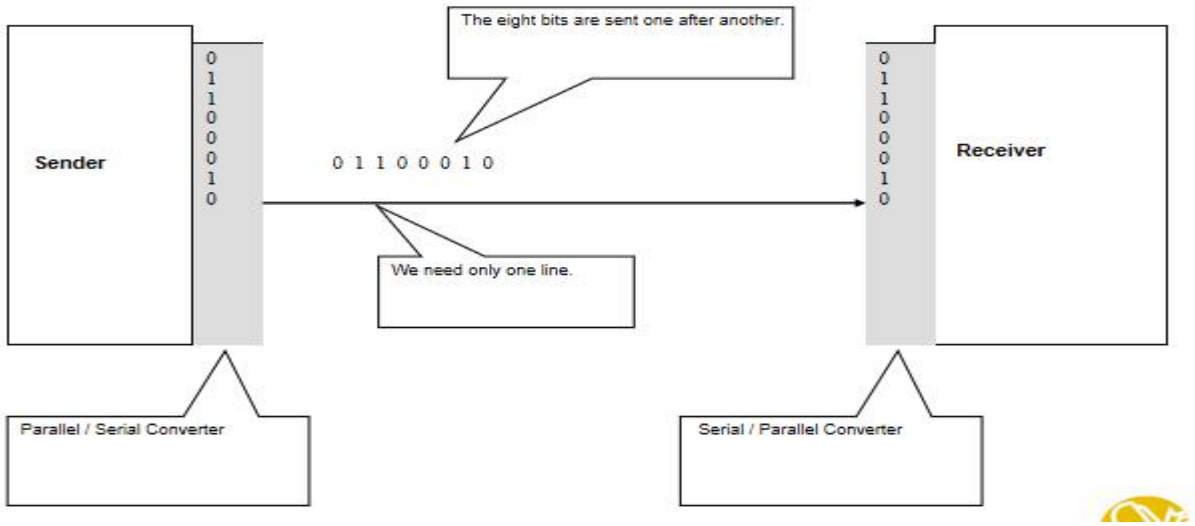
Data is synchronised by a clock, however this becomes problematic over longer distances where synchronisation errors may start to occur.

Using parallel wires is more expensive but transmission is faster.

Uses of parallel transmission

- Fast transmission within a computer system
- Short distances
- Integrated Circuits (IC), Busses

SERIAL TRANSMISSION



In serial data transmission, bits are sent sequentially (one after the other) down the same wire (channel).

Using a single wire reduces costs but slows down the speed of transmission.

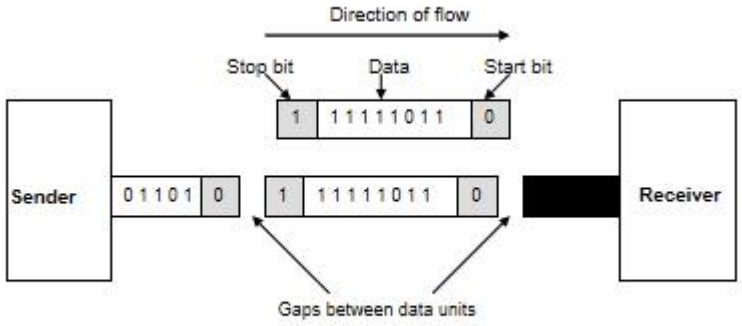
Sending data sequentially is perfect for transmitting over longer distances as there are no synchronisation issues.

Uses of serial transmission

- Transmission to another computer or to external devices
- Medium to long distances
- Universal Serial Bus (USB)

TWO TYPES OF SERIAL TRANSMISSION

ASYNCHRONOUS TRANSMISSION



In asynchronous transmission, data moves in a half-paired approach, 1 byte or 1 character at a time. It sends the data in a constant current of bytes. The size of a character transmitted is 8 bits, with a parity bit added both at the beginning and at the end, making it a total of 10 bits. It doesn't need a clock for integration—rather, it utilises the parity bits to tell the receiver how to translate the data.

It is straightforward, quick, cost-effective, and doesn't need 2-way communication to function.

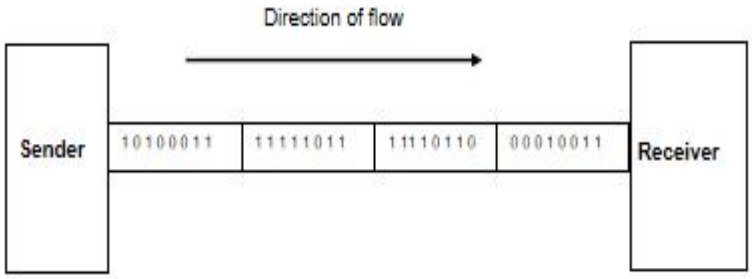
Characteristics of Asynchronous Transmission

- Each character is headed by a beginning bit and concluded with one or more end bits.
- There may be gaps or spaces in between characters.

Examples of Asynchronous Transmission

- Emails
- Forums
- Letters
- Radios
- Televisions

SYNCHRONOUS TRANSMISSION



In synchronous transmission, data moves in a completely paired approach, in the form of chunks or frames. Synchronisation between the source and target is required so that the source knows where the new byte begins, since there are no spaces included between the data.

Synchronous transmission is effective, dependable, and often utilised for transmitting a large amount of data. It offers real-time communication between linked devices.

An example of synchronous transmission would be the transfer of a large text file. Before the file is transmitted, it is first dissected into *blocks* of sentences. The blocks are then transferred over the communication link to the target location.

Because there are no beginning and end bits, the data transfer rate is quicker but there's an increased possibility of errors occurring. Over time, the clocks will get out of sync, and the target device would have the incorrect time, so some bytes could become damaged on account of lost bits. To resolve this issue, it's necessary to regularly re-synchronise the clocks, as well as to make use of check digits to ensure that the bytes are correctly received and translated.

Characteristics of Synchronous Transmission

- There are no spaces in between characters being sent.
- Timing is provided by modems or other devices at the end of the transmission.
- Special 'syn' characters goes before the data being sent.
- The syn characters are included between chunks of data for timing functions.

Examples of Synchronous Transmission

- Chatrooms
- Video conferencing
- Telephonic conversations
- Face-to-face interactions