

Swapan Purkait
swapan@nettech.in
+ 91 93315 90003
www.nettech.in



SECTION 1 Basic Networking Knowledge

In this section you are introduced to concepts associated with computer networks. The basic terms and concepts defined in this section are used throughout this course. You also learn about common network services (file, print, message, application, and database), as well as centralized and distributed network services. In addition, you learn about transmission media and how standalone computers physically connect to and interconnect segments of transmission media on various classes of networks.

Upon completing this section, you should be able to

- Define *computer networking*
- Contrast the features of the computing models.
- *local area network (LAN)*/*wide area network (WAN)*.
- Identify basic networking elements and describe the roles of clients, servers, peers, transmission media, and protocols.
- Identify the five basic network services.
- Identify the difference between centralized and distributed network architectures.
- Define the term transmission media as it relates to computer networks.
- Identify the appropriate transmission media to meet a stated business
- Identify the network connectivity devices and their functions.
- Identify the internetwork connectivity devices and their functions.

Define Computer Networking

Networking is the sharing of information and services. Computer networking provides the communication tools to allow computers to share information and abilities.

Computing Models and Network Development

Computer networking technologies are generally based on the following

- Centralized computing
- Distributed computing
- Collaborative computing

In addition, the following computing models are used to categorize the way networking services are provided:

- Client/Server
- Client/Network

Centralized Computing

In the centralized computing model, large centralized computers, called *mainframes*, are used to store and organize data. People enter data on mainframes using "local" devices called *terminals*. A terminal incorporates an input device, such as a keyboard, with some communication hardware so that a single mainframe can service requests from multiple remote terminals. In centralized computing, the mainframe provides all the data storage and computational abilities; the terminal is simply a remote input/output device. Computer networks were created when organizations began to require that mainframes share information and services with other mainframes.

Distributed Computing

In distributed computing, personal computers (PCs) have their own processing capabilities. In the distributed computing model, the application is divided into tasks, and each task is assigned to a computer for processing. The results of the processing can be sent as data to other computers. For example, in a distributed computing environment, a client accesses a database through the user interface (UI) running on the workstation. The database engine, running on the server, produces the requested reports.

Collaborative Computing Collaborative computing (also called *cooperative processing*) is a type of distributed computing using networked computers that “collaborate” by sharing processing abilities. In the collaborative computing model, two or more computers can share the same task. Collaborative computing allows computers to request processing resources from other computers as needed.

- Collaborative computing is a form of distributed computing.
- Collaborative computing allows tasks to be shared by computers as Distributed computing assigns each task to a single computer.
- Both use networked computers with processing capabilities; and both divide applications into tasks.

Client/Server Computing

In the client/server computing model, several clients (PCs) are connected to a server (PC).

- In the client/server model,
- Processing capabilities are distributed across multiple machines.
- Clients request services from servers.
- The server performs some of the processing for the client.

Applications used in a client/server network can be split into a front end that runs on the client and a *back end* that runs on the server.

In the client/server model, the following can be used:

- Standalone (non-networked) applications such as a spreadsheet program or a word processing program that runs on the client but saves its data on the server.
- A database application that provides a client interface for requests and a search engine on the server that locates records stored on one or more servers
- Programs, such as an email system, that use the server to share information

Client/Network Computing

In the client/network computing model, users log in to a network and connect to a set of services rather than to a specific server.

The five computing models are used to describe how network computing can be accomplished. Many applications are implemented as hybrids, using features of more than one model to accomplish their tasks.

Local Area Network (LAN) and Wide Area Network (WAN)

Computer networks include computers and computer operating systems associated with all computing models. A typical network includes mainframes, personal computers, and a variety of other computers and communication devices.

Computer networks are often classified by size, distance covered, the type of media used, or structure. Even though the distinctions are rapidly fading, the following network classifications are commonly used:

- Local area network (LAN)
- Wide area network (WAN)

Local Area Networks

A *local area network* (LAN) refers to a relatively small group of connected computers. LANs normally do not exceed tens of kilometers in size and provide data transmission services for a single entity, such as a company, a department, or a university. A LAN is normally contained within a building or campus and typically uses communication links that are owned and maintained by the group whose data the LAN carries. LAN transmission speeds are often measured in *megabits per second* (mbps).

Wide Area Networks

A *wide area network* (WAN) comprises multiple LANs. WANs interconnect LANs that can be at opposite sides of a country or located around the world. WANs often use telephone or satellite communications. Access to WAN links is often leased from a WAN services vendor who is responsible for maintaining the communication equipment. For most WAN links, the transmission speed attainable over the available bandwidth is measured in *kilobits per second*

(kbps). A special designation has also been given to two specific WAN categories: enterprise and global.

An enterprise network connects all LANs of a single organization. The term is normally used for networks connecting extremely large organizations, or for networks that cross regional or international boundaries.

A global network is one that spans the earth. Global networks might not cover the entire globe, but they cross multiple national boundaries and can include the networks of several organizations. The Internet is a good example of a global network.

Required Network Elements

All networks require the following elements:

- Individuals who need to *share* something
- A method or *pathway* for contacting each other
- Communication rules so that two or more individuals can *communicate*

The distinction between having a contact or communication *pathway communicating* is an important one. When you have a pathway to contact another individual, you might be heard but not understood. When you *communicate* with other people, you reach a mutual understanding.

This course covers the following basic elements of computer networks:

- Something to share: *Network Services*
- A pathway for contacting others: *Transmission Media*
- The rules for communication: *Protocols*

Network Services

Network services are the capabilities that networked computers share.

Network services are provided by numerous combinations of computer hardware and software. Depending upon the task, network services require data, input/output resources, and processing power to accomplish their goals.

In this course, the term *service provider* refers to the hardware and software combination that fulfills a specific service role. Computers and other network devices can provide different services or fill multiple roles simultaneously.

A service provider is not a computer: it is a subset of the computer software and hardware. You might understand computer networking better if you view a

service provider made up of software and hardware performs a task or role for *service requesters*.

In the computer industry, a distinction is often made between the following three types of service providers and requesters:

- *Servers are classified as service providers*. They only provide services.
- *Clients are classified as service requesters*. They only request services.
- *Peers can be classified as both a service requester or provider*. They provide and request services.

Depending on what software is running, a computer can simultaneously act as a client, a server, and a peer. Software determines the computer limitations and therefore its role as a client, server, or peer. However, most computers fill only one role at a time.

Computer networks are often classified as one of the following types:

- Peer-to-peer
- Server-centric

Peer-to-Peer Networks

Peer-to-peer networks allow any entity to both request and provide network services. Peer-to-peer network software is designed so that peers perform the same or similar functions for each other.

Server-Centric Networks

Server-centric networks involve strictly defined roles. By deserver-centric network places restrictions upon which entity can make requests or service them. The services offered by network service providers are discussed the Network Services segment of this course. Network services and computers or nodes do not always exhibit a one-to-one relationship.

Transmission Media

Transmission media is the pathway networked entities use to each other. Computer transmission media includes cable and wireless technologies that allow networked devices to contact one another. Transmission media cannot guarantee that other network devices will understand a message. It can, however, guarantee a message delivery.

Protocols

Protocols are the rules required to help entities communicate with or understand each other. A protocol can be one rule or a complete set of rules and standards that allow different devices to hold conversations.

Common Network Services

Computer applications require some combination of data processing power, and input/output resources to accomplish their tasks. Network services allow computers to share these resources using special network applications.

Many applications that provide network services are combined into a *network operating system* (NOS). Network operating systems are specifically designed to coordinate and provide multiple network services to other computer applications.

Local or desktop operating systems (OS) are the computer code that manages resources (CPU, memory, peripherals, and so on). A network operating system (NOS) is a specialized operating system that performs resource management tasks for multiple service requesters by coordinating the sharing of services on the network.

Following are the common network services:

- File services
- Print services
- Message services
- Application services
- Database services

Centralized versus Distributed Network Services

When you decide to implement a computer network, you must decide whether network services should be centralized, distributed, or some mixed or both.

Conceptually, distinct computers provide different network services. In reality, network services can be combined on a single computer or small group of computers (using a server-centric NOS) or distributed to all computers on the network (using a peer-to-peer NOS).

The following issues are involved in making service distribution

- Control of Resources
- Server specialization
- Choice of network operating systems

Control of Resources

Because computers fail and computer users ignore security standards, you should consider how network resources can be monitored and The easiest control strategy involves centralizing all the hardware and software required to service the network into one dedicated group that can be monitored by management applications. By centralizing the resources, you protect the services offered and determine which computer will support a particular network service. In contrast, when you distribute control, you allow many different computers to provide multiple services. When a service operates incorrectly in a distributed architecture, tracking down the offending party can be difficult.

Server Specialization

Server specialization means assigning network service roles to specific computers that have been optimized to fill that role. If you explicitly assign dedicated resources, you are making at least a partial commitment to centralized services.

Choice of Network Operating Systems

Although an organization can implement a specific subset of network services and organize them in a centralized or distributed manner, network architectures are often determined by available NOSs. A *server-centric* NOS provides centralized network services from dedicated servers.

Define the Term Transmission Media as it Relates to Computer Networks

Before a network service can be shared, network computers must have a pathway to contact other computers. Computers use electric currents, radio waves, microwaves, or light spectrum energy from the electromagnetic (EM) spectrum to transmit to each other. Computers use electronic voltage pulses or electromagnetic waves to send signals. The physical path through which the electrical voltages and EM waves travel is called *transmission media*.

Networked computers signal each other through the transmission media. Computer networks rely upon the ability of a transmission medium to accommodate a range of electric voltages or EM waves. For many portions of the EM spectrum, a number of transmission media types exist.

Common Computer Network Transmission Media

Transmission media can be classified as *cable and wireless*. Cable media provide a conductor for the electromagnetic signal, while wireless media do not. You would typically use a single cable media if you are installing a small LAN. You would also use special-purpose cable, or a combination of cable and wireless media, to link more distant stations such as those in a WAN. Wireless media are essential to networks with mobile computers and are widespread in enterprise and global networks. Each media type has certain characteristics.

You should be aware of their possible benefits and considerations as they relate to the following factors:

- Cost and ease of Installation
- Capacity
- Attenuation
- Immunity from interference and signal capture

Cable Media

Cable media are wires or fibers that conduct electricity or light. The following examples are covered in this section:

- Twisted pair cable
- Coaxial cable
- Fiber optic cable

Twisted Pair Cable

Twisted pair (TP) cable uses copper wire as telecommunication cable. Because copper is such a good conductor of electrons, copper wires do not constrain electromagnetic signals well. When two copper wires conduct electric signals in close proximity, a certain amount of electromagnetic interference occurs. This type of interference is called crosstalk. In addition, because of the electromagnetic range used, TP transmits and receives unwanted signals from other sources. Twisting the copper wires reduces crosstalk and signal emissions. Each intertwined strand conducts a current whose emitted waves are cancelled out by the other wires emissions.

Twisted pairs are formed by two insulated 22 to 26 gauge copper wires that are twisted around each other. When one or more twisted pairs are combined within a common jacket, they form a twisted pair cable.

The two types of TP cable are

- Unshielded
- Shielded

Coaxial Cable

Coaxial cable (Commonly called coax) is made of two conductors that share a common axis, hence the name (co, axis). Typically, the center of the cable is a relatively stiff solid copper wire or stranded wire encased in insulating plastic foam. The foam is surrounded by the second conductor, a wire mesh tube (some include conductive foil wrap), which serves as a shield from interference and signal capture. A tough, insulating plastic tube forms the cover of the cable.

Fiber Optic Cable

Fiber Optic cable is made of a light-conducting glass or plastic core surrounded by more glass, called cladding, and a tough outer sheath.

The center core provides the light path or *waveguide*; *the cladding* is composed of varying layers of reflective glass. The glass cladding is designed to refract light back into the core. Each core and cladding strand is surrounded by a tight or loose sheath. In tight configurations, the strand is completely surrounded by the outer plastic sheath. Loose configurations use a liquid gel or other material between the strand and the protective sheath.

In both cases, the sheath provides the necessary cable strength to protect the fiber from excessive temperature changes, bending, stretching or breaking.

Wireless Media

Wireless media transmit and receive electromagnetic signals without an electrical or optical conductor. However, because various forms of electromagnetic waves are used to carry signals, the EM waves are often referred to as media.

Few examples of wireless media are as follows:

- Radio wave
- Microwave
- Infrared light

Network Connectivity Devices and Their Functions

Connectivity devices are used to connect separate network or internetwork. A segment is a portion of the network transmission media that is assigned a network address and provides access to network resources for all attached clients and servers.

Connected segments can belong to the same network or to different networks, depending on the type of connectivity device used to connect

Network connectivity devices connect individual devices to a single network. For example, a computer or a printer would use network connectivity hardware to connect to UTP or some other medium.

To begin building a computer network, you need hardware devices to connect each computer to a media segment. These devices include

- Transmission media connectors
- Network interface boards
- Modem

You can connect multiple separate segments of transmission media to form one large network. For this purpose, you use the following networking devices:

- Repeaters
- Hubs (including multiport repeaters and switches)
- Bridges
- Multiplexers

Transmission Media Connectors

Transmission media connectors attach directly to the transmission media and serve as the physical interface between the media and computing devices. Every medium has one or more physical connectors that you can use.

Network Interface Boards

Network interface board includes all the circuitry needed to create the necessary physical and logical connections between your computer, or other device, and the transmission medium. Typically, a network interface board is a logic board you install in a computer to connect it to a cables connector.

However, a network interface card, a portion of the device software and a generic hardware port, or a number of external devices are all types of network interface boards.

The following terms also describe network interface boards or devices that attach to them:

- Transceivers
- Transceiver Network interface card (NIC)
- Transmission media adapter

Transceivers

transceiver is a device that can transmit as well as receive electric or electromagnetic signals on the transmission media. Most network interface boards use some type of transceiver. Transceivers are attached to the cable media by a connector. If you are using wireless media, transceivers are just transmitting and receiving devices. No mechanical connectors are required.

Network Interface Card

When the user device does not provide a suitable port or network interface board, you can use printed circuit boards called *network interface cards* (*network adapters*) include the circuitry and mechanical connections to convert the computers electric signals to the signals used on the medium. Some NICs provide more than one type of media connector. A NIC usually uses an internal transceiver (one that is built into the circuit board). However, some implementations require the use of external transceivers that attach to the cable or to the media connector of the NIC.

Transmission Media Adapter

When a network interface board uses a connector that is different from what is already attached to the transmission medium, a *transmission* is used. This adapter receives signals from one type of connector and converts them for use with another type. When you create a network, you must provide network interface boards for each computer.

Modems

A Modem (MOdulator/DEModulator) converts a computer digital signals to an analog transmission signal to use with telephone lines or microwave transceivers.

Modems are necessary because public telephone networks and microwave media use electromagnetic waves, but computers use electric pulses.

You can use modems to amplify signals when the signal from the transceiver is not powerful enough to travel the required distance without significant loss of data.

You can also use modems when more than one communication is to occur on the same medium. In this case, modems can be selected to use different electromagnetic frequency bands. In some instances, modems can take the place of NICs in connecting a device to a network. For example, you can dial in to your network from a computer with a modem, if a modem and a telephone connection available on a device on your network.

If you want remote access to your network using a modem to connect remote computers using a telephone line or microwave transceiver, you must configure a network modem (or similar device) on your network to provide remote users with access to network services.

Repeaters

Electromagnetic waves attenuate as they pass through a transmission medium. Each transmission medium can only be used for a certain distance. However, you can exceed the physical medium's maximum effective distance by using an amplification device called repeater.

One type of repeater, sometimes called an amplifier, amplifies all incoming electromagnetic waves, including undesirable noise.

Another type, referred to as a *signal regenerating repeater*, strips data out of the transmission signal. It then reconstructs and retransmits the signal on the other media segment. The new signal is an exact duplicate of the original signal, boosted to its original strength.

Signal regeneration is usually preferable; however, it requires more time and logic than simple amplification. In either case, the repeater typically connects two segments of the same network, overcoming the distance limitations of the network media.

Some repeaters also serve as transmission media adapters, connecting two different types of media. Many network implementations limit the number of repeaters that can be placed between the source and destination computers.

Hubs

Some network implementations require a central point of connection between media segments. These central points are referred to as *hubs*, *multiport repeaters*, or *concentrators*. Cables from network devices plug in to the ports on the hub.

Hubs receive transmissions from connected devices and transmit the signals to the other connected devices. The hub organizes the cables and transmits incoming signals to the other media segments.

The following types of hubs are discussed here:

- Active hubs
- Passive hubs
- Multiport repeaters
- Switches

Active Hubs

An *active hub*, which connects medium segments together, regenerates or amplifies signals. Because they generate signals, active hubs can extend the maximum cable length. All computers connected by active hubs still receive signals from all other computers.

Passive Hubs

A *passive hub*, which connects medium segments together, does not regenerate or amplify signals. It is not a repeater. The distance limitations on each segment connected to a passive hub are different than those applied to segments connected by active hubs. Additional limitations, such as not allowing two passive hubs to be connected to each other, might also be imposed.

Multiport Repeater

When a multiport repeater receives a transmission from an attached device, it regenerates the signal and then transmits it to all ports, regardless of which device the transmission is addressed to. Most active hubs are multiport repeaters.

Switches

When a switch receives a transmission, it only forwards the signal through the port that will allow the transmission to be delivered to the device to which it is addressed. In this way, a switch is similar to a bridge. Using switches, you can

set up a network where all the transmission media segments are permanently connected, but each segment is used only when a signal is directed to a computer on that segment. This can significantly improve performance by optimizing bandwidth use.

Bridges

A *bridge* extends the maximum distance of your network by connecting separate network segments. Bridges selectively pass signals from one segment to another based on the physical location of the destination device.

Bridges

- Receive all signals on all segments they are attached to.
- Determine the segment location of the source and destination devices for each signal received.
- Retransmit signals whose source and destination devices are on different segments out the port connected to the destination device.

Bridges accomplish these tasks by determining the physical location of the source and destination computers on the network media. These locations are referred to as addresses. Because they can filter signals by address, bridges usually divide an overloaded network into separate segments. The bridge prevents intrasegment traffic from reaching other segments. As long as intersegment traffic is not too heavy, this strategy reduces network traffic.

Network traffic is amount of signaling that occurs on the transmission media. Traffic is considered heavy when the transmission media is operating at or near its maximum capacity.

Suppose your network connects several hundred stations. Recently, network performance has fallen off because the network is heavily used. You can solve the problem by dividing the network's users into functional groups (groups are usually formed according to physical location and common requirements, such as server or application use). Users in one group use one media segment; users in the other group use another separate segment. Because you know that intersegment traffic is minimal, this strategy effectively isolates group traffic and improves network performance.

Multiplexers

Occasionally you use a transmission media that provides more capacity than a signal can use. To efficiently use the entire transmission media bandwidth, you can install *multiplexers*. A multiplexer combines two or more separate signals on a transmission media segment.

Identify Internetwork Connectivity Devices and Their Functions

Internetwork Connectivity Devices

In an internetwork, two or more networks are connected using *internetwork connectivity hardware*. Internetwork connectivity devices connect multiple independent networks together to provide access to remote resources.

The following devices connect distinct networks while protecting their individuality :

- Routers
- Brouters
- CSU/DSU

Routers

Routers connect two or more logically separate networks. Each network is identified by its *network address*, a logical name assigned to it. Each network in an internetwork must be assigned a unique network address.

Logical network subdivisions are called *subnetworks, or subnets*. A *subnetwork* is a logically separate (or independent) network that is physically connected to other networks as part of an internetwork.

Suppose you have four distinct subnetworks. Because each network transmits sensitive data, you want to keep all four separated. However, you also want to send occasional messages between users on the different networks. You could use a router to segregate the networks and pass data to the network for which it is intended.

Brouters

Many routers are really Brouters. Brouters are essentially routers that can also bridge. A brouter will first check to see if it supports the routing protocol being used by the packet. If not, rather than simply dropping the packet, the packet is bridged using physical address information. Here routing protocol refers to a set of rules or processes that are used to route data packets through a network.

Channel Service Unit/Digital Service Unit

Installation and maintenance costs for large amounts of transmission media and equipment can be high. As a solution to this problem, public and private service organizations provide transmission media for others to use. Public networks might require you to use *channel service units and digital service units to connect to their media*.

CSU and DSU are two components of a data communications equipment (DCE) device. A CSU/DSU device is also referred to as an integrated services unit (ISU).

Functionally, the CSU/DSU device is comparable to a modem. However, a CSU/DSU device is a digital-to-digital device, while modems are digital-to-analog devices.

CSU/DSUs prepare digital signals for transmission across digital WAN links. These devices ensure that the transmitted signal is of the proper signal strength and format. These units protect you, and other public network users, from electrical noise or unsafe electric voltages. In addition, they prepare your data for transmission according to the rules specified for the network. The CSU/DSU is usually attached to a router or remote bridge by a synchronous serial interface (such as a V.35 connection).

Summary

Computer networking has become increasingly important. LANs and WANs are common information-sharing tools that help people communicate using their computers. Acting as clients, servers, and peers, computers can provide the information and service exchange required by their users. Computer networks are valuable because of the services they provide or manage.

The following are common network services:

- File services
- Print services
- Message services
- Application services
- Database services

When an organization implements a computer network, decisions must be made on whether to centralize or distribute network services. The following factors must be considered:

- Control of resources
- Server specialization
- Choice of network operating systems

Before an organization can benefit from computer network communications, a physical path must be created for computers to contact one another. The path can be composed of one or more of the following cable and wireless media types:

- Twisted pair cable
- Coaxial cable
- Fiber optic cable

Connectivity hardware completes the path created by transmission media. It performs the following functions:

- Connects computers to the raw media
- Connects pieces or lengths of media together
- Uses the media capacity effectively
- Connects logically separate networks

The hardware and software combinations that serve these purposes are called network or internetwork connectivity devices. Network devices, which are used to form a single network, include :

- Transmission media connectors
- Network interface boards
- Modems
- Repeaters
- Hubs
- Bridges
- Multiplexers

Internetwork connectivity devices, which interconnect separate networks, include:

- Routers
- Brouters
- CSU/DUS



SECTION 2

Network Topologies

In this section you are introduced to the concept of a topology and you learn how this concept is used when designing and implementing a network.

Objectives

Upon completing this section, you should be able to

1. Define the term topology.
2. Define the types of network topologies.
3. Explain physical topology.
4. Explain logical topology.
5. Describe the role of media access schemes in a network.
6. Describe token ring networks.
7. Describe Ethernet networks.

Introduction

You should now be familiar with foundational network communication concepts. You have seen the technology required to create computer networks and discussed the reasons that network communication is an effective solution to a variety of problems. You have also seen and discussed the role of network servers and workstations, and the different classifications of networks. In this section, you learn about network topologies. To understand the idea of network topology, you were first introduced to general network concepts like communication models, network types, and network operating systems.

In this section, you learn in greater detail networking concepts you need for understanding

- How a network is laid out
- How data transmission is controlled on a network
- The role of media access schemes
- The topology of the two most common networks:
 - Token ring
 - Ethernet

What is a Topology?

A network topology is a pictorial representation of the layout of a network. Have you ever sketched a map for someone to tell them how to get somewhere, or created a floor plan of a house so you could get a better idea of how space is used?

These types of drawings are topologies. In simple terms, a topology is a pictorial representation of the layout of something.

Types of Network Topologies

Network topologies have two aspects:

- A physical topology
- A logical topology

Physical Topology

Let's use the street layout idea to begin to explain physical topology. If you had to plan the layout of the streets for a growing town, what kinds of things would you consider?

Among other things, you would make sure that all areas of town, both residential and business, are connected by the streets. You want to make sure that everyone has access to every part of town.

Computer networks must also be connected so that every computer has access to the entire network.

Logical Topology

When you plan the way traffic flows along the streets you laid out, what kinds of things do you consider? You would certainly consider which streets would carry the most traffic. From there you would consider which intersections need stop signs and which need traffic lights.

Perhaps some of your streets need to be one-way, some need to carry 2 lanes of traffic, and others 4 or more. You also have to consider which side of the road cars will travel on.

These are all considerations belonging to logical topology. As shown in the following figure, the physical topology accommodates the various options for the logical topology.

Physical Network Topologies

A physical network topology defines how network devices are connected. To understand how a network is laid out, you need to understand the following:

- Hardware specific to physical topologies
- Physical bus topologies
- Physical star topologies
- Physical ring topologies

Hardware Specific to Topologies

Cables, servers, and workstations are part of a physical network topology. You also need to know about two other components used in a network: hubs and repeaters.

Hubs

Hubs provide a common physical connection point for network devices. A hub is a single device that can be used for connecting many workstations to the network, as illustrated in the following figure.

Repeaters

Repeaters increase the distance over which a network signal can travel. As a signal travels through a cable it loses its strength due to resistance in the cable. This is overcome with the help of a repeater. When a repeater receives a weakening signal, it retransmits that signal at its original strength so the signal can arrive at its destination intact and undistorted. Most hubs have repeating capabilities built in.

Bus Topology

A physical bus network topology is a simple topology that uses one long cable, called a backbone. Short cables, called drop cables, can be attached to the backbone using T-connectors. The term bus, as it is used in electronics, has to do with transporting (bussing) signals from one point to another. You can remember the concept of a bus topology, because that's really all it does. The backbone is terminated at both ends to remove the signal from the wire after it has passed all devices. One end must also be grounded. Most bus topologies allow electromagnetic signals to travel in both directions.

Points to Consider: Bus Topology

Installation. A bus topology is relatively easy to install. You string the backbone cable from site to site. Because the shortest route is typically chosen between each device, buses require less cable than other topologies. However, the electrical and physical properties of cable impose constraints on bus networks. Every physical bus topology must limit the number of connections and the distance between them to maintain a readable signal.

Reconfiguration. Because most bus topologies are laid out to minimize the required amount of cable and to maintain the required distance between taps, reconfiguration tends to be moderately difficult. When the acceptable number of connections is reached, the backbone must be moved, modified, or replaced.

Ring Topology

The ring topology is a circle-like topology (or closed loop of point-to-point links). Each device connects to the ring or through a device, like a hub, and a cable. The feature that makes it a ring topology is that the layout is essentially a closed loop, rather than being ring-shaped.

Points to Consider: Ring Topology

Installation. Ring topologies are moderately simple to install. Because the ring requires a closed loop, more cabling is required than with bus networks. As with bus topologies, you must not exceed the maximum acceptable distance between repeating devices.

Reconfiguration. Ring networks become harder to reconfigure as the scale of relocations increases. Ring segments must be divided (or replaced with two new segments) each time a segment is changed. Rings are limited by a maximum ring length and number of devices.

Star Topology

Star topologies use a central device with drop cables extending in all directions. Each device is connected through a point-to-point link to the hub.

In star topologies, electric or electromagnetic signals travel from the networked device up its cable to the hub. From there the signal is sent to other networked devices.

Points to Consider: Star Topologies

Installation. Star topologies are moderately difficult to install. The design of the network is simple, but you must install a separate media segment for every arm of the star. Cabled star topologies require more cabling than most other topologies.

Reconfiguration. Star topologies are relatively easy to reconfigure. Moves, adds, and changes do not involve more than the connection between the changed networked device and a hub port.

Logical Network Topologies

After planning the physical layout of a network, you must consider the logical use of that layout. There are two commonly used logical topologies:

- Bus
- Ring

Recall the different ways that traffic can flow on a system of streets as an example of a logical topology. The logical topology of a network is, in essence, a strategy for directing signal flow.

Another way of looking at it is that logical topology is the set of traffic rules that keeps electronic signals traveling on the network cabling in an orderly fashion.

This traffic metaphor is a very valid way of looking at logical topology. As you will see, the terms network traffic and collisions are commonly used in networking terminology. Logical topologies are a necessary aspect of networking because electrical signals must be kept separate and distinct from each other, to keep them from colliding and distorting each other.

The devices that send the signals also must be kept in order. Devices must be told to take turns, or to watch for an opening in network traffic before sending out their messages.

Logical Bus Topology

In a logical bus topology, devices generate signals and send them throughout the network, regardless of the location of the intended receiver, as illustrated in the following figure.

A logical bus topology can only be used with the physical bus and the physical star topologies. The message sent to all devices in a logical bus topology contains information that says which device is to receive the message. The device that is supposed to receive the message receives it. Other devices ignore it.

A logical bus topology is necessary because network devices are not aware of other devices' physical locations. You cannot give a device "directions" for sending messages directly to other devices. For example, a device cannot know that another device is located "three nodes south, on the left."

So, a device must send the message to all directions. Then each device determines if the message was meant for that device.

Logical Ring Topology

In a logical ring topology, the signal is generated and travels along a specified path in a single direction:

The logical ring topology can be used with the physical ring and physical star topologies.

The difference between the logical ring and the logical bus is that signals sent in a logical bus go in all directions. Signals sent in a logical ring can only go in one direction.

A physical star topology can handle a logical ring topology because signals come in to the hub and are sent back out again to network devices in a predetermined order:

Media Access Schemes

A media access scheme is a set of rules that directs the signals sent over network transmission media. There are three types of media access schemes:

- Contention
- Token passing
- Polling

As you know from traffic rules that regulate vehicle traffic, controlling the direction of traffic flow is not enough to keep the streets safe.

For example, at busy intersections traffic lights and stop signs keep vehicles from being in the same place at the same time. Being in the same place at the same time causes vehicles to collide.

In the same way, being on network transmission media at the same time causes electronic network signals to collide. Therefore, a media access scheme (a set of rules for network traffic control) needs to be in place to control when network devices are allowed to transmit data signals.

If network devices operate without a media access scheme, devices transmit whenever they are ready. Sometimes they transmit at the same time. Signals combine and become damaged to the point that the signal data is lost. This is called a collision, and it destroys effective network communications. You cannot operate a network unless you can control or eliminate the effects of collisions.

Contention-Based Schemes

Contention-based access schemes allow network devices to transmit data whenever they want, regardless of other devices on the network. This scheme is simple and provides equal access rights to all stations. Unfortunately, the “transmit whenever ready” strategy has one important shortcoming: Stations sometimes transmit at the same time. When this happens, the result is a comingling of signals and information is lost. Contention-based access schemes call for stations to listen to the channel before transmitting. If the listening station detects a signal, it refrains from transmitting and tries again later. These are called CSMA (Carrier Sense, Multiple Access) schemes. They reduce collisions, but collisions still occur if two stations sense the cable, detect nothing, and subsequently transmit data at the same time. Therefore, this type of scheme must also be able to detect a collision. If a collision is detected, the signal is sent again. You will see these referred to as CSMA/CD protocols (meaning CSMA with collision detection).

Contention-based schemes handle average network traffic conditions very well but lose performance when network traffic gets heavy and more collisions occur.

Token-Passing Schemes

In token-passing schemes, an electronic signal (the token) is passed from one device to another. A token is a special message that temporarily gives media access control to the device holding the token. Passing the token around distributes access control among the network’s devices.

Each device knows which device it receives the token from and which device it should pass the token to. Each device periodically gets control of the token, transmits its data, and then retransmits the token for the next device to use. Protocols limit how long each device can control the token. Token-passing schemes work with physical ring and physical star topologies.

Token-passing schemes do not allow contention. One token exists on the media as devices take turns using the media. Under average traffic conditions, token-passing is slower than contention-based access schemes, but under heavy traffic conditions it performs better.

Polling Schemes

Polling is an access scheme that designates one device (called a controller, primary, or master) as a media access administrator. This device queries all other devices (referred to as secondaries) in a predetermined order to

determine whether they have information to transmit. The following figure shows the relationship of primary and secondary devices.

This access scheme is analogous to a classroom in which the teacher goes from student to student in a predetermined order. The teacher asks each student to speak for a preset amount of time and then moves on to the next student. The teacher is the primary and the students are the secondaries in this example.

Token Ring Networks

Token ring networks combine physical star and logical ring topologies with the token-passing media access scheme. This is a popular network configuration. When a station wants to transmit on the ring, it waits for a free token to pass. When it does, this source station takes the free token and adds data to it.

The station then sends the token out on the ring. As the now busy token is passed to each active station around the ring, each station checks to see which station the token is intended for. If a station is not the recipient of the token, it re-sends the token along the ring. If a station is the recipient, it copies the data that the source station added to the token.

Then it adds data to the token to indicate that it has recognized the address and copied the data. It then sends the altered token out to the ring.

The token continues around the ring until it reaches the source station. When the source sees that the data has been received and copied, it generates a new free token, which it passes to the next active station on the ring. One token is allowed to be on a ring at a time.

Ethernet Networks

Ethernet is a popular network topology standard that uses logical bus topology and can be laid out in either a physical bus or physical star topology.

Ethernet uses a contention-based access scheme. Ethernet moves messages around the network in packets of information that include the source station address, the destination station address, the type of data that must be moved, and the data itself. To send packets, a device on the network must first listen to see if any other device is using the cable. When the cable appears to be clear of traffic, the device sends its packets. If two devices are trying to transmit over the cable at the same time, the packets might physically collide with each other on the wire. The result can be damaged and unreliable packets. Ethernet expects some of these collisions and is prepared to handle them.

When a collision occurs, a signal is sent to ensure that the collision has been recognized around the network. The devices competing for the cable's bandwidth retransmit, but they delay their retransmission by a random amount of time to ensure that collisions are eliminated. When devices become aware of a packet on the wire, they check to make sure the packet is not a fragment of a packet that has been damaged by a collision. If it is a whole packet, the devices check the address. A packet addressed to a device is checked for integrity by that device before it is processed.

TCP/IP Addressing

In this section, we review the basics of the TCP/IP addressing, subnet masking.

Describe TCP/IP Addressing

Every protocol suite defines some type of addressing that identifies computers and networks. Each system attached to an IP-based Internet requires a unique, 32-bit Internet address value.

The first part of an Internet address identifies the network on which a host resides. A host can be any network device such as a printer, a workstation, or a server.

The second part of an Internet address identifies the particular host on the given network. All hosts on a network share the same network number, or network prefix, but each host must have a unique host number.

IP Address Classes

To support different sizes of networks, IP address space is divided into five address classes, A through E. Only classes A through C are assigned to hosts.

Each class designation fixes the boundary between the network number and the host number at a different point within the 32-bit address.

Class A 1 - 127
Class B 128 - 191
Class C 192 - 223
Class D 224 - 239 (Multicast)
Class E 240 - 255 (Reserved Experimental)

Following is a brief explanation of address classes:

Class A Addresses. In a class A address, the first byte is in the 0 to 127 range and also identifies the network; the final three bytes identify the node. The first bit must be zero.

Up to 126 class A networks can be created, each having up to 16,777,216 hosts.

Class B Addresses. In a class B address, the first byte is in the 128 to 191 range (the first two bits of the first byte are 1 and 0). In class B addresses, the first two bytes identify the network and the last two bytes identify the node on the network.

There are 16,384 possible class B networks. Each class B network can have up to 65,534 hosts.

Class C Addresses. In a class C address, the first byte is in the 192 to 223 range (the first three bits of the first byte are 1, 1, and 0). In class C addresses, the first three bytes identify the network and the last byte identifies the node.

There are 2,097,152 possible class C networks. Each class C network can have up to 255 hosts.

Class D Addresses. In a class D address, the first byte is in the 224 to 239 range (the first four bits of the first byte are 1, 1, 1, and 0).

Class D addresses are used for multicast packets. Multicast packets are used by a host to transmit messages to a specified group of hosts on the network. Multicast packets are typically exchanged between routers only.

Class E Addresses. In a class E address, the first byte is in the 240 to 255 range (the first five bits of the byte are 1,1,1,1, and 0). Class E addresses are reserved for experimental use and potential future addressing modes. Class E addresses are typically used for broadcasts.

IP Address Types

In addition to address classes, IP addresses can also be categorized by the number of hosts represented by the address. The following categories are used:

Unicast. This category includes addresses that allow for communication between one source sending data and one source receiving it. The single interface, or unicast, is specified by the destination address. This way, communication between any two hosts on the shared network doesn't affect any of the other hosts.

Multicast. This category includes addresses that refer to a group of hosts by using a single IP address; identified by IPv4 class D addresses. Simply, a subset of the computers on a network agree to listen to a given multicast address. Every computer in this multicast group can be reached with a single packet transmission.

Broadcast. This category includes messages that are transmitted to every host on the network. One particular class E address, 255.255.255.255, is used to identify a broadcast message. When the destination IP address is 255.255.255.255, the message is directed to all hosts on the network from which the broadcast originated. Routers do not typically forward broadcast messages to other networks.

Anycast. Similar to multicast, an anycast address references a group of systems. It transmits data by finding the closest member of a group and sends messages only to that member. Anycast is only available with IPv6.

Describe Subnet Masking

A subnet mask is an extension of the IP addressing scheme that allows a site to use a single network address for multiple physical networks. It is important to understand the purpose of subnets. You should also know how to define a subnet mask, how to create a subnet address from a subnet mask, and how to use subnet masks.

All hosts and networks must have unique addresses. This can be a problem if you are connected to the Internet and have been assigned fewer network addresses than the number of networks your company has.

TCP/IP allows you to extend a given IP network number into additional network addresses by borrowing bits from the host address bytes. This process of creating subnets on the network uses a technique called subnet masking.

As a network administrator, you are faced with the problem of assigning unique network addresses to each network within your company using a single address that has been assigned by interNIC.

To do this, you use subnet masking to redefine how each IP address within the corporation is partitioned between network and host.

Purpose of Subnets

Subnets are created for the following reasons:

To expand the network. If you reach the physical limitations of your network, you can extend the network and connect additional hosts by adding a router and creating subnets.

To reduce congestion. Traffic between hosts on a single network uses network bandwidth. As a result, the more hosts you have, the more bandwidth is required. Splitting a single network into smaller, separate subnets reduces the number of hosts per network. If hosts on a smaller network communicate mostly to other hosts on the same network, congestion is reduced.

To reduce CPU use. More hosts on a network cause more broadcasts on that network. Even if a broadcast is not sent to all hosts, each host must listen to every broadcast before deciding to accept or discard it. This uses host CPU capabilities.

To isolate network problems. By splitting a larger network into smaller networks, you limit the impact of one subnet's problems on another.

To improve security. On a broadcast network medium such as Ethernet, each host has access to all packets sent on the network. By restricting sensitive network traffic to only one network, other users on other subnets can be prevented from accessing secure data.

Subnets also ensure that the structure of a network is never visible outside your organization's private network. The route from the Internet to your registered IP address is the same.

To use multiple media. Having subnets allows you to combine different media by putting each type of media on a different subnet.

Defining a Subnet Mask

A subnet mask is a 4-byte number that is logically "ANDed" with an IP address to identify the network and host address of a host. TCP/IP requires that all IP addresses be assigned a subnet mask even if the network is not segmented into subnets.

Any bit that is part of the network address is assigned a value of 1 in the mask; any bit that is part of the host address is assigned a value of 0 in the mask.

The subnet mask is defined using part of the host portion of the IP address. The host portion you use depends on the class of the network address you were assigned.

Default mask for Class A, B and C

Class A 255.0.0.0
Class B 255.255.0.0
Class C 255.255.255.0

Private Network Addresses

To overcome IPv4 address shortages, users have identified many workarounds. One of the most successful is using private network addresses for your network. This strategy is sometimes called 10-Netting.

The 10-Netting approach works like this: Recall that several addresses are reserved for private networks. These addresses are filtered out by Internet routers and do not conflict with registered addresses. Private address blocks include the following (as per RFC 1918):

Class Beginning Address Ending Address

Class A 10.0.0.0 10.255.255.255
Class B 172.16.0.0 172.31.255.255
Class C 192.168.0.0 192.168.255.255

You can implement 10-netting by assigning hosts on the private, internal part of the network IP address from Table 1-10 and placing a router between the private internal network and the public network (the Internet).

The private interface on the router is assigned an address from the private network. The public interface on the router is assigned a registered IP address.

The router runs network address translation (NAT) software that translates addresses when packets pass from the private network to the public network.

This strategy has many advantages.

If the 10.0.0.0 range is selected, the private network can have an entire Class A network address. This allows for up to 16,777,216 hosts.

Only one registered IP address is required for the entire private network.

Security is increased because the entire private network appears to have only one IP address on the public network.

Identify the Role of TCP/IP Ports

An IP port is a number assigned to a service running on an IP host. The number is used to link the incoming data to the correct service.

TCP/IP port numbers are divided into three ranges:

Well-Known Ports, ranging from 0 through 1023

Registered Ports, ranging from 1024 through 49151

Dynamic or Private Ports, ranging from 49152 through 65535

Standard Port Numbers

Well-known ports are standard port numbers used by everyone. Well-known ports are assigned by the IANA (Internet Assigned Numbers Authority) and on most systems can only be used by system processes or by programs executed by privileged users.

Port Number Keyword Description

21 Port used by FTP

23 Port used by Telnet

25 Port used by SMTP

53 Domain Name Server

80 Port used by HTTP

110 pop3 Post Office Protocol - version 3

Protocols Used with TCP/IP

In this section you learn the function of the various protocols within the TCP/IP protocol suite.

Objectives

1. Describe Internet Protocol (IP)
2. Describe Transmission Control Protocol (TCP)
3. Describe User Datagram Protocol (UDP)
4. Describe Internet Control Message Protocol (ICMP)
5. Describe Internet Group Management Protocol (IGMP)
6. Describe Network Time Protocol (NTP)
7. Describe Telnet Protocol (TELNET)
8. Describe Hypertext Transport Protocol (HTTP)
9. Describe File Transfer Protocol (FTP)
10. Describe Trivial File Transfer Protocol (TFTP)
11. Describe Simple Mail Transfer Protocol (SMTP)
12. Describe Post Office Protocol (POP3)
13. Describe Internet Relay Chat (IRC) Protocol

Describe Internet Protocol

Purpose of IP

The Internet Protocol (IP) is used in packet-switched networks (catenet). IP transmits blocks of data, called datagrams, from sources to destinations. Sources and destinations are hosts identified by fixed-length addresses. IP can also fragment and reassemble long datagrams, if necessary, for transmission through small-packet networks.

IP does not provide end-to-end data reliability, flow control, sequencing, or other services commonly found in host-to-host protocols. IP relies on the services of its supporting networks to provide various types and qualities of service.

How IP Works

IP provides two basic functions: addressing and fragmentation.

- IP uses the addresses carried in the header to transmit datagrams to their destinations.

- IP uses fields in the header to fragment and reassemble Internet datagrams for transmission through small-packet networks.

An Internet module resides in each host engaged in Internet communication and in each gateway that interconnects networks.

These modules share common rules for interpreting address fields and for fragmenting and assembling Internet datagrams. In addition, these modules (especially in gateways) make routing decisions and provide other functions.

IP treats each datagram as an independent entity.

IP uses four key features in providing its service:

Type of Service:

Indicates the quality of the service wanted. The type of service provides a generalized set of parameters that characterize the service choices provided in the networks that make up the Internet.

Gateways use the "type of service" value to determine the actual transmission parameters for a particular network, the network to be used for the next hop, or the next gateway when routing an Internet datagram.

Time to Live:

Indicates an upper boundary on the lifetime of an Internet datagram. It is set by the sender of the datagram and reduced at the points along the route where it is processed. If the time to live reaches 0 before the Internet datagram reaches its destination, the Internet datagram is destroyed. The time to live can be thought of as a self-destruct time limit.

Options:

Provides control functions that might be useful in some situations but that are unnecessary for the most common communications. The options include functions for timestamps, security, and special routing.

Header Checksum:

Verifies that the information used in processing the Internet datagram has been transmitted correctly. If the data contains errors, the header checksum will fail. The datagram is then discarded by the entity that detects the error.

Describe

Transmission Control Protocol (TCP)

TCP is a highly reliable host-to-host protocol in packet-switched networks and internetworks. TCP provides process-to-process communication in multinetwork environments.

TCP interacts between user or application processes and a lower-level protocol such as IP.

TCP provides a set of calls for manipulating data.

For example, TCP provides calls to open and close connections and to send and receive data on established connections. TCP can also communicate with application programs asynchronously.

The interface between TCP and lower-level protocols is essentially unspecified. However, the two levels can pass information to each other asynchronously.

Typically, the lower-level protocol specifies this interface.

TCP is designed to work in a very general environment of interconnected networks.

Describe User Datagram Protocol (UDP)

UDP provides a datagram mode of packet-switching in an internetwork.

UDP assumes that IP is used as the underlying protocol.

UDP allows application programs to send messages to other programs with a minimum of protocol mechanism. UDP is transaction oriented; delivery and duplicate protection are not guaranteed.

UDP offers a minimal transport service non-guaranteed datagram delivery and gives applications direct access to the datagram service of the IP layer.

The only services UDP provides over IP are checksumming of data and multiplexing by port number.

UDP does not maintain an end-to-end connection with the remote UDP module; it only pushes the datagram out on the network and accepts incoming datagrams off the network.

UDP is used by applications that do not require the level of service provided by TCP or applications that want to use communications services (such as multicast or broadcast delivery) not available from TCP.

Network File System (NFS) and Simple Network Management Protocol (SNMP) are examples of network applications that use UDP. The service is little more than an interface to IP.

Therefore, an application program running over UDP must deal directly with end-to-end communication problems that a connection-oriented protocol would have handled. For example, UDP cannot provide

- Retransmission for reliable delivery
- Packetization and reassembly
- Flow control
- Congestion avoidance

The fairly complex interactions between IP and TCP are mirrored in the interactions between UDP and many applications using UDP.

UDP is one of two main protocols that reside on top of IP.

Describe Internet Control Message Protocol (ICMP)

Although architecturally layered on IP, ICMP is a control protocol that is an integral part of IP. For example, ICMP uses IP to carry its data end-to-end just as a transport protocol like TCP or UDP does.

ICMP provides error reporting, congestion reporting, and first-hop gateway redirection.

ICMP messages are grouped into two classes: error messages and query messages.

ICMP error messages include the following:

- Destination Unreachable
- Redirect

- Source Quench
- Time Exceeded
- Parameter Problem

ICMP query messages include the following:

- Echo
- Information
- Timestamp
- Address Mask

If an ICMP message of unknown type is received, it is silently discarded.

Every ICMP error message includes the Internet header and at least the first 8 data octets of the datagram that triggered the error. This header and data must be unchanged from the received datagram.

If the Internet layer is required to pass an ICMP error message to the transport layer, the IP protocol number must be extracted from the original header and used to select the appropriate transport protocol entity to handle the error.

Describe Internet Group Management Protocol (IGMP)

IGMP is a protocol used by hosts and gateways on a single network to establish hosts' membership in particular multicast groups.

The gateways use this information with a multicast routing protocol to support IP multicasting across the Internet.

Implementation of IGMP is optional. A host can still participate in multicasting local to its connected networks without IGMP.

Describe Network Time Protocol (NTP)

NTP synchronizes a set of network clocks using a set of distributed clients and servers. NTP is built on the User Datagram Protocol (UDP), which provides a connectionless transport mechanism.

This protocol evolved from the Time Protocol and the ICMP Timestamp message and is a suitable replacement for both.

NTP specifies the precision and estimated error of both the local clock and the reference clock it might be synchronized to.

However, the protocol itself specifies only the data representation and message formats. It does not specify the synchronizing algorithms or filtering mechanisms.

Other mechanisms have been specified in the Internet protocol suite to record and transmit when an event takes place, including the Daytime protocol and IP Timestamp option. The NTP is not meant to displace either of these mechanisms.

NTP is designed to connect a few primary reference clocks to centrally accessible resources such as gateways. These references are synchronized by wire or radio to national standards.

The gateways use NTP to cross-check the primary clocks and resolve errors caused by equipment or communication failures. Some of the local-net hosts, serving as secondary reference clocks, run NTP with one or more of these gateways.

To reduce the protocol overhead, the local-net hosts redistribute time to the remaining local-net hosts.

In the interest of reliability, selected hosts might be equipped with less accurate but less expensive radio clocks and used for backup in case of failure of the primary and secondary clocks or the communication paths to them.

In the standard configuration, a subnetwork of primary and secondary clocks assume a hierarchical organization, with the more accurate clocks near the top and the less accurate below.

NTP provides information that can be used to organize this hierarchy on the basis of precision or estimated error. NTP can even serve as a rudimentary routing algorithm to organize the subnetwork itself.

However, the NTP protocol does not include a specification of the algorithms for doing this.

Describe Telnet Protocol (TELNET)

TELNET provides a remote login capability on TCP. The operation and appearance is similar to keyboard dialing through a telephone switch. On the command line the user types TELNET DELTA and receives a login prompt from the computer called DELTA.

TELNET works well; it is an old application and has widespread interoperability. Implementations of TELNET usually work between different operating systems. For instance, a TELNET client might be on VAX/VMS and the server on UNIX System V.

TELNET, TCP/IP's virtual terminal protocol, allows a user from one host to log in to another host while appearing to be directly attached to the terminal at the remote system. This is TCP/IP's definition of a virtual terminal.

The general format of the TELNET command is

```
TELNET [ IP_address | host_name] [ port]
```

A TELNET connection is initiated when you enter the TELNET command and supply either a host name or an IP address. If neither are given, TELNET asks for one after the TELNET application begins.

Many of the TELNET features are accessed by specifying a port number in addition to a host's address. Knowledge of port numbers provides another mechanism for users to access information with TELNET.

You can use TELNET to access a remote client and provide the same functionality as local client software. You can do this by specifying a port number with the TELNET command.

Just as TCP/IP hosts have a unique IP address, an application on the host is associated with an address, which is called a port.

The Finger utility, for example, is associated with port number 79. In the absence of a Finger client, you could TELNET to port 79 using a remote host to provide the same information.

You can finger another host with TELNET by using a command like

```
TELNET host_name 79
```

Other well-known TCP/IP port numbers include 20 (FTP data transfer), 21 (FTP control), 25 (SMTP), 43 (whois), 70 (Gopher), and 185 (KNOWBOT).

Some services are available on the Internet using TELNET and special port numbers.

After logging in using TELNET, you can do anything on the remote host that you could do if you were on a directly connected terminal or had dialed up by modem.

You can use any commands that are available on the remote system that you are attached to.

Describe Hypertext Transport Protocol (HTTP)

HTTP allows basic hypermedia access to resources available from diverse applications.

HTTP is an application-level protocol that can be used to transport, retrieve, search for, update, and annotate information that is distributed and collaborative, and that includes hypermedia.

HTTP provides an open-ended set of methods and headers that indicate the purpose of a request.

HTTP/1.1 is based on the Uniform Resource Identifier (URI). HTTP/1.1 uses a uniform resource locator (URL) or uniform resource name (URN) to indicate the resource that a process should be applied to.

Messages are passed in a format similar to the format used by Internet mail as defined by the Multipurpose Internet Mail Extensions (MIME).

HTTP is also used as a generic protocol for communication between user agents and proxies or gateways to other Internet systems, including those supported by the SMTP, NNTP, FTP, Gopher, and WAIS protocols.

Describe File Transfer Protocol (FTP)

FTP is a useful and powerful TCP/IP utility for the general user. FTP allows you to upload and download files between local and remote hosts.

Anonymous FTP, in particular, is commonly available at file archive sites to allow users to access files without having to pre-establish an account at the remote host. The general form of the FTP command is

```
FTP [ IP_address | host_name]
```

You initiate an FTP control connection to a host by supplying a host name with the FTP command; optionally, you could use the host's IP address in dotted decimal form.

If you do not supply a host name or an IP address in the command line, you can initiate a connection to a host by entering "OPEN host_name" or "OPEN IP_address" after the FTP application has been started.

The remote host then asks you for a username and password.

If you are a legitimate, registered user of this host and you supply a valid username and password, you have access to all files and directories this username has rights to.

For anonymous FTP access, you can use "anonymous" as the username and "guest" as the password. (An increasing number of systems ask an anonymous FTP user to supply his or her Internet address or email address as the password.)

Describe Trivial File Transfer Protocol (TFTP)

TFTP is a simple protocol used to transfer files.

It runs on top of the Internet User Datagram Protocol (UDP) and is used to move files between machines on different networks implementing UDP. (TFTP can also be implemented on top of other datagram protocols.)

Because TFTP is designed to be small and easy to implement, it lacks most of the features of a regular FTP. The only services it provides are reading and writing files and sending mail to and from a remote server.

Like other Internet protocols, TFTP passes 8-bit bytes of data, but it cannot list directories or provide user authentication.

TFTP supports three modes of transfer:

1. NETASCII. NETASCII is an 8-bit ASCII defined in USA Standard Code for Information Interchange with the modifications specified in Telnet Protocol Specification.

2. Octet. This mode replaces the binary mode.

3. Mail. NETASCII characters are sent to a user rather than a file. The mail mode is obsolete and should not be implemented or used. Additional modes can be defined by pairs of cooperating hosts.

A TFTP transfer begins with a request to read or write a file, which also includes a request for a connection. If the server grants the request, the connection is opened and the file is sent.

The file is divided into data packets. Each data packet contains one block of data (512 bytes) and must be acknowledged by an acknowledgment packet before the next packet can be sent. A data packet of less than 512 bytes signals termination of a transfer.

Both machines involved in a transfer are considered senders and receivers. One sends data and receives acknowledgments; the other sends acknowledgments and receives data.

If a packet gets lost in the network, the intended recipient times out and retransmits its last packet (which might be data or an acknowledgment). The sender of the lost packet then retransmits the lost packet.

The sender keeps one packet on hand for retransmission. The acknowledgment guarantees that all older packets have been received.

Most errors cause termination of the connection. When the error occurs, the sender sends an error packet. The error packet is neither acknowledged nor retransmitted.

If a TFTP server or user terminates after sending an error message, the other end of the connection might not receive the message. Time-outs are used to detect a termination when the error packet has been lost.

Errors are caused by three types of events:

- Not being able to satisfy the request (file not found, access violation, or no such user)
- Receiving a packet that cannot be explained by a delay or duplication in the network (an incorrectly formed packet)

- Losing access to a necessary resource (disk full or access denied during a transfer)

Only one error condition, the source port of a received packet being incorrect, does not cause TFTP to terminate. In this case, an error packet is sent to the originating host.

To simplify implementation, this protocol is very restrictive. The fixed-length blocks make allocation straight forward, and the lock step acknowledgement provides flow control and eliminates the need to reorder incoming data packets.

Describe Simple Mail Transfer Protocol (SMTP)

SMTP is used to transfer mail reliably and efficiently.

SMTP is independent of the particular transmission subsystem and requires only a reliable, ordered data-stream channel.

An important feature of SMTP is its capability to relay mail across transport service environments. A transport service provides an interprocess communication environment (IPCE). A process can communicate directly with another process through any mutually known IPCE.

Mail is an application or use of interprocess communication. Mail can be communicated between processes in different IPCEs by relaying through a process connected to two (or more) IPCEs.

More specifically, mail can be relayed between hosts on different transport systems by a host on both transport systems.

Describe Post Office Protocol (POP3)

POP3 allows a workstation to dynamically access a mail drop on a server host. Usually, POP3 is used to allow a workstation to retrieve mail that the server is holding for it.

On certain types of smaller nodes in the Internet, maintaining a message transport system (MTS) is often impractical.

For example, a workstation might not have sufficient resources (cycles or disk space) to permit an SMTP server and the associated local mail delivery system to be kept resident and continuously running.

Similarly, keeping a workstation connected to an IP-style network for long amounts of time can be expensive or impossible. (The node is lacking the resource known as connectivity.)

Despite this, you must manage mail on these smaller nodes, which often support a user agent (UA) to aid the tasks of mail handling. To solve this problem, a node that can support an MTS entity offers a mail drop service to these smaller nodes.

All messages transmitted during a POP3 session are assumed to conform to the standard format of Internet text messages.

The byte count for a message on the server host might differ from the octet count assigned to that message due to local conventions for designating end-of-line.

A client host refers to a host making use of the POP3 service; a server host refers to a host that offers the POP3 service.

For example, if the POP3 server host internally represents end-of-line as a single character, the POP3 server simply counts each occurrence of this character in a message as 2 octets.

The lines in the message that start with the termination octet are not counted twice, because the POP3 client removes all byte-stuffed termination characters when it receives a multi-line response.

Describe Internet Relay Chat (IRC) Protocol

IRC allows you to use your workstation to chat online. The IRC protocol is a text-based protocol.

IRC has been designed to be used with text-based conferencing. It has been developed on systems using TCP/IP, although TCP/IP is not a requirement for this.

IRC is a teleconferencing system that is well-suited (through the use of the client-server model) to run on many machines in a distributed fashion.

A typical setup involves a single process (the server) forming a central point for clients (or other servers) to connect to, and performing the required message delivery/multiplexing and other functions.

- X -