**Section- A**

**Introduction to Data Communication & Networks**

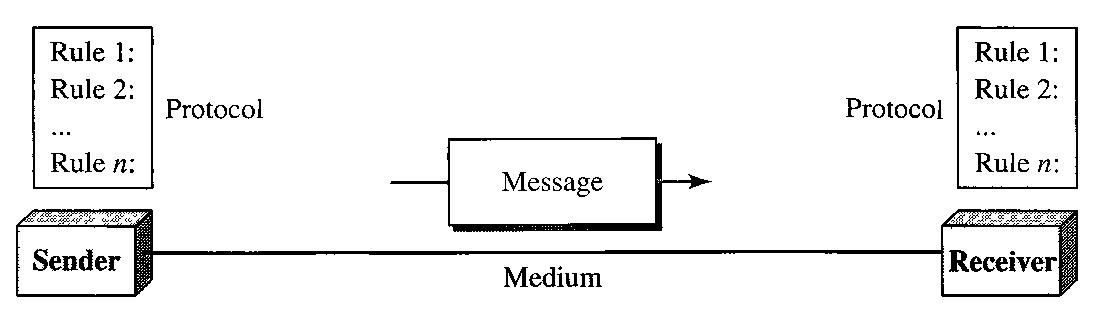
**1.1 DATA COMMUNICATIONS**

Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs). The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

1. **Delivery**. The system must deliver data to the correct destination. Data must be received bythe intended device or user and only by that device or user.
2. **Accuracy**. The system must deliver the data accurately. Data that have been altered intransmission and left uncorrected are unusable.
3. **Timeliness**. The system must deliver data in a timely manner. Data delivered late are useless.In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.
4. **Jitter**. Jitter refers to the variation in the packet arrival time. It is the uneven delay in thedelivery of audio or video packets. For example, let us assume that video packets are sent every
5. ms. If some of the packets arrive with 30-ms delay and others with 40-ms delay, an uneven quality in the video is the result.

**Components**

A data communications system has five components:



1. **Message**. The message is the information (data) to be communicated. Popular forms ofinformation include text, numbers, pictures, audio, and video.
2. **Sender**. The sender is the device that sends the data message. It can be a computer,workstation, telephone handset, video camera, and so on.
3. **Receiver**. The receiver is the device that receives the message. It can be a computer,workstation, telephone handset, television, and so on.
4. **Transmission medium**. The transmission medium is the physical path by which a messagetravels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

5. **Protocol**. A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating.

**Fnnctions of Protocol :**

•**Syntax**. The term syntax refers to the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.

•**Semantics**. The word semantics refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation?

•**Timing**. The term timing refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

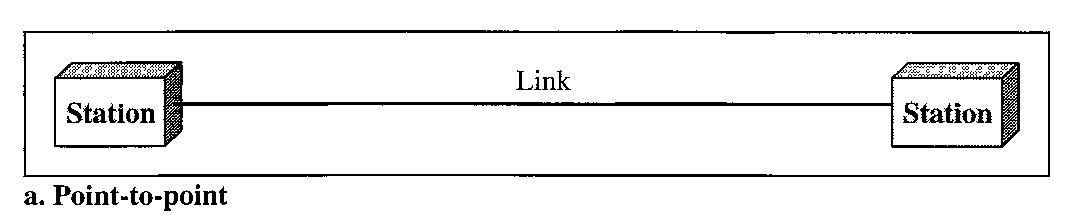
**Standards Organization :**

**Line Configuration :**

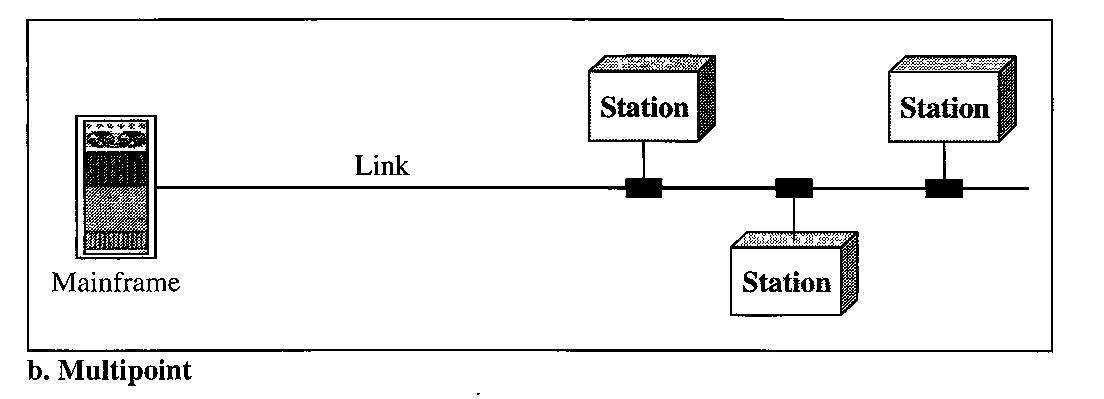
A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. For communication to occur, two devices must be connected in some way to the same link at the same time. There are two possible types of connections: point-to-point and multipoint.

**Point-to-Point** A point-to-point connection provides a dedicated link between two devices. Theentire capacity of the link is reserved for transmission between those two devices. Most point-to-

point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible.



**Multipoint** A multipoint (also called multidrop) connection is one in which more than twospecific devices share a single link. In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.



**Transmission Modes** :

**Simplex**

In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive. Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.

**Half-Duplex**

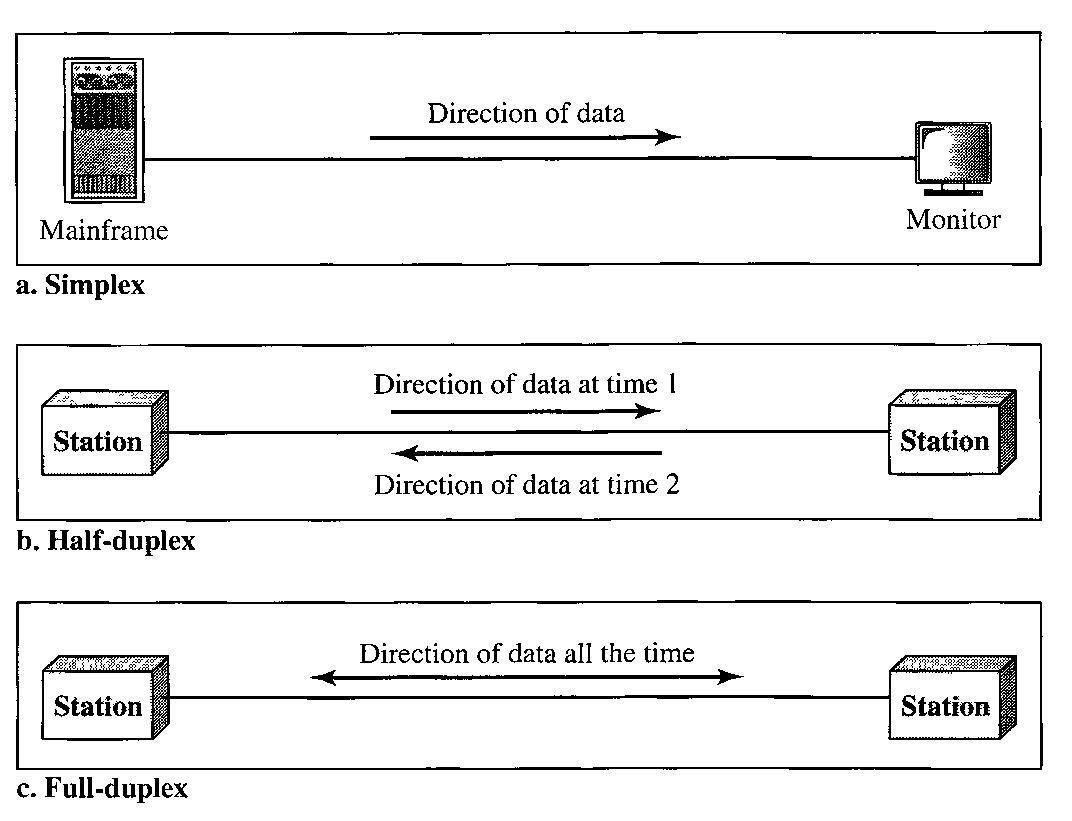
In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Walkie-talkies and CB (citizens band) radios are both half-duplex systems.

The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction.

**Full-Duplex**

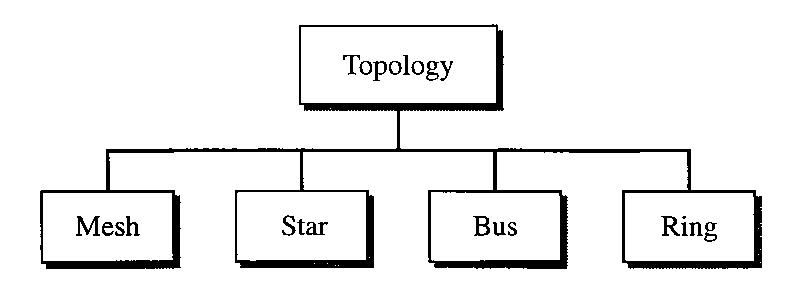
In full-duplex made (also, called duplex), both stations can transmit and receive simultaneously. In full-duplex mode, signals going in one direction share the capacity of the link with signals going in the other direction. This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving; or the capacity of the channel is divided between signals travelling in both directions.

One common example of full-duplex communication is the telephone network. The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions

****

**Network Topologies :**

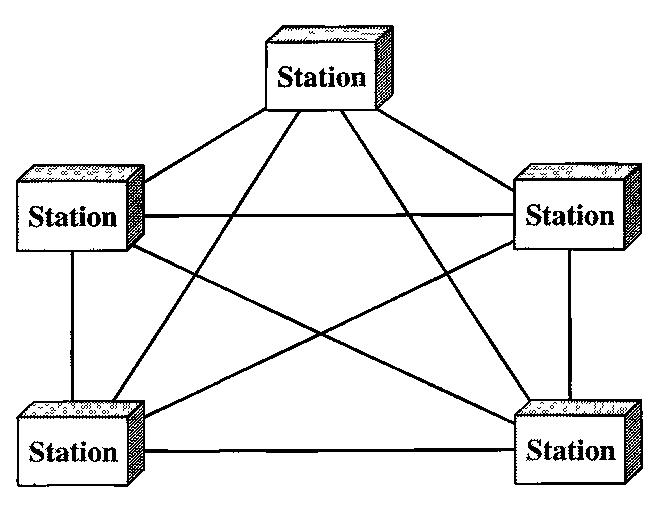
The term physical topology refers to the way in which a network is laid out physically. Two or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another. There are four basic topologies possible: mesh, star, bus, and ring.



**Mesh** In a mesh topology, every device has a dedicated point-to-point link to every other device.The term dedicated means that the link carries traffic only between the two devices it connects. To find the number of physical links in a fully connected mesh network with n nodes, we first consider that each node must be connected to every other node. Node 1 must be connected to n-1 nodes, node 2 must be connected to n-1 nodes, and finally node n must be connected to n-1 nodes. We need n(n-1) physical links. However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2. In other words, we can say that in a mesh topology, we need

**n(n - 1) / 2**

duplex-mode links.



A mesh offers several advantages over other network topologies.

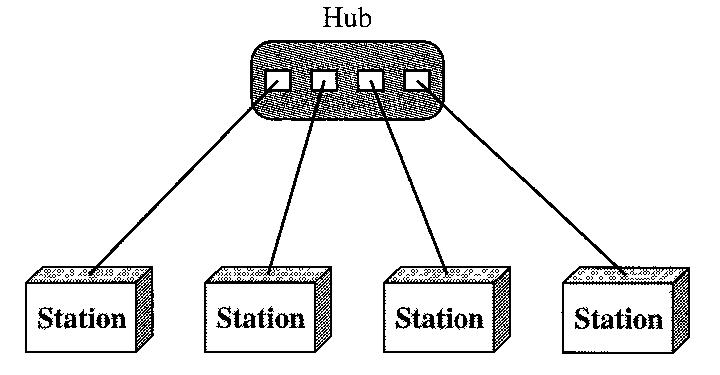
1. The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
2. A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.
3. There is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages.
4. Point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.

The main disadvantages of a mesh are related to the amount of cabling and the number of I/O ports required.

1. Because every device must be connected to every other device, installation and reconnection are difficult.
2. The sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.
3. The hardware required to connect each link (I/O ports and cable) can be prohibitively

expensive.

**Star Topology** In a star topology, each device has a dedicated point-to-point link only to acentral controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device



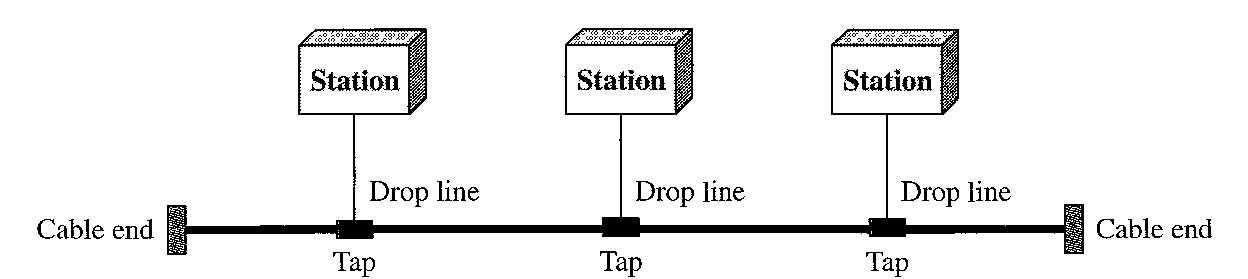
Advantages:

1. A star topology is less expensive than a mesh topology. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure. Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub.
2. Other advantages include robustness. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.

Disadvantages:

1. One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.
2. Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies.

**Bus Topology** The preceding examples all describe point-to-point connections. A bus topology,on the other hand, is multipoint. One long cable acts as a backbone to link all the devices in a network.



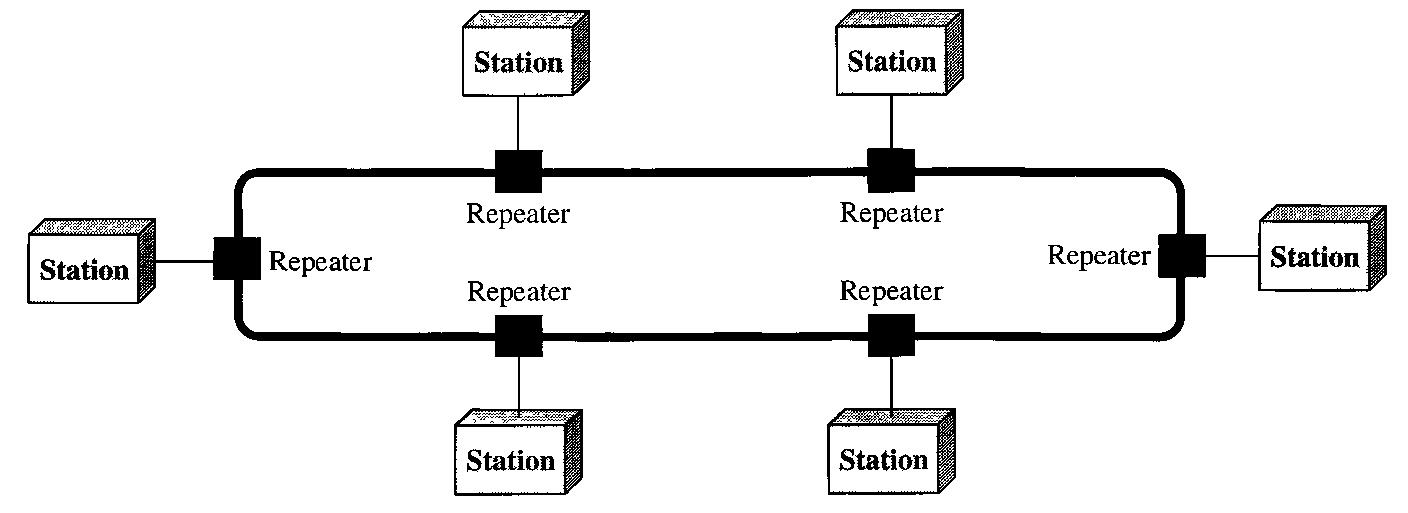
Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.

1. Advantages of a bus topology include ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies.
2. In a bus, redundancy is eliminated. Only the backbone cable stretches through the entire facility. Each drop line has to reach only as far as the nearest point on the backbone.

Disadvantages:

1. Disadvantages include difficult reconnection and fault isolation. A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices.
2. Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable. Adding new devices may therefore require modification or replacement of the backbone.
3. a fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back in the direction of origin, creating noise in both directions.

**Ring Topology** In a ring topology, each device has a dedicated point-to-point connection withonly the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.



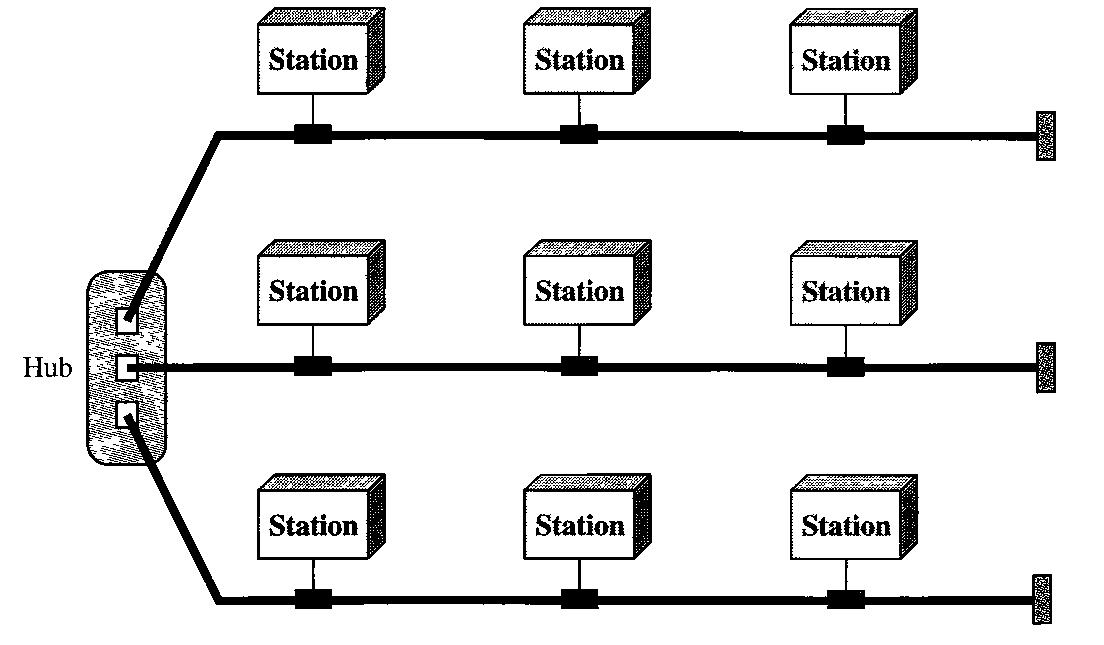
Advantages:

1. A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors.
2. To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations (maximum ring length and number of devices).
3. In addition, fault isolation is simplified. Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

Disadvantages:

1. Unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

**Hybrid Topology** A network can be hybrid. For example, we can have a main star topology witheach branch connecting several stations in a bus topology as shown:



**Categories of Networks :**

**LAN**

A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus. Depending on the needs of an organization and the type of technology used, a LAN can be as simple as two PCs and a printer in someone's home office; or it can extend throughout a company and include audio and video peripherals. Currently, LAN size is limited to a few kilometers.

**MAN**

A metropolitan area network (MAN) is a network with a size between a LAN and a WAN. It normally covers the area inside a town or a city. It is designed for customers who need a high-speed connectivity, normally to the Internet, and have endpoints spread over a city or part of city.

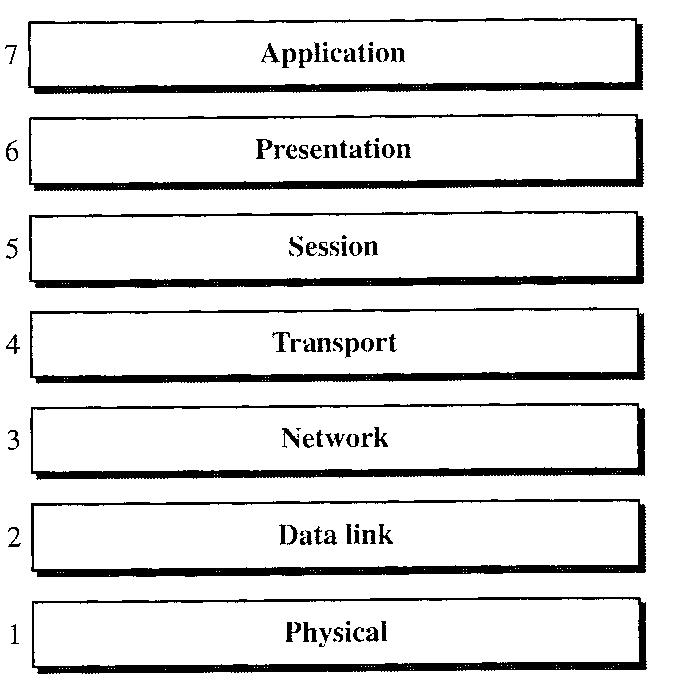
**WAN**

A wide area network (WAN) provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world.

A WAN can be as complex as the backbones that connect the Internet or as simple as a dial-up line that connects a home computer to the Internet. We normally refer to the first as a switched WAN and to the second as a point-to-point WAN. The switched WAN connects the end systems, which usually comprise a router (internet-working connecting device) that connects to another LAN or WAN.

**THE OSI MODEL**

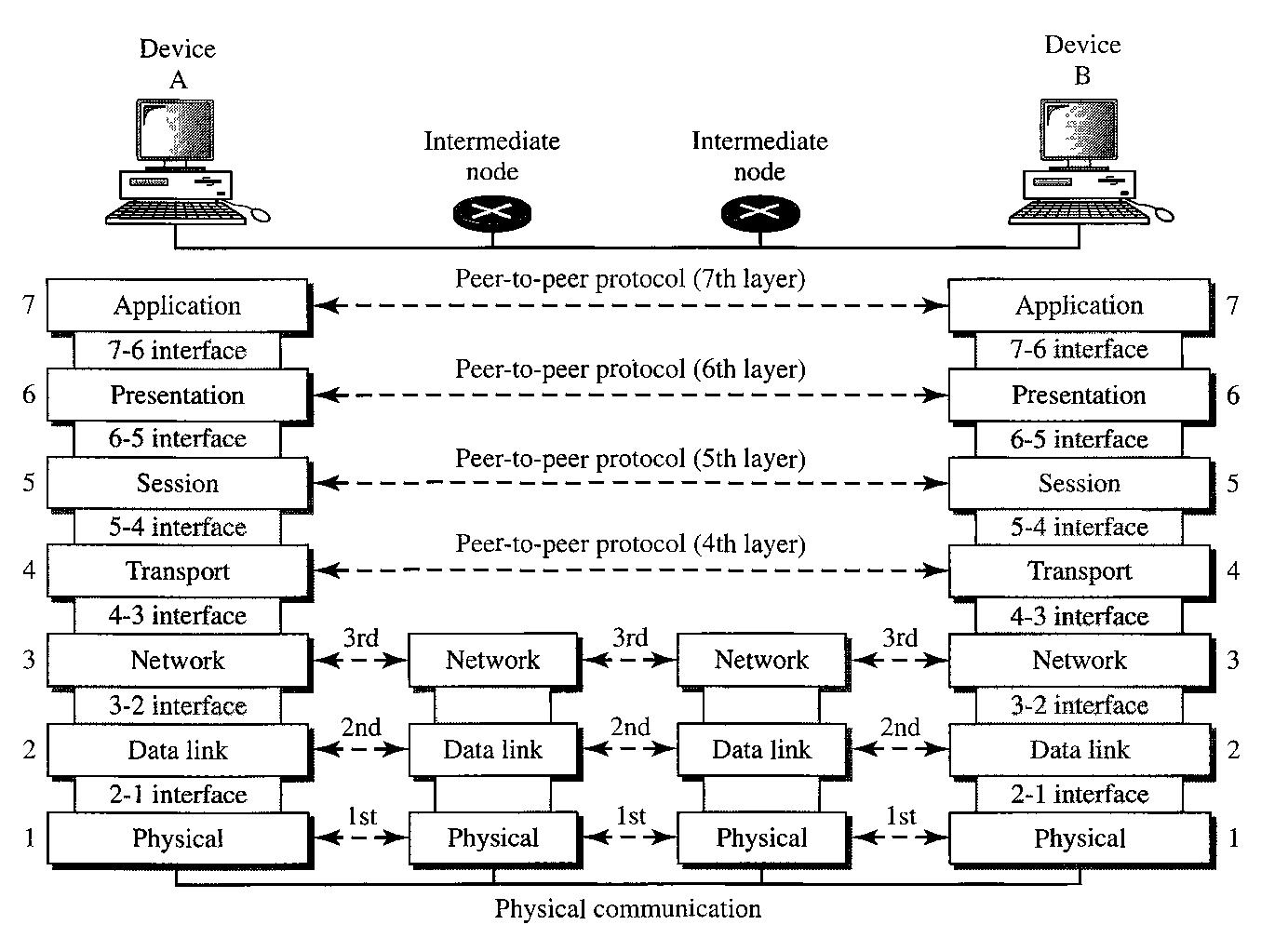
The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network.

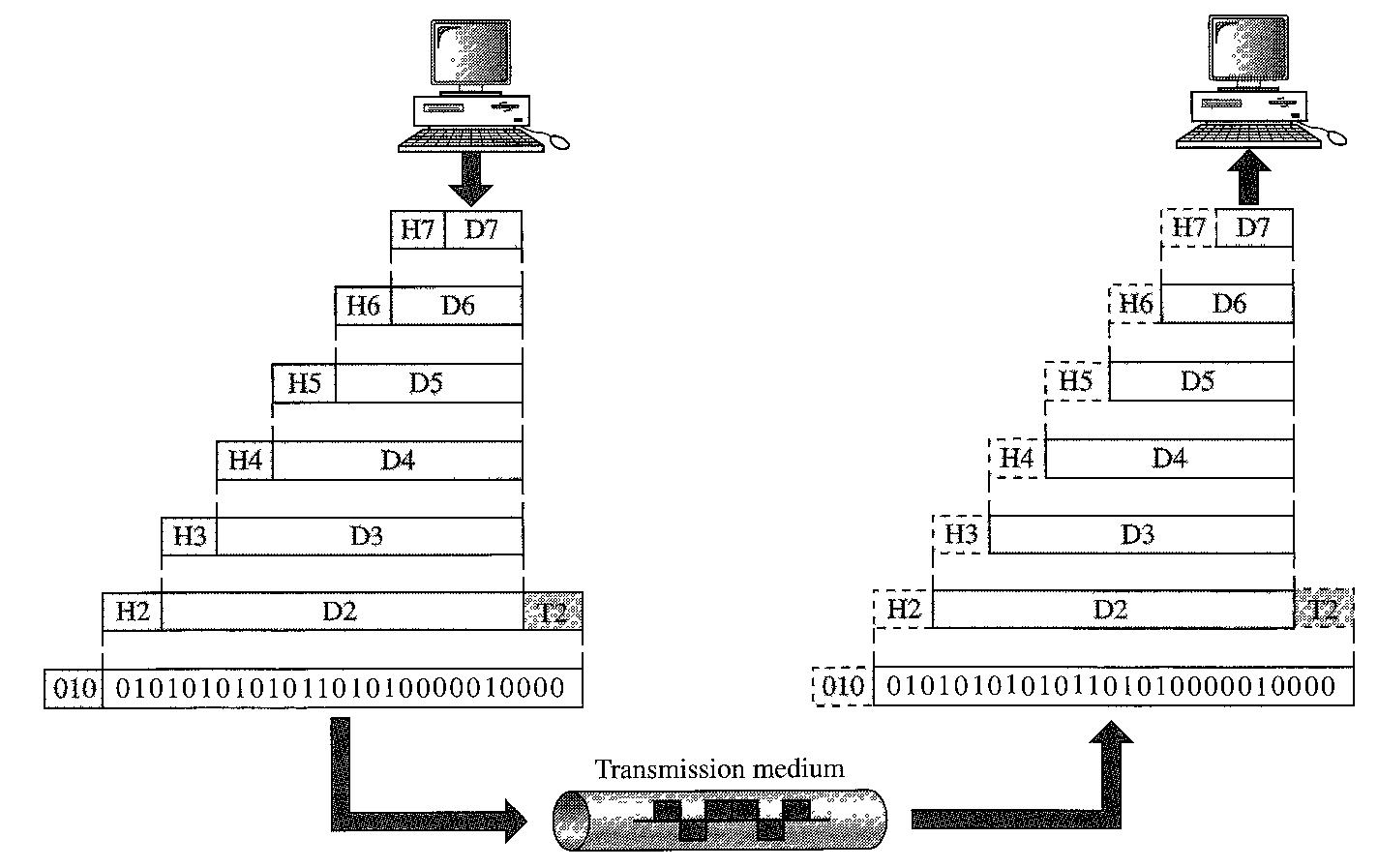


**Layered Architecture**

The OSI model is composed of seven ordered layers: physical (layer 1), data link (layer 2), network (layer 3), transport (layer 4), session (layer 5), presentation (layer 6), and application (layer 7). The following figure shows the layers involved when a message is sent from device A to device B. As the message travels from A to B, it may pass through many intermediate nodes. These intermediate nodes usually involve only the first three layers of the OSI model.

Within a single machine, each layer calls upon the services of the layer just below it. Layer 3, for example, uses the services provided by layer 2 and provides services for layer 4. Between machines, layer x on one machine communicates with layer x on another machine. This communication is governed by an agreed-upon series of rules and conventions called protocols.





**Physical Layer**

The physical layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur.

The physical layer is also concerned with the following:

* **Physical characteristics of interfaces and medium**. The physical layer defines thecharacteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.
* **Representation of bits**. The physical layer data consists of a stream of bits (sequence of0s or ls) with no interpretation. To be transmitted, bits must be encoded into signals - electrical or optical. The physical layer defines the type of encoding (how 0s and 1s are changed to signals).
* **Data rate**. The transmission rate--the number of bits sent each second--is also defined bythe physical layer. In other words, the physical layer defines the duration of a bit, which is how long it lasts.
* **Synchronization of bits**. The sender and receiver not only must use the same bit rate butalso must be synchronized at the bit level. In other words, the sender and the receiver clocks must be synchronized.
* **Line configuration**. The physical layer is concerned with the connection of devices tothe media. In a point-to-point configuration, two devices are connected through a dedicated link. In a multipoint configuration, a link is shared among several devices.
* **Physical topology**. The physical topology defines how devices are connected to make anetwork. Devices can be connected by using a mesh topology (every device is connected to every other device), a star topology (devices are connected through a central device), a ring topology (each device is connected to the next, forming a ring), a bus topology (every device is on a common link), or a hybrid topology (this is a combination of two or more topologies).
* **Transmission mode**. The physical layer also defines the direction of transmissionbetween two devices: simplex, half-duplex, or full-duplex. In simplex mode, only one device can send; the other can only receive. The simplex mode is a one-way communication. In the half-duplex mode, two devices can send and receive, but not at the same time. In a full-duplex (or simply duplex) mode, two devices can send and receive at the same time.

**Data Link Layer**

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (network layer). The figure shows the relationship of the data link layer to the network and physical layers.

Other responsibilities of the data link layer include the following:

* **Framing**. The data link layer divides the stream of bits received from the network layerinto manageable data units called frames.
* **Physical addressing**. If frames are to be distributed to different systems on the network,the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one.
* **Flow control**. If the rate at which the data are absorbed by the receiver is less than therate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.
* **Error control**. The data link layer adds reliability to the physical layer by addingmechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.
* **Access control**. When two or more devices are connected to the same link, data linklayer protocols are necessary to determine which device has control over the link at any given time.

**Network Layer**

The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination.

* **Logical addressing.** The physical addressing implemented by the data link layer handlesthe addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.
* **Routing**. When independent networks or links are connected to create internetworks(network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination.

**Transport Layer**

The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on a host. Whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does. The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.

* **Service-point addressing**. Computers often run several programs at the same time. Forthis reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header must therefore include a type of address called a service-point address (or port address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.
* **Segmentation and reassembly**. A message is divided into transmittable segments, witheach segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.
* **Connection control**. The transport layer can be either connectionless or connection-oriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection-oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.
* **Flow control**. Like the data link layer, the transport layer is responsible for flow control.However, flow control at this layer is performed end to end rather than across a single link.
* **Error control**. Like the data link layer, the transport layer is responsible for errorcontrol. However, error control at this layer is performed process-to-process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.

**Session Layer**

The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes. The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction among communicating systems

* **Dialog control**. The session layer allows two systems to enter into a dialog. It allows thecommunication between two processes to take place in either half- duplex (one way at a time) or full-duplex (two ways at a time) mode.
* **Synchronization**. The session layer allows a process to add checkpoints, orsynchronization points, to a stream of data. For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after

system recovery are pages 501 to 523. Pages previous to 501 need not be resent.

**Presentation Layer**

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems. The figure shows the relationship between the presentation layer and the application and session layers.

Specific responsibilities of the presentation layer include the following:

* **Translation.** The processes (running programs) in two systems are usually exchanginginformation in the form of character strings, numbers, and so on. The information must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.
* **Encryption.** To carry sensitive information, a system must be able to ensure privacy.Encryption means that the sender transforms the original information to another form and

sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.

* **Compression.** Data compression reduces the number of bits contained in theinformation. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

**Application Layer**

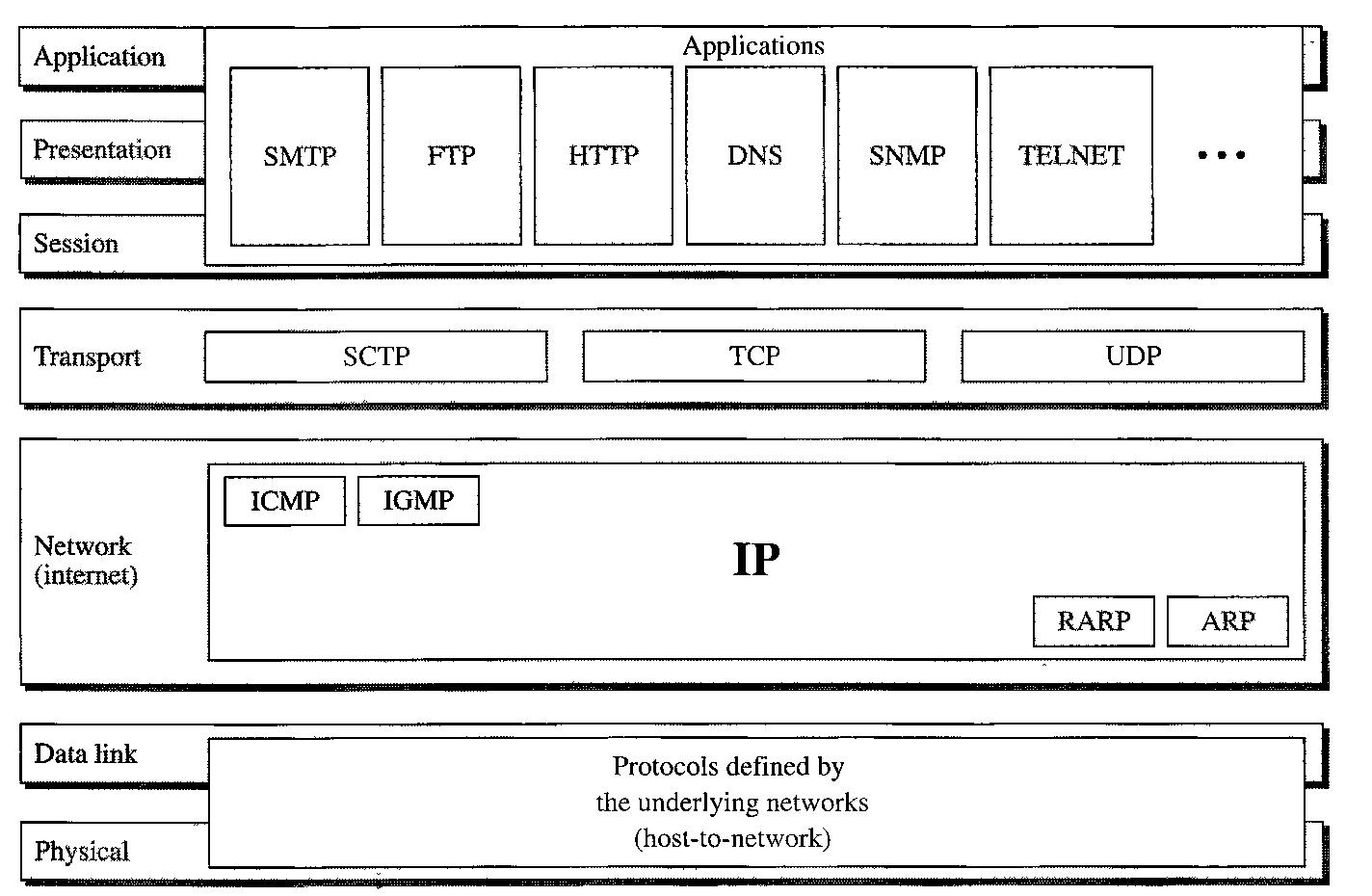
The application layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.

Specific services provided by the application layer include the following:

* + **Network virtual terminal.** A network virtual terminal is a software version of a physicalterminal, and it allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa. The remote host believes it is communicating with one of its own terminals and allows the user to log on.
  + **File transfer, access, and management**. This application allows a user to access files ina remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
  + **Mail services**. This application provides the basis for e-mail forwarding and storage.
  + **Directory services**. This application provides distributed database sources and access forglobal information about various objects and services.

**TCP/IP PROTOCOL SUITE**

The TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application. The first four layers provide physical standards, network interfaces, internetworking, and transport functions that correspond to the first four layers of the OSI model. The three topmost layers in the OSI model, however, are represented in TCP/IP by a single layer called the application layer.



**Physical and Data Link Layers**

At the physical and data link layers, TCP/IP does not define any specific protocol. It supports all the standard and proprietary protocols. A network in a TCP/IP internetwork can be a local-area network or a wide-area network.

**Network Layer**

At the network layer (or, more accurately, the internetwork layer), TCP/IP supports the Internetworking Protocol. IP, in turn, uses four supporting protocols: ARP, RARP, ICMP, and IGMP.

**Internetworking Protocol (IP)**

The Internetworking Protocol (IP) is the transmission mechanism used by the TCP/IP protocols. It is an unreliable and connectionless protocol--a best-effort delivery service. The term best effort means that IP provides no error checking or tracking. IP assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees.

IP transports data in packets called datagrams, each of which is transported separately. Datagrams can travel along different routes and can arrive out of sequence or be duplicated. IP does not keep track of the routes and has no facility for reordering datagrams once they arrive at their destination.

**Address Resolution Protocol**

The Address Resolution Protocol (ARP) is used to associate a logical address with a physical address. On a typical physical network, such as a LAN, each device on a link is identified by a physical or station address, usually imprinted on the network interface card (NIC). ARP is used to find the physical address of the node when its Internet address is known.

**Reverse Address Resolution Protocol**

The Reverse Address Resolution Protocol (RARP) allows a host to discover its Internet address when it knows only its physical address. It is used when a computer is connected to a network for the first time or when a diskless computer is booted.

**Internet Control Message Protocol**

The Internet Control Message Protocol (ICMP) is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender. ICMP sends query and error reporting messages.

**Internet Group Message Protocol**

The Internet Group Message Protocol (IGMP) is used to facilitate the simultaneous transmission of a message to a group of recipients.

**Transport Layer**

Traditionally the transport layer was represented in TCP/IP by two protocols: TCP and UDP. IP is a host-to-host protocol, meaning that it can deliver a packet from one physical device to another. UDP and TCP are transport level protocols responsible for delivery of a message from a process (running program) to another process. A new transport layer protocol, SCTP, has been devised to meet the needs of some newer applications.

**User Datagram Protocol**

The User Datagram Protocol (UDP) is the simpler of the two standard TCP/IP transport protocols. It is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer.

**Transmission Control Protocol**

The Transmission Control Protocol (TCP) provides full transport-layer services to applications. TCP is a reliable stream transport protocol. The term stream, in this context, means connection-oriented: A connection must be established between both ends of a transmission before either can transmit data.

At the sending end of each transmission, TCP divides a stream of data into smaller units called segments. Each segment includes a sequence number for reordering after receipt, together with an acknowledgment number for the segments received. Segments are carried across the internet inside of IP datagrams. At the receiving end, TCP collects each datagram as it comes in and reorders the transmission based on sequence numbers.

**Stream Control Transmission Protocol**

The Stream Control Transmission Protocol (SCTP) provides support for newer applications such as voice over the Internet. It is a transport layer protocol that combines the best features of UDP and TCP.

**Application Layer**

The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model. Many protocols are defined at this layer.

**function of common networking protocols.**

* [**TCP**](http://en.wikipedia.org/wiki/Transmission_Control_Protocol)

The Transmission Control Protocol (TCP) is one of the core protocols of the Internet Protocol Suite. It is a reliable stream delivery service that guarantees delivery of a data stream sent from one host to another without duplication or losing data.

* [**FTP**](http://en.wikipedia.org/wiki/FTP)

File Transfer Protocol (FTP) is a standard network protocol used to transfer files from one host to another host over a TCP-based network, such as the Internet. FTP is built on a client-server architecture and uses separate control and data connections between the client and server. Authentication is accomplished through the use of a clear-text sign-in protocol and is not considered to be secure.

* [**UDP**](http://en.wikipedia.org/wiki/User_Datagram_Protocol)

The User Datagram Protocol (UDP) is one of the core members of the Internet Protocol Suite, the set of network protocols used for the Internet. With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without requiring prior communications to set up special transmission channels or data paths. UDP provides an unreliable service and datagrams may arrive out of order, appear duplicated, or go missing without notice.

* [**DHCP**](http://en.wikipedia.org/wiki/Dhcp)

The Dynamic Host Configuration Protocol (DHCP) is a network configuration protocol that enables a server on an IP network to automatically assign an IP address to a computer from a predetermined range of numbers. The most essential information needed is an IP address, and a default route and routing prefix. DHCP controls the assignment of unique dynamic IP addresses and routing information, eliminating the manual task by a network administrator.

* [**TFTP**](http://en.wikipedia.org/wiki/Trivial_File_Transfer_Protocol)

Trivial File Transfer Protocol (TFTP) is a simple insecure protocol used to transfer files. It is typically implemented on top of the User Datagram Protocol (UDP) using port number 69. Packets are limited to a 512 byte limit and can be easily lost. When a packet smaller than 512 bytes is received, the server assumes the end of the file has been reached and closes the connection. Transmission is not guaranteed to be complete and has no provision for user authentication. TFTP is designed to be small and easy to implement, therefore, lacks most of the features of FTP. TFTP only reads and writes files (or mail) to or from a remote server, it cannot list directories. TFTP can be used for remote booting of devices without hard drives. Used in conjunction with a bootp server, the device receives its addressing information and the address of the TFTP server from which it should boot.

* [**DNS**](http://en.wikipedia.org/wiki/Domain_Name_System)

The Domain Name System (DNS) is a hierarchical naming system for computers, services, or any resource connected to the Internet or a private network. Internet and TCP utilities such as telnet, FTP, and SMTP use DNS to translate computer host and domain names to their corresponding IP addresses. DNS allows you to type recognizable names into your Web browser and your computer will automatically find that address on the Internet. Address information is stored in several locations in a hierarchical structure.

* [**HTTPS**](http://en.wikipedia.org/wiki/Https)

Hypertext Transfer Protocol Secure (HTTPS) is a combination of Hypertext Transfer Protocol (HTTP) with SSL/TLS protocol. It provides encrypted communication and secure identification of a network web server. HTTPS connections are often used for payment transactions on the World Wide Web and for sensitive transactions in corporate information systems. HTTPS uses port 443 by default.

* [**HTTP**](http://en.wikipedia.org/wiki/HTTP)

Hypertext Transfer Protocol (HTTP) is an application-level protocol used to request and deliver web pages between a server and browser. HTTP is the foundation of data communication for the World Wide Web.

* [**ARP**](http://en.wikipedia.org/wiki/Address_Resolution_Protocol)

Address Resolution Protocol (ARP) is a low-level network protocol used for the resolution of network layer IP addresses into corresponding link layer MAC (Media Access Control) addresses. ARP is the standard of identifying a host's hardware address when only its network IP address is known.

* [**SSH**](http://en.wikipedia.org/wiki/Secure_Shell)

Secure Shell (SSH) is a cryptographic remote login protocol for secure data communication over an unsecured network. Designed as a replacement for telnet and rlogin, which send information in plaintext, SSH client and server programs provide strong host-to-host and user authentication as well as a number of securely encrypted methods of communication to provide confidentiality and integrity of data. SSH supports data stream compression between the client and the server.

* [**POP3**](http://en.wikipedia.org/wiki/Post_Office_Protocol)

Post Office Protocol (POP3) is a simple, standardized application-layer protocol used for retrieving incoming email from a remote mail server over a TCP/IP connection and saving to a local device. A POP3 server listens on well-known port TCP/110.

* [**IMAP4**](http://en.wikipedia.org/wiki/Internet_Message_Access_Protocol)

Internet message access protocol (IMAP) is one of the two most prevalent Internet standard protocols for e-mail retrieval, the other being the Post Office Protocol (POP). Virtually all modern e-mail clients and mail servers support both protocols as a means of transferring e-mail messages from a server. IMAP is a client/server protocol in which e-mail is received and held by your Internet server and downloaded from the server by request. Imap permits the manipulation of remote mailboxes as though they were local, and works well with slower modem connections.

* [**Telnet**](http://en.wikipedia.org/wiki/Telnet)

Short for Telecommunications network, TELNET is a text based interface protocol that provides an insecure remote access to other computers. Telnet uses a command line interface and can be accessed in Windows from the Start menu by clicking <Start>, <Run>, then by typing: telnet (somesite) 23. Port number 23 is the default port used by telnet, but is usually optional and often not required.

* [**SMTP**](http://en.wikipedia.org/wiki/Smtp)

Simple Mail Transfer Protocol (SMTP) is a reliable and efficient mail transport and delivery protocol that is capable of transporting outgoing email across multiple networks. SMTP requires a reliable data stream channel for transmission.

* [**SNMP**](http://en.wikipedia.org/wiki/SNMP)

Simple Network Management Protocol (SNMP) is an "Internet-standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more." It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

* [**ICMP**](http://en.wikipedia.org/wiki/Internet_Control_Message_Protocol)

The Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet Protocol Suite. It is chiefly used by the operating systems of networked computers to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached. ICMP can also be used to relay query messages.

* [**IGMP**](http://en.wikipedia.org/wiki/IGMP)

The Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships.

* [**TLS**](http://en.wikipedia.org/wiki/Transport_Layer_Security)

Transport Layer Security (TLS) is a cryptographic protocol that provides communication security over the Internet. TLS encrypts the segments of network connections above the Transport Layer, using asymmetric cryptography for key exchange, symmetric encryption for privacy, and message authentication codes for message integrity.

|  |  |
| --- | --- |
| **Protocol** | **Common Port** |
| FTP (File Transfer Protocol) | 20, 21 |
| SSH (Secure Shell) | 22 |
| Telnet | 23 |
| SMTP (Simple Mail Transfer Protocol) | 25 |
| DNS (Domain Name Service) | 53 |
| TFTP (Trivial File Transfer Protocol) | 69 |
| HTTP (Hypertext Transfer Protocol) | 80 |
| POP3 (Post Office Protocol version 3) | 110 |
| NNTP (Network News Transport Protocol) | 119 |
| NTP (Network Time Protocol) | 123 |
| IMAP4 (Internet Message Access Protocol version 4) | 143 |
| HTTPS (Hypertext Transfer Protocol Secure) | 443 |