1st UNIT
NETWORK

A network is a set of devices (often referred to as *nodes)* connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

"Computer network'' to mean a collection of autonomous computers interconnected by a single technology. Two computers are said to be interconnected if they are able to exchange information.

The connection need not be via a copper wire; fiber optics, microwaves, infrared, and communication satellites can also be used.

Networks come in many sizes, shapes and forms, as we will see later.They are usually connected together to make larger networks, with the **Internet** being the most well-known example of a network of networks.

There is considerable confusion in the literature between a **computer network** and a **distributed system**. The key distinction is that in a distributed system, a collection of independent computers appears to its users as a single coherent system. Usually, it has a single model or paradigm that it presents to the users. Often a layer of software on top of the operating system, called **middleware**, is responsible for implementing this model. A well-known example of a distributed system is the **World Wide Web**. It runs on top of the Internet and presents a model in which everything looks like a document (Web page).

USES OF COMPUTER NETWORKS

1. Business Applications

- to distribute information throughout the company (**resource sharing).**sharing physical resources such as printers, and tape backup systems, issharing information
- **client-server model**. It is widely used and forms the basis of much network usage.
- **communication medium** among employees.**email** (**electronic mail**),which employees generally use for a great deal of daily communication.
- Telephone calls between employees may be carried by the computer network instead of by the phone company. This technology is called **IP telephony** or **Voice over IP** (**VoIP**) when Internet technology is used.
- **Desktop sharing** lets remote workers see and interact with a graphicalcomputer screen
- doing business electronically, especially with customers and suppliers. This new model is called **e-commerce** (**electronic commerce**) and it has grownrapidly in recent years.

2 Home Applications

- **peer-to-peer** communication
- person-to-person communication

- electronic commerce
- entertainment.(game playing,)

3 Mobile Users

- Text messaging or texting
- Smart phones,
- GPS (Global Positioning System)
- m-commerce
- NFC (Near Field Communication)

4 Social Issues

With the good comes the bad, as this new-found freedom brings with it manyunsolved social, political, and ethical issues.

Social networks, message boards, content sharing sites, and a host of other applications allow people to share their views with like-mindedindividuals. As long as the subjects are restricted to technical topics or hobbies like gardening, not too many problems will arise.

The trouble comes with topics that people actually care about, like politics,religion, or sex. Views that are publicly posted may be deeply offensive to some people. Worse yet, they may not be politically correct. Furthermore, opinions need not be limited to text; high-resolution color photographs and video clipsare easily shared over computer networks. Some people take a live-and-let-live view, but others feel that posting certain material (e.g., verbal attacks on particular countries or religions, pornography, etc.) is simply unacceptable and that such content must be censored. Different countries have different and conflicting laws in this area. Thus, the debate rages.

Computer networks make it very easy to communicate. They also make it easy for the people who run the network to snoop on the traffic. This sets up conflicts over issues such as **employee rights versus employer rights**. Many people read and write email at work. Many employers have claimed the right to read and possibly censor employee messages, including messages sent from a home computer outside working hours. Not all employees agree withthis, especially the latter part.

Another conflict is centered around government versus citizen’s rights.

A new twist with mobile devices is location privacy. As part of the process of providing service to your mobile device the network operators learn where you are at different times of day. This allows them to track your movements. They may know which nightclub you frequent and which medical center you visit.

Phishing ATTACK: ***Phishing*** is a type of social engineering ***attack***

TCP &UDP

often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

BOTNET ATTACK: Botnets can be used to perform distributed denial-of-service attack (DDoS attack), steal data, send spam, and allows the attacker to access the device and its connection.

The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

I. **Delivery.** The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.

2 **Accuracy.** The system must deliver the data accurately. Data that have beenaltered in transmission 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 unevendelay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 30 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.

A data communications system has five components

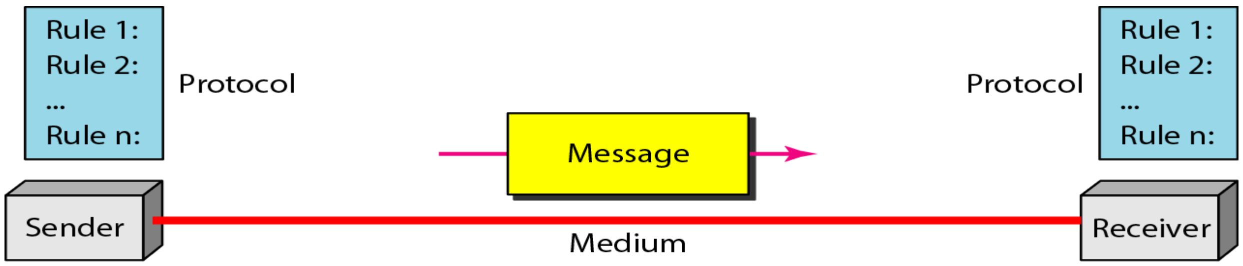
I. **Message**. The message is the information (data) to be communicated.Popular forms of information include text, numbers, pictures, audio, and video. 2 **Sender**. The sender is the device that sends the data message. It can be acomputer, workstation, telephone handset, video camera, and so on.

3. **Receiver.** The receiver is the device that receives the message. It can be acomputer, workstation, telephone handset, television, and so on.

4. **Transmission medium**. The transmission medium is the physical path by which a message travels 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, just as aperson speaking French cannot be understood by a person who speaks only Japanese.

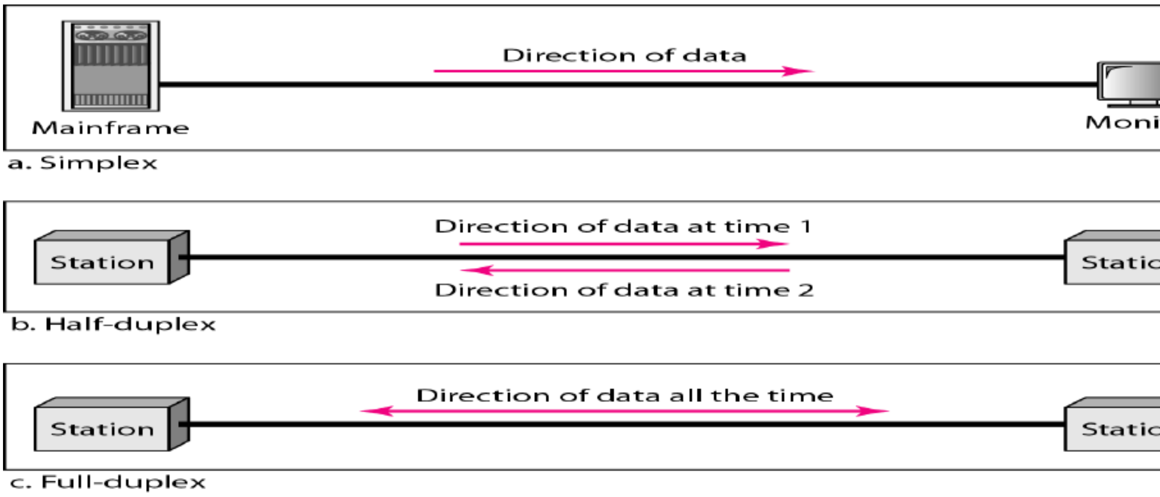


Data Representation

TextNumbersImagesAudioVideo

Data Flow

Communication between two devices can be simplex, half-duplex, or full-duplexas shown in Figure.



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 (Figure a). Keyboards and traditional monitors are examples of simplex devices.

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 (Figure b). Walkie-talkies and CB (citizens band) radios are both half- duplex systems.

Full-Duplex

In full-duplex, both stations can transmit and receive simultaneously (Figure c). One common example of full-duplex communication is the telephone network.When two people are communicating by a telephone line, both can talk andlisten at the same time. The full-duplex mode is used when communication inboth directions is required all the time.

Network Criteria

A network must be able to meet a certain number of criteria. The mostimportant of these are performance, reliability, and security.

Performance

Performance can be measured in many ways, including transit time and response time. Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time betweenan inquiry and a response. The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.

Performance is often evaluated by two networking metrics: **throughput**

and delay. We often need more throughput and less delay. However, these two criteria are often contradictory. If we try to send more data to the network, we may increase throughput but we increase the delay because of traffic congestion in the network.

Reliability: In addition to accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, andthe network's robustness in a catastrophe.

Security: Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

Physical Structures

Before discussing networks, we need to define some network attributes.

Type of Connection

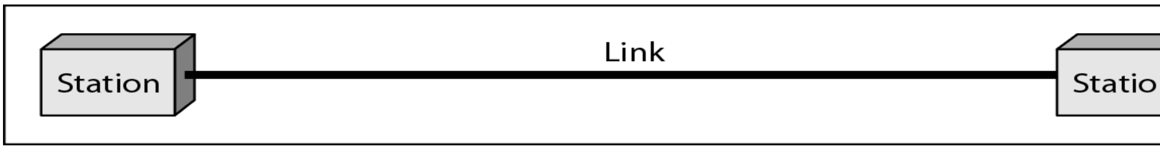
A network is two or more devices connected through links. A link is acommunications pathway that transfers data from one device to another.

There are two possible types of connections: point-to-point and multipoint. **Point-to-Point** A point-to-point connection provides a dedicated link betweentwo devices. The entire capacity of the link is reserved for transmissionbetween those two devices. Most point-to-point connections use an actuallength of wire or cable to connect the two ends, but other options, such asmicrowave or satellite links, are also possible

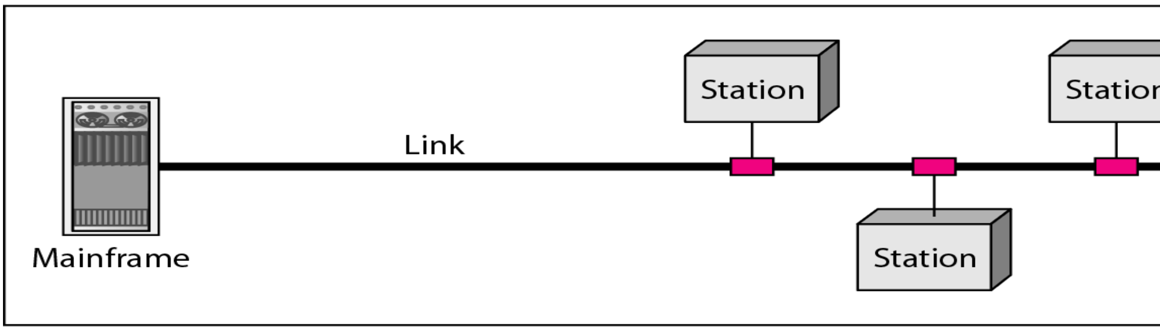
When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

Multipoint A multipoint (also called multi-drop) connection is one in which more than two specific 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.



a. Point-to-point

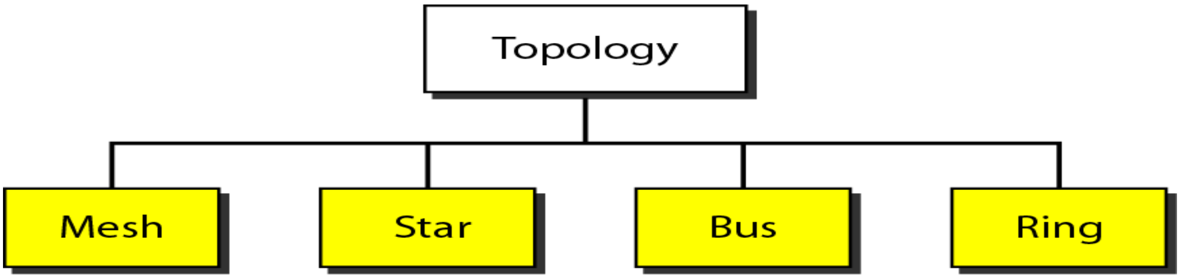


b. Multipoint

Physical Topology

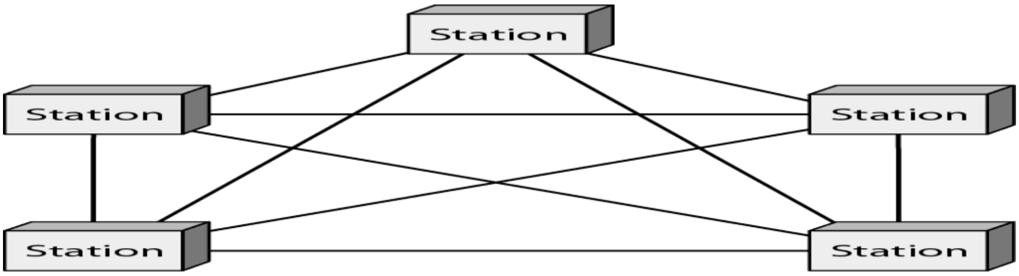
The term *physical topology* refers to the way in which a network is laid out physically.

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:

A mesh topology is the one where every node is connected to every other nodein the network.



TCP &UDP

A mesh topology can be a **full mesh topology** or a **partially connected mesh topology**.

In a *full mesh topology*, every computer in the network has a connection to each of the other computers in that network. The number of connections in this network can be calculated using the following formula (***n*** is the number ofcomputers in the network): **n(n-1)/2**

In a *partially connected mesh topology*, at least two of the computers in the network have connections to multiple other computers in that network. It is an inexpensive way to implement redundancy in a network. In the event that oneof the primary computers or connections in the network fails, the rest of the network continues to operate normally.

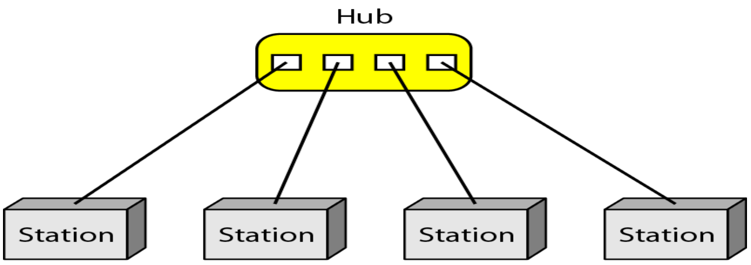
Advantages of a mesh topology

- Can handle high amounts of traffic, because multiple devices can transmitdata simultaneously.
- A failure of one device does not cause a break in the network or transmissionof data.
- Adding additional devices does not disrupt data transmission between otherdevices.

Disadvantages of a mesh topology

- The cost to implement is higher than other network topologies, making it aless desirable option.
- Building and maintaining the topology is difficult and time consuming.
- The chance of redundant connections is high, which adds to the high costsand potential for reduced efficiency.

STAR:



A star network, **star topology** is one of the most common network setups. In this configuration, every node connects to a central network device, likea hub, switch, or computer. The central network device acts as a server and the peripheral devices act as clients. Depending on the type of network card usedin each computer of the star topology, a coaxial cable or a RJ-45 network cableis used to connect computers together.

Advantages of star topology

- Centralized management of the network, through the use of

TCP &UDP

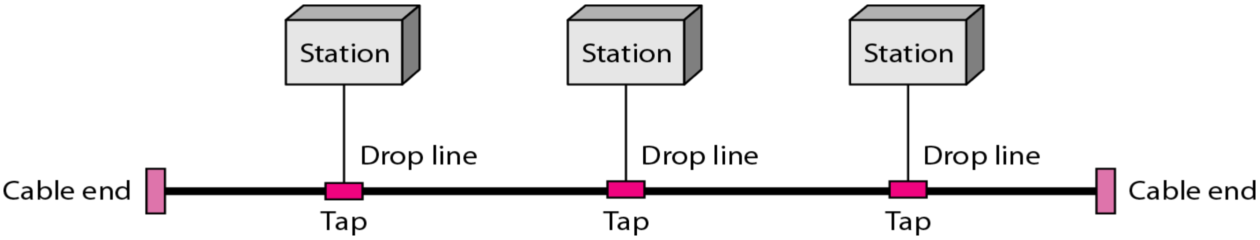
the centralcomputer, hub, or switch.

- Easy to add another computer to the network.
- If one computer on the network fails, the rest of the network continues tofunction normally.
- The star topology is used in local-area networks (LANs), High-speed LANsoften use a star topology with a central hub.

Disadvantages of star topology

- Can have a higher cost to implement, especially when using a switch orrouter as the central network device.
- The central network device determines the performance and number ofnodes the network can handle.
- If the central computer, hub, or switch fails, the entire network goes downand all computers are disconnected from the network

BUS:



a **line topology**, a **bus topology** is a network setup in which each computerand network device are connected to a single cable or backbone.

Advantages of bus topology

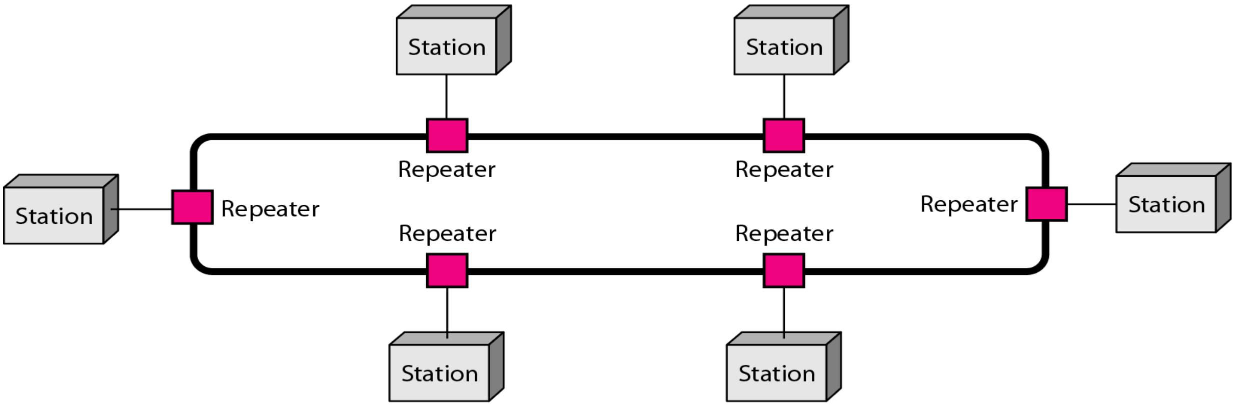
- It works well when you have a small network.
- It's the easiest network topology for connecting computers or peripheralsin a linear fashion.
- It requires less cable length than a star topology.

Disadvantages of bus topology

- It can be difficult to identify the problems if the whole network goes down.
- It can be hard to troubleshoot individual device issues.
- Bus topology is not great for large networks.
- Terminators are required for both ends of the main cable.
- Additional devices slow the network down.
- If a main cable is damaged, the network fails or splits into two

TCP &UDP

RING:



A **ring topology** is a network configuration in which device connections createa circular data path. In a ring network, packets of data travel from one device tothe next until they reach their destination. Most ring topologies allow packets to travel only in one direction, called a **unidirectional** ring network. Others permit data to move in either direction, called **bidirectional**.

The major disadvantage of a ring topology is that if any individual connection in the ring is broken, the entire network is affected.

Ring topologies may be used in either local area networks (LANs) or wide areanetworks (WANs).

Advantages of ring topology

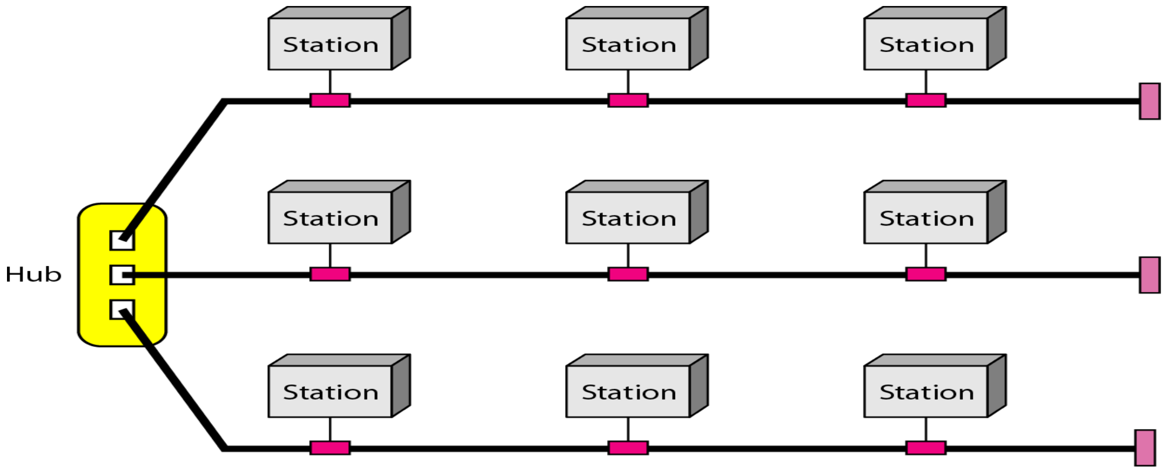
- All data flows in one direction, reducing the chance of packet collisions.
- A network server is not needed to control network connectivity betweeneach workstation.
- Data can transfer between workstations at high speeds.
- Additional workstations can be added without impacting performance ofthe network.

Disadvantages of ring topology

- All data being transferred over the network must pass through eachworkstation on the network, which can make it slower than a star topology.
- The entire network will be impacted if one workstation shuts down.
- The hardware needed to connect each workstation to the network is moreexpensive than Ethernet cards and hubs/switches.

Hybrid Topology A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology asshown in Figure

TCP &UDP



Types of Network based on size

The types of network are classified based upon the size, the area it covers and its physical architecture. The three primary network categories are LAN, WAN and MAN. Each network differs in their characteristics such as distance, transmission speed, cables and cost.
Basic types

LAN (Local Area Network)

Group of interconnected computers within a small area. (room, building,campus)
Two or more pc's can from a LAN to share files, folders, printers, applicationsand other devices.
Coaxial or CAT 5 cables are normally used for connections.Due to short distances, errors and noise are minimum.
Data transfer rate is 10 to 100 mbps.
Example: A computer lab in a school. **MAN (Metropolitan Area Network)**Design to extend over a large area.

Connecting number of LAN's to form larger network, so that resources can beshared.
Networks can be up to 5 to 50 km. Owned by organization or individual. Data transfer rate is low compare to LAN.

TCP &UDP

Example: Organization with different branches located in the city.

WAN (Wide Area Network)

Are country and worldwide network. Contains multiple LAN's and MAN's. Distinguished in terms of geographical range.Uses satellites and microwave relays. Data transfer rate depends upon the ISP provider and varies over the location.Best example is the internet.

Other types

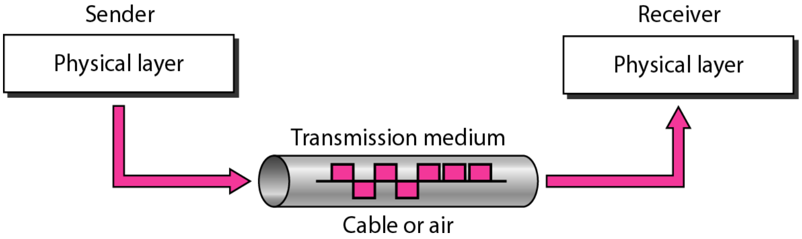
WLAN (Wireless LAN)

A LAN that uses high frequency radio waves for communication. Provides short range connectivity with high speed data transmission.**PAN (Personal Area Network)** Network organized by the individual user for its personal use.

SAN (Storage Area Network)

Connects servers to data storage devices via fiber-optic cables.E.g.: Used for daily backup of organization or a mirror copy

A **transmission medium** can be broadly defined as anything that can carryinformation from a source to a destination.



THE INTERNET

The Internet has revolutionized many aspects of our daily lives. It has affected the way we do business as well as the way we spend our leisure time. Countthe ways you've used the Internet recently. Perhaps you've sent electronic mail (e-mail) to a business associate, paid a utility bill, read a newspaper from a distant city, or looked up a local movie schedule-all by using the Internet. Or maybe you researched a medical topic, booked a hotel reservation, chattedwith a fellow Trekkie, or comparison-shopped for a car. The Internet is a communication system that has brought a wealth of information to our fingertips and organized it for our use.

A Brief History

A network is a group of connected communicating devices such as computers and printers. An internet (note the lowercase letter i) is two ormore networks that can communicate with each other. The most notable internet is called the Internet (uppercase letter I), a collaboration of more than hundreds of thousands of interconnected networks. Private individuals as well as various organizations such as government agencies, schools, research facilities, corporations, and libraries in more than 100 countries use the Internet. Millions of people are users. Yet this extraordinary communication system only came into being in 1969.

In the mid-1960s, mainframe computers in research organizations were standalone devices. Computers from different manufacturers were unable to communicate with one another. The Advanced Research Projects Agency

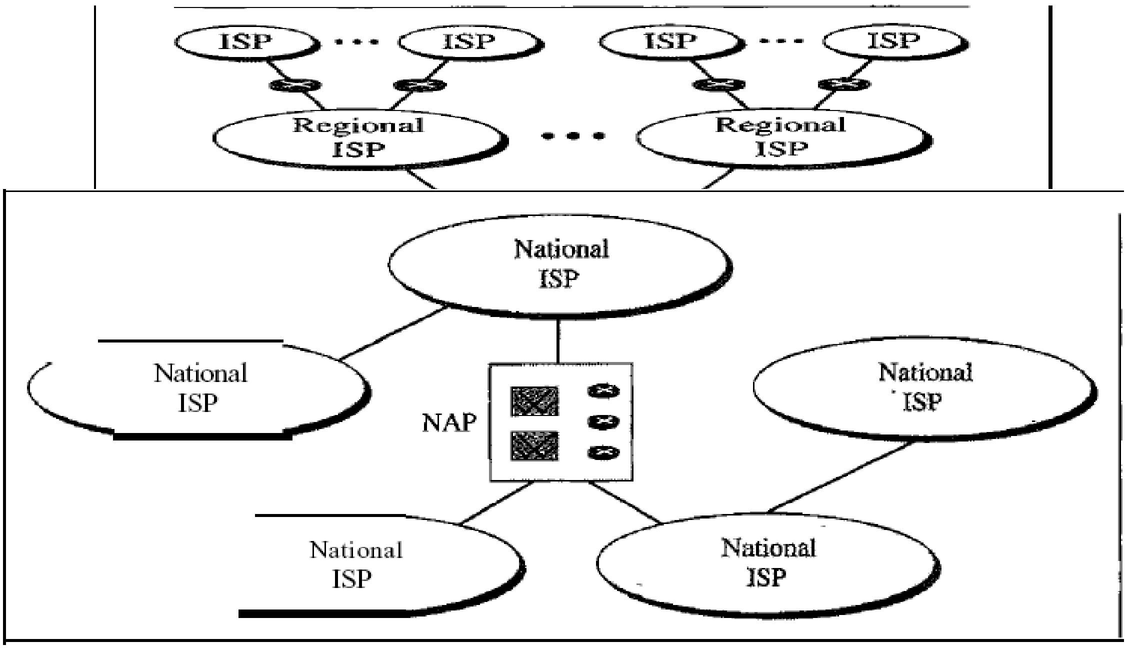
(ARPA) in the Department of Defense (DoD) was interested in finding a way to connect computers so that the researchers they funded could share their findings, thereby reducing costs and eliminating duplication of effort.

In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas for ARPANET, a small network of connected computers. The idea was that each host computer (not necessarily from the same manufacturer) would be attached to a specialized computer, called an *inteiface message processor* (IMP). The IMPs, in tum, would be connected to one another. Each IMP had to be able to communicate with other IMPs as well as with its own attached host. By 1969, ARPANET was a reality. Four nodes, at the University of California at Los Angeles (UCLA), the University of California at Santa Barbara (UCSB), Stanford Research Institute (SRI), and the Universityof Utah, were connected via the IMPs to form a network. Software called the *Network Control Protocol* (NCP) provided communication between the hosts.

In 1972, Vint Cerf and Bob Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the *Internetting Projec1.* Cerf and Kahn's landmark 1973 paper outlined the protocols to achieve end- to-end delivery of packets. This paper on Transmission Control Protocol (TCP) included concepts such as encapsulation, the datagram, and the functions ofa gateway. Shortly thereafter, authorities made a decision to split TCP into twoprotocols: Transmission Control Protocol (TCP) and Internetworking Protocol (lP). IP would handle datagram routing while TCP would be responsible for higher-level functions such as segmentation, reassembly, and error detection. The internetworking protocol became known as TCPIIP.

The Internet Today

The Internet has come a long way since the 1960s. The Internet today is not a simple hierarchical structure. It is made up of many wide- and local-area networks joined by connecting devices and switching stations. It is difficult to give an accurate representation of the Internet because it is continually changing-new networks are being added, existing networks are adding addresses, and networks of defunct companies are being removed. Todaymost end users who want Internet connection use the services of Internet service providers (lSPs). There are international service providers, national service providers, regional service providers, and local service providers. The Internet today is run by private companies, not the government. Figure 1.13 shows a conceptual (not geographic) view of the Internet.



b. Interconnection of national ISPs

International Internet Service Providers:

At the top of the hierarchy are the international service providers that connect nations together.

National Internet Service Providers:

The national Internet service providers are backbone networks created and maintained by specialized companies. There are many national ISPs operating in North America; some of the most well known are SprintLink, PSINet, UUNet Technology, AGIS, and internet Mel. To provide connectivity between the end users, these backbone networks are connected by complex switching stations (normally run by a third party) called network access points (NAPs). Some national ISP networks are also connected to one another by private switching stations called *peering points.* These normally operate at a high data rate (up to 600 Mbps).

Regional Internet Service Providers:

Regional internet service providers or regional ISPs are smaller ISPs that are connected to one or more national ISPs. They are at the third level of the hierarchy with a smaller data rate. ***Local Internet Service Providers****:*

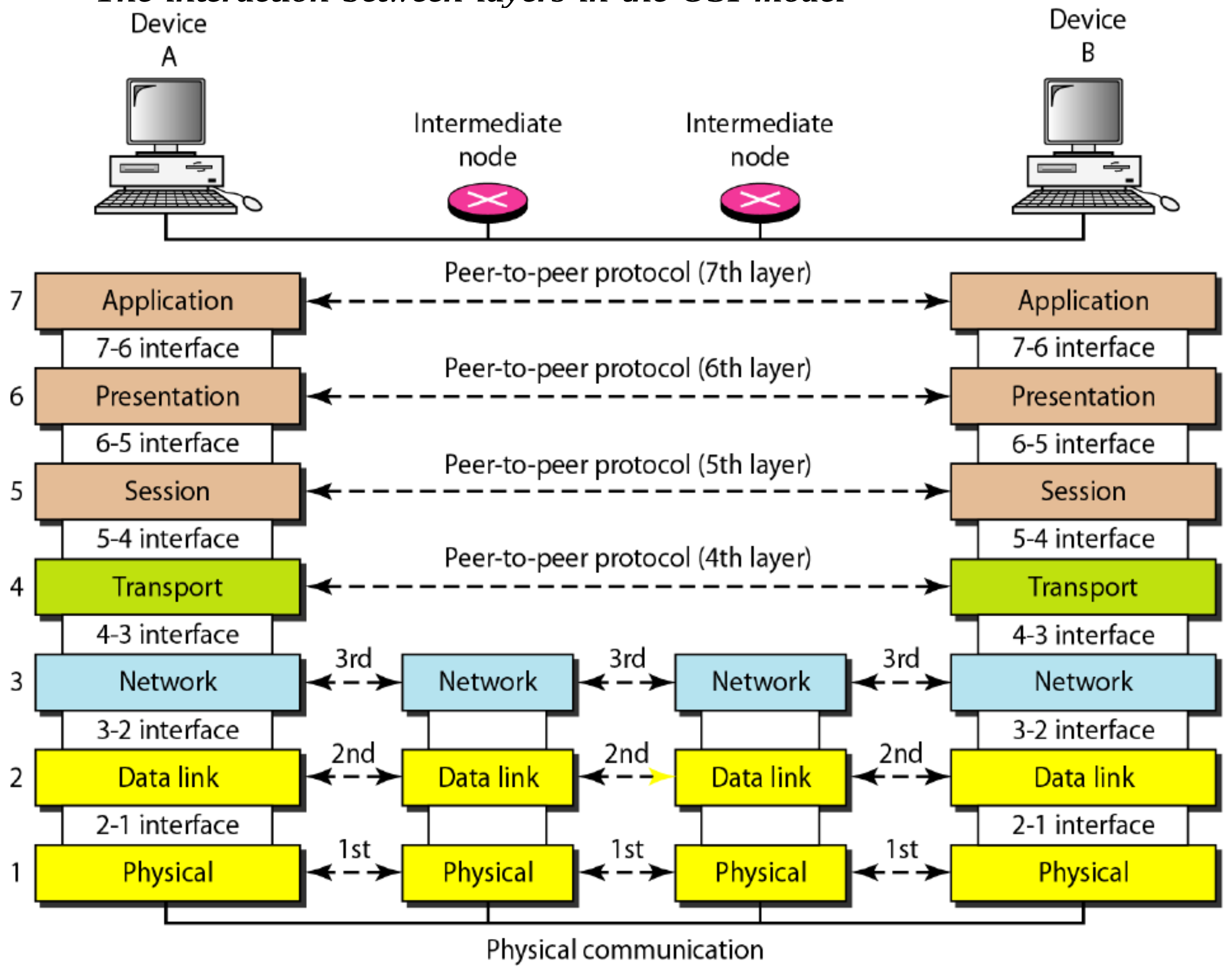
Local Internet service providers provide direct service to the end users. The local ISPs can be connected to regional ISPs or directly to national ISPs. Most end users are connected to the local ISPs. Note that in this sense, a local ISP can be a company that just provides Internet services, a corporation witha network that supplies services to its own employees, or a nonprofit organization, such as a college or a university, that runs its own network. Each of these local ISPs can be connected to a regional or national service provider.

Application Layer

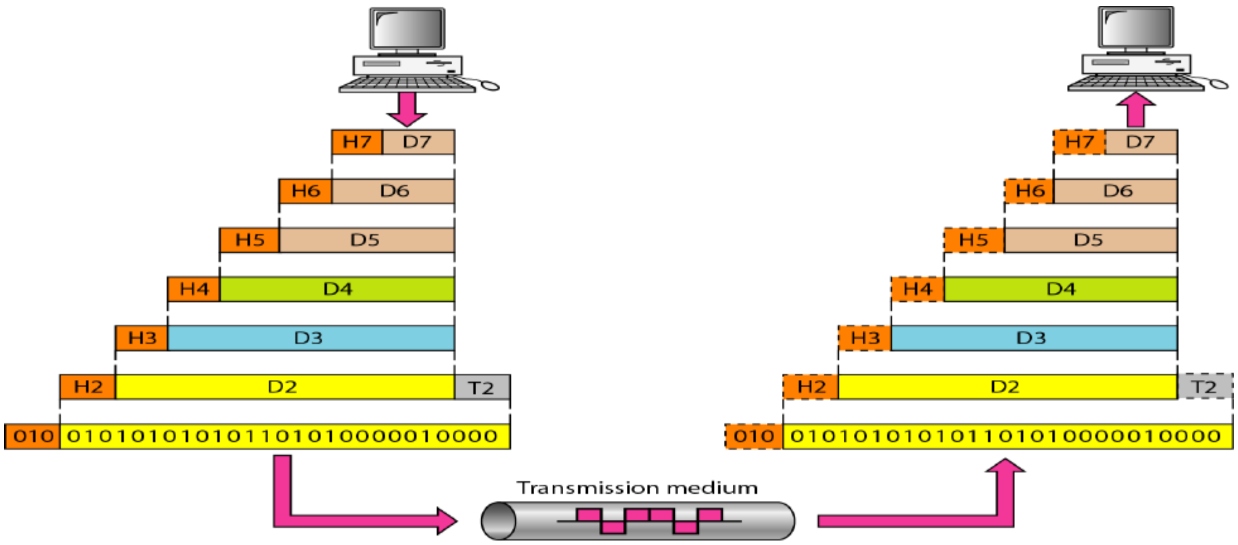
- Contains all services or protocols needed by application software or operatingsystem to communicate on the network
- Examples
  - –Firefox web browser uses HTTP (Hyper-Text Transport Protocol)
  - –E-mail program may use POP3 (Post Office Protocol version 3) to read e-mailsand SMTP (Simple Mail Transport Protocol) to send e-mails

TCP &UDP

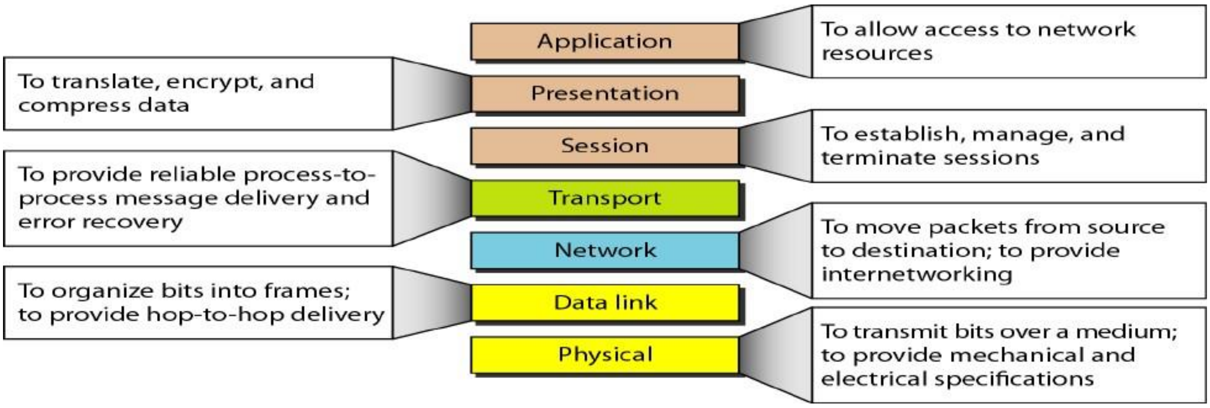
The interaction between layers in the OSI model



An exchange using the OSI model



TCP &UDP


Application
Presentation
Session
Transport
Network
Data link
Physical
To allow access to network resources
To translate, encrypt, and compress data
To establish, manage, and terminate sessions
To provide reliable process-to-process message delivery and error recovery
To move packets from source to destination; to provide internetworking
To organize bits into frames; to provide hop-to-hop delivery
To transmit bits over a medium; to provide mechanical and electrical specifications

TCP/IP Model (Transmission Control Protocol/Internet Protocol)

–A *protocol suite* is a large number of related protocols that work together toallow networked computers to communicate

Application Layer

- Application layer protocols define the rules when implementing specific networkapplications
- Rely on the underlying layers to provide accurate and efficient data delivery
- Typical protocols:
  - FTP – File Transfer Protocol
    - For file transfer
  - Telnet – Remote terminal protocol
    - For remote login on any other computer on the network
  - SMTP – Simple Mail Transfer Protocol
    - For mail transfer
  - HTTP – Hypertext Transfer Protocol
    - For Web browsing
- Encompasses same functions as these OSI Model layers ApplicationPresentation Session

Transport Layer

- TCP is a connection-oriented protocol
  - Does not mean it has a physical connection between sender and receiver
  - TCP provides the function to allow a connection virtually exists – also calledvirtual circuit
- UDP provides the functions:
  - Dividing a chunk of data into segments
  - Reassembly segments into the original chunk

TCP &UDP

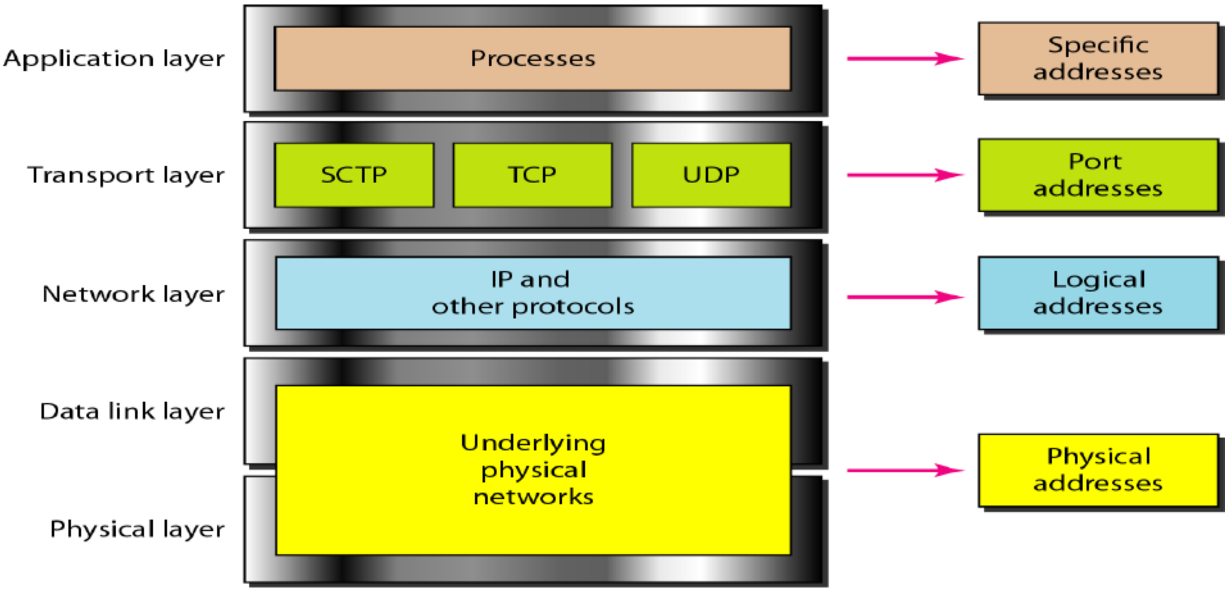
- Provide further the functions such as reordering and data resend
- Offering a reliable byte-stream delivery service
- Functions the same as the Transport layer in OSI
- Synchronize source and destination computers to set up the session betweenthe respective computers

Internet Layer

- The network layer, also called the internet layer, deals with packets and connects independent networks to transport the packets across network boundaries. The network layer protocols are the IP and the Internet Control Message Protocol (ICMP), which is used for error reporting.

Host-to-network layer

The **Host-to-network layer** is the lowest **layer** of the **TCP**/**IP** reference model. It combines the link **layer** and the physical **layer** of the ISO/OSI model. At this **layer**, data is transferred between adjacent **network** nodes in a WAN or between nodes on the same LAN.



The Web and Hyper Text Transfer Protocol

HTTP

- HTTP stands for **HyperText Transfer Protocol**.
- It is a protocol used to access the data on the World Wide Web (www).
- The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.

TCP &UDP

- This protocol is known as HyperText Transfer Protocol because of its efficiency that allows us to use in a hypertext environment where there are rapid jumps from one document to another document.
- HTTP is similar to the FTP as it also transfers the files from one host to another host. But, HTTP is simpler than FTP as HTTP uses only one connection, i.e., no control connection to transfer the files.
- HTTP is used to carry the data in the form of MIME-like format.
- HTTP is similar to SMTP as the data is transferred between client and server. The HTTP differs from the SMTP in the way the messages are sent from the client to the server and from server to the client. SMTP messages are stored and forwarded while HTTP messages are delivered immediately.

Features of HTTP:

- **Connectionless protocol:** HTTP is a connectionless protocol. HTTP client initiates a request and waits for a response from the server. When the server receives the request, the server processes the request and sends back the response to the HTTP client after which the client disconnects the connection. The connection between client and server exist only during the current request and response time only.
- **Media independent:** HTTP protocol is a media independent as data can be sent as long as both the client and server know how to handle the data content. It is required for both the client and server to specify the content type in MIME-type header.
- **Stateless:** HTTP is a stateless protocol as both the client and server know each other only during the current request. Due to this nature of the protocol, both the client and server do not retain the information between various requests of the web pages.

FILE TRANSFER

File transfer is the transmission of a computer file through a communication channel from one computer system to another. Typically, file transfer is mediated by a communications protocol. In the history of computing, numerous file transfer protocols have been designed for different contexts.

Protocols

A file transfer protocol is a convention that describes how to transfer files between two computing endpoints. As well as the stream of bits from a file stored as a single unit in a file system, some may also send relevant metadata such as the filename, file size and timestamp - and even file system permissions and file attributes.

Some examples:

TCP &UDP

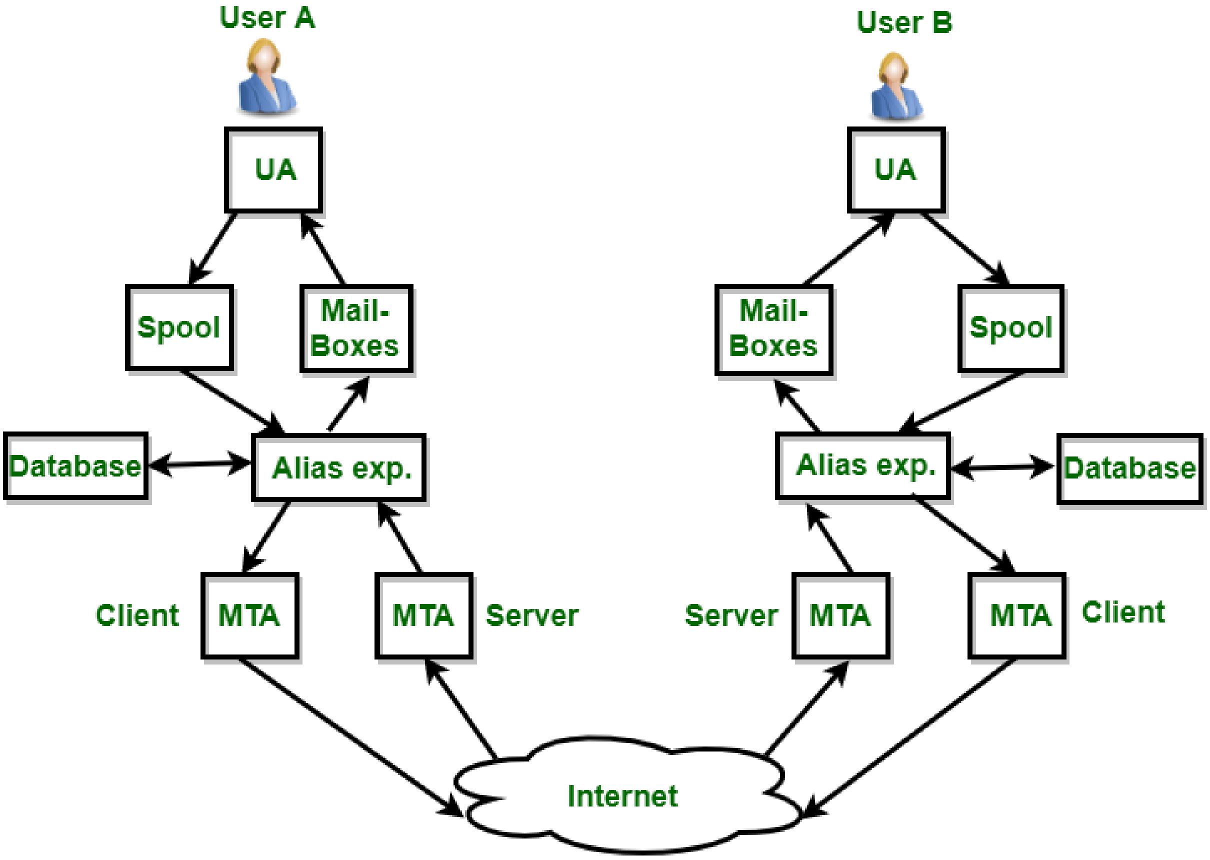
- FTP is an older cross-platform file transfer protocol[1]
- SSH File Transfer Protocol a file transfer protocol secured by the Secure Shell (SSH) protocol
- Secure copy (*scp*) is based on the Secure Shell (SSH) protocol
- HTTP can support file transfer
- Bittorent, Gnutella and other distributed file transfers systems use peer-to-peer
- In Systems Network Architecture, LU 6.2 Connect:Direct and XCOM Data Transport are traditionally used to transfer files
- Many instant messaging or LAN messenger systems support the ability to transfer files
- Computers may transfer files to peripheral devices such as USB flash drives
- Dial-up modems null modem links used XMODEM, YMODEM, ZMODEM and similar

Electronic Mail,

Electronic mail (e-mail) is a computer-based application for the exchange of messages between users. A worldwide e-mail network allows people to exchange e-mail messages very quickly. E-mail is the electronic equivalent of a letter, but with advantages in timeliness and flexibility. While a letter will take from one day to a couple of weeks to be delivered, an e-mail is delivered to the intended recipient's mailbox almost instantaneously, usually in the multiple-second to subminute range. This is the case whether the e-mail is exchanged between people on the same floor of a business, or between friends at opposite points on the globe. This article provides a comprehensive, intermediate-level overview of e-mail, including its main functions, historical and current architectures, key standards, supporting

TCP &UDP

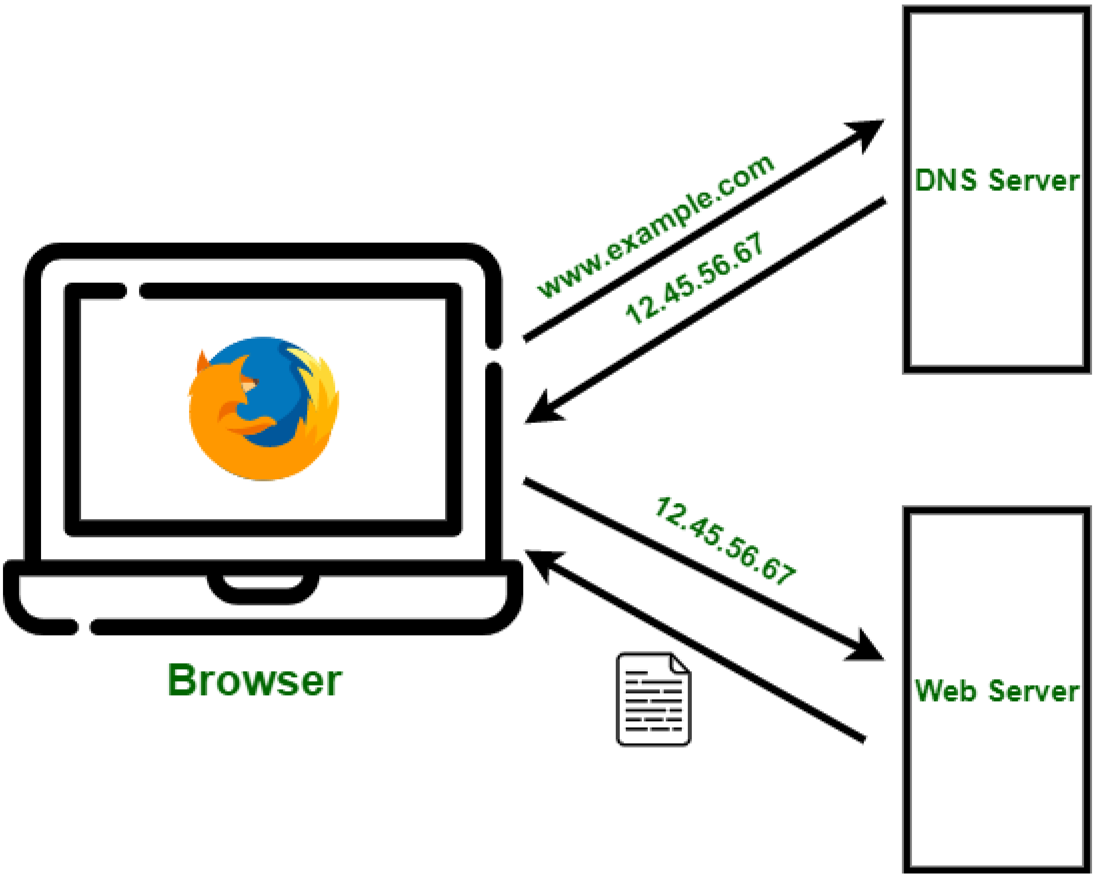
infrastructure, and contemporary and future issues.



Domain name system

The Domain Name System (DNS) is **the phonebook of the Internet**. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

TCP &UDP



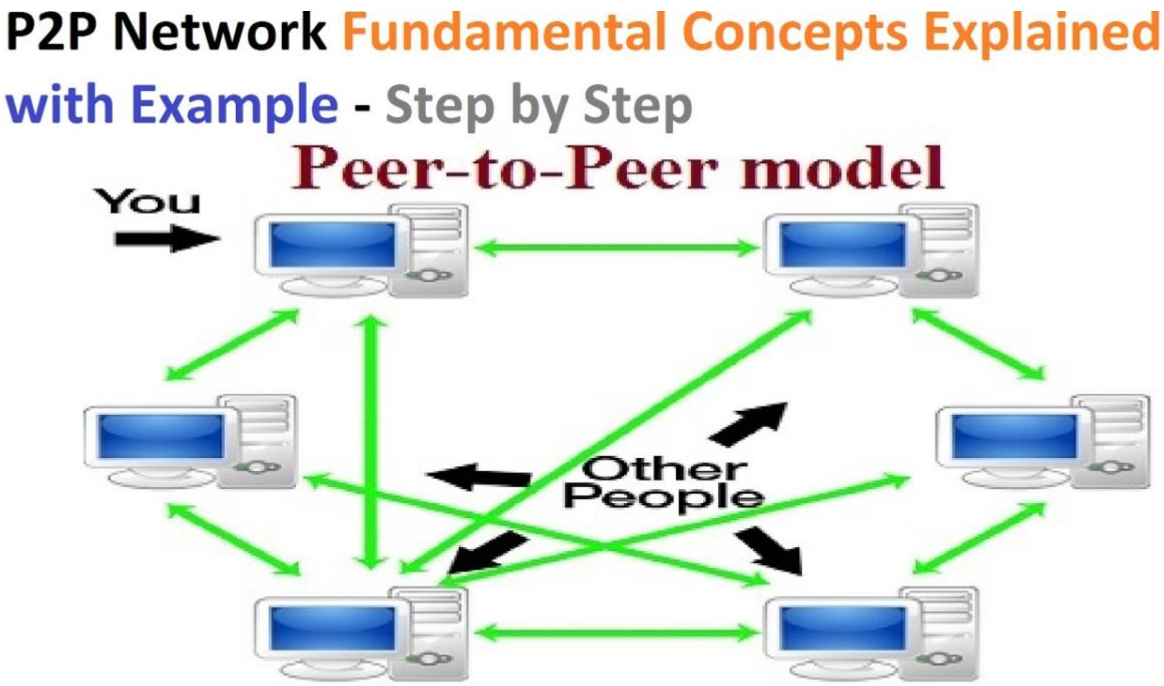
Peer-to-Peer file sharing

Peer-to-peer file sharing is the distribution and sharing of digital media using peer-to-peer (P2P) networking technology. P2P file sharing allows users to access media files such as books, music, movies, and games using a P2P software program that searches for other connected computers on a P2P network to locate the desired content.[1] The nodes (peers) of such networks are end-user computers and distribution servers (not required).

Peer-to-peer file sharing technology has evolved through several design stages from the early networks like Napster, which popularized the technology, to later models like the BitTorrent protocol. Microsoft uses it for Update distribution (Windows 10) and online playing games (e.g. the mmorpg *Skyforge*[2]) use it as their content distribution network for downloading large amounts of data without incurring the dramatic costs for bandwidth inherent when providing just a single source.

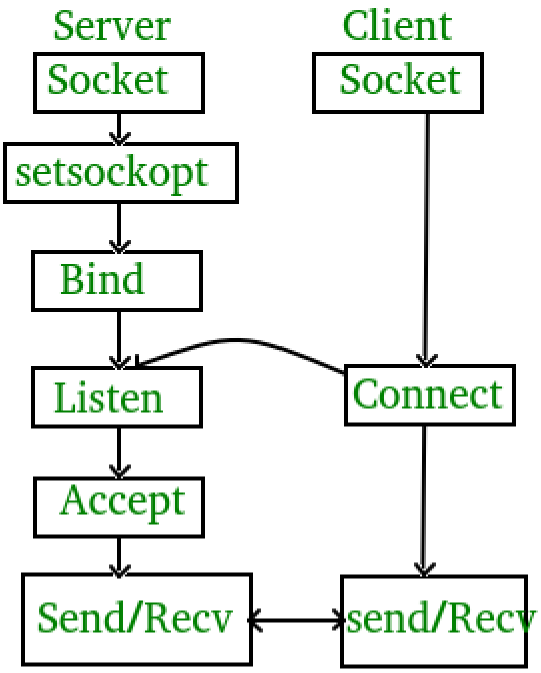
Several factors contributed to the widespread adoption and facilitation of peer-to-peer file sharing. These included increasing Internet bandwidth, the widespread digitization of physical media, and the increasing capabilities of residential personal computers. Users are able to transfer one or more files from one computer to another across the Internet through various file transfer systems and other file-sharing networks.

TCP &UDP


P2P Network Fundamental Concepts Explained with Example - Step by Step
Peer-to-Peer model
You
Other People

SOCKET PROGRAMMING

Socket programming is **a way of connecting two nodes on a network to communicate with each other**. One socket(node) listens on a particular port at an IP, while other socket reaches out to the other to form a connection. Server forms the listener socket while client reaches out to the server.



Layering concepts

TCP &UDP

The layered concept of networking was **developed to accommodate changes in technology**. Each layer of a specific network model may be responsible for a different function of the network. Each layer will pass information up and down to the next subsequent layer as data is processed.

he benefits to layering networking protocol specifications are many including:

Interoperability – Layering promotes greater interoperability between devices from different manufacturers and even between different generations of the same type of device from the same manufacturer.

Greater Compatibility – One of the greatest of all of the benefits of using a hierarchal or layered approach to networking and communications protocols is the greater compatibility between devices, systems and networks that this delivers.

Better Flexibility – Layering and the greater compatibility that it delivers goes a long way to improving the flexibility; particularly in terms of options and choices, that network engineers and administrators alike crave so much.

Flexibility and Peace of Mind – Peace of mind in knowing that if worst comes to worst and a key core network device; suddenly and without prior warning decides to give up the ghost, you can rest assured that a replacement or temporary stand-by can be readily put to work with the highest degree of confidence that it will do the job.

Even though it may not be up to doing the job at the same speed it will still do it; at least, until a better, more permanent solution can be implemented. This is a state of affairs that is much more acceptable than for a lengthy cessation of network services or assets unavailability to occur. 80% is oh so much more pleasing than 0%.

Increased Life Expectancy – Increased product working life expectancies as backwards compatibility is made considerably easier. Devices from different technology generations can co-exist thus the older units do not get discarded immediately newer technologies are adopted.

Scalability – Experience has shown that a layered or hierarchal approach to networking protocol design and implementation scales better than the horizontal approach.

Mobility – Greater mobility is more readily delivered whenever we adopt the layered and segmented strategies into our architectural design

Value Added Features – It is far easier to incorporate and implement value added features into products or services when the entire system has been built on the use of a layered philosophy.

Cost Effective Quality – The layered approach has proven time and time again to be the most economical way of developing and implementing any system(s) be they small, simple, large or complex makes no difference.

This ease of development and implementation translates to greater efficiency and effectiveness which in turn translates into greater economic rationalization and cheaper products while not compromising quality.

Modularity – I am sure that you have come across plug-ins and add-ons. These are common and classical examples of the benefits to be derived from the use of a hierarchal (layered) approach to design.

Innate Plasticity – Layering allows for innate plasticity to be built into devices at all levels and stages from the get-go, to implementation, on through optimization and upgrade cycles throughout a component’s entire useful working lifecycle thereafter.

The Graduated, Blended Approach to Migration – Compatibility enables technologies to co-exist side-by-side which results in quicker uptake of newer technologies as the older asset investments can still continue to be productive. Thus migration to newer technologies and standards can be undertaken in stages or phases over a period of time. This is what is known as the graduated blended approach; which is the opposite of the sudden adoption approach.

Standardization and Certification – The layered approach to networking protocol specifications facilitates a more streamlined and simplified standardization and certification process; particularly from an “industry” point of view. This is due to the clearer and more distinct definition and demarcation of what functions occur at each layer when the layered approach is taken.

Task Segmentation – Breaking a large complex system into smaller more manageable subcomponents allows for easier development and implementation of new technologies; as well as facilitating human comprehension of what may be very diverse and complex systems.

Portability – Layered networking protocols are much easier to port from one system or architecture to another.

Compartmentalization of Functionality – The compartmentalization or layering of processes, procedures and communications functions gives developers the freedom to concentrate on a specific layer or specific functions within that layer’s realm of responsibility without the need for great concern or modification of any other layer.

TCP &UDP