Subject: Introduction to IT

Subject Code: (18K3CSEL01)

Staff In-Charge:

1. Mrs. R.VALARMATHY.
2. Mrs. K. SHARMILA.

UNIT III: Networking: Introduction – Advantages of Networks – Save money by sharing resources - Remote services: Types of Networks - Benefits. Network Roles – Network Categories – Server Type - Network Topology –Network hardware connections – TCP/ IP Port and Addresses – Network Devices – Network Addressing.

UNIT IV: Network Cabling – Wireless Networking – Firewalls – Network Broadcasting and Multicasting: Internet Group Management Protocol -Dynamic Routing - Route Discovery Methods – SMTP - Mail Protocols.

UNIT V: Internet Basics: Networking – Internet – Important Features –Prerequisites for Internet: Hardware - Software – Factors Affecting the Speed of Internet Connectivity: Speed - Internet Protocols: IP Address – Domain naming System (DNS) – Communication Protocols – Configuring the Modem – Configuring a TCP/ IP Connection - Configuring Dial UP Networking.

Text:
"Introduction to Information Technology"-Sanjay Saxena - Vikas Publishing House Pvt. Ltd., – Reprint 2011, 2013.
Chapters: 1, 2, 3, 4, 8.

UNIT-III

Networking

Communication is impossible without some sort of language or code. In computer networks, these languages are collectively referred to as Protocols. Protocols, in computer networks are nothing but very strict rules for the exchange of messages between two or more hosts.

ADVANTAGES OF NETWORKS

A network makes it easier to communicate between computers. There are 2 major ways by which networks advantage people and organizations

1. Save money by sharing resources
2. Remote services

1. Save money by sharing resources:

- Many people can be connected using only one connection by sharing internet connection resources
- Many people are able to use one printer by sharing printing resources.
- Cost saving by sharing other resources like faxes, CD-ROM towers, network storage & directory services.
- Teacher sending notes via email instead of printing the notes,

then photocopying it, collating it, stapling it and finally handing out to the students.

2. Remote services: Remote services give customers more control and Reduce errors. Some examples include

- Customers ordering over the internet
- Business to business transactions such as ATMs

It can be explained in simple terms the way networks are put together, and how data packets are sent between networks and subnets along with how data is routed to the internet. This networking chapter is broken into five main sections.

They are:

1. Basics -Explaining the different protocols and how they work together.

2. Media - Describing the cabling and various media used to send data between multiple points in a network.

3. Architecture - Explaining some of the popular network architectures. Network architecture refers to the physical layout (topology) of a network along with the physical transmission media (Type of wire, wireless, etc) and the data access method (OSI Layer). It includes Ethernet, Token Ring. ARC net, AppleTalk, and FDDI.

4. Other Transport Protocols - Explaining IPX/SPX, NetBEUI in brief.

5. Functions - Explaining the functionalities of networking like routing, firewalls and DNS.

We will start with the networking basics in order to get a good grasp of networking concepts. It would help us in understanding how each network protocol is used to perform networking. why each protocol is needed, how it is used, and what other protocols it relies upon. We would also explain the data encapsulation techniques in preparation for transport along with some of the networking protocols such as IP, TCP, UDP, ICMP, and IGMP. In functional areas, such as routers, we would get a grasp of routing, IP masque adding and firewalls and give brief explanation of how they work, how they are set up as well as how and why they are used. Application protocols such as FTP and Telnet are also
Briefly described.

TYPES OF NETWORKS

Local Area Network (LAN) A local area network (LAN) is the communication between different computers connected by cables, to each other in a single location, usually a single floor of a building or all the computers in a small company.

Wide Area Network (WAN) WANs are the communication between one or more LANs by telephone lines leased form the various telephone companies, satellite links, packet radio, or microwave transceivers. WANs are private and owned by the businesses that operates with them. The Internet has emerged as both the largest and the least expensive WAN in the world. Many companies take advantage of it now by forming private WANs, known as VPNs, or Virtual Pnyate Networks, through encrypted communications over the internet.

Benefits

1. **Sharing information:** A network can help you to centralize the information and control over it by having one computer to store the shared information and have all other computers reference the information on that computer over the network.
2. **Sharing hardware resources:** A network allows anyone connected to the network to use printers, fax modem, scanners, tape backup units or almost any other device that can be attached to a computer.

3. **Sharing software resources:** Administrators can centrally install and configure the software and also restrict access to the software. It is easier than doing it on every one of the computers in an organization.

4. **Preserving information:** A network allows for information to be backed up on a central location. It is difficult to maintain regular backups on a number of stand-alone computers as important information can be lost easily by mistake or by accident.
5. **Protecting information:** A network provides a more secure environment for a company's important information than stand-alone computers. Networks provide an additional layer of security by way of passwords.

6. **Electronic -mail (e-mail):** Computer network also helps people to communicate through e-mail. You can attach electronic documents like photo, sound and video clip toan e-mail message.

Network Roles

The role of a computer is determined simply by its use in the network many times. There are three roles of computers in a local area network.

1. The first role is of being a client which utilizes network resources but do not provide network resources.
2. The second one is of being peers which both use and provide network resources.
3. The last one is of being servers which provide network resources.

1 . Server (domain) / Client Networks Server-based (also called client-server) networks are defined by the presence of servers on a network that Provide security and administration of the networks. It consists with many clients and one or more servers. Clients (often called the “front end”) request services, such as file storage and printing, and servers (often called the “back end”) deliver them. In Windows NT or Windows 2000, server-based networks are organized into domains. Domains are collection of networks and clients that share security trust information. Domain security and logon
permission are controlled by special servers called domain controllers. There is one master domain controller, called the Primary Domain Controller (PDC) and the secondary domain controllers called Backup Domain Controller (BDC) may assist PDC during busy times or when the PDC is not available for some reason.

The server-based networks have many advantages, including:

- Central file storage, which allows all users to work form the same set of data and provides
  - Easy backup of critical data and keeps data from getting lost among computers
  - Ability of servers to pool available hardware and software, lowering overall costs.
  - Optimized dedicated servers, which are faster than peers at sharing network.
  - Freeing of users from the task of managing network.
  - Easy manageability of a large number of users.
  - Ability to share expensive equipment, such as laser printers.
  - Less intrusive strong central security, as only a single password need to access all shared resources on the network

Server-based networks also have some disadvantages, including:

- Expensive dedicated hardware

- Expensive network operating system software's and client licenses

- A dedicated network administrator (usually required)

2 . Peer Networks Every computer on a peer network is equal and can communicate with any other computer on the network to which it has been granted access rights. So basically, every computer on a peer network functions both as a server and as a client.
The peer network is more common in small businesses.

The advantages of peer networks are:

- No extra investment for server software and hardware are needed
- No network administrator is needed
- Easy setup
- Lower cost

The disadvantages of peer networks are:

- Additional load on computers for resource sharing
- Lack of central organization, making it difficult to find data
- Users must administer their own computers
- Weak and intrusive security

3. Hybrid Networks Hybrid networks consists of all three types computers and have active domains and working groups.

Network Categories

The two main types of network categories

1.Server based In a server based network, the computers are set up to be the primary providers of services, such as file service or email services. The computers provided the service are called servers and the computer that request and use the services are called client computers.

2. Peer-to-Peer In a peer to peer various computer connected to the network can act as both client and server.

Server Type
There are several tasks for a server in a network. All these tasks could be done by one server. or a separate server for each tasks. Server is dedicated to performing specific tasks in support of other computers on the network.

1.**File Server** File servers offer the services, which are the network applications that store, retrieve, and move data. With a file server, users can exchange, read, write, and manage shared files as well as the data contained in them. There are three ways to store a file on a network. They are:

- **Online storage:** Online storage consists of hard drive storage. Hard drive is very fast but expensive so only the most current and frequently needed information is stored.

- **Offline storage:** The common offline storage devices are data tapes and removable optical disks. The biggest disadvantage of offline on

  Must retrieve the disk or tape and mount it on the server.
- **Near-line storage:** Near-line storage uses a machine, such as a tape carousel or jukebox and automatically retrieves and mounts the tape or disk. It is faster than offline but still only enough for infrequently used data and applications.

2.Print Server Print server manages and control printing on a network and also offers fax service. The print server allows multiple and simultaneous access to print and fax services. The network operating system achieves this by using print and fax queues. The queues are special storage areas where printing and faxing jobs are stored and then sent to the printer or fax device in an organized fashion.

3. Application Server Application server allows a client on the network to access and use extra computing power and expensive software applications on a shared computer. Application servers are used when efficiency and security requires a program to stay close to the data, and the data stays in one place.

4. Message Server Message server allows a wide variety of communication methods that are much complex than a simple file server can handle. Data can take the form of graphics, digitized video, or audio, text and binary. Message servers must coordinate the complex interactions between users, documents, and applications.

5. Database Server A Database server is one of the application servers. Database server allows a network with powerful database capabilities. So, users of a relatively weak client can enjoy the same power of database servers.

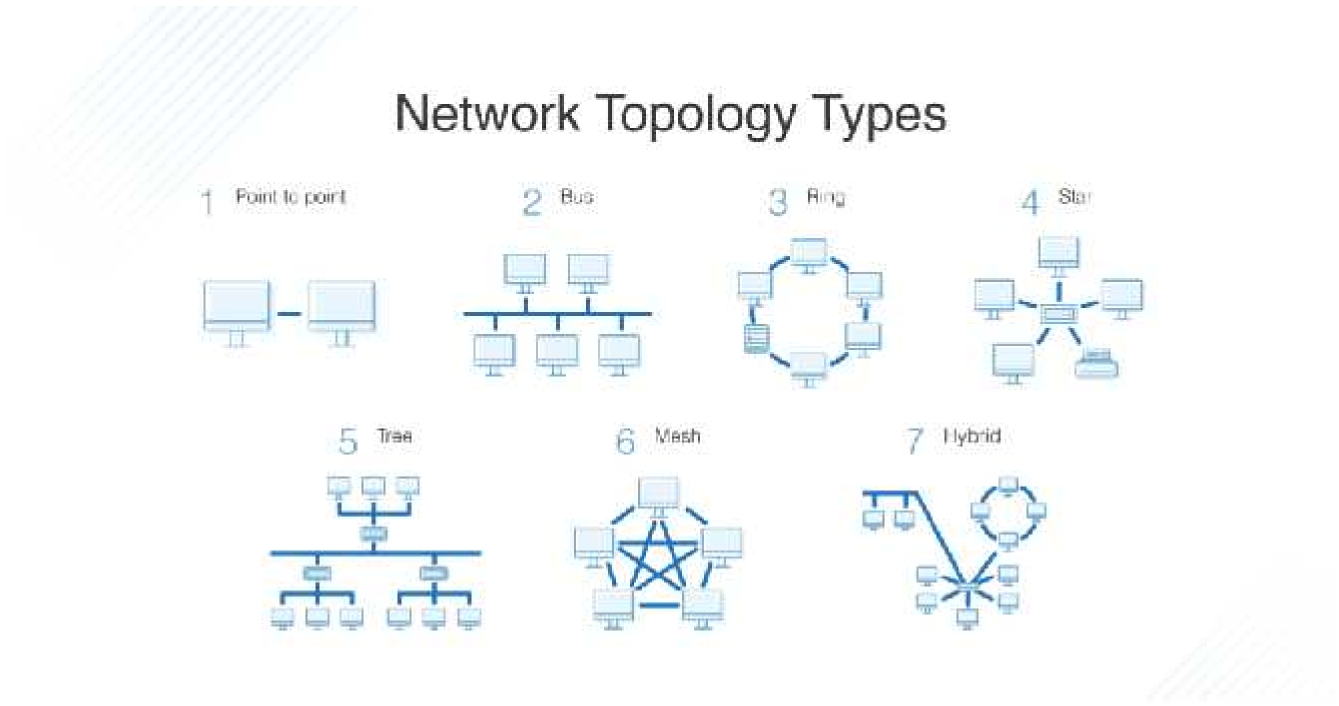
Network Topology

The network topology describes the method used to do the physical wiring of the network. In other words, network topology is the physical layout of the network and how the cable is run between them. It is important to use the right topology. Each topology has its own strengths and weakness. The main ones include bus, star, and ring.

1. Bus topology — In bus topology, both ends of the network must be terminated with a terminator. A barrel connector can be used to extend it.

2. Star topology — In star topology, all devices revolve around a central hub, which controls the network communications, and can also communicate with other hubs. Range limits are generally about 100 meters from the hub. All Ethernet networks use the star topology.

3. Ring topology - In ring topology, devices are connected from one to another, as in a ring. A data token is used to grant permission for each computer to communicate.



There are also hybrid networks such as a star-bus hybrid, star-ring network, and mesh networks with connections between various computers on the network. Mesh networks ideally allow each computer to have a direct connection to each of the other computers.

1. Bus topology A bus topology connects computers along a single or more cable to connect linearly as shown in the figure below. A network that uses bus topology is referred to as a “bus network” which was the orginal form of Ethernet networks. Ethernet 10Base2 (also known as thin-net) is used for bus topology. Bus topology is the cheapest way of connecting computers to form a workgroup or departmental LAN, but it has the disadvantage that a single loose connection or cable break can bring down the entire LAN. Termination is important issue in bus networks. The electrical signal from a transmitting computer is free to travel the entire length of the cable. Without termination, when the signal reaches the end of the wire, it bounces back and travels back up the wire. When a signal echoes back and forth along an un-terminated bus, it is called ringing. The terminators absorb the electrical energy and stop the reflections.

Advantages of bus topology are:

- Bus is easy to use and understand and an inexpensive simple network

- If is easy to extend a network by adding cable with a repeater that boosts the signal and allows it to travel a longer distance.

Disadvantages of bus topology are.

- A bus topology becomes slow by heavy network traffic with a lot of computer because networks do not coordinate with each other to reserve time to transmit.

- It is difficult to troubleshoot a bus because a cable break or loose connector will cause reflections and bring down the whole network.

1**. Star topology A star topology** links the computers by individual cables to a central unit, usually a hub. When a computer or other networking component transmits a signal to the network, the signal travels to the hub. Then, the hub forwards the signal simultaneously to all other components connected to the hub. Ethernet 10BaseT is a network based on the star topology. Star topology is the most popular way to connect computers in a workgroup or departmental network.

Advantages of star topology are:

- The failure of a single computer or cable doesn’t bring down the entire network.

- The centralized networking equipment can reduce costs in the long run by making network management much easier.

- It allows several cable types in same network with a hub that can accommodate multiple cable types.

Disadvantages of star topology are:

- Failure of the central hub causes the whole network failure.

- It is slightly more expensive than using bus topology.

1.Ring topology A ring topology connects the computers along a single path whose ends are joined to form a circle or a ring. The circle might only be logical but the physical arrangement of the cabling might be similar to star topology, with a hub or concentrator at the center. The ring topology is commonly used in token ring networks and that the ring, of a token ring network is concentrated inside a device called a Multi Station Access Unit (MAU) and in fiber Distributed Data Interface (FDDI) networks,
the ring is both a physical and logical ring and usually runs around a campus or collection of buildings to form a high-speed backbone network.

Advantages of ring topology

- One computer cannot monopolize the network.

- It continues to function after capacity is exceeded but the speed will be slow.

Disvantages of ring topology

- Failure of one computer can affect the whole network.

- It is difficult to troubleshoot.
- Adding and removing computers disrupts the network.

4. **Mesh topology** In a mesh topology, each computer on the network has redundant data paths. The mesh topology provides fault tolerance -if a wire, hub, switch, or other component fails, as data can travel along an alternate path.. A mesh topology is most often used in large backbone networks in which failure of a single switch or router can result in a large portion of the network going down.

NETWORK HARDWARE CONNECTIONS

There are three types of networks that are commonly heard about. They are
Ethernet, token-ring, and ARC net. Each one is described briefly here, although this document is mainly about Ethernet.

1. Ethernet: The network interface cards share a common cable. This cable structure does not need to form a structure, but must be essentially common to all cards on the network. Before a card transmits, it listens
for a break in traffic. The cards have collision detection, and if the card detects a collision while trying to transmit, it will retry after some random time interval.

- Each computer in the network ‘listens’ to the cable before sending anything through the network, If the network is clear, the computer will transmit.

- If another computer is already transmitting on the cable, the computer will wait and try again when the line is clear

- Sometimes, two computers attempt to transmit at the same instance. When this happens, a collision occurs, Each computer then backs off and waits a random amount of time before attempting to retransmit. It is normal to have collisions using this method, but the delays caused by collisions and transmissions is small, and does not effect speed of transmission on the network

- Ethernet protocol allows for data to be transmitted over:
  - twisted pair cable
  - coaxial cable
  - fiber optic cable

2. Fast Ethernet: Fast Ethernet allows faster transmission and has developed a new standard that supports 100 Mbps. Fast Ethernet requires the use of more expensive equipment and network cards .
3. Token Ring: Token ring networks form a complete electrical loop, or ring. Around the ring are computers, called stations. The cards, using their built in serial numbers, negotiate to determine what card will be the master interface card. This card will create what is called a token that will allow other cards to send data.

Essentially, when a card with data to send, receives a token, it sends its data to the next station up the ring to be relayed. The master interface will then create a new token and the process begins again. A single electronic ‘token’ moves around the ring from one computer to the next. If a computer wishes to transit and receives an empty token, it attaches data
to the token which then proceeds around the ring until it comes to the computer the data is meant for.

4. ARCnet: ARCnet networks designate a master card. The master card keeps a table of active cards, polling each one sequentially with transmit permission.

TCP/IP PORTS AND ADDRESSES

Each machine in the network has one or more network cards. The part of the network that does the job of transporting and managing the data across the network is called TCP/ IP which stands for Transmission Control Protocol (TCP) and Internet Protocol (IP). There are other alternative mechanisms for managing network traffic, but most, such as IPX/SPX for Netware, will not be described here in much detail. The IP layer requires a (IPv4) or 6 (IPv6) byte address to be assigned to each network interface card on each computer. This can be done automatically using network software such as dynamic host
configuration protocol (DHCP) or by manually entering static addresses into the computer.

ports

The TCP layer requires what is called a port number to be assigned to each message. This way it can determine the type of service being provided. When we are talking about “ports” we are not talking about ports that are used for serial and parallel devices, or ports used for computer hardware control. These ports are merely reference numbers used to define a service. For instance, port 23 is used for telnet services, and HTTP uses port 80

Addresses

Addresses are used to locate computers on the networks. Without an IP numbering system, it would not be possible to determine where network data packets should go. Each number represents a byte value with a possible mathematical range of 0-255. the first one or two bytes, depending on the class of network, will generally indicate the number of the
network, the third byte indicates the number of the subnet, and the fourth number indicates the host number. Broadcasting is a form of communication that all hosts on a network can read, and is normally used for performing various network queries.

IPv6 is an enhancement to the IPv4 standard due to the shortage of internet addresses. The dotted notation values are increased to 12 bit values rather than byte (8 bit) values. This increases the effective range of each possible decimal value to 4095.

The OSI Reference model

Open Systems Interconnection Basic Reference Model (OSI Reference Model or OSI Model) is an abstract description for layered communications and computer network protocol design. It was developed as part of the Open Systems Interconnection (OSI) initiative. In its most basic form, it divides network architecture into seven layers which, from top to bottom, are the Application, Presentation, Session, Transport, Network, Data-Link, and Physical

Layers.

The Physical Layer:

One of the major functions of the physical layer is to move data in the form of electromagnetic signals across a transmission medium.

Its responsible for movements of individual bits from one hop (Node) to next. Both data and the signals can be either *analog* or *digital*.

Transmission media work by conducting energy along a physical path which can be wired or wireless

- Physical characteristics of interface and medium (Transmission medium)
- Representation of bits (stream of bits (0s or 1s) with no interpretation and encoded into signals)
- Data rate (duration of a bit, which is how long it last)
- Synchronization of bits (sender and receivers clock must be synchronized)
- Line configuration (Point-to-Point, Point-to-Multipoint)
- Physical topology
- Transmission mode (Simplex, half duplex, full duplex)

The Data Link Layer:

- The data link layer provides the functional and procedural means to transfer the data between network entities and to detect and possibly correct errors that may occur in the physical layer.
- The main task of data link layer is to transform a raw transmission facility into a line that appears free of undetected transmission errors to the network layer.

The Network Layer:

It determines how the packets are routed from source to destination. The network layer controls the operations of the subnet. Routes can be based on static tables that are wired into the network that are rarely changed. they can be highly dynamic, being determined a new for each packet, to reflect the current network load. If too many packets are present in the subnet at the same time, they will get in one another`s way, forming bottlenecks. The network layer performs network routing functions, and might also perform fragmentation and reassembly, and report delivery errors. Routers operate at this layer- sending data throughout the extended network and making the Internet possible.

Transport layer:

The basic function of transport layer is to accept the data from the above , split it up into smaller units if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end.

It also determines what type of service to provide to the session layer. The transport layer provides transparent data between end users, providing reliable data transfer services to the upper layers.

It controls the reliability of a given link through flow control, segmentation/re-segmentation, and error control. It converts the messages into TCP (Transmission Control Protocol) segments or User Data Gram Protocol (UDP)etc. packets.

The session Layer:

The session Layer allows the user on different machines to establish sessions between them. It establishes, manages, and terminates the connection between the local and remote applications.

Sessions offers various services, including dialog control, token management, and synchronization.

The Presentation Layer:

The presentation layer concerned with the syntax and semantics of information transmitted.

The Application Layer:

The application layer interfaces directly to performs application services

For the application processes and also issues the request to the presentation layer. This layer provides the services to the user-defined application processes and not to the end user.

This layer contains the variety of protocols that are commonly needed by the users. One application protocol is HTTP which is the basis of the World Wide Web.

TCP/IP Reference Model:

TCP/IP Model layers

4. Application Layer
1. Transport Layer

2. Network Layer.

1.Data Link Layer.

TCP/IP includes a wide range of protocols which are used for variety of purposes on the network. The set of protocols that are a part of TCP/IP is called the TCP/IP protocol stack .

Many protocols, message types, levels, and services that TCP/IP networking support, The link layer is the hardware layer layer that provides ability to send messages between multiple locations.

Network devices:

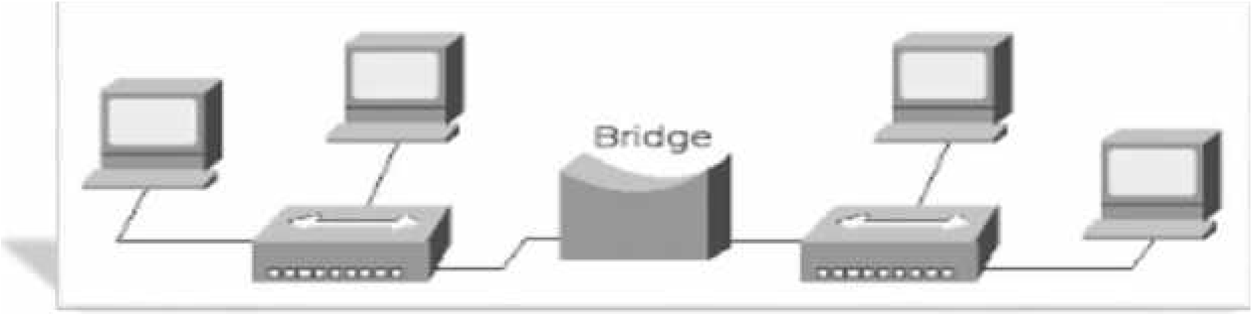
- A hub is a multiport connecting device that is used to interconnect LAN devices.
- A hub can be used to extend the physical length of a network.

Repeater:

- Repeater boost or amplifies the signal before passing it through to the next section of cable.

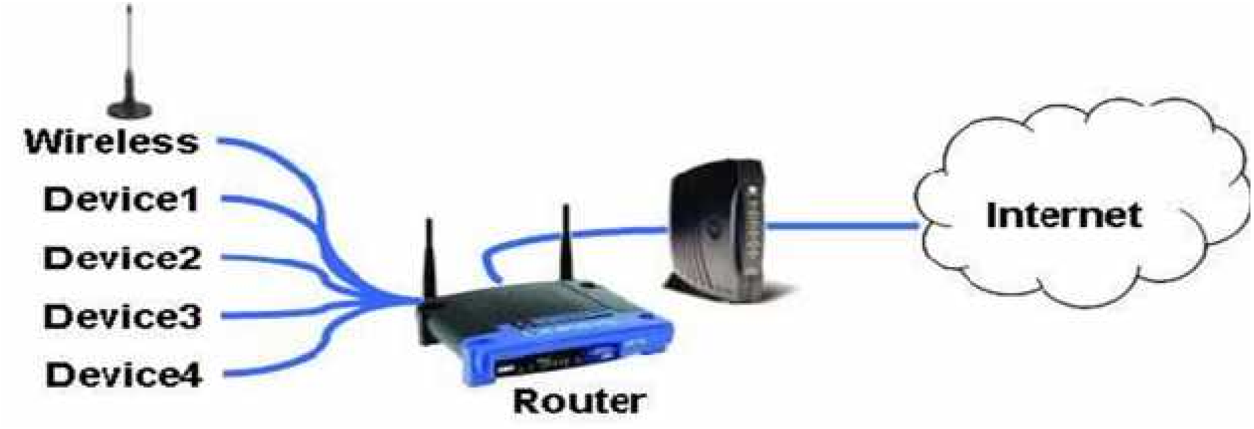
Bridges:

- It connects the network with same protocol and topology.
- The main task of a bridge computer is to receive and pass data from one LAN to another.



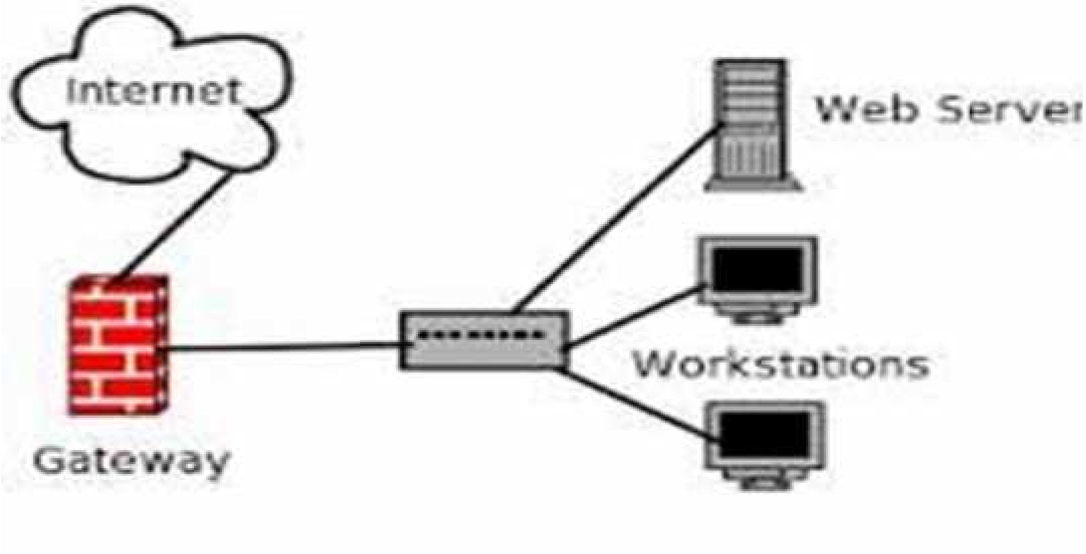
Router:

- A router is a device that connects multiple networks using similar or different protocols.
- Routers are used when several networks are connected together.



Gateway:

- Gateway is a device that connects two or more networks with different types of protocol.
- It receives data from one network and converts it according to the protocol of other network.



Address Resolution Protocol

ARP and RARP Address translation

- Address Resolution protocol provides a completely different function to the network than Reverse Address Resolution Protocol.
- It is used to resolve the Ethernet address of a NIC from an IP address inorder to construct an Ethernet packet around an IP data packet.This must happen inorder to send any data across the network.

Reverse Address Resolution Protocol:

- It is used for diskless computer to determine their IP address using the network. The RARP message format is very similar to ARP format.
- It places its own hardware address in both the sending and receiving fields in the encapsulated data packet. the RARP server will fill in the correct sending and receiving IP address in its response to the message.

Network Addressing:

IP address are broken into four octets(IPv4) seperted by dots called dotted decimal notation. An octed is a byte consisting of 8 bits.

Example: 192.168.10.1
There are two parts of an IP address: a Network ID and a host ID.

Subnet mask:

Subnetting is the process of breaking down a main class A, B or C networks into subnet for routing purposes. The advantages are network traffic isolation, simplified administration, improved security.

User DataGramProtocol:

It support the network at the transport layer. UDP is an unreliable connectionless protocol. It is a datagram service and there is no guarantee that the data will reach its intended destination. It adds very little IP data packets except for some error checking and port direction.

The following protocol or services use UDP:

- UDP
- SNMP
- BOOTP
- TFTP
- NFS
- RPC
- RIP

UDP Message Format : The UDP header includes the following

1. Source port number(16-bits) an optional field.
2. Destination port number(16-bits)
3. UDP length(16-bits)
4. UDP Checksum(16-bits)

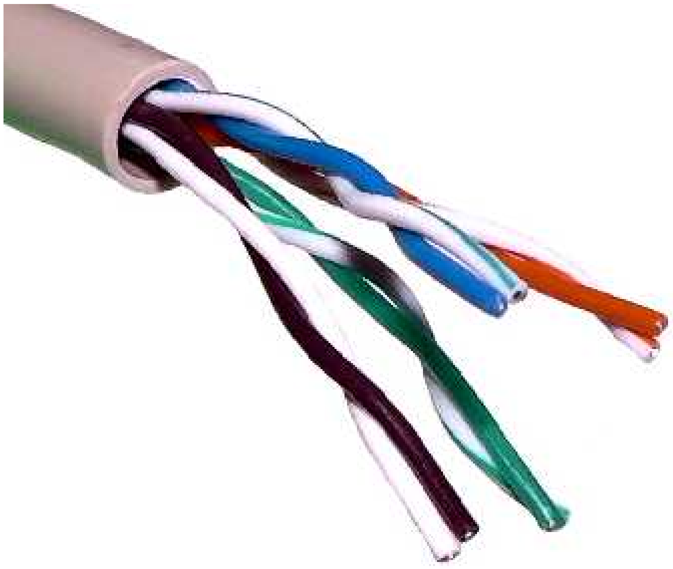
UNIT IV

NETWORK CABLING

Networking cables are networking hardware used to connect one network device to other network devices or to connect two or more computers to share printers, scanners etc. Different types of network cables, such as coaxial cable, optical fiber cable, and twisted pair cables, are used depending on the network's physical layer, topology, and size. The devices can be separated by a few meters (e.g. via Ethernet) or nearly unlimited distances (e.g. via the interconnections of the Internet).

There are several technologies used for network connections. Patch cables are used for short distances in offices and wiring closets. Electrical connections using twisted pair or coaxial cable are used within a building. Optical fiber cable is used for long distances or for applications requiring high bandwidth or

electrical isolation. Many installations use structured cabling practices to improve reliability and maintainability. In some home and industrial applications power lines are used as network cabling.



Two types of signaling methods are used to transmit information over network media: baseband and broadband.

Baseband

Baseband transmissions typically use digital signaling over a single wire; the transmissions themselves take the form of either electrical pulses or light. The digital signal used in baseband transmission occupies the entire bandwidth of the network media to transmit a single data signal. Baseband communication is bidirectional, allowing computers to both send and receive data using a single cable. However, the sending and receiving cannot occur on the same wire at the same time.

Broadband

Whereas baseband uses digital signaling, broadband uses analog signals in the form of optical or electromagnetic waves over multiple transmission frequencies. For signals to be both sent and received, the transmission media must be split into two channels. Alternatively, two cables can be used: one to send and one to receive transmissions.
Physical media
Twisted-pair cables

- ✓ In the UTP (Unshielded twisted-pair) cable, all pairs are wrapped in a single plastic sheath.
- ✓ In the STP (Shielded twisted-pair) cable, each pair is wrapped with an additional metal shield, then all pairs are wrapped in a single outer plastic sheath.

Coaxial

This cable contains a conductor, insulator, braiding, and sheath. The sheath covers the braiding, braiding covers the insulation, and the insulation covers the conductor.
Fiber optic cable functions as a "light guide," guiding the light introduced at one end of the cable through to the other end. The light source can either be a light-emitting diode (LED)) or a laser.The light source is pulsed on and off, and a light-sensitive receiver on the other end of the cable converts the pulses back into the digital ones and zeros of the original signal.

- ✓ Single Mode cable for use with lasers.

✓ Multi-Mode cable for use with Light Emitting Diode (LED)

Cable Standards

The Electronic Industries Association and Telecommunications Industries Association (EIN TIA) defined a standard called ElA/TIA 568 which is a commercial building wiring standard
for UTP cable. It defines transmission speed and twists per foot.

Category	Speed	Notes
1	None	
2	4Mps	
3	10Mps	
4	l6Mps	
5	100Mps	
6	Data patch,	

The maximum transmission length is100 meters.is100meters. This cable is susceptible to interference.

WIRELESS NETWORKING

This section may be skipped by all readers and used by those interested in wireless network technology. Transmission of waves takes place in the electromagnetic

(EM) spectrum. The carrier frequency of the data is expressed in cycles per second called hertz (Hz). Low frequency signals can travel for long distances through many obstacles but can not carry a high handwidth of data. High frequency signals can travel for shorter distances through few obstacles and carry a narrow bandwidth. Also the effect of noise on the signal is inversely proportional to the power of the radio transmitter, which is normal for all EM transmissions. The three broad categories of wireless media are:

1. Radio – 10 KHz to 1 GHz. It is broken into many bands including AM, FM, and VHF hands. The federal communications Commission (FCC) regulates the assignment of these frequencies for unregulated use are:902 928 MHz – Cordless phone, remote controls2.4 GHz 5.72 – 5.85 GHz

2. Microwave – This include Terrestrial - Used to link networks over long distances but the two microwave lowers must have a line of sight between them. The frequency is usually 4-6GHz Or 21 – 23GHz.

Satellite **-** A satellite orbits at 22,300 miles above the earth which is an altitude that will Cause it to stay in a fixed position relative to the rotation of the earth This is called a geosynchronous orbit.. A station on the ground Will send and receive signals from the satellite.

The signal can have propagation delays between 0.5 and 5 s econds dd to the distances involved. The transmission frequency is normally 11- 14GHz With a transmission speed in the range of 1- 10Mbps.

3. **Infrared** - Infrared is just below the visible range of light between 100 GHz and 1000
THz.. A light emitting diode (LED) or laser is used to transmit the signal. The original cannot travel through objects. Light may interfere with the signal. The types of infrared are
i.Point to point - 'Iransmission frequencies are 100GHz-

1000THz.Transmission is between two points and is limited to line of sight range. It is difficult to eavesdrop on the transmission.
ii.Broadcast - The signal is dispersed sevaral units may receive the signal, 111e unit used to disperse the signal, may be a reflective material or a transmitter that amplifies and retransmits the signal.

Categories of LAN Radio Communications

1. Low power, single frequency - Its feature are

- distance is in 10 of meter .
- speed range from 1-10Mbp .
- susceptible to interferes e and eavesdropping.

2 High power. ingle frequency- It feature are

- Requires FCC licen mg and high power transmitter.
- Speed range from 1-
- Suseeptible to interferene and eave dropping

Spread spectrum generally makes use of a sequential noise-like signal structure to spread the normally narrowband information signal over a relatively wideband (radio) band of frequencies. The receiver correlates the received signals to retrieve the original information signal. Originally there were two motivations: either to resist enemy efforts to jam the communications (anti-jam, or AJ), or to hide the fact that communication was even taking place, sometimes called low probability of intercept (LPI).

Frequency- hopping spread spectrum (FHSS), direct-sequence spread spectrum (DSSS), time-hopping spread spectrum (THSS), chirp spread spectrum (CSS), and combinations of these techniques are forms of spread spectrum. The first two of these techniques employ pseudorandom number sequences—created using pseudorandom number generators—to determine and control the spreading pattern of the signal across the allocated bandwidth. Wireless standard IEEE 802.11 uses either FHSS or DSSS in its radio interface.

NETWORK WAN CONNECTIONNS

- ✓ A wide area network (WAN) is a telecommunications network that extends over a large geographic area for the primary purpose of computer networking. Wide area networks are often established with leased telecommunication circuits.
- ✓ Businesses, as well as schools and government entities, use wide area networks to relay data to staff, students, clients, buyers and suppliers from various locations across the world. In essence, this mode of telecommunication allows a business to effectively carry out its daily function regardless of location.

The Internet may be considered a WAN.

Remote communication Protocol

- ✓ Serial Line Internet Protocol(SLIP_
- ✓ Point to Point PPP Overview and Role In TCP/IP

The TCP/IP protocol suite was generally designed to provide implementation of the networking stack from the network layer (layer three) and above. The core protocols of TCP/IP operate at layers three and four of the OSI model, corresponding to the Internet layer and Host-to-Host Transport layer of the TCP/IP architectural model. Other support protocols are defined at these two layers, and many application protocols run there too, as well as at the upper layers of the protocol stack.

Remote Access Services

A remote access service (RAS) is any combination of hardware and software to enable the remote access tools or information that typically reside on a network of IT devices. A remote access service connects a client to a host computer, known as a remote access server.[1] The most common approach to this service is remote control of a computer by using another device which needs internet or any other network connection.
Here are the connection steps:

1. User dials into a PC at the office.

2. Then the office PC logs into a file server where the needed

information is stored.

3. The remote PC takes control of the office PC's monitor and keyboard, allowing the remote user to view and manipulate information, execute commands, and exchange files

Ethernet is a way of connecting computers together in a local area network or LAN. It has been the most widely used method of linking computers together in LANs since the 1990s. The basic idea of its design is that multiple computers have access to it and can send data at any time. This is comparatively easy to engineer.

All cable types:

- ✓ Ethernet Specifications
- ✓ Different cable types

There are different Ethernet standards. Today, Ethernet cables look like thick telephone cables. They connect to boxes called hubs or switches. Each cable runs from a computer's network interface card (NIC) to such a box. This cable is called 10BaseT or 100BaseT, or 1000BaseT Cable.

Types of Ethernet:

10Base2 and 10Base5: These coaxial cables are like those used in television, but thinner. They are also called "thinnet" or "coax". Each computer has a "T" plugged into it, and cables plug into each side of the "T". Sometimes, instead of a "T", a vampire tap is used. It supports 10MBits per second transfer speed. It was the first to be adopted, and became rare during the 21st century.

10BaseT: Cables look like thick phone cables, but with 8 copper wires instead of 2 or 4, and they go from each computer' to a Hub or a Switch. Supported speed is 10 MBit/second.

10BaseF: Same as 10BaseT, but cables transmit light pulses, instead of electrical signals.

100BaseT: Cables look the same as 10BaseT, but can run at up to 100 MBits per second

1000BaseT: Cables look the same as 10BaseT, but can run at up to

1GBit (1000MBit) per second.

There are several types of Ethernet frames:

Ethernet II frame, or Ethernet Version 2,[f] or DIX frame is the most common type in use today, as it is often used directly by the Internet Protocol.

- ✓ Novell raw IEEE 802.3 non-standard variation frame
- ✓ IEEE 802.2 Logical Link Control (LLC) frame
- ✓ IEEE 802.2 Subnetwork Access Protocol (SNAP) frame

Types of Ethernet frames

Routing is the process of selecting a path for traffic in a network or between or across multiple networks. Broadly, routing is performed in many types of networks, including circuit-switched networks, such as the public switched telephone network (PSTN), and computer networks, such as the Internet.

In packet switching networks, routing is the higher-level decision making that directs network packets from their source toward their destination through intermediate network nodes by specific packet forwarding mechanisms. Packet forwarding is the transit of network packets from one network interface to another. Intermediate nodes are typically network hardware devices such as routers, gateways, firewalls, or switches. General-purpose computers also forward packets and perform routing, although they have no specially optimized hardware for the task.

The routing process usually directs forwarding on the basis of routing tables. Routing tables maintain a record of the routes to various network destinations. Routing tables may be specified by an administrator, learned by observing network traffic or built with the assistance of routing protocols.

Network Routing

Simple Networking Runting and Routers

Network Routing, in a narrower sense of the term, often refers to IP routing and is contrasted with bridging. IP routing assumes that network addresses are structured and that similar addresses imply proximity within the network. Structured addresses allow a single routing table entry to represent the route to a group of devices. In large networks, structured addressing (routing, in the narrow sense) outperforms unstructured addressing (bridging). Routing has become the dominant form of addressing on the Internet. Bridging is still widely used within local area networks.

A router[a] is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. Data sent through the internet, such as a web page or email, is in the form of data packets. A packet is typically forwarded from one router to another router through the networks that constitute an internetwork (e.g. the Internet) until it reaches its destination node.

A router is connected to two or more data lines from different IP networks. When a data packet comes in on one of the lines, the router reads the network address information in the packet header to determine the ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey.

The most familiar type of IP routers are home and small office routers that simply forward IP packets between the home computers and the Internet. More sophisticated routers, such as enterprise routers, connect large business or ISP networks up to the powerful core routers that forward data at high speed along the optical fiber lines of the Internet backbone.

Operation

When multiple routers are used in interconnected networks, the routers can exchange information about destination addresses using a routing protocol. Each router builds up a

routing table, a list of routes, between two computer systems on the interconnected networks.
A router has two types of network element components organized onto separate processing planes:

Control plane: A router maintains a routing table that lists which route should be used to forward a data packet, and through which physical interface connection. It does this using internal pre-configured directives, called static routes, or by learning routes dynamically using a routing protocol. Static and dynamic routes are stored in the routing table. The control-plane logic then strips non-essential directives from the table and builds a forwarding information base (FIB) to be used by the forwarding plane.
Forwarding plane: The router forwards data packets between incoming and outgoing interface connections. It forwards them to the correct network type using information that the packet header contains matched to entries in the FIB supplied by the control plane.

Applications

A typical home or small office DSL router showing the telephone socket (left, white) to connect it to the internet using ADSL, and Ethernet jacks (right, yellow) to connect it to home computers and printers.
A router may have interfaces for different types of physical layer connections, such as copper cables, fiber optic, or wireless transmission. It can also support different network layer

transmission standards. Each network interface is used to enable data packets to be forwarded from one transmission system to another. Routers may also be used to connect two or more logical groups of computer devices known as subnets, each with a different network prefix.

Routers may provide connectivity within enterprises, between enterprises and the Internet, or between internet service providers' (ISPs') networks. The largest routers (such as the Cisco CRS-1 or Juniper PTX) interconnect the various ISPs, or may be used in large enterprise networks.Smaller routers usually provide connectivity for typical home and office networks.

All sizes of routers may be found inside enterprises. The most powerful routers are usually found in ISPs, academic and research facilities. Large businesses may also need more powerful routers to cope with ever-increasing demands of intranet data traffic. A hierarchical internetworking model for interconnecting routers in large networks is in common use.

Access, core and distribution

A screenshot of the LuCI web interface used by OpenWrt. This page configures Dynamic DNS.
Access routers, including small office/home office (SOHO) models, are located at home and customer sites such as branch offices that do not need hierarchical routing of their own. Typically, they are optimized for low cost. Some SOHO routers are capable of running alternative free Linux-based firmware like Tomato, OpenWrt or DD-WRT failed verification

Distribution routers aggregate traffic from multiple access routers. Distribution routers are often responsible for enforcing quality of service across a wide area network (WAN), so they may have considerable memory installed, multiple WAN interface connections, and substantial onboard data processing routines. They may also provide connectivity to groups of file servers or other external networks.[citation needed]

In enterprises, a core router may provide a collapsed backbone interconnecting the distribution tier routers from multiple buildings of a campus, or large enterprise locations. They tend to be optimized for high bandwidth, but lack some of the features of edge routers.[failed verification]

Security

External networks must be carefully considered as part of the overall security strategy of the local network. A router may include a firewall, VPN handling, and other security functions, or these may be handled by separate devices. Routers also commonly perform network address translation which restricts connections initiated from external connections but is not recognized as a security feature by all experts.[10] Some experts argue that open source routers are more secure and reliable than closed source routers because open-source routers allow mistakes to be quickly found and corrected.

Routing different networks

Routers are also often distinguished on the basis of the network in which they operate. A router in a local area network (LAN) of a single organisation is called an interior router. A router that is operated in the Internet backbone is

described as exterior router. While a router that connects a LAN with the Internet or a wide area network (WAN) is called a border router, or gateway router.
Internet connectivity and internal use

Routers intended for ISP and major enterprise connectivity usually exchange routing information using the Border Gateway Protocol (BGP). RFC 4098 defines the types of BGP routers according to their functions:

Edge router (also called a provider edge router): Placed at the edge of an ISP network. The router uses Exterior Border Gateway Protocol (EBGP) to routers at other ISPs or large enterprise autonomous systems.

Subscriber edge router (also called a customer edge router): Located at the edge of the subscriber's network, it also uses EBGP to its provider's autonomous system. It is typically used in an (enterprise) organization.

Inter-provider border router: A BGP router for interconnecting ISPs that maintains BGP sessions with other BGP routers in ISP Autonomous Systems.

Core router: Resides within an Autonomous System as a back bone to carry traffic between edge routers.

Within an ISP: In the ISP's autonomous system, a router uses internal BGP to communicate with other ISP edge routers, other intranet core routers, or the ISP's intranet provider border routers.

Internet backbone: The Internet no longer has a clearly identifiable backbone, unlike its predecessor networks. See default-free zone (DFZ). The major ISPs' system routers make up what could be considered to be the current Internet backbone core.[15] ISPs operate all four types of the BGP routers described here. An ISP core router is used to interconnect its edge and border routers. Core routers may also have specialized functions in virtual private networks based on a combination of BGP and Multi-Protocol Label Switching protocols.
Port forwarding: Routers are also used for port forwarding between private Internet-connected servers.

Voice, data, fax, and video processing routers: Commonly referred to as access servers or gateways, these devices are used to route and process voice, data, video and fax traffic on the Internet. Since 2005, most long-distance phone calls have been processed as IP traffic (VOIP) through a voice gateway. Use of access server type routers expanded with the advent of the Internet, first with dial-up access and another resurgence with voice phone service.

Larger networks commonly use multilayer switches, with layer-3 devices being used to simply interconnect multiple subnets within the same security zone, and higher-layer switches when filtering, translation, load balancing or other higher-level functions are required, especially between zones.

Addressing Scheme in the Internet

An addressing scheme is clearly a requirement for communications in a computer network. With an addressing scheme, packets are forwarded from one location to another. Each of the three layers, 2, 3, and 4, of the TCP/IP protocol stack model produces a header, as indicated in Figure 1.12. In this figure, host 1 communicates with host 2 through a network of seven nodes, R1 through R7, and a payload of data encapsulated in a frame by the link layer header, the network layer header, and the transport layer header is carried over a link. Within any of these three headers, each source or destination is assigned an address as identification for the corresponding protocol layer. The three types of addresses are summarized as follows.

Link layer (layer 2) address. A 6-byte (48-bit) field called Media Access Control (MAC) address that is represented by a 6-field hexadecimal number, such as 89-A1-33-2B-C3-84, in which each field is two bytes long. Every input or output of a networking device has an interface to its connected link, and every interface has a unique MAC address. A MAC address is known only locally at the link level. Normally, it is safe to assume that no two interfaces share the same MAC address. A link layer header contains both MAC addresses of a source interface and a destination interface.

Network layer (layer 3) address. A 4-byte (32-bit) field called Internet Protocol (IP) address that is represented by a 4-field dot-separated number, such as 192.2.32.83, in which each field is one byte long. Every entity in a network must have an IP address in order to be identified in a communication. An IP address can be known globally at the network level. A network layer header contains both IP addresses of a source node and a destination node, Transport layer (layer 4) address. A 2-byte (16-bit) field called port number that is represented by a 16-bit number, such as 4,892. The port numbers identify the two end hosts' ports in a communication. Any host can be running several network applications at a time and thus each application needs to be identified by another host communicating to a targeted application. For example, source host 1 in Figure 1.12 requires a port number for communication to uniquely identify an application process running on the destination host 2. A transport layer header contains the port numbers of a source host and a destination host, as seen in the figure. Note that a transport-layer "port" is a logical port and not an actual or a physical one, and it serves as the end-point application identification in a host.

The details of the link layer header, including the MAC addresses and all other of the header's fields are described in Chapter 4. The details of the network layer header fields, including the IP addresses and all other of the header's fields are presented in Chapter 5. Finally, the details of the transport layer header, including the port numbers and all other of the header's fields are explained in Chapter 8. In the meanwhile, some of the basic IP addressing schemes are presented in the next section, as understanding IP addressing will help us better understand the upcoming networking concepts.

IP Addressing Scheme

The IP header has 32 bits assigned for addressing a desired device on the network. An IP address is a unique identifier used to locate a device on the IP network. To make the system scalable, the address structure is subdivided into the network ID and the host ID. The network ID identifies the network the device belongs to; the host ID identifies the device. This implies that all devices belonging to the same network have a single network ID. Based on the bit positioning assigned to the network ID and the host ID, the IP address is further subdivided into classes A, B, C, D (multicast), and E (reserved)

Consider the lengths of corresponding fields for each class.

Class A starts with 0 followed by 7 bits of network ID and 24 bits of host ID.

Class B starts with 10 followed by 14 bits of network ID and 16 bits of host ID.

Class C starts with 110 followed by 21 bits of network ID and 8 bits of host ID.

Class D starts with 1110 followed by 28 bits. Class D is used only for multicast addressing by which a group of hosts form a multicast group and each group requires a multicast address is entirely dedicated to multicast techniques and routing.

Class E starts with 1111 followed by 28 bits. Class E is reserved for network experiments only.

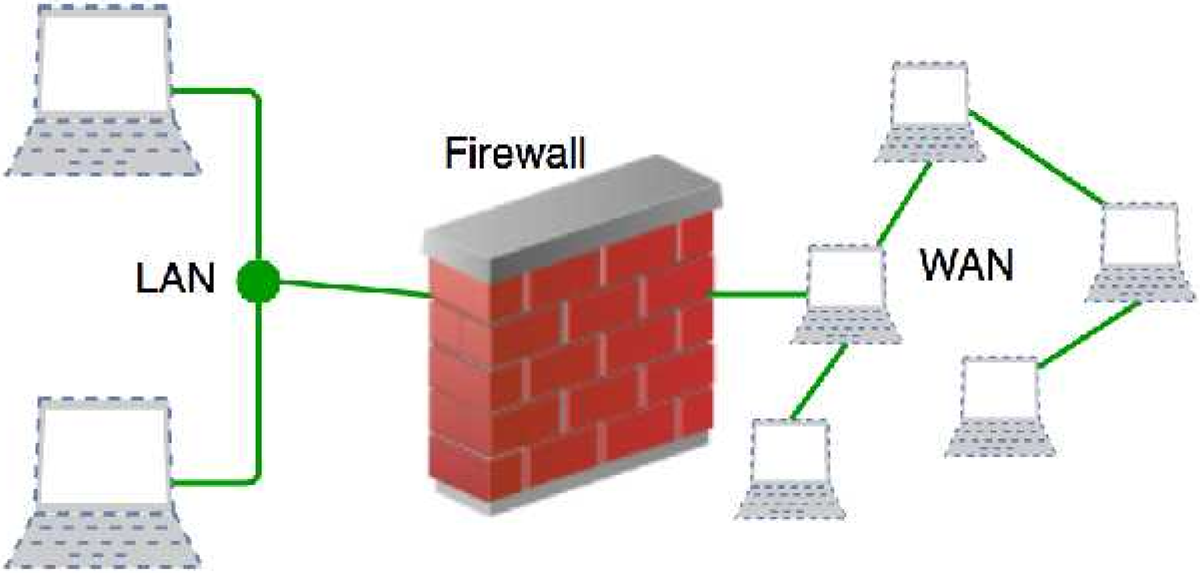
A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

Accept : allow the traffic

Reject : block the traffic but reply with an “unreachable error”

Drop : block the traffic with no reply

A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.



- ✓ The five types of firewall are:
- ✓ Packet filtering firewall
- ✓ Circuit-level gateway
- ✓ Stateful inspection firewall

- ✓ Application-level gateway (aka proxy firewall)
- ✓ Next-generation firewall (NGFW)
- ✓ Packet filtering firewall

Packet filtering firewalls operate inline at junction points where devices such as routers and switches do their work. However, these firewalls don't route packets, but rather they compare each packet received to a set of established criteria -- such as the allowed IP addresses, packet type, port number and other aspects of the packet protocol headers. Packets that are flagged as troublesome are, generally speaking, unceremoniously dropped -- that is, they are not forwarded and, thus, cease to exist.

Circuit-level gateway

Using another relatively quick way to identify malicious content, circuit-level gateways monitor TCP handshakes and other network protocol session initiation messages across the network as they are established between the local and remote hosts to determine whether the session being initiated is legitimate -- whether the remote system is considered trusted. They don't inspect the packets themselves, however.

Statefull inspection firewall

State-aware devices, on the other hand, not only examine each packet, but also keep track of whether or not that packet is part of an established TCP or other network session. This offers more security than either packet filtering or circuit monitoring alone but exacts a greater toll on network performance.

A further variant of stateful inspection is the multilayer inspection firewall, which considers the flow of transactions in process across multiple protocol layers of the seven-layer Open Systems Interconnection (OSI) model.

Application-level gateway

This kind of device -- technically a proxy and sometimes referred to as a proxy firewall -- combines some of the attributes of packet filtering firewalls with those of circuit-level gateways. They filter packets not only according to the service for which they are intended -- as specified by the destination port -- but also by certain other characteristics, such as the HTTP request string.
While gateways that filter at the application layer provide considerable data security, they can dramatically affect network performance.

The Domain Name System (DNS) is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols. By providing a worldwide, distributed directory service, the Domain Name System has been an essential component of the functionality of the Internet since 1985.

The Domain Name System delegates the responsibility of assigning domain names and mapping those names to Internet resources by designating authoritative name servers for each domain. Network administrators may delegate authority over sub-domains of their allocated name space to other name servers. This mechanism provides distributed and fault-tolerant service and was designed to avoid a single large central database.

The Domain Name System also specifies the technical functionality of the database service that is at its core. It defines the DNS protocol, a detailed specification of the data structures and data communication exchanges used in the DNS, as part of the Internet Protocol Suite.

The Internet maintains two principal namespaces, the domain name hierarchy

- ✓ and the Internet Protocol (IP) address spaces.
- ✓ The Domain Name System maintains the domain name hierarchy
- ✓ and provides translation services between it and the address
- ✓ spaces. Internet name servers and a communication protocol implement the Domain Name System.

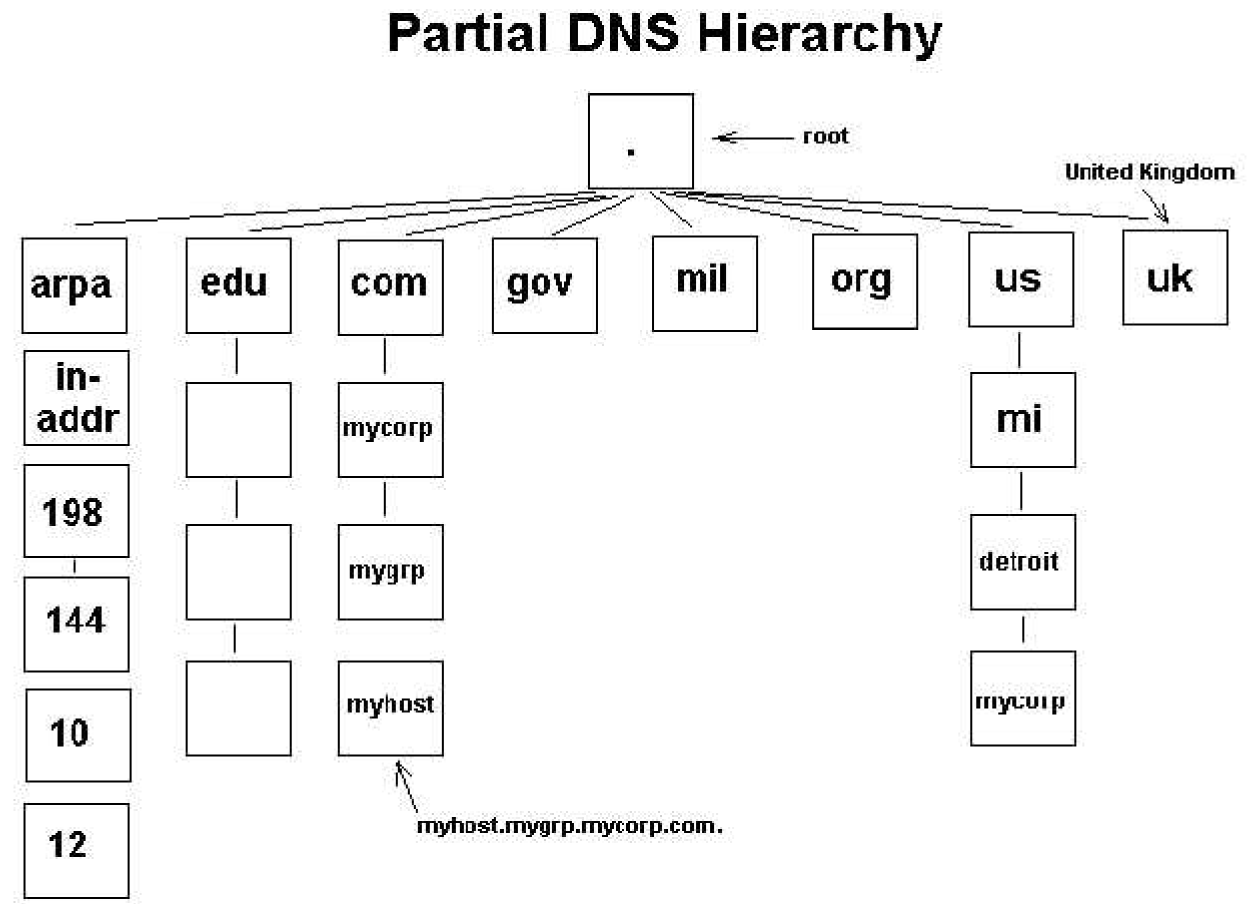
- ✓ A DNS name server is a server that stores the DNS records for a domain; a DNS name server responds with answers to queries against its database.

The most common types of records stored in the DNS database are for

Start of Authority (SOA),

- ✓ IP addresses (A and AAAA), SMTP mail exchangers (MX), name servers (NS), pointers for reverse DNS lookups (PTR), and domain name aliases (CNAME). Although not intended to be a general purpose database, DNS has been expanded over time to store records for other types of data for either automatic lookups, such as DNSSEC records, or for human queries such as

- ✓ Responsible person (RP) records. As a general purpose database, the DNS has also been used in combating unsolicited email (spam) by storing a real-time blackhole list (RBL). The DNS database is traditionally stored in a structured text file, the zone file, but other database systems are common.



- ✓ Broadcasting in computer network is a group communication, where a sender sends data to receivers simultaneously. This is an all − to − all communication model where each sending device transmits data to all other devices in the network domain.

The ways of operation of broadcasting may be

- ✓ A high level operation in a program, like broadcasting in

Message Passing Interface.

✓ A low level networking operation, like broadcasting on Ethernet.

In computer networking, multicast is group communication

✓ where data transmission is addressed to a group of destination computers simultaneously. Multicast can be one-to-many or many-to-many distribution.

✓ Multicast should not be confused with physical layer point-to-multipoint communication.

Group communication may either be application layer multicast or network assisted multicast, where the latter makes it possible for the source to efficiently send to the group in a single transmission. Copies are automatically created in other network elements, such as routers, switches and cellular network base stations, but only to network segments that currently contain members of the group. Network assisted multicast may be implemented at the data link layer using one-to-many addressing and switching such as Ethernet multicast addressing

, Asynchronous Transfer Mode (ATM), point-to-multipoint virtual circuits (P2MP)[3] or Infiniband multicast. Network assisted multicast may also be implemented at the Internet layer using IP multicast. In IP multicast the implementation of the multicast concept occurs at the IP routing level, where routers create optimal distribution paths for datagrams sent to a multicast destination address.

Multicast IP Address to MAC address mapping

Multicast IP address live in the 224.0.0.0 – 239.255.255.255 range but what about MAC addresses and Ethernet frames? What do we do on layer 2 to make multicast work? Let me show you an example of a MAC address:

This means that we have to map multiple Multicast IP addresses to the same Multicast MAC address. We don’t have enough MAC addresses to give each multicast IP address its own MAC address.

We miss 5 bits of mapping information: 25 = 32. This means we will map 32 multicast IP addresses to 1 multicast MAC address. Here’s an example:

- 224.1.1.1
- 224.129.1.1
- 225.1.1.1
- …
- …
- …
- 238.1.1.1
- 238.129.1.1
- 239.1.1.1

The multicast IP addresses above all map to the same multicast MAC address (01-00-5E-01-01-01). This can cause some problems in our networks. For example, a host that listens to the 239.1.1.1 multicast IP address will configure its network card to listen to MAC address 01-00-5E-01-01-01. If someone else is streaming to the 224.1.1.1 multicast IP address it will also end up at our host because the MAC address is the same. The host will have to look at the IP address of the received frame to see if it’s for 239.1.1.1 and discard frames that are meant for 224.1.1.1.

Now the big question remains…what multicast IP addresses map to which multicast MAC address and how do we calculate this? You can use a calculator of course but if you are studying for a Cisco exam you don’t have this luxury. Let’s take a look at how to do this!

First we’ll figure out which multicast MAC address maps to which 32 multicast IP addresses. You can use the following table to calculate between decimal, hexadecimal and binary:

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

We will take the following multicast MAC address and calculate what 32 multicast IP addresses map to it:

01:00:5e:0b:01:02

First we have to translate this MAC address from hexadecimal to binary:

0	1	0	0	5	e	0	b	0	1	0	2
0000	0001	0000	0000	0101	1110	0000	1011	0000	0001	0000	0010

Above you can see how I translated the hexadecimal address into binary, this is the full MAC address:

0000 0001   0000 0000   0101 1110   0000 1011   0000 0001   0000 0010

Now we will take the lowest 23 bits of this MAC address:

0000 0001   0000 0000   0101 1110   0000 1011
    0000 0001   0000 0010

The bits that I highlighted in red are the lowest 23 bits of the MAC address.

Now we will take the class D multicast IP address range in binary:

1110 0000   0000 0000
    0000 0000   0000 0000

The digits in blue (1110) are the class D IP address in binary (224 in decimal). The green digits are the 5 bits that we lose because we have to map a 28 bit unique multicast IP address to a 23 bit multicast MAC address. We will take the blue and green digits and put the red digits behind them:

1110 0000   0000 1011   0000 0001   0000 0010

Let’s convert this binary address into a decimal IP address:

224   11   1   2
1110 0000   0000 1011   0000 0001   0000 0010

So the complete multicast IP address is 224.11.1.2. Now we can play with the green digits to see what other multicast IP addresses map to the same MAC address:

Binary Multicast IP Address	Decimal Multicast IP Address
1110 0000 0000 1011 0000 0001 0000 0010	224.11.1.2
1110 0001 0000 1011 0000 0001 0000 0010	225.11.1.2
1110 0010 0000 1011 0000 0001 0000 0010	226.11.1.2
1110 0011 0000 1011 0000 0001 0000 0010	227.11.1.2
1110 0100 0000 1011 0000 0001 0000 0010	228.11.1.2
1110 0101 0000 1011 0000 0001 0000 0010	229.11.1.2
1110 0110 0000 1011 0000 0001 0000 0010	230.11.1.2
1110 0111 0000 1011 0000 0001 0000 0010	231.11.1.2
1110 1000 0000 1011 0000 0001 0000 0010	232.11.1.2
1110 1001 0000 1011 0000 0001 0000 0010	233.11.1.2

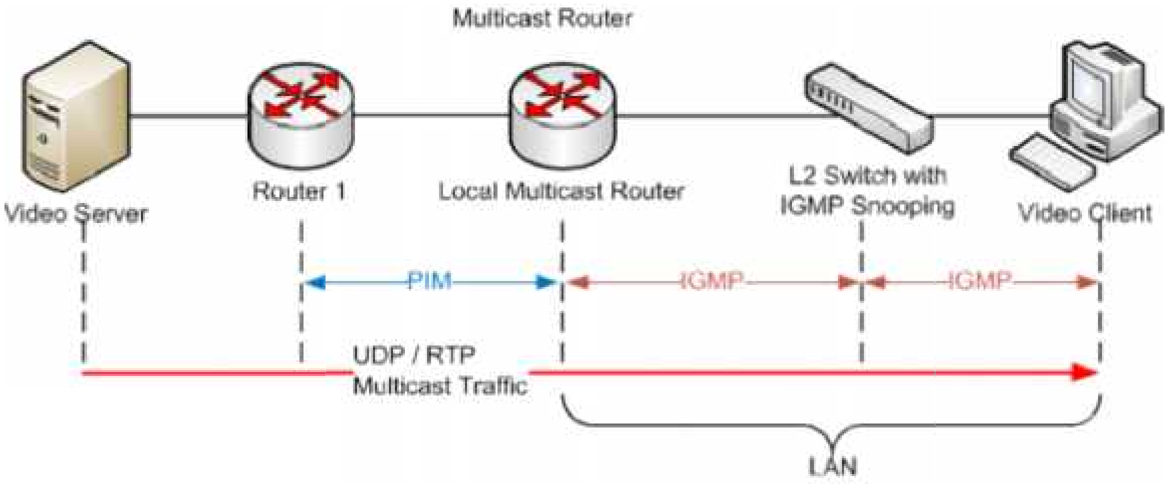
1110 1010 0000 1011 0000 0001 0000 0010	234.11.1.2
1110 1011 0000 1011 0000 0001 0000 0010	235.11.1.2
1110 1100 0000 1011 0000 0001 0000 0010	236.11.1.2
1110 1101 0000 1011 0000 0001 0000 0010	237.11.1.2
1110 1110 0000 1011 0000 0001 0000 0010	238.11.1.2
1110 1111 0000 1011 0000 0001 0000 0010	239.11.1.2
1110 0000 1000 1011 0000 0001 0000 0010	224.139.1.2
1110 0001 1000 1011 0000 0001 0000 0010	225.139.1.2
1110 0010 1000 1011 0000 0001 0000 0010	226.139.1.2
1110 0011 1000 1011 0000 0001 0000 0010	227.139.1.2
1110 0100 1000 1011 0000 0001 0000 0010	228.139.1.2
1110 0101 1000 1011 0000 0001 0000 0010	229.139.1.2
1110 0110 1000 1011 0000 0001 0000 0010	230.139.1.2
1110 0111 1000 1011 0000 0001 0000 0010	231.139.1.2
1110 1000 1000 1011 0000 0001 0000 0010	232.139.1.2
1110 1001 1000 1011 0000 0001 0000 0010	233.139.1.2
1110 1010 1000 1011 0000 0001 0000 0010	234.139.1.2
1110 1011 1000 1011 0000 0001 0000 0010	235.139.1.2
1110 1100 1000 1011 0000 0001 0000 0010	236.139.1.2
1110 1101 1000 1011 0000 0001 0000 0010	237.139.1.2
1110 1110 1000 1011 0000 0001 0000 0010	238.139.1.2
1110 1111 1000 1011 0000 0001 0000 0010	239.139.1.2

The Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships. IGMP is an integral part of IP multicast and allows the network to direct multicast transmissions only to hosts that have requested them.

IGMP can be used for one-to-many networking applications such as online streaming video and gaming, and allows more efficient use of resources when supporting these types of applications.

IGMP is used on IPv4 networks. Multicast management on IPv6 networks is handled by Multicast Listener Discovery (MLD) which is a part of ICMPv6 in contrast to IGMP's bare IP encapsulation.

A network designed to deliver a multicast service using IGMP might use this basic architecture:



IGMP operates between a host and a local multicast router. Switches featuring IGMP snooping derive useful information by observing these IGMP transactions. Protocol Independent Multicast (PIM) is then used between the local and remote multicast routers, to direct multicast traffic from hosts sending multicasts to hosts that have registered through IGMP to receive them.

IGMP operates on the network layer, just the same as other network management protocols like ICMP.[1]
The IGMP protocol is implemented on a particular host and within a router. A host requests membership to a group

through its local router while a router listens for these requests and periodically sends out subscription queries. A single router per subnet is elected to perform this querying function. Some multilayer switches include an IGMP querier capability to allow their IGMP snooping features to work in the absence of an IP multicast capability in the larger network.
IGMP is vulnerable to some attacks,[2][3][4][5] and firewalls commonly allow the user to disable it if not needed.

There are three versions of IGMP.[6] IGMPv1 is defined by RFC 1112, IGMPv2 is defined by RFC 2236 and IGMPv3 was initially defined by RFC 3376 and has been updated by RFC 4604 which defines both IGMPv3 and MLDv2. IGMPv2 improves IGMPv1 by adding the ability for a host to signal desire to leave a multicast group. IGMPv3 improves IGMPv2 by supporting source-specific multicast[7] and introduces membership report aggregation.

These versions are backwards compatible. A router supporting IGMPv3 can support clients running IGMPv1, IGMPv2 and IGMPv3. IGMPv1 uses a query-response model. Queries are sent to 224.0.0.1. Membership reports are sent to the group's multicast address. IGMPv2 accelerates the process of leaving a group and adjusts other timeouts. Leave-group messages are sent to 224.0.0.2. A group-specific query is introduced. Group-specific queries are sent to the group's multicast address. A means for routers to select an IGMP querier for the network is introduced. IGMPv3 introduces source-specific multicast capability. Membership reports are sent to 224.0.0.22.

Dynamic Routing

- ✓ Dynamic routing, also called adaptive routing,

- ✓ is a process where a router can forward data via a different route or given destination based on the current conditions of the communication circuits within a system.

- ✓ The term is most commonly associated with data networking to describe the capability of a network to 'route around' damage, such as loss of a node or a connection between nodes, so long as other path choices are available

- ✓ Dynamic routing allows as many routes as possible to remain valid in response to the change.

Systems that do not implement dynamic routing are described as using static routing, where routes through a network are described by fixed paths. A change, such as the loss of a node, or loss of a connection between nodes, is not compensated for. This means that anything that wishes to take an affected path will either have to wait for the failure to be repaired before restarting its journey, or will have to fail to reach its destination and give up the journey.

- ✓ Route discovery methods

✓ Route discovery is a process that occurs when

✓ The source node does not have a route to the requested destination.

✓ A route fails. This happens when the source node uses up its network retries without receiving an ACK.

✓ Route discovery begins by the source node broadcasting a route request (RREQ).

✓ We call any router that receives the RREQ and is not the ultimate destination, an intermediate node.

✓ Intermediate nodes may either drop or forward a RREQ, depending on whether the new RREQ has a better route back to the source node. If so, the node saves, updates and broadcasts the RREQ.

✓ When the ultimate destination receives the RREQ, it unicasts a route reply (RREP) back to the source node along the path of the RREQ. It does this regardless of route quality and regardless of how many times it has seen an RREQ before.

✓ This allows the source node to receive multiple route replies. The source node selects the route with the best round trip route quality, which it uses for the queued packet and for subsequent packets with the same destination address.

- ✓ The Simple Mail Transfer Protocol (SMTP) is a communication protocol for electronic mail transmission. As an Internet standard, SMTP was first defined in 1982 by RFC 821, and updated in 2008 by RFC 5321 to Extended SMTP additions, which is the protocol variety in widespread use today. Mail servers and other message transfer agents use SMTP to send and receive mail messages. SMTP servers commonly use the Transmission Control Protocol on port number 25.

- ✓ User-level email clients typically use SMTP only for sending messages to a mail server for relaying, and typically submit outgoing email to the mail server on port 587 or 465 as per RFC 8314. For retrieving messages, IMAP and POP3 are standard, but proprietary servers also often implement proprietary protocols, e.g., Exchange ActiveSync.

- ✓ The Internet Message Access Protocol (IMAP) is a mail protocol used for accessing email on a remote web server from a local client. IMAP and POP3 are the two most commonly used Internet mail protocols for retrieving emails. Both protocols are supported by all modern email clients and web servers.

- ✓ While the POP3 protocol assumes that your email is being accessed only from one application, IMAP allows simultaneous access by multiple clients. This is why IMAP is more suitable for you if you’re going to access your email from different locations or if your messages are managed by multiple users.

By default, the IMAP protocol works on two ports:

- ✓ Port 143 – this is the default IMAP non-encrypted port
- ✓ Port 993 – this is the port you need to use if you want to connect using IMAP securely.

- ✓ Simple Mail Transfer Protocol (SMTP) is the standard protocol for sending emails across the Internet.
- ✓ By default, the SMTP protocol works on three ports

- ✓ Port 25 – this is the default SMTP non-encrypted port
- ✓ Port 2525 – this port is opened on all SiteGround servers in case port 25 is filtered (by your ISP for example) and you want to send non-encrypted emails with SMTP;
- ✓ Port 465 – this is the port used if you want to send messages using SMTP securely.

n computing, a directory service or name service maps the names of network resources to their respective network addresses. It is a shared information infrastructure for locating, managing, administering and organizing everyday items and network resources, which can include volumes, folders, files, printers, users, groups, devices, telephone numbers and other objects. A directory service is a critical component of a network operating system. A directory server or name server is a server which provides such a service. Each resource on the network is considered an object by the directory server. Information about a particular resource is stored as a collection of attributes associated with that resource or object.

Directory service

A directory service defines a namespace for the network. The namespace is used to assign a name (unique identifier) to each of the objects. Directories typically have a set of rules determining how network resources are named and identified, which usually includes a requirement that the identifiers be unique and unambiguous. When using a directory service, a user does not have to remember the physical address of a network resource; providing a name locates the resource. Some directory services include access control provisions, limiting the availability of directory information to authorized users.
SMTP commands

- HELO. It's the first SMTP command: is starts the conversation identifying the sender server and is generally followed by its domain name.

- EHLO. An alternative command to start the conversation, underlying that the server is using the Extended SMTP protocol.

- MAIL FROM. ...
- RCPT TO. ...

- SIZE. ...
- DATA. ...
- VRFY. ...
- TURN.

Simple Network Management Protocol (SNMP) is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. Devices that typically support SNMP include cable modems, routers, switches, servers, workstations, printers, and more.

SNMP is widely used in network management for network monitoring. SNMP exposes management data in the form of variables on the managed systems organized in a management information base (MIB) which describe the system status and configuration. These variables can then be remotely queried (and, in some circumstances, manipulated) by managing applications.

Three significant versions of SNMP have been developed and deployed. SNMPv1 is the original version of the protocol. More recent versions, SNMPv2c and SNMPv3, feature improvements in performance, flexibility and security.

SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

Network Drivers

Information technology generally refers to all forms of technology used for the creation, storage, exchange and use of data, conversation and all forms of communication across multiple media. As computer technologies evolve and continually improve, companies are motivated by the need for a system that is adapted to their needs and objectives. They are considered businessmen in an information-based economy.

Network applications

- the types of messages exchanged, e.g., request messages and response messages;

- the syntax of the various message types, i.e., the fields in the message and how the fields are delineated;

- the semantics of the fields, i.e., the meaning of the information in the fields;

- rules for determining when and how a process sends messages and responds to messages.

Models for network applications:

A network application protocol typically has two parts or "sides", a client side and a server side. The client side in one end system communicates with the server side in another end system. For example, a Web browser implements the client side of HTTP and a Web server implements the server side of HTTP. In another example, e-mail, the sending mail server implements the client side of SMTP and the receiving mail server implements the server side of SMTP.

Email systems

The email system is the network of computers handling electronic mail (email) on the Internet. This system includes user machines running programs that compose, send, retrieve, and view messages, and agent machines that are part of the mail handling system. Like other complex systems, the email system is best explained by looking separately at different perspectives, applying the principle of separation of concerns.

There are two coequal ways of looking at email systems - the administrative perspective (who does what), and the process perspective (how it flows). The administrative perspective presented in this article is the simplest. It can be understood without any technical background. The process perspective presented in "Email processes and protocols" provides more technical depth, and should be understood by anyone involved in the design or operation of email systems.

In the process perspective, the mail handling system can be modeled as a sequence of relay processes, each temporarily storing the message, performing some specialized function, and passing it on to the next relay using the SMTP protocol.[1] You can tell how many relays handled a message by looking at the lines labeled "Received:" in the message header. There should be one for each relay. Relays are not our focus in this article, however. We can ignore them in higher-level models, just as routers and physical links can be ignored in discussing relays.

In the administrative perspective, the principal entities are actors, their roles, and their relationships. Who are the actors in a typical email system? What are their roles and responsibilities in handling the mail? What are their relationships with each other? What are their motivations? How can we build better security systems? A basic understanding of the administrative perspective should help answer these questions. This article provides that understanding

Message Handling System (MHS)

The message handling system (MHS) is a concept developed by ITU-T that is intended to lead to the interconnectivity of all different types of message conveying systems (facsimile, electronic mail, voicemail, telex etc). MHS set out a simple model of basic interconnection between systems. This chapter explains the model, unravels the jargon and describes the initiatives that will result.

Any method you use to schedule your time and the time of your staff could be called a scheduling system. Today, however, an efficient scheduling system almost always refers to a software program or an app. After all, scribbling staff hours on a few sticky notes in the break room could hardly be called a system at all.

Before choosing a scheduling system, take some time to consider what features your company needs and what it may need in the future. A graphic designer working from home won't use the same features that a busy restaurant uses. An office manager keeping track of conference rooms won't have the same needs that a landscaper or a plumber has. Two ways to compare scheduling software are to look at those that are static compared to those that are dynamic.

Static Scheduling Software: Best for businesses with fixed, rotating shifts, like manufacturers, call centers and hotels. It can also be used for professionals who need a good

Appointment-scheduling software. Workers can be easily rotated from one shift to another based on the frequency you need, such as weekly or biweekly.

* Dynamic Scheduling Software: Best for businesses with shifts that constantly change, like home cleaning services, restaurants and HVAC maintenance services. Staff can be scheduled for different shifts at different locations without overlaps or conflicts, and they can be quickly notified of any changes.

Server-Based vs. Cloud Solutions

Like most software solutions, you have the choice of buying software and putting it on your server or buying a cloud-based solution for a monthly fee. Cloud-based scheduling solutions are usually easy to set up, and for a small business, they are

more cost effective since you're usually paying a few dollars per month for each employee you have.
Larger companies with their own servers often buy server-based scheduling software and install it on location.

The cost of purchasing the software, installing it, backing it up and maintaining it can be prohibitive for smaller companies. However, if you have a large number of employees, it may be more cost effective than paying a monthly fee for a cloud-based solution.

A wide area network (WAN) is a telecommunications network that extends over a large geographic area for the primary purpose of computer networking. Wide area networks are often established with leased telecommunication circuits.

Businesses, as well as schools and government entities, use wide area networks to relay data to staff, students, clients, buyers and suppliers from various locations across the world. In essence, this mode of telecommunication allows a business to effectively carry out its daily function regardless of location. The Internet may be considered a WAN.

Many technologies are available for wide area network links. Examples include circuit-switched telephone lines, radio wave transmission, and optical fiber. New developments in technologies have successively increased transmission rates. In ca. 1960, a 110 bit/s (bits per second) line was normal on the edge of the WAN, while core links of 56 kbit/s to 64 kbit/s were considered fast.[citation needed] As of 2014, households are connected to the Internet with dial-up, asymmetric digital subscriber line (ADSL), cable, WiMAX, 4G[6] or fiber. The speeds that people can currently use range from 28.8 kbit/s through a 28K modem over a telephone connection to speeds as high as 100 Gbit/s using 100 Gigabit Ethernet.[citation needed

Wide area connection technologies:

The following communication and networking technologies have been used to implement WANs.[citation needed

Asynchronous Transfer Mode

Cable modem

Dial-up internet

Digital subscriber line

Fiber-optic communication

Frame Relay

ISDN

Leased line

SD-WAN

Synchronous optical networking

X.25

UNIT V

Internet Basis:

Networking

A computer network is a group of computers that use a set of common communication protocols over digital interconnections for the purpose of sharing resources located on or provided by the network nodes. The interconnections between nodes are formed from a broad spectrum of telecommunication network technologies, based on physically wired, optical, and wireless radio-frequency methods that may be arranged in a variety of network topologies.

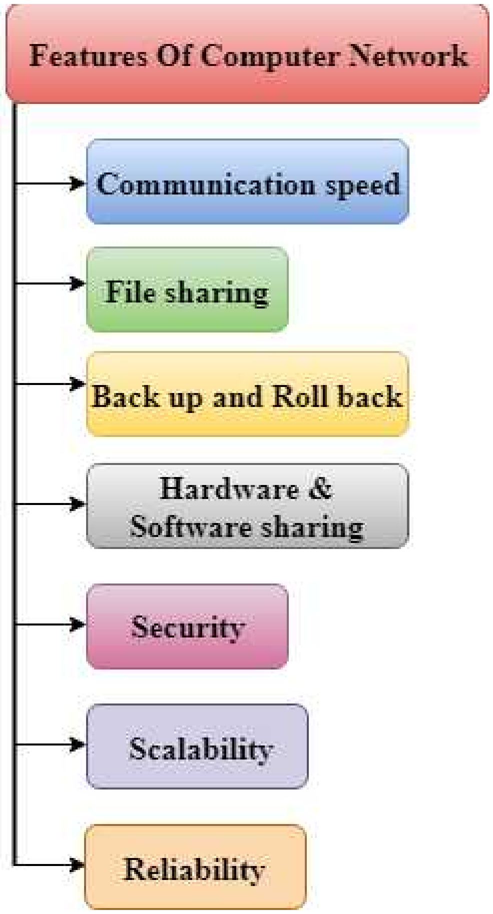
The nodes of a computer network may be classified by many means as personal computers, servers, networking hardware, or general-purpose hosts. They are identified by hostnames and network addresses. Hostnames serve as memorable labels for the nodes, rarely changed after initial assignment. Network addresses serve for locating and identifying the nodes by communication protocols such as the Internet Protocol.

Computer networks may be classified by many criteria, for example, the transmission medium used to carry signals, bandwidth, communications protocols to organize network traffic, the network size, the topology, traffic control mechanism, and organizational intent.

Internet:

He Internet (or internet) is the global system of interconnected computer networks that uses the Internet protocol suite (TCP/IP) to communicate between networks and devices. It is a network of networks that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies. The Internet carries a vast range of information resources and services, such as the inter-linked hypertext documents and applications of the World Wide Web (WWW), electronic mail, telephony, and file sharing.

Features Of Computer network



A list Of Computer network features is given below.

- Communication speed

o File sharing

- Back up and Roll back is easy
- Software and Hardware sharing

- Security

- Scalability

- Reliability

Hardware Requirement :

• To connect the Internet, any one of the following is mandatory.

• Modem is used to connect Internet thorugh Telephoneconnection.

• NIC- Network Interface Card(wired/ wireless) facility is the most important hardware required to connect Internet. For example, the Laptop can be connected Internet through the wired/wireless.

• Dongle is used to connect the Internet using cellular network

• Wi-Fi router or Hotspot is used to connect the Internet using wireless network

Software Requirement

• The operating system should support TCP (Transfer Control Protocol) / IP (Internet Protocol), SMTP (Simple Mail Transfer Protocol), FTP (File Transfer Protocol), HTTP (Hyper Text Transfer Protocol) and HTTPS (Hyper Text Transfer Protocol Secured) protocols.

• Browsers and other Internet clients access to the web applications such as Outlook, Gmail, Whatsapp, Facebook, Twitter and etc.

Factors affecting the speed and quality of internet connection

Data transfer technology. ...

Network centralizer. ...

Other devices and users. ...

Network technology and terminal device. ...

Other users. ...

Location. ...

Several operators provide a free speed test for their customers. ...

You can test the speed of your connection, for example, by using the following services:

The Internet Protocol (IP) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet.

IP has the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packet headers. For this purpose, IP defines packet structures that encapsulate the data to be delivered. It also defines addressing methods that are used to label the datagram with source and destination information.

Historically, IP was the connectionless datagram service in the original Transmission Control Program introduced by Vint Cerf and Bob Kahn in 1974, which was complemented by a connection-oriented service that became the basis for the Transmission Control Protocol (TCP). The Internet protocol suite is therefore often referred to as TCP/IP.

The first major version of IP, Internet Protocol Version 4 (IPv4), is the dominant protocol of the Internet. Its successor is Internet Protocol Version 6 (IPv6), which has been in increasing deployment on the public Internet since c. 2006.

Communication protocol:

A communication protocol is a system of rules that allow two or more entities of a communications system to transmit information via any kind of variation of a physical quantity. The protocol defines the rules, syntax, semantics and synchronization of communication and possible error recovery methods. Protocols may be implemented by hardware, software, or a combination of both.

Communicating systems use well-defined formats for exchanging various messages. Each message has an exact meaning intended to elicit a response from a range of possible responses pre-determined for that particular situation. The specified behavior is typically independent of how it is to be implemented. Communication protocols have to be agreed upon by the parties involved.

- To reach an agreement, a protocol may be developed into a technical standard. A programming language describes the same for computations, so there is a close analogy between protocols and programming languages: protocols are to communication what programming languages are to computations

- An alternate formulation states that protocols are to communication what algorithms are to computation,

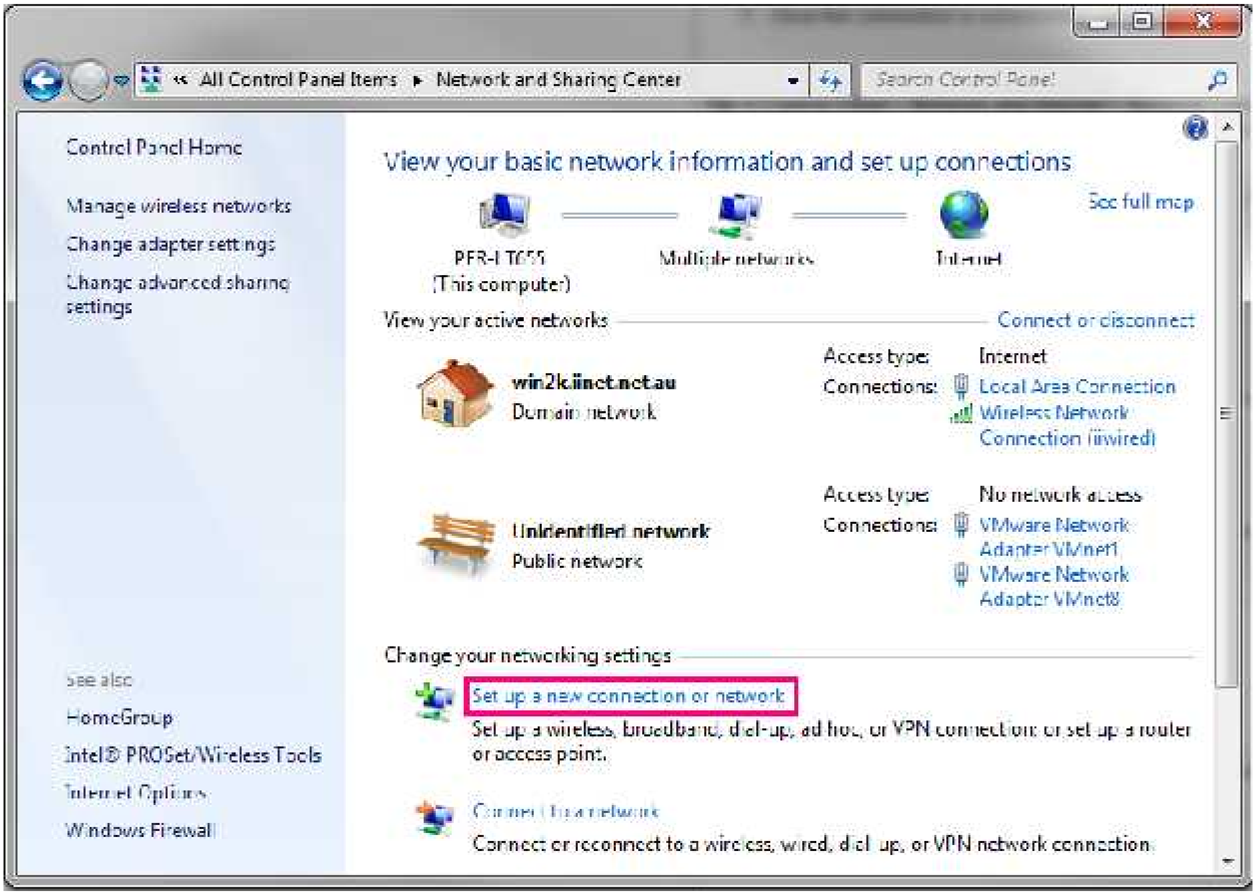
- Multiple protocols often describe different aspects of a single communication. A group of protocols designed to work together is known as a protocol suite; when implemented in software they are a protocol stack.

- Internet communication protocols are published by the

- Internet Engineering Task Force (IETF).

- The IEEE (Institute of Electrical and Electronics Engineers) handles wired and wireless networking and the International Organization for Standardization (ISO) handles other types. The ITU-T handles telecommunication protocols and formats for the

- public switched telephone network (PSTN). As the PSTN and Internet converge, the standards are also being driven towards convergence.



View your basic network information and set up connections

View your active networks

win2k.iinet.net.au
Domain network

Access type: Internet
Connections: Local Area Connection
Wireless Network Connection (iinwired)

Unidentified network
Public network

Access type: No network access
Connections: VMware Network Adapter VMnet1
VMware Network Adapter VMnet8

Change your networking settings

Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.