Important pages to refer … Page wise

Page 1 to 4 - Explain Bandwidth, Data Terminal Equipment & Data Circuit terminating equipment

Page 4 to 5 - . Amplitude Modulation Vs Frequency Modulation

Page 9 to 9 - Wired and wireless

Page 10 to 12 – ATM

Page 12 to 15 – VSAT

Page 15 to 19 – OSI model and difference btw OSI and TCP

Page 20 to 31 - Network and Network architecture

Page 32 to 33 – Synchronization

Page 33 to 34 – Error and Detection

Page 41 to 42 – Network Protocols

Page 49 to 52 – Network Interface card

Page 52 to 54 - protocols – LAN and WAN

Page 57 – Protocols – LAN and WAN

Page 61 to 63 – CSMA

Page 63 to 64 – Address resolution

Page 71 to 77 - Client server and Net centric and web centric

Page 82 to 84 – Packet and circuit switching

Page 84 to 86 – Frame relay

Page 118 to 119 – Analog vs Digital Signal
Page 123 to 124 – DHCP

Page 127 to 128 – VOIP

Page 131 – DNS

Question Bank with Solution – Networking - by MJ

1. Effective communication between two devices for data (Text including numbers, Images, Audio or Voice, Video) communication are (a)Delivery, (b)Accuracy and (c)Timeliness. Explain this statement with suitable example.

---

2. Explain the difference between Analog and Digital signals with respect to any five parameters such as signal, wave patterns, technology, transmission, bandwidth, memory, power, impedance, etc.

Ans – Refer to Page 118

---

3. What is a network interface card and how is it different from wireless network interface cards? Identify at least five suitable applications of these cards in real time environment.

Ans – Q.16 – Page 51

---

4. What is network? Explain component of a Computer network in a company.

Ans – Page 54

---

5. Define the basic component of Data Communication? Differentiate Between Analog and Digital Communication.

Ans : http://greatinformer.blogspot.in/2012/11/what-is-data-communication-components.html for data communication
http://datacombd.blogspot.in/2011/05/what-is-data-communication-what-are.html - One can check this

The primary difference between analog and digital communication is the difference in the concept behind "continuous time" and "discrete time". Continuous time signals have a value at every point in time, no matter how thin you slice between two time points. Discrete time is based upon samples. You sample the signal at some point in time and that sample represents the signal between the two time points of your sampling period. A fellow named Nyquist showed that if the period between two samples were small enough (at least 2x the highest frequency), there is no loss of information.

Therefore, analog communications is based upon continuous time signals. For example, your voice modulates a microphone and the continuous time electrical signal from that microphone is sent to the destination, sometimes by modulating a carrier signal.

A digital communications signal is based upon discrete time where the signal is first sampled and converted to a digital signal. That discrete signal is then transmitted to the destination. Digital communications is generally preferred for so many different reasons that it becomes almost impossible to identify them all in a Quora post. I'll list some and let others add to the list.

- digitized continuous time signals and inherently digital signals can be easily mixed to transmitted to their destination
- digital communications tends to be more robust in a noisy environment
- multiplexing is ridiculously simple with digital signals, making multiplex costs much lower
- digital signals can be packetized and sent over packet networks, which makes them more reliable
- different types of signals can be combined using digital communications, such as video, audio, data, sensor, etc.
- digital communications can be stored

.in analog communication, the signal can take up voltage level corresponding to any real number,
2. hence once it is corrupted with noise it is difficult to recover the correct value.
3. repeaters in analog communication are amplifiers which also amplifies noise thereby degrading the quality of the system.
4.since the voltage can take infinite levels, it would need infinite bits to represent data.
5.analog data is continuous time continuous amplitude data.

1.in digital communication signal can take up only one among two voltage levels corresponding to 1 and 0.
2. hence even if it is corrupted by channel noise it is possible to recover the original information by using a suitable threshold at the receiver.

3.repeaters in digital communication can be wave regenerators which produce new waveforms after recovering the original information from the received waveform and hence noise does not accumulate through a digital communication link as in analog link.
4.since the voltage can take only finite number of values, it requires finite number of bits for propagation.
5.digital data is discrete time discrete amplitude data. digital communication is more efficient in terms of noise immunity and quality.

---

6. Explain with suitable high level network diagram, the requirements for a new Data Centre for which you are put as the Head of Operations.

Ans – refer http://www.it.northwestern.edu/bin/docs/DesignBestPractices_127434.pdf
(not sure – Pradeep and team will come up soon with a better ans)

---

7. Explain Bandwidth, Data Terminal Equipment & Data Circuit terminating equipment (DCE).

Ans – Q.1 – Page 2

---

8. Differentiate between Synchronous and Asynchronous communication.

Ans - Synchronous

- In synchronous data transfers, the sender and receiver take some time to communicate before they make the exchange. This communication outlines the parameters of the data exchange. This usually involves establishing which end, sender or receiver, will be in control of the transfer. Here, the two parties also ensure they are using the same timing; that is, they know when each burst ends and another begins. They also set parameters for resetting their clocks during the transfer to make sure they don't drift away from the agreed-upon timing.

Asynchronous

- In asynchronous, or "best effort" transfers, sender and receiver do not establish the parameters of the information exchange. Rather, the sender places extra bits of data before and after each burst that indicate when each burst begins and ends. It then sends the information, and it is up to the receiver to determine how to reset its clock to match the timing of the signal. Unlike synchronous transfers, the receiver does not take time to communicate to the sender information about what it received.

---

9. What is network topologies and network architecture? Give two examples of each.

Ans – Q. 9 - Page 20

---

10. State the different type of Network Topologies in detail.

Ans - Q.9 – Page no. 20

---

11. Describe a Storage Area Network with respect to its (i) design, (ii) architecture, (iii) purpose, (iv) Testing approach, (v) management of SAN on day to day basis.

---

12. Explain OSI model in detail. How is it differentiated from TCP Model?

Ans - Q.8 – Page 19

---

13. Describe Network Management.

Ans - Q.10 – Page No. 31

---

14. Explain OSI model with suitable diagram and explain how it is different from the TCP Model.

Ans. – Q. 8 – Pg No. 15

---

15. What are protocols? Name any two protocols not from the same layer and explain its role?

Ans- Q.14 – Page - 41

---

16. What are protocols? Define at least one protocols w.r.t to the OSI model.

Ans- Q.14 – Page – 41

---

17. Differentiate between Wired and Wireless networks. What are the transmission Media used for both networks?

Ans – Q.5 - What are the transmission Media used for both networks? – Refer Page no. 7.

Wired and wireless networks - Refer page no. 9

---

18. Differentiate between Circuit and Packet Switching.

Ans . Refer to Page 82

---

19. Explain Network Addressing. Define the terms – MAC address, Logical IP, Valid IP, Subnet Mask, Gateway

---

20. What is Frame Relay? How it differs from Cell Relay.

Ans . Refer to page 85

---

21. What is VSAT? How does it work

Ans. Refer to page no. 15

---

22. What are DHCP and DNS? How does it work?

Ans - For DHCP – Refer pg. 124
For DNS – refer pg. 131

---

23. Define Protocols. Define protocols used in LAN and WAN.

Ans. Refer to Page 57

---

24. Define CSMA/CD. How does it work? Explain with a flow chart.

Ans – Refer page no. 61 – highlighted area

---

25. How does address resolution happens in a LAN.

Ans – Refer Page no. 64 - Highlighted area

---

26. Describe following architecture with example

a. Client Server

b. Peer to Peer

c. Net Centrica. Client Server

Ans – Refer Q.18 – Page no. 71

---

27. Short note:

a. Amplitude Modulation Vs Frequency Modulation

Ans – Refer Page no. 83

---

b. Resource Sharing

Not found ….

c. Error Detection and Correction.

Ans. Refer to page no. 34

---

d. Packet Switching.

Ans – Refer to Page no. 84

---

e. Cell Relay

Cell relay is a network technology for data transmission that uses small data packets of a fixed size called cells. Cells are the basic units of data, and are widely used in common networks for communication. Just like frames, which are data packets of variable size, cells travel from one computer to another over a network. Asynchronous transfer mode (ATM) is a particularly popular form of cell relay, and is based on cell units.

Cell relay uses data cells of a constant size. Frames are similar data packets, but they differ from cells in that they may vary in size according to the requirement or situation. This technology is not secure because its protocols do not support error handling or data recovery. As such, all sensitive and important transmissions may be delivered faster using fixed-sized cells, which are easier to carry compared to variable-sized frames or packets.

Cell relay is very reliable for delivering sensitive information. Switching devices give the exact route to cells as per the destination address embedded in a cell. One example of cell relay is ATM, a popular form used to transmit a cell with fixed size of 53 bytes.

---

f. Spanning Tree Protocol

Ans. Refer Pg no. 112

---

g. Voice over IP

Ans – Refer page no. 128

---

h. ATM Technology

Ans. Refer to Page no. 12

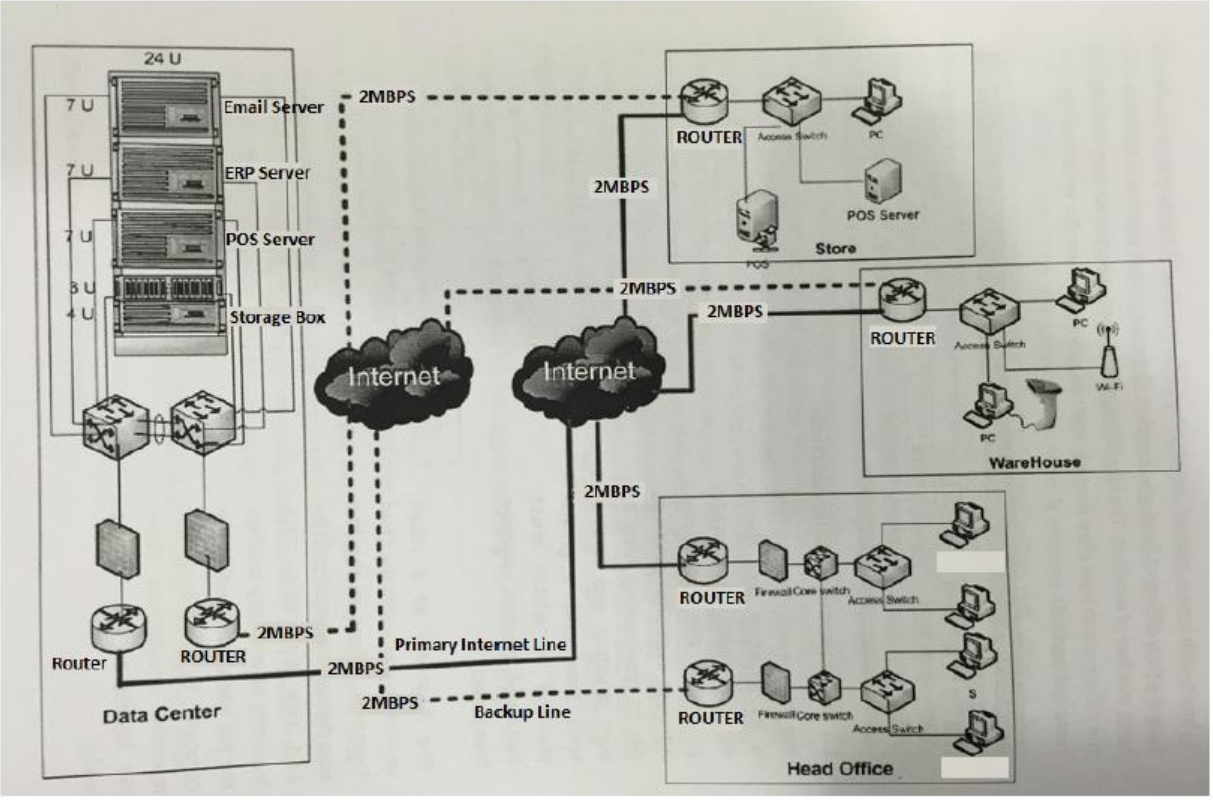
---

i. Synchronization

Ans – Refer pg. no. 32

---

28. A retail store located at one location with single floor catering to digital goods, readymade garments, cosmetics, food & beverages plans to deployment its IT infrastructure requirement at ten locations spread over three cities.
Present 5 top management alerts justifying the IT requirements that will meet their new business objectives.
State your bill of material, comment on network devices, and communication requirements for this change. Explain the top two business benefits that will be met with by the new approach.



Note: The diagram will be same the concept can change..

Ans – Will be covered By Ravi

NETWORK COMMUNICATION

SEM IV

QUESTION PAPER SOLUTIONS

QUESTION PAPERS:

2011, 2010, 2007, 2006, 2004, 2003

Compiled by Venkatesh Sangoram, Rahul Nair, Birju Mehta, Prem Kangya & Abhijeet Dalvi.

1. Explain: Bandwidth, Data Terminal Equipment &Data Circuit terminating equipment (DCE). [2011]

Ans:

Bandwidth-

1) In computer networks, bandwidth is often used as a synonym for data transfer rate - the amount of data that can be carried from one point to another in a given time period (usually a second). This kind of bandwidth is usually expressed in bits (of data) per second (bps). Occasionally, it's expressed as bytes per second (Bps). A modem that works at 57,600 bps has twice the bandwidth of a modem that works at 28,800 bps. In general, a link with a high bandwidth is one that may be able to carry enough information to sustain the succession of images in a video presentation.

It should be remembered that a real communications path usually consists of a succession of links, each with its own bandwidth. If one of these is much slower than the rest, it is said to be a bandwidth bottleneck.

2) In electronic communication, bandwidth is the width of the range (or band) of frequencies that an electronic signal uses on a given transmission medium. In this usage, bandwidth is expressed in terms of the difference between the highest-frequency signal component and the lowest-frequency signal component. Since the frequency of a signal is measured in hertz (the number of cycles of change per second), a given bandwidth is the difference in hertz between the highest frequency the signal uses and the lowest frequency it uses. A typical voice signal has a bandwidth of approximately three kilohertz (3 kHz); an analog television (TV) broadcast video signal has a bandwidth of six megahertz (6 MHz) -- some 2,000 times as wide as the voice signal.

Data Terminal Equipment-

Data Terminal Equipment (DTE) is any equipment that is either a source or destination for digital data. DTE do not generally communicate with each other to do so they need to use DCE to carry out the communication. DTE does not need to know how data is sent or received; the communications details are left to the DCE. A typical example of DTE is a computer.

Other common DTE examples include:

- Printers
- File and application servers
- PCs
- Dumb Terminals
- Routers

Any device that is a source of data transmission over a serial telecommunications link. Typically, data terminal equipment (DTE) can be a computer, a terminal, a router, an access server, or some similar device. The earliest form of DTE was the teletype machine.

Graphic D-9. Data terminal equipment (DTE).

The term "DTE" specifically refers to a device that uses serial transmission such as the transmissions involving the serial port of a computer. Most serial interface devices contain a chip called a universal asynchronous receiver-transmitter (UART) that can translate the synchronous parallel data transmission that occurs within the computer's system bus into an asynchronous serial transmission for communication through the serial port. The UART also performs other functions in a DTE:

- Error detection, to ensure that data arrives at its destination uncorrupted
- Clocking, to ensure that data is sent at the correct rate in order to be received at its destination

To connect a DTE to a telecommunications link, you use data communications equipment (DCE). The DCE provides termination for the telecommunications link and an interface for connecting the DTE to the link. An example of a DCE for connecting a DTE to the local loop Plain Old Telephone Service (POTS) connection is a modem.

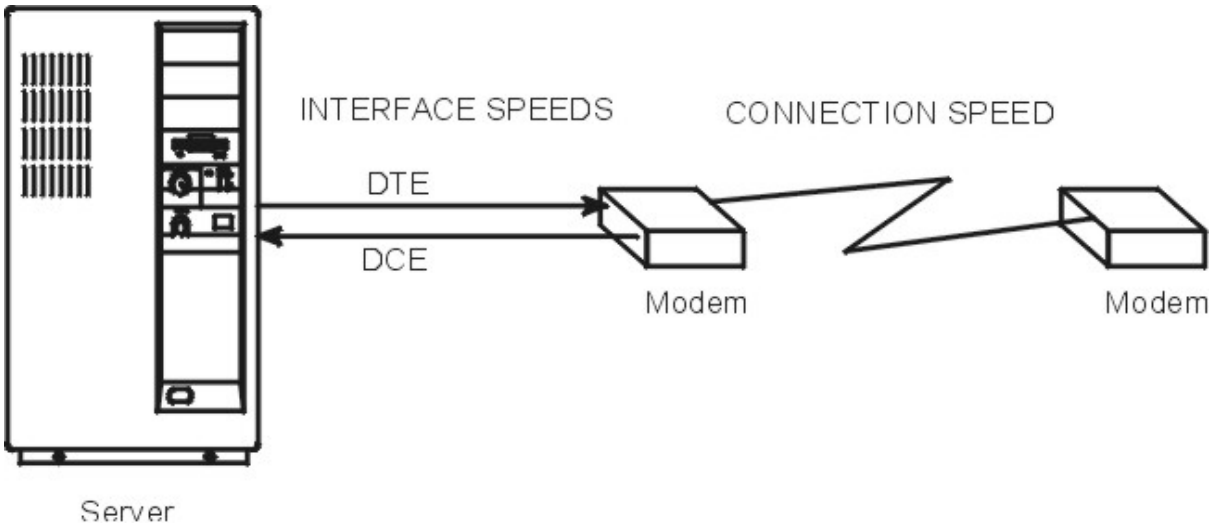
Data Terminating Equipment or Data Circuit-Terminating Equipment speeds-

Data Terminating Equipment (DTE) and Data Communication Equipment (DCE) are used to describe two different hardware groups.

The term DTE is used primarily for those devices that display user information. It also includes any devices that store or generate data for the user. The system units, terminals, and printers all fall into the DTE category.

DCE includes any device which can be used to gain access to a system over telecommunication lines. The most common forms of DCEs are modems and multiplexers.

Figure 1. Modem speed considerations



With serial communication on this operating system involving modems, as pictured in the above illustration, there are three major considerations:

- DTE interface speed (server to modem). This is the speed the server communicates to the modem.

- DCE interface speed (modem to server) sometimes called the "serial port interface speed." This is the speed at which the modem communicates to the server.
- Connection speed (modem to modem). This is the speed at which a modem communicates (or talks) to another modem.

Most modern, high-speed modems allow the DCE interface speed to be different than the connection speed. This allows the DTE speed to be locked at a single baud rate while allowing the connection speed to fluctuate, up or down as needed, for proper communication between modems.

Modern high-speed modems hold the data to be transmitted to the server in a buffer and send it when the system can accept it. They can also hold data to be transmitted to the other modem in a buffer and send it as the remote is able to accept it. This kind of data transmission requires the modem and the server to engage in flow control.

2. ***What is your understanding about following terms with suitable diagram?***
    a. ***Amplitude Modulation, [2011]***
    b. ***Frequency Modulation [2011]***
    c. ***Phase Modulation [2011]***

Ans: 

Amplitude Modulation (AM)

Amplitude Modulation occurs when a voice signal's varying voltage is applied to a carrier frequency. The carrier frequency's amplitude changes in accordance with the modulated voice signal, while the carrier's frequency does not change.

When combined the resultant AM signal consists of the carrier frequency, plus UPPER and LOWER sidebands. This is known as Double Sideband - Amplitude Modulation (DSB-AM), or more commonly referred to as plain AM.

The carrier frequency may be suppressed or transmitted at a relatively low level. This requires that the carrier frequency be generated, or otherwise derived, at the receiving site for demultiplexing. This type of transmission is known as Double Sideband - Suppressed Carrier (DSB-SC).

It is also possible to transmit a SINGLE sideband for a slight sacrifice in low frequency response (it is difficult to suppress the carrier and the unwanted sideband, without some low frequency filtering as well). The advantage is a reduction in analog bandwidth needed to transmit the signal. This type of modulation, known as Single Sideband - Suppressed Carrier (SSB-SC), is ideal for Frequency Division Multiplexing (FDM).

Another type of analog modulation is known as Vestigial Sideband. Vestigial Sideband modulation is a lot like Single Sideband, except that the carrier frequency is preserved and one of the sidebands is eliminated through filtering. Analog bandwidth requirements are a little more than Single Sideband however.

Vestigial Sideband transmission is usually found in television broadcasting. Such broadcast channels require 6 MHz of ANALOG bandwidth, in which an Amplitude Modulated PICTURE carrier is transmitted along with a Frequency Modulated SOUND carrier.

Frequency Modulation (FM)

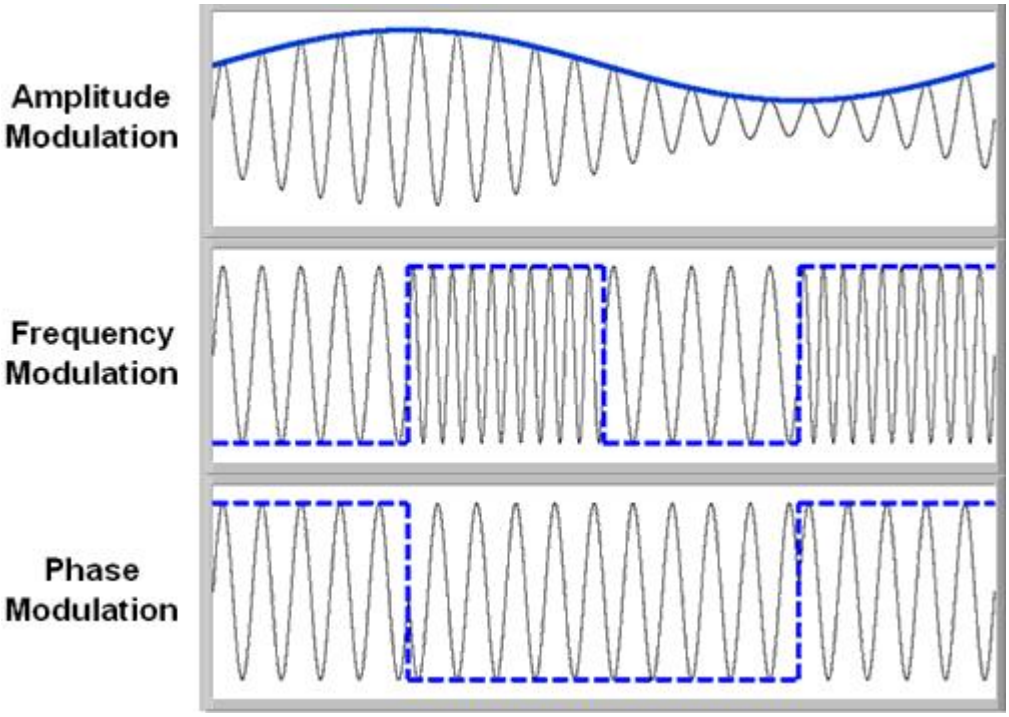
Frequency Modulation occurs when a carrier's CENTER frequency is changed based upon the input signal's amplitude. Unlike Amplitude Modulation, the carrier signal's amplitude is UNCHANGED. This makes FM modulation more immune to noise than AM and improves the overall signal-to-noise ratio of the communications system. Power output is also constant, differing from the varying AM power output.

The amount of analog bandwidth necessary to transmit a FM signal is greater than the amount necessary for AM, a limiting constraint for some systems.

Phase Modulation

Phase Modulation is similar to Frequency Modulation. Instead of the frequency of the carrier wave changing, the PHASE of the carrier changes.

As you might imagine, this type of modulation is easily adaptable to data modulation applications.



3. What is your understanding about the term CODEC and MODEM using suitable example?[2011]

Ans:A codec is a device or computer program capable of encoding or decoding a digital data stream or signal. The word codec is a portmanteau of "compressor-decompressor" or, more commonly, "coder-decoder". A codec (the program) should not be confused with a coding or compression format or standard – a format is a document (the standard), a way of storing data, while a codec is a program (an implementation) which can read or write such files. In practice, however, "codec" is sometimes used loosely to refer to formats.

A codec encodes a data stream or signal for transmission, storage or encryption, or decodes it for playback or editing. Codecs are used in videoconferencing, streaming media and video editing applications. A video camera's analog-to-digital converter (ADC) converts its analog signals into digital signals, which are then passed through a video compressor for digital transmission or storage. A receiving device then runs the signal through a video decompressor, then a digital-to-analog converter (DAC) for analog display. The term codec is also used as a generic name for a video conferencing unit.

An endec (encoder/decoder) is a similar yet different concept mainly used for hardware. In the mid 20th century, a "codec" was hardware that coded analog signals into Pulse-code modulation (PCM) and decoded them back. Late in the century the name came to be applied to a class of software for converting among digital signal formats, and including compander functions.

A modem is a contraction of modulator/demodulator (although they were referred to as "datasets" by telcos) and converts digital data from computers to analog for phone line transmission. On the receiving end the analog is converted back to digital. Codecs do the opposite (convert audio analog to digital and then computer digital sound back to audio).

An audio codec converts analog audio signals into digital signals for transmission or storage. A receiving device then converts the digital signals back to analog using an audio decompressor, for playback. An example of this are the codecs used in the sound cards of personal computers. A video codec accomplishes the same task for video signals.

4. What is Network Address Translation (NAT) and what is its role in a Network? [2011]

Ans:For a computer to communicate with other computers and Web servers on the Internet, it must have an IP address. When IP addressing first came out, everyone thought that there were plenty of addresses to cover any need. With the explosion of the Internet and the increase in home networks and business networks, the number of available IP addresses is simply not enough. The obvious solution is to redesign the address format to allow for more possible addresses. This is being developed (called IPv6), but will take several years to implement because it requires modification of the entire infrastructure of the Internet.

This is where NAT comes to the rescue. Network Address Translation allows a single device, such as a router, to act as an agent between the Internet (or "public network") and a local (or "private") network. This means that only a single, unique IP address is required to represent an entire group of computers.

Network Address Translation (NAT) is the process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network. The main use of NAT is to limit the number of public IP addresses an organization or company must use, for both economy and security purposes.

The most common form of network translation involves a large private network using addresses in a private range (10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, or 192.168.0 0 to 192.168.255.255). The private addressing scheme works well for computers that only have to access resources inside the network, like workstations needing access to file servers and printers. Routers inside the private network can route traffic between private addresses with no trouble. However, to access resources outside the network, like the Internet, these computers have to have a public address in order for responses to their requests to return to them. This is where NAT comes into play.

Internet requests that require Network Address Translation (NAT) are quite complex but happen so rapidly that the end user rarely knows it has occurred. A workstation inside a network makes a request to a computer on the Internet. Routers within the network recognize that the request is not for a resource inside the network, so they send the request to the firewall. The firewall sees the request from the computer with the internal IP. It then makes the same request to the Internet using its own public address, and returns the response from the Internet resource to the computer inside the private network. From the perspective of the resource on the Internet, it is sending information to the address of the firewall. From the perspective of the workstation, it appears that communication is directly with the site on the Internet.

When NAT is used in this way, all users inside the private network access the Internet have the same public IP address when they use the Internet. That means only one public addresses is needed for hundreds or even thousands of users.

5. ***Explain at least three transmission media each for wired and wireless with suitable examples. [2011]***

Ans:**Transmission Media**

Digital data can be transmitted over many different types of media. Selecting atransmission medium is guided by comparing transmission requirements against themedium's characteristics. Four important criteria influence the choice:

1. **Bandwidth.** Bandwidth is the maximum frequency range that can be practicallysupported by a medium. This is usually expressed in kilo Hz (kHz) or mega Hz(MHz). For example, analog transmission of human speech typically requires abandwidth of 4 kHz. Also related, is the notion of **data rate**, which denotes themaximum number of bits per second (bps) that can be transmitted. For example,a data rate of 10 mbps means that 10 million bits of data can be transmitted ineach second. Because of their obvious relationship, the terms bandwidth anddata rate are sometimes used interchangeably. Because of distortion factors,bandwidth and data rate are usually inversely proportional to the communicationdistance.

2. **Cost.** Two types of cost are relevant: (i) the cost of installing the medium,including the medium-specific equipment that may be needed, and (ii) the cost ofrunning and maintaining the medium and its equipment. There is usually a need fortradeoff between cost, bandwidth, and distance.

3. **Reliability.** Some media, by their physical nature, transmit data more reliablythan others. Low reliability translates into a higher number of errors, which needsto be balanced against the potential cost of recovering from the errors (e.g.,retransmission, more complex hardware and software).

4. **Coverage.** The physical characteristics of a medium dictate how long a signalcan travel in it before it is distorted beyond recognition. To cover larger areas,repeaters are needed to restore the signal, and this increases the costs.

Transmission media may be classified into the following categories:

· **Copper Wire**. This is the oldest form of electronic transmission medium. Its usedates back to the development of telegraph in the 1800s and earliest telephonesystems. Early installations used open wires, but these were superseded bytwisted pairs, which consist of a pair of insulated and twisted wires. Twisted pairs are superior because of reduced crosstalk.

They are veryeffective for relatively short distances (a few hundred feet), but can be used forup to a few kilometers. A twisted pair has a bandwidth to distance ratio of about1 MHz per kilometer. The performance of the twisted pair can be substantiallyimproved by adding a metallic shield around the wires. Shielded wires are muchmore resistant to thermal noise and crosstalk effects. Twisted pairs used for longdistance connections (e.g., telephone lines) are usually organized as a muchlarger cable containing numerous twisted pairs.

· **Coaxial Cable**. A coaxial cable consists of four concentric cylinders: an innerconductor, surrounded by an insulating cylinder, surrounded by an outerconductor, surrounded by a final protective cover. This combination is called acoax (see Figure 2.16). Coaxial cables are superior to twisted pairs both interms of bandwidth and communication distance, and can provide bandwidth todistance ratios in order of 10s of MHz per kilometer. Like twisted pairs, multiplecoaxes are usually housed within one cable, which may also contain twistedpairs. Coaxial cables are extensively used in LANs and long distance telephonetrunk lines.

· **Optical Fiber**. An optical fiber consists of two concentric cylinders: an innercore surrounded by a cladding. Both the core and the cladding are made oftransparent plastic or glass material (see Figure 2.16). The core is used forguiding a light beam, whereas the cladding (which has a different refractive index)acts as a reflector to prevent the light from escaping from the core. Becauseoptical fiber uses a light signal instead of electrons, it does not suffer from thevarious noise problems associated with electromagnetic signals. The signal isusually generated by a laser or Light Emitting Diode (LED). Optical fibers canprovide bandwidth to distance ratios in order of 100s of MHz per kilometer.

Like other cables, hundreds of optical fibers are usually housed within one cable.

Crosstalk is the unwanted coupling effect between two or more signal paths, which causes signaldistortion. Current trends promise that they will replace twisted pairresidential loops in the near future.

Wireless Mediums:

· **Radio**. Radio signals have been used for a long time to transmit analoginformation. They are particularly attractive for long distance communication overdifficult terrain or across the oceans, where the cost of installing cables can betoo prohibitive. A minimum radio system consists of a transmitter and a receiver.

It may operate at a variety of frequency bands, ranging from hundreds of Hz tohundreds of giga Hz (GHz). A huge range of transmission bandwidths aretherefore possible. Microwave is by far the most widely used form of radiotransmission. It operates in the GHz range with data rates in order of 100s ofmbps per channel. Telecommunication carriers and TV stations are the primaryusers of microwave transmission.An important form of microwave system is a **satellite** system, which isessentially a microwave system plus a large repeater in the sky (see Figure 2.16).

The signals transmitted by earth stations are received, amplified, andretransmitted to other earth stations by the satellite. Like other microwavesystems, the bandwidth is subdivided into channels of 10s of MHz each,providing data rates in order of 100s of mbps. Because of their high bandwidths,satellites are capable of supporting an enormous number and variety of channels,including TV, telephone, and data. The satellite itself, however, represents amajor investment and typically has a limited lifetime (at most a few decades).

Another increasingly-popular form of radio is **cellular radio**, which iscurrently being used by carriers for providing mobile telephone networks. Theseoperate in the VHF band and subdivide their coverage area into conceptual cells,where each cell represents a limited area which is served by a low-powertransmitter and receiver station. As the mobile user moves from one cell area toanother, its communication is handed over from one station to another.

· **Infra-red**. Infra-red signals are suitable for transmission over relatively shortdistances (the signal is easily reflected by hard objects). The signal is generatedand received using optical transceivers. Infra-red systems represent a cheapalternative to most other methods, because there is no cabling involved and thenecessary equipment is relatively cheap. Data rates similar to those of twistedpairs are easily possible.

However, applications are limited because of distancelimitations (of about one kilometer). One recent use of infra-red has been forinterfacing hand-held and portable computing devices to LANs.

6. ***Describe 'wired' and 'wireless' communication with suitable diagram describing Ethernet, token ring, FDDI, ATM, Bluetooth, Wi-Fi, Wi-Max and VSAT technologies. [2011]***

Wired communication

Wired Communication refers to the transmission of data over a wire-based communication technology. Examples include telephone networks, cable television or internet access, and fiber-optic communication.

Wired networks provide users with plenty of security and the ability to move lots of data very quickly. Wired networks are typically faster than wireless networks, and they can be very affordable. However, the cost of Ethernet cable can add up -- the more computers on your network and the farther apart they are, the more expensive your network will be. In addition, you'll be able to see the cables running from place to place around your home, and wires can greatly limit your mobility. A laptop owner, for example, won't be able to move around easily if his computer is tethered to the wall.

Wireless communication

Wireless telecommunications is the transfer of information between two or more points that are not physically connected.

The easiest, least expensive way to connect the computers in your home is to use a wireless network, which uses radio waves instead of wires. The absence of physical wires makes this kind of network very flexible. For example, you can move a laptop from room to room without fiddling with network cables and without losing your connection. The downside is that wireless connections are generally slower than Ethernet connections and they are less secure unless you take measures to protect your network.

If you want to build a wireless network, you'll need a wireless router. Signals from a wireless router extend about 100 feet (30.5 meters) in all directions, but walls can interrupt the signal. Depending on the size and shape of your home and the range of the router, you may need to purchase a range extender or repeater to get enough coverage. You'll also need a wireless adapter in each computer you plan to connect to the network. You can add printers and other devices to the network as well. Some new models have built-in wireless communication capabilities.

Wireless networking is used to meet many needs. Perhaps the most common use is to connect laptop users who travel from location to location. Another common use is for mobile networks that connect via satellite. A wireless transmission method is a logical choice to network a LAN segment that must frequently change locations. The following situations justify the use of wireless technology:

- To span a distance beyond the capabilities of typical cabling,
- To provide a backup communications link in case of normal network failure,
- To link portable or temporary workstations,
- To overcome situations where normal cabling is difficult or financially impractical, or
- To remotely connect mobile users or networks.

Ethernet (802.3)

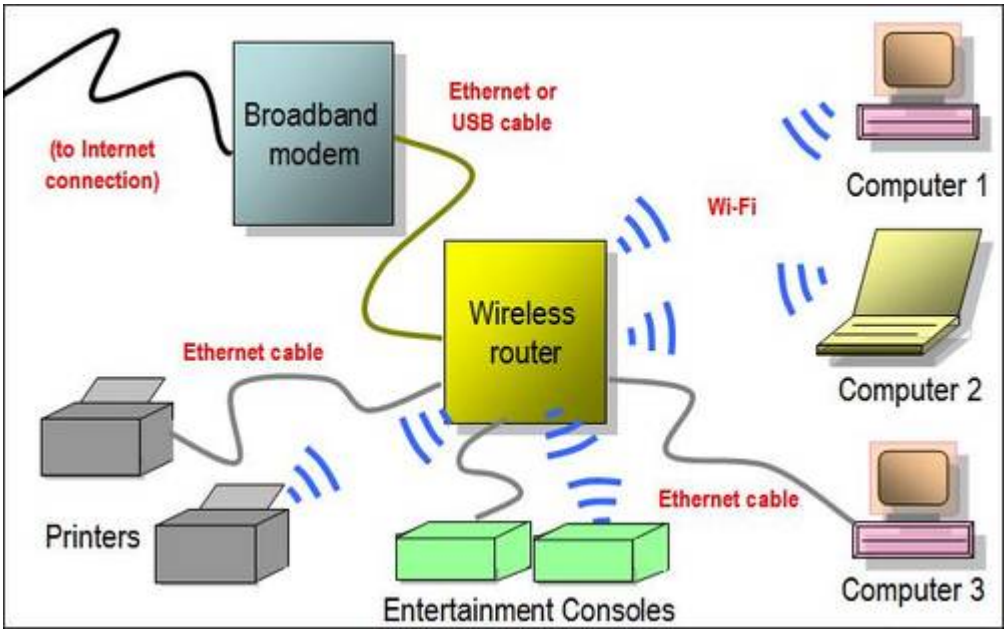
Ethernet is a family of computer networking technologies for local area networks (LANs) commercially introduced in 1980. Standardized in IEEE 802.3, Ethernet has largely replaced competing wired LAN technologies. In the OSI reference system, Ethernet is at the Data Link layer.
Systems communicating over Ethernet divide a stream of data into individual packets called frames. Each frame contains source and destination addresses and error-checking data so that damaged data can be detected and re-transmitted.

The original 10BASE5 Ethernet used coaxial cable as a shared medium. Later the coaxial cables were replaced by twisted pair and fiber optic links in conjunction with hubs or switches. Data rates were periodically increased from the original 10 megabits per second, to 100 gigabits per second. The three data transmission rates achieved with Ethernet are:
10 Mbps - 10BASE-T Ethernet
100MBps - Fast Ethernet
1000 Mbps - Gigabit Ethernet

Token Ring (IEEE 802.5)
This protocol is applicable to a ring topology. Channel access is regulated by a special message, called a token, which is passed around the ring from one station to the next. The state of the ring is encoded in the token (i.e., idle or busy). The station, wishing to transmit, needs to get hold of the idle token first. When a station gets hold of the idle token, it marks it as busy, appends to it the message it wishes to transmit, and sends the whole thing to the next station. The message goes round the ring until it reaches the intended recipient which copies the message and passes it on. When the message returns to the originator, it detaches the message, marks the token as idle and passes it on. To ensure fair access, the token should go round the ring, unused, at least once before it can be used by the same station again.

Bluetooth
Bluetooth wireless technology is a short range radio technology. Bluetooth makes it possible to transmit signals over short distances between telephone, computers and other devices and thereby simplify communication and synchronization between devices. Bluetooth is the name of a protocol for a short range (10 meter) frequency-hopping 2.4 GHz radio link between wireless devices such as a mobile phone and a PC. The idea is to make connections between different electronic items much easier and simpler, and without a lot of operator intervention. Bluetooth was launched in 1998 as a joint effort between Ericsson, IBM, Nokia, Intel and Toshiba. Instead of one-way transmission, Bluetooth allows multiple devices from multiple manufacturers to speak the same wireless language without conflicts.
Bluetooth operates over short distances of around 30 feet or less and it requires a clear line of sight between the devices. Bluetooth operates over the unlicensed 2.4Gz radio spectrum which allows Bluetooth-enabled equipment to operate anywhere in the world. Bluetooth uses more than 71 different frequencies which allow a signal to hop around from one frequency to another to avoid conflicts with other devices.

Wi-Fi and Wi-Max - read these from Prof. Max D'Costa answer bank of ITC of third Semester. Not able to copy them.
Diagram of a wireless network



Fiber Distributed Data Interface (FDDI)

Fiber Distributed Data Interface (FDDI) provides a 100 Mbit/s optical standard for data transmission in a local area network that can extend in range up to 200 kilometers (120 mi). Although FDDI logical topology is a ring-based token network, it does not use the IEEE 802.5 token ring protocol as its basis; instead, its protocol is derived from the IEEE 802.4 token bus timed token protocol. In addition to covering large geographical areas, FDDI local area networks can support thousands of users. As a standard underlying medium it uses optical fibre, although it can use copper cable, in which case it may be referred to as CDDI (Copper Distributed Data Interface).

FDDI was considered an attractive campus backbone technology in the early to mid 1990s since existing Ethernet networks only offered 10 Mbps transfer speeds and Token Ring networks only offered 4 Mbps or 16 Mbps speeds. Thus, it was the preferred choice of that era for a high-speed backbone, but FDDI has since been effectively obsolesced by fast Ethernet which offered the same 100 Mbps speeds, but at a much lower cost and, since 1998, by Gigabit Ethernet due to its speed, and even lower cost, and ubiquity.

A FDDI network contains two rings, one as a secondary backup in case the primary ring fails. The primary ring offers up to 100 Mbps capacity. When a network has no requirement for the secondary ring to do backup, it can also carry data, extending capacity to 200 Mbps.

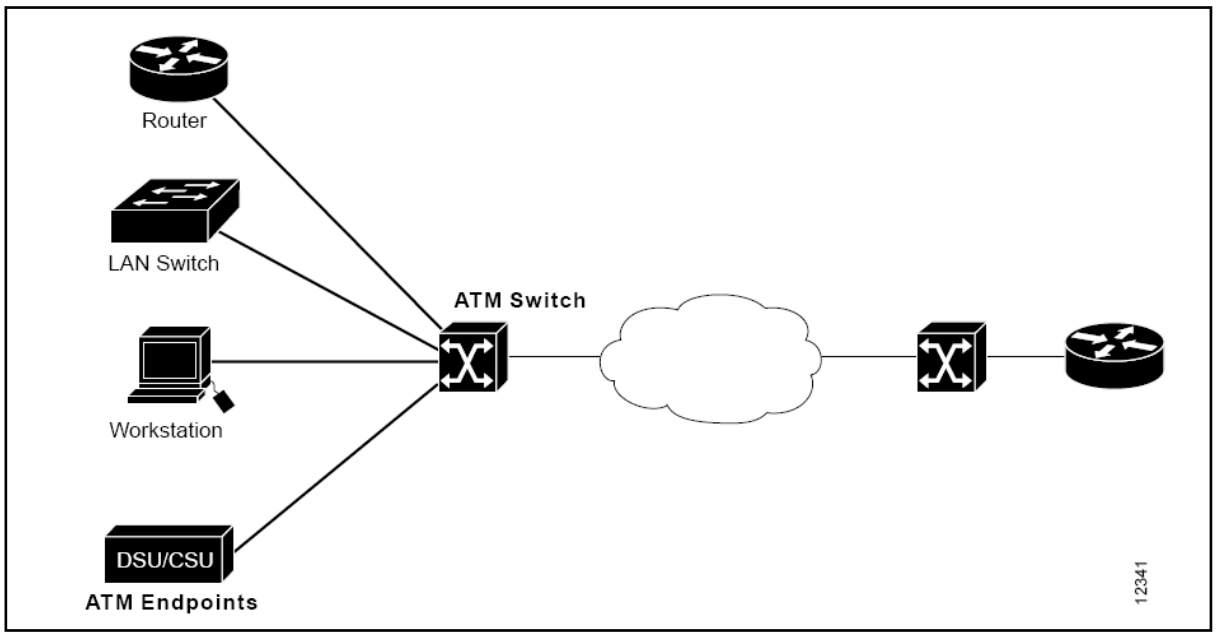
Asynchronous Transfer Mode (ATM)

Asynchronous Transfer Mode (ATM) is an International Telecommunication Union–Telecommunication standard for cell relay wherein information for multiple service types, such as voice, video, or data, is conveyed in small, fixed-size cells. ATM networks are connection oriented.

ATM is a cell-switching and multiplexing technology that combines the benefits of circuit switching (guaranteed capacity and constant transmission delay) with those of packet switching (flexibility and efficiency for intermittent traffic). It provides scalable bandwidth from a few Mbps to many Gbps. Because of its asynchronous nature, ATM is more efficient than synchronous technologies, such as time-division multiplexing (TDM). With TDM, each user is assigned to a time slot, and no other station can send in that time slot. If a station has a lot of data to send, it can send only when its time slot comes up, even if all other time slots are empty. If, however, a station has nothing to transmit when its time slot comes up, the

time slot is sent empty and is wasted. Because ATM is asynchronous, time slots are available on demand with information identifying the source of the transmission contained in the header of each ATM cell.

An ATM network is made up of an ATM switch and ATMend points. An ATM switch is responsible for cell transit through an ATM network. The job of an ATM switch is well defined: it accepts the incoming cell from an ATM endpoint or another ATM switch. It then reads and updates the cell-header information and quickly switches the cell to an output interface toward its destination. An ATM endpoint (or end system) contains an ATM network interface adapter. Examples of ATM endpoints are workstations, routers, digital service units (DSUs), LAN switches, and video coder-decoders (CODECs).



Very Small Aperture Terminal (VSAT)

Refer the answer below

7. VSAT

a. Write a note on VSAT covering its Characteristics, technologies, advantages, disadvantages [2011]

b. Various Applications for which VSAT can be used. [2011,2010]

c. What does VSAT mean to business? How does it work? [2010]

d. What are its alternatives and explain briefly for which VSAT technology can be used?[2010]

Ans:

VSAT systems provide dedicated, reliable, cost effective and private communications links for the individual and corporate users, with the provision of total system capabilities to support high bandwidth secure data, voice and video communication.

What is a VSAT system?

The use of VSAT systems is growing throughout the world as a way of establishing private satellite communications networks for large organisations that have several widely dispersed locations, or providing higher bandwidth for the individual. Depending on bandwidth requirement (data speed

and/or communications channels), VSAT systems can be relatively small (1 - 2 metre antenna) and easily installed. By linking VSAT terminals to larger hub stations (or land earth stations), a network can be established inexpensively, although in this type of configuration, VSATs can communicate only via the hub and not from remote terminal to remote terminal. This configuration is called STAR configuration. VSAT networks can readily be configured so that the hub can broadcast data to all the VSAT terminals at higher rates than they can communicate to the hub.

How does a VSAT work?

A VSAT network has three components:

- A central hub (also called a master earth station)
- The satellite
- A virtually unlimited number of VSAT earth stations in various locations - across a country or continent

Outbound information (from the hub to the VSATs) is sent up to the communications satellite's transponder, which receives it, amplifies it and beams it back to earth for reception by the remote VSATs. The VSATs at the remote locations send information inbound (from the VSATs to the hub) via the same satellite transponder to the hub station.

This arrangement, where all network communication passes through the network's hub processor, is called a "star" configuration, with the hub station at the centre of the star. One major advantage of this configuration is that there is virtually no limit on the number of remote VSATs that can be connected the hub. "Mesh" configurations also allow for direct communication between VSATs.

For satellites to gain a foothold in the delivery of advanced broadband services, seamless interconnectivity with terrestrial networks is imperative. For best results, the network should be designed to exploit the unique virtue of satellite in geostationary orbit, namely that it can be a shared resource available, as needed, to many users spread over a very large proportion of the Earth's surface. This is the concept of bandwidth-on-demand. In an ideal network, each terminal communicates with all others (full-mesh connectivity), but utilises satellite capacity only on an as-needed basis. Such an architecture can be implemented if the terminals operate in a Time Division Multiple Access (TDMA) mode (transmit in bursts) and are capable of doing this at a variety of different frequencies (FDMA and TDMA).

DAMA System (Demand Assigned Multiple Access)

A DAMA system is typically a mesh network that allows direct connection between any two nodes in the network, sharing the bandwidth of a satellite transponder space which can be allocated to each remote terminal as required. DAMA supports full mesh, point-to-point or point-to-multipoint communications - any user can connect directly to any other user anywhere within the network - and the most superior systems achieve this with TDMA. The result is economical and flexible bandwidth sharing with any mix of voice, fax, video and data traffic. The key point is that DAMA optimises the use of satellite capacity by allocating satellite resources to each active node upon demand. By using a DAMA system, satellite resources can support a very much larger number of users.

Advantages of VSAT technology

As companies compete for an increasingly savvy customer looking for value (quality and service), information technology and communications networks are becoming tools to achieve business goals. Today's networks must support the need to improve customer service, increase per site revenues and reduce costs (all driving net income growth) - in the most cost-effective manner possible. Further, network managers want virtual 100% availability. They need to easily expand the network when they acquire, move or add new sites to the operations. In addition, they require network flexibility - ease of migration from existing legacy systems as well as addition of new network applications as their companies offer additional services to its customers

Businesses and organizations give many reasons for using VSAT networks over terrestrial alternatives. Among them are:

- Cost-effective
- Flexibility
- Accessibility
- Availability
- Reliability - 99.9% for Data; 99.5%+ for Voice
- Versatility
- Transmission quality
- High network performance
- Fast transmissions
- Control
- Ability to handle large amounts of data
- Single vendor solution for both equipment and bandwidth
- Broadcast capability
- Ability to handle Voice, Video and Data

Disadvantages of VSAT technology

- Higher initial equipment/installation costs
- Latency can impact some application performance
- Requires clear line of sight between dish and satellite
- Dish installation requires site planning and about 30 days of overall installation time
- Lack of adequate coverage in some parts of the world
- Severe regulatory restrictions imposed by countries that prevent VSAT networks and solutions from reaching critical mass and therefore profitability
- Lack of skills required in the developing world to design, install and maintain satellite communication systems adequately

Who uses a VSAT system? VSAT Applications

A whole variety of industries use VSAT systems, such as oil and gas exploration corporations, banks, insurance companies, general stores, manufacturing organisations, ATMs and government/military departments, as well as VIPs.

- Supermarket shops
- Chemist shops
- Broadband direct to the home. e.g. Downloading MP3 audio to audio players

- Broadband direct small business, office etc, sharing local use with many PCs
- Internet access from on board ship Cruise ships with internet cafes, commercial shipping communications
- Garages / vehicle sales / petrol stations / motor spares
- Hotel chains, hotel internet cafes
- Insurance offices, quotations access to head office computers, VPN
- Car rental offices, ATM machines
- Airlines, travel agents, booking systems
- Airport air traffic control, flight data
- Financial institutions - Banks, ATM machines
- Lottery terminals
- Manufacturers - sales offices, service divisions, plants
- Job centres
- Customs and tax offices / border passport control checkpoints
- Internet Service Providers
- Phone booths, VoIP, SCPC
- Data file and software distributors
- Pipeline monitoring, well heads, oil rigs
- Rural telephony, data, videophone
- Schools
- Environmental monitoring, weather stations, seismic monitoring
- Mobile phone base station in remote locations or on board ships

8. Role/Functions of each layer present in **ISO's OSI model** for managing heterogeneous network. [2011,2010,2007,2004,2003]
    a. How does it compare with TCP/IP model? [2011]
    b. How error correction is handled in OSI reference model? [2007,2004]

OSI stands for Open System Interconnection. OSI model was developed in late 1970's by ISO (International Standard Organization).

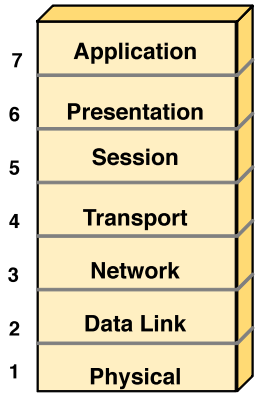
OSI model describes how data flows from one application of PC to another application of another PC.

The OSI model breaks down the entire flow of data into several layers, so that change in one layer should not affect other layers.

It is due to OSI model, various Operating Systems, Application, Protocols, hardware devices work in hand with each other to form a network.

Thus, OSI model was designed to help multiple vendors to work together. It helps multiple hardware and software / protocols to work with each other to create a Network Environment.

OSI - MODEL



REMEMBER -

Andhra Pradesh Se Tamil Nadu Data Pohoncha (Top to Bottom), OR,

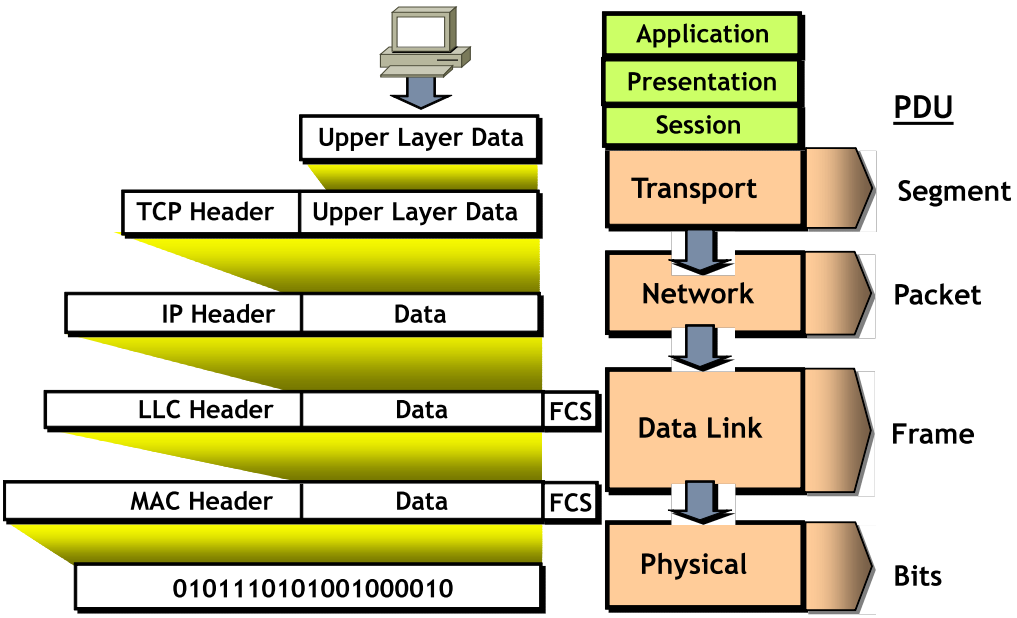
Please Do Not Take Sales Person's Advice (Bottom to Top).

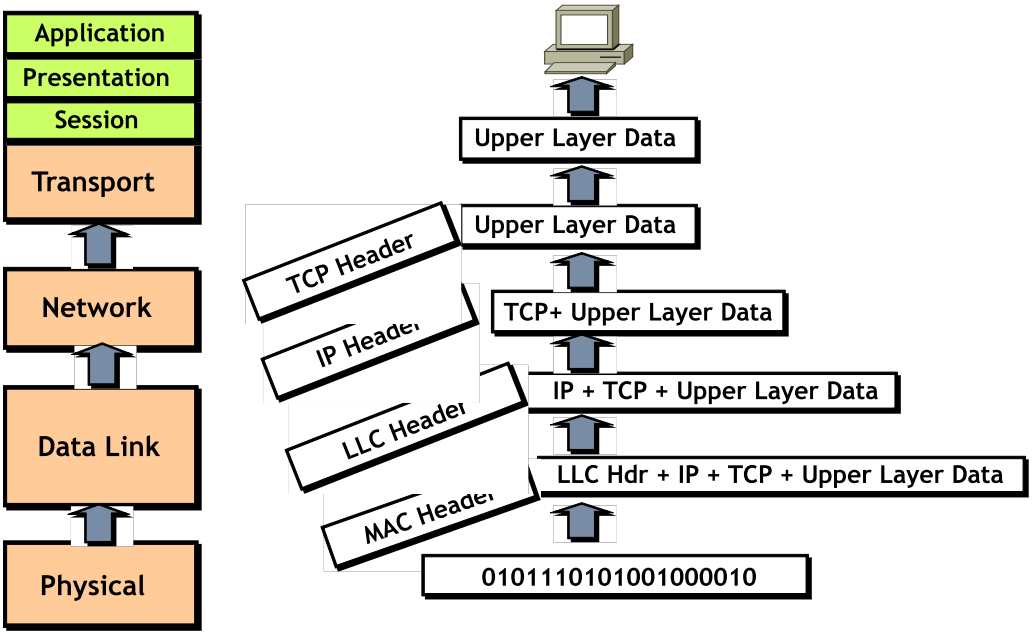
Communication between EACH Layer –

Communication between each layer is done using Header and Tailor. When the data is passed from one layer to another layer, each layer adds an extra bit of information about the layer called as Header. The Header, added by each layer, includes information about that layer itself so that the adjacent layer on the destination PC can read the header information and accordingly can take an action on the data. Tailor and normally used for CRC checking (Cyclic Redundancy Check).

The process of adding the Header is called Encapsulation and removing of the Header is called Decapsulation.

The Header + Upper Layer data + Tailor are called as PDU (Preamble Data Unit).





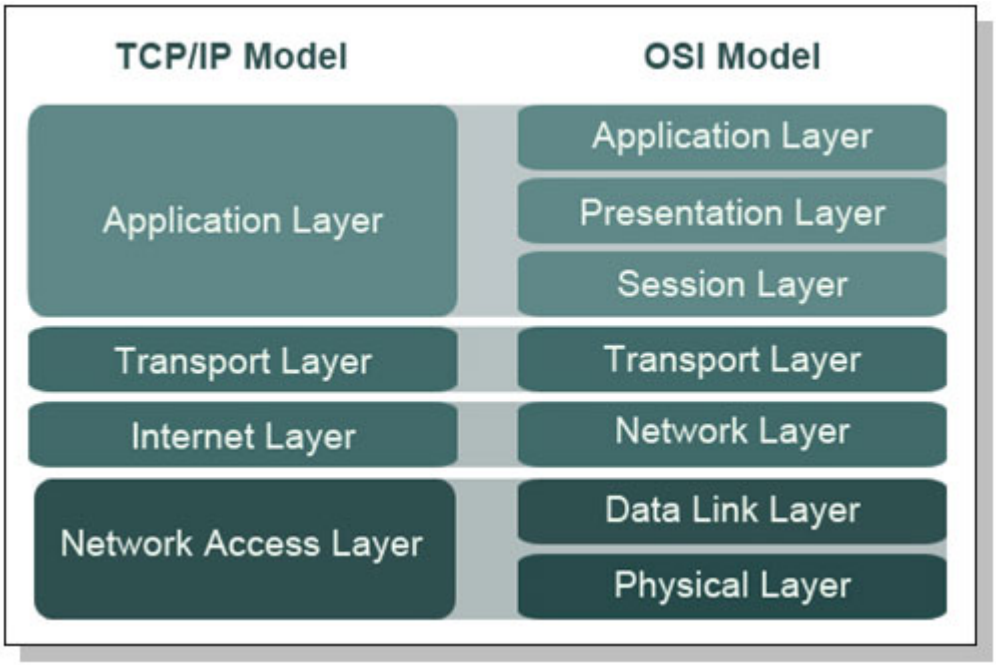
How Communication happens between two PC's using OSI reference model -

Suppose Host A wants to send data to Host B. A will therefore will use some application to send the data to B. Host A passes the request to his Application layer. The Application layer adds a Header to the data and passes the request to the next lower layer i.e. Presentation layer. Presentation layer will now add its own Header and pass the data to the lower layer. The same process begins at the next layer upto Physical layer. Physical layer, after adding its own Header, sends the data over the network to the destination i.e. Host B.

When Host B's Physical layer receives the data, it will remove the Header added by the Physical layer of the Host PC (i.e. A) and will send the data to the layer above it i.e. Data Link layer. Data Link will remove the Header and pass the data to the layer above it i.e. Network. The same process is performed till the data is received by the Application layer and is then displayed to the user on Host B.

OSI Model	Functional Responsibilities	Examples
Application	Defines User Interface, Defines Various Applications & their services.	Telnet
Presentation	Defines Format of Data. Data Formatting, Encoding, Encryption, Compression.	JPEG
Session	Keeps different applications data separate. Dialogue Management.	RPC
Transport	Distinguishes each Application by assigning a PORT-NO & hence provides end to end connectivity using reliable & unreliable methods. Reliable or Unreliable delivery. Reassembly &/or Reordering of packets.	TCP
Network	Defines END-to-END Connectivity using Logical Address (IP-Address used to identify the Destination).	IP
Data Link	Defines POINT-to-POINT Connectivity using Physical Address (MAC-Address). Get the Data across the network between two devices.	802.3
Physical	Move bits between the devices. Physical Tx of Data in bits. Deals with Physical aspects of the media.	V.35

How does OSI model compare with TCP/IP model? [2011]



The TCP/IP suite was created by Dept. of Defense (DoD) to ensure and preserve data integrity as well as maintain communications in the event of war.

Both of them are alike in design and concept and have similar functions in similar places, but how those functions occur is different.

The TCP/IP or DOD model is a condensed version of OSI model, and comprises of 4 layers, instead of 7 layers in OSI.

1. Application layer or Process layer
2. Transport layer or Host to Host layer
3. Internet layer
4. Network Access layer

- **Application layer or Process layer** - A vast array of protocols combine at the DoD model's Application layer to integrate various activities and duties spanning the focus of OSI's corresponding top 3 layers. The Application layer defines protocols for node-to-node application communication and also controls user-interface specifications.
    - We use this layer for troubleshooting, file transfer, internet activities, and a slew of other activities. This layer interacts with many types of applications, such as a database manager, email program, or Telnet.
- **Transport layer or Host to Host layer** - Host-to-Host parallels the functions of OSI's Transport layer, defining protocols for setting up the level of transmission service for applications. It tackles issues like creating reliable and end-to-end communication, and also ensures error-free delivery of data. It handles packet sequencing and maintains data integrity.
    - The Transport Layer provides flow control, error control, and serves as an interface for network applications. An example of the transport layer would be TCP- a protocol suite that is connection-oriented. We may also use UDP- a connectionless means of transporting data.
- **Internet layer** – This layer corresponds to OSI's Network layer, designating the protocols related to the logical transmission over packets over the entire network. It takes care of addressing of hosts by giving them an IP address, and it handles the routing of packets among multiple networks. It also controls the communications flow between two hosts.
- **Network Access Layer** - At the bottom of the model, the Network Access layer monitors the data exchange the host and the network. The equivalent of Data link and Physical layer of OSI reference model, the Network Access layer oversees hardware addressing and defines protocols for physical transmission of data.
    - Network Access layer interfaces with the physical network. It formats data and addresses data for subnets, based on physical hardware addresses. More importantly, it provides error control for data delivered on the physical network.

Differences-

1. OSI is a reference model and TCP/IP is an implementation of OSI model.
2. TCP/IP Protocols are considered to be standards around which the internet has developed. The OSI model however is a "generic, protocol-independent standard".
3. TCP/IP combines the presentation and session layer issues into its application layer.
4. TCP/IP combines the OSI data link and physical layers into the network access layer.
5. TCP/IP is considered to be a more credible model - This is mainly due to the fact because TCP/IP protocols are the standards around which the internet was developed therefore it mainly gains creditability due to this reason. Whereas in contrast networks are not usually built around the OSI model as it is merely used as a guidance tool.
6. The TCP/IP design generally favours decisions based on simplicity, efficiency and ease of implementation.

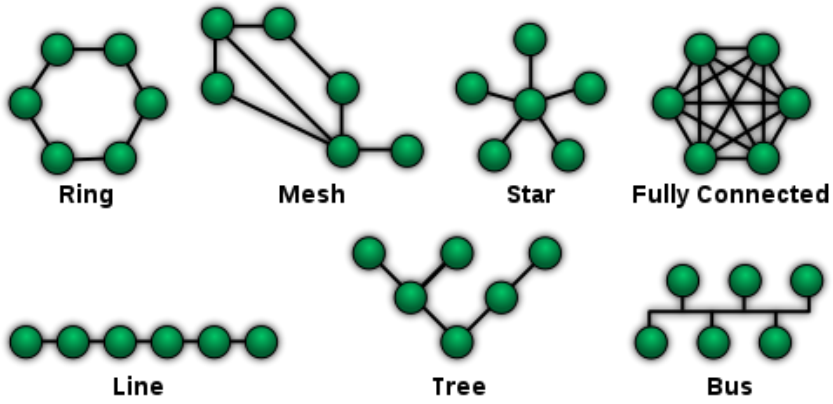
9. **'Network Topology' and 'Network architecture'** mean?
    a. Explain at least four types of topology and four types of architecture with one or more suitable diagram giving their advantages, disadvantages and application in real world situation. [2011, 2010,2004]

Network topology is the layout pattern of interconnections of the various elements (links, nodes, etc.) of a computer or biological network. Network topologies may be physical or logical. Physical topology refers to the physical design of a network including the devices, location and cable installation. Logical topology refers to how data is actually transferred in a network as opposed to its physical design. In general physical topology relates to a core network whereas logical topology relates to basic network.

Topology can be understood as the shape or structure of a network. This shape does not necessarily correspond to the actual physical design of the devices on the computer network. The computers on a home network can be arranged in a circle but it does not necessarily mean that it represents a ring topology.

Any particular network topology is determined only by the graphical mapping of the configuration of physical and/or logical connections between nodes. The study of network topology uses graph theory. Distances between nodes, physical interconnections, transmission rates, and/or signal types may differ in two networks and yet their topologies may be identical.

A local area network (LAN) is one example of a network that exhibits both a physical topology and a logical topology. Any given node in the LAN has one or more links to one or more nodes in the network and the mapping of these links and nodes in a graph results in a geometric shape that may be used to describe the physical topology of the network. Likewise, the mapping of the data flow between the nodes in the network determines the logical topology of the network. The physical and logical topologies may or may not be identical in any particular network.



Topology

There are two basic categories of network topologies:[4]

1. Physical topologies
2. Logical topologies

The shape of the cabling layout used to link devices is called the physical topology of the network. This refers to the layout of cabling, the locations of nodes, and the interconnections between the nodes and the cabling.[1] The physical topology of a network is determined by the capabilities of the network access devices and media, the level of control or fault tolerance desired, and the cost associated with cabling or telecommunications circuits.

The logical topology, in contrast, is the way that the signals act on the network media, or the way that the data passes through the network from one device to the next without regard to the physical interconnection of the devices. A network's logical topology is not necessarily the same as its physical topology. For example, the original twisted pair Ethernet using repeater hubs was a logical bus topology with a physical star topology layout. Token Ring is a logical ring topology, but is wired a physical star from the Media Access Unit.

The logical classification of network topologies generally follows the same classifications as those in the physical classifications of network topologies but describes the path that the *data* takes between nodes being used as opposed to the actual *physical* connections between nodes. The logical topologies are generally determined by network protocols as opposed to being determined by the physical layout of cables, wires, and network devices or by the flow of the electrical signals, although in many cases the paths that the electrical signals take between nodes may closely match the logical flow of data, hence the convention of using the terms *logical topology* and *signal topology* interchangeably.

Logical topologies are often closely associated with Media Access Control methods and protocols. Logical topologies are able to be dynamically reconfigured by special types of equipment such as routers and switches.

The study of network topology recognizes eight basic topologies:[5]

- Point-to-point
- Bus
- Star
- Ring or circular
- Mesh
- Tree
- Hybrid
- Daisy chain

More complex networks can be built as hybrids of two or more of the above basic topologies.

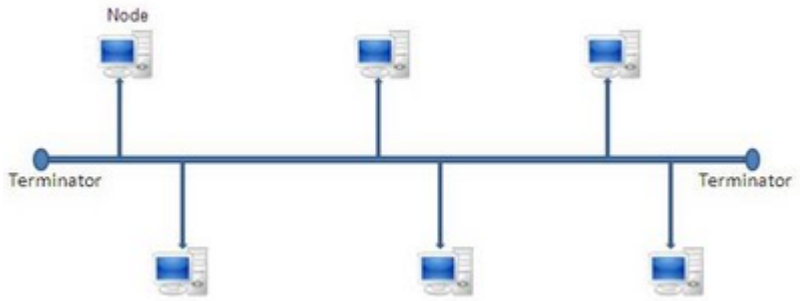
Bus Topology

Bus Topology is the simplest of network topologies. In this type of topology, all the nodes (computers as well as servers) are connected to the single cable (called bus), by the help of interface connectors. This central cable is the backbone of the network and is known as Bus (thus the name). Every workstation communicates with the other device through this Bus.

A signal from the source is broadcasted and it travels to all workstations connected to bus cable. Although the message is broadcasted but only the intended recipient, whose MAC address or IP address matches, accepts it. If the MAC /IP address of machine doesn’t match with the intended address, machine discards the signal.

A terminator is added at ends of the central cable, to prevent bouncing of signals. A barrel connector can be used to extend it. Below I have given a basic diagram of a bus topology and then have discussed advantages and disadvantages of Bus Network Topology

Ethernet bus topologies are relatively easy to install and don't require much cabling compared to the alternatives. 10Base-2 ("ThinNet") and 10Base-5 ("ThickNet") both were popular Ethernet cabling options many years ago for bus topologies. However, bus networks work best with a limited number of devices. If more than a few dozen computers are added to a network bus, performance problems will likely result. In addition, if the backbone cable fails, the entire network effectively becomes unusable.



Bus topology diagram

Advantages of Bus Topology:

1. Quite easy to implement and can be extended by adding other peripherals.
2. Cost efficient as less cable length is required.
3. Suitable for smaller networks.
4. Even if one node breaks down network doesn't get hampered..
5. Nodes or workstation can be easily taken out at will from the network.

Disadvantages of Bus Topology

1) There is a limit on central cable length and number of nodes that can be connected.
2) Dependency on central cable in this topology has its disadvantages If the main cable (i.e. bus) encounters some problem, whole network breaks down.
3) Proper termination is required to dump signals. Use of terminators is must.
4) It is difficult to detect and troubleshoot fault at individual station.
5) Maintenance costs can get higher with time.
6) Efficiency of Bus network reduces, as the number of devices connected to it increases.
7) It is not suitable for networks with heavy traffic.
8) Security is very low because all the computers receive the sent signal from the source

Ring Topology

Ring topology is a network topology in which the nodes or the computers are connected in a closed loop. Each node is connected to two other nodes and when the data is sent it travels across all nodes in one particular direction. Ring topology is used when there is heavy flow of data as it has greater capability to handle data and doesn't even require any central workstation to handle the data transmission.

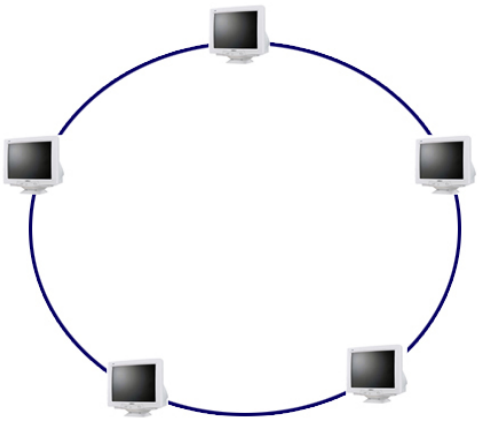


Diagram - Ring Topology

Ring topology is a network topology in which the nodes or the computers are connected in a closed loop. Each node is connected to two other nodes and when the data is sent it travels across all nodes in one particular direction. Ring topology is used when there is heavy flow of data as it has greater capability to handle data and doesn't even require any central workstation to handle the data transmission.

Advantages of Ring Topology

1. High performance delivered
2. Token ring technology reduces the need of server or central hub to manage the workstations
3. All nodes have equal opportunity to transmit the data
4. Easier to manage; easier to locate a defective node or cable problem
5. Well-suited for transmitting signals over long distances on a LAN
6. Handles high-volume network traffic
7. Enables reliable communication

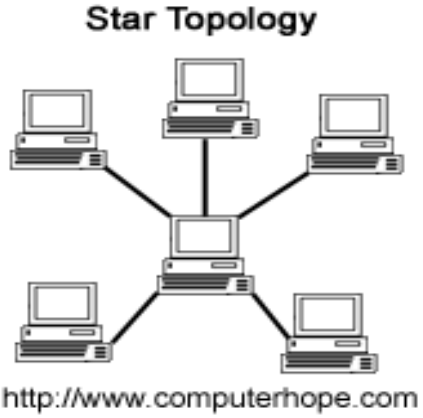
Disadvantages of Ring Topology

1. If one node is disrupted then the whole network goes down
2. It becomes difficult to add/remove nodes
3. If more than one token is generated then it may cause ambiguity in the sending of both kinds.
4. Expensive
5. Requires more cable and network equipment at the start
6. Not used as widely as bus topology
    1. Fewer equipment options
    2. Fewer options for expansion to high-speed communication

Star Topology

In Star topology every node (computer workstation or any other peripheral) is connected to central node called hub or switch. The switch is the server and the peripherals are the clients.

Data from the source is first delivered to the hub and is then transferred to the other nodes. It is easy to add or remove nodes or workstations in this topology. Star topology gives better performance as data doesn't pass through every node unlike Bus topology. If a particular workstation or a node gets an error then the entire network is not affected. But if the central workstation or the hub goes down, then the entire network collapses.
Mostly Star topology uses twisted pair cable, however it can also be used without twisted pair cable.



Advantages of a Star Topology

- Easy to install and reconfigure.
- No disruptions to the network when connecting or removing devices.
- Easy to detect faults and to remove parts.
- Less expensive.
- Includes robustness, that is, if one link fails, only that link is affected, other links remain active.

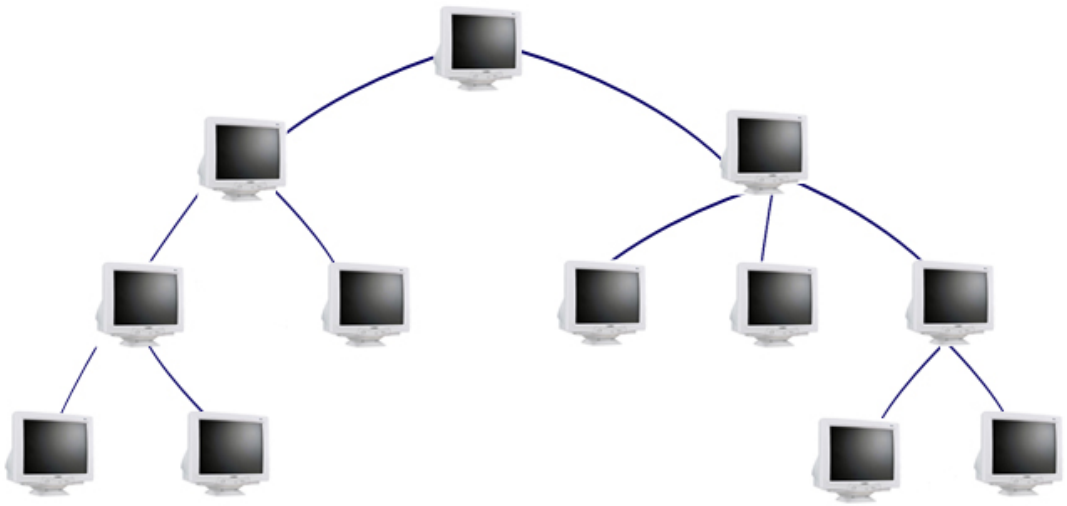
Disadvantages of a Star Topology

- If the hub fails, the whole system is dead.
- If the hub, switch, or concentrator fails, nodes attached are disabled.
- Requires more cable length than a bus topology.
- More expensive than bus topologies because of the cost of the hubs, etc.

Tree Topology

Tree topology is the combination of Bus and Star topology. Here the central workstation or the hub of the Star topologies is connected to the main Bus, along which various Star topologies are placed via their central workstation. If any particular workstation or the node is disrupted, then it will get isolated without affecting the network. But if the central hub of the Star topologies goes down then the whole section of workstation related to it also goes down.

On the other word we can say it is a type of network topology in which a central 'root' node (the top level of the hierarchy) is connected to one or more other nodes that are one level lower in the hierarchy (i.e., the second level) with a point-to-point link between each of the second level nodes and the top level central 'root' node, while each of the second level nodes that are connected to the top level central 'root' node will also have one or more other nodes that are one level lower in the hierarchy (i.e., the third level) connected to it, also with a point-to-point link, the top level central 'root' node being the only node that has no other node above it in the hierarchy



Digram - Tree Topology

Multiple hubs can exist which can be connected to smaller nodes called roots in this case. This structure gives better performance as the main hub controls the whole network.

Advantages of Tree Topology

1. It is most suitable for large networks where ring and star topologies are not efficient.
2. Since it divides the network in sub-parts, so it becomes more manageable
3. There is no hassle in either expanding or removing the nodes.
4. For individual segments there is dedicated line wiring to the local hub.

Disadvantages of Tree Topology

1. The network is vulnerable as it is wholly dependent on the central hub.
2. If the network becomes extremely large it becomes difficult to manage.

Mesh Topology

Mesh topology uses one of the two arrangements either **Full Mesh topology** or **Partial Mesh topology**. In Full Mesh topology each node is connected to every other node in the network. In Partial Mesh topology every node is not connected to each node in the network. In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects.Due to many interconnections much of the cable is required for implementation of mesh topology so it is quite expensive. However, it is reliable because if one node fails, rests of the nodes continue to work with each other.

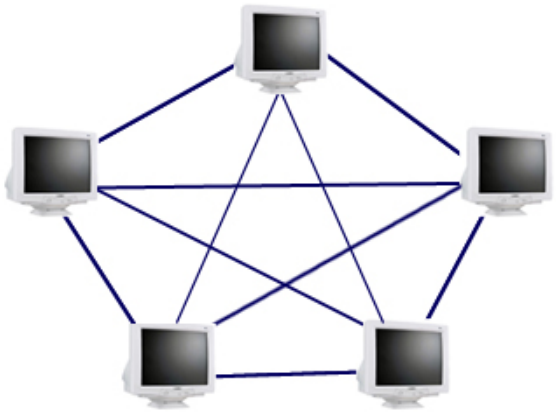


Diagram of true or Full Mash Topology

Since lot of cables is involved, mesh topology is quite expensive to implement. So its often coupled with star, ring or any other topology to form hybrid topology. WAN (Wide Area Network) like Internet uses Mesh network structure.

Advantages of Mesh Topology

1. It is efficient in a sense when one node fails, others continue to work without disruption
2. Network can be easily expanded
3. In one particular instance you can send the data from one node to many nodes
4. Since the message travels along dedicated link, mesh topology is more secure
5. Eliminates traffic problems in links sharing.
6. If one link becomes unusable, it does not incapacitate the entire system. Thus, act as robust.
7. It has privacy and security.
8. Point-to-point link make fault identification and fault isolation easy.

Disadvantages of Mesh Topology

1. It is quite expensive since a higher length of cable is required
2. Implementation can be a very arduous task
3. Installation and reconnection are difficult.
4. The hardware required to connect each link (I/O ports and cable) is expensive.
5. It is generally too costly and complex for practical networks.

Hybrid Topology:

Hybrid networks use a combination of any two or more topologies in such a way that the resulting network does not exhibit one of the standard topologies (e.g., bus, star, ring, etc.). A hybrid topology is always produced when two different basic network topologies are connected.

Advantages of a Hybrid Topology

- It provides a better result by it.
- It can be designed in many ways for various purposes.

Disadvantages of Hybrid Topology

- It is costly.

- Difficult to identify the problem if the entire network shuts down.

Summary

Topologies remain an important part of network design theory. You can probably build a home or small business computer network without understanding the difference between a bus design and a star design, but becoming familiar with the standard topologies gives you a better understanding of important networking concepts like hubs, broadcasts, and routes.

Network architecture

Network Architecture is the complete framework of an organization's computer network. The diagram of the network architecture provides a full picture of the established network with detailed view of all the resources accessible. It includes hardware components used for communication, cabling and device types, network layout and topologies, physical and wireless connections, implemented areas and future plans. In addition, the software rules and protocols also constitute to the network architecture. This architecture is always designed by a network manager/administrator with coordination of network engineers and other design engineers.

Network Architecture provides the detail overview of a network. It is used to classify all the network layers step-by-step in logical form by describing each step in detail. It is also based on the complete working definitions of the protocols. The architecture is emphasized in a distributed computing environment and its complexity cannot be understood without a framework. Therefore there is a need to develop applications or methods to layout an overview of a network

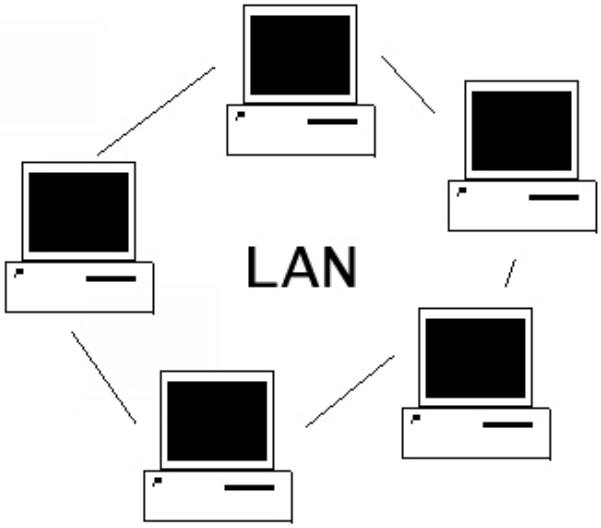
Network architecture refers to the layout of the network, consisting of the hardware, software, connectivity, communication protocols and mode of transmission, such as wired or wireless. Know about the types of network classified according to the areas covered such as LAN, MAN and WAN. Learn about the network topologies categorized according to the layout of equipments and computers such as star, loop, bus, or mesh topologies. There are many communication protocols used in the networking technology. It is important to know about the network architecture as networks play a very important role in today's world.

Network architecture, is the logical and structural layout of the network consisting of transmission equipment, software and communication protocols and infrastructure (wired or wireless) transmission of data and connectivity between components.

1. **Local Area Networks**

A local area network (LAN) is a computer network within a small geographical area such as a home, school, computer laboratory, office building or group of buildings.

A LAN is composed of inter-connected workstations and personal computers which are each capable of accessing and sharing data and devices, such as printers, scanners and data storage devices, anywhere on the LAN. LANs are characterized by higher communication and data transfer rates and the lack of any need for leased communication lines.



Local area networks, generally called LANs, are privately-owned networks within a single building or campus of up to a few kilometers in size. They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information. LANs are distinguished from other kinds of networks by three characteristics: (1) their size, (2) their transmission technology, and (3) their topology.

LANs are restricted in size, which means that the worst-case transmission time is bounded and known in advance. Knowing this bound makes it possible to use certain kinds of designs that would not otherwise be possible. It also simplifies network management.

LANs may use a transmission technology consisting of a cable to which all the machines are attached, like the telephone company party lines once used in rural areas. Traditional LANs run at speeds of 10 Mbps to 100 Mbps, have low delay (microseconds or nanoseconds), and make very few errors. Newer LANs operate at up to 10 Gbps. In this book, we will adhere to tradition and measure line speeds in megabits/sec (1 Mbps is 1,000,000 bits/sec) and gigabits/sec (1 Gbps is 1,000,000,000 bits/sec). Various topologies are possible for broadcast LANs. In network, at any instant at most one machine is the master and is allowed to transmit. All other machines are required to refrain from sending. An arbitration mechanism is needed to resolve conflicts when two or more machines want to transmit simultaneously. The arbitration mechanism may be centralized or distributed. IEEE 802.3, popularly called Ethernet, for example, is a bus-based broadcast network with decentralized control, usually operating at 10 Mbps to 10 Gbps. Computers on an Ethernet can transmit whenever they want to; if two or more packets collide, each computer just waits a random time and tries again later.

A second type of broadcast system is the ring. In a ring, each bit propagates around on its own, not waiting for the rest of the packet to which it belongs. Typically, each bit circumnavigates the entire ring in the time it takes to 21 transmit a few bits, often before the complete packet has even been transmitted. As with all other broadcast systems, some rule is needed for arbitrating simultaneous accesses to the ring. Various methods, such as having the machines take turns, are in use. IEEE 802.5 (the IBM token ring), is a ring-based LAN operating at 4 and 16 Mbps. FDDI is another example of a ring network.

Broadcast networks can be further divided into static and dynamic, depending on how the channel is allocated. A typical static allocation would be to divide time into discrete intervals and use a round-robin algorithm, allowing each machine to broadcast only when its time slot comes up. Static allocation wastes channel capacity when a machine has nothing to say during its allocated slot, so most systems attempt to allocate the channel dynamically (i.e., on demand).

Dynamic allocation methods for a common channel are either centralized or decentralized. In the centralized channel allocation method, there is a single entity, for example, a bus arbitration unit, which determines who goes next. It might do this by accepting requests and making a decision according to some internal algorithm. In the decentralized channel allocation method, there is no central entity; each machine

must decide for itself whether to transmit. You might think that this always leads to chaos, but it does not. Later we will study many algorithms designed to bring order out of the potential chaos.

A short comment about the term ''subnet'' is in order here. Originally, its only meaning was the collection of routers and communication lines that moved packets from the source host to the destination host. However, some years later, it also acquired a second meaning in conjunction with network addressing Unfortunately, no widely-used alternative exists for its initial meaning, so with some hesitation we will use it in both senses. From the context, it will always be clear which is meant. In most WANs, the network contains numerous transmission lines, each one connecting a pair of routers. If two routers that do not share a transmission line wish to communicate, they must do this indirectly, via other routers.

When a packet is sent from one router to another via one or more intermediate routers, the packet is received at each intermediate router in its entirety, stored there until the required output line is free, and then forwarded. A subnet organized according to this principle is called a store-and-forward or packet-switched subnet. Nearly all wide area networks (except those using satellites) have store-and-forward subnets. When the packets are small and all the same size, they are often called cells.

The principle of a packet-switched WAN is so important that it is worth devoting a few more words to it. Generally, when a process on some host has a message to be sent to a process on some other host, the sending host first cuts the message into packets, each one bearing its number in the sequence. These packets 23 are then injected into the network one at a time in quick succession. The packets are transported individually over the network and deposited at the receiving host, where they are reassembled into the original message and delivered to the receiving process.. In some networks all packets from a given message must follow the same route; in others each packet is routed separately. Of course, if ACE is the best route, all packets may be sent along it, even if each packet is individually routed. Routing decisions are made locally. When a packet arrives at router A,itis up to A to decide if this packet should be sent on the line to B or the line to C. How A makes that decision is called the routing algorithm. Many of them exist.

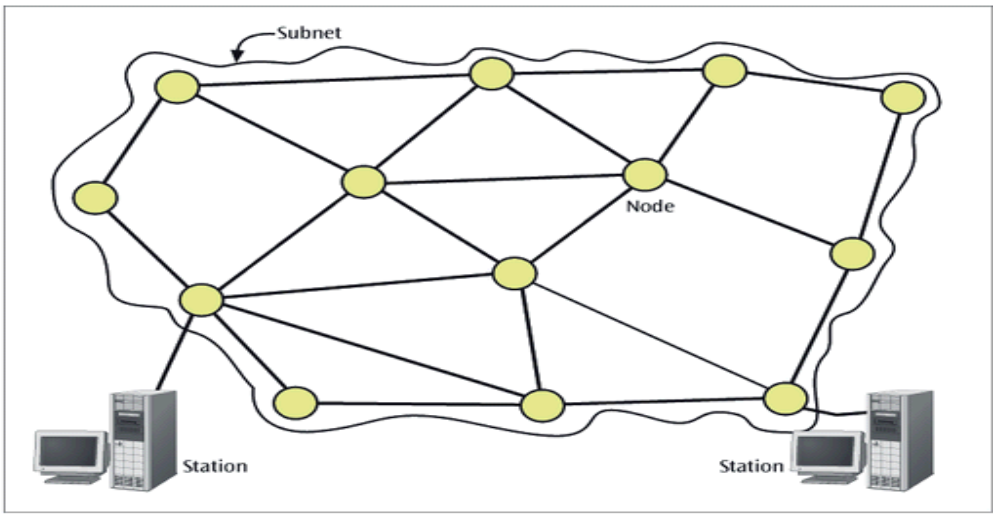
2 Wide Area Network (WAN)

A wide area network (WAN) is a network that exists over a large-scale geographical area. A WAN connects different smaller networks, including local area networks (LAN) and metro area networks (MAN). This ensures that computers and users in one location can communicate with computers and users in other locations. WAN implementation can be done either with the help of the public transmission system or a private network.

A WAN connects more than one LAN and is used for larger geographical areas. WANs are similar to a banking system, where hundreds of branches in different cities are connected with each other in order to share their official data.

A WAN works in a similar fashion to a LAN, just on a larger scale. Typically, TCP/IP is the protocol used for a WAN in combination with devices such as routers, switches, firewalls and modems

Figure 10-5
Network subnet, nodes, and two end stations



Wide Area Networks in detail

A wide area network, or WAN, spans a large geographical area, often a country or continent. It contains a collection of machines intended for running user (i.e., application) programs. We will follow traditional usage and call these machines hosts. The hosts are connected by a communication subnet, or just subnet for short. The hosts are owned by the customers (e.g., people's personal computers), whereas the communication subnet is typically owned and operated by a telephone company or Internet service provider. The job of the subnet is to carry messages from host to host, just as the telephone system carries words from speaker to listener. Separation of the pure communication aspects of the network (the subnet) from the application aspects (the hosts), greatly simplifies the complete network design.In most wide area networks, the subnet consists of two distinct components: transmission lines and switching elements. Transmission lines move bits between machines. They can be made of copper wire, optical fiber, or even radio links. Switching elements are specialized computers that connect three or more transmission lines. When data arrive on an incoming line, the switching element must choose an outgoing line on which to forward them. These switching computers have been called by various names in the past; the name router is now most

Commonly used. Unfortunately, some people pronounce it ''rooter'' and others have it rhyme with ''doubter.'' Determining the correct pronunciation will be left as an exercise for the reader. (Note: the perceived correct Answer may depend on where you live.)

In this model, each host is frequently connected to a LAN on which a router is present, Although in some cases a host can be connected directly to a router. The collection of communication lines and routers (but not the hosts) form the subnet

3 Metropolitan Area Network (MAN)

A metropolitan area network (MAN) is similar to a local area network (LAN) but spans an entire city or campus. MANs are formed by connecting multiple LANs. Thus, MANs are larger than LANs but smaller than wide area networks (WAN).

MANs are extremely efficient and provide fast communication via high-speed carriers, such as fiber optic cables.A MAN is ideal for many kinds of network users because it is a medium-size network. MANs are used to build networks with high data connection speeds for cities and towns.

The working mechanism of a MAN is similar to an Internet Service Provider (ISP), but a MAN is not owned by a single organization. Like a WAN, a MAN provides shared network connections to its users. A MAN

mostly works on the data link layer, which is Layer 2 of the Open Systems Interconnection (OSI) model.

Distributed Queue Dual Bus (DQDB) is the MAN standard specified by the Institute Of Electrical And Electronics Engineers (IEEE) as IEEE 802.6. Using this standard, a MAN extends up to 30-40 km, or 20-25 miles

Metropolitan Area Networks in detail.

A metropolitan area network, or MAN, covers a city. The best-known example of a MAN is the cable television network available in many cities. This system grew from earlier community antenna systems used in areas with poor over-the-air television reception. In these early systems, a large antenna was placed on top of a nearby hill and signal was then piped to the subscribers' houses.

At first, these were locally-designed, ad hoc systems. Then companies began jumping into the business, getting contracts from city governments to wire up an entire city. The next step was television programming and even entire channels designed for cable only. Often these channels were highly specialized, such as all news, all sports, all cooking, all gardening, and so on. But from their inception until the late 1990s, they were intended for television reception only. Starting when the Internet attracted a mass audience, the cable TV network operators began to realize that with some changes to the system, they could provide two-way Internet service in unused parts of the spectrum. At that point, the cable TV system began to morph from a way to distribute television to a metropolitan area Network. To a first approximation, a MAN might look something like the system.

10. Describe network management with respect to its performance, fault, configuration, security and quality of service (availability). [2011]

ANS: - Network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems.

- Operation deals with keeping the network (and the services that the network provides) up and running smoothly. It includes monitoring the network to spot problems as soon as possible, ideally before users are affected.
- Administration deals with keeping track of resources in the network and how they are assigned. It includes all the "housekeeping" that is necessary to keep the network under control.
- Maintenance is concerned with performing repairs and upgrades—for example, when equipment must be replaced, when a router needs a patch for an operating system image, when a new switch is added to a network. Maintenance also involves corrective and preventive measures to make the managed network run "better", such as adjusting device configuration parameters.
- Provisioning is concerned with configuring resources in the network to support a given service. For example, this might include setting up the network so that a new customer can receive voice service.

A common way of characterizing network management functions is FCAPS—Fault, Configuration, Accounting, Performance and Security.

Functions that are performed as part of network management accordingly include controlling, planning, allocating, deploying, coordinating, and monitoring the resources of a network, network planning, frequency allocation, predetermined traffic routing to support load balancing, cryptographic key distribution authorization, configuration management, management, security, performance management, bandwidth management, Route analytics and accounting management.

Data for network management is collected through several mechanisms, including agents installed on infrastructure, synthetic monitoring that simulates transactions, logs of activity, sniffers and real user monitoring. In the past network management mainly consisted of monitoring whether devices were up or

down; today performance management has become a crucial part of the IT team's role which brings about a host of challenges—especially for global organizations.

FCAPS (fault-management, configuration, accounting, performance, and security) is an acronym for a categorical model of the working objectives of network management. There are five levels, called the fault-management level (F), the configuration level (C), the accounting level (A), the performance level (P), and the security level (S).

At the F level, network problems are found and corrected. Potential future problems are identified, and steps are taken to prevent them from occurring or recurring. In this way, the network is kept operational, and downtime is minimized.

At the C level, network operation is monitored and controlled. Hardware and programming changes, including the addition of new equipment and programs, modification of existing systems, and removal of obsolete systems and programs, are coordinated. An inventory of equipment and programs is kept and updated regularly.

The A level, which might also be called the allocation level, is devoted to distributing resources optimally and fairly among network subscribers. This makes the most effective use of the systems available, minimizing the cost of operation. This level is also responsible for ensuring that users are billed appropriately.

The P level is involved with managing the overall performance of the network. Throughput is maximized, bottlenecks are avoided, and potential problems are identified. A major part of the effort is to identify which improvements will yield the greatest overall performance enhancement.

At the S level, the network is protected against hackers, unauthorized users, and physical or electronic sabotage. Confidentiality of user information is maintained where necessary or warranted. The security systems also allow network administrators to control what each individual authorized user can (and cannot) do with the system.

11. Communication—Data Communication—Telecommunication

a. Define: Communication. How does telecommunication differ from Data communication? Explain the process of telecommunication. What are the business applications of telecommunications? [2006]
b. 3 Fundamental elements involved in data communication. [2010]

12. Explain

a. Synchronization [2010]

ANS: - Definition Synchronization is a process that involves coordinating the execution of multiple threads to ensure a desired outcome without corrupting the shared data and preventing any occurrence of deadlocks and race conditions.

Synchronization also occurs between network nodes to ensure that data streams are received and transmitted correctly, and to prevent data collision. It usually uses a clock signal transmitted in sequence with a data stream to maintain proper signal timing.

There are two types of synchronization: data synchronization and process synchronization

* Process Synchronization: The simultaneous execution of multiple threads or processes to reach a handshake such that they commit a certain sequence of actions. Lock, mutex, and semaphores are examples of process synchronization.

* Data Synchronization: Involves the maintenance of data to keep multiple copies of data coherent with each other, or to maintain data integrity. For example, database replication is used to keep multiple copies of data synchronized with database servers that store data in different locations.

Synchronization forms the basis of the execution of multiple threads asynchronously in a multithreaded application. It provides the means to achieve the sharing of resources such as file handling, network connections and memory by coordinating threads and processes to avoid data corruption.

The term is used in the context of multithreaded applications where the resources to be shared across multiple threads have to be controlled, which otherwise can lead to an unpredictable and undesirable outcome. The .NET framework provides synchronization primitives using the multi-threaded applications controlled without any race conditions.

Synchronization is designed to be cooperative, demanding that every thread follow the synchronization mechanism before accessing protected resources for consistent results. Locking, signalling, lightweight synchronization types spin wait and interlocked operations are mechanisms related to synchronization

b. Error Detection & Correction [2010]

ANS**:- Error Detection**

Definition: - In networking, error detection refers to the techniques used to detect noise or other impairments introduced into data while it is transmitted from source to destination. Error detection ensures reliable delivery of data across vulnerable networks.

Error detection minimizes the probability of passing incorrect frames to the destination, known as undetected error probability.

Explanation: - The oldest method of error correction involves using parity. It works by adding an additional bit to each character word transmitted. The state of the bit is determined by a number of factors such as the type of parity and the number of logic-one bits in the data character.

Repetition code is another mechanism that relates to error detection. It is a coding schema that repeats bits across channels to achieve error-free communication. Data bits in a stream of data are divided into blocks of bits. Every block is transmitted a predetermined number of times. They are not as effective as parity, because the occurrence of errors in the same place leads to more problems. However, they are simple and used in the transmission of number stations.

Checksum is an error detection method that is a modular arithmetic sum of message code words of fixed word length. Checksum schemes involve longitudinal redundancy checks, parity bits and check digits

Error Correction

Definition - What does Error Correction mean?

Definition:-Error correction is the process of detecting errors in transmitted messages and reconstructing the original error-free data. Error correction ensures that corrected and error-free messages are obtained at the receiver side.

Explanation: - Systems capable of requesting the retransmission of bad messages in response to error detection include an automatic request for retransmission, or automatic repeat request (ARQ) processing, in their communication software package. They use acknowledgments, negative acknowledgment messages and timeouts to achieve better data transmission.

ARQ is an error control (error correction) method that uses error-detection codes and positive and negative acknowledgments. When the transmitter either receives a negative acknowledgment or a

timeout happens before acknowledgment is received, the ARQ makes the transmitter resend the message.

Error-correcting code (ECC) or forward error correction (FEC) is a method that involves adding parity data bits to the message. These parity bits will be read by the receiver to determine whether an error happened during transmission or storage. In this case, the receiver checks and corrects errors when they occur. It does not ask the transmitter to resend the frame or message.

A hybrid method that combines both ARQ and FEC functionality is also used for error correction. In this case, the receiver asks for retransmission only if the parity data bits are not enough for successful error detection and correction

Error Detection and Correction

Definition: - Error checks and correction is a process aimed at ensuring and improving data retrieval reliability. Data reliability is absolutely critical for processing, record keeping, and e-commerce.

Explanation: - Data exchanged through channels must be verified at the source and retrieval points. This data exchange may apply to a variety of paradigms, including stored data and a processor or two computers over a LAN/Internet connection. Both stored and transmitted data involve physical interaction, which creates added noise and may lead to a change in value.

Powerful error checking and correction methods are continually in the development process. An early simple method involved multiple, repeated, and compared data submissions. However, because this method abuses physical resources, it is not frequently used.

Perhaps the most efficient error-detection technique is the parity check, where a single extra bit is added at the end of each byte. Its value is decided according to a fixed rule, that is, keeping the number of “1's” even or odd per byte. The data receiver processes each byte and estimates the parity bit. If a comparison shows a difference in data, the receiver asks the transmitter to resend the data after indicating a transmission error

c. Flow Control & its purpose in data communication [2010]

ANS: - Flow Control

Definition: - Flow control is the mechanism that ensures the rate at which a sender is transmitting is in proportion with the receiver’s receiving capabilities.

In data communications, flow control is the process of managing the rate of data transmission between two nodes to prevent a fast sender from outrunning a slow receiver. It provides a mechanism for the receiver to control the transmission speed, so that the receiving node is not overwhelmed with data from transmitting node. Flow control should be distinguished from congestion control, which is used for controlling the flow of data when congestion has actually occurred. Flow control mechanisms can be classified by whether or not the receiving node sends feedback to the sending node.

Flow control is important because it is possible for a sending computer to transmit information at a faster rate than the destination computer can receive and process it. This can happen if the receiving computers have a heavy traffic load in comparison to the sending computer, or if the receiving computer has less processing power than the sending computer.

Flow control is utilized in data communications to manage the flow of data/packets among two different nodes, especially in cases where the sending device can send data much faster than the receiver can digest.

Explanation:- Networks of any size have many different devices connected and each device has unique data transmission parameters. For instance, a router is built to manage the routing of data whereas a

desktop, at the receiving end of that data, has far less sending/receiving abilities.

These differences sending/receiving abilities may lead to conflict if the sender starts transmitting data faster than the receiving node's ability. To counteract this problem, flow control is used. This technique manages the flow of data between nodes, keeping the sending/receiving capabilities of both nodes as the primary concern.

Xon-Xoff is an example of a flow control protocol that sync the sender with the receiver. It transmits off signal when the receiver no longer has space in its buffer and a transmit on signal when the receiver can resume taking data. Xon-Xoff works on asynchronous serial connections

d. Data system utilization [2010]
e. Interfacing [2010]
f. Signal Generation [2010]
g. Exchange Management [2010

13. What is Computer Networks? [2010]

a. Why do we need Networks? [2007, 2004]
b. Explain in detail the various types of communication networks with examples. [2006]

ANS: - A network is a group of connected devices or computers,

* Linked together using a wide variety of different cabling types, and for a wide variety of different purposes.
* Nodes are the various endpoints on a network
* Move information from a source to a destination
* Independent of OS, Protocols, OEM, Device configuration and Connectivity
* A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users. Networks are commonly categorized based on their characteristics
* One of the earliest examples of a computer network was a network of communicating computers that functioned as part of the U.S. military's Semi-Automatic Ground Environment (SAGE) radar system. In 1969

Computer network allows sharing of resources and information. Where at least one process in one device is able to send/receive data to/from at least one process residing in a remote device, then the two devices are said to be in a network. A network is a group of devices connected to each other. Networks may be classified into a wide variety of characteristics: the medium used to transport the data, communications protocol used, scale, topology, benefit, and organizational scope.

Communication protocols define the rules and data formats for exchanging information in a computer network, and provide the basis for network programming. Well-known communications protocols include two Ethernet, a hardware and link layer standard that is ubiquitous in local area networks, and the Internet protocol suite, which defines a set of protocols for internetworking, i.e. for data

communication between multiple networks, as well as host-to-host data transfer, and application-specific data transmission formats

Networks are used for the following key reasons:-

- To facilitate communication via email, video conferencing, instant messaging, etc.
- To enable multiple users to share a single hardware device like a printer or scanner.
- To enable file sharing across the network.
- To allow for the sharing of software or operating programs on remote systems.
- To make information easier to access and maintain among network users.

Computer Network Components

Following are the basic components of network.

- **Server**: - Powerful computers that provides services to the other computers on the network.
- **Client**: - Computer that uses the services that a server provides. The client is less powerful than server.
- **Media**: - A physical connection between the devices on a network.
- **Network Adopter**: - Network adopter or network interface card (NIC) is a circuit board with the components necessary for sending and receiving data. It is plugged into one of the available slots on the Pc and transmission cable is attached to the connector on the NIC.
- **Resources**: - Anything available to a client on the network is considered a resource .Printers, data, fax devices and other network devices and information are resources.
- **User**: - Any person that uses a client to access resources on the network.
- **Protocols**: - These are written rules used for communications. They are the languages that computers use to talk to each other on a network

Need for Computer Networks.

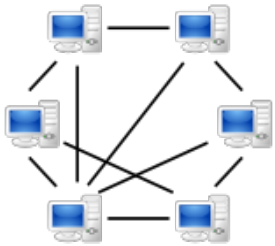
- Networks allow different users share the processing characteristics of different computers.
- Network allows users to share common set of data files and software stored in a main system.
- Network allows users to share common hardware resources such as printers, fax machines, modem etc.
- The cost of computing is reduced to each user as compared to the development and maintain of each single computer system.
- Networks allow data transmission not only among local areas but also to far areas.
- It helps to improve overall productivity.
- Lesser time required for communication.
- One of the major advantage is to collaborate and Data Protection

<u>Types of network</u>

A. Peer to Peer
B. Server Based
C. Packet Switching
D. Network Switching

E. Circuit Switching

A) Peer to peer network: - Peer-to-Peer is a communication model in which each party has the same capabilities and can initiate a communication session with the other. (Point-to-Point) ex:- Utorrent & Fileshare



Peer-to-peer is a communications model in which each party has the same capabilities and either party can initiate a communication session. Other models with which it might be contrasted include the client/server model and the master/slave model. In some cases, peer-to-peer communications is implemented by giving each communication node both server and client capabilities. In recent usage, peer-to-peer has come to describe applications in which users can use the Internet to exchange files with each other directly or through a mediating server.

IBM's Advanced Peer-to-Peer Networking (APPN) is an example of a product that supports the peer-to-peer communication model.

On the Internet, peer-to-peer (referred to as P2P) is a type of transient Internet network that allows a group of computer users with the same networking program to connect with each other and directly access files from one another's hard drives. Napster and Gnutellaare examples of this kind of peer-to-peer software. Major producers of content, including record companies, have shown their concern about what they consider illegal sharing of copyrighted content by suing some P2P users

Advantages

- P-2-P Networks are easy and simple to set up and only require a Hub/Switch to connect all the computers together.
- File & Resource sharing is centralized as long as it is set to shared folder.
- Hardware Requirements for P-2-P :-
- 10 Base T Ethernet cable and an Ethernet hub/ switch.
- Much cheaper than a Server

Disadvantages

- Data is not secure for unprotected files & resources.
- Computers are not reliable for seamless communication.
- Harmful data can also be distributed on P2P networks (ex:- Viruses & Spybot)

2 Server based

A dedicated server is one that functions only as a server and is not used as a client or workstation. Server based networks have become the standard models for networking.

In a server-based network, clients rely on the services that the server provides, such as file storing and printing. Client computers are generally less powerful than server computers

A computer network in which one centralized, powerful computer (called the **server**) is a hub to which many less powerful personal computers or workstations (called **clients**) are connected. The clients run programs and access data that are stored on the server.

Client/server describes the relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfills the request. Although the client/server idea can be used by programs within a single computer, it is a more important idea in a network. In a network, the client/server model provides a convenient way to interconnect programs that are distributed efficiently across different locations. Computer transactions using the client/server model are very common. For example, to check your bank account from your computer, a client program in your computer forwards your request to a server program at the bank. That program may in turn forward the request to its own client program that sends a request to a database server at another bank computer to retrieve your account balance. The balance is returned back to the bank data client, which in turn serves it back to the client in your personal computer, which displays the information for you.

The client/server model has become one of the central ideas of network computing. Most business applications being written today use the client/server model. So does the Internet's main program, TCP/IP. In marketing, the term has been used to distinguish distributed computing by smaller dispersed computers from the "monolithic" centralized computing of mainframe computers. But this distinction has largely disappeared as mainframes and their applications have also turned to the client/server model and become part of network computing.

Other program relationship models included master/slave, with one program being in charge of all other programs, and peer-to-peer, with either of two programs able to initiate a transaction

Advantages

- Centralized - Resources and data security are controlled through the server.
- Security - More security then Peer-to-peer network.
- Flexibility - New technology can be easily integrated into system.
- Interoperability - All components (client /server) work together.
- Accessibility - Server can be accessed remotely and across multiple platforms

Disadvantages

- Expense - Requires initial investment in dedicated server.
- Maintenance - Large networks will require a staff to ensure efficient operation.
- Dependence - When server goes down, operations will cease across the network

3) Packet switching Network

Refers to protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message.
Most modern Wide Area Network (WAN) protocols, including TCP/IP, X.25, and Frame Relay, are based on packet-switching technologies. In contrast, normal telephone service is based on a circuit-switching technology, in which a dedicated line is allocated for transmission between two parties. Circuit-switching is ideal when data must be transmitted quickly and must arrive in the same order in which it's sent. This is the case with most real-time data, such as live audio and video. Packet switching is more

efficient and robust for data that can withstand some delays in transmission, such as e-mail messages and Web pages.
In simple way we can define it as a type of network in which relatively small units of data called packets are routed through a network based on the destination address contained within each packet. Breaking communication down into packets allows the same data path to be shared among many users in the network. This type of communication between sender and receiver is known as *connectionless* (rather than *dedicated*). Most traffic over the Internet uses packet switching and the Internet is basically a connectionless network.

Contrasted with packet-switched is circuit-switched, a type of network such as the regular voice telephone network in which the communication circuit (path) for the call is set up and dedicated to the participants in that call. For the duration of the connection, all resources on that circuit are unavailable for other users. Voice calls using the Internet's packet-switched system are possible. Each end of the conversation is broken down into packets that are reassembled at the other end.

Another type of digital network that uses packet-switching is the X.25 network, a widely-installed commercial wide area network protocol. Internet protocol packets can be carried on an X.25 network. The X.25 network can also support a virtual circuit in which a logical connection is established for two parties on a dedicated basis for some duration. A permanent virtual circuit (PVC) reserves the path on an ongoing basis and is an alternative for corporations to a system of leased lines. A permanent virtual circuit is a dedicated logical connection but the actual physical resources can be shared among multiple logical connections or users

Advantage

- Line efficiency
    - Single node to node link can be shared by many packets over time
    - Packets queued and transmitted as fast as possible
- Data rate conversion
    - Each station connects to the local node at its own speed
    - Nodes buffer data if required to equalize rates
- Packets are accepted even when network is busy
    - Delivery may slow down
- Security
- Availability
- During a crisis or disaster, when the public telephone network might sto.

Disadvantages

- Under heavy use there can be a delay
- Data packets can get lost or become corrupted
- Protocols are needed for a reliable transfer
- Not so good for some types data streams e.g real-time video streams can lose frames due to the way packets arrive out of sequence.

4) Circuit switching network

A type of communications in which a dedicated channel (or *circuit*) is established for the duration of a transmission. The most ubiquitous circuit-switching network is the telephone system, which links together wire segments to create a single unbroken line for each telephone call.
The other common communications method is packet switching, which divides messages into packets and sends each packet individually. The Internet is based on a packet-switching protocol, TCP/IP.

Circuit-switching systems are ideal for communications that require data to be transmitted in real-time. Packet-switching networks are more efficient if some amount of delay is acceptable.
Circuit-switching networks are sometimes called *connection-oriented*networks. Note, however, that although packet switching is essentially connectionless, a packet switching network can be made connection-oriented by using a higher-level protocol. TCP, for example, makes IP networks connection-oriented.

Circuit-switched is a type of network in which a physical path is obtained for and dedicated to a single connection between two end-points in the network for the duration of the connection. Ordinary voice phone service is circuit-switched. The telephone company reserves a specific physical path to the number you are calling for the duration of your call. During that time, no one else can use the physical lines involved.

Circuit-switched is often contrasted with packet-switched. Some packet-switched networks such as the X.25 network are able to have virtual circuit-switching. A virtual circuit-switched connection is a dedicated logical connection that allows sharing of the physical path among multiple virtual circuit connections

Advantages

- Provides for continuous transfer without the overhead associated with packets
- Makes maximal use of available bandwidth
- Ensures dedicated bandwidth to each user

Disadvantages

- Circuit-switched networks can be relatively inefficient, because bandwidth can be wasted
- You have to provision and pay for peak bandwidth

4) Network switching

Network switching subsystem (**NSS**) (or **GSM core network**) is the component of a GSM system that carries out call switching and mobility management functions for mobile phones roaming on the network of base stations. It is owned and deployed by mobile phone operators and allows mobile devices to communicate with each other and telephones in the wider public switched telephone network (PSTN). The architecture contains specific features and functions which are needed because the phones are not fixed in one location.

The NSS originally consisted of the circuit-switched core network, used for traditional GSM services such as voice calls, SMS, and circuit switched data calls. It was extended with overlay architecture to provide packet-switched data services known as the GPRS core network. This allows mobile phones to have access to services such as WAP, MMS, and the Internet. The main part of which is the Mobile Switching Center (MSC), performs the switching of calls between the mobile and other fixed or mobile network users, as well as the management of mobile services such as authentication.

The switching system includes the following functional elements.

Home Location Register (HLR):- The HLR is a database used for storage and management of subscriptions.

Mobile Services Switching Center (MSC):- The MSC performs the switching of calls between the mobile and other fixed or mobile network users, as well as the management of mobile services such as such as registration, authentication, location updating, handovers, and call routing to a roaming subscriber

Visitor Location Register (VLR):- The VLR is a database that contains temporary information about subscribers that is needed by the MSC in order to service visiting subscribers.

Authentication Centre (AUC):-The Authentication Center is a protected database that stores a copy of the secret key stored in each subscriber's SIM card, which is used for authentication and ciphering of the radio channel. The AUC protects network operators from different types of fraud found in today's cellular world.

Equipment Identity Register (EIR):- The Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipment on the network, where its International Mobile Equipment Identity (IMEI) identifies each MS. An IMEI is marked as invalid if it has been reported stolen or is not type approved.

14. What are Network Protocols? [2010, 2006]

a. Objectives & Distinguish between OSI & TCP/IP protocols. [2006]

Network Protocol –

A 'Network Protocol' is the agreed method of communication to be used within the network. Each computer will use this protocol.

A network protocol defines rules and conventions for communication between network devices. Protocols for computer networking all generally use packet switching techniques to send and receive messages in the form of packets.

Network protocols include mechanisms for devices to identify and make connections with each other, as well as formatting rules that specify how data is packaged into messages sent and received. Some protocols also support message acknowledgement and data compression designed for reliable and/or high-performance network communication. Hundreds of different computer network protocols have been developed each designed for specific purposes and environments.

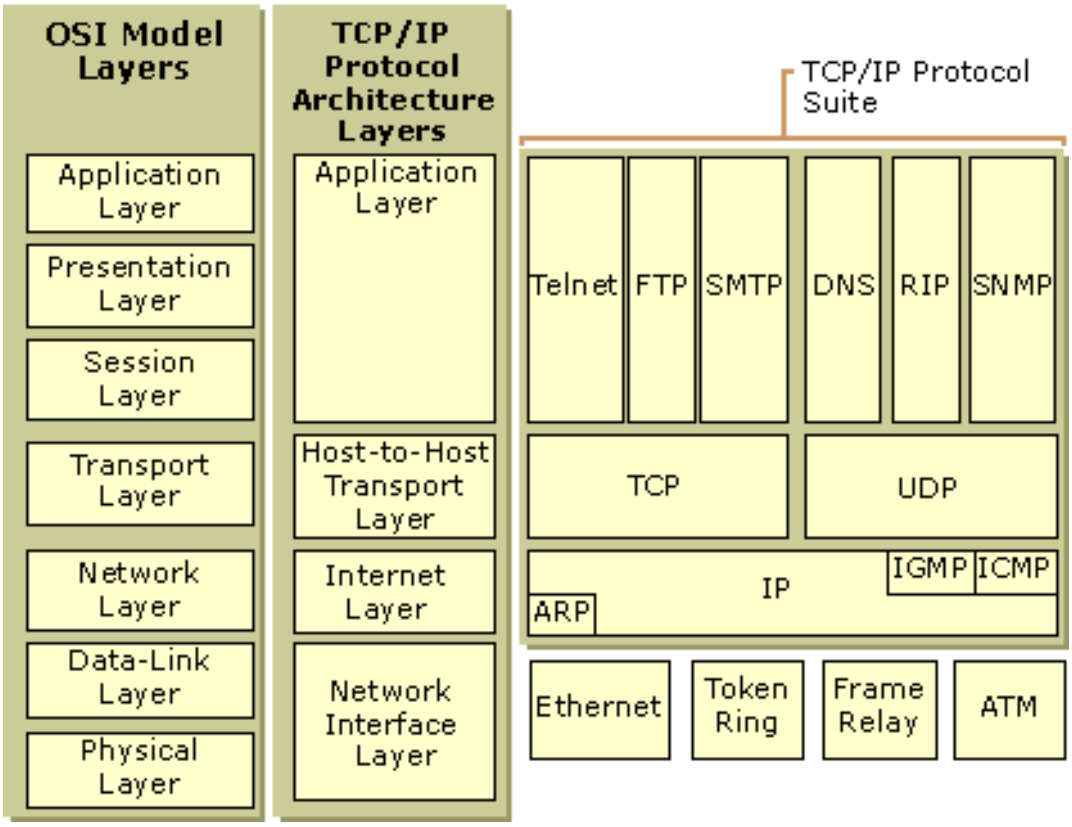
Internet Protocols

The Internet Protocol family contains a set of related (and among the most widely used network protocols. Besides Internet Protocol (IP) itself, higher-level protocols like TCP, UDP, HTTP, and FTP all integrate with IP to provide additional capabilities. Similarly, lower-level Internet Protocols like ARP and ICMP also co-exist with IP. These higher level protocols interact more closely with applications like Web browsers while lower-level protocols interact with network adapters and other computer hardware.

Routing Protocols

Routing protocols are special-purpose protocols designed specifically for use by network routers on the Internet. Common routing protocols include EIGRP, OSPF and BGP.

Objectives & Distinguish between OSI & TCP/IP protocols. [2006]



http://technet.microsoft.com/en-us/library/cc958821.aspx

Network Interface Layer -

The Network Interface layer (also called the Network Access layer) is responsible for placing TCP/IP packets on the network medium and receiving TCP/IP packets off the network medium. TCP/IP was designed to be independent of the network access method, frame format, and medium. In this way, TCP/IP can be used to connect differing network types. These include LAN technologies such as Ethernet and Token Ring and WAN technologies such as X.25 and Frame Relay. Independence from any specific network technology gives TCP/IP the ability to be adapted to new technologies such as Asynchronous Transfer Mode (ATM).

The Network Interface layer encompasses the Data Link and Physical layers of the OSI model. Note that the Internet layer does not take advantage of sequencing and acknowledgment services that might be present in the Data-Link layer. An unreliable Network Interface layer is assumed, and reliable communications through session establishment and the sequencing and acknowledgment of packets is the responsibility of the Transport layer.

Internet Layer -

The Internet layer is responsible for addressing, packaging, and routing functions. The core protocols of the Internet layer are IP, ARP, ICMP, and IGMP.

The Internet Protocol (IP) is a routable protocol responsible for IP addressing, routing, and the fragmentation and reassembly of packets.

The Address Resolution Protocol (ARP) is responsible for the resolution of the Internet layer address to the Network Interface layer address such as a hardware address.

The Internet Control Message Protocol (ICMP) is responsible for providing diagnostic functions and reporting errors due to the unsuccessful delivery of IP packets.

The Internet Group Management Protocol (IGMP) is responsible for the management of IP multicast groups.

The Internet layer is analogous to the Network layer of the OSI model.

Transport Layer -

The Transport layer (also known as the Host-to-Host Transport layer) is responsible for providing the Application layer with session and datagram communication services. The core protocols of the Transport layer are Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

TCP provides a one-to-one, connection-oriented, reliable communications service. TCP is responsible for the establishment of a TCP connection, the sequencing and acknowledgment of packets sent, and the recovery of packets lost during transmission.

UDP provides a one-to-one or one-to-many, connectionless, unreliable communications service. UDP is used when the amount of data to be transferred is small (such as the data that would fit into a single packet), when the overhead of establishing a TCP connection is not desired or when the applications or upper layer protocols provide reliable delivery.

The Transport layer encompasses the responsibilities of the OSI Transport layer and some of the responsibilities of the OSI Session layer.

Application Layer -

The Application layer provides applications the ability to access the services of the other layers and defines the protocols that applications use to exchange data. There are many Application layer protocols and new protocols are always being developed.

The most widely-known Application layer protocols are those used for the exchange of user information:

The Hypertext Transfer Protocol (HTTP) is used to transfer files that make up the Web pages of the World Wide Web.

The File Transfer Protocol (FTP) is used for interactive file transfer.

The Simple Mail Transfer Protocol (SMTP) is used for the transfer of mail messages and attachments.

Telnet, a terminal emulation protocol, is used for logging on remotely to network hosts.

Additionally, the following Application layer protocols help facilitate the use and management of TCP/IP networks:

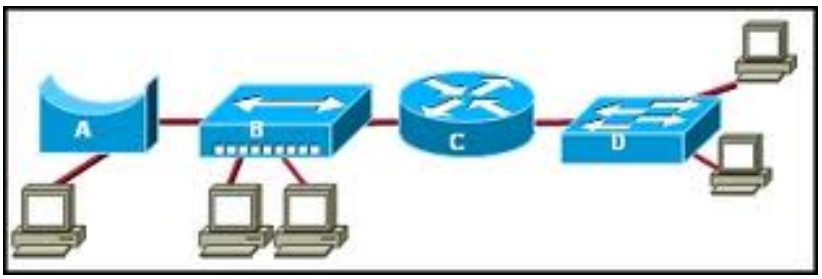
The Domain Name System (DNS) is used to resolve a host name to an IP address.

The Routing Information Protocol (RIP) is a routing protocol that routers use to exchange routing information on an IP internetwork.

The Simple Network Management Protocol (SNMP) is used between a network management console and network devices (routers, bridges, intelligent hubs) to collect and exchange network management information.

Examples of Application layer interfaces for TCP/IP applications are Windows Sockets and NetBIOS. Windows Sockets provides a standard application programming interface (API) under Windows 2000. NetBIOS is an industry standard interface for accessing protocol services such as sessions, datagrams, and name resolution. More information on Windows Sockets and NetBIOS is provided later in this chapter.

15. Explain using a single network diagram the following network devices: [2010,2004]
    a. Hub
    b. Repeater
    c. Bridge
    d. Router
    e. Switch



SYMBOLS

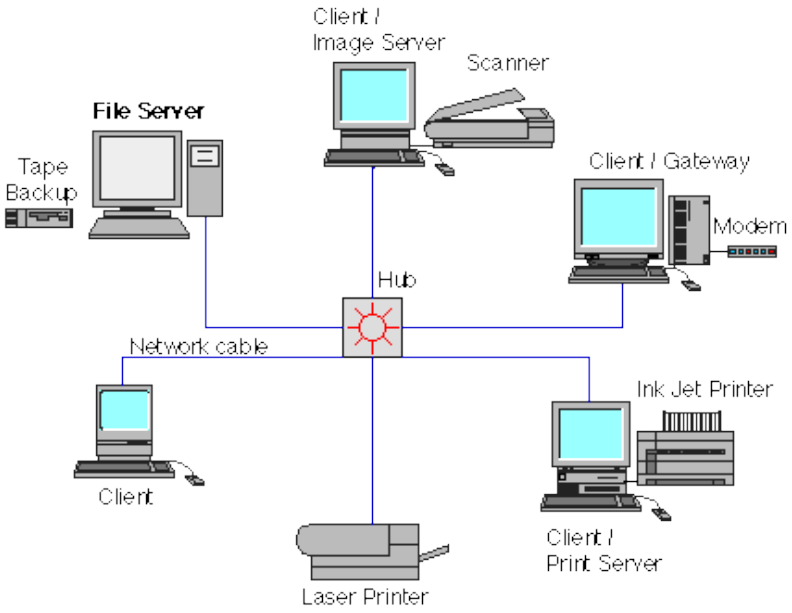
A – Bridge B – Switch

C – Router D – Switch

First off these devices are all connectivity devices, they work at various layers of the OSI model and all have unique functions.

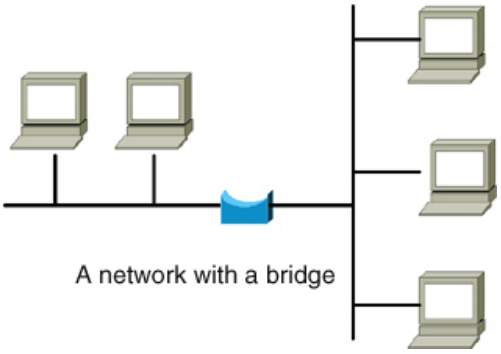
HUB –

- A common connection point for devices in a network OR place of convergence where data arrives from one or more directions and is forwarded out in one or more other directions.
- Operates at L1 of OSI reference model.
- Each computer will be connected to a single 'port' on the hub.
- So if you purchase an '8 port hub', you will be able to connect up to eight computers together.



Switch / Bridge –

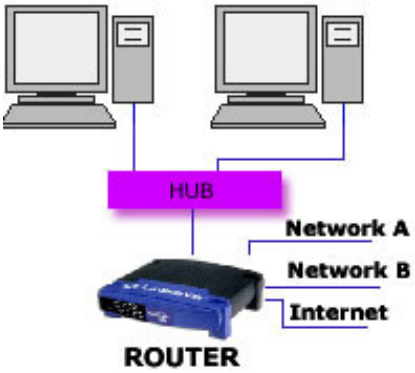
- Unlike hubs, network switches contains more "intelligence" and are capable of inspecting data packets as they are received, determining the source and destination device of that packet, and forwarding it appropriately.
- By delivering each message only to the connected device it was intended for, a network switch conserves Network Bandwidth and offers generally better performance than a hub.
- A switch has a number of ports and it stores the addresses of all devices that are directly or indirectly connected to it on each port.
- As a data packet comes into the switch, its destination MAC address is examined & a direct connection is made between the two machines
- Operates at L2 of OSI reference model.



Router –

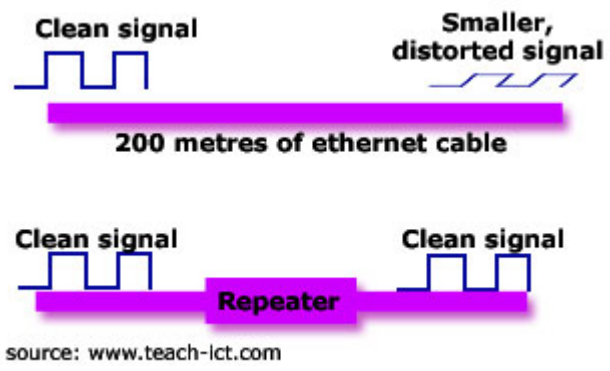
- A device that connects two or more different Networks.
- Operates at L3 i.e. Network layer of OSI reference model.
- A Router is a device that transfers data from one network to another in an intelligent way. It has the task of forwarding data packets to their destination by the most efficient route.
- In order to do this, the router has a micro-computer inside it. This holds a table in memory that contains a list of all the networks it is connected to, along with the latest information on how busy each path in the network is, at that moment.

- When a data packet arrives, the router does the following:-
    - Reads the data packet's destination address
    - Looks up all the paths it has available to get to that address.
    - Checks on how busy each path is at the moment
    - Sends the packet along the least congested (fastest) path.
- Other tasks the Router can perform:
    - Exchange Protocol information across networks.
    - Filter traffic - useful for preventing hacker attacks for example



Repeaters –

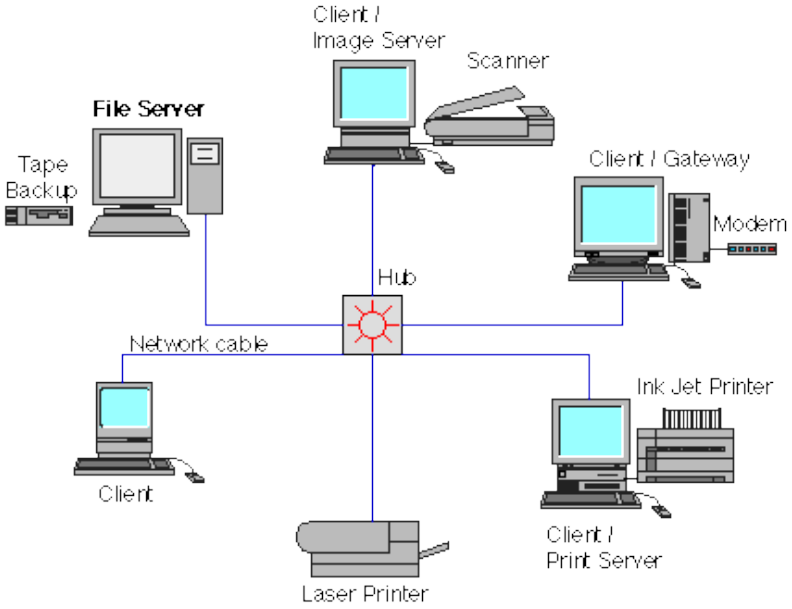
- Since a signal loses strength as it passes along a cable, it is often necessary to boost the signal with a device called a repeater. The repeater electrically amplifies the signal it receives and rebroadcasts it.
- Repeaters can be separate devices or they can be incorporated into a concentrator. They are used when the total length of your network cable exceeds the standards set for the type of cable being used.
- A Repeater boosts the signal back to its correct level.
- Here are some typical maximum cable lengths –
    - Copper cable - 100 m
    - Thick Ethernet - 500 m
    - Thin Ethernet - 185 m



First off these devices are all connectivity devices, they work at various layers of the OSI model and all have unique functions.

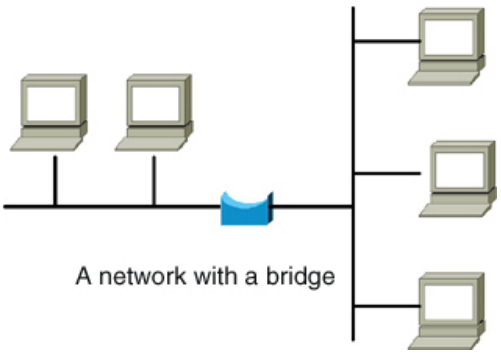
HUB –

- A common connection point for devices in a network OR place of convergence where data arrives from one or more directions and is forwarded out in one or more other directions.
- Operates at L1 of OSI reference model.
- Each computer will be connected to a single 'port' on the hub.
- So if you purchase an '8 port hub', you will be able to connect up to eight computers together.



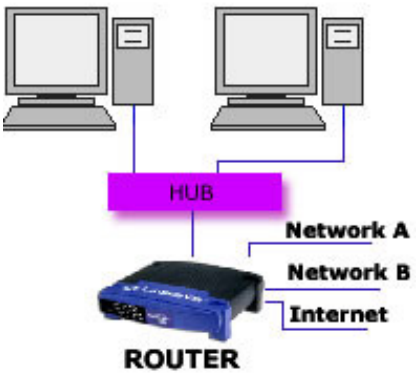
Switch / Bridge –

- Unlike hubs, network switches contains more "intelligence" and are capable of inspecting data packets as they are received, determining the source and destination device of that packet, and forwarding it appropriately.
- By delivering each message only to the connected device it was intended for, a network switch conserves Network Bandwidth and offers generally better performance than a hub.
- A switch has a number of ports and it stores the addresses of all devices that are directly or indirectly connected to it on each port.
- As a data packet comes into the switch, its destination MAC address is examined & a direct connection is made between the two machines
- Operates at L2 of OSI reference model.



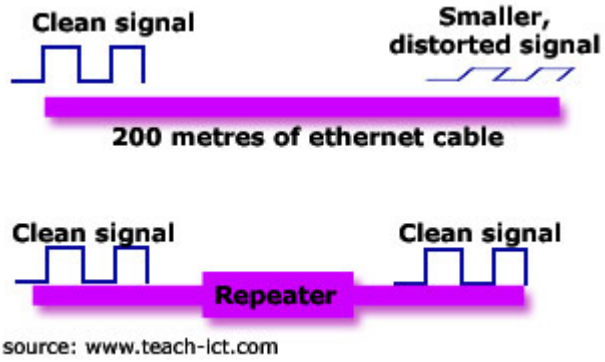
Router –

- A device that connects two or more different Networks.
- Operates at L3 i.e. Network layer of OSI reference model.
- A Router is a device that transfers data from one network to another in an intelligent way. It has the task of forwarding data packets to their destination by the most efficient route.
- In order to do this, the router has a micro-computer inside it. This holds a table in memory that contains a list of all the networks it is connected to, along with the latest information on how busy each path in the network is, at that moment.
- When a data packet arrives, the router does the following:-
    - Reads the data packet's destination address
    - Looks up all the paths it has available to get to that address.
    - Checks on how busy each path is at the moment
    - Sends the packet along the least congested (fastest) path.
- Other tasks the Router can perform:
    - Exchange Protocol information across networks.
    - Filter traffic - useful for preventing hacker attacks for example



Repeaters –

- Since a signal loses strength as it passes along a cable, it is often necessary to boost the signal with a device called a repeater. The repeater electrically amplifies the signal it receives and rebroadcasts it.
- Repeaters can be separate devices or they can be incorporated into a concentrator. They are used when the total length of your network cable exceeds the standards set for the type of cable being used.
- A Repeater boosts the signal back to its correct level.
- Here are some typical maximum cable lengths –
    - Copper cable - 100 m
    - Thick Ethernet - 500 m
    - Thin Ethernet - 185 m



16. What are Network Interface cards? Different types of NIC with suitable application in industry. [2010]

NIC is an acronym for Network Interface Card or Network Interface Controller. However, a NIC is actually referred to as a network adapter by most of the population. A NIC is an expansion card, a hardware device attached to a non-portable computer (like a desktop) allowing that computer some new ability. As an expansion card, the NIC specifically allows a computer the ability to connect to a network (such as Ethernet or Wi-FI).

Function

NIC cards serve as conduits between a computer and a network (like Internet). They translate the data on the computer into a form that is transferrable via a network cable and control the data as it is sent to other devices on the network.

Configuration Types

There are three different types of NIC arrangements, or configurations: jumper, software and the newest technology, Plug-and-Play (PnP).

Jumper Configurable NIC Cards

1. Jumper configurable NIC cards are efficient and easy to use for older equipment. They have physical jumpers (small devices that control computer hardware without the need for software) that determine settings for the interrupt request line, input/output address, upper memory block and type of transceiver.

Software Configurable NIC Cards

2. Software configurable NIC must be manually configured when installed, but contain a proprietary software program that allows the operator to configure the NIC via a menu, or choose the auto configuration mode that determines what configuration is most suitable.

Plug-and-Play Configurable NIC Cards

3. Most NICs today use the PnP technology as it does not have to be manually configured, though it can be. PnP NICs will auto-configure upon installation during the system boot-up sequence, but can cause conflicts with the hard drive.

Network Interface Card :-

Network adapter is a device that enables a computer to talk with other computer/network. Using unique **hardware addresses (MAC address)** encoded on the card chip, the data-link protocol employs these addresses to discover other systems on the network so that it can transfer data to the right destination.

There are **two types of network cards**: **wired and wireless**. The wired NIC uses cables and connectors as a medium to transfer data, whereas in the wireless card, the connection is made using antenna that employs radio wave technology. All modern laptop computers incorporated wireless NIC in addition to the wired adapter.

Network Card Speed

Network Interface card, one of the main computer network components, comes with different speeds, 10Mbps, 100Mbps, and 1000Mbps, so on. Recent standard network cards built with Gigabit (1000Mbps) connection speed. It also supports to connect slower speeds such as 10Mbps and 100Mbps. However, the speed of the card depends on your LAN speed.

For example, if you have a switch that supports up to 100Mbps, your NIC will also transfer a data with this same speed even though your computer NIC has still the capability to transfer data at 1000Mbps (1Gbps). In modern computers, network adapter is integrated with a computer motherboard. However if you want advanced and fast Ethernet card, you may buy and install on your computer using the PCI slot found on the motherboard (desktop) and ExpressCard slots on laptop.

A network interface controller (NIC) (also known as a network interface card, network adapter, LAN adapter and by similar terms) is a computer hardware component that connects a computer to a computer network.

Early network interface controllers were commonly implemented on expansion cards that plugged into a computer bus; the low cost and ubiquity of the Ethernet standard means that most newer computers have a network interface built into the motherboard

The network controller implements the electronic circuitry required to communicate using a specific physical layer and data link layer standard such as Ethernet, Wi-Fi or Token Ring. This provides a base for a full network protocol stack, allowing communication among small groups of computers on the same LAN and large-scale network communications through routable protocols, such as IP.

Although other network technologies exist (e.g. token ring), Ethernet has achieved near-ubiquity since the mid-1990s.

Every Ethernet network controller has a unique 48-bit serial number called a MAC address, which is stored in read-only memory. Every computer on an Ethernet network must have at least one controller. Normally it is safe to assume that no two network controllers will share the same address, because controller vendors purchase blocks of addresses from the Institute of Electrical and Electronics Engineers (IEEE) and assign a unique address to each controller at the time of manufacture.[2]

The NIC allows computers to communicate over a computer network. It is both an OSI layer 1 (physical layer) and layer 2 (data link layer) device, as it provides physical access to a networking medium and provides a low-level addressing system through the use of MAC addresses. It allows users to connect to each other either by using cables or wirelessly.

Whereas network controllers used to operate on expansion cards that plugged into a computer bus, the low cost and ubiquity of the Ethernet standard means that most newer computers have a network interface built into the motherboard. Newer server motherboards may even have dual network interfaces built-in. The Ethernet capabilities are either integrated into the motherboard chipset or implemented via a low-cost dedicated Ethernet chip, connected through the PCI (or the newer PCI express) bus. A separate network card is not required unless additional interfaces are needed or some other type of network is used.

The NIC may use one or more of two techniques to indicate the availability of packets to transfer:

- Polling is where the CPU examines the status of the peripheral under program control.
- Interrupt-driven I/O is where the peripheral alerts the CPU that it is ready to transfer data.

and may use one or more of two techniques to transfer packet data:

- Programmed input/output is where the CPU moves the data to or from the designated peripheral to memory.
- Direct memory access is where an intelligent peripheral assumes control of the system bus to access memory directly. This removes load from the CPU but requires more logic on the card. In addition, a packet buffer on the NIC may not be required and latency can be reduced.

An Ethernet network controller typically has an 8P8C socket where the network cable is connected. Older NICs also supplied BNC, or AUI connections. A few LEDs inform the user of whether the network is active, and whether or not data transmission occurs. Ethernet network controllers typically support 10 Mbit/s Ethernet, 100 Mbit/s Ethernet, and 1000 Mbit/s Ethernet varieties. Such controllers are designated 10/100/1000 - this means they can support a notional maximum transfer rate of 10, 100 or 1000 Megabits per second.

A **wireless network interface controller** (WNIC) is a network interface controller which connects to a radio-based computer network rather than a wire-based network such as Token Ring or Ethernet. A WNIC, just like other NICs, works on the Layer 1 and Layer 2 of the OSI Model. A WNIC is an essential component for wireless desktop computer. This card uses an antenna to communicate through microwaves. A WNIC in a desktop computer usually is connected using the PCI bus. Other connectivity options are USB and PC card. Integrated WNICs are also available, (typically in Mini PCI/PCI Express Mini Card form).

The term is usually applied to IEEE 802.11 adapters; it may also apply to a NIC using protocols other than Specifications

The IEEE 802.11 standard sets out low-level specifications for how all 802.11 wireless networks operate. Earlier 802.11 interface controllers are usually only compatible with earlier variants of the standard, while newer cards support both current and old standards.

Specifications commonly used in marketing materials for WNICs include:

- Wireless data transfer rates (measured in Mbit/s); these range from 2 Mbit/s to 54 Mbit/s.[1]
- Wireless transmit power (measured in dBm)

- Wireless network standards (may include standards such as 802.11b, 802.11g, 802.11n, etc.) 802.11g offers data transfer speeds equivalent to 802.11a – up to 54 Mbit/s – and the wider 300-foot (91 m) range of 802.11b, and is backward compatible with 802.11b.

Most Bluetooth cards do not implement any form of the 802.11 standard.

Range

Wireless range may be substantially affected by objects in the way of the signal and by the quality of the antenna. Large electrical appliances, such as refrigerators, fuse boxes, metal plumbing, and air conditioning units can impede a wireless network signal. The theoretical maximum range of IEEE 802.11 is only reached under ideal circumstances and true effective range is typically about half of the theoretical range.[1] Specifically, the maximum throughput speed is only achieved at extremely close range (less than 25 feet (7.6 m) or so); at the outer reaches of a device's effective range, speed may decrease to around 1 Mbit/s before it drops out altogether. The reason is that wireless devices dynamically negotiate the top speed at which they can communicate without dropping too many data packets 802.11, such as one implementing Bluetooth connections.

17. Describe using examples: LAN, WAN, MAN & Campus Area Networks[2010]
    a. Diff between LAN & WAN and the protocols used in these 2 technologies. [2003]
    b. LAN [2007]
        i. Various topologies for LAN [2007, 2003]
        ii. Medias used for LAN and their choice [2007, 2004, 2003]
        iii. CSMA/CD and how Ethernet tackles it [2007,2004]
        iv. Functions of HUB, Bridge and Switch [2007, Differences-2004].
        v. Speed and Distance limitation for various media. [2004]
        vi. Address resolution in a LAN [2004, 2003]
    c. WAN [2007]
        i. Various alternatives for connectivity between locations [2007, 2004]
        ii. Choice of topologies [2007, 2004]
        iii. Routing protocols and their selection [2007, 2004]
        iv. Performance criterion for WAN [2007]

A network consists of two or more computers that are linked in order to share resources (such as printers and CD-ROMs), exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

The three basic types of networks include –

- Local Area Network (LAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN)
- Campus Area Networks (CAN)

Local Area Network –

A Local Area Network (LAN) is a network that is confined to a relatively small area. It is generally limited to a geographic area such as a writing lab, school, or building. Rarely are LAN computers more than a mile apart.

In a typical LAN configuration, one computer is designated as the file server. It stores all of the software that controls the network, as well as the software that can be shared by the computers attached to the network. Computers connected to the file server are called workstations. The workstations can be less powerful than the file server, and they may have additional software on their hard drives. On most LANs, cables are used to connect the network interface cards in each computer.

A local area network is a network in its simplest form. Data transfer speeds over a local area network can reach up to 10 Mbps (such as for an Ethernet network) and 1 Gbps (as with FDDI or Gigabit Ethernet). A local area network can reach as many as 100, or even 1000, users.

By expanding the definition of a LAN to the services that it provides, two different operating modes can be defined:

- In a "peer-to-peer" network, in which communication is carried out from one computer to another, without a central computer, and where each computer has the same role.
- In a "client/server" environment, in which a central computer provides network services to users.

Metropolitan Area Network –

MANs (Metropolitan Area Networks) connect multiple geographically nearby LANs to one another (over an area of up to a few dozen kilometers) at high speeds. Thus, a MAN lets two remote nodes communicate as if they were part of the same local area network.

A MAN is made from switches or routers connected to one another with high-speed links (usually fiber optic cables).

A Metropolitan Area Network (MAN) covers larger geographic areas, such as cities or school districts. By interconnecting smaller networks within a large geographic area, information is easily disseminated throughout the network. Local libraries and government agencies often use a MAN to connect to citizens and private industries.

One example of a MAN is the MIND Network located in Pasco County, Florida. It connects all of Pasco's media centers to a centralized mainframe at the district office by using dedicated phone lines, coaxial cabling, and wireless communications providers.

Wide Area Network –

A WAN (Wide Area Network or extended network) connects multiple LANs to one another over great geographic distances.

The speed available on a WAN varies depending on the cost of the connections (which increases with distance) and may be low.

WANs operate using routers, which can "choose" the most appropriate path for data to take to reach a network node.

The most well-known WAN is the Internet.

Wide Area Networks (WANs) connect larger geographic areas, such as Florida, the United States, or the world. Dedicated transoceanic cabling or satellite uplinks may be used to connect this type of network.

Using a WAN, schools in Florida can communicate with places like Tokyo in a matter of minutes, without paying enormous phone bills. A WAN is complicated. It uses multiplexers to connect local and metropolitan networks to global communications networks like the Internet. To users, however, a WAN will not appear to be much different than a LAN or a MAN.

Campus Area Network –

A campus network, campus area network, corporate area network or CAN is a computer network made up of an interconnection of local area networks (LANs) within a limited geographical area.

The networking equipment's (switches, routers) and transmission media (optical fiber, copper plant, Cat5 cabling etc.) are almost entirely owned by the campus tenant / owner: an enterprise, university, government etc.

College or university campus area networks often interconnect a variety of buildings, including administrative buildings, academic buildings, university libraries, campus or student centers, residence halls, gymnasiums, and other outlying structures, like conference centers, technology centers, and training institutes.

Early examples include the Stanford University Network at Stanford University, Project Athena at MIT, and the Andrew Project at Carnegie Mellon University.

Much like a university campus network, a corporate campus network serves to connect buildings. Examples of such are the networks at Googleplex and Microsoft's campus. Campus networks are normally interconnected with high speed Ethernet links operating over optical fiber such as Gigabit Ethernet and 10 Gigabit Ethernet.

Difference between LAN & WAN and the protocols used in these 2 technologies [2003]

	LAN	WAN
Definition:	LAN (Local Area Network) is a computer network covering a small geographic area, like a home, office, schools, or group of buildings.	WAN (Wide Area Network) is a computer network that covers a broad area (e.g., any network whose communications links cross metropolitan, regional, or national boundaries over a long distance

	LAN	WAN
Speed:	high speed(1000mbps)	less speed(150mbps)
Data transfer rates:	LANs have a high data transfer rate	WANs have a lower data transfer rate as compared to LANs
Example:	Network in an organization can be a LAN	Internet is a good example of a WAN
Technology:	Tend to use certain connectivity technologies, primarily Ethernet and Token Ring	WANs tend to use technology like MPLS, ATM, Frame Relay and X.25 for connectivity over the longer distances
Connection:	one LAN can be connected to other LANs over any distance via telephone lines and radio waves	Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites
Components:	layer 2 devices like switches, bridges. layer1 devices like hubs , repeaters	Layers 3 devices Routers, Multi-layer Switches and Technology specific devices like ATM or Frame-relay Switches etc.
Fault Tolerance:	LANs tend to have fewer problems associated with them, as there are a smaller amount of systems to deal with.	WANs tend to be less fault tolerant. as it consists of a large amount of systems there is a lower amount of fault tolerance.
Data Transmission Error:	Experiences fewer data transmission errors	Experiences more data transmission errors as compared to LAN
Ownership:	Typically owned, controlled, and managed by a single person or organization	WANs (like the Internet) are not owned by any one organization but rather exist under collective or distributed ownership and management over long distances
Set-up costs:	If there is a need to set-up a couple of extra devices on the network, it is not very expensive to do that	In this case since networks in remote areas have to be connected hence the set-up costs are higher. However WANs using public networks can be setup very cheaply, just software (VPN etc)

	LAN	WAN
Geographical Spread:	Have a small geographical range and do not need any leased telecommunication lines	Have a large geographical range generally spreading across boundaries and need leased telecommunication lines
Maintenance costs:	Because it covers a relatively small geographical area, LAN is easier to maintain at relatively low costs.	Maintaining WAN is difficult because of its wider geographical coverage and higher maintenance costs.
Bandwidth:	High bandwidth is available for transmission.	Low bandwidth is available for transmission
Geographical Area:	LAN covers 100 m	WAN covers more than 100 m
	LAN is more secure and less expensive to implement	WAN is less secure and more expensive to implement

Feature	LAN	WAN
Speed	1000 Mbps	150 Mbps
Bandwidth for Transmission	High	Low
Data Transfer Rate	High	Low
Geographical Coverage	Small	Large
Connecting Hardware	10Base-T Cable	Leased Line or Satellite
Technology Used	Token Ring & Ethernet	ATM, Frame Relay, X.25
Transmission Errors	Few	More
Setup Cost	Low	High
Maintenance Costs	Less	More
Network Topology	Peer to Peer	Client Server Model
Security	More Secure than WAN	Open to Threats
Standard	Ethernet	T1
Signal Deterioration	No	Yes
Equipment Needed	Hub, Switch	Router, Modem
Expansion	Using a NIC	Using an Extra Router
Range	1 km	Up to 10000 kms
Printer Sharing	Yes, if in the same LAN	No

Protocols used in LAN –

LAN protocols are distinguished by their capability to efficiently deliver data over shorter distances, such as a few hundred feet, through various mediums, such as copper cabling. Different protocols exist for different purposes and exist in different "layers" of the "Open Systems Interconnect," or OSI, model. Typically when using the word "LAN" to describe a protocol, the intent is to describe lower level, or physical, layers. Some of the most common LAN protocols are "Ethernet," "Token Ring" and "Fiber Distributed Data Interface," or "FDDI."

"Ethernet" is by far the most common type of LAN protocol. It is found in homes and offices throughout the world and is recognizable by its common "CAT5" copper cable medium. It uses a switch or hub to which all systems connect to exchange data.

"Token Ring" is an older LAN technology that is not prevalent anymore. The basic premise of "Token Ring" is a single "token" is passed from system to system, or through a hub, and only the intended recipient reads the token.

"FDDI" defines how LAN traffic is transmitted over fiber cabling. Fiber cabling is used when longer distances, usually between floors or buildings, are required, or where heightened security is required.

Protocols used in WAN –

WAN protocols are distinguished by their capability to efficiently deliver data over longer distances, such as hundreds of miles. This is generally required to bridge data between multiple LANs. The Internet is the world's largest WAN. Routers, modems and other WAN devices are used to transmit the data over various mediums, commonly fiber cabling. Some of the most common WAN protocols in use today are "Frame Relay," "X.25," "Integrated Services Digital Network," or "ISDN," and "Point-to-Point Protocol," or "PPP."

"Frame Relay" and "X.25" are similar in that they are both packet-switching technologies for sending data over large distances. "Frame Relay" is newer and faster, whereas "X.25" delivers data more reliably.

"PPP" is a protocol that is used to transmit data for other protocols over mediums that they would not normally support, such as sending the "Internet Protocol," or IP, over serial lines.

"ISDN" is a method of combining multiple dial-up lines on a public telephone network into a single data stream.

Wireless LAN Protocols –

Wireless LANs, sometimes referred to as "WLAN" or "Wi-Fi," are becoming increasingly prevalent. They operate essentially the same as a traditional LAN, but use wireless signals between antennas as the medium, rather than cabling. Most of the wireless protocols in use today are based on the 802.11 standard and are differentiated by the letter appearing after the number. The four main protocols are "802.11a," "802.11b," "802.11g" and "802.11n."

"802.11a" is designed to carry data over shorter distances at higher speeds of up to 54 megabits per second, or Mbps. "802.11b" does the opposite, operating at lower speeds of up to only 11 Mbps but with higher reliability at longer distances and with more obstructing objects in the environment.

"802.11g" combines the better of the previous two protocols, operating at up to 54 Mbps over longer distances. "802.11n" is the latest wireless protocol to be released. It can operate at speeds of greater than 150 Mbps over longer distances than the other protocols.

http://www.ehow.com/list_6905045_wan_lan-protocols.html

a. LAN [2007]
    i. Various topologies for LAN [2007, 2003]
    ii. Medias used for LAN and their choice [2007, 2004, 2003]
    iii. CSMA/CD and how Ethernet tackles it [2007,2004]
    iv. Functions of HUB, Bridge and Switch [2007, Differences-2004].
    v. Speed and Distance limitation for various media. [2004]
    vi. Address resolution in a LAN [2004, 2003]

LAN Topologies –

Network topology is the layout pattern of interconnections of the various elements (links, nodes, etc.).

Network topologies may be physical or logical.

Physical topology refers to the physical design of a network including the devices, location and cable installation.

Logical topology refers to how data is actually transferred in a network as opposed to its physical design.

In general physical topology relates to a core network whereas logical topology relates to basic network.

Basic Topologies –

- Bus
- Star
- Tree or Extended Star
- Ring or circular
- Mesh

BUS –

- Each node is connected to a single bus cable.
- A signal from the source travels in both directions to all machines connected on the bus cable until it finds the intended recipient.
- If the machine address does not match the intended address for the data, the machine ignores the data. Alternatively, if the data matches the machine address, the data is accepted.

Advantages

- Easy to connect a computer or peripheral to a linear bus.
- Requires less cable length than a star topology

Disadvantages

- Entire network shuts down if there is a break in the main cable.
- Terminators are required at both ends of the backbone cable.
- Difficult to identify the problem if the entire network shuts down.
- Not meant to be used as a stand-alone solution in a large building.

STAR –

- A star topology is designed with each node (file server, workstations, and peripherals) connected directly to a central network hub, switch, or concentrator.
- Data on a star network passes through the hub, switch, or concentrator before continuing to its destination. The hub, switch, or concentrator manages and controls all functions of the network.
- It also acts as a repeater for the data flow. This configuration is common with twisted pair cable; however, it can also be used with coaxial cable or fiber optic cable.

Advantages

- Easy to install and wire.
- No disruptions to the network when connecting or removing devices.
- Easy to detect faults and to remove parts.

Disadvantages

- Requires more cable length than a linear topology.
- If the hub, switch, or concentrator fails, nodes attached are disabled.
- More expensive than linear bus topologies because of the cost of the hubs, etc.

TREE or Expanded STAR –

- A tree topology combines characteristics of linear bus and star topologies.
- It consists of groups of star-configured workstations connected to a linear bus backbone cable.
- Tree topologies allow for the expansion of an existing network, and enable schools to configure a network to meet their needs.

Advantages

- Point-to-point wiring for individual segments.
- Supported by several hardware and software venders.

Disadvantages

- Overall length of each segment is limited by the type of cabling used.
- If the backbone line breaks, the entire segment goes down.
- More difficult to configure and wire than other topologies.

RING –

- A ring topology is a LAN architecture that consists of a series of devices connected to one another by unidirectional transmission links to form a single closed loop.

Advantages

- Very orderly network where every device has access to the token and the opportunity to transmit
- Performs better than a bus topology under heavy network load
- Does not require a central node to manage the connectivity between the computers

Disadvantages

- One malfunctioning workstation can create problems for the entire network
- Moves, adds and changes of devices can affect the network
- Communication delay is directly proportional to number of nodes in the network
- Bandwidth is shared on all links between devices

i. Medias used for LAN and their choice [2007, 2004, 2003]

Media - The pathway to send data and information between two or more entities on a network

Factors to be considered –

- Bandwidth – transmission capacity
- Attenuation – weakening of a signal over distance
- EMI – electromagnetic interference

Types –

- Copper
  - Unshielded Twisted Pair (3,5,5e,6,7)
  - Shielded Twisted Pair
  - Coaxial Cable (Thinnet, Thicknet)
- Fiber Optic
  - Single-mode
  - Multi-mode
- Infrared
- Radio & Microwave

Coaxial Cabling –

- Coaxial cable is a copper-cored cable surrounded by a heavy shielding and is used to connect computers in a network.
- Coaxial cabling is used in bus-style Ethernet networks. Coaxial cable consists of a copper wire core surrounded by a plastic cladding sheathed in a wire mesh. Coaxial cable comes in two sizes which are called thinnet and thicknet.

Unshielded Twisted Pair –

- Twisted-pair is a type of cabling that is used for telephone communications and most modern Ethernet networks.
- A pair of wires forms a circuit that can transmit data. The pairs are twisted to provide protection against crosstalk, the noise generated by adjacent pairs.
- There are two basic types, shielded twisted-pair (STP) and unshielded twisted-pair (UTP).
- Two pairs of wires, one for transmit, and one for receive, each of the pair twisted and placed close to each other.
- There are several grades of coaxial cable with category ratings. There are Category 3 (<10 Mbps), Category 5 (10 Mbps), Category 5e (10/100 Mbps) and Category 6 (100/1000 Mbps) versions of unshielded twisted pair.

Fiber Optic –

- Fiber-optic cable consists of light conducting glass or plastic core, surrounded by more outer glass called 'cladding' & a tough outer sheath / jacket.
- Data is carried over this light conducting glass / plastic core in form of modulated light pulses.
- Signals that represent data are converted into beams of light.

Radio & Microwave –

- If the cost of running cables is too high or computers need to be movable without being tethered to cables, wireless is an alternative method of connecting a LAN.
- Wireless networks use Infrared (IR), Radio frequency (RF) & satellite/microwaves to carry signals from one computer to another without a permanent cable connection. These are now being put to use in wireless Ethernet and Bluetooth communications technologies.

i. CSMA/CD and how Ethernet tackles it [2007,2004]

In the past, we had networks that contained devices called hubs. These hubs created what we called a shared network. That means each computer that communicated in the network had equal access to the same electrical paths as the others. Since the paths could carry only one communication at a time, the computers had to "take turns" accessing the wire.

A protocol called Carrier Sense Multiple Access with Collision Detection (CSMA/CD) was developed for this purpose.

Carrier Sense Multiple Access/ Collision Detection (CSMA/CD) is a method that allows only one station to transmit at a time. This means a host or PC before sending any data first looks up for any collision in network and if there is no collision then PCs starts sending the data.

Simply put, a host or PC before sending a data checks whether there is any one already sending some data. If someone is doing so, the host or PC waits to get the channel to free up for transmission.

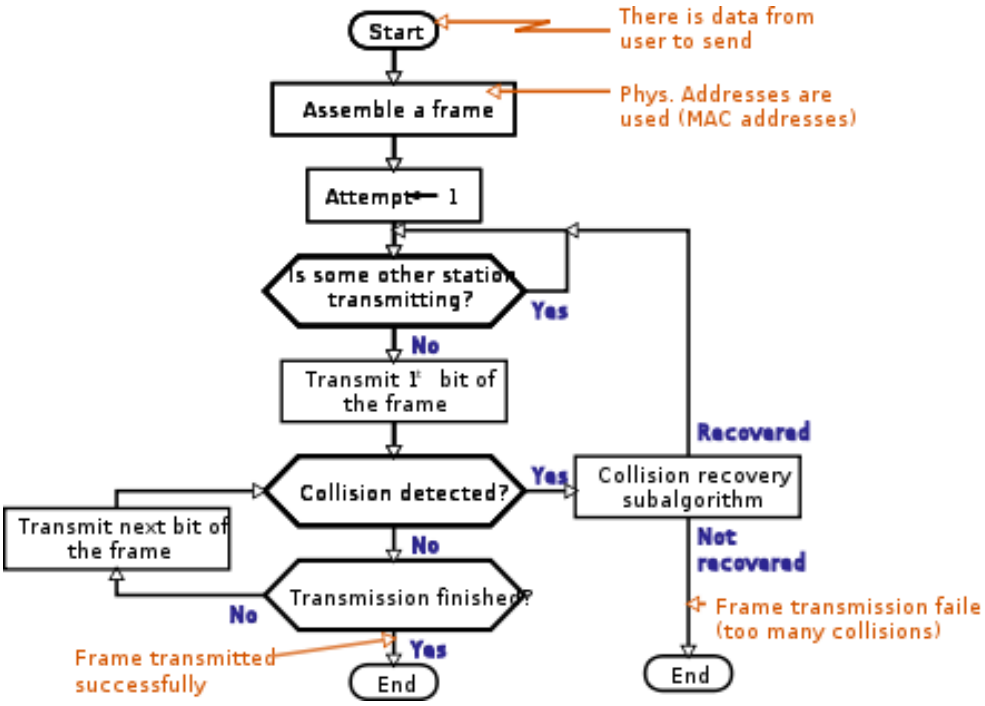
Carrier sense multiple access with collision detection (CSMA/CD) is a Media Access Control method in which –

- A carrier sensing scheme is used.

- A transmitting data station that detects another signal while transmitting a frame, stops transmitting that frame, transmits a jam signal, and then waits for a random time interval before trying to resend the frame.
- The jam signal is a signal that carries a 32-bit binary pattern sent by a data station to inform the other stations that they must not transmit.

CSMA/CD is modification of pure carrier sense multiple access (CSMA). CSMA/CD is used to improve CSMA performance by terminating transmission as soon as a collision is detected, thus shortening the time required before a retry can be attempted.

This can be likened to what happens at a dinner party, where all the guests talk to each other through a common medium (the air). Before speaking, each guest politely waits for the current speaker to finish. If two guests start speaking at the same time, both stop and wait for short, random periods of time (in Ethernet, this time is measured in microseconds). The hope is that by each choosing a random period of time, both guests will not choose the same time to try to speak again, thus avoiding another collision.



Main procedure

1. Is my frame ready for transmission? If yes, it goes on to the next point.
2. Is medium idle? If not, wait until it becomes ready[note 1]
3. Start transmitting.
4. Did a collision occur? If so, go to collision detected procedure.
5. Reset retransmission counters and end frame transmission.

Collision detected procedure

1. Continue transmission until minimum packet time is reached to ensure that all receivers detect the collision.
2. Increment retransmission counter.
3. Was the maximum number of transmission attempts reached? If so, abort transmission.

4. Calculate and wait random backoff period based on number of collisions.
5. Re-enter main procedure at stage 1.

ii. Functions of HUB, Bridge and Switch [2007, Differences-2004]

Already Discussed

iii. Speed and Distance limitation for various media [2004]

Types	Transmission Media	Speed	Distance
Ethernet	Copper (first coax then twisted-pair)	10Mbps	100m
10BaseT	Twisted-pair copper	10Mbps	100m
100BaseTX	Twisted-pair copper	100Mbps	100m
100BaseFX	Multimode fiber	100Mbps	400m
1000BaseT	Multimode fiber	1Gbps	100m
1000BaseX		1Gbps	Overall standard for 1Gbps on fiber and copper
10GBaseSR	Multimode fiber	10Gbps	26m
10GBaseLR	Single-mode fiber	10Gbps	25km (about 16 miles)
10GBaseER	Single-mode fiber	10Gbps	40km (about 25 miles)
10GBaseSW	Multimode fiber	10Gbps	26m
10GBaseLW	Single-mode fiber	10Gbps	10km
10GBaseEW	Single-mode fiber	10Gbps	40km
10GBaseT	Twisted-pair cable	10Gbps	100m

http://my.safaribooksonline.com/book/certification/networkplus/9780470430996/domain-2-network-media-and-topologies/categorize_lan_technology_types_and_p

iv. Address resolution in a LAN [2004, 2003]

Address Resolution Protocol (ARP) is a telecommunications protocol used for resolution of network layer addresses into link layer addresses, a critical function in multiple-access networks i.e. to map IP network addresses to the hardware addresses used by a data link protocol.

ARP is a request and reply. It is communicated within the boundaries of a single network, never routed across internetwork nodes.

The term address resolution refers to the process of finding an address of a computer in a network. The address is "resolved" using a protocol in which a piece of information is sent by a client process executing on the local computer to a server process executing on a remote computer. The information received by the server allows the server to uniquely identify and provide the required address. The address resolution

procedure is completed when the client receives a response from the server containing the required address.

The Ethernet address is a link layer address and is dependent on the interface card which is used. IP operates at the network layer and is not concerned with the link addresses of individual nodes which are to be used. ARP is therefore used to translate between these two types of address. The ARP client and server processes operate on all computers using IP over Ethernet. The processes are normally implemented as part of the software driver that drives the network interface card.

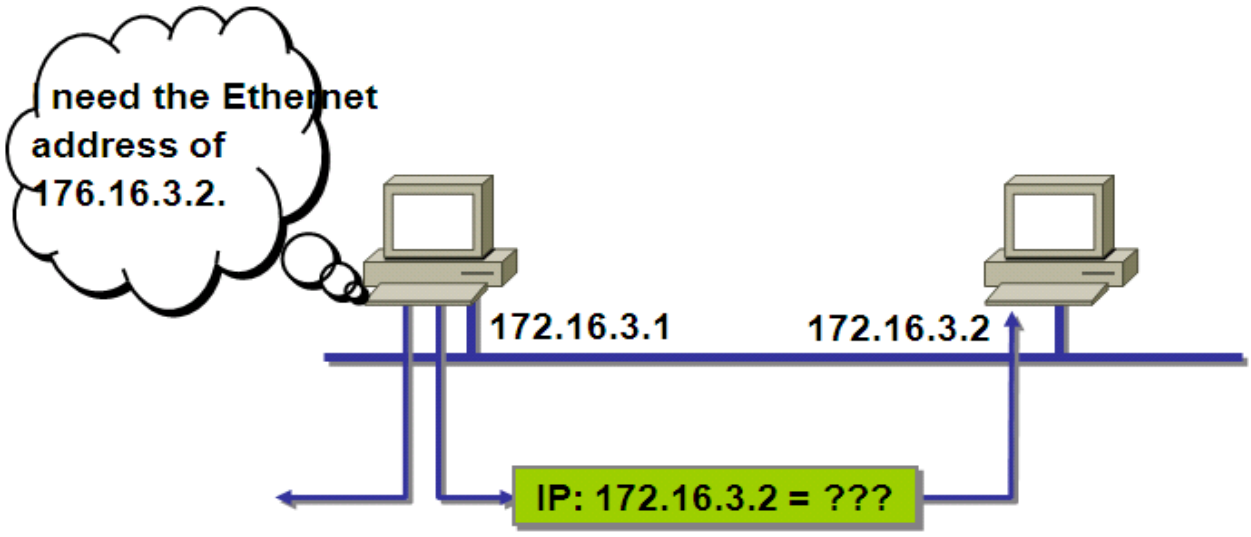
There are four types of ARP messages that may be sent by the ARP protocol. These are identified by four values in the "operation" field of an ARP message. The types of message are –

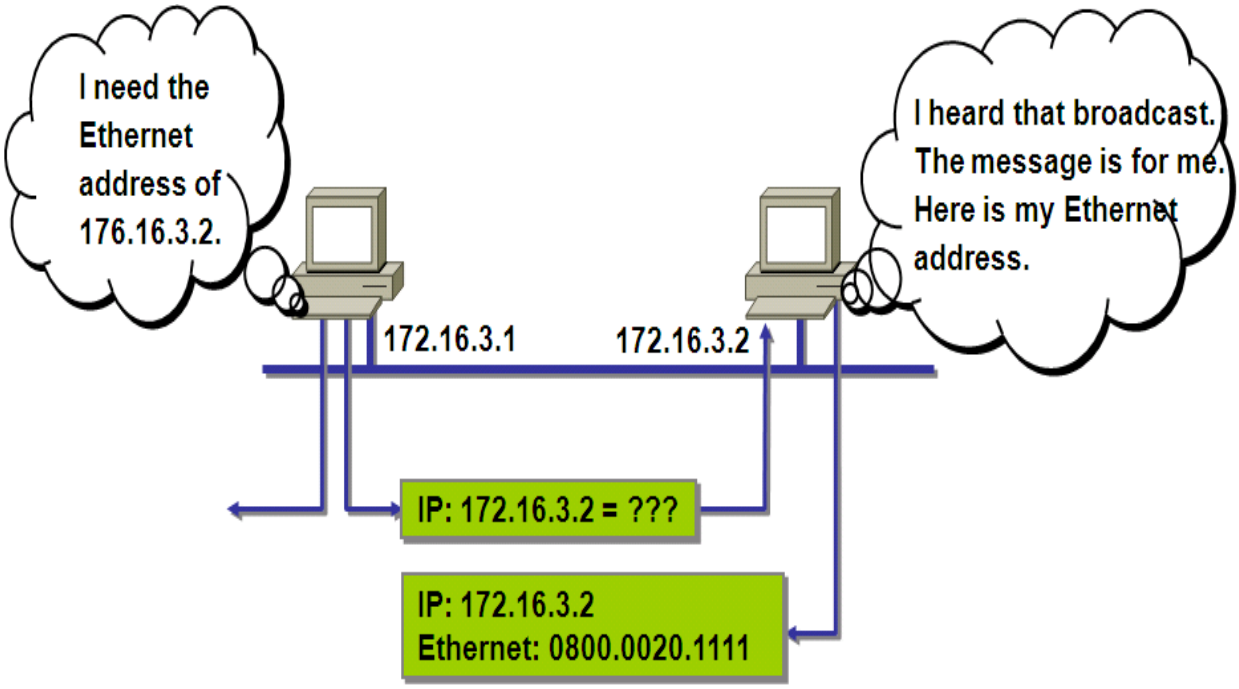
- ARP request
- ARP reply
- RARP request
- RARP reply

The ARP request message ("who is X.X.X.X tell Y.Y.Y.Y", where X.X.X.X and Y.Y.Y.Y are IP addresses) is sent using the Ethernet broadcast address, and an Ethernet protocol type of value 0x806 i.e. Y.Y.Y.Y & 0X806 are IP-Add and MAC of the Requestor, asking on the network “Who is Y.Y.Y.Y, I need your MAC”. Since it is broadcast, it is received by all systems in the same collision domain (LAN). This ensures that if the target of the query is connected to the network, it will receive a copy of the query. Only this system responds. The other systems discard the packet silently.

The target system forms an ARP response ("X.X.X.X is hh:hh:hh:hh:hh:hh", i.e. I’m X.X.X.X and my MAC is hh:hh:hh:hh:hh:hh). This packet is unicast to the address of the source computer sending the query (in this case Y.Y.Y.Y). Since the original request also included the hardware address (Ethernet source address – 0x806) of the requesting computer, this is already known, and doesn't require another ARP message to find this out.

http://www.erg.abdn.ac.uk/~gorry/eg3561/inet-pages/arp.html




I need the Ethernet address of 176.16.3.2.
I heard that broadcast. The message is for me. Here is my Ethernet address.
172.16.3.1
172.16.3.2
IP: 172.16.3.2 = ???
IP: 172.16.3.2
Ethernet: 0800.0020.1111

b. WAN [2007]

ii. Various alternatives for connectivity between locations [2007, 2004]

Option	Description	Advantages	Disadvantages	Sample Protocols
Leased Line	Point-to-point connection between two computers LANs	Most Secure	Expensive	PPP, HDLC, SDLC
Circuit Switching	A dedicated circuit path is created between endpoints. Best example is dialup connections	Less expensive	Call Setup	PPP, ISDN
Packet Switch	Devices transport packets via a shared single point-to-point or point-to-multipoint link across. Variable length packets are transmitted over PVCs or SVCs	Highly efficient use of bandwidth	Shared media across link	X.25, Frame Relay
Cell Relay	Similar to packet switching, but uses fixed-length packets. Data is divided into fixed length cells and then transported across virtual circuits	Best for simultaneous use of voice and data	Overhead can be considerable	ATM
Internet	Connectionless packet switching using the internet as the WAN infrastructure. Uses network addressing to deliver packets. Because of security issues VPN technology must be used.	Least expensive, globally available	Lea	

http://ciscoskills.net/2011/10/19/types-of-wan-links/

Leased Line - It is the most expensive of all types and also the most secure. It uses a point to point connection from the WAN hub to the specific LAN point. This option is used by most big software corporations as not only does it offer superior security features but also higher data transfer rate. It uses the PPP(Point to point protocol), the HNAS, the HDLC or SDLC protocol. They are all specialized protocol mechanisms designed for security and error-free operation.

Circuit Switching - These are relatively cheaper connections and rely on making a physical circuit path between two points. The dial up connection is examples of such type. They use the landline telephone infrastructure for data transmission. The speed offered is usually 30 Kbps to 150 Kbps. The protocols used are PPP or ISDN.

Packet Switching - They use dynamic circuit paths with single point to multiple point linking. The data is sliced into variable sized packets irrespective of its type. Varying types of data use the same media link and therefore there is congestion and queuing delays in delivery. It uses the X.25 Frame relay protocol which is one of the first protocols ever developed.

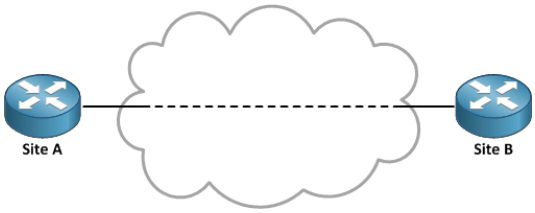
Cell Relay - This is quite similar in structure to packet switching type but divides data into equally sized packets or cells. It is supposed to be very efficient for synchronous voice and video transmission and gives amazing clarity. It uses the ATM (Asynchronous Transfer mode) protocol.

http://wiki.answers.com/Q/What_are_the_types_of_WAN_connections

iii. Choice of topologies [2007, 2004]

1. Point to Point
2. Point to Multipoint
3. Multipoint to Multipoint
4. Metro Ethernet
5. MPLS VPN

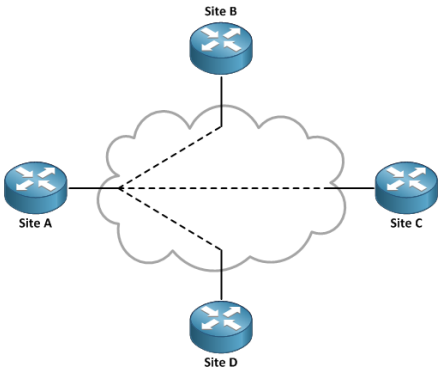
Point-to-Point –



A point-to-point circuit, as its name implies, connects exactly two points. This is the simplest type of WAN circuit. Packets sent from one site are delivered to the other and vice versa. There is typically some amount of processing and encapsulation performed across the carrier's infrastructure, but it is all transparent to the customer.

A point-to-point circuit is typically delivered as a layer two transport service, which allows the customer to run whatever layer three protocols they want with an arbitrary addressing scheme. A customer can change or add an IP subnet in use on a layer two circuit without coordinating with their provider.

Point-to-Multipoint

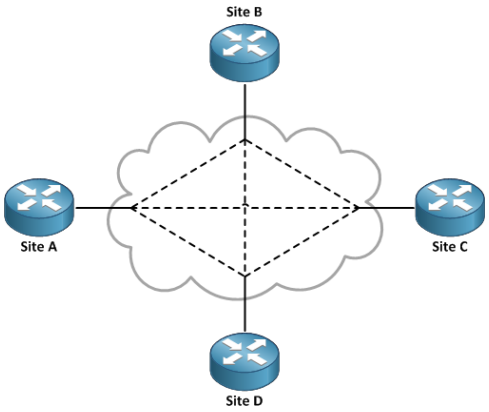


The primary detractor of point-to-point circuits is that they don't scale efficiently. Suppose you wanted to deploy a hub-and-spoke style WAN topology with twenty branch sites connecting to a single main office. You could deploy twenty point-to-point circuits, one to each spoke site from the hub, but that would result in a clutter of twenty separate physical connections at the hub site. Installing twenty circuits would be

rather expensive, and you might not even be able to fit them all on the same device. This is where a point-to-multipoint circuit would be ideal.

With a point-to-multipoint circuit, we only need a single circuit to the hub site to be shared by all spoke circuits. Each spoke is assigned a unique tag which identifies its traffic across the hub circuit. The type of tagging is medium-dependent; we'll use an Ethernet circuit with IEEE 802.1Q VLAN trunking as an example. (The spoke circuits may have their traffic tagged or untagged, depending on the specific carrier's service parameters.) Each spoke gets a virtual circuit and routed subinterface on the hub circuit. The resulting layer three topology is the same as using several point-to-point circuits but is more practical in implementation.

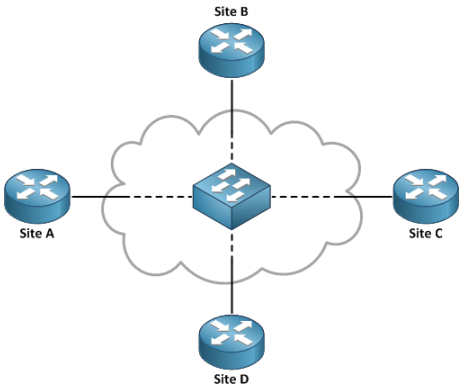
Multipoint-to-Multipoint



While more efficient than a tree of point-to-point circuits, the major drawback of a point-to-multipoint circuit is that spoke-to-spoke traffic must traverse the hub site. This isn't a problem if the spoke sites never need to talk to one another, but can quickly lead to problems if users at one spoke site need to access resources at another.

The logical evolution of the topology may be to expand to a multipoint-to-multipoint design, in which all sites are effectively hub sites. Each site is configured with a virtual circuit to each of the other sites, forming a full mesh of virtual point-to-point circuits across the WAN. But as you can see, multipoint-to-multipoint is hindered by the same scaling limitations as point-to-point: For n sites, n(n-1)/2 virtual circuits are necessary to form a full mesh. Although the number of physical circuits grows linearly as sites are added, the administrative effort to maintain so many virtual circuits can be a nightmare.

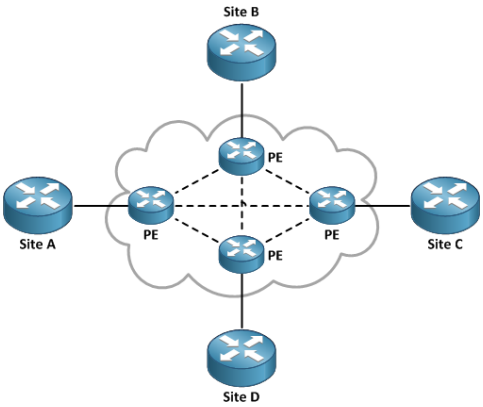
Metro Ethernet



Metro Ethernet is a layer two metropolitan area network (MAN) service which simplifies the WAN topology greatly by effectively emulating one big LAN switch spanning an entire metro area. All sites connected into the metro Ethernet cloud are placed into a single multi-access segment. This allows each site to communicate directly across the carrier's infrastructure with any other site.

The catch here is that, as its name implies, metro Ethernet is typically limited to within a single geographic area. One could not, for example, order metro Ethernet connectivity among Los Angeles, Dallas, and New York. Its multi-access nature also introduces design considerations pertaining to the mapping of routing protocol adjacencies that should not be overlooked.

MPLS VPN



Unlike the previous classes, MPLS VPN is a layer three WAN technology. It can be delivered over any layer two transport which supports IP. A point-to-point circuit is installed between the customer site and the MPLS provider's nearest point of presence. A dynamic routing protocol such as OSPF or BGP is run between the customer edge (CE) and the provider edge (PE) routers to exchange routing information which then is propagated to the other sites within the MPLS VPN.

MPLS is a great choice for WAN connectivity because it offers national and international reach, high redundancy (through the carrier's multipath routed infrastructure), and linear scaling. Another important benefit is that MPLS removes the need to maintain a full mesh of routing adjacencies, which is of particular concern when using BGP. Rather than forming a mesh of adjacencies among all site routers, each site router needs only to peer with the provider and the provider handles all inter-site routing across its infrastructure.

The term MPLS can lead to confusion, because MPLS is only run across the carriers infrastructure (the P and PE routers), not on the customer's actual circuit. It is referred to as an MPLS VPN (as opposed to just MPLS) because the customer's network is implemented as a distinct VPN among many others belonging to the carrier's other customers.

http://packetlife.net/blog/2013/feb/6/wan-circuit-topologies/

iv. Routing protocols and their selection [2007, 2004]

WAN Protocols –

Frame Relay	A packet switching technology that emerged in the early 1990's. Frame Relay is a Date Link and Physical Layer specification that provides high performance. Frame Relay assumes that the facilities used are less error prone than when X.25 was being implemented and that they use less overhead. Frame Relay is more cost-effective than point-to-point links and can run at speeds of 64Kbps to 45Mbps. Frame Relay provides features for dynamic-bandwidth allocation and congestion control.
X.25	ITU-T standard that defines how connections between DTE and DCE are maintained for remote terminal access and computer communications in PDNs(Public Data Networks). X.25 specifies LAPB, a data link layer protocol, and PLP, a network layer protocol. Frame Relay has to some degree superseded X.25.
ISDN	Integrated Services Digital Network is a set of digital services that transmit voice and data over existing phone lines. ISDN can offer a cost-effective solution for remote users who need a higher-speed connection than what an analog dial-up link offers. ISDN is also a good choice as a backup link for other types of links such as Frame Relay or a T-1 connection.
LAPB	Link Access Procedure Balanced was created to be used as a connection-oriented protocol at the Data Link layer for use with X.25. It can also be used as a simple Data Link transport. LAPB has a tremendous amount of overhead because of its strict timeout and windowing techniques. You can use LAPB instead of the lower-overhead HDLC if your links are very error prone. However, that typically is not a problem anymore.
HDLC	High-Level Data Link Control was derived from Synchronous Data Link Control (SDLC), which was created by IBM as a Data Link connection protocol. HDLC is a connection-oriented protocol at the Data Link layer, but it has very little overhead compared to LAPB. HDLC was not intended to encapsulate multiple Network layer protocols across the same link. The HDLC header carries no identification of the type of protocol being carried inside the HDLC encapsulation. Because of this, each vendor that uses HDLC has their own way of identifying the Network layer protocol, which means that each vendor's HDLC is proprietary for their equipment.
SDLC	Synchronous Data Link Control. SNA data link layer communications protocol. SDLC is a bit-oriented, full-duplex serial protocol that has spawned numerous protocols, including HDLC and LAPB.
PPP	Point-to-Point protocol is an industry standard protocol. Because many versions of HDLC are proprietary, PPP can be used to create point-to-point links between different vendor's equipment. It uses a Network Control Protocol field in the Data Link header to identify the Network layer protocol. It allows authentication and multilink connections and can be run over asynchronous and synchronous links.

v. Performance criterion for WAN [2007]

http://my.safaribooksonline.com/book/networking/ip/157870071x/routers-and-wans/ch04lev1sec2

Having reviewed some of the various ways to construct networks using routers, it is also important to establish some criteria for measuring the efficacy of your network. Many different criteria, or metrics, can be applied. Some of these are fairly objective and can be automatically extracted from the network monitoring protocols native to virtually every network device. Others are subjective and can be next to impossible to determine in advance. Some of the more common metrics include the following:

- Component uptime
- Traffic volumes
- Delay
- Resource utilization rates

18. Describe following architectures with examples: [2010]
    a. Client-Server [Advantages & Disadvantages-2006 (10 marks)]
    b. Net-Centric
    c. Web-Centric

The **client/server model** is a computing model that acts as distributed application which partitions tasks or workloads between the providers of a resource or service, called servers, and service requesters, called clients.[1] Often clients and servers communicate over a computer network on separate hardware, but both client and server may reside in the same system. A server machine is a host that is running one or more server programs which share their resources with clients. A client does not share any of its resources, but requests a server's content or service function. Clients therefore initiate communication sessions with servers which await incoming requests.

Schematic clients-server interaction.

The *client/server* characteristic describes the relationship of cooperating programs in an application. The server component provides a function or service to one or many clients, which initiate requests for such services.

Functions such as email exchange, web access and database access are built on the client/server model. Users accessing banking services from their computer use a web browser client to send a request to a web server at a bank. That program may in turn forward the request to its own database client program, which sends a request to a database server at another bank computer to retrieve the account information. The balance is returned to the bank database client, which in turn serves it back to the web browser client, displaying the results to the user. The client–server model has become one of the central ideas of network computing. Many business applications being written today use the client–server model, as do the Internet's main application protocols, such as HTTP, SMTP, Telnet, and DNS.

The interaction between client and server is often described using sequence diagrams. The Unified Modeling Language has support for sequence diagrams.

Specific types of clients include web browsers, email clients, and online chat clients.

Specific types of servers include web servers, ftp servers, application servers, database servers, name servers, mail servers, file servers, print servers, and terminal servers. Most web services are also types of servers.

Comparison to peer-to-peer architecture

A client/server network involves multiple clients connecting to a single, central server. The file server on a client/server network is a high capacity, high speed computer with a large hard disk capacity.

By contrast, peer-to-peer networks involve two or more computers pooling individual resources such as disk drives, CD-ROMs and printers. These shared resources are available to every computer in the network, while each of them communicates in a session. Each computer acts as both the client and the server which means all the computers on the network are equals, that is where the term peer-to-peer comes from. The advantage of peer-to-peer networking is the easier control concept not requiring any additional coordination entity and not delaying transfers by routing via server entities. However, the collision of session may be larger than with routing via server nodes.

In the peer to peer network, software applications can be installed on the single computer and shared by every computer in the network. They are also cheaper to set up because most desktop operating systems have the software required for the network installed by default. On the other hand, the client/server model works with any size or physical layout of LAN and doesn't tend to slow down with a heavy use.

Peer-to-peer networks are typically less secure than a client/server networks because security is handled by the individual computers, not controlled and supervised on the network as a whole. The resources of the computers in the network can become congested as they have to support not only the workstation user, but also the requests from network users. It may be difficult to provide system wide services when the client operating system typically used in this type of network is incapable of hosting the service.

Client/server networks with their additional capacities have a higher initial setup cost for networking than peer to peer networks. The long-term aspect of administering a client/server network with applications largely server-hosted surely saves administering effort compared to administering the application settings per each client. In addition the concentration of functions in performing servers allows for lower grade performance qualification of the clients.

It is possible to set up a server on a modern desktop computer, but it is recommended to consider investment in enterprise-wide server facilities with standardised choice of hardware and software and with a systematic and remotely operable administering strategy. It is easier to configure and manage the server hardware and software compared to the distributed administering requirements with a flock of computers

Challenges

Generally a server may be challenged beyond its capabilities. Then a single server may cause a bottleneck or constraints problem. However, servers may be cloned and networked to fulfill all known capacity and performance requirements. Limitations include network load, network address volume, and transaction recovery time.

Aspects of comparison for other architectural concepts today include cloud computing as well. Possible design decision considerations might be:

- As soon as the total number of simultaneous client requests to a given server increases, the server can become overloaded. Contrast that to a P2P network, where its aggregated bandwidth actually increases as nodes are added, since the P2P network's overall bandwidth can be roughly computed as the sum of the bandwidths of every node in that network. However, this simple model ends with the **bandwidth of the network**: Then congestion comes on the network and not with the peers.

- Any single entity paradigm lacks the robustness of a redundant configuration. Under client–server, should a critical server fail, clients' requests cannot be fulfilled by this very entity, but may be taken by another server, as long as required data is accessible. In P2P networks, resources are usually distributed among many nodes which generate as many locations to fail. If dynamic re-routing is established, even if one or more nodes depart and abandon a downloading file, for example, the remaining nodes should still have the data needed to complete the download.

- Mainframe networks use dumb terminals. All processing is completed on few central computers. This is a method of running a network with different limitations compared to fully fashioned clients.

- Using intelligent client terminals increases the maintenance and repair effort. Lesser complete netbook clients allow for reduction of hardware entities that have limited life cycles.

Net-Centric:

Net-centric or **netcentric** refers to participating as a part of a continuously-evolving, complex community of people, devices, information and services interconnected by a communications network to achieve optimal benefit of resources and better synchronization of events and their consequences.

In military connotation frequently associated with terms "Net-centric Operations (NCO)" and "Net-centric Warfare (NCW)". Many people use the terms "net-centric" and "network-centric" interchangeably. Some consider "network-centric" to refer to activities within a particular network and "net-centric" to refer to activities that cross networks.

Many experts believe the terms "information-centric" or "knowledge-centric" would capture the concepts more aptly because the objective is to find and exploit information, the network itself is only one of several enabling factors

Netcentric, or "network-centric", refers to participating as a part of a continuously-evolving, complex community of people, devices, information and services interconnected by a communications network to optimize resource management and provide superior information on events and conditions needed to empower decision makers. Many experts believe the terms "information-centric" or "knowledge-centric" would capture the concepts more aptly because the objective is to find and exploit information, the network itself is only one of several enabling factors along with sensors, data processing and storage, expert analysis systems and intelligent agents, and information distribution. The best commercial practitioners of globally distributed supply chain management and customer relationship management employ net-centric methods. Network Centric Product Support (NCPS) is a specific example of the netcentric architecture that is being applied to a range of applications including the NextGen airtraffic control as well as other transportation applications. Netcentric warfare is also a tenet of modern information warfare concepts.

A Net-centric Enterprise Architecture is defined in lay terms as a: "massively distributed architecture with components and/or services available across and throughout an enterprise's entire lines-of-business."

The formal definition of a "NetCentric Enterprise Architecture" is: "A NetCentric Enterprise Architecture is a light-weight, massively distributed, horizontally-applied architecture, that distributes components and/or services across an enterprise's information value chain using Internet Technologies and other NetworkProtocols as the principal mechanism for supporting the distribution and processing of information services."

Net Centric Computing

Recent advances in computer and telecommunications networking, particularly those based on TCP/IP, have increased the importance of networking technologies in the computing discipline. Net-centric computing covers a range of sub-specialties including: computer communication network concepts and protocols, multimedia systems, Web standards and technologies, network security, wireless and mobile computing, and distributed systems.

Mastery of this subject area involves both theory and practice. Learning experiences that involve hands-on experimentation and analysis are strongly recommended as they reinforce student understanding of concepts and their application to real-world problems. Laboratory experiments should involve data collection and synthesis, empirical modelling, protocol analysis at the source code level, network packet monitoring, software construction, and evaluation of alternative design model

The underlying principle of Net-Centric Computing (NCC) is a distributed environment where applications and data are downloaded from servers and exchanged with peers across a network on as as-needed basis. NCC is an on-going area of interest to a wide-variety of software engineering researchers and practitioners, in part because it is an enabling technology for modern distributed systems (e.g., Web applications). As such, knowledge of NCC is essential requirement in architecting,constructing,and evolving the complex software systems that power today's enterprizes.The widespread interest in Ubiquitous and Pervasive Computing systems will give a new impulse to Net-Centric Computing (NCC) systems. Solutions such as OSGi have the capability to become the foundation of a new middleware for NCC systems and offer the possibility to browse the physical world in the same way as the web content is browsed. The activities for Net-Centric Technology consist of three Layers.

The Information Service Layer pertains to the abstraction of objects. The focus here is on the quality, security, auditability and control.–

The Network Service Layer pertains to all aspects of communications, particularly configuration, fault management, security, performance and accounting, The Component Control Layer pertains to the development, acquisition and implementation of components that form the infrastructure or distributed. For several years, business and technology observers have been talking about the major changes being brought by universal networking capabilities,such as the Internet. Today's technology solutions are what we can call "convergence" solutions: They represent the convergence of computing power, communications capability and content the information, data or knowledge that forms the "stuff" of the solution. At the heart of the solution, however, is the network hence, network-centric, or "netcentric,"solutions. Net-centric computing refers to an emerging technology architecture and an evolutionary stage of client/server computing. The common architecture of netcentric computing supports access to information through multiple electronic channels (personal and network computers,cell phones, kiosks, telephones, etc.). This information is made accessible to many more users not just an organization's workforce but also its customers, suppliers and business partners through technology

ies that employ open, commonly accepted standards (Internet, Java, Web browsers and so forth).

WEB CENTRIC

++++++++++++++++++

The power to influence has shifted to the web. The web provides access to more information from more sources than ever before and people are drawn to it when they need answers. They bounce from site to site and source to source looking for information, advice, and opinions. It's convenient. It's open 24x7. And it allows people to engage in conversations about what matters to them.

As the central location for information, the web has revolutionized how our prospects and customers find, gather, and digest information, how they engage with our brand, and how they make buying decisions. It's become the most influential and visited communications channel ever built.

Leverage the web to drive action.

Your prospects and customers are spending a great deal of time on the web. Their web-centric behavior gives you the opportunity to be seen and to influence them on a regular basis. To capitalize on this behavior, the web must be at the core of your marketing and communications strategy. We call this Web-centric Marketing.

Web-centric Marketing focuses on how best to use the web to support and reach your business goals. Your plan should:

- Identify all online sources, or influencers, your audiences might visit.
- Specify how you'll utilize your site, as well as the other online sources you've identified, to help you achieve your goals and influence your buyer.
- Specify how you will incorporate the web into all your outreach efforts.

Act web-centric.

1. Widen your circle of influence.

With the explosion of blogs, social networking, and user-generated content, your web site is no longer the most influential source of information for your buyer. Today your buyer has immediate access to an incredible amount of unbiased information developed by other "industry experts". You need to create a presence on the sites they go to for information.

- Find out where they do their research and where they look for answers.
- Hunt down sites that offer up the latest opinions and news related to the products, services, or issues you focus on.
- Create a presence on those sites through advertising, sponsorships, and articles. The key is to be where your prospects are when they're looking for insight.

2. Look for ways to push your content to other sites.

Don't limit your content, or your knowledge, to just your site.

- Push out your webinars, podcasts, and white papers.
- Publish articles on industry sites or in industry eNewsletters.
- Collaborate with others on joint webinars or podcasts.

Having your content and your opinions on other sites gives you outside validation and added credibility. It's another opportunity to get in front of your prospects and influence their thinking.

3. Everybody's talking and your prospects are listening.

IT decision makers spend more time each week reading or interacting with social media than they do with editorial content or vendor-produced content.[1]

Prospects trust user-generated content more than vendor content because they see it as more objective.

So get objective sources talking about you.

- Start by identifying peer-to-peer and community sites where your prospects go for opinions.
- Track down the most commonly visited blogs related to your product or services. Get them to blog about you.
- Join in the conversation yourself by sharing your insights and knowledge. Avoid anything that looks like you're trying to "sell" them.

4. Start a conversation with your prospects.

It's not just about having others talk about you; you need to get the conversation started on your site too. Your prospects are actively engaged in, or reading, multiple conversations on the web. They expect to be able to engage in conversations with you too (or at least feel you are open to what they have to say).

- Allow visitors to vote on the most helpful white paper, webinar, or article on your site, then bubble that content up for others to see.
- Create polls related to industry issues and publish the results.
- Create your own corporate blog where experts in your company share their thoughts and arrange for other experts to join in the discussion.

Send the message that you care about what your customers think and that you're not afraid to let everyone know how they feel. Companies that provide insights and relevant content visitors benefit from are seen as more transparent and as thought leaders to be respected.

5. Engage with rich media.

In addition to providing a multitude of information from a variety of sources, the web also allows companies to serve up content in a variety of formats.

When surveyed, 78% of regular web users felt online video made content more compelling and valuable. 84% said online video enhances technology related content, while 57% said it impacts their purchasing decision.[2]

Flash animation, video, podcasts, and webcasts offer more dynamic, richer experiences that help engage your visitor and impact their buying decisions.

- Create short (1 - 2 minute) overviews of your areas of expertise.
- Create a customer case study video library.
- Walk visitors through product demos or technical deep dives.

6. Think web-centric in off-line channels too.

It's not all about the web. Traditional marketing channels are still alive and kicking. Offline marketing such as magazine advertisements, direct mail, seminars, or tradeshows increased online activity.

80% of technology buyers said offline marketing materials "frequently" or "often" drove them to specific sites for more information.[3]

Look for ways to extend the off-line experience online.

- Drive prospects to targeted landing pages or microsites for more information.
- Offer up free online assessments, or ROI tools to help prospects better evaluate your offerings.
- Hold a webinar or live chat session with your product experts to answer prospects' questions.

It's the combination of pushing people to your web site from multiple channels, both offline and online, that seems to be working best.

Use the web to gain a competitive edge.

It's a web-centric world. As the central location for finding information, the web is changing how we engage with our prospects and how they learn about us and what we have to offer. Our prospects and customers are spending a great deal of their day on the web and that's a great opportunity for us to reach out to them.

For B2B marketers to be successful at generating awareness, building brands, and driving sales, they must find ways to leverage this web-centric world to their advantage. Marketers who understand and capitalize on this behaviour will have a competitive edge over those who don't.

Web-Centric Approach

Our web-centric approach helps you take advantage of the marketing realities that exist today - that every brand interaction you have with a buyer leads to an online interaction. And it's those online interactions that give you the best opportunity to really connect with buyers everywhere they are and keep them jazzed up about you.

The real power of web-centric marketing is that it connects your brand with your buyers on their terms "the way they prefer" anywhere and at any time.

- If buyers start with search engines, your brand will top your competitors.
- If buyers want to check out the social media channels, your brand will be part of the conversation in blogs, tweets and on social networks.
- If buyers go directly to your website, your site will be ready to deliver an awesome brand experience and start relationships that lead to sales.
- And since buyers are going mobile, your site will be optimized to deliver spot-on content for any platform or screen size.

Introduction.

For innovative companies that have transitioned from a primarily traditional marketing approach to a web-centric strategy, the impact on marketing productivity has been similar to the impact that the assembly line had on manufacturing productivity a century ago.

For companies that haven't yet ventured beyond the basic website stage or haven't developed a clear web-centric strategy for integrating and automating their marketing and sales processes, competition has never seemed greater and new customers have never been more difficult or expensive to find.

Just how pervasive is this transition to web-centricity among today's marketers?

With breathtaking speed, the Internet is becoming the environment in which virtually all business development activity is taking place. This white paper will help explain what a web-centric strategy is, and provide insights for a smooth and timely transition to it.

What does a web-centric strategy do?

A web-centric strategy streamlines marketing and sales processes, and leverages the Internet's extensive technological capabilities to acquire customers faster and retain them longer. A web-centric strategy does not replace traditional marketing communications tactics and sales channels – it makes them dramatically more productive.

Web-centric Strategy Overview

A company's website has become the primary point of contact with prospective customers. And the Internet has proven to be an efficient platform for integrating and automating virtually every marketing and sales process. As a result, the role of the web has been elevated from simply a spoke in the marketing mix wheel to being the hub of the marketing strategy.

The hub of a web-centric strategy typically includes the following components:

Website.

Segments users, tracks their online activity and captures lead data.

Delivers high customer value information, tools and services.

Web Portals.

Login accessible portals with the information, tools and services required to support key customer and channel partner relationships.

Systematic Marketing

A secure marketing and sales portal for the management of contact data, campaigns, web content and analytics.

Web Portals

Systematic Marketing Solutions

Direct Marketing

End Users Public Relations

Advertising Trade Shows

Resellers & Dealers Distributors

Sales Force

Website for a Web-centric Strategy

What's makes a website designed for a web-centric strategy different?

Segment, track and capture leads. A core objective of a website designed for the web-centric marketing strategy is to segment, track and capture leads. The segmentation process begins by funneling prospective customers to areas of relevant information

Relevant information refers, for example, to presenting only those products and services that align with the prospect's application and are available in their region. The segmentation process has three important purposes: It streamlines the gathering of purchase decision information for the prospect, it demonstrates a value-added specialization in the prospect's application, and it enables your website to automatically recognize and present the prospect with segment-specific information when they return.

Once segmented, the prospect's online activity can be tracked to reveal areas of interest, product requirements, their stage in the buying process and other qualifying characteristics and marketing information. This segmentation and qualification data is, at this point, associated with an anonymous prospect.

Capturing contact information related to a website lead is one of the most important objectives of a web-centric strategy, and results in identifying a previously anonymous prospect that is already associated with segmentation and qualification data.

The prospect's motivation for providing their contact data is to obtain high value information, tools and services from your website. Deliver high customer value content.

This objective requires a deep understanding of what information and tools will be valued most by a prospect, and delivering them in alignment with the prospect's buying process. In terms of information, more is not necessarily better. Better is better, so strive to provide the best information, organized

logically. Time-saving online tools that will help a prospect make an educated buying decision and advance them to the next stage of the marketing-sales pipeline will be considered well worth the price of their contact information.

Web Portals for a Web-centric Strategy

What is a web portal and what role do web portals play in the web-centric marketing strategy?

Web portal defined.

A web portal is a self-service center that provides access to information, applications and services intended for a specific market segment. Customer and partner portals are usually login secured and provide resources not available to the general public.

Support key customer and channel partner relationships.

The objective of web portals that support customer and partner relationships in a web-centric marketing strategy is two-fold: They reduce the cost of delivering the services required to maintain relationships while improving processes that drive revenue performance.

Customers and partners are ever more demanding. Web portals allow you to deliver the resources and capabilities necessary to satisfy this demand in a convenient and personalized way. Different types of customers and partners require different processes, and portals can easily provide resources and capabilities within the context of the type of customer or partner being served.

Web portals allow authorized customers and partners – wherever they are around the world – to perform work processes themselves simply by opening their web browser and logging in. Portals can provide access to a broad range of information, applications and services including product configuration and price modeling, opportunity management, order fulfillment and tracking, technical support and other vital business services.

Extending these online self-service capabilities to key customers and channel partners will improve relationships while increasing productivity.

Systematic Marketing™ Solutions enable VRM process

What is the primary strategic process that Systematic Marketing enables?

Virtual Relationship Marketing (VRM).

VRM is a proven, strategic process for producing the steady stream of high-probability opportunities your sales force and channel partners need to achieve growth.

Stages of the Marketing-Sales Pipeline strengthened by Virtual Relationship Marketing Popular studies have shown that only 11% of leads generated made a purchase within 3 months of their inquiry, and another 42% made a purchase in 4 to 12 months. This means there are nearly four times as many qualified but longer-term prospects than there are immediate selling opportunities at any time.

These less-immediate opportunities often fall through the cracks because seldom are efforts made to build a relationship with longer-term prospects. Few marketing and sales people have time today for the constant personal contact required unless it's done virtually.

The goal of Virtual Relationship Marketing is to get prospects to qualify themselves and tell you when they are ready to buy. Done correctly, VRM will create the perception of personal contact in a way that is welcomed by the prospect and establishes "trusted advisor" status for the sales person.

SystematicMarketing™ Solutions for a Web-centric Strategy

The Systematic Marketing Solutions.Ascend2's Systematic Marketing Solutions were designed specifically for the management of contact data, campaigns, web content and analytics, and the execution of Virtual Relationship

Marketing processes in a web-centric environment. These integrated applications are made available to marketing and sales users through a secure web portal:

Manage contacts.

Store and manage critical information on leads, prospects and customers. Capture online and offline leads, and track through pipeline. Generate sales contact lists. Identify and alert sales force and channel partners of high-probability selling opportunities.

Manage campaigns.

Search and segment lists for targeted email, direct mail and telemarketing. Compose and mass-personalize messages, and track responses to VRM campaigns.

Manage content.

Easily produce custom landing pages for email, direct mail and search engine marketing campaigns. Update online product catalogs, news and other dynamic content.

Consult analytics.

View dashboard graphics and summary tables of marketing and sales pipeline status and other performance metrics linked to detailed marketing reports. Website analytics provide a live view of online visitors and their activities.

19. Network Addressing [2007]
    a. What is MAC address, its structure? [2007, 2004,2003]
    b. IP addressing scheme, Class A B C Networks [2007, 2004, 2003]
    c. Subnet mask and Gateway [2007,2004, 2003]
    d. Using subnet mask to
        i. Split a class C network [2007, 2004]
        ii. Combine more than one class C network [2007]
    e. How can you do super netting? [2004, 2003]
    f. Diff between: Internal IP address and valid IP [2004]

20. Switching networks. Different types of switching networks with examples. Elaborate concept of Frame Relay [2006]

Switching Methods

Switching is the generic method for establishing a path for point-to-pointcommunication in a network. It involves the nodes in the network utilizing their directcommunication lines to other nodes so that a path is established in a piecewisefashion. Each node has the capability to 'switch' to a neighboring node (i.e., a node to which it is directly connected) to further stretch the path until itis completed.

One of the most important functions of the network layer is to employ theswitching capability of the nodes in order to route messages across the network.

There are two basic methods of switching: circuit switching and packet switching. These are separately discussed below.

Circuit Switching

In circuit switching, two communicating stations are connected by a *dedicated*communication path which consists of intermediate nodes in the network and thelinks that connect these nodes. What is significant about circuit switching is that thecommunication path remains intact for the duration of the connection, engaging thenodes and the links involved in the path for that period. (However, these nodes andlinks are typically capable of supporting many channels, so only a portion of their capacity is taken away by the circuit.)shows a simple circuit switch which consists of a 3×3 matrix. capable of connecting any of its inlets (*a*, *b*, and *c*) to any of its outlets (*d*, *e*, and *f*).

Each crosspoint appears as a circle. A hollow circle means that the crosspoint is *off*(i.e., the two crossing wires are not connected). A solid circles means that thecross point is *on* (i.e., the crossing wires are connected).

Circuit switching relies on dedicated equipment especially built for the purpose,and is the dominant form of switching in telephone networks. Its main advantage liesin its predictable behavior: because it uses a dedicated circuit, it can offer a constantthroughput with no noticeable delay in transfer of data.

This property is important intelephone networks, where even a short delay in voice traffic can have disruptiveeffects.

Circuit switching's main weakness is its inflexibility in dealing with computerorienteddata. A circuit uses a fixed amount of bandwidth, regardless of whether it isused or not. In case of voice traffic, the bandwidth is usually well used because mostof the time one of the two parties in a telephone conversation is speaking. However,computers behave differently; they tend to go through long silent periods followed bya sudden burst of data transfer. This leads to significant underutilization of circuit Bandwidth

Another disadvantage of circuit switching is that the network is only capable ofsupporting a limited number of simultaneous circuits.

Packet Switching

Packet switching was designed to address the shortcomings of circuit switching indealing with data communication. Unlike circuit switching where communication iscontinuous along a dedicated circuit, in packet switching, communication is discretein form of packets. Each packet is of a limited size and can hold

up to a certainnumber of octets of user data. Larger messages are broken into smaller chunks sothat they can be fitted into packets. In addition to user data, each packet carries additional information (in form of a header) to enable the network to route it to itsfinal destination.

A packet is handed over from node to node across the network. Each receivingnode temporarily stores the packet, until the next node is ready to receive it, and thenpasses it onto the next node. This technique is called **store-and-forward** andovercomes one of the limitations of circuit switching.

A packet-switched network hasa much higher capacity for accepting further connections. Additional connections areusually not blocked but simply slow down existing connections, because they increase the overall number of packets in the network and hence increase thedelivery time of each packet.

Each channel has an associated buffer which it uses to store packets in transit. Theoperation of the switch is controlled by a microprocessor. A packet received on anyof the channels can be passed onto any of the other channels by the microprocessormoving it to the corresponding buffer.

Two variations of packet switching exist: virtual circuit and datagram.

The **virtual circuit** method (also known as **connection-oriented**) is closer to circuit switching. Here a complete route is worked out prior to sending data packets.The route is established by sending a connection request packet along the route tothe intended destination. This packet informs the intermediate nodes about theconnection and the established route so that they will know how to route subsequentpackets.

The result is a circuit somewhat similar to those in circuit switching, exceptthat it uses packets as its basic unit of communication. Hence it is called a virtualcircuit.

Each packet carries a virtual circuit identifier which enables a node to determineto which virtual circuit it belongs and hence how it should be handled. (The virtualcircuit identifier is essential because multiple virtual circuits may pass through thesame node at the same time.) Because the route is fixed for the duration of the call,the nodes spend no effort in determining how to route packets.

When the two hosts initiate a connection, the network layer establishes a virtualcircuit (denoted by shaded switches) which is maintained for the duration of theconnection. When the hosts disconnect, the network layer releases the circuit. Thepackets in transit are displayed as dark boxes within the buffers. These packetstravel only along the designated virtual circuit.

The **datagram** method (also known as **connectionless**) does not rely on a pre-established route, instead each packet is treated independently. Therefore, it ispossible for different packets to travel along different routes in the network to reachthe same final destination.

As a result, packets may arrive out of order, or even neverarrive (due to node failure). It is up to the network user to deal with lost packets, andto rearrange packets to their original order. Because of the absence of a pre-established circuit, each packet must carry enough information in its header to enablethe nodes to route it correctly.

The advantage of the datagram approach is that because there is no circuit,congestion and faulty nodes can be avoided by choosing a different route. Also,connections can be established more quickly because of reduced overheads. Thismakes datagrams better suited than virtual circuits for brief connections.

Forexample, database transactions in banking systems are of this nature, where eachtransaction involves only a few packets.

The advantage of the virtual circuit approach is that because no separate routingis required for each packet, they are likely to reach their destination more quickly;this leads to improved throughput. Furthermore, packets always arrive in order.

Virtual circuits are better suited to long connections that involve the transfer of largeamounts of data (e.g., transfer of large files).

FrameRelay and Charasterictis
++++++++++++++++++++++++

Frame Relay is a standardized wide area network technology that specifies the physical and logical link layers of digital telecommunications channels using a packet switching methodology. Originally designed for transport across Integrated Services Digital Network (ISDN) infrastructure, it may be used today in the context of many other network interfaces. The Frame Relay network handles the transmission over a frequently-changing path transparent to all end-users.

Frame Relay has become one of the most extensively-used WAN protocols. Its cheapness (compared to leased lines) provides one reason for its popularity. The extreme simplicity of configuring user equipment in a Frame Relay network offers another reason for Frame Relay's popularity.

With the advent of Ethernet over fiber optics, MPLS, VPN and dedicated broadband services such as cable modem and DSL, the end may loom for the Frame Relay protocol and encapsulation.[citation needed] However many rural areas remain lacking DSL and cable modem services. In such cases the least expensive type of non-dial-up connection remains a 64-kbit/s frame-relay line. Thus a retail chain, for instance, may use Frame Relay for connecting rural stores into their corporate WAN.

Frame Relay operates at the physical and data link layers of the OSI model.

Virtual Circuits

The Frame Relay frame is transmitted to its destination by way of virtual circuits (logical paths from an originating point in the network) to a destination point. Virtual circuits may be permanent (PVCs) or switched (SVCs). PVCs are set up administratively by the network manager for a dedicated point-to-point connection; SVCs are set up on a call-by-call basis.

Advantages of Frame Relay

Frame Relay offers an attractive alternative to both dedicated lines and X.25 networks for connecting LANs to bridges and routers. The success of the Frame Relay protocol is based on the following two underlying factors:

- Because virtual circuits consume bandwidth only when they transport data, many virtual circuits can exist simultaneously across a given transmission line. In addition, each device can use more of the bandwidth as necessary, and thus operate at higher speeds.

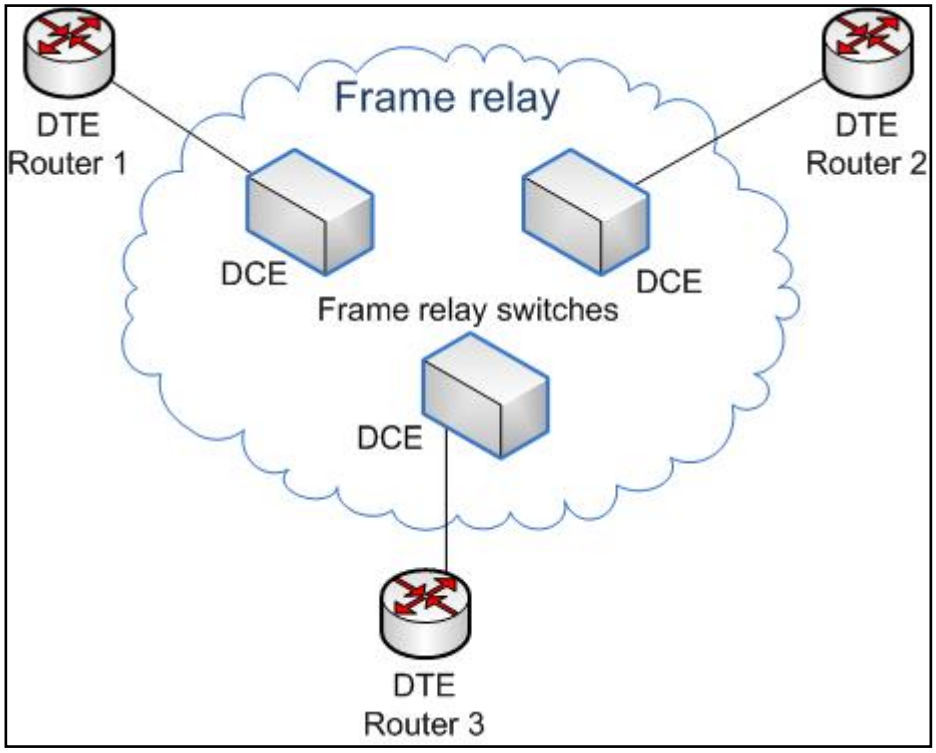
- The improved reliability of communication lines and increased error-handling sophistication at end stations allows the Frame Relay protocol to discard erroneous frames and thus eliminate time-consuming error-handling processing.

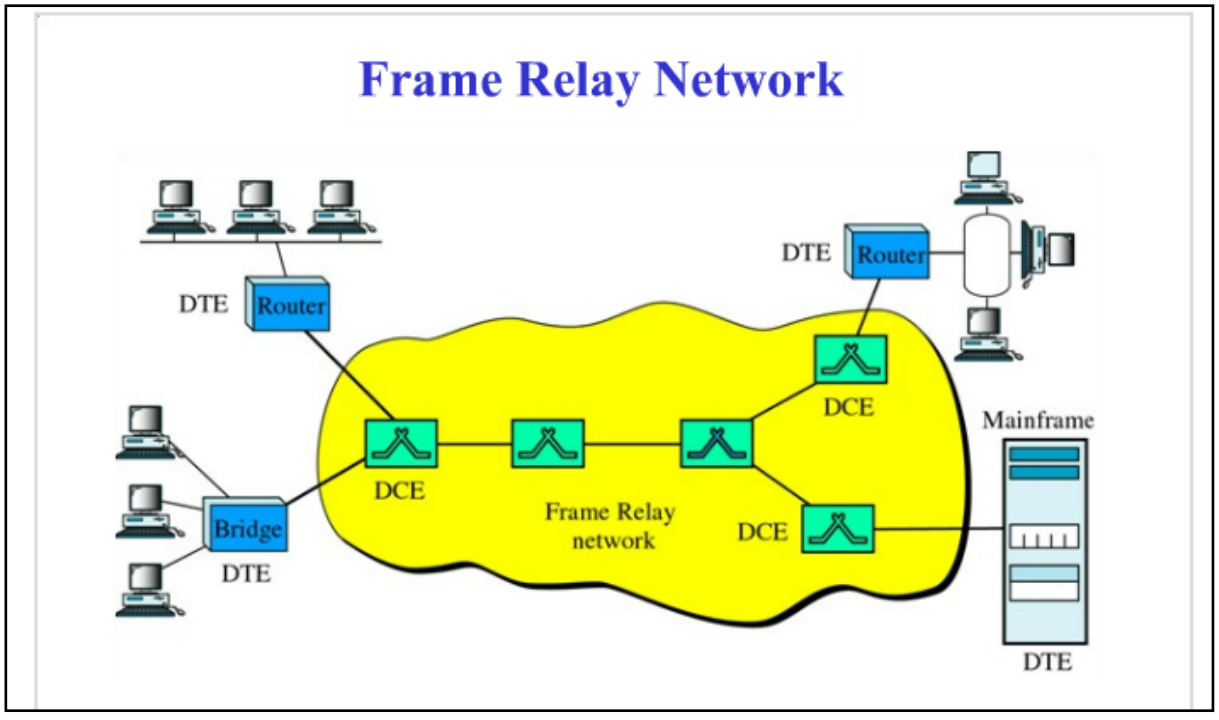
Basic network diagram of a frame relay:

Data terminal equipment (DTE) is an end instrument that converts user information into signals or reconverts received signals.

Data circuit-terminating equipment (DCE) is a device that sits between the data terminal equipment (DTE) and a data transmission circuit.

Usually, the DTE device is the terminal (or computer), and the DCE is a modem.





a. Discuss Routing and Switching. Highlight the differences between them [2003]

Routing and switching can be two terms that are difficult to differentiate, so here is a simple explanation that may help to clarify things. First of all switching and routing are not the same thing. Switching involves moving packets between devices on the same network. Conversely, routing involves moving packets between different networks.

Switches operate at layer 2 of the OSI Model. A switch, also referred to as a multi-port bridge, is able to determine where a packet should be sent by examining the MAC address within the data link header of the packet (the MAC address is the hardware address of a network adapter). A switch maintains a database of MAC addresses and what port they are connected to.

Routers, on the other hand, operate at layer 3 of the OSI Model. A router is able to determine where to send a packet using the Network ID within the Network layer header. It then uses the routing table to determine the route to the destination host.

A network router is a more sophisticated network device compared to either a network switch or a network hub. Like hubs and switches, routers are typically small, box-like pieces of equipment that multiple computers can connect to. Each features a number of ports on the front or back of the unit that provide the connection points for these computers, a connection for electric power, and a number of LED lights to display device status. While routers, hubs and switches all share similar physical appearance, routers differ substantially in their inner workings.

Traditional routers are designed to join together multiple local area networks (LANs) with a wide area network (WAN). Routers serve as intermediate destinations for network traffic. They receive incoming network packets, look inside each packet to identify the source and target network addresses, then forward these packets where needed to ensure the data reaches its final destination.

Routers for home networks (often called broadband routers) are designed specifically to join the home (LAN) to the Internet (WAN) for the purpose of Internet connection sharing. In contrast, switches (and hubs) are not capable of joining multiple networks or sharing an Internet connection. A network with only switches (hubs) must instead designate one computer as the gateway to the Internet, and that device must possess two network adapters for sharing, one for the home LAN and one for the Internet WAN. With a router, all home computers connect to the router as peers, and the router performs all gateway functions.

Additionally, broadband routers contain several features beyond those of traditional routers such as integrated DHCP server and network firewall support. Most notably, though, broadband routers typically incorporate a built-in Ethernet switch. This allows several switches (hubs) to be connected to them, as a means to expand the local network to accommodate more Ethernet devices.

Wi-Fi wireless networks also utilize routers but technically do not have the concept of a wireless switch or hub, although a wireless access point can be roughly compared to a wired switch. Switch are basically layer2 device and it works on Hardware technology with map the mac addresses and it works with switch table.

Router is known as layer3 device and works also on hardware technology and map the mac addresses. it basically connects two different networks or netids to each other.it works with routing table.

1.Switch are said to be l2 device only but Router are said to be L3 device.

2.Switch is said to be H/W Device.Router are said to be S/W device.

3.Switch perform faster than the router because it is a H/W Device.

Routers and switches are both pieces of networking equipment that help data move across the network to their final location, but they work differently, and actually function at different levels of the networking stack. What is the difference between a router and a switch?

The least intelligent kind of networking device is a hub, which takes data in one port, and then retransmits it out every other port. So any information sent or received by any single computer on a hub is retransmitted to every other computer. This is bad for security, obviously, but it also uses up a lot of bandwidth on the network, as computers have to receive data that they don't need.

A switch uses a little more intelligence. It learns the IP address of each computer attached to it, by matching up IP addresses with hardware MAC addresses. When data comes into the switch, it only sends data back out the port assigned to that computer's MAC address. Switches are said to work at a hardware level, and help relieve bandwidth across the network.

A router is the most intelligent networking device. But routers aren't like really intelligent switches, they actually work in a completely different way. Routers are designed to connect networks together. So, your internal network might have IP addresses, like 192.0.0.100, while your Internet service provider might give your computer an IP address that starts with 64.x.x.x. A router can take internal traffic bound for destinations out on the Internet in general, and route it from your internal network to the external network. Whenever you change networks, you need a router. And vice versa when information comes from the external network to your home network.

So, just to restate, switches connect computers together within the same network, while routers connect entire networks together

21. "Internet has changed the outlook of communication" explain giving advantages and disadvantages of Internet communication. [2006]

Pls refer Web Technology PPT done in class.

22. Describe the following: [2006]
    a. Ethernet.

The Ethernet standards comprise several wiring and signaling variants of the OSI physical layer in use with Ethernet. The original 10BASE5 Ethernet used coaxial cable as a shared medium. Later the coaxial cables were replaced by twisted pair and fiber optic links in conjunction with hubs or switches. Data rates were periodically increased from the original 10 megabits per second to 100 gigabits per second.

Systems communicating over Ethernet divide a stream of data into shorter pieces called frames. Each frame contains source and destination addresses and error-checking data so that damaged data can be detected and re-transmitted. As per the OSI model Ethernet provides services up to and including the data link layer.

Since its commercial release, Ethernet has retained a good degree of compatibility. Features such as the 48-bit MAC address and Ethernet frame format have influenced other networking protocols.

Ethernet was developed at Xerox PARC between 1973 and 1974.It was inspired by ALOHAnet, which Robert Metcalfe had studied as part of his PhD dissertation. The idea was first documented in a memo that

Metcalfe wrote on May 22, 1973, where he named it after the disproven luminiferous ether as an "omnipresent, completely-passive medium for the propagation of electromagnetic waves. In 1975, Xerox filed a patent application listing Metcalfe, David Boggs, Chuck Thacker and Butler Lampson as inventors. In 1976, after the system was deployed at PARC, Metcalfe and Boggs published a seminal paper

Metcalfe left Xerox in June 1979 to form 3Com. He convinced Digital Equipment Corporation (DEC), Intel, and Xerox to work together to promote Ethernet as a standard. The so-called "DIX" standard, for "Digital/Intel/Xerox" specified 10 Mbit/s Ethernet, with 48-bit destination and source addresses and a global 16-bit Ether type-type field. It was published on September 30, 1980 as "The Ethernet, A Local Area Network. Data Link Layer and Physical Layer Specifications"Version 2 was published in November, 1982 and defines what has become known as Ethernet II. Formal standardization efforts proceeded at the same time.

Ethernet initially competed with two largely proprietary systems, Token Ring and Token Bus. Because Ethernet was able to adapt to market realities and shift to inexpensive and ubiquitous twisted pair wiring, these proprietary protocols soon found themselves competing in a market inundated by Ethernet products and by the end of the 1980s, Ethernet was clearly the dominant network technology. In the process, 3Com became a major company. 3Com shipped its first 10 Mbit/s Ethernet 3C100 transceiver in March 1981, and that year started selling adapters for PDP-11s and VAXes, as well as Multibus-based Intel and Sun Microsystems computers. This was followed quickly by DEC's Unibus to Ethernet adapter, which DEC sold and used internally to build its own corporate network, which reached over 10,000 nodes by 1986, making it one of the largest computer networks in the world at that time.[13] An Ethernet adapter card for the IBM PC was released in 1982 and by 1985, 3Com had sold 100,000.

Since then Ethernet technology has evolved to meet new bandwidth and market requirements.[14] In addition to computers, Ethernet is now used to interconnect appliances and other personal devices.[1] It is used in industrial applications and is quickly replacing legacy data transmission systems in the world's telecommunications networks.[15] By 2010, the market for Ethernet equipment amounted to over $16 billion per year.[16]

Standardisation

In February 1980, the Institute of Electrical and Electronics Engineers (IEEE) started project 802 to standardize local area networks (LAN). The "DIX-group" with Gary Robinson (DEC), Phil Arst (Intel), and Bob Printis (Xerox) submitted the so-called "Blue Book" CSMA/CD specification as a candidate for the LAN specification.[10] In addition to CSMA/CD, Token Ring (supported by IBM) and Token Bus (selected and henceforward supported by General Motors) were also considered as candidates for a LAN standard. Competing proposals and broad interest in the initiative led to strong disagreement over which technology to standardize. In December 1980, the group was split into three subgroups, and standardization proceeded separately for each proposal.

Delays in the standards process put at risk the market introduction of the Xerox Star workstation and 3Com's Ethernet LAN products. With such business implications in mind, David Liddle (General Manager, Xerox Office Systems) and Metcalfe (3Com) strongly supported a proposal of Fritz Röscheisen (Siemens Private Networks) for an alliance in the emerging office communication market, including Siemens' support for the international standardization of Ethernet (April 10, 1981). Ingrid Fromm, Siemens' representative to IEEE 802, quickly achieved broader support for Ethernet beyond IEEE by the establishment of a competing Task Group "Local Networks" within the European standards body ECMA TC24. As early as March 1982

ECMA TC24 with its corporate members reached agreement on a standard for CSMA/CD based on the IEEE 802 draft. Because the DIX proposal was most technically complete and because of the speedy action taken by ECMA which decisively contributed to the conciliation of opinions within IEEE, the IEEE 802.3 CSMA/CD standard was approved in December 1982.IEEE published the 802.3 standard as a draft in 1983 and as a standard in 1985.

Approval of Ethernet on the international level was achieved by a similar, cross-partisan action with Fromm as liaison officer working to integrate International Electro technical Commission, TC83 and International Organization for Standardization (ISO) TC97SC6, and the ISO/IEEE 802/3 standard was approved in 1984.

Evolution

Ethernet evolved to include higher bandwidth, improved media access control methods, and different physical media. The coaxial cable was replaced with point-to-point links connected by Ethernet repeaters or switches to reduce installation costs, increase reliability, and improve management and troubleshooting. Many variants of Ethernet remain in common use.

Ethernet stations communicate by sending each other data packets: blocks of data individually sent and delivered. As with other IEEE 802 LANs, each Ethernet station is given a 48-bit MAC address. The MAC addresses are used to specify both the destination and the source of each data packet. Ethernet establishes link level connections, which can be defined using both the destination and source addresses. On reception of a transmission, the receiver uses the destination address to determine whether the transmission is relevant to the station or should be ignored. Network interfaces normally do not accept packets addressed to other Ethernet stations. Adapters come programmed with a globally unique address. An Ethertype field in each frame is used by the operating system on the receiving station to select the appropriate protocol module (i.e. the Internet protocol module). Ethernet frames are said to be self-identifying, because of the frame type. Self-identifying frames make it possible to intermix multiple protocols on the same physical network and allow a single computer to use multiple protocols together. Despite the evolution of Ethernet technology, all generations of Ethernet (excluding early experimental versions) use the same frame format and hence the same interface for higher layers), and can be readily interconnected through bridging.

Due to the ubiquity of Ethernet, the ever-decreasing cost of the hardware needed to support it, and the reduced panel space needed by twisted pair Ethernet, most manufacturers now build Ethernet interfaces directly into PC motherboards, eliminating the need for installation of a separate network card.

Shared media

10BASE5 Ethernet equipment

Ethernet was originally based on the idea of computers communicating over a shared coaxial cable acting as a broadcast transmission medium. The methods used were similar to those used in radio systems, with the common cable providing the communication channel likened to the Luminiferous waether in 19th century physics, and it was from this reference that the name "Ethernet" was derived.

Original Ethernet's shared coaxial cable (the shared medium) traversed a building or campus to every attached machine. A scheme known as carrier sense multiple access with collision detection (CSMA/CD) governed the way the computers shared the channel. This scheme was simpler than the competing token ring or token bus technologies.[note 4] Computers were connected to an Attachment Unit Interface (AUI)

transceiver, which was in turn connected to the cable (later with thin Ethernet the transceiver was integrated into the network adapter). While a simple passive wire was highly reliable for small networks, it was not reliable for large extended networks, where damage to the wire in a single place, or a single bad connector, could make the whole Ethernet segment unusable.

Through the first half of the 1980s, Ethernet's 10BASE5 implementation used a coaxial cable 0.375 inches (9.5 mm) in diameter, later called "thick Ethernet" or "thicknet". Its successor, 10BASE2, called "thin Ethernet" or "thinnet", used a cable similar to cable television cable of the era. The emphasis was on making installation of the cable easier and less costly.

Since all communications happen on the same wire, any information sent by one computer is received by all, even if that information is intended for just one destination.[note 6] The network interface card interrupts the CPU only when applicable packets are received: The card ignores information not addressed to it.[note 7] Use of a single cable also means that the bandwidth is shared, such that, for example, available bandwidth to each device is halved when two stations are simultaneously active.

Collisions corrupt transmitted data and require stations to retransmit. The lost data and retransmissions reduce throughput. In the worst case where multiple active hosts connected with maximum allowed cable length attempt to transmit many short frames, excessive collisions can reduce throughput dramatically. However, a Xerox report in 1980 studied performance of an existing Ethernet installation under both normal and artificially generated heavy load. The report claims that 98% throughput on the LAN was observed. This is in contrast with token passing LANs (token ring, token bus), all of which suffer throughput degradation as each new node comes into the LAN, due to token waits. This report was controversial, as modeling showed that collision-based networks theoretically became unstable under loads as low as 37% of nominal capacity. Many early researchers failed to understand these results. Performance on real networks is significantly better. The 10BASE-T standard introduced a collision-free full duplex mode of operation that eliminated collisions. Modern Ethernets are entirely collision-free.

Repeaters and hubs

A 1990s network interface card supporting both coaxial cable-based 10BASE2 (BNC connector, left) and twisted pair-based 10BASE-T (8P8C connector, right)

Main article: Ethernet hub

For signal degradation and timing reasons, coaxial Ethernet segments had a restricted size. Somewhat larger networks could be built by using an Ethernet repeater. Early repeaters had only two ports, allowing, at most, a doubling of network size. Once repeaters with more than two ports became available, it was possible to wire the network in a star topology. Early experiments with star topologies (called "Fibernet") using optical fiber were published by 1978.

Shared cable Ethernet was always hard to install in offices because its bus topology was in conflict with the star topology cable plans designed into buildings for telephony. Modifying Ethernet to conform to twisted pair telephone wiring already installed in commercial buildings provided another opportunity to lower costs, expand the installed base, and leverage building design, and, thus, twisted-pair Ethernet was the next logical development in the mid-1980s.

Ethernet on unshielded twisted-pair cables (UTP) began with StarLAN at 1 Mbit/s in the mid-1980s. In 1987 SynOptics introduced the first twisted-pair Ethernet at 10 Mbit/s in a star-wired cabling topology with a

central hub, later called LattisNet. These evolved into 10BASE-T, which was designed for point-to-point links only, and all termination was built into the device. This changed repeaters from a specialist device used at the center of large networks to a device that every twisted pair-based network with more than two machines had to use. The tree structure that resulted from this made Ethernet networks easier to maintain by preventing most faults with one peer or its associated cable from affecting other devices on the network.

Despite the physical star topology and the presence of separate transmit and receive channels in the twisted pair and fiber media, repeater based Ethernet networks still use half-duplex and CSMA/CD, with only minimal activity by the repeater, primarily the Collision Enforcement signal, in dealing with packet collisions. Every packet is sent to every port on the repeater, so bandwidth and security problems are not addressed. The total throughput of the repeater is limited to that of a single link, and all links must operate at the same speed.

Bridging and switching

Patch cables with patch fields of two Ethernet switches

Main articles: Ethernet switch and Bridging (networking)

While repeaters could isolate some aspects of Ethernet segments, such as cable breakages, they still forwarded all traffic to all Ethernet devices. This created practical limits on how many machines could communicate on an Ethernet network. The entire network was one collision domain, and all hosts had to be able to detect collisions anywhere on the network. This limited the number of repeaters between the farthest nodes. Segments joined by repeaters had to all operate at the same speed, making phased-in upgrades impossible.

To alleviate these problems, bridging was created to communicate at the data link layer while isolating the physical layer. With bridging, only well-formed Ethernet packets are forwarded from one Ethernet segment to another; collisions and packet errors are isolated. Prior to learning of network devices on the different segments, Ethernet bridges (and switches) work somewhat like Ethernet repeaters, passing all traffic between segments. After the bridge learns the addresses associated with each port, it forwards network traffic only to the necessary segments, improving overall performance. Broadcast traffic is still forwarded to all network segments. Bridges also overcame the limits on total segments between two hosts and allowed the mixing of speeds, both of which are critical to deployment of Fast Ethernet.

In 1989, the networking company Kalpana introduced their EtherSwitch, the first Ethernet switch. This worked somewhat differently from an Ethernet bridge, where only the header of the incoming packet would be examined before it was either dropped or forwarded to another segment. This greatly reduced the forwarding latency and the processing load on the network device. One drawback of this cut-through switching method was that packets that had been corrupted would still be propagated through the network, so a jabbering station could continue to disrupt the entire network. The eventual remedy for this was a return to the original store and forward approach of bridging, where the packet would be read into a buffer on the switch in its entirety, verified against its checksum and then forwarded, but using more powerful application-specific integrated circuits. Hence, the bridging is then done in hardware, allowing packets to be forwarded at full wire speed.

When a twisted pair or fiber link segment is used and neither end is connected to a repeater, full-duplex Ethernet becomes possible over that segment. In full-duplex mode, both devices can transmit and receive

to and from each other at the same time, and there is no collision domain. This doubles the aggregate bandwidth of the link and is sometimes advertised as double the link speed (e.g., 200 Mbit/s).[note 9] The elimination of the collision domain for these connections also means that all the link's bandwidth can be used by the two devices on that segment and that segment length is not limited by the need for correct collision detection.

Since packets are typically delivered only to the port they are intended for, traffic on a switched Ethernet is less public than on shared-medium Ethernet. Despite this, switched Ethernet should still be regarded as an insecure network technology, because it is easy to subvert switched Ethernet systems by means such as ARP spoofing and MAC flooding.

The bandwidth advantages, the improved isolation of devices from each other, the ability to easily mix different speeds of devices and the elimination of the chaining limits inherent in non-switched Ethernet have made switched Ethernet the dominant network technology.

Advanced networking

A core Ethernet switch

Simple switched Ethernet networks, while a great improvement over repeater-based Ethernet, suffer from single points of failure, attacks that trick switches or hosts into sending data to a machine even if it is not intended for it, scalability and security issues with regard to broadcast radiation and multicast traffic, and bandwidth choke points where a lot of traffic is forced down a single link.[citation needed]

Advanced networking features in switches and routers combat these issues through means including spanning-tree protocol to maintain the active links of the network as a tree while allowing physical loops for redundancy, port security and protection features such as MAC lock down and broadcast radiation filtering, virtual LANs to keep different classes of users separate while using the same physical infrastructure, multilayer switching to route between different classes and link aggregation to add bandwidth to overloaded links and to provide some measure of redundancy.

IEEE 802.1aq (shortest path bridging) includes the use of the link-state routing protocol IS-IS to allow larger networks with shortest path routes between devices. In 2012 it was stated by David Allan and Nigel Bragg, in 802.1aq Shortest Path Bridging Design and Evolution: The Architect's Perspective that shortest path bridging is one of the most significant enhancements in Ethernet's history.[28]

The Ethernet physical layer evolved over a considerable time span and encompasses coaxial, twisted pair and fiber optic physical media interfaces and speeds from 10 Mbit to 100 Gbit. The most common forms used are 10BASE-T, 100BASE-TX, and 1000BASE-T. All three utilize twisted pair cables and 8P8C modular connectors. They run at 10 Mbit/s, 100 Mbit/s, and 1 Gbit/s, respectively. Fiber optic variants of Ethernet offer high performance, electrical isolation and distance (tens of kilometers with some versions). In general, network protocol stack software will work similarly on all varieties.

Ethernet frames

Main article: Ethernet frame

A data packet on the wire is called a frame. A frame begins with preamble and start frame delimiter, followed by an Ethernet header featuring source and destination MAC addresses. The middle section of the frame consists of payload data including any headers for other protocols (e.g., Internet Protocol)

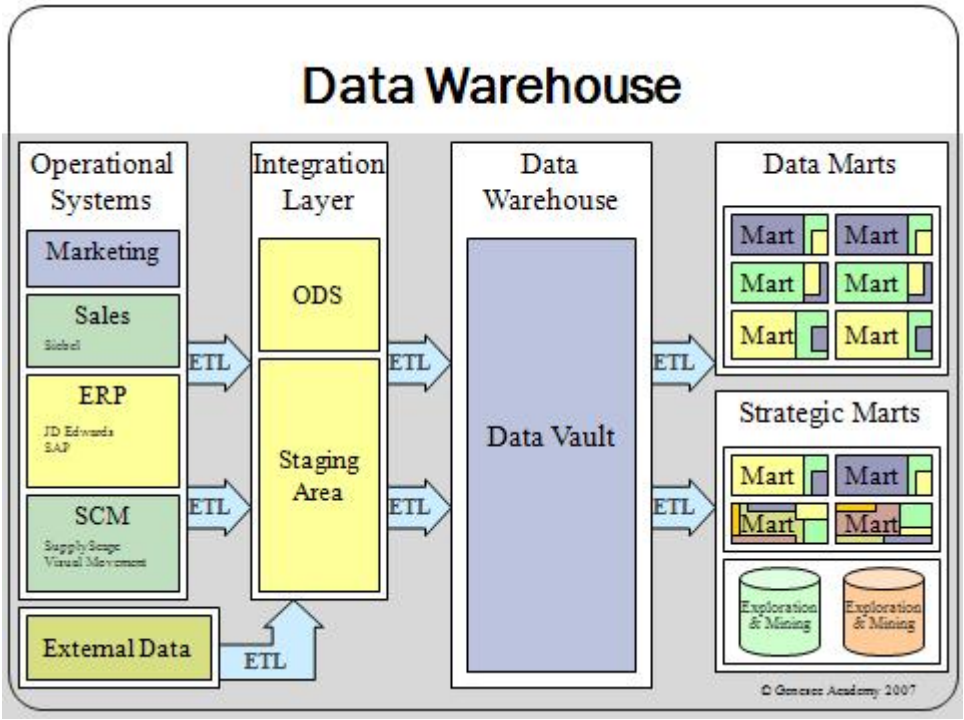
carried in the frame. The frame ends with a 32-bit cyclic redundancy check, which is used to detect corruption of data in transit.

b. Data Warehousing

A data warehouse constructed from integrated data source systems does not require ETL, staging databases, or operational data store databases. The integrated data source systems may be considered to be a part of a distributed operational data store layer. Data federation methods or data virtualization methods may be used to access the distributed integrated source data systems to consolidate and aggregate data directly into the data warehouse database tables. Unlike the ETL-based data warehouse, the integrated source data systems and the data warehouse are all integrated since there is no transformation of dimensional or reference data. This integrated data warehouse architecture supports the drill down from the aggregate data of the data warehouse to the transactional data of the integrated source data systems.

Data warehouses can be subdivided into data marts. Data marts store subsets of data from a warehouse.

This definition of the data warehouse focuses on data storage. The main source of the data is cleaned, transformed, cataloged and made available for use by managers and other business professionals for data mining, online analytical processing, market research and decision support (Marakas & O'Brien 2009). However, the means to retrieve and analyze data, to extract, transform and load data, and to manage the data dictionary are also considered essential components of a data warehousing system. Many references to data warehousing use this broader context. Thus, an expanded definition for data warehousing includes business intelligence tools, tools to extract, transform and load data into the repository, and tools to manage and retrieve metadata.



Benefits of a data warehouse

A data warehouse maintains a copy of information from the source transaction systems. This architectural complexity provides the opportunity to:

- Maintain data history, even if the source transaction systems do not.
- Integrate data from multiple source systems, enabling a central view across the enterprise. This benefit is always valuable, but particularly so when the organization has grown by merger.
- Improve data quality, by providing consistent codes and descriptions, flagging or even fixing bad data.
- Present the organization's information consistently.
- Provide a single common data model for all data of interest regardless of the data's source.
- Restructure the data so that it makes sense to the business users.
- Restructure the data so that it delivers excellent query performance, even for complex analytic queries, without impacting the operational systems.
- Add value to operational business applications, notably customer relationship management (CRM) systems.

The concept of data warehousing dates back to the late 1980s. when IBM researchers Barry Devlin and Paul Murphy developed the "business data warehouse". In essence, the data warehousing concept was intended to provide an architectural model for the flow of data from operational systems to decision support environments. The concept attempted to address the various problems associated with this flow, mainly the high costs associated with it. In the absence of a data warehousing architecture, an enormous amount of redundancy was required to support multiple decision support environments. In larger corporations it was typical for multiple decision support environments to operate independently. Though each environment served different users, they often required much of the same stored data. The process of gathering, cleaning and integrating data from various sources, usually from long-term existing operational systems (usually referred to as legacy systems), was typically in part replicated for each environment. Moreover, the operational systems were frequently reexamined as new decision support requirements emerged. Often new requirements necessitated gathering, cleaning and integrating new data from "data marts" that were tailored for ready access by users.

c. Network Operating system

Network Operating System also referred to as the Dialoguer,[1] is the software that runs on a server and enables the server to manage data, users, groups, security, applications, and other networking functions.[2] The network operating system is designed to allow shared file and printer access among multiple computers in a network, typically a local area network (LAN), a private network or to other networks. The most popular network operating systems are MicrosoftWindows Server 2003, MicrosoftWindows Server 2008, UNIX, Linux, Mac OS X, Novell NetWare, and BSD

Network Operating Systems are based on a client/server architecture in which a server enables multiple clients to share resources.[2]

Use in Routers

Network Operating Systems (**NOS of windows**) are embedded in a router or hardware firewall that operates the functions in the network layer (layer 3) of the OSI model.[1]

- Examples:
  - JUNOS, used in routers and switches from Juniper Networks,
  - Cisco IOS (formerly "Cisco Internetwork Operating System").
  - TiMOS, used in routers from Alcatel-Lucent
  - Huawei VRP (Versatile Routing Platform), used in routers from Huawei
  - MikroTik RouterOS™ (is a router operating system and software which turns a regular Intel PC or MikroTik RouterBOARD™ hardware into a dedicated router.)

- ZyNOS, used in network devices made by ZyXEL.
- ExtremeXOS, used in network devices made by Extreme Networks. Also called EXOS.

Peer-to-Peer

In a peer-to-peer network operating system users are allowed to share resources and files located on their computers and access shared resources from others. This system is not based with having a file server or centralized management source. A peer-to-peer network sets all connected computers equal; they all share the same abilities to use resources available on the network.[3]

- Examples:
  - AppleShare used for networking connecting Apple products.
  - Windows for Workgroups used for networking peer-to-peer windows computers.

Advantages

- Ease of setup
- Less hardware needed, no server needs to be purchased.

Disadvantages

- No central location for storage.
- Lack of security that a client/server type offers.

Client/Server

Client/server network operating systems allow the network to centralize functions and applications in one or more dedicated file servers. The server is the center of the system, allowing access to resources and instituting security. The network operating system provides the mechanism to integrate all the components on a network to allow multiple users to simultaneously share the same resources regardless of physical location.[3][4]

- Examples:
  - Novell Netware
  - Windows Server

Advantages

- Centralized servers are more stable.
- Security is provided through the server.
- New technology and hardware can be easily integrated into the system.
- Servers are able to be accessed remotely from different locations and types of systems.

Disadvantages

- Cost of buying and running a server are high.
- Dependence on a central location for operation.
- Requires regular maintenance and updates.

Security Issues Involved in using a Client/Server Network

In a client/server network security issues may evolve at three different locations: the client, the network, and the server. All three points need to be monitored for unauthorized activity and need to be secured against hackers or eavesdroppers.

The Client

The client is the end user of the network and needs to be secured the most. The client end usually exposes data through the screen of the computer. Client connections to server should be secured through passwords and upon leaving their workstations clients should make sure that their connection to the server is securely cut off in order to make sure that no hackers or intruders are able to reach the server data. Not only securing the workstations connection to the server is important but also securing the files on the workstation (client) is important as it ensures that no hackers are able to reach the system. Another possibility is that of introducing a virus or running unauthorized software on the client workstation thus threatening the entire information bank at the server (Exforsys Inc., 2007).

The users themselves could also be a security threat if they purposely leave their IDs logged in or use easy IDs and passwords to enable hacking. Users may also be sharing their passwords in order to give the hackers access to confidential data (Wilson, Lin, & Craske, 1999). This can be overcome by giving passwords to each client and regularly asking clients to change their passwords. Also passwords should be checked for guessability and for their strength and uniqueness.

The Network

The network allows transmission of data from the clients to the server. There are several points on the network where a hacker could eavesdrop or steal important packets of information. These packets may contain important confidential data such as passwords or company details. It is important that these networks are secured properly to keep unauthorized professionals away from all the data stored on the server. This can be done by encrypting important data being sent on the network. However, encryption may not be the only possible way of protecting networks as hackers can work their way around encryption. Another method could be conducting security audits regularly and ensuring identification and authorisation of individuals at all points along the network. This should discourage potential hackers (Wilson, Lin, & Craske, 1999). Making the entire environment difficult to impersonate also makes sure that the clients are reaching the true files and applications on the server and that the server is providing information to authorized personnel only.

The Server

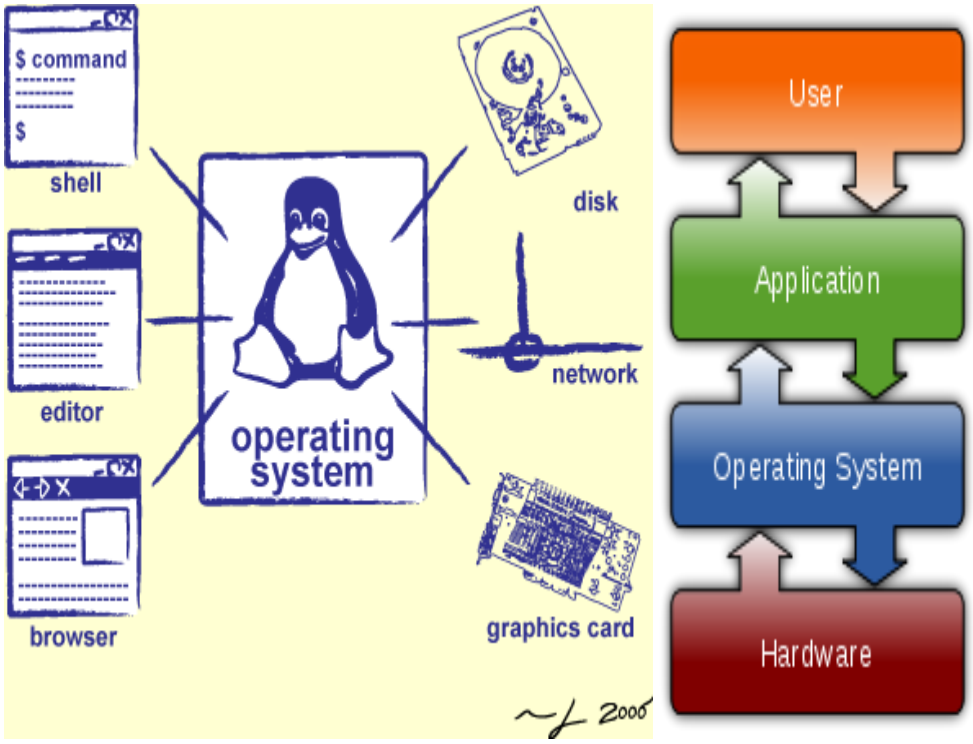
The server can be secured by placing all the data in a secure, centralized location that is protected through permitting access to authorized personnel only. Virus protection should also be available on server computers as vast amounts of data can be infected. Regular upgrades should be provided to the servers as the software and the applications need to be updated. Even the entire body of data on a server could be encrypted in order to make sure that reaching the data would require excessive time and effort (Wilson, Lin, & Craske, 1999).

An operating system (OS) is a set of software that manages computer hardware resources and provide common services for computer programs. The operating system is a vital component of the system software in a computer system. Application programs require an operating system to function.

Time-sharing operating systems schedule tasks for efficient use of the system and may also include accounting for cost allocation of processor time, mass storage, printing, and other resources.

For hardware functions such as input and output and memory allocation, the operating system acts as an intermediary between programs and the computer hardware, although the application code is usually executed directly by the hardware and will frequently make a system call to an OS function or be interrupted by it. Operating systems can be found on almost any device that contains a computer—from cellular phones and video game consoles to supercomputers and web servers.

Examples of popular modern operating systems include Android, BSD, iOS, Linux, Mac OS X, Microsoft Windows,[3] Windows Phone, and IBM z/OS. All these, except Windows and z/OS, share roots in UNIX.



Types

Real-time - A real-time operating system is a multitasking operating system that aims at executing real-time applications. Real-time operating systems often use specialized scheduling algorithms so that they can achieve a deterministic nature of behavior. The main objective of real-time operating systems is their quick and predictable response to events. They have an event-driven or time-sharing design and often aspects of both. An event-driven system switches between tasks based on their priorities or external events while time-sharing operating systems switch tasks based on clock interrupts.

Multi-user - A multi-user operating system allows multiple users to access a computer system concurrently. Time-sharing system can be classified as multi-user systems as they enable a multiple user access to a computer through the sharing of time. Single-user operating systems, as opposed to a multi-user operating system, are usable by a single user at a time. Being able to use multiple accounts on a Windows operating system does not make it a multi-user system. Rather, only the

network administrator is the real user. But for a UNIX-like operating system, it is possible for two users to login at a time and this capability of the OS makes it a multi-user operating system.

Multi-tasking vs. Single-tasking - When only a single program is allowed to run at a time, the system is grouped under a single-tasking system. However, when the operating system allows the execution of multiple tasks at one time, it is classified as a multi-tasking operating system. Multi-tasking can be of two types: pre-emptive or co-operative. In pre-emptive multitasking, the operating system slices the CPU time and dedicates one slot to each of the programs. Unix-like operating systems such as Solaris and Linux support pre-emptive multitasking, as does AmigaOS. Cooperative multitasking is achieved by relying on each process to give time to the other processes in a defined manner. 16-bit versions of Microsoft Windows used cooperative multi-tasking. 32-bit versions, both Windows NT and Win9x, used pre-emptive multi-tasking. Mac OS prior to OS X used to support cooperative multitasking.

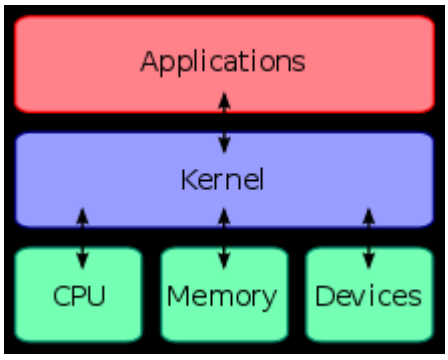
Distributed - A distributed operating system manages a group of independent computers and makes them appear to be a single computer. The development of networked computers that could be linked and communicate with each other gave rise to distributed computing. Distributed computations are carried out on more than one machine. When computers in a group work in cooperation, they make a distributed system.

Embedded - Embedded operating systems are designed to be used in embedded computer systems. They are designed to operate on small machines like PDAs with less autonomy. They are able to operate with a limited number of resources. They are very compact and extremely efficient by design. Windows CE and Minix 3 are some examples of embedded operating systems.

Components

The components of an operating system all exist in order to make the different parts of a computer work together. All software—from financial databases to film editors—needs to go through the operating system in order to use any of the hardware, whether it be as simple as a mouse or keyboard or complex as an Internet connection.

1. **Kernel -** A kernel connects the application software to the hardware of a computer.



With the aid of the firmware and device drivers, the kernel provides the most basic level of control over all of the computer's hardware devices. It manages memory access for programs in the RAM, it determines which programs get access to which hardware resources, it sets up or resets the CPU's

operating states for optimal operation at all times, and it organizes the data for long-term non-volatile storage with file systems on such media as disks, tapes, flash memory, etc.

Program execution - The operating system provides an interface between an application program and the computer hardware, so that an application program can interact with the hardware only by obeying rules and procedures programmed into the operating system. The operating system is also a set of services which simplify development and execution of application programs. Executing an application program involves the creation of a process by the operating system kernel which assigns memory space and other resources, establishes a priority for the process in multi-tasking systems, loads program binary code into memory, and initiates execution of the application program which then interacts with the user and with hardware devices.

Interrupts - Interrupts are central to operating systems, as they provide an efficient way for the operating system to interact with and react to its environment. The alternative — having the operating system "watch" the various sources of input for events (polling) that require action — can be found in older systems with very small stacks (50 or 60 bytes) but are unusual in modern systems with large stacks. Interrupt-based programming is directly supported by most modern CPUs. Interrupts provide a computer with a way of automatically saving local register contexts, and running specific code in response to events. Even very basic computers support hardware interrupts, and allow the programmer to specify code which may be run when that event takes place.

Modes - Modern CPUs support multiple modes of operation. CPUs with this capability use at least two modes: protected mode and supervisor mode. The supervisor mode is used by the operating system's kernel for low level tasks that need unrestricted access to hardware, such as controlling how memory is written and erased, and communication with devices like graphics cards. Protected mode, in contrast, is used for almost everything else. Applications operate within protected mode, and can only use hardware by communicating with the kernel, which controls everything in supervisor mode. CPUs might have other modes similar to protected mode as well, such as the virtual modes in order to emulate older processor types, such as 16-bit processors on a 32-bit one, or 32-bit processors on a 64-bit one.

Memory management - Among other things, a multiprogramming operating system kernel must be responsible for managing all system memory which is currently in use by programs. This ensures that a program does not interfere with memory already in use by another program. Since programs time share, each program must have independent access to memory.

Cooperative memory management, used by many early operating systems, assumes that all programs make voluntary use of the kernel's memory manager, and do not exceed their allocated memory. This system of memory management is almost never seen any more, since programs often contain bugs which can cause them to exceed their allocated memory. If a program fails, it may cause memory used by one or more other programs to be affected or overwritten. Malicious programs or viruses may purposefully alter another program's memory, or may affect the operation of the operating system itself. With cooperative memory management, it takes only one misbehaved program to crash the system.

Virtual memory - The use of virtual memory addressing (such as paging or segmentation) means that the kernel can choose what memory each program may use at any given time, allowing the operating system to use the same memory locations for multiple tasks.

If a program tries to access memory that isn't in its current range of accessible memory, but nonetheless has been allocated to it, the kernel will be interrupted in the same way as it would if the program were to exceed its allocated memory.

Multitasking - Multitasking refers to the running of multiple independent computer programs on the same computer; giving the appearance that it is performing the tasks at the same time. Since most computers can do at most one or two things at one time, this is generally done via time-sharing, which means that each program uses a share of the computer's time to execute.

An operating system kernel contains a piece of software called a scheduler which determines how much time each program will spend executing, and in which order execution control should be passed to programs. Control is passed to a process by the kernel, which allows the program access to the CPU and memory. Later, control is returned to the kernel through some mechanism, so that another program may be allowed to use the CPU. This so-called passing of control between the kernel and applications is called a context switch.

Disk access and file systems - Access to data stored on disks is a central feature of all operating systems. Computers store data on disks using files, which are structured in specific ways in order to allow for faster access, higher reliability, and to make better use out of the drive's available space. The specific way in which files are stored on a disk is called a file system, and enables files to have names and attributes. It also allows them to be stored in a hierarchy of directories or folders arranged in a directory tree.

Device drivers - A device driver is a specific type of computer software developed to allow interaction with hardware devices. Typically this constitutes an interface for communicating with the device, through the specific computer bus or communications subsystem that the hardware is connected to, providing commands to and/or receiving data from the device, and on the other end, the requisite interfaces to the operating system and software applications. It is a specialized hardware-dependent computer program which is also operating system specific that enables another program, typically an operating system or applications software package or computer program running under the operating system kernel, to interact transparently with a hardware device, and usually provides the requisite interrupt handling necessary for any necessary asynchronous time-dependent hardware interfacing needs.

2. **Networking -** Currently most operating systems support a variety of networking protocols, hardware, and applications for using them. This means that computers running dissimilar operating systems can participate in a common network for sharing resources such as computing, files, printers, and scanners using either wired or wireless connections. Networks can essentially allow a computer's operating system to access the resources of a remote computer to support the same functions as it could if those resources were connected directly

to the local computer. This includes everything from simple communication, to using networked file systems or even sharing another computer's graphics or sound hardware. Some network services allow the resources of a computer to be accessed transparently, such as SSH which allows networked users direct access to a computer's command line interface.

Client/server networking allows a program on a computer, called a client, to connect via a network to another computer, called a server. Servers offer (or host) various services to other network computers and users. These services are usually provided through ports or numbered access points beyond the server's network address. Each port number is usually associated with a maximum of one running program, which is responsible for handling requests to that port. A daemon, being a user program, can in turn access the local hardware resources of that computer by passing requests to the operating system kernel.

3. **Security** - A computer being secure depends on a number of technologies working properly. A modern operating system provides access to a number of resources, which are available to software running on the system, and to external devices like networks via the kernel.

The operating system must be capable of distinguishing between requests which should be allowed to be processed, and others which should not be processed. While some systems may simply distinguish between "privileged" and "non-privileged", systems commonly have a form of requester identity, such as a user name. To establish identity there may be a process of authentication. Often a username must be quoted, and each username may have a password. Other methods of authentication, such as magnetic cards or biometric data, might be used instead. In some cases, especially connections from the network, resources may be accessed with no authentication at all (such as reading files over a network share). Also covered by the concept of requester identity is authorization; the particular services and resources accessible by the requester once logged into a system are tied to either the requester's user account or to the variously configured groups of users to which the requester belongs.

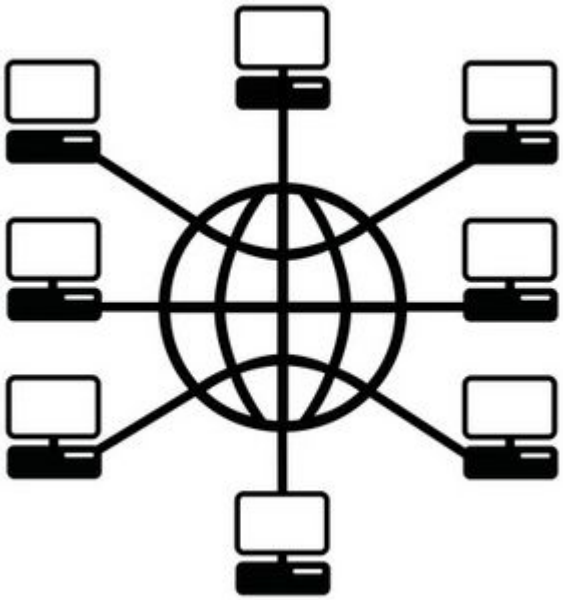
4. **User interface** - Every computer that is to be operated by an individual requires a user interface. The user interface is not actually a part of the operating system—it generally runs in a separate program usually referred to as a shell, but is essential if human interaction is to be supported. The user interface requests services from the operating system that will acquire data from input hardware devices, such as a keyboard, mouse or credit card reader, and requests operating system services to display prompts, status messages and such on output hardware devices, such as a video monitor or printer. The two most common forms of a user interface have historically been the command-line interface, where computer commands are typed out line-by-line, and the graphical user interface, where a visual environment (most commonly a WIMP) is present.

d. Components of Client server applications

A client/server network has three main components: workstations, servers and the network devices that connect them. Workstations are the computers that are subordinate to servers. They send requests to servers to access shared programs, files and databases, and are governed by policies defined by servers. A

server "services" requests from workstations and can perform many functions as a central repository of files, programs, databases and management policies. Network devices provide the communication path for servers and workstations. They act as connectors and route data in and out of the network.

A client/server network has three main components: workstations, servers and the network devices that connect them. Workstations are the computers that are subordinate to servers. They send requests to servers to access shared programs, files and databases, and are governed by policies defined by servers. A server "services" requests from workstations and can perform many functions as a central repository of files, programs, databases and management policies. Network devices provide the communication path for servers and workstations. They act as connectors and route data in and out of the network.



Workstations

- Workstations, or client computers, initially differentiate themselves by the operating systems running them. In a client/server network, Windows 2000, Windows XP, Windows Vista and Windows 7 are examples of workstation operating systems. Aside from being relatively cheaper than server operating systems, their functions and processes are essentially intended for client computers. Centralized databases, shared programs, management and security policies are not part of their operating systems. What they have are localized versions of databases, programs and policies that can be applied individually to them. Workstations also have lower technical specifications than servers in the areas of memory, hard drive space and processor speed, because they are not required to process requests or record data from multiple

Servers

- Servers are distinguished by different sets of operating systems like Windows 2000 Server, Windows 2003 or Windows 2008. They also have higher memory and hard drive space and faster processors because they store and service multiple (and often simultaneous) requests from workstations. A server can assume many roles in a client/server network. It can be a file server, a mail server, a database server and domain controller all at the same time. A well-set-up network, however, delineates these roles to different servers to optimize performance. A server, regardless of what role it has, essentially acts as a centralized repository of network files, programs, databases

and policies. It makes for easier management and backup because it is not dependent to individual user configurations, but can be universally and uniformly implemented across the network.

Network Devices

- Network devices connect workstations and servers. They ensure that requests to and from workstations are routed properly to the correct server. Several network devices each provide different types of network connectivity. In a simple client/server network, a hub can connect a server to multiple workstations. It acts as a repeater, passing on data from one device to another. Bridges separate network segments. This is useful for offices with several departments to distinguish which department a particular workstation belongs to. Another network device, a switch, is similar to a bridge, but can detect conflicts between network segments like same IP addresses or computer names across departments. Wide-area networks use routers to connect network segments in different locations. Routers are also used to connect networks, or route information to the Internet.

Other Components

- Client/server networks usually have network printers or scanners, which are shared and can be used by all computers in the network. Instead of installing them individually to each computer, they can be placed in one location that everyone can access. This saves both space and money.

e. Electronic Data Interchange

Electronic data interchange (EDI) is a method for transferring data between different computer systems or computer networks. It is commonly used by big companies for e-commerce purposes, such as sending orders to warehouses or tracking their order. It is more than mere e-mail; for instance, organizations might replace bills of lading and even cheques with appropriate EDI messages. It also refers specifically to a family of standards.

National Institute of Standards and Technology defined electronic data interchange as "the computer-to-computer interchange of strictly formatted messages that represent documents other than monetary instruments. EDI implies a sequence of messages between two parties, either of whom may serve as originator or recipient. The formatted data representing the documents may be transmitted from originator to recipient via telecommunications or physically transported on electronic storage media." It distinguishes mere electronic communication or data exchange, specifying that "in EDI, the usual processing of received messages is by computer only. Human intervention in the processing of a received message is typically intended only for error conditions, for quality review, and for special situations. EDI can be formally defined as the transfer of structured data, by agreed message standards, from one computer system to another without human intervention.

Specifications

Organizations that send or receive documents between each other are referred to as "trading partners" in EDI terminology. The trading partners agree on the specific information to be transmitted and how it should be used. This is done in human readable specifications (also called Message Implementation Guidelines). While the standards are analogous to building codes, the specifications are analogous to blue prints. (The specification may also be called a "mapping," but the term mapping is typically reserved for specific machine-readable instructions given to the translation software.) Larger trading "hubs" have existing Message Implementation Guidelines which mirror their business processes for processing EDI and

they are usually unwilling to modify their EDI business practices to meet the needs of their trading partners. Often in a large company these EDI guidelines will be written to be generic enough to be used by different branches or divisions and therefore will contain information not needed for a particular business document exchange. For other large companies, they may create separate EDI guidelines for each branch/division..

Transmission

Trading partners are free to use any method for the transmission of documents. Furthermore, they can either interact directly, or through a third party.

Serial communications

At one time a common method of transmitting EDI messages was using a Bisync modem; one partner would have one or more modems set up to receive incoming calls, and the other would call it with their own modem. It was also possible to use a dedicated leased line or a network such as Telex. Some organizations may have transmitted EDI files via BBS.

Internet

As more organizations connected to the Internet, eventually most or all EDI was pushed onto it. Initially, this was through ad-hoc conventions, such as unencrypted FTP of ASCII text files to a certain folder on a certain host, permitted only from certain IP addresses. However, the IETF has published several informational documents (the "Applicability Statements"; see below under Protocols) describing ways to use standard Internet protocols for EDI.

Peer-to-Peer

EDI standards are written such that trading partners could connect directly to each other. For example, an automotive manufacturer might maintain a modem-pool that all of its hundreds suppliers are required to dial into to perform EDI. However, if a supplier does business with several manufacturers, it may need to acquire a different modem (or VPN device, etc.) and different software for each one.

Value-added networks

To address the limitations in peer-to-peer adoption of EDI, VANs (value-added networks) were established. A VAN acts as a regional post office. It receives transactions, examines the 'from' and the 'to' information, and routes the transaction to the final recipient. VANs may provide a number of additional services, e.g. retransmitting documents, providing third party audit information, acting as a gateway for different transmission methods, and handling telecommunications support. Because of these and other services VANs provide, businesses frequently use a VAN even when both trading partners are using Internet-based protocols. Healthcare clearinghouses perform many of the same functions as a VAN, but have additional legal restrictions.

VANs may be operated by various entities:

- telecommunication companies;
- industry group consortia;
- a large company interacting with its suppliers/vendors.

Advantages over paper systems

EDI and other similar technologies save a company money by providing an alternative to, or replacing, information flows that require a great deal of human interaction and materials such as paper documents, meetings, faxes, etc. Even when paper documents are maintained in parallel with EDI exchange, e.g. printed shipping manifests, electronic exchange and the use of data from that exchange reduces the handling costs of sorting, distributing, organizing, and searching paper documents. EDI and similar technologies allow a company to take advantage of the benefits of storing and manipulating data electronically without the cost of manual entry. Another advantage of EDI is reduced errors, such as shipping and billing errors, because EDI eliminates the need to rekey documents on the destination side. One very important advantage of EDI over paper documents is the speed in which the trading partner receives and incorporates the information into their system thus greatly reducing cycle times. For this reason, EDI can be an important component of just-in-time production systems.

f. Transmission Mode and Directions

The way in which data is transmitted from one place to another is called data transmission mode. It is also called the data communication mode. It indicates the direction of flow of information. Sometimes, data transmission modes are also referred to as directional modes.

When a person is giving a lecture, information is conveyed in one direction. Similarly, during a conversation between two persons, spoken messages are exchanged in both directions. These messages may be exchanged alternatively or simultaneously.

There are three data transmission modes.

(i) Simplex mode:

In simplex mode, data is transmitted in only one direction. A terminal can only send data and cannot receive it or it can only receive data but cannot send data.

Today, this mode of data communication is not popular, because most of the modem communications require two-way exchange of data. However, this mode of communication is used in business field at certain point-of-sale terminals in which sales data is entered without a corresponding reply. The other examples of simplex communication modes are Radio and T.V transmissions.

In computer system, the keyboard, monitor and printer are examples of simplex devices. The keyboard can only be used to enter data into computer, while monitor and printer can only accept (display/print) output.

(ii) Half-Duplex Mode:

In half-duplex mode, data can be transmitted in both directions but only in one direction at a time. In this mode, data is sent and received alternatively. It is like a one-lane bridge where two-way traffic must give way in order to cross the other.

In half-duplex mode, at a time only one end transmits data while other end receives. In addition, it is possible to perform error detection and request the sender to re-transmit information.

The Internet browsing is an example of half duplex. When we issue a request to download web document or webpage, it is downloaded and displayed before we issue another request.

(iii) Full-Duplex Mode:

In full-duplex mode, data can be transmitted in both directions at the same time on the same channel. It is the fastest directional mode of communication. The telephone communication system is an example of full-duplex communication mode.

Types of Data Transmission Modes:
There are two types of data transmission modes. These are:

(i) Parallel Transmission.
(ii) Serial Transmission.

(i) Parallel Transmission:

In parallel transmission, a group of bits of data flow at the same time (in parallel) through separate communication lines. It is very fast data transmission. The automobile traffic on a multi-lane highway is an example of parallel transmission.

Inside the computer, usually a group of bits of data flow from one component to another at the same time. If a computer uses 32-bit internal structure, then 32-bits of data can be transferred from one component of computer to another at the same time. Parallel transmission is commonly used to transfer data from computer to printer.

(ii) Serial Transmission:

In serial data transmission, a group of bits of data flow in sequential Order through single communication line. The flow of traffic on one-lane residential street is an example of serial data transmission mode. Serial transmission is typically slower than parallel transmission, because data is. sent sequentially in a bit-by-bit on a single communication line.

The telephone line system uses the serial transmission to transmit data from one location to another. In computer system, mouse also uses serial transmission to send the command signals inside the computer.

Synchronous and Asynchronous Transmissions:

Synchronous Transmission:

In synchronous transmission, data is transmitted block-by-block or word-byword at the same time. Each block may contain several bytes of data. In this mode, data is saved before sending. A large volume of data can be transmitted at a time. The data transmission is very fast. It is most commonly used by remote communication systems.

In synchronous transmission, a special communication device known as 'synchronized clock' is required to

schedule the transmission of information. This special communication device or equipment is expensive.

Asynchronous Transmission:

In asynchronous transmission, data is transmitted one byte at a 'time'. The data is transmitted character-by-character as the user types it on a keyboard. In this mode, data is not saved before sending.

An asynchronous line that is idle (not being used) is identified with a value 1, also known as mark state. This value is used by the communication devices to find whether the line is idle or free.

In asynchronous transmission, a special signal is sent by sender to the receiver before sending the message. It is known as start bit. A start bit has a value of 0, also called a space state. Thus, when the line switches from a value of 1 to a value of 0, the receiver is alerted for receiving the message. The asynchronous transmission is most commonly used by microcomputers.

Imran Zafar writes articles about computer basics and database management such as meaning of computer, file organization and relation in database.

g. Emerging technologies in telecommunications

IT and communications

Emerging technology	Status	Potentially marginalized technologies	Potential applications	Related articles
4G cellular communication	First commercial LTE networks deployed in Sweden December 2009; candidate systems LTE-advanced and IEEE 802.16m (Mobile WiMAX Release 2) in development	broadband	Pervasive computing	Mobile broadband, mobile TV, Interactive TV, 3D-TV,[75]holographic cameras[75]
Ambient intelligence	Theory			
Artificial brain	Research[76]		Neurological disease's treatments, artificial intelligence	Blue Brain Project
Artificial intelligence	Theory, experiments; limited uses in specialized domains[77][78][79]	Human decision, analysis, etc.	Creating intelligent devices	Progress in artificial intelligence, technological

Emerging technology	Status	Potentially marginalized technologies	Potential applications	Related articles
				singularity, applications of artificial intelligence
Atomtronics	Theory			
Augmented Reality	diffusion			
Cybermethodology				
Emerging memory technologies T-RAM, Z-RAM, TTRAM, CBRAM, SONOS, RRAM, Racetrack memory, NRAM, Millipede memory	In development	Current memory technologies		
Fourth-generation optical discs (3D optical data storage, Holographic data storage)	Research, prototyping[80]	All other mass storage methods/devices, magnetic tape data storage, optical data storage	Storing and archiving data previously erased for economic reasons	Holographic Disc stores Ultra HD big Electronic IT companies are interested in this technology it has bigger capacity than Blu-ray Disc 10x times more than optical storage
General-purpose computing on graphics processing units	Diffusion of non standardized methods	CPU for a few specialized uses	Order of magnitude faster processing of parallelizable	

Emerging technology	Status	Potentially marginalized technologies	Potential applications	Related articles
			algorithms	
Machine augmented cognition, exocortices	Diffusion of primitive amplifications; working prototypes of more; theory, experiments on more substantial amplification	Libraries, schools, training, pocket calculators		
Machine translation	Diffusion[81][82]	Human translation of natural languages, in areas where misunderstanding is non-critical and language is formalized	Easier and cheaper cross-cultural communication	
Machine vision	Research, prototyping, commercialization[76]	Biotic vision and perception, including humans	Biometrics, controlling processes (e.g., in driverless car, automated guided vehicle), detecting events (e.g., in visual surveillance), interaction (e.g., in human-computer interaction), robot vision	Computer vision, pattern recognition, digital image processing
Mobile collaboration	Development, commercialization[83]	Traditional video-conferencing systems	Extends the capabilities of video conferencing for use on hand-held mobile devices in real-time	

Emerging technology	Status	Potentially marginalized technologies	Potential applications	Related articles
			over secure networks. For use in diverse industries such as manufacturing, energy, healthcare.[84]	
Optical computing	Theory, experiments; some components of integrated circuits have been developed[85]	Many electronics devices, integrated circuits	Smaller, faster, lower power consuming computing	
Quantum computing	Theory, experiments,[86] commercialization[87]	Atomtronics, Electronic computing, optical computing, quantum clock	Much faster computing, for some kinds of problems, chemical modeling, new materials with programmed properties, theory of high-temperature superconductivity and superfluidity	
Quantum cryptography	Commercialization[88]		Secure communications	
Radio-frequency identification	Diffusion of high cost[89][90][91]	Barcode	Smartstores - RFID based self checkout (keeping track of all incoming and outgoing products), food packaging,	

Emerging technology	Status	Potentially marginalized technologies	Potential applications	Related articles
			smart shelves, smart carts. See: potential uses	
Semantic Web or answer machine	Theory, research	Search engines	Making the web machine-readable by annotating data on the web based on its meaning	
Speech recognition	Research,Development,Commercialization	Mechanical input devices		
Three-dimensional integrated circuit	Development, commercialization[92][93]	Conventional integrated circuit		
Virtual Reality	diffusion	Television	Entertainment, education	

h. ISDN [2003-Define]

Integrated Service Digital Network, or ISDN, is the original high-speed internet service. It sparked the high-speed internet development between service providers during the 1990's and, of course, revolutionized internet use. Much like its predecessor, the dial-up internet service, ISDN utilizes a phone line. In fact, it set the standard for telephone data service.

ISDN internet service was the improvement upon dial-up, and it also paved the way for DSL and cable-modem internet service thereafter. It can be considered the step of internet evolution that lies between dial-up and DSL/Cable. Modernizing internet use and bringing high-speed access inside the home, ISDN became the standard by which rival broadband internet service providers competed. Although ISDN internet service still exists, like the dial-up connection it is being replaced by faster and cheaper services that the broadband companies are providing. Regardless, broadband high-speed internet service is still compared with ISDN today since they both represent the standard of their times.

ISDN internet service is basically a telephone-based network system that operates by a circuit switch, or dedicated line. It can transmit data and phone conversations digitally over normal telephone wires. This makes it both faster and of higher quality than dial-up internet service. During the 1990's this revolutionized the way people did business. No longer would you have to miss a call in order to access your

internet, or shut down the internet to make a telephone call. As such, ISDN internet service made video teleconferencing not only possible, but very popular at this time as well.

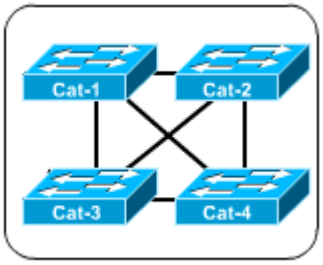
There are two different types, or lines, of ISDN internet service. The first is a basic rate ISDN line. Called a Basic Rate Interface (BRI), this line has two data, or bearer, channels that operate at 64 kbit/sec. Two or more ISDN-BRI lines can be combined as well, yielding speeds of 256 kbit/sec. Combining these lines is common for video conferencing use or for transmitting data at higher speeds. The second type of ISDN line is called a primary rate line, or Primary Rate Interface (PRI). This line had 23 bearer channels and has a total speed of 1,544 kbit/sec. It is used mostly for telephone communication rather than data transmission, particularly within companies that have large, private telephone exchange systems operating inside their business.

The advantages of having ISDN internet service definitely lies in the data lines themselves. Not only do you have constant data speed via these lines, each bearer channel runs at 64 kbit/sec with the ability to be combined to reach greater speeds. ISDN internet serviced also allows for multiple data transmission, so telephone calls and data downloading are no longer mutually exclusive. The disadvantages, however, is that the digital clarity of ISDN voice communication and its speedy data transmission come at an extra cost. ISDN is billed like a phone line, but with an added cost for service. And although its operational distance from the ISDN central office is greater than that for DSL, its terminal adaptor (similar to a modem) is more expensive than DSL or cable modems. While this equipment and service continue to remain costly, it is leaving the way open for other internet services, like broadband, to quickly replace ISDN's share of the marketplace.

23. Discuss Spanning Tree Protocol. [2003]

Spanning-Tree Protocol (STP) is a **loop-prevention protocol used in switching environment**. It is a technology that allows switches to **communicate with each other to discover physical loops** in the network. The protocol uses an **algorithm** to create a *loop-free logical* topology.

Looping means a packet sent by a switch from one outbound port is received by the same switch. Then the topology is said to be in loop. Loops may occur in a network for a variety of reasons. However, loops can occur by configuration error due to creating redundant links.



When a switch receives a frame and it does not find any entry for destination address in MAC table it broadcasts it to all ports. So, when other switches receive the same packet and if they too don’t find any entry in their MAC table, they will also broadcast the frame to all available ports. Thus every switch in the topology uses broadcast unless and until the destination is found and thus can create a loop.

So in order to resolve this scenario a protocol called as STP was developed by DIX (Digital, Intel and Xerox) as a switching loop prevention protocol. Then IEEE created their own version of STP called as 802.1d. **The goal behind developing STP is to create a loop free network by block redundant link.**

How STP works

Before we learn how STP works, we have to go through some basic concepts regarding it.

- **Bridge ID -** A Bridge ID is a single 8 byte value which consists of two fields i.e. Bridge Priority and MAC address.

- **Bridge Priority -** The Bridge Priority is 2 byte value assigned to switch between values 0 to 65535. The default value is 32768.

- **MAC address -** Every switch has its own MAC address like Host MAC address.

- **Root Bridge -** A root bridge is bridge with lowest bridge ID. The Root Bridge **takes seniority** in loop prevention.

- **Port Cost -** Switches uses a concept of cost to find how switches are closer to each other. The cost of each link is calculated as –

Port cost = 1000/bandwidth of port

Therefore,

10 Mbps port cost = 1000/100 = 100 cost

100 Mbps port cost = 1000/100 = 10 cost

- **Path Cost -** Path cost is the **total cost** of each port from one switch to another switch.

Election of Root Bridge - The **first step** used by STP for loop avoidance is **election of Root Bridge**.

A root bridge is designated or elected by an election between switches. Each switch sends BPDU to each other containing its Bridge ID. The switch with **lowest bridge ID** wins the race and is elected as Root Bridge. All ports on Root Bridge are called as designated ports, which are always in forwarding state.

Next, all switch **ports which are directly connected to root Bridge** are called as **Root Port**. Root port are ports which are directly connected to root bridge or which have shortest path cost to root bridge.

STP port states

Forwarding state - Sending / receiving user data

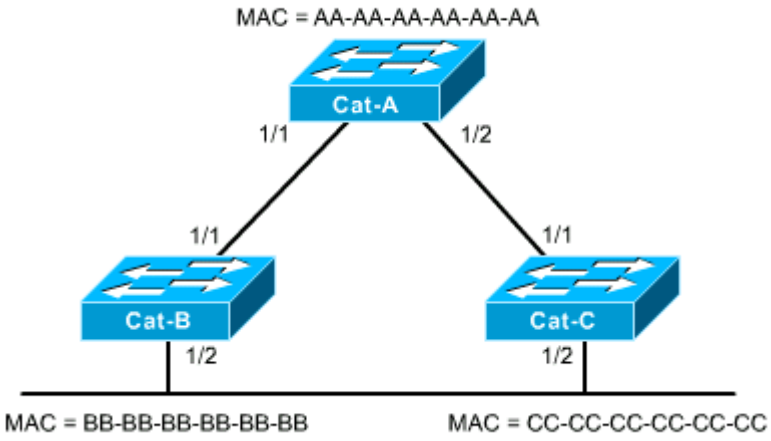
Learning state - Building switch table

Listening state - Building topology

Blocking - No data send and receive

Disable - Down state

Let's see a sample topology and find out how STP works to create a loops free environment.



In the above topology each switch sends BPDU to each other for election of Root Bridge. In this case, **CAT-A** switch wins and is elected as **Root bridge** based on Bridge ID. **Every port on Root Bridge is called are Designated port**.

After election of Root bridge the next step is to **elect root port**. **The root port of a bridge is the port that is closest to the root bridge**. Every non-root bridge should have a root port. The election of root port on each non-root bridge is **done via port cost and path cost**. So in our case switch CAT-B has 2 paths to Root Bridge - one is via port 1/1 and other is via port 1/2. But the path via 1/1 is lowest than 1/2, **so port 1/1 is elected as root port.**

Assuming all switches ports are of 100 mbps,

Port cost of 1/1 port = 1000/100 = 10

Path cost of 1/1 to root bridge = cost of port 1/1 on CAT-A + cost of port 1/1 on CAT-B

= 10+10 = 20

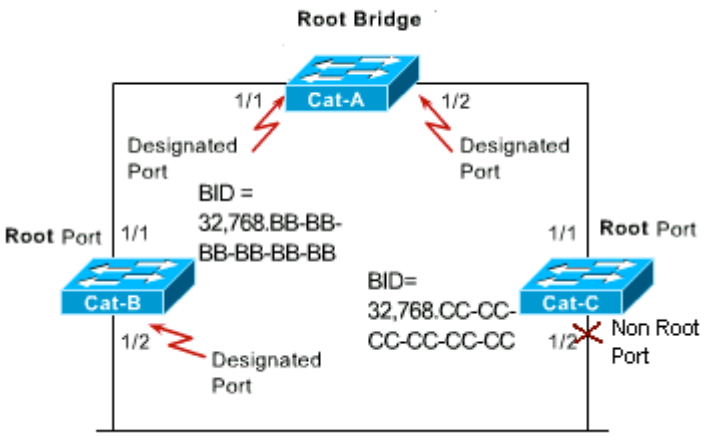
Port cost of 1/2 port = 1000/100 = 10

Path cost of 1/2 to root bridge = cost of port 1/2 on CAT-A + cost of port 1/1 on CAT-C + cost of 1/1 on CAT-c + cost of port 1/2 on CAT-A

= 10+10+10+10 = 40

So the total path cost of 1/1 on CAT-B is lower than cost of 1/2. **So port 1/1 is elected as root port**. The other remaining port is called as designated port i.e. port 1/2

The same root applies to port 1/1 on CAT-C switch. The port 1/1 is elected as root port for CAT-C switch.



After election of root ports on each switch, the **next step** is **election of designated ports**.

Since both port on switch CAT-B and CAT-C are nearest to Root Bridge and have equal cost there is a tie. To solve this tie we have to select one switch as designated switch. The designated switch is elected based on Bridge ID. The switch with **lowest Bridge ID** is elected as Designated switch. So in our case CAT-B is designated Bridge and port 1/2 on it is called as designated port. The port on CAT-C is called as **Non-Root Port**, **which is always in blocking state** and **will not be able to send and receive data on this port thus preventing looping**. This is how STP works in order to avoid looping.

24. SN:
    a. Proprietary Technology v/s Open Technology [2010,2004]

Broadly, the platforms can be categorised into two groups: Open Source and Proprietary.

Open Source Systems:

- Are built and maintained by groups of interested people all over the world. While there is typically one controlling body, they belong to no one.
- Make the source code available to all. Anyone with the skills and time can extend and modify the code and create new functionality as required.
- Can be hosted anywhere. You can host an open source web site with just about any ISP or hosting company on their servers or your own.
- Are typically free – or at least the software itself is. Customisation, design, and hosting are not.

Proprietary Systems:

- Are built and maintained by a single company.
- Typically do not allow access to the source code, although the best of them provide an open framework (or API) that means they can be extended by others.
- Are typically hosted by the company that created them, although some can be hosted elsewhere.
- Typically require a license fee of some sort, although it is often built into the hosting charges.

There are pros and cons for each, and which is best for you will depend on your requirements.

Open Source

There are a number of popular open source platforms, including Wordpress, Joomla, Drupal, DotNetNuke, Mambo and many many more. Which one is best will typically depend on who you ask; every web developer has a favourite and all will tell you theirs is the most complete, easiest to use and most cost effective!

The only thing for sure at the moment is that Wordpress is by far the most popular and is rapidly becoming the default standard. If starting fresh with an open source solution you would need to have a very good reason not to choose Wordpress.

- So when is an open source solution best for you:
- You want a solution that is quick and cheap up front and don't mind using a basic template design to get started. Recommended only for the smallest of businesses that just need a brochure to get started.
- You have the time and expertise to create your own website from one of the template sites (technically not quite open source – while they are typically based on Wordpress they lock you in to a proprietary host).
- You have a unique idea and need to build custom functionality into your website.
- Your online presence is your business and you will be investing all of your time enhancing, tweaking and improving your website.
- Your blog is your business, in which case you really should use Wordpress.
- You are comfortable making choices about technology including add-ons and enhancements and hosting. The great thing about open source is there are hundreds of companies making add-ons, the bad thing is at some point you will need to evaluate and choose.
- You (or your technology partner) have a plan to keep the software updated for bugs, security issues and enhancements.

Key issues with open source:

- You get what you pay for. Building a website on an open source solutions is not free, but basic template sites are very cheap. They also look cheap. Expect to pay well for a good, unique design.
- Support for, and upgrades to the software are typically not included. While there are thousands of developers in the open source community enhancing the software, none of them are working on your website. Unless you have a support agreement with your developer, your website will remain on the version it was installed on, complete with any bugs and security issues. If you want access to the latest enhancements you will typically have to pay your developer to install them.
- While you have access to the source code, the design may not be yours. Template websites in particular have this problem, and you often cannot move the design to another host and definitely not to another platform. You also typically cannot use the design on printed material or elsewhere. If you are getting custom design make sure you own it and not the designer/developer (applies equally to Proprietary).

- The majority of web developers using open source solutions are not actually software developers. While they may be experts at customising the design and working with various modules, they will not be able to develop truly custom software or fix bugs and other shortcomings. They will be reliant on the community for that.
- In theory you can move your website to another developer if unhappy. In reality this can be difficult due to design ownership, customisations and modules, and because each developer has their own preference for and knowledge of the various systems and add-ons. Moves that do not involve a redesign and/or rebuild are rare.
- Pick the wrong software and in 2-3 years' time you might find the community have moved on and development has stalled (hence the recommendation above to choose Wordpress which is unlikely to lose favour any time soon).

Proprietary Systems

Like open source, proprietary systems come in many, many flavours. A decade ago just about every software developer that did webdesign created their own CMS (Content Management System). Most of these have disappeared over the years as the open source solutions have improved.

The key issue with proprietary systems is that you must be comfortable with the company behind them. They must have the size and expertise to not only keep your website running, but be able to invest in the continual development of the product. You also need to understand that you probably can't move your website elsewhere, so at least make sure you have ownership over the design and content (a tip that applies equally to open source solutions).

A Proprietary solution will be best for you if:

- Your online presence is important to you, but not necessarily your whole business.
- Your online presence is your business, but you just need to focus on the content not the technology and your functional needs are met by the software.
- You do not require custom development other than a great design.
- You have no interest in the technology behind it and just want to take care of the content (and the rest of your business).
- You don't want to deal with updates, bugs and security issues and want a full service hosting plan.
- You don't want to deal with decisions on which modules may be best, or deal with issues like upgrading the platform and finding that 3 of the 16 add-ons you use also require an upgrade to continue to function.
- You want to just pick a solution and a partner and have it tick away in the background for the next several years, but also have the technology stay up to date.

Key issues with Proprietary solutions include:

- Companies and software solutions come and go. You must have confidence in the company offering the solution and that they will both be around and able to continually invest in the product.

- You need to ensure you have ownership and access to the content and design should you decide to move on for any reason (applies equally to open source solutions). Many companies will not provide this by default.
- You may have little option for software enhancements or customisations or they may be very expensive. You are likely to be limited to the standard modules and functionality available, so make sure the solution is comprehensive and developing (even if you don't need all of it now a comprehensive product suite is a good sign for the future.).
- Many of the proprietary platforms have simply not kept up with changes like social networking and Google's many updates to search algorithms. Many of them are simply woefully inadequate and/or difficult to use – solutions aimed at vertical markets (like real estate or plant and machinery) are often in this bucket as they made a grab for market share early on and then simply stopped developing. Again, make sure your technology partner continues to invest.

Hopefully that helps. They key with open source solutions is to pick both the right technology, and the right partner to assist you with it. At the moment the technology favourite is Wordpress, and there is no shortage of companies working with it (some very good, and many that struggle). For those on a very tight budget or who need highly customised software we recommend Wordpress.

The key with a proprietary solution is to pick the right company with the complete product set and the capacity to continue to support and develop the solution. Bloomtools is a leader in this market internationally, because they tick all the boxes including product set, R&D and company stability. It is the best solution for the majority of small and medium businesses who are serious about getting results from their online presence and want cost effective, set-and-forget technology.

b. Analog & Digital Signals, their comparison [2010,2004]

Analog vs Digital

Analog and digital signals are used to transmit information, usually through electric signals. In both these technologies, the information, such as any audio or video, is transformed into electric signals. The difference between analog and digital technologies is that in analog technology, information is translated into electric pulses of varying amplitude. In digital technology, translation of information is into binary format (zero or one) where each bit is representative of two distinct amplitudes.

Comparison chart

	Analog	Digital
Signal:	Analog signal is a continuous signal which represents physical measurements.	Digital signals are discrete time signals generated by digital modulation
Waves:	Denoted by sine waves	Denoted by square waves
Representation:	Uses continuous range of values to represent information	Uses discrete or discontinuous values to represent information

	Analog	Digital
Example:	Human voice in air, analog electronic devices.	Computers, CDs, DVDs, and other digital electronic devices.
Technology:	Analog technology records waveforms as they are.	Samples analog waveforms into a limited set of numbers and records them.
Data transmissions:	Subjected to deterioration by noise during transmission and write/read cycle.	Can be noise-immune without deterioration during transmission and write/read cycle.
Response to Noise:	More likely to get affected reducing accuracy	Less affected since noise response are analog in nature
Flexibility:	Analog hardware is not flexible.	Digital hardware is flexible in implementation.
Uses:	Can be used in analog devices only.	Computing and digital electronics
Applications:	Thermometer	PCs, PDAs

Definitions of Analog vs Digital signals

An Analog signal is any continuous signal for which the time varying feature (variable) of the signal is a representation of some other time varying quantity, i.e., analogous to another time varying signal. It differs from a digital signal in terms of small fluctuations in the signal which are meaningful.

A digital signal uses discrete (discontinuous) values. By contrast, non-digital (or analog) systems use a continuous range of values to represent information. Although digital representations are discrete, the information represented can be either discrete, such as numbers or letters, or continuous, such as sounds, images, and other measurements of continuous systems.

Properties of Digital vs Analog signals

Digital information has certain properties that distinguish it from analog communication methods. These include

- Synchronization – digital communication uses specific synchronization sequences for determining synchronization.
- Language – digital communications requires a language which should be possessed by both sender and receiver and can should specify meaning of symbol sequences.
- Errors – disturbances in analog communication causes errors in actual intended communication but disturbances in digital communication does not cause errors enabling error free communication. Errors should be able to substitute, insert or delete symbols to be expressed.
- Copying – analog communication copies are quality wise not as good as their originals while due to error free digital communication, copies can be made indefinitely.
- Granularity – for a continuously variable analog value to be represented in digital form there occur quantization error which is difference in actual analog value and digital representation and this property of digital communication is known as granularity.

Differences in Usage in Equipment

Many devices come with built in translation facilities from analog to digital. Microphones and speaker are perfect examples of analog devices. Analog technology is cheaper but there is a limitation of size of data that can be transmitted at a given time.

Digital technology has revolutionized the way most of the equipments work. Data is converted into binary code and then reassembled back into original form at reception point. Since these can be easily manipulated, it offers a wider range of options. Digital equipment is more expensive than analog equipment.

Comparison of Analog vs Digital Quality

Digital devices translate and reassemble data and in the process are more prone to loss of quality as compared to analog devices. Computer advancement has enabled use of error detection and error correction techniques to remove disturbances artificially from digital signals and improve quality.

Differences in Applications

Digital technology has been most efficient in cellular phone industry. Analog phones have become redundant even though sound clarity and quality was

Analog technology comprises of natural signals like human speech. With digital technology this human speech can be saved and stored in a computer. Thus digital technology opens up the horizon for endless possible uses.

c. Noise & Attenuation of signals & measure to reduce it. [2010]

Definition:

In communication studies and information theory, anything that interferes in the communication process between a speaker and an audience.

Noise can be external or internal, and it can disrupt the communication process at any point.

Examples and Observations:

- Four Kinds of Noise
  "There are four kinds of noise. Physiological noise is distraction caused by hunger, fatigue, headaches, medication, and other factors that affect how we feel and think. Physical noise is interference in our environments, such as noises made by others, overly dim or bright lights, spam and pop-up ads, extreme temperatures, and crowded conditions. Psychological noise refers to qualities in us that affect how we communicate and interpret others. For instance, if you are preoccupied with a problem, you may be inattentive at a team meeting. Likewise, prejudice and defensive feelings can interfere with communication. . . . Finally, semantic noise exists when words themselves are not mutually understood. Authors sometimes create semantic noise by using jargon or unnecessarily technical language.
  (Julia T. Wood, Interpersonal Communication: Everyday Encounters, 6th ed. Wadsworth 2010)

- Noise in Intercultural Communication
  For effective communication in an intercultural interaction, participants must rely on a common

language, which usually means that one or more individuals will not be using their native tongue. Native fluency in a second language is difficult. especially when nonverbal behaviors are considered. People who use another language will often have an accent or or might misuse a word or phrase, which can adversely affect the receiver's understanding of the message. This type of distraction, referred to as semantic noise, also encompasses jargon, slang, and even specialized professional terminology."
(Edwin R. McDaniel et al., "Understanding Intercultural Communication: The Working Principles." Intercultural Communication: A Reader, 12th ed., ed. by Larry A. Samovar, Richard E. Porter, and Edwin R. McDaniel. Wadsworth, 2009)

- Noise is any random or persistent disturbance that obscures, reduces, or confuses the clarity or quality of the message being transmitted. In other words, it is any interference that takes place between the sender and the receiver. This is why we generally identify any communication problem that can't be fully explained as "noise." The biggest single cause of noise in the communication process may be the assumption that the act of communicating is a simple process - that it doesn't require much thought or practice and all effective managers were born with this skill. This is not true. Effective communication comes with study and practice. The effectiveness of the communication process is dependent upon the capabilities of the senders and receivers.

- To overcome the noise barrier to effective communication, one must discover its source. This may not be easy. Noise appears in a variety of ways. During a conversation, have you ever been distracted by the pictures on the wall, the view from the window, a report lying open on a desk, or a conversation taking place in an adjacent room? Many people have been so distracted.

- In the perusal of a written communication, have you ever been confused by irrelevant material or the illogical approach taken by the author? Again, many people have.

- Once the source, or sources, of the noise has been identified, steps can be taken to overcome it. The noise barrier can't always be overcome but, fortunately, just the awareness of its existence by either the sender or the receiver of a message can help to improve the communication flow.

Definition - What does Attenuation mean?

Attenuation is a telecommunications term that refers to a reduction in signal strength commonly occurring while transmitting analog or digital signals over long distances.

Attenuation is historically measured in dB but it can also be measured in terms of voltage.

Attenuation can relate to both hard-wired connections and to wireless transmissions.

There are many instances of attenuation in telecommunications and digital network circuitry. Inherent attenuation can be caused by a number of signaling issues including:

- Transmission medium - All electrical signals transmitted down electrical conductors cause an electromagnetic field around the transmission. This field causes energy loss down the cable and gets worse depending upon the frequency and length of the cable run. Losses due to

- Crosstalk from adjacent cabling causes attenuation in copper or other conductive metal cabling.

- Conductors and connectors - Attenuation can occur as a signal passes across different conductive mediums and mated connector surfaces.

Repeaters are used in attenuating circuits to boost the signal through amplification (the opposite of attenuation). When using copper conductors, the higher the frequency signal, the more attenuation is caused along a cable length. Modern communications use high frequencies so other mediums which have a flat attenuation across all frequencies, such as fiber optics are used instead of traditional copper circuits.

Different types of attenuation include:

- Deliberate attenuation can occur for example where a volume control is used to lower the sound level on consumer electronics.
- Automatic attenuation is a common feature of televisions and other audio equipment to prevent sound distortion by automatic level sensing that triggers attenuation circuits.
- Environmental attenuation relates to signal power loss due to the transmission medium, whether that be wireless, copper wired or fiber optic connected.

d. Various bodies that form standards for networking & communication. [2010]

An Internetwork
An internetwork is simply a network of networks. The networks can be in the same building, on a campus or across the country. They can use the same or different technology. In allcases, however, they need an internetworking device, such as a router or bridge, to propagate the required packets to the other network and a routing protocol to decide which ones need to make the trip.
Interconnectivity Networks are usually homogeneous. They are designed for and owned by one organization. Allowance can be made for the types of machines found on the system and the applications used by its members. Internetworks, however, often connect networks owned by different organizations. Allowing them to communicate with each other requiresinternetworking devices that can convert the electrical signals from one kind of system to another. Interconnectivity is usually seen as a problem at the physical level of the network.
Interoperability Although an IBM PC and an Apple Macintosh may communicate over the same Ethernet network, will they understand each other? This is a problem in interoperability. It can be related to the transport protocols, the network operating system or even between software applications.

Standards Organizations (or who controls our lives anyway?)

- International Standards Organization (ISO)
- Open Systems Interconnect (OSI) reference model of networking
- Institute of Electrical and Electronic Engineers (IEEE)
- 802.3 committee, governs Ethernet
- 802.5 committee, governs Token Ring
- 802.11 committee, governs wireless LANs
- American National Standards Institute (ANSI)
- ASCII and ANSI character codes
- FDDI
- Comite Consultatif Internationale Telegraphique et Telephonic
- (CCITT), International Telephone Union (ITU)
- V series modems, error correcting and compression protocols
- X series data communication protocols

- H.323, a Voice over IP protocol
- Electrical Industry Association (EIA)
- Cable specs especially 6 categories of UTP cable.
- RS232
- Internet Engineering Task Force (IETF)
- TCP/IP
- SIP, a Voice over IP protocol
- All Internet protocols
- World Wide Web Consortium (W3W)
- HTML, XML, CSS, DOM

NOTE: Please explain above points in short in your own language.

e. DHCP. How does it efficiently use IP addresses? [2007]

Short for Dynamic Host Configuration Protocol, DHCP is a protocol for assigning IP addresses dynamically to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task.DHCP also supports a mix of static and dynamic IP addresses.

Normally the DHCP server provides the client with at least this basic information:

- IP Address
- Subnet Mask
- Default Gateway

Other information can be provided as well, such as Domain Name Service (DNS) server addresses and Windows Internet Name Service (WINS) server addresses. The system administrator configures the DHCP server with the options that are parsed out to the client.

How does the DHCP work?

In a network, a DHCP server manages a pool of IP addresses, as well as default gateway details, DNS details and other information for the clients' network configuration. When a new computer is introduced into a DHCP server-enabled network, it will send a query to the DHCP server requesting all the necessary information. When the query reaches the DHCP server, it will grant the new computer a new IP address and a lease - a time frame for which the computer can use this IP address, as well as other configuration details. The whole process takes place immediately after the new computer boots, and to be successful, it has to be completed before initiating IP based communication with other hosts in the network.

DHCP allocation methods

Depending on its configuration, the DHCP server can work in 3 ways:

1. **Dynamic allocation**

When the DHCP server is configured to use dynamic allocation, this means that it uses a lease policy. This way, when an assigned IP address from the available pool is no longer used, it will be transferred back to

the pool, making it available for someone else to use. The advantage of this method is that the IP addresses are used to their maximum - as soon as they are no longer used by the client, they are instantly made available to others. The disadvantage of this method is that a client will always have a random IP address.

2. **Automatic allocation**

The automatic allocation method resembles very much the dynamic allocation method - as soon as a client connects, the DHCP server provides him with an IP address from the IP address pool. However, when automatic allocation is used, the DHCP server keeps a database of previous IP grants, and tries to give the client the same IP address he used the last time, if available.

3. **Static allocation**

The static allocation method is very popular in modern ISP networks, which do not use dial-up methods. With the static allocation, the DHCP sever keeps a database with all clients' LAN MAC addresses and gives them an IP address only if their MAC address is in the database. This way, the clients can be sure that they will be getting the same IP address every time.

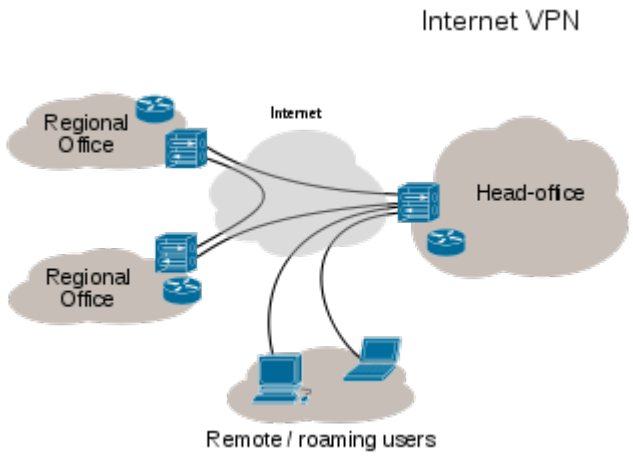
A DHCP server can be set to work using a combination of the allocation methods. For example, in a public WiFi network, all of the known hosts and permanent clients can use the static allocation, whereas for guests, the dynamic allocation is used. This way, known hosts can always use the same IP address and the IP address pool is equally available to everyone.

f. VPN's-their utility [2007,2004, 2003]

A virtual private network (VPN) extends a private network and the resources contained in the network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if it were a private network with all the functionality, security and management policies of the private network.[1] This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.

The VPN connection across the Internet is technically a wide area network (WAN) link between the sites but appears to the user as a private network link—hence the name "virtual private network".

VPNs can be either remote-access (connecting an individual computer to a network) or site-to-site (connecting two networks together). In a corporate setting, remote-access VPNs allow employees to access their company's intranet from home or while traveling outside the office, and site-to-site VPNs allow employees in geographically separated offices to share one cohesive virtual network. A VPN can also be used to interconnect two similar networks over a dissimilar middle network; for example, two IPv6 networks over an IPv4 network



VPN systems can be classified by:

- the protocols used to tunnel the traffic
- the tunnel's termination point, i.e., customer edge or network-provider edge
- whether they offer site-to-site or remote-access connectivity
- the levels of security provided
- the OSI layer they present to the connecting network, such as Layer 2 circuits or Layer 3 network connectivity

Security mechanism in VPN

VPNs typically require remote access to be authenticated and make use of encryption techniques to prevent disclosure of private information.

VPNs provide security through tunneling protocols and security procedures[7] such as encryption. Their security model provides:

- Confidentiality such that even if traffic is sniffed, an attacker would only see encrypted data which they cannot understand; (see Packet analyzer and Deep packet inspection);
- Allowing Sender authentication to prevent unauthorized users from accessing the VPN;
- Message integrity to detect any instances of transmitted messages having been tampered with

Secure VPN protocols include the following:

- IPSec (Internet Protocol Security) was developed by the Internet Engineering Task Force (IETF), and was initially developed for IPv6, which requires it. This standards-based security protocol is also widely used with IPv4. Layer 2 Tunneling Protocol frequently runs over IPSec. Its design meets most security goals: authentication, integrity, and confidentiality. IPSec functions through encrypting and encapsulating an IP packet inside an IPSec packet. De-encapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination.
- Transport Layer Security (SSL/TLS) can tunnel an entire network's traffic, as it does in the OpenVPN project, or secure an individual connection. A number of vendors provide remote access VPN

capabilities through SSL. An SSL VPN can connect from locations where IPsec runs into trouble with Network Address Translation and firewall rules.

- Datagram Transport Layer Security (DTLS), is used in Cisco AnyConnect VPN or OpenConnect VPN, to solve the issues SSL/TLS has with tunneling over UDP.
- Microsoft Point-to-Point Encryption (MPPE) works with the Point-to-Point Tunneling Protocol and in several compatible implementations on other platforms.
- Microsoft's Secure Socket Tunneling Protocol (SSTP), introduced in Windows Server 2008 and in Windows Vista Service Pack 1. SSTP tunnels Point-to-Point Protocol (PPP) or Layer 2 Tunneling Protocol traffic through an SSL 3.0 channel.
- MPVPN (Multi Path Virtual Private Network). Ragula Systems Development Company owns the registered trademark "MPVPN".
- Secure Shell (SSH) VPN - OpenSSH offers VPN tunneling (distinct from port forwarding) to secure remote connections to a network or inter-network links. OpenSSH server provides a limited number of concurrent tunnels and the VPN feature itself does not support personal authentication.

Authentication in VPN

- Tunnel endpoints must authenticate before secure VPN tunnels can be established.
- User-created remote access VPNs may use passwords, biometrics, two-factor authentication or other cryptographic methods.
- Network-to-network tunnels often use passwords or digital certificates, as they permanently store the key to allow the tunnel to establish automatically and without intervention from the user.

Mobile VPN

Mobile VPNs are used in a setting where an endpoint of the VPN is not fixed to a single IP address, but instead roams across various networks such as data networks from cellular carriers or between multiple Wi-Fi access points.[24] Mobile VPNs have been widely used in public safety, where they give law enforcement officers access to mission-critical applications, such as computer-assisted dispatch and criminal databases, while they travel between different subnets of a mobile network.[25] They are also used in field service management and by healthcare organizations,[26] among other industries.

Increasingly, mobile VPNs are being adopted by mobile professionals who need reliable connections.[26] They are used for roaming seamlessly across networks and in and out of wireless-coverage areas without losing application sessions or dropping the secure VPN session. A conventional VPN cannot survive such events because the network tunnel is disrupted, causing applications to disconnect, time out,[24] or fail, or even cause the computing device itself to crash.[26]

Instead of logically tying the endpoint of the network tunnel to the physical IP address, each tunnel is bound to a permanently associated IP address at the device. The mobile VPN software handles the necessary network authentication and maintains the network sessions in a manner transparent to the application and the user.The Host Identity Protocol (HIP), under study by the Internet Engineering Task Force, is designed to support mobility of hosts by separating the role of IP addresses for host identification from their locator functionality in an IP network. With HIP a mobile host maintains its logical connections

established via the host identity identifier while associating with different IP addresses when roaming between access networks.

g. ATM technology [2007]
h. Circuit Switched and Packet Switched Networks [2007, 2004]
i. VOICE over IP [2007]

Voice over IP (VoIP, abbreviation of voice over Internet Protocol) commonly refers to the communication protocols, technologies, methodologies, and transmission techniques involved in the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. Other terms commonly associated with VoIP are IP telephony, Internet telephony, voice over broadband (VoBB), broadband telephony, IP communications, and broadband phone.

Internet telephony refers to communications services—voice, fax, SMS, and/or voice-messaging applications—that are transported via the Internet, rather than the public switched telephone network (PSTN). The steps involved in originating a VoIP telephone call are signaling and media channel setup, digitization of the analog voice signal, encoding, packetization, and transmission as Internet Protocol (IP) packets over a packet-switched network. On the receiving side, similar steps (usually in the reverse order) such as reception of the IP packets, decoding of the packets and digital-to-analog conversion reproduce the original voice stream.[1] Even though IP telephony and VoIP are used interchangeably, IP telephony refers to all use of IP protocols for voice communication by digital telephony systems, while VoIP is one technology used by IP telephony to transport phone calls.

VoIP systems employ session control protocols to control the set-up and tear-down of calls as well as audio codecs which encode speech allowing transmission over an IP network as digital audio via an audio stream. The choice of codec varies between different implementations of VoIP depending on application requirements and network bandwidth; some implementations rely on narrowband and compressed speech, while others support high fidelity stereo codecs. Some popular codecs include u-law and a-law versions of G.711, G.722 which is a high-fidelity codec marketed as HD Voice by Polycom, a popular open source voice codec known as iLBC, a codec that only uses 8 kbit/s each way called G.729, and many others.

VoIP is available on many smartphones and Internet devices so that users of portable devices that are not phones, may place calls or send SMS text messages over 3G or Wi-Fi.

VOIP protocols

- Voice over IP has been implemented in various ways using both proprietary and open protocols and standards. Examples of the network protocols used to implement VoIP include:
- H.323
- Media Gateway Control Protocol (MGCP)
- Session Initiation Protocol (SIP)
- Real-time Transport Protocol (RTP)
- Session Description Protocol (SDP)

- Inter-Asterisk eXchange (IAX)
- JingleXMPP VoIP extensions
- The H.323 protocol was one of the first VoIP protocols that found widespread implementation for long-distance traffic, as well as local area network services. However, since the development of newer, less complex protocols such as MGCP and SIP, H.323 deployments are increasingly limited to carrying existing long-haul network traffic. In particular, the Session Initiation Protocol (SIP) has gained widespread VoIP market penetration.
- A notable proprietary implementation is the Skype protocol, which is in part based on the principles of peer-to-peer (P2P) networking.

Advantages of VoIP

There are several advantages to using voice over IP. The biggest single advantage VoIP has over standard telephone systems is cost. In addition, international calls using VoIP are usually very inexpensive. One other advantage, which will become much more pronounced as VoIP use climbs, is that calls between VoIP users are usually free. Using services such as TrueVoIP, subscribers can call one another at no cost to either party.[13]

Operational cost

VoIP can be a benefit for reducing communication and infrastructure costs. Examples include:

- Routing phone calls over existing data networks to avoid the need for separate voice and data networks.
- The ability to transmit more than one telephone call over a single broadband connection.
- Secure calls using standardized protocols (such as Secure Real-time Transport Protocol). Most of the difficulties of creating a secure telephone connection over traditional phone lines, such as digitizing and digital transmission, are already in place with VoIP. It is only necessary to encrypt and authenticate the existing data stream.

j. Modulation, its needs and methods [2004]

Today vast amounts of information are communicated using radio communications systems. Both analogue radio communications systems, and digital or data radio communications links are used.

However one of the fundamental aspects of any radio communications transmission system is modulation, or the way in which the information is superimposed on the radio carrier.

In order that a steady radio signal or "radio carrier" can carry information it must be changed or modulated in one way so that the information can be conveyed from one place to another.

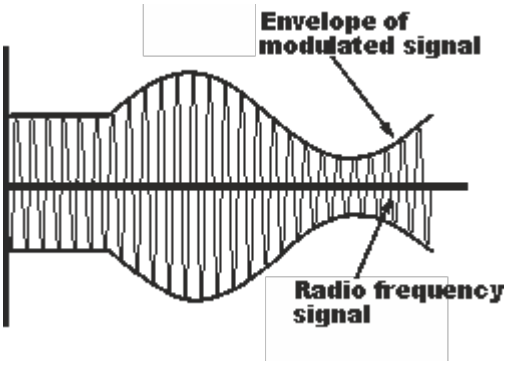
There are very many ways in which a radio carrier can be modulated to carry a signal, each having its own advantages and disadvantages. The choice of modulation have a great impact on the radio communications system. Some forms are better suited to one kind of traffic whereas other forms of

modulation will be more applicable in other instances. Choosing the correct form of modulation is a key decision in any radio communications system design.

Basic types of modulation

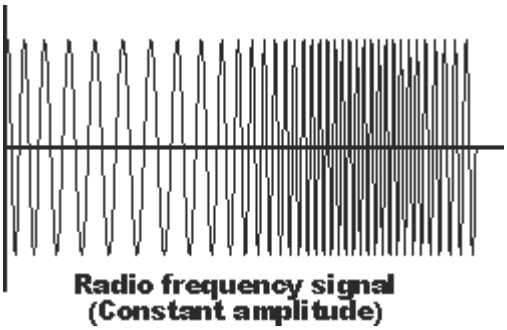
There are three main ways in which a radio communications or RF signal can be modulated:

- Amplitude modulation, AM: As the name implies, this form of modulation involves modulating the amplitude or intensity of the signal.



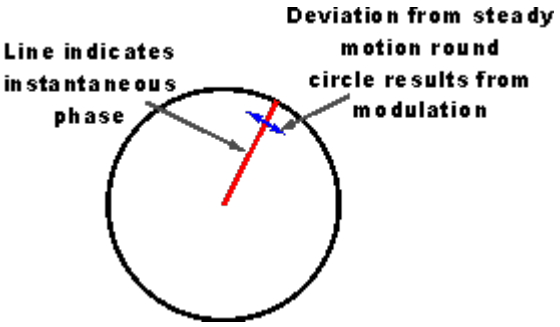
Amplitude modulation was the first form of modulation to be used to broadcast sound, and although other forms of modulation are being increasingly used, amplitude modulation is still in widespread use. Read more . . .

- Frequency modulation, FM: This form of modulation varies the frequency in line with the modulating signal.



Frequency modulation has the advantage that, as amplitude variations do not carry any information on the signal, it can be limited within the receiver to remove signal strength variations and noise. As a result is form of modulation has been used for many applications including high quality analogue sound broadcasting. Read more . . .

- Phase modulation, PM: As the name indicates, phase modulation varies the phase of the carrier in line with the modulating signal.



Phase modulation and frequency modulation have many similarities and are linked - one is the differential of the other. However phase modulation lends itself to data transmissions, and as a result its use has grown rapidly over recent years.

Each type of modulation has its own advantages and disadvantages, and accordingly they are all used in different radio communications applications.

In addition to the three main basic forms of modulation or modulation techniques, there are many variants of each type. Again these modulation techniques are used in a variety of applications, some for analogue applications, and others for digital applications.

Angle Modulation

Angle modulation is a name given to forms of modulation that are based on altering the angle or phase of a sinusoidal carrier. Using angle modulation there is no change inth e amplitude of the carrier.

The two forms of modulation that fall into the angle modulation category are frequency modulation and phase modulation.

Both types of angle modulation, namely frequency modulation and phase modulation are linked because frequency is the derivative of phase, i.e. frequency is the rate of change of phase.

Another way of looking at the link between the two types of modulation is that a frequency modulated signal can be generated by first integrating the modulating waveform and then using the result as the input to a phase modulator. Conversely, a phase modulated signal can be generated by first differentiating the modulating signal and then using the result as the input to a frequency modulator.

Signal bandwidth

One key element of any signal is the bandwidth it occupies. This is important because it defines the channel bandwidth required, and hence the number of channels that can be accommodated within a given segment of radio spectrum. With pressure on the radio spectrum increasing, the radio signal bandwidth is an important feature of any type of radio emission or transmission.

The bandwidth is governed by two major features:

- The type of modulation Some forms of modulation use their bandwidth more effectively than others. Accordingly where spectrum usage is of importance, this alone may dictate the choice of modulation.

- The bandwidth of the modulating signal: A law called Shannon's law determines the minimum bandwidth through which a signal can be transmitted. In general, the wider the bandwidth of the modulating signal, the wider the bandwidth required.

Modulating signal type

Apart from the form of modulation itself the type of signal being used to modulate the carrier also has a bearing on the signal. Analogue and data are two very different forms of modulating signal and need to be treated differently. While different formats of actual modulation may be used, the type of signal being applied via the modulator also has a bearing on the signal.

Signals for high quality stereo broadcasting will be treated differently to signals that provide digital telemetry for example. As a result, it is often important to know the signal type that needs to be carried by the RF carrier.

k. DNS & DHCP as TCP/IP services [2003]

DNS –

Short for Domain Name System (or Service or Server), an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4.

The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

What is DNS?

What does actually stand behind that almighty 3-letter abbreviation - DNS? DNS refers to Domain Name System and represents a powerful Internet technology for converting domain names to IP addresses. Its special mission is to be a mediator between the IP addresses, the system-side names of the websites and their respective domains, and their user-side alpha-numeric titles. Another important function of the DNS is to control the delivery of email messages.

Behind every site, there is an IP address. But, while it's easy to remember the name of a website, it's quite hard to remember the exact IP address. For example, everybody knows about Google.com, but if you had to remember "74.125.45.100", things would have been much harder.

How does DNS work?

A DNS program works like this - every time a domain name is typed in a browser it is automatically passed on to a DNS server, which translates the name into its corresponding IP address (e.g. the domain name NTC Hosting.com is translated to 66.40.65.49). Thanks to the DNS, we do not need to bother to remember complicated numeric combinations to reach a certain website - we can use its meaningful and much easier to remember domain name instead.