SHRI MAHENDRA COMPUTERS, JODHPUR

Computer Networking

Advanced network

HEMANT PRAJAPAT

2008

contact no. 094131-64787

Chapter 1

BASICS OF NETWORKING

- Introduction
- Application of a Network
- Analog & Digital Signals
- Serial & Parallel Transmission
- Asynchronous & Synchronous Transmission.
- Bandwidth

Network:

A computer network is a collection of devices that can store and manipulate electronic data and is interconnected in such a way that network users can store, retrieve and share information.

A network may be vast, comprising of hundreds of computers spread across continents; it may link together mainframes minicomputers and micros, printers, fax machines and pagers; its users may be host of individual enthusiasts or firms; or the network may consist of not more than two machines connected with the sole purpose of sharing a printer or hard disk. In the near future, numerous other types of devices will be network connectable, including interactive TVs, videophones, navigational and environmental control systems.

The larger network systems are generally referred to as Wide Area Networks. Some are run by single organizations, with perhaps the biggest being the world-wide area network run by IBM for its own use, linking its many research establishments and sales organizations. In UK many of the leading chain stores and supermarkets have networks that span the whole country with every store feeding data back to the central organization.

A computer network is a resource, which enables the businesses to gather, analyze, organize and disseminate the information that is essential to their profitability.

The rise of intranets and extranets is an indication of the crucial importance of computer networking to businesses. Intranets and extranets are private business networks that are based on Internet technology.

The Importance of Computer Networks:

Information and communication are two of the most important strategic issues for the success of every enterprise. Today every organization uses a substantial number of computers and communication tools, to communicate with other departments and participate in information retrieval programs, effective usage of information technology, computer networks

are necessary. These networks are a kind (one might call it paradigm) of organization of computer systems produced by the need to merge computers and communications. At the same time they are the means to converge the two areas; the unnecessary distinction between tools to process and store information and tools to collect and transport information can disappear. Computer networks can manage to put down the barriers between information held on several (not only computer) systems. Only with the help of computer networks can a borderless communication and information environment be built.

Computer networks allow the user to access remote programs and remote databases either of the same organization or from other enterprises or public sources. Computer networks provide communication possibilities faster than other facilities. Because of these optimal information and communication possibilities, computer networks may increase the organizational learning rate, which many authors declare as the only fundamental advantage in competition.

What Makes up A Network?

The most important components are, obviously, the computers. A design or engineering office may well have a network composed largely of high-resolution graphic terminals to run their CAD software, with a smattering of PC'S for routine word processing and accounting.

Peripherals: Hard disk drives and tape streamers, printers and plotters, modems and mice. With a network, usually fewer peripherals are needed than with the same number of separate computers, for each user will have access to every peripheral that is attached to the network.

Cables are needed to create the physical links between the computers. Special networking software or Netware is also essential. This provides a means of identifying and addressing each component, and controls the flow of data around the system. When a file is sent to be printed, it is the Netware that ensures that it reaches the right printer;

Applications of Computer Networks

a. Sharing of applications:

This allows all network users to share the same application, saving disk space, because the application only needs to be installed on one of the computers.

b. Sharing of Databases:

Second aspect being multi-user access and modify to the same database at the same time is definitely better than having the same database in all the computers and periodically combine all the modifications together. it is particularly useful for companies like banks and travel agencies.

c. Sharing Resources:

It allows each user to have access to the peripheral devices like printers and scanners. It is certainly cheaper than each terminal having its own peripheral device.

d. Personal Communications:

It allows users to communicate with each other, sending computer files to another user; just by clicking a button and it improves company's efficiency. Users can send messages quickly without any to movement.

e. Cost Effective Resource Sharing:

By selecting the right mix of printers and allowing each network user an appropriate access to them, one could have enough printing power to take care of the needs of all users; one can ensure that, a network enables to share any networkable equipment or software and realize the same benefits that one can enjoy from sharing printer. On a network, users can share modems; data storage devices, such as hard disks and CD-ROM drives; data backup devices, such as tape drivers; E-mail systems; fax machines; and all networkable software. When you compare sharing these resources to purchasing them for each computer, the cost savings can be enormous.

Analog & Digital Signals

Analog Data:

Data that is in the form of continuously variable physical quantities.

Analog Signaling:

An analog signal is one that varies in a continuous manner such as voice or music.

Analog Transmission:

Transmission of a continuously variable signal as opposed to a discretely variable signal. Physical quantities such as temperature are continuously variable and so are described as "analog".

Digital Data:

Information represented by a code consisting of a sequence of discrete elements.

Digital Data Network:

A network specially designed for transmission of data, wherever possible in digital form, as distinct from analog networks such as telephone systems, on which data transmission is an exception.

The purpose of computer networks is to enable users to manipulate data so that it can be stored, retrieved and shared. To understand how available technology enables us to do this, we need to define a few terms and understand some basic concepts.

Computers in a network must "communicate" with each other to have the desired benefits of the network. These signals can be either "analog" or "digital".

Digital signals, on the other hand, are distinctively different. Digital signals have very few values. Each signal is unique from a previous digital value and unique from the one to come. In effect, a digital signal is a snapshot of a condition and does not represent continual movement.

The most obvious example of digital data is that communication on-board a computer. Since a computer's memory is simply a series of switches that can either be on or off, digital data directly represents one of these two conditions. We typically represent this on and off status with 1s and 0s where 1 represents an "on" bit and 0 represents "off".

Broadband networks incorporate technology similar to that of cable television. Data, whether it is video, audio, or digital, is transmitted on the wire at certain frequencies. The typical medium is coaxial cable.

Digital technology is generally utilized exclusively for baseband networks. These networks devote the entire cable to network transmission.

Comparing analog and digital signals, advantages lie on either end of the spectrum. Analog signals suffer far less from attenuation over long distances. This rather makes sense. Since digital data can only be a 1 or 0.

Digital devices are lot less sophisticated, meaning that they are fairly easy to manufacture and cost-effective. Digital devices are more resilient to EMI and make more efficient use of the cabling bandwidths than analog systems do.

Parallel Transmission:

Parallel Transmission is the technique that sends each bit simultaneously over a separate line. Normally parallel Transmission technique is used to send data a byte (8bits over eight lines) at a time to a high speed printer or other locally attached peripherals.

Serial Transmission:

The standard method of ASCII transmission where bits are sent, one at a time, in sequence. Each 7-bit ASCII character is preceded by a start bit and ended with a parity bit and stop bit.

A group of SNA networks connected in series by gateways is called as Serial Network.

Serial Transmission is a technique in which each bit of information is sent sequentially on a single channel, rather than simultaneously as in parallel transmission. Serial Transmission is the normal mode of data communications. Parallel Transmission is often used between computer and local peripheral devices.

Data Transmission:

One major difficulty in data transmission is that of synchronizing the receiver with the sender. Two approaches exist to solve the problem of synchronization: these are asynchronous transmission and synchronous transmission.

Asynchronous Transmission:

In this approach, synchronization is implemented at character level and each individual character is transmitted along with the necessary control information to allow this to take place. The control information consists of additional bits added to each character, START BITS – which indicate that it is about to cease. Usually, the stop bits are of the same polarity as the Channel idle state.

The initial change in the state of polarity, from the idle state to the first bit, is known as the START PULSE. Clearly, this enables the receiver's clock to be synchronized with the transmitter's clock.

Asynchronous transmission has various advantages; the advantages being:

1. One principal advantage is that each individual character is complete in itself – therefore if a character is corrupted during transmission, its successor and predecessor will be unaffected.

2. Particularly suited for applications where the characters are generated at irregular intervals e.g. data entry from the key board.

The advantages of asynchronous transmission system are:

1. Successful transmission inevitably depends on the recognition of the start bits – clearly these can be easily missed or occasionally spurious start but can be generated by line interference.
2. High proportions of the transmitted bits are unique for control purposes and thus carry no useful information.
3. As a result of the effects of distortion the speed of transmission is limited.

Asynchronous serial transmission is normally used for speeds of up to 3000 bits per second for simple, single character error detection.

Synchronous Transmission:

In this system the message is transmitted via single channel. However, in this instance it is imperative to note that there is no control information associated with individual characters. The characters are grouped together in blocks of some fixed size and each block transmitted is preceded by one or more special synchronization characters, which can be recognized by the receiver. ASCII provides a control character.

The advantages of asynchronous transmission are:

1. The amount of central information which requires to be transmitted is restricted to only a few characters at the start of each block.
2. The system is not as prone to distortion as asynchronous communication and can thus be used at higher speeds.

Synchronous transmission also suffers from a few detrimental attributes they are:

1. If an error does occur rather than just a single character the whole block of data is lost.

2. The sender cannot transmit characters simply as they occur and consequently has to store them until it as built up a block, thus the system is unsuitable for applications where characters are generated at irregular intervals.

Bandwidth

In the simplest sense, bandwidth refers to the amount of information that can be transferred between computers. The band width is the speed at which the physical connection can move data, and it actually constrains web access or access across the network more than the speed of your computer. For example a 14.4 kbps modem can receive only about 1.2 – 1.4 kilobytes of data per second, even if there is no other traffic on the network.

Bandwidth describes the amount of data a network can transport in a certain period of time. In other words, bandwidth is a capacity for rate of transfer, usually expressed in bits per second.

Many networks today are based on a technology called Ethernet, which has a standard bandwidth of 10 Mbps. 10 mega bites of data can move through any given spot on the network. And the new Fast Ethernet has transmission speeds of 100 Mbps. As technology continues to evolve, even more advanced networks have been developed that offer transmission rates greater than 1 GB/s.

Questions

1. Explain the basis of networks? Why networking is essential?
2. What are the important applications of networking?
3. Explain analog & digital techniques in detail?
4. What do you mean by serial and parallel transmission and explain them in detail?
5. What is Asynchronous and Synchronous Transmission and discuss them in detail?

Chapter 2

INTERNET & WIDE AREA NETWORK (WAN)

- Internet Basics
- Internet in India
- Internet Protocols
- Telnet
- World Wide Web
- Hyper Text Transfer Protocol
- Web Servers
- Browsers
- Search Engines
- Usenet
- Fire Walls
- Intranets

INTERNET

Internet is network of computers that offer access to people and information. Over 60 million people use Internet, and the number is expected to increase over 120 million within a few years. The kind of information freely available from internet includes Government documents, scientific data, hobbyist lists, business and personal information, advertising databases and much more.

The kinds of communication that can be availed on the internet include the following:

1. Exchanging short social notes.
2. Getting the latest news around the world.
3. Conducting business negotiations.
4. Collaborating on scientific research.
5. Exchanging information with others who have similar hobbies or interests.

6. Transferring computer files.

Internet in India

In India Internet was started to serve the educational institutions to help in their research work. In 1986, IIT was linked up with Indian Institute of Science by ERNET, which later connected with foreign universities. On 15th August 1996 Government called VSNL and started its dial-up services as first Internet Service Provider. Now, there are more than 100 ISPs given license to provide Internet Service. Some of them are MTNL, Satyam Computers Ltd., Wintech, etc.

Internet Protocols

TCP/IP

Transfer Control Protocol and Internet Protocol are two sets of rules that allow computers and networks to communicate effectively. They regulate the flow of data and make sure that it reaches its destination safe and sound.

TCP and IP goes hand-in-had to enable the safe delivery of data over a network, the data is split into a number of smaller packets. TCP/IP attaches a header to the data packet, which contains information like the address, its origin, length of the packet and so on. IP, on the other hand, works like a postal department and ensures that once the data packets reach the receiver's end, they are re-assembled in the same sequence they were broken up and are ready for the application they are meant for.

IP works as routing agent falls under the network layer which has function of making decision for transmitting data across device not connected to each other.

Layers of Travel

The two protocols TCP/IP are stacked over each other and occupy the network layer and the transport layer. These layers are a part of virtual model of networking called OPEN SYSTEM INTERCONNECTION (OSI) model. The OSI model consists of Physical, Data link, Network, Transport, Session, Presentation and Application layers.

The physical layer transmits data from one location to another and is made up of physical aspects of the network like cables and connectors. The data link layer ensures error-free transmission of data and consists of networking cards, modems, etc. The function of the

network layer is to make routing decisions for transmitting data across devices that are not connected to each other.

As IP is a routing agent, it falls under this layer. The transport layer comes next and its primary function is to ensure error free transmission of data. Transfer Control Protocol or TCP falls under this layer. The remaining layers such as the Session, Presentation and Application layers from the application group, which synchronizes links across programs and converts network data to user readable formats.

TCP

As Transport layer protocol, TCP accepts message information from the applications, and divides it into multiple segments, and encapsulates each segment into a datagram. Each datagram is passed over to the network layer protocol (IP) for further transmission and routing. At the receiver's end, TCP reassembles the data and distributes it to the concerned application program.

TCP transmits data in the form of packets that comprise of a header and a data block. The header consists of information like the address of the packet, its origin, the length of the packet and more. The data block carries the payload, which is the text or pictures that we down load or browse off the Net.

Internet Protocol

Internet protocol or IP works like postal department. It routes data packets to the address mentioned in the header and fragments them. These are then marked so that the fragmentation sequence is maintained and are reassembled upon reaching their destination.

The routing of data grams over a network can occur over different paths and the possibility of some data grams arriving out of sequence is not ruled out. In addition, as data grams flow between various networks, they also face physical limitations in terms of the amount of data that can be transferred over a particular network.

IP is also attached to a small header on the data packet, which provides information about the handling of the datagram, identification of fragmented data grams and the like. The version field contains a 4, bit code that identifies the IP protocol used to create the datagram.

The identification field proves the identity of a datagram. In case the datagram has been further fragmented, the fragment offset field specifies the other offset of the datagram.

The flag field contains information about the nature of fragmentation. It provides information about the current fragment and also gives the total number of the fragments. The header also has a field called 'Time to Live' or TTL that defines the number of routers a data packet can encounter en route to its destination computer, thereby avoiding chocked networks.

IP operates on gateway machines that move data from the department to the organization, then to the region and finally across the world.

IP ADDRESS & URL

To connect from one machine to another machine on the Internet, we need to know its IP address, which is an identifier for a particular machine on a particular network. These are referred as IP numbers or Internet addresses.

The IP address is represented by four decimal numbers separated by dots and is basically divided into the host computer section.

Classification to Internets:

Class A: This comprises of very large networks with millions of nodes. They have their IP addresses ranging from 1.0.0.0 to 127.0.0.0. The first number before the dot defines the network with the remaining three sections assigned to hosts.

Class B: These are smaller networks and can have only about 65,000 nodes. Their IP addresses range from 128.0.0.0 to 191.0.0.0. The first two numbers are allocated to the network and the remaining two numbers for the hosts.

Class C: These are much smaller networks, which support a maximum of 254 nodes. The IP addresses range from 192.0.0.0 to 223.0.0.0. In this case, the first three numbers denote the network and the last one denotes the host.

To make the operation simpler, ordinary names are assigned to each address using the Domain Name System. Each Domain Name corresponds to a numeric IP address. The Internet uses the IP address to identify the network and the node and send data to the same. For example: As you type in the address www.yahoo.com form your browser, the Internet actually connects you to the IP number 204.71.200.74 (Which is the domain name for the web site).

Uniform Resource Locaters (URL)

URL is the way to represent site name on the World Wide Web. URLs are similar to postal addresses or telephone numbers which are used to represent the destinations. Most URL consists of 3 parts:

1. Service Name
2. Host Name
3. Request

The most common service names you use in URLs are “http”, “together”, “ftp” and “news”. These refer to Web servers, Gopher servers, FTP servers and Usenet news servers, respectively. A few URLs do not have a host name.

Domain Name Servers

Internet works on the numbering system. These numbers are called IP. When we connect to the net we have seen a set of 4 numbers being dialed i.e. for each address on the Internet there is a unique set of these 32 bit numbers. Domain Name Servers are the servers, which maintain a distributed list of all domains against Internet Protocol address.

Earlier to Domain Name Servers there was a system of having a host table maintained by SRI-NIC. It was updated twice a week to include new sites. System would download the copy of this table through FTP.

There are two types of servers as below:

1. Resolver
2. DNS

There are a number of servers, which maintain the addresses of sites. When browser needs the address of any site, resolver queries the nearest name server, replies immediately if it knows the answer or it asks another server. Thus every server has two roles to play:

1. As a server for name server.
2. Super server to extend functionality.

All web sites are arranged in 7 branches namely arpa, com, edu, net, gov, mil, org. Following this are 236 country name abbreviations like ".in" for India. This helps to locate the site easily. The IP addresses of name servers at each of the domain name tags are maintained by 10 root servers.

When a DNS fields a query that it cannot answer

1. It sends a query to root server
2. Root server says it does not know but a machine at say 195.95.251.10 might know
3. DNS sends a query to the above machine
4. Server at 195.95.251.10 knows the answer
5. DNS returns answer to your PC.

Special features of DNS

Cache: Name server caches all IP address for domain names that were requested recently. So that if requested again it responds immediately.

Load Balancing: Large sites like www.msn.com can have multiple addresses for same domain name. Name servers currently return all IP addresses leaving PC to choose at random. But some name servers will now evaluate all addresses to find out he one with least load.

FTP

File Transfer Protocol, which is the standard system for moving files on the Internet. With it, it is possible to send or receive files to and from a machine on the Internet. The machine to which we are connecting must have FTP server and its address generally starts with 'ftp' code.

FTP requires that we be directly linked to the machine in question. So we are unlikely to use FTP to transfer your files unless we or our client has dedicated FTP server permanently connected to the Net.

As FTP computer knows the name of the Internet services we are calling from, we only need to type 'username@' followed by return. Once logged on, we can get access to public accessible software. Here one can get all sorts of files inside them. Thus, numerous FTP servers all over the world allow the people any where on the Internet to log in and download whatever files have been placed on the FTP server.

TELNET

Telnet is a way of connecting to another machine on the Internet, and using it as if it were our own. In most cases we need to log-in and details of how to do this may be displayed after we have connected to it. A useful telnet site, especially if we are unable to access the full graphical splendor of the Web is: telnet.w3.org. This is a text based web browsing system.

The telnet command is a user interface to a protocol called, not surprisingly, TELNET. Both computers in order for the telnet program, to work must use the TELNET protocol. UNIX computer on the Internet uses the TELNET protocol, so this is rarely an issue. Telnet has many uses on the Internet:

1. Hundreds of library catalogs are available only through direct connection to the library's computers. Using telnet server long distance charges of dial on directly to those computers; some don't even allow direct dialing.

2. If you have accounts on more than one computer on the Internet, you can log into the one closest to you and use telnet to log into the others.

3. Researchers collaborating across the country can log into a single computer to run joint experiments.

THE WORLD WIDE WEB

The World Wide Web is an architectural frame work for accessing linked documents spread out over thousands of machines all over the Internet. Its enormous popularity stems from the fact that it has a colorful graphical interface that is easy for beginners to use, and provides an enormous wealth of information on almost, every conceivable subject.

The Web began in 1989 at CERN, the European center for nuclear research. CERN has several accelerators at which large team of scientists from the participating European Countries carry out research in particle physics. The Web grew out of the need to have these large teams of internationally dispersed researchers collaborate using a constantly changing collection of reports, blueprints, drawings, photos, and other documents.

Hyper Text Transfer Protocol (HTTP)

The HTTP is a method used to make hyper text documents readable on the World Wide Web. Web servers and clients speak to each other using HTTP, so end users don't need to know anything about its intricacies.

HTTP is a stateless protocol, meaning that the client and the server programs speak to each other only once and that a connection is not retained. A web client program sends a single request to the web server for information, and the web sever responds with a single reply.

Web Servers:

Is a software program that sits on your server (The physical machine that is designed to store and serve web pages). Any server configured to communicate using TCP/IP uses ports. Not serial or parallel ports like the ones on the back of your computer, but the ones that look different and serve the same purpose. E.g. Port 80 is the default web server port and all hyper text transfer protocols.

As HTTP request comes to the server it checks the appropriate permissions and then either transmits the page or if the permissions are not adequate, it sends an error message.

The Web server has certain restrictions to what it can process. When the server receives a request for a page having embedded scripts, it cannot process these by itself. It therefore uses additional software that performs auxiliary processing called middleware, which is written in Perl, C or C++. Most middleware revolve around interaction with the database.

Type of Web Servers

FTP Servers:

FTP or File Server Transfer Protocol servers are Internet computers that use this protocol and provide data to Internet users for downloading. Firstly the user should log in to FTP server, where the access rights are derived for different directories.

DNS Servers:

Every computer in the Internet is provided with a specific IP address consisting of four numbers like 123.123.123.123. Since remembering the numbers is difficult, the Internet users want to reach a specific computer on the WWW can also use description. A DNS server includes a database of IP Address. Mapping Web is referred by Internet software to retrieve the IP address.

Gopher Servers:

In the past few years many new tools for searching for information on the Internet have developed. One of them is Gopher Server. It is a Client/Server system that teaches you to navigate through the Internet.

Usenet News Servers:

It is a system where messages about any subject can be posted and other people on the Internet can reply to them. This topic includes politics, science, religion etc. There are more than 5000 active new groups,

Browsers

Browser is a kind of program, which can understand the hyper text protocol and present it into textual or graphical view. Some of the popular browsers are Internet Explorer, Netscape Navigator, Opera, Mosiac etc.

Search Engines:

Searching on the net comprise the enormous and exhaustive task of connecting to each server and finding the requisite information on it. David Filo and Jerry Lang, studying electronics at Stanford University decided to do something about it. They decided to develop a universal database using which one could find information in a quick and simple way. Consequently the worlds first search engine Yahoo! was born in April 1994.

Today there exist a variety of search engines, all of them they would possibly cover almost a major part of the information on the web at any given time. Search engines are composed of databases that comprise indexing schemes, a query processor and ‘spiders’. Spiders are programs that are designed to look up web pages which are listed in every database, follow up on each and every link and update their databases to reflect the updated information. The records in these databases consist of the Uniform Resource Locater or more simply, the dares where the website or page is located, the title of the page and the keywords for that page along with a short summary of the site in a few lines.

How do Search Engines Work?

A Search engine continuously sends so-called 'spiders', a special kind of program, which starts in a homepage of a server and pursues all links stepwise. Word indices are created from individual pages and the database us updated.

1. In some search engines, the operators make entries using forms. Depending on the system, the data is released only after editorial processing.
2. To search for data, the search criteria are entered in the form provided by the search engine. The query is forwarded to the database.
3. The result displays a list with all pages hat correspond to the search criteria. At the same time, the entries are displayed as links. You can reach the corresponding pages with a click.

Search site types:

Search sites are basically of two types, search directories and search engines. Search directories are lists of web sites organized into categories and sub-categories. Search directories are created manually rather than being automated. Their coverage is far less than that of search engines but comprise recommendations and reviews of sites.

Search engines are huge computer generated databases containing information on millions of web sites. They have programs called spiders that automatically look up websites and update their databases. Altavista, Hotbot, Lycos*, Infoseek*, Excite* and Webcrawler* are search engines (* these are hybrid sites i.e. they are search engines as well as offering search directories)

Web Services:

The web service is that facility to provide the user with or without charge with some limitations. Hotmail was one of the first success stories on the Net. It promises you free web-based e-mail account that you can access from anywhere in the world. We can send and receive E-mail; through there is a strong limit of 2 MB. The popular services are:

E-mail Service	www.hotmail.com
Faxing	www.tcp.in or www.tacstems.com/fax.htm
Pager Service	www.icq.com

Electronic Card	www.123greetings.com
Free web pages	www.geocities.com or www.xoom.com

Hyper Text Markup Language (HTML)

It is language for describing how documents are to be formatted. The term "Markup" comes from the old days when copy editors actually marked up documents to tell the printer-in those days, Markup languages thus contain explicit commands for formatting. For example, in HTML, <B> means start boldface <\B> means leave bold face mode.

Documents written in a markup language can be contrasted to documents produced with WYSIWYG (What You See Is What You Get) word processor, such as MS-Word or MS-Perfect. These systems may store their files with hidden embedded markup so they can reproduce them later, but not all of them work this way. By embedding the markup commands within each HTML file and standardizing them, it becomes possible for any web browser to read and reformat any web page.

Commonly used HTML Tags:

<HTML> </HTML>	Beginning and end of web page.
<TITLE> </TITLE>	The text between these tags does not appear on the page but becomes the title of the page that appears in the browser title bar.
<BODY> </BODY>	Beginning and end of the paragraph.
<P> </P>	Beginning and end of the paragraph.
<SCRIPT> </SCRIPT>	Makes the beginning and end of a script section. The script itself is not displayed on the page only the result is dictated.

USENET

A newsgroup is a worldwide discussion forum on some specific topic. People interested in the subject can "subscribe" to the newsgroup. Subscribers can use a special kind of user agent, a newsgroup, to read all the articles posted to the newsgroup. People can also post articles to the newsgroup. Each article posted to a newsgroup is automatically delivered to all the

subscribers, wherever they may be in the world. Delivery typically takes between a few seconds and a few hours, depending how far off the beaten path the sender and receiver are.

Alt is to the official groups as a flea market is to a department store. It is a chaotic, unregulated mishmash of newsgroups on all topics, some of which are very popular, and most of which are worldwide.

The Comp groups were the original USENET groups. Computer scientists, computer professionals and computer hobbyists populate these groups. Each one features technical discussions on a topic related to computer hardware or software.

The Sci and humanities groups are populated by scientists, scholars, and amateurs with an interest in physics, chemistry biology, Shakespeare, and so on.

The news hierarchy is used to discuss and manage the news system itself. System administrators can get help here.

The hierarchies covered so far have a professional, somewhat academic tone.

Soc, which has many newsgroups concerning, politics, gender, religion, various national cultures and genealogy.

Talk covers controversial topics and is populated by people who are strong on opinions, weak on facts. Air is a complete alternative tree that operates under its own rules.

In nearly all cases, when the newsreader is started, it checks a file to see which newsgroups the user subscribers to. It then typically displays a one-line summary or each as-yet-unread article in the first newsgroup and waits for the user to select one or more for reading. The selected articles are then displayed one at a time. News readers also allow users to subscribe and unsubscribe to newsgroups. Changing a subscription simply means editing the local file listing which newsgroups the user is subscribed to.

News readers also handle posting. The user composes an article and then gives a command or clicks on an icon to send the article on its way. Within a day, it will reach almost everyone in the world subscribing to the newsgroup to which it was posted.

The sociology of USENET is unique, to put it mildly. Never before has it been possible for thousands of people who do not know each other to have world wide discussions on a vast variety of topics. A moderated newsgroup is one in which only one person, the moderator, can post articles to the newsgroup. All postings to a moderated newsgroup are automatically sent to the moderator, who posts the good ones and discards the bad ones.

SHELL ACCOUNT PPP/SLIP ACCOUNT

Shell account describes the authorization to access another computer at the operating system level. Shell accounts are useful to the user who needs data in textual format. In shell account, user has no direct IP-Link via SLIP/PPP.

PPP/SLIP

Computer using the TCP/IP Communication protocol to another TCP/IP computer over a modem or a serial line, both computers must be running on an additional protocol. This can either be PPP (point to point) or SLIP (special Line IP). Both protocols perform the same task but they are not interoperable (i.e. both ends of the connection must be running on either PPP or SLIP). PPP was derived in 1991 by IETF (Internet Engineering Task Force)

Firewalls

For Networks integrated with the Internet, there is a need to ensure safety to our network. A study revealed that out of the 250,000 attacks on the Department's computer

systems, about 65 percent succeed. To minimize such problems, the companies need to add a fire wall between the network and the Internet.

The firewall consists of hardware such as routers and host systems software. A firewall is basically a data packet between trusted and un-trusted networks. Any kind of network that uses TCP/IP for data transmission depends on source address, and the port number. A firewall uses these addresses and port numbers to control the flow of data packets between the trusted and un-trusted network.

Classification of Fire Walls:

- Packet filter,
- Application proxy or Application gateway
- Packet Inspection Firewall.

1. Application filter firewall: It is the fastest and simplest of the three and is also one of the earliest. Usually the Router (hardware) based, in this system a packet filter compares the header information source and destination address, and port number-of each incoming or outgoing packet against a table of access control rules.

2. Application proxy firewall: Proxy firewalls are built on the principle that security can be reliable only if there is no direct connection between the trusted and un-trusted networks. An application firewall works by examining what application or service (such as e-mail or file transfer) a data packet is directed to. If the service is available to that packet, then it is allowed to pass through.

3. Packet inspection firewall: The content of the packets is also considered. This inspection of packet can be either based on its ‘state’ or ‘session’. In Case of state filtering, the firewall only allows the incoming packet if it can be matched with an outbound request (or’ invitation) for that packet.

In case of session filtering, the network station in tracked. Once the trusted user terminates the session, all incoming packets with identity pertaining to that session are rejected.

Real like firewalls:

There are two types in which a firewall can be set up:

- Dual homed gateway: Here there is only one firewall with two connections, one for trusted network another for un-trusted network.

- Demilitarized zone: Here two firewalls are used. The first firewall has one connection leading to un-trusted network and second leading to host systems that can be accessed through untrusted network. The area between the firewalls is called demilitarized zone.

INTRANET:

It is a network connecting as an affiliated set of clients using standard internet protocols, especially TCP/IP and HTTP. It is also defined as an IP-based network of nodes behind a firewall, or behind several firewalls connected by secure, possibly virtual, networks.

Advantages of Intranet:

Streamlining business process:

Intranets are phenomenally powerful tools to streamline business process. From decision support, customer service and product engineering to distributed channel operations, from sales force automation and executive information systems, business applications based on intranets can substantially improve the efficiency of complex operations. This is possible because intranet applications are typically much less expensive

to develop and deploy, and much easier to use than applications based on older proprietary platforms. Benefiting from a universal client interface the Web browser-intranet business applications can be deployed and managed from a central location. At the same time, standard based protocols and development technologies enable separate departments across a company to create intranet solutions that remain compatible and compliant with company wide systems and process.

Facilitating Information Dissemination:

A key benefit of the intranet technology is its ability to provide up-to-date information quickly and cost-effectively to the entire user community. An intranet puts vital information at the fingertips of employees, regardless of their location or the location of the information. Information disseminated on an intranet enables a high degree of coherence for the entire company because communications are consistent. A 'news' section of an intranet, for example, can include recent company press releases regarding management strategies, partnerships, and new products. A finance section can keep employees informed of vital financial reports and forecasts. A customer section can allow customers to check the status of an order or repair. Vendors can submit invoices online and check procurement status.

By giving people the ability to access time-critical information, intranets improve the decision-making process by empowering individuals with the knowledge necessary for faster and better informed business decisions. Intranets allow the centralization of information, which makes it easier to maintain and keep data up to data. The benefit to the end-user is the simplicity and speed of information access. For example, the interactive capability enabled by hyper-text links makes it easy for users to gather all the information they need from Web pages quickly, just by clicking on a related icon or button. Providing instant and secure access to business-critical information saves time and increases productivity, and publishing information online eliminates the production, duplication and distribution costs associated with paper.

Enriching Communications and Collaboration:

Intranet technologies enable teams to share knowledge and information regardless of their locations or time zones. Engineering groups can share research data, design concepts,

schedules and other project materials for comments and reviews during a development process. Training groups can distribute training schedules and multimedia computer-associated training courses using Web-based technologies. Project terms can take advantage of intranet newsgroups and threaded discussion to communicate issues and solutions, and can use online chat technology when real-time interaction is required. With intranet teleconferencing, participants can share conference materials in a variety of formats, including text, graphics, audio and video.

Questions

1. Explain the basic principles of Internets?
2. Give a brief overview of Indian Internet Scenario?
3. Explain the concepts of TCP/IP?
4. What are Telnet & World Wide Web? Briefly explain them?
5. Bring out the highlights of Hypertext Transfer Protocol, Web Servers and Browsers?
6. What are Search Engines & Why it is important?
7. What are Firewalls and Intranets? Explain them?

Chapter 3

LOCAL AREA NETWORK

- Introduction
- International Organization for Standardization
- TCP/IP Reference model
- The Network Operating System
- Client Server Network Operating System
- Classification of LAN

Local Area Network

LAN is an interconnection of computers and peripheral devices within a limited geographical area utilizing a communication link and operating under some from of standard control. LAN is a computer network confined to a building or a cluster of buildings; it is typically personal to an organization and is installed for the exclusive use of an office or factory of a given organization.

International Organization for Standardization (ISO):

ISO is made up of over 160 technical committees with over 2,300 sub committees across the globe. Most of these committees work with national standards organizations from several countries. All told, there are over 75 of these national groups. ISO has provided to networking the OSI model (Open Systems Interconnection). It is basically contains details all and the functions of networking and provides a framework in which all vendors around the world can create systems that can communicate with one another. Is a standard attempts to define the structure of a network as a 7 layer hierarchy each of which has a well defined function.

The main aim of OSI standard is to define the way that a network node should look from the outside, i.e. from other network nodes. This enables the interconnection of networks, which differ in terms of the implementation in internal organization and operation. A brief description of seven layers of the OSI model is given below.

1. **Physical Layer:** Is the level at which the interchange of electrical signals, which represents data and control information takes place. This includes a specification of electrical and mechanical characteristics of the physical connection.

2. **Data Link Layer:** Takes the bare bit-level communication system provided by the physical layer and superimposes onto this a means for transmitting data and control information. The protocol used may be character oriented, where control characters are used to delimit the various fields of the basic transmission block, or may relay upon positional significance. Acknowledgement of receipt of data and error control is both implemented at this level with the facility of retransmission if necessary.

3. **Network Layer:** Takes the packet size data blocks, which are handed down from the transport layer and attaches to these the address and routing information, which completes the packet. The choice of routing algorithm is arbitrary and so routing can be fixed or adaptive, in which case packets are routed according to current network traffic loads.

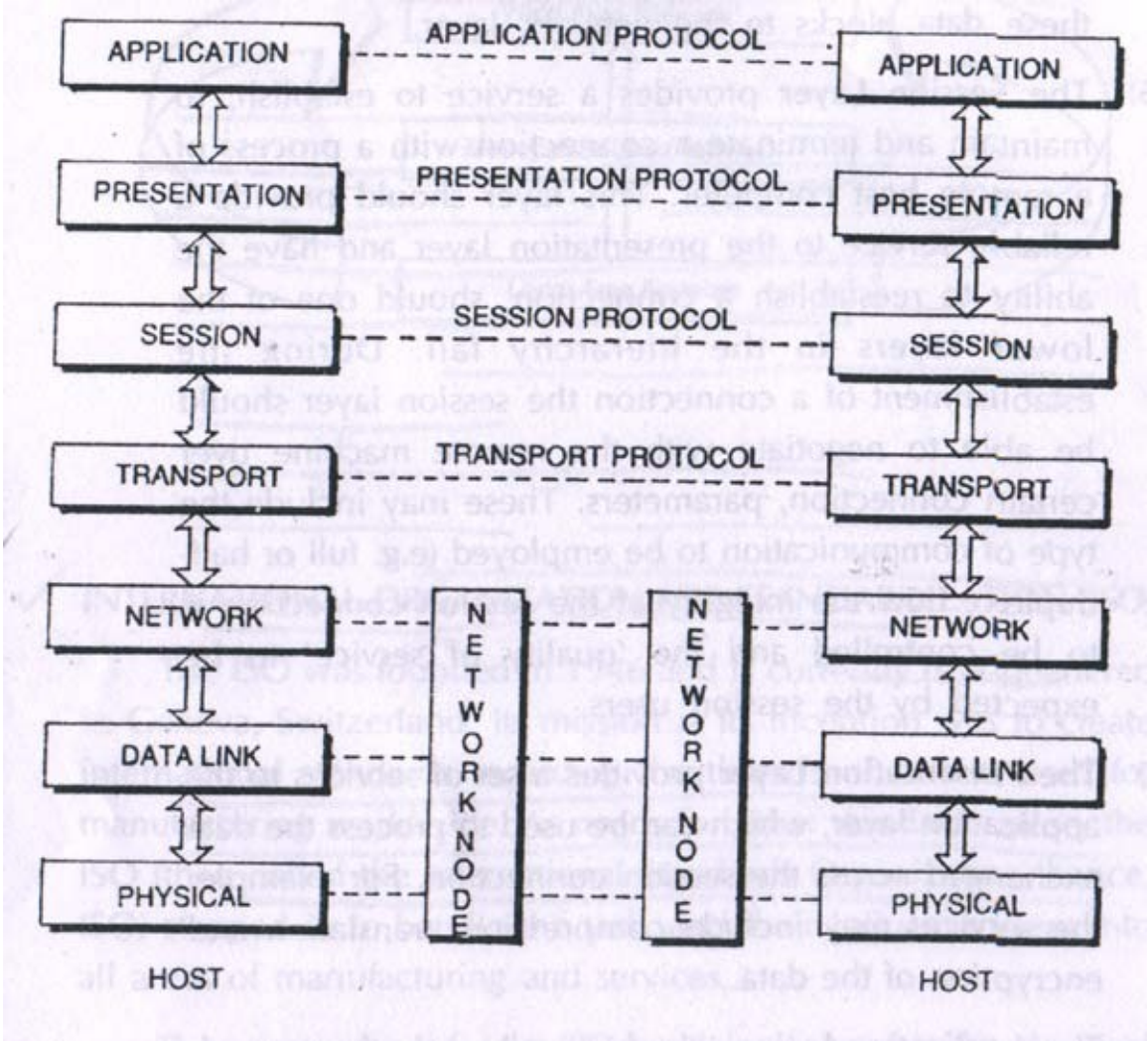
4. **Transport Layer:** Provides a reliable data transmission and reception service for the session layer. The data is transmitted in the most efficient way that is suitable for the needs of the session layer. This may be an error – free virtual connection with acknowledgements on a per packet basis for secure data exchange. It could also be a transmission service with no guarantee of delivery, which may be suitable for certain, types of traffic, digital voice for instance. The transport layer takes data from the session layer and splits it up in to pies, the size of packet data field.

5. **Session Layer:** Provides a service to establish, to maintain and terminate a connection with a process of a remote host computer. This layer should provide a reliable service to the presentation layer and have the ability to reestablish a connection, should one of the lower layers in the hierarchy fail. Session layer should be able to negotiate with the remote machine over certain connection, parameters.

These may include the type of communication to be employed, how the integrity of session connection is to be controlled.

6. **Presentation Layer:** Provides a set of services to the application layer, which can be used to process the data exchanged across the session connection.

7. **Application Layer:** Is the highest layer in the network hierarchy. This layer protocol interacts directly with the application software wanting to transfer data across the network. All the other layers in the hierarchy exist for the sole purpose of satisfying.



TCP/IP Reference Model:

Unlike ISO model this model uses 4 layers. These are

- Network Access
- Internet
- Transport
- Process

Layer 4: Is the highest layer of TCP/IP concerned with the application process the user requires.

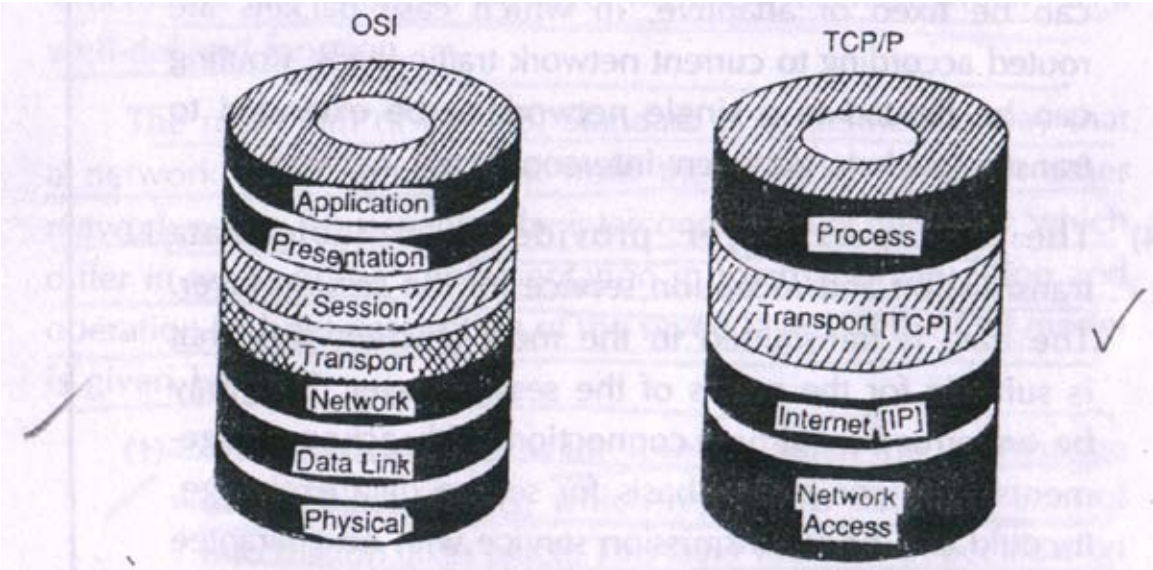
Layer 3: "Transport" layer uses the Transmission Control Protocol (TCP) to pass the message from the user process to the internet (IP) layer

- The transport layer is where a long message is subdivided in smaller "packets" in preparation for east in "transporting".
- These packets are properly called datagrams.
- At the other end, this layer reassembles the "Packets" it receives into their correct order and puts the original message back together for the application to use.

Layer 2: IP, the Internet Protocol is responsible for routing individual datagrams across the interconnected networks.

Layer 1: Network Access: The bottom layer, here is where the data link to the physical media is prepared according to the desired type of connection.

- The completed message is often referred to as a frame
- The "trailer" is added at this point.
- Is finally converted into an electromagnetic signal by special DCE hardware and placed on the physical medium.



The above diagram compares TCP/IP with OSI model.

The advantage of ISO model over TCP/IP model can be stated as follows:

- More carefully thought out and more "modern"
- Has seven layers, as compared to the four used in TCP/IP
- Used more as a "reference model" is the standard by which others are often compared.

Characteristics & Uses of LAN

A LAN typifies a distributed environment and finds applications in a number of areas. Some examples are:

1. Office automation
2. Factory automation
3. Distributed Computing
4. Fire and Security Systems
5. Process Control
6. Document Distribution.

The characteristics of the ideal LAN can be summarized as follows:

High Speed: Data rates of currently available LANs cover a wide range. The slowest transfer data at around 100 kbps while the fastest have data rates of up to 100 kbps.

Low Cost: Many applications of LANs involve low cost microprocessors systems; it is desirable that connection of such systems to a LAN should be economic. Another factor that influences the cost of a LAN is the wiring, which must be installed. There are both the costs of the wirer and its installation to consider. LANs use very inexpensive cable such as twisted – pair telephone wire.

High reliability/Integrity: Since LAN is s set of multiple interconnected systems; it offers a good backup capability in the event of one or two systems failing in the network. This enhances the reliability and availability of the systems to users.

Installation flexibility: LAN offers flexibility in locating the equipment. Most computers on a LAN are physically placed at the user table, which is most convenient for working and improves productivity significantly.

Expandability: Unlike a large centralized system, a LAN may evolve with time. It may be put into operation with a small investment, and more systems.

East of Access: The connection pattern of a LAN is normally a simple topological form such as a ring or a tree and this has implications for the routing of packets on a LAN.

The other advantages of LAN are as follows:

1. LAN provides a resource-sharing environment. All the LAN users may share expensive peripherals, hosts and databases.
2. LAN adhering to a certain standard, permits multi-vendor systems to be connected to it.
3. In LAN, the systems are generally so chosen as to meet most of the user requirements locally and the network is used only for resource and information sharing purposes.

Components of LAN

Workstations: In LAN, a workstation refers to a machine that will allow users access to a LAN and its resources while providing intelligence on board allowing local execution of applications. It may allow data to be stored locally or remotely on a file server. Obviously, diskless workstations require all data to be stored remotely, including that data necessary for the diskless machine to boot up. Executable files may reside locally or remotely as well, meaning a workstation can run its own programs or those copied off the LAN.

Servers: A server is a computer that provides the data, software and hardware resources that are shared on the LAN. A LAN can have more than one server; each has its unique name on the network and all LAN users identify the server by its name.

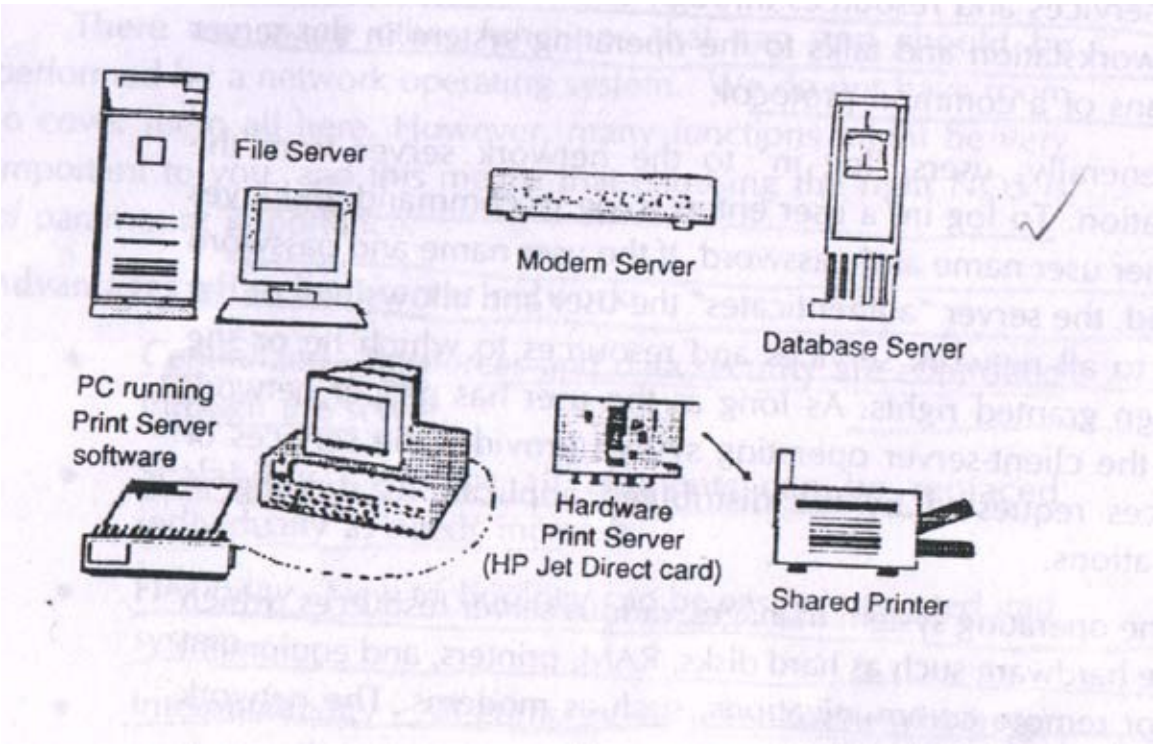
1. **Dedicated Server:** A server that functions only as a storage area for data and software and allows access to hardware resources is called a dedicated server. Dedicated servers need to be powerful computers.

2. **Non-Dedicated Server:** In many LANs, the server is just another work station. Thus, there is a user networking on the computer and using it as a workstation, but part of the computer also doubles up as a server. Such a server is called a non-dedicated server. Since, it is not completely dedicated to serving. LANs do not require a dedicated server since resource sharing amongst a few workstations is proportionately on a smaller scale.

3. **Other Types of Servers:** In large installations, which have hundreds of workstations sharing resource, a single computer is often not sufficient to function as a server.

Some of the other servers have been discussed here under:

1. **File Server:** A file server stores files that workstations can access and it also decides on the rights and restrictions that the users need to have while accessing files on LAN.
2. **Printer Server:** A Printer server takes care of the printing requirement of a number of workstations.
3. **Modern Server:** It allows LAN users to use the modern to transmit long distance messages. Server attached to one or two modems would serve the purpose.



CLIENTS

A client is any machine that requires something from a server. In the more common definition of a client, the server supplies files and sometimes processing power to the smaller machines connected to it. Each machine is a client. Thus a typical ten PC local area network may have one large server with all the major files and databases on it and all the other machines connected as clients. This type of terminology is common with TCP/IP networks, where no single machine is necessarily the central repository.

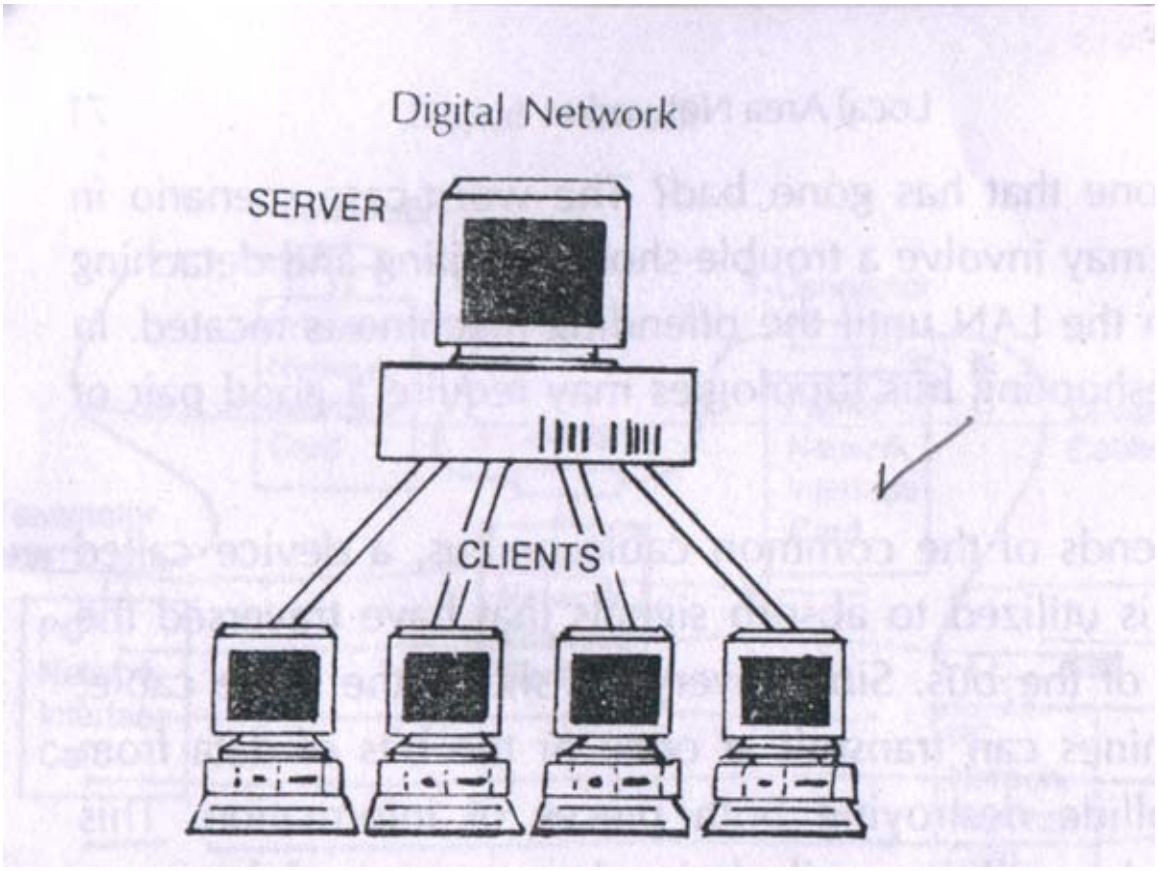
NODES:

Small networks that comprise of a server and a number of PC. Each PC on the network is called a node. A node essentially means any device that is attached to the network. Because each machine has a unique name or number (so the rest of the network can identify it), you will hear the term node name or node number quite often.

NETWORK INTERFACE CARDS

The Network Interface card, or LAN adapter, functions as an interface between the computer and the network cabling, so it must serve two masters. Inside the computer, it controls the flow of data to and from the Random-Access Memory (RAM). Outside the computer, it controls the flow of data in and out of the network cable system. An interface card has a specialized port that matches the electrical signaling standards used on the cable and the specific type of cable connector.

One must select a network interface card that matches your computer's data bus and the network cable. Token ring LANs require token ring NICs, Ethernet LANs require Ethernet NICs, etc. The peripheral component interface bus has emerged as a new standard for adapter card interfaces. It is advisable to but PCI-equipped computers and using PCI LAN adapters wherever possible. Software is required to interface between a particular NIC and an operating system.



Connectors:

Connectors used with TP included RJ-11 and RJ-45 modular connectors in current use by phone companies. Occasionally other special connectors, such as IBM's Data Connector, are used. RJ-11 connectors accommodate 4 wires or 2 twisted pairs, while RJ-45 houses 8 wires or 4 twisted pairs.

The Network Operating System

The Network Operating System software acts as the command center, enabling all of the network hardware and all other network software to function together as one cohesive, organized system. In other words, the network operating system is the very heart of the network.

Client Server Network Operating Systems:

On a Client Server Network, the network operating system is installed and runs on a computer called the network server. The server must be a specific type of computer. A client-server operating system is responsible for coordinating the use of all resources and services available from the server on which it is running. The client part of a client-server network is any other network device or process that makes requests to use server resources and services. To log in, a user enters a log in command and gives his user name and password. If the user name and password are valid, the server "authenticates" the user and allows him access to all network services and resources to which he has been granted rights.

The OS manages various server resources, which include hardware such as hard disks, RAM, printers and equipment used for remote communications, such as modems. The network file system is also a server resource. The network operating system provides many services, including coordinating file access and file sharing, managing server memory, managing data security, scheduling tasks for processing coordinating printer access, and managing inter network communications. The most important functions performed by a client server operating system are ensuring the reliability of data stored on the server and managing server security.

Advantages of a client/server network:

1. Centralized – Resources and data security are controlled through the server.
2. Scalability – Any or all elements can be replaced individually as needs increase.
3. Flexibility – New technology can be easily integrated into system.
4. Interoperability – All components (client/network/server) work together.
5. Accessibility – Server can be accessed remotely and across multiple platforms.

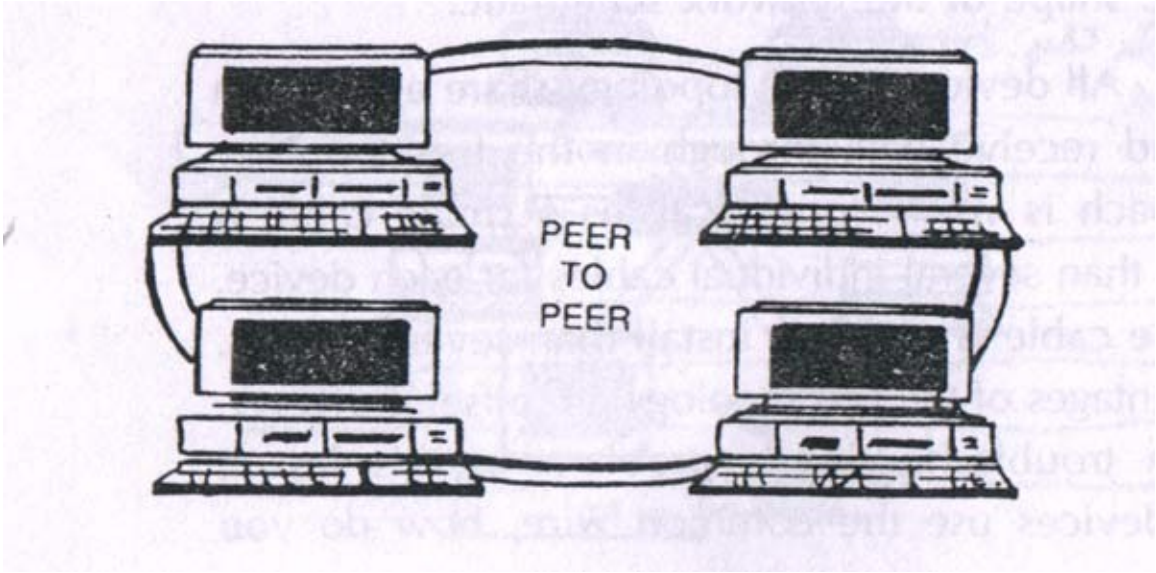
Disadvantages of a client/server network:

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

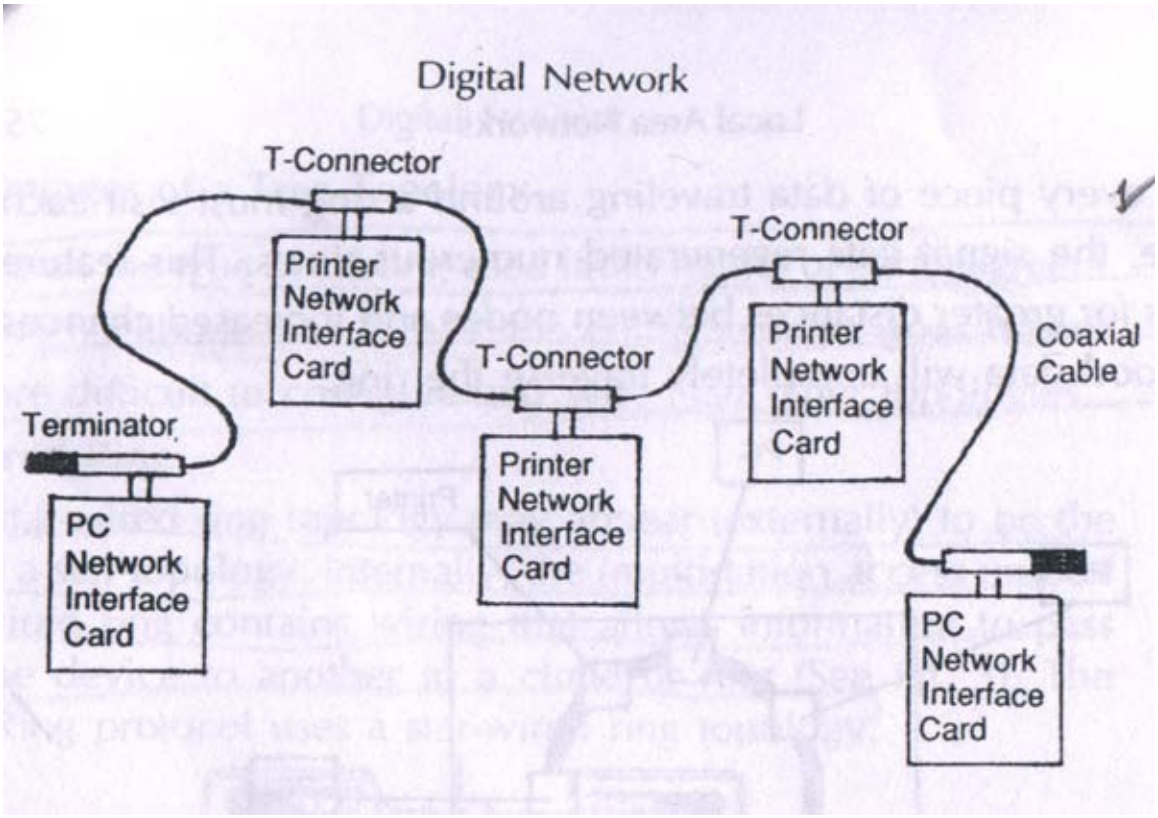
Peer-to-Peer Network Operating Systems:

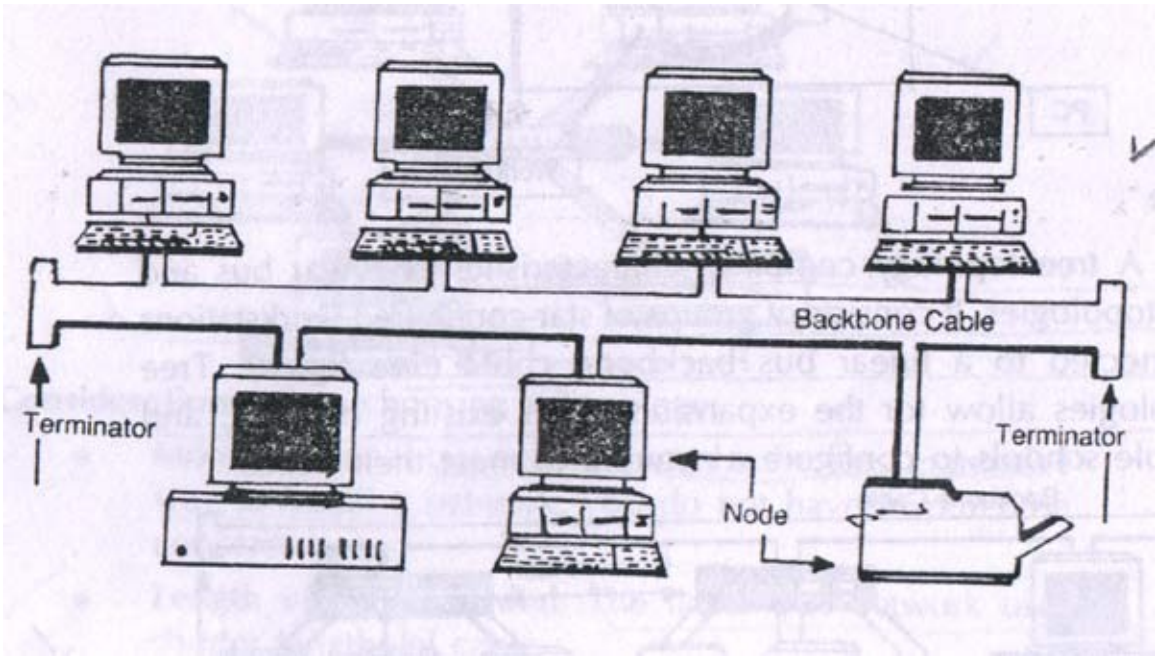
Enable networked computers to function as both a server and a workstation. In a peer-to-peer network, the operating system is installed on every networked computer; this enables any networked computer to provide resources and services to all other networked computers.

Peer-to-peer operating systems have both advantages and disadvantages when compared to client-server operating systems. They provide many of the same resources and services so do client server operating systems, and under the right circumstances, can provide good performance.



Peer-to-peer networks provide fewer services than client-server operating systems. Also, the services they provide are a great deal less robust than those provided by mature, full-featured client-server operating systems and the performance of peer-to-peer networks commonly decreases significantly.





Advantages of a peer-to-peer

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

Disadvantages of a peer-to-peer network

1. Decentralized – No central repository for files and applications.
2. Security – Does not provide the security available on a client/serer network.

Classification of LAN:

Network topologies: A network topology is the way the cabling is laid out. This doesn't mean the physical layout, but how the logical layout looks when viewed in a simplified diagram.

Bus Topology: In this topology all devices share a common wire to transmit and receive data. This approach is very economical, as single cable is cheaper to purchase than several individual cables. Additionally, a single cable is easier to install than several cables. These apparent advantages of the bus topology are offset, by the difficulty in trouble shooting a problem in this layout. Trouble shooting in bus topologies may require a good pair of sneakers.

On the ends of the common cable, a device a called a terminator is utilized to absorb signals that have traversed the entire length of the bus. Since every one shares the same cable no two machines can transmit at once or the bits of data from each will collide destroying both pieces of information. This event is called a collision and obviously too many of them can be disastrous to traffic flow on a network. A data reflection can occur any time an electronic signal encounters a short or an open. The end result is the same reflected data collides with the "good" data on the LAN and traffic flow is impacted.

Advantages of a Linear Bus Topology

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

Disadvantages of a Linear Bus Topology

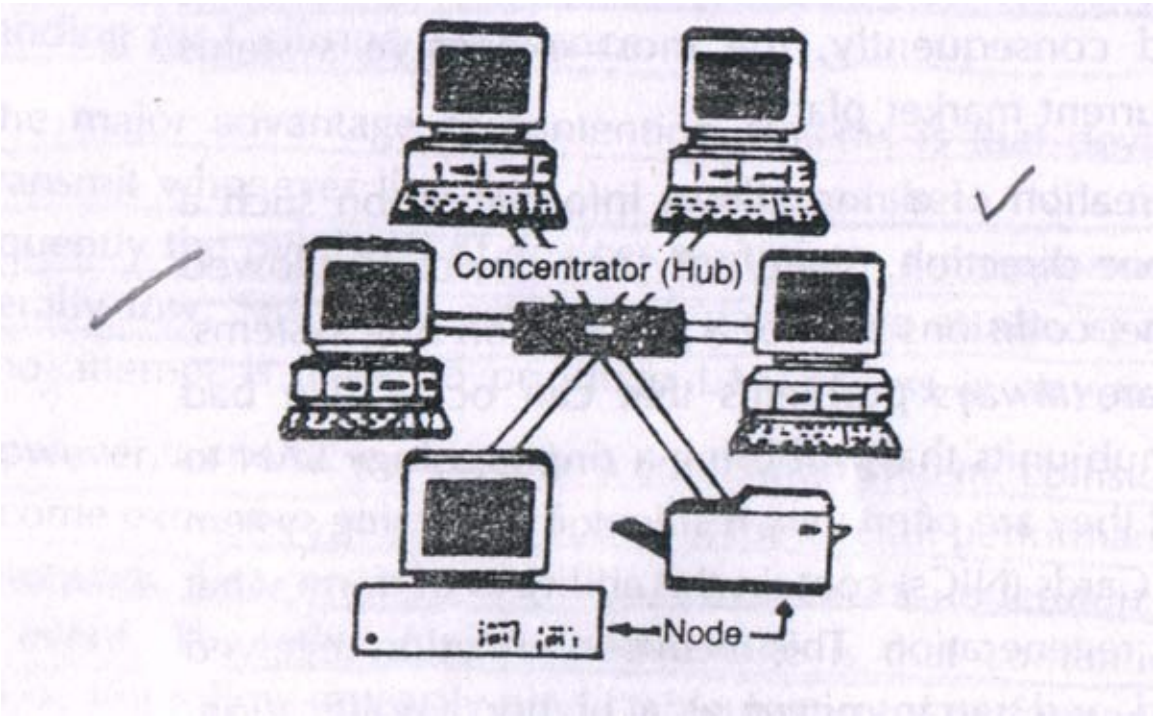
1. Entire network shuts down if there is a break in the main cable.
2. Terminators are required at both ends of the backboned cables.
3. It is difficult to identify the problem if the entire network shuts down.

4. Not good as a stand-alone solution in a large building.

STAR Topology:

Star topology derives its name from the arrangement of devices so that they radiate from a central point. At the central point we usually see a device generically called a hub. Key benefits of the star topology is the hub unit which may vary in function from a simple signal splitter to one that amplifies and keeps statistics on data traveling through them. Star topology a popular choice in the networking market place. Hubs that amplify signals coming through are called active hubs or multi-port repeaters.

Star topologies do require more cable than a simple bus topology, but most use a relatively inexpensive type of cable called twisted pair cabling which helps control costs of wiring. The hubs themselves require expense and the level of that expense is direct attributable to how complex a hub is needed.



Trouble shooting is bit easier than Bus topology. At the very least, one may disconnect devices from a central hub to isolate a problem as opposed to visiting each individual machine. It's obvious how the central hub device offers advantages, but there is one drawback. The hub itself represents a single point of failure. If you lose a hub, you effectively lose all workstations attached to it.

Advantages of a Star Topology

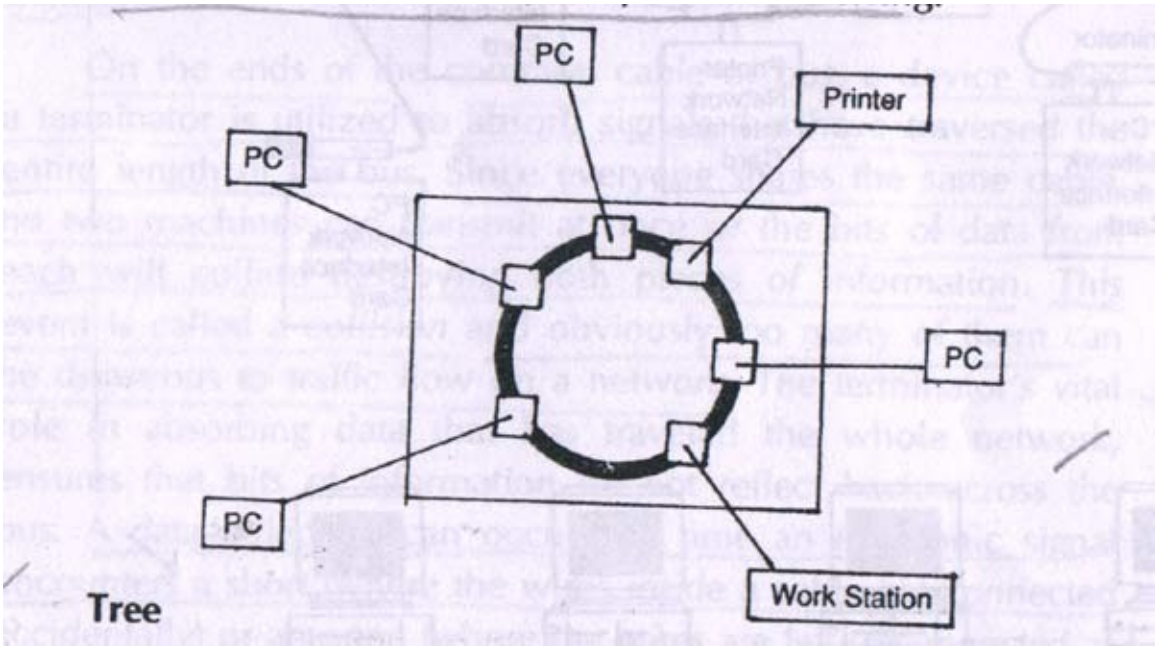
1. Easy to install and wire.
2. No disruptions to the network when connecting or removing devices.
3. Easy to detect faults and to remove parts.

Disadvantages of a Stat Topology

1. Requires more cable length than a linear topology.
2. If the hub fails, nodes attached are disabled.
3. More expensive than linear bus topologies because of the cost of the concentrators.

Ring Topology:

It describes the logical layout of token ring and FDDI networks. In this a ring is created to which each device is attached. A special signal called a token travel around this ring visiting each machine letting it know that it is that machine's turn to transmit. Since the token visits every node, every one gets the chance to transmit, creating a very "fair" LAN. The simplistic explanation belies the true complexity of ring topology systems available today. Token ring LANs, and their FDDI cousins, are the most sophisticated fault-tolerant, and consequently, the most expensive systems available in the current market place.



Tree

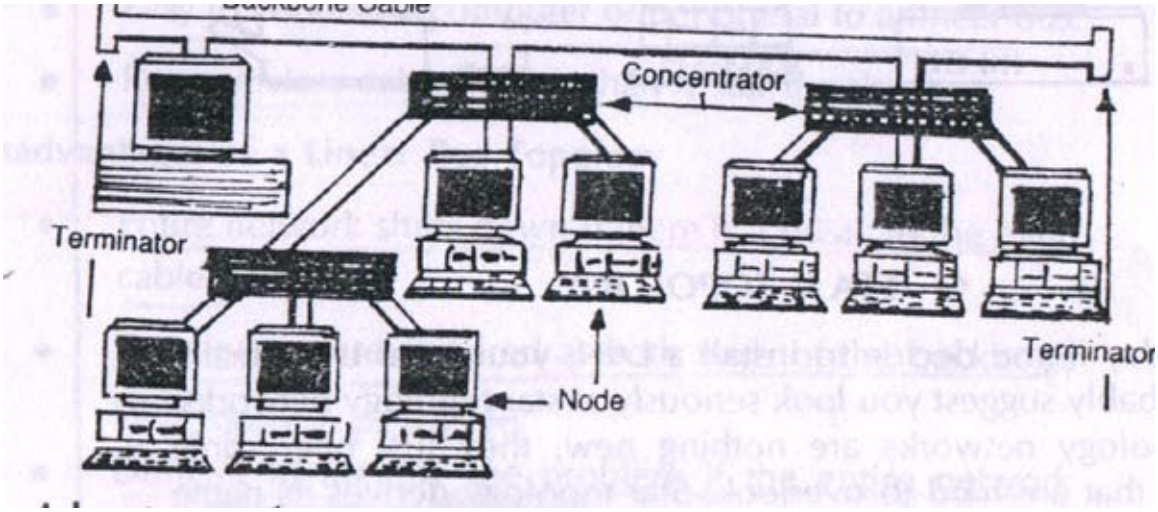
The logical creation of a ring allows information on such a LAN to travel in one direction. Since only one device is allowed to transmit at a time, collisions are not a problem on ring systems. Typical ring system NICs contain the ability to perform what is known as signal regeneration, this means information received by them is copied and retransmitted at a higher amplification. Since every piece of data traveling around a ring must visit each device. The signal gets regenerated numerous times. This feature allows for greater distances between nodes and increased chances that good data will completely traverse the ring.

Tree Topology:

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.

Advantages of a tree topology:

1. Point-to-point wiring for individual segments.
2. Supported by several hardware and software vendors.

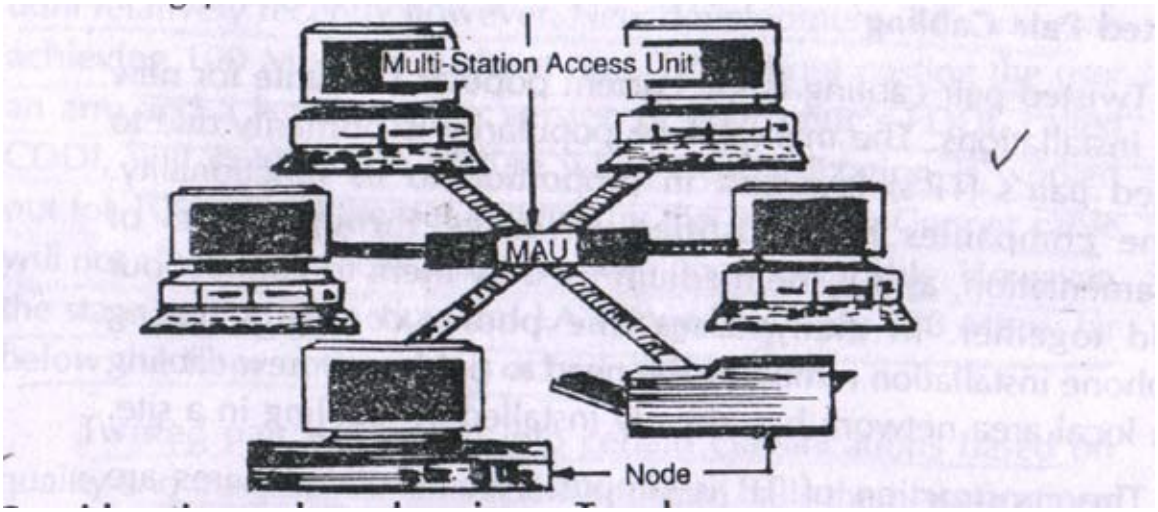


Disadvantages of a tree topology

1. Overall the type of cabling used limits length of each segment.
2. If the backbone line breaks, the entire segment goes down.
3. More difficult to configure and wire than other topologies.

STAR-WIRED RING.

A star-wired ring topology may appear (externally) to be the same as a star topology. Internally, the multi-station access unit of a star-wired ring contains wiring that allows information to pass from one device to another in a circle or ring.



CONSIDERATIONS WHEN CHOOSING A TOPOLOGY:

- **Money.** A liner bus network may be the least expensive way to install a network;
- **Length of cable needed.** The linear bus network uses shorter lengths of cable.
- **Future growth.** With a star topology, adding another concentrator easily does expanding a network.
- **Cable type.** The most common cable is unshielded twisted pair, which is most often used with star topologies.

LAN Access Control

Collision Sense Multiple Access / Collision Detection (CSMA/CD).

In bus topology systems, all devices are attached to a common wire. As mentioned in a previous section, this means that only one device may use the common wire at a time. Since several devices may need to use the wire at once, machines are said to be contending for the media.

Ethernet systems use a channel access method known as CSMA/CD, short for Carrier Sense Multiple Access / Collision Detection. Though this seems a lot of words, the meaning is quite simple. Carrier Sense means that each device checks the LAN before it starts transmitting to see if some other device is using the media then. If another signal (containing a "carrier") was present, than the device attempting to send would wait until the LAN is clear. Then it transmits its data. The collision detection part means that each workstation listens to make sure that only one signal is present on the LAN. In the event there are two then obviously the data from one device has collided with that of another.

Local Talk LANs used by Macintosh PCs also use CSMA contention schemes, but these machines incorporate a technology called time-division multiplexing to allow avoidance of collisions. In fact, Local Talk Systems are said to be CSMA/CA systems, with CA standing for Collision Avoidance.

The major advantage of contention systems is that devices may transmit whenever they like just as long as the LAN is free. Consequently the over headed of devices waiting on the opportunity is generally low.

However, as traffic increases in a contention system, collisions can become excessive, impacting the overall performance of the network. The capacity of the LAN may be far underutilized in this event. The other major disadvantage is that contention systems do not follow an easily predictable pattern of performance degradation as traffic increases.

Token Passing Scheme

This technology is used for token ring systems. Its incorporation along with complementary fault-tolerance capabilities yields a LAN with a fair amount of sophistication, manageability and reliability.

In this channel accesses a small signal called a token which regularly visits each device. The token gives permission for the device to transmit if it needs to. If transfer of data is needed, the device receives a set amount of time to broadcast its data. When it is done, the machine then retransmits the token to another machine giving that recipient permission to transmit, and so the

system continues. This mechanism ensures opportunity for all devices to gain access to the LAN. Because of its predictable behavior, token scheme LANs offers the advantage of priorities, where a certain group of devices may have enhanced access to the LAN if warranted.

As traffic demand increases on a token LAN, the overall throughput of data rises as well, until a point is reached where the networks simply cannot accommodate anymore. The function in this case is somewhat like a waterwheel. The wheel itself receives water from a sluice. You may increase the capacity of the wheel, but the sluice can only hold so much water.

Throughput characteristics of token LANs are so predictable, because of the characteristics of traffic demand. These systems are ideal for heavy traffic situations. Complexity of such a LAN does come at some cost. Token systems require overhead to carry out their many functions including fault-tolerance. Token ring systems are additionally considerably more expensive than Ethernet systems. Factors weighing in deciding which system to choose should include traffic demand and budgetary restraints.

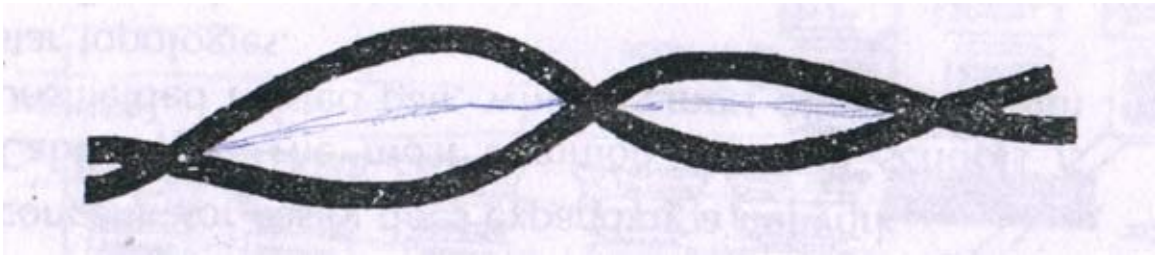
LAN CABLING

Cable is the medium thorough which information usually moves from one network device to another. There are several types of cable, which are commonly used with LANs. The type of cable chosen for a network is related to the network's topology, protocol, and size. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network. The various types of cables are as follows:

TWISTED PAIR CABLING:

Twisted pair cabling is the current popular favorite for new LAN installations. The marketplace popularity is primarily due to twisted pair's (TP's) low cost in proportion to its functionality.

The construction of TP is simple. Two insulated wires are twisted around one another a set number of times within one foot of distance. If properly manufactured, the twists themselves fall in no consistent pattern. This is to help offset electrical disturbances, which can affect TP cable such as radio frequency interference (RFI) and electromagnetic interference (EMI). These "pairs" of wires are then bundled together and coated to form a cable.



Twisted pair comes in two different varieties- shielded and unshielded. Shielded twisted pair (STP) is often implemented with Local Talk by Apple and by IBM's token ring systems. STP is simply TP cabling with a foil or mesh wrap inside the outer coating. This Special layer is designed to help offset interference problems. The shielding has to be properly grounded, however, or it may cause serious problems for the LAN.

TP cabling has been around a while and is a tried and true medium. It hasn't been able to support high-speed data transmissions until relatively recently however. New development is focusing on achieving 100 Mbps throughput on UTP without costing the user an arm and a leg. A copper version of fiber optic's FDDI, called CDDI, will continue to mature while standardization is worked out for 100 Mbps Ethernet systems by the mid 90s. Copper cable will not allow the speeds attainable with fiber optic cable. However, the standard for fiber stipulates LAN speeds of only 100 M bps, for below the fiber optic cable's actual capacity.

Twisted pair is grouped into certain classifications based on quality and transmission characteristics. IBM calls the classifications "types". UTP by itself is often grouped by "grades".

UNSHIELDED TWISTED PAIR GRADES

Grade 1 Suitable for voice transmission and data transfer up to 1 Mbps.

Grade 2 Capable of carrying data at 4 Mbps.

Grade 3 Carries data at up to 10 Mbps.

Grade 4 Rated at 20 Mbps.

Grade 5 Support speeds at up to 100 Mbps.

TWISTED PAIR CABLE TYPES (IBM STANDARDS)

Type 1 STP, two pair, 22 gauge, solid conductors, and braided-shield.

Type 2 Type 1 cable with additional four pairs of UTP.

Type 3 UTP, 22 or 24 gauge, 2 twists per foot, and four pairs.

Type 5 Fiber optic cable used to link MAUs.

Type 6 Two pair, stranded (not solid) 26 gauges, patch cables.

Type 8 cable Two pair, 26 gauge, and untwisted but untwisted but shielded

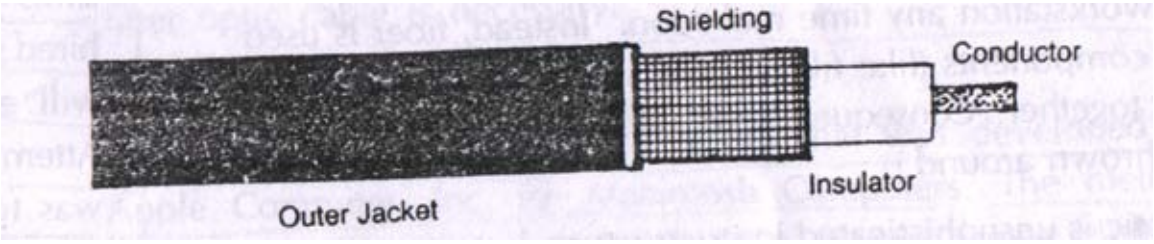
TWISTED PAIR CABLE:

ADVANTAGES	*DISADVANTAGES*
1. Inexpensive 2. Often available in existing phone system 3. Well tested and easy to get.	1. Susceptible to RFI and EMI 2. Not as durable as coax. 3. Doesn't support as high a speed as other media.

COAXIAL CABLE:

Coaxial cable or just "coax" enjoys a huge installed base among LAN sites in the US. It has fit the bill perfectly for applications requiring stable transmission characteristics over fairly long distances. It has been used in ARC net systems, Ethernet systems and is sometimes used to connect one hub device to another in order systems.

Construction-wise coax is little more complex than TP. It is typically composed of a copper conductor that serves as the "core" of the cable. This conductor is covered by a piece of insulating plastic, which is covered by a wire mesh serving as both a shield and second conductor. PVC or other coating then coats this second conductor. The conductor within a conductor sharing a single axis is how the name of the cable is derived.



Coaxial cable's construction and components make it superior to twisted pair for carrying data. It can carry data farther and faster than TP can. These characteristics improve as the size of the coax increases. There are several different types of coax used in the network world. Each has its own RG specification that governs size and impedance, the measure of a cable's resistance to an alternating current. Different cable can differ widely in many important areas.

COMMON COAXIAL CABLE TYPES USED IN NETWORKING:

Type Common Usage Impedance

RG-8 Thick Ethernet 50 Ohms

RG-11 Broadband LANs 75 Ohms

RG-58 Thin Ethernet 50 Ohms

RG-59 Television 75 Ohms

RG-62 ARC net 93 Ohms

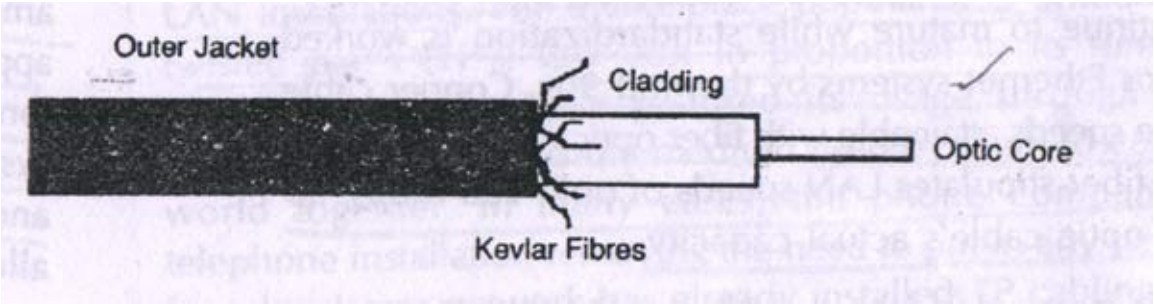
COAXIAL CABLE

ADVANTAGES	***DISADVANTAGES***
1. Fairly resistant to RFI and EMI 2. Supports Faster data rates than twisted pair 3. More durable than TP	1. Can be effected by strong interference 2. More costly than TP. 3. Bulkier and more rigid than TP

FIBER OPTICS:

Fiber has come into importance on its own as the premier bounded media for high-speed LAN use. Because of fiber's formidable expense, however, we are not likely to see it at the local workstation any time real soon.

Fiber optic is unsophisticated in its structure, but expensive in its manufacture. The crucial element for fiber is glass that makes up the core of the cabling. The glass fibers may be only a few microns thick or bundled to produce something more sizable. It is worth noting that there are two kinds of fiber optic cable commercially available-single mode and multimode. AT use single mode in the telecommunications industry and T or US sprint to carry huge volumes of voice data. Multimode is what we use in the LAN world.



The glass core of a fiber optic cable is surrounded by and bound to a glass tube called "cladding". Cladding adds strength to the cable while disallowing any stray light wave from leaving the central core. A plastic then surrounds this cladding or PVC outer jacket which provides additional strength and protection for the inwards. Some fiber optic cables incorporate Kevlar fibers for added strength and durability. Kevlar is the stuff of which bulletproof vests are made, so it's tough.

Fiber optic is lightweight and is utilized often with LEDs (Light Emitting Diodes) and ILDs (Injection Laser Diodes). Since it contains no metal, it is not susceptible to problems that copper wiring encounters like RFI and EMI. Plus, fiber optic is extremely difficult to tap, so security is not a real issue.

The biggest hindrance to fiber is the cost. Special tools and skills are needed to work with fiber. These tools are expensive and hired skills are expensive too. The cable itself is pricey, but demand will ease that burden as more people invest in this medium. Attempts have been made to ease the cost of fiber. One solution was to create synthetic cables from plastic as opposed to glass. While this cable worked, it didn't possess the near capabilities of glass fiber optic, so its acceptance has been somewhat limited. The plastic fiber cables are constructed like glass fiber only with a plastic core and cladding.

The bandwidth or capacity of fiber is enormous is comparison with copper cabling. Multimode fiber can carry data in excess of 5 gigabits per second. Single mode fiber used in telecommunications has a theoretical top speed in excess of 25,000 Gbps. That much data is the equivalent of all the catalogued knowledge of man transmitted through a single small glass tube in less than 20 seconds.

The standard governing implementation of fiber optic in the marketplace is called the *fiber distributed data interface* standard or FDDI. FDDI specifies the speed of the LAN, the construction of the cable, and distance of transmission guidelines. FDDI behaves very much like token ring, only much faster. An added feature for FDDI is a backup ring in case the main ring fails. This fault tolerance along with the fault tolerance already incorporated in token ring technology makes FDDI LANs pretty resilient.

LAN Protocols:

A protocol is a set of rules that governs the communications between computers on a network. These rules include guidelines that regulate the following characteristics of a network; access method, allowed physically topologies, types of cabling, and speeds of data transfer.

Ethernet:

The Ethernet protocol is by far the most widely used. It uses an access method called CSMA/CD (Carrier Sense Multiple Access / Collision Detection). This is a system where each

computer listens to the cable before sending anything through the network. If the network is clear, the computer will transmit. If some other node is already transmitting on the cable, the computer will wait and try again when the line is clear, sometimes, two computers attempt to transmit at the same instant, when this happens a collision occurs. Each computer then backs off and waits a random amount of time before attempting to retransmit. With this access method, it is normal to have commissions.

This protocol allows for linear bus, star, or tree topologies. Data can be transmitted over twisted pair, coaxial or fiber optic cable at a speed of 10 Mbps.

Fast Ethernet: For an increased speed of transmission, the Ethernet protocol has developed to new standard that supports 100 Mbps. This is commonly called Fast Ethernet. Fast Ethernet requires the use of different, more expensive network concentrators/hubs and network interface cards.

Local Talk: Local talk is a network protocol that was developed by Apple Computer, Inc. for Macintosh Computers. The method used by local talk is CSMA/CS (Carrier Sense Multiple Access with Collision Avoidance). It is similar to CSMA/CD except that a computer signals its intent to transmit before it actually does so. Local Talk adapters and special twisted pair cable can be used to connect a series of computers through the serial port. The Macintosh operating system allows the establishment of a peer-to-peer network without the need for additional software.

The Local Talk protocol allows for linear bus, star, or tree topologies using twisted pair cable. A primary disadvantage of Local Talk is seed, its speed of transmission is only 230 Kbps.

Token Ring:

IBM developed this protocol in the mid 1980s. The access method used involves token passing. In token ring the computers are connected so that the signal travels around the network from one computer to another in a logical ring. A single electronic token moves around the ring from one computer to next. If a computer does not have information to transmit, it simply passes the token on to the next workstation. If a computer wishes to transmit and receives an

empty token, it attaches data to the token. The token then proceeds around the ring until it comes to the computer for which the data is meant. At this point, the receiving computer captures the data. The token ring protocol requires a star wired ring using twisted pair or fiber optic cable. It can operate at transmission speeds of 4 Mbps or 16 Mbps.

FDDI:

Fiber Distributed Data Interface (FDDI) is a network protocol, used primarily to interconnect two or more local area networks, often over large distance. The access method used by FDDI involves token passing. FDDI uses a dual ring physical topology. Transmission normally occurs on one of the rings; however, if a break occurs, the system keeps information moving by automatically using portions of the second ring to create a new complete ring. A major advantage of FDDI is speed. It operates over fiber optic cable at 100 Mbps.

Protocol	***Cable***	***Speed***	***Topology***
Ethernet	Twisted Pair, Coaxial, Fiber	10 Mbps	Linear Bus, Star, Tree
Fast Ethernet	Twisted Pair, Fiber	100 Mbps	Star
Local Talk	Twisted Pair	23 Mbps	Linear Bus or Star
Token Ring	Twisted Pair	4 Mbps – 16 Mbps	Star – Wired Ring
FDDI	Fiber	100 Mbps	Dual Ring

LAN Standards:

Institute of Electrical and Electronic Engineers (IEEE): The IEEE has done notable work in the standards area of networking. This organization is huge with over 300,000 members consists up of engineers, technicians, scientists, and students in related areas. The computer society of IEEE alone has over 100,000 members. IEEE is credited with having provided definitive standards in Local Area Networking. These standards fall under a group of standards known as the 802 project. The 802 standards were the culmination of work performed by the subcommittee starting in 1980. The first published work was 802.1, which specified a framework for LAN's and inter-networking. This was followed in 1985 with specific LAN-oriented standards titled 802.2-802.5. Most of the work performed by the 802 project committee revolves around the first two layers of the OSI model initiated by the ISO. These layers involve the physical medium on which we move data and the way that we interact with it. In order to

better define these functions, the IEEE split the Data Link Layer of the OSI model up into two separate components.

802 IEEE committee responsible for setting standards concerning cabling, physical topologies, logical topologies and physical access methods for networking products. The Computer Society of IEEE's 802 project committee is divided into several sub-committees that deal with specific standards in these general areas. Specifically the Physical Layer and the Data Link Layer of the ISO's OSI model are addressed.

802.1 This work defines an overall picture of LANs and connectivity.

802.1B This set of standards specifically address the network management.

802.1D Standards for bridges used to connect various types of LANs together were set up with 802.1D.

802.2 Called the Logical Link Control (LLC) standards, this specification governs the communication of packets of information from one device to another on a network.

802.3 Defines the way data has access to a network for multiple topology systems using CSMA/CD. A prime example is Ethernet and Star LAN Systems.

802.4 Standards developed for a token passing scheme on a bus topology. The primary utilization of this specification was the Manufacturing Automation Protocol LANs developed by General Motors, operates at 10 Mbps.

802.5 This standard defines token ring systems. It involves the token passing concept on a ring topology with twisted pair cabling. IBM's token ring system uses this specification; the speed is either 4 Mbps or 16 Mbps.

802.6 Metropolitan Area Networks are defined by this group. MANs are networks that are larger than LANs typically falling within 50 Kilometers. They operate at speeds ranging from 1 Mbps up to about 200 Mbps.

802.7 These are standards concerning broadband LANs.

802.8 This group sets up standards for LANs using fiber optic cabling and access methods.

802.9 This specification covers voice and digital data integration.

802.10 These members set standards for interoperable security.

802.11 Wireless LANs are the subject of this particular subcommittee's works. Both infrared and radio LANs are covered.

Advantages of LAN over Mini and Mainframe Computers

Mainframe computers or Mini computers have a huge processing power. Many users are attached to the CPU with the help of 'dumb terminals'. Though, the processing power and number of people interacting with the computer is great economically, such computing power would be very expensive. The advantage of the Mainframe and Mini system are rather rigid giving very little room for the flexibility in design and approach. LAN on the contrary is modular which can be altered as per the user requirement.

Flexibility is another advantage of the networked PCs. The setup and operations of Mainframe and Mini systems are rather rigid giving very little room for the flexibility in design and approach LAN on the contrary is modular which can be altered as per the user requirement.

Scalability is very difficult and time and money consuming for Mainframes and Minis while LAN is ideally suitable for this. Skilled and highly qualified engineers are required for the

operations of Mainframe and Minis whiles users themselves can manage LANs without any problem. Even the installation and commissioning is extremely easy for LANs.

Questions

1. Bring out the concept of Local Area Network?
2. Explain the "International Standard Organization (ISO) functions and bring out the techniques of OSI model?
3. What is TCP/IP reference model?
4. What are LAN Protocols & LAN standards? Explain?
5. Discuss the Characteristics & Users of LAN?

Chapter 4

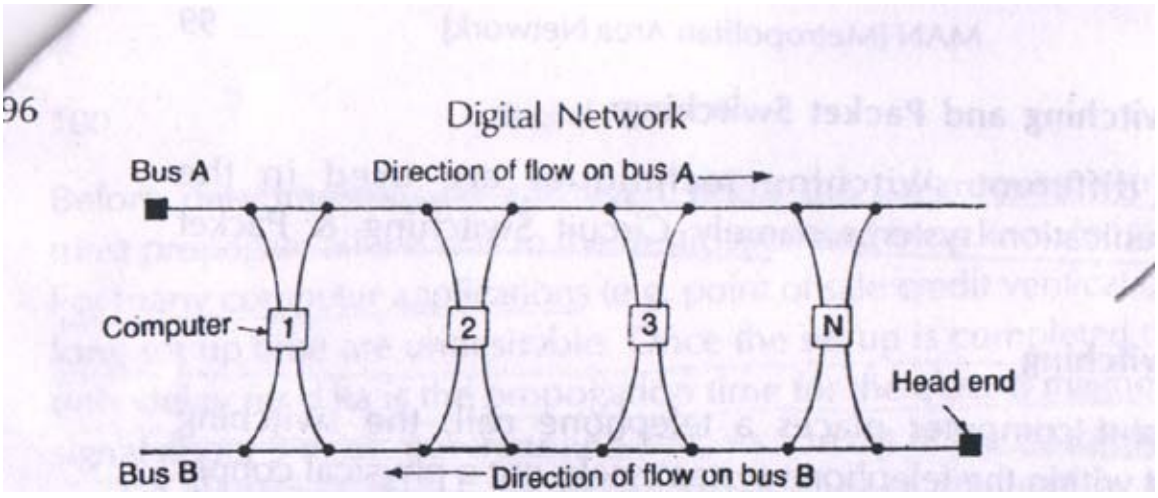
METROPOLITAN AREA NETWORK

- Introduction
- Circuit Switching & Packet Switching
- Synchronous and Asynchronous Transfer Mode
- ATM Classes of Services

Metropolitan Area Network

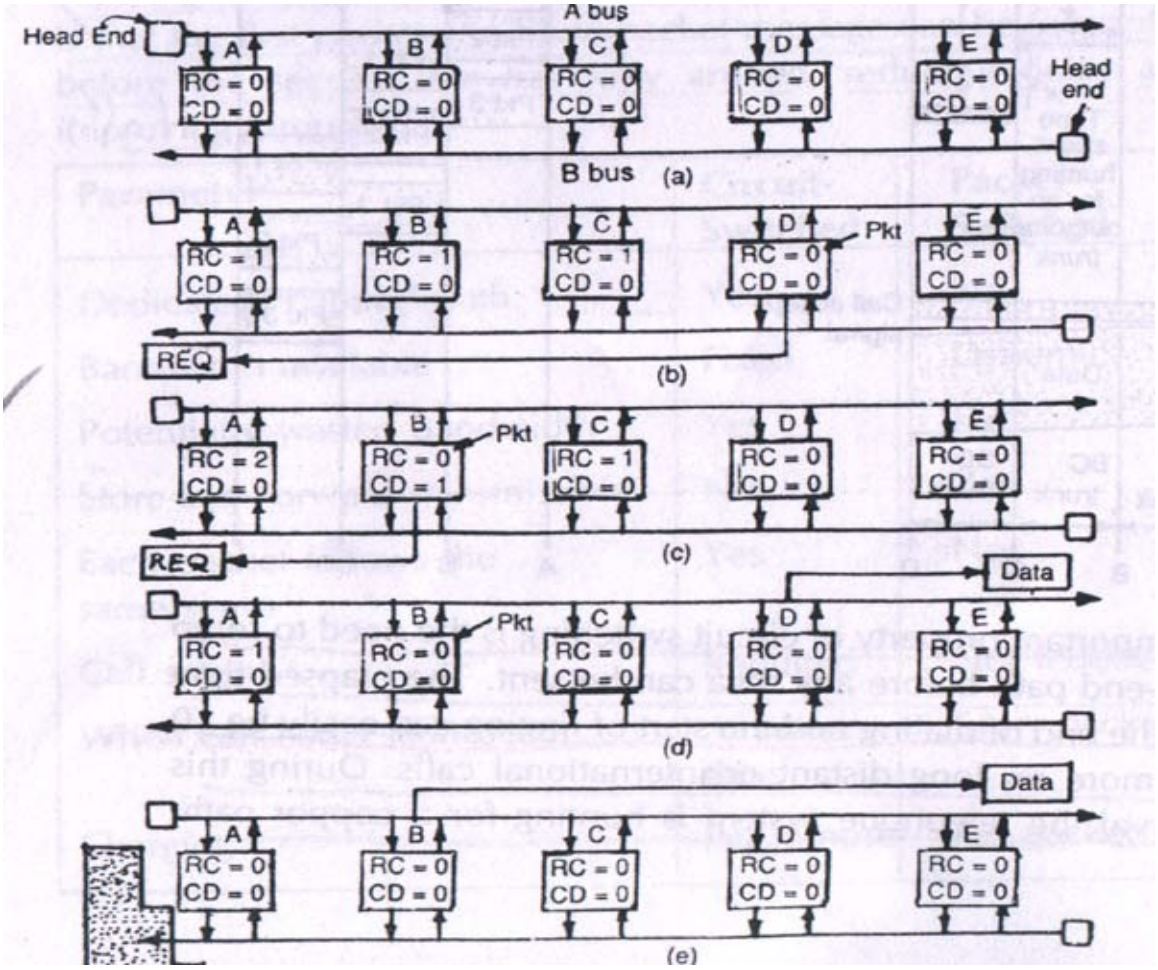
Is basically a bigger version of LAN and uses similar technology. It covers a group of near by corporate offices or a city and might be either private or public. It can support both data and voice and might even be related to the local cable television network.

The technology aspect of MAN is that there is a broadcast medium, to which all the computers are attached. For networks covering an entire city, IEEE defined one MAN called DQDB (Distributed Queue Dual Bus), as standard 802.6.



The basic geometry 802.6 is that two parallel uni-directional busses make through the city with stations attached to both busses in parallel. Each bus has a head end, which generates a steady stream of 53 byte cells. Each cell travels down stream from the head end. When it

reaches the end it falls off the bus. Traffic that is destined for a computer to the right of the sender uses the upper bus. Traffic to the left uses the lower one.

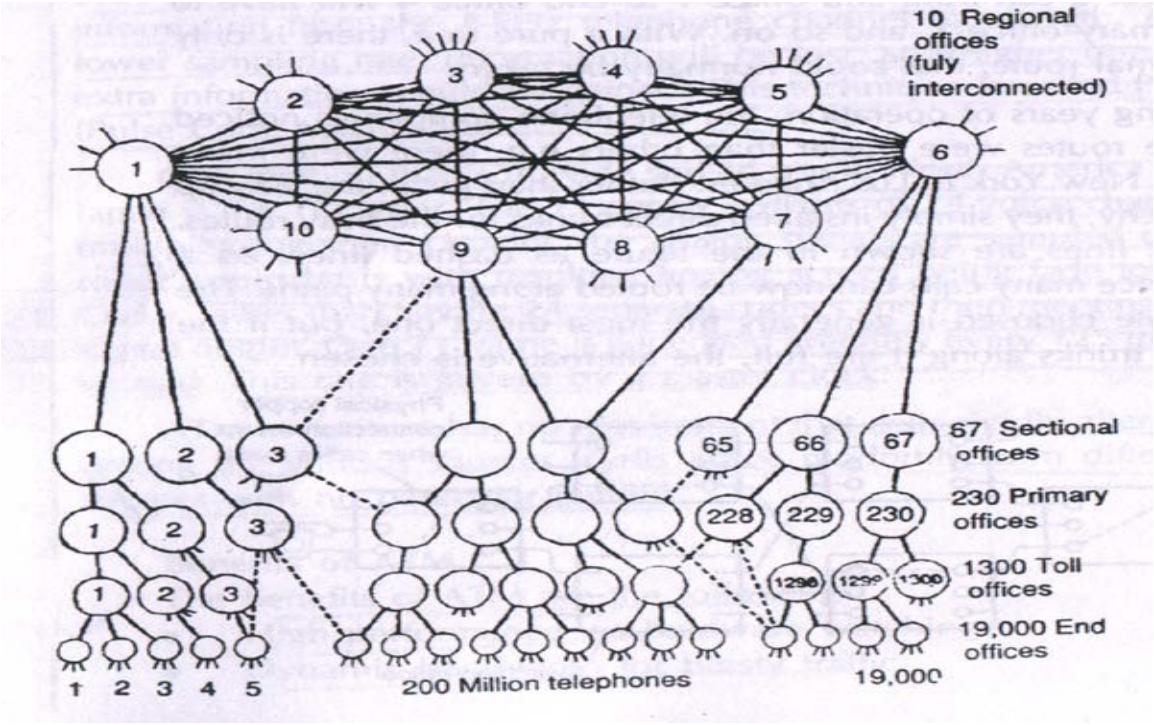


Each cell carries a 44 byte payload field, and it also holds two protocol bits, busy set to indicate that a cell is occupied, and request, which can be set when a station wants to make a request. Here stations queue up in the order till they become ready to send and transmit in FIFO order. The basic rule is that stations are polite. This politeness is needed to prevent a situation in which the station nearest to the head end simply grasp all the empty cells as they come by and fills them up, starving every down stream.

To simulate the FIFO queue, each station maintains two counters, RC & CD. RC (Request Counter) counts the number of downstream request pending until the station itself has a frame to send at that point RC is copied to CD, RC is reset to 0, and now counts the number of request made after the station became ready. For simplicity in the discussion below it is assumed that a station can have only one cell ready for transmission at a time.

Data Transfer in DQDB:

To send the cell, a station must first make a reservation by setting the request bit in some cell on the reverse bus. As this cell propagates down the reverse bus, every station along the way notes it and increments it's RC. Initially all the RC counters are 0 and no cells are queued up as shown in the figure. Then station D makes a request, which causes station C, B, and A, to increment their RC counters, after that D makes a request copying its current RC value in CD. At this point the head end on bus A generates an empty cell. As it passes by B, that station sees that its CD > 0, so it may not use the empty cell (when a station has a cell queue, CD represents its position in the queue, with 0 being front of the queue). Instead it decrements CD. When the still empty cell gets to B, that station sees that CD = 0, meaning that no one is ahead of it on the queue, so it inserts its data into the cell and sets the busy bit. In this way stations queue up to take turns without a centralized queue manager. Many carriers throughout the entire cities are now installing DQDB systems. Typically they run for up to 160 KM at speeds of 44.736 Mbps.

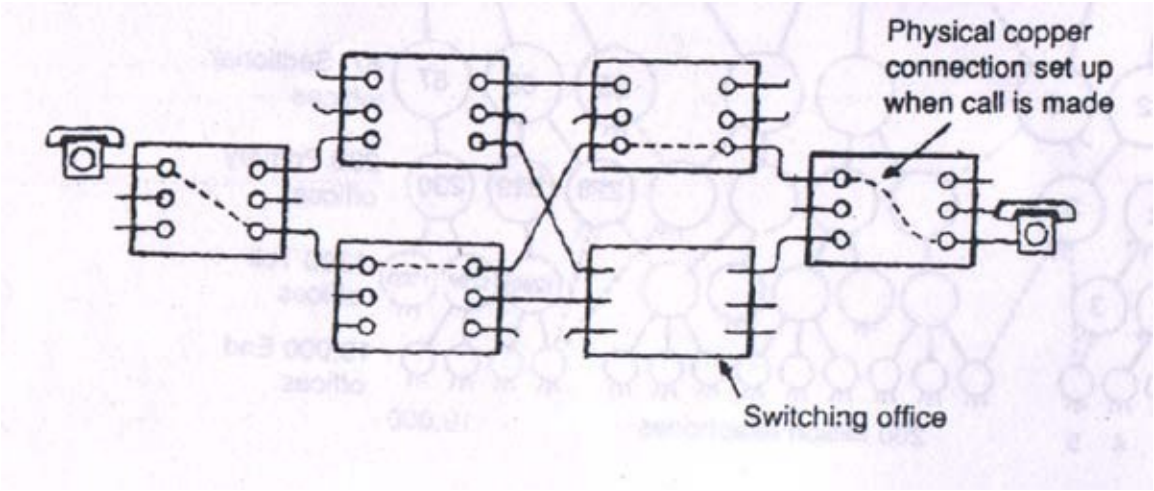


ATM (Asynchronous Transfer Mode)

The PSTN (Public Switched Telephone Network):

In AT & T system which can be looked at as a general model the telephone system has five classes of switching offices. Calls are generally connected at the lowest possible level. Thus, if a subscriber is connected to end office 1 calls another subscriber connected to end office 1 the call will be completed to that office. However calls from customer attached to end office 1 to a customer attached to end office 2 will have to go to toll office 1. However a call from end office 1 to end office 4 will have to go to primary office 1, and so on. With a pure tree, there is only one minimal route that could normally be taken.

The telephone companies noticed that some routes were busier than other e.g. There were many calls from New York to Los Angeles. Rather than go all the way up the hierarchy, they simply installed direct trunks for the busy routes. Few such lines are shown in the figure as dashed lines. As a consequence many calls can now be routed along many paths. The actual route choosed is generally the most direct one, but if the necessary trunks along it are full, the alternative is chosen.

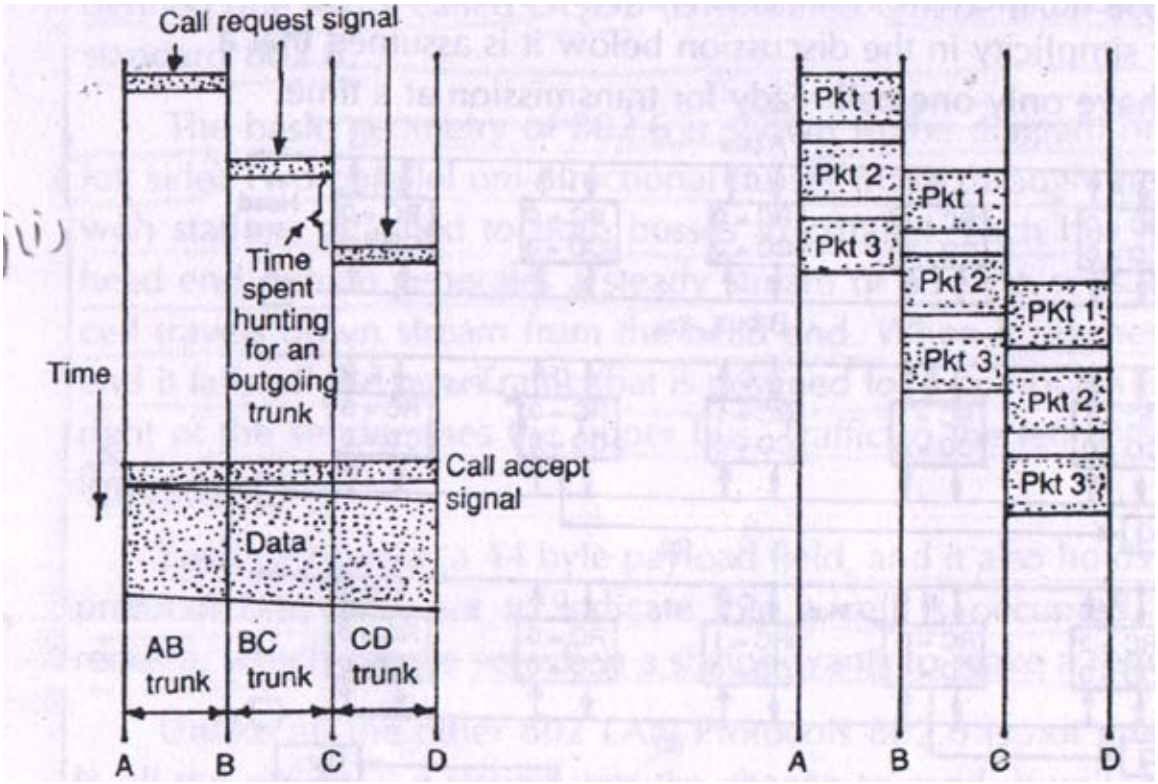


Circuit Switching and Packet Switching

Two different switching techniques are used in the telecommunications systems namely Circuit Switching and Packet Switching.

Circuit Switching:

When a computer places a telephone call, the switching equipment within the telephone system seeks out a physical copper path all the way from the senders telephone to the receiver telephone, this technique is called Circuit Switching and is shown fig (i).



An important property of circuit switching is the need to setup an end-to-end path before any data can be sent. The elapsed time between the end of dialing and the start of ringing can easily be 10 seconds, more on long distant or international calls. During this time interval the telephone system is hunting for a copper path. For many computer applications long setup time are undesirable. Once the setup is completed the only delay for data is the propagation time for the electro magnetic signal about 5 msec. per thousand Km's. As a result of the established path there is no danger of congestion i.e. once the call is put through, you never get busy signals, although you might get one before the connection has been established due to lack of switching or trunk capacity.

Packet Switching:

In packet Switching fixed length blocks or packets or information is sent over the transmission line. By making sure that no user can monopolize any transmission line for very long packet switching networks are well suited for handling interactive traffic. The further advantage of packet switching is that the first packet of a Multi-packet message can be forwarded before the second one has fully arrived, reducing delay and improvement throughput.

Parameter	***Circuit – Switched***	***Packet – Switched***
Dedicated "copper" path	Yes	No
Bandwidth available	Fixed	Dynamic
Potentially Wasted Bandwidth	Yes	No
Store-and-forward transmission	No	Yes
Each packet follows the same route	Yes	No
Call Setup	Required	Not Required
When can congestion occur	At setup time	Not packet
Charging	Per minute	Per packet

Synchronous & Asynchronous Transfer Mode:

Analog signals at digitized in the end office by a device called Codec (Code Decoder), reducing 8-bit number. The Codec makes 8000 samples per second (125 micro second per sample) because the Nyquist Theorem says that this is sufficient to capture all the information from the 4 kHz telephone channel bandwidth. At a lower sampling rate, information will be lost; at a higher one, no extra information would be gained. This technique is called PCM (Pulse Code Modulation).

One method that is in wide use in North America and Japan is the T1 carrier. The T1 carrier consists of 24 voice channel multiplex together. Usually, the analog signals are sampled on a round robin basis with resulting analog screen being fade to the Codec rather than having 24 separate Codecs and then merging the digital output. One T1 frame is generated precisely every 125 micro second. This rate is governed by a master clock.

ATM in contrast has no requirement that cells rigidly alternate among the various sources. Cells arrive randomly from different sources with no particular pattern.

The benefits of ATM are the following:

1. High performance via hardware watching
2. Dynamic bandwidth for bursty traffic
3. Class-of-service support for multimedia

4. Scalability in speed and network size
5. Opportunities for simplification via VC architecture
6. International standards compliance

The high-level benefits delivered through ATM services deployed on ATM technology using International ATM standards can be summarized as follows:

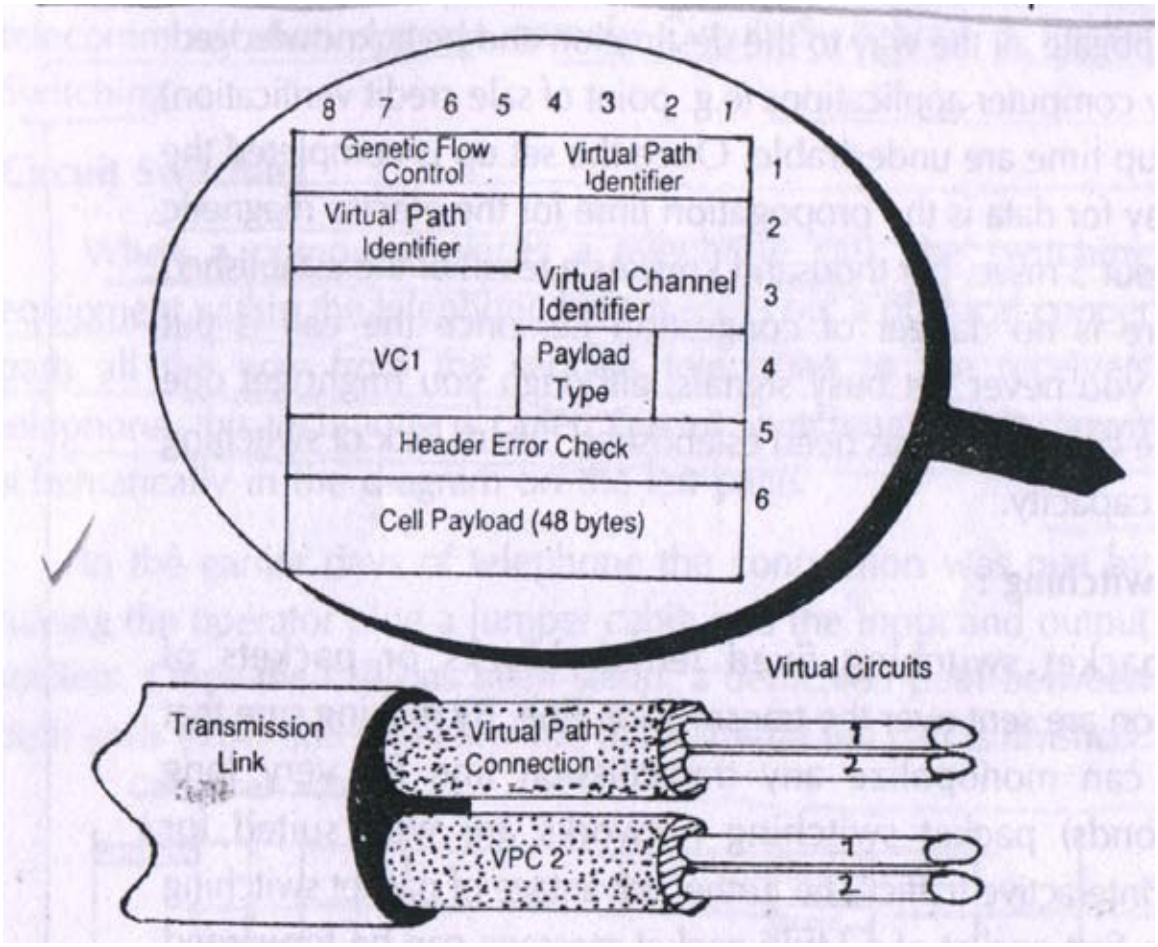
High performance via hardware switching with terabit switches on the horizon. Dynamic bandwidth for bursty traffic meeting application needs and delivering high utilization of networking resources. Most applications are or can be viewed as inherently bursty; data applications are LAN-based and are very bursty, voice is bursty since both parties are either speaking at once or all the time; video is bursty since the amount of motion and required resolution varies over time.

Class-of-service support for multimedia traffic allowing applications with varying throughput and latency requirement to be met on a single network.

Scalability in speed and network size supporting link speeds of T-1/E-1 to OC-12 (622 Mbps) today and into the multi Gbps range before the end of the decade. Common LAN/WAN architecture allowing ATM to be used consistently from one desktop to another.

Opportunities for simplification via switched VC architecture. This is particularly for LAN-Based traffic, which today is connectionless in nature. The simplification possible through ATM VCs could be in areas such as billing, traffic management, security, and configuration management.

International Standards compliance in central office and customer-premise environments allowing for multi-vendor operation.



ATM Technology:

In ATM networks, all information is formatted into fixed length cells consisting of 48 bytes (8 bits per byte) of payload and 5 bytes of cell header. The fixed cell size ensures that time-critical information such as voice or video is not adversely affected by long data frames or packets. The header is organized for efficient switching in high-speed hardware implementations and carries payload-type information, virtual-circuit identifiers, and header error check.

ATM is connection oriented. Organizing different streams of traffic in separate cells allows the user to specify the resources required and allows the network to allocate resources based on these needs. Multiplexing multiple streams of traffic on each physical facility combined with the ability send the streams to many different destinations enables cost savings through a reduction in the number of interfaces and facilities required constructing a network.

ATM standards defined two types of ATM connections:

a) Virtual path connections (VPC) which contain virtual channel connections (VCC).

b) A virtual channel connection (or virtual circuit) is the basic unit, which caries a single of cells, in order, from user to user.

A collection of virtual circuits can be bundled together into a virtual path connection. A virtual path connection can be created from end-to end across an ATM network. In this case, the ATM network does not route cells belonging to a particular virtual circuit. All cells belonging to a particular virtual path are routed the same way through the ATM network, thus resulting in faster recovery in case of major failures.

An ATM network also uses virtual paths internally for purposes of bundling virtual circuits together between switches. Two ATM switches may have many different virtual channel connections between them, belonging to different users. These can be bundled by the two ATM switches into a virtual path connection. This can serve the purpose of a virtual trunk between the two switches. This virtual trunk can then be handled as a single entity by, perhaps, multiple intermediate virtual path cross connects between the two virtual circuit switches.

Virtual circuits can be statistically configured as permanent virtual circuits (PVCs) or dynamically controlled via signaling as switched virtual circuits (SVCs). They can also be point-to-point or point-to-multipoint, thus providing a rich set of service capabilities. SVCs are the preferred mode of operation because they can be dynamically established, thus minimizing reconfiguration complexity.

ATM CLASSES OF SERVICES:

ATM is connection oriented and allows the user to dynamically specify the resources required on a per-connection basis (per SVC). There are the five classes of service defined for ATM (as per ATM Forum UNI 4.0 specification). The Qos parameters for these service classes are summarized in the following table.

ATM Service Classes:	
Service Class Constant Bit Rate (CBR)	Quality of service parameter This class is used for emulating circuit switching. The cell rate is constant with time. CBR applications are quite sensitive to cell-delay variation. Examples of applications that can use CBR are telephone traffic, video conferencing, and television.
Variable Bit Rate-Non-Real Time	This class allows users to send traffic at a rate that varies with time depending on the availability of user information. Statistical multiplexing is provided to make optimum use of network resources. Multimedia e-mail is an example of VBR-NRT.
Variable Bit Rate-Real Time	This class is similar to VBR-NRT but is designed for applications that are sensitive to cell delay variation. Examples for real time VBR are voices with speech activity detection (SAD) and interactive compressed video.
Available Bit Rate (ABR)	This class of ATM services provides rate based flow control and is aims at data traffic such as file transfer and e-mail. Although the standard does not require the cell transfer delay and cell-loss ration to be guaranteed or minimized; it is desirable for switches to minimize delay and loss as much as possible. Depending upon the state of congestion in the network, the source is required to control its rate. The users are allowed to declare a minimum cell rate, which is guaranteed to the connection by the network
Unspecified Bit Rate (UBR)	This class is the catch-all “other” class, and is widely used today for TCP/IP.

Questions

1. What is Metropolitan Area Network? Explain?

2. What is DQDB structure?
3. What is Asynchronous Transfer Mode? Discuss.
4. Explain the Concept of Circuit and Packet Switching?
5. Explain in detail the functions of Asynchronous and Synchronous Transfer Mode?
6. What is ATM Technology & Explain its benefits?

Chapter 5
COMMERCIAL LAN SYSTEMS ETHERNET

- The Ethernet LAN
- Standard Ethernet Limitations
- 10 Mbps Switched Ethernet
- 100 Mbps Fast Ethernet
- The Arc Net LAN
- The IBM Token Ring LAN
- Fiber Distributed Data Interface.

WHAT IS ETHERNET?

Ethernet is a type of network cabling and signaling specifications (OSI Model layers 1 [physical] and 2 [data link] originally developed by Xerox in the late 1970s. It is the least expensive high-speed LAN alternative Ethernet adapter cards for a PC range from $60 to $120. They transmit and receive data at the speed of 10 million bits per second through up to 300 feet of telephone wire to a "hub" device normally stacked in a wiring closet. The hub adds less than $50 to the cost of each desktop connection. Data is transferred between wiring closets using either a heavy coax cable ("Thicknet") or fiber optic cable.

Invention of Ethernet

Dr. Robert Metcalfe at Xerox PARC created the Ethernet. He realized that he could improve on the Aloha system of arbitrating access to a shared communications channel. He developed a new system that included a mechanism that detects when a collision occurs (collision detect). The system also includes "listen before talk", in which stations listen for activity (carrier sense) before transmitting, and supports access to a shared channel by multiple stations. Put all these components together. Ethernet channel access protocol is called Carrier Sense Multiple Access with Collision Detect (CSMA/CD). Metcalfe also developed a much more sophisticated backoff algorithm, which in combination with the CSMA/CD protocol, allows the Ethernet system to function all the way upto 100 percent load.

In late 1972, Metcalfe and his Xerox PARC colleagues developed the first experimental Ethernet system to interconnect the Xerox Alto. The Alto was a personal workstation with a graphical user interface, and experimental Ethernet was used to link Altos to one another, and to servers and laser printers. The signal clock for the experimental Ethernet interfaces was derived from the Alto's system clock, which resulted in a data transmission rate on the experimental Ethernet of 2.94 Mbps.

To base the name on the word "ether" as a way of describing an essential feature of the system: the physical medium carries bits to all stations, much the same way that the old "luminiferous ether" was once through to propagate electromagnetic waves through space. Thus, Ethernet was born.

Operation of Ethernet.

Each Ethernet-equipped computer, also known as a station, operates independently of all other stations on the network, there is no central controller. All stations attached to an Ethernet are connected to a shared signaling system, also called the medium. Ethernet signals are transmitted serially, one bit at a time, over the shared signal channel to every attached station. To send data a station first listens to the channel, and when the channel is idle the station transmits its data in the form of an Ethernet frame, or packet.

All stations on the network must contend equally for the next frame transmission opportunity. This ensures that access to the network channel is fair, and that no single station can lock out the other stations. Access to the shared channel is determined by the Medium Access Control (MAC) mechanism embedded in the Ethernet interface located in each station.

Access and collisions

Ethernet uses a protocol called **CSMACD**. This stands for "Carrier Sense, Multiple Access, Collision Detect". The "Multiple Access" part means that every station is connected to a single copper wire (or a set of wires that are connected together to form a single data path). The "Carrier Sense" part says that before transmitting data, a station checks the wire to see if any other station is already sending something. If the LAN appears to be idle then the station can begin to send data.

Need for Collusion Detect

An Ethernet station sends data at a rate of 10 megabits per second. That bit allows 100 nanoseconds per bit. Light and electricity travel about one foot in a nanosecond. Therefore, after the electric signal for the first bit has traveled about 100 feet down the wire, the station has begun to send the second bit. An Ethernet cable can run for hundreds of feet. If two stations are located, say, 250 feet apart on the same cable and both begin transmitting at the same time, and then they will be in the middle of the third bit before the signal from each reaches.

"Collision Detect" part. Two stations can begin to send data at the same time, and their signals will "collide" nanoseconds later. When such a collision occurs, the two stations stop transmitting, "back off", and try again later after a randomly chosen delay period.

Ethernet can be built using a repeater. A repeater is a simple station that connected to two wires. Any data that it receives on one wire repeats bit-for-bit on the other wire. When collisions occur, it repeats the collision as well.

The connection to the desktop uses ordinary telephone wire, the hub back in the telephone closet contains a repeater for every phone circuit. Any data coming down any phone line is copied onto the main Ethernet coax cable, and any data from the main cable is duplicated and transmitted down every phone line. The repeaters in the hub electrically isolate each phone circuit, which is necessary if a 10 megabit signal is going to be carried 300 feet on ordinary wire.

Any system based on collision detect must control the time required for the worst round trip through the LAN. As the term "Ethernet" is commonly defined, this round trip is limited to 50 microseconds (millionths of a second). AT a signaling speed of 10 million bits per second, this is enough time to transmit 500 bits. At 8 bits per byte, this is slightly less than 64 bytes.

Given below are some of the devices used:

- **Receives and then immediately retransmits each bit.** It has no memory and does not depend on any particular protocol. It duplicates everything, including the collisions.

- **Receives the entire message into memory.** If a collision or noise damages the message, then it is discarded. If the bridge knows that the message was being sent between two stations on the same cable, then it discards it. Otherwise, the message is queued up and will be retransmitted on another Ethernet cable. Its actions are transparent to the client and server workstations.

- **Acts as an agent to receive and forward messages.** The router has an address and is known to the client or server machines. Typically, machines directly send messages to each other when they are on the same cable, and they send the router messages addressed to another zone, department, or sub-network. Routing is a function specific to each protocol. For IPX, the Novel server can act as a router. For SNA, an APPN

Network Node does the routing. TCP/IP can be routed by dedicated devices, UNIX workstations, or OS/2 servers.

There is a specialized device that finds problems in an Ethernet LAN. It plugs into any attachment point in the cable, and, sends out its own voltage pulse. The effect is similar to a sonar "ping". If the cable is broken then there is no proper terminating resistor. The pulse will hit the loose end of the broken cable and will bounce back. The test device senses the echo, computes how long the round trip took, and then reports how far away the break is in the cable.

If the Ethernet cable is shorted out, a simple volt meter would determine that the proper resistor is missing from the signal and shield wires. Again, by sending out a pulse and timing the return, the test device can determine the distance to the problem.

Ethernet Frame and Ethernet Address

The heart of the Ethernet system is the Ethernet frame, which is used to deliver data between computers. The frame consists of a set of bits organized into several fields. These fields include address fields, a variable size data field that carries from 46 to 1,500 bytes of data, and an error checking field that checks the integrity of the bits in the frame to make sure that the frame has arrived intact.

The first two fields in the frame carry 48-bit address, called the destination and source address. The IEEE controls, the assignment of these addresses by administering a portion of the address field. The IEEE does this by providing 24-bit identifiers called "Organizationally Unique Identifiers" (OUIs), since a unique 24-bit identifier is assigned to each organization, in turn, creates 48-bit address using the assigned OUI as the first 24 bits of the address. This 48-bit address is also known as the physical address, hardware address or MAC address.

When Ethernet frame is sent onto the shared signal channel, all Ethernet interfaces look at the first 48 bit field of the frame, which contains the destination address. The interfaces compare the destination address of the frame with their own address. The Ethernet interface with the same address as the destination address in the frame will read in the entire frame and deliver it to the networking software running on that computer. All other network interfaces

will stop reading the frame when they discover that the destination address does not match their own address.

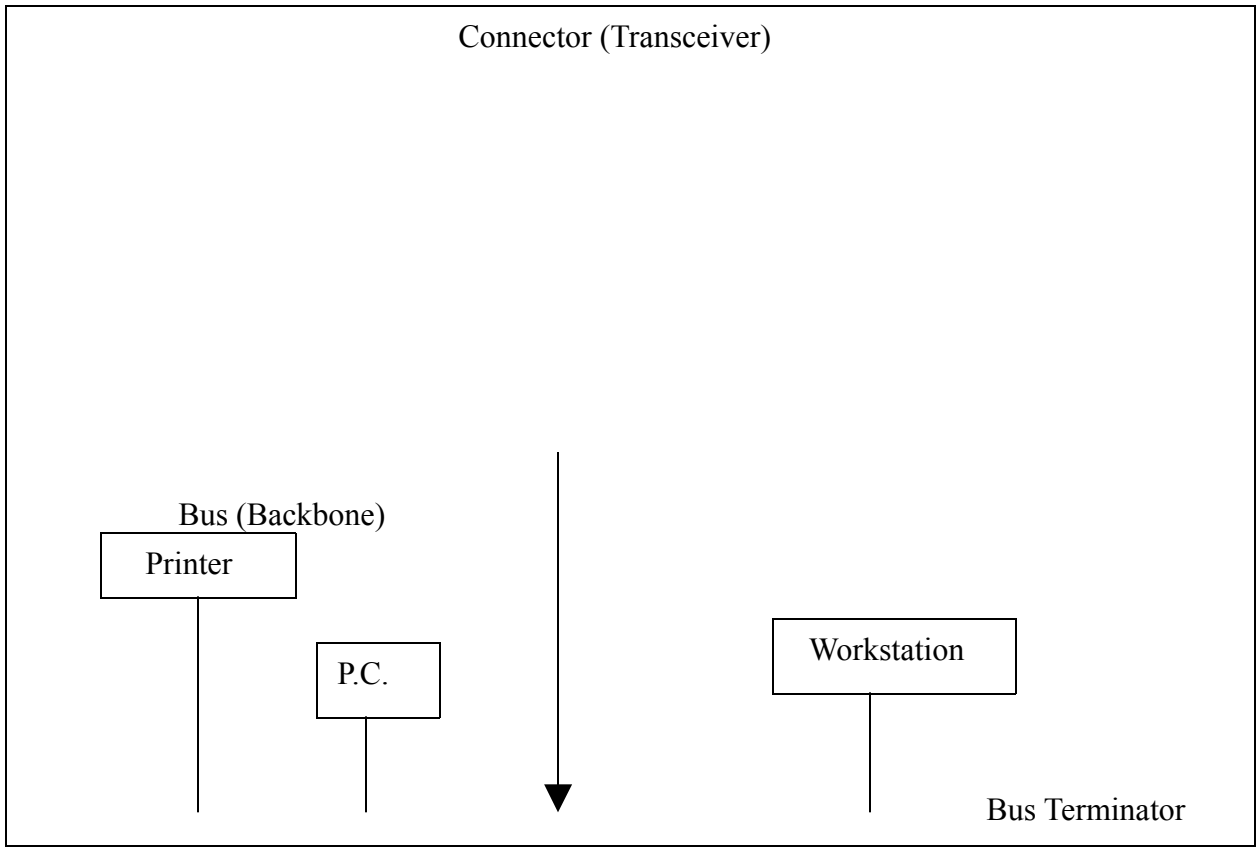
Given below is a diagram of Ethernet frames.

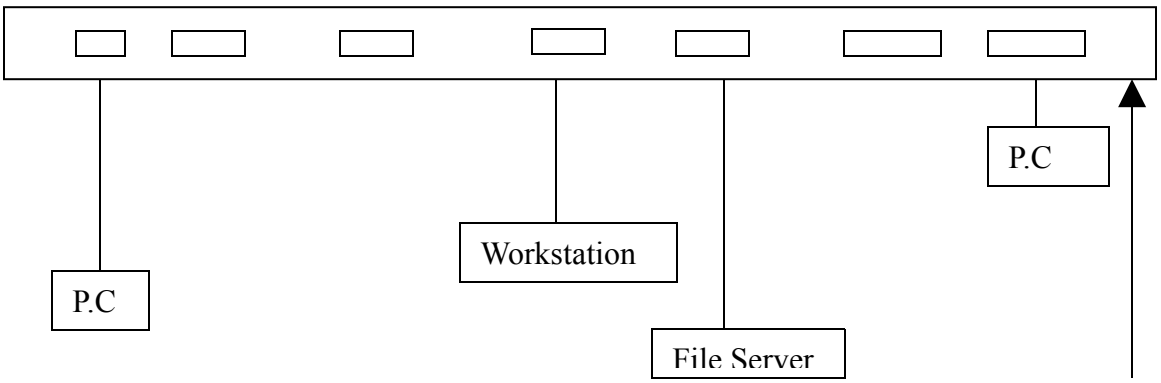
Preamble	SFD	Destination	Source	LEN	Data	PAD	CRC
7	1	2 or 6	2 or 6	2	0-1500	0-46	4

Ethernet Frames

High-Level Protocols and Ethernet Addresses

Computers attached to an Ethernet can send application data to one another using high-level protocol software, such as the TCP/IP protocol suite used on the worldwide Internet. The high-level protocol packets are carried between computers in the data field of Ethernet frames. The system of high-level protocols carrying application data and the Ethernet system are independent entities that cooperate to deliver data between computers.





Multiple Ethernet segments can be linked together to form a large Ethernet LAN using a signal amplifying and retiming device called a repeater. Through the use of repeaters, a given Ethernet system of multiple segments can grow as a "non-rooted branching tree. "This means that each media segment is an individual branch of the complete signal system. Even though the media segments may be physically connected in a star pattern, with multiple segments attached to a repeater, the logical topology is still that of a single Ethernet channel that carries signals to all stations.

The notion of "tree" is just a formal name for systems like this, and a typical network design actually ends up looking more like a complex concatenation of network segments. On media segments that support multiple connections, such as coaxial Ethernet, you may install a repeater and a link to another segment at any point on the segment. Other types of segments known as link segments can only have one connection at each end this is described in more detail in the individual media segment chapters.

"Non-rooted" means that the resulting system of linked segments may grow in any direction, and does not have a specific root segment. Most importantly, segments must never be connected in a loop. Every segment in the system must have two ends, since the Ethernet system will not operate correctly in the presence of loop paths.

There are media segments linked with repeaters and connecting to stations. A signal sent from any station travels over that station's a signal sent from any station travels over that station's segment and is repeated onto all other segments. This way all other stations hear it over the single Ethernet channel.

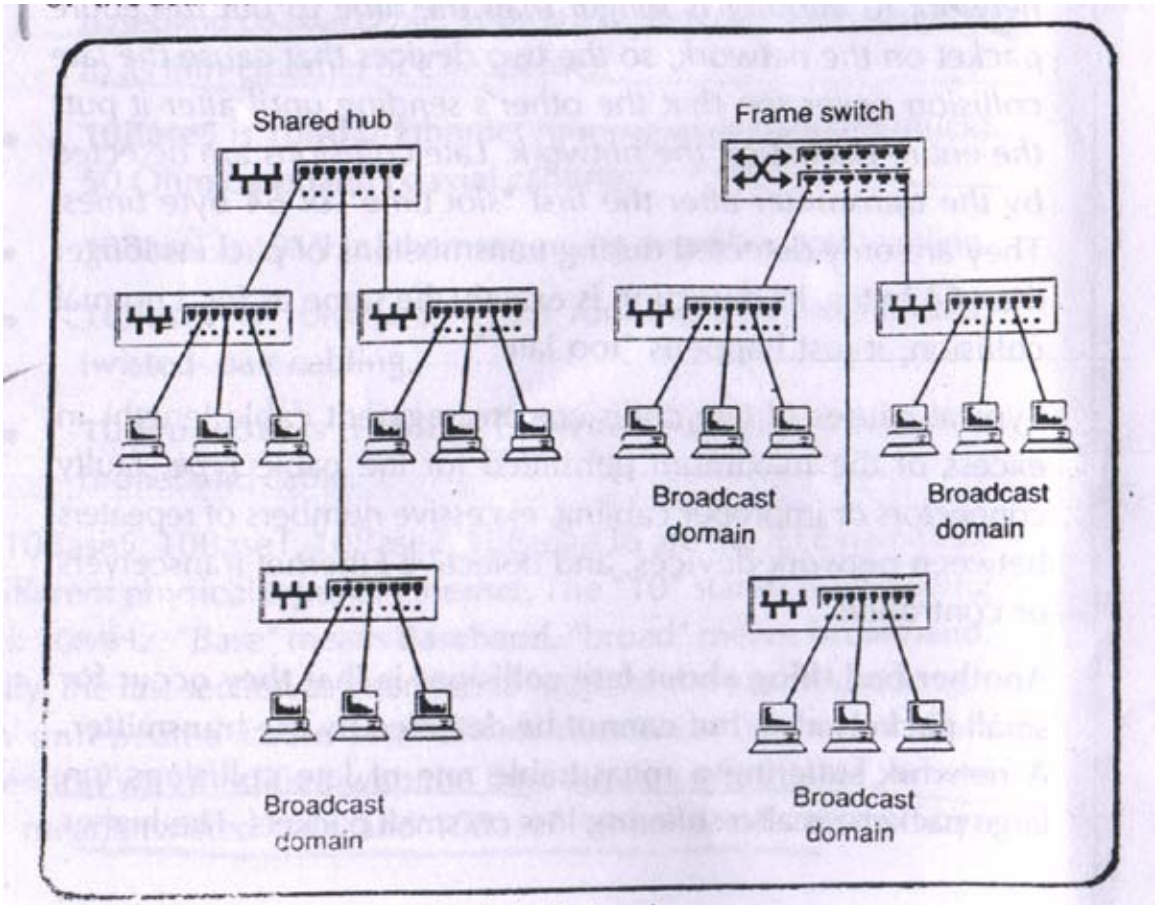
Extending Ethernet with Hubs

Ethernet was designed to be easily expandable to meet the networking needs of a given site. To help extend Ethernet systems, networking vendors sell devices that provide multiple Ethernet ports. These devices are known as hubs, since they provide the central portion or hub, of a media system.

There are two major kinds of hubs: repeater hubs and switching hubs. Each port of a repeater hub links individual Ethernet media segments together to create a larger network that operates as a single Ethernet LAN. The total set of segments and repeaters in the Ethernet LAN must meet the round trip timing specifications. The second kind of hub provides packet switching, typically based on bridging ports.

The important thing to know at this point is that each port of a packet switching hub provides a connection to an Ethernet media system that operates as a separate Ethernet LAN. Unlike a repeater hub whose individual ports combine segments together to create a single large LAN, a switching hub makes it possible to divide a set of Ethernet media systems into multiple LANs that are linked together by way of the packet switching electronics in the hub.

A given Ethernet LAN can consist of merely a single cable segment linking some number of computers, or it may consist of a repeater hub linking several such media segments together. All Ethernet LANs can themselves be linked together to form extended network systems using packet switching hubs. While an individual Ethernet LAN can typically support anywhere from a few up to several dozen computers, the total system of Ethernet LANs linked with packet switches at a given site may support many hundreds or thousands of machines.



Shared hub and switched network

DEFINITIONS AND STANDARDS

The IEEE was assigned the task of developing formal international standards for all Local Area Network technology. It formed the "802" committee to look at Ethernet, Token Ring, Fiber Optic, and other LAN technology. The objective of the project was not just to standardize each LAN individually, but also to establish rules that would be global to all types of LANs so that data could easily move from Ethernet to Token Ring or Fiber Optics.

The IEEE was careful to separate the new and old rules. It recognized that there would be a period when old DIX messages and new IEEE 802 messages would have to coexist on the same LAN. It published a set of standards of which the most important are:

- 802.3 – Hardware standards for Ethernet cards and cables.
- 802.5 – Hardware standards for Token Ring cards and cables.
- 802.2 – The new message format for data on any LAN.

The 802.3 standard further refined the electrical connection to the Ethernet. It was immediately adopted by all the hardware vendors.

However, the 802.2 standard would require a change to the network architecture of all existing Ethernet users. Apple had to change its Ether talk, and did so when converting from phase 1 to phase 2 Appletalk. DEC had to change its DECNET. Novell added 802 as an option to its IPX, but it supports both DIX and 802 message formats at the same time.

The TCP/IP protocol used by the Internet refused to change. Internet standards are managed by the IETF group, and they decided to stick with the old DIX message format indefinitely. This produced a deadlock between two standards organizations that has not been resolved.

IBM waited until the 802 committee released its standards, and then rigorously implemented the 802 rules for everything except TCP/IP where the IETF rules take precedence. This means that NETBEUI (the format for NETBIOS on the LAN) and SNA obey the 802 conventions.

So "Ethernet" suffers from too many standards. The old DIX rules for message format persist for some uses (Internet, DECNET, and some Novell). The new 802 rules apply to other traffic (SNA, NETBEUI). The most pressing problem is to make sure that Novell clients and servers are configured to use the same frame format.

LIMITATIONS OF ETHERNET:

- Old style Ethernet bus wiring is prone to cable failure and quickly consumes allowed distances due to the aesthetic wiring needs.
- Ethernets fail in three common ways,
    1. A nail can be driven into the cable breaking the signal wire.
    2. A nail can be driven touching the signal wire and shorting it to the external grounded metal shield.
    3. Finally, a station on the LAN can break down and start to generate a continuous stream of junk, blocking everyone else from sending.
- Ethernet is particularly susceptible to performance loss from such problems when people ignore the "rules" for wiring Ethernet.
- There are practical limitations to the distance of a shared medium and the number of workstations you can connect to it.

- ❖ The electrical characteristics of the cable also dictate LAN limitations. Network designers have to find a balance between the type of cable used, the transmission rates, signal loss over distance and the signal emanations. All these factors must stay within physical bounds and restrictions specified by various standards and government bodies.
- ❖ Delay is another factor. On Ethernet networks, workstations on either end of a long cable may not even detect that they are transmitting at the same time, thus causing a collision that results in corrupted data.
- ❖ Sometimes late collisions occur when two devices transmit at the same time, but due to cabling errors (most commonly, excessive network segment length to repeaters between devices) neither detects a collision. The reason this happens is because the time to propagate the signal from one end of the network to another is longer than the time to put the entire packet on the network, so the two devices that cause the late collision never see that the other's sending until after it puts the entire packet on the network.

A network suffering a measurable rate of late collisions (on large packets) is also suffering loss on small packets.

10 Mbps SWITCHED ETHERNET

The following list describes the different varieties of 10 Mbps Switched Ethernet:

- 10 Base 2 is 10MHz Ethernet running over thin, 50 Ohm baseband coaxial cable. 10Base2 is also commonly referred to as thin-Ethernet or Cheapernet.
- **10Base5 is** 10 MHz Ethernet running over standard (thick) 50 Ohm baseband coaxial cabling.
- **10Base f** is 10MHz Ethernet running over fiber-optic cabling.
- **10BaseT** is 10MHz Ethernet running over unshielded, twisted-pair cabling.
- **10Broad 36** is 10MHz Ethernet running through a broadband cable.

How does 10 Mbps Ethernet work?

The PHY is the actual transceiver that can be a separate device or it can be integrated on the network card. The transceiver interface is called AUI (Attachment Unit Interface). When a network card doesn't contain the interface there will be a Sub-D15 female connector. On the cable will be a transceiver with a male connector. This means that an AUI-cable will ALWAYS be male-female.

The difference between the different 10 Mbps topologies is in the PHY part. This section connects directly to the cable and is responsible for everything that is medium depended like: line encoding, transmission voltages, SQE, etc.

With AUI there are two ways power can be provided to the units. You either have a positive or negative polarity.

Signal Quality Error (SQE):

The Signal Quality Error signal is also called 'heartbeat' and is a kind of keep alive notification between the transceiver and the Ethernet device. SQE can be ON or OFF between a transceiver and a workstation or file server. It MUST be set OFF between a transceiver and a Repeater.

Max Speed -10 Mbps
Cable Standard-Ethernet Coax Cable
Connectors-N-Type
Terminators-50 Ohm
Max.length of a segment-500m/164oft
Max.number of taps per segment-100
Max .number of stations per network-1024
Min.distance between taps-2.5m/8.3ft
Max.length of transceiver cable-50m/164ft
Max.number of repeaters-4
Topology-Bus.

100 Mbps FAST ETHERNET

There are two LAN standards that can carry Ethernet frames at 100-Mbps.

When the IEEE standardization committee met to begin work on a faster Ethernet system, two approaches were presented. One approach was to speed up the original Ethernet system to 100 Mbps, keeping the original CSMA/CD medium access control mechanism. This approach is called 100BASE-T Fast Ethernet.

Another approach presented to the committee was to create an entirely new medium access control mechanism, one based on hubs that controlled access to the medium using a "demand priority" mechanism. This new access control system transports standard Ethernet frames, but it does it with a new medium access control mechanism. This system was further extended to allow it to transport token ring frames as well. As a result, this approach called 100VG-AnyLAN.

100-Mbps Media Systems

Compared to the 10-Mbps specifications, the 100-Mbps system results in a factor of ten reductions in the bit-time, which is the amount of time it takes to transmit a bit on the Ethernet channel. This produces a tenfold increase in the speed of the packets over the media system. However, the other important aspects of the Ethernet system include the frame format, the amount of data a frame may carry, and the media access control mechanism, are all unchanged.

The Fast Ethernet specifications include mechanism for Auto-Negotiation of the media speed. This makes it possible for vendors to provide dual-speed Ethernet interfaces that can be installed and run at either 10-Mbps or 100-Mbps automatically.

The IEEE identifiers include three pieces of information.

- The first item, "100", stands for the media speed of 100-Mbps.
- The "BASE" stands for "base band," Which is a type of signaling. Baseband signaling simply means that Ethernet signals are the only signals carried over the media system.
- The third part of the identifier provides an indication of the segment type. The "T4" segment type is a twisted-pair segment that uses four pairs of telephone-grade twisted-pair wire. The "TX" segment type is a twisted-pair segment that uses two pairs of wires and is based on the data graded twisted-pair physical medium standard developed by

ANSI. The "FX" segment type is a fiber optic link segment based on the fiber optic physical medium standard developed by ANSI and that uses two strands of fiber cable. The TX and FX medium standards are collectively known as 100BASE-X.

Components Used for a 100-Mbps Connection

The physical medium is used to carry Ethernet signals between computers. This could be any one of the three 100-Mbps media types.

Physical Layer Device

This device performs the same general function as transceiver in the 10-Mbps Ethernet system. It may be a set of integrated circuits inside the Ethernet port of a network device, therefore invisible to the user, or it may be a small box equipped with an MII cable, like the outboard transceiver and transceiver cable.

Medium Independent Interface

The MII is an optional set of electronics that provides a way to link the Ethernet medium access control functions in the network device with the Physical Layer Device (PHY) that sends signals onto the network medium.

The MII is designed to make the signaling differences among the various media segments transparent to the Ethernet chips in the network device.

The MII electronics may be linked to an outboard transceiver through a 40-pin MII connector and a short MII cable.

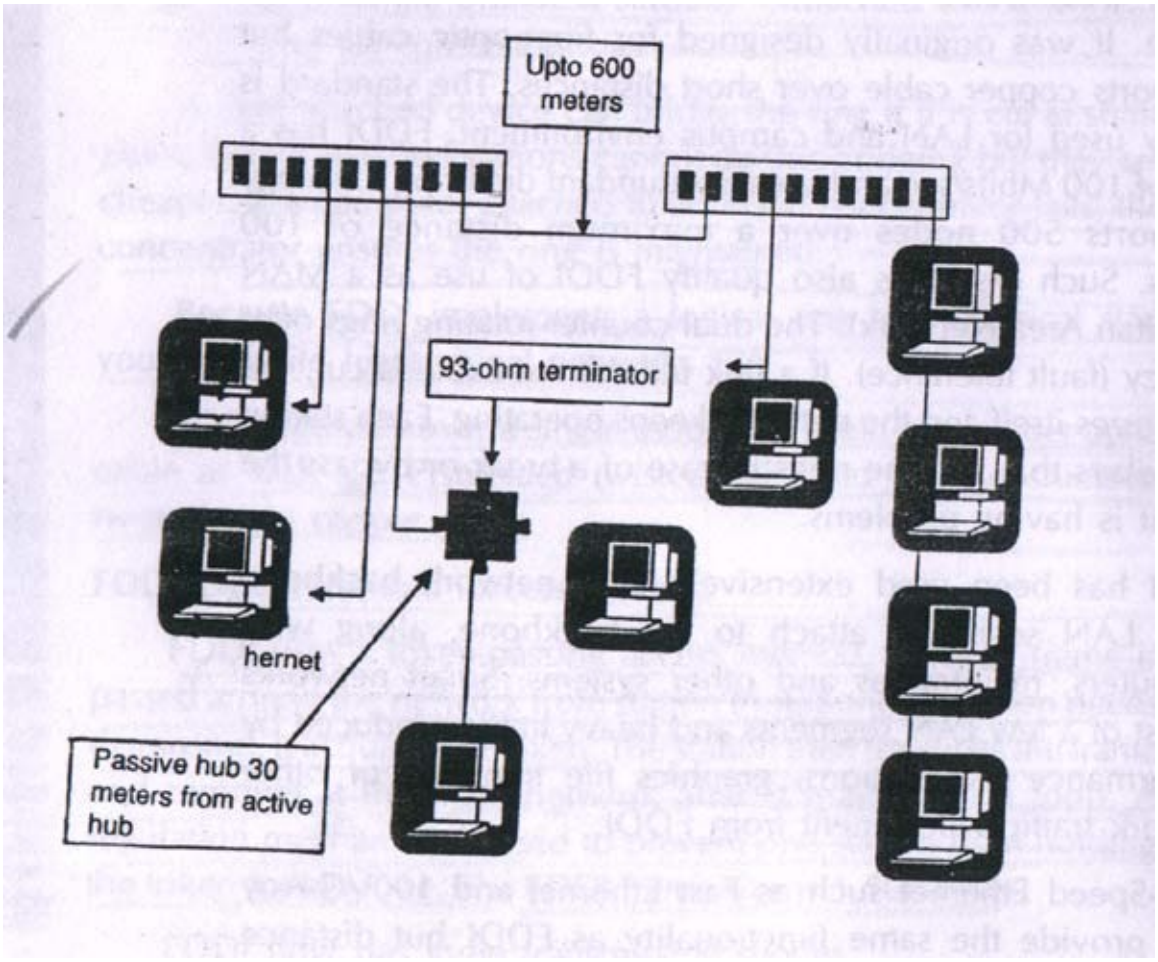
Putting it All Together

For a typical station connection the DET (computer) contains an Ethernet interface which forms up and sends Ethernet frames that carry data between computers attached to the network. The Ethernet interface is attached to the media system using a set of equipment that might include an outboard MII cable and PHY with its associated MDI (twisted-pair RJ45-style jack or fiber optic connector). The interface or repeater port might also be designed to include the PHY electronics internally, in which case all you will see is MDI for whatever physical medium the interface or port was designed to support.

ARCNET CONFIGURATION

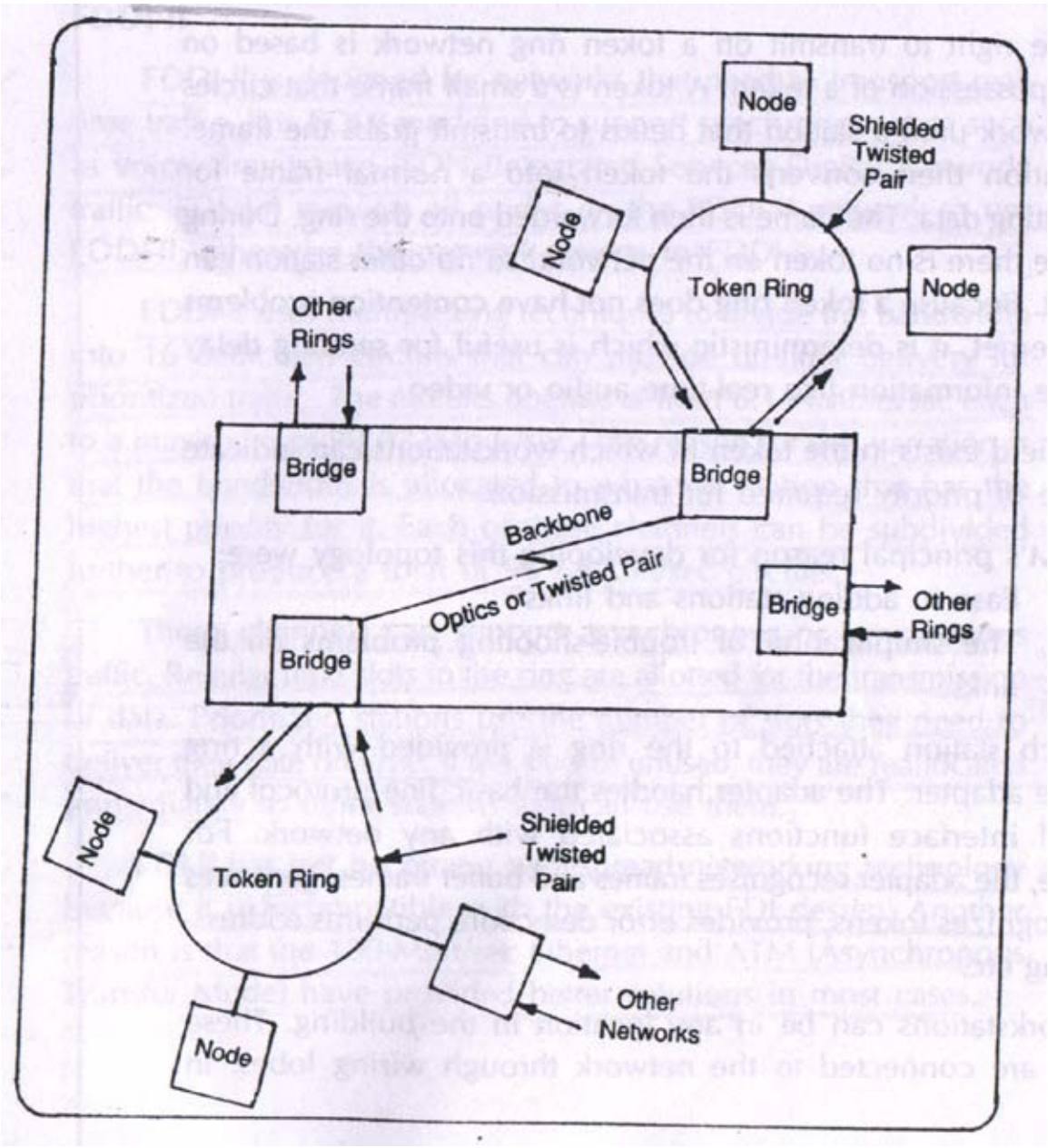
The ARC net (Attached Resource Computing Network) is a base band. Token passing network system that offers flexible star and bus topologies at a low price. Transmission speeds

are 2.5 Mbits per second. ARC net uses a token-passing protocol on a token bus network topology. ARCnet is showing its age and is no longer sold major vendors.



IBM TOKEN RING

In 1985 IBM announced its major entry into LAN field with the IBM Token ring. The IBM topology permits several rings to be attached through the bridges. A backbone ring then connects the bridges. The bridge will provide a cross-ring network by copying frames that are forwarded from one ring to another. The bridges also provide for speed translations if rings are operating at different data rates. More ever each ring still retains its own capacity and will continue operating in the event another ring on the bridge fails. IBM Token ring approach provides resiliency to station and link failure.



FIBER DISTRIBUTED DATA INTERFACE (FDDI)

FDDI is a high-speed networking technology developed by the ANSI (American National Standards Institute) X3T9.5 committee. It was originally designed for fiber-optic cables but now supports copper cable over short distances. The standard is commonly used for LAN and campus environment. FDDI has a data rate of 100 Mbits/sec and uses a redundant dual ring topology that supports 500 nodes over a maximum distance of 100 kilometers. Such distances also qualify FDDI of use as a MAN (Metropolitan Area Network). The dual counter-

rotating rings offer redundancy (fault tolerance). if a link fails or the cable is cut, the ring configures itself and the network keeps operating. Each station contains relays that join the rings in case of a break or bypass the station if it is having problems.

FDDI has been used extensively as a network backbone topology. LAN segments attach to the backbone, along with minicomputers, mainframes and other systems. Small networks that consist of a few LAN segments and heavy traffic produced by high-performance workstations, graphics file transfers, or other internetwork traffic will benefit from FDDI.

FDDI Configuration

The topology is called a physical ring of trees but logically the entire network forms a ring. The two FDDI rings are known as the primary ring and the secondary ring. Both may be used as a transmission path or one may be set aside for use as a back up in the event of a break in the primary ring.

There are three types of devices that can attach to the ring:

- DAS (dual attached station) – connected to both rings, such as a critical server and other pieces of equipment.
- DAC (dual attached concentrator) - connected to both rings and provides a connection point for stations.
- SAS (single attached station) – attached to the primary ring via connector.

If a computer attached to an FDDI concentrator fails, the concentrator ensures the ring is maintained.

Because FDDI implements a logical ring in a physical star, you can build hierarchical networks.

FDDI operates over a single-mode and multi-mode fiber optic cable as well a STP (shielded twisted pair) and UTP (unshielded twisted pair) copper cable.

FDDI Operation and Access Method

FDDI uses a token-passing access method. A token frame is passed around the network from station to station; if a station needs to transmit, it acquires the token. The station then transmits the frame and removes it from the network after it makes a full loop. A regulation mechanism is used to prevent one station from holding the token for too long. The FDDI frame size is 1,500 bytes.

FDDI now has three transmission modes.

- **Asynchronous ring mode:** This is token-based. Any station can access the network by acquiring the token. In this mode traffic is not prioritized.

- **Synchronous token-passing ring mode: A**llows prioritization. FDDI cards with synchronous capabilities give network managers the ability to set aside part of the bandwidth for time-sensitive traffic. Asynchronous workstations then contend for the rest. Synchronous capabilities are added via software upgrades.

The above two modes are available in the original FDDI standard. The third mode, circuit-based can provide dedicated circuits that can be prioritized for voice and other real time traffic. This mode is available in the new FDDI-II standard, which requires new adapter cards.

FDDI-II:

Is designed for networks that need to transport real-time traffic. It is FDDI modified to support synchronous data such as voice circuits and ISDN (Integrated Services Digital Network) traffic. FDDI-II requires all nodes on the FDDI-II network to use FDDI-II; otherwise the network reverts to FDDI.

FDDI uses multiplexing technologies to divide the bandwidth into 16 dedicated circuits that can provide on-time delivery for prioritized traffic. The circuits operate at from 6.144Mbits/sec each to a maximum of 99.072 Mbits/sec. The reason for this variation is that the

bandwidth is allocated to whatever station that has the highest priority for it. Each of these channels can be subdivided further to produce a total of 96 64Kbit/sec circuits.

These channels can support asynchronous or synchronous traffic. Regular time slots in the ring are allotted for the transmission of data. Prioritized stations use the number of slots they need to deliver their data on time. If the slots are unused, they are reallocated immediately to other stations that can use them.

FDDI-II has not become a widespread networking technology because it is incompatible with the existing FDDI design. Another reason is that the 100-Mbit/sec Ethernet and ATM (Asynchronous Transfer Mode) have provided better solutions in most cases.

Questions

1. What is Ethernet? What are its limitations?
2. Explain the functions of 10Mbps & 100Mbps Ethernets?
3. What is an ARCNET LAN? Explain.
4. Explain in brief IBM Token ring? Fibre Distributed Data Interface (FDDI) Techniques?

Chapter 6
INTEGRATED SERVICES DIGITAL NETWORK

- Introduction
- Types of ISDN
- Functions of ISDN
- ISDN Standards
- Future Applications of ISDN
- User Network Interfaces

Introduction to ISDN

The telephone service has been developed over the last 100 years. Initially its sole aim was to provide simple one to one voice communications between subscribers, but we have seen that technology has influenced the telephone network in two ways.

Firstly improvements in technology such as the introduction of digital switching, computer control and common channel signaling have meant that the network can offer its users far more facilities than simple one to one voice calls.

Secondly the introduction of new technology in other business areas has resulted in a situation in which the POTS (Plain Old Telephone Service) are carrying a wide variety of data communications traffic. Although it is true to say that the major use of the network is still for voice communications, a growing percentage of the traffic is accounted for by digital traffic, i.e. data communications and facsimile.

The limitations of Traditional Communications Networks, which used analogue switching and transmission are caused by the following factors:

1. The old network is noisy, resulting in bit errors.
2. Call setup times are long, the call set up time may exceed the holding time.
3. Transmission is limited to specific bandwidth pathway.
4. Routing of calls is not fixed, and thus variations in transmission performance due to effects such as group delay are experienced on different calls between any two given locations.

Over recent years the communications infrastructure has evolved in such a way that services are provided on dedicated networks, each with its own subscriber access and interface requirements. The services provided can be categorized into:

1. Point to Point Digital Leased lines
2. Circuit Switch Telegraph (Telex)
3. Packet Switch data network

The cost of building and maintaining dedicated networks is so large that it can only be contemplated if the demand for the service is large enough to generate sufficient revenue to make it economic. These high costs therefore prohibit the introduction of new specialized communication services.

large market.

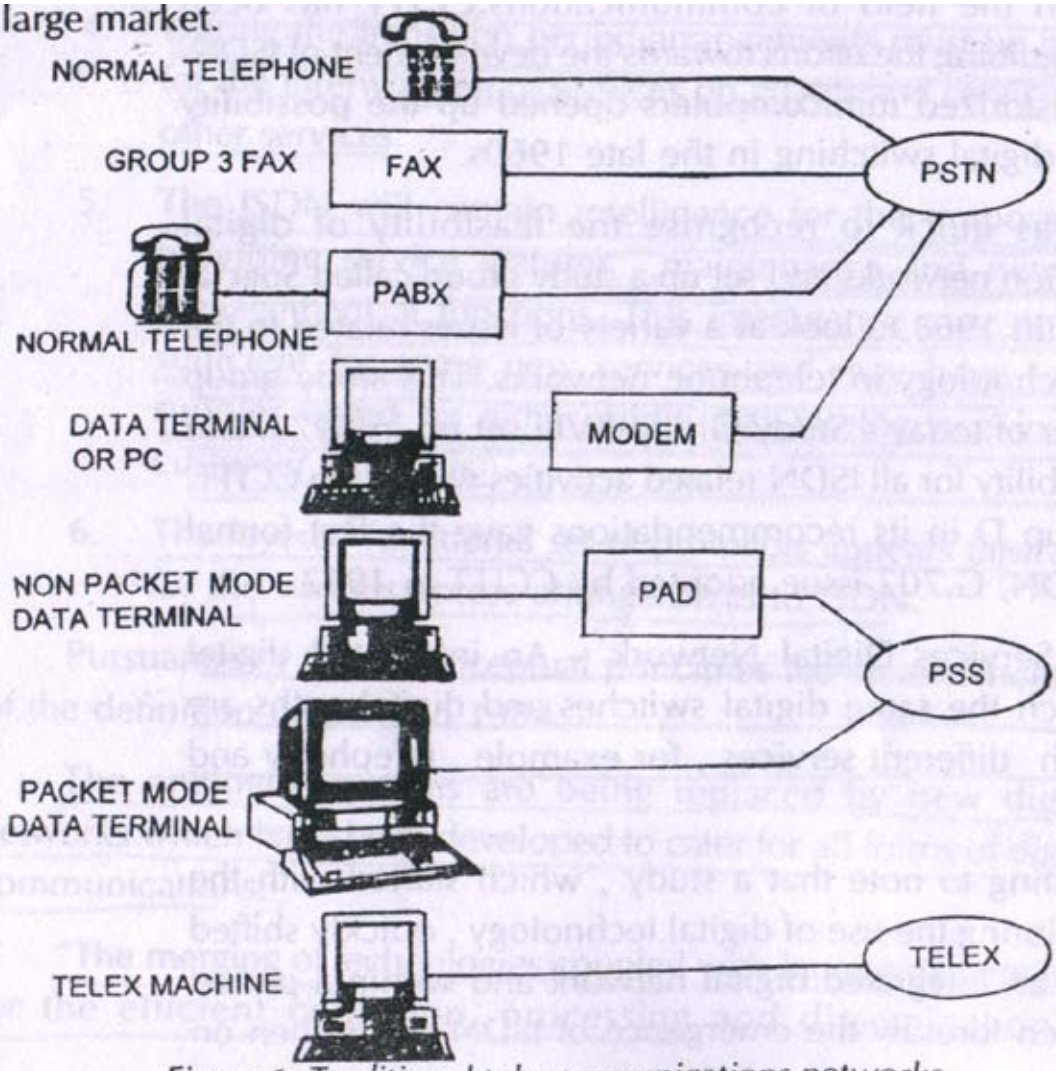


Figure 1. Traditional telecommunications networks

MOTIVATION FOR ISDN

Three factors are responsible for the development towards ISDN:

1. Sociological or societal needs
2. Economic necessities
3. Technological development

Sociological or societal needs:

The rapid developments in various facets of the society call for increasing and complex communication facilities. A biotechnologist today would like to examine a blood example remotely, simultaneously compare the analytical results of other samples stored in a centralized database, consult his assistant who is presently in a laboratory some distance away, and report the finding as the findings as the investigation progresses, to his superior who is in another building. To meet such a demand, we need to electronically transmit the microscopic image of the blood sample and reproduce the same graphically on the computer screen of the biotechnologist, at a rate fast enough to faithfully reproduce the movements of living cell, etc.

As another example, a senior executive of a company, who often has to take important decisions at home or late in the evening or while on a holiday would like to give instant effect to his decisions. This may call for access to different computer systems connected in the form of a network, processing facilities, all in the place where he is at present.

In effect, the society is demanding a telecommunication system that can support universal access to a host of services. In such a system, it should be possible for a user to the network anywhere in the world the equipment of his choice to obtain a particular service. The user will be allotted a permanent identification number or code, like the income tax permanent account number or the social security number, which would be valid for his lifetime.

Traditionally, network providers have put up separate and independent networks to support different services. Telex network data network, telephone network and CATV networks are examples of such a development. Independent networks call for separate administration, maintenance staff, and building for housing switching systems. The independent and duplicate infrastructural facilities lead to high capital cost, low maintenance efficiency and high maintenance cost. In addition, the network facilities are never fully utilized as the services are independently supported on different networks.

Searching for new solutions is of no avail unless technology developments make possible such solutions. In fact, it is the technology factor that brought about the independent network solutions earlier. The end equipment's for different services were analog in nature and had different electrical, electronic, signal and communication characteristics. It was necessary to design different communication characteristics. It was necessary to design different networks to

suit each of these devices. The desire of the network providers to use a common network infrastructure can fructify only if there are uniform for all the services.

Today, the digital technology has matured to a level where all the above - mentioned functions of a telecommunications network can be realized in the digital domain.

Evolution

Integrated Digital Services Network (ISDN) has been perhaps the most important development to emerge in the field of Computer Communications in the 1980's and it will probably continue to dominate the developments in the 1990's too. Unlike many other developments, ISDN is a well conceived and planned area of development in the field of communications. CCITT has been pioneering and guiding the efforts towards the development of ISDN.

CCITT was quick to recognize the feasibility of digital telecommunication networks and set up a study group called Special Study Group D in 1968 to look at a variety of issues related to the use of digital technology in telephone networks. This study group is the forerunner of today's Study Group XVIII set up in 1976, and has the responsibility for all ISDN related activities within the CCITT.

Integrated Services Digital Network – An integrated digital network in which the same digital switches and digital paths are used to establish different services, for example, telephony and data.

In 1980 the first set of ISDN standards emerged which laid down the conceptual principles on which ISDN should be based.

1. ISDN will be based on and will evolve from the telephony IDN by progressively incorporating additional functions and network features including those of any other dedicated networks.

2. New Services introduced into the ISDN should be so arranged and should be compatible with 64 Kbps switched digital connections.

3. The transition from the existing networks to a comprehensive ISDN may require a period of time extending over one or two decades.

4. During the transition period arrangements must be made for the networking of services on ISDNs and services on other services.

5. The ISDN will contain intelligence for the purpose of providing service features, maintenance and network management at functions. This intelligence may not be sufficient for some new services and may have to be supplemented by either additional intelligence in the customer terminals.

6. The layered functional set of protocols appears desirable for the various access arrangements to ISDN.

The analogue systems are being replaced by new digital networks which have been developed to cater for all forms of digital communications.

"The merging of technologies coupled with increasing demands for the efficient collection, processing and dissemination of information is leading to the development of integrated systems that transmit and process all types of information. The ultimate goal of this evolution in communications is called the Integrated Services Digital Network (ISDN). The standard movement was started by the International Telephone and Telegraph Consultative Committee (CCITT).

The ISDN will eventually be a worldwide public telecommunications network which will deliver a wide variety of services. The ISDN will be defined by the standardization of user interfaces, and will be implemented as a network of digital switches and transmission paths which support a broad range of traffic types and provide value added processing services.

Meaning & Definition

In early 1972, two definitions were formulated by CCITT which described the development of an analog into a digital telephone network and its further evolution in to an ISDN.

"An Integrated Digital Network (ISDN) is a network in which connections established by digital switching are used for transmission of digital signals." "An Integrated Digital Network (ISDN) is an integrated Digital Network (IDN) in which the same digital switches and digital switches and digital paths are used to establish connections for different services."

"Integrated Services" refers to ISDN's ability to deliver two simultaneous connections, in any combination of data, voice, video and fax, over a single line. Multiple devices can be attached to the line and send as needed.

"Digital" in ISDN refers to its purely digital transmission, as opposed to the analog transmission of plain old telephone service. ISDN transmits data digitally, resulting in a very clear transmission quality. There is none of the static and noice of analog transmissions that can slow transmission speed.

"Network" refers to the fact that ISDN is not simply a point-to-point solution like a leased line. ISDN networks extend from the local telephone exchange to the remote user and include all of the telecommunications and switching equipment in between. When you have ISDN, you can make connection throughout the world to other ISDN equipment. If your ISDN equipment includes analog capabilities, you can also connect analog.

While ISDN accommodates telephones and fax machines, its most popular advantage is in computer applications. You can plug an ISDN adapter into a phone jack, like you would an analog modem and get a much faster connection with no line noise.

An ISDN is a network, in general evolving from telephony ISDN, which provides end-to-end digital connectivity to support a wide range of services, including voice and non-voice services, to which users have access by a limited set of standard multipurpose user network interfaces.

The key points of the above definition have to be noted.

1. The ISDN is an infrastructure to support a wide variety of services and is not a network designed for any specific service.

2. The end-to-end digital connectivity implies that the digitization process begins right at the user premises.

3. It should be possible to support every conceivable service on ISDN, for any such service is either a voice or non-voice service.
4. A small set of carefully chosen interfaces should enable the support of all possible services. The users of ISDN should not be burdened with too many specialized interfaces, but at the same time, an expensive universal interface should be avoided.

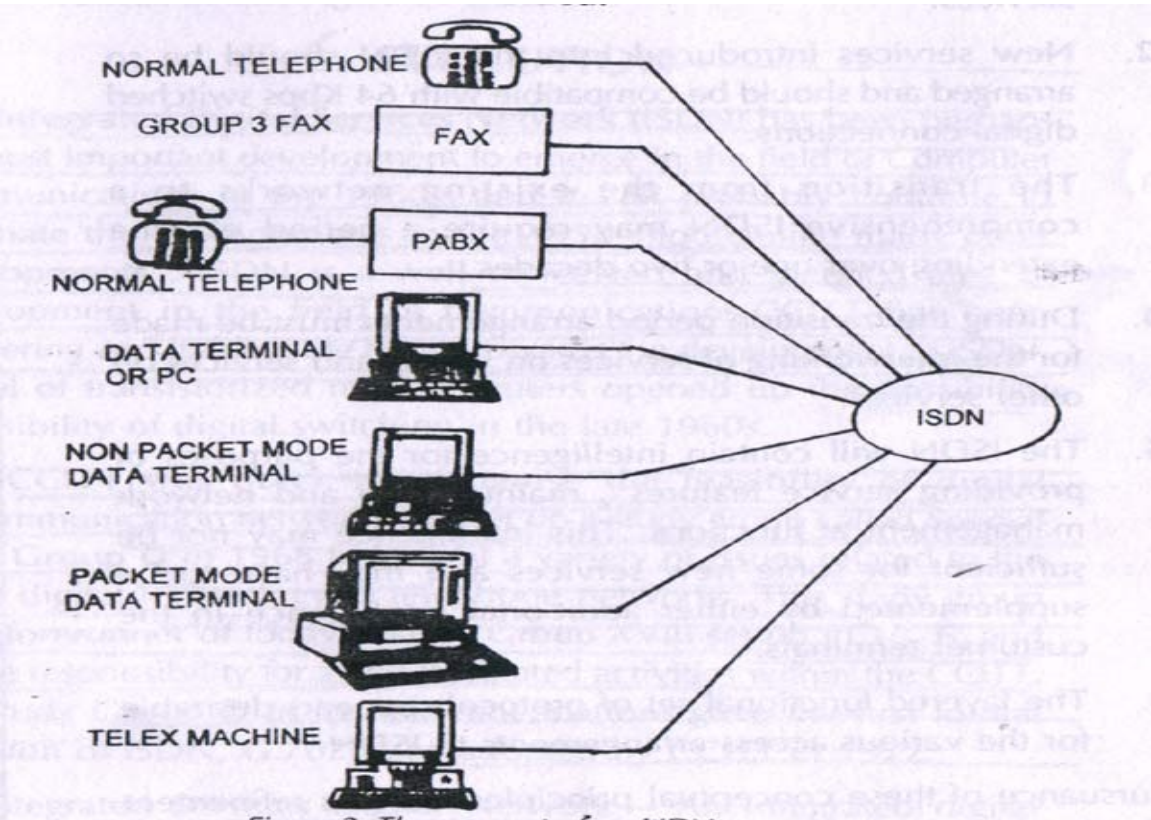
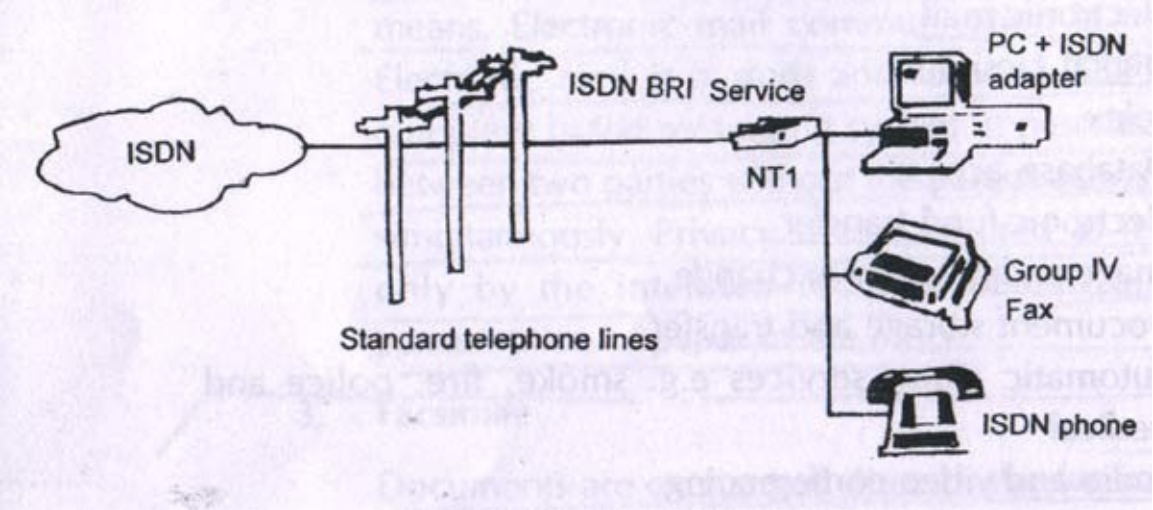


Figure 2. The concept of an ISDN

TYPES OF ISDN SERVICES

Types of ISDN Services:

1. **Basic Rate Interface (BRI):** It provides two single 64 Kbps channels per line. When the two channels are bounded in a single connection, you get a speed of 128 Kbps, which is about four times the actual top speed of the fastest analog modems. Telecommuters, for example, benefit immensely from ISDN, whether you access the corporate LAN in the evenings or maintain a full-time, remote home office; ISDN is the next best solution.



2. **Primary Rate Interface (PRI):** is intended for users with greater capacity requirements. Typically the channel structure is 23 B channels plus one 64 Kbps D channel for a total of 1536 kbps. In Europe, PRI, consists of 30 B channels plus one 64 Kbps D channel for a total of 1984 Kbps.

Services offered by ISDN:

ISND envisaged being an intelligent network. In the future, concepts of artificial intelligence and expert systems will be applied to network functions. In particular, network maintenance and network are the potential areas for the application of AI concepts and expert systems.

Supplementary Services:

Supplementary services call for additional functionalities both in the lower layers and in the upper layers, depending on whether they supplement a basic bearer service or a basic tele-service.

Broadband ISDN:

Is defined as a network capable of supporting data rates greater than the primary rate supported by ISDN. In the context of BISDN, the original ISDN concept is often termed narrow-band ISDN (NISND) The main aim of BISDN is to support video and image services. BISDN services are broadly classified as:

1. Interactive Services
2. Distribution Services

Interactive Services may be classified as:

Conversational Services

Messaging Services

Retrieval Services

Distribution Services are classified as

Broadcast Services

Cyclic Services

a) Conversational Services: It Supports end-to-end information transfer on real time, bi-directional basis. There is a wide range of applications that may be supported using conversational services, the most important one being the video telephony or videophone. Other applications include video conferencing and video surveillance. A number of data oriented conversational applications may also be supported. These include distributed databases, program downloading, inter-process communication and large volume high speed data exchange as encountered in CAD/CAM or graphics based applications.

b) Messaging Services: It Offers store and forward communication. Analogous to X.400 messaging services on NISDN, voice mail, video mail and document mail containing texts, graphics etc. may become the important messaging services on BISDN.

c) Retrieval Services: In BISDN offer the capability to retrieve sound passages, high resolution images, graphics, short video scenes, animated pictures etc. from centralized or distributed databases. BISDN retrieval services are an enhancement of videotext services in NISDN.

d) Broadcast distribution services: It provides support for broadcasting video, facsimile and graphical images to subscribers. For example such applications include television broadcasting over the network and electronic newspaper distribution.

d) Cyclical distribution services: It offers some control to the user in the presentation of information on the screen. The cyclic distribution services are an enhancement of the conventional teletext services.

New Services:

ISDN will support a variety of services including the existing voice and data services and a host of new services. Short list of some of the important new services are:

1. Videotex
2. Electronic mail
3. Digital facsimile
4. Telex
5. Database access
6. Electronic fund transfer
7. Image and graphics exchange
8. Document Storage and transfer
9. Automatic alarm services e.g. smoke, fire, police and medical.
10. Audio and Video conferencing.

A few of the services are described in the following areas:

1. **Videotex:** Is a generic term for systems that provide easy to use, low cost computer based services via communication facilities. Three forms of videotext that exists are:
    - **View Data:** is fully interactive videotext, this means that requests for information or service from a user and performs to send, receive and act by a centralized computer.
    - **Teletex:** It is broadcast or pseudo-interactive videotext service. Teletex users may select the information to be seen, the pace at which the information is to be displayed, and often, the sequence of display. Teletex is one way communication system and there is no real interaction between the user and the computer.
    - **Open channel teletex:** is totally interactive and is a one-way videotext. With this form of videotext, the user receives pre-selected information in a predetermined order.

2. **Electronic mail:** Electronic mail is popularly known as the e-mail and may be defined as the communication of textual messages via electronic means. Electronic mail communication is from user-to-user means. Electronic mail is a store and forward (S&F) service. It is a computer based messaging system. It permits communication between two parties without the parties actually being present simultaneously. Privacy is also ensured as only the intended recipient can open it. Email also reduces the consumption of paper in the office.

3. **Facsimile:** Documents are exchanged through the facsimile systems and it is emerging as a major application of telecommunication systems. It is capable of transmitting and receiving printed matter which may include graphics, drawings, and pictures, hand written text, etc.

4. **Teletex:** It is an upgrade to the conventional telex service. The terminal-to-terminal communication service of telex will be turned into office-to-office document transmission system by teletex. Teletex envisages direct communication between electronic typewriters, word processors and personal computers.

5. **Database access:** A user can by suitable search query, obtain all the information generated in a particular topic. There are over 5000 databases in different parts of the world, covering a wide variety of subjects, which include social sciences, science and technology, engineering and industry. These databases may be accessed online using the telephone network, modem and a personal computer.

How Does ISDN Function?

Signaling: ISDN uses a common channel signaling scheme, the signaling is done over the D channel which acts as the common signaling channel for the B and H channels which carry the user information. D channel may also be used for carrying some user information, if there is spare capacity. In such cases also, the required signaling is done on the D channel. Signaling in ISDN falls into two distinct categories:

1. User level Signaling
2. Network level Signaling

All user generated signaling and the signaling features that are open to the user are treated as user level signaling and are defined as part of the layer 3 user network interface standards. The signaling facilities employed by the network to support user level signaling and to implement network control functions, not directly related to the user are treated as network level signaling.

User level signaling in ISDN permits a user to:

1. Establish, control and terminate circuit switched connections in B channel,
2. Carry out user-to-user signaling and
3. Establish, control and terminate packet switched connections in B or D channels.

User level signaling is of two types:

1. Message based signaling
2. Stimulus signaling

Message based signaling is employed when the user end equipment is an intelligent terminal. In ISDN parlance, as intelligent terminal is known as functional terminal. It provides a user-friendly interface for signaling and performs the functions of forming, sending, receiving and replying messages. The process of establishing, controlling and terminating a call is achieved by exchanging messages between the network and terminal. The messages may be placed under four groups:

1. Call Establishment Messages
2. Call Control Messages
3. Call Discount Messages
4. Miscellaneous Messages

Call establishment group includes set-up, call proceeding, alert, connect and connect acknowledge messages. Alert signal corresponds to ring back signal and is used when a non-automatic answering terminal is used at the receiving end. If the auto-answering facility is available, the terminal responds with connect signal directly and the alert signal is skipped

Call control group includes suspend and resume messages and also user-to-user messages.

Call disconnect group includes disconnect release and release complete messages. The primary function of the miscellaneous messages is to negotiate network facilities to support additional service.

All user level messages have a common message format. There fields are mandatory for all messages:

1. Protocol discriminator
2. Call reference
3. Message type

As the D channel may carry computer and telemetry data etc. in addition to signaling messages, it is necessary to have a mechanism for differentiating packets and their associated

protocols. The protocol discriminator field is provided for this purpose. At present, only two message protocols are supported: the ISDN signaling messages protocol and the level 3-packet protocol. The field has 3 sub-fields: length sub-field, flag and the reference value. The call reference field gives reference to the B, H or D channel information transfer activity to which a signaling packet pertains. Depending on the service and the channel used, the length of the call reference value may vary.

Stimulus signaling is used when the user and equipments are dumb devices with no intelligence, like digital telephone. As the devices do not have functional capabilities, stimulus-signaling messages are generated as a direct result of actions by the terminal user. These signals just indicate events like handset off-hook or depression of a specific push button, which are all due to manual action by the user.

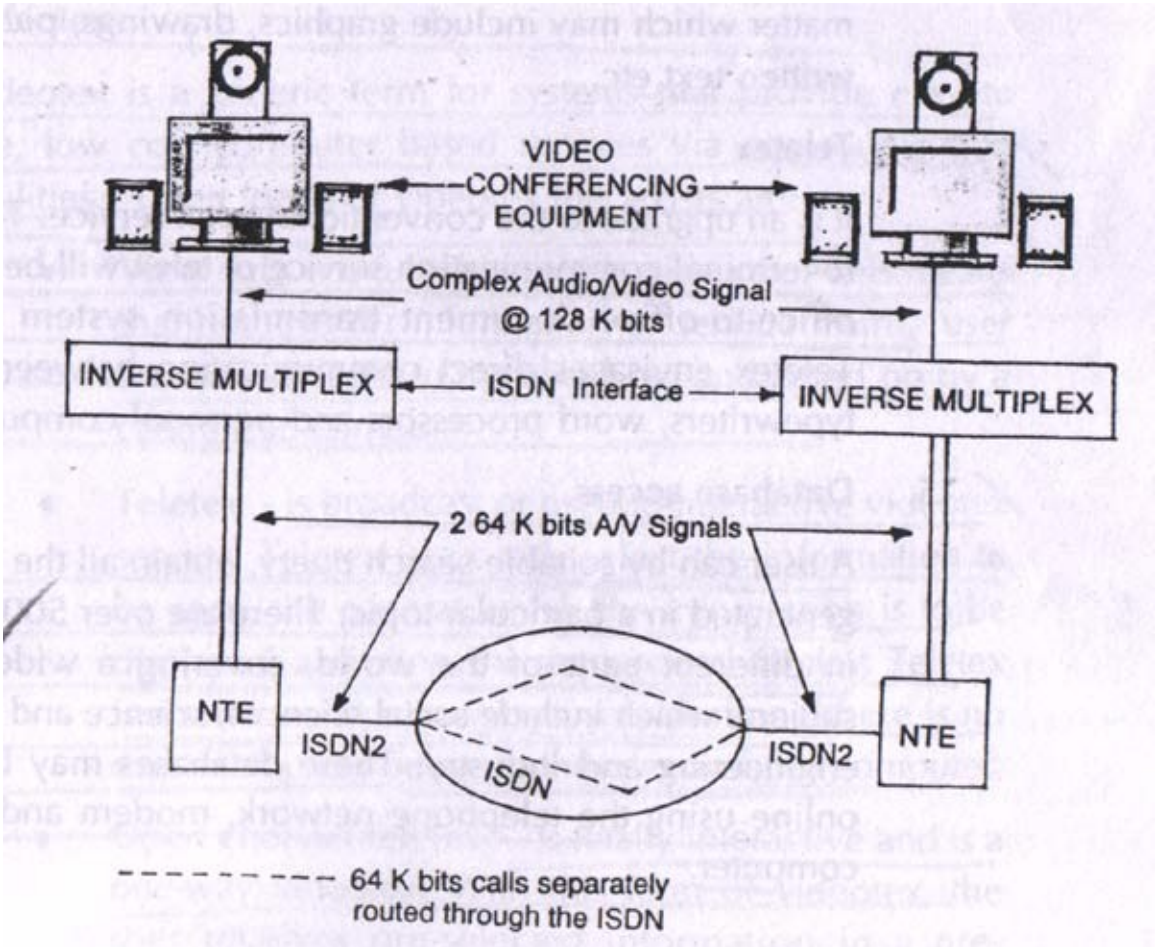


Figure 4

Network Level Signaling:

Network Level signaling in ISDN is concerned with inter-office signaling. Signaling features accessible by the user to obtain enhanced services, from the network and other network related signaling. One of the main aims has been to evolve flexible design for the signaling system to accommodate new services and connection types that may come about in the future to be supported in the future.

About 40 network level messages have been standardized so far and these messages may be placed under 9 broad categories:

1. Forward address
2. General Setup
3. Backward Setup
4. Call supervision
5. Circuit supervision
6. Circuit group supervision
7. In-call modification
8. End-to-end
9. User-to-user

Messages belonging to 1 to 4 categories above are used to support the call setup process initiated by the user and start the accounting and charging functions. Circuit and circuit group supervision messages permit blocking and de-blocking of circuit and circuit groups respectively. Other functions include connection release, temporary suspension and subsequent resumption of circuits.

ISDN Recommendation: It describes a reference model for user-network interfaces to the ISDN. The definitions of equipment in the Reference model are:

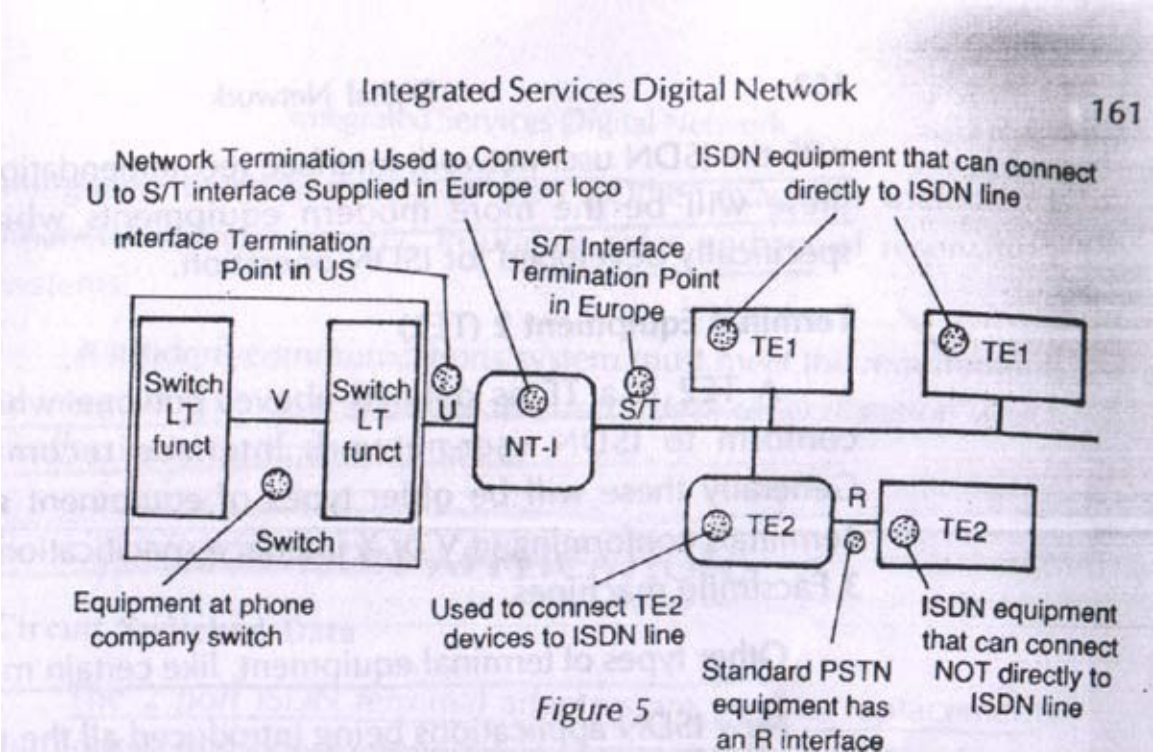


Figure 5

Network Termination 1(NT1): The main function of this equipment is the physical and electrical termination of the transmission line between the local exchange and the customer's premises. Other functions of the NT1 include maintenance and performance monitoring by providing digital loop back facilities, and the ability to feed DC power from the transmission line to other equipment in the installation.

Network Termination 2 (NT2): This may be a PABX, a local area network (LAN) or a terminal controller. The functions associated with an NT2 include protocol handling, multiplexing, switching, concentration and other maintenance functions.

Terminal Equipment (TE): A TE is a user equipment, typically a telephone or data terminal, the functions of which include physical and procedural interfaces and maintenance, as well as the general communications function of the device.

Terminal Equipment 1 (TE1): A TE1 is a TE as defined above, and will be a digital telephone, data terminal, facsimile terminal or other workstation that complies with the ISDN user-network interface recommendations. Generally it covers more modern equipments which have been specially developed for ISDN operation.

Terminal Equipment 2(TE2): A TE2 is a TE as defined above, but does not conform to ISDN user-network interface recommendations. Generally these will be older types of equipment such as data terminals conforming to V or X interface specifications and group 3 facsimile machines.

Other types of terminal equipment, pertaining to certain manufactures.

New ISDN applications being introduced all the time. Typically new applications include LAN bridges and ISDN PC cards to permit PC to PC bulk file transfer. Users of LANs, operating on geographically dispersed sites are now able to transfer data between each other. The transactions being transparent to the users who do not require knowledge of the location or address of the user to whom they wish to communicate.

Transmission Channels: There are 3 types of fundamental channels in ISDN around which the entire information transmission is organized.

1. Basic information Channel
2. Signaling Channel
3. High speed channel

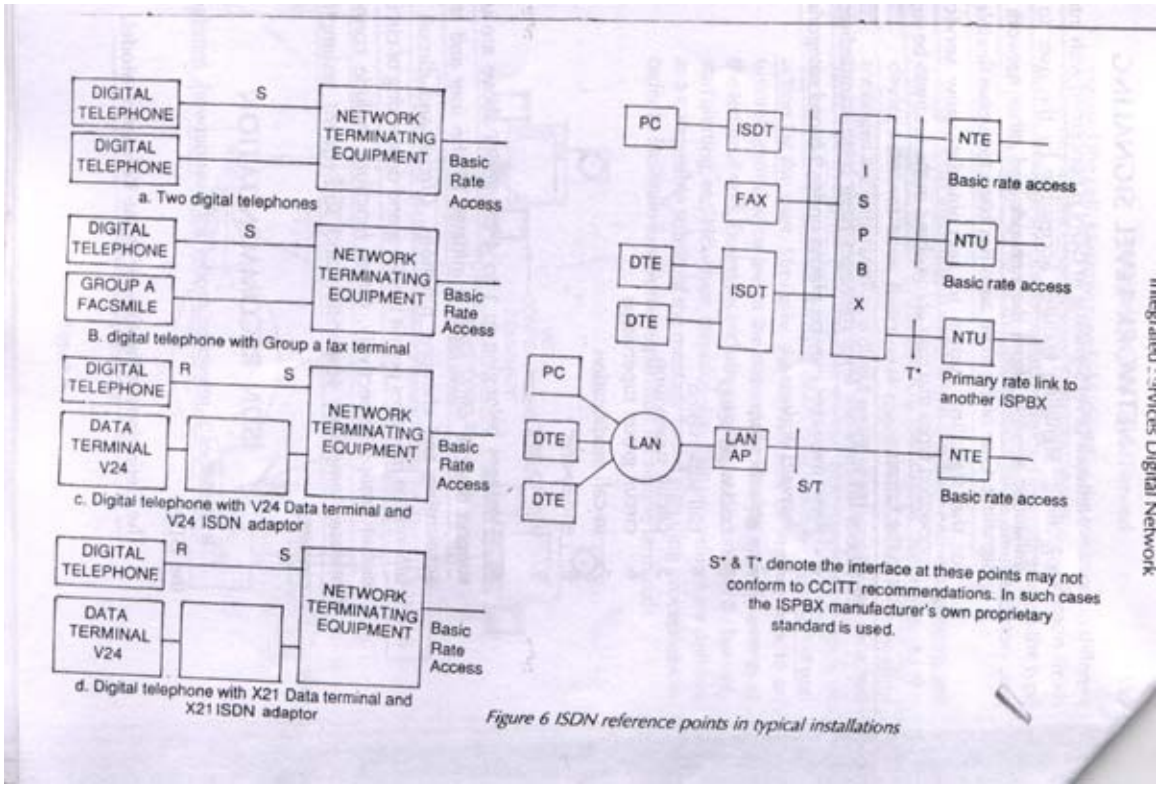


Figure 6 ISDN reference points in typical installations

Video Conferencing: Earlier, in order to achieve acceptable quality for a videoconference, a leased digital link operating at 2Mbit/s was required. Today such quality can be achieved with digital circuits operating at rates as low as 128 Kbits/s. Techniques such as video and speech compression are used to produce a highly complex digital signal in which the bandwidth occupied by the video and audio signals are constantly changing. The added advantage of such an ISDN based VC system is that there is no longer a requirement for a costly permanent leased circuit between sites, video conferences can simply be dialed up when required and are charged on a pay as you go basis.

Encrypted speech: The evolution of ISDN has brought with it the digital telephone. It is now a relatively simple matter to produce a secure speech link between two users, by introducing some form of encryption device between the digital telephone and the B channel over which it is to be connected. D channel signaling messages are not encrypted, as they would then be unreadable by the local exchange.

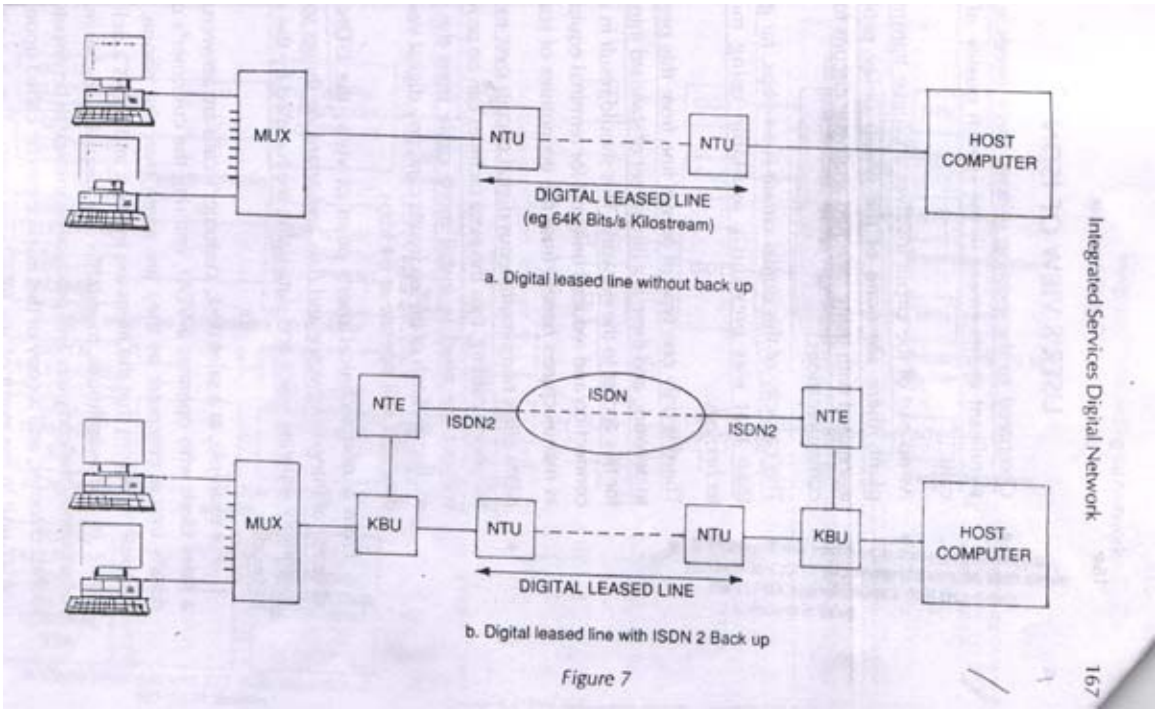


Figure 7

ISDN Standards:

Standardization is an essential process in the introduction of any major and complex international service. The capability of providing true international connectivity and interpretability between networks is critically dependent on the availability of standards and the strict adherence to them. The importance of standards has been well recognized in the context of ISDN from the very early stages. CCITT has been playing a leading role and acting as a coordinating body by issuing ISDN related recommendations and thereby guiding the introduction of ISDN internationally.

The first definition of ISDN appeared in CCITT's recommendations issued in 1972. Subsequent studies led to the emergence of the first ISDN standard in 1980. A CCITT service is said to be completely standardized only when:

1. End-to-end compatibility is guaranteed.
2. Terminals to provide the service is standardized
3. Procedures for obtaining the service are specified
4. Service subscribers are listed in the international directories.
5. Testing and maintenance procedures are standardized and

6. Charging and accounting rules are spelt out.

User Level Interface

Comprehensive user network interface definitions are key to ensuring worldwide ISDN compatibility. Example of an interface standard that serves us so well and yet goes almost unnoticed is the electrical power user interface. We can purchase an electrical appliance almost anywhere in the world and plug it in our house socket. In ISDN, user network interfaces have been given careful consideration to avoid potential inconsistencies that may arise. ISDN caters to a variety of services such as voice, data telemetry and image. In such a situation like this, one encounters conflicting requirements.

On one hand, a number of custom designed interfaces may ideally suit each service but would lead to a proliferation of interfaces.

On the other hand, one single multi-purpose interface may turn out to be overkill for most of the services. Keeping such factors in mind, two information rate access interfaces have been standardized for ISDN.

1. Basic rate access
2. Primary rate access

Numbering & Addressing

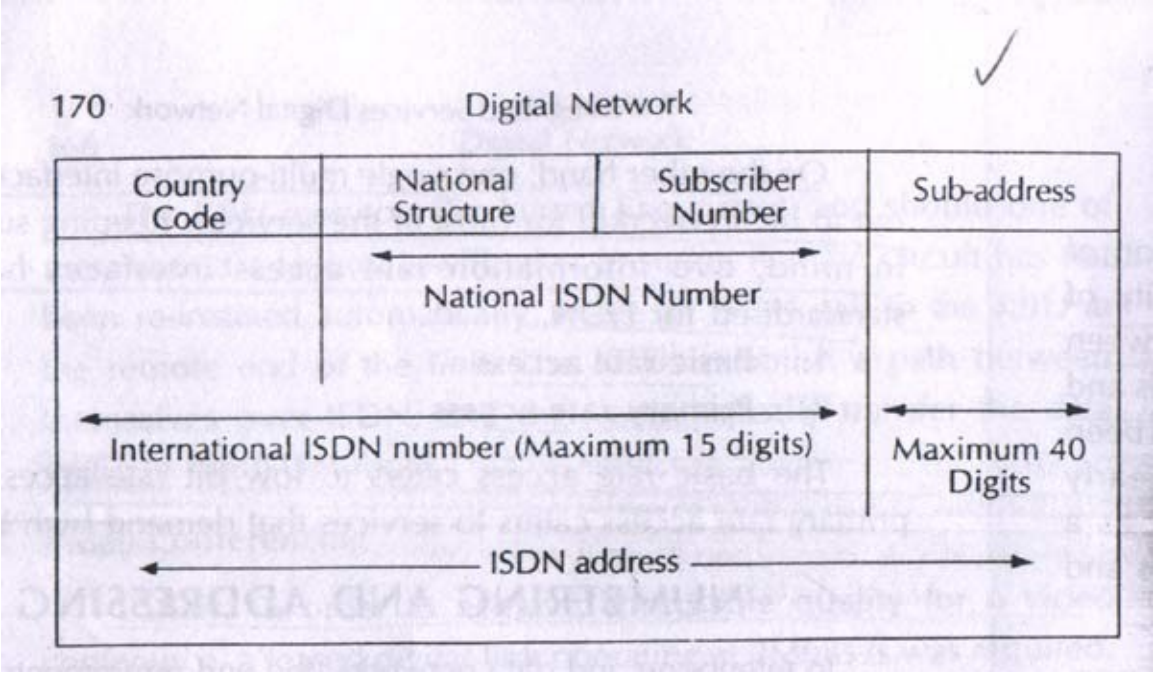
In telephone and data networks, the end \equipments are more often single units than multiple devices units like PABX or LAN. Historically, a telephone, a computer, or a terminal has been the pre-dominant end equipment. The numbering systems for these networks have also evolved to identify single equipment end-points. In ISDN, multiple devices at the end points are more of a norm than single units, in view of the multiple service environments. It then becomes necessary to identify specific end equipment. For example, computer of facsimile to render the service. Identifying this specific equipment is a two-level process; first the end-point is

identified as in the case of telephone or data networks and then the equipment at the end-point. The component of the ISDN addresses which is used to identify the end-point. The component of the ISDN address which is used to identify the end-point is known as the ISDN number.

ISDN services are placed under two broad categories:

1. Bearer Services
2. Tele Services

Both the Bearer and Tele service functionalities may be enhanced by adding to the basic service, the functionalities of what are known as supplementary services. Supplementary services cannot stand-alone and are always offered in conjunction with either a Bearer service or a Tele Service.



Questions

1. What is an Integrated Services digital network? What are the types of ISDN? Explain its functions
2. Explain in brief the ISDN Standards?
3. Explain the Concepts of User Network Interfaces?
4. Bring out the future applications of ISDN?

Chapter 7

STORAGE AREA NETWORKS

- Introduction
- Benefits
- Manageability
- Open Standard Platforms
- Advanced Application Capabilities
- Advanced Storage Management

STORAGE AREA NETWORKS

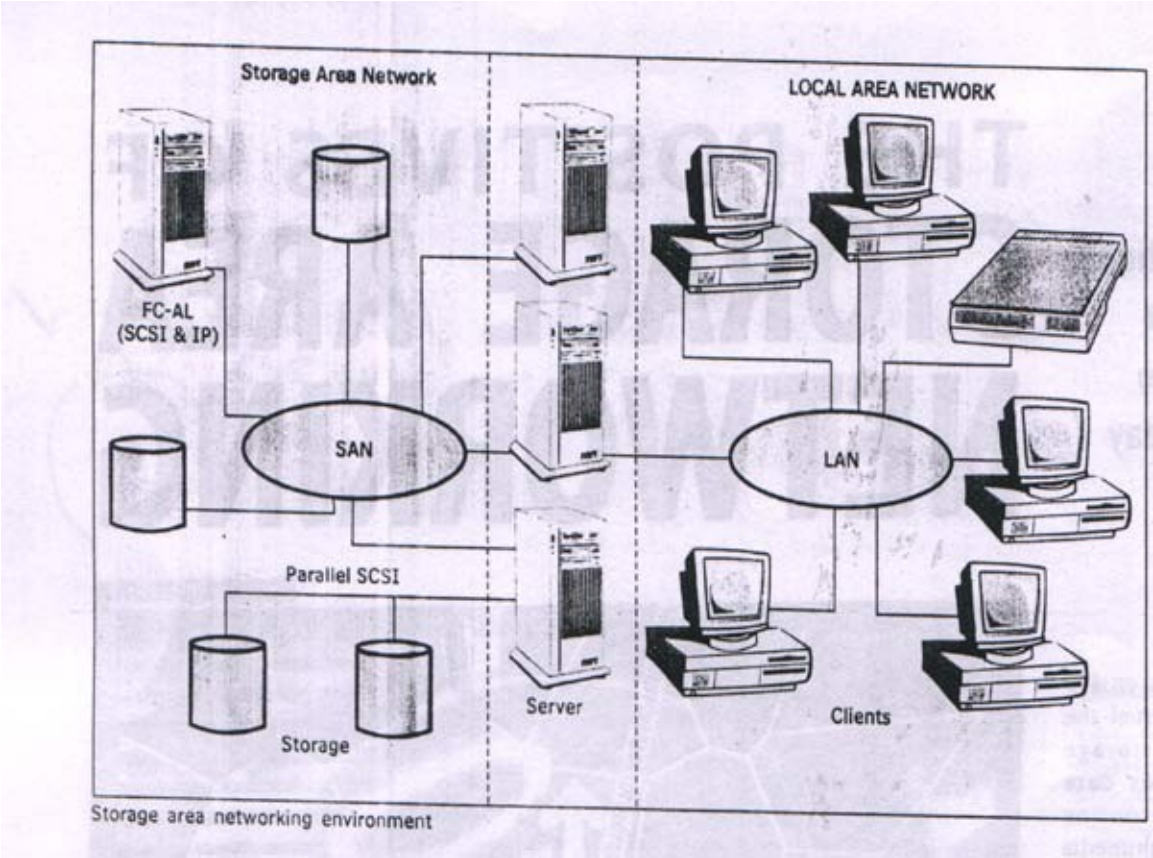
This technology is evolutionary, and the demand for its applications is surging. Storage area networking promises to revolutionize modern day network computing.

From a client network perspective, the SAN environment complements the ongoing advancements in LAN and WAN technologies by extending the benefits of improved performance and capabilities all the way from the client and backbone through to servers and storage.

Rapid growth in data intensive applications continues to fuel the demand for raw data storage capacity. Applications such as data warehousing, data mining, on-line transaction processing, Multimedia, Internet and Intranet browsing have led to a near doubling of the total storage capacity being shipped globally on an annual basis. And analyst predictions that the number of network connections for server-storage subsystems will exceed the number of client connections are further fuelling the demand for network storage.

LIMITATIONS LOOM OVER SURGE OF DATA:

With the rise of client net working, data-centric computing applications and electronic communication applications, virtually all network-stored data has become mission-critical in nature. This increasing reliance on the access to enterprise data is challenging the limitations of traditional server-storage solutions. As a result, the ongoing need to add more storage, serve more users and backup more data has become a monumental task.



Storage area networking environment

Having endured for nearly two decades, the parallel Small Computer System Interface (SCSI) bus that has facilitated server-storage connectivity for Local Area Network (LAN) servers is imposing serve limitation on network storage.

Impending limitations of existing network server connectivity:

- Bandwidth to service clients and maintain data availability.
- Scalability for long term, rapid growth.
- Flexibility to provide optimum balance of server and storage capacity.
- Manageability for ease of installation and maintainability.

The solution: Storage Area Networking.

The Storage Area Network (SAN) is an emerging data communication platform, which interconnects servers and storage at giga baud speeds. By combining LAN networking models with the core building blocks for server performance and mass storage capacity, SAN eliminates the bandwidth bottlenecks and scalability limitations imposed by previous SCSI bus – based architectures.

In addition to the fundamental connectivity benefits of SAN, the new capabilities, facilitated by its networking approach, enhance its value as a long-term infrastructure. These capabilities, which include compute clustering, topological flexibility, fault tolerance, high availability, and remote management, further elevate SAN's ability to address the growing challenges of data-intensive, mission-critical applications. From a client network perspective the SAN environment complements the ongoing advancements in LAN and WAN technologies by extending the benefits of improved performance and capabilities all the way from the client and backbone through to servers and storage.

Benefits of the storage area network environment:

- High bandwidth.
- Modular scalability
- High availability and fault tolerance.
- Manageability.
- Total cost of ownership.

Fibre Channel: the open SAN solution.

Over the past year, Fibre Channel-Arbitrat ed Loop (FC-AL) has emerged as the high-speed, serial technology of choice for server-storage connectivity. Most organizations prefer this solution because of the widely endorsed open standards. This broad acceptance is attributed not only to FC-AL's high bandwidth and high scalability but also to its unique ability to support multiple protocols, such as SCSI and IP, over a single physical connection. This enables the SAN infrastructure to serve as both a server-interconnect and as a direct interface to storage devices and storage arrays.

High Bandwidth

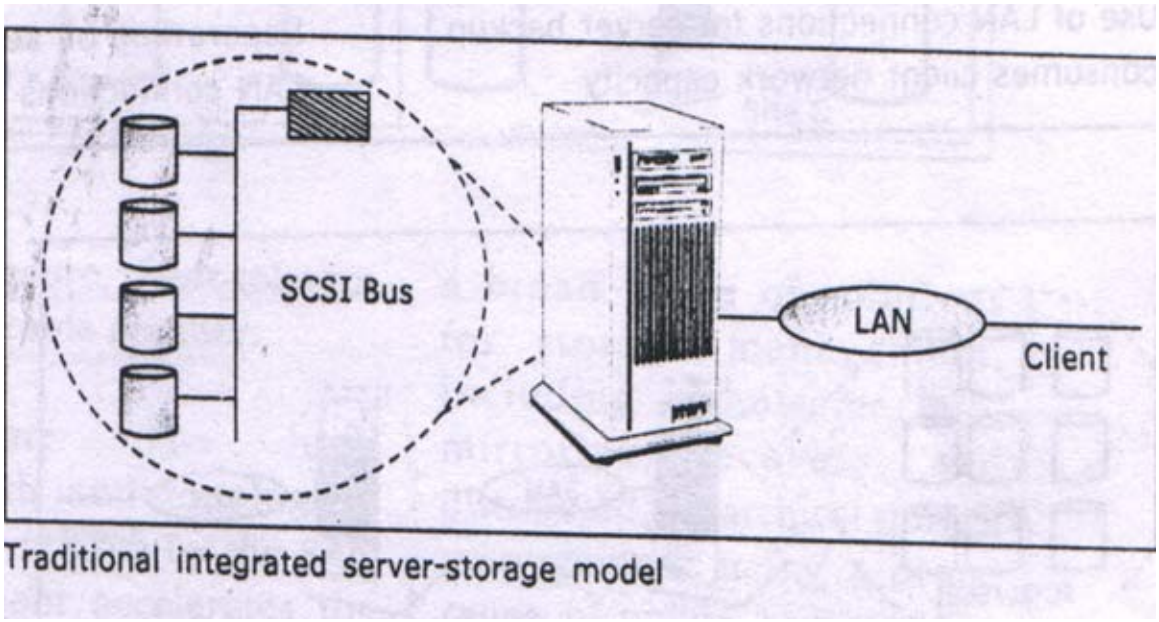
FC-AL provides a 2.5 to 10-fold increase in effective data bandwidth over the traditional parallel SCSI storages interface. Additionally, it offers future expandability. While the current FF-AL standard for bandwidth is 1 giga baud, planned enhancements to 2 and 4 giga baud give FC-AL a solid platform to address longer-term band-width requirements.

SAN vs TCO benefits

San benefits	TCO benefits
Connects the existing LANs	Optimizing the existing investments
Fully managed environment	Minimized support cost
Integrated fault tolerance	Minimized down time
Independently scalable servers and storage	Complements Network Computer (NC) paradigm
	Highly efficient scaling of resources

Server and storage scalability:

The modular scalability of FC-AL is a key to enabling an infrastructure for long-term growth and manageability. Traditional parallel SCSI bus connections have been limited to a total of 7 or 15 storage devices. AS bus bandwidth is pushed further and further this limit is compressed to ever fewer devices per bus. In contrast, FC-AL supports up to 126 nodes per loop with a typical configuration consisting of a combination of servers and multi-disk arrays per node.



Traditional integrated server-storage model

Scalability in terms of capacity management and capacity balancing is an area of significant differentiation between FC-AL and SCSI. Largely dictated by the limits on physical cable length, parallel SCSI storage connectivity requires close proximity to its host system, typically a server. This translates to a single, integrated server-storage enclosure that contains both server processing power and one or two SCSI buses of limited scalability.

Inter-dependent capacity scaling with integrated server-storage model

Under this single server-storage enclosure model, the scaling of server capacity and storage capacity becomes inflexible and inefficient. Single enclosures typically hold only 4-10 drives. In order to scale the storage capacity beyond this limit, additional server-storage enclosures, including the cost of the server processor board and peripherals is required. With a diverse combination of data-intensive applications and server processing-intensive applications running concurrently in the enterprise, the need for more flexible and efficient scaling is needed.

With less stringent cable length limitations, FC-AL enables the networking of separate server and storage enclosures within the SAN environment.

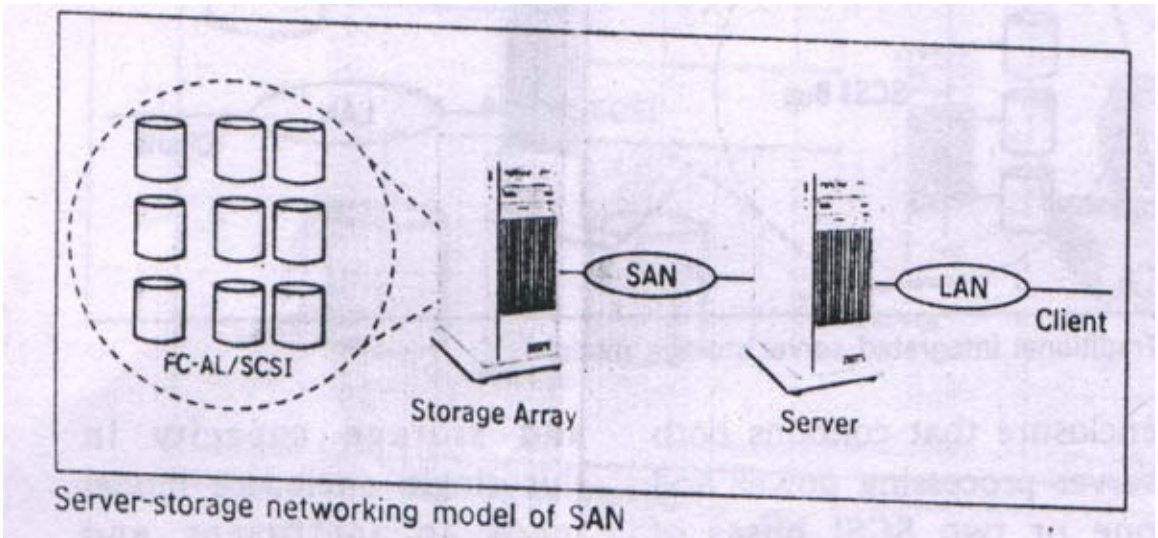
This capability provides a more flexible and cost-effective path for the independent scaling of server performance and storage capacity, where either may be expanded independently to achieve an optimum balance.

Modular connectivity

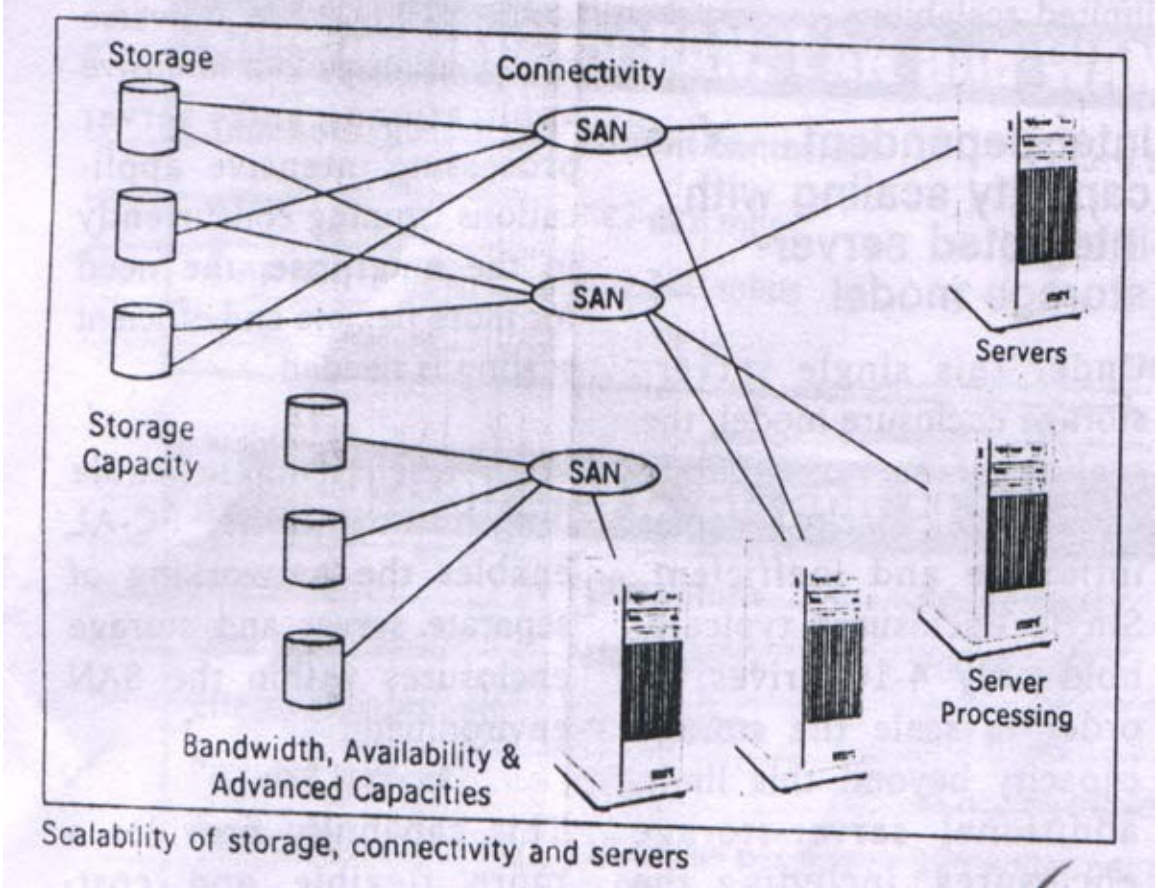
In addition to superior flexibility in scaling server processing capacity and data storage capacity, the networking approach of FC-AL introduces aspects of interconnect scalability that have not been possible with previous architectures. Through the use of modular networking devices such as hubs, switches, bridges and routers, advanced SAN topologies can be created to scale overall bandwidth, enhance availability, enable advanced SAN application capability, and enable advanced SAN application capabilities in storage management and load balancing.

Advanced storage management

Storage management challenge	**SAN solution**
Length of time required to backup data	Bandwidth and protocol efficiency accelerate backup
Inability to backup, mirror or restore remotely	Cable length up to 10 km support remote operation.
Lack of alternatives to local backup and mirroring.	Ideal platform for distributed hierarchical storage management.
Use of LAN connections for server backup consumes client network capacity	Separation of server-storage connections from LAN connections reduces LAN traffic.



Server-storage networking model of SAN



Scalability of storage, connectivity and servers

High availability and fault tolerance.

Many FC-AL devices provide features that ease the general deployment of fault-tolerant SANs. One example of these on board capabilities is the feature of dual porting, which has become standard on FC-AL disk drives, to facilitate dual loop configurations. These dual loops

provide a redundant path to each storage device in the array in case one of the loops is down or is busy.

Dual loop array configuration.

The implementation of Redundant Array of Independent Disks (RAID) configuration is storage arrays and has become a standard approach for fault tolerance and is fully supported by the SAN environment. In fact, to even further embrace the RAID approach, FC-AL disk drives provide internal exclusive-or (XOR) logic, which effectively provides Level 5 RAID capabilities from within the disk drive itself.

Manageability

Visibility down to the node and device level is essential to case the efforts of installation, deployment and maintenance of any network. By embracing a network management approach, SAN connectivity devices, such as hubs and switches, have integrated highly evolved management capabilities modeled after proven LAN and WAN management techniques. A fully managed SAN platform can offer monitoring and bypass control of individual nodes, loops, enclosures, storage devices, and connectivity devices.

Open standards platforms for SAN management.

- SCSI command set.
- SCSI Enclosure Services (SES)
- SCSI Self Monitoring Analysis and Reporting Technology (S.M.A.R.T)
- SAF-TE(SCSI Accessed Fault-Tolerant Enclosures)
- Simple Network Management Protocol (SNMP)
- Web-Based Enterprise Management (WBEM).

By embracing the best-practice network management standards established by LAN and WAN platforms, information regarding SAN topology, status and alerts can be easily be accessed by system administrators. It can also simplify remote system recovery and restoration in the event of a failure. Traffic monitoring capabilities can also be embedded into the SAN

management system to facilitate sophisticated, cost-effective load balancing and capacity planning.

Ease of integration.

With advance capabilities of networked servers and storage, the ability to integrate SAN solutions into an existing network provides tremendous value in ease-of integration.

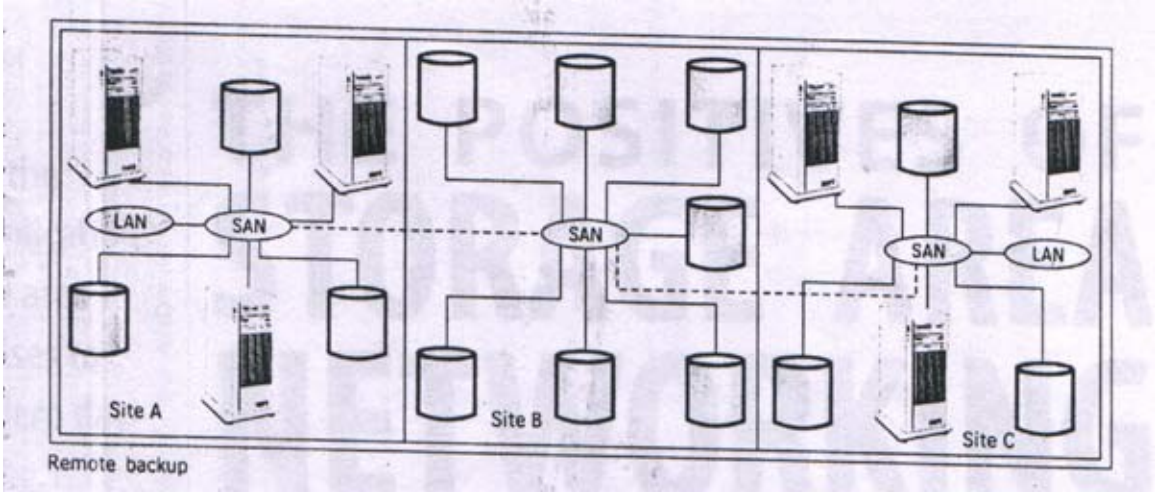
Since the SAN environment exists behind the server, existing server-LAN connections can easily be leveraged to facilitate a gateway between LAN and SAN, and allow the utilization of legacy servers. The broad cabling options supported by FC-AL also ease the introduction of SAN s into existing campus networks. SAN connection distances up to 10km can be achieved without the need to pull new cable. As a key building block of SAN deployment, SAN connectivity devices offer dynamically configurable, hot – plugging capabilities. Combined with a graphical management interface, these features simplify troubleshooting and accelerate installation.

Total Cost of Ownership

Offering an infrastructure for cost-effective, long-term growth, fault tolerance and manageability, the SAN environment provides Total Cost Of Ownership (TCO) advantages, which have never before been possible with servers ,storage or server storage connectivity.

Advanced application capabilities

By introducing the network like features of extended connection distance, IP support, and use of hubs, bridges switches and routers for complex topologies , the SAN infrastructure enables a broad range of new capabilities include: advanced storage management and server storage clustering.



Advanced storage management

Problem: Increasing amounts of network-storage data have become cumbersome, if not impossible, to maintain in a timely, secure, fault-tolerant and restorable manner.

Solution: The high bandwidth and topological flexibility offered by the SAN environment accelerates the data backup process and facilities new, innovative platforms for remote backup, mirroring and hierarchical storage. Perhaps the biggest challenge facing storage management is the need to provide efficient, secure, high availability access to critical data. To efficiently overcome these challenges, a number of fundamental issues must be addressed:

The bandwidth and connectivity limitations imposed by server-to-storage parallel SCSI connections and server-LAN connections offer little to address these formidable tasks. Through its bandwidth, extended connectivity and transport efficiency, the SAN environment uniquely offers a broad range of solutions for storage management, including remote backup, mirroring, recovery and distributed hierarchical storage management using a broad range of online and near-line storage devices.

With the increasing complexity of networked computing systems and global enterprise solutions it is refreshing when a single technology yields both unmatched performance and exceptional Total Cost of Ownership benefits. In the case of Fibre Channel Arbitrated loop and the rapidly developing Storage Area Network, an evolutionary open technology promises to

revolutionize the network centric, data- intensive computing era through a new, innovative market space.

Questions

1. What is Storage Area Network? What are its benefits?
2. What do you mean by Open Standard Platforms?
3. Bring out the advanced application capabilities of SAN?
4. What is advanced Storage Management?

Chapter 8

CURRENT TRENDS IN COMPUTER NETWORK

BLUE TOOTH TECHNOLOGY

- Introduction
- Bluetooth History
- System Challenges
- Bluetooth Security
- The Basic Structure
- Bluetooth for Embedded Internet
- The Need for Bluetooth

Introduction to Bluetooth

Bluetooth is the radio technology that allows devices within 30 feet of each other to communicate without wires. The Bluetooth technology eliminates the need for numerous and inconvenient cable attachments for connecting computers, mobile phones, mobile computers and handheld devices. All the things that can be connected by cable now can be connected without it using Bluetooth technology.

Bluetooth is not a new wireless LAN; it is something much simpler, more powerful and is a cable replacement. It is a 'radio block' that enables devices to talk to each other. It replaces the cables that traditionally join pieces or equipment together. It makes them accessible behind walls and has capability of connecting multiple units

Bluetooth is the name given to a new technology standard using short-range radio links, intended to replace the cable(s) connecting portable and/or fixed electronic devices. The standard defines a uniform structure for a wide range of devices to communicate with each other, with minimal user effort. Its key features are robustness, low complexity, low power and

low cost. The technology also offers wireless access to LANs, PSTN, the mobile phone network and the internet for a host of home appliances and portable handheld interfaces (Fig. 1).

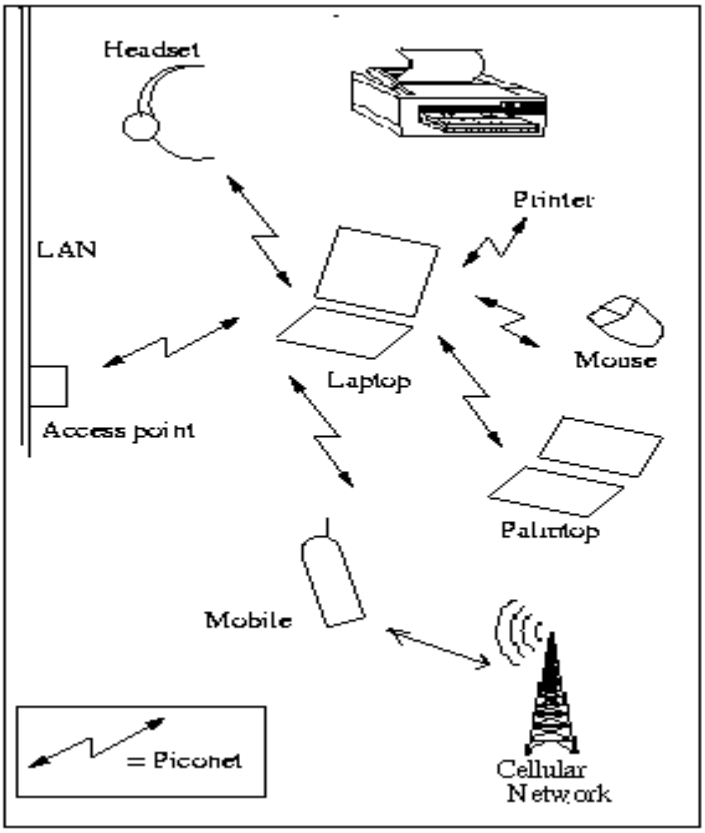


Figure 1:

Wireless connectivity over Bluetooth.

Bluetooth enabled electronic devices connect and communicate wirelessly via short-range, ad hoc networks called piconets. Each unit can simultaneously communicate with up to seven other units per piconet. Moreover, each unit can simultaneously belong to several Pico nets. These piconets are established dynamically and automatically as Bluetooth devices enter and leave the radio proximity.

Bluetooth is further fueled by the demand for mobile and wireless access to LANs, internet over mobile and other existing networks, where the backbone is wired but the interface is free to move. This not only makes the network easier to use but also extends its reach. The advantages and rapid proliferation of LANs suggest that setting up personal area networks, that is, connections among devices in the proximity of the user, will have many beneficial uses. Bluetooth could also be used in home networking applications. With increasing numbers of

homes having multiple PCs, the need for networks that are simple to install and maintain, is growing. There is also the commercial need to provide "information push" capabilities, which is important for handhelds and other such mobile devices and this has been partially incorporated in Bluetooth. Bluetooth's main strength is its ability to simultaneously handle both data and voice transmissions, allowing such innovative solutions as a mobile hands-free headset for voice calls, print to fax capability, and automatically synchronizing PDA, laptop, and cell phone address book applications.

Bluetooth History

Bluetooth was invented in 1994 by L. M. Ericsson of Sweden. The standard is named after Harald Blaatand "Bluetooth" II, king of Denmark 940-981A.D. A runic stone has been erected in his capitol city Jelling (Jutland) that depicts the chivalry of Harald and the "runes" say:

1. Harald christenized the Danes.
2. Harald controlled Denmark and Norway.
3. Harald thinks notebooks and cellular phones should seamlessly communicate.

The Bluetooth Special Interest Group (SIG) was founded by Ericsson, IBM, Intel, Nokia and Toshiba in February 1998, to develop an open specification for short-range wireless connectivity. The group is now promoted by 3COM, Microsoft, Lucent and Motorola also. More than 1900 companies have joined the SIG.

The following section describes some of the requirements from the Bluetooth system and in essence, suggests the functionalities planned for it.

System Challenges

The Bluetooth system is now recognized more than just a cable replacement technology. Various innovative usage models have opened up new areas where Bluetooth can be used.

- The most important requirement from the wireless link is that there should be a universal framework that offers means to access information across a diverse set of devices
- In the practical scenario all devices are not expected to be capable of all functionalities and users too may expect their familiar devices to perform their basic functions in the usual way. So Bluetooth must offer the facility for collaboration between devices, in the proximity of one another, where every device provides its inherent function based on its form.

- The standard must enable the devices to establish ad hoc connections. Also, introduced is the unconscious connectivity" paradigm, where devices can connect to those in proximity almost without any user command or interaction.
- Support for both data and voice is expected as these are two most important kinds of information being transmitted over networks today.
- The standard should be able to incorporate new usage models without requiring any registration of the new service with a central authority.
- The communications should offer similar protection as in cables. There should not be any compromises on security in switching over to wireless.
- The implementations of the standard should be simple, small and power efficient for easy mobile usage.
- It is necessary for the rapid deployment of the system and for the Bluetooth benefits to actually reach the users that a large number of devices be enabled with the Bluetooth standard. The devices to be enabled comprise a highly no uniform set and no single company can have the expertise to manufacture all these.

Connection Establishment in Bluetooth

1. **Inquiry:** The device on reaching a new environment would automatically initiated an inquiry to find out what access points are within its range. This will result in the following events:
    a. All nearby access points respond with their addresses.
    b. The device picks one out of the responding devices.
2. **Paging:** The device will invoke a baseband procedure called paging. This result in synchronization of the device with the access point, in terms of its clock offset and phase in the frequency hop.
3. **Link establishment:** The LMP will now establish a link with the access point. As the application in this case is email, an ACL link will be used. Various setup steps will be carried out as described below.
4. **Service Discovery:** The LMP will use the SDP(Service Discovery Protocol) to discover what services are available from the access point, in particular whether email access or access to the relevant host is possible from this access point or not.

5. **L2CAP channel:** With information obtained from SDP, the device will create an L2CAP channel to the access point. This may be directly used by the application or another protocol like RFCOMM.
6. **RFCOMM channel:** Depending on the need of the email application an RFCOMM or other channel will be created over the L2CAP channel.
7. **Security:** If the access point restricts its access to a particular set of users or otherwise offers secure mode communications to people having some prior registration with it, then at this stage, the access point will send a security request for "pairing". This will be successful if the user knows the correct PIN code to access the service.
8. **PPP:** Assuming that a PPP link is used over serial modem as in dial up networking, the same application will now be able to run PPP over RFCOMM.
9. **Network Protocols:** The network protocols like TCP/IP, IPX, and AppleTalk can now send and receive data over the link.

Bluetooth Security

The Bluetooth system is intended to be used as a uniform interface to all of a person's information sources and will thus be expected to transfer sensitive personal data. Security of the data is thus understandably an important issue. Further, Bluetooth devices are expected to be omnipresent and at some places the access to these devices by public users may have to be restricted. This calls for authentication procedures to be provided. As the channel used is wireless and the packets being transmitted are available to all members of a piconet, the security initialization communications should not send any information that can allow an unauthorized device to know the secret authentication keys.

The application may itself encrypt its data for added security. That can add to the safety of the data, but the most of the authentication is based on the link level security procedures.

The basic structure

The procedures for security use four values: the device address (which is public), a private authentication key (128 bits), private encryption key (8-128 bits, configurable) and a random number. As the keys have to be secret, they cannot be obtained by inquiry. The exchange procedures will be described below. The security procedure requires a secret PIN to be known to the user.

1. An initialization key is generated using the PIN, the length of the PIN, a random number and the device address. The dependence on the device address makes it more difficult for a fraudulent device to try a large number of PINs as each has now to be tried with different device addresses.
2. An authentication procedure is carried out using the challenge response scheme. The verifier unit sends a random number generated by a specific process for the authentication. This random number is such that a claimant device which has the correct initialization key.
3. The claimant may also carry out verification on the verifier using a similar procedure as above.
4. Each Bluetooth unit has a unit key, installed in its non volatile memory. The device now uses the initialization key to encrypt this unit key and sends it to the other device.
5. The second device may add its own unit key to the unit key of the first device and generate a combination link key if both the devices are capable of handling this.

An encryption key is now generated from the link key, a random number and another number obtained from a fixed procedure. Both the devices can generate this encryption key as all the required information is known to both devices.

Bluetooth for Embedded Internet

98% of the computing devices (microprocessors and microcontrollers) sold today are embedded products and only the remaining small fraction consists of general purpose microprocessors used in PCs or workstations. Not just electronic equipment like video players, music systems or telephones but even mundane consumer goods like washing machines, dishwashers, ovens and toasters now have an embedded processor sitting behind the control panel.

This revolution has come about due to the ever increasing number of transistors being packed into a smaller and smaller area of silicon enabling high computational powers to be provided at very low cost. Combine this with the increasing proliferation of wired and wireless networking which has completely transformed the way information flows around us.

The convergence of the above two technologies is leading to what is called the "embedded internet"- the immense new value that is emerging by connecting these computational components. The internet will not be restricted to being a newtork of PCs and the like, but will now include all intelligent devices located in the human environment.

How far is it?

Cheap microcontrollers today are just capable of supporting an embedded operating system, the TCP/IP stack and run a Web server based on the omnipresent HTTP. Examples of thin servers abound a notable one being the Fairchild ACE1101MT8 processor supported fingernail sized web server. What is now needed is for this devices to support server side programming or client server computational models that can enable these devices to process exchanged data. Themost obvious mechanisms for this are the cgi interface and Java applets. Thin servers can almost run cgi and Embedded Java is being developed too. JINI is another service that is being developed for similar applications.

Computation power alone is not sufficient to create real world utility. The processing has to be on physical data and the output has to be used by physical devices. This requires sensors to pick up information and actuators to bring about the desired changes. Various efforts are on this direction. MEMS or Micro electromechanical systems are a hot area of research and are soon expected to provide us usable and cost effective sensors and actuators which can be deployed rapidly for the purpose.

The GPS (Global Positioning System) can now be accessed from extremely small devices, like those built into watches or PDAs. Passive or battery-less electronic tags have been successfully used and are already in commercial use, for instance at music stores to prevent theft.

The Need for Bluetooth.

Wireless is important for the embedded devices to become really ubiquitous. This throws up certain issues like low power consumption, connections without user interaction, ability to route data on an ad hoc basis and their related addressing issues. Data security and access control can not also be neglected

With its extensive support for integration with existing protocols and APIs, Bluetooth seems to be the major contender among other such wireless solutions for the physical layer connectivity. The embedded internet based on Bluetooth seems all set to revolutionalize our living and work environments today.

WIRELESS APPLICATION PROTOCOL

WAP stands for Wireless Application Protocol. The popularity of digital wireless user - agents has been staggering growth in recent years with a massive global increase in the use of mobile phones. The addition of further capabilities mans that the mobile phone is no longer merely a telephone but a communication device capable of running applications and communicating with other devices and applications over a Wireless Network. WAP is the development of established internet protocols and concepts intended to standardize the way in which pages, mobile phones, and personal digital assistants access information and services.

Limitations of WAP

There are some limitations to WAP devices and the main aspects being:-

1. Small display monitor
2. Limited processing power and memory
3. Limited battery life and power
4. Limited data input and users interaction capabilities
5. Limited bandwidth and connection speeds.
6. Frequent unstable connections

WAP Forum:

A forum was formed in 1997 by the leading mobile phone manufactures like Ericsson, Motorola, Nokia and Phone.com and is called the WAP forum. Within two years, more than 100 companies joined the group to define the standards for providing internet content and services to wireless devices. WAP is actually not a single protocol; rather, is a collection of protocols and standards that make up a complete lightweight protocol stack along with special markup and scripting languages, which together define a complete solution

Devices used in WAP

Some of the WAP devices are hand-held-digital-wireless devices such as mobile phones, pagers, two-way radios, smart phones, and communicators-from low-end to high-end. The Base Station Switching Center is the control element for the base transmitter stations, but need not be co-located with the BTS. Thus in a dense metropolitan area, several antenna sites may be used, but they require only one small BSC switching site. Whenever the mobile handset is switching on and at regular intervals thereafter, it uses the control channel to register it's presence to the

nearest mobile switching center. The mobile switching centers are the main controlling elements of the networks. Each control has a given geographic area over which a number of BTS are spread. The information is held by the home MSCs in a database called the Home Location Register or HLR. The local MSCs duplicates some of this information in a temporary visitor location Register or VLR, until the caller leaves the MSCs are. The telephone networks are circuit switched networks.

OS compatible with WAP

WAP is designed work with almost all wireless networks and application environments. It can be built on any operating System including Windows, OS/9, Java OS, etc. It provides service interoperability even between different device families.

WAP Browsers

It runs on the WAP device and displays the contents it receives. It also provides the front-end, through which the user can navigate the WAP application. The browser may be built into the phone or mobile device, or into the SIM card, the device contains. Some of the WAP browsers currently available are given in the box

How the WAP protocol Works?

A simple WAP application consists of files, located on a web server, written in Wireless Markup Language (WML) and possibly script files written in WML script and graphics files in WML Bitmap format. The WAP follows the steps mentioned below:-

1. The User presses a phone key that has a URL assigned to it.
2. The phone sends a URL request to a WAP gateway using the WAP protocol
3. The gateway creates a conventional HTTP request for the specified URL and sends it to the WEB server.
4. The HTTP request is processed by the server. The URL may refer to a static WAP file or may use a CGI script to create the WAP content. The server will fetch the file and add an HTTP header to it, or if the URL specifies a script application, the server will run the script.

5. The web server returns the WML content with the added HTTP header.
6. The WAP gateway verifies the HTTP header, and the WML content, then encodes them into binary form. The gateway then creates a WAP response containing WML and sends it to the phone.
7. The Phone receives the WAP response and processes the WML to display the appropriate content.

WAP Summary:

1. WAP does for wireless devices that HTTP does for web browsers - it allows them to become clients in an Internet-based client/server world.
2. WAP is a protocol, a data transport mechanism. In many ways it is similar to HTTP and WAP was also built on top of established standards, such as IP, URLs, and XML.
3. WAP is not a single protocol; rather, it is a collection of protocols and standards that make up a complete lightweight protocol stack along with special markup and scripting languages which together define a complete solution.
4. WAP forum is the industry association comprising of hundreds of members that have developed the de facto world standard for wireless information and telephony services on digital mobile phones and other wireless terminals.
5. WAP devices: Handheld digital wireless devices such as mobile phones, pagers, two-way radios, smart phones, and communicators - from low / end to high / end.
6. The WAP browsers run on the WAP device and display the contents it receives. It also provides the front-end, through which the user can navigate the WAP application. The browser may be built into the phone of mobile device, or into the SIM card.

Introduction to WML

In June 1997, phone.com originally known as unwired planet along with Nokia, Motorola and Ericsson launched the WAP forum - a nonprofit organization dedicated to the development and proliferation of a single standard protocol for wireless application. Using phone.com's HDML (Handheld device markup language) as the basis for its own standard markup language, the Forum created and distributed WML - a language different form, but in many respects similar to HDML. WML is a markup language used for describing the structure of documents to be delivered to wireless devices. WML is to wireless browsers as HTML is to a browser on a desktop computer. WML was created to address the display bandwidth and memory limitations of mobile and wireless devices such as cellular phones and wireless handheld computers. Since WML uses an XML vocabulary, it could be useful to understand some basic principles of XML (Extensible Markup Language), a tag-based system used for defining, validating and sharing document formats. Although they are very similar, WML differs from XML in the following ways:

1. WML's white-space handling rules are not as elaborate as XML's.
2. WML relies on well-formed expressions.
3. WML has a built-in method for handling international characters.

Security in WAP

Security in WAP has been implemented in such a way to provide maximum benefits with little or no hassles. Security on the internet is provided at a number of levels through the involvement of various protocols, the most common of which is the Transport Layer Security Protocol TLS formerly known as secure socket Layer (SSL). WAP implements most of its security in wireless transport layer security protocol, based on TLS with subtle differences. WTLS is capable of running over Wireless Data-gram protocol or User Data-gram Protocol.

WAP & Internet:

Let us view how WAP differs from internet. In this model, connection is established with the WAP gateway through the network operator rather than through the ISP. The phone call is routed through the network operator’s modem to a Remote Access Server (RAS). There is also a level encryption. The RAS server also performs authentication and routes the data to a WAP gateway. This is not the feature in the regular process of internet communication, The WAP

gateway then converts the WML script to and from the binary format that is transmitted over the air and passes on the data to the web server using HTTP protocol. The WAP forum defined a new protocol WTLS that is based on TLS and provides a similar level of security. WAP utilizes a security certificate in order to present the public/private key pair generated once for the client to the WAP gateway and secure the WTLS layer for authentication.

Limitations of Wireless devices are the display of mobile phones is very small and navigation poses a problem. Currently most of the mobile devices are phones and the only input facility available is the keypad. WAP devices are basically mobile phones and they have limited Processing Power and RAM. WAP devices have very little bandwidth as compared to that of a PC. Providing users with graphics when they are using is more difficult and the deck size is small.

Important Aspects of WAP:

1. WAP is a collection of languages and tools and an infrastructure for implementing services for mobile phones.
2. WAP introduces a gateway between the phones and the servers providing content to the phones.
3. The WAP gateway talks to the phone using the WAP protocol stack, and translates the requests it receives to normal HTTP.
4. Authentication is the process of making sure that another party is actually who they claim to be.
5. Encryption is the process of encoding information in to a different format that cannot be easily understood and only the intended recipient understands.
6. Cryptography: The art of keeping messages hidden or sure.
7. WAP implements most of its security in WTLS, based on TLS with subtle differences. WTLS is capable of running over WDP or UDP.

8. Eavesdropper attack, impersonation attack, man in the Middle attack is a few threat models.

Converting Existent Web sites to WAP:

By converting existing sites i.e. HTML content to WML, HTML is the most common form of text on the web and the content converters are also known as "trans coders". Some WAP gateways do this automatically. Converters work by extracting text from a source page, then re-formatting that text in to the target markup language, in this case WAP. The converter is performing the conversion of formatted data to pure date, so we, as the conversion author decide the format we want the output to be in. The intermediate data can be manipulated without back-end and front-end processes affecting that manipulation. We can either extract all the possible contents in the page such as title, welcome messages, and links and so on or extract specific parts of the page say just the news headlines, or just the stock quotes.

Introduction to E-mail:

Email is an asynchronous message exchange technology. This simply means that when you send an E-mail message the recipients doesn't have to be available at that instant to receive the mail, but may collect the message at his own leisure. From the users point of view e-mail is sent via SMTP, collected from their mailbox using POP3 or IMAP, and any address book information is searched for using LDAP or ACAP.

What WAP & E-mail can offer?

The popularity achieved by very limited short messaging technology (SMS) indicates the demand for messaging via mobile phones certainly exists and giving mobile phones all the functionality of e-mail definitely seems to be the next logical step. E-mail is substantially more advanced technology than SMS, even if it is only used for simple SMS like that messages. Message recipients are not limited in how they receive their messages. Rather than only being able to access the messages from a single mobile phone, the user can use any e-mail client he

prefers. WAP devices and e-mail capabilities seem to be an ideal technological fit. Since, they allow for useful synergy of personal communication technology, delivering the convenience of portability from mobile phones, while allowing instant access to e-mail, providing asynchronous access to written messages.

Push Technology:

The internet user pulls the content from the network. There is a lot of information that is available and needs to be pushed to the user at a certain predefined interval or notify the users when certain important events occur. For e.g. Tourist or hotel information can be pushed to wireless device users in a particular area. The push technologies help us to provide this functionality to a WAP user. This technology is already in existence in the mobile phone networks using SMS and cell broadcast mechanism in GSM networks but they lack an important feature, interactivity.

Push Framework:

Push architecture consists of client server architecture. The server having the potential of push initiator, WAP client can listen for push requests. The push initiator sends an instruction to a proxy gateway which broadcasts the command to wireless networks using the Push-over-the-air protocol, which shall be discussed later. The message is basically XML packets. The contents are very brief, containing a message followed by a link to a web-site. The Push Access Protocol (PAP) is designed to work on the top of one of the application level protocols like HTTP or SMTP on the internet Push-Over-the-air (OTA) protocol is used on top of the WSP

layer of the WAP stack of protocols. The Push-proxy-gateway is placed between the push origin server (PI) and the WAP client. It has to implement the entire PAP protocol stack plus PAP and OTA.

Future in WAP

1. It provides the user with permanent connectivity, removing one of the major frustrations of GSM, namely dropped connections and the inconvenience and delay of having to dial up repeatedly to perform a WAP based transaction or interaction over GSM, or indeed any other circuit-switched network.

2. GSM is a circuit-switched technology. On the other hand, packet switched technologies-such as GPRS and 3G-allow users of mobile devices to establish a connection with their barrier, which is then maintained indefinitely.

3. EDGE stands for Enhanced Data Rates for Global Evolution. EDGE is a further enhancement of GSM based technology and may eventually offer data transmission rates that match those of 3G networks.

4. Bluetooth offers inexpensive, easy to build and use, low power consumption, wireless communication over short distance by means of small radio chips. Bluetooth, like a number of other key technologies such as voice recognition, improved displays and key boards, will make the user experience more convenient and rewarding for wireless devices.

5. The EPOC32 operating system designed and built for mobile computing is no doubt one of the best platform contenders for wireless client devices in terms of its capabilities and architecture.

6. In future we are likely to have a portable device, which can be called a Wireless information device (WID), which is going to be far smarter than anything currently available. Unified messaging, combining voice, e-mail, video-mail, fax and any other messaging service imaginable will become a reality. There will be many slips and stumbles along the way for many of these things to be realized. However, we can see the foundation technologies, ideas and services all around us.

Wireless LANs

TO UNWIRE AN ENTERPRISE

Wireless LANs (WLANs) provide flexible connectivity as an extension, or an alternative to a wired LAN within a building or a campus. WLANs are usually used to connect handled terminals and notebook computers to exchange real-time data with enterprise applications on the corporate backbone. These networks are growing popular in vertical markets for applications related to health-care, consulting and sales, retail, manufacturing, and education and research. The Wireless LAN (WLAN) market is likely to grow to about US$ 3 billion by 2002, according to Cahner's In-Stat Group.

WLANs augment wired LANs, making it possible to access shared information within the campus without needing to physically connect to the network. There is no need to extend the existing cabling or to configure additional nodes. And the enhanced mobility provides productivity and service opportunities that are otherwise not possible.

APPLICATIONS:

Often WLANs provide the last few meters of connectivity to the corporate backbone within a campus. Take a look at some of the applications availability of information has greatly enhanced their efficiency.

- Trade shows and product demonstrations make great use of WLANs for providing temporary connectivity.
- WLANs are very effective in rapidly changing connectivity scenarios because they make moves, additions and changes the network much easier.
- Warehouse workers roaming around the warehouse exchange information with the central database over WLANs,
- WLANs are also being used as back-ups for wired LANs in mission-critical applications.
- Teams meeting in corporate conference rooms make quicker decisions with immediate access to real time information over WLANs.
- WLANs are of great help to the service industry, such as restaurants, car rentals, and so on-because the availability of real time information is very vital to the efficiency of this industry.

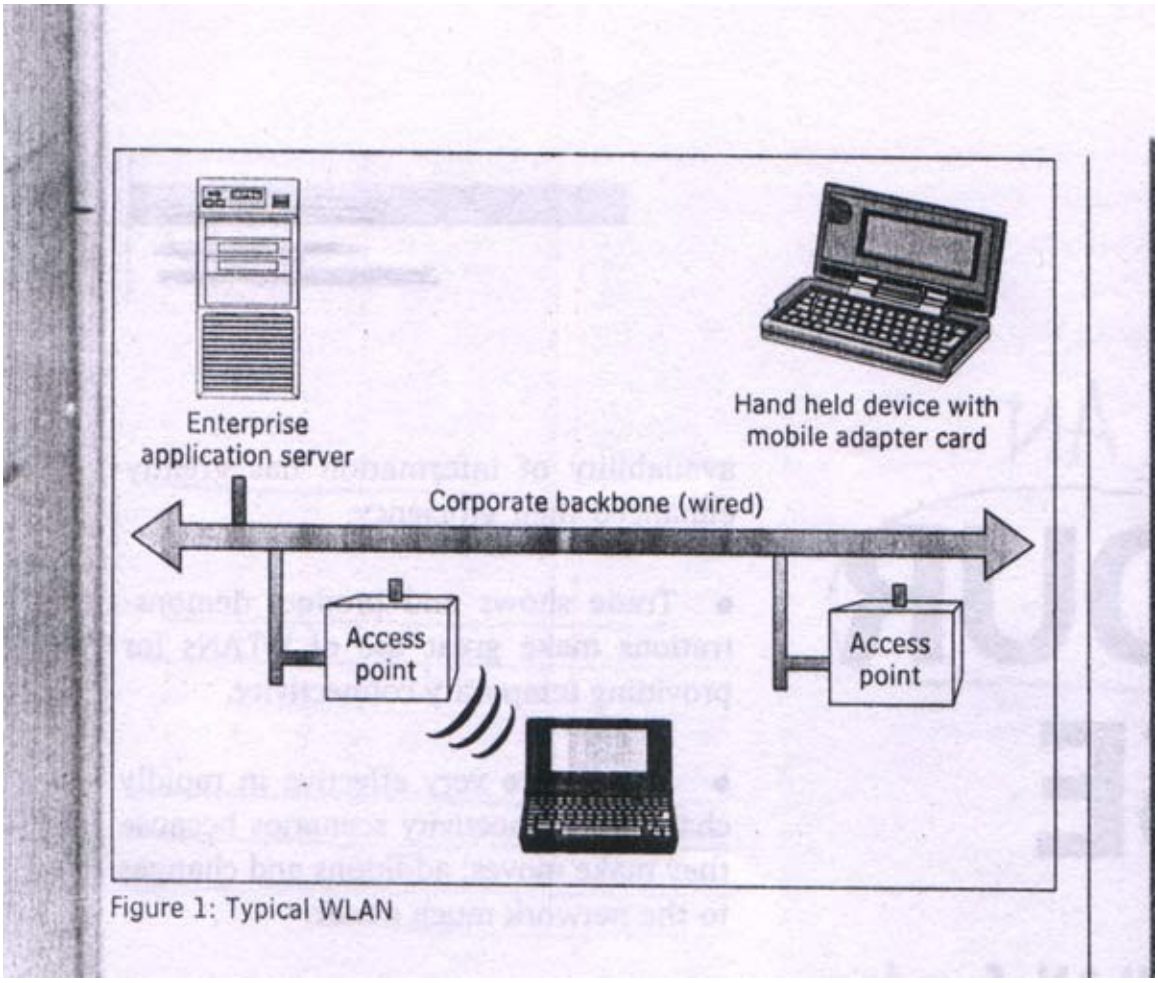


Figure 1: Typical WLAN

MAJOR BENEFITS:

Improved productivity with mobility: Access to real time information anywhere in the organization makes possible higher levels of service.

Ease of installation: WLAN installation is so much easier because there is no need to draw cables. The WLAN reach is also much wider than that of wired LANs.

Lower cost of ownership: Although the initial investment in WLANs may be more as compared to wired LANs, the cost of ownership over the entire life cycle, keeping in view the frequent moves, is significantly lower.

Scalability: WLANs are highly scalable as they can be set up in a variety of topologies to meet specific requirements.

WLAN TECHNOLOGIES:

WLANs use radio or infrared (IR) waves to communicate information from one point to another. In a typical WLAN configuration, a transmitter/receiver device, called an access point, interfaces with the wired network using standard cabling. The access point buffers and transmits data from the wireless LAN to the wired networks, A single access point can support a small group of users within a few hundred feet. The antenna of the access device is mounted at a location to provide radio coverage in the desired area. A number of such access points along the wired network augment the reach of the wired network.

At the user end, the handled devices have a WLAN adapter, which interfaces with the operating system of the device and the airwaves via an antenna. Typically, a WLAN can provide throughput to the order of 1-11 Mbps.

Wireless LANs can operate on any of the following technologies:

- **Narrowband** radio system transmits and receives user information on a specific radio frequency. Each user operates on a different frequency.

- **Spread spectrum** is used by most wireless LANs. It is a wide-band radio frequency technique developed for reliable, secure mission-critical communication systems.

- **Infrared** uses very high frequency, just below the visible light in the electromagnetic spectrum, to carry data. Just like light, IR cannot penetrate opaque objects. It is either directed line-of-sight or diffused. Inexpensive line-of-sight) systems may provide a very limited range suitable only for personal area networks. High-performance IR systems

may be impractical for wireless users and may be used to implement fixed sub-networks using line-of-sight.

Why should you deploy WLANs?

WLANs provide tremendous flexibility, scalability and mobility. Some reasons why they should be deployed are:

Area of coverage:

Based on the power of the equipment, an entire indoor area can be covered using WLANs. The range varies from 100ft to 500ft. Micro cells created by using access points can increase.

Reliability:

Though it may seem that radio interference would downgrade the performance of WLANs, sturdy designs and the limited distance over which a WLAN has to operate ensures robust connections. These connections can often be more reliable than wired LANs.

Interoperability:

WLANs seamlessly integrate with wired LANs, including Ethernet and Token Ring.

Interoperability between WLANs is becoming easier with standardization. Industry standards like IEEE 802.11 make it possible for WLANs from different vendors to work together.

Interference:

Since the radio frequencies used by WLANs may not be licensed, there is a possibility of WLANs interfering with some other devices like microwave ovens. Most vendors of WLANs design their products to take care of this interference.

Costs:

Costs include the cost of wireless access points and the wireless LAN adapters. The number of access points depends on the size of the area that is to be covered. The price of

access points ranges from US$ 600 to US$ 1500 WLAN adapters cost between US$ 150 and US$ 500. But WLANs save on the cost of cabling and the cost of implementing changes to the network.

Safety:

The output power of WLAN equipment is much less than that of a handheld cellular phone. Since radio waves fade very rapidly over distance, exposure to RF energy to the people in the vicinity is very little. No ill effects on health have been attributed to WLANs.

Security:

Wireless technology has its origin from the military. Security provisions are typically built into WLANs, often making them more secure than most wired networks. Complex encryption techniques make eavesdropping extremely difficult.

Integration with existing applications:

While planning access to the wireless infrastructure, existing applications should not be disrupted or redeveloped. Towards this, WML could be used for faster deployment. For more flexible and maintainable systems, XML-based architecture is recommended.

Depending upon specific business needs, it's perhaps time to build a very scalable and flexible WLAN solution to suit your corporate requirements.

Questions

1. What is Blue tooth Technology? Bring out the brief history of Blue tooth technology?
2. What are the System Challenges & Security aspects in Blue tooth?
3. Explain how Blue tooth is essential for embedded Internets?
4. What are the needs for Blue tooth Technology? Explain?
5. What is a WAP? What are its limitations? Why WAP forum?
6. What are WAP Protocols? Give a small note on WML.
7. Bring out the concept of Push Technology & Push Framework?
8. What is Wireless LAN? What are its limitations? Bring out the major benefits of WLAN?

9. Explain the Technological aspects of WLAN.
10. Where is the need to deploy WLAN?

Reference Books:

1. Data Communications & Distributed Networks – Wyless D Black
2. Local Area Network Architectures – David Hutchison
3. Encyclopedia of Networking – Tom Sheldon
4. Integrated Digital Network – LS Lawton
5. Integrated Services Digital Network – John Lane
6. ISDN Tutorials – ISDN – Yahoo Search Engine