CHAPTER 1 - INTRODUCTION TO COMPUTER NETWORK

1. INTRODUCTION

A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users. Networks are commonly categorized based on their characteristics.

Application of Networks

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

There are many types of networks, including:

- Local Area Networks (LAN)
- Personal Area Networks (PAN)
- Home Area Networks (HAN)
- Wide Area Networks (WAN)
- Campus Networks
- Metropolitan Area Networks (MAN)
- Enterprise Private Networks
- Internetworks
- Backbone Networks (BBN)
- Global Area Networks (GAN)
- The Internet

LAN

This is the abbreviation for Local Area Network which is when there are multiple computers and peripheral devices connected to a campus or in an office or other room. They are sharing a common connection that has 10-100 Mbps data transmission speed and are connected by Ethernet cables, usually running on high-speed internet connection. LAN computer terminals may be physically connected using cables or setup wireless, thus called WLAN. LAN is less expensive than WAN or MAN.

WAN

This is the abbreviation for Wide Area Network and is the biggest network which can interconnect networks around the world. Companies such as Microsoft or other worldwide organizations utilize WAN connection between their various branches by communicating via microwave satellites.

WAN has a data transmission speed of 256Kbps to 2Mbps, offering a faster speed than LAN or MAN. WAN is used to connect LANs that are not in the same area and is more expensive than LAN or MAN.

MAN

MAN is the abbreviation for Metropolitan Area Network and bigger than LAN network. It connects computer users that are in a specific geographical area. An example of MAN is your cable television or a large university.

MAN's data transmission speed is 5-10Mbps, which is faster and more expensive than LAN but slower and smaller than WAN.

1.1. USES OF COMPUTER NETWORK

The computer networks are playing an important role in providing services to large organizations as well as to the individual common man.

Service Provided by the Network for Companies:

• Many organizations have a large number of computers in operation. These computers may be within the same building, campus, city or different cities.

• Even though the computers are located in different locations, the organizations want to keep track of inventories, monitor productivity, do the ordering and billing etc.

• The computer networks are useful to the organizations in the following ways:

1. Resource sharing.

2. for providing high reliability.

3. To save money.

4. It can provide a powerful communication medium.

The computer networks offer the following services to an individual person:

1. Access to remote information

2. Person to person communication

3. Interactive entertainment.

Access to remote information:

Access to remote information involves interaction· between a person and a remote database. Access to remote information comes in many forms like:

(i) Home shopping, paying telephone, electricity bills, e-banking, on line share market etc.

(ii) Newspaper is. On-line and is personalized, digital library consisting of books, magazines, scientific journals etc.

(iii) World wide web which contains information. about the arts, business, cooking, government, health, history, hobbies, recreation, science, sports etc.

Interactive entertainment:

Interactive entertainment includes:

(i) Multi person real-time simulation games.

(ii) Video on demand.

(iii) Participation in live TV programs likes quiz, contest, discussions etc.

In short, the ability to merge information, communication and entertainment will surely give rise to a massive new industry based on computer networking.

1.2. NETWORKING MODEL

a) Client-Server Model

Client-server architecture (client/server) is a network architecture in which each computer or process on the network is either a client or a server. Servers are powerful computers or processes dedicated to managing disk drives (file servers), printers (print servers), or network traffic (network servers). Clients are PCs or workstations on which users run applications. Clients rely on servers for resources, such as files, devices, and even processing power.

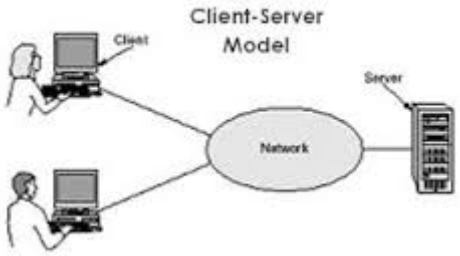
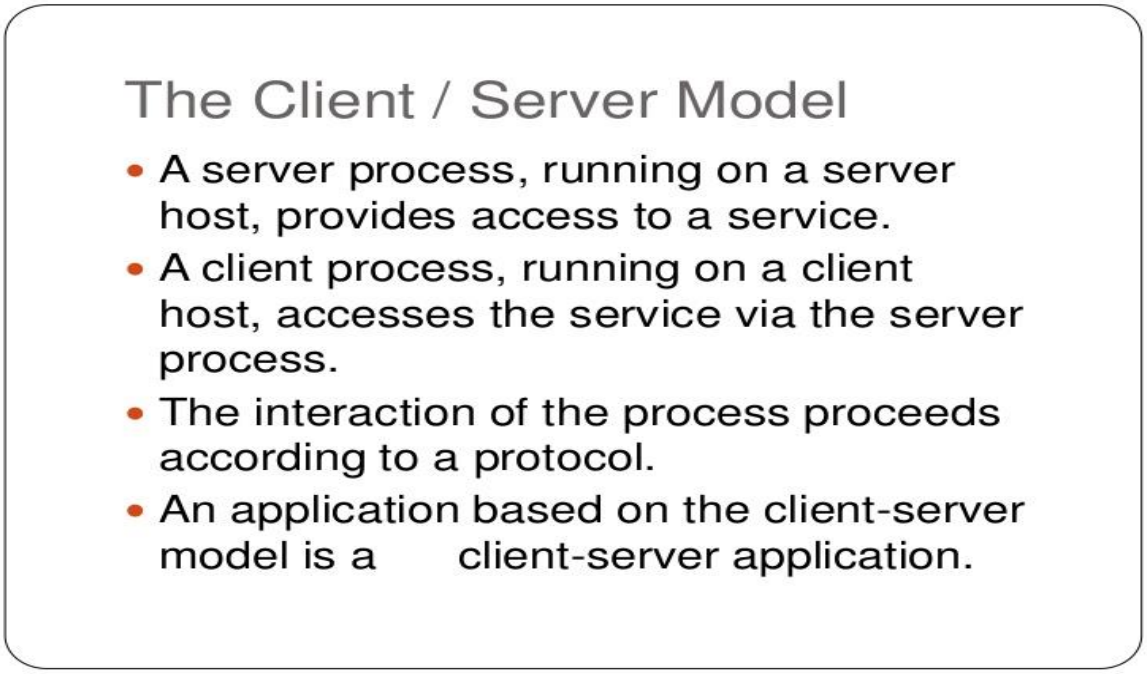
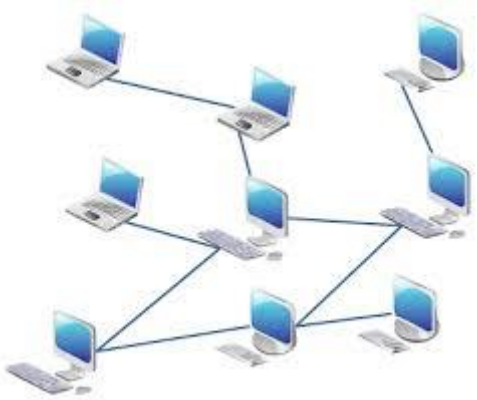


Fig: Client-Server model



b). P2P model

Peer-to-peer (P2P) is a decentralized communications model in which each party has the same capabilities and either party can initiate a communication session. Unlike the client/server model, in which the client makes a service request and the server fulfills the request, the P2P network model allows each node to function as both a client and server. In its simplest form, a peer-to-peer (P2P) network is created when two or more PCs are connected and share resources without going through a separate server computer. Most P2P programs are focused on media sharing.



c) Active network

An active network is a network in which the nodes are programmed to perform custom operations on the messages that pass through the node. For example, a node could be programmed or customized to handle packets on an individual user basis or to handle multicast packets differently than other packets. Active network approaches are expected to be especially important in networks of mobile users. "Smart packets" use a special self-describing language that allows new kinds of information to be carried within a packet and operated on by a node.

1.3. PROTOCOLS AND STANDARDS

A protocol is the special set of rules that end points in a telecommunication connection use when they communicate. Protocols specify interactions between the communicating entities. Protocols exist at several levels in a telecommunication connection. For example, there are protocols for the data interchange at the hardware device level and protocols for data interchange at the application program level. In the standard model known as Open Systems Interconnection (OSI), there are one or more protocols at each layer in the telecommunication exchange that both ends of the exchange must recognize and observe. Protocols are often described in an industry or international standard. Standard is a common set of rules.

NEED OF LAYERED ARCHITECTURE IN COMPUTER NETWORK

It simplifies the design process as the functions of each layers and their interactions are well defined.

- The layered architecture provides flexibility to modify and develop network services.
- The number of layers, name of layers and the tasks assigned to them may change from network to network. But for all the networks, always the lower layer offers certain services to its upper layer.
- The concept of layered architecture redefines the way of convincing networks. This leads to a considerable cost savings and managerial benefits.
- Addition of new services and management of network infrastructure become easy.

DESIGN ISSUE OF LAYERED ARCHITECTURE IN COMPUTER NETWORK

There might be a negative impact on the performance as we have the extra overhead of passing through layers instead of calling a component directly.

Development of user-intensive applications can sometime take longer if the layering prevents the use of user interface components that directly interact with the database.

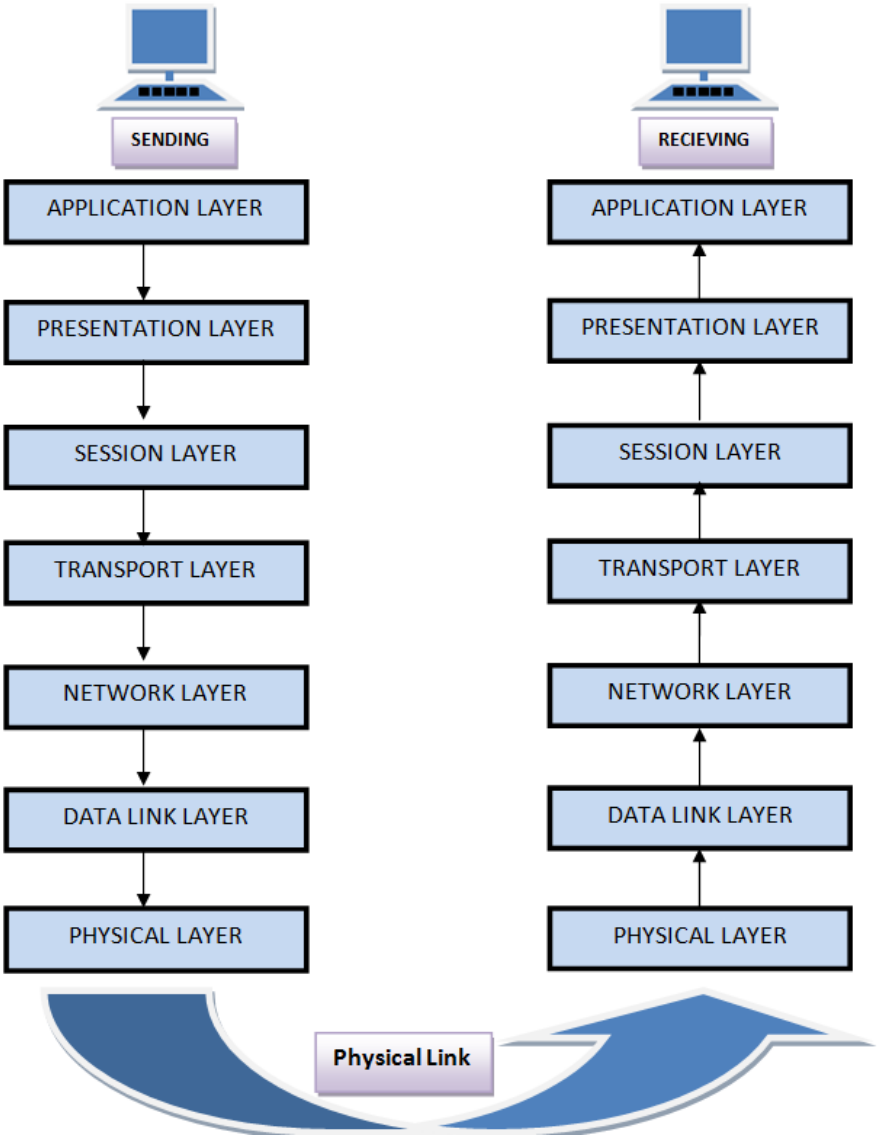
The use of layers helps to control and encapsulate the complexity of large applications, but adds complexity to simple applications.

Changes to lower level interfaces tend to percolate to higher levels, especially if the relaxed layered approach is used.

1.4. OSI MODEL AND TCP/IP MODEL

There are many users who use computer network and are located all over the world. To ensure national and worldwide data communication ISO (ISO stands for International Organization of Standardization.) developed this model. This is called a model for open system interconnection (OSI) and is normally called as OSI model.OSI model architecture consists of seven layers. It

Defines seven layers or levels in a complete communication system.



Layer 1: The Physical Layer:

1. It is the lowest layer of the OSI Model.
2. It activates, maintains and deactivates the physical connection.
3. It is responsible for transmission and reception of the unstructured raw data over network.
4. Voltages and data rates needed for transmission is defined in the physical layer.
5. It converts the digital/analog bits into electrical signal or optical signals.
6. Data encoding is also done in this layer.

Layer 2: Data Link Layer:

1. Data link layer synchronizes the information which is to be transmitted over the physical layer.
2. The main function of this layer is to make sure data transfer is error free from one node to

another, over the physical layer.
3. Transmitting and receiving data frames sequentially is managed by this layer.
4. This layer sends and expects acknowledgements for frames received and sent respectively. Resending of non-acknowledgement received frames is also handled by this layer.
5. This layer establishes a logical layer between two nodes and also manages the Frame traffic control over the network. It signals the transmitting node to stop, when the frame buffers are full.

Layer 3: The Network Layer:

1. It routes the signal through different channels from one node to other.
2. It acts as a network controller. It manages the Subnet traffic.
3. It decides by which route data should take.
4. It divides the outgoing messages into packets and assembles the incoming packets into messages for higher levels.

Layer 4: Transport Layer:

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as Multiplexing, Segmenting or Splitting on the data are done by this layer
3. It receives messages from the Session layer above it, convert the message into smaller units and passes it on to the Network layer.
4. Transport layer can be very complex, depending upon the network requirements.

Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.

Layer 5: The Session Layer:

1. Session layer manages and synchronize the conversation between two different applications.
2. Transfer of data from source to destination session layer streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided.

Layer 6: The Presentation Layer:

1. Presentation layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data.
2. While receiving the data, presentation layer transforms the data to be ready for the application layer.
3. Languages (syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role of translator.
4. It performs Data compression, Data encryption, Data conversion etc.

Layer 7: Application Layer:

1. It is the topmost layer.
2. Transferring of files disturbing the results to the user is also done in this layer. Mail services,

directory services, network resource etc are services provided by application layer.

3. This layer mainly holds application programs to act upon the received and to be sent data.

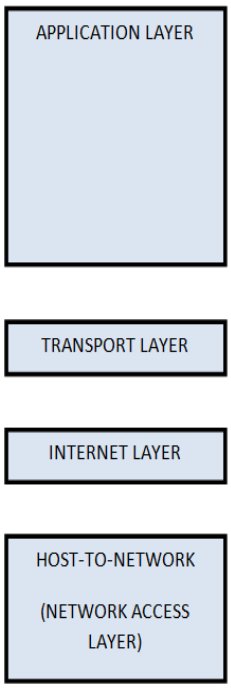
Merits of OSI reference model:

1. OSI model distinguishes well between the services, interfaces and protocols.
2. Protocols of OSI model are very well hidden.
3. Protocols can be replaced by new protocols as technology changes.
4. Supports connection oriented services as well as connectionless service.

Demerits of OSI reference model:

1. Model was devised before the invention of protocols.
2. Fitting of protocols is tedious task.
3. It is just used as a reference model.

TCP/IP is transmission control protocol and internet protocol. Protocols are set of rules which govern every possible communication over the internet. These protocols describe the movement of data between the host computers or internet and offers simple naming and addressing schemes.



Overview of TCP/IP reference model

TCP/IP that is Transmission Control Protocol and Internet Protocol was developed by Department of Defense's Project Research Agency (ARPA, later DARPA) as a part of a research project of network interconnection to connect remote machines.

The features that stood out during the research, which led to making the TCP/IP reference model

were:

- Support for a flexible architecture. Adding more machines to a network was easy.
- The network was robust, and connections remained intact until the source and destination machines were functioning.

The overall idea was to allow one application on one computer to talk to(send data packets) another application running on different computer.

Description of different TCP/IP protocols

Layer 1: Host-to-network Layer

1. Lowest layer of the all.
2. Protocol is used to connect to the host, so that the packets can be sent over it.
3. Varies from host to host and network to network.

Layer 2: Internet layer

1. Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.
2. It is the layer which holds the whole architecture together.
3. It helps the packet to travel independently to the destination.
4. Order in which packets are received is different from the way they are sent.
5. IP (Internet Protocol) is used in this layer.

Layer 3: Transport Layer

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
3. The applications can read and write to the transport layer.
4. Transport layer adds header information to the data.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
6. Transport layer also arrange the packets to be sent, in sequence.

Layer 4: Application Layer

The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

1. TELNET is a two-way communication protocol which allows connecting to a remote machine and run applications on it.
2. FTP (File Transfer Protocol) is a protocol that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
3. SMTP (Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
4. DNS (Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.

Merits of TCP/IP model

1. It operated independently.
2. It is scalable.
3. Client/server architecture.
4. Supports a number of routing protocols.
5. Can be used to establish a connection between two computers.

Demerits of TCP/IP

1. In this, the transport layer does not guarantee delivery of packets.
2. The model cannot be used in any other application.
3. Replacing protocol is not easy.
4. It has not clearly separated its services, interfaces and protocols.

1.5. COMPARISION OF OSI AND TCP/IP

OSI(Open System Interconnection)	TCP/IP(Transmission Control Protocol / Internet Protocol)
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	5. TCP/IP model is, in a way implementation of the OSI model.
6. Network layer of OSI model provides both connection oriented and connectionless service.	6. The Network layer in TCP/IP model provides connectionless service.
7. OSI model has a problem of fitting the protocols into the model.	7. TCP/IP model does not fit any protocol
8. Protocols are hidden in OSI model and are easily replaced as the technology changes.	8. In TCP/IP replacing protocol is not easy.
9. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	9. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
10. It has 7 layers	10. It has 4 layers

1.6. EXAMPLE NETWORK

VoIP

Once upon a time, the public switched telephone system was primarily used for voice traffic with a little bit of data traffic here and there. But the data traffic grew and grew, and by 1999, the number of data bits moved equaled the number of voice bits (since voice is in PCM on the trunks, it can be measured in bits/sec). By 2002, the volume of data traffic was an order of magnitude more than the volume of voice traffic and still growing exponentially, with voice traffic being almost flat (5% growth per year).

As a consequence of these numbers, many packet-switching network operators suddenly became interested in carrying voice over their data networks. The amount of additional bandwidth required for voice is minuscule since the packet networks are dimensioned for the data traffic. However, the average person's phone bill is probably larger than his Internet bill, so the data network operators saw Internet telephony as a way to earn a large amount of additional money without having to put any new fiber in the ground.

Voice over IP (VoIP) commonly refers to the communication protocols, technologies, methodologies, and transmission techniques involved in the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet.

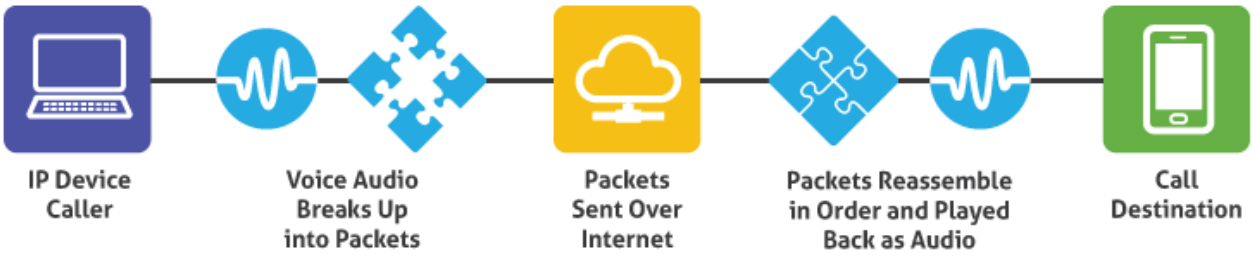
The steps involved in originating a VoIP telephone call are signaling and media channel setup, digitization of the analog voice signal, encoding, packetization, and transmission as Internet Protocol (IP) packets over a packet-switched network. On the receiving side, similar steps (usually in the reverse order) such as reception of the IP packets, decoding of the packets and digital-to-analog conversion reproduce the original voice stream. Even though IP Telephony and VoIP are terms that are used interchangeably, they are actually different; IP telephony has to do with digital telephony systems that use IP protocols for voice communication, while VoIP is actually a subset of IP Telephony. VoIP is a technology used by IP telephony as a means of transporting phone calls.

VoIP systems employ session control protocols to control the set-up and tear-down of calls as well as audio codec which encode speech allowing transmission over an IP network as digital audio via an audio stream. VoIP is available on many smart phones and Internet devices so that users of portable devices that are not phones, may place calls or send SMS text messages over 3G or Wi-Fi.

A VoIP phone is necessary to connect to a VoIP service provider. This can be implemented in several ways:

- Dedicated VoIP phones connect directly to the IP network using technologies such as wired Ethernet or wireless Wi-Fi. They are typically designed in the style of traditional digital business telephones.
- An analog telephone adapter is a device that connects to the network and implements the electronics and firmware to operate a conventional analog telephone attached through a modular phone jack. Some residential Internet gateways and cable modems have this function built in.

- A soft phone is application software installed on a networked computer that is equipped with a microphone and speaker, or headset. The application typically presents a dial pad and display field to the user to operate the application by mouse clicks or keyboard input.



Advantages

a. Operational Cost
b. Quality of Service
c. Portability
d. Features like call forwarding, call waiting, three party conversation
e. Flexibility

Disadvantages

a. No service during power outage
b. Reliability
c. Security

NGN

A next-generation network (NGN) is a packet-based network which can provide services including Telecommunication Services and able to make use of multiple broadband, quality of Service-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It offers unrestricted access by users to different service providers. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users.

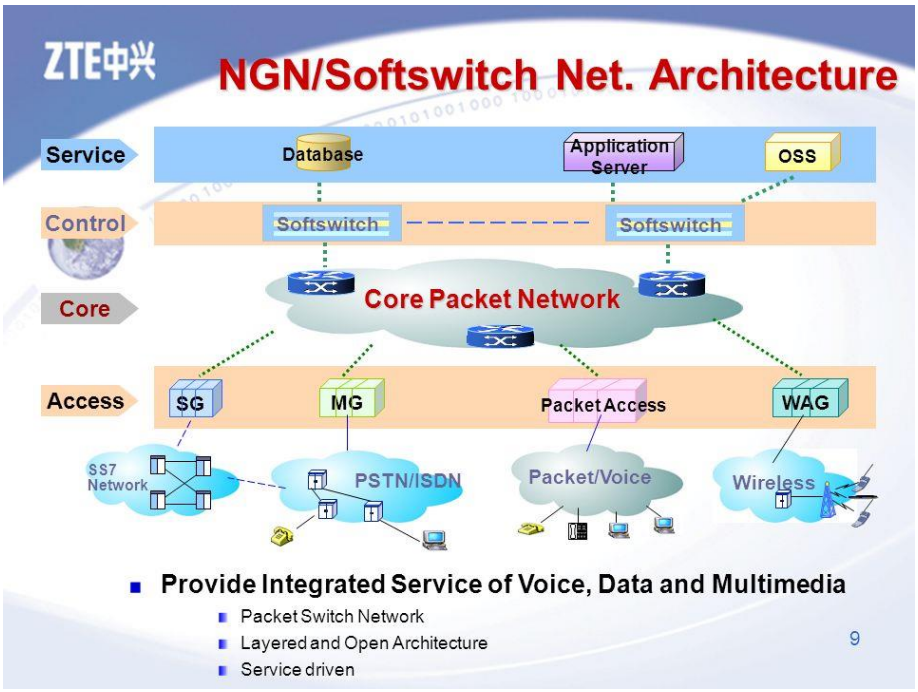
NGN involves three main architectural changes that need to be looked at separately:

- In the core network, NGN implies a consolidation of several (dedicated or overlay) transport networks each historically built for a different service into one core transport network (often based on IP and Ethernet). It implies amongst others the migration of voice from a circuit-switched architecture (PSTN) to VoIP, and also migration of legacy services such as X.25, frame relay (either commercial migration of the customer to a new service like IP VPN, or technical emigration by emulation of the "legacy service" on the NGN).

- In the wired access network, NGN implies the migration from the dual system of legacy voice next to xDSL setup in local exchanges to a converged setup in which the DSLAMs

integrate voice ports or VoIP, making it possible to remove the voice switching infrastructure from the exchange.

- In the cable access network, NGN convergence implies migration of constant bit rate voice to CableLabs PacketCable standards that provide VoIP and SIP services. Both services ride over DOCSIS as the cable data layer standard.



MPLS

Multiprotocol Label Switching (**MPLS**) is a mechanism in high-performance telecommunications networks that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table. The labels identify virtual links (paths) between distant nodes rather than endpoints. MPLS can encapsulate packets of various network protocols. MPLS supports a range of access technologies, including T1/E1, ATM, Frame Relay, and DSL.

MPLS is a highly scalable, protocol agnostic, data-carrying mechanism. In an MPLS network, data packets are assigned labels. Packet-forwarding decisions are made solely on the contents of this label, without the need to examine the packet itself. This allows one to create end-to-end circuits across any type of transport medium, using any protocol. The primary benefit is to eliminate dependence on a particular OSI model data link layer technology, such as Asynchronous Transfer Mode (ATM), Frame Relay, Synchronous Optical Networking (SONET) or Ethernet, and eliminate the need for multiple layer-2 networks to satisfy different types of traffic. MPLS belongs to the family of packet-switched networks.

MPLS operates at a layer that is generally considered to lie between traditional definitions of layer 2 (data link layer) and layer 3 (network layer), and thus is often referred to as a "layer 2.5" protocol. It was designed to provide a unified data-carrying service for both circuit-based clients and packet-switching clients which provide a datagram service model. It can be used to carry many different kinds of traffic, including IP packets, as well as native ATM, SONET, and Ethernet frames. A

number of different technologies were previously deployed with essentially identical goals, such as Frame Relay and ATM. MPLS technologies have evolved with the strengths and weaknesses of ATM in mind. Many network engineers agree that ATM should be replaced with a protocol that requires less overhead, while providing connection-oriented services for variable-length frames. MPLS is currently replacing some of these technologies in the marketplace. It is highly possible that MPLS will completely replace these technologies in the future, thus aligning these technologies with current and future technology needs.

Features

a. Packet classification

b. Congestion avoidance

c. Congestion management

d. Path Protection

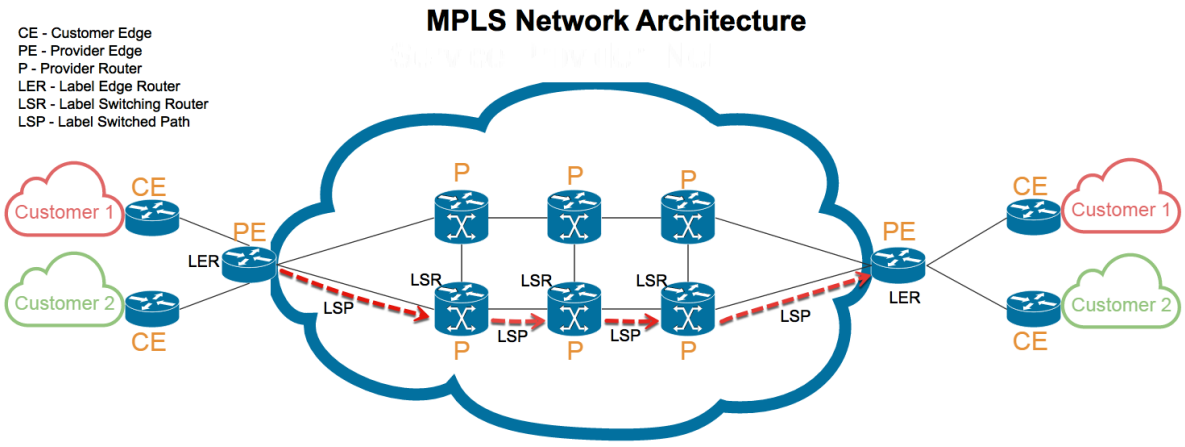
e. Security

Advantage

a. Scalability of network layer routing

b. Flexibility of delivering routing services

c. Increased performance



xDSL

When the telephone industry finally got to 56 kbps, it patted itself on the back for a job well done. Meanwhile, the cable TV industry was offering speeds up to 10 Mbps on shared cables, and satellite companies were planning to offer upward of 50 Mbps. As Internet access became an increasingly important part of their business, the telephone companies began to realize they needed a more competitive product. Their answer was to start offering new digital services over the local loop. Services with more bandwidth than standard telephone service are sometimes called broadband, although the term really is more of a marketing concept than a specific technical concept.

Initially, there were many overlapping offerings, all under the general name of xDSL (Digital Subscriber Line), for various x. Below we will discuss these but primarily focus on what is probably going to become the most popular of these services, ADSL (Asymmetric DSL).

The reason that modems are so slow is that telephones were invented for carrying the human voice and the entire system has been carefully optimized for this purpose. Data have always been stepchildren. At the point where each local loop terminates in the end office, the wire runs through a filter that attenuates all frequencies below 300 Hz and above 3400 Hz. The cutoff is not sharp—300 Hz and 3400 Hz are the 3 dB points—so the bandwidth is usually quoted as 4000 Hz even though the distance between the 3 dB points is 3100 Hz. Data are thus also restricted to this narrow band.

The trick that makes xDSL work is that when a customer subscribes to it, the incoming line is connected to a different kind of switch, one that does not have this filter, thus making the entire capacity of the local loop available. The limiting factor then becomes the physics of the local loop, not the artificial 3100 Hz bandwidth created by the filter. Unfortunately, the capacity of the local loop depends on several factors, including its length, thickness, and general quality.

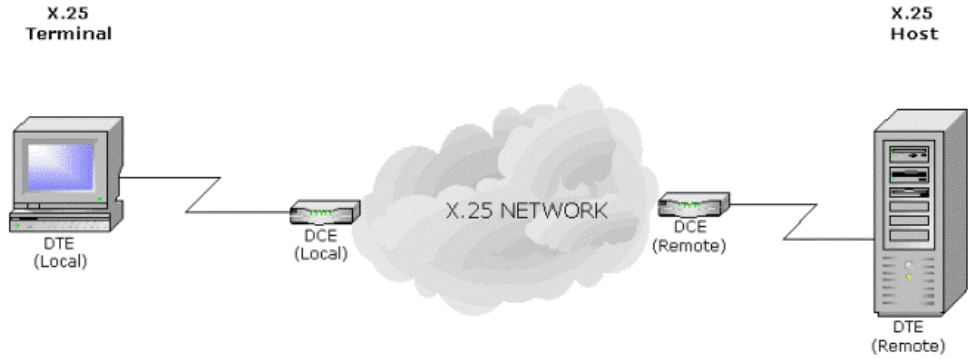
The xDSL services have all been designed with certain goals in mind. First, the services must work over the existing twisted pair local loops. Second, they must not affect customers' existing telephones and fax machines. Third, they must be much faster than 56 kbps. Fourth, they should be always on, with just a monthly charge but no per-minute charge.

X.25

A connection-oriented network is X.25, which was the first public data network. It was deployed in the 1970s at a time when telephone service was a monopoly everywhere and the telephone company in each country expected there to be one data network per country—theirs. To use X.25, a computer first established a connection to the remote computer, that is, placed a telephone call. This connection was given a connection number to be used in data transfer packets (because multiple connections could be open at the same time). Data packets were very simple, consisting of a 3-byte header and up to 128 bytes of data. The header consisted of a 12-bit connection number, a packet sequence number, an acknowledgement number, and a few miscellaneous bits. X.25 networks operated for about a decade with mixed success.

Frame Relay

In the 1980s, the X.25 networks were largely replaced by a new kind of network called frame relay. The essence of frame relay is that it is a connection-oriented network with no error control and no flow control. Because it was connection-oriented, packets were delivered in order (if they were delivered at all). The properties of in-order delivery, no error control, and no flow control make frame relay akin to a wide area LAN. Its most important application is interconnecting LANs at multiple company offices. Frame relay enjoyed a modest success and is still in use in places today.



Frame Relay	X.25
■No error detection ->greater speeds	■Error detection -> error-free delivery
■Physical and data link layers. -> high performance, greater transmission	■Physical, data link and network layers
■Prepare and send frames ■Frames contain expanded address field -> direct frames to destinations with minimal processing	■Prepare and send packets ■Packets contain fields used for error and flow control
■Can dynamically allocate bandwidth	■Has fixed bandwidth available

Ethernet (IEEE 802.3) Local Area Network (LAN)

Ethernet protocols refer to the family of local-area network (LAN) covered by the IEEE 802.3. In the Ethernet standard, there are two modes of operation: half-duplex and full-duplex modes. In the half duplex mode, data are transmitted using the popular Carrier-Sense Multiple Access/Collision Detection (CSMA/CD) protocol on a shared medium. The main disadvantages of the half-duplex are the efficiency and distance limitation, in which the link distance is limited by the minimum MAC frame size. This restriction reduces the efficiency drastically for high-rate transmission. Therefore, the carrier extension technique is used to ensure the minimum frame size of 512 bytes in Gigabit Ethernet to achieve a reasonable link distance.

Four data rates are currently defined for operation over optical fiber and twisted-pair cables:

- 10 Mbps – 10Base-T Ethernet (IEEE 802.3)
- 100 Mbps – Fast Ethernet (IEEE 802.3u)
- 1000 Mbps – Gigabit Ethernet (IEEE 802.3z)
- 10-Gigabit – 10 Gbps Ethernet (IEEE 802.3ae).

In this document, we discuss the general aspects of the Ethernet. The specific issues regarding Fast Ethernet, Gigabit and 10 Gigabit Ethernet will be discussed in separate documents.

The Ethernet system consists of three basic elements: 1. the physical medium used to carry Ethernet signals between computers, 2. a set of medium access control rules embedded in each Ethernet interface that allow multiple computers to fairly arbitrate access to the shared Ethernet channel, and 3. an Ethernet frame that consists of a standardized set of bits used to carry data over the system.

As with all IEEE 802 protocols, the ISO data link layer is divided into two IEEE 802 sub layers, the Media Access Control (MAC) sub layer and the MAC-client sub layer. The IEEE 802.3 physical layer corresponds to the ISO physical layer.

The MAC sub-layer has two primary responsibilities:

- Data encapsulation, including frame assembly before transmission, and frame parsing/error detection during and after reception

- Media access control, including initiation of frame transmission and recovery from transmission failure

The MAC-client sub-layer may be one of the following:

- Logical Link Control (LLC), which provides the interface between the Ethernet MAC and the upper layers in the protocol stack of the end station. The LLC sub layer is defined by IEEE 802.2 standards.
- Bridge entity, which provides LAN-to-LAN interfaces between LANs that use the same protocol (for example, Ethernet to Ethernet) and also between different protocols (for example, Ethernet to Token Ring). Bridge entities are defined by IEEE 802.1 standards.

Each Ethernet-equipped computer 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. 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.

After each frame transmission, all stations on the network must contend equally for the next frame transmission opportunity. Access to the shared channel is determined by the medium access control (MAC) mechanism embedded in the Ethernet interface located in each station. The medium access control mechanism is based on a system called Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

As each Ethernet frame is sent onto the shared signal channel, all Ethernet interfaces look at the destination address. If the destination address of the frame matches with the interface address, the frame will be read entirely and be delivered 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.

When it comes to how signals flow over the set of media segments that make up an Ethernet system, it helps to understand the topology of the system. The signal topology of the Ethernet is also known as the logical topology, to distinguish it from the actual physical layout of the media cables. The logical topology of an Ethernet provides a single channel (or bus) that carries Ethernet signals to all stations.