

Department of Information Science and Technology

Veer Narmad South Gujarat University

Instruction to network in computer network

Submitted by..

Name	Roll no.
Aahir Kinal	1
Ambaliya Shreya	3
Gaudani Poonam	24
Gorasiya Parul	27
Hirapara Kinal	28
Joshi pooja	34

Kanthariya Ronika

41

Kodinariya Dhara

50

Lathiya Panktee

55

Malaviya Surbhi

57

Maniya Ravina

60

Submitted to...

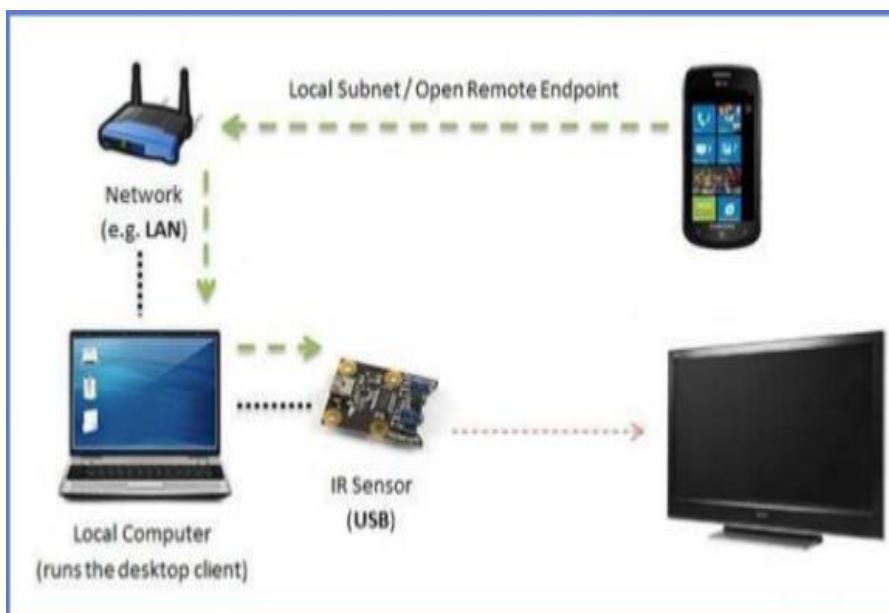
Pandey sir

1.1 - What is Data Communication?

- Exchange of data between two devices via some forms of transmission medium(such as wire cable) is data communications.
- For data communications to occur, the communicating devices must be part of a communication system made of a combination of hardware and software.
- The effectiveness of a data communication system depends on four fundamental characteristics:-

- 1.Delivery
- 2.Accuracy
- 3.Timeliness
- 4.Jitter

Components of Data



Communication:

- 1.Sender
- 2.Receiver
- 3.Message
- 4.Transmission medium
- 5.protocol

The five components of data communication are:

1.Message:- It is the information to be communicated.

Popular forms of information include text, pictures, audio, video etc.

2.Sender:- It is the device which sends the data messages. It can be a computer, workstation, telephone handset etc.

3.Receiver:- It is the device which receives the data messages. It can be a computer, workstation, telephone handset etc.

4.Transmission Medium:- It is the physical path by which a message travels from sender to receiver. Some examples include twisted-pair wire, coaxial cable, radio waves etc.

5.Protocol:- It is a set of rules that governs the data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating.

https://www.tutorialspoint.com/data_communication_computer_network/data_communication_computer_network_overview.htm

<http://datacombd.blogspot.in/2011/05/explain-five-components-of-data.html?m=1>

1.2 - Direction of Data Flow

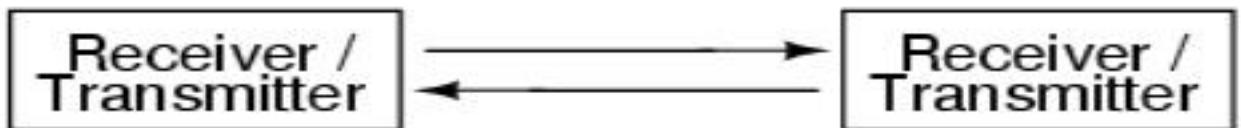
Buses and networks are designed to allow communication to occur between individual devices that are interconnected. The flow of information, or data, between nodes, can take a variety of forms:

With simplex communication, all data flow is unidirectional: from the designated transmitter to the designated receiver. BogusBus is an example of simplex communication, where the transmitter sent information to the remote monitoring location, but no information is ever sent back to the water tank. If all we want to do is send information one-way, then simplex is just fine. Most applications, however, demand more:

Simplex communication

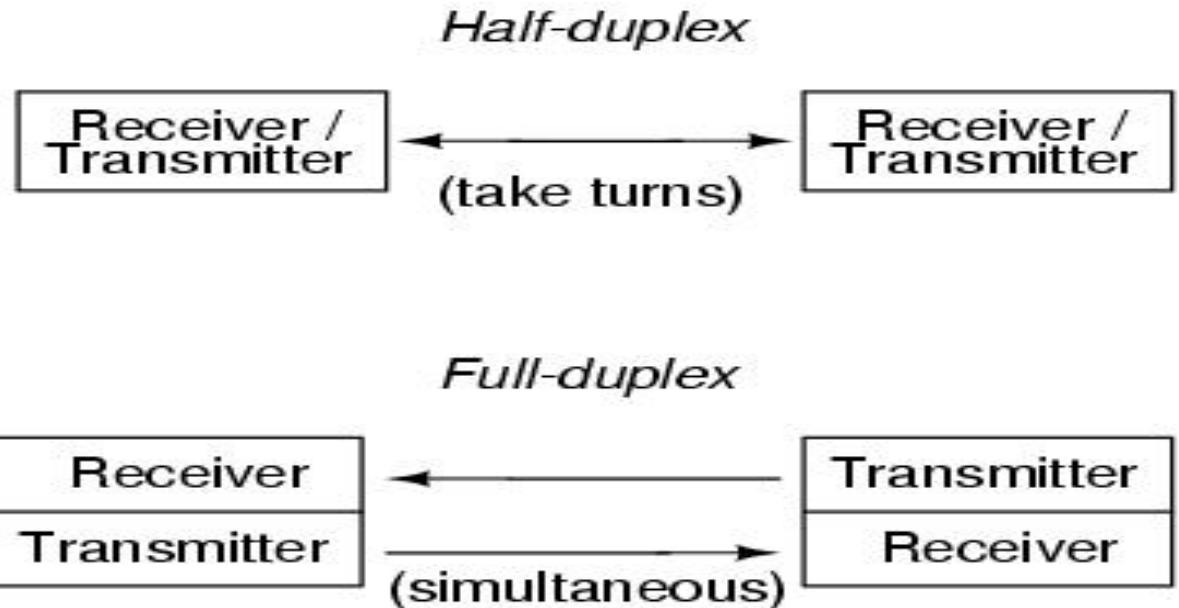


Duplex communication



With duplex communication, the flow of information

is bi-directional for each device. Duplex can be further divided into two sub-categories:



Half-duplex communication may be likened to two tin cans on the ends of a single taut string: Either can may be used to transmit or receive, but not at the same time. Full-duplex communication is more like a true telephone, where two people can talk at the same time and hear one another simultaneously, the mouthpiece of one phone transmitting to the earpiece of the other, and vice versa. Full-duplex is often facilitated through the use of two separate channels or networks, with an individual set of wires for each direction of communication. It is sometimes accomplished by means of multiple-frequency carrier waves, especially in radio links, where one frequency is reserved for each direction of communication.

1.3-Basic Networking Concepts

- 1.Introduction
- 2.Types of network
- 3.Network topology diagram
- 4.Data transmission
- 5.Interconnection

1.Introduction

- A network consist of two or more computers that are linked via some medium.
- Example:-Printers and CD ROMs.
- The Computer on Network may be linked by cable , telephone lines , satellites .
- Each of the device on the network can be thought of as a node ; each node has a unique address.
- Address are numeric quantities that are easy for computers to work with , but not humans to remember.
- Some networks also provide names that humans can more easily remember than numbers.
- Example : www.javasoft.com , corresponding to the above numeric address.

2. Types of Network

There are two principle kinds of networks:

1. Wide Area Networks (WANs)
2. Local Area Networks (LANs)

1. WANs :

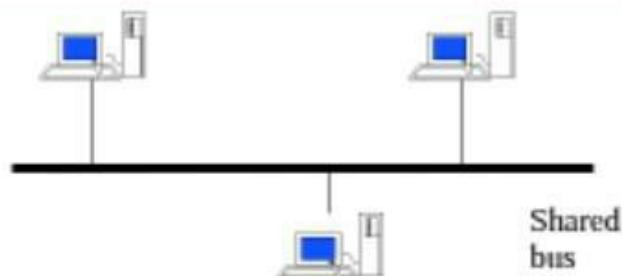
- A WAN provides long-distance transmission of data , image , video ,audio information over large geographical areas.
- That Cover cities , countries and continents or even the all world.
- Based on packet switch technology.
- A WAN can be as complex as the backbones that connects as simple as a dial-up line that connects home computer to the internet.
- We normally refer to the first as a switch WAN and the second as a point to point WAN.
- The point -to - point WAN is normally a line leased from a telephone or cable TV provider that connects a home PC .
- Example :
 1. Asynchronous Transfer Mode (ATM)
 2. Integrated Service Digital Network (ISDN)

2. LANs

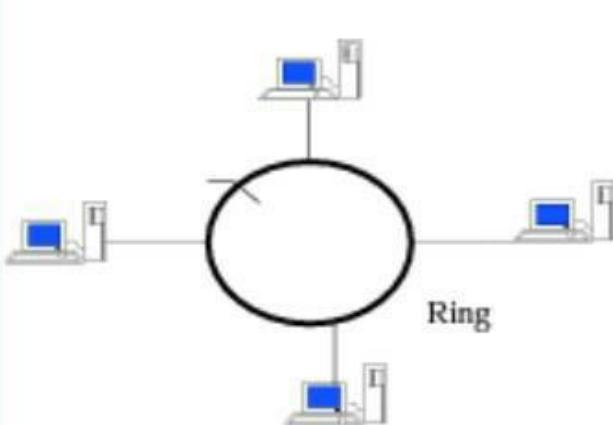
-> A local area network is usually privately owned and office , campus , university ,building.

Depending on the needs of an organization and the type of technology used a LAN can be as simple as two PCs and a printer is someone's home office or it can extended throughout a company and include audio video peripherals.

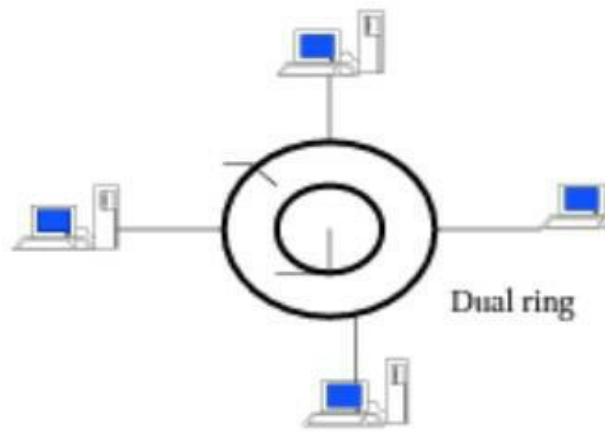
-> currently LAN size is limited to a few kilometers.



(a) Ethernet LAN



(b) Token Ring LAN



(c) FDDI LAN

Network connectivity type	Speed	Transmission time for 10 Mbytes
(Telephone) dial-up modem	14.4 Kbps	90 min
ISDN modem	56/128 Kbps	45/12min
T1 connection	1.54 Mbps	50s
Ethernet	10 Mbps	9s
Token ring	4/16 Mbps	
Fast Ethernet	100 Mbps	
FDDI	100 Mbps	
Gigabit Ethernet	1 Gbps	
ATM	25Mbps/2.4Gbs	

Network Topology Diagram

- The specification of the network topology diagram requires the definition of the characteristics and entities underlie the network.

- Geographical location of the different components or subnets involved in the network.
- Description of the LAN topology.
- Description of the WAN topology.
- Description of the network connectors such as routers , bridge , repeaters and gateways.

Data transmission

- It using packet switching
- Message are broken into unit it called packets & sent from one computer to another.
- In the destination ,packet reconstruct the original message.
- Each packets has a maximum size & consist of a header &dataarea.
- Header content the header of source & destination computers .sequencely information is require or necessary to transfer.

Interconnection

Networks of a low capacity may be connected together via a backbone network which is a

network of high capacity such as a FDDI network , a WAN network etc.

LANs and WANs can be interconnected via T1 or T3 digital leased lines.

According to the protocols involved , network interconnection is achieved using one or several of the following devices:

- Bridge : a computers or device that links two similar LANs based on the same protocols.
- Router : a communication computer that connects different type of network using different protocols.
- B-router or Bridge/Router : a single device that combines both the functions of bridge and router.
- Gateway : A network device that connect two different system , using direct and systematic translation between protocols.

<https://www.ece.uvic.ca/notes>

1.4 – Advantages, Need and Use of Network

Advantages

1. make file sharing easier:

It allows easier accessibility for people to share their file , which greatly help them with saving more time and effort.

2. Highly flexible :

It gives user the opportunity to explore everything about assential thing such as without affecting their functionality.

3. Not expensive:

Installing networking software on your device would not cost too much.

4. Increase in storage capacity of the software:

Since you are going to share file and resource to other people , you need to make sure that all the data and file are properly stored in the system.

URL

<https://futureofworking.com/8-advantages-and-disadvantages-of-computer-networking/>

Need

1.file sharing:

You can share the data file through computer network.

2. Hardware sharing:

Users can share printer , CD-ROMS drives , hard drives .

You can not share the device without network.

3. Application sharing:

Users can implement client / server application.

4 . network gaming :

A numbes of games are available on network , which allows multi-user to play from different location.

URL

<http://www.omnisecu.com/basic-networking/why-we-need-computer-network.php>

Use

1.resource sharing:

I allows all program , and data available to anyone on the network irrespective of the physical location of the resource and the user.

2. high reliability due to alternative source of data:

Eg . All file could be replicated on more than one machines, si if onr of them is unavailable due to hardware failure or any other reason, the other copies can be used.

3 . Money saving:

Computer networking is an important financial aspect for organization because it save money.

The organization , if it want security for its operation it can go in for the domain model in which there is a server and clients . All the clients can communicate and access data through the server.

4. communication medium:

medium among widely separated people.

A computer network provides a powerful

communication URL

<http://googleweblight.com/i?u=http://ecomputernotes.com/computernetworkingnotes/computer-network/what-is-a-computer-network&grqid=8T8xi29e&hl=en-IN>

1.5- Categories of Network

Different Types of networks

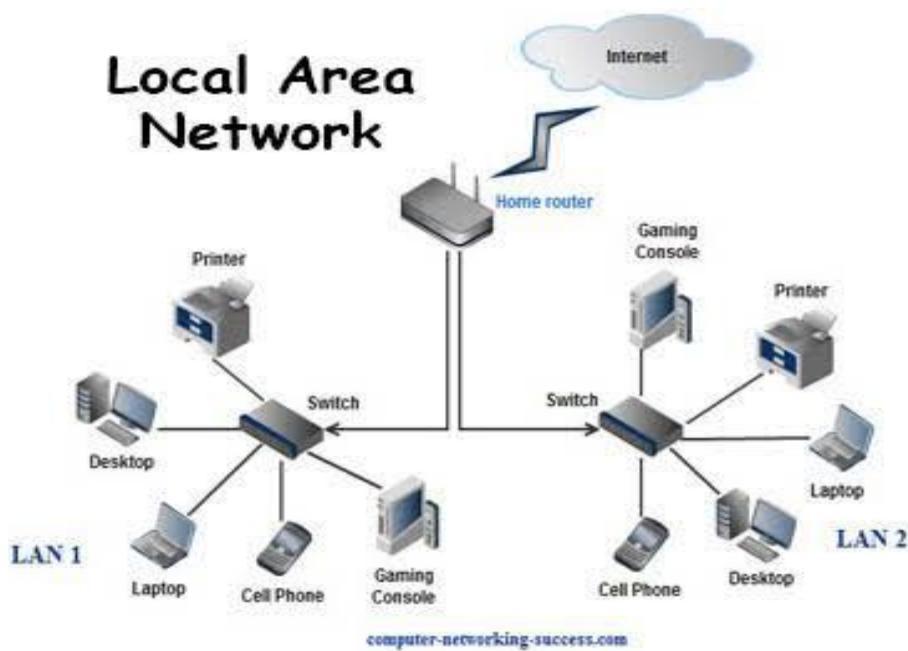
- There are many ways in which different networks can be classified, such as their size, capabilities and the geographical distance they cover. A network is simply a group of two or more computer systems linked together in some way so that they can share data between them. Different types of networks

provides different services, and require different things to work properly.

- Most network types are known as different types of ‘area’ networks- this is due to the history of networks, and dates back to the time when computer networks were defined by their literal scale. This is no longer always the case due to new technology. Some of the most common types of network you are likely to encounter are detailed here below:

- **LAN : Local Area Network**

This is one of the original categories of network, and one of the simplest. LAN network connect computers together over relatively small distances, such as within a single building or within a small group of building.

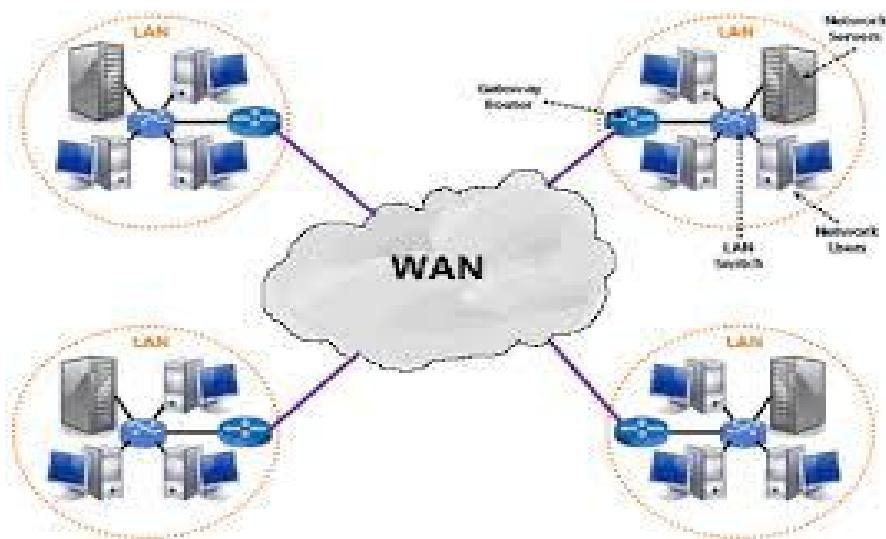


Homes often have LAN networks too, especially if there is more than one device in the home. Often they do not contain more than one subnet, if any, and are usually controlled by a single administrator. They do not have to be connected to the internet to work, although they can be.

- **WAN: Wide Area Network**

This is another of the original categories of network, and slightly more complex in nature. WAN networks connect computers together over large physical distances, remotely connecting them over one huge network and allowing them to communicate even when far apart. The Internet is

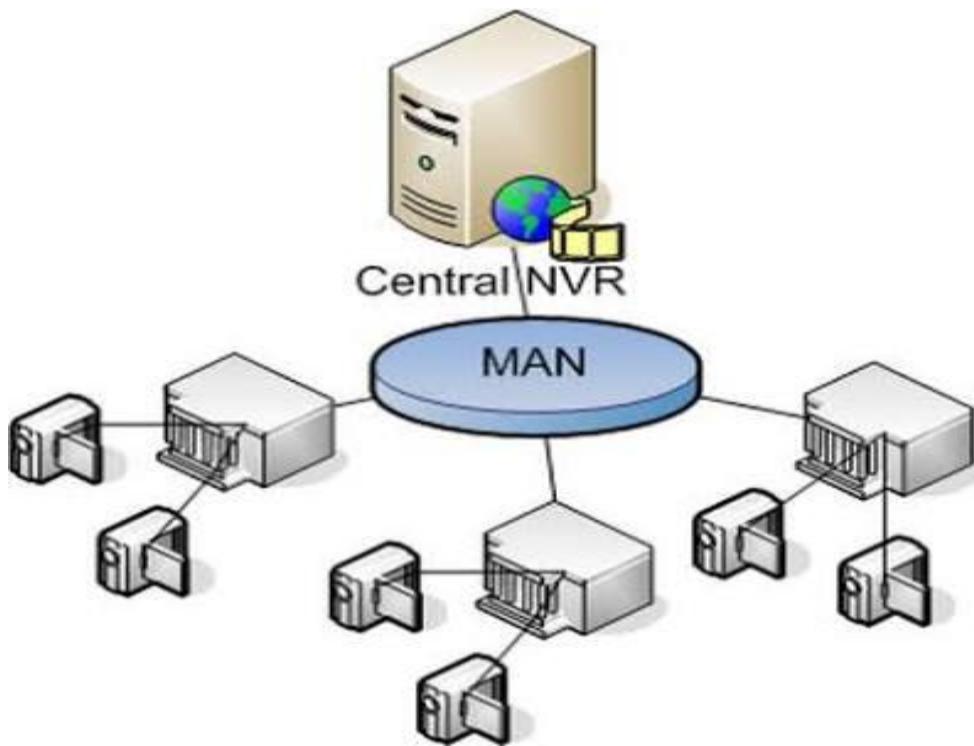
a WAN, and connects computer all around the world together.



LAN connect to WANs, such as the internet using routers to transfer data and information quickly and securely. WANs are usually too large to be controlled by one administrator, and so usually have collective ownership, or in the case of the internet, is publicly owned.

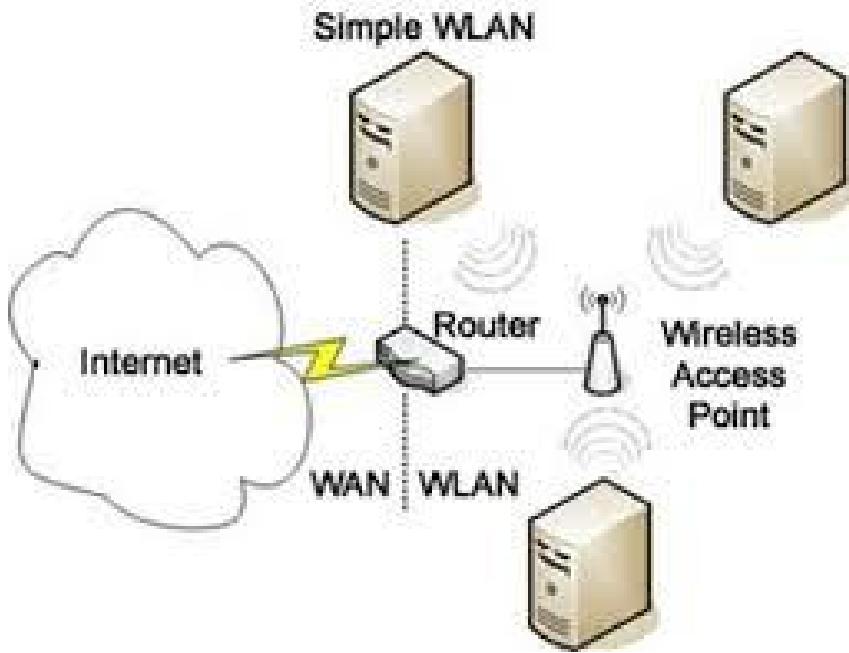
- **MAN: Metropolitan Area Network**

This is a network which is large than a LAN but smaller than a WAN, and incorporates elements of both. It typically spans a town or city and is owned by a single person or company, such as a local council or a large company.



- **WLAN : Wireless Local Area Network**

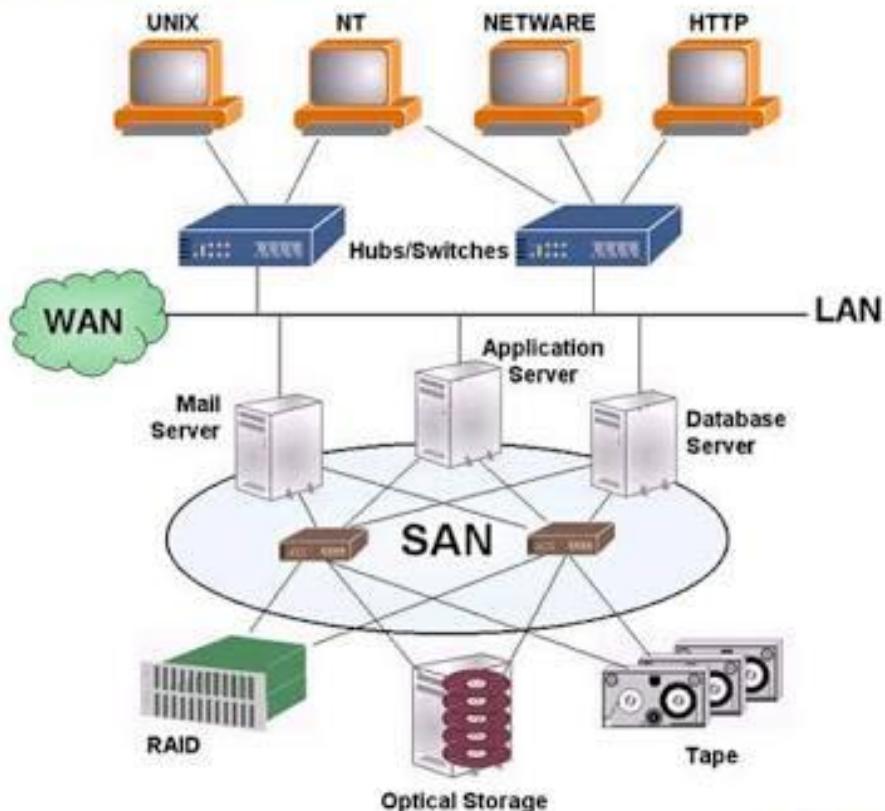
This is a LAN which works using wireless network technology such as Wi-Fi. This type of network is becoming more popular as wireless technology is further developed and is used more in the home and by small businesses. It means devices do not need to rely on physical cables and wires as much and can organise their space more effectively.



- **SAN: Storage Area Network**

This is a network that connects servers directly to devices which store large amounts of data without relying on a LAN or WAN network to do so. This can involve another type of connection known as Fibre Channel, a system similar to Ethernet which handles high-performance disk storage for applications on a number of professional networks.

④ Storage Area Networks



Source: eISAN Report 2001

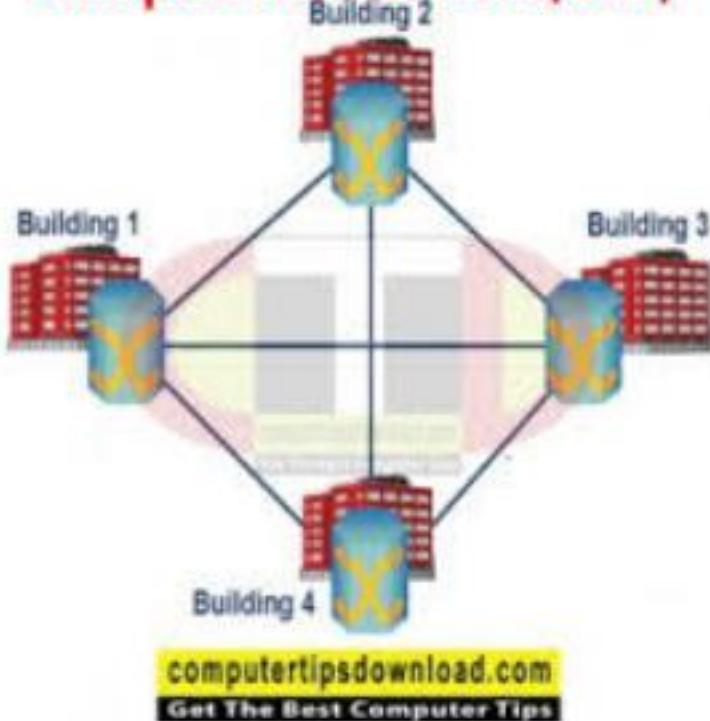
Copyright © 2000 eISAN.com Inc.



- **CAN: Campus Area Network**

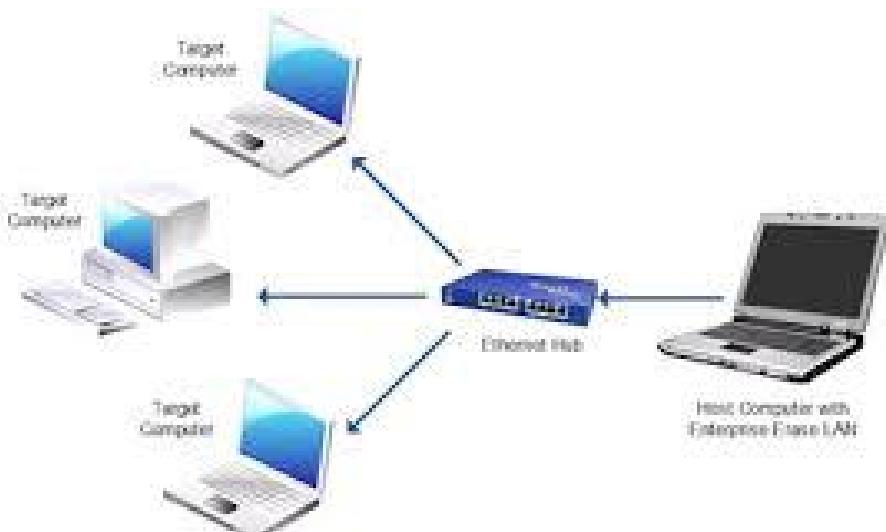
This is network which larger than a LAN, but smaller than MAN. This is typical in area such as a university, large school or small business. It is typically spread over a collection of buildings which are reasonably local to each other. It may have an internet Ethernet as well as capability of connecting to the internet.

Campus Area Network (CAN)



- **SAN: System Area Network**

This network connects computers together on an especially high-speed connection, in a configuration known as a cluster. This means computers which are connected together so as to work as a single system, and can be done as a result of very high speed computers and new low cost microprocessor. They are usually used to improve performance for cost effectiveness.

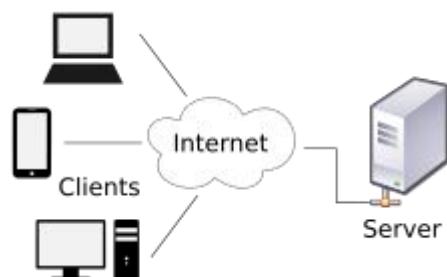


System Area Network - www.certiology.com

www.studytonight.com

1.6 - Client Server Model

From Wikipedia, the free encyclopedia



- A computer network diagram of clients communicating with a server via the Internet.
- The client–server model is a distributed application structure that partitions tasks or workloads between the providers of a resource or service, called servers, and service requesters, called clients.

- Often clients and servers communicate over a computer network on separate hardware, but both client and server may reside in the same system.
- A server host runs one or more server programs which share their resources with clients. A client does not share any of its resources, but requests a server's content or service function.
- Clients therefore initiate communication sessions with servers which await incoming requests.
- Examples of computer applications that use the client–server model are Email, network printing, and the World Wide Web.
- “The client-server model is a distributed application structure. That partitions tasks or workloads between the providers of a resource or service, called servers, and service requests, called CLIENT”
- A client is a program on the local machine requesting service from a server which means it is started by the user and terminates when the services is completed.
- A server is a program running on the remote machine providing service to the client.
- When it starts, it open the door for incoming requests from client ,but it never indicate a service unit it is requested to do so.
- A server program is an infinite program , when it starts , it runs infinitely unless a problem arises.

- It waits for incoming request from clients when a request arrives it respond to request.

Contents

1. Client and server role
2. Client and server communication
3. Example
4. History of Server Model
 - a. 4.1 Client-host and server-host
5. Centralized computing
6. Comparison with peer-to-peer architecture

1)Client and server role

- The *client-server* characteristic describes the relationship of cooperating programs in an application. The server component provides a function or service to one or many clients, which initiate requests for such services.
- Servers are classified by the services they provide. For example, a web server serves web pages and a file server serves computer files. A shared resource may be any of the server computer's software and electronic components, from programs and data to processors and storage devices. The sharing of resources of a server constitutes a *service*.
- Whether a computer is a client, a server, or both, is determined by the nature of the application that requires the service functions. For example, a single computer can run web server and file server

software at the same time to serve different data to clients making different kinds of requests. Client software can also communicate with server software within the same computer.^[2] Communication between servers, such as to synchronize data, is sometimes called *inter-server* or *server-to-server* communication.

2)Client and server communication

- In general, a service is an abstraction of computer resources and a client does not have to be concerned with how the server performs while fulfilling the request and delivering the response. The client only has to understand the response based on the well-known application protocol,
- i.e. the content and the formatting of the data for the requested service.
- Clients and servers exchange messages in a request-response messaging pattern. The client sends a request, and the server returns a response. This exchange of messages is an example of inter-process communication. To communicate, the computers must have a common language, and they must follow rules so that both the client and the server know what to expect.
- The language and rules of communication are defined in a communications protocol. All client-server protocols operate in the application layer. The application layer protocol defines the basic patterns of the dialogue. To formalize the data exchange even further, the server may implement an application programming interface (API).

- The API is an abstraction layer for accessing a service. By restricting communication to a specific content format, it facilitates parsing. By abstracting access, it facilitates cross-platform data exchange.^[4]
- A server may receive requests from many distinct clients in a short period of time. A computer can only perform a limited number of tasks at any moment, and relies on a scheduling system to prioritize incoming requests from clients to accommodate them.
- To prevent abuse and maximize availability, server software may limit the availability to clients. Denial of service attacks are designed to exploit a server's obligation to process requests by overloading it with excessive request rates.

3) Example

- When a bank customer accesses online banking services with a web browser (the client), the client initiates a request to the bank's web server. The customer's login credentials may be stored in a database, and the web server accesses the database server as a client.
- An application server interprets the returned data by applying the bank's business logic, and provides the output to the web server. Finally, the web server returns the result to the client web browser for display.
- In each step of this sequence of client–server message exchanges, a computer processes a request and returns data. This is the request-response messaging pattern. When all the requests are met,

the sequence is complete and the web browser presents the data to the customer.

- This example illustrates a design pattern applicable to the client–server model: separation of concerns.

4)History of Server Model

- An early form of client–server architecture is remote job entry, dating at least to OS/360 (announced 1964), where the request was to run a job, and the response was the output.
- While formulating the client–server model in the 1960s and 1970s, computer scientists building ARPANET (at the Stanford Research Institute) used the terms *server-host* (or *serving host*) and *user-host* (or *using-host*), and these appear in the early documents RFC 5 and RFC 4. This usage was continued at Xerox PARC in the mid-1970s.
- One context in which researchers used these terms was in the design of a computer network programming language called Decode-Encode Language (DEL).^[5] The purpose of this language was to accept commands from one computer (the user-host), which would return status reports to the user as it encoded the commands in network packets. Another DEL-capable computer, the server-host, received the packets, decoded them, and returned formatted data to the user-host.
- A DEL program on the user-host received the results to present to the user. This is a client–server transaction. Development of DEL was just beginning in 1969, the year that the United States Department of Defense established ARPANET (predecessor of Internet).

4-A)Client-host and server-host

Client-host and server-host have subtly different meanings than client and server. A host is any computer connected to a network. Whereas the words server and client may refer either to a computer or to a computer program, server-host and user-host always refer to computers. The host is a versatile, multifunction computer; clients and servers are just programs that run on a host. In the client–server model, a server is more likely to be devoted to the task of serving.

An early use of the word client occurs in "Separating Data from Function in a Distributed File System", a 1978 paper by Xerox PARC computer scientists Howard Sturgis, James Mitchell, and Jay Israel. The authors are careful to define the term for readers, and explain that they use it to distinguish between the user and the user's network node (the client).

5)Centralized computing

- Further information: History of personal computers, Decentralized computing, and Computer cluster
- The client–server model does not dictate that server-hosts must have more resources than client-hosts. Rather, it enables any general-purpose computer to extend its capabilities by using the shared resources of other hosts. Centralized computing, however, specifically allocates a large amount of resources to a small number of computers. The more computation is offloaded from client-hosts to the central computers, the simpler the client-hosts can be.

- It relies heavily on network resources (servers and infrastructure) for computation and storage. A diskless node loads even its operating system from the network, and a computer terminal has no operating system at all; it is only an input/output interface to the server. In contrast, a fat client, such as a personal computer, has many resources, and does not rely on a server for essential functions.
- As microcomputers decreased in price and increased in power from the 1980s to the late 1990s, many organizations transitioned computation from centralized servers, such as mainframes and minicomputers, to fat clients.^[11] This afforded greater, more individualized dominion over computer resources, but complicated information technology management.^{[10][12][13]} During the 2000s, web applications matured enough to rival application software developed for a specific microarchitecture. This maturation, more affordable mass storage, and the advent of service-oriented architecture were among the factors that gave rise to the cloud computing trend of the 2010s.^[14]

6)Comparison with peer-to-peer architecture

- In addition to the client–server model, distributed computing applications often use the peer-to-peer (P2P) application architecture.
- In the client–server model, the server is often designed to operate as a centralized system that serves many clients. The computing power, memory and storage requirements of a server must be scaled appropriately to the expected work-load (*i.e.*, the number of clients connecting simultaneously).

Load-balancing and failover systems are often employed to scale the server implementation.

- In a peer-to-peer network, two or more computers (peers) pool their resources and communicate in a decentralized system. Peers are coequal, or equipotent nodes in a non-hierarchical network. Unlike clients in a client–server or client–queue–client network, peers communicate with each other directly. In peer-to-peer networking, an algorithm in the peer-to-peer communications protocol balances load, and even peers with modest resources can help to share the load. If a node becomes unavailable, its shared resources remain available as long as other peers offer it. Ideally, a peer does not need to achieve high availability because other, redundant peers make up for any resource downtime; as the availability and load capacity of peers change, the protocol reroutes requests.
- Both client-server and master-slave are regarded as sub-categories of distributed peer-to-peer systems

Hybrid Network

Hybrid network based advertising system and method

... **Hybrid network based** advertising system and method US 20020082914 A1. Abstract. The invention relates to a ... ad planning server is operable to generate at least one report **based** on data ... that are available to **network** processing devices such as **network** servers, **peers** and/or ...

HyPO: A Peer-to-Peer based hybrid overlay structure

... Abstract-For supporting Peer to Peer (P2P) **based** live media streaming, a P2P overlay **network** should be ... In this paper, we have proposed a **Hybrid** P2P Overlay (HyPO) approach for live media ... The mesh overlay is organized by **peers** that have the similar bandwidth ranges in ...

A survey and comparison of peer-to-peer overlay network schemes

... is the number of **peers** in the system. The underlying **network** path between two **peers** can be significantly different from the path on the **DHT-based** overlay **network**. Therefore, the lookup latency in **DHT-based** P2P overlay ...

A genetic-algorithm-based neighbor-selection strategy for hybrid peer-to-peer networks

... In this paper we investigate the neighbor-selection problem in a **hybrid P2P network**. We model the **peers** as nodes in an undirected graph and try to determine the connections between them **based** on the proportion of contents one possesses, and the goal is to maximize the ...

Gossip-based search selection in hybrid peer-to-peer networks

... A **hybrid** peer-to-peer (P2P) search **network** combines an unstructured flooding **network** with a structured distributed hash table (DHT)-**based** global index [1,2]. In such networks, partial keyword queries can either be flooded to all **peers**, or the set of **peers** storing documents ... 43-50 are block diagrams illustrating portions of the **hybrid network** in accordance with a ... 52A-52C illustrate **network** block diagrams in connection with a dial-in environment in ... 76 illustrates the operation of a computer-**based** voice gateway for selectively routing telephone calls ...

Hybrid CDN-P2P architectures for live video streaming: Comparative study of connected and unconnected meshes

... This paper is compared the performance of two main **hybrid** CDN-P2P architectures includes: (i ... node, and (ii) CDN-P2P connected mesh in which

CDN nodes and **peers** participate in ... The comparison is preformed in addition, to the pure mesh-based P2P video streaming, using ...

Service level management in a hybrid network architecture

... 2A is a flowchart showing illustrating media communication over a **hybrid network** in accordance with a ... The **network** will be required to provide more direct access to all **peers** wishing to ... Text files and images can be sent over existing packet-based networks because the delivery ...

Providing collaborative installation management in a network-based supply chain environment

... 11 illustrates a flowchart for a methodology for providing maintenance and service in a **network-based** supply chain in accordance with an embodiment ... 27 is a flowchart showing illustrating media communication over a **hybrid network** in accordance with a preferred ...

www.ecomputernes.com

1.7 - NETWORK TOPOLOGY

--> Computers in a network have to be connected in some logical manner. The layout pattern of the interconnections between computers in a network is called network topology. You can think of topology as the virtual shape or structure of the network. Network topology is also referred to as 'network architecture'.

--> Two Types of Network Topology

1. Point-to-Point Network Topology

2. Multipoint Network Topology

1. Point-to-Point Network Topology :

--> Point-to-point topology is the simplest of all the network topologies. The network consists of a direct link between two computers. This is faster and more reliable than other types of connections since there is a direct connection. The disadvantage is that it can only be used for small areas where computers are in close proximity.

2. Multipoint Network Topology :

--> A connection of a number of terminals in parallel, analogous to a multidrop connection. Sometimes the terms are used synonymously, although multidrop strictly implies that the connections are all served from a common connection point (node), whereas multipoint implies that connections are made through a series of (analog) bridging connections where some or all of the terminals are served by different common carrier offices interconnected by communication trunks.

Types Of Topology

- 1 . Mesh
- 2 . Star
- 3 . Ring
- 4 . BUS
- 5 . Hybrid
- 6 . Tree

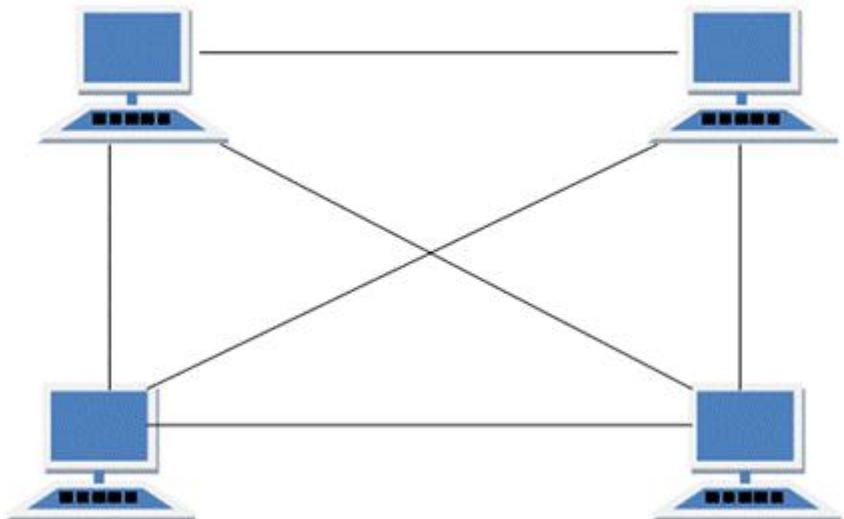
1 . Mesh

--> In mesh topology, every node has a direct point-to-point connection to every other node. Because all connections are direct, the network can handle very high-volume traffic. It is also robust because if one connection fails, the others remain intact. Security is also high since data travels along a dedicated connection.

Advantages of Mesh Topology:

Each connection can carry its own data load.

1. It is robust.
2. fault diagnosed easily.
3. provides security and privacy.



DisAdvantages of Mesh Topology

1. Installation and configuration is difficult.
2. Cabling cost is more.
3. Bulk wiring is required.

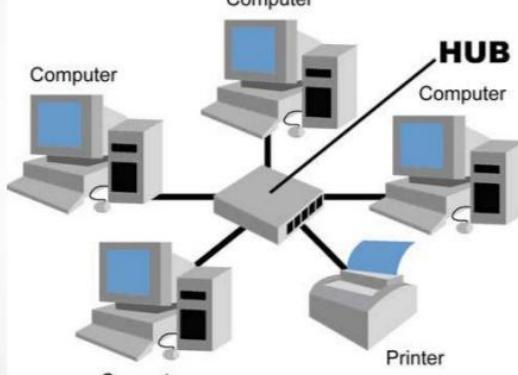
2 . Star :

--> In star topology, each computer is connected to a central hub using a point-to-point connection. The central hub can be a computer server that manages the network, or it can be a much simpler device that only makes the connections between computers over the network possible.

Advantages of Star Topology:

1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.

Star Topology



Disadvantages of Star Topology:

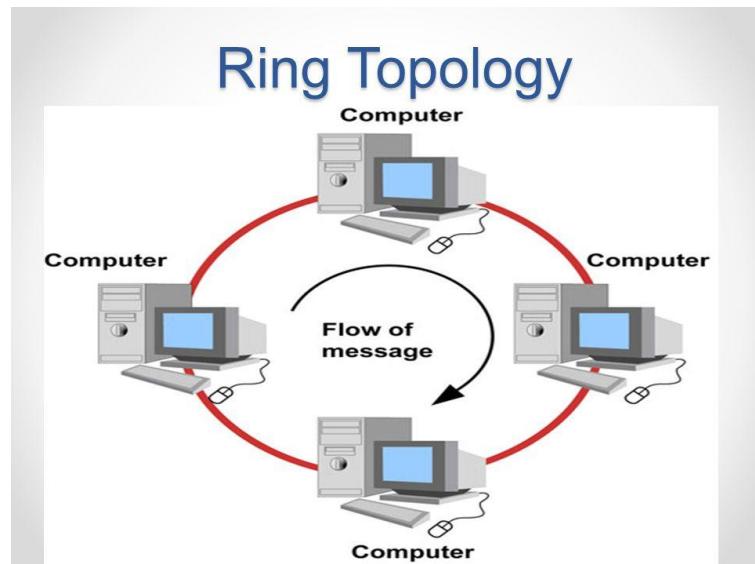
1. Cost of installation is high.
4. Expensive to use.
5. If the hub fails then the whole network is stopped because all the nodes depend on the hub.
6. Performance is based on the hub that is it depends on its capacity

3 . Ring :

--> In ring topology, the computers in the network are connected in a circular fashion, and the data travels in one direction. Each computer is directly connected to the next computer, forming a single pathway for signals through the network. This type of network is easy to install and manage.

Advantages of Ring Topology:

1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand



DisAdvantages of Ring Topology:

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

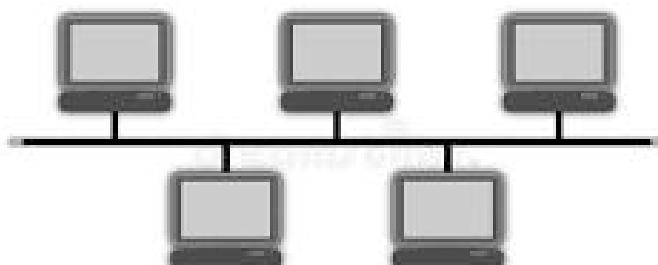
4 . BUS :

--> Bus topology uses one main cable to which all nodes are directly connected. The main cable acts as a backbone for the network. One of the computers in the network typically acts as the computer server. The first advantage of bus topology is that it is easy to connect a computer or peripheral device. The second advantage is that the cable requirements are relatively small, resulting in lower cost.

Advantages of BUS Topology:

1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.

Bus Topology



Disadvantages of BUS Topology:

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance

of the network decreases.

3. Cable has a limited length.
4. It is slower than the ring topology.

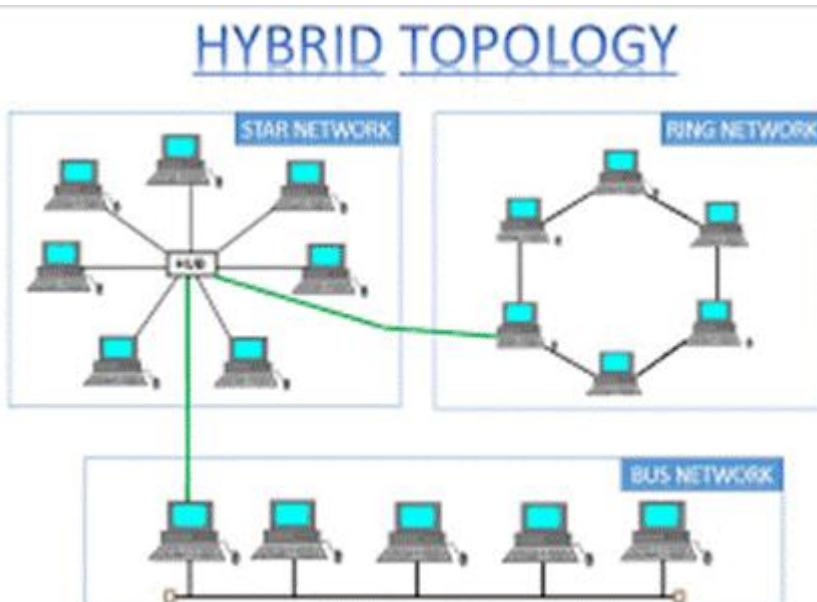
5 . Hybrid :

A hybrid topology uses a combination of two or more topologies. Hybrid networks provide a lot of flexibility, and as a result, they have become the most widely used type of topology. Common examples are star ring networks and star bus networks. Tree topology is one specific example of a star bus network.

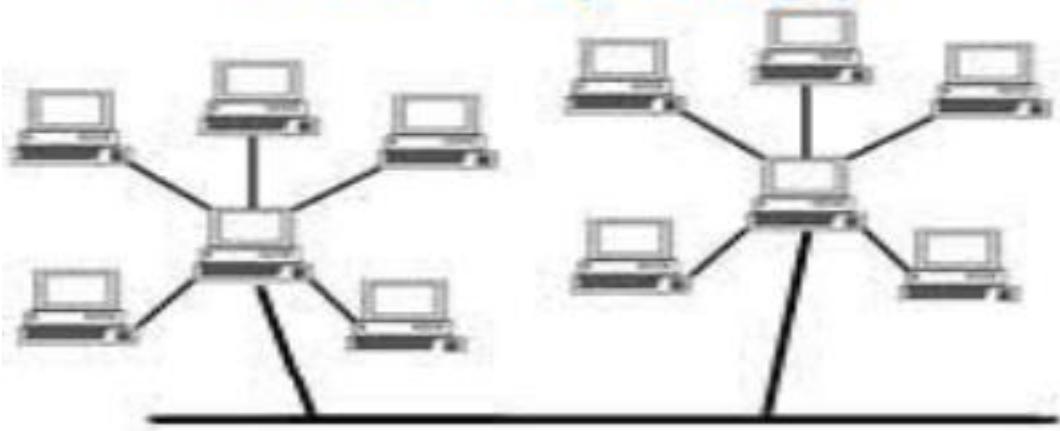
Advantages of Hybrid Topology:

1.

Reliable as
Error detect
ing and
trouble
shooti
ng is
easy.



Tree Topology



ComputerHope.com

e.

3. Scalable as size can be increased easily.
4. Flexible.

Disadvantages of Hybrid Topology:

1. Complex in design.
2. Costly.

6 . Tree :

--> Tree topology combines multiple star topologies onto a bus. Hub devices for each star topology are connected to the bus. Each hub is like the root of a tree of devices. This provides great flexibility for expanding and modifying the network.

Advantages of Tree Topology:

1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.
3. Easily managed and maintained.
4. Error detection is easily done.

Disadvantages of Tree Topology:

1. Heavily cabled.
2. Costly.
3. If more nodes are added maintenance is difficult.
4. Central hub fails, network fails.

www.studytonight.com

1.8 - Review of Protocols

Definition of Protocol

--> A network protocol defines rules and conventions for communication between network devices.

--> Network protocols include mechanisms for devices to identify and make connections with each other, as well as formatting rules that specify how data is packaged into messages sent and received.

--> Some protocols also support message acknowledgment and data compression designed for

reliable and/or high performance network communication.

Types of Protocol

There are different types of protocol such as:

1. Transmission Control protocol(TCP)
2. Internate Protocol(IP)
3. Internet Address Protocol(IP Address)
4. Post Office Protocol(POP)
5. Simple Mail Transport Protocol(SMTP)
6. File Transfer protocol(FTP)
7. Hyper Text Transfer Protocol(HTTP)
8. Ethernet
9. Telnet
- 10.Gopher

Purpose of Network Protocols:-

Without protocols, devices would lack the ability to understand the electronic signals they send to each other over network connection. Network protocols serve these basic function:

- >Address data to the correct recipient(s)
- >Physically transmit data from source to destination, with security protection if needed
- >Receive messages and send responses appropriately

Layers of Protocols

The protocol can be specified into four layers to help identify some of the protocols with which you should be familiar (see the fig).

Fig OSI model related to common network protocols.

Figure illustrates how some of the major protocols would correlate to the OSI model in order to communicate via the Internet.

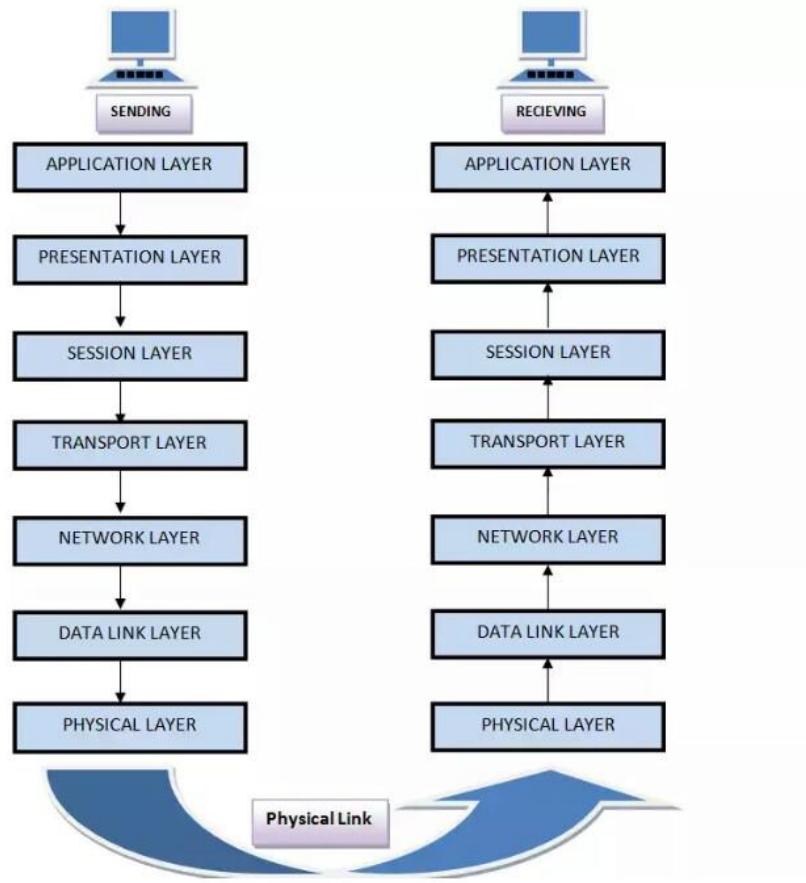
In this model, there are four layers, including:

1. Ethername(Physical/Data Link Layers)
2. IP/IPX(Network Layer)
3. TCP/SPX(Transport Layer)
4. HTTP,FTP,Telnet,SMTP and DNS(Combined Session/Presentation/Application Layers)

www.Indiastudychannel.com

1.9 - OSI MODEL

- There are N number of users who use computer network and are located over the world.
- So to ensure, national and worldwide data communication, systems must be developed which are compatible to communicate with each other.
- IOS has developed this. IOS stands for International Organization of Standardization.
- This is called a model for Open System Interconnection(OSI) and is commonly known as OSI model.
- This OSI model is a seven layer architecture.
- It defines seven layer or levels in a complete communication system.



Feature of OSI Model:-

1. Big picture of communication over network is understandable through this OSI model.
2. We see how hardware and software work together.
3. We can understand new technologies as they are developed.
4. Troubleshooting is easier by separate networks.
5. Can be used to compare basic functional relationship on different networks.

Function of Different Layers:-

Layer 1: The Physical Layer:-

1. It is the lower 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. Voltage and data rates needed for transmission is defined in the physical layer.
5. It converts the digital/analog bit 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 acknowledgement 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 frames 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 rout 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 signal 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 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 application.
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 the receiver will understand the information 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 can be different of the two communication 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 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 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.

1.10 - Transport Control Internet Protocol

The history of TCP/IP:-

- The Defense Advanced Research Projects Agency (DARPA), the research branch of the U.S. Department of Defense, created the TCP/IP model in the 1970s for use in ARPANET, a wide area network that preceded the internet.

- TCP/IP was originally designed for the Unix operating system, and it has been built into all of the operating systems that came after it.
- TCP (Transmission Control Protocol) is a standard that defines how to establish and maintain a network conversation via which application programs can exchange data.
- TCP works with the Internet Protocol (IP), which defines how computers send packets of data to each other.
- Together, TCP and IP are the basic rules defining the Internet.

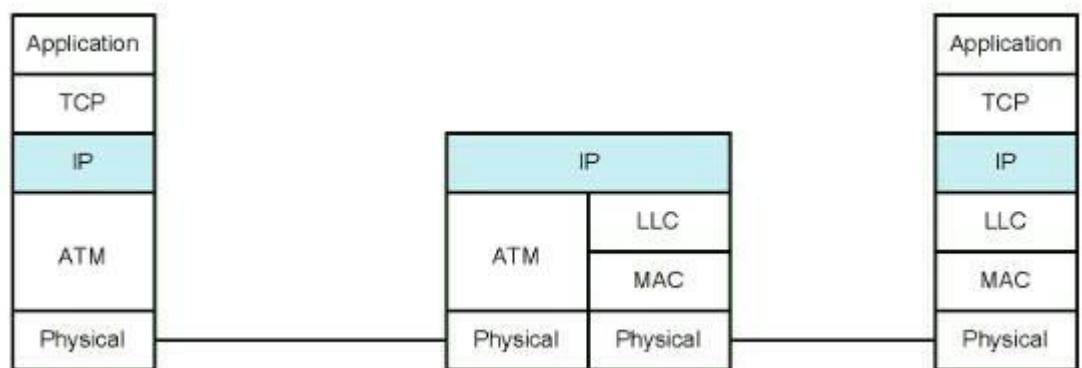
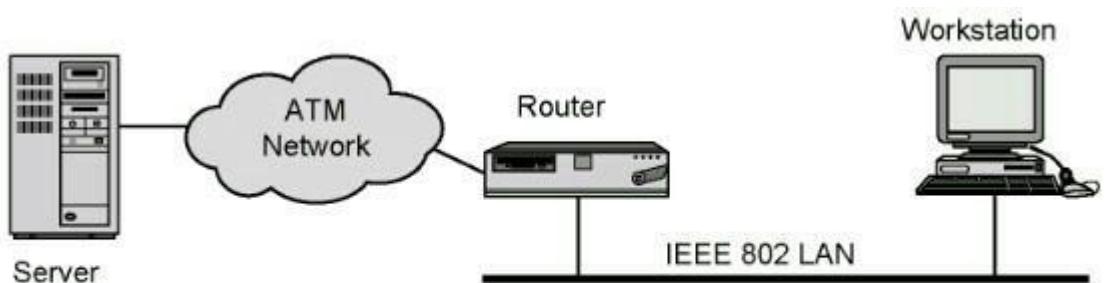
TCP/IP Protocol Suite :-

- The internet protocol suite is unique in that it is made up of non proprietary protocols.
- This means they do not belong to any one company and that technology is available to anyone who wishes to use it.
- The internet protocol suite was defined as its own model, so it is known as Internet model or Department of Defense Model.
- Both TCP and IP, two separate protocols that work hand-in-hand, perform chores that

manage and guide the general mobility of data packets over the Internet.

- They both use special headers that define each packet's contents and, if there is more than one, how many others should be expected.
- TCP concerns itself with making the connections to remote hosts. IP, on the other hand, deals with addressing so that messages are directed to where they are intended.

Configuration of TCP/IP Protocol:-



TCP/IP also has the following characteristics:-

- Good failure recovery
- The ability to add networks without interrupting existing services
- High error-rate handling
- Platform independence
- Low data overhead

How TCP/IP works:-

- TCP/IP uses the client/server model of communication in which a user or machine (a client) is provided a service (like sending a webpage) by another computer (a server) in the network.
- Collectively, the TCP/IP suite of protocols is classified as stateless, which means each client request is considered new because it is unrelated to previous requests. Being stateless frees up network paths so they can be used continuously.
- The transport layer itself, however, is stateful.
- It transmits a single message, and its connection remains in place until all the packets in a message have been received and reassembled at the destination.

- The TCP/IP model differs slightly from the seven-layer Open Systems Interconnection (OSI) networking model designed after it, which defines how applications can communicate over a network.

Advantages of TCP/IP:-

- TCP/IP is nonproprietary and, as a result, is not controlled by any single company. Therefore, the internet protocol suite can be modified easily.
- It is compatible with all operating systems, so it can communicate with any other system.
- The internet protocol suite is also compatible with all types of computer hardware and networks.
- TCP/IP is highly scalable and, as a routable protocol, can determine the most efficient path through the network.

TCP always guarantees three things - your data reaches its destination, it reaches there in time and it reaches there without duplication.

- It automatically breaks up data into packets for you.

- Disadvantages of TCP/IP:-
- Transmission Control Protocol/Internet Protocol, are its size and its speed.
- TCP cannot be used for broadcast and multicast connections

<https://googleweblight.com/i?u=https://technet.microsoft.com/en-us/library/bb726993.aspx&grqid=kxORPHMH&hl=en-IN>

Subject : Computer Networks

Chapter : 2. The OSI Model

Faculty : Devendra G. Pandey sir

Sem. : 3th

Div. : A

Roll No.	Name	Work
15 4)	Dhankecha Parth	(2.3) (1 to
16	Dobariya Priyank	(2.2)
35 7)	Kalathiya Divyesh	(2.3) (5 to
39	Kanthariya Chaitanya	(2.1)

2. The OSI Model

THE OSI MODEL

2.1 Layer architecture

2.2 OSI model

2.3 The OSI model layer functions

2.1 Layer architecture

LAYERED ARCHITECTURE:

The OSI model is consist of seven layer which are:-

Layer 1: Physical

Layer 2: Data link

Layer 3: Network

Layer 4: Transport

Layer 5: Session

Layer 6: Presentation

Layer 7: Application

When the message is sent from device A to device B, it can travels through many intermediate node but usually it uses the first three layer only.

For Single Machine:- It calls the service of a layer which is just below of it.

Eg: Layer 3 uses the service provided by layer 2.

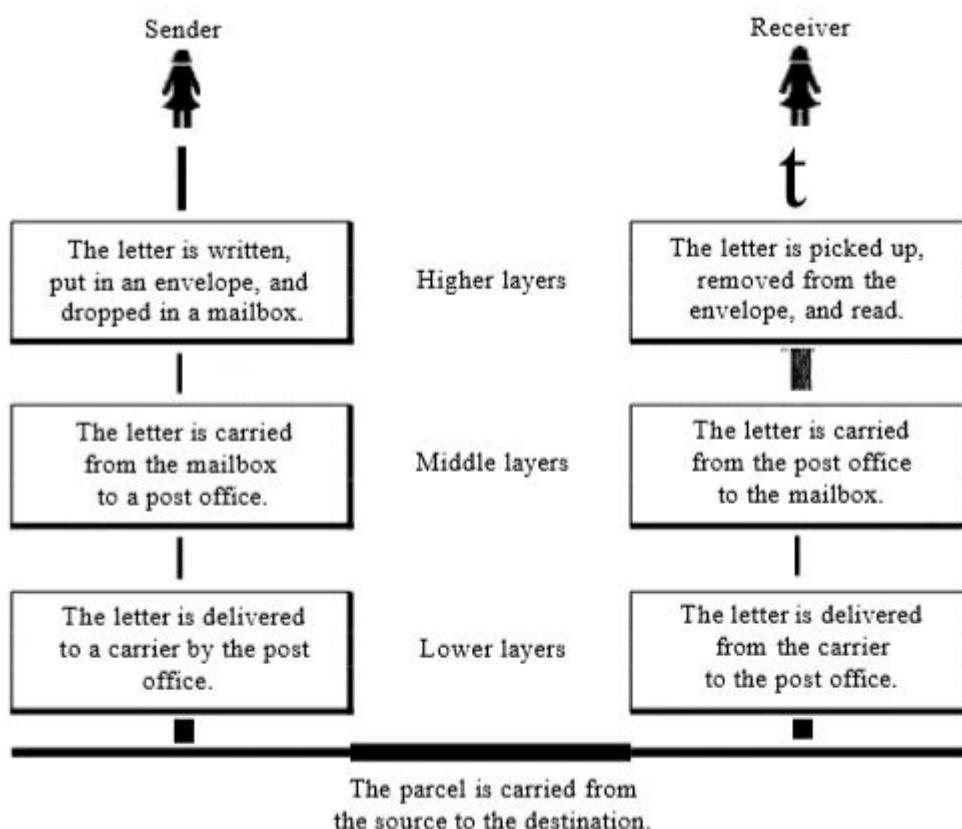
For Multiple Machines:- It communicates to the same layer agreed upon series of rules which is also called as protocols.

Eg: Device A at x layer communicate with Device B at x layer.

The process on machine-machine communicate at the same layer is called peer to peer process.

Image Reference :

http://3.bp.blogspot.com/-O271b_XFPnY/VNoE4vUSyxl/AAAAAAAABg/HnxpWDQoAPM/s1600/task-layer-condt.png



Peer to Peer Process:-

The network layer provides a service to the transport layer. And the transport layer present data to the internetwork sub system. The network layer has the task of moving the data through the internetwork. it accomplishes this task by encapsulating the data and attaching a header creating a packet(the layer 3 PDU). The header contains information required to complete the transfer. Such as source and destination logical address.

At Physical level: The communication is direct.

Eg .: device A sends the data to Device B(through intermediate node).

At Higher layer: Each layer adds its own information to the message from the above layer and sends the whole package to the layer which is below it.

Eg .: layer 2 takes the data which is mean to it and then transfer the rest of the data to layer 3 , similarly all the layer follows the process.

Encapsulation: the data or information which are in the form of packet are fully transfer to one Level to another level is called and encapsulation

Eg. : the packet at level (N -1) there is the whole data from level N

An exchange using the OSI model

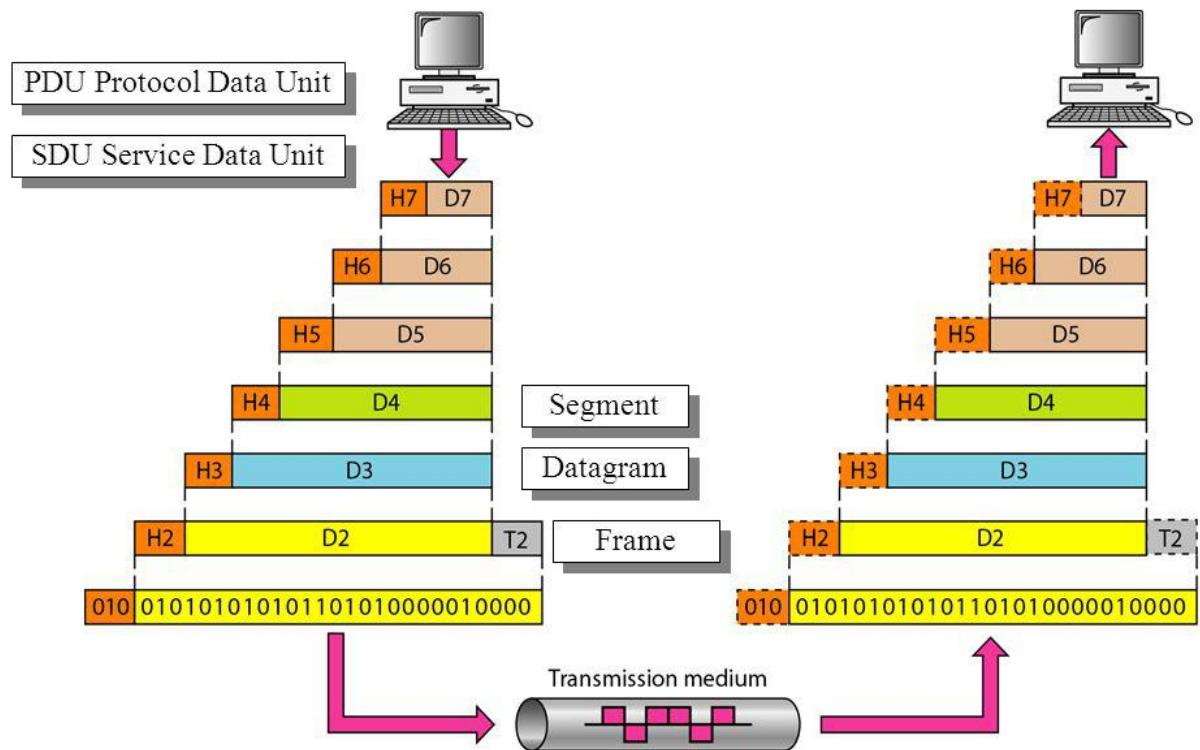


Image:

<http://slideplayer.com/slide/9036097/27/images/10/An+exchange+using+the+OSI+model.jpg>

Interfaces between two layers:-

The passing of the data and network information down through the layer of the sending Machine and back up through the layers of receiving machine is made possible by an interface between each pair of adjacent layers.

Each interface defines what information and services a Layer must provide for the layer above it. Well-defined interface and layer function provide modularity to a network.

Reference :

Content line :

The Data Communication and Networking (4th edition) Page : 29

2.2 OSI MODEL

Shortcut to Remember all layers :

Application layer	All
Presentation layer	People
Session layer	Study
Transport layer	To
Network layer	Not
Data Link layer	Do
become	
Physical layer	Problem
builder	

OSI MODEL : (OPEN SYSTEM INTERCONNECTION)

- The process starts out at layer 7 and then moves all layers (layer to layer) in descending order.
- Except Layer 7 and 1 all layer a header is added to the data unit .

- When the formatted data passes through the physical layer it is changed into an electromagnetic signals link.
- At layer 2 trailer is added .
- The signal passes into layer 1 and is transformed back into bits.
- The data units then move back up through the OSI layer.
- AS each block of data reaches to next higher layer , the header and trailers attached to it at the corresponding sending layers are removed and application appropriate to the layer taken.
- At last it reaches layer 7 (Application layer) the message is again in a form appropriate to the application and its made available to the recipient.

Physical layer:

- Physical layer coordinates the function required to transmit a bit stream over a physical media.
- This layer use to provide transmission medium and devices .

Data Link layer:

- The data link layer or layer 2 is the second layer of the seven-layer OSI model of computer networking.
- This layer is the protocol layer that transfers data between adjacent network nodes in a wide area network (WAN) or between nodes on the same local area network (LAN) segment.

Network Layer:

- The network layer is responsible for the source to destination delivery of a packet possibly across multiple network .
- If two links are connected to the same link there is no need of Network layer.

Transport layer:

- The transport layer is responsible for source to destination delivery of entire message.
- Network layer work on end to end delivery of individual packets it does not recognize any relationship between those packets.
- Transport layer work on the whole message arrives in that and in-order.

Session layer:

- The services provided by the first three layers are not sufficient for some process.
- The session layer is the network dialog controller which establishes, maintains and synchronizes the interaction between communicating systems.

Presentation layer:

- The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.

Application layer:

- The application layer enables user to access the network.
- It provides interface and support for services such as electronic mail, remote file access and transfer, shared database management and other types of distributed information services.

Reference :

The Data Communication and Networking (4th edition)
page :30 to 33

Layer	Function	Example
Application (7)	Services that are used with end user applications	SMTP,
Presentation (6)	Formats the data so that it can be viewed by the user Encrypt and decrypt	JPG, GIF, HTTPS, SSL, TLS
Session (5)	Establishes/ends connections between two hosts	NetBIOS, PPTP
Transport (4)	Responsible for the transport protocol and error handling	TCP, UDP
Network (3)	Reads the IP address from the packet.	Routers, Layer 3 Switches
Data Link (2)	Reads the MAC address from the data packet	Switches
Physical (1)	Send data on to the physical wire.	Hubs, NICs, Cable

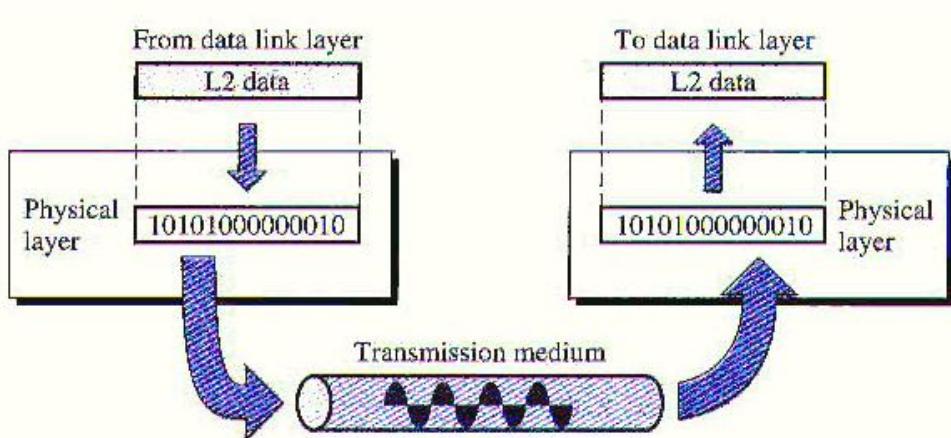
Image reference :

<http://certbros.com/wp-content/uploads/2015/01/OSI-Model.png?x61375>

2.3 Function in OSI model

1. PHYSICAL LAYER :-

**Physical layer is a lowest layer of OSI layer.
Physical layer deals with communication media. It perform the task to carry a bit stream over a physical transmission medium.**



Functions performed by physical layer are as follows:

1. Physical characteristics of medium
2. Representation of bits
3. Data rate
4. Line configuration
5. Physical topology
6. Transmission mode

1. Physical characteristics of medium

It defines the physical characteristics of interface means transmission medium between two device. It also defines the type of transmision medium.

2. Representation of bits

Data obtained by physical layer is in a bit-stream(0s & 1s) with no interpretation. To transpot the data through medium it convert it into electrical signals sothat it transfer through phyical medium.

3. Data rate

Physical layer defines the duration of bits means that the number of bits sent each second is called data rate of transmission.

4. Line configuration

It also depend on the connection of devices to the media. It likes the point-to-point configuration,multipoint configuration.

5. Physical topology

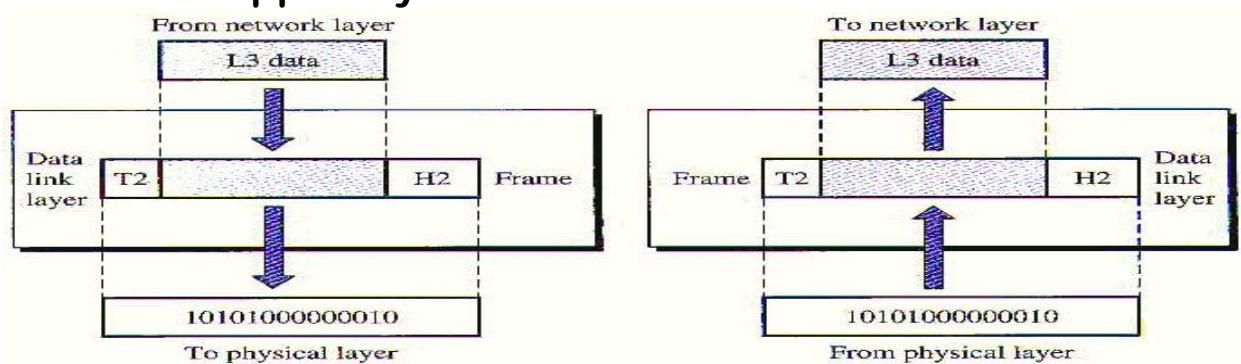
Physical topology defines how the devices are connected to each other. Device can be connected using mesh topology, star topology, ring topology ,bus topology ,hybrid topology.

6. Transmission medium

It also defines the transmission mode means direction between two device is like simplex ,half duplex, or full duplex.

2. Data Link Layer

Data link layer is responsible for delivering of the data from one device to another device without any error. It make the physical layer appear error-free to the upper layer.



Responsibilities of Data Link Layer:-

1. Framing
 2. Physical addressing
 3. Flow control
 4. Error control
 5. Access control
1. Framing

Data unit with additional information is called a frame. It divides the stream of bits into manageable frame.

2. Physical addressing

Data link layer adds the header to the stream to define the the sender and receiver of the frame so that it will send to the right destination.

3. Flow control

If the data rate of the receiver's machine is less than the data rate of sender machine then it will control the flow of data.

4. Error control

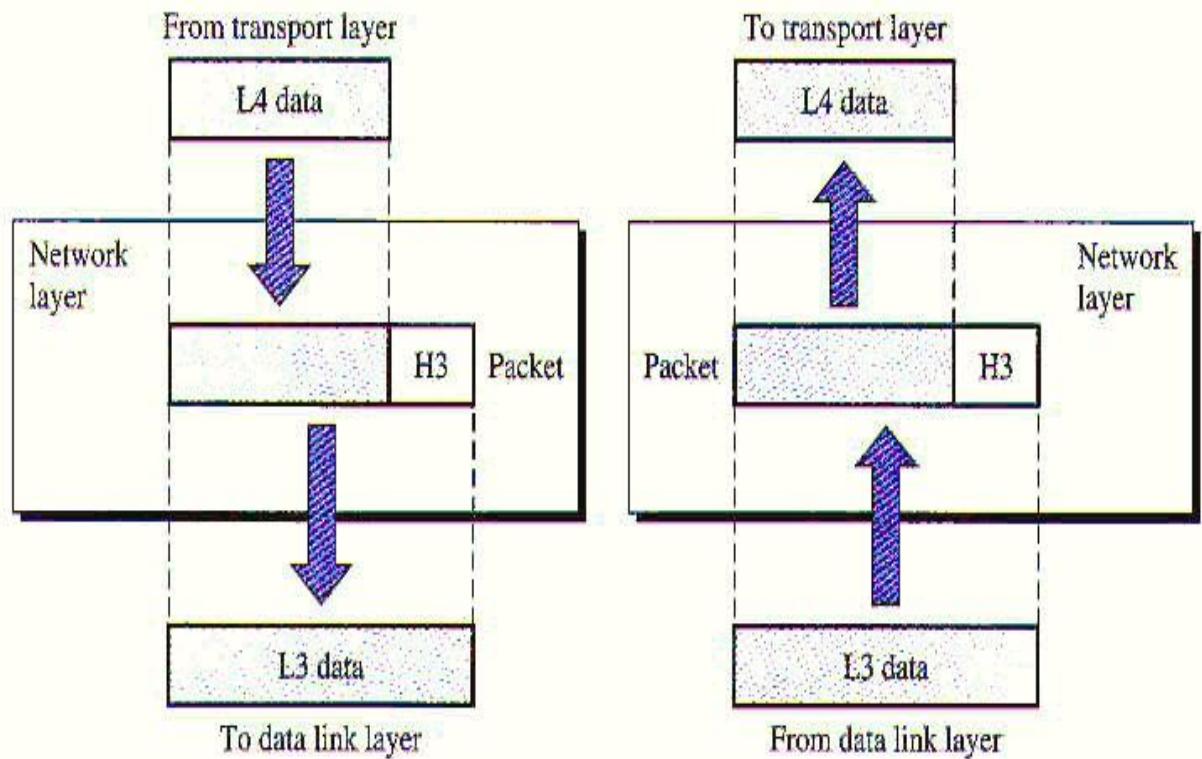
It adds the functionality to physical layer to detect error and retransmit the lost frames. It is achieved by adding the trailer to the frame.

5. Access control

When two or more devices are connected to the same link,it determines which device has control over the link at any given time.

3. Network Layer

The nework layer is responsible for source-to-destination delivery of a data across multiple links. When a message must be routed to other connected networks, the network layer has access to lookup tables to at various sites along the way to assist in addressing a packet to the next node in the chosen route.



Responsibilities of Network Layer:-

1. Logical Addressing
2. Routing
3. Multiplexing

1. Logical addressing

Physical addressing is implemented at data link layer to handle the addressing problem locally. If the packet passes the network boundary, it needs another addressing to distinguish source and destination. For this addressing network layer is included the headers to the packet coming from the upper layer which includes the logical address of sender and receiver.

2. Routing

When independent networks or links are connected to create internetwork, the connecting devices (called routers or switches) route or switch the packets to their final destination. One of the

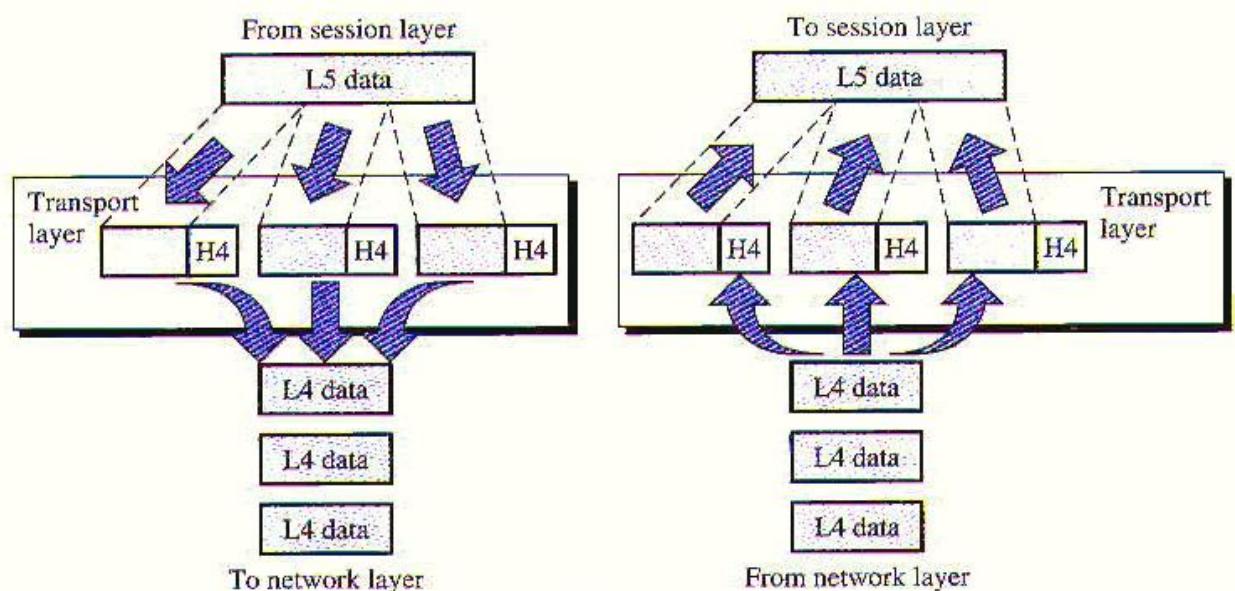
functions of the network layer is to provide this mechanism.

3. Multiplexing

It uses one physical line to carry data between many devices.

4. Transport Layer

The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on a host. By comparison, the network layer was responsible for the end-to-end delivery of individual packets only. The transport layer ensures that individual packets making up a message arrive in order and in the same condition that they were sent.



Responsibilities of transport layer:-

1. Service-point addressing
2. Segmentation
3. Synchronization
4. Flow control
5. Error control

1. Service-point addressing

Computers often runs several program at same time. So, end-to-end means delivery from a specific process on one computer to a specific process on other. It include a type of address called a service-point-address. So, it get packets at correct destination.

2. Segmentation

A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.

3. Flow control

Like a data link layer the transport layer is also responsible for flow control. However, flow control at this layer is performed end to end rather than across single link.

4. Error control

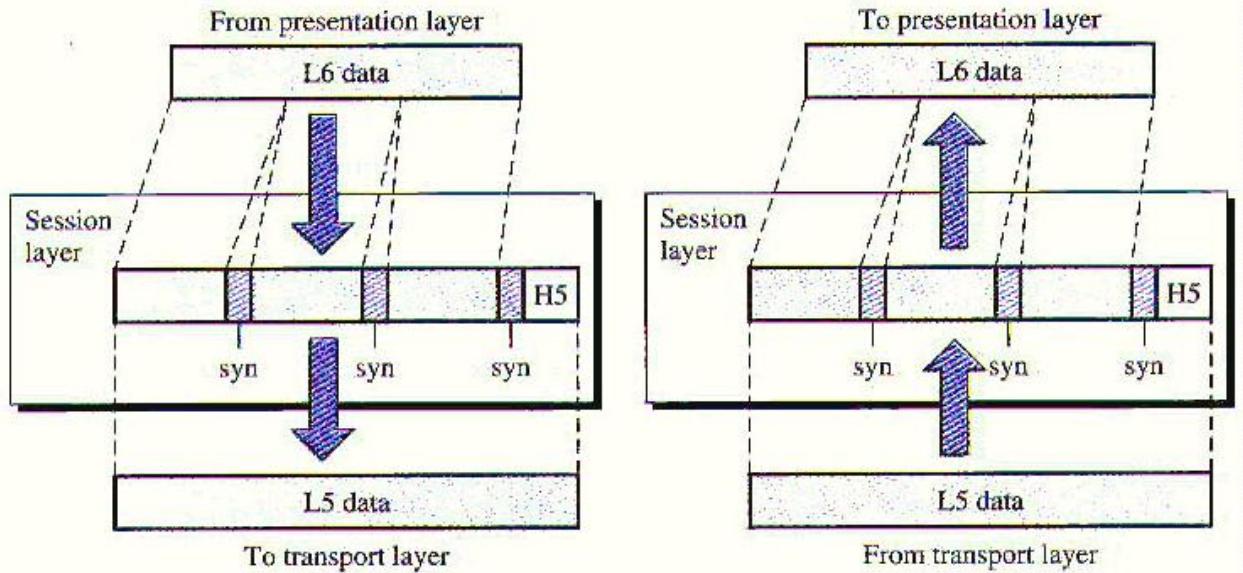
Error control at this layer is process-to-process. The sending treansport layer makes sure that the entire message arrives at the receiving transport layer without error. Error correction is usually achieved through retransmission.

5. Session Layer

The session layer is the ***network dialog controller***. It is responsible for establishing, maintaining and synchronizing the interaction between communicating devices. When communication or a sub-part is finished, the session layer ensures that each session closes gracefully

rather than abruptly causing the communication programs to hang.

The session layer is responsible for dialog control and synchronization.



The specific responsibilities of session layer include the following:

1. Dialog control
2. Synchronization

1. Dialog control

The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either halfduplex(one way at a time) or full-duplex (two ways at a time) mode.

2. Synchronization

The session layer allows a process to add checkpoints, or synchronization points, to a stream of data. For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case,

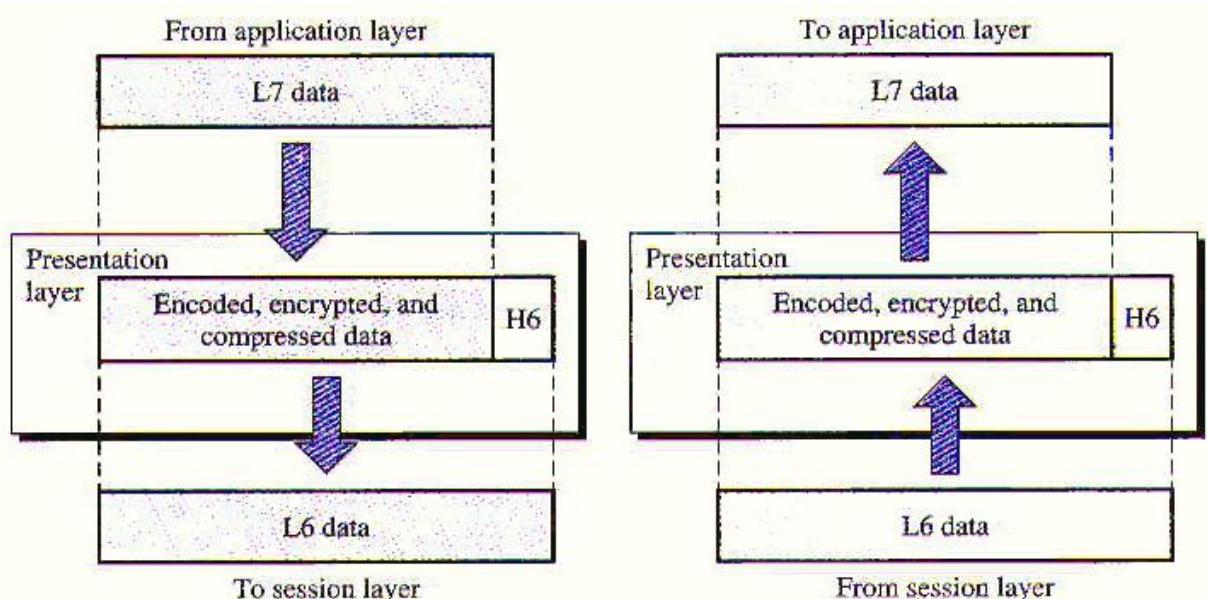
if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent.

6. Presentation Layer

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems. The presentation layer ensures interoperability between communicating devices.

Responsibilities of presentation layer are as following:

- 1. Translation**
- 2. Encryption**
- 3. Compression**



1. Translation

The information must be changed to bit stream before being transmitted. Different computers

have different encoding system. So, presentation layer at sender change information from its dependent format and at receiver change it from its dependent format.

2. Encryption

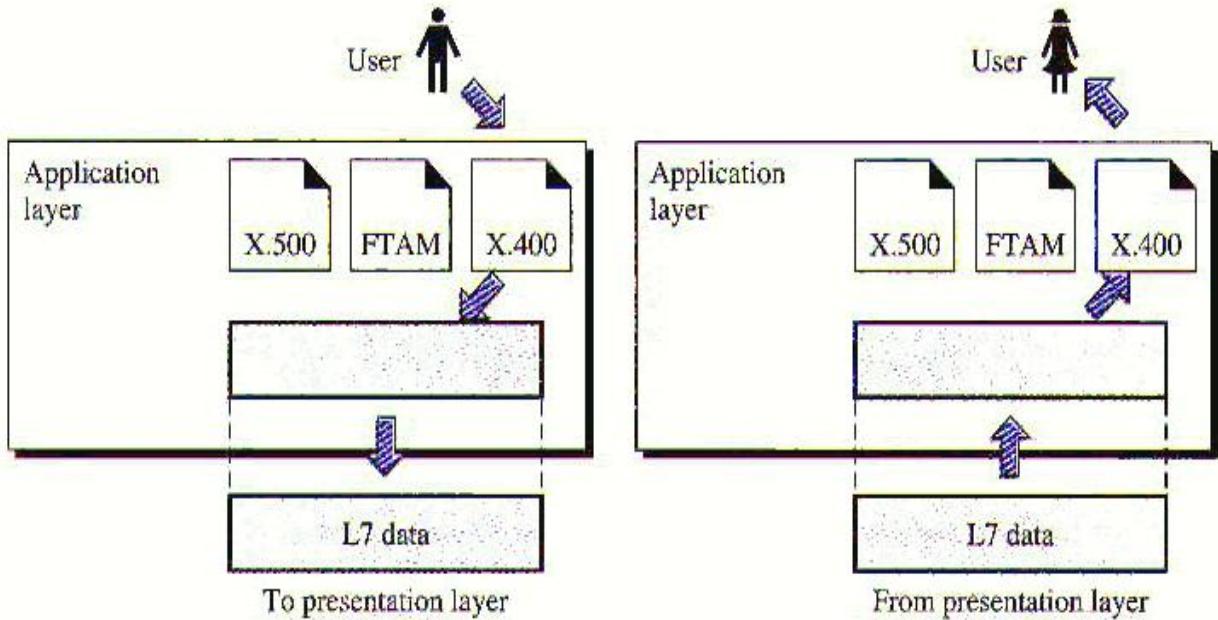
To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.

3. Compression

Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

7. Application Layer

The application layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer.



The application layer is responsible for providing service for user.

Responsibilities of application layer:-

- 1. Network virtual terminal**
- 2. File transfer,access, and management**
- 3. Mail Services**
- 4. Directory services**

1. Network virtual terminal

It is a software version of a physical terminal, and it allows a user to log on to a remote host. It is an interface which is intermediate between user and network for communicating with user.

2. File transfer,access, and management

This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.

3. Mail services

This application provides the basis for e-mail forwarding and storage.

4. Directory services

This application provides distributed database sources and access for global information about various objects and services.

References:-

- 1. http://ru6.cti.gr/bouras-old/WP_Simoneau_OSIModel.pdf**
- 2. <http://www.computernetworkingnotes.com/ccna-study-guide/osi-seven-layers-model-explained-with-examples.html>**
- 3. <http://www.ict.griffith.edu.au/~sdrew/cit1507/m5/m5t2.htm>**
- 4. Data Communications and Networking 4th edition
page : 33**

-BEHROUZ A FOROUZAN

Subject : Computer Networks

Chapter : 3. Introduction to physical Layer

Faculty : Devendra G. Pandey sir

Sem. : 3th

Div. : A

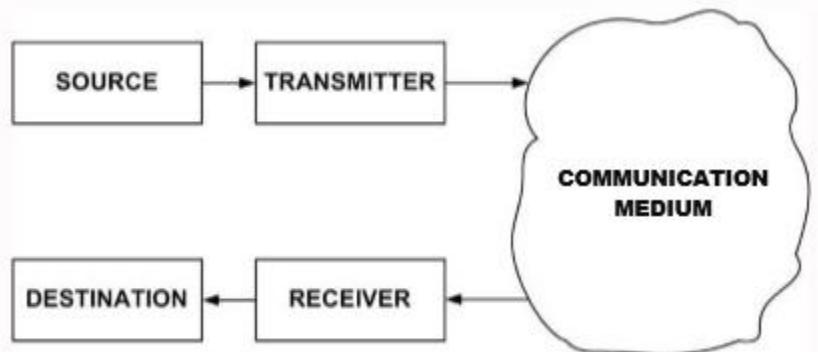
Roll No.	Name	
Work		
42 3.3.2 , 3.3.3)	Kapadiya Nancy	(3.3.1 , (3.3.2)
18	Galiawala Riddhi	(3.3.6)
4 3.3.9)	Pandey Aniket	(3.3.8 , (3.3.9)
5	Asondariya Parth	(3.2.6)
6	Baraiya Honey	(3.2.1)
7	Bhutwala Kevin	(3.4.1)
9	Borkar Krishna	(3.2.5)
10 3.1.6 , 3.1.7)	Chaudhari Jiger	(3.1.1 , (3.1.6)
11	Chauhan Dinal	(3.1.2)
13	Chavda Bhavik	(3.5.3)
16 3.5.2)	Dobariya Priyank	(3.3.5 , (3.5.2)
23	Gandhi Shelja	(3.4.4)
26 3.1.4)	Gondaliya Dhvani	(3.4.3 , (3.1.4)
29	Ijner Nikita	(3.1.3)
30	Jariwala Mohit	(3.2.3)
31	Jashani Shobham	(3.5.1)
33	Jhaveri Viraj	(3.1.5)
37	Kansara Kalp	(3.4.2)
43	Kapadia Shreya	(3.2.4)
45	Kelawala Jiya	(3.3.7)
46	Kelawala Misha	(3.3.4)
54 3.3.2 , 3.3.3)	Lathia Jhanvi	(3.3.1 , (3.3.2)
56	Lodaliya Snehal	(3.2.2)
58 3.1.7 , 3.1.6)	Mali Devanshu	(3.1.1 , (3.1.7)

3. Introduction to Physical later

3.3.1 Data and Signals

1. introduced:

One of the major functions of the physical layer is to move data in the form of electromagnetic signals across a transmission medium. Whether you are collecting numerical statistics from another computer, sending animated pictures from a design workstation, or causing a bell to ring at a distant control centre, you are working with the transmission of data across network connections.



1. Transmitter:-

As data cannot be sent in its native form, it is necessary to convert it into signal. This is performed with the help of a transmitter such as modem. The signal that is sent by the transmitter is represented by $s(t)$.

2. Communication Medium:

The signal can be sent to the receiver through a communication medium, which could be a simple twisted-pair of wire, a coaxial cable,

optical fiber or wireless communication system. It may be noted that the signal that comes out of the communication medium is $s'(t)$, which is different from $s(t)$ that was sent by the transmitter. This is due to various impairments that the signal suffers as it passes through the communication medium.

3. Receiver:

The receiver receives the signal $s'(t)$ and converts it back to data $d'(t)$ before forwarding to the destination. The data that the destination receives may not be identical to that of $d(t)$, because of the corruption of data.

4. Destination:

Destination is where the data is absorbed. Again, it can be a computer system, a telephone handset, a television set and so on.

2. Analog and Digital:

Both data and the signals that represent them can be either **analog** or **digital** in form.

3. Analog and Digital Data:

- Data can be analog or digital. The term **analog data** refers to information that is continuous; **digital data** refers to information that has discrete states.
- For example, an analog clock that has hour, minute, and second hands gives information

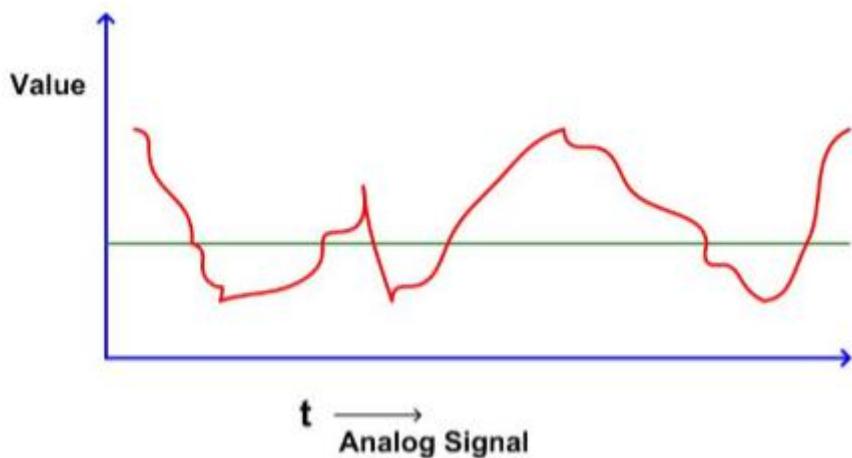
in a continuous form; the movements of the hands are continuous.

- On the other hand, a digital clock that reports the hours and the minutes will change suddenly from 8:05 to 8:06.
- Analog data, such as the sounds made by a human voice, take on continuous values.
- When someone speaks, an analog wave is created in the air.
- This can be captured by a microphone and converted to an analog signal or sampled and converted to a digital signal.
- Digital data take on discrete values. For example, data are stored in computer memory in the form of Os and 1s. They can be converted to a digital signal or modulated into an analog signal for transmission across a medium.
- Data can be analog or digital. Analog data are continuous and take continuous values. Digital data have discrete states and take discrete values.

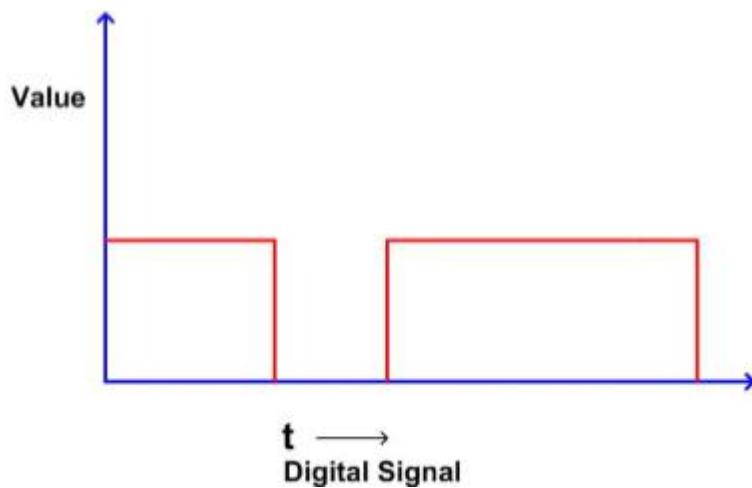
Analog and Digital Signals:

- It is electrical, electronic or optical representation of data, which can be sent over a communication medium. Stated in mathematical terms, a signal is merely a function of the data. For example, a microphone converts voice data into voice signal, which can be sent over a pair of wire. Analog signals are continuous-valued;

digital signals are discrete-valued. The independent variable of the signal could be time (speech, for example), space (images), or the integers (denoting the sequencing of letters and numbers in the football score). Figure 2.1.2 shows an analog signal.

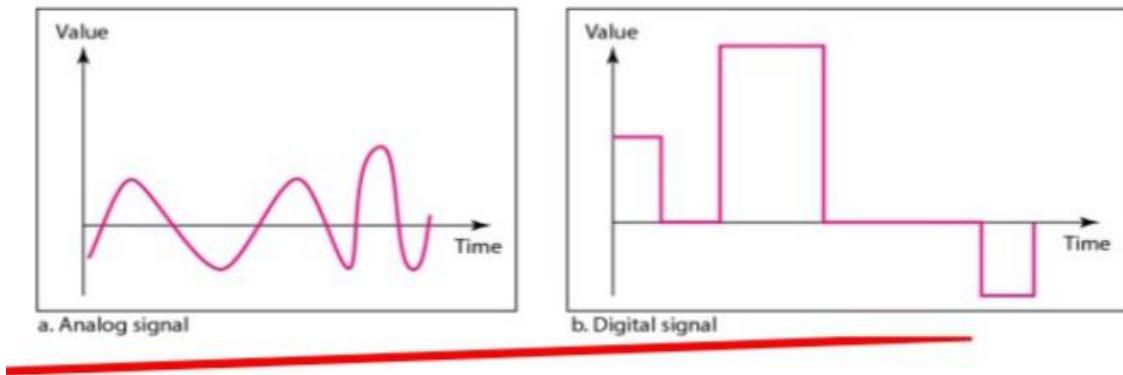


- Digital signal can have only a limited number of defined values, usually two values 0 and 1, as shown in



- Signaling: It is an act of sending signal over communication medium Transmission: Communication of data by propagation and processing is known as transmission.

Comparision of Analog and Digital Signals:



Periodic and Nonperiodic Signals:

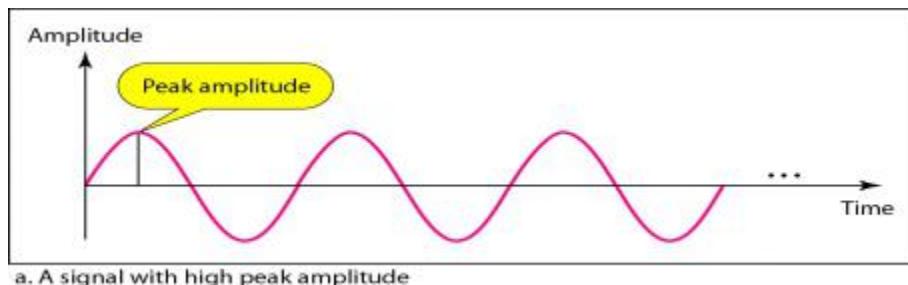
- Both analog and digital signals can take one of two forms: *periodic* or *nonperiodic*.
- A periodic signal completes a pattern within a measurable time frame, called a period, and repeats that pattern over subsequent identical periods. The completion of one full pattern is called a cycle. A nonperiodic signal changes without exhibiting a pattern or cycle that repeats over time.
- Both analog and digital signals can be periodic or nonperiodic. In data communications, we commonly use periodic analog signals (because they need less bandwidth) and nonperiodic digital signals (because they can represent variation in data).

Periodic Analog Signals:

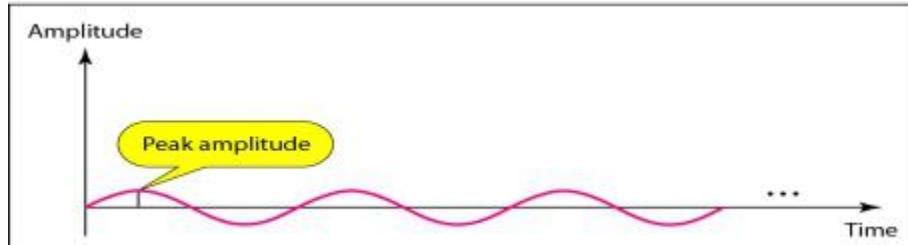
- Periodic analog signals can be classified as simple or composite. A simple periodic analog signal, a sine wave, cannot be decomposed into simpler signals. A composite periodic analog signal is composed of multiple sine waves.

Signal Amplitude:

- The peak amplitude of a signal is the absolute value of its highest intensity, proportional to the energy it carries. For electric signals, peak amplitude is normally measured in *volts*. Figure 3.3 shows two signals and their peak amplitudes.



a. A signal with high peak amplitude



● b. A signal with low peak amplitude

Frequency:

- Frequency is the rate of change with respect to time.
- Change in a short span of time means high frequency.
- Change over a long span of time means low frequency.
- If a signal does not change at all, its frequency is zero
- If a signal changes instantaneously, its frequency is infinite.

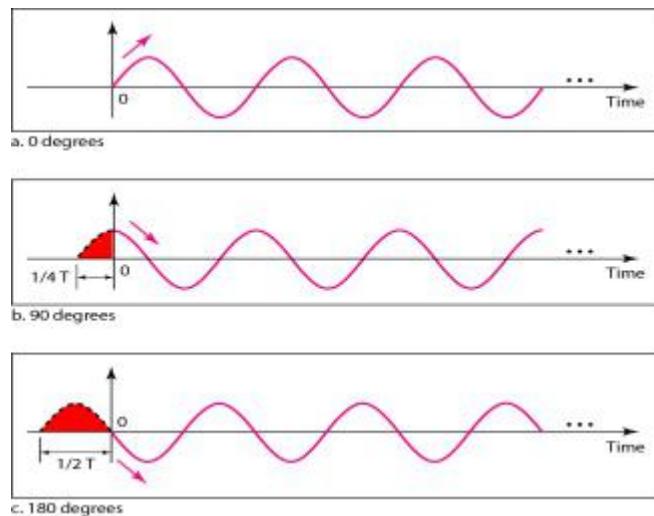
Frequency and Period:

- Frequency and period are the inverse of each other.
- $$f = \frac{1}{T} \quad \text{and} \quad T = \frac{1}{f}$$
- Units of period and frequency:

<i>Unit</i>	<i>Equivalent</i>	<i>Unit</i>	<i>Equivalent</i>
Seconds (s)	1 s	Hertz (Hz)	1 Hz
Milliseconds (ms)	10^{-3} s	Kilohertz (kHz)	10^3 Hz
Microseconds (μ s)	10^{-6} s	Megahertz (MHz)	10^6 Hz
Nanoseconds (ns)	10^{-9} s	Gigahertz (GHz)	10^9 Hz
Picoseconds (ps)	10^{-12} s	Terahertz (THz)	10^{12} Hz

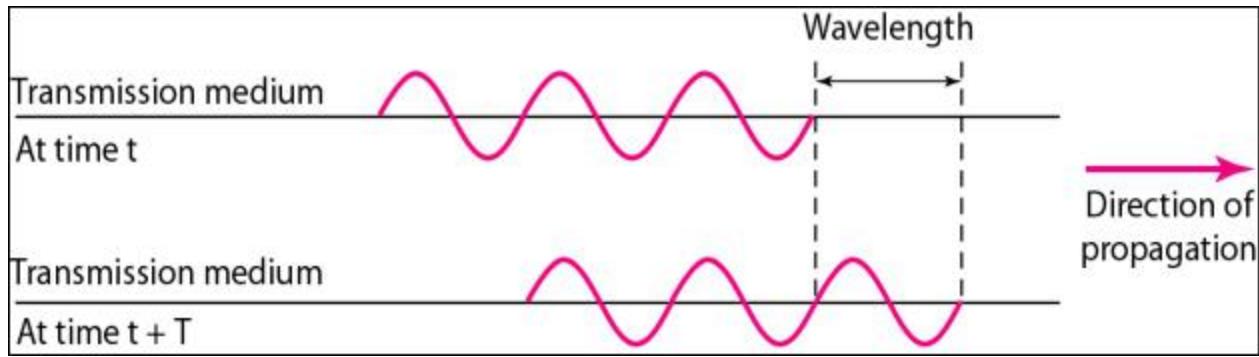
Phase:

- Phase describes the position of the waveform relative to time 0.



Wavelength and Frequency:

- Wavelength = Propagation speed x Period
 - = Propagation speed / Frequency



Reference :

1. Book:- data communication and networking 4th edition page :57
- 2.<http://nptel.ac.in/courses/10615080/pdf/M2I1.pdf>
- 3.https://en.wikipedia.org/wiki/Digital_signal

3.1.2 Digital Transmission

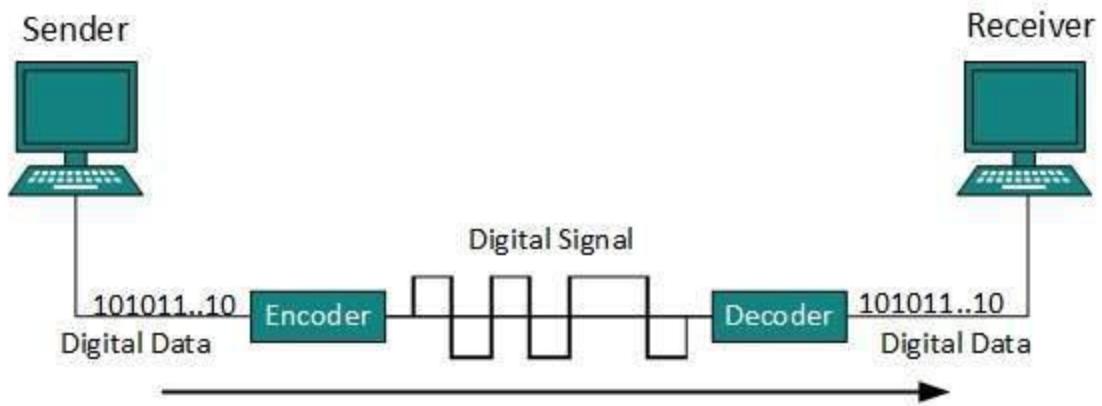
- Data or information can be stored in two ways, analog and digital. For a computer to use the data, it must be in discrete digital form. Similar to data, signals can also be in analog and digital form. To transmit data digitally, it needs to be first converted to digital form.

Digital-to-Digital Conversion

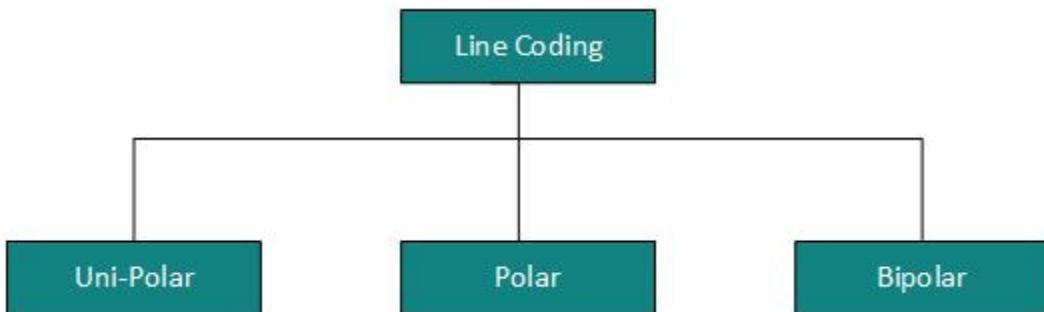
- This section explains how to convert digital data into digital signals. It can be done in two ways, line coding and block coding. For all communications, line coding is necessary whereas block coding is optional.

Line Coding

The process for converting digital data into digital signal is said to be Line Coding. Digital data is found in binary format. It is represented (stored) internally as series of 1s and 0s.

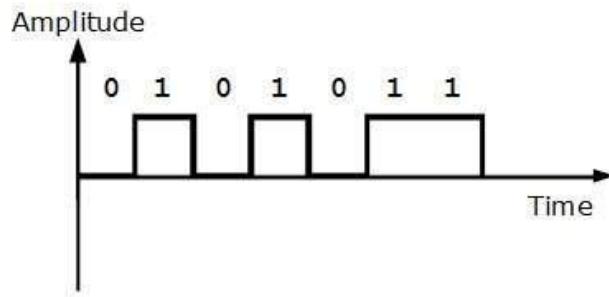


Digital signal is denoted by discreet signal, which represents digital data. There are three types of line coding schemes available:



Uni-polar Encoding

Unipolar encoding schemes use single voltage level to represent data. In this case, to represent binary 1, high voltage is transmitted and to represent 0, no voltage is transmitted. It is also called Unipolar-Non-return-to-zero, because there is no rest condition i.e. it either represents 1 or 0.



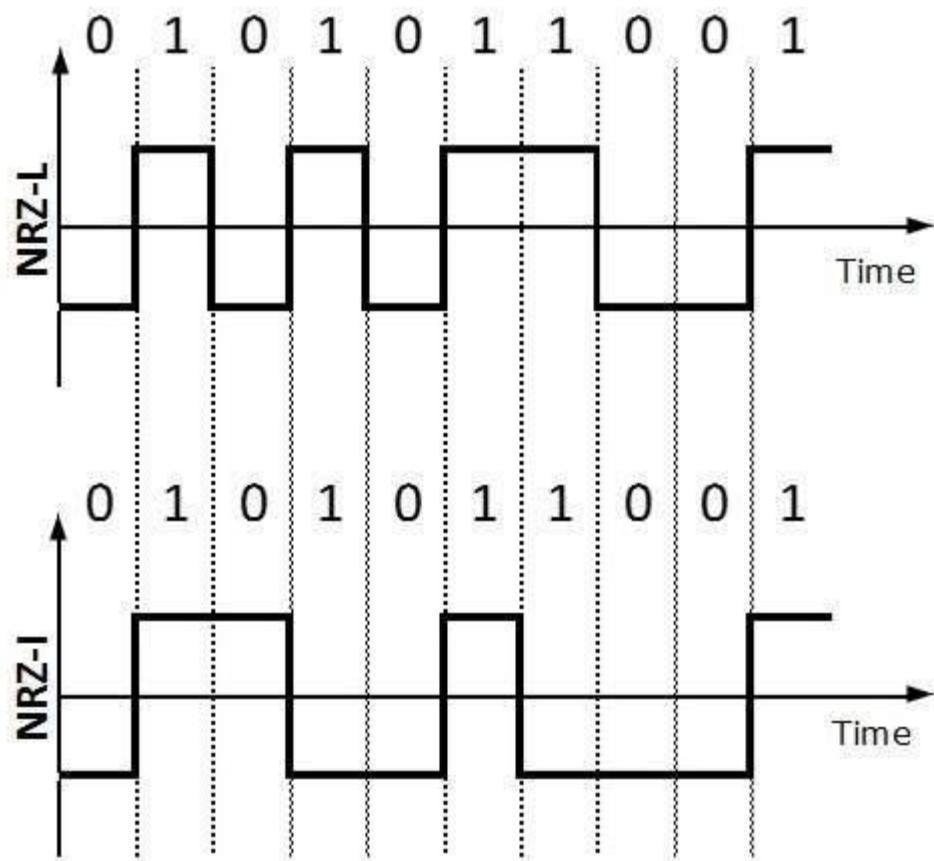
Polar Encoding

Polar encoding scheme uses multiple voltage levels to represent binary values. Polar encodings is available in four types:

- Polar Non-Return to Zero

It uses two different voltage levels to represent binary values. Generally, positive voltage represents 1 and negative value represents 0. It is also NRZ because there is no rest condition.

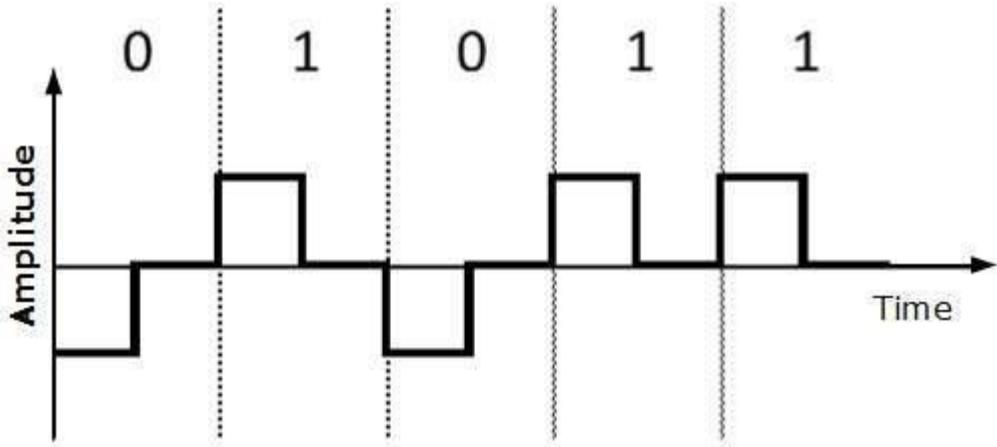
NRZ scheme has two variants: NRZ-L and NRZ-I.



NRZ-L changes voltage level at when a different bit is encountered whereas **NRZ-I** changes voltage when a 1 is encountered.

- **Return to Zero**

Problem with NRZ is that the receiver cannot conclude when a bit ended and when the next bit is started, in case when sender and receiver's clock are not synchronized.



RZ uses three voltage levels, positive voltage to represent 1, negative voltage to represent 0 and zero voltage for none. Signals change during bits not between bits.

- **Manchester**

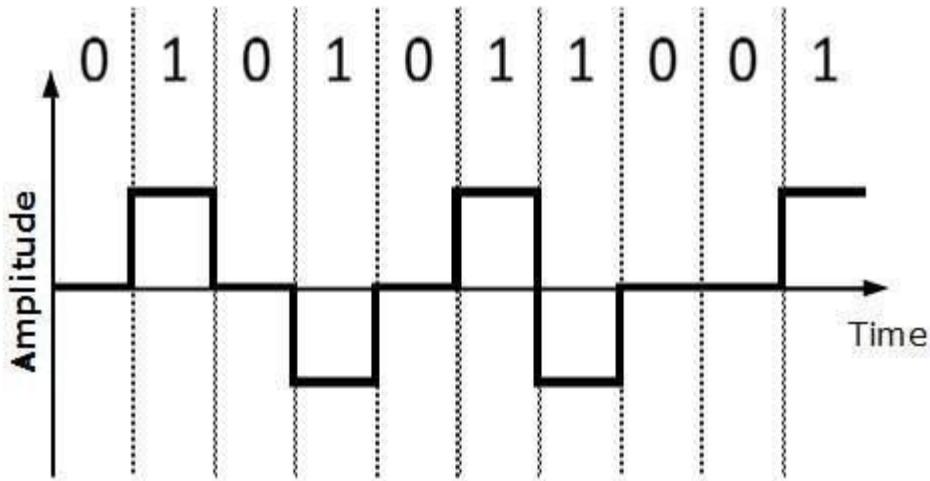
This encoding scheme is a combination of RZ and NRZ-L. Bit time is divided into two halves. It transits in the middle of the bit and changes phase when a different bit is encountered.

- **Differential Manchester**

This encoding scheme is a combination of RZ and NRZ-I. It also transit at the middle of the bit but changes phase only when 1 is encountered.

Bipolar Encoding

Bipolar encoding uses three voltage levels, positive, negative and zero. Zero voltage represents binary 0 and bit 1 is represented by altering positive and negative voltages.



Block Coding

To ensure accuracy of the received data frame redundant bits are used. For example, in even-parity, one parity bit is added to make the count of 1s in the frame even. This way the original number of bits is increased. It is called Block Coding.

Block coding is represented by slash notation, mB/nB . Means, m -bit block is substituted with n -bit block where $n > m$. Block coding involves three steps:

- **Division**
- **Substitution**
- **Combination.**

After block coding is done, it is line coded for transmission.

Analog-to-Digital Conversion

Microphones create analog voice and camera creates analog videos, which are treated as analog data. To transmit this analog data over digital signals, we need analog to digital conversion.

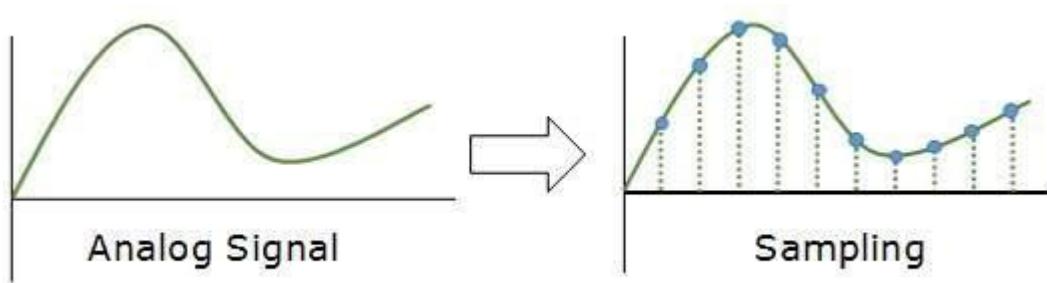
Analog data is a continuous stream of data in the wave form whereas digital data is discrete. To

convert analog wave into digital data, we use Pulse Code Modulation (PCM).

PCM is one of the most commonly used method to convert analog data into digital form. It involves three steps:

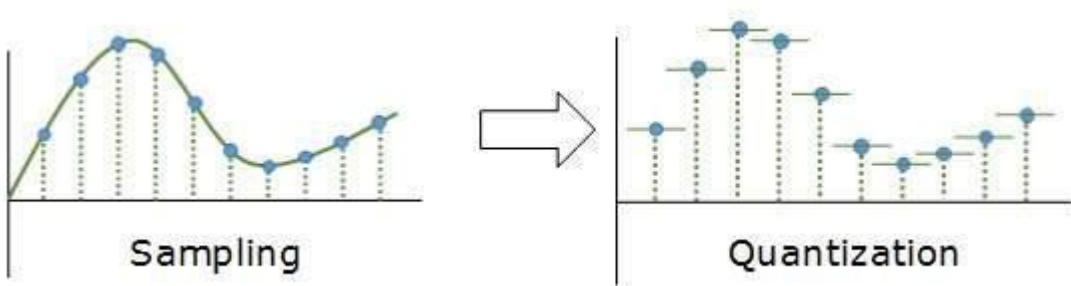
- **Sampling**
- **Quantization**
- **Encoding.**

Sampling



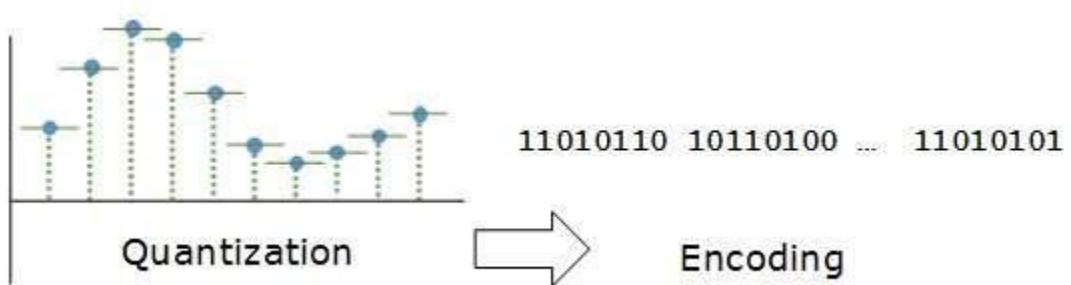
The analog signal is sampled every T interval. Most important factor in sampling is the rate at which analog signal is sampled. According to Nyquist Theorem, the sampling rate must be at least two times of the highest frequency of the signal.

Quantization



Sampling yields discrete form of continuous analog signal. Every discrete pattern shows the amplitude of the analog signal at that instance. The quantization is done between the maximum amplitude value and the minimum amplitude value. Quantization is approximation of the instantaneous analog value.

Encoding



In encoding, each approximated value is then converted into binary format.

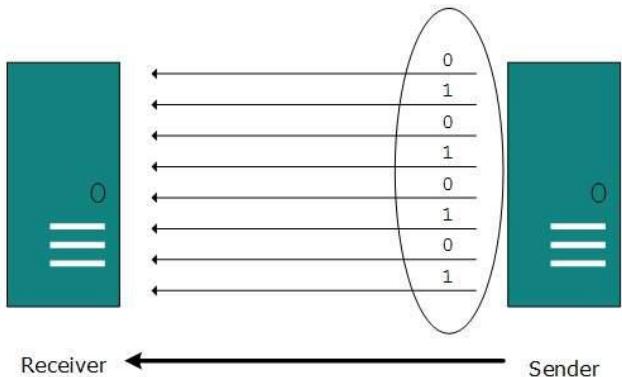
Transmission Modes

The transmission mode decides how data is transmitted between two computers .The binary data in the form of 1s and 0s can be sent in two different modes

1. Parallel and

2. Serial.

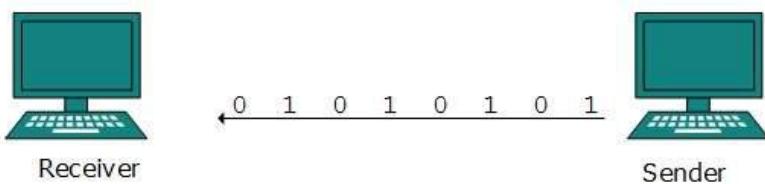
Parallel Transmission



The binary bits are organized into groups of fixed length. Both sender and receiver are connected in parallel with the equal number of data lines. Both computers distinguish between high order and low order data lines. The sender sends all the bits at once on all lines. Because the data lines are equal to the number of bits in a group or data frame, a complete group of bits is sent in one go. Advantage of Parallel transmission is high speed and disadvantage is the cost of wires, as it is equal to the number of bits sent in parallel.

Serial Transmission

In serial transmission, bits are sent one after another in a queue manner. Serial transmission requires only one communication channel.



Serial transmission can be either asynchronous or synchronous.

Asynchronous Serial Transmission

It is named so because there is no importance of timing. Data-bits have specific pattern and they help receiver recognize the start and end data bits. For example, a 0 is prefixed on every data byte and one or more 1s are added at the end.

Two continuous data-frames may have a gap between them.

Synchronous Serial Transmission

Timing in synchronous transmission has importance as there is no mechanism followed to recognize start and end data bits. There is no pattern or prefix/suffix method. Data bits are sent in burst mode without maintaining gap between bytes. Single burst of data bits may contain a number of bytes. Therefore, timing becomes very important.

It is up to the receiver to recognize and separate bits into bytes. The advantage of synchronous transmission is high speed, and it has no overhead of extra header and footer bits as in asynchronous transmission.

REFERENCE LINK :

<https://ariewibisono.wordpress.com/2014/04/13/physical-layer-digital-transmission/>

3.1.3 Analog Transmission

The analog transmission methods is still very popular, in particular for shorter distances, due to

significantly lower costs and complex multiplexing and timing equipment is unnecessary, and systems that simply do not need multiplexed digital transmission.

Analog transmission is a transmission method of conveying voice, data, image, signal or video information using a continuous signals which varies in amplitude, phase, or some other property in proportion to that of a variable.

Modulation, basic to the transmission of a message signal over a channel, is defined as the process by which some characteristic of a carrier is varied in accordance with a modulating wave.

In analog modulation, the modulating wave consists of an analog message signal (e.g., voice signal, video signal), and the carrier consists of a sine wave.

There are analog transmission systems and digital transmission systems. In an analog transmission system, signals propagate through the medium as continuously varying electromagnetic waves. In a digital system, signals propagate as discrete voltage pulses (that is, a positive voltage represents binary 1, and a negative voltage represents binary 0), which are measured in bits per second.

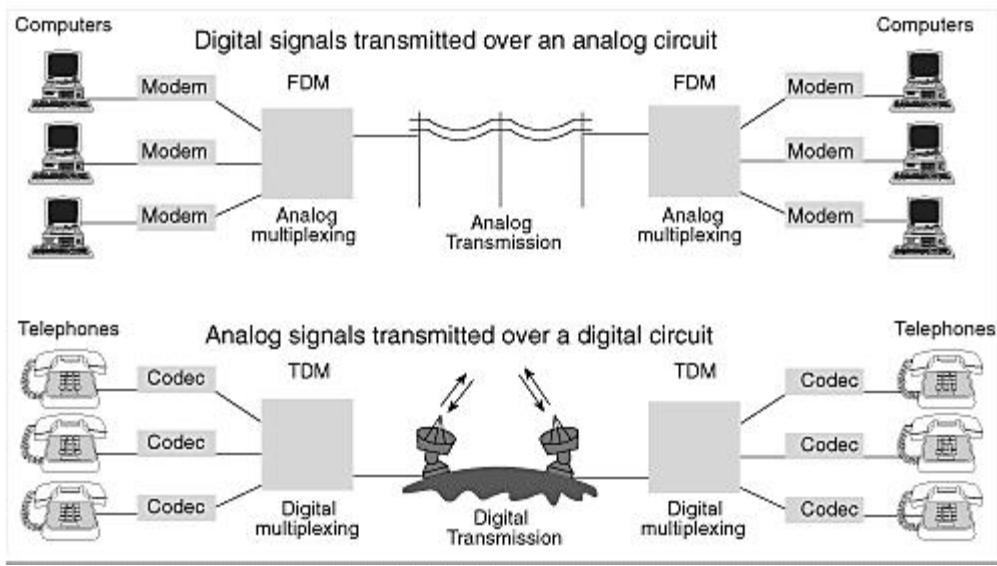
The medium for an analog transmission may be twisted-pair cable, coaxial cable, optical-fiber cable, the atmosphere, water, or space. A technique called "modulation" is used to combine an input signal (the data) onto a carrier signal. The carrier signal is a specific frequency. When tuning a radio, you select a particular carrier frequency in order to tune in that radio station. There are two primary modulation techniques: amplitude modulation, which varies the

amplitude (height) of the carrier signal; frequency modulation, which modulates the frequency of the carrier. Refer to "[Modulation Techniques](#)" for more information.

The frequency ranges of several analog transmission systems are listed here:

300-3,000 kHz	AM radio
3 to-30 MHz	Shortwave and CB radio
30-300 MHz	VHF television and FM radio
300-3,000 MHz	UHF television and cellular telephones, and microwave systems

In data communications, analog signals are used to transmit information over the telephone system or over radio transmission systems (such as satellite links). A modem converts digital data to analog signals. Alternatively, analog signals can be converted to digital information using a *codec* (*coder/decoder*). This process is called *digitizing*. Phones that connect to all-digital communication links use codecs to convert analog voice signals to digital signals. The phone company digitizes voice transmissions between its central offices and long-distance sites. In fact, the only remaining analog portion of the phone system is the twisted-pair wire that runs between homes and the telephone companies' central offices, which are usually less than a mile distance from the subscriber.



Reference :

**Tom Sheldon and Big Sur Multimedia.
The Data Communication and Networking (4th edition)
Page : 141**

3.1.4 Bandwidth

What is bandwidth

Bandwidth refers to the amount of information that can be transmitted over a network in a given amount of time, usually expressed in bits per second or bps.

It is often confused with speed.

Speed is the time it takes for one piece of information to get from point one to another point.

It is usually measured in bps (bits per second) or in the higher units of it such as kbps, mbps , etc.

Example: two moving carpets or "bands" of different widths, both moving at identical speeds. Two boxes, one placed on each moving carpet will both reach the end at the same time, but the wider carpet can carry more boxes than the narrow one.

Thus, higher the bandwidth the more information it can contain than the low range bandwidth.

Types:

- 1.Narrow Band
- 2.Wide Band
- 3.Broad Band

1.Narrow Band :

Narrowband is used where small amount of data volume is to be transmitted.

2. Wide Band :

Medium volume of data.

3. Broad Band :

A high speed, high capacity transmission medium that supports wide range frequency and also carries multiple signals at a time.

EX : cable tv, microwave satellite etc are examples of broadband.

REFERENCE LINK:

<http://www.vicomsoft.com/glossary/bandwidth/>

<http://www.theinfozones.com/2014/10/what-is-bandwidth-and-its-types.html>

3.1.5 Transmission Media

- **Transmission medium**

- Physical path between transmitter and receiver

- May be guided (wired) or unguided (wireless)

- Communication achieved by using em waves

- **Characteristics and quality of data transmission**

- Dependent on characteristics of medium and signal

- Guided medium

- * Medium is more important in setting transmission parameters

- Unguided medium

- * Bandwidth of the signal produced by transmitting antenna is important in setting transmission parameters.

- * Signal directionality

- Lower frequency signals are omnidirectional

- Higher frequency signals can be focused in a directional beam

- **Design of data transmission system**

- Concerned with data rate and distance

- Bandwidth

- * Higher bandwidth implies higher data rate

- Transmission impairments

- * Attenuation

- * Twisted pair has more attenuation than coaxial cable which in turn is not as good as optical fiber

- Interference

- * Can be minimized by proper shielding in guided media

- Number of receivers

- * In a shared link, each attachment

- introduces attenuation and distortion on the line

Guided transmission media

- Transmission capacity (bandwidth and data rate) depends on distance and type of network (point-to-point or multipoint)
- Twisted pair
 - Least expensive and most widely used
 - Physical description
 - * Two insulated copper wires arranged in regular spiral pattern
 - * Number of pairs are bundled together in a cable
 - * Twisting decreases the crosstalk interference between adjacent pairs in the cable, by using different twist length for neighboring pairs
 - Applications
 - * Most common transmission media for both digital and analog signals
 - * Less expensive compared to coaxial cable or optical fiber
 - * Limited in terms of data rate and distance
 - * Telephone network
 - Individual units (residence lines) to local exchange (end office)
 - Subscriber loops
 - Supports voice traffic using analog signaling
 - May handle digital data at modest rates using modems
 - * Communications within buildings
 - Connection to digital data switch or digital pbx within a building
 - Allows data rate of 64 kbps
 - Transmission characteristics
 - * Requires amplifiers every 5-6 km for analog signals
 - * Requires repeaters every 2-3 km for digital signals

- * Attenuation is a strong function of frequency
 - Higher frequency implies higher attenuation
- * Susceptible to interference and noise
- * Improvement possibilities
 - Shielding with metallic braids or sheathing reduces interference
 - Twisting reduces low frequency interference
 - Different twist length in adjacent pairs reduces crosstalk
- Unshielded and shielded twisted pairs
 - * Unshielded twisted pair (utp)
 - Ordinary telephone wire
 - Subject to external electromagnetic interference
 - * Shielded twisted pair (stp)
 - Shielded with a metallic braid or sheath
 - Reduces interference
 - Better performance at higher data rates
 - More expensive and difficult to work compared to utp
- Category 3 and Category 5 utp
 - * Most common is the 100-ohm voice grade twisted pair
 - * Most useful for lan applications
 - * Category 3 utp
 - Transmission characteristics specified up to 16 mhz
 - Voice grade cable in most office buildings
 - May have data rates up to 16 Mbps over limited distances

- Typical twist length 7.5 to 10 cm
 - * Category 4 utp
 - Transmission characteristics specified up to 20 mhz
 - * Category 5 utp
 - Transmission characteristics specified up to 100 mhz
 - Data grade cable in newer buildings
 - May have data rates up to 100 Mbps over limited distances
 - Much more tightly twisted, with typical twist length 0.6 to 0.85 cm, for better performance
- Coaxial cable
 - Physical description
 - * Consists of two conductors with construction that allows it to operate over a wider range of frequencies compared to twisted pair
 - * Hollow outer cylindrical conductor surrounding a single inner wire conductor
 - * Inner conductor held in place by regularly spaced insulating rings or solid dielectrical material
 - * Outer conductor covered with a jacket or shield
 - * Diameter from 1 to 2.5 cm
 - * Shielded concentric construction reduces interference and crosstalk
 - * Can be used over longer distances and support more stations on a shared line than twisted pair
 - Applications
 - * Most common use is in cable tv
 - * Traditionally part of long distance telephone network

- * Can carry more than 10,000 voice channels simultaneously using frequency-division multiplexing
- * Short range connections between devices
- Transmission characteristics
 - * Used to transmit both analog and digital signals
 - * Superior frequency characteristics compared to twisted pair
 - * Can support higher frequencies and data rates
 - * Shielded concentric construction makes it less susceptible to interference and crosstalk than twisted pair
 - * Constraints on performance are attenuation, thermal noise, and intermodulation noise
 - * Requires amplifiers every few kilometers for long distance transmission
 - * Usable spectrum for analog signaling up to 500 mhz
 - * Requires repeaters every few kilometers for digital transmission
 - * For both analog and digital transmission, closer spacing is necessary for higher frequencies/data rates
- Optical fiber
 - Thin, flexible material to guide optical rays
 - Cylindrical cross-section with three concentric links
- 1. Core
 - * Innermost section of the fiber
 - * One or more very thin (dia. 8-100 μm) strands or fibers
- 2. Cladding
 - * Surrounds each strand

- * Plastic or glass coating with optical properties different from core

- * Interface between core and cladding prevents light from escaping the core

3. Jacket

- * Outermost layer, surrounding one or more claddings

- * Made of plastic and other materials

- * Protects from environmental elements like moisture, abrasions, and crushing – Comparison with twisted pair and coaxial cable

- * Capacity

- Much higher bandwidth

- Can carry hundreds of Gbps over tens of kms

- * Smaller size and light weight · Very thin for similar data capacity

- Much lighter and easy to support in terms of weight (structural properties)

- * Significantly lower attenuation

- * EM isolation

- Not affected by external em fields

- Not vulnerable to interference, impulse noise, or crosstalk

- No energy radiation; little interference with other devices; security from eavesdropping

- * Greater repeater spacing

- Lower cost and fewer error sources

– Applications

- * Long haul trunks

- Increasingly common in telephone networks

- About 1500km in length with high capacity (20000 to 60000 voice channels)
- * Metropolitan trunks
 - Average length of about 12 km with a capacity of 100,000 voice channels
 - Mostly repeaterless to join phone exchanges in metro areas
- * Rural exchange trunks
 - Circuit lengths from 40 to 160 km
 - Fewer than 5000 voice channels
 - Connect exchanges of different phone companies
- * Subscriber loops
 - Central exchange to subscriber
 - May be able to handle image and video in addition to voice and data
- * Local area networks
 - 100Mbps to 1Gbps capacity
 - Can support hundreds of stations on a campus
- Transmission characteristics
 - * Single-encoded beam of light transmitted by total internal reflection
 - * Transparent medium should have higher refractive index compared to surrounding medium Refractive Index
- The ratio of the speed of light in a vacuum to the speed of light in a medium under consideration
 - * Optical fiber acts as a waveguide for frequencies in the range of about 10¹⁴ to 10¹⁵ Hz (IR and visible regions of spectrum)
 - * Step-index multimode · Rays at shallow angles are reflected and propagated along the fiber

- Other rays are absorbed by the surrounding material
- * Multimode transmission
 - Allows for multiple propagation paths, with different path lengths and time to traverse the fiber
 - Signal elements can be spread over time
 - Limits the rate at which data can be accurately received
 - Best suited for transmission over very short distances
- * Single-mode transmission
 - Reduced fiber core will allow fewer angles to be reflected
 - Single transmission path reduces distortion
 - Typically used for long-distance applications
- * Graded-index multimode
 - Lies in between single-mode and multimode
 - Higher refractive index at the center implies that the rays close to axis advance slowly compared to rays close to the cladding
 - Light in the core curves helically reducing its traveling distance (does not zig zag off the cladding)
 - Shorter path and higher speed makes light at periphery as well as at the axis travel at the same speed
- * Light sources
 1. Light-emitting diode (led)
 - Cheaper and works over a greater temperature range

- Longer operational life

2. Injection laser diode (ild)

- More efficient and can sustain greater data rates

– Wavelength-division multiplexing

* Multiple beams of light at different frequencies can be transmitted simultaneously

* Form of frequency-division multiplexing (fdm) commonly known as wavelength-division multiplexing (wdm)

Wireless Transmission

- Transmission and reception are achieved using an antenna

– Transmitter sends out the em signal into the medium

– Receiver picks up the signal from the surrounding medium

- Directional transmission

– Transmitter sends out a focused em beam

– Transmitter and receiver antennae must be carefully aligned

– More suitable for higher frequency signals

- Omnidirectional transmission

– Transmitted signal spreads out in all directions

– May be received by many antennae

- Frequency ranges for wireless transmission

1. 2 ghz – 40 ghz

– Microwave frequencies

– Highly directional beams for point-to-point communications

– Also used for satellite communication

2. 30 mhz – 1 ghz

- Broadcast radio range
- Suitable for omnidirectional purposes

3. 3×10^{11} Hz – 2×10^{14} Hz

- Infrared portion of the spectrum
- Useful for local point-to-point and multipoint applications within confined areas
- tv remote

- Terrestrial microwave – Physical description

- * Parabolic dish antenna, about 3m in diameter
- * Fixed rigidly with a focused beam along line of sight to receiving antenna
 - * With no obstacles, maximum distance (d, in km) between antennae can be $d = 7.14\sqrt{Kh}$ where h is antenna height and K is an adjustment factor to account for the bend in microwave due to earth's curvature, enabling it to travel further than the line of sight; typically K = 4.3
 - * Two microwave antennae at a height of 100m may be as far as $7.14 \times \sqrt{133} = 82$ km
 - * Long distance microwave transmission is achieved by a series of microwave relay towers

- Applications

- * Long haul telecom service
- * Fewer repeaters than coaxial cable but needs line of sight

- Transmission characteristics

- * Frequencies in the range of 2 – 40 GHz
- * Higher frequency implies higher bandwidth leading to higher data rates
- * Loss L due to attenuation over distance d at wavelength λ is expressed as $L = 10 \log_{10} \frac{4\pi d}{\lambda} + 2$ dB
 - Loss varies as the square of distance

- For twisted pair and coaxial cable, loss varies logarithmically with distance
 - * Repeaters may be placed further apart compared to coaxial cable
 - * Attenuation may increase with rainfall, especially above 10 ghz
 - * Interference is a problem, leading to regulated assignment of frequencies
- Satellite microwave
 - Physical description
 - * Communication satellite is a microwave relay station between two or more ground stations (also called earth stations)
 - * Satellite uses different frequency bands for incoming (uplink) and outgoing (downlink) data
 - * A single satellite can operate on a number of frequency bands, known as transponder channels or transponders
 - * Geosynchronous orbit (35,784 km)
 - * Satellites cannot be too close to each other to avoid interference
 - Current standard requires a 4° displacement in the 4/6 ghz band and 3° displacement at 12/14 ghz
 - This limits the number of available satellites
 - Applications
 - * Television/telephone/private business networks
 - * vsat – Very small aperture terminals
 - Used to share a satellite capacity for data transmission
 - Transmission characteristics
 - * Optimum frequency range in 1–10 ghz
 - * Below 1 ghz, significant noise from galactic, solar, and atmospheric noise, and terrestrial electronic devices

- * Above 1 ghz, signal attenuated by atmospheric absorption and precipitation
 - * Most satellites use 5.925–6.425 ghz band for uplink and 4.2–4.7 ghz band for downlink (4/6 band)
 - * Propagation delay of about a quarter second due to long distance
 - Problems in error control and flow control
 - Inherently broadcast, leading to security problems
- Broadcast radio
- Physical description
 - * Omnidirectional transmission
 - * No need for dish antennae
- Applications
 - * Frequencies from 3 kHz to 300 ghz
 - * Radio/Television/Data networking
- Transmission characteristics
 - * 30 mhz to 1 ghz (uhf band) used for broadcast communications
 - * Ionosphere transparent to radio waves above 30 mhz
 - Transmission limited to line of sight
 - Distant transmitters do not interfere with each other due to reflection from atmosphere
 - * Less sensitive to attenuation from rainfall
 - * Maximum distance between transmitter and receiver is given by same equation as microwave; same for attenuation
 - * Impairment due to multipath interference · Reflection from land, water, natural, man-made objects
 - Infrared
 - Limited to short distances and highly directional
 - Cannot penetrate walls

– No licensing; no frequency allocation issues

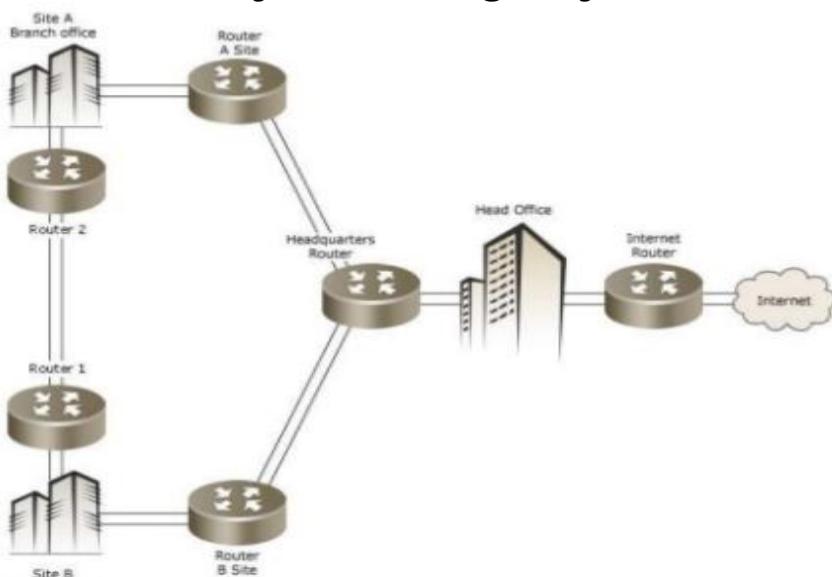
Reference :

The DATA Communication and Networking
(4th Edition) page :191

3.1.6 Switching

switched networks

- series of interlinked nodes, is called a switches.
- devices capable of creating a temporary connections between two or more devices linked to the switches.
- some of these switches are connected to the end systems(computers or telephones).
- others used only for routing only.



Reference Link:-

(https://www.google.co.in/search?q=message+switching+details+++slideshare&oq=message+switching+details+++slideshare&gs_l=psy-ab.3...4047.6167.0.7130.8.7.0.0.0.0.0..0..0...1.1.64.psy-ab..8.0.0.nOhsmRTB1ag)

1. circuit-switched networks

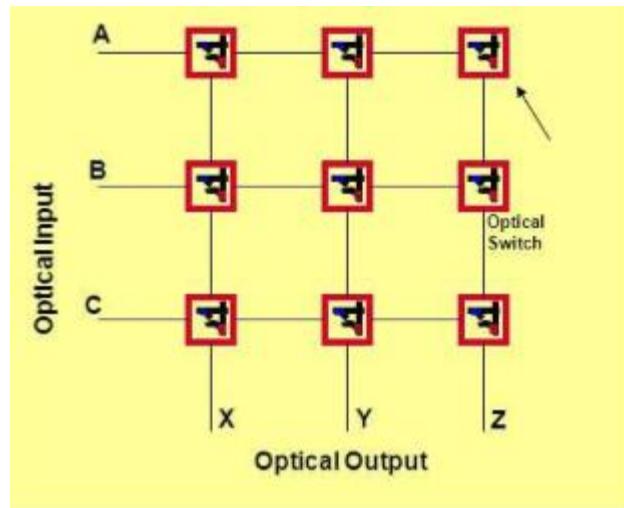
- A circuits switched network consists of a set of switches connected by physical links.
- A connection between 2 stations is a dedicated path made of one or more links.
- However each connection uses only one dedicated channel on each link.
- Each links is divided into n channels using FDM or TDM.
- circuit -switching takes place at the physical layer
- data transferred between the two stations are not packetized.the data are a continuous flow sent by the source station and received by the destination station.
- there is no addressing involved during data transfer. of course,there is end-to-end addressing used during the setup phase.

There are a two circuit switching:-

1. space division switch
2. time division switch

1. space division switch:-

In space division switching, the paths in the circuit are separated from each other spatially.



**SPACE DIVISION SWITCHING
3 x 3 matrix**

- **Crossbar Switches**
 - a. A crossbar switch connects n inputs to m outputs in a grid, using micro switches at each cross point.
 - b. The major limitation of this design is the number of cross points required.
 - c. Connecting n inputs to m outputs using a crossbar switch requires $m \times n$ cross points.
 - d. Such switches are also inefficient because fewer than 25 percent of given switch are used and other remains idle.

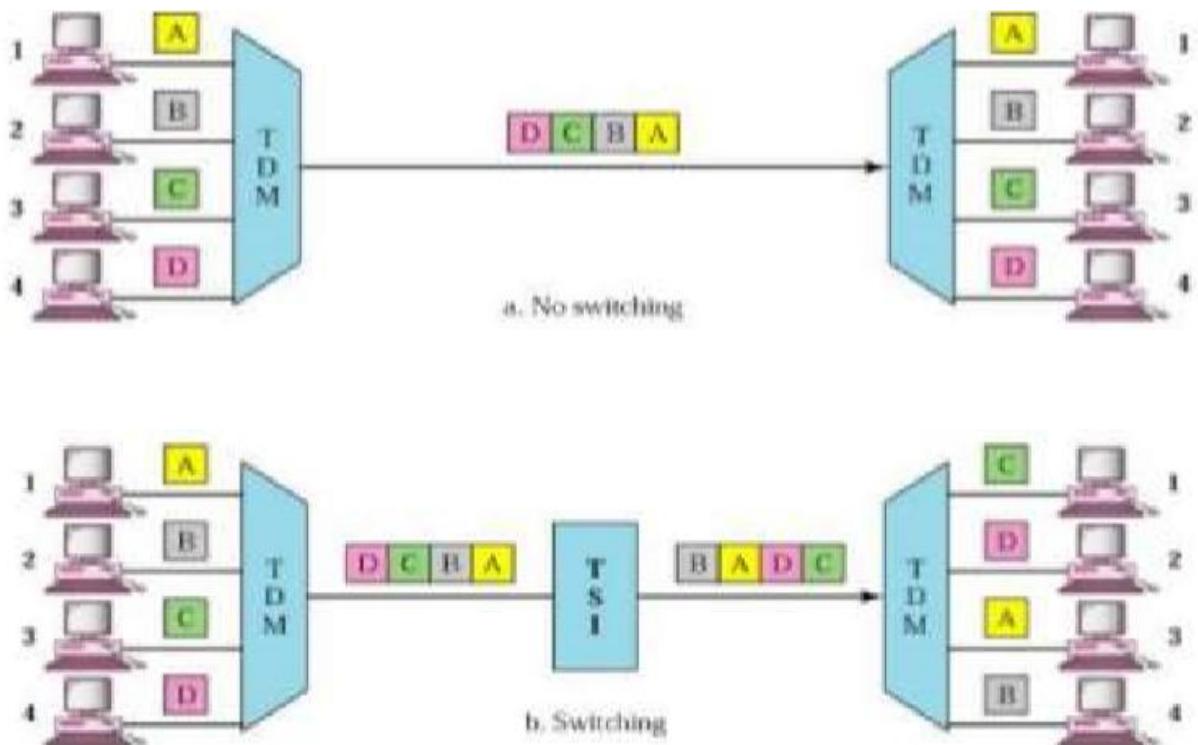
2. multistage switch

- The problem of crossbar switch can overcome by multistage switch.
- In multistage switching, devices are linked to switches that, are linked to a hierarchy of other switches.
- The design of multistage switch depends on the number of stages and

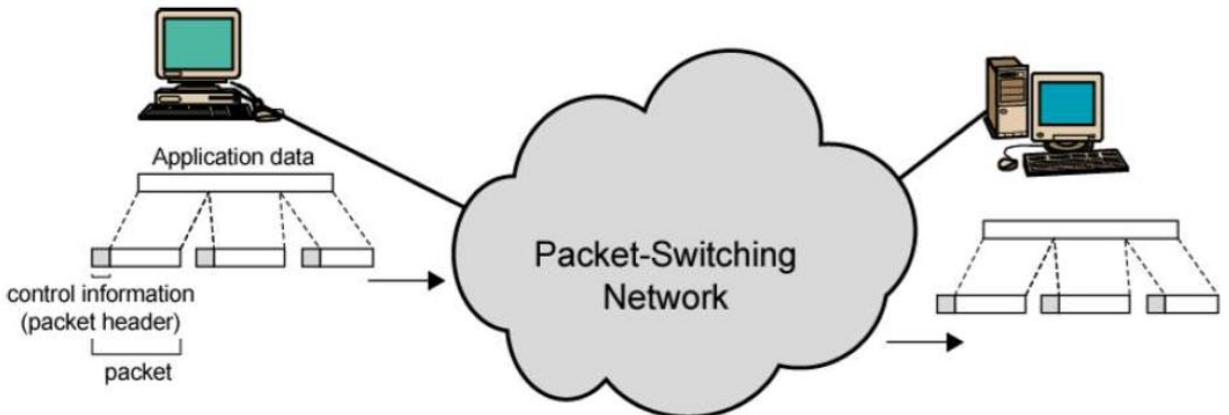
the number of switches required in each stage.

- Normally, middle stage has fewer switches than the first and last stage.

3. time division switch:-



- Time division switching uses time division multiplexing to achieve switching.
- There are two popular methods used in time division multiplexing
 1. Time slot interchange
 2. TDM Bus
 3. packet switched network



- message need to be divided into packets.
- size of the packet is determined by the network and the governing protocol.
- no resource reservation, but allocated on demand.
- the allocation is done first come, first served based.
- when a switch receives a packets, the packet must wait if there are other packets being processed, this lack of reservation may create delay

at each nodes packet is received and stored it to the next node. let us consider simple switching network. consider a packet to be sent from a station to station c.

1. the packet includes control information that the intended destination is b.
2. the packet is sent from a to node 3 node 3 stores the packet and determine the next route and queues the packet to go to that link b-4 link
3. when the link is available the packet sends the data from (4 to 5) and finally node 5 to destination b
4. the packets are queued up and transmitted as rapidly as possible over the link.

2.1 datagram networks

- each packet(called as a datagrams in this approach) is treated independently of all others.
- all packets (or datagrams) belong to the same message may travel different paths to reach their destination.
- datagram switching is done at the network layer
- packet may also be lost or dropped because of a lack of resources.
- the datagram network are referred to connection network.
- there are no setup or teardown phases.

2.2 virtual-circuit networks

- it's a cross between circuit switched network and datagram network, and has some characteristics of both.

characteristics:-

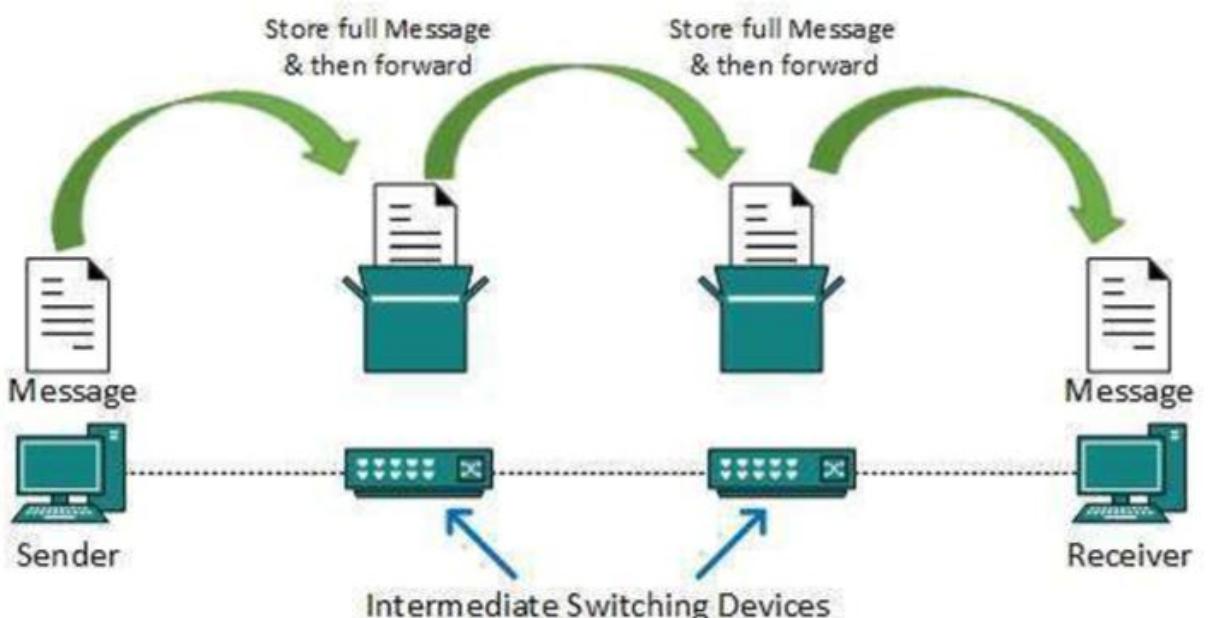
- packet from a single message travel along the same path.
- three phases to transfer data
 - set up
 - data transfer
 - tear down
- resource can be allocated during setup phase.
- data are packetized and each packet carries an address in the header.
- implemented in data link layer.

Reference Link:-

(<https://www.slideshare.net/sdsnehaldalvi/circuit-switching-packet-switching>)

3. message switching

- with message switching there is no need to establish a dedicated path between two stations.
- when a station sends a message, the destination address is appended to the message.
- the message is then transmitted through the network, in its entirety, from node to node.
- each node receives the entire message, stores it in its entirety on disk, and then transmits the message to the next node.
- this type of network is called a store-and-forward network.



a message-switching node is typically a general-purpose computer. the device needs sufficient storage capacity to store the incoming messages, which could be long. a time delay is introduced using this type of scheme due to store-and-forward time, plus the time required to find the next node in the transmission path.

Disadvantages:-

- message switching is not compatible with interactive applications.

- store-and-forward devices are expensive, because they must have large disks to hold potentially long messages.

Reference Link:-

(https://www.google.co.in/search?q=message+switching+details+++slideshare&oq=message+switching+details+++slideshare&gs_l=psy-ab.3...4047.6167.0.7130.8.7.0.0.0.0.0.0....0...1.1.64.psy-ab..8.0.0.nOhsmRTB1ag)

3.1.7 IEEE 802.2 Standards

IEEE 802 STANDARDS

WHAT IS MEAN BY IEEE 802?

IEEE 802 is an Institute of Electrical and Electronics Engineers (IEEE) standard set that covers the physical and data link layers of the (OSI) model. IEEE Standard comprises a family of networking standards that cover the physical layer specifications of technologies from Ethernet to wireless.

It is subdivided into 22 which covers the physical and data-link aspects of networking.

Reference :-

<https://www.techopedia.com/definition/19935/ieee-802>

https://en.wikipedia.org/wiki/IEEE_802

IEEE 802 NETWORKING STANDARDS:-

standard topic diagram reference from:-

networking complete third edition.
BPB publication

STANDARD	TOPIC
802.1 access bridges.(internetworking)	LAN/MAN management and media control(MAC)
802.2	Logical link control
802.3	CSMA/CD
802.4	TOKEN BUS
802.5	TOKEN RING
802.6	DISTRIBUTED QUEUE DUAL BUS
802.7 NETWORK	BROADBRAND LOCAL AREA
802.8	FIBER-OPTIC LANs and MANs
802.9 interface	INTEGRATED SERVICES (IS) LAN
802.10	LAN/MAN SECURITY
802.11b	Wireless LAN
802.12	Demand priority Access Method
802.13	Unused standard number

802.14	Defunct working group
802.15 network)	Wireless PAN(personal area
802.16	Wireless MAN
802.17	Resilient packet Ring
802.18	Wireless advisory group
802.19	Coexistence advisory group
802.20	mobile broadband wireless

802.1:-

IEEE 802.1 handles the architecture, security, management and internetworking of local area networks (LAN), metropolitan area networks (MAN) and wide area area networks (WAN) standardized by IEEE 802.

IT IS COMPRASED OF FOUR GROUPS

- 1.internetworking**
- 2.audio/video bridging**
- 3.data center bridging**
- 4.security**

The Internetworking group handles overall architecture, link aggregation, protocol addressing, network path identification/calculation and other technical practices and recommendations.

Reference :

<https://www.techopedia.com/definition/19936/ieee-8021-working-group-ieee-8021>

802.2(Logical link control):-

<http://network-communications.blogspot.in/2011/06/802-standards-ieee-8022-8023-8025-80211.html>

The technical definition for 802.2 is "the standard for the upper Data Link Layer sublayer also known as the Logical Link Control layer. It is used with the 802.3, 802.4, and 802.5 standards (lower DL sublayers)."

802.2 specify the general interface between network layer like (ip,ipx,etc) and data link layer like (ethernet,token,ring).

802.3 Ethernet:-

<http://network-communications.blogspot.in/2011/06/802-standards-ieee-8022-8023-8025-80211.html>

802.3 is the standard which Ethernet operates by. It is the standard for CSMA/CD (Carrier Sense Multiple Access with Collision Detection). This standard encompasses both the MAC and Physical Layer standards

CSMA/CD is what Ethernet uses to control access to the network medium (network cable). If there is no data, any node may attempt to transmit, if

the nodes detect a collision, both stop transmitting and wait a random amount of time before retransmitting the data.

802.4 Token Bus:-

reference from:-

networking complete third edition.
BPB publication

This standard specifies a physical and logical bus topology that uses coaxial or fiber-optic cable and a token-passing media access method. It is used mainly for factory automation and is seldom used in computer networking.

802.5 Token Ring:-

<http://network-communications.blogspot.in/2011/06/802-standards-ieee-8022-8023-8025-80211.html>

Token Ring was developed primarily by IBM. Token ring is designed to use the ring topology and utilizes a token to control the transmission of data on the network.

The token is a special frame which is designed to travel from node to node around the ring. When it does not have any data attached to it, a node on the network can modify the frame, attach its data and transmit. Each node on the network checks the token as it passes to see if the data is intended for

that node, if it is; it accepts the data and transmits a new token. If it is not intended for that node, it retransmits the token on to the next node.

3.2.1 Function of Data Link Layer

Framing:

Frames are the streams of bits received from the network layer into manageable data units. This division of stream of bits is done by Data Link Layer. Data-link layer takes packets from Network Layer and encapsulates them into Frames. Then, it sends each frame bit-by-bit on the hardware. At receiver's end, data link layer picks up signals from hardware and assembles them into frames.

Physical Addressing:

The Data Link layer adds a header to the frame in order to define physical address of the sender or receiver of the frame, if the frames are to be distributed to different systems on the network.

Synchronization:

When data frames are sent on the link, both machines must be synchronized in order to transfer to take place.

Multi-Access

When host on the shared link tries to transfer the data, it has a high probability of collision. Data-link layer provides mechanism such as CSMA/CD to equip capability of accessing a shared media among multiple Systems.

Flow Control:

A flow control mechanism to avoid a fast transmitter from running a slow receiver by buffering the extra bit is provided by flow control. This prevents traffic jam at the receiver side.

Error Control:

Error control is achieved by adding a trailer at the end of the frame. Duplication of frames are also prevented by using this mechanism. Data Link Layers adds mechanism to prevent duplication of frames.

Access Control:

Protocols of this layer determine which of the devices has control over the link at any given time, when two or more devices are connected to the same link.

Reference :

The DATA Communication and Networking (4th Edition) page: 265

3.2.2 & 3.2.3 Error detection and correction and code

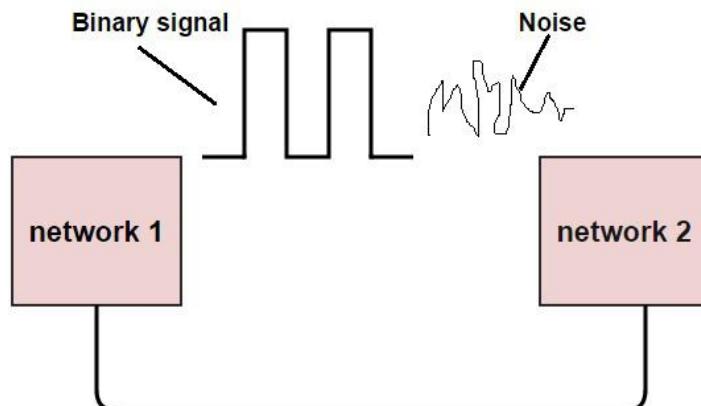
Introcution

In digital systems, the analog signals will change into digital sequence (in the form of bits). This sequence of bits is called as “Data stream”. The change in position of single bit also leads to catastrophic (major) error in data output. Almost in all electronic devices, we find errors and we use error detection and correction techniques to get the exact or approximate output.

What is an Error

The data can be corrupted during transmission (from source to receiver). It may be affected by external noise or some other physical imperfections. In this case, the input data is not same as the received output data. This mismatched data is called “Error”.

The data errors will cause loss of important / secured data. Even one bit of change in data may affect the whole system’s performance. Generally the data transfer in digital systems will be in the form of ‘Bit – transfer’. In this case, the data error is likely to be changed in positions of 0 and 1 .



Types Of Errors

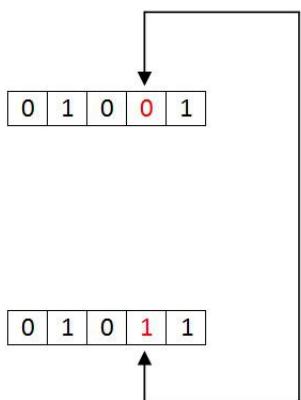
In a data sequence, if 1 is changed to zero or 0 is changed to 1, it is called “Bit error”.

There are generally 3 types of errors occur in data transmission from transmitter to receiver. They are

- Single bit errors
- Multiple bit errors
- Burst errors

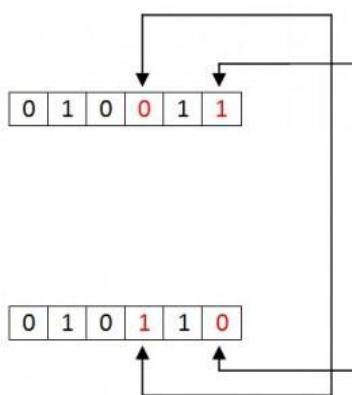
Single Bit Data Errors

The change in one bit in the whole data sequence , is called “Single bit error”. Occurrence of single bit error is very rare in serial communication system. This type of error occurs only in parallel communication system, as data is transferred bit wise in single line, there is chance that single line to be noisy.



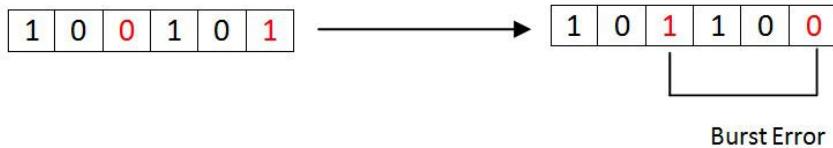
Multiple Bit Data Errors

If there is change in two or more bits of data sequence of transmitter to receiver, it is called “Multiple bit error”. This type of error occurs in both serial type and parallel type data communication networks.



Burst Errors

The change of set of bits in data sequence is called “Burst error”. The burst error is calculated in from the first bit change to last bit change.



Here we identify the error form fourth bit to 6th bit. The numbers between 4th and 6th bits are also considered as error. These set of bits are called “Burst error”. These burst bits changes from transmitter to receiver, which may cause a major error in data sequence. This type of errors occurs in serial communication and they are difficult to solve.

Error Detecting Codes

In digital communication system errors are transferred from one communication system to another, along with the data. If these errors are not detected and corrected, data will be lost . For effective communication, data should be transferred with high accuracy .This can be achieved by first detecting the errors and then correcting them.

Error detection is the process of detecting the errors that are present in the data transmitted from transmitter to receiver, in a communication system. We use some redundancy codes to detect these errors, by adding to the data while it is transmitted from source (transmitter). These codes are called “Error detecting codes”.

Types of Error detection

1. Parity Checking

2. Cyclic Redundancy Check (CRC)
3. Longitudinal Redundancy Check (LRC)
4. Check Sum

1. Parity Checking

Parity bit means nothing but an additional bit added to the data at the transmitter before transmitting the data. Before adding the parity bit, number of 1's or zeros is calculated in the data. Based on this calculation of data an extra bit is added to the actual information / data. The addition of parity bit to the data will result in the change of data string size.

This means if we have an 8 bit data, then after adding a parity bit to the data binary string it will become a 9 bit binary data string.

Parity check is also called as “Vertical Redundancy Check (VRC)”.

There are two types of parity bits in error detection, they are

- Even parity
- Odd parity

Even Parity

- If the data has even number of 1's, the parity bit is 0. Ex: data is 10000001 -> parity bit 0
- Odd number of 1's, the parity bit is 1. Ex: data is 10010001 -> parity bit 1

Odd Parity

- If the data has odd number of 1's, the parity bit is 0. Ex: data is 10011101 -> parity bit 0

- Even number of 1's, the parity bit is 1. Ex: data is 10010101 -> parity bit 1

NOTE:

The counting of data bits will include the parity bit also.

The circuit which adds a parity bit to the data at transmitter is called “Parity generator”. The parity bits are transmitted and they are checked at the receiver. If the parity bits sent at the transmitter and the parity bits received at receiver are not equal then an error is detected. The circuit which checks the parity at receiver is called “Parity checker”.

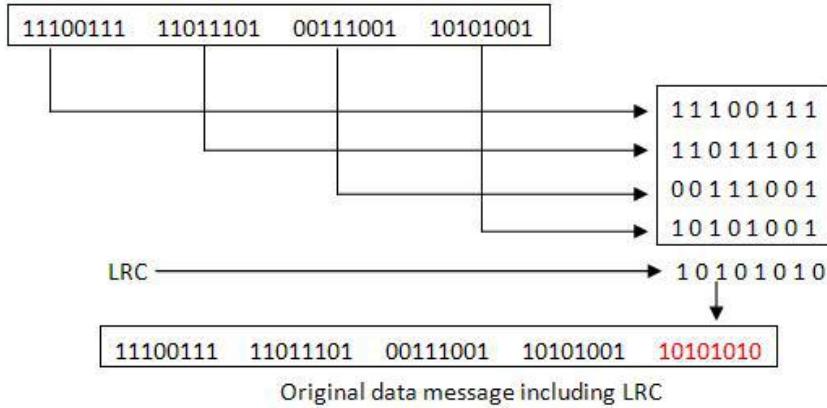
Messages with even parity and odd parity

3. Longitudinal Redundancy Check

In longitudinal redundancy method, a BLOCK of bits are arranged in a table format (in rows and columns) and we will calculate the parity bit for each column separately. The set of these parity bits are also sent along with our original data bits.

Longitudinal redundancy check is a bit by bit parity computation, as we calculate the parity of each column individually.

This method can easily detect burst errors and single bit errors and it fails to detect the 2 bit errors occurred in same vertical slice.



Error Correcting Codes

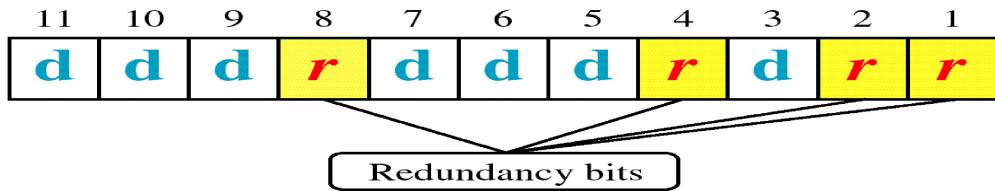
The codes which are used for both error detecting and error correction are called as “Error Correction Codes”. The error correction techniques are of two types. They are,

- Single bit error correction
- Burst error correction

The process or method of correcting single bit errors is called “single bit error correction”. The method of detecting and correcting burst errors in the data sequence is called “Burst error correction”.

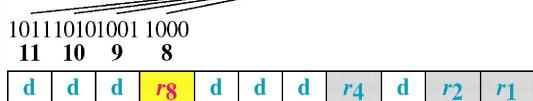
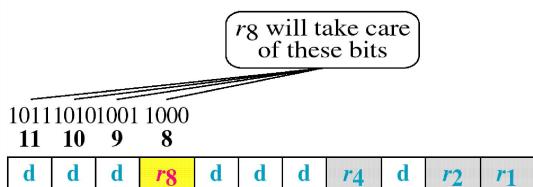
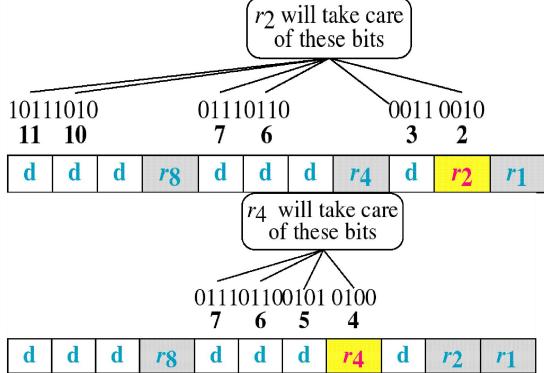
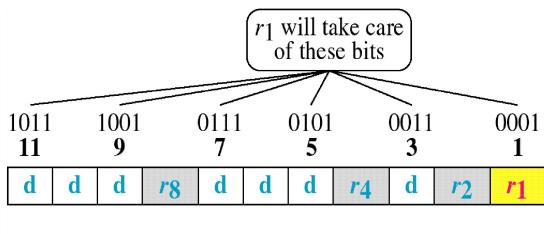
Hamming code or Hamming Distance Code is the best error correcting code we use in most of the communication network and digital systems.

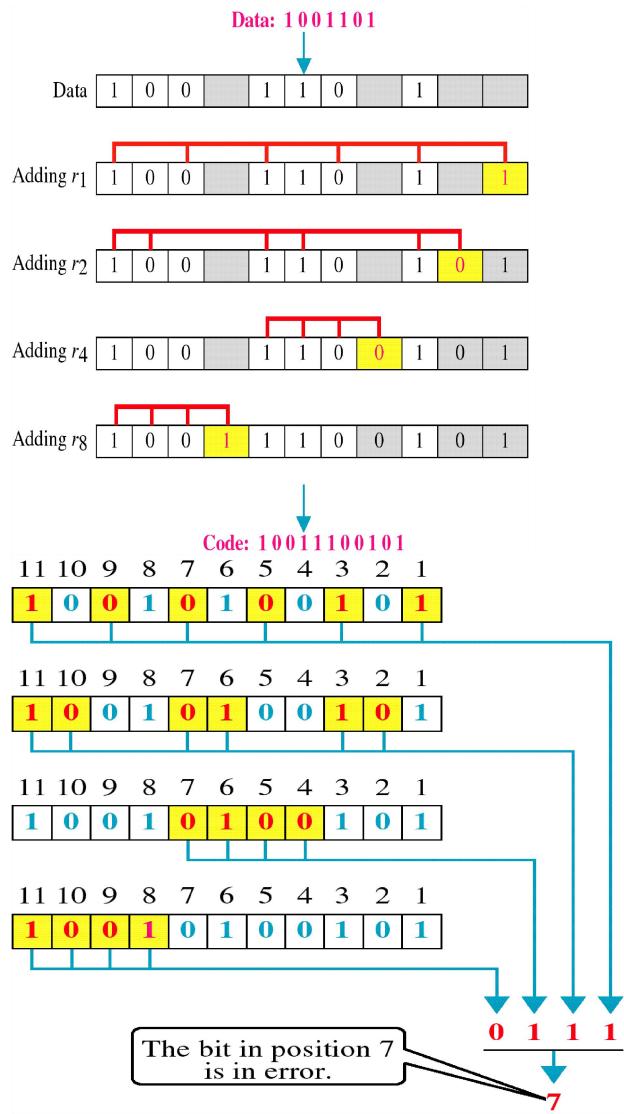
- ◎ Hamming code can be applied to data units of any length and uses relationships between data and redundancy bits .



◎ Redundancy Bits:

- R1: bits 1,3,5,7,9,11
- R2 : bits 2,3,6,7,10,11
- R3: bits 4,5,6,7
- R8: bits: 8,9,10,11





Reference from:-

<http://www.electronicshub.org/error-correction-and-detection-codes/>

3.2.4 Data Link Control and Protocols

Data-link layer is responsible for implementation of point-to-point flow and error control mechanism.

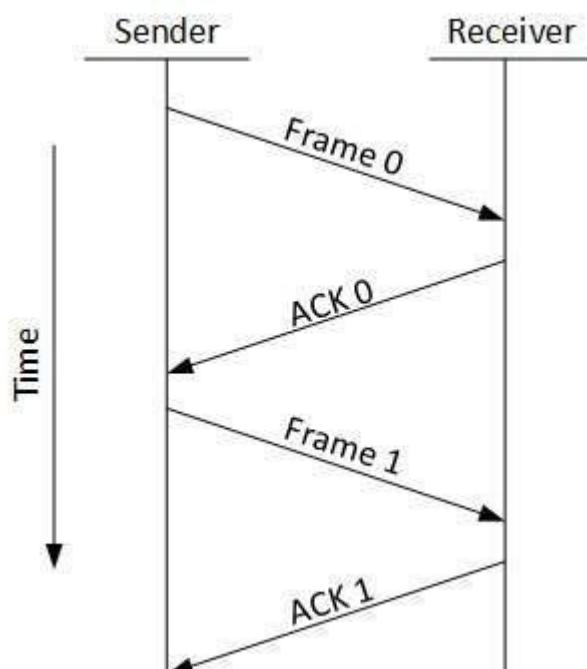
Flow Control

When a data frame (Layer-2 data) is sent from one host to another over a single medium, it is required that the sender and receiver should work at the same speed. That is, sender sends at a speed on which the receiver can process and accept the data. What if the speed (hardware/software) of the sender or receiver differs? If sender is sending too fast the receiver may be overloaded, (swamped) and data may be lost.

Two types of mechanisms can be deployed to control the flow:

- **Stop and Wait**

This flow control mechanism forces the sender after transmitting a data frame to stop and wait until the acknowledgement of the data-frame sent is received.



- **Sliding Window**

In this flow control mechanism, both sender and receiver agree on the number of data-frames after which the acknowledgement should be sent. As we learnt, stop and wait flow control mechanism wastes resources, this protocol tries to make use of underlying resources as much as possible.

Error Control

When data-frame is transmitted, there is a probability that data-frame may be lost in the transit or it is received corrupted. In both cases, the receiver does not receive the correct data-frame and sender does not know anything about any loss. In such case, both sender and receiver are equipped with some protocols which helps them to detect transit errors such as loss of data-frame. Hence, either the sender retransmits the data-frame or the receiver may request to resend the previous data-frame.

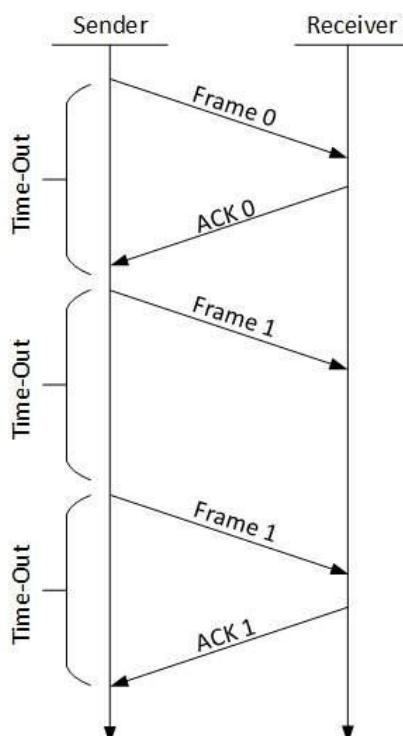
Requirements for error control mechanism:

- **Error detection** - The sender and receiver, either both or any, must ascertain that there is some error in the transit.
- **Positive ACK** - When the receiver receives a correct frame, it should acknowledge it.
- **Negative ACK** - When the receiver receives a damaged frame or a duplicate frame, it sends a NACK back to the sender and the sender must retransmit the correct frame.
- **Retransmission:** The sender maintains a clock and sets a timeout period. If an acknowledgement of a data-frame previously

transmitted does not arrive before the timeout the sender retransmits the frame, thinking that the frame or its acknowledgement is lost in transit.

There are three types of techniques available which Data-link layer may deploy to control the errors by Automatic Repeat Requests (ARQ):

- Stop-and-wait ARQ



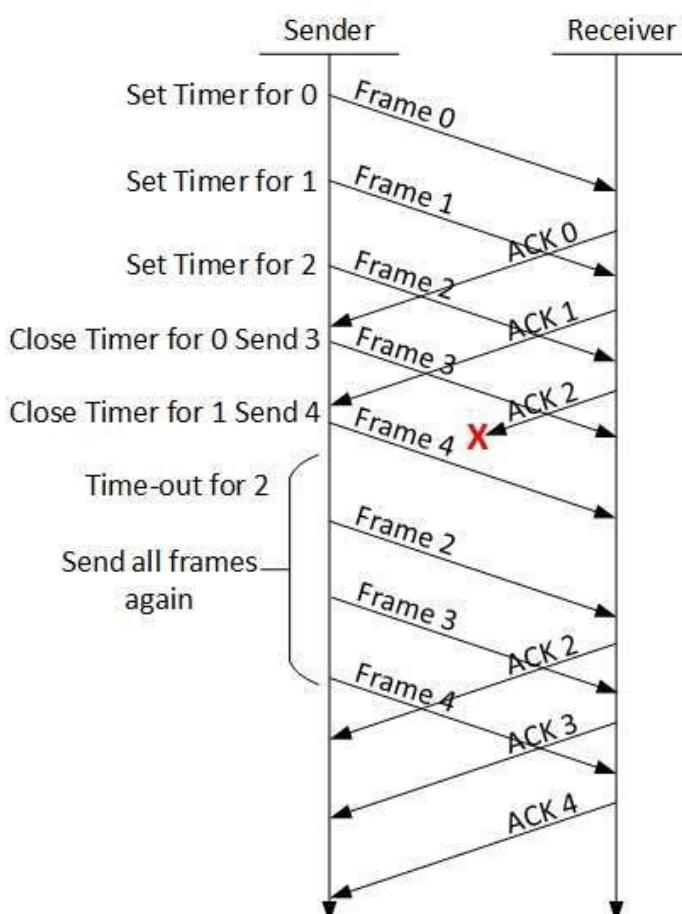
The following transition may occur in Stop-and-Wait ARQ:

- The sender maintains a timeout counter.
- When a frame is sent, the sender starts the timeout counter.
- If acknowledgement of frame comes in time, the sender transmits the next frame in queue.
- If acknowledgement does not come in time, the sender assumes that either the frame or its acknowledgement is lost in transit.

- Sender retransmits the frame and starts the timeout counter.**
- If a negative acknowledgement is received, the sender retransmits the frame.

• Go-Back-N ARQ

Stop and wait ARQ mechanism does not utilize the resources at their best. When the acknowledgement is received, the sender sits idle and does nothing. In Go-Back-N ARQ method, both sender and receiver maintain a window.



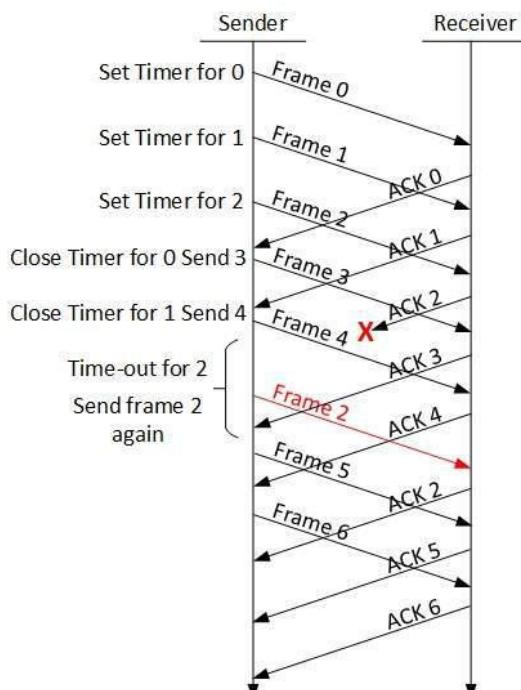
The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones. The receiving-window enables the receiver to receive multiple frames and acknowledge them.

The receiver keeps track of incoming frame's sequence number.

When the sender sends all the frames in window, it checks up to what sequence number it has received positive acknowledgement. If all frames are positively acknowledged, the sender sends next set of frames. If sender finds that it has received NACK or has not receive any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK.

- **Selective Repeat ARQ**

In Go-back-N ARQ, it is assumed that the receiver does not have any buffer space for its window size and has to process each frame as it comes. This enforces the sender to retransmit all the frames which are not acknowledged.



In Selective-Repeat ARQ, the receiver while keeping track of sequence numbers, buffers the frames in memory and sends NACK for only frame which is missing or damaged.

The sender in this case, sends only packet for which NACK is received.

Reference from:-

https://www.tutorialspoint.com/data_communication_computer_network/data_link_control_and_protocols.htm

3.2.5 Multiple Access Protocol : CSMA/CD , LAN , Ethernet

WHAT IS A MULTIPLE ACCESS PROTOCOL?

- Multiple access protocol is used to coordinate access to the link.
- Nodes can regulate their transmission onto the shared broadcast channel by using access protocol.
- It is used both wired and wireless local area network
And Satellite network.
- All nodes are capable of transmitting Frame, more than two nodes can transmit frames at the same time.
- If so, the transmitted frames collide at all of the receivers.

REFERENCE

- Google

definition

NETWORK LINK:

- 1) Point-to-point link
- 2) broadcast link

1) Point-to-point link:

It consists of a single sender at one end of the link and a single receiver at the other end of the link.

2) Broadcast link:

It can have multiple sending and receiving nodes all connected to the same, single shared broadcast channel.

Example: Ethernet, wireless LAN

REFERENCE
- WWW.SLIDEShare.NET

MULTIPLE-ACCESS-PROTOCOLS:

We can consider the data link layer as two sub layers. The upper sub layer is responsible for data link control, and the lower sub layer is responsible for resolving access to the shared media.

- Many formal protocols have been devised to handle access to a shared link. We categorize them into 3 groups..
- 1-random access protocols
- 2-controlled access protocols
- 3-channelization protocols

- In random access or contention methods, no station is superior to another station and none is assigned the control over another.

REFERENCE
- EXAMRADAR.COM

RANDOM -ACCESS-PROTOCOL

EXAMPLE-CSMA/CD

FULL-FORM-CARRIER SENSE MULTIPLE ACCESS/COLLISION

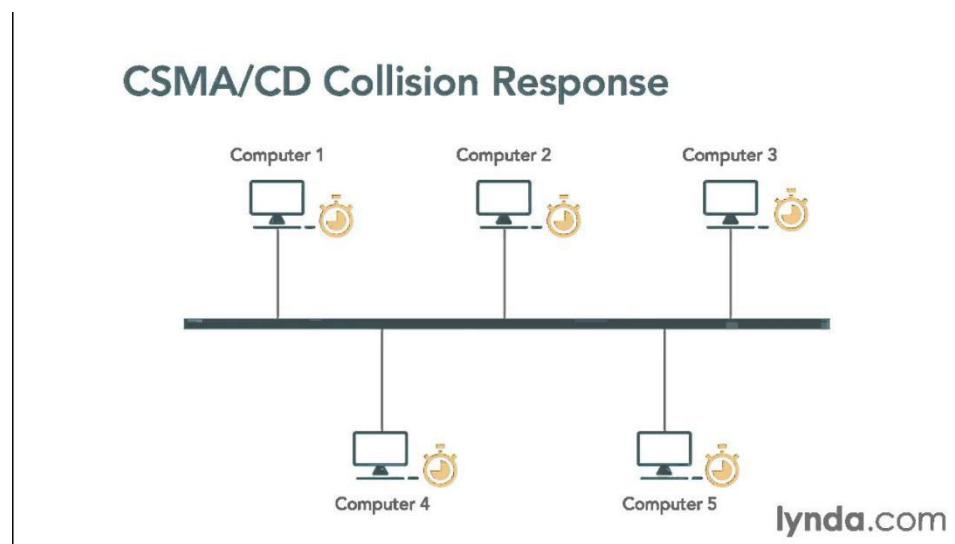
->CSMA

RULES OF CSMA/CD

-CARRIER SENSING

-COLLISION DETECTION

CSMA/CD:



Reference :

<https://i.ytimg.com/vi/xLsejOjV9aY/maxresdefault.jpg>

-carrier sensing, deferral as in CSMA

-collisions detected within short time

-colliding transmissions aborted, reducing channel wastage

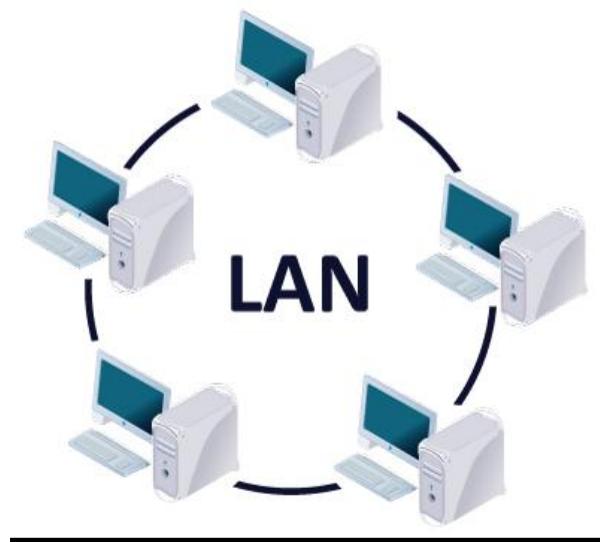
Collision detection:

- easy in wired LANs: measure signal strengths, compare transmitted, received signals
- difficult in wireless LANs: receiver shut off while transmitting

Human analogy

- the polite conversationalist
- > collision are detected within a few bit times transmission is then aborted, reducing the channel wastage considerably.
- >persistent retransmission is implemented collision.

LANs:ETHERNET:



Reference :

<http://catalog.wlimg.com/5/524841/other-images/table-435564.jpg>

Collision detection is in wired LANs.

Collision detection cannot be done in wireless LANs

CSMA/CD approach channel utilization=1 in LANs:

- Low ratio of propagation over frame transmission time.

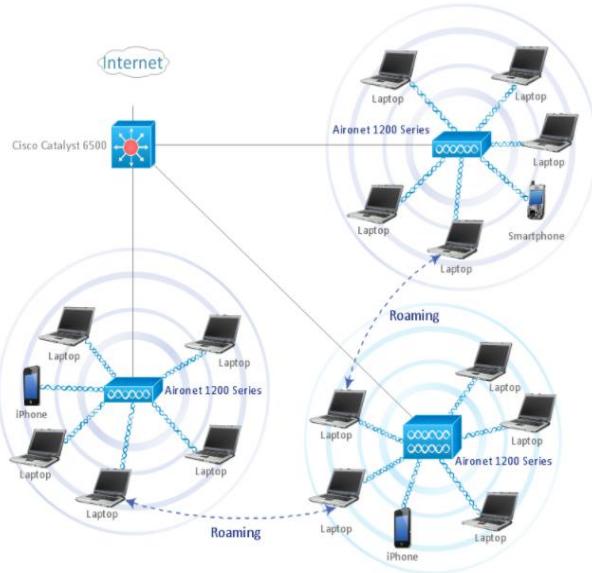
REFERENCE -SLIDEShare.NET

- Ethernet is a family of computer network technologies for local area network (LAN) and larger networks.
- A LAN market has seen several such as Ethernet, token ring, FDDI etc..
- They have been used for satellite and wireless channels.
- when a user is accesses the internet from a university or corporate campus, the access is almost always by way of a LAN.
- The LAN us a single link between each user host and the router; it therefore uses a link –layer protocol, which incorporates a multiple access protocol.

Reference - www.net.t-labs.tu-berlin.de

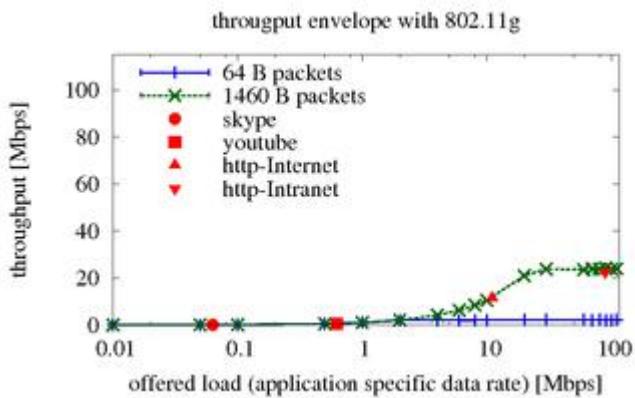
3.2.6 Introduction : Wireless LAN, Connecting devices, Repeaters, Hubs, Bridges, Switches, Concept of VLAN

A wireless local area network (WLAN) is a wireless computer network that links two or more devices using a wireless distribution method (often spread-spectrum or OFDM radio) within a limited area such as a home, school, computer laboratory, or office building. This gives users the ability to move around within a local coverage area and yet still be connected to the network. A WLAN can also provide a connection to the wider Internet.

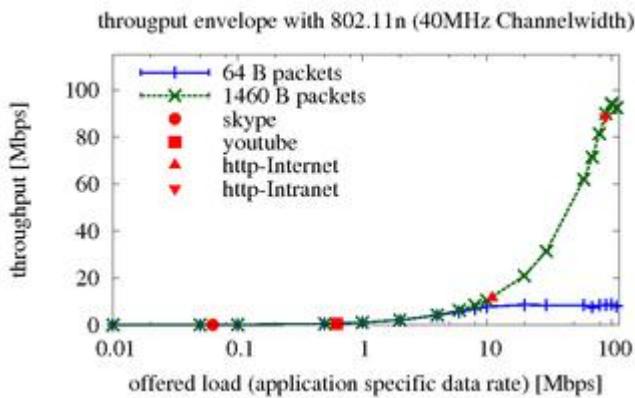


WIRELESS LAN

WLAN, organised in various layer 2 variants (IEEE 802.11), has different characteristics. Across all flavours of 802.11, maximum achievable throughputs are either given based on measurements under ideal conditions or in the layer 2 data rates. This, however, does not apply to typical deployments in which data are being transferred between two endpoints of which at least one is typically connected to a wired infrastructure and the other endpoint is connected to an infrastructure via a wireless link.



Graphical representation of [Wi-Fi](#) application specific (UDP) performance envelope 2.4 GHz band, with 802.11g



Graphical representation of [Wi-Fi](#) application specific (UDP) performance envelope 2.4 GHz band, with 802.11n with 40 MHz

This means that typically data frames pass an 802.11 (WLAN) medium and are being converted to 802.3 (Ethernet) or vice versa.

Due to the difference in the frame (header) lengths of these two media, the packet size of an application determines the speed of the data transfer. This means that an application which uses small packets (e.g. VoIP) creates a data flow with a high overhead traffic (e.g. a low good put).

Other factors which contribute to the overall application data rate are the speed with which the application transmits the packets (i.e. the data rate) and the energy with which the wireless signal is received.

The latter is determined by distance and by the configured output power of the communicating devices.

Same references apply to the attached throughput graphs which show measurements of UDP throughput measurements. Each represents an average (UDP) throughput (the error bars are there, but barely visible due to the small variation) of 25 measurements.

Each is with a specific packet size (small or large) and with a specific data rate (10 Kbit/s – 100 Mbit/s). Markers for traffic profiles of common applications are included as well. This text and measurements do not cover packet errors but information about this can be found at above references. The table below shows the maximum achievable (application specific) UDP throughput in the same scenarios (same references again) with various difference WLAN (802.11) flavours. The measurement hosts have been 25 meters apart from each other; loss is again ignored.

Image link : <http://www.conceptdraw.com/How-To-Guide/wireless-network-wlan>

Details_of_Described_topic_link:

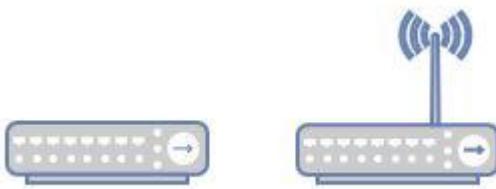
https://en.wikipedia.org/wiki/Wireless_LAN

Hubs

A hub, also called a network hub, is a common connection point for devices in a network. Hubs are devices commonly used to connect segments of a LAN. The hub contains multiple ports. When a packet arrives at one port, it is copied to the other

ports so that all segments of the LAN can see all packets.

Hubs and switches serve as a central connection for all of your network equipment and handles a data type known as frames. Frames carry your data. When a frame is received, it is amplified and then transmitted on to the port of the destination PC.



In a hub, a frame is passed along or "broadcast" to every one of its ports. It doesn't matter that the frame is only destined for one port. The hub has no way of distinguishing which port a frame should be sent to. Passing it along to every port ensures that it will reach its intended destination. This places a lot of traffic on the network and can lead to poor network response times.

Compared to a standard switch, the hub is slower as it can send or receive information just not at the same time, but typically costs more than a hub.

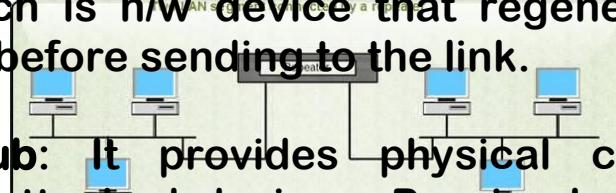
Hub is used to create connections between stations in a physical star topology. Hub is a central n/w device that connects network nodes. It is also referred as concentrators. It enables central n/w management. It can have multiple inputs & outputs all active at one time. It Permits large numbers of computer to be connected on a single or multiple LANs. It enables high speed communication. Provide connection for several different media types. (Coaxial, fiber optic, twisted pair).

There is Full Description of Type of Hubs :

Basically three types of hub

1. Active Hub
2. Passive Hub
3. Intelligent Hub .

1.Active Hub : Most hubs are active in that they regenerate and retransmit the signals the same way a repeater does. In fact. Because hubs usually have eight to twelve ports for computers to connect to, they are often called multi port repeaters. Active hubs need electrical power to run It contains a repeater which is h/w device that regenerates the received bits before sending to the link.



2.Passive Hub: It provides physical connection between the attached devices. Passive hubs act as connection points and do not amplify or regenerate the signal; the signal passes through the hub. Passive hubs do not require electricity to run.

3. Intelligent Hubs : Intelligent hubs' are enhanced active hubs. It will accommodate several different types of cables. A hub—based network can be expanded by connecting more than one hub. It also has functions which can add intelligence to a hub like Hub management (control the hub) and switching hub (which includes circuitry that very quickly routes signals between ports).

Refrence link :

<http://www.webopedia.com/TERM/H/hub.html>

Repeaters

A [network](#) device used to regenerate or replicate a signal. Repeaters are used in transmission systems to regenerate [analog](#) or [digital](#) signals distorted by transmission loss. Analog repeaters frequently can only amplify the signal while digital repeaters can reconstruct a signal to near its original quality. In a data network, a repeater can relay messages between subnetworks that use different [protocols](#) or cable types. [Hubs](#) can operate as repeaters by relaying messages to all connected computers. A repeater cannot do the intelligent [routing](#) performed by [bridges](#) and [routers](#).

- A repeater connects two segments of your network cable. It retimes and regenerates the signals to proper amplitudes and sends them to the other segments. When talking about, ethernet topology, you are probably talking about using a hub as a repeater. Repeaters require a small amount of time to regenerate the signal. This can cause a propagation delay which can affect network communication when there are several repeaters in a row. Many network architectures limit the number of repeaters that can be used in a row. Repeaters

work only at the physical layer of the OSI network model.

- These types of network repeaters make it easy to connect with different types of media too. This is necessary because of the fact that different countries and cities use different types of network repeaters and mediums around the world depending upon affordability and technological advancement. There is one issue with certain types of network repeaters such as analogue and digital repeaters- they cannot filter through the traffic because of which the transmission of signals is difficult and communication may be difficult. In addition to this there are certain types of network environments that network repeaters are not able to work across because of the fact that they just are not compatible with them for numerous reasons.
- It is shown that maximum four repeaters are used to extend Ethernet segments into a single Ethernet network. However, connection between two segments can be extended over a long distance by using fiber modems. This is, known as Fiber Optic Intra Repeater Link (FOIRL).

Classification of Repeaters:-

- Repeaters can be classified into two categories. These are local and remote repeaters. Local repeaters are used to connect LAN segments separated by a very small distance.
- Remote repeaters are used to connect LAN segments that are far from each other. A transmission line known as a link segment is provided between two remote repeaters. No nodes can be connected to this line.
- Figure :

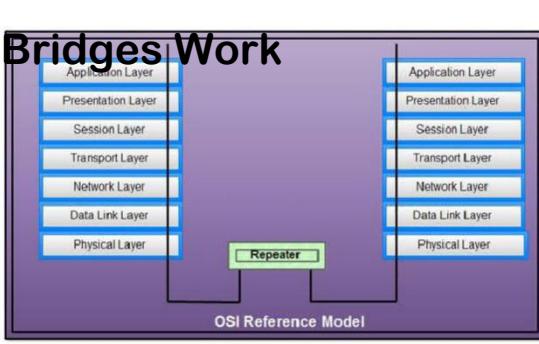
Refrence_Link:

<http://www.webopedia.com/TERM/R/repeater.html>

Bridges

A network bridge helps to join two otherwise separate computer networks together to enable communication between them. Bridge devices are used with local area networks (LANs) for extending their reach to cover larger physical areas.

How Network Bridges Work



Bridge devices inspect incoming network traffic and determine whether to forward or discard it according to its intended destination. An Ethernet bridge, for example, inspects each incoming Ethernet frame - including the source and destination MAC addresses, and sometimes the frame size - in making individual forwarding decisions.

Bridge devices operate at the data link layer (Layer 2) of the OSI model.

Types of Network Bridges

Several different kinds of bridge devices exist, each designed for specific kinds of networks including

Wireless bridges - support Wi-Fi wireless access points

Wi-Fi Ethernet bridges - allows connecting Ethernet clients and interfacing them to a local Wi-Fi network, useful for older network devices that lack Wi-Fi capability.

Wireless Bridging

Bridging is especially popular on Wi-Fi computer networks. In Wi-Fi, wireless bridging requires access points communicate with each other in a special mode that supports the traffic needing to flow between them. Two access points that support wireless bridging mode work in pairs. Each continues to support their own local networks of connected clients while additionally communicating with the other to handle bridging traffic.

Network professionals sometimes use the term "BSS" - Basic Service Set - to refer to an access point and its local clients.

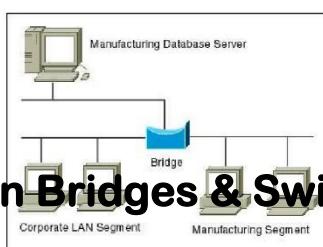
Wireless bridging joins two BSS networks together.

Bridging mode can be activated on an access point through an administrative setting or sometimes a physical switch on the unit. Not all access points support wireless bridging mode; consult the manufacturer's documentation to determine whether a given model supports this feature.

For more, see: [What Wireless Bridging Can Do For Computer Networks](#).

Difference Between Bridges and Repeaters

Bridge and network repeater devices share a similar physical appearance; sometimes, a single unit performs both functions. Unlike bridges, however, repeaters do not perform any traffic filtering and do not join two networks together but instead pass along all traffic they receive. Repeaters serve primarily to regenerate traffic signals so that a single network can reach longer physical distances.



Difference between Bridges & Switches and Routers :

In wired computer networks, bridges serve a similar function as network switches. Traditional wired bridges support one incoming and one outgoing network connection (accessible through a hardware port), whereas switches usually offer four or more

hardware ports. Switches are sometimes called multi-port bridges for this reason.

Likewise, bridges lack the intelligence of network routers: Bridges do not understand the concept of remote networks and cannot redirect messages to different locations dynamically but instead support only one outside interface.

- A bridge is a computer networking device that builds the connection with the other bridge networks which use the same protocol. It works at the Data Link layer of the OSI Model and connects the different networks together and develops communication between them. It connects two local-area networks; two physical LANs into larger logical LAN or two segments of the same LAN that use the same protocol.
- Apart from building up larger networks, bridges are also used to segment larger networks into smaller portions.
- The bridge does so by placing itself between the two portions of two physical networks and controlling the flow of the data between them.
- Bridges nominate to forward the data after inspecting into the MAC address of the devices connected to every segment. The forwarding of the addresses.

- Data is dependent on the acknowledgement of the fact that the destination address resides on some other interface.
- It has the capacity to block the incoming flow of data as well. Today Learning bridges have been introduced that build a list of the MAC addresses on the interface by observing the traffic on the network.
- This is a leap in the development field of manually recording of MAC.

Types of Bridges

- There are mainly three types in which bridges can be characterized:

- I. Transparent Bridge
- II. Translation Bridge
- III. Source Route Bridge

Link : <https://www.lifewire.com/how-network-bridges-work-816357>

Switches

A switch is a device in a [computer network](#) that electrically and logically connects together other devices. Multiple data cables are plugged into a switch to enable communication between different networked devices. Switches manage the flow of data across a network by transmitting a received [network packet](#) only to the one or more devices for which the packet is intended. Each



networked device connected to a switch can be identified by its [network address](#), allowing the switch to regulate the flow of traffic. This maximizes the security and efficiency of the network.

When a [repeater hub](#) is replaced with an Ethernet switch, the single large [collision domain](#) used by the hub is split up into smaller ones, reducing or eliminating the possibility and scope of [collisions](#) and, as a result, increasing the potential [throughput](#).

Because [broadcasts](#) are still being forwarded to all connected devices, the newly formed [network segment](#) continues to be a [broadcast domain](#).

A switch is more intelligent than a repeater hub, which simply retransmits packets out of every port of the hub except the port on which the packet was received, unable to distinguish different recipients, and achieving an overall lower network efficiency.

Network design

An Ethernet switch operates at the [data link layer](#) (layer 2) of the [OSI model](#) to create a separate [collision domain](#) for each switch port. Each device connected to a switch port can transfer data to any of the other ones at a time, and the transmissions will not interfere – with the limitation that, in [half duplex](#) mode, each switch port can only either receive from or transmit to its connected device at a certain time. In [full duplex](#) mode, each switch port can simultaneously transmit and receive, assuming the connected device also supports full duplex mode.

In the case of using a [repeater hub](#), only a single transmission could take place at a time for all ports combined, so they would all share the bandwidth and run in [half duplex](#). Necessary arbitration would also result in collisions, requiring retransmissions.

Applications

The network switch plays an integral role in most modern [Ethernet local area networks](#) (LANs). Mid-to-large sized LANs contain a number of linked [managed](#) switches. [Small office/home office](#) (SOHO) applications typically use a single switch, or an all-purpose [converged device](#) such as a [residential gateway](#) to access small office/home [broadband](#) services such as [DSL](#) or [cable Internet](#). In most of these cases, the end-user device contains a [router](#) and components that interface to the particular physical broadband technology. User devices may also include a telephone interface for [Voice over IP](#) (VoIP) protocol.

Reference link :

https://en.wikipedia.org/wiki/Network_switch

Info of VLAN

-by John Burke

A local area network, or [LAN](#), provides the nodes connected to it with direct ([Layer 2](#)) access to one another. It is usually comprised of one or more [Ethernet](#) switches. Computers on different LANs talk to each other using [Layer 3](#) (IP), via a [router](#).

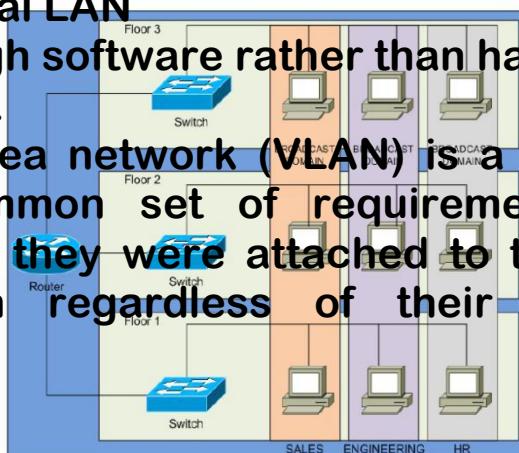
A virtual LAN (VLAN) abstracts the idea of the LAN; A VLAN might comprise a subset of the ports on a single [switch](#) or subsets of ports on multiple switches. By default, systems on one VLAN don't see the traffic associated with systems on other VLANs on the same network.

VLANs allow network administrators to [partition](#) their networks to match the functional and security requirements of their systems without having to run

new cables or make major changes in their current network infrastructure. [IEEE](#)802.1Q is the standard defining VLANs; the VLAN identifier or tag consists of 12 bits in the Ethernet frame, creating an inherent limit of 4,096 VLANs on a LAN.

[Ports](#) on switches can be assigned to one or more VLANs, allowing systems to be divided into logical groups -- e.g., based on which department they are associated with -- and rules to be established about how systems in the separate groups are allowed to communicate with each other. These can range from the simple and practical (computers in one VLAN can see the printer on that VLAN, but computers outside that VLAN cannot), to the complex and legal (e.g., computers in the trading departments cannot interact with computers in the retail banking departments).

- VLAN stands for Virtual Local Area Network.
- viewed as a group of devices on different physical LAN
- can communicate with each other as if they were all on the same physical LAN
- Configured through software rather than hardware
- Extremely flexible.
- A virtual local area network (VLAN) is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain regardless of their physical location.



- A traditional LAN would require all users of the same requirements and same IP subnet (broadcast domain) be connected to the same equipment.

Traditional LAN:

-A traditional LAN would require all users of the same requirements and same IP subnet (broadcast domain) be connected to the same equipment.

VLAN based LAN

- By utilizing

VLANs, the same users can be spread out over various Geographical Locations and still Remain in their Same IP subnet (Broadcast Domain).

How VLAN works?

- VLANs are identified by a number Valid ranges 1-4094.

- On a VLAN-capable switch, you assign ports with the appropriate VLAN number.
- The switch then only allows data to be sent between ports with the same VLAN.
- Since almost every network is larger than a single switch, there needs to be a way to have traffic sent between two different switches.
- One way to do it is to assign a port on each switch with a VLAN and run a cable between the switches.
- Not very feasible or cost effective..

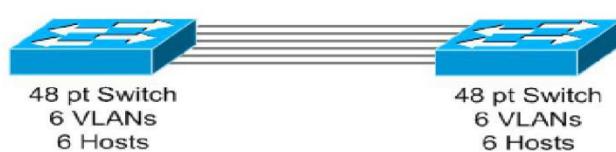
- For example, if there were 6 hosts on each switch on 6 different VLANs, you would need 6 ports on each switch to connect the switches together.
- This would mean that if you had 24 different VLANs you could only have 24 hosts on a 48 port switch.
- There was a standard developed to make it so that a single connection between two switches could be used to send traffic for all VLANs.
- 802.1q – Provides a VLAN tag in front of the Layer 2 frame.
- You enable 802.1q tagging (trunking) on the ports between the switches.
- The switch receives the frame with the 802.1q header and strips it off.
- It determines what VLAN and sends the data to the appropriate port.

Types of VLAN membership

- There are two types of VLAN membership methods exists:

- 1) Static
- 2) Dynamic

1) Static VLANs



- In a static VLAN , The network administrator creates a VLN and then assigns switch ports to the VLAN.
- Static VLANs are also called port based VLANs.
- The association with the VLAN does not change until the administrator changes the port assignment.
- The ports on a single switch can be assigning multiple VLANs.
- Even though two devices are connected to different ports on a same switch , traffic will not pass between them if the connected ports are on different VLANs.
- We need a 3 layer device (typically a router)to enable communication between two VLANs.

2) Dynamic VLANs

- In a dynamic VLAN ,the switch automatically assigns the port to a VLAN using info from the user device like MAC address ,IP address ,etc.
- When a device is connected to a switch port the switch queries the database to establish VLAN membership.
- Dynamic VLAN support instant movabilty of end Devices .
- When we move a device from a port on one switch to a port on another switch, the dynamic VLANs will automatically configure the membership of the VLAN.

Benefits of VLAN:

- Geographically separated users on the same IP subnet (broadcast domain).
- Limit the size of broadcast domains and limit broadcast activity.
- Security benefits by keep hosts separated by VLAN and limiting what devices can talk to those hosts.

- Cost savings as you don't need additional hardware and cabling.
- Operational benefits because changing a user's IP subnet (Broadcast Domain) is in software.

Reference link :

<http://searchnetworking.techtarget.com/definition/virtual-LAN>

3.3.1 Introduction to Network layer

Network Layer :

Layer-3 in the OSI model is called Network layer out of the 7 layers.

Network layer takes the responsibility for routing packets from source to destination within or outside a subnet. Two different subnet may have different addressing schemes or non-compatible addressing types. Same with protocols, two different subnet may be operating on different protocols which are not compatible with each other. Network layer has the responsibility to route the packets from source to destination, mapping different addressing schemes and protocols.

Network layer manages options pertaining to host and network addressing, managing sub-networks, and internetworking.

Functionalities:

Devices which work on Network Layer mainly focus on routing. Routing may include various tasks to achieve a single goal. These can be:

- Addressing devices and networks.

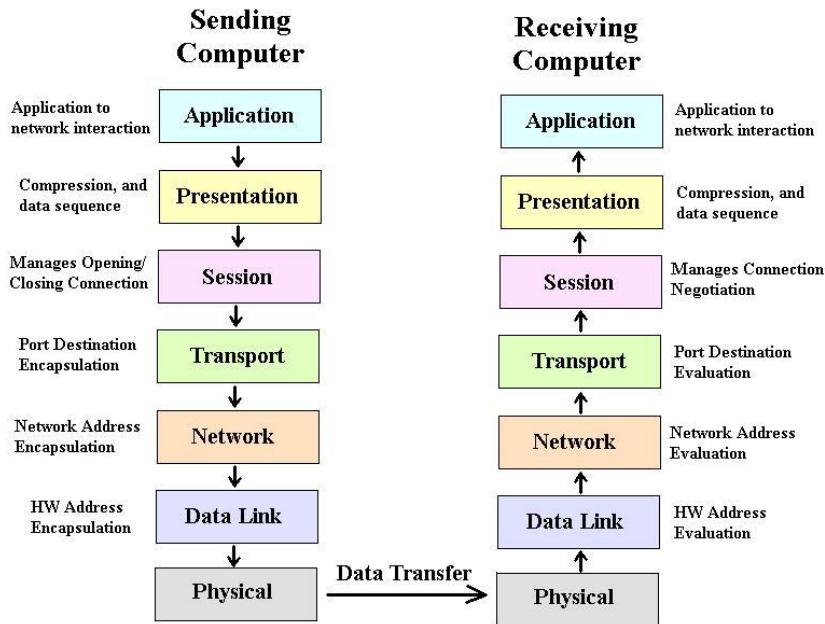
- Populating routing tables or static routes.
- Queuing incoming and outgoing data and then forwarding them according to quality of service constraints set for those packets.
- Internetworking between two different subnets.
- Delivering packets to destination with best efforts.
- Provides connection oriented and connection less mechanism.

Features

- Quality of service management
- Load balancing and link management
- Security
- Interrelation of different protocols and subnets with different schema.
- Different logical network design over the physical network design.
- L3 VPN and tunnels can be used to provide end to end dedicated connectivity.

Internet protocol is widely respected and deployed Network Layer protocol which helps to communicate end to end devices over the internet. It comes in two flavours. IPv4 which has ruled the world for decades but now is running out of address space. IPv6 is created to replace IPv4 and hopefully mitigates limitations of IPv4 too.

Network Layer Interaction



Reference :

Bibliography

https://www.tutorialspoint.com/data_communication_computer_network/network_layer_introduction.htm
image:

<http://www.comptechdoc.org/independent/networking/protocol/protlayers.html>

3.3.2 Connectionless Service

Connectionless Service :-

A connectionless service is a concept in data communications used to transfer data at the transport layer (layer 4) of the OSI model. It describes the communication between two nodes or terminals in which data is sent from one node to the other without first ensuring that the destination is

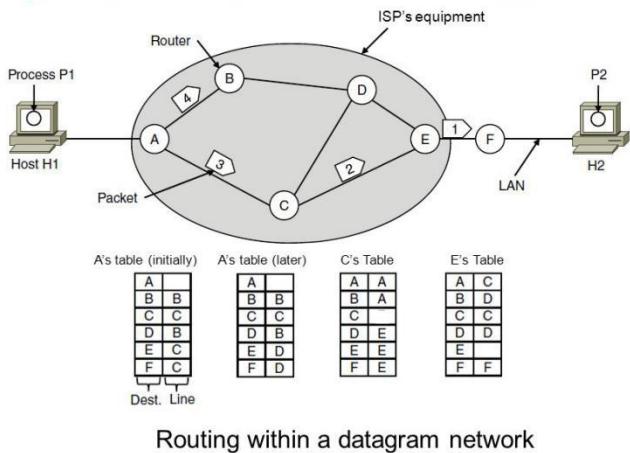
available and ready to receive the data. A session connection between the sender and the receiver is not required, the sender just starts sending the data. The message or datagram is sent without prior arrangement, which is less reliable but provides faster transaction than a connection-oriented service.

User Datagram Protocol (UDP) is a connectionless protocol, while Transmission Control Protocol (TCP) is a connection-oriented network protocol.

Connectionless service means that a terminal or node can send data packets to its destination without establishing a connection to the destination. This works because of error handling protocols, which allow for error correction like requesting retransmission. LANs are actually connectionless systems with each computer able to transmit data packets as soon as it can access the network.

The Internet is a large connectionless packet network in which all packet delivery is handled by Internet providers. TCP adds connection-oriented services in addition to IP when required. TCP can provide all the top level connection services required to ensure proper data delivery.

Implementation of Connectionless Service



Computer Networks, Fifth Edition by Andrew Tanenbaum and David Wetherall, © Pearson Education-Prentice Hall, 2011

Reference :

<https://www.techopedia.com/definition/26229/connectionless-service>

<https://www.slideshare.net/kashyapdavariya/computer-network-ppt-9714464>

3.3.3 Connection Oriented Services

Connection Oriented Service:-

A connection-oriented service is a technique used to transport data at the session layer. Unlike its opposite, connectionless service, connection-oriented service requires that a session connection to be established between the sender and receiver, similar to a phone call. This method is normally considered to be more reliable than a connectionless service, although not all connection-oriented

protocols are considered reliable.

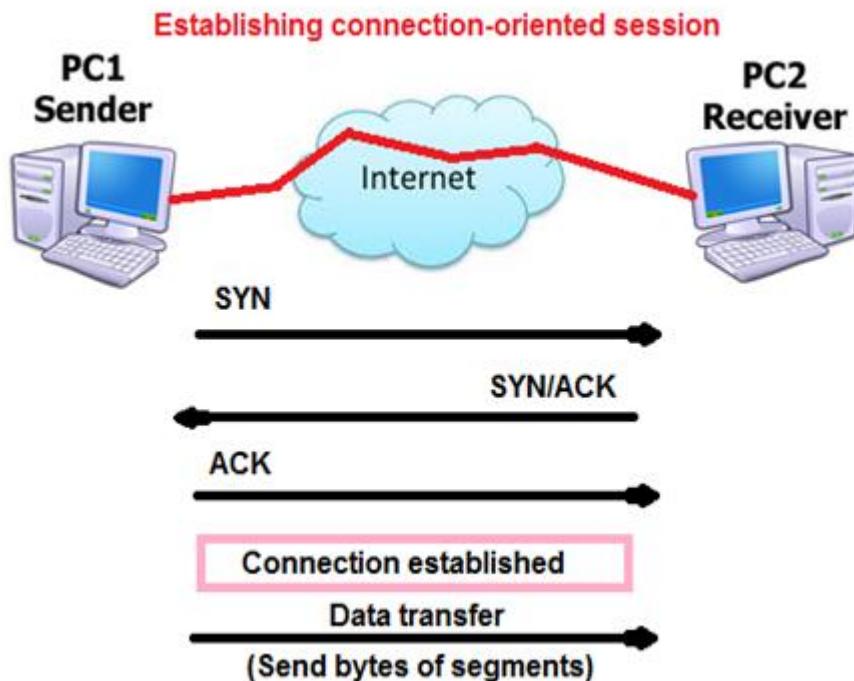
A connection-oriented service can be a circuit-switched connection or a virtual circuit connection in a packet-switched network. For the latter, traffic flows are identified by a connection identifier, typically a small integer of 10 to 24 bits. This is used instead of listing the destination and source addresses.

A connection-oriented service needs an established connection between peers before data can be sent between the connected terminals. This handles real-time traffic more efficiently than connectionless protocols because data arrives in the same order as it was sent. Connection-oriented protocols are also less error-prone.

Asynchronous transfer mode is a connection-oriented service, and it has yet to be replaced by Ethernet for carrying real-time and isochronous traffic streams. Increasing bandwidth does not always solve service problems. A good connection-oriented service can often deliver more quality than large bandwidth. Even so, some connection-oriented services have been made to accommodate both connectionless and connection-oriented data.

In a connection-oriented, packet-switched data link layer or network layer protocol, all data is sent over the same path during a communication session. The protocol does not have to provide each packet with routing information (complete source and destination address), but only with a channel/data stream number, often called a virtual circuit identifier (VCI). Routing information may be provided to the network nodes during the connection establishment phase, where the VCI is defined in tables in each node. Thus,

the actual packet switching and data transfer can be taken care of by fast hardware, as opposed to slow, software-based routing.



Reference :

<https://www.techopedia.com/definition/26230/connection-oriented-service>

<https://people.emich.edu/gmoreno/Culminating/HowToCreate.html>

image: <http://www.cnt4all.com>

3.3.4 Internetworking , Addressing

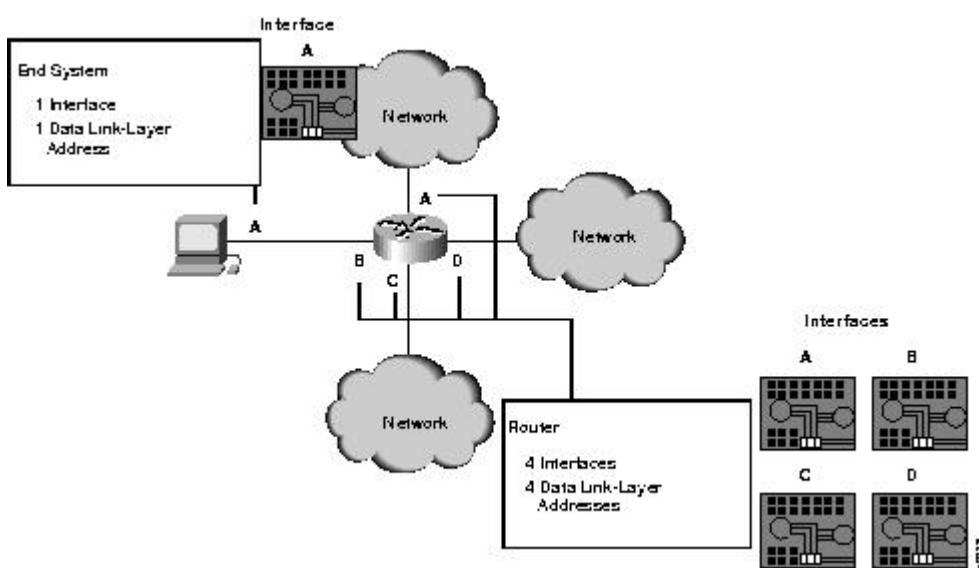
- **Internet Addressing**

Internet addresses identify devices separately or as members s of a group. Addressing schemes vary depending on the protocol family and the OSI layer. Three types of internet addresses are commonly used: **data-link layer addresses, Media Access Control (MAC) addresses, and network-layer addresses.**

Data Link Layer:

A data-link layer address uniquely identifies each physical network connection of a network device. Data-link addresses sometimes are referred to as **physical** or **hardware** addresses. Data-link addresses usually exist within a **flat address space** and have a pre-established and typically fixed relationship to a specific device.

End systems generally have only one physical network connection, and thus have only one data-link address. Routers and other internetworking devices typically have multiple physical network connections and therefore also have multiple data-link addresses.

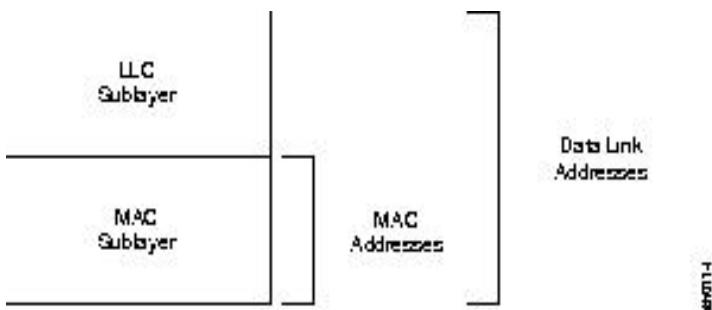


MAC

Address:

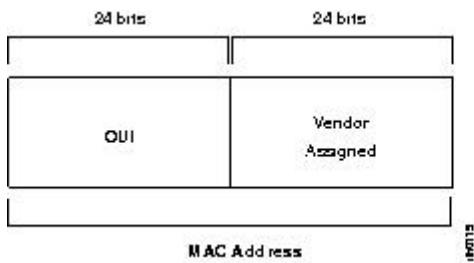
Media Access Control (MAC) addresses [consist of](#) a subset of data-link layer addresses. MAC addresses identify network entities in LANs [that](#) implement the IEEE MAC addresses of the data-link layer. [As with](#) most data-link addresses, MAC addresses are unique for each LAN interface.

MAC addresses, data-link addresses, and the IEEE sublayers of the data-link layer are all related.



MAC addresses are 48 bits in length and are expressed as 12 hexadecimal digits. The first 6 hexadecimal digits, [which are administered by the IEEE](#), [identify](#) the manufacturer or vendor [and thus comprise](#) the Organizational Unique Identifier (OUI). The last 6 hexadecimal digits [comprise](#) the interface

serial number, or another value administered by the specific vendor. MAC addresses sometimes are called burned-in addresses (BIAs) because they are burned into read-only memory (ROM) and are copied into random-access memory (RAM) when the interface card initializes.



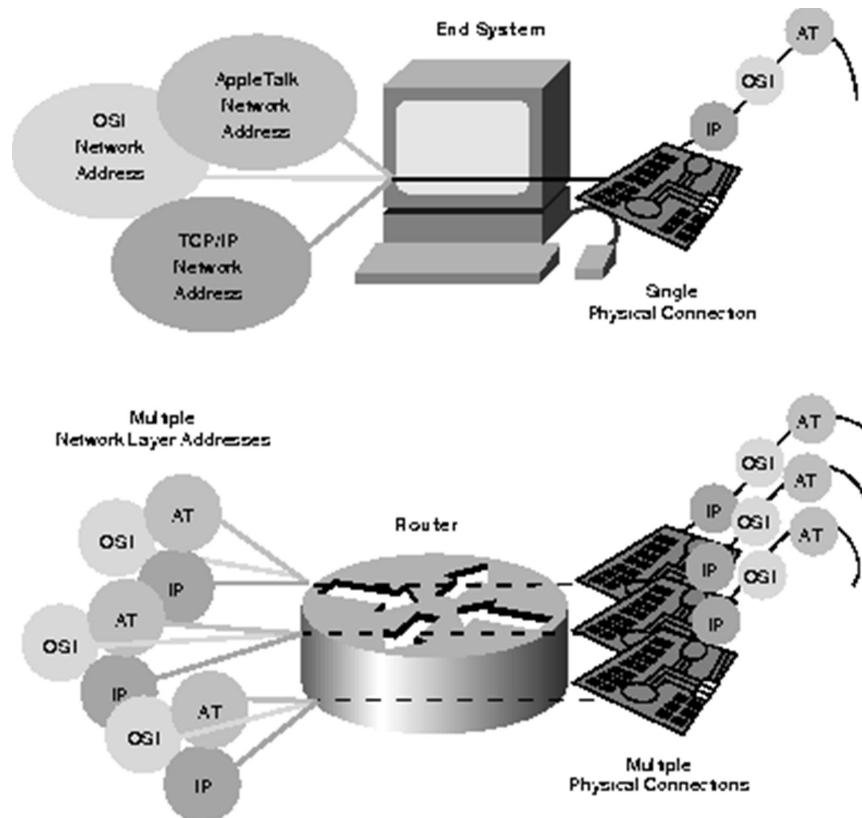
Network -Layer Address:

A network-layer address identifies an entity at the network layer of the OSI layers. Network addresses usually exist within a hierarchical address space and sometimes are called *virtual* or *logical* addresses.

The relationship between a network address and a device is logical and unfixed; it typically is based either on physical network characteristics (the device is on a particular network segment) or on groupings that have no physical basis (the device is part of an AppleTalk zone). End systems require one network-layer address for each network-layer protocol they support. (This assumes that the device has only one physical network connection.) Routers and other internetworking devices require one network-layer address per physical network connection for each network-layer protocol supported. A router, for example, with three

interfaces each running AppleTalk, TCP/IP, and OSI must have three network layer addresses for each interface. The router therefore has nine network layer addresses.

Each network interface must be assigned a network address for each protocol supported.



Reference :

<https://www.cisco.com/cpress/cc/td/cpress/fund/ith/ith01gb.htm>

3.3.5 Routing Algorithms

Routing Algorithm :-

Several intradomain and interdomain routing protocols are in use. In this section, we cover only the most popular ones. We discuss two intradomain routing protocols: We also introduce one interdomain routing protocol: path vector.

- 1). Distance Vector Routing**
- 2). Link State Routing**

Routing Information Protocol (RIP) is an implementation of the distance vector protocol. Open Shortest Path First (OSPF) is an implementation of the link state protocol.

Border Gateway Protocol (BGP) is an implementation of the path vector protocol.

1. Distance Vector Routing :-

In distance vector routing, the least-cost route between any two nodes is the route with minimum distance. In this protocol, as the name implies, each node maintains a vector (table) of minimum distances to every node. The table at each node also guides the packets to the desired node by showing the next stop in the route (next-hop routing).

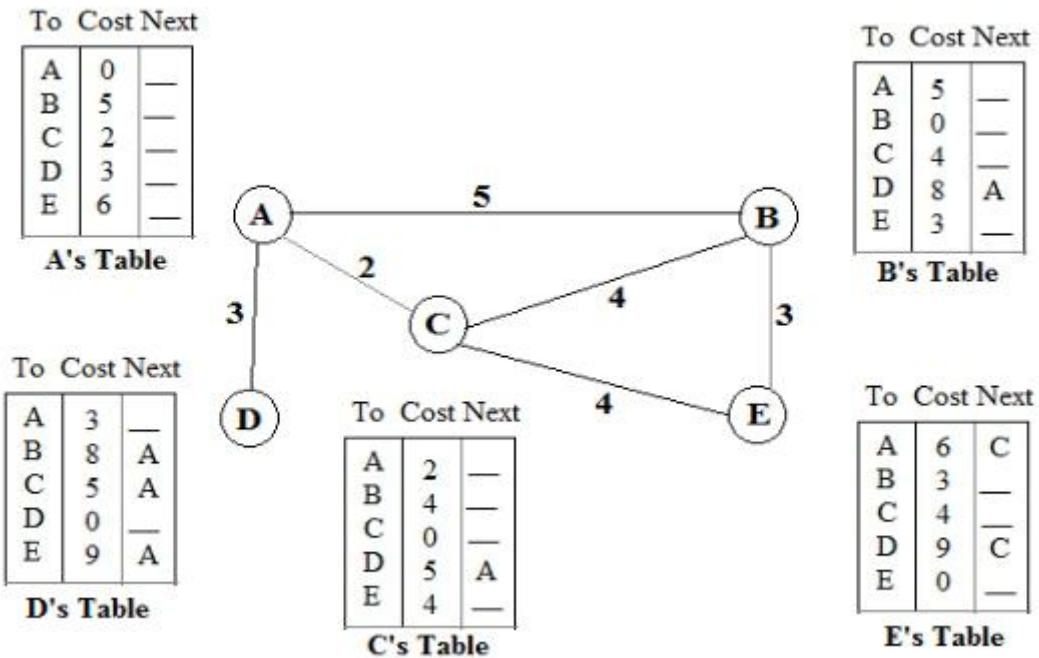


Figure (a), Distance Vector Routing Table

In Figure (a), we show a system of five nodes with their corresponding table.

We can think of nodes as the cities in an area and the lines as the roads connecting them. A table can show a tourist the minimum distance between cities.

The table for node A shows how we can reach any node from this node. For example, our least cost to reach node E is 6. The route passes through C.

Initialisation:-

The tables in Figure (a) are stable; each node knows how to reach any other node and the cost. At the beginning, however, this is not the case. Each node can know only the distance between itself and its immediate neighbours, those directly connected to it.

So for the moment, we assume that each node can send a message to the immediate neighbours and find the distance between itself and these neighbours. Figure (b) shows the initial tables for each node. The distance for any entry that is not a neighbour is marked as infinite (unreachable).

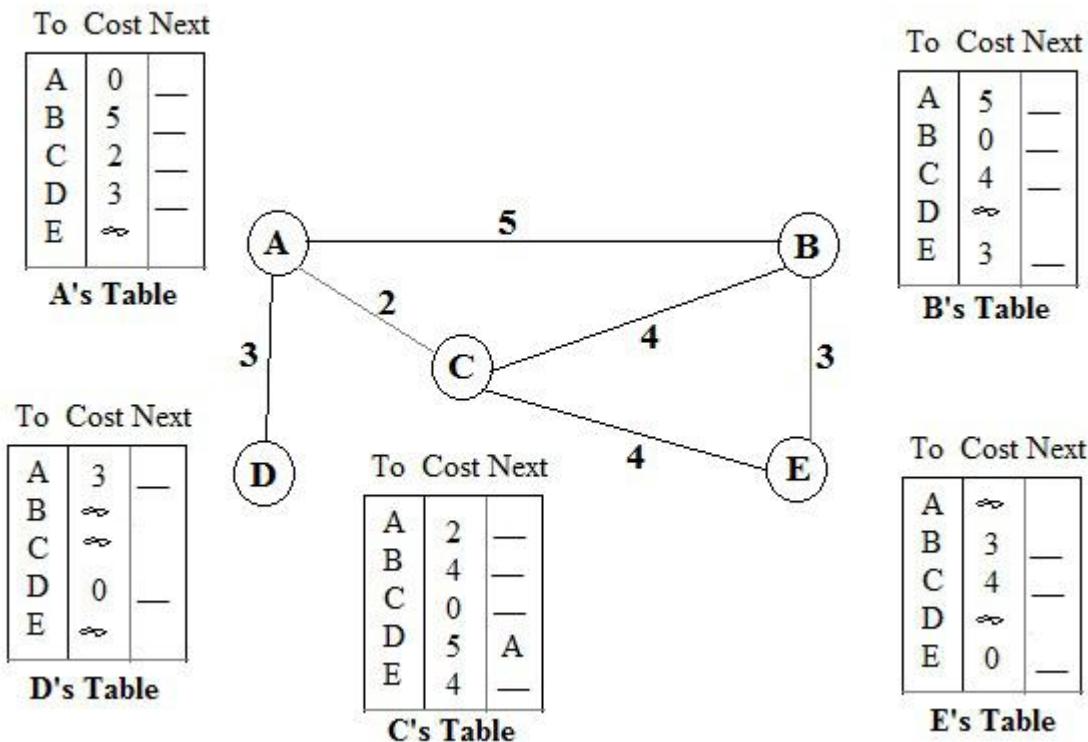


Figure (b). Initialisation of Table in Distance vector routing

Sharing:-

The whole idea of distance vector routing is the sharing of information between neighbours. Although node A does not know about node E, node C does. So if node C shares its routing table with A, node A can also know how to reach node E. On the other hand, node C does not know how to reach node D, but node A does. If node A shares its routing table with node C,

node C also knows how to reach node D. In other words, nodes A and C, as immediate neighbours, can improve their routing tables if they help each other.

There is only one problem. How much of the table must be shared with each neighbour? A node is not aware of a neighbour's table. The best solution for each node is to send its entire table to the neighbours and let the neighbours decide what part to use and what part to discard. However, the third column of a table (next stop) is not useful for the neighbours. When the neighbours receive a table, this column needs to be replaced with the sender's name. If any of the rows can be used, the next node is the sender of the table. A node therefore can send only the first two columns of its table to any neighbours. In other words, sharing here means sharing only the first two columns.

Updating:-

When a node receives a two-column table from neighbours, it needs to update its routing table. Updating takes three steps:

- 1) The receiving node needs to add the cost between itself and the sending node to each value in the second column. The logic is clear. If node C claims that its distance to a destination is x mi, and the distance between A and C is y mi, then the distance between A and that destination, via C, is $x + y$ mi.
- 2) The receiving node needs to add the name of the sending node to each row as the third

column if the receiving node uses information from any row. The sending node is the next node in the route.

- 3) The receiving node needs to compare each row of its old table with the corresponding row of the modified version of the received table.
 - a) If the next-node entry is different, the receiving node chooses the row with the smaller cost. If there is a tie, the old one is kept.
 - b) If the next-node entry is the same, the receiving node chooses the new row. For example, suppose node C has previously advertised a route to node X with distance 3. Suppose that now there is no path between C and X; node C now advertises this route with a distance of infinity. Node A must not ignore this value even though its old entry is smaller. The old route does not exist anymore. The new route has a distance of infinity.

Figure (c), shows how node A updates its routing table after receiving the partial table from node C.

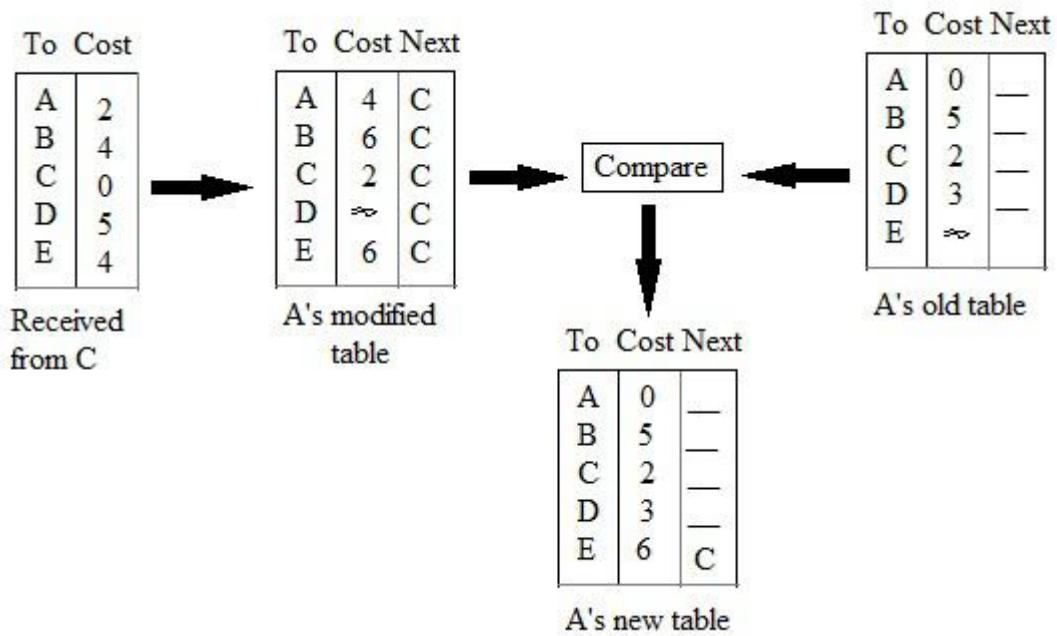


Figure (c). Updating in Distance vector routing

There are several points we need to emphasize here. First, as we know from mathematics, when we add any number to infinity, the result is still infinity. Second, the modified table shows how to reach A from A via C. If A needs to reach itself via C, it needs to go to C and come back, a distance of 4. Third, the only benefit from this updating of node A is the last entry, how to reach E. Previously, node A did not know how to reach E (distance of infinity); now it knows that the cost is 6 via C.

Each node can update its table by using the tables received from other nodes. In a short time, if there is no change in the network itself, such as a failure in a link, each node reaches a stable condition in which the contents of its table remains the same.

2. Link State Routing :-

Link state routing has a different philosophy from that of distance vector routing. In link state routing, if each node in the domain has the entire topology of the domain the list of nodes and links, how they are connected including the type, cost (metric), and condition of the links (up or down)-the node can use Dijkstra's algorithm to build a routing table. Figure (a) shows the concept.

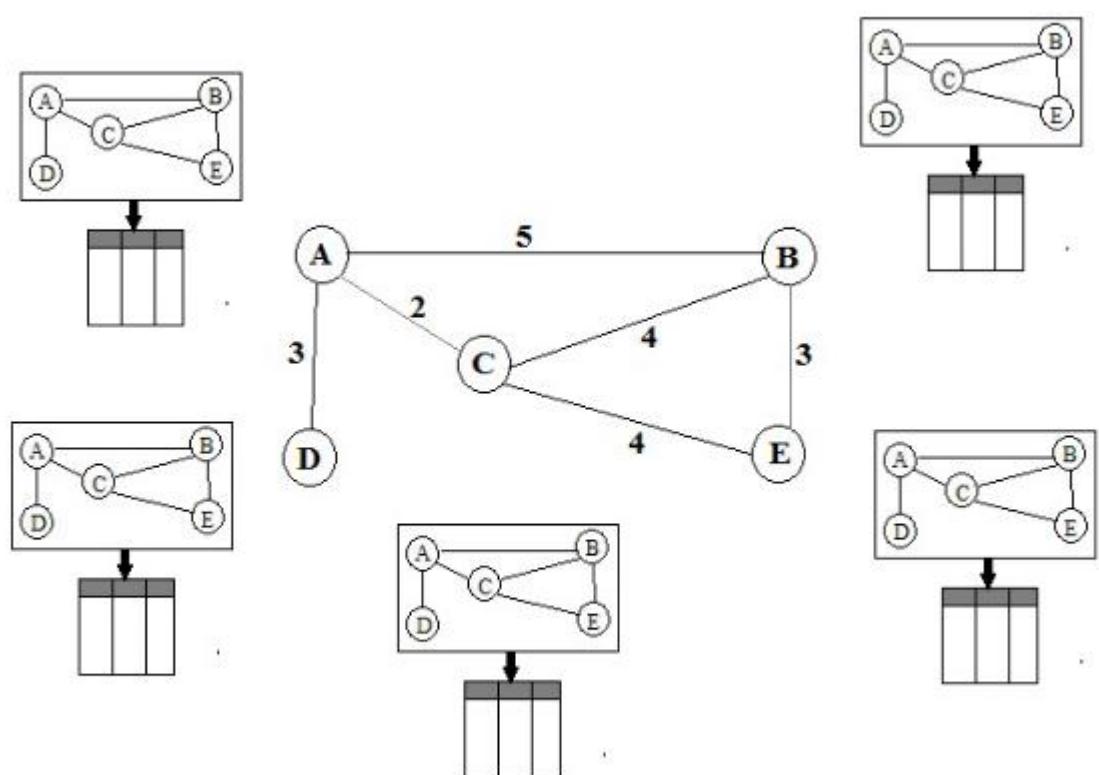


Figure (a), Concept of Link State Routing

The figure shows a simple domain with five nodes. Each node uses the same topology to create a routing table, but the routing table for each node is unique because the calculations are based on different interpretations of the topology. This is

analogous to a city map. While each person may have the same map, each needs to take a different route to reach her specific destination.

The topology must be dynamic, representing the latest state of each node and each link. If there are changes in any point in the network (a link is down, for example), the topology must be updated for each node.

How can a common topology be dynamic and stored in each node? No node can know the topology at the beginning or after a change somewhere in the network. Link state routing is based on the assumption that, although the global knowledge about the topology is not clear, each node has partial knowledge: it knows the state (type, condition, and cost) of its links. In other words, the whole topology can be compiled from the partial knowledge of each node. Figure (b) shows the same domain as in Figure (a), indicating the part of the knowledge belonging to each node.

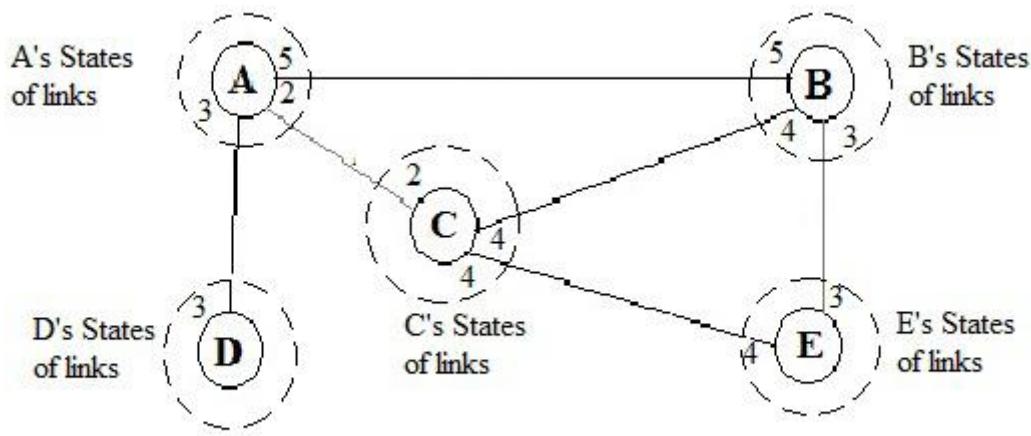


Figure (b), Link State Knowledge

Node A knows that it is connected to node B with metric 5, to node C with metric 2, and to node D with metric 3. **Node C** knows that it is connected to node A with metric 2, to node B with metric 4, and to node E with metric 4. **Node D** knows that it is connected only to node A with metric 3. And so on. Although there is an overlap in the knowledge, the overlap guarantees the creation of a common topology-a picture of the whole domain for each node.

Building Routing Tables:-

In link state routing, four sets of actions are required to ensure that each node has the routing table showing the least-cost node to every other node.

1. Creation of the states of the links by each node, called the link state packet (LSP).

2. Dissemination of LSPs to every other router, called flooding, in an efficient and reliable way.

- 3. Formation of a shortest path tree for each node.**
- 4. Calculation of a routing table based on the shortest path tree.**

Creation of Link State Packet (LSP):-

A link state packet can carry a large amount of information. For the moment, however, we assume that it carries a minimum amount of data: the node identity, the list of links, a sequence number, and age. The first two, node identity and the list of links, are needed to make the topology. The third, sequence number, facilitates flooding and distinguishes new LSPs from old ones. The fourth, age, prevents old LSPs from remaining in the domain for a long time. LSPs are generated on two occasions:

- 1. When there is a change in the topology of the domain.** Triggering of LSP dissemination is the main way of quickly informing any node in the domain to update its topology.
- 2. On a periodic basis.** The period in this case is much longer compared to distance vector routing. As a matter of fact, there is no actual need for this type of LSP dissemination. It is done to ensure that old information is removed from the domain. The timer set for periodic dissemination is normally in the range of 60 min or 2 h based on the implementation. A longer period ensures that flooding does not create too much traffic on the network.

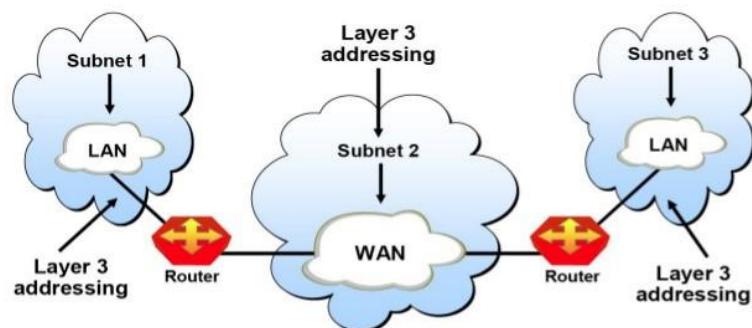
Flooding of LSPs:-

After a node has prepared an LSP, it must be disseminated to all other nodes, not only to its neighbours. The process is called flooding and based on the following:

1. The creating node sends a copy of the LSP out of each interface.
2. A node that receives an LSP compares it with the copy it may already have. If the newly arrived LSP is older than the one it has (found by checking the sequence number), it discards the LSP. If it is newer, the node does the following:
 - a. It discards the old LSP and keeps the new one.
 - b. It sends a copy of it out of each interface except the one from which the packet arrived. This guarantees that flooding stops somewhere in the domain (where a node has only one interface).

3.3.6 Introduction to Networking Layer in Internet

INTRODUCTION



➤ Layer 3, the network layer of the OSI model, provides an end-to-end logical addressing system so that a packet of data can be routed across several layer 2 networks (Ethernet, Token Ring, Frame Relay, etc.).

[\(https://image.slidesharecdn.com/chapter4-170213100055/95/chapter-4-4-638.jpg?cb=1486980079\)](https://image.slidesharecdn.com/chapter4-170213100055/95/chapter-4-4-638.jpg?cb=1486980079)

- The network layer has host-to-host (computer-to-computer) communication.
- A computer needs to communicate with another computer.
 - Computers - communicate through Internet.
- The packet transmitted by the sending computer may pass through several LANs or WANs before reaching the destination computer.
- For this level of communication, we need a global addressing scheme; we called this logical addressing.
- Today, we use the term IP address to mean a logical address in the network layer of the TCP/IP protocol suite. IPv4 Addresses IPv6 Addresses 3/77 |
- The Internet addresses are 32 bits in length; this gives us a maximum of 2³² addresses.
 - These addresses are referred to as IPv4 (IP version 4) addresses or simply IP addresses.
- The need for more addresses motivated a new design of the IP layer called the new generation of IP or IPv6 (IP version 6).
 - In this version, the Internet uses 128-bit addresses - give much greater flexibility in address allocation.
 - These addresses are referred to as IPv6 (IP version 6) addresses.

- There are two popular approaches to packet switching
 - i. The datagram approach
 - ii. The virtual circuit approach.

❖ DATAGRAM APPROACH

- Each packet is treated independently of all other packets.
- Connectionless service.
- No need of reservation of resources because no dedicated path for a connection session.
- Packets are free to go to any path on any intermediate router which is decided on the go by dynamically changing routing tables on routers.
- As packet is free to choose its own path -
 - Associated with a header with proper information about source and the upper layer data.
- Connectionless Property-
 - Makes data packets reach destination in any order, means they need not reach in the order in which they were sent.
- Datagram networks are not reliable as Virtual Circuits.
- Always easy and cost efficient to implement.
- No extra headache of reserving resources and making a dedicated each time an application has to communicate.

❖ VIRTUAL CIRCUIT APPROACH

- Connection - oriented –
 - There is a reservation of resources like buffers, CPU, bandwidth ,etc. for the time in which the newly setup VC is going to be used by a data transfer session.
- First packet goes and reserves resources for the subsequent packets which as a result follow the same path for the whole connection time.
- A global header is required only for the first packet of the connection and not for other packets.
- Data follows a particular dedicated path.
- Packets reach in order to the destination.
- Highly reliable means of transfer.
- Each time a new connection has to be setup with reservation of resources and extra information handling at routers, it's simply costly to implement Virtual Circuits.

- A global addressing system that uniquely identifies every host and router is necessary for delivery of a packet from network to network.
- The Internet address (or IP address) is 32 bits (for IPv4) that uniquely and universally defines a host or router on the internet.
 - i. The portion of the IP address that identifies the network is called the net id.

ii. The portion of the IP address that identifies the host or router on the network is called the host id.

- There are five classes of IP addresses.
 - Classes A, B, and C differ in the number of hosts allowed per network.
 - Class D is for multicasting,
 - Class E is reserved.
- The class of a network is easily determined by examination of the first byte.
- **UNICAST COMMUNICATION**
 - One source sending a packet to one destination.
- **MULTICAST COMMUNICATION**
 - One source sending a packet to multiple destinations.

SUB NETTING

- Sub netting divides one large network into several smaller ones.
- Sub netting adds an intermediate level of hierarchy in IP addressing.
- **DEFAULT MASKING**
 - A process that extracts the network address from an IP address.

- **SUBNET MASKING**

- A process that extracts the sub network address from an IP address

- Super netting combines several networks into one large one.
- In classless addressing, there is variable-length blocks that belongs to no class. The entire address space is divided into blocks based on organization needs.
- The first address and the mask in classless addressing can define the whole block.
- A mask can be expressed in slash notation which is a slash followed by the number of 1s in the mask.
- Every computer attached to the Internet must know its IP address, the IP address of a router, the IP address of a name server, and its subnet mask (if it is part of a subnet).
- DHCP is a dynamic configuration protocol with two databases.
- The DHCP server issues a lease for an IP address to a client for a specific period of time.
- Network address translation (NAT) allows a private network to use a set of private addresses for internal communication and a set of global Internet addresses for external communication.
- NAT uses translation tables to route messages.

- The IP protocol is a connectionless protocol. Every packet is independent and has no relationship to any other packet.
- Every host or router has a routing table to route IP packets.
- In next-hop routing, instead of a complete list of the stops the packet must make, only the address of the next hop is listed in the routing table.
- In network-specific routing, all hosts on a network share one entry in the routing table.
- In host-specific routing, the full IP address of a host is given in the routing table.
- In default routing, a router is assigned to receive all packets with no match in the routing table.
- A static routing table's entries are updated manually by an administrator.
- Classless addressing requires hierarchical and geographic routing to prevent immense routing tables.

Reference:

- <http://www.geeksforgeeks.org/differences-between-virtual-circuits-datagram-networks/>
- [Data Communications and Networking 4e forouzan.pdf](http://www.geeksforgeeks.org/differences-between-virtual-circuits-datagram-networks/)

3.3.7 IP Protocol , IP Address

Internet Protocol

The Internet Protocol (IP) is the method by which data is sent from one computer to another on the Internet. Each computer on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet.

When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate domain. That gateway then forwards the packet directly to the computer whose address is specified.

Because a message is divided into a number of packets, each packet can, if necessary, be sent by a different route across the Internet. Packets can arrive in a different order than the order they were sent in. The Internet Protocol just delivers them. It's up to another protocol, the Transmission Control Protocol (TCP) to put them back in the right order.

IP is a connectionless protocol, which means that there is no continuing connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. (The reason the packets do get put in the right order is because of TCP, the connection-oriented protocol that keeps track of the packet sequence in a message.) In the Open Systems Interconnection (OSI) communication model, IP is in layer 3, the Networking Layer.

The most widely used version of IP today is Internet Protocol Version 4 (IPv4). However, IP Version 6 (IPv6) is also beginning to be supported. IPv6 includes the capabilities of IPv4 and any server that can support IPv6 packets can also support IPv4 packets.

Reference website:

<http://searchunifiedcommunications.techtarget.com/definition/Internet-Protocol>

Internet Protocol Address (IP Address)

An Internet Protocol address (IP address) is a logical numeric address that is assigned to every single computer, printer, switch, router or any other device that is part of a TCP/IP-based network.

The IP address is the main component on which the networking architecture is built; no network exists without it. An IP address is a logical address that is used to uniquely identify every node in the network.

Because IP addresses are logical, they can change. They are similar to addresses in a town or city because the IP address gives the network node an address so that it can communicate with other nodes or networks, just like mail is sent to friends and relatives.

The numerals in an IP address are divided into 2 parts:

- The network part specifies which networks this address belongs to and
- The host part further pinpoints the exact location.

Reference: https://en.wikipedia.org/wiki/IP_address

3.3.8 Classes of IP Addresses

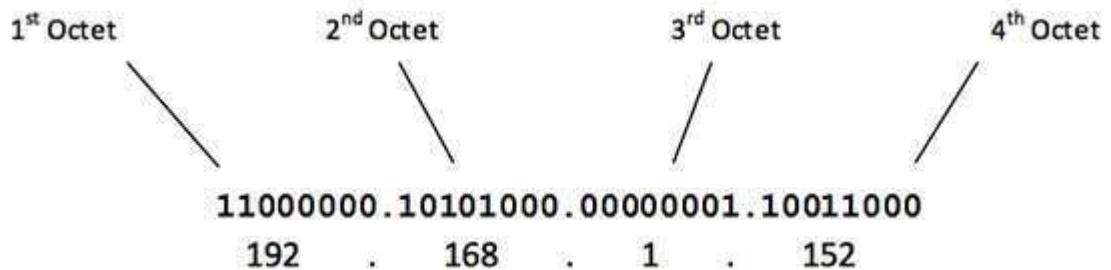
IPV4 Address Classes

Internet Protocol hierarchy contains several classes of IP Addresses to be used efficiently in various situations as per the requirement of hosts per network. Broadly, the IPv4 Addressing system is divided into five classes of IP Addresses. All the five classes are identified by the first octet of IP Address.

Note:

Internet Corporation for Assigned Names and Numbers is responsible for assigning IP addresses.

The first octet referred here is the left most of all. The octets numbered as follows depicting dotted decimal notation of IP Address:



The number of networks and the number of hosts per class can be derived by this formula:

$$\text{Number of networks} = 2^{\text{network_bits}}$$

$$\text{Number of Hosts/Network} = 2^{\text{host_bits}} - 2$$

When calculating hosts' IP addresses, 2 IP addresses are decreased because they cannot be assigned to hosts, i.e. the first IP of a network is network number and the last IP is reserved for Broadcast IP.

Class A Address :

The first bit of the first octet is always set to 0 zero. Thus the first octet ranges from 1 – 127, i.e.

00000001 – 01111111
1 – 127

Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses.

The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks ($2^7 - 2$) and 16777214 hosts ($2^{24} - 2$).

Class A IP address format is thus:

0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH

Class B Address :

An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e.

10000000 – **10**111111
128 – 191

Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x.

Class B has 16384 (2^{14}) Network addresses and 65534 ($2^{16} - 2$) Host addresses.

Class B IP address format is:

10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH

Class C Address :

The first octet of Class C IP address has its first 3 bits set to 110, that is:

110000000 – **110**111111
192 – 223

Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x.

Class C gives 2097152 (2 ^21) Network addresses and 254 (2^ 8 -2) Host addresses.

Class C IP address format is:

110NNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH

Class D Address :

Very first four bits of the first octet in Class D IP addresses are set to 1110, giving a range of:

**11100000 – 11101111
224 – 239**

Class D has IP address range from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

Class E Address :

This IP Class is reserved for experimental purposes only for R&D or Study. IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Like Class D, this class too is not equipped with any subnet mask.

Reference :

<https://www.google.co.in/search?q=classes+ip+addresses+computer+networks&oq=classes+of+ip+address+computer&aqs=chrome.1.69i57j0l2.10197j0j8&client=ubuntu&sourceid=chrome&ie=UTF-8>

3.3.9 Routers, B-routers , Gateways

Routers:

Routers are network layer devices and are particularly identified as Layer- 3 devices of the OSI Model. They process *logical* addressing information in the Network header of a packet such as IP Addresses. Router is used to create larger complex networks by **complex traffic routing**. It has the ability to connect **dissimilar LANs** on the same protocol. It also has the ability to limit the flow of broadcasts. A router primarily comprises of a hardware device or a system of the computer which has more than one network interface and routing software.



Functionality :

When a router receives the data, it determines the destination address by reading the header of the packet. Once the address is determined, it searches in its **routing table** to get know how to reach the destination and then forwards the packet to the higher hop on the route. The hop could be the final destination or another router.

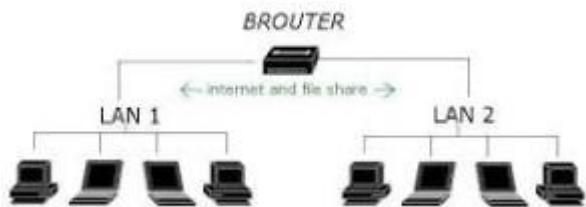
Routing tables play a very pivotal role in letting the router makes a decision. Thus a routing table is ought to be *updated* and *complete*. The two ways through which a router can receive information are:

- **Static Routing:** In static routing, the routing information is fed into the routing tables manually. It does not only become a time-taking task but gets prone to errors as well. The manual updating is also required in case of statically configured routers when change in the topology of the network or in the layout takes place. Thus static routing is feasible for tinniest environments with minimum of one or two routers.
- **Dynamic Routing:** For larger environment dynamic routing proves to be the practical solution. The process involves use of peculiar routing protocols to hold communication. The purpose of these protocols is to enable the other routers to transfer information about to other routers, so that the other routers can build their own routing tables.

B-routers:

B-routers are the combination of both the bridge and routers. They take up the functionality of the both networking devices serving as a *bridge* when

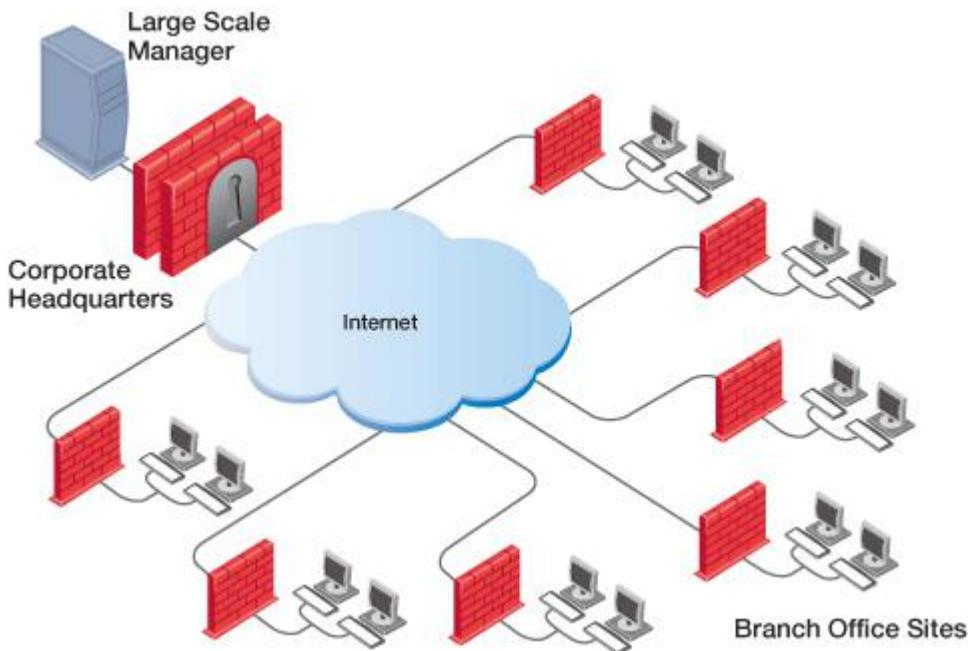
forwarding data between networks, and serving as a *router* when routing data to individual systems. B-router functions as a filter that allows some data into the local network and redirects unknown data to the other network.



B-routers are rare and their functionality is embedded into the routers functioned to act as bridge as well.

Gateways:

Gateway is a device which is used to connect multiple networks and passes packets from one packet to the other network. Acting as the ‘gateway’ between different networking systems or computer programs, a gateway is a device which forms a link between them. It allows the computer programs, either on the same computer or on different computers to share information across the network through protocols. A router is also a gateway, since it interprets data from one network protocol to another.



Others such as bridge converts the data into different forms between two networking systems. Then a software application converts the data from one format into another. Gateway is a viable tool to translate the data format, although the data itself remains unchanged. Gateway might be installed in some other device to add its functionality into another.

Reference :

<https://www.google.co.in/search?q=routers+and+gateways+in+networking&oq=routers+routers+and+gateways+in+&aqs=chrome.1.69i57j0.17036j0j7&client=ubuntu&sourceid=chrome&ie=UTF-8>

3.4.1. Transport Service Primitives

Transport Service Primitives

- A PRIMITIVE means operations.
- A service in a computer network consists of a set of primitives.
- The primitives are to be used by the user to access the service.
- The primitive asks the service to do some action or to report on an action.
- The primitive varies for different services.
- The following are some of the primitives used in a Transport Layer.

Primitive	TPDU sent	Meaning
LISTEN	None	Block until some process tries to connect
CONNECT	Connection Request	Actively attempt to establish connection
SEND	Data	Send data
RECEIVE	None	Block until a data TPDU arrives
DISCONNECT	Disconnect Request	Release the connection

- Consider an application with a server and a number of remote clients.
- To start with, the server executes a LISTEN primitive, typically by calling a library procedure that makes a system call to block the server until a client turns up.
- For lack of a better term, we will reluctantly use the somewhat ungainly acronym TPDU (Transport Protocol Data Unit) for messages sent from transport entity to transport entity.
- Thus, TPDUs (exchanged by the transport layer) are contained in packets (exchanged by the network layer).
- In turn, packets are contained in frames (exchanged by the data link layer).
- When a frame arrives, the data link layer processes the frame header and passes the contents of the frame payload field up to the network entity.

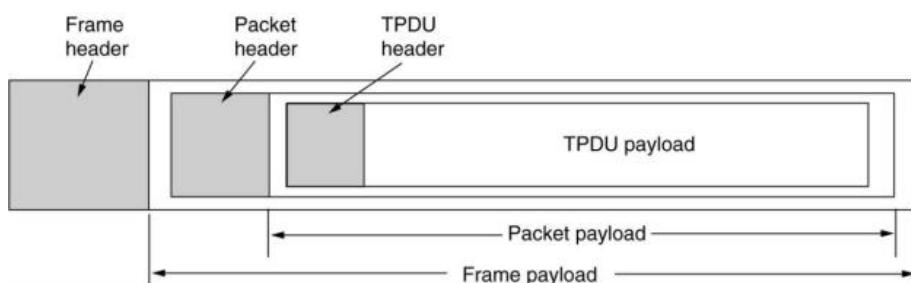


Figure: The nesting of TPDUs, packets, and frames

- When a client wants to talk to the server, it executes a CONNECT primitive.
- The transport entity carries out this primitive by

blocking the caller and sending a packet to the server.

- Encapsulated in the payload of this packet is a transport layer message for the server's transport entity.
- The client's CONNECT call causes a CONNECTION REQUEST TPDU to be sent to the server.
- When it arrives, the transport entity checks to see that the server is blocked on a LISTEN (i.e., is interested in handling requests).
- It then unblocks the server and sends a CONNECTION ACCEPTED TPDU back to the client.
- When this TPDU arrives, the client is unblocked and the connection is established.
- Data can now be exchanged using the SEND and RECEIVE primitives.
- In the simplest form, either party can do a (blocking) RECEIVE to wait for the other party to do a SEND. When the TPDU arrives, the receiver is unblocked.
- It can then process the TPDU and send a reply.
- As long as both sides can keep track of whose turn it is to send, this scheme works fine.
- When a connection is no longer needed, it must be released to free up table space within the two transport entities.
- Disconnection has two variants: asymmetric and symmetric.

Reference :

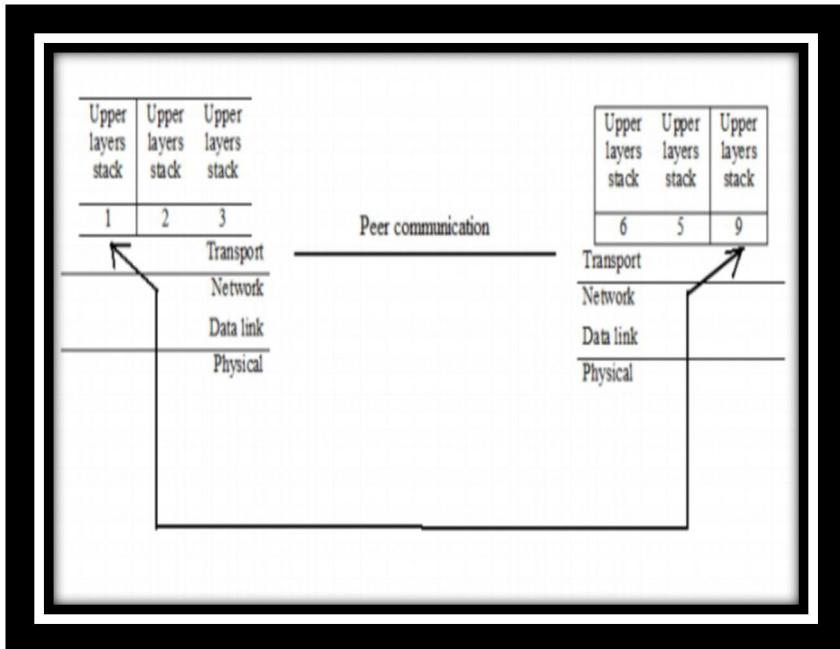
http://www.darshan.ac.in/Upload/DIET/Documents/CE/Transport%20Layer_12112014_080118AM.pdf

3.4.2. Addressing, Connection Establishment, Flow Control

Addressing

- The transport layer interacts with the functions of the session layer. However, many protocols (or protocol stacks, meaning groups of protocols that interact at different levels) combine sessions, presentation, and application level protocols into a single package, called an application. In these cases, delivery to the application. So communication occurs not just from end machine to end machine but from end application to end application. Data generated by an application on one machine must be received not just by the other machine but by the correct application on that other machine.
- In most cases, therefore, we end up with communication between many-to-many entities, called **Service Access Points**. But how does the network identify which service access point on

one host is communicating with which service access point on the other host?



- To ensure accurate delivery from service access point to service access point, we need another level of addressing in addition to those at the data link and network levels. Data link protocols need to know which two computers within a network are communicating. Network level protocols need to know which two computers within an internet are communicating. But at the transport level, the protocol needs to know which upper layer protocols are communicating.

Connection Establishment

- A connection is typically used for client-server interaction. A server advertizes a particular server at a well-known address and clients establish connections to that socket to avail of the offered service. Thus the connection establishment procedure is asymmetric.
- A server creates a socket, binds it to a “well-known” port number associated with the service, and then passively ``listens” on the socket for requests to be served. It is possible for any unrelated process to rendezvous with the server. A client requests services from a server by initiating a “connection” to the server's socket. The client uses the connect system call to initiate a connection.
- Once a connection is established, both client and server may exchange data using several system calls.
- To establish a connection, TCP uses a three-way handshake. Before a client attempts to connect with a server, the server must first bind to and listen at a port to open it up for connections: this is called a passive open. Once the passive open is established, a client may initiate an active open. To establish a connection, the three-way (or 3-step) handshake occurs:
 1. **SYN:** The active open is performed by the client sending a SYN to the server. The client sets the segment's sequence number to a random value A.

2. SYN-ACK: In response, the server replies with a SYN-ACK. The acknowledgment number is set to one more than the received sequence number i.e. A+1, and the sequence number that the server chooses for the packet is another random number, B.

3. ACK: Finally, the client sends an ACK back to the server. The sequence number is set to the received acknowledgement value i.e. A+1, and the acknowledgement number is set to one more than the received sequence number i.e. B+1.

- At this point, both the client and server have received an acknowledgment of the connection. The steps 1, 2 establish the connection parameter (sequence number) for one direction and it is acknowledged. The steps 2, 3 establish the connection parameter (sequence number) for the other direction and it is acknowledged. With these, a full-duplex communication is established.
- A connection is a link between two or more computer systems that need to exchange messages and data. On a shared network and inter network, connections are usually virtual, meaning that a connection state is set up in software that tracks the exchange of data

across what appears to be a dedicated circuit to the application that is using it. These connections take place in the transport layer and are handled by TCP in the Internet protocol suite. This topic discusses TCP connections.

- A connection is a requirement of a reliable data delivery service. It is set up before the actual data exchange takes place. The connection is used to acknowledge the receipt of packets and retransmit those that are lost. The opposite of this is a best-effort service. A file transfer is an example of a service that requires guaranteed delivery services.
- To reliably exchange data, an application on one network system creates an end-to-end connection with an application on another network system. A single computer may establish and terminate multiple connections at any time. The packets from these connections are multiplexed over a single physical link. Thus, they are virtual connections. In addition, each connection is full duplex, allowing bi-directional packet exchange.

Flow Control

- Data-link layer is responsible for implementation of point-to-point flow and error control mechanism.
- When a data frame Layer – 2 *data* is sent from one host to another over a single medium, it is required that the sender and receiver should work at the same speed. That is, sender sends at a speed on which the receiver can process and accept the data. What if the speed hardware/ software of the sender or receiver differ? If sender is sending too fast the receiver may be overloaded, swamped and data may be lost.
- Two types of mechanisms can be deployed to control the flow:

Stop and Wait:

This flow control mechanism forces the sender after transmitting a data frame to stop and wait until the acknowledgement of the data-frame sent is received.

Sliding Window:

In this flow control mechanism, both sender and receiver agree on the number of data- frames after

which the acknowledgement should be sent. As we learnt, stop and wait flow control mechanism wastes resources, this protocol tries to make use of underlying resources as much as possible.

Error Control

- When data-frame is transmitted, there is a probability that data-frame may be lost in the transit or it is received corrupted. In both cases, the receiver does not receive the correct data-frame and sender does not know anything about any loss. In such case, both sender and receiver are equipped with some protocols which helps them to detect transit errors such as loss of data-frame. Hence, either the sender retransmits the data-frame or the receiver may request to resend the previous data-frame.
- Requirements for error control mechanism:

Error detection:

The sender and receiver, either both or any, must ascertain that there are some errors in the transit.

Positive ACK:

When the receiver receives a correct frame, it should acknowledge it.

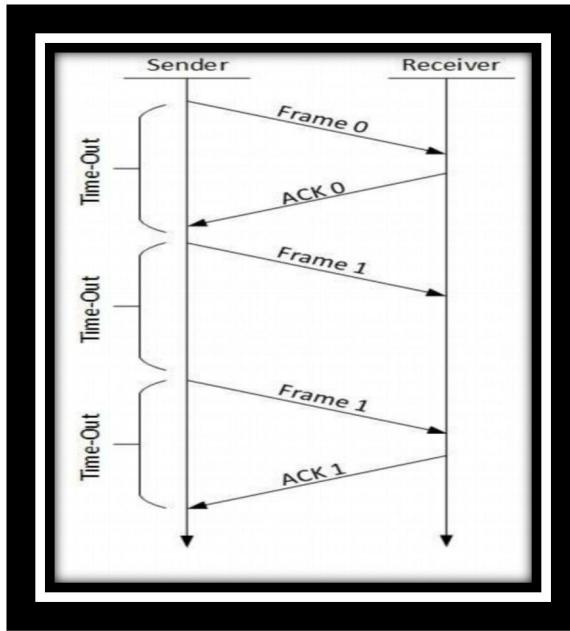
Negative ACK:

When the receiver receives a damaged frame or a duplicate frame, it sends a NACK back to the sender and the sender must retransmit the correct frame.

Retransmission:

The sender maintains a clock and sets a timeout period. If an acknowledgement of a data-frame previously transmitted does not arrive before the timeout the sender retransmits the frame, thinking that the frame or its acknowledgement is lost in transit.

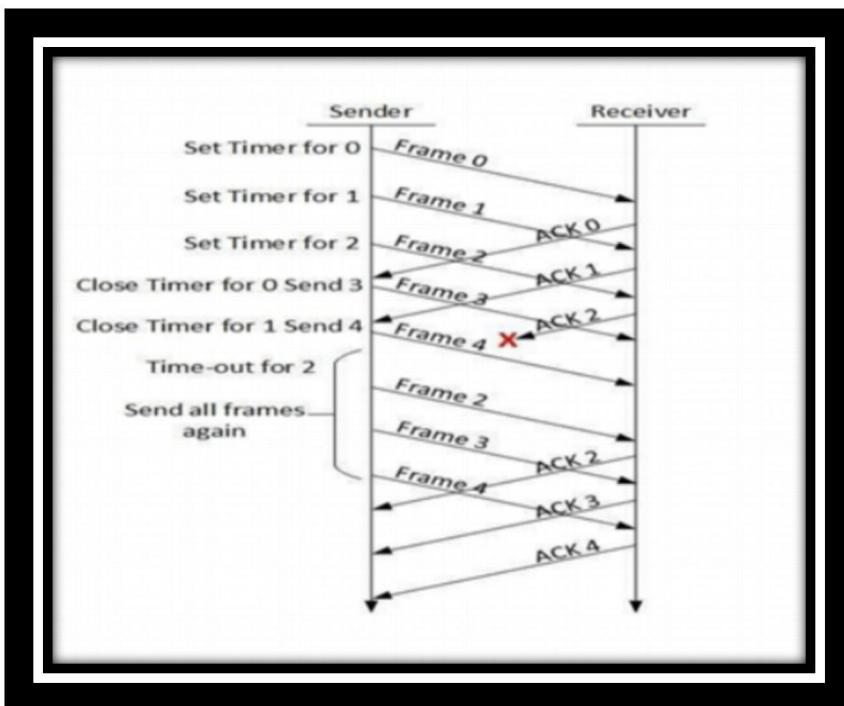
- There are three types of techniques available which Data-link layer may deploy to control the errors by Automatic Repeat Requests ARQ:
 - Stop-and-wait ARQ:



The following transition may occur in Stop-and-Wait ARQ:

- The sender maintains a timeout counter.
- When a frame is sent, the sender starts the timeout counter.
- If acknowledgement of frame comes in time, the sender transmits the next frame in queue.
- If acknowledgement does not come in time, the sender assumes that either the frame or its acknowledgement is lost in transit. Sender retransmits the frame and starts the timeout counter.
- If a negative acknowledgement is received, the sender retransmits the frame.

- **Go-Back-N ARQ**

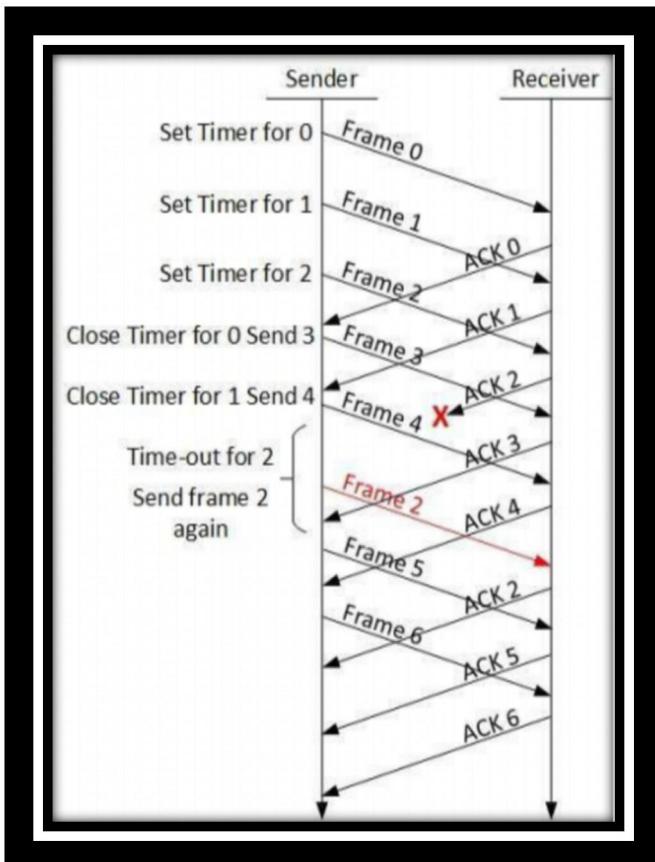


- The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones. The receiving-window enables the receiver to receive multiple frames and acknowledge them.
- The receiver keeps track of incoming frame's sequence number.
- When the sender sends all the frames in window, it checks up to what sequence number it has received positive acknowledgement. If all frames are positively acknowledged, the

sender sends next set of frames. If sender finds that it has received NACK or has not received any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK.

Selective Repeat ARQ:

- In Go-back-N ARQ, it is assumed that the receiver does not have any buffer space for its window size and has to process each frame as it comes.
- This enforces the sender to retransmit all the frames which are not acknowledged.
- In Selective-Repeat ARQ, the receiver while keeping track of sequence numbers, buffers the frames in memory and sends NACK for only frame which is missing or damaged.



Reference :

<https://www.vskills.in/certification/tutorial/information-technology/basic-network-support-professional/tcp-connection-establish-and-terminate/>

3.4.3. Multiplexing

Multiplexing : It is used to combine multiple signals like analog or digital for transmission over a single line or media. A common type of multiplexing combines several low-speed signals for transmission over a single high-speed connection.

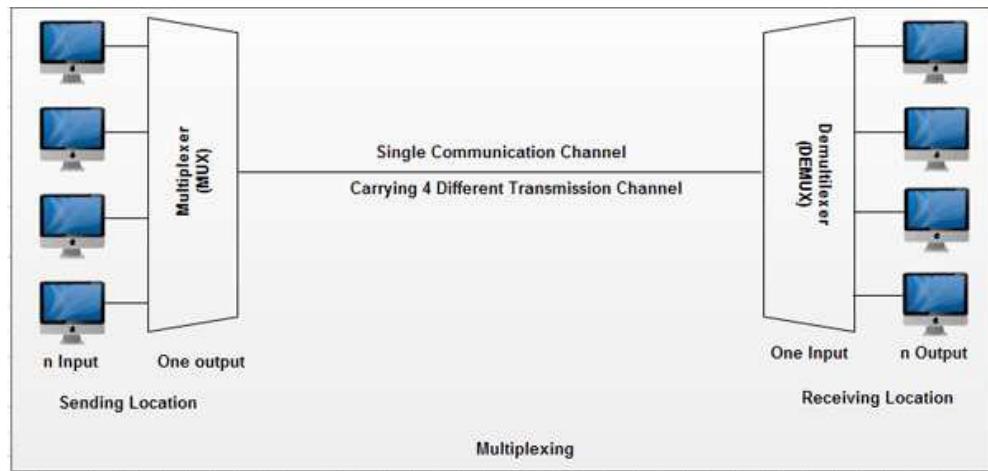
WHAT MULTIPLEXER DOES?

A device named Multiplexer (MUX) combines n input lines to generate one output line.

Ex: (Many to One) therefore multiplexer has several inputs and outputs. At the receiving end, a device called demultiplexer (DEMUX) is used that separates signal into its component signals. So DEMUX has one input and several outputs.

Concept of Multiplexing :

As shown in fig multiplexer takes 4 input lines and diverts them to single output line. The signal from 4 different devices is combined and carried by this single line. At the receiving side, a demultiplexer takes this signal from a single line & breaks it into the original signals and passes them to the 4 different receivers.

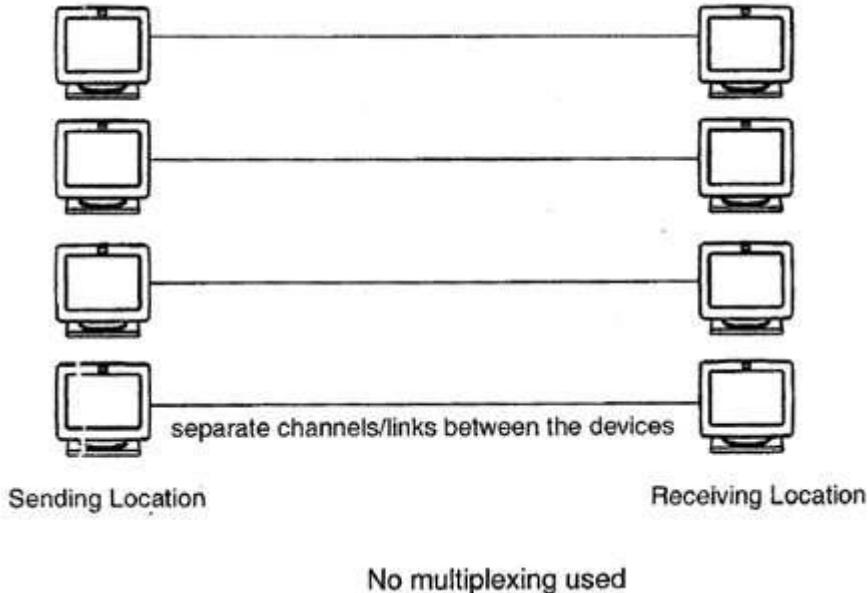


Advantages :

If no multiplexing is used between the users at two different sites that are distance apart, then separate communication lines would be required as shown in fig.

It is not only costly and difficult to manage. If multiplexing is used then, only one line is required. This leads to the reduction in the line cost and also it

would be easier to keep track of one line than several lines.



The following are several examples of different multiplexing methods:

Frequency Division Multiplexing (FDM) – FDM stands for frequency division multiplexing, a multiplexing technique that uses different frequencies to combine multiple streams of data for transmission over a communications medium. FDM assigns a discrete carrier frequency to each data stream and then combines many modulated carrier frequencies for transmission. For example, television transmitters use FDM to broadcast several channels at once.

Time Division Multiplexing (TDM) – TDM stands for Time Division Multiplexing, a type of multiplexing that

combines data streams by assigning each stream a different time slot in a set. TDM repeatedly transmits a fixed sequence of time slots over a single transmission channel. Within T-Carrier systems, such as T-1 and T-3, TDM combines **Pulse Code Modulated (PCM)** streams created for each conversation or data stream.

Wavelength Division Multiplexing (WDM) - Short for wavelength division multiplexing, a type of multiplexing developed for use on optical fiber. WDM modulates each of several data streams onto a different part of the light spectrum. **WDM** is the optical equivalent of FDM.

REFERENCE LINK:

<http://ecomputernotes.com/computernetworkingnotes/multiple-access/multiplexing-what-is-multiplexing-explain-its-multiplexing-methods>

AUTHOR: DINESH THAKUR

3.4.4. Introduction to Transport Layer Protocol and Their Features

OSI Model is recognized as Transport Layer – 4. All modules and procedures pertaining to transportation of data or data stream are categorized into this layer. As all other layers, this layer communicates with its peer Transport layer of the remote host.

Transport layer offers peer-to-peer and end-to-end connection between two processes on remote hosts. Transport layer takes data from upper layer *i. e.* Application layer and then breaks it into smaller size

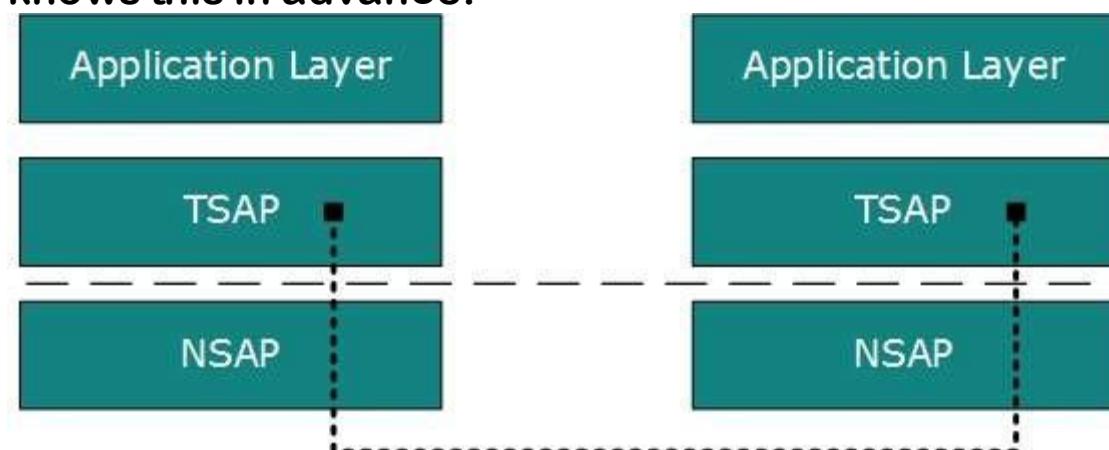
segments, numbers each byte, and hands over to lower layer Network Layer for delivery.

Functions

- This Layer is the first one which breaks the information data, supplied by Application layer in to smaller units called segments. It numbers every byte in the segment and maintains their accounting.
- This layer ensures that data must be received in the same sequence in which it was sent.
- This layer provides end-to-end delivery of data between hosts which may or may not belong to the same subnet.
- All server processes intend to communicate over the network are equipped with well-known
- Transport Service Access Points TSAPs also known as port numbers.

End-to-End Communication

A process on one host identifies its peer host on remote network by means of TSAPs, also known as Port numbers. TSAPs are very well defined and a process which is trying to communicate with its peer knows this in advance.



For example, when a DHCP client wants to communicate with remote DHCP server, it always requests on port number 67. When a DNS client wants to communicate with remote DNS server, it always requests on port number 53 UDP.

The two main Transport layer protocols are:

1. **Transmission Control Protocol**

It provides reliable communication between two hosts.

2. **User Datagram Protocol**

It provides unreliable communication between two hosts.

Reference :

http://www.tutorialspoint.com/data_communication/computer_network/transport_layer_introduction.h

This list shows some protocols that are commonly placed in the transport layers of the [Internet protocol suite](#), the [OSI protocol suite](#), [NetWare's IPX/SPX](#), [AppleTalk](#), and [Fibre Channel](#).

- ATP, [AppleTalk Transaction Protocol](#)
- CUDP, [Cyclic UDP](#)
- DCCP, [Datagram Congestion Control Protocol](#)
- FCP, [Fibre Channel Protocol](#)
- IL, [IL Protocol](#)
- MPTCP, [Multipath TCP](#)
- RDP, [Reliable Datagram Protocol](#)
- RUDP, [Reliable User Datagram Protocol](#)
- SCTP, [Stream Control Transmission Protocol](#)
- SPX, [Sequenced Packet Exchange](#)
- SST, [Structured Stream Transport](#)

- TCP, [Transmission Control Protocol](#)
- UDP, [User Datagram Protocol](#)
- [UDP-Lite](#)
- μTP, [Micro Transport Protocol](#)

reference :

https://en.wikipedia.org/wiki/Transport_layer#Protocols

3.5.1 Introduction to Establishing Session

- A **session** is a semi-permanent interactive information interchange.
- Also known as a dialogue, a conversation or a meeting, between two or more communicating devices, or between a computer and user .
- A session is set up or established at a certain point in time, and then torn down at some later point.
- An established communication session may involve more than one message in each direction.
- A session is typically, but not always, stateful, meaning that at least one of the communicating parts needs to save information about the session history in order to be able to communicate, as opposed to [stateless](#) communication, where the communication consists of independent requests with responses.

- An established session is the basic requirement to perform a [connection-oriented communication](#).
- A session also is the basic step to transmit in [connectionless communication](#) modes. However any unidirectional transmission does not define a session. [1]
- **Communication Transport** may be implemented as part of protocols and services at the [application layer](#), at the [session layer](#) or at the [transport layer](#) in the [OSI model](#).
- Application layer examples:
 - [HTTP sessions](#), which allow associating information with individual visitors
 - A [telnet](#) remote login session
- Session layer example:
 - A [Session Initiation Protocol](#) (SIP) based [Internet phone](#) call
- Transport layer example:
 - A [TCP](#) session, which is synonymous to a TCP [virtual circuit](#), a TCP connection, or an established TCP [socket](#).
- In the case of transport protocols that do not implement a formal session layer (e.g., [UDP](#)) or where sessions at the application layer are generally very short-lived (e.g., [HTTP](#)), sessions are maintained by a higher level program using a method defined in the data being exchanged. For example, an [HTTP](#) exchange between a browser and a remote host may include an [HTTP cookie](#) which identifies state, such as a unique [session ID](#), information about the user's preferences or authorization level.

- Most client-server sessions are maintained by the transport layer - a single connection for a single session.
- However each transaction phase of a Web/HTTP session creates a separate connection.
- Maintaining session continuity between phases requires a session ID.
- The session ID is embedded within the <A HREF> or <FORM> links of dynamic web pages so that it is passed back to the CGI.
- CGI then uses the session ID to ensure session continuity between transaction phases.
- Two type of web session:
 - A) Server side web session
 - B) Client side web session

A) Server side web sessions

- Server-side sessions are handy and efficient, but can become difficult to handle in conjunction with load-balancing/high-availability systems and are not usable at all in some embedded systems with no storage.
- The load-balancing problem can be solved by using shared storage or by applying forced peering between each client and a single server in the cluster, although this can compromise system efficiency and load distribution.
- A method of using server-side sessions in systems without mass-storage is to reserve a portion of RAM for storage of session data

- This method is applicable for servers with a limited number of clients (e.g. router or access point with infrequent or disallowed access to more than one client at a time).

B) Client side web sessions

- Client-side sessions use cookies and cryptographic techniques to maintain state without storing as much data on the server.
- When presenting a dynamic web page, the server sends the current state data to the client (web browser) in the form of a cookie.
- The client saves the cookie in memory or on disk.
- This mechanism may work well in some contexts; however, data stored on the client is vulnerable to tampering by the user or by software that has access to the client computer.
- To use client-side sessions where confidentiality and integrity are required, the following must be guaranteed:
 - 1) Confidentiality: Nothing apart from the server should be able to interpret session data.
 - 2) Data integrity: Nothing apart from the server should manipulate session data (accidentally or maliciously).
 - 3) Authenticity: Nothing apart from the server should be able to initiate valid sessions
- To accomplish this, the server needs to encrypt the session data before sending it to the client, and modification of such information by any other party should be prevented via cryptographic means.

- Transmitting state back and forth with every request is only practical when the size of the cookie is small.
- In essence, client-side sessions trade server disk space for the extra bandwidth that each web request will require.
- Moreover, web browsers limit the number and size of cookies that may be stored by a web site. To improve efficiency and allow for more session data, the server may compress the data before creating the cookie, decompressing it later when the cookie is returned by the client.

Session management

- In [human-computer interaction](#), **session management** is the process of keeping track of a user's activity across sessions of interaction with the [computer system](#).
- Typical session management tasks in a [desktop environment](#) include keeping track of which applications are open and which documents each application has opened, so that the same state can be restored when the user logs out and logs in later.
- For a website, session management might involve requiring the user to re-login if the session has expired (i.e., a certain time limit has passed without user activity). It is also used to store information on the server-side between HTTP requests.

Desktop session management

- A desktop session manager is a program that can save and restore desktop sessions.
- A desktop session is all the windows currently running and their current content.
- Session management on [Linux](#)-based systems is provided by [X session manager](#)
- On [Microsoft Windows](#) systems, session management is provided by the Session Manager Subsystem (smss.exe)

Browser session management

- Session management is particularly useful in a [web browser](#) where a user can save all open pages and settings and restore them at a later date.
- To help recover from a system or application crash, pages and settings can also be restored on next run.
- [Google Chrome](#), [Mozilla Firefox](#), [Internet Explorer](#), [Omni-Web](#) and [Opera](#) are examples of web browsers that support session management. Session management is often managed through the application of [cookies](#).

Web server session management

- [Hypertext Transfer Protocol](#) (HTTP) is stateless: a client computer running a web browser must establish a new [Transmission Control Protocol](#) (TCP) network connection to the web server with each new HTTP GET or POST request.

- The web server, therefore, cannot rely on an established TCP network connection for longer than a single HTTP GET or POST operation.
- Session management is the technique used by the web developer to make the stateless HTTP protocol support session state.
- For example, once a user has been authenticated to the web server, the user's next HTTP request (GET or POST) should not cause the web server to ask for the user's account and password again. For a discussion of the methods used to accomplish this see [HTTP cookie](#) and [Session ID](#)

Session Management over SMS

- Just as HTTP is a stateless protocol, so is [SMS](#).
- As SMS became interoperable across rival networks in 1999, [\[2\]](#) and text messaging started its ascent towards becoming a ubiquitous global form of communication, [\[3\]](#) various enterprises became interested in using the SMS channel for commercial purposes.

Reference :

[https://en.m.wikipedia.org/wiki/Session_\(computer_science\)](https://en.m.wikipedia.org/wiki/Session_(computer_science))

The Data Communication and Networking (4th Edition)

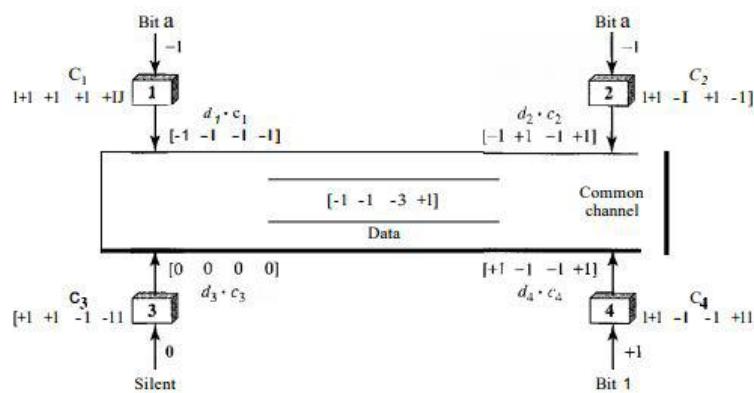
3.5.2 Presentation with Content Encoding and Decoding

As a simple example, we show how four stations share the link during a 1-bit interval. The procedure can easily be repeated for additional intervals. We assume that stations 1 and 2 are sending a 0 bit and channel 4 is sending a 1 bit. Station 3 is silent. The data at the sender site are translated to -1, -1, 0, and +1. Each station multiplies the corresponding number by its chip (its orthogonal sequence), which is unique for each station. The result is a new sequence which is sent to the channel. For simplicity, we assume that all stations send the resulting sequences at the same time. The sequence on the channel is the sum of all four sequences as defined before. Figure 12.26 shows the situation.

Now imagine station 3, which we said is silent, is listening to station 2. Station 3 multiplies the total data on the channel by the code for station 2, which is [+1 -1 +1 -1], to get

$$[-1 -1 -3 +1] \cdot [+1 -1 +1 -1] = -4/4 = -1 \dots \text{bit 1}$$

Figure 12.26 Sharing channel in CDMA



Reference :

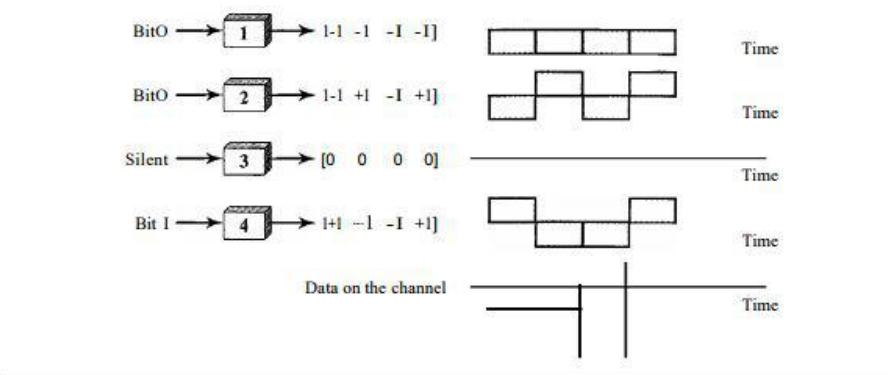
The Data Communication and Networking (4th Edition) Page : 387

Image :

Signal Level

The process can be better understood if we show the digital signal produced by each station and the data recovered at the destination (see Figure 12.27). The figure shows the corresponding signals for each station (using NRZ-L for simplicity) and the signal that is on the common channel.

Figure 12.27 Digital signal created by four stations in CDMA



Reference :

The Data Communication and Networking (4th Edition) Page : 388

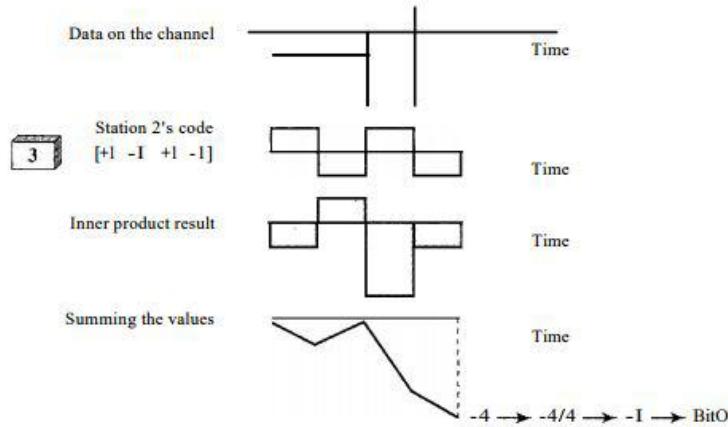
Image :

The Data Communication and Networking (4th Edition) Page : 388

Figure 12.28 shows how station 3 can detect the data sent by station 2 by using the code for station 2. The total data on the channel are multiplied (inner product operation) by the signal representing station 2 chip code to get a new signal. The station then integrates and adds the area under the signal, to get

the value -4, which is divided by 4 and interpreted as bit O.

Figure 12.28 Decoding of the composite signal for one in CDMA



Reference :

The Data Communication and Networking (4th Edition) Page : 388

Image :

The Data Communication and Networking (4th Edition) Page : 389

Sequence Generation

To generate chip sequences, we use a Walsh table, which is a two-dimensional table with an equal number of rows and columns, as shown in Figure 12.29.

Figure 12.29 General rule and examples of creating Walsh tables

$W_1 = \begin{bmatrix} +1 \end{bmatrix}$	$W_{2N} = \begin{bmatrix} W_N & W_N \\ \overline{W_N} & \overline{\overline{W_N}} \end{bmatrix}$
a. Two basic rules	
$W_1 = \begin{bmatrix} +1 \end{bmatrix}$ $W_2 = \begin{bmatrix} +1 & +1 \\ +1 & -1 \end{bmatrix}$	$W_4 = \begin{bmatrix} +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 \end{bmatrix}$
b. Generation of W_1 , W_2 , and W_4	

In the Walsh table, each row is a sequence of chips. W_1 for a one-chip sequence has one row and one column. We can choose -1 or +1 for the chip for this trivial table (we chose +1). According to Walsh, if we know the table for N sequences W_N we can create the table for $2N$ sequences W_{2N} , as shown in Figure 12.29. The W_N with the overbar $\overline{W_N}$ stands for the complement of W_N where each +1 is changed to -1 and vice versa. Figure 12.29 also shows how we can create W_2 and W_4 from W_1 . After we select W_1 , W_2 can be made from four W_1 's, with the last one the complement of W_1 . After W_2 is generated, W_4 can be made of four W_2 's, with the last one the complement of W_2 . Of course, W_8 is composed of four W_4 's, and so on. Note that after W_N is made, each station is assigned a chip corresponding to a row. Something we need to emphasize is that the number of sequences N needs to be a power of 2. In other words, we need to have $N = 2^m$.

Example 12.6

Find the chips for a network with

- a. Two stations
- b. Four stations

Solution

We can use the rows of W_2 and W_4 in Figure 12.29:

- a. For a two-station network, we have $[+1 \ 1]$ and $[+1 \ -1]$.
 - b. For a four-station network we have $[+1 \ +1 \ +1 \ +1]$, $[+1 \ -1 \ +1 \ -1]$, $[+1 \ +1 \ -1 \ -1]$, and $[+1 \ -1 \ -1 \ +1]$.

Example 12.7

What is the number of sequences if we have 90 stations in our network?

Solution

The number of sequences needs to be $2m$. We need to choose $m = 7$ and $N = 27$ or 128 . We can then use 90 of the sequences as the chips.

Example 12.8

Prove that a receiving station can get the data sent by a specific sender if it multiplies the entire data on the channel by the sender's chip code and then divides it by the number of stations.

Solution

Let us prove this for the first station, using our previous four-station example. We can say that the data on the channel $D = Cdl . ("1 + d2 . ("2 + d3 . ("3 + d4 . ("4)"$) The receiver which wants to get the data sent by station I multiplies these data by ("I"

D . ("1 =(d1 • ("1 + d2 . ("2 + d3 . ("3 + d4 . ("4) . ("1
 $= d1 \cdot (1 + d2 \cdot (2 + d3 \cdot (3 + d4 \cdot (4 \cdot$
 $(1$
 $= d1 \times N + d2 \times 0 + d3 \times 0 + d4 \times 0$
 $= d1 \times N$ When we divide the result by N, we get $d1'$

Reference :

The Data Communication and Networking (4th Edition) Page : 390

3.5.3 Introduction to application layer protocols

- An application layer protocol defines how an application processes (clients and servers), running on different end systems, pass messages to each other.
- Application layer protocols can be broadly divided into two categories:
 1. Protocols which are used by users. For example, SMTP, DNS, FTP, POP, HTTP.
 2. Protocols which help and support protocols used by users. For example DNS.

Simple Mail Transfer Protocol (SMTP)

- SMTP is used to transfer electronic mail from one user to another.
- SMTP was originally developed in the early 1980s and remains one of the most popular protocols in use worldwide.
- When an email is submitted to send, the sending process is handled by Message transfer agent which is normally comes inbuilt in email client software.
- Email software most commonly uses SMTP for sending and either the POST OFFICE PROTOCOL 3(POP3) or Internet Message Access Protocol (IMAP) Protocols for receiving email.

File Transfer Protocol (FTP)

- The File Transfer Protocol (FTP) is the most widely used protocol for file transfer over any type of network.
- FTP is one of the most widely used protocol for file transfer, between computers.
- FTP relies completely on TCP to provide reliability across the underlying unreliable best effort IP based networks.
- FTP uses two separate sessions (TCP connections), one for control and another for data.

Post Office Protocol (POP)

- The Post Office Protocol (POP) is simple mail retrieval protocol used by email software to retrieve mails from mail server.
- When client needs to retrieve mails from server, it opens a connection with server on TCP port, then user can access his mails and download them to the local computer.
- POP works in two modes, DELETE mode to delete emails from server after retrieval and KEEP mode to not delete emails from server.

Hyper Text Transfer Protocol (HTTP)

- Hyper Text Transfer Protocol (HTTP) is well organized documentation system which uses hyperlinks to link pages in Text Documents.
- To access the web pages, user normally uses web browsers, who are responsible for initiating, maintaining, and closing TCP connections.

Domain Name System (DNS)

- The Domain Name System (DNS) translates Internet domain and host names to IP addresses.
- On the Internet, DNS automatically converts between the name we type in our web browser address bar to the IP addresses of web servers hosting those sites.
- Larger corporations also use DNS to manage their own company intranet.

Reference :

https://www.tutorialspoint.com/data_communication_computer_network/application_protocols.htm

4.Network Configuration and Administration

Submitted To:- Mr.Devendra Pandey

(Assistant Professor)

Prepared by:- Kushakiya Pinak 53

Jhaveri Kashyap 32

Gandhi Pruthvi 22

Kanthariya Riken 40

Kevadiya Bhautik	47
Gajjar Axay	18
Kukadiya Jay	51
Santra Karan	44

Table of Contents

1. Installing and configuring network adapters

- Network Configuration
- Network Administration
- Installing and configuration network adapters
 - What does Network Adapter mean
 - How Does a Wireless Adapter Work
 - Types of Adapters
 - Wireless Standards
 - Speeds
 - Security
 - How to install network adapter
 - How to configure network adapter

2. Managing Network bindings

- Binding Between Architectural Levels
- Combining Network Bindings
- Configuring Network Bindings
- Specifying Binding Order

3. Sharing files and printers User profiles

- PEER TO PEER FILE SHARINGS
- USES
- BENEFITS
- LIMIITATIONS
- COMMON FILE SYSTEMS AND PROTOCOLS
- FILE AND PRINTER SHARING

4. Folder security and Account policies

- Password-Protect Folders
- Encrypt external USB drives

- How to password-protect a folder with Folder Guard
- User account policy
- Policy content

5. Trust relationship between domains

- Identity and Access (IDA)
- IDA Responsibilities
- IDA Technologies Supported by AD
- Trust
- Trust Types
- Trust Level
- Troubleshooting Trust
- Domain Controller (DC)
- Requires One or More DCs

6. Computer Management

- What does Computer Management Mean?
- Backup your Files
- Three Kinds of Backups
- A Bootable Backup (or “Clone”)
- External Backup Drive
- Cloud Backup
- Use Antivirus Software
- Ways to get Rid of Virus?
- Software Updates
- What happens if I don’t Update?
- Physical Cleaning

7. Workstation Management

- Purpose
- Overview
- Benefits
- Standard Features

- Laptops
- Desktops
- Workstations Hardware Inventory
- Workstation Software

8. Network Management commands

- Network Setup and Commands

1``Network Configuration

❖ What does Network Configuration mean?

- Network configuration is the process of setting a network's control, flow and operation to support the network communication of an organization and/or network owner.
- This broad term incorporates multiple configuration and setup processes on network hardware, software and other supporting devices and components.
- Network configuration is also known as **Network setup**.
- Network configuration allows a system administrator to set up a network to meet communication objectives.
- The Process involves the following tasks,
- Router configuration:-Router configuration specifies the correct IP addresses and route settings, etc.
- Host configuration:-Host configuration sets up a network connection on a host computer by logging the default network settings, such as IP addressing, Network name and ID/Password, to enable network connection and communication.

Network Administration

❖ What does Network Administration mean?

- A network administration is an IT expert who manages an organization's network.
- The network administrator must possess a high level of technological knowledge and is most commonly the highest level of technical staff within an organization.
- Network administrator keeps networks operational and monitor functions and operations within the network.
- A network administrator is responsible for installing, maintaining and upgrading any software or hardware required to efficiently run a computer network.

→ The computer network may extend to a local area Network (LAN), Wide area Network (WAN), the Internet and intranets.

Installing and configuration network adapters

What does Network Adapter mean?

Definition: -

A network adapter is the component of a computer's internal hardware that is used for communicating over a network with another computer.

It enable a computer to connect with another computer, server or any networking device over an LAN connection. A network adapter can be used over a wired or wireless network.

Techopedia explains Network Adapter A network adapter is usually the only component within a computer for interfacing or connecting with a network.

Typically, it is built on a printed circuit board with jumpers that connect it with the computer's motherboard.

A network adapter for wired networks has an RJ-45 port that uses twisted or untwisted pair cable for network connectivity.

Wireless adapters connect with the network through a built-in or externally connected antenna. Both network adapters support popular LAN protocols such as TCP/IP.

How Does a Wireless Adapter Work?

Adapter connect to the Internet and to other computers without using wires.

They send data via radio waves to routers that pass it on to broadband modems or internal networks. Most laptops and tablet computers have built-in wireless adapters, but you often have to install them on

desktop computers. Before adding them to office desktops and establishing a wireless network in your office, the kind of adapter

you get must match your needs.

Types of Adapters: -

A wireless adapter has to obtain signals from inside the computer, change them into radio waves and send them out via an antenna.

For a desktop computer, the electronic card either plugs in to a PCI slot inside the computer case, into a USB port from the outside, or into an Ethernet port via an Ethernet network cable.

For laptops that don't have a built-in adapter, the electronic card can fit into a PCMCIA slot or a mini PCI slot on the side of the laptop.

For tablets or notebooks that don't have an adapter, the electronic card can fit into a memory card slot.

The desktop PCI cards have an antenna that extends out of the back of the computer, while the other cards have the antennas inside the card cases.

Wireless Standards: -

The radio waves used by wireless adapters have to satisfy one of the 802.11 broadcast standards of the Institute of Electrical and Electronics Engineers (IEEE).

The most recent standard in common use as of January 2013 is 802.11n, but older adapter models use the "b" or "g" standards.

These standards determine the speed of data transfer at which the adapters broadcast, and all use the 2.4GHz radio frequency band.

Adapters using the recent standards also support the older standards.

A draft standard expected to be approved in 2013 is 802.11 ac which will be able to use the less-crowded 5GHz radio frequency band.

Speeds: -

The oldest standard, IEEE 802.11b, specifies broadcast speeds of up to 11Mbps. The later model adapters broadcast at IEEE 802.11g speeds that can range up to 54Mbps.

The IEEE 802.11n standard can theoretically reach speeds of 300Mbps but the adapters using it are usually slower because the radio frequencies are crowded and there is interference.

The draft 802.11c standard will theoretically be able to reach 1Gbps and will in fact be quite fast because it can operate in the 5GHz frequency band.

A business can purchase adapters and routers now satisfying the 802.11ac standard to reduce obsolescence.

Security: -

Wireless adapters broadcast the signals from your computer with a range of about 200 feet. Anyone with a wireless adapter installed in their computers or laptops can pick up your signal and access your files.

Securing your wireless network is especially critical for businesses protecting sensitive material and their intellectual property.

To avoid this unauthorized access, wireless adapters use encryption to secure their signals. The WEP, WPA and WPA2 protocols offer password-protected and encrypted transmissions for wireless networks. Your adapter must support these protocols to use them; most do support them.

The WEP protocol has some weaknesses, while the WPA2 protocol has the strongest security.

How to install network adapter?

1. Open Device Manager, and then follow the instructions in the procedure.
2. Locate the media that contains the driver for your network adapter.
3. On the A network adapter was not found page, click Open Device Manager to install drivers.
4. In Device Manager, click the Action menu, and then click Add legacy hardware.

How to configure network adapter?

How to Add and Configure Network Adapters for a Virtual Machine You can configure one or more virtual network adapters for a virtual machine by creating or modifying a Virtual Machine Manager hardware profile.

Typically, you use a virtual network adapter to connect a virtual machine to one of the following types of virtual network :-

1. Internal network:-

If you connect a virtual network adapter configured for a virtual machine to an internal network, only other virtual machines deployed on the same host are connected to and can communicate over that internal network.

2. External network:-

If you connect a virtual network adapter configured for a virtual machine to a physical network adapter on the host on which the virtual machine is deployed, the virtual machine can access the network to which the physical host computer is connected and can function on the host's local area network (LAN) in the same way that physical computers connected to the LAN can function. If the host computer can access the Internet, the virtual machine can access the Internet.

The following procedure assumes one of the following:

You are creating a new stand-alone hardware profile and are configuring the Hardware Settings tab.

You are configuring hardware profile settings on the Configure Hardware page of the New Template Wizard or the New Virtual Machine Wizard.

You are configuring the properties of an existing stand-alone hardware profile on its Hardware Settings tab or are configuring an existing template or virtual machine on the Hardware Configuration tab.

To add and configure a virtual network adapter for a virtual machine To add a virtual network adapter to the hardware profile, in the left pane, click Network Adapters, and then click Network Adapter on the top menu.

By default, a virtual network adapter that you add is not connected to a virtual network. Optionally, you can configure virtual machines created from this hardware profile to use one or more virtual network adapters that connect the virtual machines to internal networks or to external networks once the virtual machines are deployed on a host.

In the left pane, click the network adapter that you just added, and then, in the results pane, either accept the defaults (and modify them later) or configure the following options:-

1. Connected to Under Virtual network, in the Connected to drop-down list box, choose one of the following options:
Not connected (default). Select this option for a virtual machine that you do not want to connect to any network or that you want to configure later.
2. Internal Network: Select this option for a virtual machine that you want to connect to an isolated internal network that enables communication only among virtual machines on the same host.
3. Virtual machines attached to the internal virtual network cannot communicate with the host, with any other physical computers on the host's LAN, or with the Internet.
4. External Network Adapter Name: Select this option to specify that a virtual machine created by using this hardware profile will be connected to a physical network adapter on its host. Virtual machines attached to a physical network adapter can communicate with any

physical or virtual computer that the host can communicate with and with any resources available on the intranet and over the Internet that the host computer can access.

5. Ethernet (MAC) address : Like the MAC address on physical computers, a virtual MAC address on virtual machines uniquely identifies each computer on the same subnet. Select one of the following options:

Dynamic :-

Select this option if you want to enable a dynamic MAC address for a virtual machine.

Static :-

Select this option if you want to specify a static MAC address for a virtual machine. Type a static MAC address in the field provided.

To save the settings, do one of the following:

Option 1 :-

If this hardware profile is a new or existing stand-alone hardware profile, click Apply to save the settings.

Option 2 :-

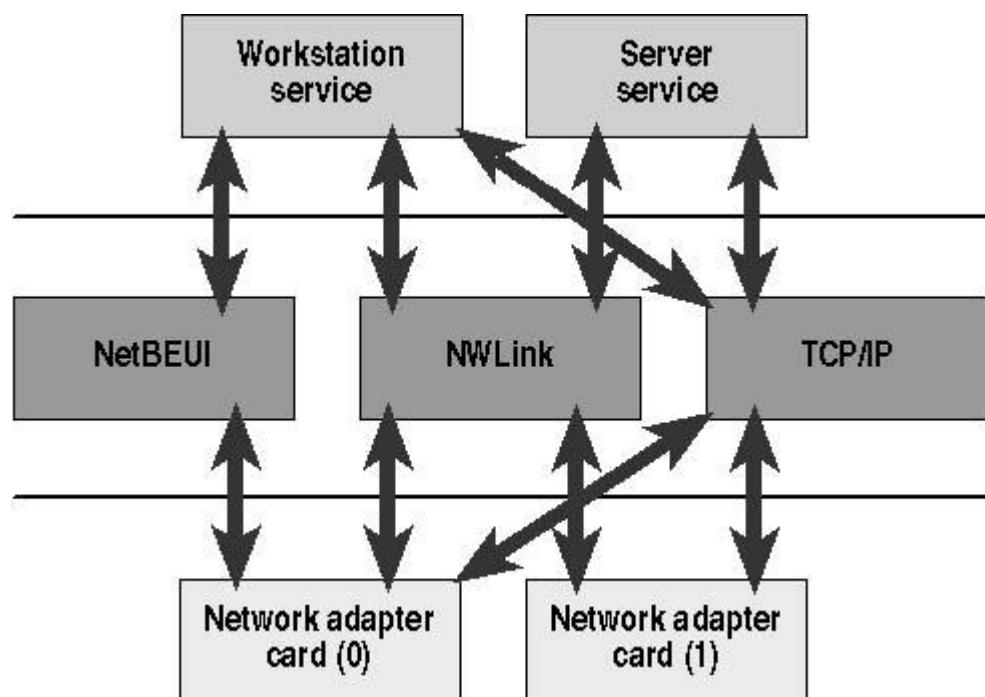
If this hardware profile is on the Configure Hardware page in the New Virtual Machine Wizard or the New Template Wizard (and you have completed any other settings you want to configure on this hardware profile), click Next to save the settings and continue to the next page. Alternatively, to save your settings not only in this wizard but also as a stand-alone profile, click Save Profile, type a name in the Name field on the General tab (and, optionally, change any other settings); click Apply, click OK to return to the Configure Hardware page; click Next to continue to the next wizard page, and then complete the wizard as usual.

Option 3 :-

If this hardware profile is on the properties page of an existing virtual machine or template, click Apply to save the settings.

Network Bindings

Network bindings enable communication among network adapter card drivers, protocols, and services. Figure 4.10 shows an example of network bindings. In this example, the workstation service is bound to each of three protocols, and each protocol is bound to at least one network adapter card. This lesson describes the function of bindings in a network and the process for configuring them.



The Windows XP Professional network architecture uses a series of interdependent layers. The bottom layer of the network architecture ends at the network adapter card, which places information on the cable, allowing information to flow between computers.

Binding Between Architectural Levels

Binding is the process of linking network components on different levels to enable communication between those components. A network component can be bound to one or more network components above or

below it. The services that each component provides can be shared by all other components that are bound to it. For example, in Figure 4.10, TCP/IP is bound to both the Workstation service and the Server service.

Combining Network Bindings

Many combinations of network bindings are possible. In the example shown in Figure 4.10, all three protocols are bound to the Workstation service, but only the routable protocols, NWLink and TCP/IP, are bound to the Server service. It is possible to select which protocols are bound to the network adapter cards if you are a member of the Administrators group. Network adapter card (0) is bound to all three protocols, and network adapter card (1) is bound only to the routable protocols.

When adding network software, Windows XP Professional automatically binds all dependent network components accordingly. Network Driver Interface Specification (NDIS) 5.1 provides the capability to bind multiple protocols to multiple network adapter card drivers.

Configuring Network Bindings

You can configure your network bindings using My Network Places.

To configure network bindings, complete the following steps:

1. Click Start and then click Control Panel.
2. In the Control Panel window, click Network And Internet Connections.
3. In the Network And Internet Connections window, click Network Connections.
4. In the Network Connections window, on the Advanced menu, click Advanced Settings.
5. In the Advanced Settings dialog box, under Client For Microsoft Networks, do one of the following:
 - o To bind the protocol to the selected adapter, select the check box to the left of the adapter.

There should be a check mark in the check box.

- To unbind the protocol from the selected adapter, clear the check box to the left of the adapter.

There should *not* be a check mark in the check box.

Only an experienced network administrator familiar with the requirements of the network software should attempt to change binding settings.

Specifying Binding Order

You also can specify binding order to optimize network performance. For example, a computer running Windows XP Professional has NWLink IPX/SPX and TCP/IP installed. However, most of the servers to which this computer connects are running only TCP/IP. Verify that the Workstation binding to TCP/IP is listed before the Workstation bindings for the NWLink IPX/SPX protocol. In this way, when a user attempts to make a connection to a server, the Workstation service first attempts to establish the connection using TCP/IP.

To specify binding order, complete the following steps:

1. Click Start and then click Control Panel.
2. In the Control Panel window, click Network And Internet Connections.
3. In the Network And Internet Connections window, click Network Connections.
4. In the Network Connections window, on the Advanced menu, click Advanced Settings.
5. In the Advanced Settings dialog box, under Client For Microsoft Networks, click the protocol for which you want to change the binding order.
6. Use the arrow buttons to change the binding order for protocols that are bound to a specific adapter:
 - To move the protocol higher in the binding order, click the upward pointing arrow.
 - To move the protocol lower in the binding order, click the downward pointing arrow.

3.SHARING FILES & PRINTERS

There has always been demand for file sharing. This way probably the most fundamental requirement users stressed when demanding network services. Following that, there has always been a marked demand for resource sharing-in other words, sharing printers, tape drives, and myriad other expensive resources. There are two basic tenets for a NOS to be considered usable.

Some examples of sharable resources are computer programs, data, storage devices, and printers. E.G. **shared file access** (also known as disk sharing and folder sharing), **shared printer access** (printer sharing), shared scanner access, etc. The shared resource is called a shared disk (also known as **mounted** disk), shared drive volume, shared file, shared document, shared printer or shared scanner.

PEER TO PEER FILE SHARINGS

Peer to peer file sharing is based on the peer to peer (p2p) application architecture. A peer to peer network supports unstructured access to network attached resources. Each device in a peer to peer network can be a client and server simultaneously. All devices in the network are capable of accessing data, software, and other network resources directly. In other words, each networked computer is a peer of every other networked computer; there is no hierarchy.

USES

Peer to peer networking has two primary uses. First, it's ideally suited for small organizations with a limited budget for information technologies and limited need for information sharing. Alternative, workgroups within larger organizations can also use this methodology for a tighter sharing of information within a particular group.

BENEFITS

There are main **four** benefits of peer to peer file sharing:

- Peer to peer networks are relatively easy to implement and operate. They are little more than a collection of client computers that have a network operating system that permits peer to peer resource sharing.
- Peer to peer networks are also inexpensive to operate. They lack expensive, sophisticated, dedicated servers that require special administrative care and climate conditioning.
- A peer to peer network can be established with familiar operating systems such as windows 95/98, windows NT/2000, and windows for workgroup.

- Their lack of a hierarchical dependence makes peer to peer networks much more fault tolerant than server based networks.

LIMITATIONS

The peer to peer network suffers from numerous security weaknesses:

- Users must maintain multiple passwords, typically one for each machine they used to access. Users tend to devise very creative means of coping with an excess of passwords. Most of these ways directly compromise the security of every machine in the peer to peer network.
- The lack of central repository for shared resources imposes the burden of finding information squarely on each user. This difficulty can be overcome with method and producers, provided each member of the workgroup compiles.

COMMON FILE SYSTEMS AND PROTOCOLS

Shared file and printers access require an operating system on the client that supports access to resources on a server, an **operating systems** on the server that supports access to its resources from a client, and an application layer (in the four or five layer **TCP/IP reference model**) file sharing protocols and transport layer protocol to provide that shared access. Modern operating systems for personal computers include distributed file systems that support file sharing, while hand-held computing devices sometimes require additional software for shared file access.

The most common such file systems and protocols are:

PRIMARY OPERATING SYSTEMS	APPLICATIONS PROTOCOLS	TRANSPORT PROTOCOLS
Mac OS	SMB, APPLE filing protocol	TCP, UDP or Apple talk
UNIX-Like systems	Network file systems(NFS), SMB	TCP or UDP
MS-DOS, Windows	SMB, also known as CIFS	TCP, NBT(includes UDP), NBF, or other NetBIOS transport
Novell NetWare(server) MS-DOS, Windows(client)	NCP and SAP	SPX(over IPX), or TCP

FILE AND PRINTER SHARING

Microsoft's domain services use a namespace structure to define logical network names for users, printers, and other resources in a Windows NT environment. A flat namespace structure is acceptable for simple network in single geographic locations; however, it has significant limitations in environment that are more complex. In fact, all your users and network resources are organized in one list. You can see why organizing users and network resources in one list is time consuming when you do not use hierarchical file system. This is why Novell is still considered a better choice in this area of functionality.

FOLDER SECURITY

There are three types of folder security :-

- 1) Password Protected Folders
- 2) Using Encrypt External USB drives
- 3) With the use of Folder guard

Lock folders and drives with passwords



1) Password-Protect Folders

If you want to protect folders with passwords **without encrypting the files**, then [Folder Guard](#) is the tool you need. The password protection is instantaneous, no matter how many files the folder contains or how large the files are. However, the [password protection](#) takes effect only on your computer, where Folder Guard is running: if you move the folder to another computer, it will not be protected, unless that computer has Folder Guard installed and configured, as well. [Read more about Folder Guard...](#)



2) Encrypt external USB drives

If you have an external drive that you want to protect with a password, then [USB Crypt](#) is the software you need. This software creates an [encrypted area on the external drive](#) that you can use to keep your sensitive files. You can use the [encrypted drive](#) with other computers, that don't have USB Crypt software installed. If you lose the encrypted drive, your files will be safely protected with the password you've chosen. [Read more about USB Crypt...](#)

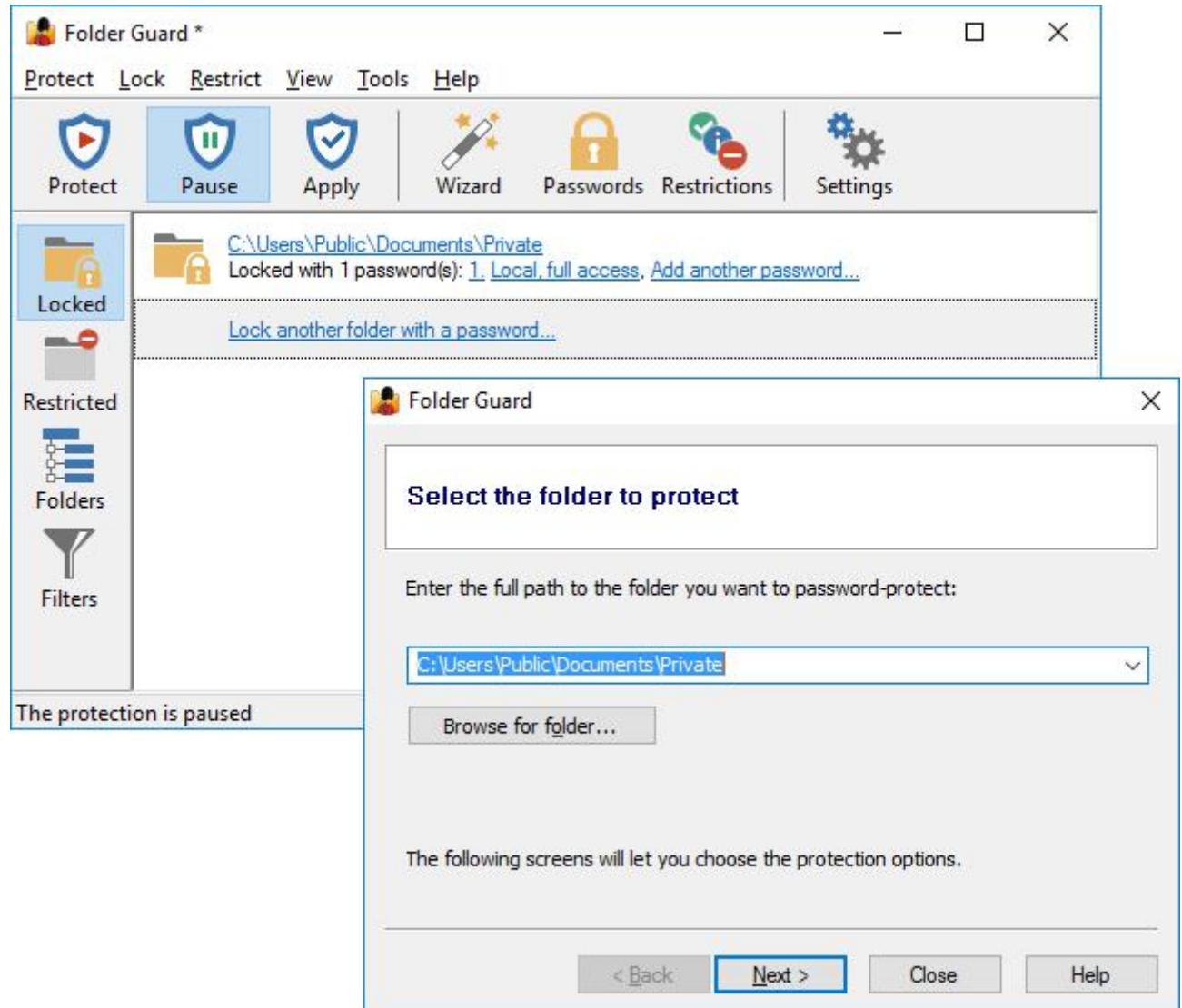
3) How to password-protect a folder with Folder Guard

You can use [Folder Guard](#) software to protect folders with



passwords.

To lock a folder with a password: run Folder Guard and drag and drop the folder you want to protect to its window, or click the *Lock another folder with a password* link:

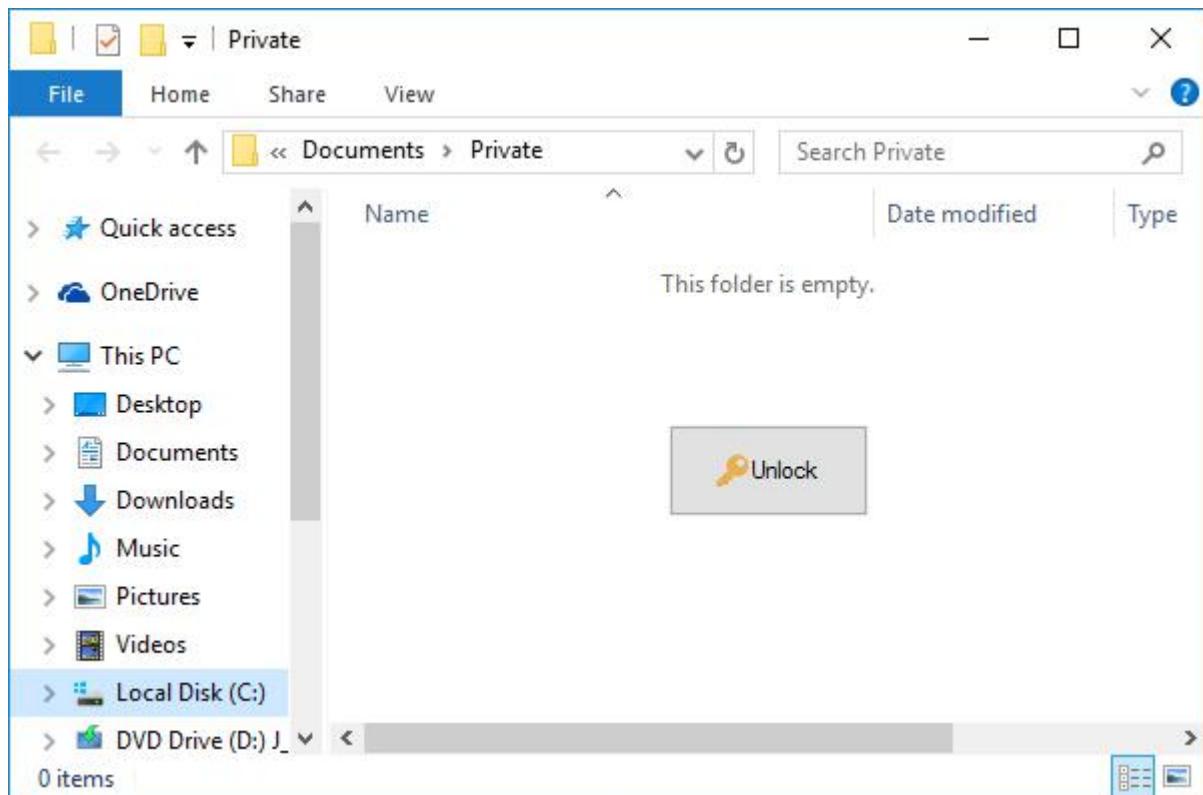


Select the folder to protect, enter the desired password, adjust the password properties, as needed:

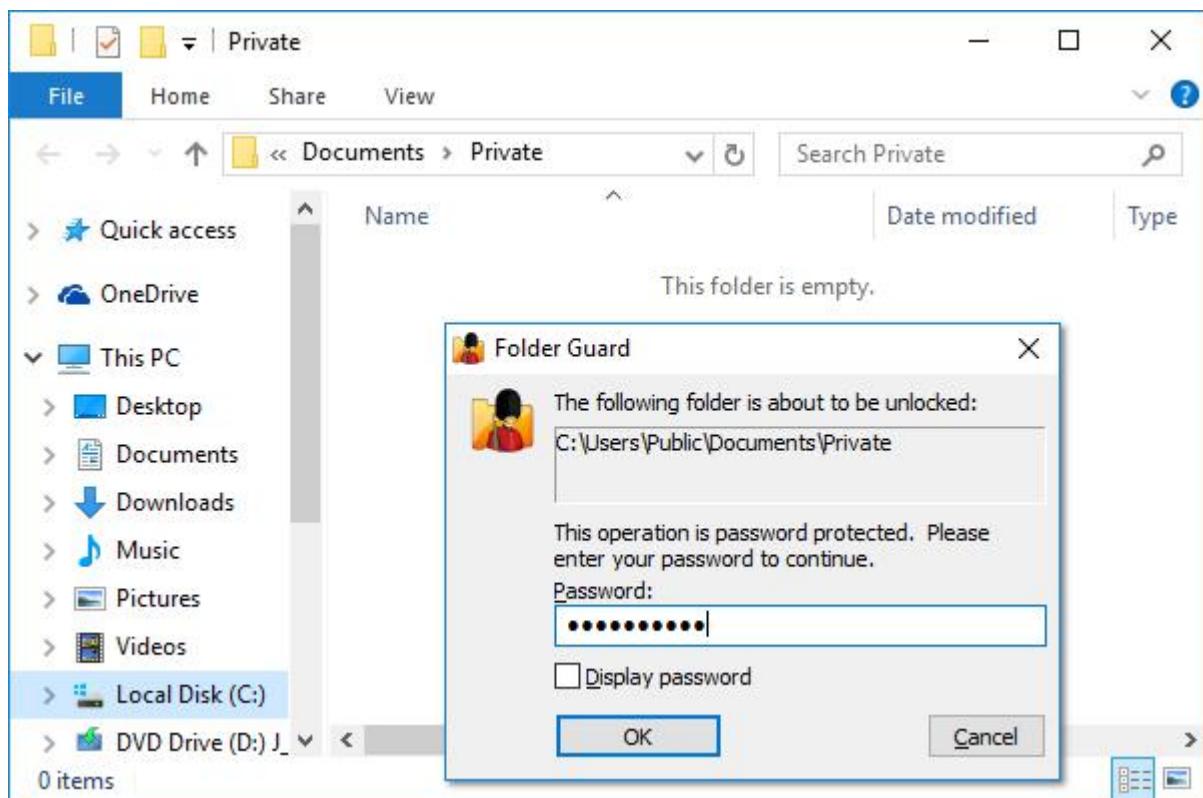


You can specify that the password may be used only by the local users, or by the network users, or both. You can choose the password to unlock a full access to the folder, or give the user the read-only access. (You can create several different passwords for the same folder, giving different access types to the users.)

Now apply the changes and try to open the folder you have just protected. Navigate to the protected folder, and you should see an empty window with the Unlock button in the middle:



Click the Unlock button, and prompt for the password should appear:



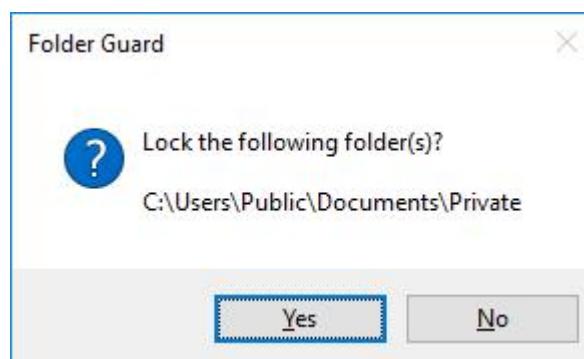
If you have entered the correct password, the folder should become unprotected and you should be able to work with the files and subfolders



it contains without restrictions, as usual. However, if you don't enter the correct password, the folder will remain protected.

(Note that in order to unlock the folder this way, you need to double-click on the folder in the right-hand panel of the Windows Explorer window. If you select the folder in the left-hand panel that shows the folder tree, the password prompt will not be shown and the *Access denied* message will be shown instead.)

Now, after you have unlocked the folder, try to close the Windows Explorer window, and you should see a prompt to lock the folder back:



Reply yes, and the folder will be locked back with the password again, and will remain inaccessible until you enter the correct password again.

In addition to the basic password-protection described above, [Folder Guard](#) lets you customize the way it works to suit your specific requirements:

Encrypt and password-protect external drives with *USBCrypt* software for Windows 10,8,7, and XP.

User rating: ★★★★★ 4.7/5

[Purchase](#) or [download](#) a free trial. [Read more...](#)

- You can direct Folder Guard to add the *Lock* and *Unlock* commands to the Windows shortcut menu. You can use them to lock and unlock the password-protected folders by right-clicking on them, instead of (or in addition to) double-clicking on the folders as described above.
- If you have locked many folders with passwords, you can make them all accessible at once by running Folder Guard and pausing the protection (you will need to enter your Master password, of course!) When you are done working with the protected folders,

- run Folder Guard and choose to resume the protection, to lock all folders at once with one click.
- Instead of locking files and folders with passwords, you can completely [hide](#) them!

User account policy

A user account policy is a document which outlines the requirements for requesting and maintaining an account on computer systems or networks, typically within an organization. It is very important for large sites where users typically have accounts on many systems. Some sites have users read and sign an account policy as part of the account request process.

Policy content

Should state who has the authority to approve account requests. Should state who is allowed to use the resources (e.g., employees or students only) should state any citizenship/resident requirements. Should state if users are allowed to share accounts or if users are allowed to have multiple accounts on a single host. Should state the users' rights and responsibilities. Should state when the account should be disabled and archived. Should state how long the account can remain inactive before it is disabled. Should state password construction and aging rules.

Example:

Some example wording: “Employees shall only request/receive accounts on systems they have a true business need to access. Employees may only have one official account per system and the account ID and login

name must follow the established standards. Employees must read and sign the acceptable use policy prior to requesting an account.”

ACTIVE DIRECTORY DOMAIN AND TRUST

Identity and Access(IDA)

An IDA infrastructure should:

Store information about users, groups, computers and other identities.

An identity is representation of an entity that will perform actions on a server.

A component of the IDA is the identity store that contains properties that uniquely identify the object such as:

Username

Security identifier (SID)

Password

The Active Directory (AD) data store is an identity store.

The directory itself is hosted on and managed by a domain controller—a server performing the Activity Directory Domain Services (ADDS) role.

IDA responsibilities

Authentication

A Duses Kerberos Authentication

Access Control

Maintains an Access Control List (ACL)

Reflects a security policy composed of permissions that specify access levels for particular identities.

Audit Trail

Allows monitoring of changes and activities within the IDA infrastructure

IDA Technologies supported by AD

Identity

Applications

Trust

Integrity

Partnership

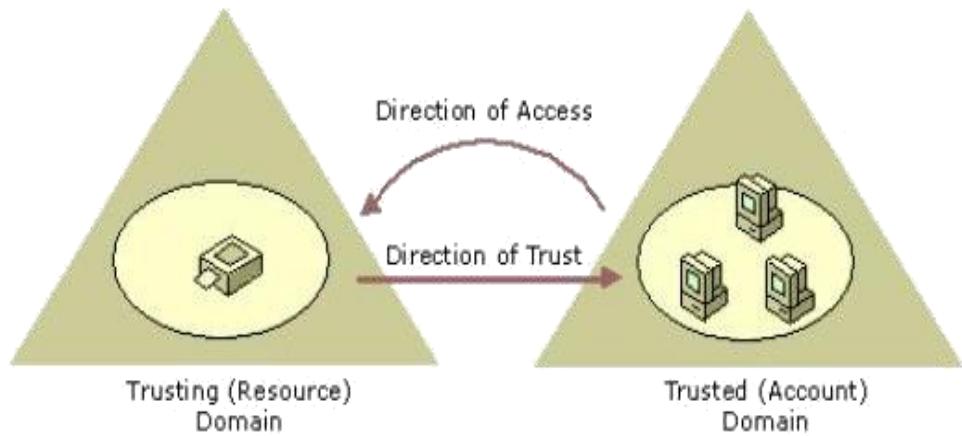
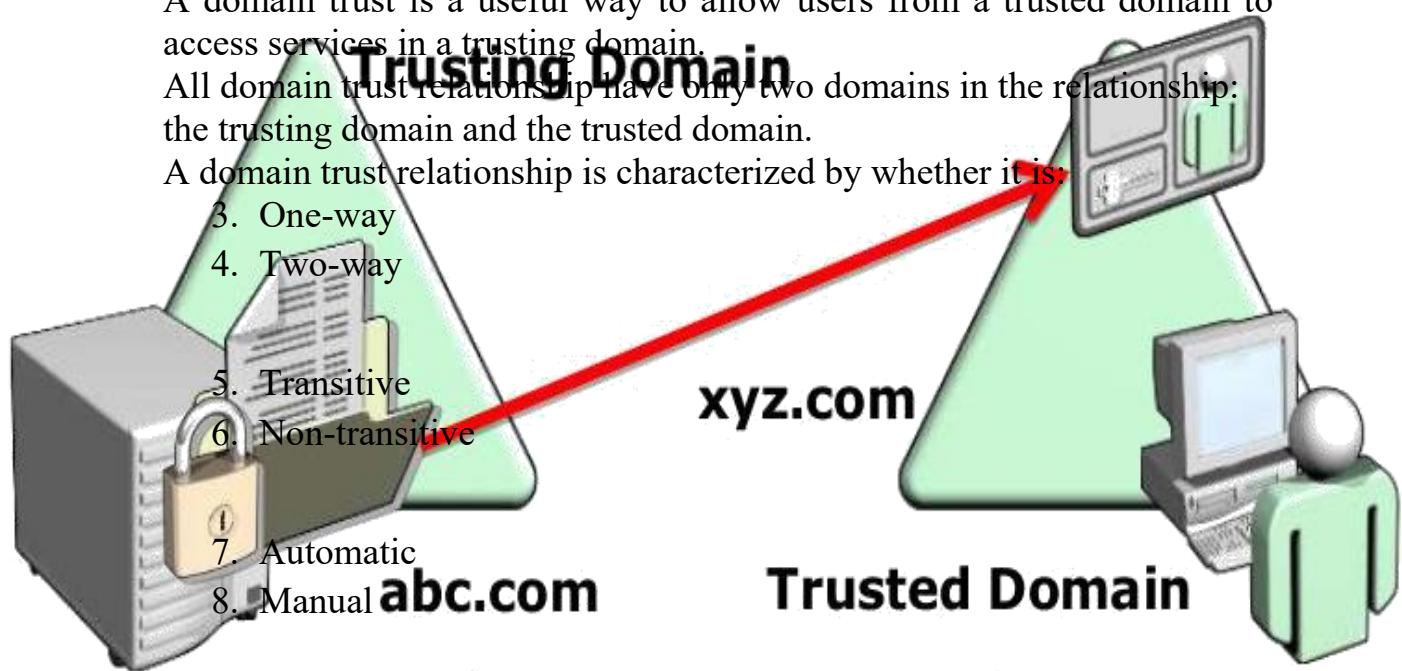
Trust

A domain trust is a useful way to allow users from a trusted domain to access services in a trusting domain.

All domain trust relationships have only two domains in the relationship: the trusting domain and the trusted domain.

A domain trust relationship is characterized by whether it is:

3. One-way
4. Two-way
5. Transitive
6. Non-transitive
7. Automatic
8. Manual



TRUST TYPES

Trust type	Transitivity	Direction	Description
External	Nontransitive	One-way or two-way	Use external trusts to provide access to resources that are located on a Windows NT 4.0 domain or on different forest
Realm	Transitive or nontransitive	One-way or two-way	Use realm trusts to form a trust relationship between a non-Windows Kerberos realm and an Active Directory domain.
Forest	Transitive	One-way or two-way	Use forest trusts to share resources between forests
TRUST LEVEL			
Shortcut	Forest-Wide Authentication: Forest-wide authentication setting permits unrestricted access by any users in the trusted forest to all available shared resources	One-way or two-way	Use shortcut trusts to improve user logon times between two domains within An Active Directory forest.
	Selective Authentication: Selective authentication is a security setting that can be enabled to define the area of access.		



TROUBLESHOOTING TRUST

Some common trust errors:

The trust relationship between this workstation and the primary domain failed.

Cause: There is incorrect time synchronization between domain controllers or workstation, the server might be down, or the trust relationship might be broken.

Solution: Run the command-line tool Netdom to verify, reset, or establish the trust between computers.

Rejoining client to domain.

Clients are not able to access resources in a domain outside the forest.

Cause: A failure occurred on the external trust between the domains.

Solution: Reset and verify the trust between domains.

Verify trust password is same.

Domain Controller (DC)

The DCs are servers that perform the AD DC role.

The DCs also run the Kerberos Key Distribution Center (KDC) service.
Domain.

Requires one or more DCs

DCs replicate the domain's partition of the data store so that any DC can authenticate any identity in the domain.

Is a scope of administrative policies such as password complexity and account lockout policies.

What does Computer Management mean?

Computer management is the process of managing, monitoring and optimizing a computer system for performance, availability, security and/or any base operational requirement.

It is broad term that includes manual and automated administrative processes in the operations of a computer.

Computer management is also known as PC management or desktop management.

A computer needs to be maintained in order to keep working properly. computer maintenance keeps your computer working in good shape and contributes to keeping computer troubles at bay . Computer management includes backing up your files, install software updates, use antivirus software, use disk tools and physical cleaning of computer.

Back Up Your Files

One of the most stressful experiences for a computer user is data loss, which means that parts of a database can no longer be retrieved. Losing only a few files can mean hours or days of work lost. Imagine the consequences of losing all the data on your computer. Most computers use a hard disk drive as the primary storage device. Hard disk drives can function for many years, but at some point, they will crash. It's a matter of when, not if.

Data loss can also result from other types of damage, such as fire or water damage, or your equipment could be stolen. For things like theft and damage, you normally have insurance. However, the cost of a new hard disk drive is probably the least of your worries if yours has crashed and the data cannot be recovered. Think of all your files: your favorite music, your family photographs, financial documents, other personal files. How much are those worth to you?

The simplest definition of a computer backup is an exact copy. In the case of computer files, we are referring to copies of the original files that you have on your laptop, desktop, or external drive. Creating a backup of original content means having that data saved in two places, but it's also important to make sure that those two places aren't on the same type of device. For example, if you have 3 copies of a working document on your computer, if your computer crashes, you will still lose all three. This makes the backup method and medium, an important thing to consider for your backup strategy!

Your best insurance policy is to create a backup of your files. You can burn a CD or DVD with your most critical files, copy your files to an external hard disk drive or use an online backup service. Whatever strategy you use, just make sure to create a backup copy of your files on a regular basis.

Backup software facilitates creating a backup of the files on your computer. Backup software helps you copy the most important files to another storage device, such as an external hard disk. You can also make an exact copy of your hard disk.

Increasingly, backup software uses cloud storage to create backups. This typically means you pay a fee to use the storage space of a third party and use their backup software to manage which files are going to be backed up. If your computer were to crash completely or get stolen, you can download all your files to a new computer from the cloud.

Three Kinds of Backups

There are many ways to backup your files. Even manual copies (like saving a copy to a USB drive) are a kind of backup, they just aren't a very good kind, because you have to do it manually, you have to do it repeatedly, and you have to manage things like deleting and renaming files. A good backup system is as easy as possible (so you're more likely to use it) but the best backup systems automatically perform incremental backups so you don't need to think about it or remember to do anything about it once the system is set up.

A Bootable Backup (or “Clone”)

A "bootable backup" (sometimes called a "clone") is like a spare tire for your car. If you get a flat tire, a spare will let you finish your trip or at least get you to the point where you can get more help. A clone is a complete copy of your computer's primary hard drive (sometimes called a "boot drive"). If your computer's primary drive died tomorrow you could hook up the clone, reboot your computer from it, and have immediate access to not only all of your files but also all of the software you use, including all of the settings and configuration changes that you have made. If you are in the middle of an important project or just don't have time to replace the boot drive immediately, a clone can really save the day. A clone also has a copy of all your files as they were when the clone was last updated, which means that if you accidentally deleted a file, you can copy it back from the clone to your boot drive.

External Backup Drive

External drive backups are mainly intended to provide a backup of your personal files, especially irreplaceable things like pictures. Instead of looking at your entire hard drive, this type of backup only looks at certain folders, such as your home directory. The archive part of this type of backup means that if files are on your primary hard drive are changed (or even deleted) you can go back to undo the changes and even recover those deleted files. If your computer dies you can simply plug the external backup drive into a different computer and immediately have access to all of your files, as well as the history of changes and deleted files.

Cloud Backup

Having a backup (or two) next to your computer is a good start, but it still puts your data at risk for theft, fire, or other disaster. Your best protection against that type of loss is to keep another backup somewhere else. While you could make a clone and bring it to a friend's house or your office, or even put it into a safe-deposit box, chances are that you would not remember to keep it updated because it would be inconvenient.

In fact, cloud backups are the easiest kind to create and maintain. To get started you simply need to create an account, download software, run it once to enter your account information, and (optionally) set any preferences that you might want. After the initial setup you don't need to do anything, the software will automatically keep your computer backed up any time it is turned on and connected to the Internet.

Use Antivirus Software

Computer systems face a number of security threats. The most serious threats consist of viruses and other harmful programs. A computer virus is a computer program that can cause damage to a computer's software, hardware or data. It is referred to as a 'virus' because it has the capability to replicate itself and hide inside other computer files.

There are many types of viruses, and new ones are being developed all the time. Once a virus is present on a computer, it typically performs some type of harmful action, such as corrupting data or obtaining sensitive information. Computer viruses are only one type of malware, short for 'malicious software.' Malware is used by attackers to disrupt computer operation.

The best way to deal with the threat of computer viruses is to use antivirus software. Antivirus software helps to protect a computer system from viruses and other harmful programs. As the first line of defense, antivirus software prevents viruses from getting into your computer system. Antivirus software scans your online activity to make sure you are not downloading infected files. Antivirus software also helps to detect and remove viruses from your computer system if you get infected.

One of the most common ways to get a virus on your computer is to download a file from the Internet that is infected. If you get an e-mail from someone you don't know with a file attached to it, be careful opening up these attachments because it could be infected with a virus. New viruses are coming out all the time, so antivirus software needs to be updated very frequently.

Typically, antivirus software is scheduled to run a scan on your entire computer system on a regular basis and to prompt you to download updates. Running antivirus software and keeping it up to date is one of the most important things you can do as part of computer maintenance.

Ways to get rid of viruses?

Signature-based detection –

This is most common in Traditional antivirus software that checks all the .EXE files and validates it with the known list of viruses and other types of malware. or it checks if the unknown executable files shows any misbehavior as a sign of unknown viruses.

Heuristic-based detection –

This type of detection is most commonly used in combination with signature-based detection. Heuristic technology is deployed in most of the antivirus programs. This helps the antivirus software to detect new or a variant or an altered version of malware, even in the absence of the latest virus definitions.

Behavioral-based detection –

This type of detection is used in Intrusion Detection mechanism. This concentrates more in detecting the characteristics of the malware during execution. This mechanism detects malware only while the malware performs malware actions.

Sandbox detection –

It functions most likely to that of behavioral based detection method. It executes any applications in the virtual environment to track what kind of actions it performs. Verifying the actions of the program that are logged in, the antivirus software can identify if the program is malicious or not.

Data mining techniques –

This is of the latest trends in detecting a malware. With a set of program features, Data mining helps to find if the program is malicious or not.

Software updates

An update is a software file that contains fixes for problems found by other users or the software developer. Installing an update fixes the code and prevents the problems from happening on your computer. Because updates fix problems with a program, they are almost always free and available through the program or the companies website. Updates are necessary to fix any problems with a software program or hardware device that were not detected before the product was released to the public.

What happens if I don't update?

There are several things that can happen if you do not update, below are the most common symptoms you would encounter if you do not update.

Fix errors - Most updates fix errors and if you don't update you'll get those errors.

Security vulnerabilities - Updates also patch security holes, if you don't update your personal information may be compromised.

Fix conflicts - It is not uncommon to discover conflicts with other programs and hardware. If you don't update, conflicts may happen and cause problems with other programs.

Physical cleaning

As a computer runs, it generates static electricity, which attracts dust and hairs. These nasty bits clump together and gunk up the heat sink, case fans, and other computer components. It's not only gross but also ends up blocking airflow, which causes overheating. So beyond annual spring-cleanings, it's important to routinely clear out any messy buildups in your rig. Without further ado, let's start scrubbing down our PCs!

One should clean the computer within a while to avoid major damage to the computer. Cleaning the computer screen, mouse, keyboard, CPU and other tangible parts of the machine will help you to run your computer smoothly and in managed manner.

Workstation Management

Purpose

This Service Description is applicable to **Workstation Management** services offered by MN.IT Services and described in the MN.IT Service Catalog. This document defines the scope, Service Components and Support Services required in delivering the **Workstation Management** offering.

Overview

Workstation Management provides technical support for State-owned personal computers (PC). Workstations receiving standard desktop

support are managed with standard processes, tools, and policies. Remote administration tools are used whenever possible to minimize interruptions and provide faster service.

Support provided by Workstation Management Technicians include: installations, configurations, connections, maintenance, troubleshooting, and repair of computers, accessories and peripherals.

Benefits

Workstation Management services improve business efficiencies, increases productivity, and provide cost savings. With standard hardware and software, advanced deployment and management tools, and innovative client features, Workstation Management provides a consistent computing experience for end users within an organization.

These are the top benefits of workstation management:

- Single point of contact for reporting incidents or service requests, available 24 x 7 x 365. [SEP]
 - Standard software with uniform configurations ensures end users have the same set of applications to allow for collaboration while reducing training needs. [SEP]
 - Common requested software can be deployed faster and have greater compatibility than unique software. [SEP]
 - Workstation Management decreases the amount of time to deploy new hardware and software. [SEP]
 - Periodic hardware refreshes ensures your business has devices to meet business requirements and the performance demands of new applications. Additionally, newer hardware is less prone to failure. [SEP]
 - Asset tracking provides information about what hardware and software is utilized by the business. [SEP]
 - Devices will be secured to the Enterprise Security Office (ESO) standard to reduce the risk of virus, [SEP] malware and system exploits. [SEP]
- **Standard Features**
- [SEP] This section describes the standard features of the Workstation

Management service. Where applicable, customer options are noted, along with feature limits and the responsibilities of MN.IT Services.

Operating Systems The operating system (OS) links the workstation hardware resources (e.g., hard drive, processor and memory), user input/output devices (e.g., keyboard, mouse and monitor), and the workstation software applications (e.g., Microsoft Office, web browser, etc.). The primary supported operating system by MN.IT Services is the Microsoft Windows client operating system; more specifically Windows 7 and Windows XP. All standard workstations will have Windows 7 Enterprise installed, unless there is business justification to run a different operating system. OS X, iOS, and Android are supported by MN.IT Services on a limited, best effort basis. Support consists of basic hardware setup, connectivity to the network (wired and/or wireless) and configuration of standard business applications (e.g., email). Limits

- OS X, iOS, and Android are supported on a limited, best effort basis.

Customer Responsibility • Provide end user training on how to use the operating system. **MN.IT Services Responsibility** • Provide

Microsoft Windows client operating system. **Workstation Hardware**

The minimum hardware specification (e.g., memory, processor, disk, etc.) for workstations (e.g., laptops and desktops) is maintained and periodically updated by MN.IT Service's Information Technology Standards and Resource Management division (ISRM). This group also ensures devices meet the State of Minnesota's end user accessibility requirements. Workstation hardware must be assigned either to an employee, project, or business unit. To maintain audit readiness, tracking software may be installed on workstation hardware. This ensures the status of physical hardware items and the use of software installed on those systems can be monitored. Within each workstation hardware type there are two classifications:

Standard – A *Standard laptop* or *Standard desktop* offers the computing power and resources needed by most end users to complete their day-to-day tasks.

Performance - A *Performance laptop* or *Performance desktop* offers additional computing power (e.g., processor and/or memory) which is needed when business requirements exceed the standard hardware (e.g., software development applications, CAD, and graphic design packages). For more information and details about these classifications, visit the [Minnesota IT Hardware Standards](#) website. 2

- Identifying organization strategy and new business initiatives, which may affect workstation hardware selection.
 - Aligning workstation needs to organization strategy and new initiatives.
[L][SEP]
 - Procuring workstations. [L][SEP]
 - Maintaining and periodically updating the standard hardware specification(s). [L][SEP]
 - Supporting full hardware life cycle (procurement, installation, configuration, break/fix, and retirement). [L][SEP]
 - Rebuilding workstations when they are transferred from one end user to another. [L][SEP]
 - Disposing of a failed or end-of-life hard drives in a manner which meets or exceeds the Enterprise Security Office (ESO) specifications. [L][SEP]
 - Coordinating hardware return merchandise authorization (RMA) requests with vendors for failed components. [L][SEP]
-
- **Laptops**
 - [L][SEP]A laptop computer - sometimes called a notebook computer - is a battery or AC-powered personal computer. Additionally, a laptop can effectively be turned into a desktop computer with a docking station, a hardware frame that supplies connections for peripheral input/output devices such as a printer or monitor. End users assigned with a State-owned laptop will be provided with the following equipment: [L][SEP]
 - (1) keyboard [L][SEP]
 - (1) mouse [L][SEP]
 - (1) monitor – external (if required) [L][SEP]
 - (1) docking station (if required) [L][SEP]
 - (1) power cord [L][SEP]
 - (1) laptop battery [L][SEP]Limits [L][SEP]
 - Laptop bags are not provided by MN.IT Services. [L][SEP]Customer

Responsibility [SEP] • Identify whether a “standard” or “performance” laptop is required to fulfill the end user or business role need. [SEP] MN.IT Services Responsibility

Laptop hardware refresh within 36 to 48 months from initial purchase [SEP]

Monitor (external) refresh within 5 to 6 years from initial purchase, or as required [SEP]

Connect the laptop to the customer Local Area Network (LAN) [SEP]

Optionally connect the laptop to the customer Wireless Network (Wi-Fi).

Desktops

[SEP] A desktop computer is a personal computer that is designed to fit conveniently on top of a typical office desk. End users assigned with a State-owned desktop will be provided with the following equipment: [SEP]

- (1) Keyboard

(1) monitor Customer Responsibility [SEP]

- Identify whether a “standard” or “performance” desktop is required to fulfill the end user or business role need.
- Hardware refresh within 36 to 48 months of initial purchase. [SEP]
- Monitor refresh within 5 to 6 years from initial purchase, or as required. [SEP]
- Connect the desktop to the customer Local Area Network (LAN). [SEP]

Workstation Hardware Inventory

- [SEP] The workstation hardware inventory process involves tracking desktop and laptop assets through their life cycle and facilitating their transition through different life cycle phases (e.g., acquisition through disposal). The process collects and maintains the following list of information:

- Hardware manufacturer [SEP]
- Make/Model [SEP]

- Serial number [L]
[SEP]
- Asset number [L]
[SEP]
- Current assignee [L]
[SEP]
- Hardware basics (e.g., amount of RAM, total hard drive size and processor) [L]
[SEP]
 - Current operating system [L] MN.IT Services Responsibility
[SEP]
- Maintaining workstation hardware inventory [L]
[SEP]

Workstation Software

To ensure laptops and desktops are deployed consistently, standard operating system builds (including the installation of the workstation client operating system and standard software) will be used. These installations can be automated and greatly reduce the time required to deploy a workstation.

Software is classified into the following categories (with additional information in the sections below):

- **Required software** – Mandatory software installed on all workstations.
[L]
[SEP]
- **Standard software** – Provides a common application set to all end users.
[L]
[SEP]
- **Common requested software** – Software not relevant to all end users, but common enough to manage and support.
[L]
[SEP]
- **Unique software** – Unique software purchased on a “one-off” basis and installed to fulfill a specific business need.
[L]
[SEP]
- **Prohibited software** – Applications that are potentially damaging or enables the improper storage or transmittal of government data.
[L]
[SEP]

Required software

All State-owned workstations must have required software installed, which ensures workstations are protected from known viruses, malware exploits and system vulnerabilities. It also provides hardware and software inventory, workstation configuration, and remote support capabilities.

Required software includes:

- Antivirus [L1]
- Malware/spyware protection [L1]
- Local firewall (e.g., Windows Firewall) [L1]
- Hard drive encryption (e.g., Microsoft Bitlocker) [L1]
- Workstation management utilities (e.g., Active Directory Group Policy, Microsoft System Center Configuration Manager) [L1] Limits [L1]
- This software is not to be disabled or uninstalled in any form.

Customer Responsibility • Notify MN.IT Services if required software is not functional.

MN.IT Services Responsibility • Provide updates to required software on an as needed basis.

Standard software

Deploying standard software to workstations stems from the goals of providing a common application set to all end users and streamlining costs associated with application development, software installation, system administration, software licensing and support. By choosing standard software, MN.IT Services also is positioned to negotiate better pricing and maintenance fees.

Standard software is approved and supported by MN.IT Services.
Standard software includes:

- Microsoft Office productivity suite (e.g., Microsoft Office 2010 including: Access, Excel, InfoPath, One Note, Outlook, PowerPoint, SharePoint Workspace, and Word) [L1]
- Microsoft Visio viewer [L1]
- Microsoft Lync [L1]
- Middleware (i.e., Java runtime engine, Microsoft .Net Framework) [L1]
- Media players (i.e., Adobe Shockwave, Adobe Flash, Windows Media Player) [L1]
- PDF Reader (i.e., Adobe Reader) [L1]

- Web Browser (i.e., Internet Explorer) [L] [SEP] MN.IT Services Responsibility

[L]
[SEP]

- Provide and install updates to standard software on an as needed basis

Common requested software

Common requested software (common software) can be added to workstations with Standard software installed, but the software may not be relevant to all end users and may incur an additional cost.

Common software is approved by MN.IT Services.

Examples of common requested software:

- Virtual Private Network (VPN) client [L]
- Microsoft Visio [L]
- Microsoft Project [L] Limits [L]
- Troubleshooting application errors is done on a best effort basis

Customer Responsibility

7. Approve requests for common requested software [L]
 8. Purchasing the initial software, along with any future upgrades that are required [L]
 9. Provide installation media and license key(s) [L]
 10. Providing end users with training to use the software [L] MN.IT Services Responsibility [L]
- Preforming the initial installation of software on authorized computers

Unique software

Some business units or end users may require unique or “one-off” additional software (e.g., graphics programs, analytic or web development tools, etc.) to perform their day-to-day business. The installation of such software is permissible where the business unit provides the necessary installation media and license key(s).

Limits

- MN.IT Services does not support or test these applications [L]
[SEP]
- If an end user reports an incident for a workstation that has unique software installed, it may be uninstalled [L] in attempt to resolve the issue Customer Responsibility
 - Purchasing the initial software, along with any future upgrades that are required [L]
[SEP]
 - Providing installation media and license key(s) [L]
[SEP]
 - Applying patches when they become available, thus ensuring the integrity and security for other computers attached to the network [L]
[SEP]
 - Troubleshooting any application errors with unique software [L]
[SEP]
 - Providing end users with training on how to use the unique software [L]
[SEP]

Maintaining software inventory of unique software, including media and license key management [L] MN.IT Services Responsibility [L]
[SEP]

- Preforming the initial installation of unique software on authorized computers

Prohibited software

Some software poses serious risk to business; therefore, it is prohibited to download, install or use applications that are potentially damaging or enables the improper storage or transmittal of government data.

Prohibited software types:

- Software used to “crack” license keys or passwords

9. Peer-to-Peer (P2P) or File sharing software. Examples include but are not limited to: Bit Torrent, e Mule, Gutella, LimeWire and Kazaa
[L]
[SEP]

10. Software identified as “Freeware” or “Shareware”, where the End User License Agreement (EULA) specifically states NOT for use on Government/commercial systems [L]
[SEP]

11. Software that the State does not legally own or have received expressed permission from the copyright holder to use [L] Any system found running prohibited software will be required to remove the software immediately. Some systems, depending on

the software found running on it, will be required to be completely rebuilt to ensure the system is "clean" (not compromised).

[L][SEP]MN.IT Services Responsibility

1. Educate end users about prohibited software, including the types of software they should not download, install, or use [L][SEP]
2. Monitor for the use of prohibited software **Workstation Software Inventory** [L][SEP]The workstation software inventory process involves tracking software assets through their life cycle and facilitating their transition through different life cycle phases (e.g., acquisition through disposal). The process collects and maintains the following list of information: [L][SEP]
 3. Software manufacturer [L][SEP]
 4. Title [L][SEP]
 5. Version [L][SEP]
 6. Serial number/license key(s) [L][SEP]
 7. Current assignee [L][SEP]Customer Responsibility [L][SEP]
 - Maintaining workstation software inventory for unique and common requested software

MN.IT Services Responsibility • Maintaining workstation software inventory for required and standard software

Software updates

Software vendors will periodically release updates/patches to increase functionality, resolve known issues and address system vulnerabilities. To ensure these updates are deployed in a timely and consistent basis, an automated software update system may be used to advertise, install and track software updates and patches.

End users will be notified when updates are available for installation. Additionally, end users may be able to postpone the installation before the updates will be forcibly installed; which ensures they are installed in a timely manner and reduces security risks to unpatched systems.

Customer Responsibility

2. Ensuring users are connecting their assets to a corporate network on a regular basis to get updates [L][SEP]

3. Installing the updates when they become available (and rebooting if necessary) [L1] MN.IT Services Responsibility [SEP]

- Maintaining the automated software update system, including release and patch management

Optional Service Features

This section describes optional features for the Workstation Management service offering. These optional features are available to customers at additional cost.

Workstation Backups and Restores

Workstation backup and restore is the process of copying data preemptively for the specific purpose of restoring that same data. Data is often restored due to hardware failure, accidental deletion or corruption of data, a previous version is desired, or the device is lost or stolen.

It is recommended that files be stored in centralized (non-local) location such as a file server or SharePoint. This enables end users to quickly access data after a hardware failure or if the device is lost or stolen; as they do not need to wait for data restoration.

Limits

- The entire workstation hard drive is not backed up, rather only the locations where end users should be storing files (i.e. "My Documents" and their "desktop")
- Backups provide a "point-in-time" snapshot of the data being backed up. Therefore a backup may not always contain the most recent version of a file, nor does it maintain all of the "versions" (saves) of a file between backups
- Workstations need to be connected to the office intranet for backups to occur Customer Responsibility
- Identifying specific end users or business roles that should have their workstation backed up [L1] [SEP]
- Specifying which files and/or folders should be restored MN.IT Services Responsibility [L1] [SEP]
- Deploying and configuring the necessary backup client to authorized workstations [L1] [SEP]

- Managing and maintaining backup and restore services [L1]
- Restoring files and/or folders as requested [SEP] **Accessories and Peripherals** [L1] An accessory or peripheral is a device connected to a workstation, but not part of it, and is more or less dependent on the workstation for operation. Examples of accessories and peripherals are printers, image scanners, microphones, speakers, monitors, webcams, and digital cameras. [L1] Limits [SEP]
- MN.IT Services does not provide support for accessory or peripheral applications, unless they are deemed “standard” software

Customer Responsibilities

6. Identify the types of accessories and peripherals needed to complete day-to-day business [SEP]
7. When necessary, train end users on how to use the accessory or peripheral [L1] **MN.IT Responsibilities**
- a. Identify and ensure proposed accessories and peripherals solutions meet business requirements [L1]
- b. Procure, deploy and maintain accessories and peripherals required for day-to-day business [L1]

Printers

Depending on an end user’s role within an organization, their feature requirements for printing capabilities will vary. To fulfill the requirements of office-based end users, networked multi-function devices (MDF) are utilized to provide a wide range of features including color and black and white printing, ability to print on different paper sizes, stapling and/or hole-punching. Often these devices include other capabilities such as fax, scanning and copying.

Limits • Support for local (USB) connected printers is limited to initial setup and connection

Customer Responsibilities

- Providing paper in the sizes utilized by the printer and required by the business (e.g., legal, letter, 11x17, etc.) [L1]
- Providing toner/ink for local (USB) connected printers **MN.IT Responsibilities** [L1]

- Maintaining network printer device [SEP]
- Configuring new network printers on the print server [SEP]
- Managing and maintaining the print server [SEP]**Additional External Monitor** [SEP]In some cases, business may decide that specific end users or business roles within the organization should have more than one external monitor. For some end uses, having more than one external monitor can increase productivity. Examples of this include: end uses can dedicate one monitor to critical information or use it compare multiple documents side-by-side. Some of the disadvantages of having more than one external monitor are the additional cost, potential for more distractions (because of the additional windows that can be displayed), and the required desktop space they consume within an office. [SEP]**Limits** [SEP]

- Hardware configurations may limit the number of external monitors that can be physically connected to a workstation

Customer Responsibilities

4. Identify specific end users or business roles that should have additional external monitors [SEP]
5. Approve or reject requests from non-authorized user. [SEP]**MN.IT Responsibilities** [SEP]

- Procure and connect the additional external monitor(s)

File Server

A file server provides a centralized (non-local workstation) location for shared disk access, i.e. shared storage of computer files (such as documents, images, databases, etc.) that can be accessed by the workstations that are attached to the same computer network. File servers provide two types of file shares:

5. Personal – File shares assigned to a specific end user for their sole use [SEP]
6. Shared – File shares assigned to a group or project with permissions granted to several groups or individuals for collaboration [SEP]File Server services provides an organization with an aggregate amount of storage which is equal to 2 Gigabytes (GB) times the number of end users. This aggregate includes storage of all personal and shared file shares. [SEP]

Aggregate example: an organization with 50 end users has 100 Gigabytes (GB) of total storage available across personal and shared file shares. Additional file server storage is available for an additional fee.

Customer Responsibilities

4. Requesting the creation, deletion and modification of personal and shared file shares [SEP]
5. Managing content within personal and shared file shares [SEP] MN.IT Responsibilities [SEP]
4. Managing and maintaining the file server services, including data backup [SEP]
5. Creating, deleting and modifying personal and shared files shares [SEP]**Personal accessories and devices** [SEP] Business organizations can choose whether or not end users should use personal-owned accessories and devices such as a digital cameras and home-based printers. MN.IT Services does not prohibit the use of personal accessories or devices, however these devices are not supported. Furthermore, any software installed to use a personal-owned device will be treated as “unique software” (as identified in this Service Description). [SEP] Limits [SEP]
5. Responsibilities [SEP]
7. Provide guidance to end users if personal-owned equipment should be used, and if so, in what manner [SEP]
8. For devices that store government data, they must meet or exceed any security requirements established by the Enterprise Security Office (ESO) [SEP] **Web Content Filtering** [SEP] Web content filtering (also known as web filtering or web blocking) is commonly used by organizations to prevent computer users from viewing inappropriate web sites or content, or as a pre-emptive security measure to prohibit access of known malware hosts [SEP] Customer Responsibilities [SEP]
 - Identifying workstations that should be exempt from web content filteringMN.IT Responsibilities • Managing and maintaining web content filtering services

Office Moves

From time to time, end users may change office locations. MN.IT Services can assist with disconnecting workstation hardware in the current office location and/or re-connecting it in the new office location.

Limits • May not be available in all office locations, including home offices

Customer Responsibility • Provide notification to MN.IT services to determine if sufficient resources are available

MN.IT Services Responsibility • Assist with disconnecting and/or reconnecting workstation hardware

Professional Services

5. Review business requirements and determine if professional services can be offered [SEP]

6. Provide the professional services description, responsibilities and rate(s) for the proposed service(s) [SEP]

Additional Service Information [SEP]

Planning for Service Changes and Growth

[SEP] Workstation Management is designed and deployed based on the number of laptops/desktop computer deployed within an organization. Additional capacity is built into the initial planning and deployment of services based on common growth scenarios. [SEP] When user growth greater than 5 percent is predicted, the customer is asked to notify the MN.IT Services through the standard change request process to allow appropriate evaluation and planning of service expansion. This notification process applies to increasing the number of total workstations as well as expanding the scope of customer usage scenarios (such as deployment of mobile devices) or introducing new applications that run within the workstation environment. [SEP] Customer Responsibilities [SEP]

7. Provide workstation usage and growth estimates [SEP]
 8. Provide advance notification of any significant user growth or workstation service usage beyond initial estimates [SEP]
- MN.IT Services Responsibilities [SEP]
- Plan capacity based on the customer's sustained growth rate and add infrastructure and workstations as required [SEP]
 - Adjust growth capacity to enable evaluation and planning for necessary service expansion.

Related Information [L] [SEP] **Optional: References to applicable documents such as:**

- Minnesota Statues 207 Chapter 16E (Office of Enterprise Technology) [L] [SEP]
- Enterprise Technology Fund 970 Rate Schedule [L] [SEP]
- Operational documents and information on MN.IT Services website [L] [SEP]
- Workstation Management Service Level Agreement [L] [SEP]

[L]
[SEP]

Network setup and commands

arp	This program lets the user read or modify their arp cache.
dig(1)	Send domain name query packets to name servers for debugging or testing.
finger	Display information about the system users.
ftp	File transfer program.
ifconfig	Configure a network interface.
ifdown	Shutdown a network interface.
ifup	Brings a network interface up. Ex: ifup eth0
ipchains	IP firewall administration used to set input, forward, and output rules.
netconf	A GUI interactive program to let you configure a network on Redhat systems.
netconfig	Another GUI step by step network configuration program.
netstat	Displays information about the systems network connections, including port connections, routing tables, and more. The command "netstar -r" will display the routing table.
nslookup	Used to query DNS servers for information about hosts.
pftp	Same as ftp.
ping	Send ICMP ECHO_REQUEST packets to network hosts.
portmap	DARPA port to RPC program number mapper. Must be running to make RPC calls.
rarp	Manipulate the system's RARP table.
rcp	Remote file copy. Copies files between two machines.
rexec	Remote execution client for an exec server. The host uses the rexecd server.
ripquery	Query RIP gateways. Request all routes known by an RIP gateway by sending an RIP request.
rlogin	Starts a terminal session on a remote host.
route	Show or manipulate the IP routing table.
rsh	Executes command on remote host.
rup	Displays summary of current system status of a remote host or all hosts on the network.
ruptime	Show host status of local machines.
rwhod	System status server, maintains database used by rwho and

	ruptime.
showmount	Show mount information for an NFS server.
tcpd	Access control facility for internet services. Can be set up to monitor requests for Telnet, finger, ftp, exec, rsh, rlogin, tftp, talk, comsat. It filters access for these requests.
tcpdchk	Tcp wrapper configuration checker.
tcpdump	Dump traffic on a network. Prints out headers of packets that match the boolean expression.
tcpdmatch	Predicts how the tcp wrapper will handle a specific request for a service.
Telnet	User interface to the TELNET protocol, setting up a remote console session.
traceroute	Print the route that packets take to the specified network host.
ipx_configure	Tool to setup Netware access.
ncpmount	Netware filesystem mounting program.
nprint	Novell print command.
pqlist	Netware printer list for a given server.
pserver	Netware print server.
slist	Netware server list.

Subject : Computer Networks

Class : B.Sc.(IT) 3rd – Sem

Div. : A

Topic : Network Security

Made by :

**Mansi Donga
Riddhi**

Hinal Biscuitwala

Hinal Chauhan
Bhavini Gamit
Rutvi Kansara

Shweta Gamit

Contents

- Introduction.
- Various types of security.
- Planning a security approach.
- Security problems and their consequences.
- Introduction to firewalls.
- Encryption and decryption standards.
- Secure Socket Layer.

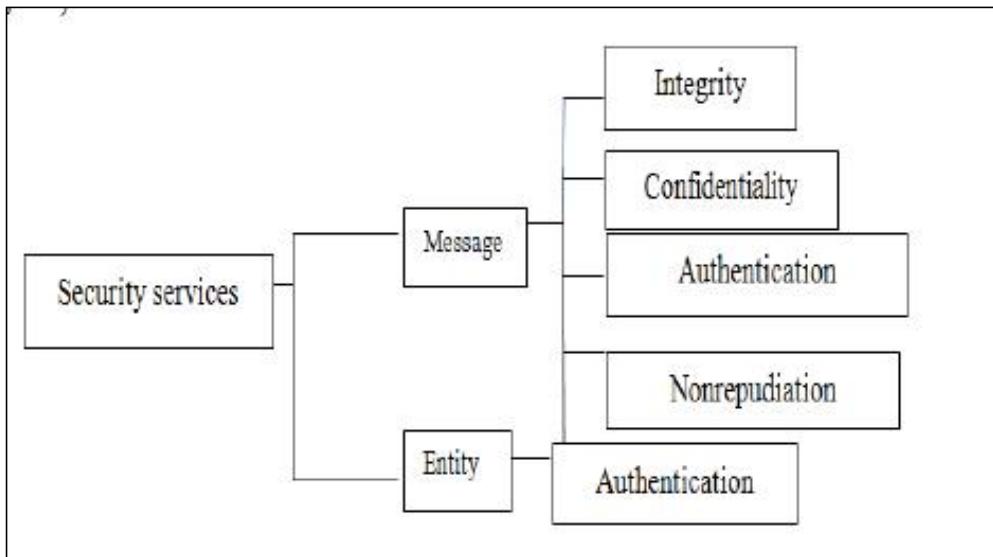
- Virtual Private Network.

5. Network security

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of computer network and network accessible resources.

Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them to access information and programs within their authority.

Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. It secures the network, as well as protecting and overseeing operations being done. Network security problems can be divided roughly into four closely intertwined areas: secrecy, authentication, non-repudiation, and integrity control.



- **Message Confidentiality**

Message confidentiality or privacy means that the sender and the receiver expect confidentiality. The transmitted message must make sense to only the intended receiver. The message must be encrypted at the sender site and decrypted at the receiver site.

- **Message Integrity**

Message integrity means that the data must arrive at the receiver exactly as they were sent. There must be no changes during the transmission, neither accidentally or maliciously. The integrity of the message must be preserved in a secure communication.

- **Message Authentication**

Message authentication is a service beyond message integrity. In message authentication the receiver needs

to be sure of the sender's identity and that an imposter has not sent the message.

- **Message Nonrepudiation**

Message nonrepudiation means that a sender must not be able to deny sending a message that he or she, in fact, did send. The burden of proof falls on the receiver. For example, when a customer sends a message to transfer money from one account to another, the bank must have proof that the customer actually requested this transaction.

- **Entity Authentication**

In entity authentication (or user identification) the entity or user is verified prior to access to the system resources (files, for example). Entity authentication is a technique designed to let one party prove the identity of another party. An entity can be a person, a process, a client, or a server. The entity whose identity needs to be proved is called the claimant; the party that tries to prove the identity of the claimant is called the verifier. For example, a student who needs to access her university resources needs to be authenticated during the logging process. This is to protect the interests of the university and the student.

- **Types of network security**

1. Access Control

Not every user should have access to your network. To keep out potential attackers, you need to recognize each user and each device. Then you can enforce your security policies. You can block non-compliant endpoint devices or give them only limited access. This process is network access control (NAC).

2. Antivirus and antimalware software

“Malware” short for “malicious software”, includes viruses, worms, Trojans, ransomware, and spyware. Sometimes malware will inject a network but lie dormant for days or even weeks. The best antimalware programs not only scan for malware upon entry, but also continuously track files afterward to find anomalies, remove malware, and fix damage.

3. Application security

Any software you can use to run your business needs to be protected, whether your IT staff builds it or whether you buy it. Unfortunately, any application may contain holes, or vulnerabilities, that attacker can use to infiltrate your network. Application security encompasses the hardware, software, and processes you use to close those holes.

4. Behavioural analytics

To detect abnormal behaviour, you must know what normal behaviour looks like. Behavioural analytics tools automatically discern activities that deviate from the norm. Your security team can then better identify indicators of compromise that pose a potential problem and quickly remediate threats.

5. Email security

Email gateways are the number one threats vector for a security breach. Attackers use personal information and social engineering tactics to build sophisticated phishing campaigns to deceive recipients and send them to sites serving up malware. An email security application blocks incoming attacks and controls outbound messages to prevent the loss of sensitive data.

6. Firewalls

A firewall is a device (usually a router or a computer) installed between the internal network of an organization and the rest of the Internet. It is designed to forward some packets and filter (not forward) others. A firewall can be hardware, software, or both. A firewall can be used to deny access to a specific host or a specific service in the organization.

7. Intrusion prevention system

An intrusion prevention system (IPS) scans network traffic to actively block attacks. Cisco Next-Generation IPS (NGIPS) appliances do this by correlating huge amounts of global threat intelligence to not only block malicious activity but also track the progression of suspect files and malware across the network to prevent the spread of outbreaks and reinfection.

8. Mobile device security

Cybercriminals are increasingly targeting mobile devices and apps. Within the next 3 years, 90 percent of IT organization may support corporate applications on personal mobile devices. Of course, you need to control which devices can access your network. You will also need to configure their connections to keep network traffic private.

9. Network segmentation

Software - defined segmentation puts network traffic into different classifications and makes enforcing security policies easier. Ideally, the classifications are based on endpoint identity, not mere IP addresses. You can assign access rights based on role, location, and more so that the right level of access is given to the right people and suspicious devices are contained and remediate.

10. Security information and event management

SIEM products pull together the information that your security staff needs to identify and respond to threats. These products come in various forms, physical and virtual appliances and server software.

11. VPN

A virtual private network encrypts the connection from an endpoint to a network, often over the Internet. Typically, a remote access VPN uses IPSec or Secure Sockets Layer to authenticate the communication between device and network.

12. Wireless security

Wireless networks are not as secure as wired ones. Without stringent security measures, installing a wireless LAN can be like putting Ethernet ports everywhere, including the parking lot. To prevent an exploit from taking hold, you need products specifically designed to protect a wireless network.

13. Web security

A web security solution will control your staff's web use, block web-based threats, and deny access to malicious websites. It will protect your web gateway on site or in the cloud. "Web security" also refers to the steps you take to protect your own website.

Planning a security approach

Secure networking ensures that the network is available to perform its appointed task by protecting it from attacks originating inside and outside the organization.

Traditional thinking equates this to a handful of specific requirements, including user authentication, user device protection and point solutions. Application traffic must be securely delivered across the network, avoiding threats such as theft of intellectual property or private data.

In addition, the underlying infrastructure must be protected against service disruption (in which the network is not available for its intended use) and service theft (in which an unauthorized user accesses network bandwidth or an authorized user accesses unauthorized services).

■ Secure networking layers

Secure networking involves securing the application traffic as it traverses the network. It should encompass these areas:

- **Perimeter security** protects the network applications from outside attack, through technologies such as firewall and intrusion detection.

- **Communications security** provides data confidentiality, integrity and no repudiation, typically through the use of Secure Sockets Layer or IPSec virtual private networks (VPN).
- **Access security** ensures that each user has access to only those network elements and applications required to perform his job.
- **Physical security** protects the network from physical harm or modification, and underlies all security practices. The most obvious forms of physical security include locked doors and alarm systems

■ **Standards for secure networking**

To ensure a consistent set of requirements, lower training costs and speed the introduction of new security capabilities, IT managers should use these 10 security techniques across their networks.

1. Use a layered defence. Employ multiple complementary approaches to security enforcement at various points in the network, therefore removing single points of security failure.
2. Incorporate people and processes in network security planning. Employing effective processes,

such as security policies, security awareness training and policy enforcement, makes your program stronger.

3. Clearly define security zones and user roles. Use firewall, filter and access control capabilities to enforce network access policies between these zones using the least privileged concept.
4. Maintain the integrity of your network, servers and clients. The operating system of every network device and element management system should be hardened against attack by disabling unused services.
5. Control device network admission through endpoint compliance. Account for all user device types --wired and wireless. Don't forget devices such as smart phones and handhelds, which can store significant intellectual property and are easier for employees to misplace or have stolen.
6. Protect the network management information. Ensure that virtual LANs (VLAN) and other security mechanisms (IPSec, SNMPv3, SSH, TLS) are used to protect network devices and element management systems so only authorized personnel have access. Establish a backup process for device configurations, and implement a change management process for tracking.
7. Protect user information. WLAN/Wi-Fi or Wireless Mesh communications should use VPNs or 802.11i with Temporal Key Integrity Protocol for security

purposes. VLANs should separate traffic between departments within the same network and separate regular users from guests.

8. Gain awareness of your network traffic, threats and vulnerabilities for each security zone, presuming both internal and external threats.
9. Use security tools to protect from threats and guarantee performance of critical applications.
10. Log, correlate and manage security and audit event information. Aggregate and standardize security event information to provide a high-level consolidated view of security events on your network. This allows correlation of distributed attacks and a network wide awareness of security status and threat activity.

Security problems and their consequences

The need of security in any network is apparent. The desire for authentication has been the main focus of many administrators. Malware infections cause a number of problems. Machines become unresponsive or sluggish resulting in users becoming frustrated and administrators spending precious time trying to find the problem. When a machine is infected, some administrators often want to simply re-install the operating system, however a responsible system administrator or security analyst would want to investigate and assess the situation before doing anything else. All of these tasks take time and

resources. People have to stop working; the hardware has to be replaced and so on.

■ External and internal threats

Computer network security problems should be given thought during the planning phase of nay network, be it a huge organizational LAN or a small home network. All kinds of computer networks face different types of security problems.

Threats to any computer network arise from both external and internal entities. External threats include unauthorized access by outsiders such as hackers, virus attack etc. Among internal threats is exploitation of network by its users – knowingly or unknowingly. Internal threats arise due to malicious intentions and/or ignorance of the users of your computer network. Example of internal threat can be a person downloading something from internet that results in a malware attack.

Viruses, worms, Trojan horses can corrupt data on user's computer, infect other computers, weaken computer security, or provide back doors into protected networked computers. Although seemingly less dangerous than viruses that can corrupt digital content on a user's computer, spyware, adware and other forms of security risk also represent a significant problem to small businesses, their users, and the company networks.

All types of threats and security risks can seriously impair business operations, network use, and computer

performance while performing many tasks unknown to the user of an infected computer.

■ Security Risks

- Not all security breaches result from manipulation of network technology
 - Staff members purposely or inadvertently reveal passwords.
 - Undeveloped security policies.
- Malicious and determined intruders may “cascade” their techniques.
- Human errors, ignorance, and omissions cause majority of security breaches.
- Risks associated with people:
 - Social engineering or snooping to obtain passwords.
 - Incorrectly creating or configuring user IDs, groups, and their associated rights on file server.
 - Overlooking security flaws in topology or hardware configuration.

- Overlooking security flaws in OS or application configuration.
- Lack of documentation and communication.
- Risks inherent in network hardware and design:
 - Transmissions can be intercepted.
 - Networks using leased public lines vulnerable to eavesdropping.
 - Network hubs broadcast traffic over entire segment.
 - Unused hub, router, or server ports can be exploited and accessed by hackers.
 - Not properly configuring routers to mask internal subnets.

■ **Solutions to this security problems**

First of all you need to plan to assess the vulnerabilities of your network. A vulnerability assessment plan should cover the key areas that, if affected, can bring down the network or create huge data loss. These items include

1. Server protection (the main computer in case of peer to peer network),
2. Firewalls and antivirus on the server,

- 3.** The method your server employs to communicate with other computers, and
- 4.** How other peripherals on the network (computers, printers, etc.) can pose a danger to network.

Introduction to firewalls

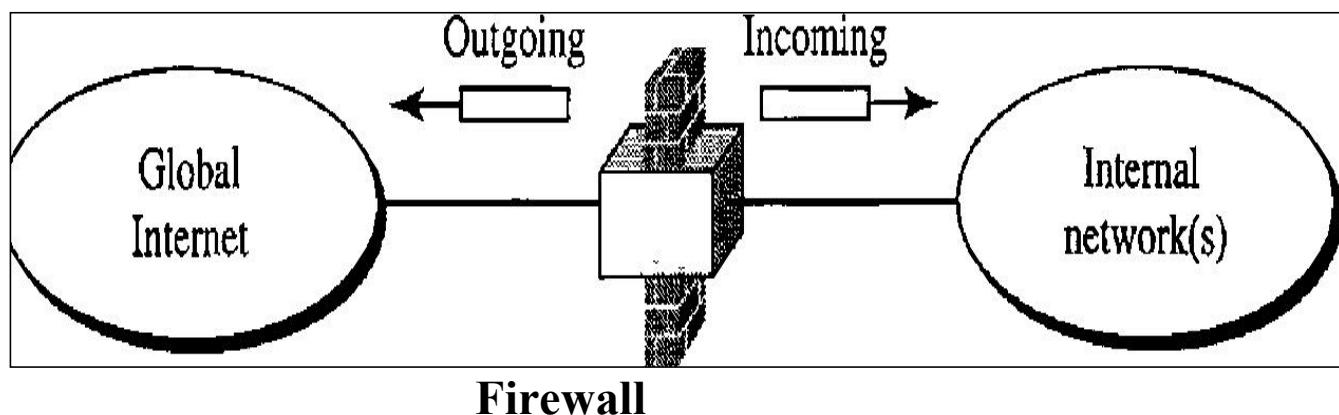
Firewalls are network devices that enforce an organization's security policy. Since their development, various methods have been used to implement firewalls. These methods filter network traffic at one or more of the seven layers of the ISO network model, most commonly at the application, transport, network, and data-link levels. Newer methods, which have not yet been widely adopted, include protocol normalization and distributed firewalls. Firewalls involve more than the technology to implement them. Specifying a set of filtering rules, known as a policy, is typically complicated and error-prone.

High-level languages have been developed to simplify the task of correctly defining a firewall's policy. Once a policy has been specified, testing is required to determine if the firewall correctly implements the policy. Because some data must be able to pass in and out of a firewall, in order for the protected network to be useful, not all attacks can be stopped by firewalls. Some emerging technologies, such as Virtual Private Networks (VPN) and peer-to-peer networking pose new challenges for existing firewall technology.

- **The Need for Firewalls**

National firewalls (attempt to) limit the activities of their users on the Internet. They are one part of an overall security policy; they enforce the rules about which network traffic is allowed to enter or leave a network. These policies restrict the use of certain applications, restrict which remote machines may be contacted, and/or limit the bandwidth.

A firewall is a device (usually a router or a computer) installed between the internal network of an organization and the rest of the Internet. It is designed to forward some packets and filter (not forward) others.



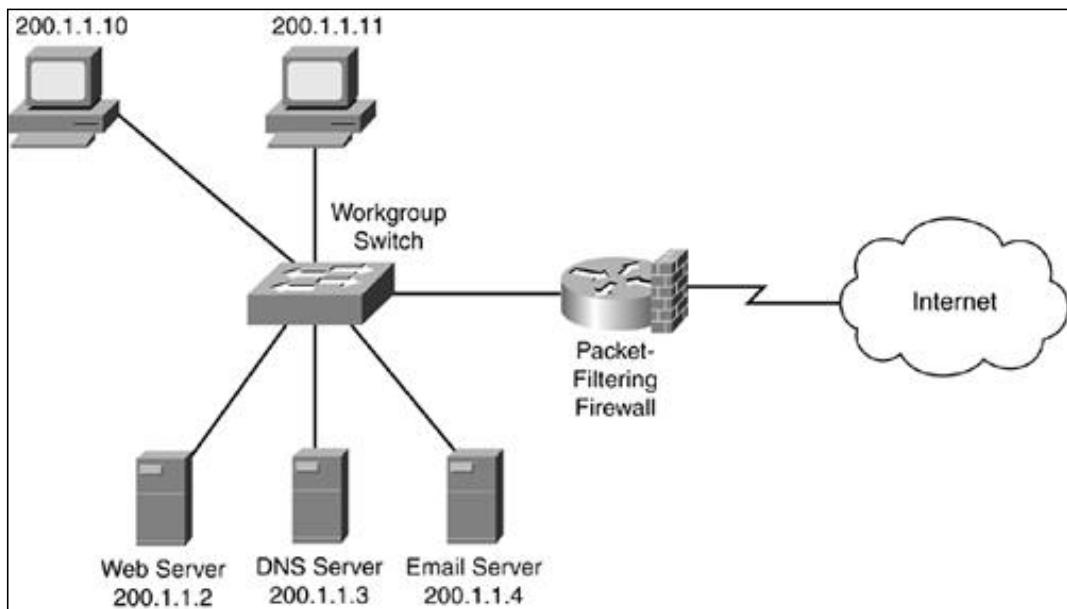
A firewall may filter all incoming packets destined for a specific host or a specific server such as HTTP. A firewall can be used to deny access to a specific host or a specific service in the organization. A firewall is usually

classified as a packet-filter firewall or a proxy-based firewall.

- **Packet-Filter Firewall**

Packet filtering is a firewall technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols and ports. It can forward or block packets based on the information in the network layer and transport layer headers: source and destination IP addresses, source and destination port addresses, and type of protocol (TCP or UDP). A packet-filter firewall is a router that uses a filtering table to decide which packets must be discarded (not forwarded). A packet filter firewall filters at the network or transport layer.

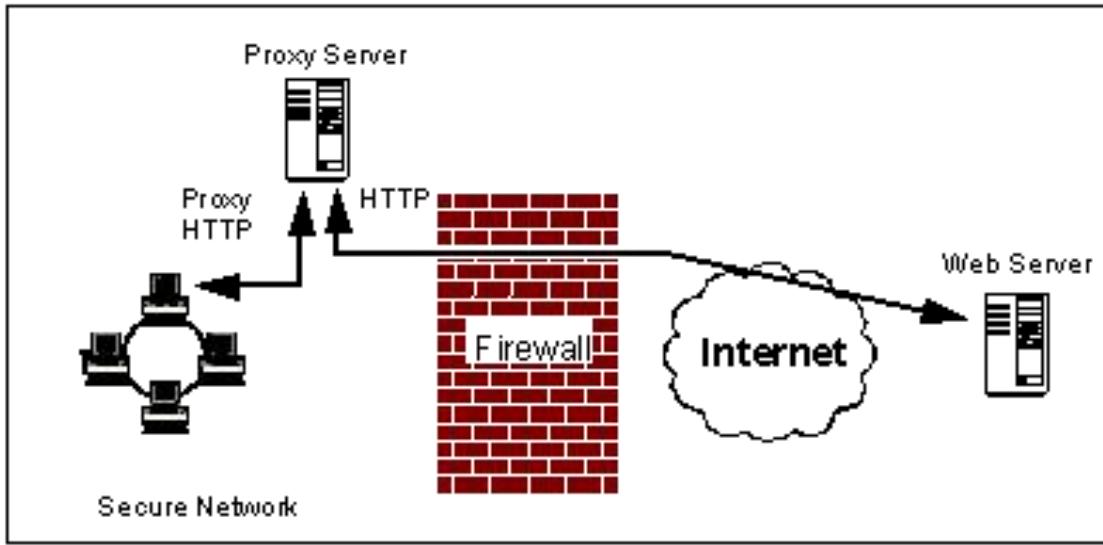
Packet filtering checks source and destination IP addresses. If both IP addresses match, the packet is considered secure and verified. Because the sender may use different applications and programs, packet filtering also checks source and destination protocols, such as User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). Packet filters also verify source and destination port addresses.



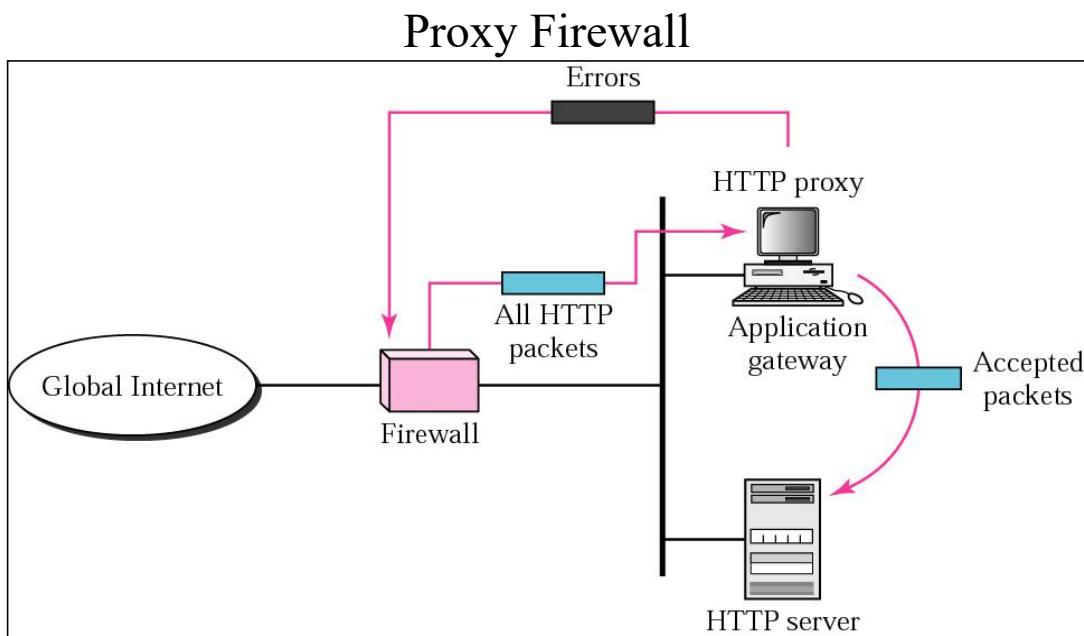
Packet-Filter Firewall

- **Proxy Firewall**

Sometimes we need to filter a message based on the information available in the message itself (at the application layer). As an example, assume that an organization wants to implement the following policies regarding its Web pages: Only those Internet users who have previously established business relations with the company can have access; access to other users must be blocked. In this case, a packet-filter firewall is not feasible because it cannot distinguish between different packets arriving at TCP port 80 (HTTP). Testing must be done at the application level (using URLs). One solution is to install a proxy computer (sometimes called an application gateway), which stands between the customer (user client) computer and the corporation computer.

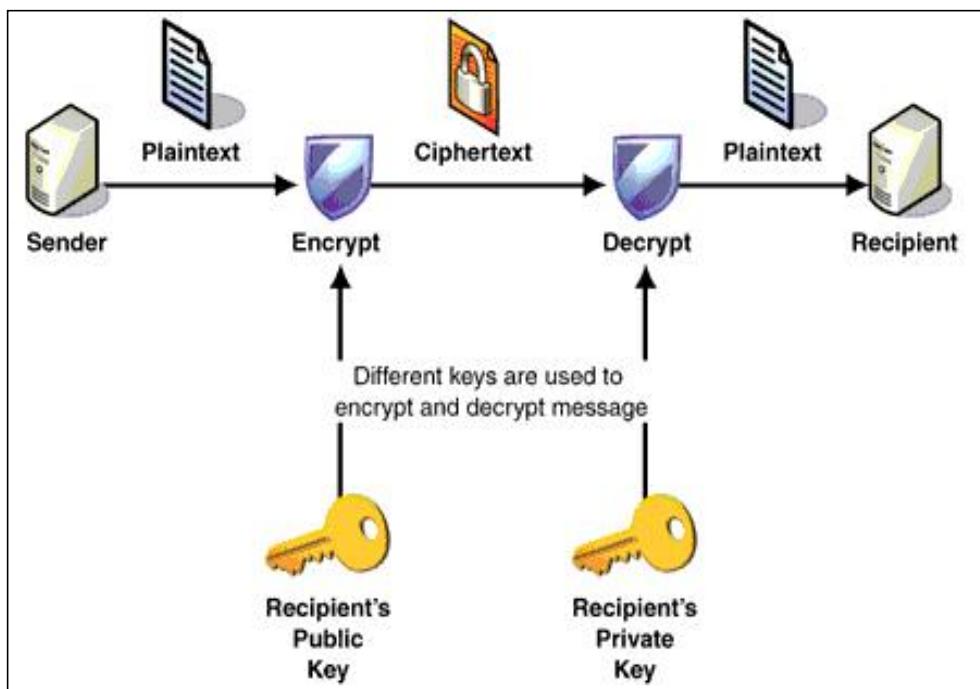


When the user client process sends a message, the proxy firewall runs a server process to receive the request. The server opens the packet at the application level and finds out if the request is legitimate. If it is, the server acts as a client process and sends the message to the real server in the corporation. If it is not, the message is dropped and an error message is sent to the external user. In this way, the requests of the external users are filtered based on the contents at the application layer.



Encryption and decryption standards

Encryption and decryption are the heart of the SSL security algorithm in which information traverse between browser and server is converted into complex text which is called encryption of data. And at the receiver side, the complex text again converted into original information which is called decryption of data.



Encryption is a cipher text that is hard to decode and the data sender and receiver can only encrypt the information. To recover the content of an encrypted text, there should have a correct algorithm key. The more compound the encryption algorithm, the harder it turns to eavesdrop on the communications. Encryption can be applied to keep

the intruder away from getting the content of the transmitted data.

To decrypt the encryption, a data receiver needs decryption key. Encryption keys are of two types:

Symmetric encryption and **Public key encryption**.

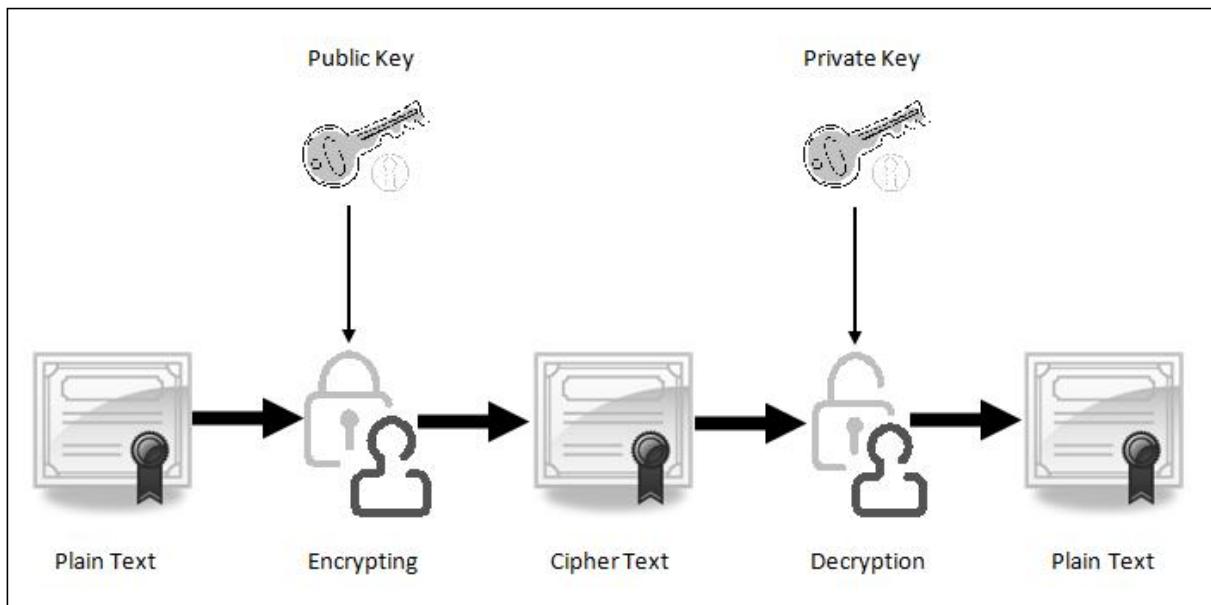
Symmetric encryption carries the same two keys being used for communication while in public key encryption; the key is distributed publicly for anyone to encrypt the message. Only the receiver has the access to the decryption key.

Encryption is used in securing data transition done through networks, wireless microphones, mobile, wireless intercom, Bluetooth device, automatic teller machine. Encryption is extremely important where data like credit card or debit card information is transferred between the user's browser and the website server. To make your data stronger and encrypted, a person or organization has to take a legitimate SSL certificate from a reputed certificate authority.

Private Key and public key are a part of encryption that encodes the information. Both keys work in two encryption systems called symmetric and asymmetric. Symmetric encryption (private-key encryption or secret-key encryption) utilize the same key for encryption and decryption.

Asymmetric encryption utilizes a pair of keys like public and private key for better security where a message sender encrypts the message with the public key and the

receiver decrypts it with his/her private key. Public and Private key pair helps to encrypt information that ensures data is protected during transmission.



Public and Private Key - SSL Encryption

- **Public Key:**

Public key uses asymmetric algorithms that convert messages into an unreadable format. A person who has a public key can encrypt the message intended for a specific receiver. The receiver with the private key can only decode the message, which is encrypted by the public key. The key is available via the public accessible directory.

- **Private Key:**

The **private key** is a secret key that is used to decrypt the message and the party knows it that exchange message. In the traditional method, a secret key is shared within communicators to enable encryption and decryption the message, but if the key is lost, the system becomes void.

To avoid this weakness, PKI (public key infrastructure) came into force where a public key is used along with the private key. PKI enables internet users to exchange information in a secure way with the use of a public and private key.

Secure Socket Layer

Secure Socket Layer (SSL) is designed to provide security and compression services to data generated from the application layer.

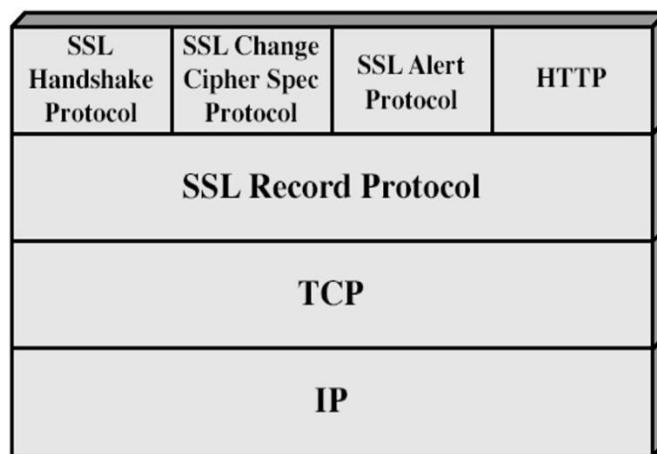
Typically, SSL can receive data from any application layer protocol, but usually the protocol is HTTP. The data received from the application are compressed (optional), signed, and encrypted. The data are then passed to a reliable transport layer protocol such as TCP.

It is designed to make use of TCP to provide a reliable end-to-end secure service. SSL is not a single protocol but rather two layers of protocols as illustrated in figure. It can be seen that one layer makes use of TCP directly. This layer is known as the SSL Record Protocol and it provides basic security services to various higher layer protocols. An independent protocol that makes use of the

record protocol is the Hypertext Markup Language (HTTP) protocol.

Another three higher level protocols that also make use of this layer are part of the SSL stack. They are used in the management of SSL exchanges and are as follows:

1. Handshake Protocol.
2. Change Cipher Spec Protocol.
3. Alert Protocol.



The SSL record protocol, which is at a lower layer and offers services to these three higher level protocols, is discussed first.

- **SSL Record Protocol**

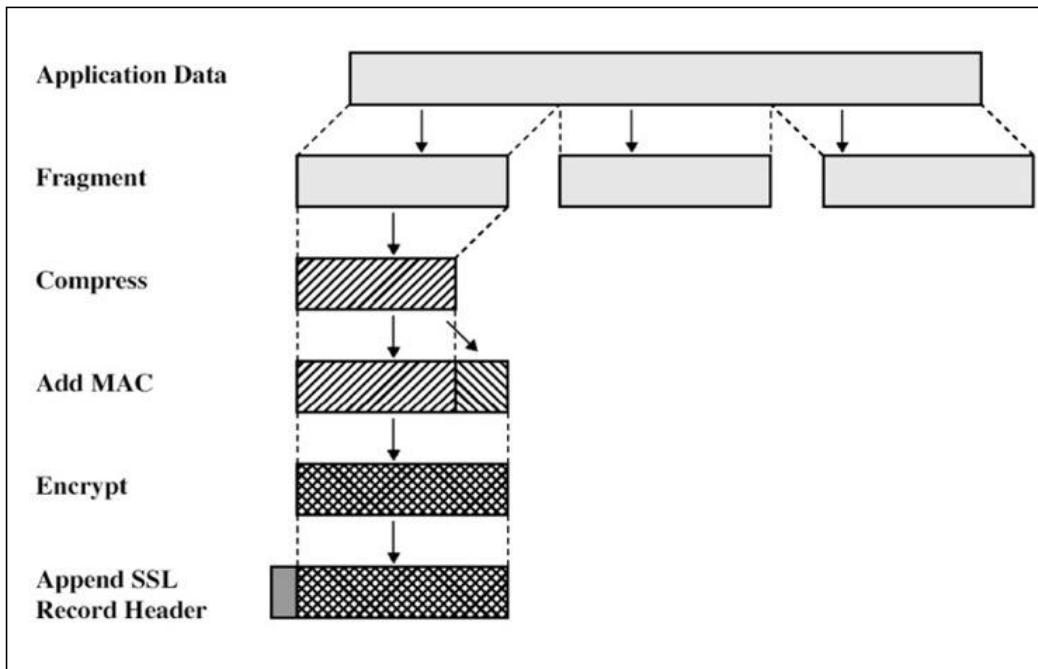
This protocol provides two services for SSL connections:

1. Confidentiality - using conventional encryption.
2. Message Integrity - using a Message Authentication Code (MAC).

In order to operate on data the protocol performs the

following actions.

- It takes an application message to be transmitted and fragments it into manageable blocks.
- These blocks are then optionally compressed which must be lossless and may not increase the content length by more than 1024 bytes.
- A message authentication code is then computed over the compressed data using a shared secret key. This is then appended to the compressed (or plaintext) block.
- The compressed message plus MAC are then encrypted using symmetric encryption. Encryption may not increase the content length by more than 1024 bytes, so that the total length may not exceed $214 + 2048$.
- The final step is to prepend a header, consisting of the following fields:

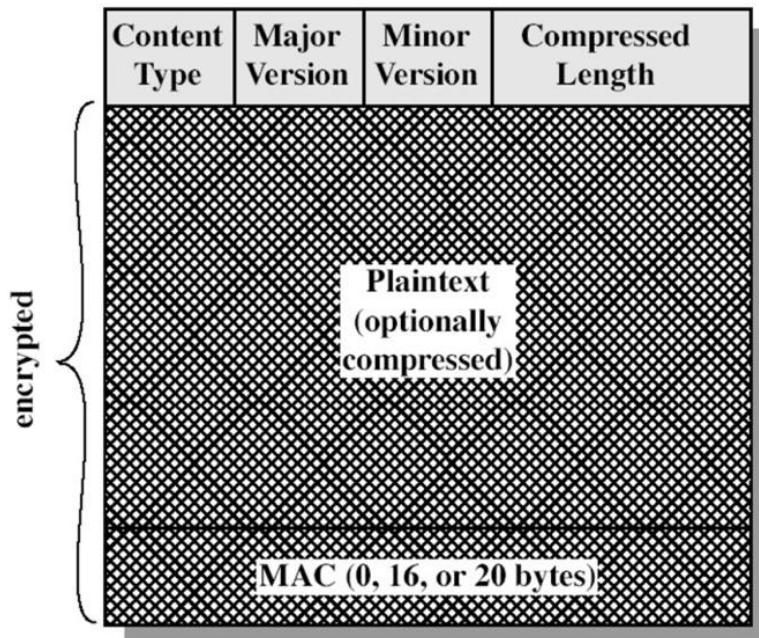


- **Change Cipher Spec Protocol**

This consists of a single message which consists of a single byte with the value 1. This is used to cause the pending state to be copied into the current state which updates the cipher suite to be used on this connection.

- **Alert Protocol**

This protocol is used to convey SSL-related alerts to the peer entity. It consists of two bytes the first of which takes the values 1 (warning) or 2 (fatal). If the level is fatal SSL immediately terminates the connection.



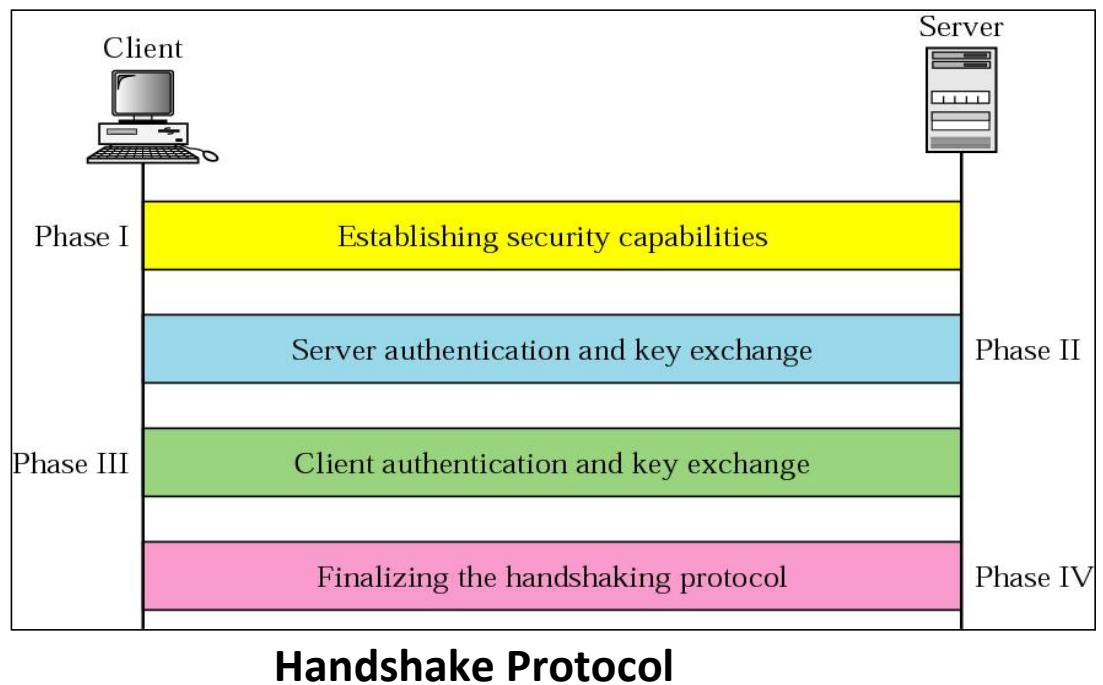
- **Handshake Protocol**

This is the most complex part of SSL and allows the server and client to authenticate each other and to negotiate an encryption and MAC algorithm and cryptographic keys to be used to protect data sent in an SSL record. The Handshake Protocol uses messages to negotiate the cipher suite, to authenticate the server to the client and the client to the server (if needed), and to exchange information for building the cryptographic secrets.

This protocol is used before any application data is sent. It consists of a series of messages exchanged by the client and server. Each message has three fields:

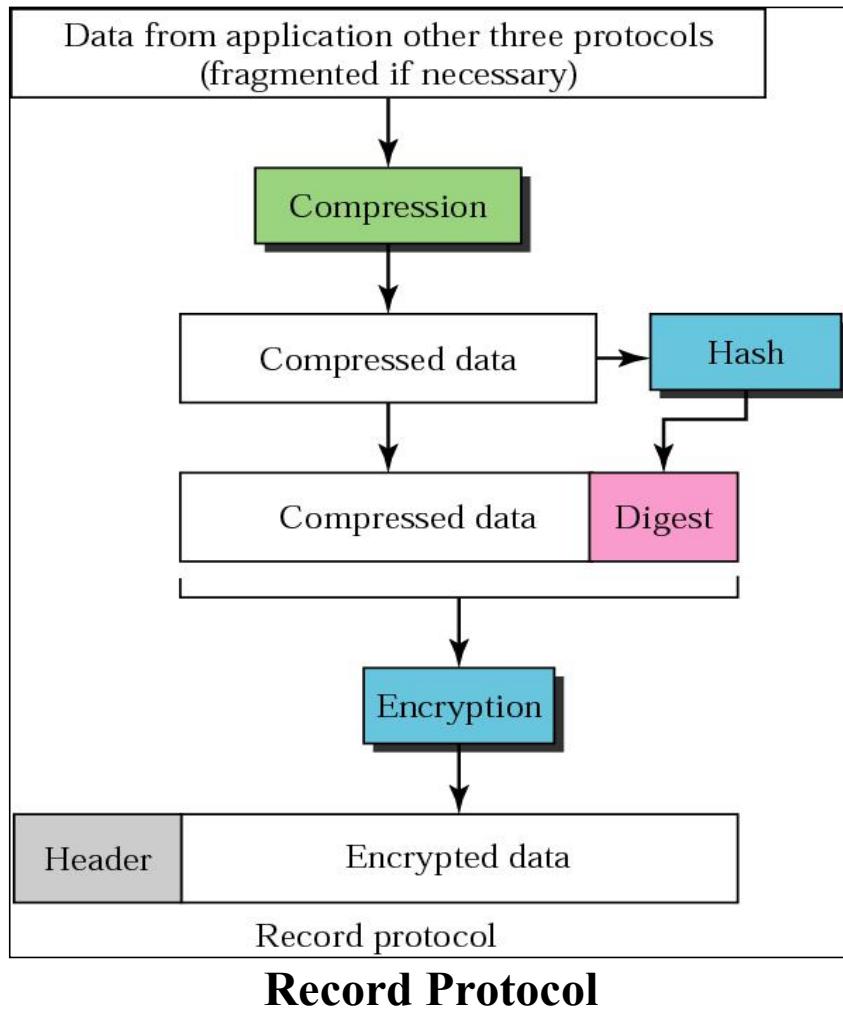
1. Type (1 byte): Indicates one of 10 messages such as “hello request”.

2. Length (3 bytes): The length of the message in bytes.
3. Content (0 byte): The parameters associated with this message such version of SSL being used.



- **Record Protocol**

The **Record Protocol** carries messages from the upper layer (Handshake Protocol, Change Cipher Spec Protocol, Alert Protocol, or application layer). The message is fragmented and optionally compressed; a MAC is added to the compressed message by using the negotiated hash algorithm. The compressed fragment and the MAC are encrypted by using the negotiated encryption algorithm. Finally, the SSL header is added to the encrypted message. The process at the receiver is reversed.



Record Protocol

Virtual Private Networks

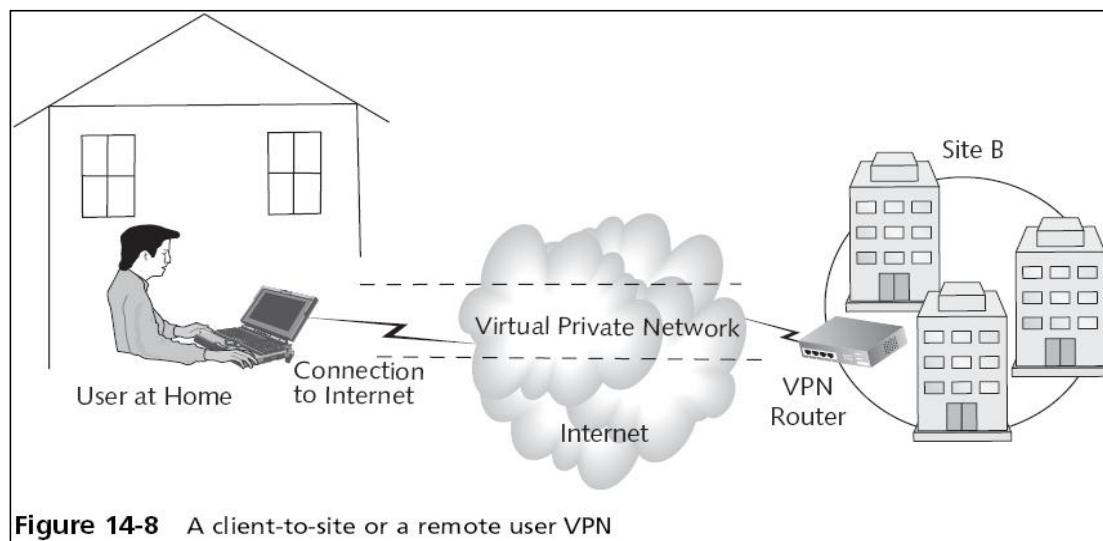
Virtual Private Networks (VPNs) is a popular technology for creating a connection between an external computer and a corporate site over the Internet. It is a technology that is gaining popularity among large organizations that use the global Internet for both intra- and inter-organization communication, but require privacy in their internal communications. It is a technology that creates a safe and encrypted connection over a less secure network, such as Internet.

VPN technology was developed as a way to allow remote users and branch offices to securely access corporate applications and other resources. To ensure safety, data travels through secure tunnels and VPN users must use authentication methods – including passwords, tokens, and other unique identification methods – to gain access to the VPN. To establish a VPN connection, you need VPN-capable components.

VPN creates a network that is private but virtual. It is private because it guarantees privacy inside the organization. It is virtual because it does not use real private WANs; the network is physically public but virtually private.

- **Client-to-site VPN** (also known as remote user VPN)

A VPN that allows designated users to have access to the corporate network from remote locations.



- **Site-to-site VPN**

A VPN that allows multiple corporate sites to be connected over low-cost Internet connections. It uses gateway device to connect the entire network in one location to the network in another – usually a small branch connecting to a data centre. End-node devices in the remote location do not need VPN clients because gateway handles the connection.

You can choose from several tunnelling protocols to create secure, end-to-end tunnels

- Point-to-Point Tunnelling Protocol (PPTP)
- Layer 2 Tunnelling Protocol (L2TP)
- Generic Routing Encapsulation (GRE)
- Using ISDN, Frame Relay or ATM
- Designed to replace a WAN

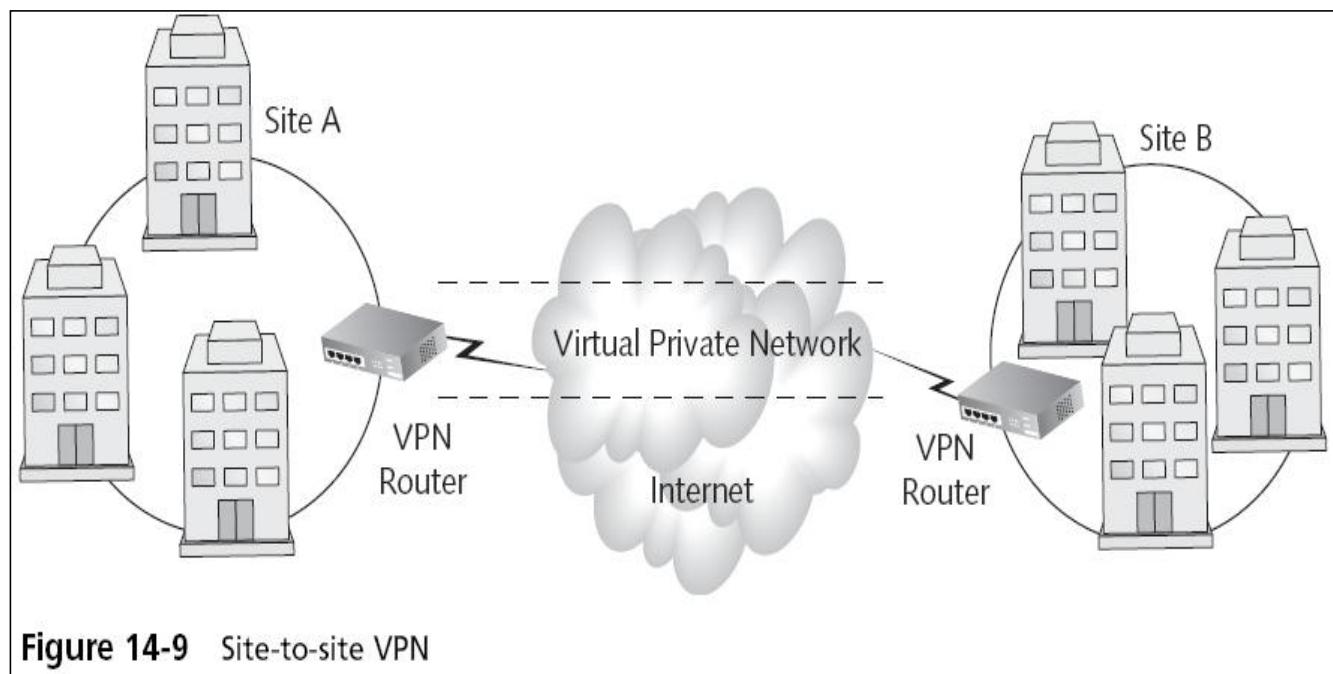


Figure 14-9 Site-to-site VPN

A virtual network overlaid on top of the ubiquitous interconnection of the Internet and a private network for confidential communications and exclusive usage. In a virtual private network (VPN), "virtual" implies that

there is no physical network infrastructure dedicated to the private network. Instead, a single physical network infrastructure is shared among various logical networks.

In VPNs, various networking technologies are applied toward the goal of providing private communications within the public Internet infrastructure. Separate private networking solutions are expensive and cannot be updated quickly to adapt to changes in business requirements. The Internet is inexpensive but does not by itself ensure privacy.

VPN Technology

VPN technology uses IPSec in the tunnel mode to provide authentication, integrity, and privacy. Tunnelling To guarantee privacy and other security measures for an organization, VPN can use the IPSec in the tunnel mode. In this mode, each IP datagram destined for private use in the organization is encapsulated in another datagram. To use IPSec in tunnelling, the VPNs need to use two sets of addressing, as shown in Figure

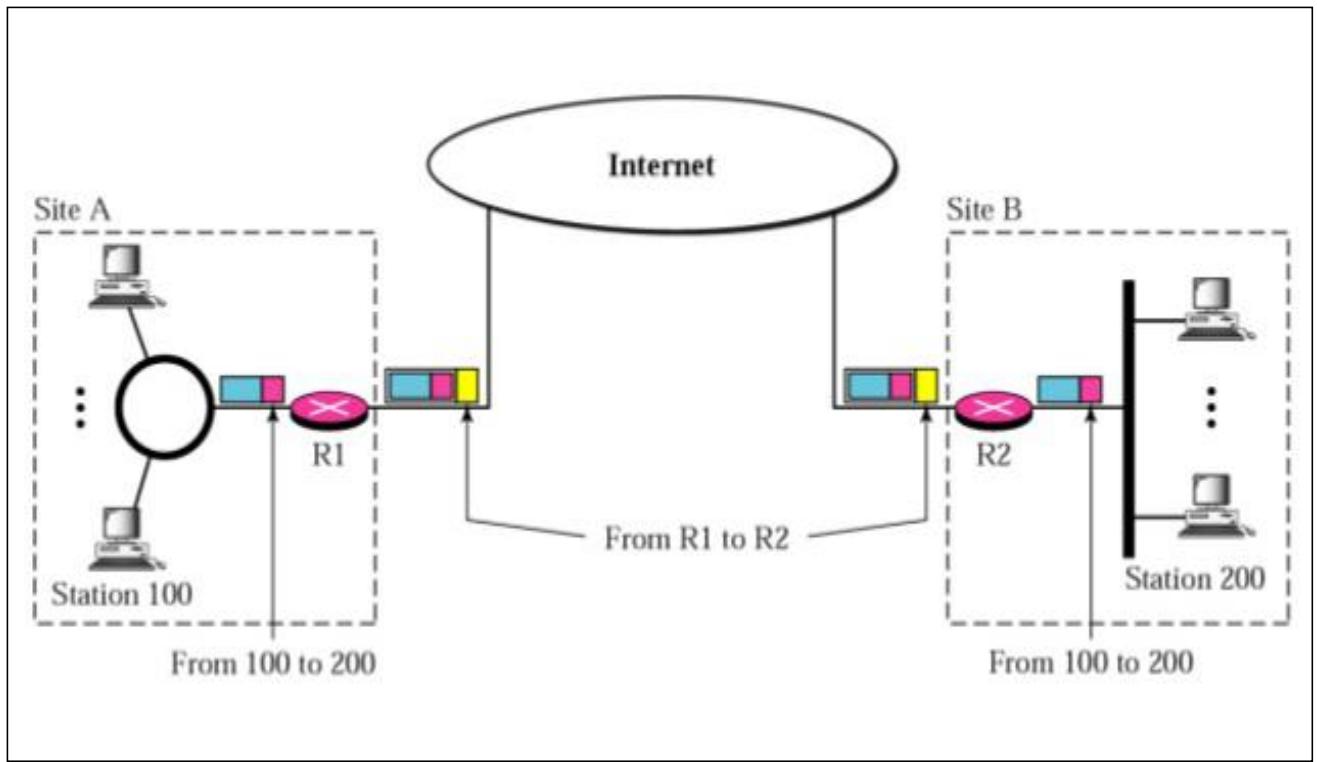


Fig. Addressing in a VPN

The public network (Internet) is responsible for carrying the packet from R1 to R2. Outsiders cannot decipher the contents of the packet or the source and destination addresses. Deciphering takes place at R2, that finds the destination address of the packet and delivers it.

Reference

- Data Communications and Networking (by Behrouz A. Forouzan)
- Computer Networks (by Andrew S. Tanenbaum and David J. Wetherall)
- www.google.com
- www.tutorialspoint.com
- www.techopedia.com