Dr. D. Y. Patil Pratishthan's

Institute of Advanced Computing & Software Development

IACSD

Data Communication & Networking

Table of Contents

Basics Of Networking ………………………………….. ………………………1

Layers of OSI Model ……………………………………………………………….13

TCP/IP Model ……………………………………………………………………...21

INTERNET PROTOCOL ……………………………………………………………25

Network Devices ……………………………………………………………………32

Information Security…………………………………………………………………39

Basics Of Networking

Today computer networks are everywhere.You will find them in homes, offices, factories, hospitals leisure centres etc.But how are they created? What technologies do they use?
In this tutorial you will learn the basic networking technologies, terms and concepts used in all types of networks both wired and wireless, home and office.

Home and Office Networks

- The network you have at home uses the same networking technologies, protocols and services that are used in large corporate networks and on the Internet.
- The only real difference between an home network and a large corporate network is the size.
- A home network will have between 1 and 20 devices and a corporate network will have many thousands.

Networking Types and Structures

Networks can be **wired** or **wireless** with most networks being a mixture of both.

Wired vs Wireless Networks

- Early (pre 2008) networks were predominately wired.
- Today however most networks will use a mixture of wired and wireless network.
- Wired networks use Ethernet as the data link protocol.
- This is unlikely to change with the IOT, as IOT devices will be predominantly wireless.

Wired Networks- Advantages and Disadvantages

Wired networks have the following advantages/disadvantages:

Advantages:

- Ethernet ports are found on almost all laptops/PCs and netbooks even on those 8 years old.

- Wired networks are faster than Wireless. Data rates were periodically increased from the original 10 megabits per second, to 1gigabits per second. Most home networks use 10-100Mbps.
- More secure than Wireless

Disadvantages

- Need to Use cable which can be unsightly, difficult to run and expensive.
- Can't be used easily between buildings (planning etc).
- **Note** a new technology that uses mains cable overcomes many of these disadvantages. powerline networking is common on home/small office networks
- **Not supported on Mobile phones and tablets**.

Wireless Networks – Advantages and Disadvantages

Wireless networks use Wi-fi as the data link protocol. However other wireless options are being developed for the IOT (Internet of things).

Wireless Networks have the following advantages/disadvantages:

Advantages

- Generally easier to set up.
- Can be used both on home and public networks
- No cables required.
- Can be used with mobile phones and tablets.

Wireless Networks Disadvantages

- Generally Slower than wired networks.
- Limited by range.
- Open to eavesdropping.
- Not as secure depending on set up.

Networking Topologies and Layout

There are many different ways network nodes can be connected together.

This isn't normally a consideration in small networks but has networks get larger it becomes more important.

There are many different ways network nodes can be connected together.

Common connection technologies like Wi-Fi, Bluetooth etc are designed to work using a particular network topology.

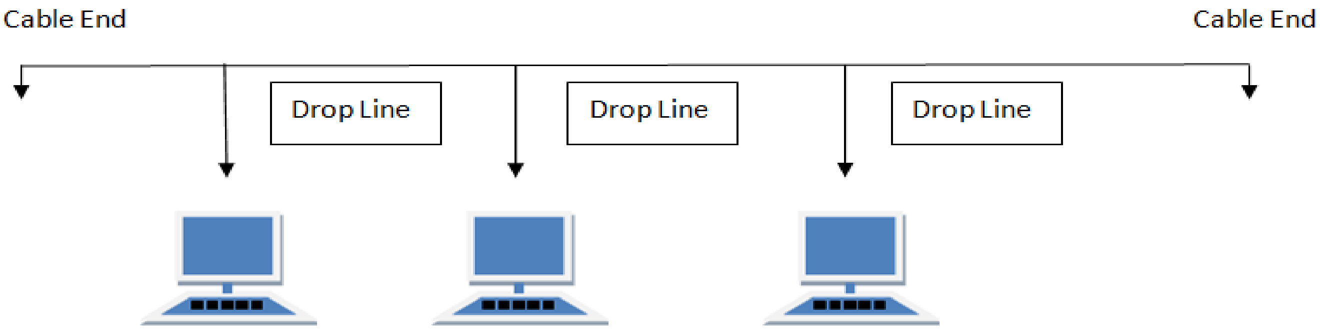
When designing networks and choosing connection protocols having an understanding of these topologies is important.

Common are:

- Bus
- Ring
- Mesh
- Star
- Hybrid

BUS Topology

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.



Features of Bus Topology

1. It transmits data only in one direction.
2. Every device is connected to a single cable

Advantages of Bus Topology

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

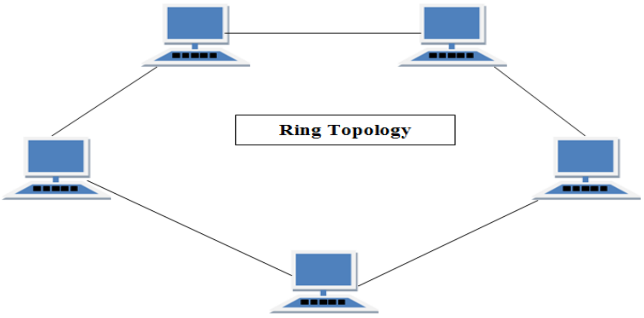
4. It is easy to understand.
5. Easy to expand joining two cables together.

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.

RING Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.



Features of Ring Topology

1. A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
2. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.
3. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
4. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

Advantages of Ring Topology

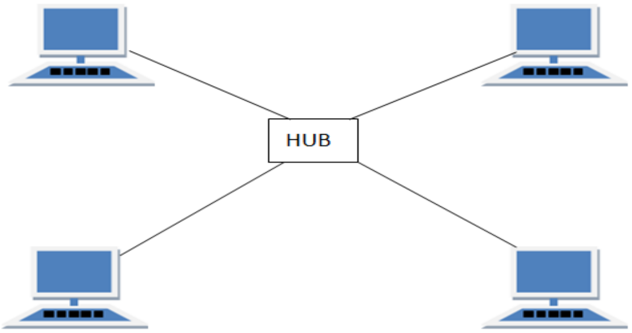
1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

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.

STAR Topology

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.



Features of Star Topology

1. Every node has its own dedicated connection to the hub.
2. Hub acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fibre or coaxial cable.

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.
5. Only that node is affected which has failed, rest of the nodes can work smoothly.

Disadvantages of Star Topology

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

MESH Topology

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has n(n-1)/2 physical channels to link n devices.

There are two techniques to transmit data over the Mesh topology, they are :

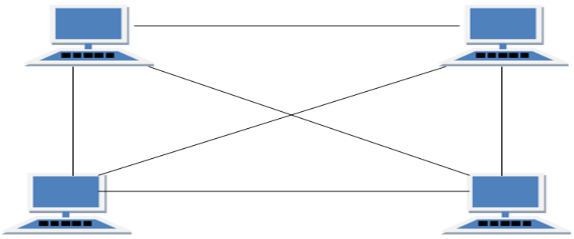
1. Routing
2. Flooding

MESH Topology: Routing

In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those node etc. We can even have routing logic, to re-configure the failed nodes.

MESH Topology: Flooding

In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and the its very unlikely to lose the data. But it leads to unwanted load over the network.



Types of Mesh Topology

1. **Partial Mesh Topology :** In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
2. **Full Mesh Topology :** Each and every nodes or devices are connected to each other.

Features of Mesh Topology

1. Fully connected.
2. Robust.
3. Not flexible.

Advantages of Mesh Topology

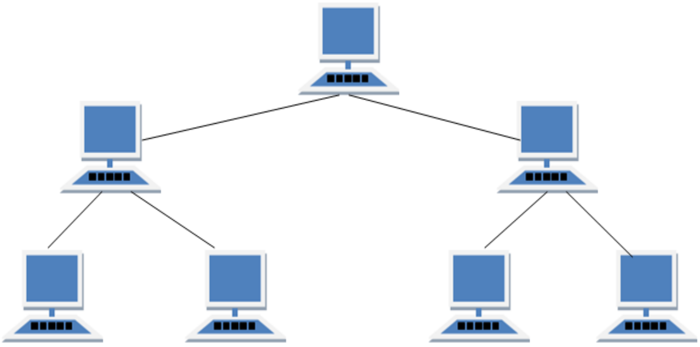
1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

Disadvantages of Mesh Topology

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

TREE Topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.



Features of Tree Topology

1. Ideal if workstations are located in groups.
2. Used in Wide Area Network.

Advantages of Tree Topology

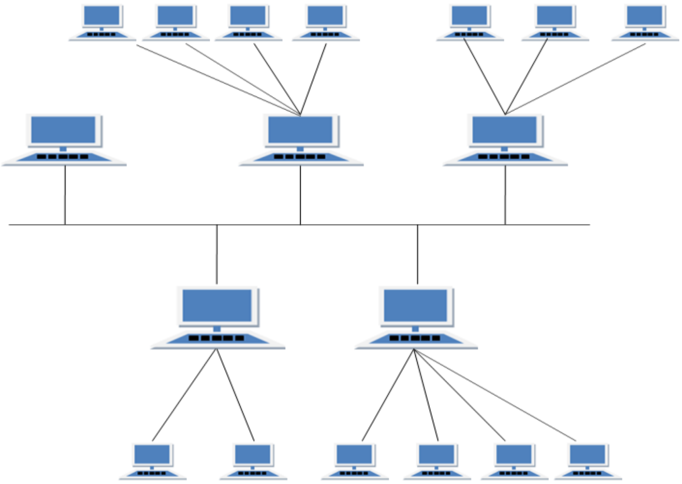
1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.
3. Easily managed and maintained.
4. Error detection is easily done.

Disadvantages of Tree Topology

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

HYBRID Topology

It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).



Features of Hybrid Topology

1. It is a combination of two or topologies
2. Inherits the advantages and disadvantages of the topologies included

Advantages of Hybrid Topology

1. Reliable as Error detecting and trouble shooting is easy.
2. Effective.
3. Scalable as size can be increased easily.
4. Flexible.

Disadvantages of Hybrid Topology

1. Complex in design.
2. Costly.

Early Ethernet networks used a bus structure, modern Ethernet networks and Wi-Fi Networks. use a **star bus** (hybrid) structure.

However both Wi-Fi and bluetooth are being upgraded to support mesh networking.

Networking Topology- Physical vs Logical

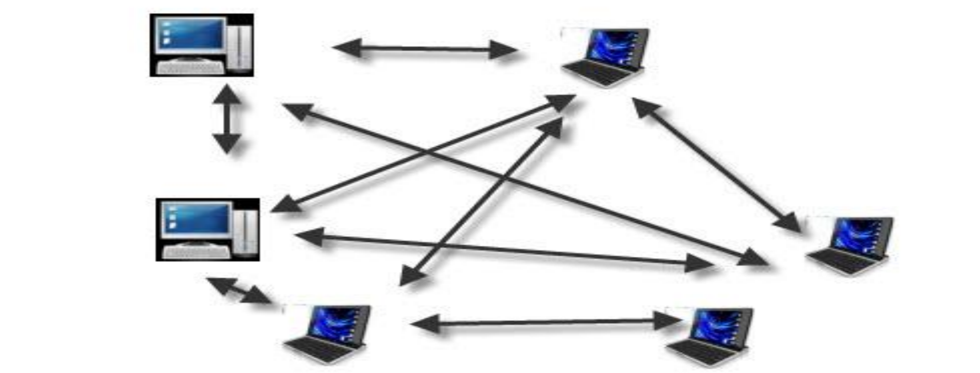
- How the nodes on a network communicate with each other can be very different to how they are physically interconnected.
- Most Home and small office networks use a **physical bus topology.**
- Common **logical typologies** are **Peer to Peer** and **Client Server**.
- The web (WWW) is a **client server network** at the logical level.

Peer to Peer and Client Server Networking

Peer to Peer

- In a **peer to peer** network all nodes are equal and any node can talk to any other node.
- No node has any special role. This was the original networking model of windows networking. (windows for Workgroups)

Peer To Peer Networking Model



Any node can exchange data with any other node.
Each node is a client and a sever

Advantages and Disadvantages

Advantages:

- Easier to setup
- Not dependent on a single node

- More resilient
- Better distribution of network traffic
- No central administrator required
- Less expensive hardware required

Disadvantages:

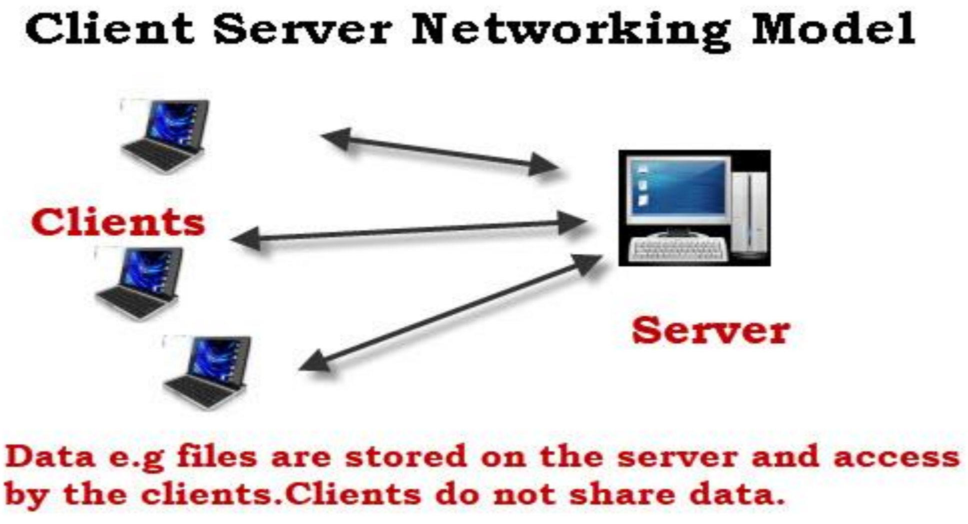
- Less secure and more difficult to secure
- More difficult to administer
- More difficult to backup
- More difficult to locate information.

A Modern example of **Peer to Peer** networking is **BitTorrent.**

Although this networking model isn't currently popular it could become more popular with the Internet of things (IOT).

Client Server

- In a **Client Server** network a server has a special role e.g **file server**, **domain controller**, **web server** etc.
- A client connects to a server to use the appropriate services.
- This is the networking model **used on the web** and the Internet and on modern large Windows networks.


Client Server Networking Model
Clients
Server
Data e.g files are stored on the server and access by the clients.Clients do not share data.

Advantages and Disadvantages

Advantages:

- Easy to find resources as they are on a dedicated node i.e. A server
- Easy to secure
- Easy to administer
- Easy to backup

Disadvantages:

- Servers are a single point of failure
- Expensive hardware required
- Network traffic get concentrated

A Modern example of Client Server networking is **the Web. Facebook,Twitter,Google search** and many other web services use this networking model**.**

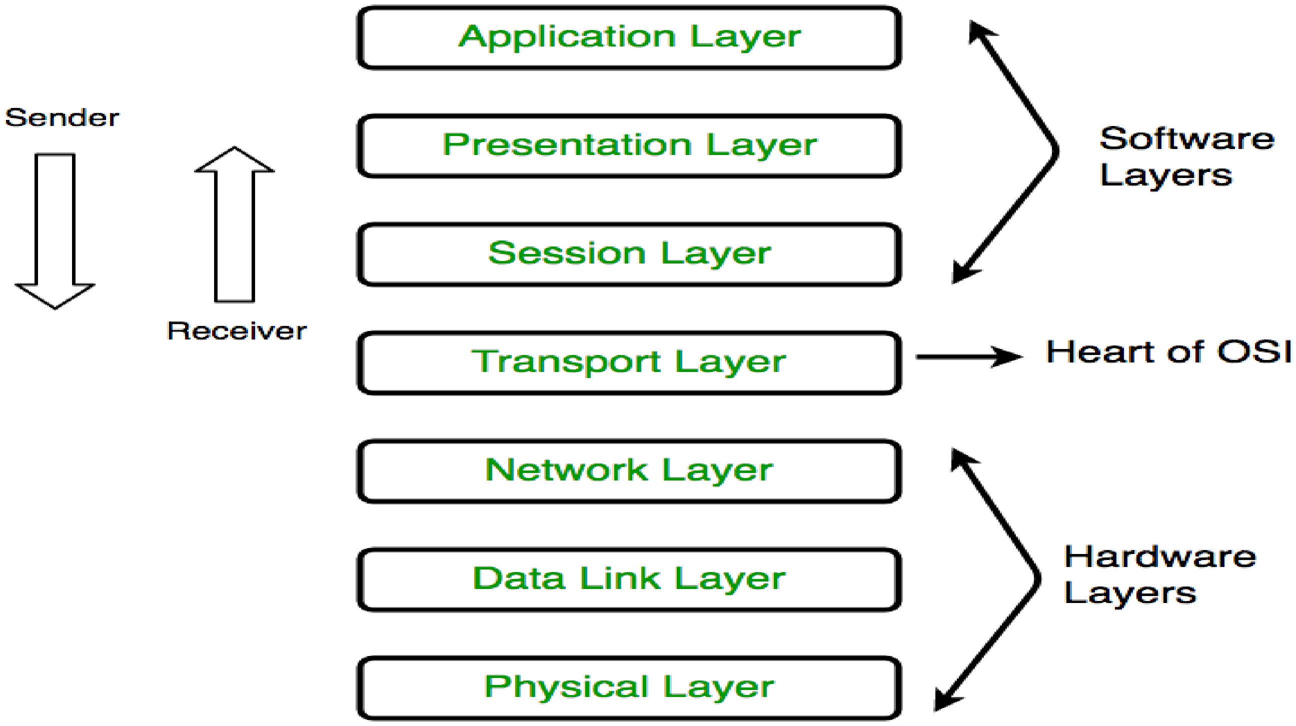
Network Size

Networks vary considerably in size.The following are commonly used terms:

- **PAN** -Personal Area Network – Linking local devices e,g, PC to printer
- **LAN** – Local Area network- links devices in an office or offices
- **MAN** – Metropolitan Area network – links devices across multiple buildings like a campus
- **WAN** – Wide area network – links devices across a country/countries.

Layers of OSI Model

- OSI stands for **Open Systems Interconnection**.
- It has been developed by ISO – '**International Organization of Standardization**', in the year 1974.
- It is a 7 layer architecture with each layer having specific functionality to perform.
- All these 7 layers work collaboratively to transmit the data from one person to another across the globe.



1. Physical Layer (Layer 1) :

- The lowest layer of the OSI reference model is the physical layer.
- It is responsible for the actual physical connection between the devices.
- The physical layer contains information in the form of **bits.**
- It is responsible for the actual physical connection between the devices.

- When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.

1100	0111	0011

The functions of the physical layer are :

1. **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.
2. **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
3. **Physical topologies:** Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topolgy.
4. **Transmission mode:** Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full-duplex.

* Hub, Repeater, Modem, Cables are Physical Layer devices.
** Network Layer, Data Link Layer and Physical Layer are also known as **Lower Layers** or **Hardware Layers**.

2. Data Link Layer (DLL) (Layer 2) :

- The data link layer is responsible for the node to node delivery of the message.
- The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer.
- When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.

Data Link Layer is divided into two sub layers :

1. Logical Link Control (LLC)
2. Media Access Control (MAC)

The packet received from Network layer is further divided into frames depending on the frame size of NIC(Network Interface Card).

DLL also encapsulates Sender and Receiver’s MAC address in the header.
The Receiver’s MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking “Who has that IP address?” and the destination host will reply with its MAC address.

The functions of the data Link layer are :

1. **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.

2. **Physical addressing:** After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.

3. **Error control:** Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.

4. **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus , flow control coordinates that amount of data that can be sent before receiving acknowledgement.

5. **Access control:** When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.

** Packet in Data Link layer is referred as **Frame**.*
*** Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.*
**** Switch & Bridge are Data Link Layer devices.*

3. Network Layer (Layer 3) :

- Network layer works for the transmission of data from one host to the other located in different networks.
- It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available.
- The sender & receiver's IP address are placed in the header by network layer.

The functions of the Network layer are :

1. **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of network layer is known as routing.

2. **Logical Addressing:** In order to identify each device on internetwork uniquely, network layer defines an addressing scheme. The sender & receiver's IP address are placed in the header by network layer. Such an address distinguishes each device uniquely and universally.

* *Segment* in Network layer is referred as **Packet**.

** Network layer is implemented by networking devices such as routers.

4. Transport Layer (Layer 4) :

- Transport layer provides services to application layer and takes services from network layer. The data in the transport layer is referred to as *Segments*.
- It is responsible for the End to End delivery of the complete message.
- Transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.

• At sender's side:

Transport layer receives the formatted data from the upper layers, performs **Segmentation** and also implements **Flow & Error control** to ensure proper data transmission.

It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.

Note: The sender need to know the port number associated with the receiver's application. Generally, this destination port number is configured, either by default or manually. For example, when a web application makes a request to a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default port assigned.

• At receiver's side:

Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.

The functions of the transport layer are :

1. **Segmentation and Reassembly:** This layer accepts the message from the (session) layer , breaks the message into smaller units . Each of the segment produced has a header associated with it. The transport layer at the destination station reassembles the message.
2. **Service Point Addressing:** In order to deliver the message to correct process, transport layer header includes a type of address called service point address or port address. Thus by specifying this address, transport layer makes sure that the message is delivered to the correct process.

The services provided by transport layer :

1. **Connection Oriented Service:** It is a three-phase process which include
   – Connection Establishment
   – Data Transfer
   – Termination / disconnection
   In this type of transmission, the receiving device sends an acknowledgment, back to the source after a packet or group of packet is received. This type of transmission is reliable and secure.

2. **Connection less service:** It is a one phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection oriented Service is more reliable than connection less Service.

** Data in the Transport Layer is called as **Segments**.*
*** Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.*
*Transport Layer is called as **Heart of OSI** model.*

5. Session Layer (Layer 5) :

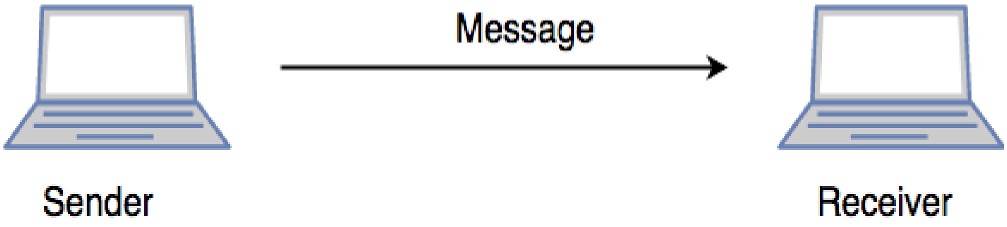
This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.

The functions of the session layer are :

1. **Session establishment, maintenance and termination:** The layer allows the two processes to establish, use and terminate a connection.
2. **Synchronization :** This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
3. **Dialog Controller :** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

***All the below 3 layers(including Session Layer) are integrated as a single layer in TCP/IP model as “Application Layer”.*
***Implementation of these 3 layers is done by the network application itself. These are also known as **Upper Layers** or **Software Layers**.*
SCENARIO:
Let’s consider a scenario where a user wants to send a message through some Messenger application running in his browser. The “Messenger” here acts as the application layer which provides the user with an interface to create the data. This message or so-called Data is compressed, encrypted (if any secure data) and converted into bits (0’s and 1’s) so that it

can be transmitted.



6. Presentation Layer (Layer 6) :

Presentation layer is also called the **Translation layer**.The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

The functions of the presentation layer are :

1. **Translation :** For example, ASCII to EBCDIC.
2. **Encryption/ Decryption :** Data encryption translates the data into another form or
2. code. The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
3. **Compression:** Reduces the number of bits that need to be transmitted on the network.

7. Application Layer (Layer 7) :

- At the very top of the OSI Reference Model stack of layers, we find Application layer which is implemented by the network applications.
- These applications produce the data, which has to be transferred over the network.
- This layer also serves as a window for the application services to access the network and for displaying the received information to the user.
  Ex: Application – Browsers, Skype Messenger etc.
  ***Application Layer is also called as Desktop Layer.*

The functions of the Application layer are :

1. Network Virtual Terminal

2. FTAM-File transfer access and management
3. Mail Services
4. Directory Services

OSI model acts as a reference model and is not implemented in Internet because of its late invention. Current model being used is the TCP/IP model.

TCP/IP Model

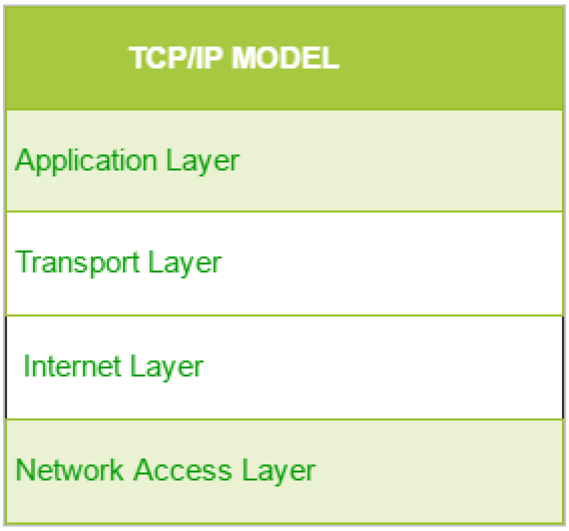
- The **OSI Model** we just looked at is just a reference/logical model.
- It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components.
- But when we talk about the TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols.
- It stands for Transmission Control Protocol/Internet Protocol.

The **TCP/IP model** is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model.

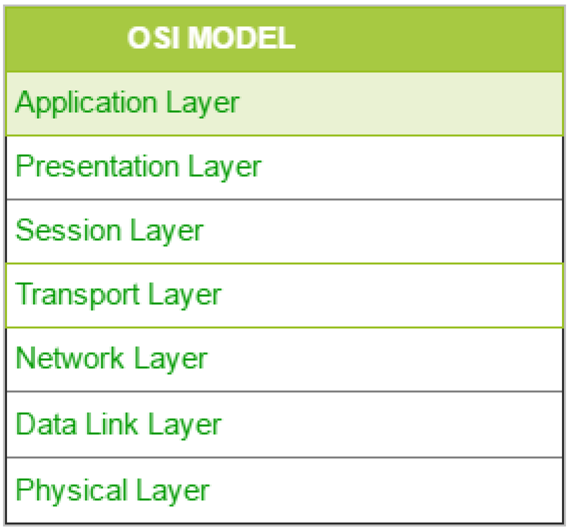
The layers are:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer

The diagrammatic comparison of the TCP/IP and OSI model is as follows :



TCP/IP MODEL
Application Layer
Transport Layer
Internet Layer
Network Access Layer



OSI MODEL
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

Difference between TCP/IP and OSI Model:

TCP/IP	OSI
TCP refers to Transmission Control Protocol.	OSI refers to Open Systems Interconnection.
TCP/IP has 4 layers.	OSI has 7 layers.
TCP/IP is more reliable	OSI is less reliable
TCP/IP does not have very strict boundaries.	OSI has strict boundaries
TCP/IP follow a horizontal approach.	OSI follows a vertical approach.
TCP/IP uses both session and presentation layer in the application layer itself.	OSI uses different session and presentation layers.
TCP/IP developed protocols then model.	OSI developed model then protocol.

The first layer is the Process layer on the behalf of the sender and Network Access layer on the behalf of the receiver. During this article, we will be talking on the behalf of the receiver.

1. Network Access Layer –

- This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model.
- It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.
  We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer.
- It is described as residing in layer 3, being encapsulated by layer 2 protocols.

2. Internet Layer –

- This layer parallels the functions of OSI's Network layer.

- It defines the protocols which are responsible for logical transmission of data over the entire network.

The main protocols residing at this layer are :

1. **IP –** stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers.

   IP has 2 versions:
   IPv4 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.

2. **ICMP –** stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.

3. **ARP –** stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

3. Host-to-Host Layer –

- This layer is analogous to the transport layer of the OSI model.
- It is responsible for end-to-end communication and error-free delivery of data.
- It shields the upper-layer applications from the complexities of data.

The two main protocols present in this layer are :

1. **Transmission Control Protocol (TCP) –**It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.

2. **User Datagram Protocol (UDP) –** On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

4. Process Layer –

This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer.
It is responsible for node-to-node communication and controls user-interface specifications.
Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD.

- **HTTP and HTTPS –** HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.

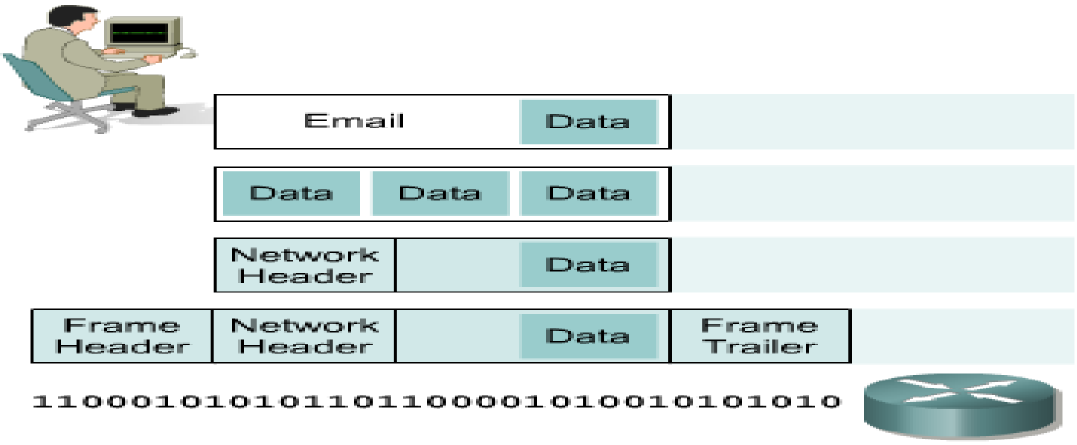
- **SSH –** SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.

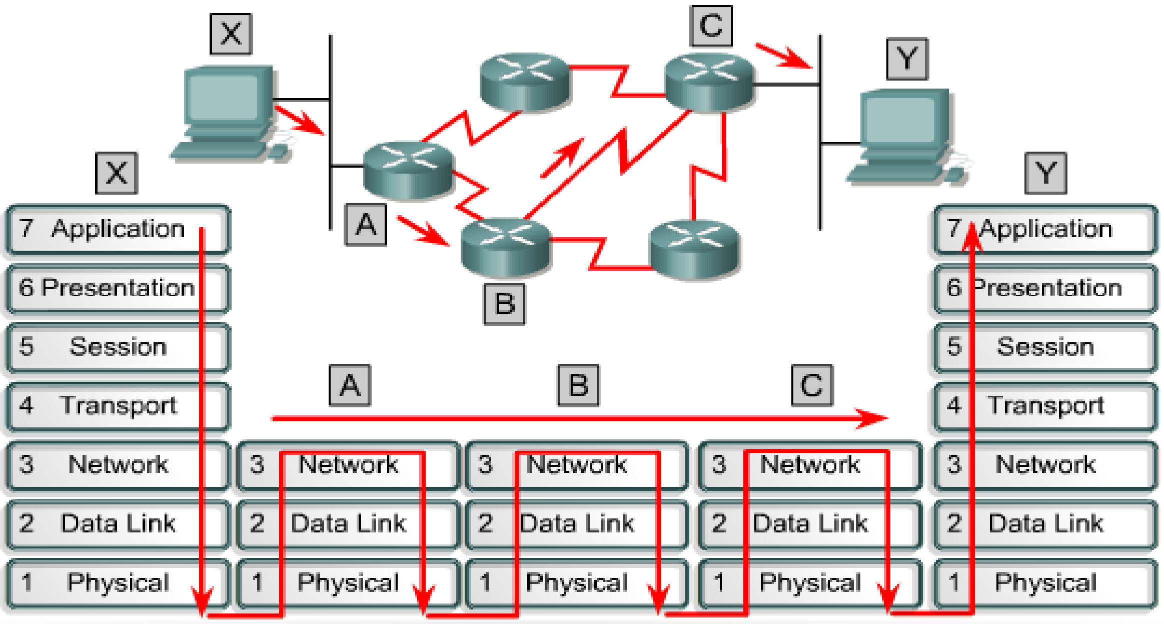
- **NTP –** NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it’s out of sync.

INTERNET PROTOCOL

IP as a Routed Protocol

- IP is a connectionless, unreliable, best-effort delivery protocol.
- IP accepts whatever data is passed down to it from the upper layers and forwards the data in the form of IP Packets.
- All the nodes are identified using an IP address.
- Packets are delivered from the source to the destination using IP address

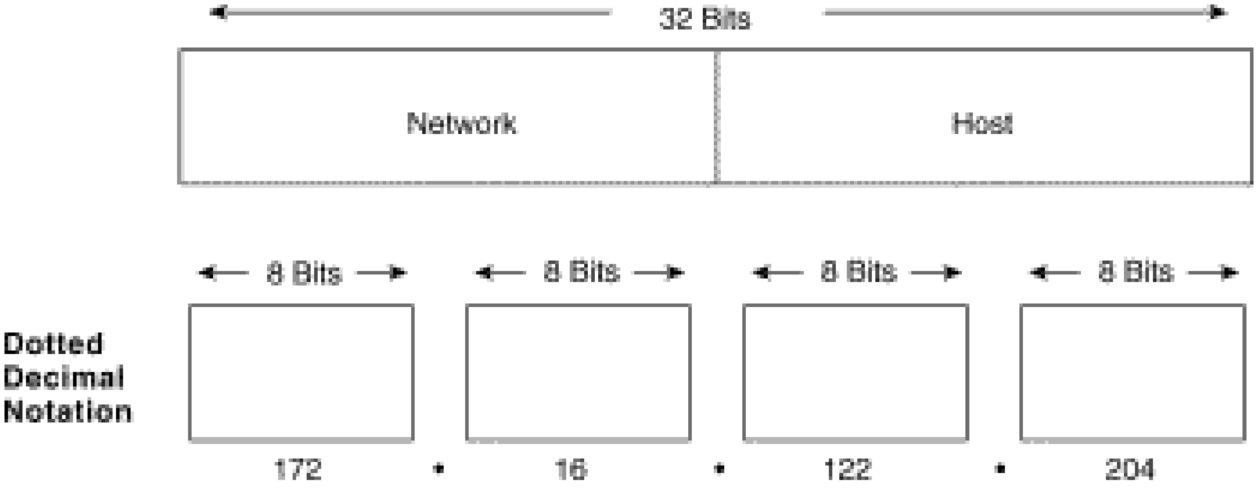


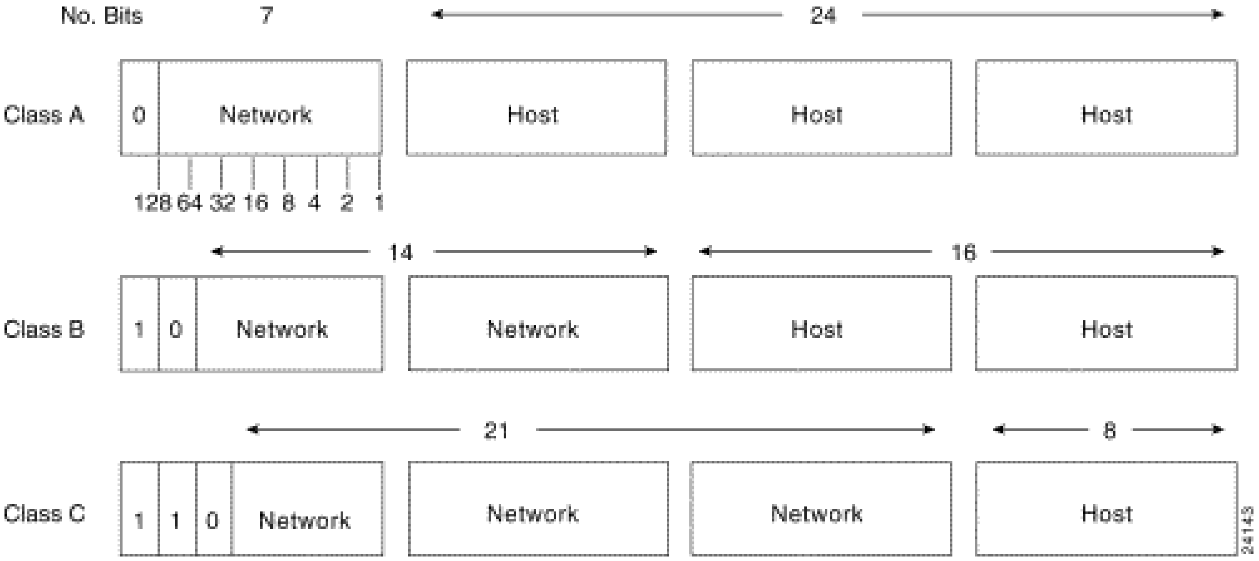


Each router provides its services to support upper-layer functions.

IP Address

- IP address is for the INTERFACE of a host. Multiple interfaces mean multiple IP addresses, i.e., routers.
- 32 bit IP address in dotted-decimal notation for ease of reading, i.e., 193.140.195.66
- Address 0.0.0.0, 127.0.0.1 and 255.255.255.255 carries special meaning.
- IP address is divided into a network number and a host number.
- Also bits in Network or Host Address cannot be all 0 or 1.





Class A : Address begins with bit 0. It has 8 bit network number (range 0.0.0.0 -to- 127.255.255.255), 24 bit host number.

Class B : Address begins with bits 10. It has 16 bit network number (range 128.0.0.0-to- 191.255.255.255), 16 bit host number.

Class C : Address begins with bits 110. It has 24 bit network number (range 192.0.0.0 - to- 223.255.255.255), 8 bit host number.

Class D : Begins with 1110, multicast addresses (224.0.0.0-to-239.255.255.255)

Class E : Begins with 11110, unused

Subnet Mask

- Consider IP address = 192.168.2.25
- First few bits (left to right) identify network/subnet
- Remaining bits identify host/interface

  Number of subnet bits is called subnet mask, e.g.
- Subnet IP Address range is 192.168.2.0 – 192.168.2.255

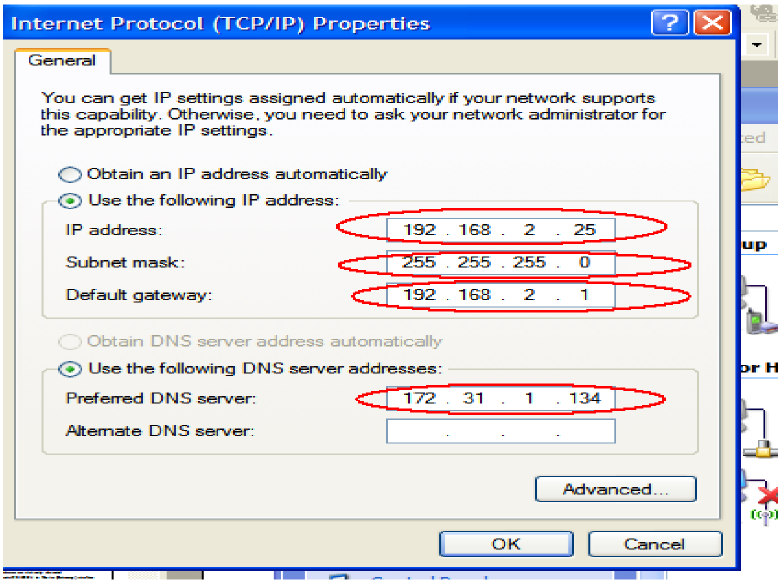
  Mask = 255.255.255.0
- Subnet IP Address range is 192.168.2.0 – 192.168.2.15

  Mask = 255.255.255.240

IP Address, Subnet Mask and Gateway

- IP Address and Subnet Mask define the Subnet
- For Example IP address 172.31.1.0 and Subnet Mask of 255.255.240.0 means that the subnet address ranges from 172.31.0.0 to 172.31.15.255
- Another notation is 172.31.1.0/28
- The first Address is the Network Address and the last Address is the Broadcast Address. They are reserved and cannot be assigned to any node.

- The Gateway Address is the Address of the router where the packet should be sent in case the destination host does not belong to the same subnet
- IP Configuration of an Interface



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 2 . 25

Subnet mask: 255 . 255 . 255 . 0

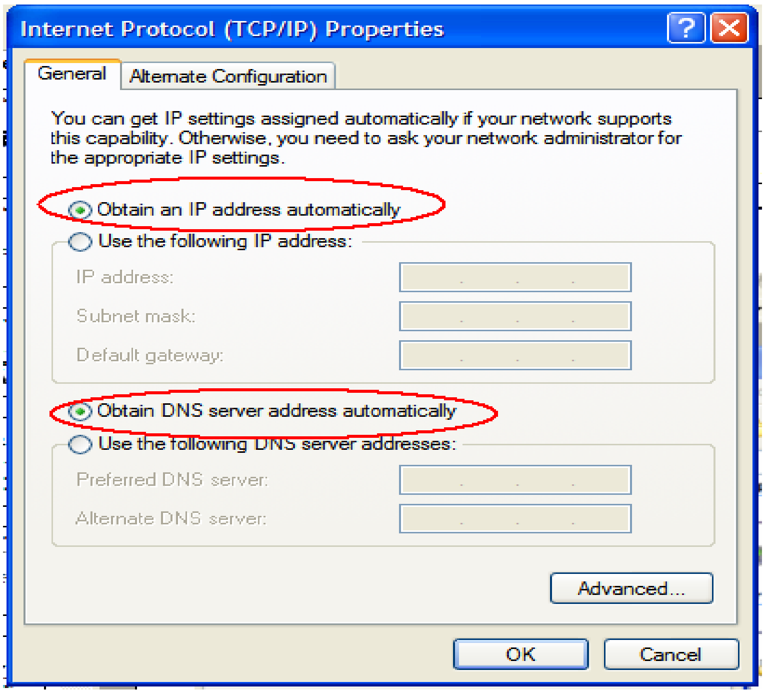
Default gateway: 192 . 168 . 2 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 172 . 31 . 1 . 134

Alternate DNS server: . . .



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

ARP

- ARP (Address Resolution Protocol) is used in Ethernet Networks to find the MAC address of a node given its IP address.
- Source node (say 192.168.2.32) sends broadcast message (ARP Request) on its subnet asking ``Who is 192.168.2.33''.

- All computers on subnet receive this request
- Destination responds (ARP Reply) since it has 192.168.2.33
    - Provides its MAC address in response

IPv6

- Internet Protocol Version 4 is the most popular protocol in use today, although there are some questions about its capability to serve the Internet community much longer.
- IPv4 was finished in the 1970s and has started to show its age.
- The main issue surrounding IPv4 is addressing—or, the lack of addressing—because many experts believe that we are nearly out of the four billion addresses available in IPv4.
- Although this seems like a very large number of addresses, multiple large blocks are given to government agencies and large organizations.
- IPv6 could be the solution to many problems posed by IPv4
- IPv6 uses 128 bit address instead of 32 bit address.
- The IPv6 addresses are being distributed and are supposed to be used based on geographical location.

port number

- Network ports are provided by the TCP or UDP protocols at the Transport layer.
- They are used by protocols in the upper layers of the OSI model.
- Port numbers are used to determine what protocol incoming traffic should be directed to.
- Ports allow a single host with a single IP address to run network services.
- Each port number identifies a distinct service, and each host can have 65535 ports per IP address.
- Port use is regulated by the Internet Corporation for Assigning Names and Numbers (ICANN).

By ICANN there are three categories for ports:

- From 0 to 1023 – well known ports assigned to common protocols and services
- From 1024 to 49151 – registered ports assigned by ICANN to a specific service
- From 49152 to 65 535 – dynamic (private, high) ports range from 49,152 to 65,535. Can be used by any service on an ad hoc basis. Ports are assigned when a session is established, and released when the session ends.

Well known ones are:

Port	**Service name**	**Transport protocol**
20, 21	File Transfer Protocol (FTP)	TCP
22	Secure Shell (SSH)	TCP and UDP
23	Telnet	TCP
25	Simple Mail Transfer Protocol (SMTP)	TCP
50, 51	IPSec	
53	Domain Name System (DNS)	TCP and UDP
67, 68	Dynamic Host Configuration Protocol (DHCP)	UDP
69	Trivial File Transfer Protocol (TFTP)	UDP
80	HyperText Transfer Protocol (HTTP)	TCP
110	Post Office Protocol (POP3)	TCP
119	Network News Transport Protocol (NNTP)	TCP

123	Network Time Protocol (NTP)	UDP
135-139	NetBIOS	TCP and UDP
143	Internet Message Access Protocol (IMAP4)	TCP and UDP
161, 162	Simple Network Management Protocol (SNMP)	TCP and UDP
389	Lightweight Directory Access Protocol	TCP and UDP
443	HTTP with Secure Sockets Layer (SSL)	TCP and UDP
3389	Remote Desktop Protocol	TCP and UDP

Network Devices

HUB

- Hub is one of the basic icons of networking devices.
- which works at physical layer and hence connect networking devices physically together.
- Hubs are fundamentally used in networks that use **twisted pair cabling** to connect devices.
- They are designed to transmit the packets to the other appended devices without altering any of the transmitted packets received.
- They act as pathways to direct electrical signals to travel along.
- They transmit the information regardless of the fact if data packet is destined for the device connected or not.

Hub falls in two categories:

Active Hub:

- They are smarter than the passive hubs.
- They not only provide the path for the data signals infact they regenerate, concentrate and strengthen the signals before sending them to their destinations. Active hubs are also termed as **‘repeaters’**.

Passive Hub:

- They are more like point contact for the wires to built in the physical network.
- They have nothing to do with modifying the signals.

Ethernet Hubs

- It is a device connecting multiple Ethernet devices together and makes them perform the functions as a single unit.
- They vary in speed in terms of data transfer rate.
- Ether utilizes **Carrier Sense Multiple Access with Collision Detect (CSMA/CD)** to control Media access.
- Ethernet hub communicates in **half-duplex** mode where the chances of data collision are inevitable at most of the times.

Switches

- Switches are the linkage points of an Ethernet network.
- Just as in hub, devices in switches are connected to them through twisted pair cabling.
- But the difference shows up in the manner both the devices; hub and a switch treat the data they receive.

- **Hub**works by sending the data to all the ports on the device whereas a **switch** transfers it only to that port which is connected to the destination device.
- A switch does so by having an in-built learning of the MAC address of the devices connected to it.
- Since the transmission of data signals are well defined in a **switch** hence the network performance is consequently enhanced.
- Switches operate in **full-duplex** mode where devices can send and receive data from the switch at the simultaneously unlike in half-duplex mode.
- The transmission speed in switches is double than in Ethernet hub transferring a 20Mbps connection into 30Mbps and a 200Mbps connection to become 300Mbps. Performance improvements are observed in networking with the extensive usage of switches in the modern days.

The following method will elucidate further how data transmission takes place via switches:

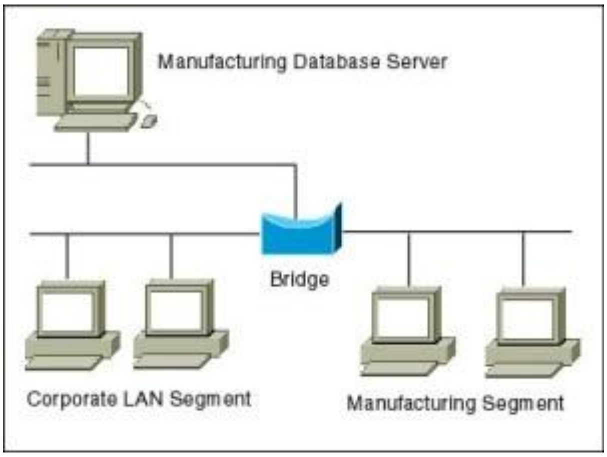
- **Cut-through transmission**: It allows the packets to be forwarded as soon as they are received. The method is prompt and quick but the possibility of error checking gets overlooked in such kind of packet data transmission.

- **Store and forward**: In this switching environment the entire packet are received and 'checked' before being forwarded ahead. The errors are thus eliminated before being propagated further. The downside of this process is that error checking takes relatively longer time consequently making it a bit slower in processing and delivering.

- **Fragment Free**: In a fragment free switching environment, a greater part of the packet is examined so that the switch can determine whether the packet has been caught up in a collision. After the collision status is determined, the packet is forwarded.

Bridges

- 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 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.

Types of Bridges:

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

- **Transparent Bridge:** As the name signifies, it appears to be transparent for the other devices on the network. The other devices are ignorant of its existence. It only blocks or forwards the data as per the MAC address.

- **Source Route Bridge:** It derives its name from the fact that the path which packet takes through the network is implanted within the packet. It is mainly used in Token ring networks.

- **Translational Bridge:** The process of conversion takes place via Translational Bridge. It converts the data format of one networking to another. For instance Token ring to Ethernet and vice versa.

Switches superseding Bridges:

Ethernet switches are seen to be gaining trend as compared to bridges. They are succeeding on the account of provision of logical divisions and segments in the networking field. Infact switches are being referred to as **multi-port bridges** because of their advanced functionality

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.

Information Security

- All measures taken to prevent unauthorized use of electronic data
  - unauthorized use includes disclosure, alteration, substitution, or destruction of the data concerned
- Provision of the following three services
  - Confidentiality
    - concealment of data from unauthorized parties
  - Integrity
    - assurance that data is genuine
  - Availability
    - system still functions efficiently after security provisions are in place
- No single measure can ensure complete security

Why is information security important

- Governments, commercial businesses, and individuals are all storing information electronically
  - compact, instantaneous transfer, easy access
- Ability to use information more efficiently has resulted in a rapid increase in the value of information
- Information stored electronically faces new and potentially more damaging security threats
  - can potentially be stolen from a remote location
  - much easier to intercept and alter electronic communication than its paper-based predecessors

Building blocks of a secure system

- Confidentiality: concealment from unauthorized parties
  - identification – unique identifiers for all users

- – authentication
    - user: assurance that the parties involved in a real-time transaction are who they say they are
    - data: assurance of message source
  - – authorization - allowing users who have been identified and authenticated to use certain resources
- Integrity: assurance the data is has not been modified by unauthorized parties
  - – non-repudiation
    - proof of integrity and origin of data which can be verified by any third party at any time

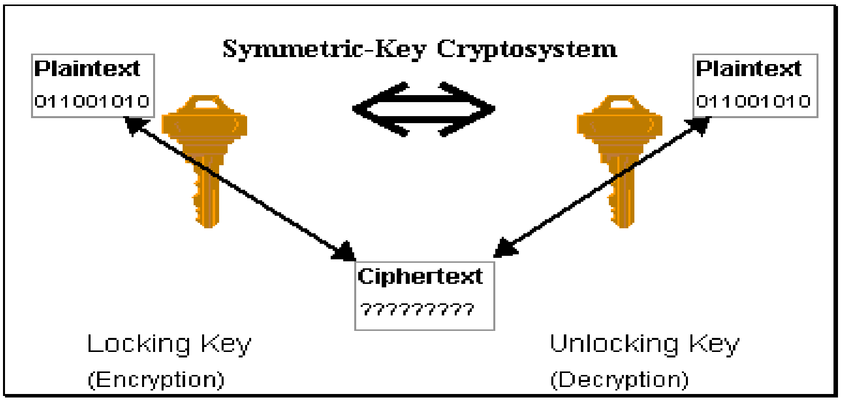
Completing the security process

- Confidentiality + integrity → system security
- However, it is not enough for system to be secure
- System must also be available
  - – must allow guaranteed, efficient and continuous use of information
  - – security measures should not prohibitively slow down or crash system or make it difficult to use
    - what good is a secure system if you can't use it?
- Cryptographic systems
  - – high level of security and flexibility
  - – can potentially provide all objectives of information security: confidentiality, integrity, and availability

Symmetric and public key cryptosystems

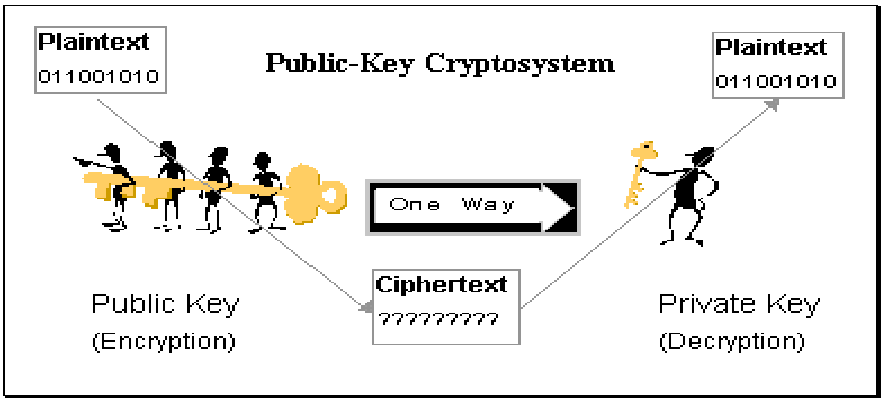
Symmetric-key cryptosystem

- same key is used for encryption and decryption
- system with 1000 users requires 499,500 keys
  - – each pair of users requires a different key



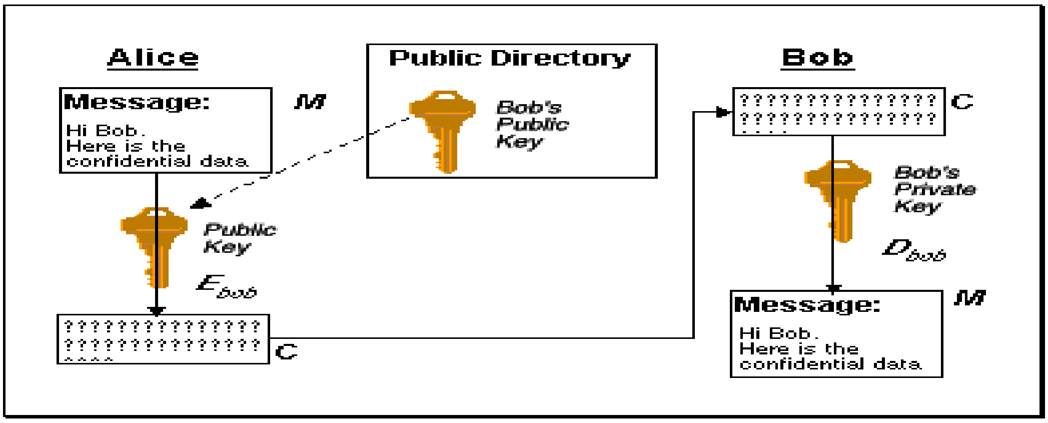
Public-key cryptosystem

- separate keys for encryption and decryption
- system with 1000 users requires 2000 keys
  - each individual user has exactly two keys



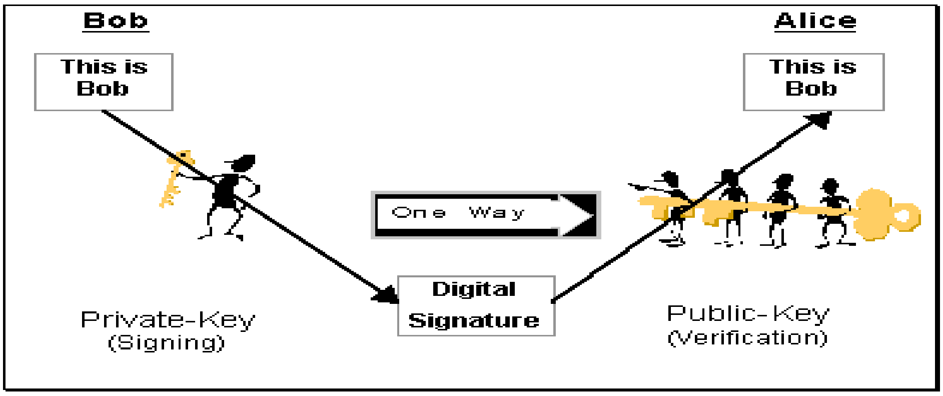
Public-key encryption: confidentiality

- Alice wants to send message M to Bob
  - uses Bob's publickey to encrypt M
- Bob uses his privatekey to decrypt M
  - only Bob has key
  - no one else candecipher M
- Identification provided by public key encryption
- But … anyone can send message to Bob using his public key
  - how are we sure the message came from Alice?



Digital signatures

- Electronic equivalentofhandwritten signatures
- Handwrittensignaturesare hard to forge
- Electronicinformation iseasy to duplicate
- Digital signatures using public key encryption
  - Idea:
    - Bob uses his private key to “sign” a message
    - Alice verifies signature using Bob’s public key
- Data authentication provided by digital signatures



Signed challenges

- Alice wants assurance of real-time communication
- Bob tries to provide assurance by digital signature
- Alice is assured message originated from Bob
  - digital signatures provide data origin authentication
  - But … Eve can intercept signature and use it to authenticate herself as Bob at any later time

- Signed challenge
  - Alice sends random number (a challenge) to Bob
  - Bob replies with challenge encrypted with signature
- User authentication provided by signed challenges
  - combination of digital signature and unpredictability of Alice's random number challenge

Certification authority

- A third party trusted by all users that creates, distributes, revokes, & manages *certificates*
- Certificates bind users to their public keys
- For example, if Alice wants to obtain Bob's public key
  - she retrieves Bob's certificate from a public directory
  - she verifies the CA's signature on the certificate itself
  - if signature verifies correctly, she has assurance from the trusted CA this really is Bob's public key
  - she can use Bob's public key to send confidential information to Bob or to verify Bob's signatures, protected by the assurance of the certificate
- Integrity is provided by the certification authority

Attacks

- Compromise systems in ways that affect services of information security
  - attack on confidentiality:
    - unauthorized disclosure of information
  - attack on integrity:
    - destruction or corruption of information
  - attack on availability:
    - disruption or denial of services

Prevention, detection, response

- proper planning reduces risk of attack and increases capabilities of detection and response if an attack does occur

Prevention

- Establishment of policy and access control

  - who: identification, authentication, authorization
  - what: granted on “need-to-know” basis
- Implementation of hardware, software, and services
  - users cannot override, unalterable (attackers cannot defeat security mechanisms by changing them)
  - examples of preventative mechanisms
    - passwords - prevent unauthorized system access
    - firewalls - prevent unauthorized network access
    - encryption - prevents breaches of confidentiality
    - physical security devices - prevent theft
- Maintenance

Detection

- Determine that either an attack is underway or has occurred and report it
- Real-time monitoring
  - or, as close as possible
  - monitor attacks to provide data about their nature, severity, and results
- Intrusion verification and notification
  - intrusion detection systems (IDS)
  - typical detection systems monitor various aspects of the system, looking for actions or information indicating an attack
    - example: denial of access to a system when user repeatedly enters incorrect password

Response

- Stop/contain an attack
  - must be timely!
    - incident response plan developed in advance
- Assess and repair any damage
- Resumption of correct operation
- Evidence collection and preservation
  - very important
    - identifies vulnerabilities
    - strengthens future security measures