

IBPS (SO) IT Officer: Data Communication and Networking Study Notes



Computer Networks means an **interconnected** set of an autonomous systems that permits distributed processing to information.

Five components of networks :

- Sender Computer
- Sender equipment (Modem)
- Communication Channel (Telephone Cables)
- Receiver Equipment (Modem)
- Receiver Computer

There are two aspects in computer networks :

- **Hardware:** It includes a physical connection (using an adapter, cable, router, bridge, etc)
- **Software:** It includes a set of protocols (nothing but a set of rules)

Methods of Message Delivery: A message can be delivered in the following ways

- **Unicast:** One device sends the message to the other to its address.
- **Broadcast:** One device sends the message to all other devices on the network. The message is sent to an address reserved for this goal.
- **Multicast:** One device sends the message to a certain group of devices on the network.

Types of Networks :

Mainly three types of network based on their coverage areas: **LAN**, **MAN**, and **WAN**.

LAN (Local Area Network):

- LAN is a privately owned network within a single building or campus. A **local area network** is a relatively smaller and privately owned network with the maximum span of **10 km**.

MAN (Metropolitan Area Network)

- MAN provides regional connectivity within a campus or small geographical area like cable television networks in the city. It is defined for less than **50 Km**.

WAN (Wide Area Network)

- A Wide Area Network (WAN) spans a **large** geographical area often a country, provides **no limit** of distance.

Note: The Internet (Network of networks) is a system of linked networks that are worldwide in scope and facilitate **data communication services** such as remote **login**, file transfer, electronic mail, World Wide Web and newsgroups etc.

Characteristics of Networking :

- **Topology:** The geometrical arrangement of the computers or nodes.
- **Protocols:** How they communicate.
- **Medium:** Through which medium.

Network Topology

- Network topology is the arrangement of the various elements of a computer or biological network.



IBPS SO 2021 MAINS
Special Course (AFO)

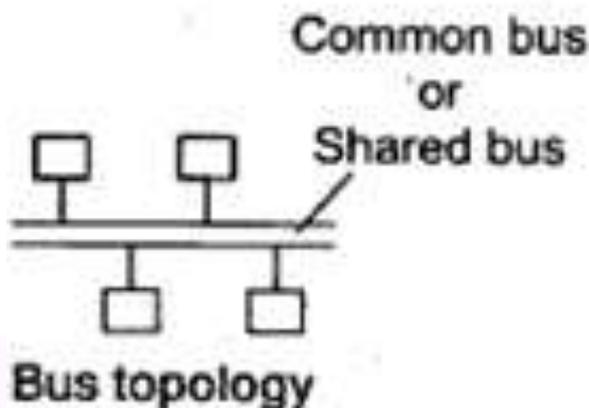
START FREE TRIAL

- It is the topological structure of a network and may be depicted physically or logically. Physical topology refers to the placement of the network's various components, including device location and cable installation, while logical topology shows how data flows within a network, regardless of its physical design.

The common network topologies include the following sections:

- **Bus Topology:**

Bus topology is a specific kind of **network topology** in which all of the various devices in the network are connected to a single cable or line.



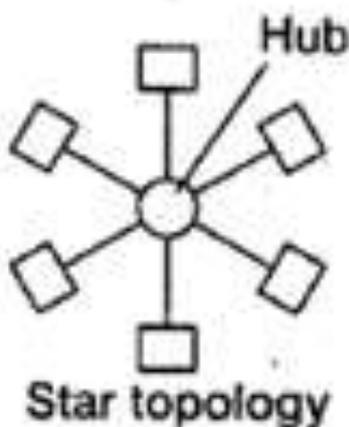
Note:

- a. In **bus topology** at the first, the message will go through the bus then one user can communicate with other.
- b. The drawback of this **topology** is that if the network cable breaks, the entire network will be down.

- **Star Topology :**

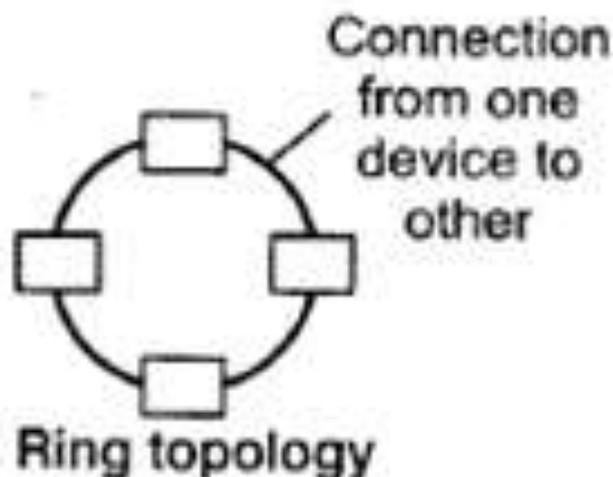
Star topology is a **network topology** where each individual piece of a network is attached to a central node (often called a hub or switch).

The attachment of these network pieces to the central component is visually represented in a form similar to a star.



- **Ring Topology:**

Ring topology is a type of **network topology** where each node is exactly connected to two other nodes, **forward** and **backward**, thus forming a **single continuous** path for signal transmission.



Note:

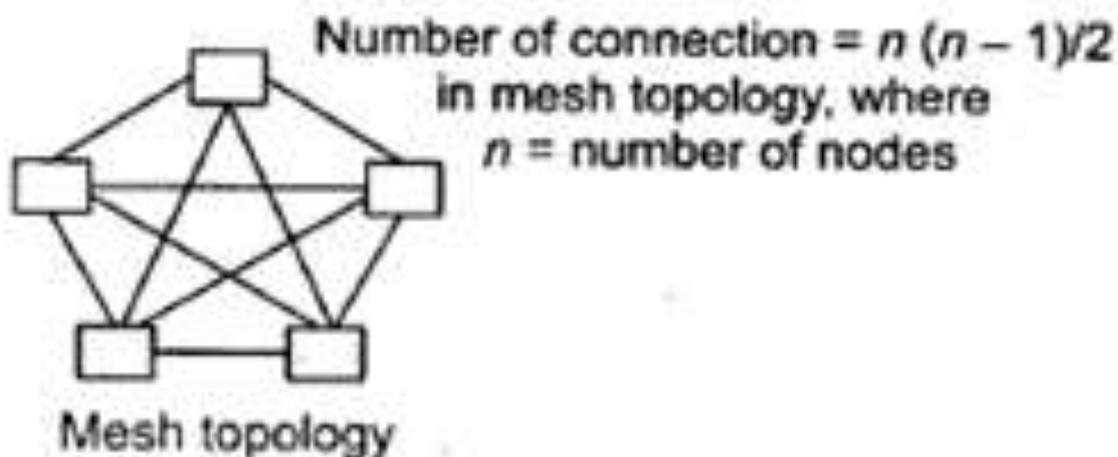
Two types of the Ring Topology based on the data flow:

Unidirectional: A Unidirectional ring topology handles data traffic in either clockwise or anticlockwise direction. This data network, thus, can also be called as a half-duplex network.

Bi-directional: A Unidirectional ring topology is thus easy to maintain compared to the bidirectional ring topology.

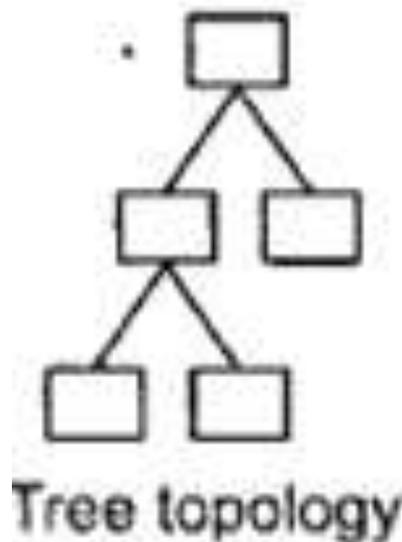
- **Mesh Topology:**

Each system is connected to all other systems in the network.



- **Tree Topology:**

A tree topology is a special type of structure in which many connected elements are arranged like the branches of a tree.



Note:-

- In **bus topology** at **first**, the message will go through the **bus** then one user can **communicate** with others.
- In **star topology**, first, the message will go to the **hub** then that message will go to another user.
- In-ring **topology**, user **can communicate** as randomly.
- In a **mesh topology**, any user can **directly communicate** with other users.

Hardware/Networking Devices

Networking hardware may also be known as network equipment computer networking devices.

- **Network Interface Card (NIC):** NIC provides a physical connection between the networking cable and the computer's internal bus. NICs come in three basic varieties 8 bit, 16 bit and 32 bit. The larger the number of bits that can be transferred to NIC, the faster the NIC can transfer data to the network cable.
- **Repeater:** Repeaters are used to connect together two Ethernet segments of any media type. In larger designs, signal quality begins to deteriorate as segments exceed their maximum length. We also know that signal transmission is always attached to energy loss. So, a periodic refreshing of the signals is required.
- **Hubs:** Hubs are actually multi-part repeaters. A hub takes any incoming signal and repeats it out all ports.
- **Bridges:** When the size of the LAN is difficult to manage, it is necessary to break up the network. The function of the bridge is to connect separate networks together. Bridges do not forward bad or misaligned packets.



IBPS SO 2021 MAINS
Special Course (AFO)

START FREE TRIAL

- **Switch:** Switches are an expansion of the concept of bridging. Cut through switches examine the packet destination address, only before forwarding it onto its destination segment, while a store and forward switch accept and analyze the entire packet before forwarding it to its destination. It takes more time to examine the entire packet, but it allows catching certain packet errors and keeping them from propagating through the network.
- **Routers:** Router forwards packets from one LAN (or WAN) network to another. It is also used at the edges of the networks to connect to the Internet.
- **Gateway:** Gateway acts as an entrance between two different networks. Gateway in organizations is the computer that routes the traffic from a work station to the outside network that is serving web pages. ISP (Internet Service Provider) is the gateway for Internet service at home.

Data Transfer Modes:

There are mainly **three modes** of data transfer.

- **Simplex:** Data transfer only in one direction e.g., radio broadcasting.
- **Half Duplex:** Data transfer in both directions, but not simultaneously e.g., talkback radio.
- **Full Duplex or Duplex:** Data transfer in both directions, simultaneously e.g., telephone

Data representation :

Information comes in different forms such as text, numbers, **images**, **audio**, and **video**.

- **Text:** Text is represented as a bit pattern. The number of bits in a pattern depends on the number of symbols in the language.
- **ASCII:** The American National Standards Institute developed a code called the American Standard Code for Information Interchange. This code uses 7 bits for each symbol.
- **Extended ASCII:** To make the size of each pattern 1 byte (8 bits), the ASCII bit patterns are augmented with an extra 0 at the left.
- **Unicode:** To represent symbols belonging to languages other than English, a code with much greater capacity is needed. Unicode uses 16 bits and can represent up to 65,536 symbols.
- **ISO:** The international organization for standardization known as ISO has designed code using a 32-bit pattern. This code can represent up to 4,294,967,296 symbols.
- **Numbers:** Numbers are also represented by using bit patterns. ASCII is not used to represent numbers. The number is directly converted to a binary number.
- **Images:** Images are also represented by bit patterns. An image is divided into a matrix of pixels, where each pixel is a small dot. Each pixel is assigned a bit pattern. The size and value of the pattern depend on the image. The size of the pixel depends on what is called the resolution.
- **Audio:** Audio is a representation of sound. Audio is by nature different from text, numbers or images. It is continuous, not discrete



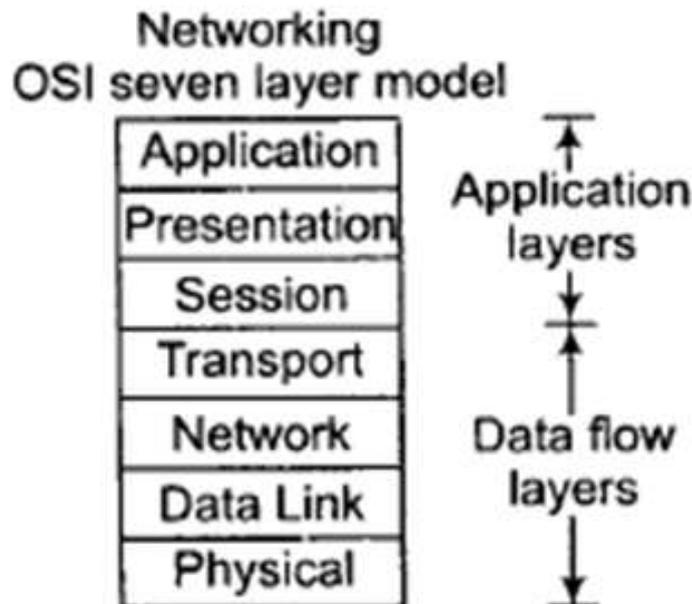
IBPS SO 2021 MAINS
Special Course (AFO)

START FREE TRIAL

- **Video:** Video can be produced either a continuous entity or it can be a combination of images.

Open System Interconnection (OSI) Model

The **Open System Interconnection** (OSI) model is a reference tool for understanding data communication between any two networked systems. It divides the communication processes into 7 layers. Each layer performs specific functions to support the layers above it and uses the services of the layers below it.



- **Physical Layer:** The physical layer coordinates the functions required to transmit a bitstream over a physical medium. It deals with the mechanical and electrical specifications of interface and transmission medium. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur.
- **Data Link Layer:** The data link layer transforms the physical layer, a raw transmission facility, to a reliable link and is responsible for Node-to-Node delivery. It makes the physical layer appear error-free to the upper layer (i.e, network layer).
- **Network Layer:** The network layer is responsible for source to destination delivery of a packet possibly across multiple networks (links). If the two systems are connected to the same link, there is usually no need for a network layer. However, if the two systems are attached to different networks (links) with connecting devices between networks, there is often a need for the network layer to accomplish source to destination delivery.
- **Transport Layer:** The transport layer is responsible for- source to destination (end-to-end) delivery of the entire message. The network layer does not recognize any relationship between the packets delivered. The network layer treats each packet independently, as though each packet belonging to a separate message, whether or not it does. The transport layer ensures that the whole message arrives intact and in order.



- **Session Layer:** The session layer is the network dialog controller. It establishes, maintains and synchronizes the interaction between communicating systems. It also plays an important role in keeping application data separate.
- **Presentation Layer:** This layer is responsible for how an application formats data to be sent out onto the network. This layer basically allows an application to read (or understand) the message.

Ethernet

It is basically a **LAN technology** that strikes a good balance between speed, cost, and ease of installation.

- Ethernet topologies are general bus and/or bus-star topologies.
- Ethernet networks are passive, which means Ethernet hubs do not reprocess or alter the signal sent by the attached devices.
- Ethernet technology uses broadcast topology with baseband signaling and a control method called Carrier Sense Multiple Access/Collision Detection (CSMA/CD) to transmit data.
- The IEEE 802.3 standard defines Ethernet protocols for (Open Systems Interconnect) OSI's Media Access Control (MAC) sublayer and physical layer network characteristics.
- The IEEE 802.2 standard defines protocols for the Logical Link Control (LLC) sublayer.

Ethernet refers to the family of a local area network (LAN) implementations that include three principal categories.

- **Ethernet and IEEE 802.3:** LAN specifications that operate at 10 Mbps over coaxial cable.
- **100-Mbps Ethernet:** A single LAN specification, also known as Fast Ethernet, which operates at 100 Mbps over twisted-pair cable.
- **1000-Mbps Ethernet:** A single LAN specification, also known as Gigabit Ethernet, that operates at 1000 Mbps (1 Gbps) over fiber and twisted-pair cables.

IEEE Standards

- **IEEE 802.1:** Standards related to network management.
- **IEEE 802.2:** Standard for the data link layer in the OSI Reference Model
- **IEEE 802.3:** Standard for the MAC layer for bus networks that use CSMA/CD. (Ethernet standard)
- **IEEE 802.4:** Standard for the MAC layer for bus networks that use a token-passing mechanism (token bus networks).
- **IEEE 802.5:** Standard for the MAC layer for token-ring networks.



- **IEEE 802.6:** Standard for Metropolitan Area Networks (MANs).

IEEE Physical Standard Maximum Speed Maximum Cable Length

IEEE Standard	Physical Standard	Maximum Speed	Maximum Cable Length
802.3a	10base2	10 Mbps	185 meters
802.3	10base5	10 Mbps	500 meters
802.3i	10baseT	10 Mbps	100 meters
802.3j	10baseF	10 Mbps	2000 meters

FLOW CONTROL:

Flow control coordinates the amount of data that can be sent before receiving ACK. It is one of the most important duties of the data link layer.

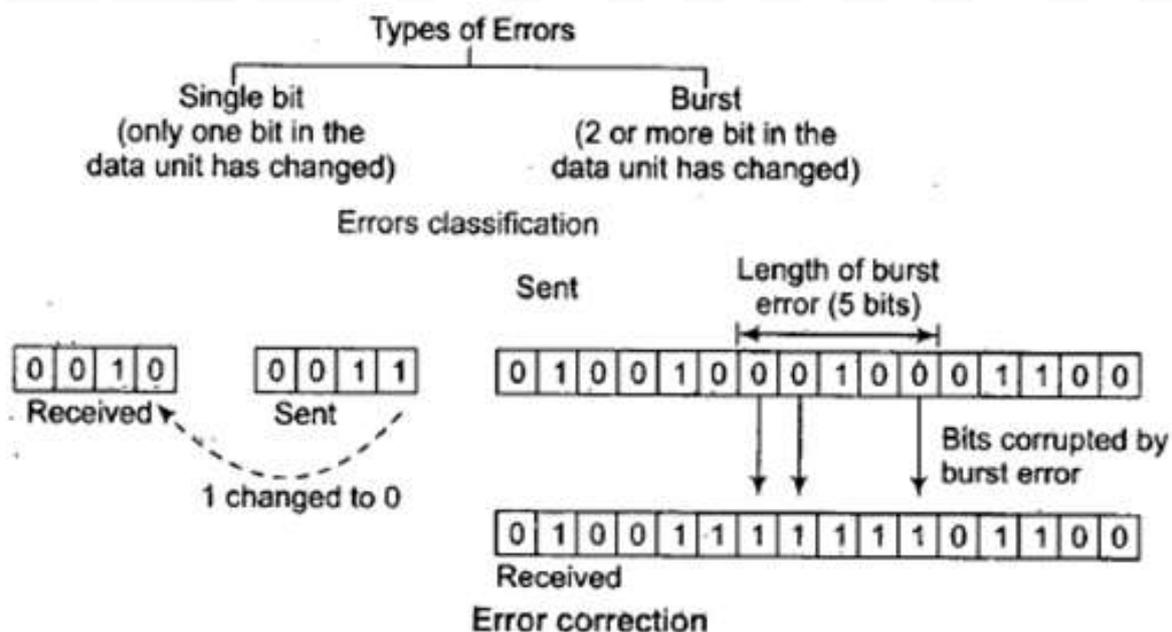
ERROR CONTROL:

Error control in the data link layer is based on ARQ (automatic repeat request), which is the retransmission of data.

- The term error control refers to methods of error detection and retransmission.
- Anytime an error is detected in an exchange, specified frames are retransmitted. This process is called ARQ.

Error Control (Detection and Correction)

Many factors including line noise can alter or wipe out one or more bits of a given data unit.



- Reliable systems must have the mechanism for detecting and correcting such errors.
- Error detection and correction are implemented either at the data link layer or the transport layer of the OSI model.



IBPS SO 2021 MAINS
Special Course (AFO)

START FREE TRIAL

Checksum

There are two algorithms involved in this process, checksum generator at sender end and checksum checker at the receiver end.

The **sender** follows these steps:

- The data unit is divided into k sections each of n bits.
- All sections are added together using 1's complement to get the sum.
- The sum is complemented and becomes the checksum.
- The checksum is sent with the data.

The **receiver** follows these steps:

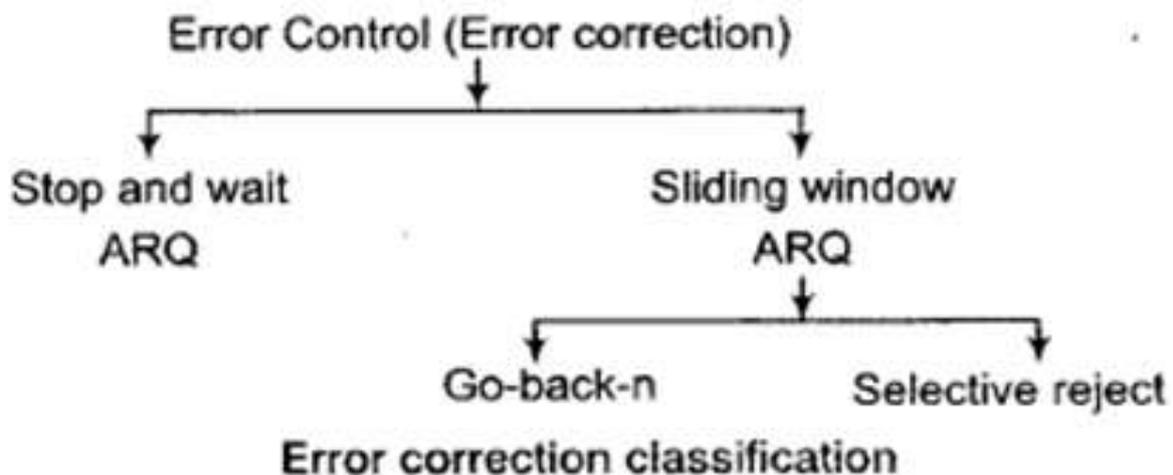
- The received unit is divided into k sections each of n bits.
- All sections are added together using 1's complement to get the sum.
- The sum is complemented.
- If the result is zero, the data are accepted, otherwise, they are rejected.

Cyclic Redundancy Check (CRC):

CRC is based on binary division. A sequence of redundant bits called CRC or the CRC remainder is appended to the end of a data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number. At its destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be intact and therefore is accepted.

Error Correction:

Error correction in the data link layer is implemented simply anytime, an error is detected in an exchange, a negative acknowledgment NAK is returned and the specified frames are retransmitted. This process is called an Automatic Repeat Request (ARQ). Retransmission of data happens in three Cases: Damaged frame, Lost frame and Lost the acknowledgment.



Stop and Wait for ARQ: Include retransmission of data in case of lost or damaged framer. For retransmission to work, four features are added to the basic flow control mechanism.

- If an error is discovered in a data frame, indicating that it has been corrupted in transit, a NAK frame is returned. NAK frames, which are numbered, tell the sender to retransmit the last frame sent.

IBPS SO 2021 MAINS
Special Course (AFO)

START FREE TRIAL

- The sender device is equipped with a timer. If an expected acknowledgment is not received within an allotted time period, the sender assumes that the last data frame was lost in transit and sends it again.

Sliding Window ARQ: To cover retransmission of lost or damaged frames, three features are added to the basic flow control mechanism of the sliding window.

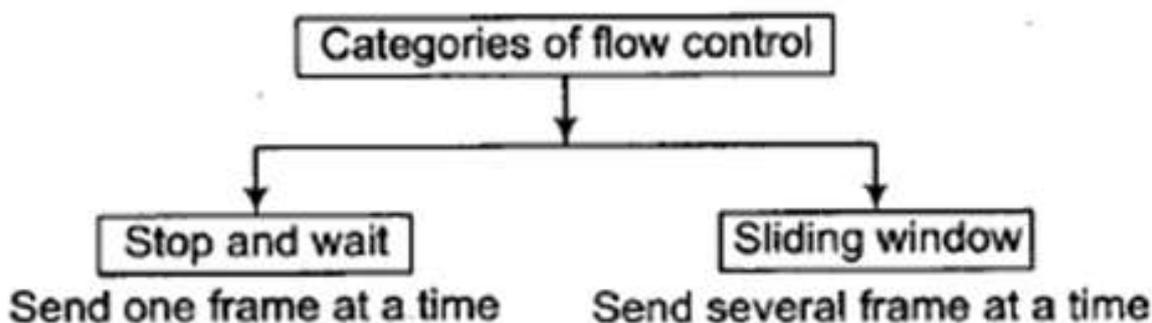
- The sending device keeps copies of all transmitted frames until they have been acknowledged.
- In addition to ACK frames, the receiver has the option of returning a NAK frame, if the data have been received damaged. NAK frame tells the sender to retransmit a damaged frame. Here, both ACK and NAK frames must be numbered for identification. ACK frames carry the number of next frames expected. NAK frames, on the other hand, carry the number of the damaged frame itself. If the last ACK was numbered 3, an ACK 6 acknowledges the receipt of frames 3, 4 and 5 as well. If data frames 4 and 5 are received damaged, both NAK 4 and NAK 5 must be returned.
- Like stop and wait for ARQ, the sending device in sliding window ARQ is equipped with a timer to enable it to handle lost acknowledgments.

Go-back-n ARQ: In this method, if one frame is lost or damaged all frames sent since the last frame acknowledged are retransmitted.

Selective Reject ARQ: In this method, only a specific damaged or lost frame is retransmitted. If a frame is corrupted in transmit, an NAK is returned and the frame is resent out of sequence. The receiving device must be able to sort the frames it has and insert the retransmitted frame into its proper place in the sequence.

Flow Control

One important aspect of the data link layer is flow control. Flow control refers to a set of procedures used to restrict the amount of data the sender can send before waiting for an acknowledgment.



Stop and Wait: In this method, the sender waits for an acknowledgment after every frame it sends. Only when an acknowledgment has been received is the next frame sent. This process continues until the sender transmits an End of Transmission (EOT) frame.

- We can have two ways to manage data transmission when a fast sender wants to transmit data to a low-speed receiver.



- The receiver sends information back to the sender giving it permission to send more data i.e., feedback or acknowledgment based flow control.
- Limit the rate at which senders may transmit data without using feedback from the receiver i.e., Rate based-flow control.

Advantages of Stop and Wait: It's simple and each frame is checked and acknowledged well.

Disadvantages of Stop and Wait:

- It is inefficient if the distance between devices is long.
- The time spent waiting for ACKs between each frame can add a significant amount to the total transmission time.

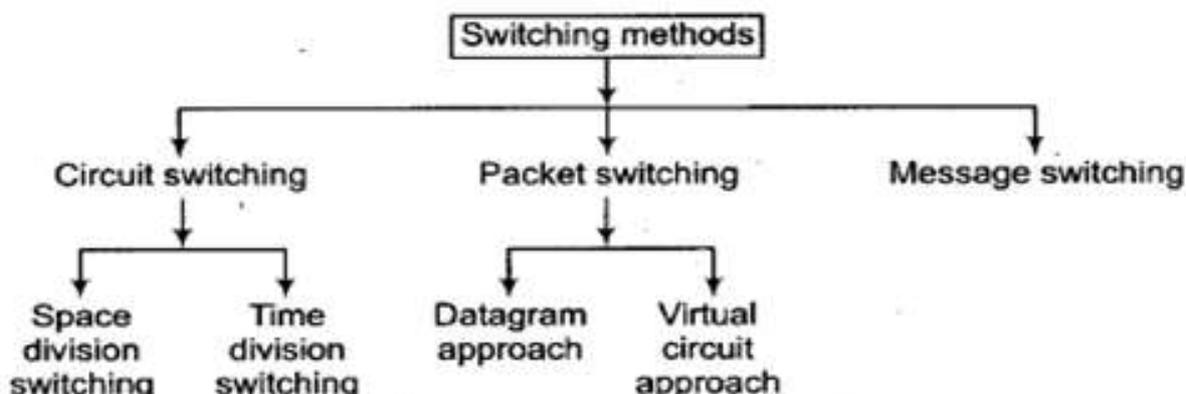
Sliding Window: In this method, the sender can transmit several frames before needing an acknowledgment. The sliding window refers to imaginary boxes at both the sender and the receiver. This window can hold frames at either end and provides the upper limit on the number of frames that can be transmitted before requiring an acknowledgment.

- The frames in the window are numbered modulo-n, which means they are numbered from 0 to n -1. For example, if n = 8, the frames are numbered 0, 1, 2, 3, 4, 5, 6, 7, 0, 1, 2, 3, 4, 5, 6, 7, 0, 1...so on. The size of the window is (n -1) in this case size of window = 7..
- In other words, the window can't cover the whole module (8 frames) it covers one frameless that is 7.
- When the receiver sends an ACK, it includes the number of the next frame it expects to receive. When the receiver sends an ACK containing the number 5, it means all frames up to number 4 have been received.

Switching

We have multiple devices we have a problem of how to connect them to make one-to-one communication possible. Two solutions could be like as given below

- Install a point-to-point connection between each pair of devices (Impractical and wasteful approach when applied to a very large network).
- For a large network, we can go for switching. A switched network consists of a series of interlinked nodes, called switches.



Classification of Switching

- **Circuit Switching:** It creates a direct physical connection between two devices such as phones or computers.
- **Space Division Switching:** Separates the path in the circuit from each other spatially.
- **Time Division Switching:** Uses time-division multiplexing to achieve switching. Circuit switching was designed for voice communication. In a telephone conversation e.g., Once a circuit is established, it remains connected for the duration of the session.

Disadvantages of Circuit Switching

- Less suited to data and other non-voice transmissions.
- A circuit-switched link creates the equivalent of a single cable between two devices and thereby assumes a single data rate for both devices. This assumption limits the flexibility and usefulness of a circuit-switched connection.
- Once a circuit has been established, that circuit is the path taken by all parts of the transmission, whether or not it remains the most efficient or available.
- Circuit switching sees all transmissions as equal. Any request is granted to whatever link is available. But often with data transmission, we want to be able to prioritize.

Packet Switching

To overcome the disadvantages of the circuit switch. The packet switching concept came into the picture.

In a packet-switched network, data are transmitted in discrete units of potentially variable-length blocks called packets. Each packet contains not only data but also a header with control information (such as priority codes and source and destination address). The packets are sent over the network node to the node. At each node, the packet is stored briefly, then routed according to the information in its header.

There are two popular approaches to packet switching.

1. Datagram
2. Virtual circuit

Datagram Approach: Each packet is treated independently from all others. Even when one packet represents just a piece of a multi-packet transmission, the network (and network layer functions) treats it as though it existed alone.

Virtual Circuit Approach: The relationship between all packets belonging to a message or session is preserved. A single route is chosen between the sender and receiver at the beginning of the session. When the data are sent, all packets of the transmission travel one after another along that route.

We can implement it into two formats:

- Switched Virtual Circuit (SVC)
- Permanent Virtual Circuit (PVC)

SVC (Switched Virtual Circuit)

This SVC format is comparable conceptually to dial-up lines in circuit switching. In this method, a virtual circuit is created whenever it is needed and exists only for the duration of the specific exchange.



IBPS SO 2021 MAINS
Special Course (AFO)

START FREE TRIAL

PVC (Permanent Virtual Circuit)

The PVC format is comparable to leased lines in circuit switching. In this method, the same virtual circuit is provided between two users on a continuous basis. The circuit is dedicated to specific users. No one else can use it and because it is always in place, it can be used without connection establishment and connection termination.

Message Switching

It is also known as **store and forward**. In this mechanism, a node receives a message, stores it, until the appropriate route is free, and then sends it along.

Store and forward is considered a switching technique because there is no direct link between the sender and receiver of a transmission. A message is delivered to the node along one path, then rerouted along another to its destination.

In message switching, the messages are stored and relayed from secondary storage (disk), while in packet switching the packets are stored and forwarded from primary storage (RAM).

Internet Protocol:

It is a set of technical rules that defines how computers communicate over a network.

IPv4:

It is the first version of Internet Protocol to be widely used and accounts for most of today's Internet traffic.

- Address Size: 32 bits
- Address Format: Dotted Decimal Notation: 192.149.252.76
- Number of Addresses: $2^{32} = 4,294,967,296$ Approximately
- IPv4 header has 20 bytes
- IPv4 header has many fields (13 fields)
- It is subdivided into classes <A-E>.
- Address uses a subnet mask.
- IPv4 has lack of security.

IPv6:

It is a newer numbering system that provides a much larger address pool than IPv4.

- Address Size: 128 bits
- Address Format: Hexadecimal Notation: 3FFE:F200:0234:AB00:0123:4567:8901:ABCD
- Number of Addresses: 2^{128}
- IPv6 header is double, it has 40 bytes
- IPv6 header has fewer fields, it has 8 fields.
- It is classless.
- It uses a prefix and an Identifier ID known as IPv4 network
- It uses a prefix length.
- It has a built-in strong security (Encryption and Authentication)

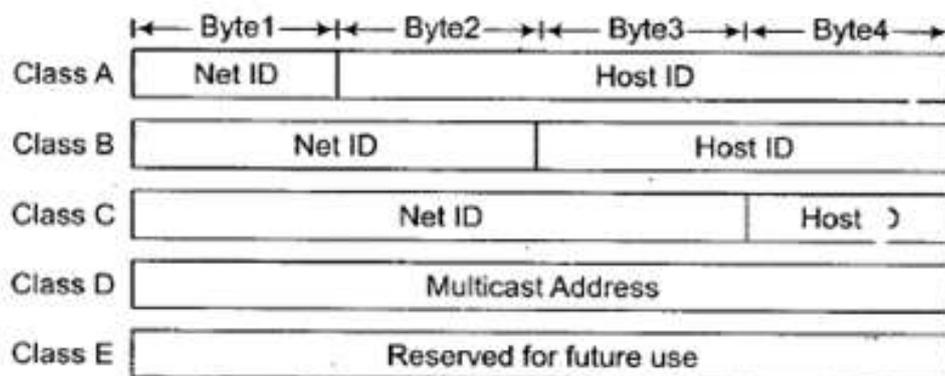


Classes and Subnetting

There are currently five different field length pattern in use, each defining a class of address. An IP address is 32 bit long. One portion of the address indicates a network (Net ID) and the other portion indicates the host (or router) on the network (i.e., Host ID).

To reach a host on the Internet, we must first reach the network, using the first portion of the address (Net ID). Then, we must reach the host itself, using the 2nd portion (Host ID).

The further division a network into smaller networks called **subnetworks**.



For Class A: First bit of Net ID should be 0 like in following pattern

01111011 . 10001111 . 11111100 . 11001111

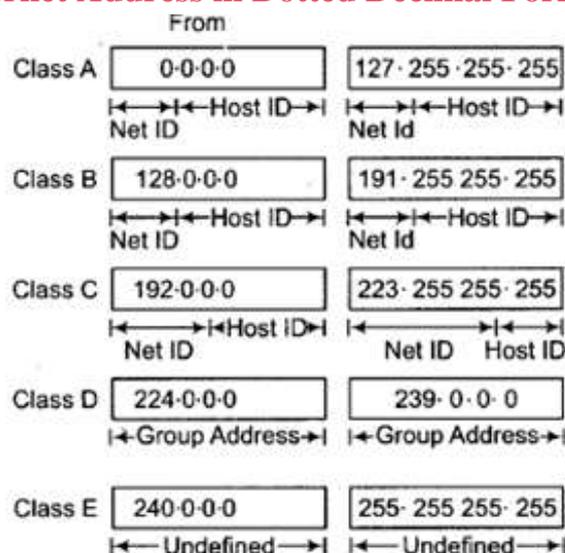
For Class B: First 2 bits of Net ID should be 1 and 0 respectively, as in below pattern 10011101 . 10001111 . 11111100 . 11001111

For Class C: First 3 bits Net ID should be 1, 1 and 0 respectively, as follows 11011101 . 10001111 . 11111100 . 11001111

For Class D: First 4 bits should be 1110 respectively, as in pattern 11101011 . 10001111 . 11111100 . 11001111

For Class E: First 4 bits should be 1111 respectively, like 11110101 . 10001111 . 11111100 . 11001111

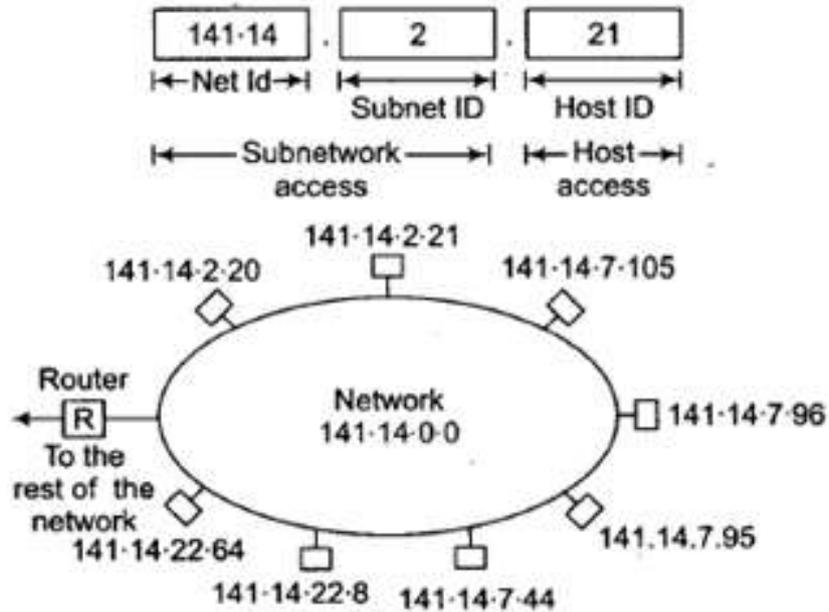
Class Ranges of Internet Address in Dotted Decimal Format



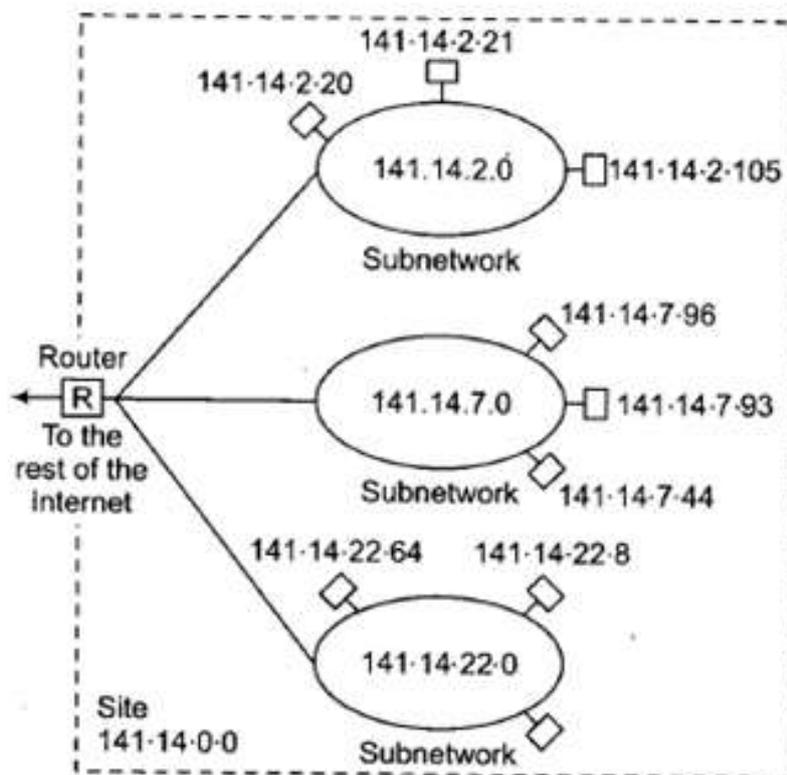
IBPS SO 2021 MAINS
Special Course (AFO)

START FREE TRIAL

Three Levels of Hierarchy: Adding subnetworks creates an intermediate level of hierarchy in the IP addressing system. Now, we have three levels: net ID; subnet ID and host ID. e.g.,



A network with two level of hierarchy (not subnetted)



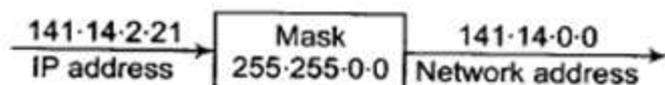
A network with three level of hierarchy (subnetted)



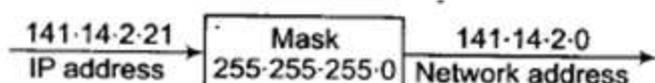
Masking

Masking is process that extracts the address of the physical network form an IP address. Masking can be done whether we have subnetting or not. If we have not subnetted the network, masking extracts the network address form an IP address. If we have subnetted, masking extracts the subnetwork address form an IP address.

Masks without Subnetting: To be compatible, routers use mask even, if there is no subnetting.



Masks with Subnetting: When there is subnetting, the masks can vary



Masks for Unsubnetted Networks

Class	Mask	Address	Network
A	255.0.0.0	15.32.56.7	15.0.0.0
B	255.255.0.0	135.67.13.9	135.67.0.0
C	255.255.255.0	301.34.12.72	201.34.12.0
D	N/A	N/A	N/A
E	N/A	N/A	N/A

Masks for Subnetted Networks

Class	Mask	Address (Example)	Network Address
A	255.255.0.0	15.32.567	15.32.0.0
B	255.255.255.0	135.67.13.9	135.67.13.0
C	255.255.255.192	201.34.12.72	201.34.12.0
D	N/A	N/A	N/A
E	N/A	N/A	N/A

Types of Masking

There are two types of masking as given below

Boundary Level Masking :

If the masking is at the boundary level (the mask numbers are either 255 or 0), finding the subnetwork address is very easy. Follow these 2 rules

- The bytes in IP address that corresponds to 255 in the mask will be repeated in the subnetwork address.
- The bytes in IP address that corresponds to 0 in the mask will change to 0 in the subnetwork address.

e.g.,

IP address	45 . 23 . 21 . 8
Mask	255 . 255 . 0 . 0
Subnetwork address	45 . 23 . 0 . 0



IBPS SO 2021 MAINS
Special Course (AFO)

START FREE TRIAL

Non-boundary Level Masking :

If the masking is not at the boundary level (the mask numbers are not just 255 or 0), finding subnetwork address involves using the bit-wise AND operator, follow these 3 rules

- The bytes in IP address that corresponds to 255 in the mask will be repeated in the subnetwork address.
- The bytes in the IP address that correspond to 0 in the mask will be changed to 0 in the subnetwork address.
- For other bytes, use the bit-wise AND operator

e.g.,

IP address	213 . 23 . 47 . 37
Mask	<u>255 . 255 . 255 . 240</u>
Subnetwork address	213 . 23 . 47 . 32

As we can see, 3 bytes are easy to determine. However, the 4th bytes needs the bit-wise AND operation.

Router :

A **router** is a hardware component used to interconnect networks. Routers are devices whose primary purpose is to connect two or more networks and to filter network signals so that only desired information travels between them. Routers are much more powerful than bridges.

- A router has interfaces on multiple networks
- Networks can use different technologies
- The router forwards packets between networks
- Transforms packets as necessary to meet standards for each network
- Routers are distinguished by the functions they perform:
 - **Internal routers:** Only route packets within one area.
 - **Area border routers:** Connect to areas together
 - **Backbone routers:** Reside only in the backbone area
 - **AS boundary routers:** Routers that connect to a router outside the AS.

Routers can filter traffic so that only authorized personnel can enter restricted areas. They can permit or deny network communications with a particular Web site. They can recommend the best route for information to travel. As network traffic changes during the day, routers can redirect information to take less congested routes.

- Routers operate primarily by examining incoming data for its network routing and transport information.
- Based on complex, internal tables of network information that it compiles, a router then determines whether or not it knows how to forward the data packet towards its destination.
- Routers can be programmed to prevent information from being sent to or received from certain networks or computers based on all or part of their network routing addresses.
- Routers also determine some possible routes to the destination network and then choose the one that promises to be the fastest.



Two key router functions of Router:

- Run routing algorithms/protocol (RIP, OSPF, BGP)
- Forwarding datagrams from incoming to outgoing link.

Address Resolution Protocol (ARP)

ARP is used to find the physical address of the node when its Internet address is known. Anytime, a host or a router needs to find the physical address of another has on its network; it formats an ARP query packet that includes that IP address and broadcasts it over the network. Every host on the network receives and processes the ARP packet, but the intended recipient recognizes its Internet address and sends back its physical address.

Reverse Address Resolution Protocol (RARP)

This protocol allows a host to discover its Internet address when it knew only its physical address. RARP works much like ARP. The host wishing to retrieve its Internet address broadcasts a RARP query packet that contains its physical address to every host of its physical network. A server on the network recognizes the RARP packet and returns the host's Internet address.

Internet Control Message Protocol (ICMP)

The ICMP is a mechanism used by hosts and routers to send notifications of datagram problems back to the sender. IP is essentially an unreliable and connectionless protocol. ICMP allows IP (Internet Protocol) to inform a sender if a datagram is undeliverable.

ICMP uses each test/reply to test whether a destination is reachable and responding. It also handles both control and error messages but its sole function is to report problems not correct them.

Internet Group Message Protocol (IGMP)

The IP can be involved in two types of communication unitasking and multitasking. The IGMP protocol has been designed to help a multitasking router to identify the hosts in a LAN that are members of a multicast group.

Addressing at Network Layer

In addition to the physical addresses that identify individual devices, the Internet requires an additional addressing connection to an address that identifies the connection of a host of its network. Every host and router on the Internet has an IP address which encodes its network number and host number. The combination is unique in principle; no 2 machines on the Internet have the same IP address.

Firewall

A firewall is a device that prevents unauthorized electronic access to your entire network.

The term firewall is generic and includes many different kinds of protective hardware and software devices. Routers comprise one kind of firewall.

Most firewalls operate by examining incoming or outgoing packets for information at OSI level 3, the network addressing level.

Firewalls can be divided into 3 general categories: packet-screening firewalls, proxy servers (or application-level gateways), and stateful inspection proxies.



IBPS SO 2021 MAINS
Special Course (AFO)

START FREE TRIAL

- **Packet-screening firewalls** examine incoming and outgoing packets for their network address information. You can use packet-screening firewalls to restrict access to specific Websites or to permit access to your network only from specific Internet sites.
- **Proxy servers** (also called application-level gateways) operate by examining incoming or outgoing packets not only for their source or destination addresses but also for information carried within the data area (as opposed to the address area) of each network packet. The data area contains information written by the application program that created the packet—for example, your Web browser, FTP, or TELNET program. Because the proxy server knows how to examine this application-specific portion of the packet, you can permit or restrict the behavior of individual programs.
- Stateful inspection proxies monitor network signals to ensure that they are part of a legitimate ongoing conversation (rather than malicious insertions)

Transport Layer Protocols: There are two transport layer protocols as given below.

UDP (User Datagram Protocol)

UDP is a connectionless protocol. UDP provides a way for application to send encapsulate IP datagram and send them without having to establish a connection.

- Datagram oriented
- unreliable, connectionless
- simple
- unicast and multicast
- Useful only for few applications, e.g., multimedia applications
- Used a lot for services: Network management (SNMP), routing (RIP), naming (DNS), etc.

UDP transmitted segments consisting of an 8 byte header followed by the payload. The two parts serve to identify the endpoints within the source and destination machine. When UDP packets arrives, its payload is handed to the process attached to the destination ports.

- **Source Port Address (16 Bits)**

The total length of the User Datagram (16 Bits)

- **Destination Port Address (16 Bits)**

Checksum (used for error detection) (16 Bits)

TCP (Transmission Control Protocol)

TCP provides full transport layer services to applications. TCP is a reliable stream transport port-to-port protocol. The term stream in this context means connection-oriented, a connection must be established between both ends of transmission before either may transmit data. By creating this connection, TCP generates a virtual circuit between the sender and receiver that is active for the duration of the transmission.

TCP is a reliable, point-to-point, connection-oriented, full-duplex protocol.



IBPS SO 2021 MAINS
Special Course (AFO)

START FREE TRIAL

Source port address 16 Bits		Destination port address 16 Bits						
Sequence number (32 Bits)								
Acknowledgement Number (32 Bits)								
HLEN 4 Bits	Reserved 6 Bits	U	A	P	R	S	F	Window size 16 Bits
		R	C	S	S	Y	I	
		G	K	H	T	N	N	
Checksum 16 Bits				Urgent Pointer 16 Bits				
Options and Padding								

Flag bits

- URG: Urgent pointer is valid If the bit is set, the following bytes contain an urgent message in the sequence number range “SeqNo <= urgent message <= SeqNo + urgent pointer”
- ACK: Segment carries a valid acknowledgement
- PSH: PUSH Flag, Notification from sender to the receiver that the receiver should pass all data that it has to the application. Normally set by sender when the sender’s buffer is empty
- RST: Reset the connection, The flag causes the receiver to reset the connection. Receiver of a RST terminates the connection and indicates higher layer application about the reset
- SYN: Synchronize sequence numbers, Sent in the first packet when initiating a connection
- FIN: Sender is finished with sending. Used for closing a connection, and both sides of a connection must send a FIN.

TCP segment format

Each machine supporting TCP has a TCP transport entity either a library procedure, a user process or port of kernel. In all cases, it manages TCP streams and interfaces to the IP layer. A TCP entities accepts the user data stream from local processes, breaks them up into pieces not exceeding 64 K bytes and sends each piece as separate IP datagrams.

Sockets

A socket is one end of an inter-process communication channel. The two processes each establish their own socket. The system calls for establishing a connection are somewhat different for the client and the server, but both involve the basic construct of a *socket*.

The steps involved in establishing a socket on the *client* side are as follows:

1. Create a socket with the socket() system call
2. Connect the socket to the address of the server using the connect() system call
3. Send and receive data. There are a number of ways to do this, but the simplest is to use the read() and write() system calls.



The steps involved in establishing a socket on the server side are as follows:

1. Create a socket with the `socket()` system call
2. Bind the socket to an address using the `bind()` system call. For a server socket on the Internet, an address consists of a port number on the host machine.
3. Listen for connections with the `listen()` system call
4. Accept a connection with the `accept()` system call. This call typically blocks until a client connects with the server.
5. Send and receive data

When a socket is created, the program has to specify the address domain and the socket type.

Socket Types

There are two widely used socket types, stream sockets, and datagram sockets.

Stream sockets treat communications as a continuous stream of characters, while datagram sockets have to read entire messages at once. Each uses its own communications protocol. Stream sockets use TCP (Transmission Control Protocol), which is a reliable, stream oriented protocol, and datagram sockets use UDP (Unix Datagram Protocol), which is unreliable and message oriented. A second type of connection is a datagram socket. You might want to use a datagram socket in cases where there is only one message being sent from the client to the server, and only one message being sent back. There are several differences between a datagram socket and a stream socket.

1. Datagrams are unreliable, which means that if a packet of information gets lost somewhere in the Internet, the sender is not told (and of course the receiver does not know about the existence of the message). In contrast, with a stream socket, the underlying TCP protocol will detect that a message was lost because it was not acknowledged, and it will be retransmitted without the process at either end knowing about this.
2. Message boundaries are preserved in datagram sockets. If the sender sends a datagram of 100 bytes, the receiver must read all 100 bytes at once. This can be contrasted with a stream socket, where if the sender wrote a 100 byte message, the receiver could read it in two chunks of 50 bytes or 100 chunks of one byte.
3. The communication is done using special system calls `sendto()` and `recvfrom()` rather than the more generic `read()` and `write()`.
4. There is a lot less overhead associated with a datagram socket because connections do not need to be established and broken down, and packets do not need to be acknowledged. This is why datagram sockets are often used when the service to be provided is short, such as a time-of-day service.

Application Layer Protocols (DNS, SMTP, POP, FTP, HTTP)

There are various application layer protocols as given below

- **SMTP (Simple Mail Transfer Protocol):** One of the most popular network service is electronic mail (e-mail). The TCP/IP protocol that supports electronic mail on the Internet is called Simple Mail Transfer Protocol (SMTP). SMTP is system for sending



IBPS SO 2021 MAINS
Special Course (AFO)

START FREE TRIAL

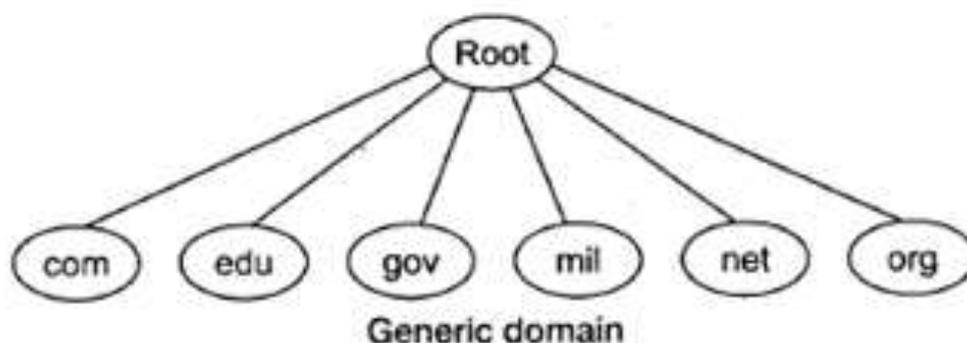
messages to other computer. Users based on e-mail addresses. SMTP provides services for mail exchange between users on the same or different computers.

- **TELNET (Terminal Network):** TELNET is client-server application that allows a user to log onto remote machine and lets the user to access any application program on a remote computer. TELNET uses the NVT (Network Virtual Terminal) system to encode characters on the local system. On the server (remote) machine, NVT decodes the characters to a form acceptable to the remote machine.
- **FTP (File Transfer Protocol):** FTP is the standard mechanism provided by TCP/IP for copying a file from one host to another. FTP differs from other client-server applications because it establishes 2 connections between hosts. One connection is used for data transfer, the other for control information (commands and responses).
- **Multipurpose Internet Mail Extensions (MIME):** It is an extension of SMTP that allows the transfer of multimedia messages.
- **POP (Post Office Protocol):** This is a protocol used by a mail server in conjunction with SMTP to receive and holds mail for hosts.
- **HTTP (Hypertext Transfer Protocol):** This is a protocol used mainly to access data on the World Wide Web (www), a repository of information spread all over the world and linked together. The HTTP protocol transfer data in the form of plain text, hyper text, audio, video and so on.
- **Domain Name System (DNS):** To identify an entity, TCP/IP protocol uses the IP address which uniquely identifies the connection of a host to the Internet. However, people refer to use names instead of address. Therefore, we need a system that can map a name to an address and conversely an address to name. In TCP/IP, this is the domain name system.

DNS in the Internet

DNS is protocol that can be used in different platforms. Domain name space is divided into three categories.

- **Generic Domain:** The generic domain defines registered hosts according, to their generic behaviour. Each node in the tree defines a domain which is an index to the domain name space database.



IBPS SO 2021 MAINS
Special Course (AFO)

START FREE TRIAL

- **Country Domain:** The country domain section follows the same format as the generic domain but uses 2 characters country abbreviations (e.g., US for United States) in place of 3 characters.
- **Inverse Domain:** The inverse domain is used to map an address to a name.

Overview of Services

Service	Type	Direction
DNS	UDP	Out
HTTP/HTTPS	TCP	Out
FTP	TCP/UDP	Out
TELNET	TCP/UDP	Out
POP3	TCP	Out
SMTP	TCP	Out
IRCU	TCP/UDP	Out
IDENT	TCP	In
Private File Service	TCP/UDP	In/Out
NNTP	TCP/UDP	Out
NTP	TCP/UDP	Out
Remote Desktop	TCP/UDP	In/Out

Network Security : As millions of ordinary citizens are using networks for banking, shopping, and filing their tax returns, network security is looming on the horizon as a potentially massive problem.

Network security problems can be divided roughly into four intertwined areas:

1. **Secrecy:** keep information out of the hands of unauthorized users.
2. **Authentication:** deal with determining whom you are talking to before revealing sensitive information or entering into a business deal.
3. **Nonrepudiation:** deal with signatures.
4. **Integrity control:** how can you be sure that a message you received was really the one sent and not something that a malicious adversary modified in transit or concocted?

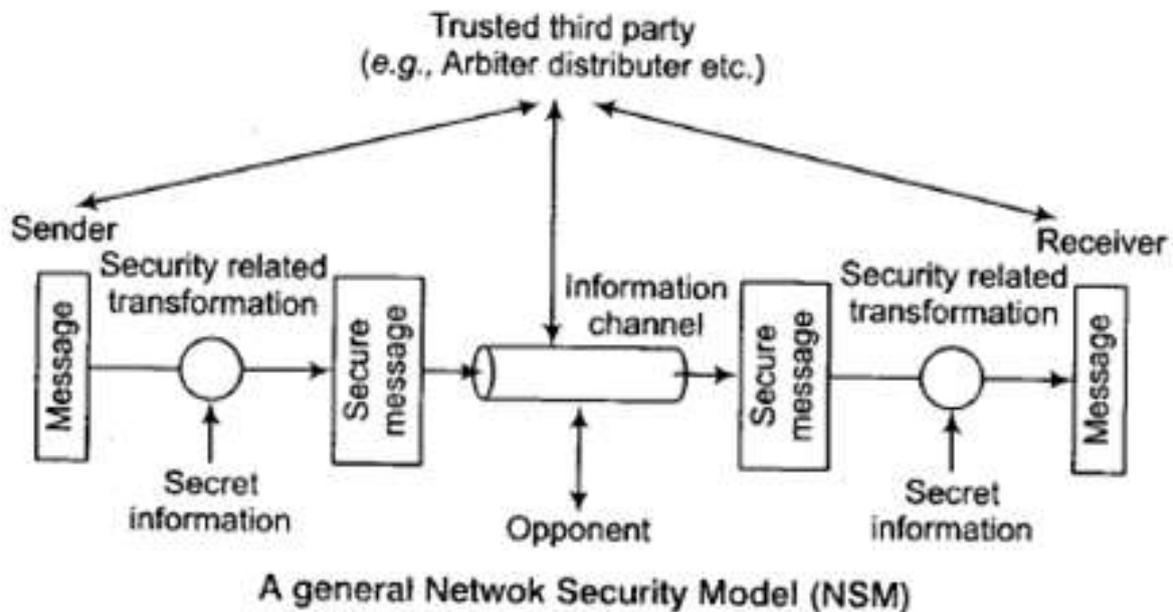
There is no one single place -- every layer has something to contribute :

- In the physical layer, wiretapping can be foiled by enclosing transmission lines in sealed tubes containing argon gas at high pressure. Any attempt to drill into a tube will release some gas, reducing the pressure and triggering an alarm (used in some military systems).
- In the data link layer, packets on a point-to-point line can be encoded.
- In the network layer, firewalls can be installed to keep packets in/out.
- In the transport layer, entire connection can be encrypted.

IBPS SO 2021 MAINS
Special Course (AFO)
START FREE TRIAL

Model for Network Security

Network security starts with authenticating, commonly with a username and password since, this requires just one detail authenticating the username i.e., the password this is some times teamed one factor authentication.



Using this model require us to

- Design a suitable algorithm for the security transformation.
- Generate the secret in formations (keys) used by the algorithm.
- Develop methods to distribute and share the secret information.
- Specify a protocol enabling the principles to use the transformation and secret information for security service.

Cryptography

It is a science of converting a stream of text into coded form in such a way that only the sender and receiver of the coded text can decode the text. Nowadays, computer use requires automated tools to protect files and other stored information. Uses of network and communication links require measures to protect data during transmission.

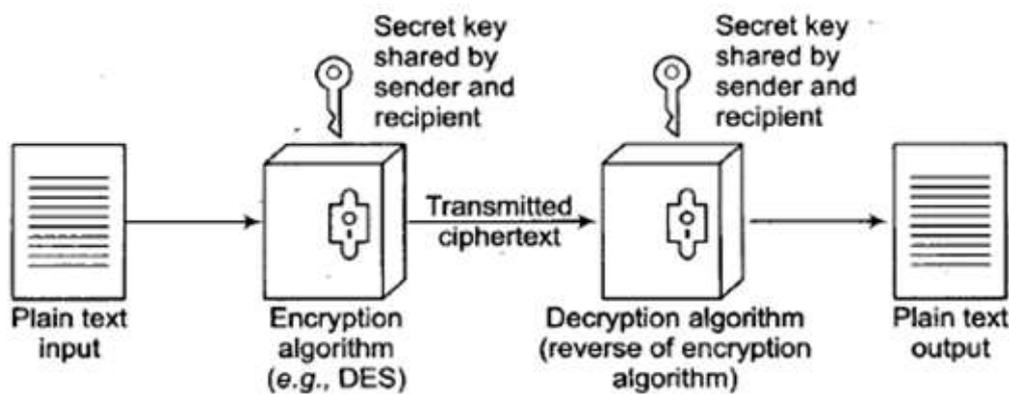
Symmetric / Private Key Cryptography (Conventional / Private key / Single key)

Symmetric key algorithms are a class of algorithms to cryptography that use the same cryptographic key for both encryption of plaintext and decryption of ciphertext. The may be identical or there may be a simple transformation to go between the two keys.

In symmetric private key cryptography the following key features are involved

- Sender and recipient share a common key.
- It was only prior to invention of public key in 1970.
- If this shared key is disclosed to opponent, communications are compromised.
- Hence, does not protect sender form receiver forging a message and claiming is sent by user.





Symmetric cipher model (used in symmetric encryption)

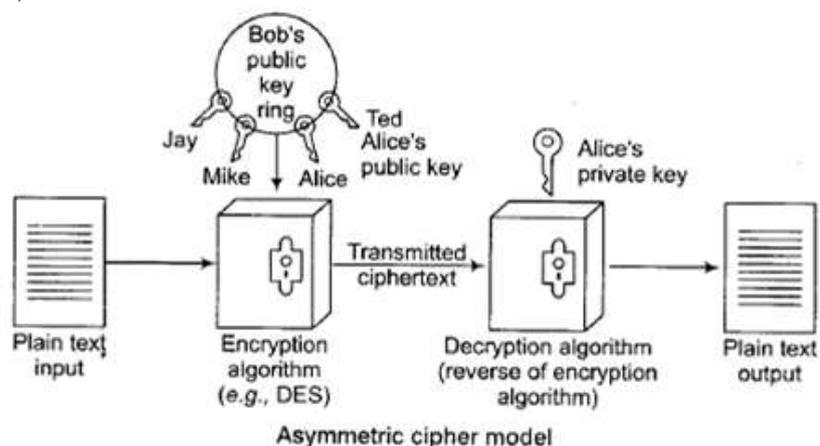
Advantage of Secret key Algorithm: Secret Key algorithms are efficient: it takes less time to encrypt a message. The reason is that the key is usually smaller. So it is used to encrypt or decrypt long messages.

Disadvantages of Secret key Algorithm: Each pair of users must have a secret key. If N people in world want to use this method, there needs to be $N(N-1)/2$ secret keys. For one million people to communicate, a half-billion secret keys are needed. The distribution of the keys between two parties can be difficult.

Asymmetric / Public Key Cryptography

A public key cryptography refers to a cryptographic system requiring two separate keys, one of which is secret/private and one of which is public although different, the two parts of the key pair are mathematically linked.

- **Public Key:** A public key, which may be known by anybody and can be used to encrypt messages and verify signatures.
- **Private Key:** A private key, known only to the recipient, used to decrypt messages and sign (create) signatures. It is symmetric because those who encrypt messages or verify signature cannot decrypt messages or create signatures. It is computationally infeasible to find decryption key knowing only algorithm and encryption key. Either of the two related keys can be used for encryption, with the other used for decryption (in some schemes).



IBPS SO 2021 MAINS
Special Course (AFO)

START FREE TRIAL

In the above public key cryptography mode

- Bob encrypts a plaintext message using Alice's public key using encryption algorithm and sends it over communication channel.
- On the receiving end side, only Alice can decrypt this text as she only is having Alice's private key.

Advantages of Public key Algorithm:

1. Remove the restriction of a shared secret key between two entities. Here each entity can create a pair of keys, keep the private one, and publicly distribute the other one.
2. The no. of keys needed is reduced tremendously. For one million users to communicate, only two million keys are needed.

Disadvantage of Public key Algorithm: If you use large numbers the method to be effective. Calculating the cipher text using the long keys takes a lot of time. So it is not recommended for large amounts of text.

Message Authentication Codes (MAC)

In cryptography, a Message Authentication Code (MAC) is a short piece of information used to authenticate a message and to provide integrity and authenticity assurance on the message. Integrity assurance detects accidental and intentional message changes, while authenticity assurance affirms the message's origin.

A keyed function of a message sender of a message m computes $MAC(m)$ and appends it to the message.

- **Verification** : The receiver also computes $MAC(m)$ and compares it to the received value.
- **Security of MAC** : An attacker should not be able to generate a valid $(m, MAC(m))$, even after seeing many valid messages MAC pairs, possible of his choice.
- **MAC from a Block Cipher**

MAC from a block cipher can be obtained by using the following suggestions

- Divide a message into blocks.
- Compute a checksum by adding (or xoring) them.
- Encrypt the checksum.
- MAC keys are symmetric. Hence, does not provide non-repudiation (unlike digital signatures).
- MAC function does not need to be invertible.
- A MACed message is not necessarily encrypted.

DES (Data Encryption Standard)

- The data encryption standard was developed in IBM.
- DES is a symmetric key crypto system.
- It has a 56 bit key.
- It is **block cipher**, encrypts 64 bit plain text to 64 bit cipher texts.
- Symmetric cipher: uses same key for encryption and decryption
- It Uses 16 rounds which all perform the identical operation.
- Different subkey in each round derived from main key



IBPS SO 2021 MAINS
Special Course (AFO)

START FREE TRIAL

- Depends on 4 functions: Expansion E, XOR with round key, S-box substitution, and Permutation.
- DES results in a **permutation** among the 2^{64} possible arrangements of 64 bits, each of which may be either 0 or 1. Each block of 64 bits is divided into two blocks of 32 bits each, a left half block **L** and a right half **R**. (This division is only used in certain operations.)

DES is a block cypher: meaning it operates on plaintext blocks of a given size (64-bits) and returns cipher text blocks of the same size. Thus DES results in a **permutation** among the 2^{64} possible arrangements of 64 bits, each of which may be either 0 or 1. Each block of 64 bits is divided into two blocks of 32 bits each, a left half block **L** and a right half **R**. (This division is only used in certain operations.)

Authentication Protocols

Authentication: It is the technique by which a process verifies that its communication partner is who it is supposed to be and not an imposter. Verifying the identity of a remote process in the face of a malicious, active intruder is surprisingly difficult and requires complex protocols based on cryptography.

The general model that all authentication protocols use is the following:

- An initiating user A (*for Alice*) wants to establish a secure connection with a second user B (*for Bob*). Both are sometimes called principals.
- Starts out by sending a message either to, or to a trusted **key distribution center (KDC)**, which is always honest. Several other message exchanges follow in various directions.
- As these messages are being sent, a nasty intruder, T (for Trudy), may intercept, modify, or replay them in order to trick and When the protocol has been completed, is sure she is talking to and is sure he is talking to. Furthermore, in most cases, the two of them will also have established a secret **session key** for use in the upcoming conversation.

In practice, for performance reasons, all data traffic is encrypted using secret-key cryptography, although public-key cryptography is widely used for the authentication protocols themselves and for establishing the (secret) session key.

Authentication based on a shared Secret key

Assumption: and share a secret key, agreed upon in person or by phone.

This protocol is based on a principle found in many (**challenge-response**) authentication protocols: one party sends a random number to the other, who then transforms it in a special way and then returns the result.

Three general rules that often help are as follows:

1. Have the initiator prove who she is before the responder has to.
2. Have the initiator and responder use different keys for proof, even if this means having two shared keys, and.
3. Have the initiator and responder draw their challenges from different sets.



Authentication using Public-key Cryptography

Assume that and already know each other's public keys (a nontrivial issue).

Digital Signatures: For computerized message systems to replace the physical transport of paper and documents, a way must be found to send a “signed” message in such a way that

- The receiver can verify the claimed identity of the sender.
- The sender cannot later repudiate the message.
- The receiver cannot possibly have concocted the message himself.

Secret-key Signatures: Assume there is a central authority, Big Brother (BB), that knows everything and whom everyone trusts.

If later denies sending the message, how could prove that indeed sent the message?

- First points out that will not accept a message unless it is encrypted.
- Then produces, and says this is a message signed by which proves sent to.
- is asked to decrypt, and testify that is telling the truth.

What happens if replays either message?

- can check all recent messages to see if was used in any of them (in the past hour).
- The timestamp is used throughout, so that very old messages will be rejected based on the timestamp.

Public-key Signatures: It would be nice if signing documents did not require a trusted authority (e.g., governments, banks, or lawyers, which do not inspire total confidence in all citizens).

Under this condition,

- sends a signed message to by transmitting.
- When receives the message, he applies his secret key to get , and saves it in a safe place, then applies the public key to get it.
- How to verify that indeed sent a message to?
- Produces both and The judge can easily verify that indeed has a valid message encrypted by simply applying to it. Since is private, the only way could have acquired a message encrypted by it is if did indeed send it.

Another new standard is the **Digital Signature Standard (DSS)** based on the El Gamal public-key algorithm, which gets its security from the difficulty of computing discrete logarithms, rather than factoring large numbers.

Message Digest

- It is easy to compute.
- No one can generate two messages that have the same message digest.
- To sign a plaintext, first computes, and performs, and then sends both and to.
- When everything arrives, applies the public key to the signature part to yield, and applies the well-known to see if the so computed agrees with what was received (in order to reject the forged message).

