A Handbook on
Computer Science

11

Computer Networks

CONTENTS

ISO/OSI Stack, LAN Technologies (Ethernet, Token Ring)

1

OSI Model

- Open Systems Interconnection Reference Model, developed in 1984 by the International Standards Organization (ISO).
- It is a way of sub-dividing a communications system into smaller parts called layers.
- A layer is a collection of conceptually similar functions that provide services to the layer above it and receives services from the layer below it.
- Provides a set of design standards for equipment manufacturers so they can communicate with each other. It is basic guideline for protocol development.

1. Physical Layer

- Conveys the bit stream through the network at the electrical and mechanical level.
- Defines physical means of moving data over network devices.
- Interfaces between network medium and devices.
- Defines optical, electric and mechanical characteristics: voltage levels, timing of voltage changes, physical data rates, transmission distances and physical connection.

2. Data Link Layer

- Takes a string of bits and delivers it across a link.
- Conveys the bit stream through the network at the electrical and mechanical level (i.e., Layer 1).
- Turns packets into raw bits and bits into packets.

Framing and Error detection :

(*i*) Break the bit stream up into frames.

(*ii*) Compute an error-detection code.

(*iii*) Transmit each frame separately.

3. Network Layer

- Translates logical network address and names to their physical address (e.g., device name to MAC address).
- **Responsible for :**
  - (*i*) Addressing.
  - (*ii*) Determining routes for sending.
  - (*iii*) Managing network problems such as packet switching, data congestion and routing.
- Breaks the data into smaller unit and assembles data.
- Shields higher layers from details of how the data gets to its destination.

4. Transport Layer

- Divides streams of data into chucks or packets
- Reassembles the message from packets
- Provide error-checking to guarantee error-free data delivery, with no losses or duplications.
- Provides acknowledgment of successful transmissions.
- Requests retransmission if some packets don't arrive error-free.
- Provides flow control and error-handling.

5. Session Layer

- Establishes, maintains and ends sessions across the network.
- Responsible for name recognition (identification) so only the designated parties can participate in the session.
- Provides synchronization services by planning check points in the data stream.
- If session fails, only data after the most recent checkpoint need be transmitted.
- Manages who can transmit data at a certain time and for how long.

6. Presentation

- Translates from application to network format and vice-versa.

- All different formats from all sources are made into a common uniform format that the rest of the OSI can understand.
- Responsible for protocol conversion, character conversions, data encryption/decryption, expanding graphics commands and data compression.
- Sets standards for different systems to provide seamless communication from multiple protocol stacks.

7. Application Layer

- Used for applications specially written to run over the network.
- Allows access to network services that support applications.
- Directly represents the services that directly support user applications (e.g., file transfer and email).
- What the user sees or does.

PROTOCOLS	
Application	NNTP, SIP, SSI, DNS, FTP, Gopher, HTTP, NFS, NTP, SMPP, SMTP, DHCP, SNMP, Telnet, Netconf
Presentation	MIME, XDR, TLS, SSL
Session	Named Pipes, NetBIOS, SAP, SIP, L2TP, PPTP
Transport	TCP, UDP, SCTP, DCCP
Network	IP (IPv4, IPv6), ICMP, IPsec, IGMP, IPX, AppleTalk
Data Link	ATM, SDLC, HDLC, ARP, CSLIP, SLIP, PLIP, IEEE 802.3, Frame Relay, ITU-T G.hn DLL, PPP, X.25
Physical	EIA/TIA-232, EIA/TIA-449, ITU-T V-Series, I.430, I.431, POTS, PDH, SONET/SDH, PON, OTN, DSL, IEEE 802.3 IEEE 802.11, IEEE 802.15, IEEE 802.16, IEEE 1394, ITU-T G.hn PHY, USB, Bluetooth

Token Ring (IEEE 802.5)

- **Characteristics of Token Ring**
  - (*i*) It offers connectionless communication.
  - (*ii*) It uses ring topology.
  - (*iii*) It uses token passing as an access control method.
  - (*iv*) There are no collisions, priorities are possible, offers deterministic service.

- **Token Holding Time (THT):**
  (*i*) The maximum time a token frame can be with held by a station, by default it is set to 10 msecs.
  (*ii*) No station can keep the token beyond THT (It solves monopolization problem)
- **Monitor:**
  (*i*) The station with highest priority/MAC address and which generates the token frame is called monitor.
  (*ii*) Monitor maintains Minimum TRT and Maximum TRT.

  Min TRT = Propagation delay + (Number of stations × Delay at each station)

  Max TRT = Propagation delay + (Number of stations × THT)
- **Frame format of 802.5:**
  (*i*) To bypass a faulty station two data rates are there
    (a) 4 Mbps (minimum ring length of 1200 meters)
    (b) 16 Mbps (minimum ring length of 300 meters)
  (*ii*) Frame format of 802.5
    (a) Data Frame

SD	AC	FC	DA	SA	Data	CRC	ED	FS
Bytes (1)	(1)	(1)	(2/6)	(1)	(0-4500)	(4)	(1)	(1)

Starting Delimiter (SD): JK0JK000 [J&K are non data symbols]

Access Control (AC): PPPTMRRR $\begin{bmatrix} T = 1 \text{ for data} \\ = 0 \text{ for token} \end{bmatrix}$

Ending Delimeter (ED): JK1JK1IE [I = Intermediate frame Indication, E = Error detection bit]

Frame Status (FS): ACrrACrr [r = unused bit]

A (Destination)	*C* (Frame Acceptance)
0	0 → Destination not present and frame not accepted
0	1 → Not posible
1	0 → Destination present and frame not accepted
1	1 → Destination present and frame accepted

(b) Token Frame

SD	AC	ED
(1)	(1)	(1)

(c) Abort Frame

SD	ED
(1)	(1)

- **Ring Latency (RL):** Time taken for a bit to travel around ring.

$$RL = \frac{d}{v} + \frac{Mb}{R} \text{ (seconds)} = \frac{dR}{v} + Mb \text{ (bits)}$$

where d : Length of link (meters), v : Velocity (m/s),
M : Number of station, R : Data rate of link (bps)

- Data transfer rate $= \dfrac{f}{t_1 + t_2 + \dfrac{f}{B}}$;

where f : Frame length, B : Channel capacity or bandwidth,
t_1 : Ring latency time, t_2 : token observing time

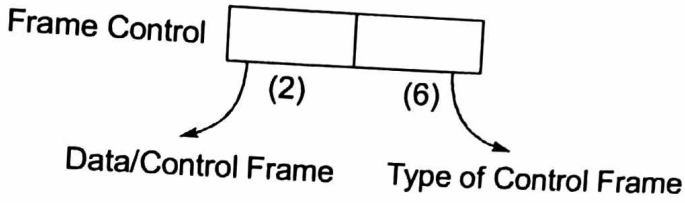
- Length of link (in bits) $= R \times \dfrac{d}{v}$

$$\text{Utilization} = \frac{T_1}{T_1 + T_2} = \frac{1}{1 + \dfrac{a}{N}}; \text{ if } a < 1$$

$$= \frac{1}{a\left(1 + \dfrac{1}{N}\right)}; \text{ if } a > 1$$

where T_1 : Average time to transmit a data frame
T_2 : Average time to pass a token
N : Number of stations

- **For minimum Token Size:** Propagation delay = Transmission delay
- **Types of Control Frame:**
  - (*i*) **Becon Frame:** (000010) to find major faults in ring
  - (*ii*) **Claim Token:** (000011) used in election process of monitor
  - (*iii*) **Purge:** (000100) used to clear unwanted signals
  - (*iv*) **Active monitor present:** (000101) to inform all the stations that monitor is alive
  - (*v*) **Stand by monitor present:** (000110) to carryout neighbour identification process
  - (*vi*) **Duplicate address test:** (000000) For virtual PC, physical address may change



Delay Token Ring Reinsertion Strategy (DTR)	Early Token Ring Reinsertion Strategy (ETR)
(a) Token is reinserted after getting the entire data packet (b) Efficiency is low and always only one packet is available on the link (c) Reliability is high. THT = 10 ms (d) It is used under no load conditions (e) Cycle time = $a + b + c + d$	(a) Token is reinserted as soon as data transmission is over (b) Efficiency is high and many packets can be available on the link (c) Reliability is low, no meaning of THT (d) It is used under high load conditions (e) Cycle time = $a + c + d$ a : Packet transmission time b : Ring latency c : Token transmission d : Propagation delay between stations

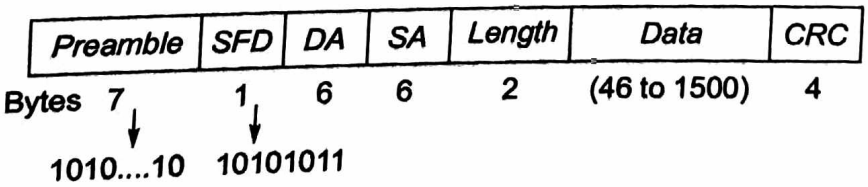
Ethernet (IEEE 802.3)

- **Characteristics of Ethernet:**
  - (*i*) It offers connectionless communication
  - (*ii*) No acknowledgment, no flow and error control
  - (*iii*) It uses bus topologies for its operation
  - (*iv*) It uses CSMA/CD as accessing technology

  Maximum duration for contention slot = 2 × Propagation delay

  $$\text{Contention Period} = \frac{2 \times \text{Propagation delay}}{A}; A = 1/e$$

- **Frame Format:**



Minimum Ethernet Frame Size:

$DA + SA$ + Length + Data (min) + CRC

= 6 + 6 + 2 + 46 + 4 bytes = 64 bytes

Maximum Ethernet Frame Size:

$DA + SA$ + Length + Data (max) + CRC

= 6 + 6 + 2 + 1500 + 4 bytes = 1518 bytes

- Channel efficiency (utilization η) $= \dfrac{1}{1+\dfrac{2BLe}{vf}} = \dfrac{1}{1+5.44a}$

$$a = \frac{\text{Propagation delay}}{\text{Transmission delay}} = \frac{d/v}{f/B}$$

If length of packet increases η also increases

where f: Frame length, v: Speed of signal propagation

e: Contention slots/frame, L: Cable Length (d)

B: Network bandwidth, a: Propagation delay

$2T$: Duration of each slot = 2 × propagation delay

A: Slot probability = $(1/e)$

- The probability of one station succeeding in putting its traffic on a network of 'n' stations is given as $nP(1-P)^{n-1}$
- **CSMA/CD for ethernet:**

$$\text{Utilization } \eta = \frac{1}{1+6.44a}\left[\begin{matrix}\text{used when ack information}\\ \text{is not provided}\end{matrix}\right]$$

$$C.P. = \text{Number of slots} \times \text{Slot duration} = e \times 2 \times (d/v)$$

$$\text{Utilization} = \frac{T.P.}{T.P.+C.P.} = \frac{\left(\frac{1}{2a}\right)}{\left(\frac{1}{2a}\right)+\left(\frac{1-A}{A}\right)}$$

where, $\dfrac{1}{2a}$ = Transmision Interval

$\dfrac{1-A}{A}$ = Contention Interval

$A = \left(1-\dfrac{1}{N}\right)^{N-1}$; N = Number of stations

Flow Control

- The procedures to be followed by the transmitter sender and receiver for efficient transmission and reception is called as flow control.
- **Two approaches** < **Stop and wait – Error control (stop and wait ARQ)**; **Sliding Window Protocol (SWP)**

Stop and Wait ARQ

- Only one frame at a time on the link ⇒ poor utilization ⇒ poor efficiency
- Efficiency $\eta = \dfrac{t_{transmit}}{(t_{transmit}) + (2\, t_{propagation})}$

$$= \frac{f/B}{f/B + RTT} = \frac{1}{1+2a} \quad \left[\because \quad a = \frac{t_{propagation}}{t_{transmission}}\right]$$

- It is an example of closed loop control protocol.
- Positive ACKs are numbered in Stop and Wait.
  Negative ACKs are not numbered
- **Throughput = 1 window/RTT = 1 Packet/RTT**
- It is a **special category of SWP** of window size = 1

Go-back N (GBN) ARQ

- Receiver window size (RWS) = 1
- Sender window size (SWS) = $2^K - 1$ where, K is number of bits received for window size in the header.
- Efficiency = $(2^K - 1) \times \dfrac{t_{transmission}}{t_{transmission} + RTT}$
- $W_S + W_R \leq$ ASN (Available Sequence Number)
- Uses cumulative/Piggybacking acknowledgments
- GBN is called as "conservating protocol".

Selective Repeat (SR)

- $W_S = W_R = \dfrac{N}{2}$; $N \rightarrow$ maximum ASN (2^K)
- It uses piggybacking/cumulative/Independent acknowledgments.
- It accepts out of order of packets.
- Efficiency = $(2^{K-1}) \times \dfrac{t_{transmit}}{t_{transmit} + RTT}$
- With piggyback throughput = $\dfrac{2 \times Packet}{RTT}$
- Round Trip Time (RTT): It is minimum acknowledgment waiting time.
  RTT = 2 × Propagation delay
- **Time Out:** It is the maximum acknowledgment waiting time

Wireless IEEE 802.11:

- **Wireless hosts:** In the case of wired networks, hosts are the end-system devices that run applications.
- **Wireless links:** A host connects to a base station (defined below) or to another wireless host through a wireless communication link.
- **Base station:** A base station is responsible for sending and receiving data (e.g., packets) to and from a wireless host that is associated with that base station. Access points in 802.11 wireless LANs are examples of base stations.

  Two Types of mode:

  (*i*) **Infrastructure mode:** since all traditional network are provided by the network to which a host is connected via the base station.

  Types of Infrastructure mode:

  (a) **Single-hop, infrastructure-based:** Base station is used in these networks which is connected to a larger wired network where all communication is between this base station and a wireless host over a single wireless hop.

  (b) **Multi-hop, infrastructure-based:** A base station is present that is wired to the larger network where some wireless nodes may have to relay their communication through other wireless nodes in order to communicate via the base station.

  (*ii*) **Adhoc networks:** wireless hosts have no such infrastructure with which to connect. In the absence of such infrastructure, the hosts themselves must provide for services.

  Types of Adhoc mode:

  (a) **Single-hop, infrastructure-less:** In this no base station that is connected to a wireless network.

  (b) **Multi-hop, infrastructure-less:** There is no base station in these networks, and nodes may have to relay messages among several other nodes in order to reach a destination.

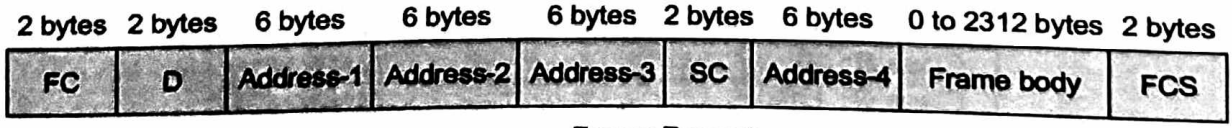
- **Basic service set (BSS):** A BSS contains one or more wireless stations and a central base station, known as an access point (AP) in 802.11.
- Each 802.11 wireless station has a 6-byte MAC address also each AP also has a MAC address for its wireless interface.
- 802.11b and 802.11g use the 2.4 Ghz ISM band offering only 33 non-overlapping channels.
- 802.11a uses 55GHz ISM band offering at-least 23 non-overlapping channels.

- 802.11n can use either the 2.4 GHz or the 55 GHz band while 802.11c uses only the 55 GHz band.
- **WiFi jungle:** Any physical location where a wireless station receives a sufficiently strong signal from two or more APs.
- **Scanning:** The process of scanning channels and listening for beacon frames is known as **Passive scanning**. In **Active scanning**, wireless station broadcasting a probe frame that will be received by all APs within the wireless host's range. APs respond to the probe request frame with a probe response frame. The wireless host can then choose the AP with which to associate from among the responding APs.

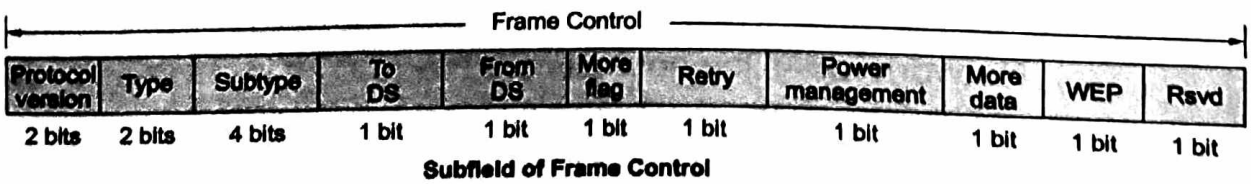
  (*i*) Passive scanning:
  (a) Beacon frames sent from Aps.
  (b) Association request frame sent: Host to selected AP.
  (c) Association response frame sent: Selected AP to Host.

  (*ii*) Active scanning:
  (a) Probe request frame broadcast from Host.
  (b) Probes response frame sent from APs.
  (c) Association request frame sent: Host to selected AP.
  (d) Association response frame sent: Selected AP to Host.
- Instead of using collision detection, 802.11 uses collision-avoidance techniques. Second, because of the relatively high bit error rates of wireless channels, 802.11 (unlike Ethernet) uses a link-layer acknowledgment/retransmission (ARQ) scheme.
- The 802.11 MAC protocol uses **link-layer acknowledgments SIFS and DIFS.**
- Binary exponential backoff uses.
- **Hidden Terminal Problem** is avoided by using RTS (Request to Send) and CTS (Clear to Send).

Frame Format:



Frame Format



Subfield of Frame Control

■■■

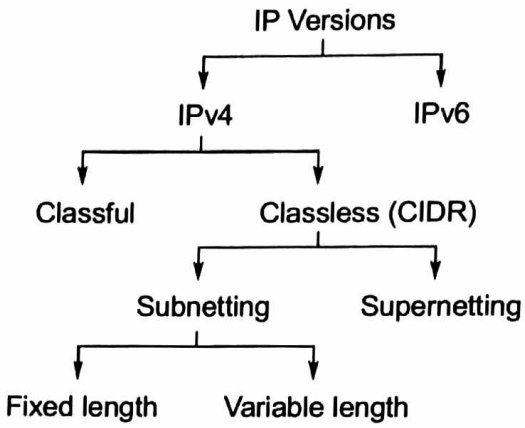
IP (v4), (v6) and Routing Algorithms

2

IPv4

IP Address

Used for global unique identification



IPv4 Address

- For flexibility 32 bit address is divided into 4 chunks each of 8 bits so that readability increases.
- IP address has 2 parts ***(i)*** Network ID ***(ii)*** Host ID.
- **Classfull Address:**

  (*i*) Identification of classes in decimal notation

  Class *A*: (0-127), **Class *B*:** (128-191), **Class *C*:** (192-223), **Class *D*:** (224-239), **Class *E*:** (240-255)

  (*ii*) Identification of a class in binary notation is done with the help of Network Identification Bit (NIB).

Class *A* : 0	Unicast (One-to-One)	*N·H·H·H/8*
Class *B* : 10		*N·N·H·H/16*
Class *C* : 110		*N·N·N·H/24*
Class *D* : 1110	Multicast	
Class *E* : 1111	R&D	

(a) **Network id:** All the host bits are made '0'. It is address of the network to which host belongs to.

(b) **Broadcast id:** Used to broadcast any packet to all machines in the network. All host bits are made '1'.

(*iii*) **Class A:**

Number of network bits = 7, **Number of host bits** = 24

Number of hosts = $2^{24} - 2$, **Number of networks** = $2^7 - 2$

Note:

- Having all zeros/all ones either in network id or host id is ruled out and they are meant for special purpose.

(*iv*) **Class B:**

Number of network bits = 14, **Number of host bits** = 16

Number of hosts = $2^{16} - 2$, **Number of networks** = 2^{14}

(*v*) **Class C:**

Number of network bits = 21, **Number of host bits** = 8

Number of hosts = $2^8 - 2$, **Number of networks** = 2^{21}

- **Special Purpose Addresses:**

  (*i*) **Loop back Address:**

  (a) To verify the TCP/IP protocol suite of own machine i.e. used for self connectivity checking.

  (b) It is also extensively used for interprocess communication.

  (c) **127.X.X.X** [X ranges from 0 to 255]

  But **127.0.0.0 and 127.255.255.255** not allowed.

  (*ii*) **Default Route:** If a packet destination address is not known, then if the default route is present in the routing table of the router, then the packet is not discarded but forwarded to the next router.

  0.0.0.0

  (*iii*) **Direct Broadcasting:** Packet sent to all in remote network.

  N.255.255.255, N.N.255.255, N.N.N.255

  (*iv*) **Limited Broadcasting:** Packet has to be broadcasted within same network. **255.255.255.255**

- **Private Address:** This IP cannot be routed in the internet, but only in intranet range:

  (*i*) **10.X.X.X**, (*ii*) **172.16.X.X to 172.31.X.X**, (*iii*) **192.168.X.X**

- **Limitations of Logical Addressing:** No flexibility, No security, Not permanent to system.

- **Rules to Deploy A Router:**

  Rule 1: All the interfaces of the router must belong to different networks.

  Rule 2: The LANs interconnected must belong to different networks.

Rule 3: The ethernet interface and the LAN must belong to the same network.

Rule 4: The routers sharing a same link must belong to the same network.

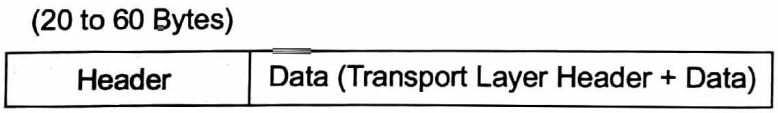
Solutions are: Supernetting, Subnetting, Physical addressing system.

Subnetting	Supernetting
(I) Dividing a network into multiple subnets is subnetting. (ii) Bits are borrowed from host id. (iii) It is applicable for single network. (iv) Number of 1s in subnet mask is always equal to more than network id bits.	(i) Aggregation of two or more n/ws to generate single IP address for the group is supernetting. (ii) Bits are borrowed from network id. (iii) It is applicable for two or more networks. (iv) Number of 1s always less than n/w id bits. (v) It reduces routing table entries. (vi) Network ids of the network must be in sequence.

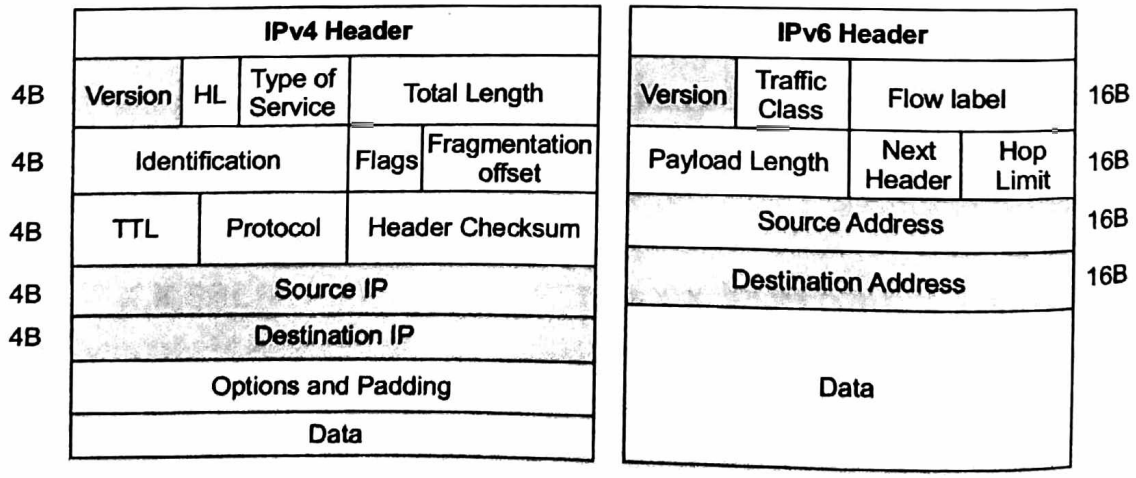
IP Datagram

IPv4

- It is **best effort** service and **connectionless** approach
- IP datagram



- **Header Format (IPv4 and IPv6):**



- At source, header length is divided by 4 and at destination multiplied by 4. During fragementation, constant scale factor '8' must be used (fragments must be divisible by 8 except last segment).

Options

- The header of the IPv4 datagram is made of two parts: a fixed part and a variable part.
- The fixed part is 20 bytes long and the variable part can be a maximum of 40 bytes.
- Options are not required for a datagram. They can be used for network testing and debugging.
- **End of Option:** An end-of-option option is a 1-byte option used for padding at the end of the option field. It, however, can only be used as the last option.
- **No Operation:** A **no-operation option** is a 1-byte option used as a filler between options.
- **Record Route:** A record route option is used to record the Internet routers that handle the datagram. It can list up to nine router addresses. It can be used for debugging and management purposes.
- **Strict Source Route:** A strict source route option is used by the source to predetermine a route for the datagram as it travels through the Internet.
- **Loose Source Route:** A loose source route option is similar to the strict source route, but it is less rigid. Each router in the list must be visited, but the datagram can visit other routers as well.

Timestamp: A timestamp option is used to record the time of datagram processing by a router.

IPv6

- **IPv6 Header** is always present and is a fixed size of 40 bytes.
- **Extenson Headers:** Zero or more extension headers can be present and are of varying lengths. A Next Header field in the IPv6 header indicates the next extension header. Within each extension header is a Next Header field that indicates the next extension header. The last extension header indicates the upper layer protocol (such as TCP, UDP, or ICMPv6) contained within the upper layer protocol data unit.
- **Upper Layer Protocol Data Unit:** The upper layer protocol data unit (PDU) usually consists of an upper layer protocol header and its payload (for example, an ICMPv6 message, a UDP message, or a TCP segment).
- The IPv6 packet payload is the combination of the IPv6 extension headers and the upper layer PDU. Normally, it can be up to 65,535 bytes long. Payloads greater than 65,535 bytes in length can be sent using the Jumbo Payload option in the Hop-by-Hop Options extension header.

Values of the Next Header Field:

Value (in decimal)	Header
0	Hop-by-Hop Options Header
6	TCP
17	UDP
41	Encapsulated IPv6 Header
43	Routing Header
44	Fragment Header
46	ResourceReSerVationProtocol
50	Encapsulating Security Payload
51	Authentication Header
58	ICMPv6
59	No next header
60	Destination Options Header

- **IPv6 Extension Headers:** IPv6 extension headers that must be supported by all IPv6 nodes: ***(i)*** Hop-by-Hop Options header, ***(ii)*** Destination Options header, ***(iii)*** Routing header, ***(iv)*** Fragment header, ***(v)*** Authentication header, ***(vi)*** Encapsulating Security Payload header ***(vii)*** tension header must fall on a 64-bit (8-byte) boundary. Extension headers of variable size contain a Header Extension Length field and must use padding as needed to ensure that their size is a multiple of 8 bytes.
- It is recommended that extension headers be placed in the IPv6 header in the following order: ***(i)*** Hop-by-Hop Options header, ***(ii)*** Destination Options header (for intermediate destinations when the Routing header is present), ***(iii)*** Routing header ***(iv)*** Fragment header ***(v)*** Authentication header ***(vi)*** Encapsulating Security Payload header ***(vii)*** Destination Options header (for the final destination).
- When an IPv6 packet is fragmented, it is initially divided into unfragmentable and fragmentable parts:
- The unfragmentable part of the original IPv6 packet must be processed by each intermediate node between the fragmenting node and the destination. This part consists of the IPv6 header, the Hop-by-Hop Options header, the Destination Options header for intermediate destinations, and the Routing header.

- The fragmentable part of the original IPv6 packet must only be processed at the final destination node. This part consists of the Authentication header, the Encapsulating Security Payload header, the Destination Options header for the final destination, and the upper layer PDU.

ARP (Address Resolution Protocol)

- Mapping from Logical to Physical Address
  (*i*) When user knows IP address (obtained from the DNS if the sender is the host or it is found in a routing table if the sender is a router) but not the MAC address.
  (*ii*) ARP Request (includes the physical and IP addresses of the sender and the IP address of the receiver) is broadcasted but ARP Reply(includes the recipient's IP and physical address) is uni-casted.
  (*iii*) ARP can be useful if the ARP reply is cached (kept in cache memory for a while) because a system normally sends several packets to the same destination. A system that receives an ARP reply stores the mapping in the cache memory and keeps it for 20 to 30 minutes unless the space in the cache is exhausted. Before sending an ARP request, the system first checks its cache to see if it can find the mapping.
  (*iv*) An ARP packet is encapsulated directly into a data link frame. An ARP packet is encapsulated in an Ethernet frame.

  Note that the type field indicates that the data carried by the frame are an ARP packet.

  Cases in which the services of ARP can be used:
  (*i*) **The sender is a host and wants to send a packet to another host on the same network.**
  (*ii*) **The sender is a host and wants to send a packet to another host on another network.**
  (*iii*) **The sender is a router that has received a datagram destined for a host on another network. It checks its routing table and finds the IP address of the next router.**
  (*iv*) **The sender is a router that has received a datagram destined for a host on the same network.**
- **RARP (Reverse Address Resolution Protocol):** mapping from Physical to Logical Address

(*i*) Finds the logical address for a machine that knows only its physical address (Present on NIC).

(*ii*) The requesting machine must be running a RARP client program; the responding machine must be running a RARP server program.

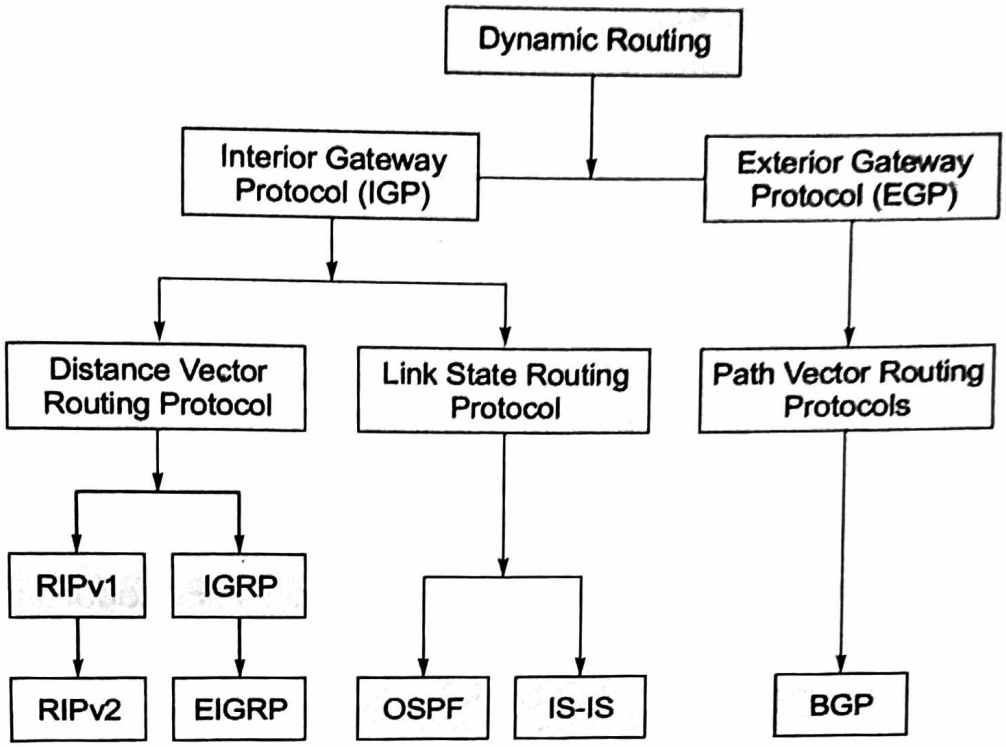
(*iii*) A RARP request is created and broadcast on the local network. Another machine on the local network that knows all the IP addresses will respond with a RARP reply.

Problem with RARP: Broadcasting is done at the data link layer. The physical broadcast address, all 1's in the case of Ethernet, does not pass the boundaries of a network. This means that if an administrator has several networks or several subnets, it needs to assign a RARP server for each network or subnet.

Routing Algorithms

1. **Flooding:** Every incoming packet is sent out on every outgoing line except the one it arrived on.
2. **Broadcast Routing: (a)** Flooding, **(b)** Multidimensional routing, **(c)** Sink tree (spanning tree) and **(d)** Reverse path forwarding

   It sends the packets from a host to all other remaining hosts in the network simultaneously.
3. **Multicast Routing:** It sends the packets from a host to specific groups. **(a)** Shared tree, **(b)** Source based tree, **(c)** Least unit cost path tree and **(d)** Reverse path multicasting (uses prune message)
4. **Distance Vector Routing:** Routing only to neighbours and knowledge about whole network. RIP, IGRP uses split horizon technique.
5. **Link State Routing (OSPF) [Dijkstra's Algorithm]:** It discovers the neighbour of each router and learn their network addresses, cost of reaching each neighbours, sends the packet to all other routers.
6. **Path Vector Routing (BGP):** It lists all autonomous system visited inorder to reach the destination network by this route.
7. **Hierachical Routing (Intra region and Inter region routing):** Routing is based on regions and it maintains two tables namely "Full Table (for all routers in all regions) and "Hierachical Table" (for all routers within the region and knows about other regions but not routers of other regions).



- **A problem** with distance vector routing is instability,
  - (*i*) **Two-node loop problem**
  - (*ii*) **Defining Infinity:** Most implementations of the distance vector protocol define the distance between each node to be 1 and define 16 as infinity.
- **A Solution: Split Horizon and Split Horizon and Poison Reverse.**
- **RIP (Routing Information Protocol):**
  - (*i*) RIP is an intra-domain routing protocol.
  - (*ii*) The metric used by RIP is very simple; the distance is defined as the number of links (networks) to reach the destination. For this reason, the metric in RIP is called a hop count.
  - (*iii*) **Infinity is defined as 16,** which means that any route in an autonomous system using RIP cannot have more than 15 hops.

  OSPF (Open Shortest Path First or OSPF):
  - (*i*) OSPF protocol is an intradomain routing protocol based on link state routing.
  - (*ii*) Its domain is also an autonomous system.
  - (*iii*) **Types of Links:** (a) Point-to-point link, (b) Transient, (c) Stub link, (d) Virtual link.
- **Path Vector Routing:** Path vector routing proved to be useful for interdomain routing.

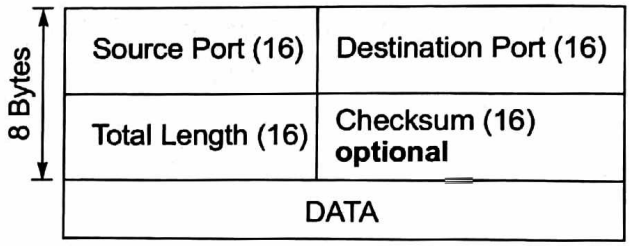
■■■

TCP/UDP and Application Layer protocols

3

User Datagram Protocol

- It is **connectionless** (No Acknowledgment) and **unreliable** approach.
- It is iterative compared to concurrent TCP.
- It is used for Broadcasting and Multicasting, all real time application (or) services utilises UDP with help of RTP (Video conference, Live Telecast) because it has fixed header size.
- It is message oriented and there is no flow control.
- **Pseudoheader** (Consist Source IP, Destination IP, Protocol used in IP, TCP/UDP segment length) of UDP is same as TCP.
- **Header Format:**

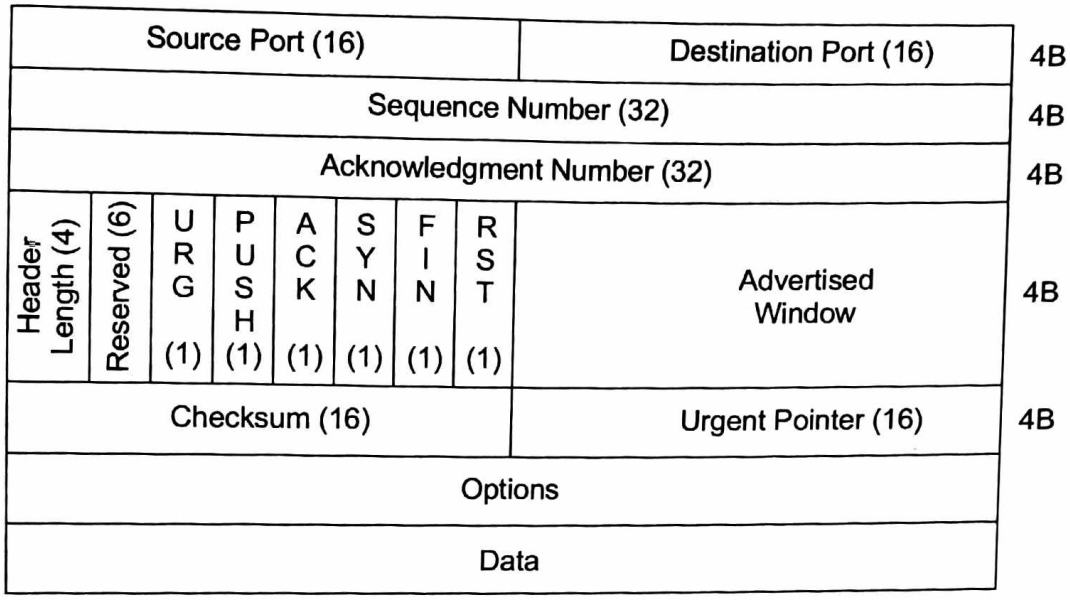


- Applications that require bulk data transfer and fastness (than reliability) uses UDP.
- Protocols which takes services of UDP are NFS, SNMP-161, RIP-520, TFTP-69, DNS-53 and Ping (ICMP)-7.

Transmission Control Protocol

- It is reliable, port to port, byte/stream transport layer protocol.
- It supports **full duplex, connection oriented** (cumulative acknowledgment) approach.
- Not useful for broadcasting and multicasting.
- It is slow start protocol
- It uses sliding window protocol for flow control, the window size is set and controlled by receiver.
- TCP connections have three phases: ***(i)*** Connection establishment, ***(ii)*** Data Transmission and ***(iii)*** Connection Termination.

- Header Format:



Note:

- TCP uses random initial sequence number. After exhausting all the sequence number, sequence number are repeated.
- Probability of getting a number = $1/2^{32}$.

- Protocols which takes services of TCP are:
  HTTP (80), FTP (Data (20), Control (21)), Telnet (23), SMTP (25), POP3(110)

Congestion Control

Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened.

1. **In Open-Loop Congestion Control** policies are applied to prevent congestion (handled by either the source or the destination) before it happens.

- **Retransmission Policy (sometimes unavoidable)**
  (*i*) If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted, which may increase congestion in the network.
  (*ii*) The retransmission policy and the retransmission timers must be designed to optimize efficiency and at the same time prevent congestion.
- **Window Policy:** The Selective Repeat window is better than the Go-Back-N window for congestion control.

- Acknowledgment Policy (policy imposed by the receiver).
- **Discarding Policy:** A good discarding policy by the routers may prevent congestion and at the same time may not harm the integrity of the transmission
- **Admission Policy:** An admission policy, which is a quality-of-service mechanism, can also prevent congestion in virtual-circuit networks.

2. **Closed-Loop Congestion Control:** Closed-loop congestion control mechanisms try to alleviate congestion after it happens.

   (i) **Backpressure:**

   (a) Is a node-to-node congestion control that starts with a node and propagates, in the opposite direction of data flow, to the source.

   (b) In backpressure, the warning is from one node to its upstream node, although the warning may eventually reach the source station.

   (ii) **Choke Packet:**

   (a) A choke packet is a packet sent by a node to the source to inform it of congestion.

   (b) In the choke packet method, the warning is from the router, which has encountered congestion (intermediate nodes are not warned), to the source station directly.

   (iii) **Implicit Signaling:**

   (a) No communication between the congested node or nodes and the source.

   (b) The source guesses that there is a congestion somewhere in the network from other symptoms.

   (iv) **Explicit Signaling:** The node that experiences congestion can explicitly send a signal to the source or destination.

   (v) **Backward Signaling:** A bit can be set in a packet moving in the direction opposite to the congestion warn the source that there is congestion and that it needs to slow down to avoid the discarding of packets.

   (vi) **Forward Signaling:** A bit can be set in a packet moving in the direction of the congestion warn the destination that there is congestion.

Traffic Shaping is a technique which involves in making a **Bursty Incoming Traffic** into an average output or a regulated output.

Two Approaches (i) Leaky Bucket
(ii) Token Bucket

M = Maximum regulated output rate
C = Capacity of bucket
ρ = Token filling rate
t = Time period of incoming traffic
$\therefore C = (M - \rho)t$

- **TCP congestion Control:** Two approaches are used
  (*i*) Slow Start and Additive Increase
  (*ii*) **Multiplicative Decrease:** Congestion window always starts MSS = 1 and increases exponentially upto threshold value, then increases linearly upto Sender Window Size (SWS) and when timeout occurs, congestion window reduced to 1 MSS and threshold value reduced to half of congestion window size.
- **TCP Error Control:** 3 parameters are used
  (*i*) **Checksum:** It detects errors.
  (*ii*) **ACK:** There is no negative acknowledgment in TCP, as well as there is No ACK for received ACK.
  If any segment is corrupted (found through checksum), such segments are not acknowledged.
  (*iii*) **Time-out:** Transport layer uses dynamic RTT for time out calculation. Different timers are deployed for error control like Time Awaited Timer, Keep-Alive Timer, Persistence Timer, Retransmission Timer.
- **Purpose of Pseudoheader:** It is used to identify whether packet is received by the correct destination or not. It is prepared at the source with source values, again it is prepared at destination with destination values.
- **TCP State Transition Diagram:** The functionality of TCP connection setup, communication phase and termination phase can be easily depicted by the state transition diagram where the TCP will be only at one state at a time w.r.t. server or client.

  Limitations:
  1. Error control procedures are not depicted.
  2. Retransmissions are not shown.

Socket

- The socket is the software abstraction used to represent the "terminals" of a connection between two machines.

- Client and servers establish connections and communicate via sockets, which are communication links that are created over the Internet using TCP (or UDP).
- Sockets are the endpoints of internet communication stream or channel (logical).
- Clients create client sockets and connect them to server sockets.
- If two processes wish to communicate they must each create a socket. Once created, the socket must then be bound to a specific network address.
- One process must initiate the connection (This process is called the client). The other process must wait for a connection request (This process is the server). The client start by trying to establish a connection with the listening socket at a server.

BOOTP (Bootstrap Protocol)

- Client/server protocol designed to provide physical address to logical address mapping.
- BOOTP is not a dynamic configuration protocol.
- BOOTP is an application layer protocol. The administrator may put the client and the server on the same network or on different networks.
- BOOTP messages are encapsulated in a UDP packet, and the UDP packet itself is encapsulated in an IP packet.
- Client can send an IP(uses all 0's as as the source address and all 1's as the destination address).
- The BOOTP request is broadcast because the client does not know the IP address of the server.

  Problem with RARP solved by BOOTP: A broadcast IP datagram cannot pass through any router. One of the hosts can be used as a relay agent which knows the unicast address of a BOOTP server. After receives BOOTP broadcasting packet, it encapsulates the message in a unicast datagram and sends the request to the BOOTP server.

DHCP (Dynamic Host Configuration Protocol)

- The Dynamic Host Configuration Protocol (DHCP) has been devised to provide **static and dynamic** address allocation that can be manual or automatic.
- **Static Address Allocation:** In this case DHCP acts as BOOTP does. It is backward compatible with BOOTP. A DHCP server has a database that statically binds physical addresses to IP addresses.

- **Dynamic Address Allocation:** DHCP has a second database with a pool of available IP addresses(which makes it dynamic).
  (*i*) **The dynamic aspect of DHCP** is needed when a host moves from network to network or is connected and disconnected from a network. DHCP provides temporary IP addresses for a limited time.
  (*ii*) The DHCP server issues a **lease** for a specific time. When the lease expires, the client must either stop using the IP address or renew the lease. The server has the option to agree or disagree with the renewal. If the server disagrees, the client stops using the address.
  (*iii*) **One major problem with the BOOTP protocol** is that the table mapping the IP addresses to physical addresses needs to be manually configured while DHCP, on the other hand, allows both manual and automatic configurations.

Application Layer Protocols

Domain Name System (DNS)

- It is used to keep track of computers, services, resources both in LAN and WAN environment.
- It is used to map an URL to an IP address.
- It uses both TCP as well as UDP services on port 53.
- It uses 4 servers for application: **(*i*)** Root server, **(*ii*)** Top level domain server, **(*iii*)** Authoritative server and **(*iv*)** Local DNS.
- It offers 4 services: **(*i*)** Name Translation, **(*ii*)** Host Aliasing, **(*iii*)** Mail Aliasing and **(*iv*)** Load Balancing.
- It uses distributed databases to store information in terms of records.

File Transfer Protocol (FTP)

- It takes services of TCP < Data (20), Control (21)
- It has set of status codes and error codes.
- It has 3 modes of operation: **(*i*)** Active, **(*ii*)** Passive, and **(*iii*)** Extended passive mode.
- There are 2 modes of access:

Two Modes of Access

FTP	TFTP
(i) For authorized users (ii) Username, password required (iii) Upload (iv) Uses TCP	(i) For anonymous users (ii) Username, password not required (iii) Download (iv) Uses UDP on port 69

Hyper Text Transfer Protocol (HTTP)

- It takes services of TCP on **port 80.**
- It is **"stateless protocol"** since it does not have any mapping from one transaction onto other and treats a request and reply as a pair everytime.
- It offers security through Secure Sockets Layer (a protocol for transmitting private documents via internet).
- It is used to access webpages from www.
- It has 8 methods for it's operation. They are: ***(i)*** Head, ***(ii)*** Get, ***(iii)*** Put, ***(iv)*** Post, ***(v)*** Delete, ***(vi)*** Trace, ***(vii)*** Connect and ***(viii)*** Options.
- There are two types of connection in HTTP:
  - ***(i)*** **Non Persistent:** For every process the connection is established newly.
  - ***(ii)*** **Persistent:** A single TCP connection is set on which multiple request and response can be made.

Simple Mail Transfer Protocol (SMTP)

- It uses port 25 on TCP.
- Components of SMTP are:
  - *(i)* User Agent (UA)
  - *(ii)* Mail Transfer Agent (MTA)
  - *(iii)* Multipurpose Internet Mail Extension (MIME)
  - *(iv)* Mail Access Protocol (MAP):
    - (a) POP3
    - (b) Internet MAP (IMAP4)

Internet Control Messaging Protocol (ICMP)

- It is used for error reporting and query messages which help in network debugging.

- It is encapsulated into an IP datagram and then transmitted into the network, if the protocol field in IP datagram is 1 then the IP datagram is said to be carrying ICMP message.
- It uses the services of TCP and UDP on port 7 as ping command.
- **Types of Messages:**
  - (*i*) **Error reporting:** **(a)** Destination unreachable, **(b)** Source quench, **(c)** Parameter problem, **(d)** Time exceeded and **(e)** Redirection.
  - (*ii*) **Query Message:** **(a)** Router Solicitation and Router Advertisement, **(b)** Address Mask Request and Reply, **(c)** Time Stamp Echo Request and Reply and **(d)** Echo Request and Reply

Post Office Protocol Version 3 (POP 3)

- It is a pull protocol which takes services of TCP on **port 110.**
- At present IMAP4 is most used for MAP services

■■■

Network Security (Cryptography)

4

Cryptography

- **Plaintext** (The original message, before being transformed) and **Ciphertext** (After the message is transformed).
- An **encryption algorithm** transforms the plaintext into ciphertext while a decryption algorithm transforms the ciphertext back into plaintext.

Types of cryptography

1. **Symmetric Key (Secrete key Cryptography):** Same key (shared) is used by the sender (for encryption) and the receiver (for decryption).

Types of Symmetric Key Cryptography:

- **Substitution Cipher:** A substitution cipher substitutes one symbol with another: (a) Monoalphabetic cipher, (b) Polyalphabetic cipher.
- **Shift Cipher:** The simplest monoalphabetic cipher is probably the shift cipher.
- **Transposition Ciphers:** There is no substitution of characters; instead, their positions change. In a transposition cipher, the key is a mapping between the position of the symbols in the plaintext and cipher text.
- **Rotation Cipher:** Input bits are rotated to the left or right. The rotation cipher can be keyed or keyless.
  - ***(i)*** **In keyed rotation**, the value of the key defines the number of rotations (If the length of the original stream is N, after N rotations, we get the original input stream). The decryption algorithm for the rotation cipher uses the same key and the opposite rotation direction.
  - ***(ii)*** **In keyless rotation** the number of rotations is fixed.
- **Block Ciphers:** These ciphers are referred to as block ciphers because they divide the plaintext into blocks and use the same key to encrypt and decrypt the blocks.
  - ***(i)*** **Data Encryption Standard (DES):**
  - (a) The algorithm encrypts a 64-bit plaintext block using a 64-bit key.
  - (b) DES has two transposition blocks (P-boxes) and 16 complex round ciphers (they are repeated).

(c) The initial and final permutations are keyless straight permutations that are the inverse of each other. The permutation takes a 64-bit input and permutes them according to predefined values.

DES Function is the **heart of DES**.

(*ii*) Triple DES:

(a) Uses three DES blocks where encrypting block uses an encryption-decryption-encryption combination of DESs, while the decryption block uses a decryption-encryption-decryption combination.

(b) Two different versions of 3DES are in use: (a) 3DES with two keys, (b) 3DES with three keys.

(c) To make the key size 112 bits and at the same time protect DES from attacks such as the man-in-the-middle attack, 3DES with two keys was designed.

(*iii*) Advanced Encryption Standard (AES):

(a) The Advanced Encryption Standard (AES) was designed because DES's key was too small.

(b) Triple DES increased the key size, the process was too slow.

(c) AES is a very complex round cipher. AES is designed with three key sizes: 128, 192, or 256 bits.

2. **Asymmetric-Key Cryptography (Public key Cryptography):** Two keys: a private key(kept by the receiver) and a public key(announced to the public).

- **RSA (Rivest, Shamir, and Adleman algorithm):**

(*i*) It uses two numbers, e and d, as the public and private keys.

(*ii*) RSA is a public-key cryptosystem that is often used to encrypt and decrypt symmetric keys.

(a) Bob chooses two very large prime numbers p and q. Remember that a prime number is one that can be divided evenly only by 1 and itself.

(b) Bob multiplies the above two primes to find n, the modulus for encryption and decryption. In other words, $n = p \times q$.

(c) Bob calculates another number $\phi(n) = (p - 1) \times (q - 1)$.

(d) Bob chooses a random integer e. He then calculates d so that $d \times e = 1 \bmod \phi$.

- Bob announces e and n to the public; he keeps $\phi(n)$ and d secret.

(*i*) In RSA, e and n are announced to the public; d and $\phi(n)$ are kept secret.

(*ii*) Although RSA can be used to encrypt and decrypt actual messages, it is very slow if the message is long. RSA, therefore, is useful for short messages such as a small message digest or a symmetric key to be used for a symmetric-key cryptosystem.

(*iii*) RSA is used in digital signatures and other cryptosystems that often need to encrypt a small message without having access to a symmetric key.

(*iv*) RSA is also used for authentication.

- **Diffie-Hellman:**

(*i*) Diffie-Hellman, on the other hand, was originally designed for key exchange.

(*ii*) In Diffie-Hellman cryptosystem, two parties create a symmetric session key to exchange data without having to remember or store the key for future use.

(*iii*) The **symmetric key** for the session is K.

$(g^x \bmod p)^Y \bmod p = (g^Y \bmod p)^x \bmod p = g^{xy} \bmod p$.

(*iv*) **Problems arise in Diffie-Hellman:** Man-in-the-Middle Attack, It is also known as a bucket brigade.

Solution: The man-in-the-middle attack can be avoided if Bob and Alice first authenticate each other: **(a)** Message Confidentiality, **(b)** Message Integrity, **(c)** Message Authentication, **(d)** Message Nonrepudiation and **(e)** Entity Authentication.

(*v*) For a long message, symmetric-key cryptography is much more efficient than asymmetric-key cryptography.

- **Message Integrity:** Encryption and decryption provide secrecy, or confidentiality, but not integrity.
- **Message Digest Functions:** A message digest is a cryptographic hash function containing a string of digits created by a one-way hashing formula. Message digests are designed to protect the integrity of a piece of data or media to detect changes and alterations to any part of a message.

(*i*) Every bit of the message digest function's output is potentially influenced by every bit of the function's input.

(*ii*) If any given bit of the function's input is changed, every output bit has a 50 percent chance of changing.

(*iii*) Given an input file and its corresponding message digest, it should be computationally infeasible to find another file with the same message digest value.

- **MD2(Message digest 2):**
  (*i*) This message digest is probably the most secure of Rivest's message digest functions, but takes the longest to compute.
  (*ii*) MD2 produces a 128-bit digest.
- **MD4(Message digest 4):**
  (*i*) This message digest algorithm was developed as a fast alternative to MD2.
  (*ii*) MD4 produces a 128-bit digest.
- **MD5(Message digest 5):**
  (*i*) MD5 is a modification of MD4 that includes techniques designed to make it more secure.
  (*ii*) MD5 and SHA-1 are both used in SSL and in Microsoft's Authenticode technology.
  (*iii*) MD5 produces a 128-bit digest.
- **SHA(Secure Hash Algorithm):** SHA produces a 160-bit digest.

SHA-I (Secure Hash Algorithm 1):

(*i*) SHA-I is a revised version of SHA.
(*ii*) Each creates a digest of length N from a multiple-block message.
(*iii*) Each block is 512 bits in length.
(*iv*) SHA-I has a message digest of 160 bits (5 words, each of 32 bits).

Message Authentication:

(*i*) A hash function guarantees the integrity of a message (guarantees that the message has not been changed).
(*ii*) The digest created by a hash function is normally called a modification detection code (MDC). The code can detect any modification in the message.

MAC (Message Authentication Code):

(*i*) To provide message authentication we need message authentication code.
(*ii*) An MDC uses a keyless hash Function a MAC uses a keyed hash function.
(*iii*) A keyed hash function includes the symmetric key between the sender and receiver when creating the digest.

(*iv*) If the two MACs are identical, the message has not been modified and the sender of the message is verified.

- **Digital Signature:**
  (*i*) A digital signature use a pair of asymmetric keys (a public one and a private one).
  (*ii*) The sender can sign the message digest using receiver's public key, and the receiver can verify the message digest using own private key.
  (*iii*) A digital signature can provide message integrity, message authentication, and non-repudiation.

■■■