PRATHYUSHA ENGINEERING COLLEGE
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
2.3.2 C- E-Contents developed by Faculty

S.NO	SUBJECT CODE	SUBJECT NAME	Name of the faculty
1	EC8004	Wireless Networks	Mr T Rubesh Kumar
2	EC8551	Communication Networks	Mr E Dilliraj
3	EC8094	Satellite Communication	Dr S Malathi
4	ME8591	Principles of Management	Ms P Vadivu

WIRELESS LAN

Introduction-WLAN technologies: IEEE802.11: System architecture, protocol architecture, 802.11b, 802.11a – Hiper LAN: WATM, BRAN, HiperLAN2 – Bluetooth: Architecture, WPAN – IEEE 802.15.4, Wireless USB, Zigbee, 6LoWPAN, WirelessHART

PART-B

WIRELESS NETWORK: A network that is established without any physical links are referred to as wireless network. The medium involved between transmitter and receiver is radio waves.

1. List the advantages and limitations (drawbacks) of WLAN Techniques.

ADVANTAGES OF WLAN

- **Flexibility:** Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls. Senders and receivers can be placed anywhere (also non-visible, e.g., within devices, in walls etc.).

- **Planning:** Only **wireless ad-hoc networks allow for communication without previous planning,** wired network needs wiring plans. For wired networks, additional cabling is required.

- **Design:** Wireless networks allow for the **design of small, independent devices** which can be placed on a pocket also. Wireless senders and receivers can be hidden in historic buildings.
- **Robustness:** Wireless networks **can survive during disasters also**. Ex. During flood etc. also. If the wireless devices survive, people can still communicate.

- **Cost: After providing wireless access** to the infrastructure via an access point **for the first user, adding additional users to a wireless network need not have to pay more**.

Note: Using a fixed network, each user in a lecture hall/room should have a plug for the network although many of them might not be used permanently. Constant plugging and unplugging will sooner or later destroy the plugs.

LIMITATIONS / DISADVANTAGES OF WLAN

● **Quality of service: WLANs** typically **offer lower quality than their wired counterparts**. The main **reasons** for this are the **lower bandwidth due to limitations in radio transmission** and **higher delay/delay variation due to extensive error correction and detection mechanisms.**

● **Proprietary solutions:** Due to slow standardization procedures, many companies have come up with proprietary solutions offering standardized functionality plus many enhanced features. However, these additional features only work in a homogeneous environment, i.e., when adapters from the same vendors are used for all wireless nodes.

● **Restrictions:** All wireless products have to compete with national and international regulations. Several government and non-government institutions worldwide regulate the operation and restrict frequencies to minimize interference.

● **Safety and security:** Using radio waves for data transmission might interfere with other high-tech equipment in, e.g., hospitals. Senders and receivers are even operated by laymen hence, radiation should be low.

Note: Special precautions have to be taken to prevent safety hazards. All standards must offer (automatic) encryption, privacy (secret) mechanisms. Otherwise more and more wireless networks will be hacked.

2. What are the goals or objectives to be achieved by WLAN?

● **Global operation:** WLAN products should sell in all countries so**, national and international frequency regulations have to be considered.**

● **Low power:** Devices communicating via a WLAN are typically the devices which runs on battery power. The LAN design should take this into account and implement special power-saving modes and power management functions.

- **License-free operation:** LAN operators do not want to apply for a special license to be able to use the product. The **equipment must operate in a license-free band**, such as the **2.4 GHz ISM band**.

● **Robust transmission technology:** Compared to their wired counterparts, WLANs operate under difficult conditions. If they use radio transmission, many other electrical devices can interfere with them (vacuum cleaners, hairdryers, etc.).

WLAN transceivers cannot be adjusted for perfect transmission in a standard office or production environment. Antennas are typically omnidirectional, not directed. Senders and receivers may move from one place to other.

● **Simplified spontaneous cooperation:** To be useful in practice, WLANs should not require complicated setup routines but should operate spontaneously after power-up.

● **Easy to use:** In contrast to huge and complex wireless WANs, wireless LANs are made for simple use. They should not require complex management, but rather **work on a plug-and-play basis.**

● **Protection of investment:** A lot of money has already been invested into wired LANs. The new WLANs should protect this investment by being interoperable with the existing networks. This means that simple bridging between the different LANs should be enough to interoperate, i.e., the wireless LANs should support the same data types and services that standard LANs support.

● **Safety and security:** Wireless LANs should be safe to operate; radiation should be less, e.g., in hospitals. Intruder should not capable to read personal data of the user during transmission, hence suitable encryption mechanisms should be integrated.

● **Transparency for applications:** Existing applications should continue to run over WLANs, the only difference being higher delay and lower bandwidth. The fact of wireless access and mobility should be hidden if it is not relevant, but the **network should also support location aware applications**, e.g., by providing location information.

---

3. Compare Infra red vs radio transmission techniques or explain the transmission technologies used in WLAN.

Two types of technologies are involved.

1. Infrared 2. Radio waves

1. INFRARED: It is based on the transmission of infrared light at **900 nm wavelength**. Here, LED/LASER acts as source and photodiode acts as receiver. Two methods are used in IR.

(i) Diffused IR: In this method the transmitter diffuses the IR rays in whole room and the receiver can be kept any were on the room to receive the signal. **Line of sight (LOS) not required** in this method.

(ii) Direct LOS: In this method the sender and receiver both will be aligned such that they both are available in the LOS region.

Advantages:

1. No radiation
2. It operates at unlicensed region.
3. Electrical devices do not interfere with IR transmission.
4. Shielding is simple.

Limitations/Disadvantages:

1. Low data rate (115 Kb/s).
2. IR cannot penetrate walls or even any obstacles also.
3. For good transmission QOS and high data rate clear LOS is required.
4. It can support only for short distance 30-50 feet under ideal condition.
5. Signals are affected by sunlight, snow, ice and fog.

Note: In wireless network 802.11 alone uses IR in addition to radio wave whereas HIPERLAN and Bluetooth relays on radio waves alone.

2. RADIO WAVES: It transmits at 900, 1800 and 1900 MHz. The source is radio waves.

Advantages:

1. Radio transmission can penetrate walls, furniture, plants, etc.
2. It does not require a clear line of sight (LOS).
3. It provides high data transmission rate. (54 Mb/s).

Limitations/Disadvantages:

1. Radio transmission is permitted only in certain frequency bands which are not same in all countries in world wide.
2. Shielding is not simple.
3. Radio transmission can interfere with other electrical devices and the data can be damaged.

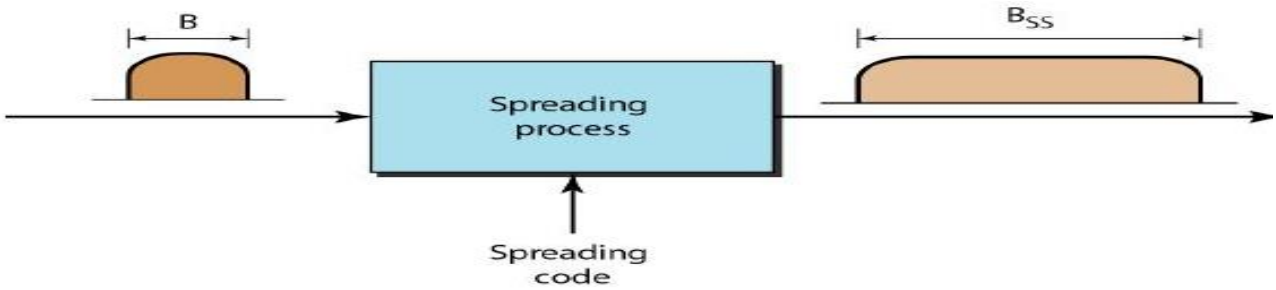
Comparison of IR over radio waves.

Infrared	Radio waves
It uses LED/LASER as source and photodiode as receiver.	It uses RF signal as source and antenna as receiver.
Shielding is simple	Shielding is not simple.
It cannot penetrate walls.	It can easily penetrate any obstacles.
It requires a clear line of sight (LOS).	It does not require a clear line of sight (LOS).
IR does not interfere with other electrical devices	Radio transmission can interfere with other electrical devices
Operates in unlicensed band.	Operates in a limited licensed band region.
Low data rate (115 Kb/s).	High data transmission rate. (54 Mb/s).
For short distance transmission 30-50 feet under ideal condition..	It can be applied for long distance transmission.
Signals are affected by sunlight, snow, ice and fog	Signals are not affected by sunlight, snow, ice and fog

Explain about spread spectrum technique:

In radio waves we have two types: 1. Spread spectrum 2. UHF narrow band

Spread spectrum: Is a technique in which the **frequency** of the transmitted **signal is deliberately varied.** (i.e) the bandwidth of signal is deliberately varied to **obtain wider bandwidth**.



Need / Advantage

1. To achieve secure communication.

2. To increase resistance to avoid interference.

3. To prevent detection of data by intruder (hacking person).

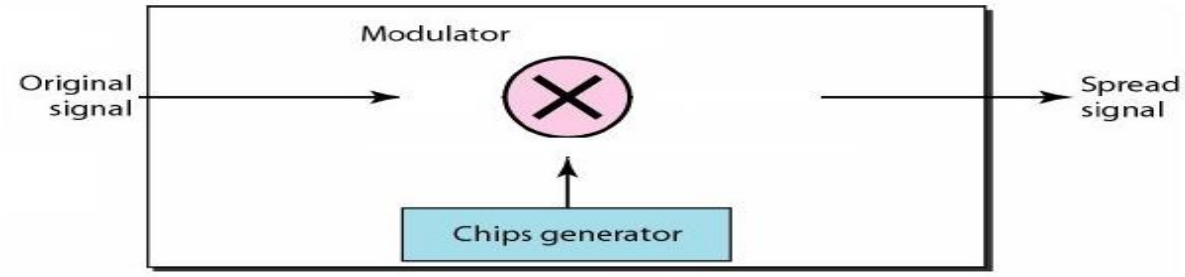
4. For longer operating distance transmission.

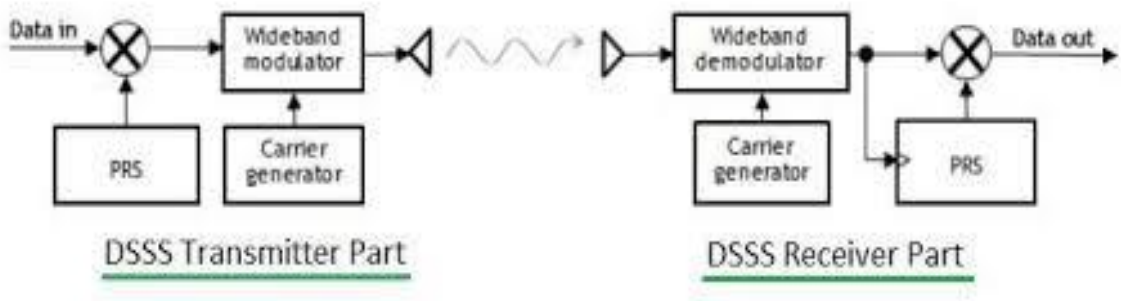
It is achieved by two methods.

1. DSSS 2. FHSS

1. Direct sequence spread spectrum (DSSS): In this method the data signal to be transmitted is combined with chipping code which is generated from code generator. The resulting signal is the spread spectrum signal. It is obtained by performing EX-OR operation of user data with each string of bits generated from the code generator.

The resultant spread spectrum signal is modulated and transmitted.





The chipping code is generated by pseudo random sequence (PRS) generator. The DSSS receiver performs the inverse function of transmitter.

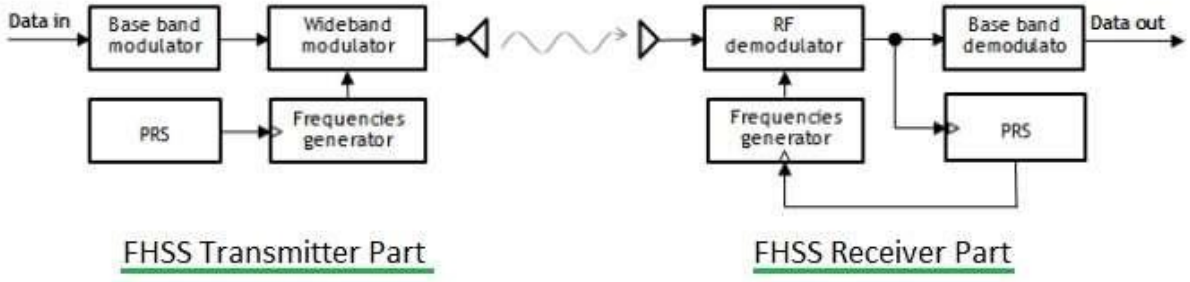
Note: In DSSS each individual bit is replaced by a string of bits. In this way the data is widened and spreading is achieved.

Advantages:

- It has best discrimination against multipath signals.
- It avoids intentional interference such as jamming effectively.
- Performance of DSSS system in presence of noise is better than FHSS system.

2. Frequency hopping spread spectrum (FHSS): In this method a **wide frequency band is divided into multiple channels** and signals are **jumping (hopping)** sequentially from one channel to another in a sequence which is known to transmitter and receiver alone.

The multiple carrier signals are generator by frequency generator.



Advantages:

1. Provides robust transmission path in the presence of interferences.
2. It provides security against any kind of intrusion as only transmitter and receiver are aware of PN codes.
3. It can be employed in point to multipoint applications.

Comparison between DSSS and FHSS (Refer class notes)

FHSS	DSSS
1. It spreads the signal by hopping (jumping) from one carrier frequency to another carrier frequency.	It spreads the signal by adding redundant (additional) bit to the signal prior to transmission
2. Here, in FHSS the frequency is randomised.	Here, the frequency is constant.
3. In FHSS data is constant	Here, data is randomized.
4. A wide band signal is divided into multiple frequencies	The spreading is achieved by using specific encoding scheme.
5. Highly resistance to noise.	Less resistance to noise.
6. Limited throughput.	High throughput than FHSS.
7. To unknown receiver FHSS appears to be short duration impulse	To unknown receiver DSSS appears as a low power wideband noise.

8. It does not require encryption additionally.	8. It requires encryption additionally.

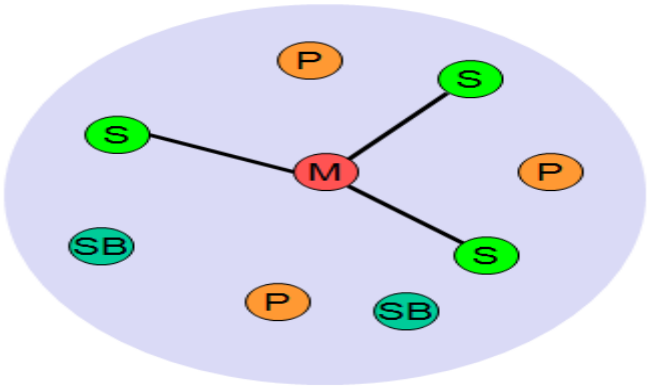
Explain Bluetooth architecture and its layers:

INTRODUTION

- A **Bluetooth** is an **ad hoc network**, which means that the **network** is formed **spontaneously or when necessary.**
- It is a **short range, low cost** wireless communication device that **uses radio technology.**
- It **operates** at **2.4 GHz.**
- It allows the users to **transmit real time voice and data information.**
- Its transmission mode provides protection against interferences and safety in sending of information.
- Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers, cameras, printers, coffee makers, and so on.
- Bluetooth defines two types of networks: **Piconet and Scatternet.**

PICONET

- A collection of devices connected in an Ad-Hoc fashion is referred to as piconet.
- Here, one station acts as master and the other stations or nodes acts as slaves.
- It can **have up to eight stations,** one of which is called the master; the rest are called slaves.
- Maximum of seven slaves. Only one master. The **reason for only 8 active devices is the Bluetooth uses 3 bits for address.**

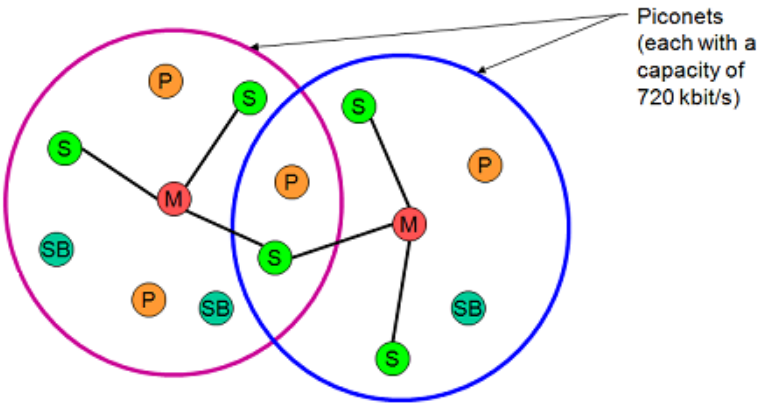


M=Master P=Parked
S=Slave SB=Standby

- Slaves synchronize their clocks and hopping sequence with the master.
- But an additional eight slaves can stay in parked state, which means they can be synchronized with the master but cannot take part in communication until it is moved from the parked state.

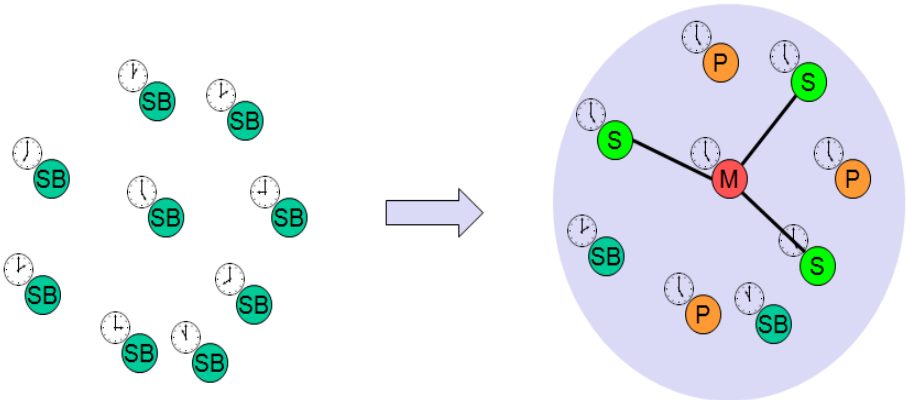
SCATTERNET

- More number of piconets which are linked together is referred to as scatternet.
- A slave station in one piconet acts as master in another piconet.
- Bluetooth devices has a built-in short-range radio transmitter.



Note: If a parked device need to communicate and there are already active slaves then one slave has to switch to park mode to allow the parked device to switch to active mode.

Steps involved in forming a piconet / Explain how piconet is formed:



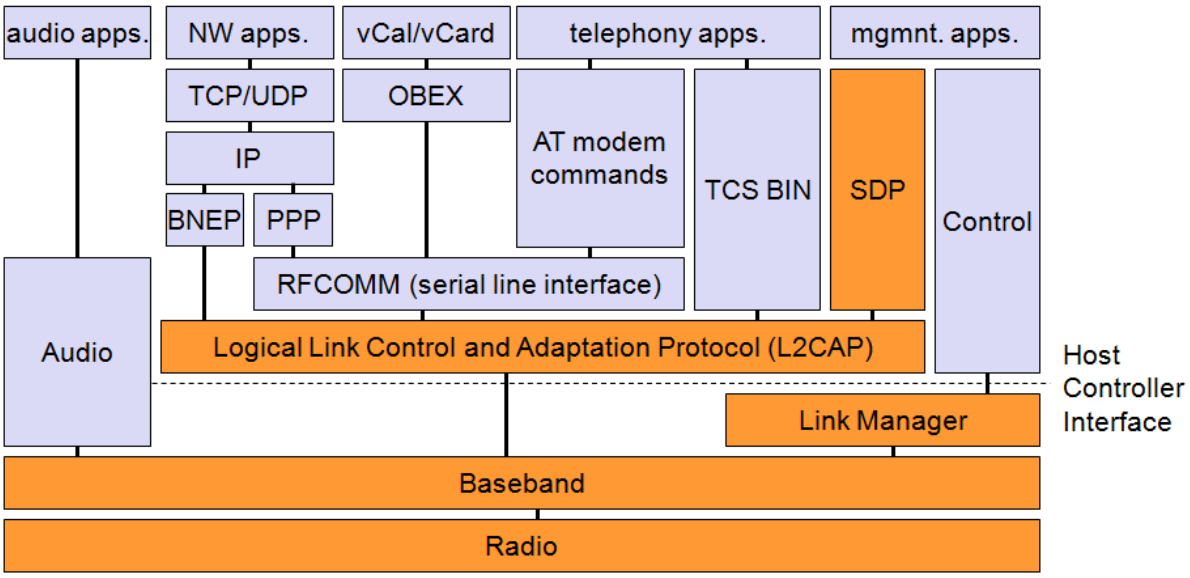
In **general** the **master sends its clock and device ID** since all active devices have to synchronize with each other. The unit establishing/initiating the piconet automatically becomes the master and the remaining devices will be as slaves.

By adjusting the internal clock of each device according to master the other devices participate in piconet.

Note: All **active devices are assigned a 3 bit active member address (AMA)**. All **parked devices** uses an **8 bit parked member address (PMA).**

Devices in stand-by no need an address.

BLUETOOTH PROTOCOL STACK: The Bluetooth protocol stack consists of a series of layers.



AT: attention sequence
OBEX: object exchange
TCS BIN: telephony control protocol specification – binary
BNEP: Bluetooth network encapsulation protocol

SDP: service discovery protocol
RFCOMM: radio frequency comm.

1. RADIO LAYER:

It is roughly **equivalent to a physical layer** in OSI model. It defines the carrier frequencies and output power. It uses license free frequency band 2.4 GHz.

It uses **Frequency-hopping spread spectrum.** Changes it modulation frequency **1600 hops p**er second. The time between two hops is called a slot, which is an interval of 625 µs.

- Bluetooth transceivers use **Gaussian FSK for modulation** and are available in different power levels. Based on power levels classified as:
- **Power class 1:** Maximum power is 100 mW and minimum is 1 mW (can be applied upto 100m range without obstacles).
- **Power class 2:** Maximum power is 2.5 mW and minimum is 0.25 mW. (can be applied upto 10m range without obstacles).
- **Power class 3:** Maximum power is 1 mW

2. BASEBAND LAYER:

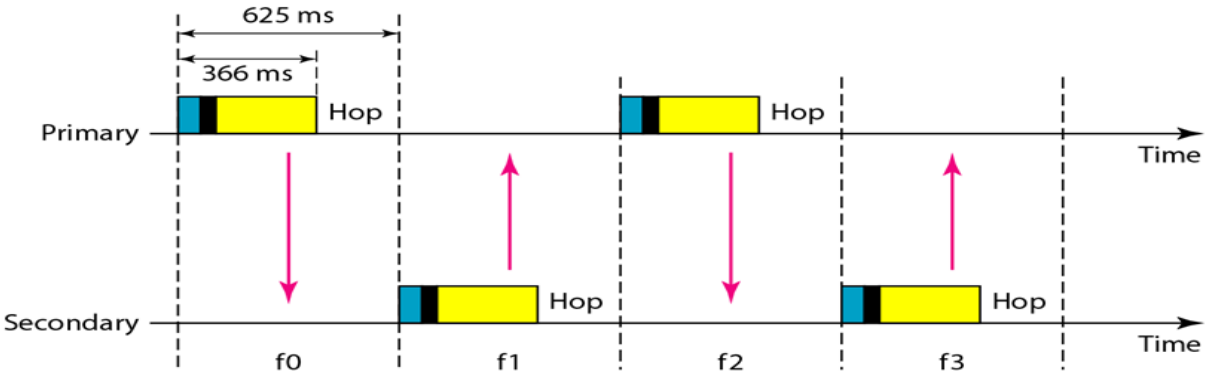
Roughly equivalent to MAC sublayer in LANs. It is **responsible for** searching other devices to **establish connection** within them It is also **responsible for assigning master and slaves and takes care of QOS.** It uses TDD TDMA i.e Time division duplex TDMA.

Time division duplexing TDMA (TDD-TDMA) is a kind of **half-duplex communication** in which the slave and receiver send and receive data, **but not at the same time** (half-duplex). However, the **communication for each direction uses different hops**, like walkie-talkies.

Single-secondary communication

- Also called Single-slave communication
    - Master (primary) uses even-numbered slots.
    - Slave (secondary) uses odd-numbered slots.

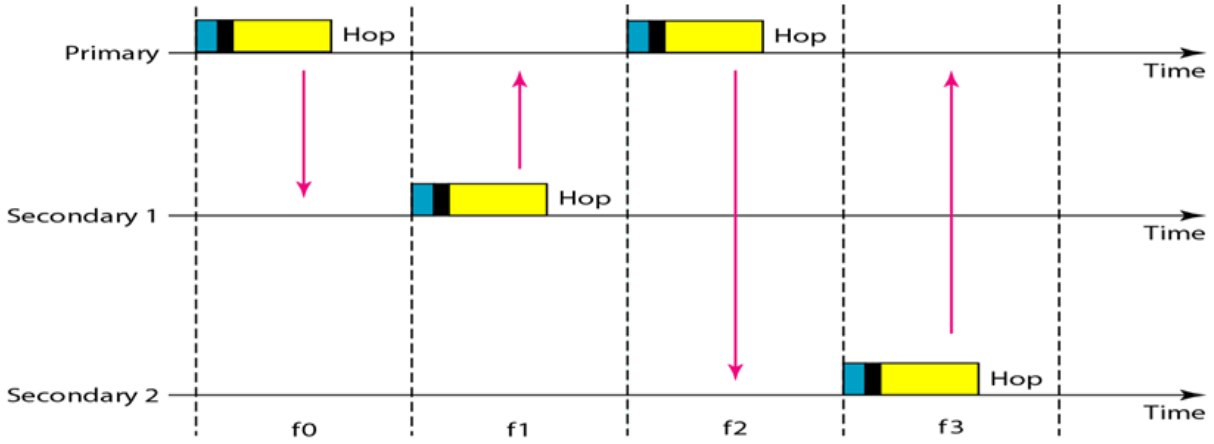
In slot 0, the primary sends, the secondary receives in slot 1 the secondary send and primary receives.



Multiple-secondary communication: The number of secondary (slave) is more than one also called Multiple-slave communication.

- Master uses even-numbered slots

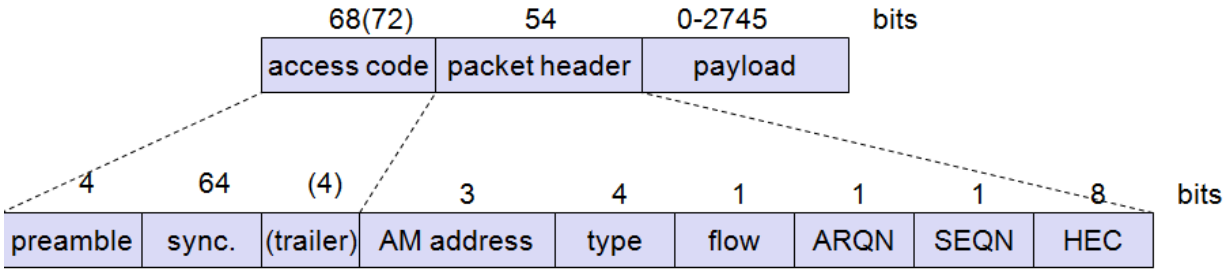
- Slave sends in the next odd-numbered slot if the packet in the previous slot was addressed to it.



In slot 0, the master sends a frame to slave 1. In slot 1 only slave 1 sends a frame to the primary because the previous frame was address to secondary 1 other slaves are silent.

In slot 2, the master sends a frame to slave 2. In slot 3 slave 2 sends a frame to the primary because the previous frame was addressed to slave 2 other slaves are silent. The cycle continues.

BASEBAND PACKET FORMAT OR FRAME FORMAT OF BLUETOOTH



Access code: It is used for synchronization and piconet identification. It consists of 4 bit preamble, a synchronization field and a trailer.

Packet header: It consists of

1. AMA Active Member Address: It identifies to which station the frame is intended.

2. Type: This 4 bit field identifies the frame type, the type of error correction used in data field.

3. Flow (F): When it is set as 1 the corresponding slave alerts the master that its buffer is full and it cannot receive data further.

4. ARQN Automatic repeat request sequence number: This 1 bit subfield used to piggyback the ACK into a frame. Bluetooth uses stop and wait ARQ.

5. SEQN Sequence number: This 1 bit field is used to number the frames to detect during retransmission.

6. HEC Header error correction: Used to detect errors in header section.

PHYSICAL LINKS: Here **two types of links** are created. Synchronous connection oriented link **(SCO)** and an Asynchronous connectionless link **(ACL)**.

SCO will be used in cases of **avoiding latency** is **more important** than integrity that is in **real time application**. No retransmission is done here.

ACL is used when **integrity is more important** than latency. Retransmission can be achieved.

3. **LINK MANAGER PROTOCOL:** It takes care of link setup and management between devices including security functions and parameter negotiation.

Note: Sometimes this topic (LMP) may ask separately also so study this topic fully.

It provides

(i**) Authentication, pairing and encryption:** The pairing service is needed to establish an initial trust relationship between two devices that have never communicated before. The result of pairing is link key generation.

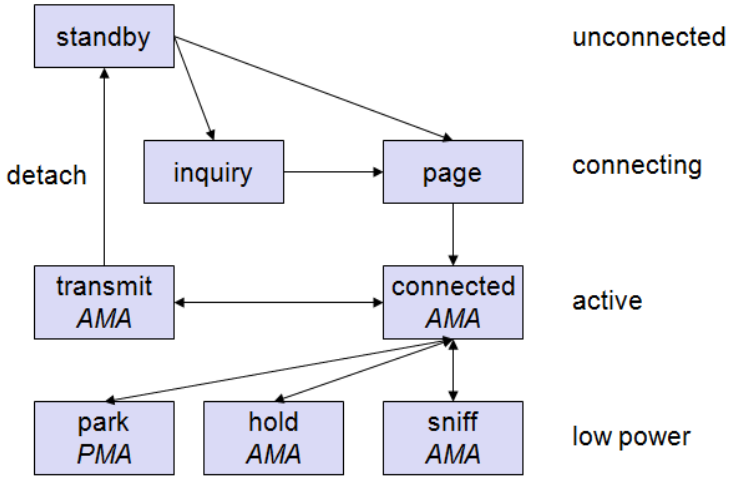
(ii) **Synchronization:** Precise (accurate) synchronization is a major important factor in Bluetooth network. The clock offset is updated each time when a packet is received from the master.

(iii) **Power control**: A bluetooth device can measure the received signal strength. Depending on this signal level the device can direct the sender to increase or decrease its transmitting power.

(iv) **Quality of service negotiation**: It takes care of the transmission time between a master and particular slave. Depending on the quality of channel the master can control the number of slots in slaves.

(v) **Link supervision**: LMP control the activity of the link. It may setup new SCO links or it may declare the failure of a link.

The figure below shows the baseband states of blueooth device.



Standby mode: Every device which is not currently participating in a piconet is in standby mode. This is a low power mode.

Inquiry mode: A station can come to this mode in two cases. Either when a station wants to form a piconet or to see what is going on. The device performs inquiry procedure by sending an inquiry access code (IAC) which is common to all bluetooth devices.

As soon as a device detects an inquiry it returns a packet containing its device and timing information required by the master to initiate a connection. From that moment onwards the device acts as slave.

If the inquiry is successful a device enters the page mode.

To save battery power a bluetooth device can go into one of three low power states:

1. Sniff state: In this mode the **device is less active**. It will sleep and only listen for transmissions at a set interval (ex. every 100 ms).

2. Hold State: It is **temporary, power saving mode** where a **device sleeps for a defined period** and then returns back to active mode when that interval has passed. The master can command a slave device to hold.

3. Park State: It is the **deepest of sleeping modes.** A master can command a slave to park and that slave will become inactive until the master tells it to wake up.

4. L2CAP (Logical Link Control and Adaptation Protocol)

Note: Sometimes this topic (L2CAP) may ask separately also so study this topic fully.

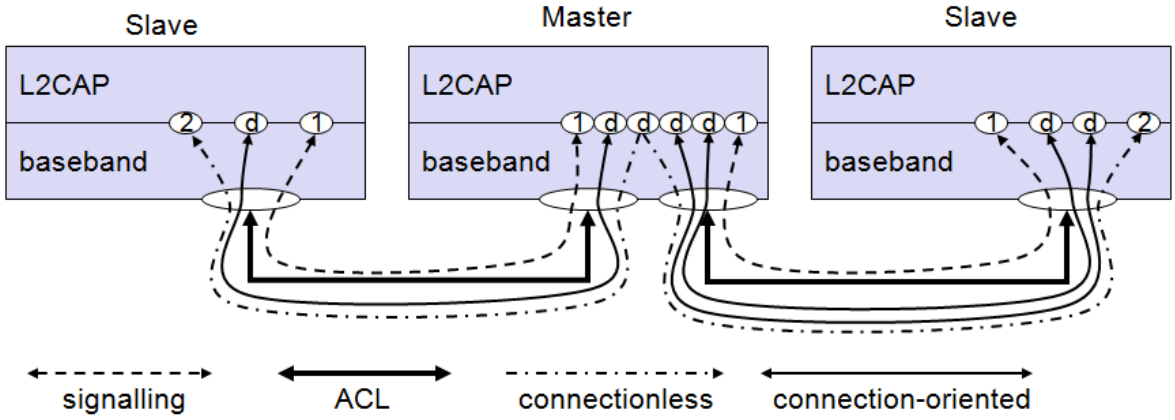
The L2CAP is associated with Asynchronous connectionless link (ACL) only. L2CAP provides three different types of logical channels between master and slave.

(i) Connectionless: These unidirectional channels are typically used for broadcasts from master to its slaves.

(ii) Connection-oriented: This channel is bi-directional and supports QOS flow specifications in both direction. These flow defines average/peak data rate, maximum burst size, latency and jitter.

(iii) Signalling: This is used to exchange signalling messages between L2CAP entities (end users).

Each channel is identified by its channel identifier (CID). For signalling channels CID value is 1, for connection-less channels the CID value is 2 and for connection oriented channel a unique CID(≥ 64) is assigned at each end of the channel to identify the connection.

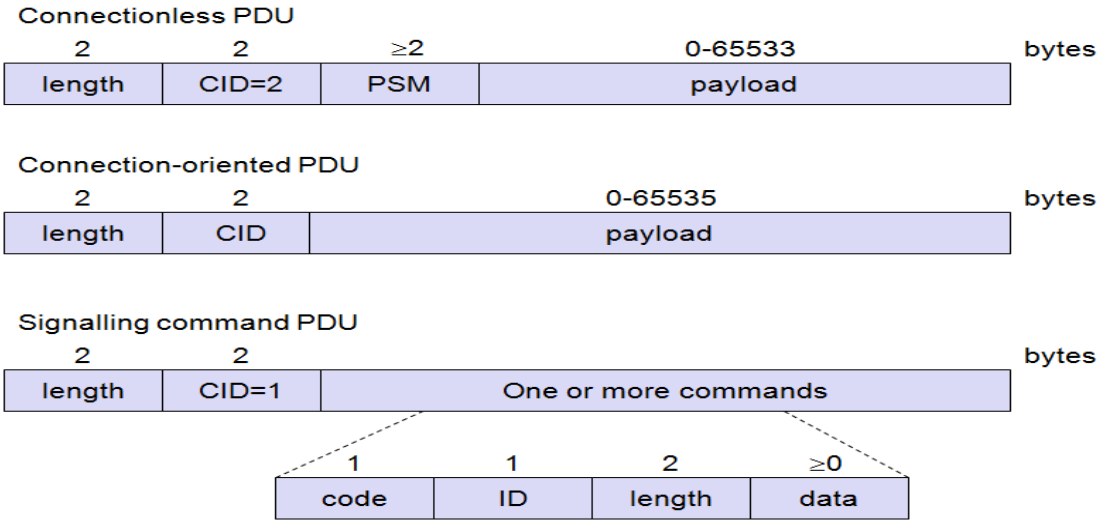


The figure below shows the three packet types belonging to three logical channel types.

Length: Indicates the length of the payload.

CID: Channel identifier for multiplexing/demultiplexing.

Payload contains one or more commands. Each command has its own code for connection reject, connection request.



OR

The major functions of L2CAP are:

1. **Segmentation and Reassembly:** It accepts the packets of upto 64Kb from the upper layers and breaks them into frames for transmission. At the receiving end these frames are reassembled into packets again.

2. Multiplexing: It handles the multiplexing and demultiplexing of multiple packet sources.

3. **Group Management:** It provides one way transmission to a group of other Bluetooth devices.

4. **Quality of service management:** During links establishment and normal operation.

5. PROTOCOLS ABOVE L2CAP

(i) WAP: Wireless access protocol: It **provides limited display size and resolution** on mobile devices.

(ii) OBEX: Object exchange protocol: It is used to browse the contents of folders on a remote device

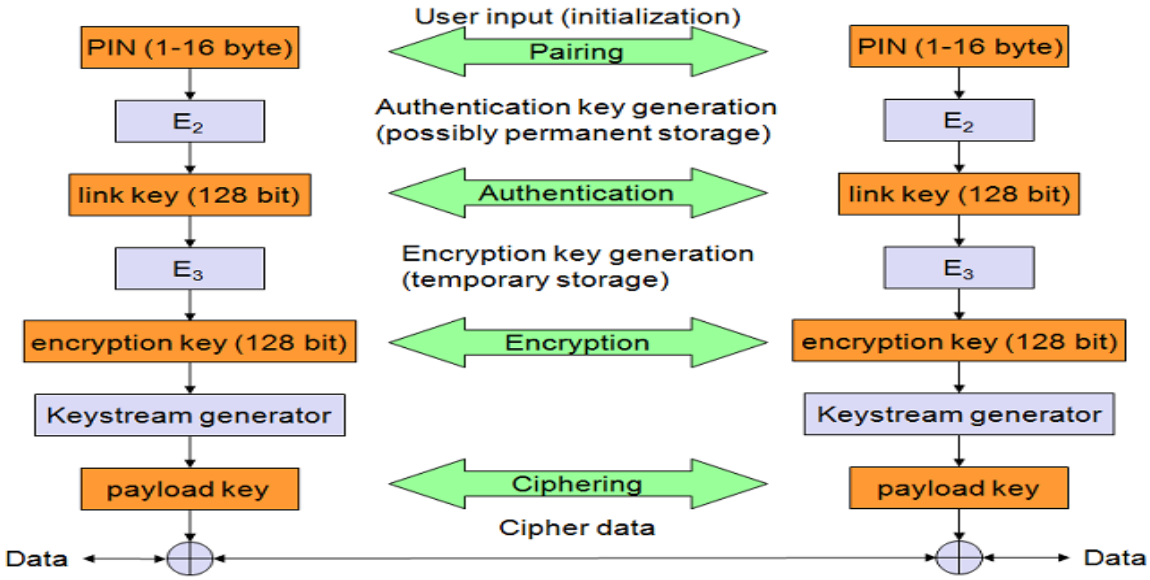
(iii) RF COMM: Radio Frequency Communication. Bluetooth prime objective is to eliminate cables and provide support for serial communication without cables. RFCOMM provides virtual serial port.

(iv) Telephony apps: (TCS BIN): It defines how telephone calls should be sent across a Bluetooth link.

(v) Service Discovery protocol: Bluetooth devices should work together with other devices in unknown environments in an ad-hoc fashion. For that purpose, Bluetooth defines the **service discovery protocol (SDP).** It discovers and learns about the services offered by other device.

It connects two or more Bluetooth devices to provide service such as faxing, printing and teleconferencing.

6. SECURITY: It involves the various steps mentioned below.



Step 1. The first step called **pairing** is necessary if two Bluetooth devices have never met before. To setup trust between the two devices a user can enter a secret PIN into both devices. This PIN can have a length of up to 16 byte.

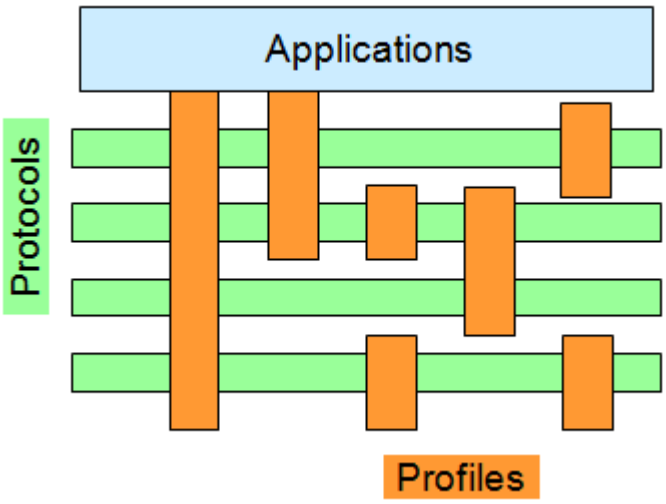
Step 2. Based on the PIN the **link key** can be **generated for authentication**. The link key is of 128 bit.

Step 3. Based on the link key values, generated for authentication an **encryption key is generated for security**. The encryption key is of 128 bits.

Step 4. Based on the encryption key, the device address a **payload key is generated as cipher text** (converting information into un human readable form). The payload key is a stream of pseudo-random bits.

Note: Ciphering process involves XOR of the user data and payload key.

7. PROFILES: Although Bluetooth started as a very simple architecture for spontaneous ad-hoc communication, many different protocols, components, extensions, and mechanisms have been developed over the last years. Application designers and vendors can implement similar, or even identical, services in many different ways using different components and protocols from the Bluetooth core standard. To provide compatibility among the devices offering the same services, Bluetooth specified many profiles in addition to the core protocols.



The following **basic profiles** have been specified: generic access, service discovery, cordless telephony, intercom, serial port, headset, dialup networking, fax, LAN access, generic object exchange, object push, file transfer, and synchronization.

Additional profiles are: advanced audio distribution, PAN, audio video remote control, basic printing, basic imaging, generic audio video distribution, hands-free, and hardcopy cable replacement.

APPLICATIONS

1. It replaces the cables with radio links.
2. It acts as hotspots for wireless networking.
3. To transfer patient information from remote area to hospitals.
4. It is used in wireless head sets.

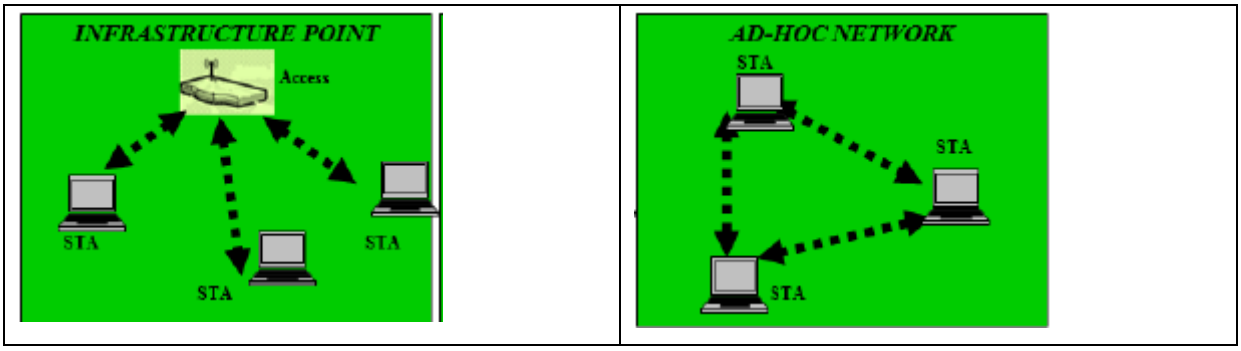
5. It is also used in printers.

LIMITATIONS:

1. Poor data security.
2. Short battery life.
3. Data speed is slow.

Comparison between Ad-Hoc and Infrastructure:

Infrastructure	**Ad-Hoc**
In infrastructure mode, the communication occurs only between the wireless nodes and access points (AP) , but not directly between wireless nodes	In ad-hoc mode, each node communicates directly with other nodes, so no access point control is needed.
IEEE 802.11 & HIPERLAN2 are based on infrastructure mode.	Bluetooth is a typical ad-hoc network.
Most infrastructure based WLAN uses TDMA-based protocols	Most Ad-hoc based WLAN uses contention MAC protocols (e.g. CSMA)
It has AP hence individual stations no need to worry about checking of channel busy or ideal. It will be taken care by AP. Hence that burden is reduced for individual stations involved in the network.	Since, it does not have access point (AP) the responsibility of channel detection such as busy or idle have to be done by all stations involved in the network.
Physical infrastructure is needed	Physical infrastructure is not required

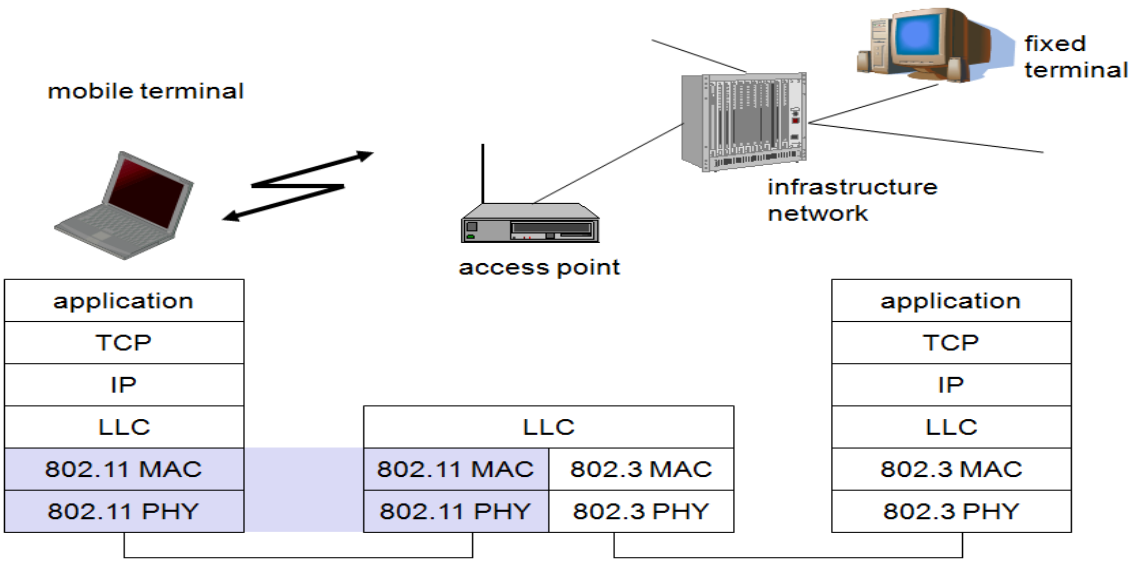


Explain IEEE 802.11 architecture:

802.11 standard defines two kinds of network with respect to access point. They are Ad-Hoc Network and Infrastrucutre network.

1. SYSTEM ARCHITECTURE - REFER HAND WRITTEN NOTES

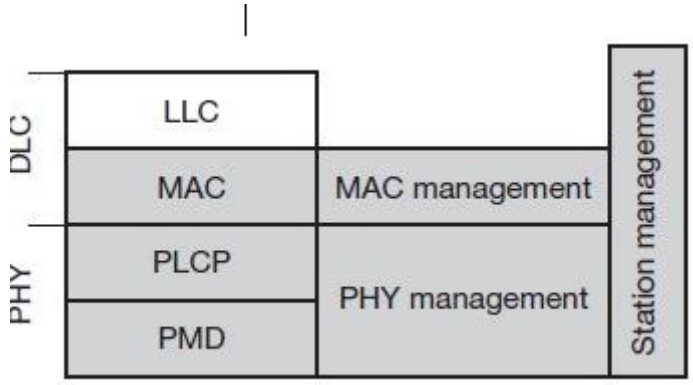
2. PROTOCOL ARCHITECTURE: The IEEE 802.11 consists of physical layer and data link layer. The data link layer has two sublayers called MAC sublayer and LLC sublayer



At the mobile terminal end the physical layer and MAC layer is 802.11 and at the fixed terminal it is 802.3.

PHYSICAL LAYER

The physical layer is subdivided into the **physical layer convergence protocol (PLCP)** and the **physical medium dependent PMD** as shown in figure below.



PLCP sublayer

- It provides a carrier sense signal, i.e it checks whether the channel is idle or busy. It is referred to as **clear channel assessment (CCA).**
- It provides a common PHY service access point (SAP) independent of the transmission technology.

PMD sublayer: Handles modulation and encoding/decoding of signals.

MAC management:

- Provides association and re-association of a station to an access point and roaming between different access points.
- It also providess authentication, encryption, synchronization of a station with regard to an access point, and power management to save battery power.
- MAC management also provides MAC **management information base (MIB).**

PHY management include channel tuning and PHY MIB maintenance.

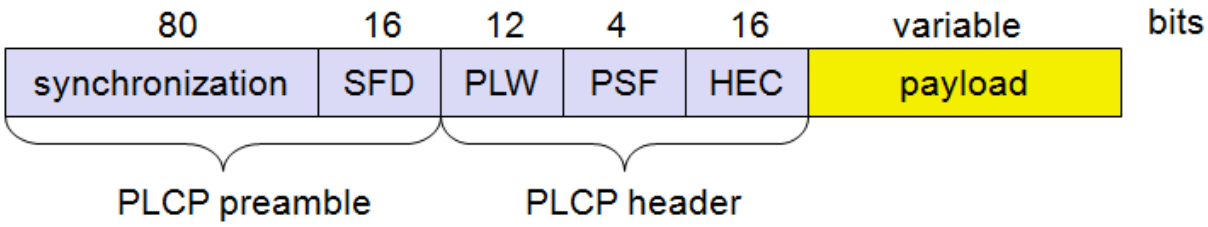
Station management interacts with both management layers and is responsible for additional higher layer functions .

1. PHYSICAL LAYER: Three physical medias are defined in the original 802.11 standard. FHSS, DSSS, OFDM and IR.

Spread spectrum: Involves the use of higher band width than the required data rate to minimize interference and to reduce the error rate.

(i) FHSS (Frequency hopping spread spectrum): In this technique spread spectrum is achieved by frequency jumping from one carrier to another, if there is an interference at a given frequency it only affects a small fraction of transmission.

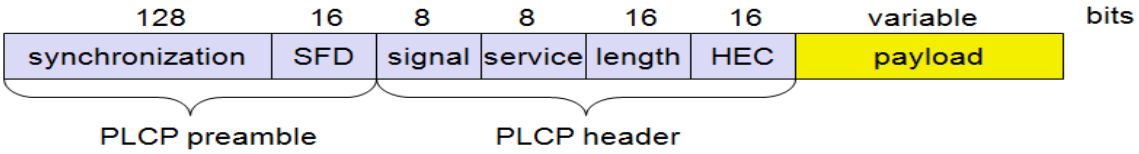
FHSS PHY packet format



The fields of the frame fulfill the following functions:

- **Synchronization:** The PLCP preamble starts with 80 bit synchronization, which is a 010101... bit pattern. This pattern is used for synchronization of potential receivers and signal detection by the CCA.
- **Start frame delimiter (SFD):** The following 16 bits indicate the start of the frame and provide frame synchronization. The SFD pattern is 0000110010111101.
- **PLCP_PDU length word (PLW):** PLCP header indicates the **length of the payload** in bytes including the 32 bit CRC at the end of the payload. PLW can range between 0 and 4,095.
- **PLCP signalling field (PSF):** This 4 bit field indicates the **data rate** of the payload following. All bits set to zero (0000) indicates the lowest data rate of 1 Mbit/s and the maximum is 8.5 Mbit/s (1111). This system obviously does not accommodate today's higher data rates.
- **Header error check (HEC)**: Finally, the PLCP header is protected by a 16 bit checksum with the standard ITU-T generator polynomial $G(x) = x^{16} + x^{12} + x^5 + 1$.

(ii) DSSS (Direct sequence spread spectrum): It increases the data rate of a signal by mapping each data bit into string of bits with one string used for binary 1 and other for binary 0.



- **Synchronization:** The first 128 bits are not only used for synchronization, but also gain setting, energy detection (for the CCA), and frequency offset compensation. The synchronization field only consists of scrambled 1 bits.

  ● **Start frame delimiter (SFD):** This 16 bit field is used for synchronization at the beginning of a frame and consists of the pattern 1111001110100000.

  ● **Signal:** Originally, only two values have been defined for this field to indicate the data rate of the payload. The value 0x0A indicates 1 Mbit/s, 0x14 indicates 2 Mbit/s (and thus DQPSK). Other values have been reserved for future use, i.e., higher bit rates.

  ● **Service:** This field is reserved for future use; however, 0x00 indicates an IEEE 802.11 compliant frame.

  ● **Length:** 16 bits are used in this case for length indication of the payload in microseconds.

  ● **Header error check (HEC):** Signal, service, and length fields are protected by this checksum using the ITU-T CRC-16 standard polynomial.

(iii) OFDM (Orthogonal frequency division multiplexing): It uses multiple carrier signals at different frequencies; it is used in IEEE 802.11a with data rate from 6 to 54 Mbps.

(iv) Infra Red: The PHY layer, which is based on infra red (IR) transmission, uses near visible light at 850–950 nm. Infra red light is not regulated apart from safety restrictions (using lasers instead of LEDs). The standard does not require a line-of-sight between sender and receiver, but should also work with diffuse light. This allows for point-to-multipoint communication. The maximum range is about 10 m if no sunlight or heat sources interfere with the transmission. Typically, such a network will only work in buildings, e.g., classrooms, meeting rooms etc.

MAC LAYER:

The functions provided by MAC layer are:

1. It regulates the frames properly to the exact radio frequency band so that station transmissions do not interfere with one another.

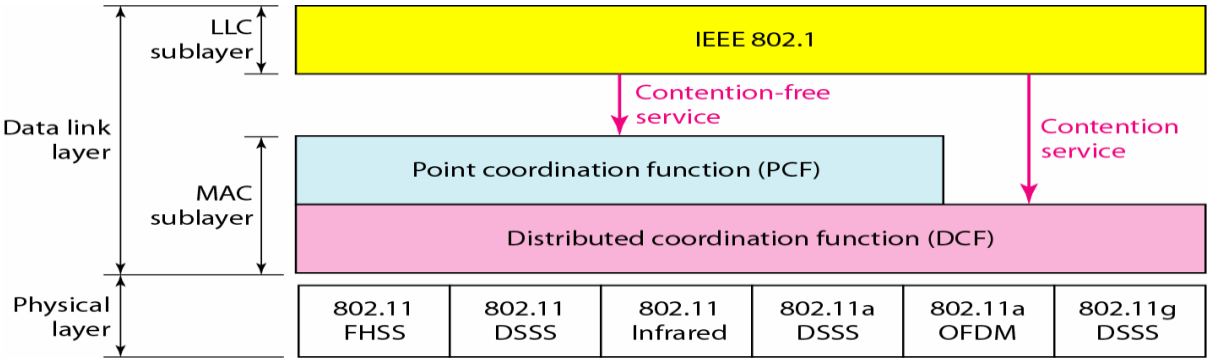
2. Error checking

3. Authentication

4. Power conservation

The MAC has further two layers called **point coordination function (PCF) and Distributed co-ordination function (DCF).**

DCF: It uses CSMA/CA as the access method. Wireless LAN cannot implement CSMA/CD due to the hidden station problem.



PCF: Used to provide contention free service. Higher priority traffic makes use of PCF.

LLC: It provides functions such as Error control.

Wireless LANs cannot implement CSMA/CD for three reasons:

1. For collision detection a station must be able to send data and receive collision signals at the same time.

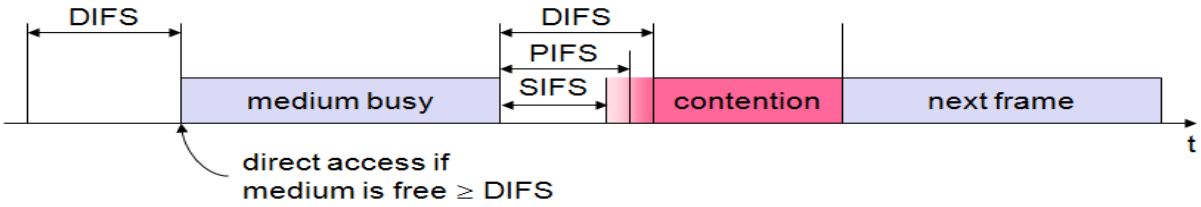
2. Collision may not be detected because of the hidden station problem.

3. The distance between stations may result in Signal fading which prevent a station at one end from hearing a collision at the other end.

Therefore, collisions are avoided by using three methods in CSMA/CD:

1. Interframe space
2. Contention window
3. Acknowledgements

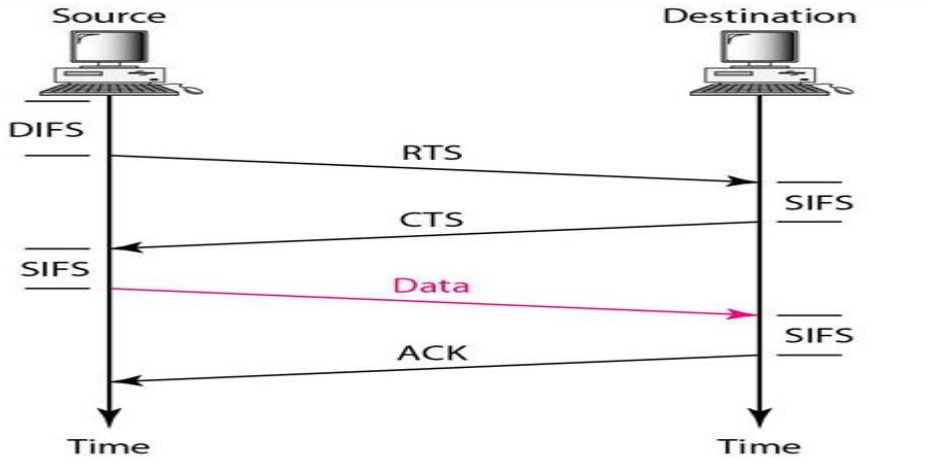
Interframe space: During a contention phase several nodes try to access the medium.



Short inter-frame spacing (SIFS): The shortest waiting time for medium access (so the **highest priority**) is defined for short control messages, such as acknowledgements of data. Immediate actions.

PCF inter-frame spacing (PIFS): A waiting time between DIFS and SIFS (and thus a medium priority) is used for a time-bounded service. PIFS is defined as SIFS plus one slot time.

DCF inter-frame spacing (DIFS): This parameter denotes the **longest waiting time** and has the **lowest priority** for medium access. This waiting time is used for asynchronous data service within a contention period.



DIFS is defined as SIFS plus two slot times.

The station which is ready to send starts sensing the medium if the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending. if the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time) CW = 7, 15, 31, 63, 127 if another

station occupies the medium during the back-off time of the station, the back-off timer stops (fairness).

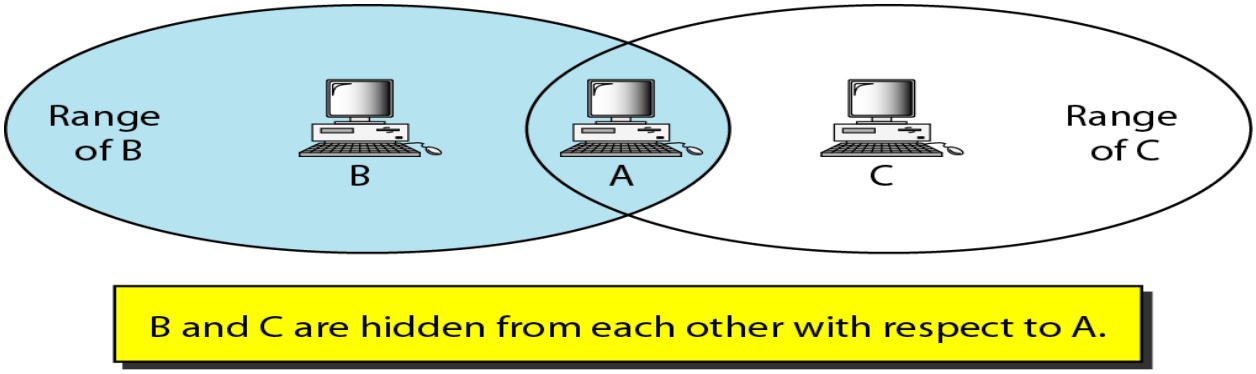
Contention window: It is an amount of time divided into slots. A station that is ready to send choses a random number of slots as its wait time.

Station set one slot for the first time and then double each time the station cannot detect an idle channel after the IFS time.

In this method; the station finds the channel busy it does not restart the process it just stops the timer and restarts it when the channel is sensed as idle. This method gives priority to the station with longest waiting time.

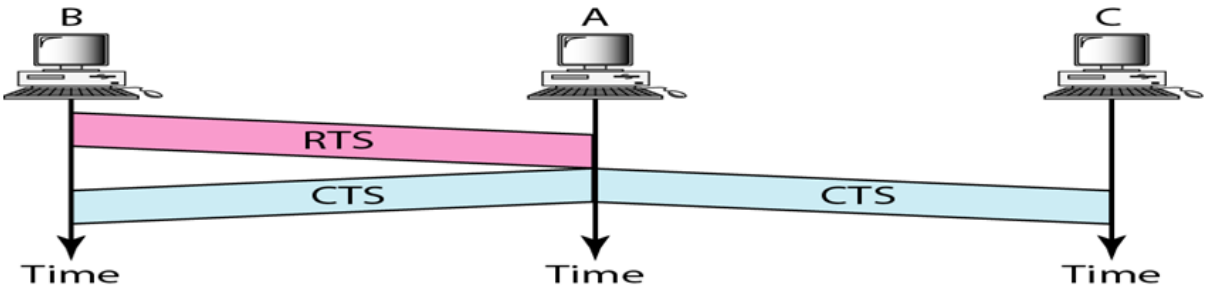
Acknowledgements: The data may be corrupted during the transmission. The positive ACK and the time out can help guarantee that the receiver has received the frame.

Hidden Station Problem



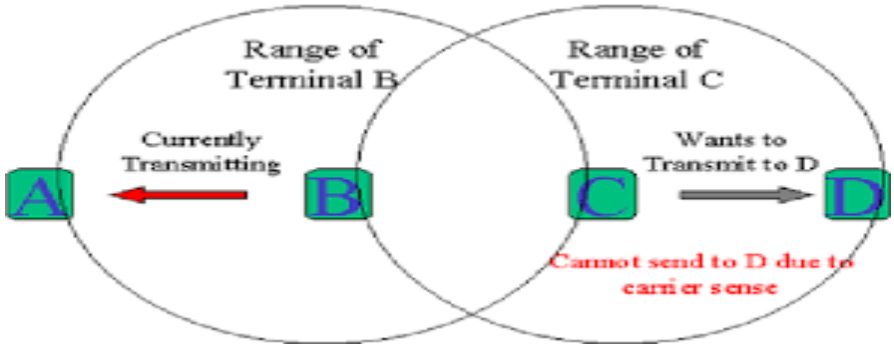
There is no mechanism for collision detection, if the sender has not received a CTS frame from the receiver, assumes there has been a collision, the sender tries again.

The solution to the hidden station problem is the use of the handshake frames (RTS and CTS) that we discussed earlier. Figure shows that the RTS message from B reaches A, but not C.



However, because both Band C are within the range of A, the CTS message, which contains the duration of data transmission from B to A reaches C. Station C knows that some hidden station is using the channel and **refrains** (from transmitting until that duration is over).

Exposed Station Problem: In wireless networks, when a node is prevented from sending packets to other nodes because of neighboring transmitter it is known as exposed node problem.



Here, we have 4 nodes A,B,C,D where the two receivers A & D are out of range of each other whereas the two transmitters B & C are in the range of each other.

Here transmission takes place between B & A at the same time C can transmit to D. But C by mistake it senses the channel and concludes channel is busy.

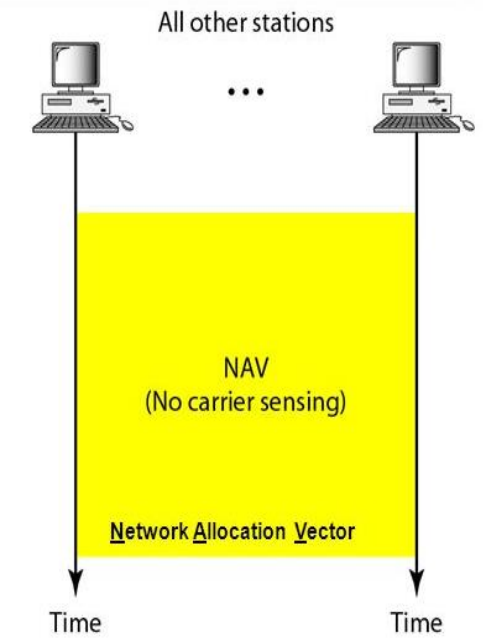
Therefore, unnecessary delay arrives.

NOTE

Hidden terminal causes collision.	Exposed terminals causes unnecessary delay.

Network allocation vector (NAV) used to avoid collision.

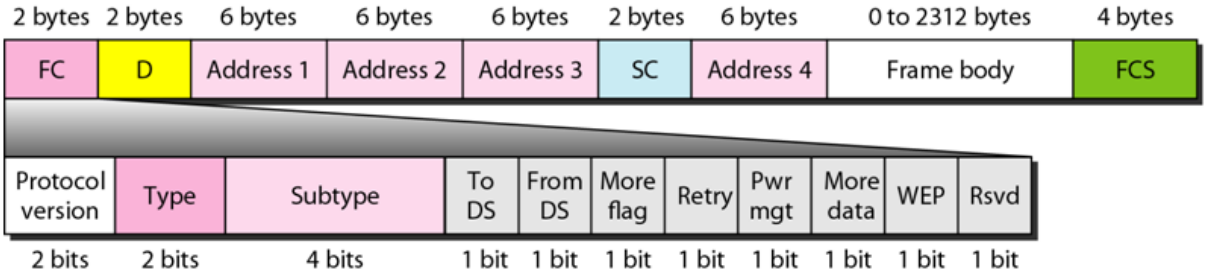
- RTS frame includes the duration of time that it needs to occupy the channel.



- Stations affected by this transmission create a timer called (NAV)
- The network allocation vector (NAV) shows the time must expire before these allowed to check the channel for idleness.

Explain MAC frame format:

❖ The MAC layer frame consists of nine fields



- **Frame control**: 2 bytes long and defines the type of frame and some control information.
- **D**: In all frame types except one, this field defines the duration of the transmission that is used to set the value of NAV. In one control frame, this field defines the frame ID.
- **Addresses**: There are four address fields, each 6 bytes long. The meaning of each address field depends on the value of the *To DS and From DS subfields.*

- **Sequence control:** This field defines the sequence number of the frame to be used in flow control.
- **Frame body:** This field can be between 0 and 2312 bytes, it contains information based on the type and the subtype defined in the FC field.
- **FCS:** The FCS field is 4 bytes long and contains a CRC-32 error detection sequence.
- **Protocol version:** This 2 bit field indicates the current protocol version and is fixed to 0 by now. If major revisions to the standard make it incompatible with the current version, this value will be increased.
- **Type:** The type field determines the function of a frame: management (=00), control (=01), or data (=10). The value 11 is reserved. Each type has several subtypes as indicated in the following field.
- **Subtype:** Example subtypes for management frames are: 0000 for association request, 1000 for beacon. RTS is a control frame with subtype 1011, CTS is coded as 1100. User data is transmitted as data frame with subtype 0000. All details can be found in IEEE, 1999.
- **To DS/From DS:** Explained in the following in more detail.
- **More fragments:** This field is set to 1 in all data or management frames that have another fragment of the current data.
- **Retry:** If the current frame is a retransmission of an earlier frame, this bit is set to 1. With the help of this bit it may be simpler for receivers to eliminate duplicate frames.
- **Power management:** This field indicates the mode of a station after successful transmission of a frame. Set to 1 the field indicates that the station goes into power- save mode. If the field is set to 0, the station stays active.
- **More data:** In general, this field is used to indicate a receiver that a sender has more data to send than the current frame. This can be used by an access point to indicate to a station in power-save mode that more packets are buffered. Or it can be used by a station to indicate to an access point after being polled that more polling is necessary as the station has more data ready to transmit.
- **Wired equivalent privacy (WEP):** This field indicates that the standard **security mechanism** of 802.11 is applied.
- **Order:** If this bit is set to 1 the received frames must be processed in strict order. MAC

frames can be transmitted between mobile stations and an access point over a DS.

Two bits within the Frame Control field, '**to DS**' and '**from DS**', differentiate these cases and control the meaning of the four addresses used. Table gives an overview of the four possible bit values of the DS bits and the associated interpretation of the four address fields.

to DS	from DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	–
0	1	DA	BSSID	SA	–
1	0	BSSID	SA	DA	–
1	1	RA	TA	DA	SA

Write short notes on HIPERLAN:

HIPERLAN:

- High performance LOCAL AREA NETWORK
- It was given by ETSI(European Telecommunication Standard Institute)

OBJECTIVE OF HIPERLAN/NEDD FOR HIPERLAN

- HIPERLAN **does not conflict with microwave and other kitchen appliances** which are operated on 2.4 GHZ. Since HIPERLAN operates at around 5GHZ.
- It can be **used for high speed short range applications** (23.5 Mb/s for a range of 50m)

CLASIFICATION OF HIPERLAN

- HIPERLAN 1
- HIPERLAN 2
- HIPERLAN 3 OR HIPERACCESS
- HIPERLAN 4 OR HIPERLINK

HIPERLAN 1:

- It is an Radio LAN
- It Operates at 5.15 to 5.3GHZ
- It Covers up to 50 meters
- Its data rate is up to 23.5Mb/s

- Services offered by HIPERLAN 1 is compatible with the standard MAC services provided by IEEE 802.X LANS
- Address is based on 48 bit MAC address

SPECIAL FEATURE OF HIPERLAN 1:

- It supports or **forwards the data** or **extends the communication where radio waves cannot able to provide energy further with the help of relays**.
- These relays are **special relays also called power conservation nodes** or power savers (P-saver).

Principle:

For power conservation a node will generate a specific wake up pattern. This pattern determines at what time the node is ready to receive the data remaining time the node can turn off its receiver and save energy. These nodes are called power-savers.

The **node which contains the bit pattern for power conservation are called p-supporters** and the **node which awakes & goes to rest in the particular period are called p-server**.

Explain the access scheme used in HIPERLAN 1 or what are the various phases involved in HIPERLAN 1:

Access scheme involved in HIPERLAN:

EY-NPMA [Elimination -Yield non primitive priority multiple access]

Principle:

In general every user will have a priority to access the channel based on their requirement. Hence in HIPERLAN EY-NPMA arised which divides the channel based on the requirement as

- Prioritization phase
- Contention phase
- Transmission phase

Prioritization:

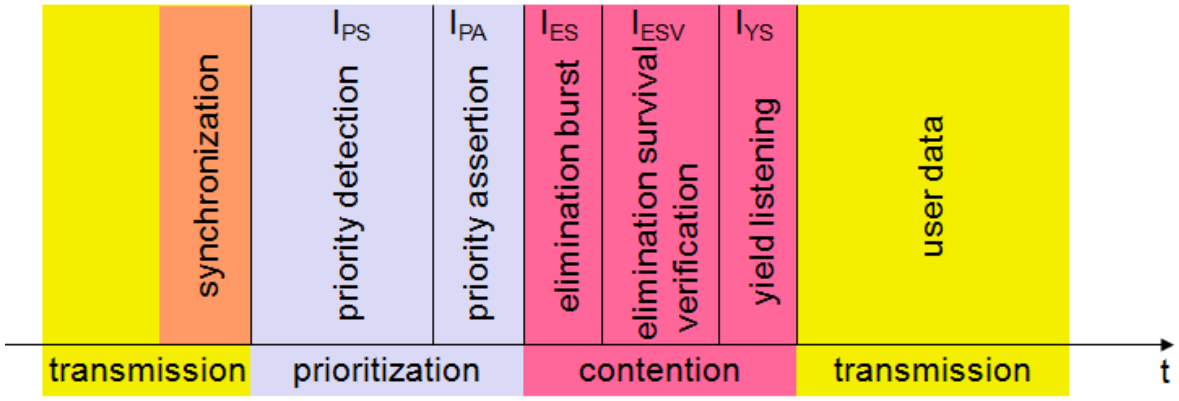
It determines the highest priority of data packet ready to be sent by competing nodes.

Contention:

Here all contenders are eliminated except the one who is also having highest current priority.

Transmission:

In this phase it transmits the packet of remaining node.



Diagram

- For every node to transmit the data the access cycle starts with synchronization to the current sender. Initially prioritization phase allows after that contention phase which is further divided into elimination & yield phase.
- The purpose of elimination phase is to eliminate as many contending nodes as possible and making only one node to be available.
- The remaining node can transmit its data in transmission phase.
- Each phase is divided into various slots.
- Ps-time slot for priority detection phase
- Pa-time slot for priority assert phase
- Similarly, ES, Esv & Ys for elimination burst, elimination survival verification & for yield listening

PRIORITIZATION PHASE:

Objective:

The node with lower priority should not get access or chance at any cost while the higher priority nodes are waiting. Even though there exists more load on low priority station.

Operation:

In this phase the time is divided into 5 slots (slot 0 highest priority) to slot 4 (lowest priority). If a station wishes to transmit it checks all the slots. If all the slots were find to idle then the node transmits immediately a burst.

Elimination phase: Multiple nodes now enter the elimination phase again time is divided into slots (12)

- During this period each terminal runs a random number generator to select one of the 12 dividable slots.
- During these 12 slots the mobile station sends a burst for verification of channel is busy or idle.
- When it does not hear any other burst after transmission next burst will be sent after 12 th slots in the elimination phase.

YIELD PHASE:

- In this phase the remaining nodes only listens into the medium without sending any additional bursts.
- Again time is divided into 0 to 9 slots. Each node now listens for its yield listening period. If it finds idle the station will transmit the date.

---

2. Write short note on HIPERLAN 2:

Need:

1. To obtain high QOS.

2. To provide dynamic frequency selection

Features of HIPERLAN 2:

1. High throughput transmission: HIPERLAN 2 not only offers upto 54 Mb/s at physical layer but also 35 Mb/s at network layer.

2. Connection oriented: Prior to data transmission HIPERLAN 2 networks .establish logical connections between a sender and receiver.

3. Quality of service support: Since connections are defined priority QOS achieving its simple. Each connection has its own set of QOS parameters (band, delay, and jitter)

4. Dynamic frequency selection: HIPERLAN 2 does not require frequency planning of cellular networks. All access points have an appropriate frequency within their coverage area. All APS listen to neighbouring AP s as well as to other radio sources in the environment.

The best frequency is chosen depending on the current interference level and usage of radio channels.

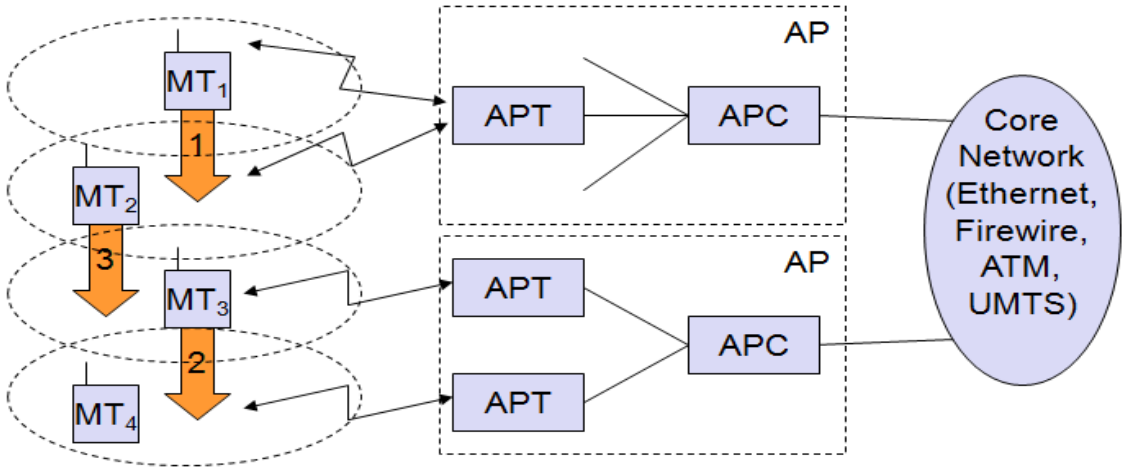
5. Security support: Authentication as well as encryption is supported by HIPERLAN 2 both mobile terminal & AP can authenticate each other.

6. Mobility support: Mobile terminals can move around while transmission always takes place between the terminal & access point with the best radio signal handover between access points is performed automatically.

7. Power scale: mobile terminals can negotiate certain wake up patterns to save power.

REFERENCE MODEL & CONFIGURATION / HIPERLAN 2 BASIC STRUCTURE & HANDOVER SCENARIO

- In the example shown below two access points (AP) are attached to a core network core networks might be ethernet LANS, ATM networks, UMTS 3G cellular phone n/w etc.



- Each AP consists of an access point controller (APC) and one more .Access point transceivers (APT).
- An APT can comprise one or more sectors.
- Four mobile terminals shown in fig below can move from one cell to other cell.
- The stations automatically by themselves assign the APT/AP with best transmission quality.
- No frequency planning is necessary since the APS by themselves select the appropriate frequency via dynamic selection technique.

Three handover situations may occur:

1. **Sector handover (Inter sector):** Here sector antenna is used. The radiation pattern will be in some sector shape. Used in all base stations. Hanged on cell point towers. Antenna radiates a horizontal fan-shaped beam in vertical axis so it does not spill over into neighbouring sectors.

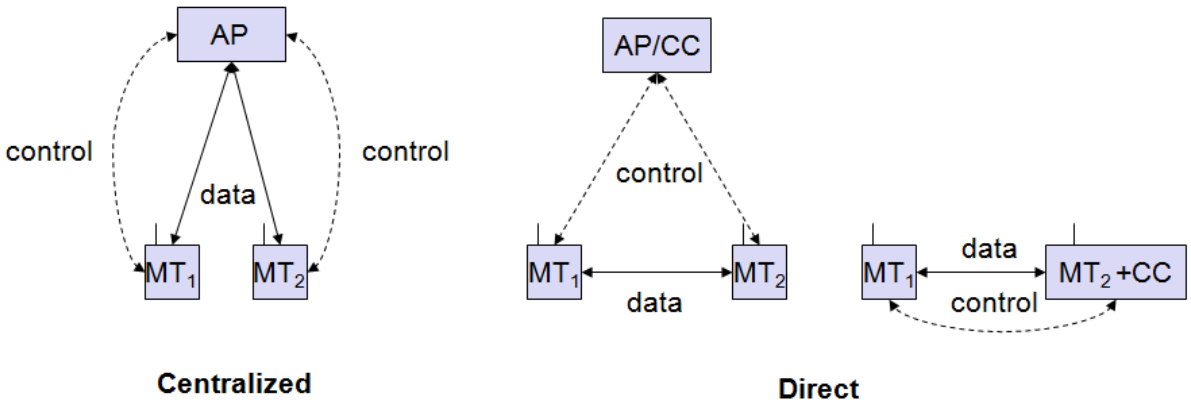
2. Radio handover: In the fig shown above the MT3 moves the service one APT to another APT but both is connected to some AP. Hence all encryption keys authentication and connection parameters do not have to be renegotiated.

3. Network handover: MT2 moves from one APT to other APT but both are connected to different AP, these cases will be supported by core network.

OPERATING MODES INVOLVED IN HIPERLAN 2:

- Centralised mode
- Direct mode

Centralized mode (CM): Here all Aps are connected to core network and MTS are associated with AP's even if two MTs share the same cell all data is transferred via the AP.

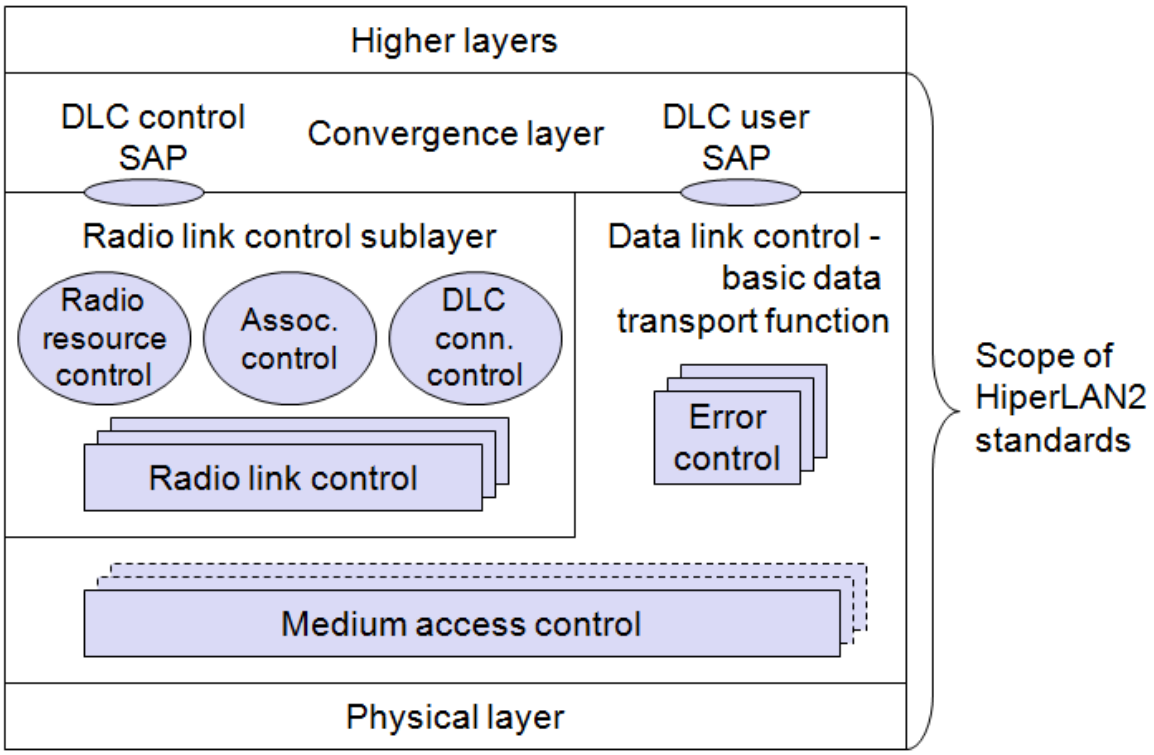


Direct mode (DM): **D**ata is exchanged directly between MTS if they can receive each other but the network still has to be controlled. This can be done via an AP that contains a central controller (CC) or via an MT that contains the CC functionality.

HIPERLAN2 PROTOCOL STACK (LAYERS):

It is divided into 3 sections

1. Physical layer 2.Data link control (DLC) 3. Higher layers

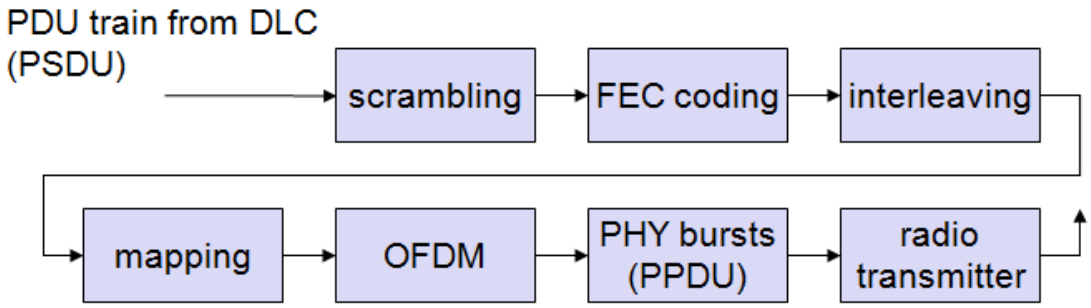


Physical layer: Performs modulation, forward error correction, signal detection synchronization.

Data link control layer: It consists of two layers: Radio link control sublayer and error control layer.

- The RLC takes care of association, authentication as well as resource allocation functions.
- The radio resource control (RRC) handles handover between APs and within an AP. These functions control the dynamic frequency selection and power save mechanisms of the MTs.
- On the top of the DLC layer there is the **convergence layer**. It takes care of **segmentation and reassembly functions.**

HIPERLAN2 physical layer reference configuration: The first step is scrambling for DC blocking and whitening of the spectrum. The result of this step is scrambled bits.



The second step is **FEC coding for error protection**. The type of coding depends on the type of data and the usage of antenna. The result of this is encoded bit.

The third step is **interleaving is done to avoid fading**. These datas are mapped on to corresponding data bits. The results of this mapping are subcarrier modulation symbols.

The **OFDM modulation step converts these symbols into a baseband signal with the help of inverse FFT.**

The last step before radio transmission is creation of PHY bursts.

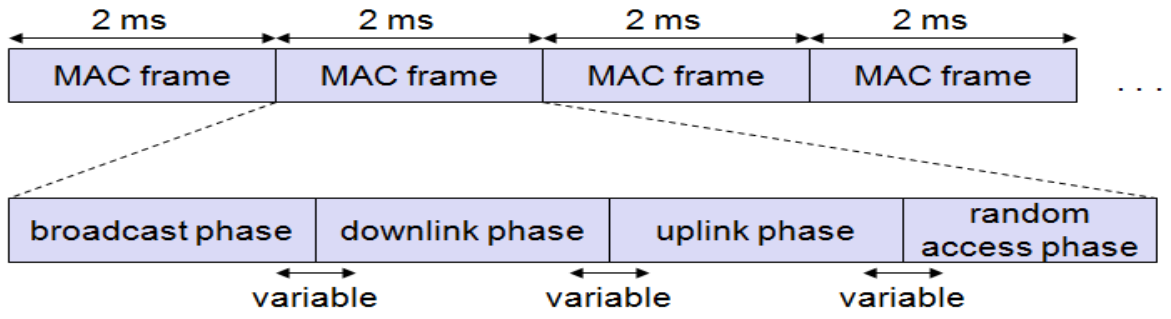
Data link layer: Here each MAC frame is sub-divided into four phases with variable boundaries.

Broadcast phase: The AP of a cell broadcasts the content of the current frame plus information about the cell (identification, status, resources).

Downlink phase: Transmission of user data from AP to the MTs.

Uplink phase: Transmission of user data from MTs.to an AP**.**

Random access phase: The transmission will take place from already registered MTs and from non- registered MTs

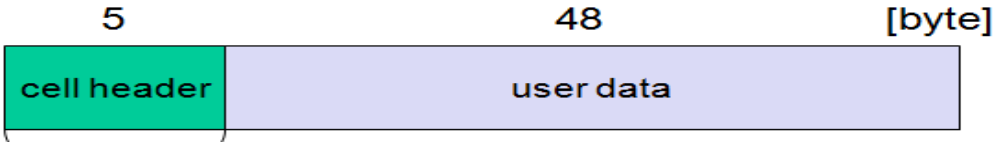


WATM:

Wireless ATM also called wireless, mobile ATM or WMATM.

ATM: Asynchronous Transfer Mode.

It is a switching technique used by telecommunication networks that uses Asynchronous Time Division Multiplexing.



In ATM the datas are transmitted as fixed size called cells .Each cell is of 53 bytes.

Motivations of WATM/features of ATM:

- ATM supports both CBR &VBR (i.e) constant bit rate & variable bit rate data.
- Suitable for customers that need red time audio (or) video services without compression.
- High data rate
- Low error rate between switching centres
- Low operating cost

The following features motivated ATM to achieve these in wireless set up.

Parameters to be considered for mobile ATM:

1. Location management: should be capable of identifying the mobile terminal present location.

2. **Mobile routing: E**venthough, the location of the terminal is identified the network has to transfer the data in an appropriate route for efficient routing.

3. QOS: The set up should provide high QOS to the data delivered.

4. Handover signalling: the network should be capable of identifying the new Access point (AP) whenever the mobile terminal moves from one network to another network.

WATM services/applications of WATM:

1. Office environments, online multimedia database access, multimedia conferencing.

2. Universities, school, training centres, in distance learning.

3. Industry: Real time data transmission, information retrieval, surveillance.

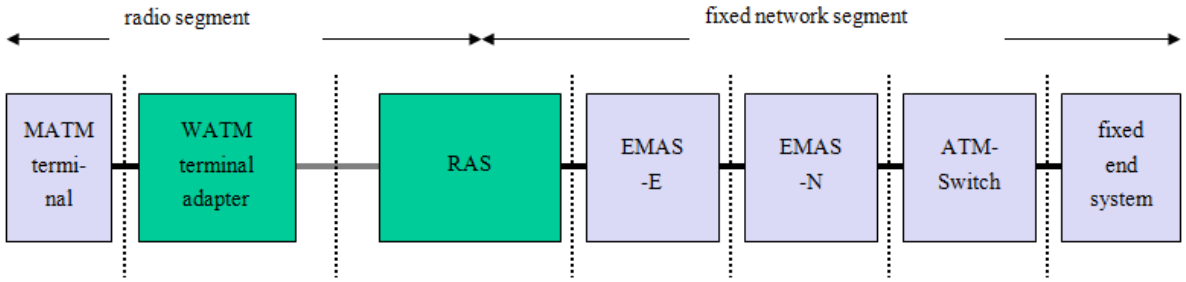
4. Hospitals: Medical images, remote diagnosis of patients at home.

5. Network vehicles: All vehicles used for the transportation of people or goods will have local area network WATM could provide service for these applications. Even WATM helps in preventing accidents.

Wireless ATM reference model/generic WATM:

Reference model: it consists of two sections .

1. Fixed ATM network
2. Radio Access segment



- (MATM) Mobile ATM terminal uses a wireless ATM (WATM) terminal adapter to get access from a radio access system
- Mobile ATM terminals could be laptops.
- The WATM terminal adapter enables wire access (i.e) it includes the transceiver etc.
- The radio access system with the radio transceiver is connected to a mobility enhanced ATM switch(EMAS-E), which in turn connects to the ATM network with mobility aware switch (EMAS-N).
- Finally a wired end system is connected as a partner in communication system.

The wireless ATM radio access structure consists of radio physical layer (PHY), medium access control (MAC), data link control (DLC) & wireless control.

Mobile ATM: It deals with higher layer control/signalling functions needed to support mobility. It includes handover, location management, routing addressing and traffic management.

Radio Access layer it consists of

- Physical layer
- MAC (Medium Access layer)
- DLC(data link layer)
- RRC(Radio Resource Control)

Handover:

- In general mobile terminal moves from one place to another. Hence it is necessary to handover its on going connections from the old radio port to the new one.
- The decision to change the radio port is made either by the mobile terminal or the base station based on signal strength measurements.

Parameters or constraints during handover:

1. Handover of multiple connections: WATM must support more than one connection, this results in rerouting of every connection after handover. However, resource availability may not allow rerouting of all connections which leads to QOS degradation. In such cases a terminal may decide to accept a lower quality or to drop single.

2. Handover of point to multi port connections: Since seamless (continuation) or consistent connection is one of the major advantages of ATM technology. WATM handover should support these types of connection.

3. QOS support: Handover should aim to preserve the QOS of all connections during handover, but it is not possible due to limited resources, hence QOS renegotiation and dropping of connections on a priority basis may be required.

4. Data integrity and security: WATM handover should minimize cell loss and avoid all duplication or reordering.

Location management:

Generally, the user can move from its home switch or home agent to a foreign agent while it moving its physical or permanent address of home agent should be known to the home base station. Then only the current location of the mobile terminal can be identified even in the foreign network.

It is achieved by registering in the base station of every network when it leaves the home agent.

Parameters to be considered in location management:

1. Transparency of mobility: Transparent roaming between different domains should be possible.

2. Security: All location and user information collected for location management and accounting should be protected against unauthorized disclosure.

3. Efficiency and scalability: Every function and system involved in location management must be scalable and efficient. The performance of all operations should be practically independent of network size, number of current connections and network load.

4. Identification: Location management must provide the identity of all entities in the network.

Mobile quality of service (M-QOS): Two different types of QOS can be provided during handover:

1. Hard handover QOS: The QOS with the current RAS may be guaranteed due to the current availability of resources no QOS guarantees are given after the handover. If there are not enough resources after handover (to many users are already in the target cell) the system cuts off the connection. This is the only possible solution if the applications and terminals cannot adopt to the new situation. It is referred to as hard handover QOS.

2. Soft handover QOS: Even for current wireless segment only statistical QOS guarentees can be given and the applications also have to adopt after the handover during congestion period or strong interference. It is referred to as soft handover QOS.

WATM REFERENCE MODEL WITH DIFFERENT SCENARIOS:

It is the standard ATM terminal that offers the ATM services defined for fixed ATM networks.

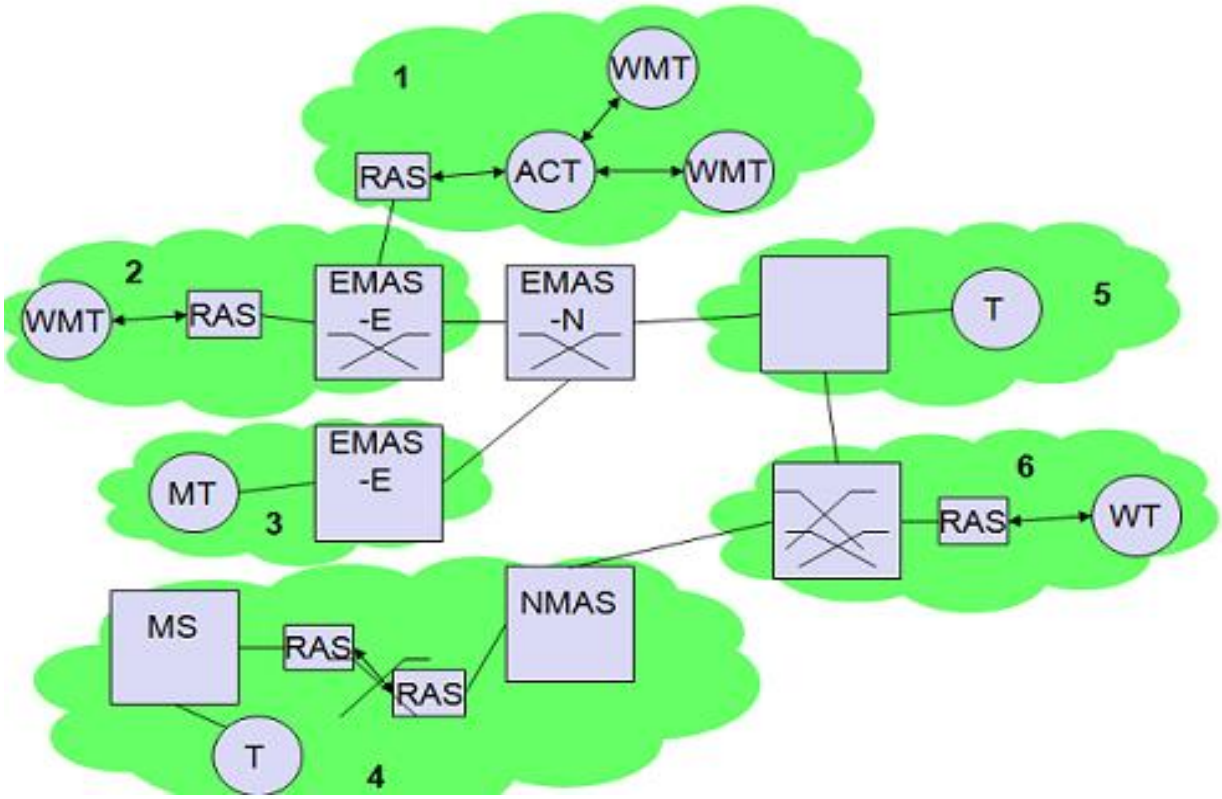
MT (mobile terminal): Is a standard ATM terminal that can move between different access points within a certain domain.

WT (wire terminal): It is a fixed terminal that can be accessed by a wireless link.

WMT (Wireless Mobile Terminal): It is a combination of WT and mobile terminal.

RAS (Radio access system): Is systems which access the network via radio link.

ACT (Ad-Hoc controller terminal): For the configuration of ad-hoc network special terminal types may be required within the wireless network. These terminals control wireless access without an RAS.



Based on these entities several scenarios may be formed.

1. Wireless ad-hoc ATM network (scenario 1): WMTs can communicate with each other without a fixed network. Communication can be setup without any infrastructure. Access control can be accomplished via the ACT. If the ad-hoc network needs a connection to a fixed network this can be provided by means of an RAS.

2. Wireless mobile ATM terminals (scenario 2): In this configuration a WMT communicate only with the help of EMAS-E

3. Mobile ATM terminals (scenario 3): This configuration allows for simple network reconfiguration. Users can change the access points of their ATM equipment over time without the need for reconfiguration by hand.

4. Mobile ATM switches (scenario 4): This is the most complex configuration investigated within an ATM environment. The examples of this configuration are networks in aircraft, trains or ships.

5. **Fixed ATM terminals (scenario 5):** In this scenario terminals and switches do not include capabilities for mobility or wireless access.

6. Fixed wireless ATM terminals (scenario 6): To provide simple access to ATM networks without wiring a fixed wireless link is the ideal solution. This scenario does not require any changes or enhancements in the fixed network.

Comparison of wireless networks

Criteria	**IEEE 802.11 b**	**IEEE 802.11 a**	**HIPERLAN 2**	**Bluetooth**
Frequency	2.4 GHz	5 GHz	5 GHz	2.4 GHz
Maximum transmission rate	11 Mb/s	54 Mb/s	54 Mb/s	< 1 Mb/s
Throughput	6 Mb/s	34 Mb/s	34 Mb/s	< 1 Mb/s
Medium Access	CSMA/CA	CSMA/CA	AP centralized	Master centralized
Frequency technique	None	802.11 h	DFS	FHSS
Connectivity	Connectionless	Connectionless	Connection oriented	Connectionless + Connection Oriented
Error control	ARQ	ARQ, FEC (PHY)	ARQ, FEC (PHY)	ARQ, FEC (MAC)
Transmit power	100 mW	0.05 / 0/25 / 1 W	0.2 / 1 W	1/2.5/100 mW

Explain about ZIGBEE technology:

NEED:

In this present communication world there are numerous high data rate communication standards that are available, but none of them meet the requirement of sensors and control devices standards. Therefore, for **sensing the nodes which are placed in a dense region** and were **human involvement is not possible** in such places ZIGBEE can be employed.

Characteristics:

- Zigbee technology is low-cost and low-power consumption.
- Low data rate.
- Suitable for industrial applications, home automation, etc.
- It covers 10-100 meters.

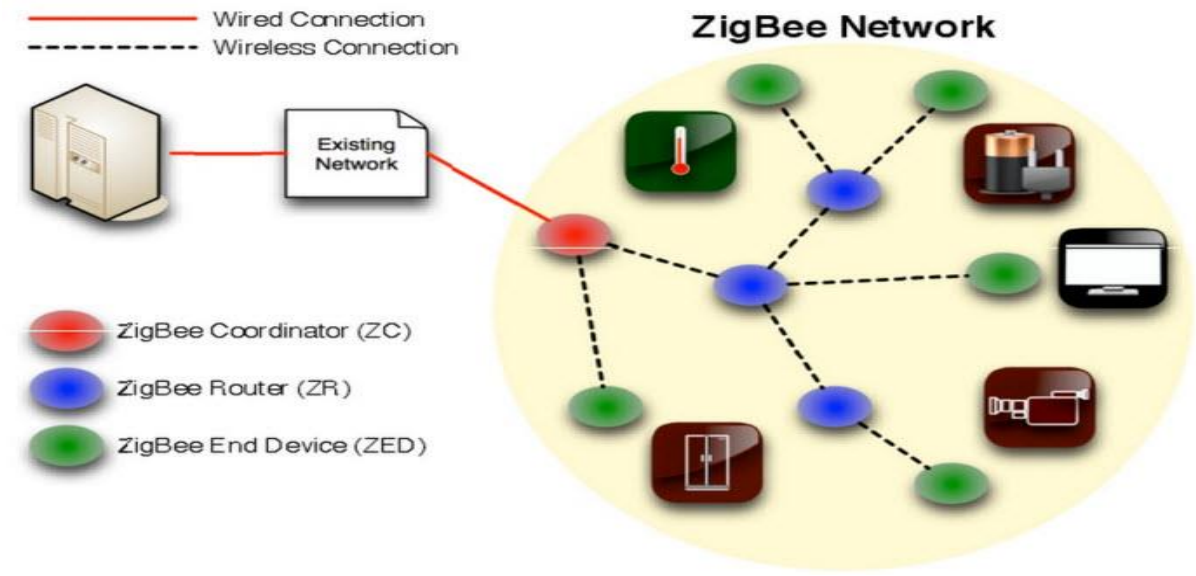
NOTE: This communication system is **less expensive** and simpler than other wireless networks such as Bluetooth and Wi-Fi.

PRINCIPLE

In this technology **sensors are used** in order to sense the multiple parameters such as pressure, temperature and for military applications. The **sensing** node has an **inbuilt 8 bit or 16 bit microcontroller**.

These Zigbee's WPANs **operate at 868 MHz, 902-928MHz and 2.4 GHz** frequencies. The date rate of 250 kbps is best suited for periodic as well as intermediate two way transmission of data between sensors and controllers.

ZIGBEE ARCHITECTURE: Zigbee system structure consists of three different types of devices such as **Zigbee coordinator, Router and End device.**



Zigbee coordinator: Every Zigbee network must consist of at least one coordinator which **acts as a root and bridge** of the network. The coordinator is **responsible for handling and storing the information** while performing receiving and transmitting data operations.

Zigbee routers: It acts as intermediate devices that permit data to pass to and fro through them to other devices.

End devices: It have limited functionality to communicate with the parent nodes.

The number of routers, coordinators and end devices depends on the type of network such as star, tree and mesh networks.

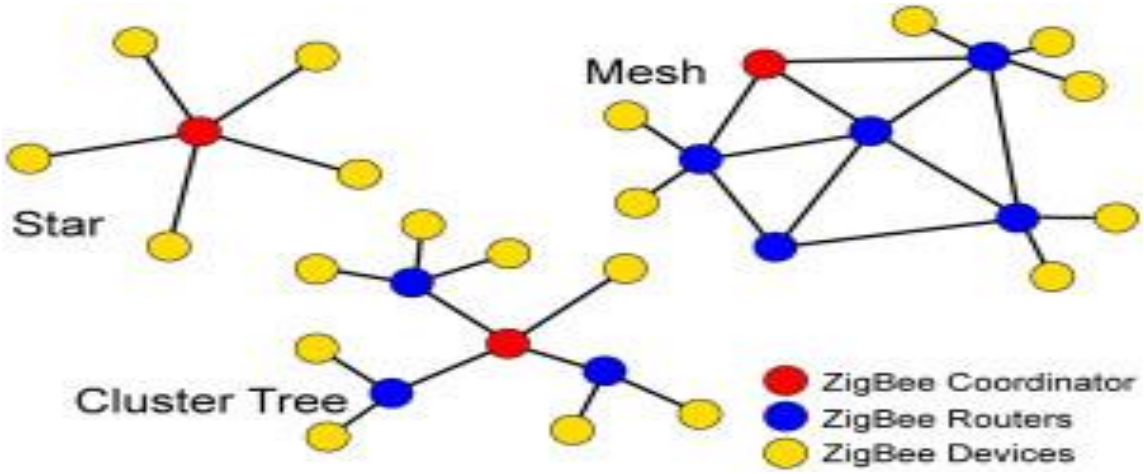
Operating Modes: In Zigbee data is transferred in two modes.

Non-beacon mode and Beacon mode

Beacon mode: In a beacon mode, the coordinators and routers **continuously monitor** active state of incoming data hence **more power is consumed**. In this mode, the **routers and coordinators do not sleep** because at **any time any node can wake up and communicate.**

Non Beacon mode: In non beacon mode, when there is **no data communication** from end devices, then the **routers and coordinators enter into sleep state**. **Periodically** this **coordinator wakes up** and **transmits the beacons** to the routers in the network. It has **longer battery life**.

Zigbee Topologies



STAR TOPOLOGY: In a star topology, the network consists of one coordinator which is responsible for initiating and managing the devices over the network. All other devices are called end devices that directly communicate with coordinator.

Application: This is used in industries where all the end point devices are needed to communicate with the central controller, and this topology is simple and easy to deploy.

MESH TOPOLOGY: In mesh the Zigbee network is extended with several routers where coordinator is responsible for staring them. These structures allow any device to communicate with any other adjacent node for providing redundancy to the data.

Advantage: If any node fails, the information is routed automatically to other device by these topologies. As the redundancy is the main factor in industries, hence mesh topology is mostly used.

CLUSTER-TREE In a cluster-tree network, each cluster consists of a coordinator with leaf nodes, and these coordinators are connected to parent coordinator which initiates the entire network.

Applications of Zigbee Technology

Industrial Automation: In manufacturing and production industries, a communication link continually monitors various parameters and critical equipments. Hence Zigbee considerably reduce this communication cost as well as optimizes the control process for greater reliability.

Home Automation: Zigbee is perfectly suited for controlling home appliances remotely as a lighting system control, heating and cooling system control, safety equipment operations.

Smart Metering: Zigbee remote operations in smart metering include energy consumption response, pricing support, security over power theft, etc.

Smart Grid monitoring: Zigbee operations in this smart grid involve remote temperature monitoring, fault locating, reactive power management, and so on.

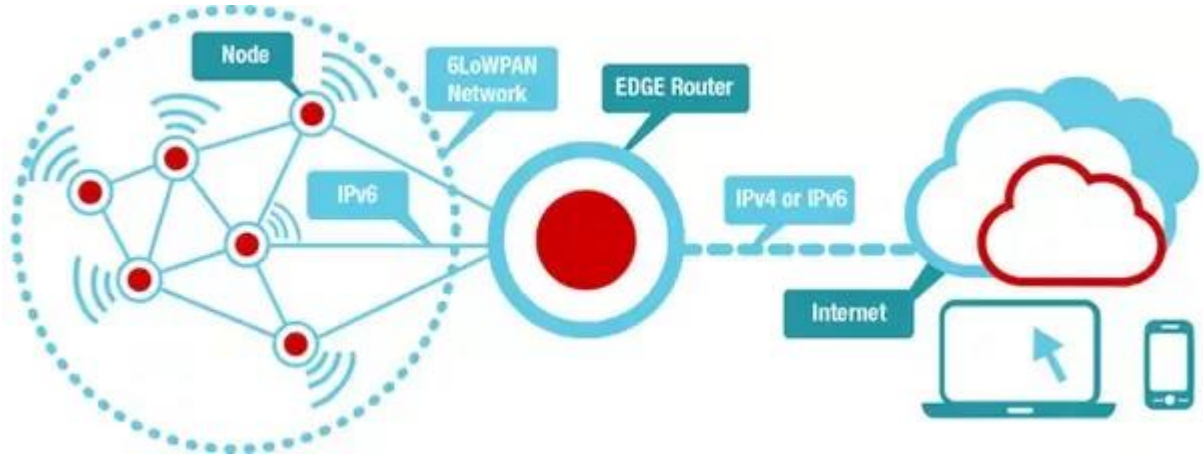
Write Short notes on 6LOWPAN:

6LoWPAN is an acronym of IPv6 over Low -Power Wireless Personal Area Networks.

PRINCIPLE:

6LoWPAN is a wireless mesh network that operates with low-power. Here, every node have its own IPv6 address, which allows it to connect directly with the Internet using open standards.

Advantage: With 6LoWPAN, it's possible to connect more things to the cloud. This technology is a great option to use with IoT (Internet of Things) applications.



Devices connected with this network typically works together in order to connect the physical environment to real world applications for example, wireless sensors networks. Some of the common topologies it includes are like star, mesh, and combinations of star and mesh.

Reason for choosing IPv6

- No need of network address translation (NAT).
- Possibility of adding innovative techniques such as location aware addressing.
- High security.
- Reduce the size of their routing tables by making them more hierarchical

Characteristics of 6LoWPAN:

1. Compact in size.

2. Usually it's a battery operated hence it uses low power

3. Low cost.

Advantage of 6LoWPAN:

1 It uses open IP standard.

2. It offers end-to-end IP addressable nodes.

3. There's no need for gateway, a router can connects the 6LoWPAN network to IP.

4. It offers self-healing, robust and scalable mesh routing, with one-to-many & many-to-one routing.

5. The mesh routers of 6LoWPAN can route data destined to others, whereas hosts can sleep for long duration of time.

Applications:

- Energy/Water savings
- Home security
- Home Safety
- Remote healthcare
- Air quality monitoring

Comparison of Zigbee VS 6LoWPAN

ZIGBEE	6LOWPAN
Here, the nodes (devices) **could not communicate directly** with other devices over internet.	Here, the nodes (devices) **could communicate directly** with other devices over internet.
Here, the **data exchanges** between stations are **only through** the central hub called **coordinator**.	Here, the **data** can be **exchange between stations directly** based on their request.
Time consumption for data transfer is more.	Time consumption for data transfer is less.
Network layer is used for data transfer.	IPv6 is used for data transfer.

Explain about WHART:

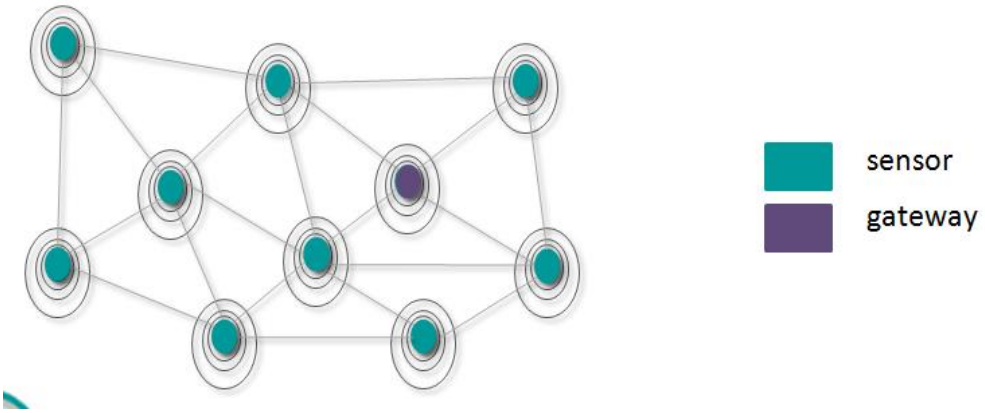
- **HART Communication Protocol (Highway Addressable Remote Transducer).**
- It is an hybrid (analog+digital) industrial automation open protocol.
- **Ex**: Caller ID in landline display which display who is calling in analog network.
- HART technology is a master/slave protocol, which means that a smart field (slave) device only speaks when spoken to / by a master.

WHART-Features

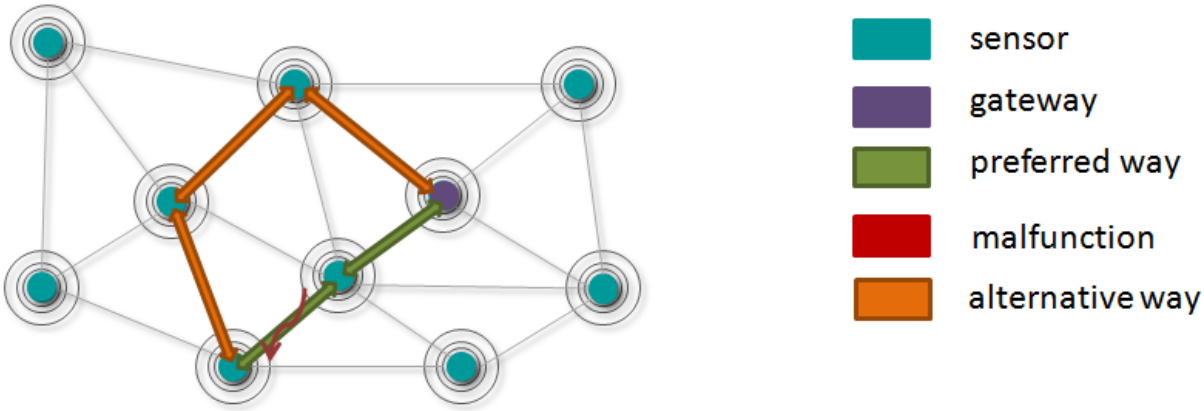
- ❑ It is an open & interoperable standard
- ❑ It is based on the established HART protocol
- ❑ It uses known tools and procedures for configuration, maintenance, & diagnosis
- ❑ It requires minimal training
- ❑ It allows wireless access to existing field devices
- ❑ It can be used worldwide without any license

PRINCIPLE

- The Wireless HART network is a mesh network where each sensor acts as both a router and repeater.
- The range of the network doesn't depend on the location of the central gateway, allowing set up of large distributed network structures.



Intelligent Network Structure: If there is an interrupted communication path, the system automatically re-routes the signal in order to maintain uninterrupted communication.



In the network shown above suddenly a link has been failed immediately the sensor finds an alternate route to transfer the data without interruption.

Applications

- Tank Farms
- Oil Refineries
- Mobile Equipment
- Ad hoc Monitoring
- Pipelines

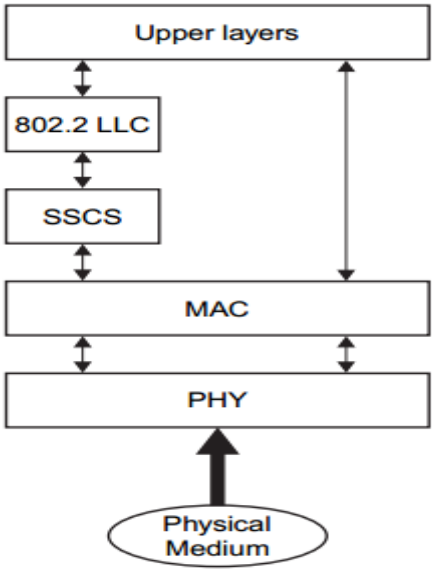
Comparison of Zigbee and WirelessHART

Features	Zigbee	WirelessHART
Topology supported	Star and Mesh	Star and Mesh
Frequency Bands	868/915 MHz, 2.4 GHz	2.4 GHz
Standard	IEEE 802.15.4	IEEE 802.15.4, HART comm. protocol
MAC mechanism	CSMA/CD	TDMA
Channel Hopping	Not supported	Supported
Ability to cope with very large networks	No	Yes

Latency and reliability determinism	No	Yes
Built-in security features	Yes	Yes
Wireless mesh routing	Supported	Supported
Data rate	250 Kbps	250 Kbps
Range	about 100 meters	about 100 meters
Power consumption	Low	Medium
Cost	Medium	Medium

Explain IEEE 802.15.4 LR-WPAN device architecture:

The fig shows an LR-WPAN device. The device consists of a physical layer which contains the RF transceiver, a MAC sublayer to transfer all types of data and a network layer for configuration, message routing.



PHYSICAL LAYER: It provides two services: PHY data service and PHY management service

The functions are activation and deactivation of radio transceiver

Energy detection

Link quality indication

Channel selection

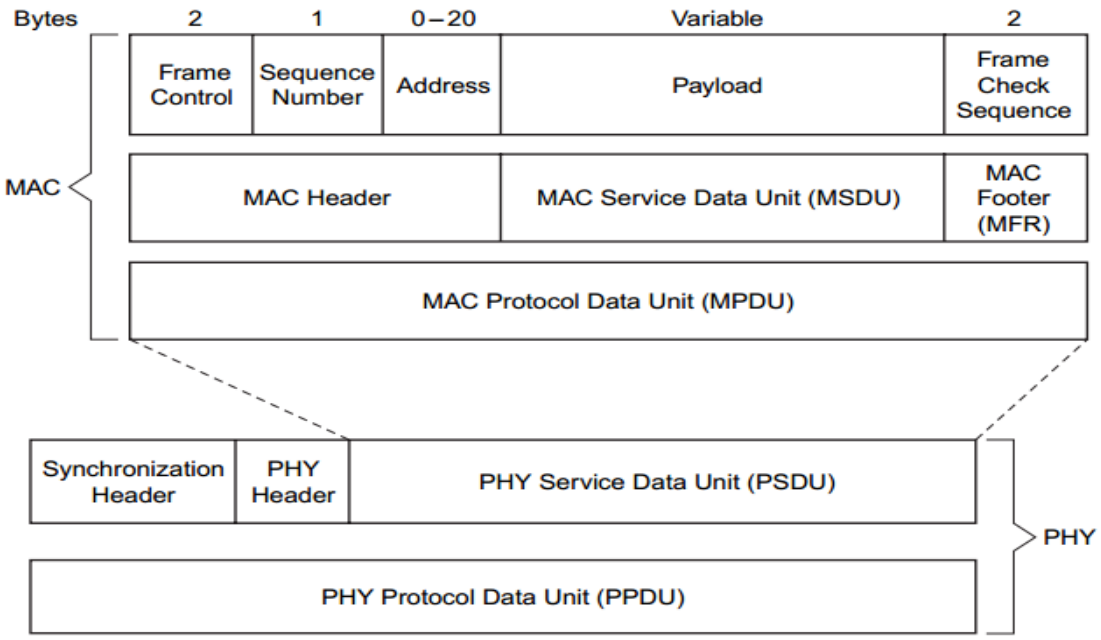
Clear channel assessment CCA.

It supports direct sequence spread spectrum.

To maintain a simple interface with MAC physical layer share a packet structure. It consists of preamble, SOD, header and payload.

Preamable for synchronization, SOD for indicates the starting of frame, header is used to indicates the packet length.

DATA LINK LAYER It is divided into 2 sublayers MAC and LLC. The features of MAC are:



1. Association and disassociation
2. Frame validation
3. Guaranteed time slot management
4. Beacon management

The MAC protocol data unit consists of MAC header, MAC service data unit and MAC footer. The field of the MAC header consists of frame control field which indicates the type

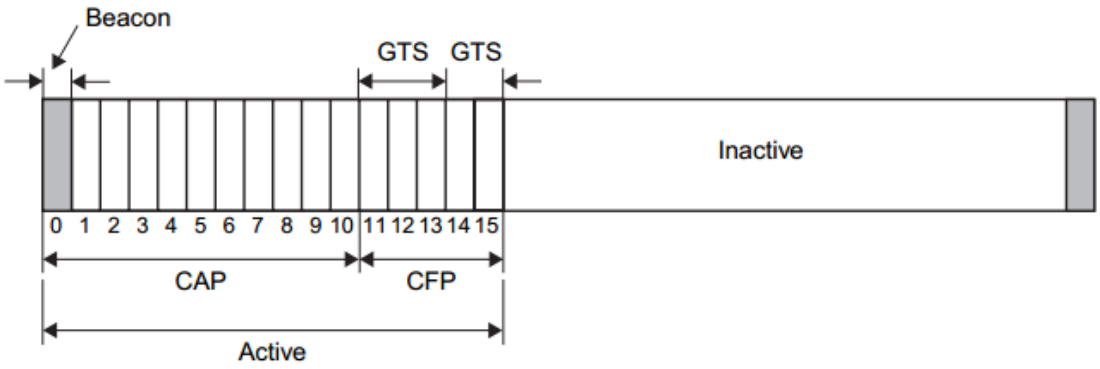
of MAC frame being transmitted, the second field indicates the sequence number for ACK and the address field.

The payload field is variable in length. The data contain in the payload depends on the frame type. The MAC has 4 different frames: they are Beacon frame, data frame, ACK frame and command frame.

The FCS is used for error detect**ion.**

SUPER FRAME STRUCTURE

Some applications require a dedicated band width to achieve low latency. To achieve this 802 .15.4 uses a super frame mode. In super frame mode Beacons are transmitted at regular intervals. The beacon frame is sent in the first slot of each super frame. Particular time slots are assigned. It is referred to us Guaranteed time slot.



NETWORK LAYER: It is responsible for topology construction and maintenance as well as addressing, routing and security. The protocols used are AODV and DSDV.

UNIT – II

MOBILE NETWORK LAYER

Introduction - Mobile IP: IP packet delivery, Agent discovery, tunneling and encapsulation, IPV6- Network layer in the internet- Mobile IP session initiation protocol - mobile ad-hoc network: Routing: Destination Sequence distance vector, IoT: CoAP

Part – A

1. What is a Mobile IP?

Mobile IP is a protocol developed to allow internetwork mobility for wireless nodes without the need of change in IP addresses.

2. What are the entities of Mobile IP?

Mobile Node (MN)	Foreign Network (FN)
Correspondent Node (CN)	Foreign Agent (FA)
Home Network (HN)	Home Agent (HA)

3. What are the benefits of Mobile IP?

The major benefit of Mobile IP is that it makes the user to move from a fixed location. Mobile IP is capable to track and deliver information to mobile devices without needing to change the device's long-term Internet Protocol (IP) address.

4. What is Care-Of Address (COA)?

The Care of Address defines the current location of the MN from an IP point of view. All IP packets sent to the MN are delivered to the COA, not directly to the subnet.

5. What is agent advertisement?

It is one of a technique to find to which FA the MN is connected. In this method both **FA&HA advertise their presence periodically using special agent advertisement mess6.**

6. What is the need for registration?

The main purpose of the registration is to inform the HA of the current location for correct forwarding of packets.

7. Define – Encapsulation and Decapsulation

Encapsulation is the mechanism of taking a packet consisting of packet header and data and putting it into the data part of a new packet. The reverse operation, taking a packet out of the data part of another packet, is called decapsulation.

8. What is triangular routing?

In general if the data from CN wants to transmit to MN the following procedure takes place.

First the data transfers from CN to HA and then from HA to COA or MN and then from MN to CN. This **process involves large amount of delay**. This **insufficient behaviour of a non-optimized mobile IP is called triangular routing.**

9. What is DHCP?

If a new computer is connected to a network, DHCP can provide it with all the necessary information for full system integration into the network, e.g., addresses of a DNS server and the default router, the subnet mask, the domain name, and an IP address.

10. What is SIP?

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying and terminating sessions with one or more participants.

11. What are the functions of Session Initiation Protocol (SIP)?

SIP has following major functions

1. SIP allows for the establishment of user location.
2. SIP provides a mechanism for call management.
3. SIP provides feature negotiation, so that all the parties in the call can agree to the features supported among them.

12. What are the characteristics of MANET? (M/J - 12)

The characteristics of MANET are

Dynamic Topologies

Bandwidth Constraints and Variable Capacity Links

Energy Constrained Operations

Limited Physical Security

13. Differentiate an ad hoc network and a cellular network with respect to

a) Bandwidth usage

b) Cost effectiveness **(N/D - 12)**

PARAMETER	CELLULAR NETWORK	AD HOC NETWORK
Bandwidth usage	Easier to employ bandwidth reservation	Bandwidth reservation requires complex medium access control protocols
	Guaranteed bandwidth (designed for voice traffic)	Shared radio channel (more suitable for best-effort data traffic)
Cost effectiveness	Cost of network maintenance is high (backup power source, staffing, etc.)	Self-organization and maintenance properties are built into the network. Hence the cost of network maintenance is less.

14. What are the challenging issues in ad hoc network maintenance? (M/J - 12)

1. Asymmetric links
2. Redundant links
3. Interference
4. Dynamictopology

15. Why are ad hoc networks needed? (M/J - 12)

Ad hoc networking is often needed where an infrastructure network cannot be deployed and managed. The presence of dynamic and adaptive routing protocols enables quick formation of ad hoc networks and is suitable for emergency situations like natural disasters, spontaneous meetings or military conflicts.

16. List out the applications of ad hoc networks.

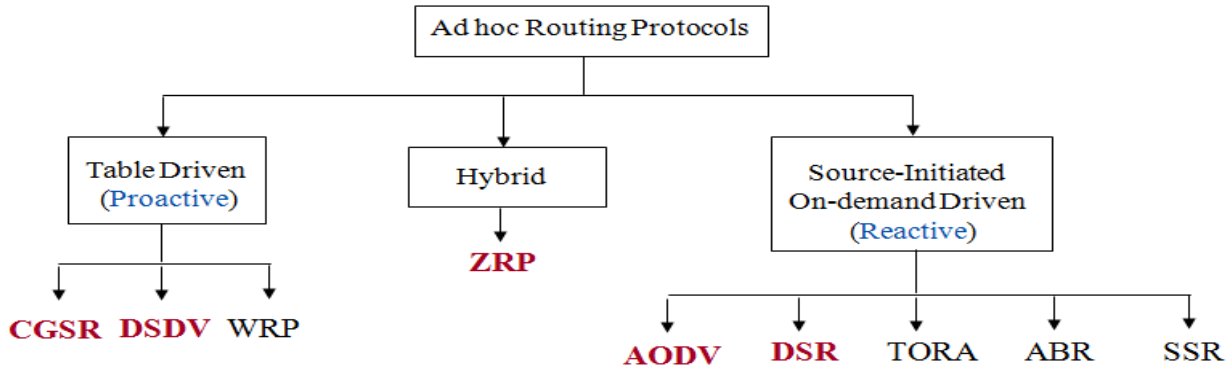
Ad hoc networks are widely used in

1. Military applications and battlefields
2. Collaborative and distributed computing
3. Emergency search and rescue operations
4. Wireless sensor and mesh networks

17. Give the classifications of routing protocol in MANET.

Routing protocols can be classified into three types:

1. Proactive routing protocol 2. Reactive routing protocol 3. Hybrid protocols.



18. List the Source-initiated On-Demand Routing Protocols.

The Source-initiated On-Demand Routing Protocols are

Ad-hoc On-Demand Distance Vector Routing (AODV)

Dynamic Source Routing (DSR)

Temporarily Ordered Routing Algorithm (TORA)

Associatively Based Routing (ABR)

Signal Stability Based Routing (SSR)

19. Differentiate proactive and reactive routing protocols. Write examples for each. (M/J- 12)

S.No	Proactive Routing Protocols (Table-driven)	Reactive Routing Protocols (Source-initiated on-demand)
1	Stores the routing information	It does not store any routing information.
2	Creates more overhead	Reduced amount of overhead
3	It does not experience any delay when the first node wishes to transmit.	It experiences more delay when the first node wishes to transmit.
4	**More** amounts of **resources are wasted.**	**Resources are not wasted.**
5	**Examples** of proactive routing protocols are **DSDV, OLSR, and WRP.**	**Examples** of reactive routing protocols are **DSR, AODV**.

20. What is DSDV?

Distance-Vector Routing (DSDV) is a table driven routing scheme for ad-hoc mobile networks. The main contribution of the algorithm was to solve the routing loop problem.

21. List out the advantages and disadvantages of DSDV routing protocols.

The advantages and disadvantages of DSDV routing protocols are

Advantage:

- It does not have looping problem.
- DSDV requires low memory requirements.
- Converge quickly (finds the optimum path fastly).
- No latency (delay) caused due to route discovery.

Disadvantages:

- No sleeping nodes (it means all the nodes will be active at all time)
- Creates more overhead. It means most of the routing information are never used.

PART-B

What is the need for mobile IP?

In **olden days** the IP assumes that the **stations (computers)** connected to the internet will **always be fixed** and hence it can be identified with the IP address which is a permanent address easily.

Datagrams (packets) are sent to the computer based on the IP address information only.

Real fact: But in **modern days** the **devices** such as laptop, tab and other mobile devices made the persons (stations) to **move from one place to other.** In such cases the permanent IP address which is assigned by the home agent will not be helpful. To find the solution for this problem only we go for mobile IP.

-

What is mobile IP?

Is an Internet Engineering Task Force (IETF) standard communication protocol that is designed to allow mobile device users to move from one network to another while maintaining their permanent IP address.

Advantage:

The mobile IP allows for location independent routing of IP datagrams on the internet. Each **mobile node is identified by** its **home address, disregarding its current location** in the internet.

What are the Quick Solutions for mobile IP:

1. **Permanent IP address:** It is one solution. Here emergency communication and quick reachability is possible via the permanent IP address.
2. **Dynamically updating the IP address** with respect to current location. The problem here is domain name system (DNS) needs some time before it updates the internal tables. This approach does not work if the mobile node moves quite often. **Updating millions of IP address for each node is quite impossible.**
3. **Updating the routing table of the routers**. Based on the router new routing table information the datagrams can be sent easily. But **fast and frequent updating of router is not possible.**
4. The **TCP relays on IP address**, changing the IP address while having a TCP connection open means it will break the connection. Since a TCP connection is identified by source IP address, source port, destination IP address & destination port. Therefore, a TCP connection cannot survive any address change.

Note:

Theoretically we can speak routers or routing table can be updated. But practically routers are devices to fast forward and not for fast update. The **fast update leads to instability of the internet**. Since the routers are the "brains" no service provider will allow to change the IP address.

Therefore the above quick solutions are not practically possible.

PART-B

1. Explain the Requirements of Mobile IP.

Since, the quick 'solutions' obviously did not work, a more general architecture had to be designed. Many field trials and proprietary systems finally led to mobile IP as a standard to enable mobility in the internet. Several requirements accompanied the development of the standard:

- **Compatibility:** The installed base of Internet computers, i.e., computers running TCP/IP connected to the internet is huge. A **new standard cannot introduce changes for applications or network protocols already in use**

  . People still want to use their favourite browser for www and do not want to change applications just for mobility, the same holds for operating systems. Mobile IP has to be integrated into existing operating systems or at least have to work with them.

Routers within the internet should not necessarily require other software. While it is possible to enhance the capabilities of some routers to support mobility, it is almost impossible to change all of them.

Transparency: Mobility should remain 'invisible' for many higher layer protocols and applications. Besides maybe noticing a lower bandwidth and some interruption in service, higher layers should continue to work even if the mobile computer has changed its point of attachment to the network.

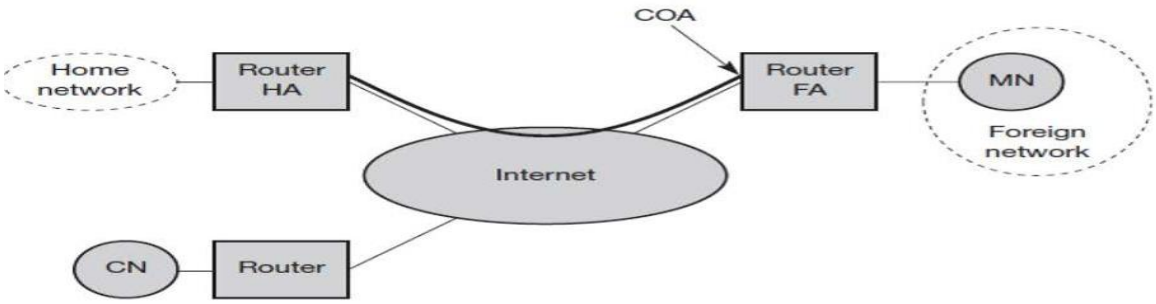
The only effects of mobility should be a higher delay and lower bandwidth. However, there are some applications for which it is better to be 'mobility aware'. Examples are cost-based routing or video compression. If a video application knows that only a low bandwidth connection is currently available, it could use a different compression scheme.

- **Scalability and efficiency:** Introducing a new mechanism to the internet must not jeopardize its efficiency. **Enhancing IP for mobility must not generate too many new messages flooding the whole network**. Special care has to be taken considering the lower bandwidth of wireless links. Many mobile systems will have a wireless link to an attachment point, so only some additional packets should be necessary between a mobile system and a node in the network.
- **Security:** Mobility poses many security problems. The minimum requirement is that of all the messages related to the management of Mobile IP should be authenticated. The IP layer must be sure that if it forwards a packet to a mobile host that this host receives the packet. The IP layer can only guarantee that the IP address of the receiver is correct. **There are no ways of preventing fake IP addresses or other attacks.**

The **goal of a mobile IP** can be summarized as: **'supporting end-system mobility while maintaining scalability, efficiency, and compatibility in all respects with existing applications and Internet protocols'.**

2. Explain the Entities and terminology of mobile networks.

● **Mobile node (MN):** A mobile node is an **end-system** or **router** that can **change its point of attachment to the internet.** Mobile nodes are not necessarily small devices such as laptops with antennas or mobile phones; a router onboard in an aircraft can be a powerful mobile node.



Correspondent node (CN): At least one partner is needed for communicate. In the following the **CN represents this partner for the MN**. The CN can be a fixed or mobile node.

Home network: The **home network** of a **mobile** device is the **network** within which the device receives its identifying **IP** address (**home** address). The **home** address of a **mobile** device is the **IP** address assigned to the device within its **home network**.

Home agent (HA): The HA provides several services for the MN and is located in the home network. The tunnel for packets towards the MN starts from the HA. The HA maintains a location registre i.e., it is informed of the MN's location by the current COA.

Foreign network: The foreign network is the **current subnet the MN visits** and which is **not the home network.**

● **Foreign agent (FA):** The FA is a network which provides multiple services when the MN enters into the new (foreign) network. The FA can have the COA (Care of Address), acting as tunnel endpoint and forwarding packets to the MN. The FA can be the default router for the MN. FAs can also provide security services because they belong to the foreign network as opposed to the MN which is only visiting.

● **Care-of address (COA):** The COA **defines the current location of the MN** from an IP point of view. All IP packets sent to the MN are delivered to the COA, not directly to the IP address of the MN. Packet delivery toward the MN is achieved using a tunnel.

● **Foreign agent COA:** The COA could be located at the FA, i.e., the COA is an IP

address of the FA. The FA is the tunnel end-point and forwards packets to the MN.

- **Co-located COA:** The COA is **co-located if the MN temporarily** acquired an additional IP address which acts as COA. This address is now topologically correct, and the tunnel endpoint is at the MN. One problem associated with this approach is the **need for additional addresses** if MNs request a COA.

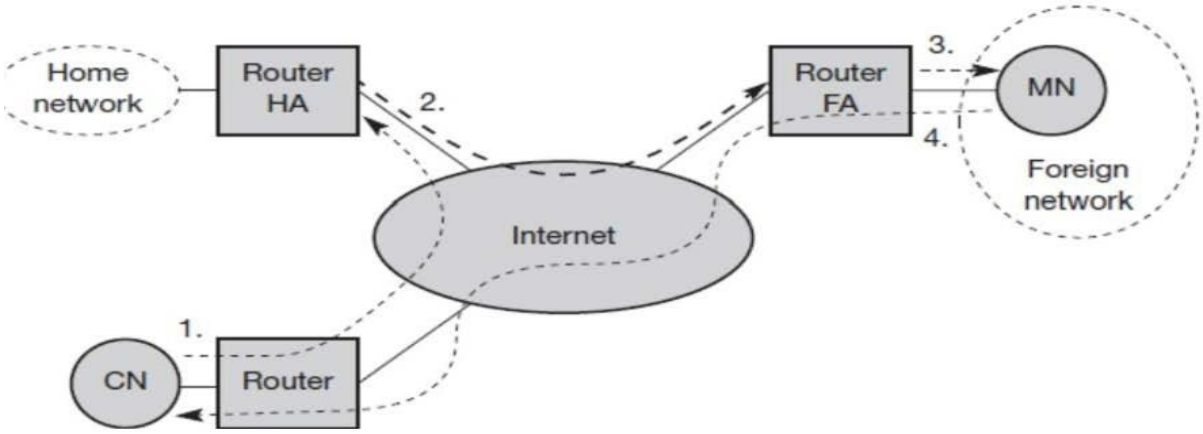
3. Explain the Operation of packet delivery to and from the mobile node.

(OR)

Explain the concept of IP packet delivery.

Need: To transfer the packet from CN (correspondent node) to MN (mobile node).

Assumption: CN does not know the exact location of MN.



STEP 1: CN sends the packet as usual to the IP address of MN with source address as CN and destination address as MN. Since, the internet does not have any information of current location of MN it routes the packet to the router home agent.

STEP 2: The HA now diverts the packet, since it knows the MN is not in home network. The HA diverts the packet to the FA by a process called **tunneling.** Tunnelling is a virtual path way.

In tunnelling with original data and original address (CN as source & MN as destination) an additional address called COA (care of address) is added to the whole content & send. The technique is referred as encapsulation.

STEP 3: The FA now decapsulates the packet i.e. removes the additional header & sends (delivers) only the original data & header to the MN. The MN does not know any information so far what happened. It knows only address is CN & destination address is MN.

STEP4: The MN sends the packet from MN as source address & CN as destination address. The router with the FA acts as a default router & routes the packet to the internet & then to the correspondent node(CN) through the router if the CN is fixed.

If the CN is mobile then the data from MN follows steps 1 to step 3 in either opposite direction.

4. Explain the need for AGENT DISCOVERY:

Need: When the mobile node (MN) moves from one location to another location it does not know to which FA the MN is connected. In order to detect the FA the agent discovery is used by the MN.

(OR)

Agent discovery is used by the MN to find to which FA the MN is connected for the above two methods are used.

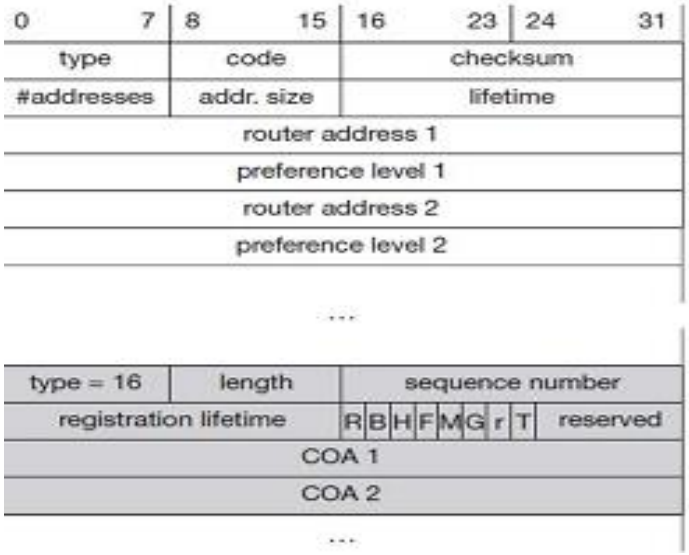
The two methods used for Agent discovery are:

1. Agent advertisement.
2. Agent solicitation (request).

AGENT ADVERTISEMENT: It is one of a technique to find to which FA the MN is connected. In this method both **FA&HA advertise their presence periodically using special agent advertisement messages**

For the **advertisement ICMP messages are used** Internet control message protocol.

- ICMP messages are generally used to provide error reporting & query messages , when the sender host cannot able to detect the destination host.
- In the Agent advertisement upper part represents ICMP packet while the lower part is the extension needed for mobility.
- The IP destination address can be 224.00.1 for multicast & if it is broadcast 255.255.255.255



The **type** is set to 9.

CODE: It is set to 0.when the agent rates traffic from both mobile & non-mobile nodes. It is set to 16 when the agent rates traffic from mobile nodes & not from non-mobile nodes.

No.of.Address: It shows the number of addresses with this packet.

LIFE TIME: The length of the time over which this advertisement is valid.

PREFERENCE LEVEL: For each address help a node to choose the routes that is the most

eager one to get a new node.

The fields of the extension of the packet for mobility are:

1. TYPE : It is set to 16.
2. LENGTH : It defines the number of COA's provided with the message.
3. SEQUENCE NUMBER: It indicates the total number of advertisements from the beginning.
4. REGISTRATION LIFE TIME: It specifies the maximum time a MN can request during registration.

AGENT SOLICITATION:

PRINCIPLE:

When a MN enters a new network, it verifies the advertisement messages. If advertisement messages are not there, the (MN) will send agent **solicitation (request) message.**

- In high dynamic wireless networks, the MN sends three solicitation messages, one per second.
- Before getting the agent address the MN will loss many data packets.
- When the MN receives the address of the agent, it will use it for data transmission.
- If the MN does not receive the answer, it should decrease the rate of solicitations.

NOTE: After the advertisements and solicitations the MN receives the COA (care of address) for an FA. By using this address the MN can make communication.

5. Explain the steps involved for REGISTRATION in mobile IP:

Need/Purpose:

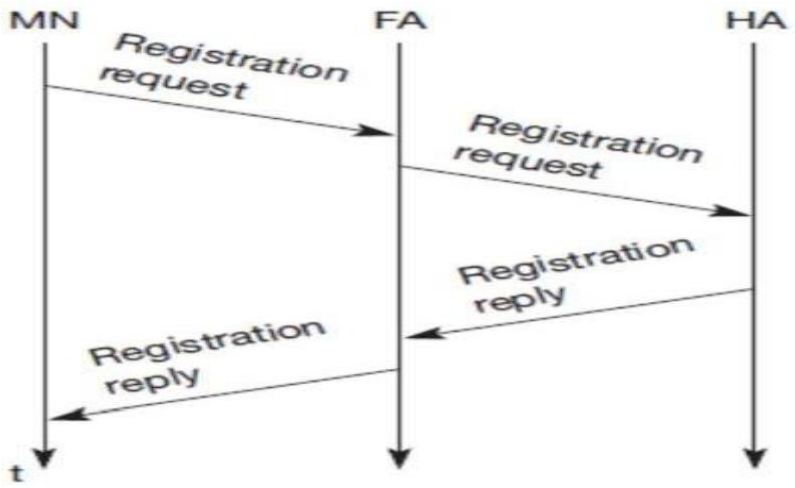
Once the MN identifies or receives COA message it should inform this to the corresponding home agent.

- The necessary for informing this then only the packets from HA will be forwarded to the MN correctly.

  Registration can be done in 2 ways:

  1. Registration of a MN to the HA via FA.
  2. Registration of MN to the HA directly.

Case (1): COA is permanent .If the COA is at the FA, registration is done as shown in fig. below

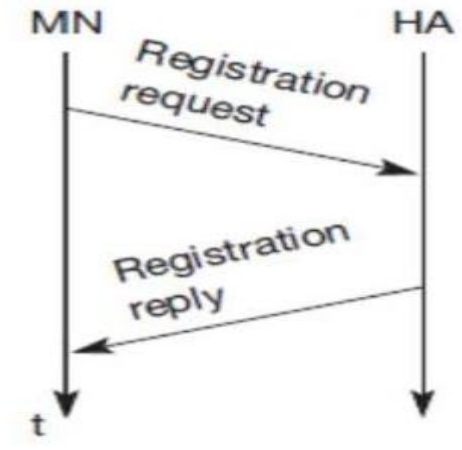


- The MN sends its registration request containing the COA to FA which forwards the request to HA. The HA now sets up a mobility binding containing MN home. IP address and the current COA.
- After the mobility binding the time for the registration is set or initialized.

- Registration expires automatically after the lifetime and is deleted. So an MN should reregister before expiration.
- Registration mechanism helps or avoids longer time waiting in mobility binding.

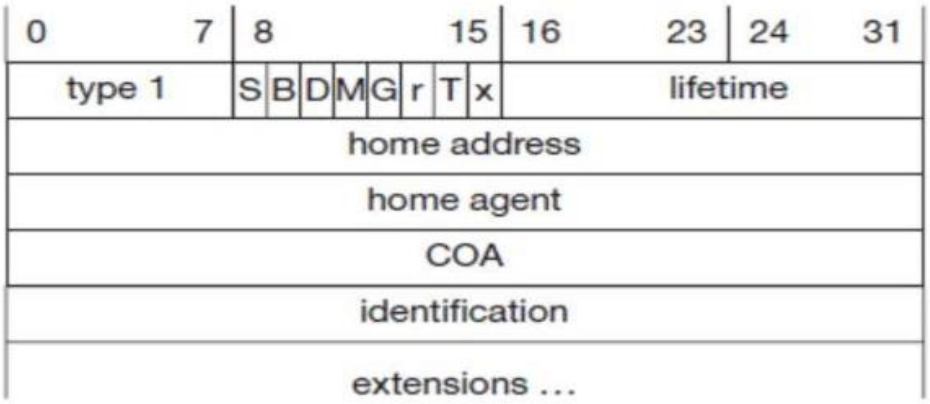
- After setting up the mobility binding, the HA sends a reply message back to the FA which forwards it to the MN.

Case (2): If the COA is co located (temporary) registration is very simple. The MN sends the registration request directly to HA and receives the reply directly.



REGISTRATION REQUEST:MESSAGE FORMAT

- UDP packets are used for registration request.
- UDP is used because of low overhead and better performance compared to TCP in wireless environment. The fields for registration is defined below.



Type is set to 1 for registration request.

If "S" bit is set to 1 it indicates the bindings are requested to retain which allows for simultaneous binding.

When the B bit is set it indicates the MN wants to receive the broadcast message from HA.

If D bit is set it indicates the MN uses co-located (temporary) care of address.

M and G indicates the use of minimal encapsulation or generic routing encapsulation.

T indicates reverse tunneling.

R and X are set to zero.

Lifetime denotes the validity of registration in seconds. A value of zero indicates de registration.

Home address is fixed IP address of MN.

Home agent is IP address of HA.

COA represents tunnel end point.

The identification bits are used to match the registration request with reply messages. It is used for protection.

The extension bits arte used for authentication.

Registration reply message format:

- Here type field is set to 3
- Code value will indicate the result (status) of registration request

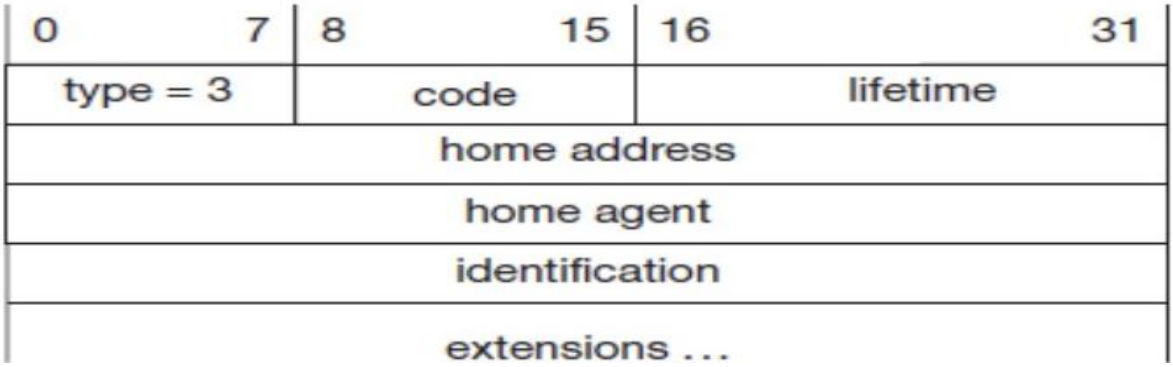
Ex: If code 0 indicates registration accepted

If code 1 indicates registration accepted

But simultaneous mobility binding unsupported

Lifetime:

Same as mentioned above in registration request

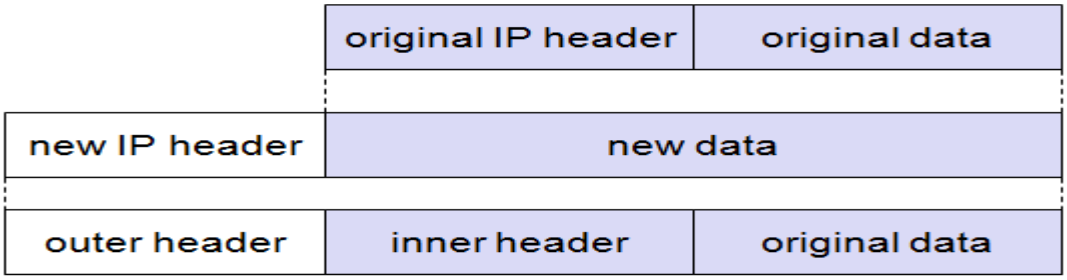


6. Explain how tunnelling is achieved in an IP network & the different types of encapsulation techniques:

Tunnel: It is a virtual path established between Home Agent (HA) and end of COA or at Foreign Agent (FA). Packets entering a tunnel are forwarded inside the tunnel and leave the tunnel unchanged.

Tunneling: It is a process of sending a packet through a tunnel. It is achieved by encapsulation.

Encapsulation: It is the mechanism of taking a packet consisting of a packet header and data and putting it into the data part of new packet.

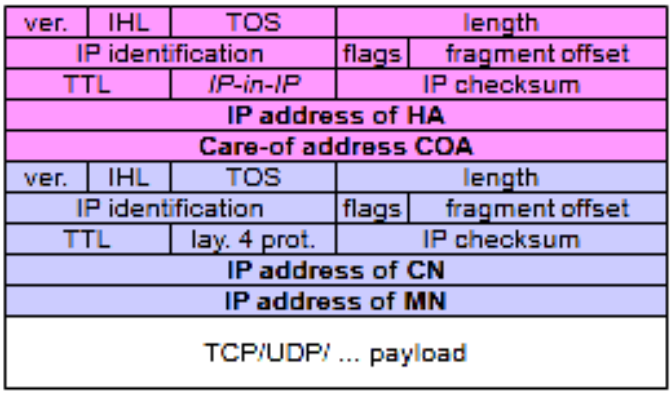


Decapsulation: The reverse operation taking a packet out of the data part from a new packet.

Note: The new IP header is also called outer header & original IP header (OIP header) is also called inner header.

Types of Encapsulation

1. IP – IP ENCAPSULATION: Compare to all three methods the mandatory for mobile IP is IP – in – IP encapsulation. The packets inside the tunnel is shown in fig below.



IP in IP consists of two sections. The outer header at the top and the inner header at the bottom.

Outer header:

- Version 4

- IHL (Internet Header Length) denotes the length of the outer header.
- DS (TOS) is fast copied from the inner header
- *Length field:* Indicates the length of the encapsulated packet
- TTL must be high enough then only the packet can reach the end point
- IP – in – IP: Indicates the type of protocol used in payload. It is set to 4
- IP checksum: For error detection
- IP address of HA provides tunnel source address
- COA: Indicates the tunnel end point

Inner header:

All fields are same as above except IP address of CN and IP address of MN since they both represents original data and original header.

IP address of CN → original sender CN IP address

IP address of MN → original destination MN IP address

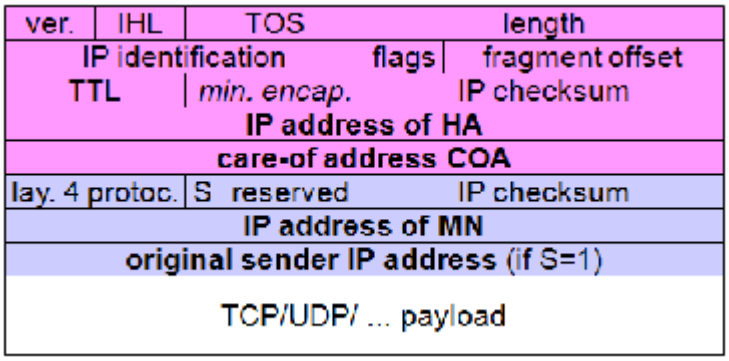
Finally the payload follows the two headers.

2. MINIMAL ENCAPSULATION

Need:

Most of the fields in IP-in-IP are redundant (extra). Ex.TOS is just copied fragmentation is often not needed.

Therefore, minimal encapsulation is an optional encapsulation method for mobile IP.



- Minimal encapsulation must not be used when an original datagram is already fragmented. Since there is no field in minimal forwarding header to store fragmented in formation.
- Here, the **value for minimal encapsulation is 55.**

- The inner header is different for minimal encapsulation. In the inner header IP address of MN and original sender IP address is placed if s=1.
- Finally here also the payload follows the two header.

3. GENERIC ROUTING ENCAPSULATION

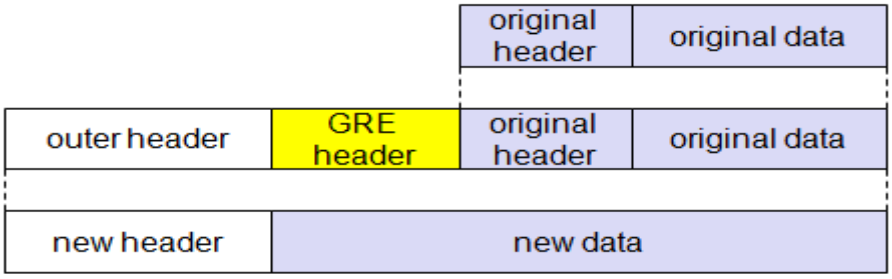
Need: IP-in-IP encapsulation and minimal encapsulation technique suitable only for IP whereas GRE can be able to support other network protocols such as FRP, FTP etc.., in additional to IP.

FTP→ File transfer protocol

FRP→File retrieval protocol

Principle:

Here, with the original date and original header a new GRE header is appended at the front and formed as a new data. At end with the new data an additional new header is added.

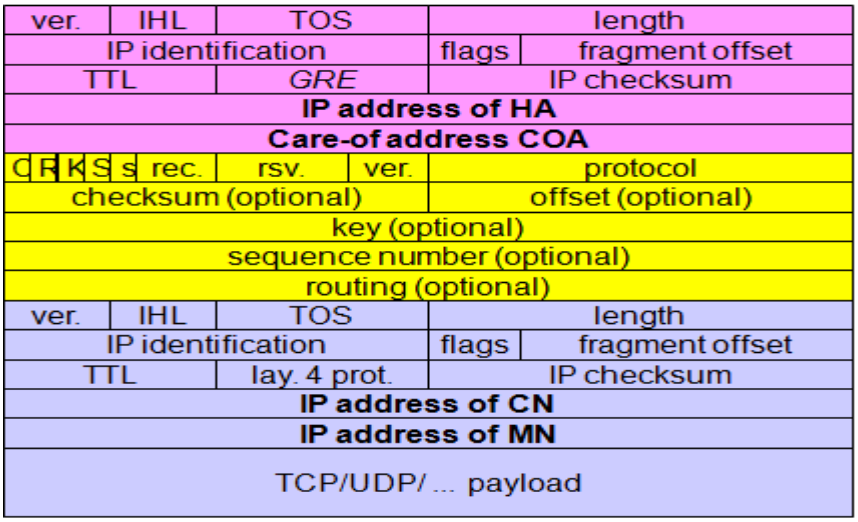


Router header:

The type value of GRE at router header is 47. The router header carries IP address of HA as source address and COA as destination address.

Length→ indicates length of the outer header

TTL→ indicates time to live which indicates the amount of time a pocket taken to reach the tunnel end point.



The flags in the outer header are

C→bit indicates if c is set, it indicate the checksum field contains valid IP checksum of GRE header and data.

R→if R is set. It indicates the routing fields are present and contain valid information.

K→if K is set, it means authentication is perfect.

S→if S is set, it indicates the sequence number field is present.

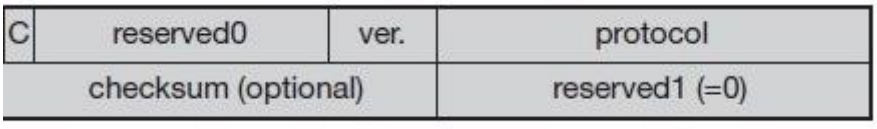
s→if s is set, it indicates strict source rating is used

Rec→Recursion control field represents the count of allowed recursive encapsulation.

- This field acts as a counter. As soon as pocket arrives at an encapsulator it checks whether this field is zero or non zero. The non zero value indicates still there are further encapsulated data.
- The reserved field and version field contains "0" for GRE version.
- Here the next field in protocol in GRE defines the type of protocol of the payload.

Note: Recursion field will not be available either IP-in-IP or in minimal encapsulation method.

Simplified version of GRE is shown below



Here C indicates again checksum and the next 5 bits are set to zero then followed by 7th and 8th bit (i.e.) reserved and version both values as mentioned previous initialized to zero (0).

---

7. What is triangular routing problem in mobile IP? How it can be avoided?

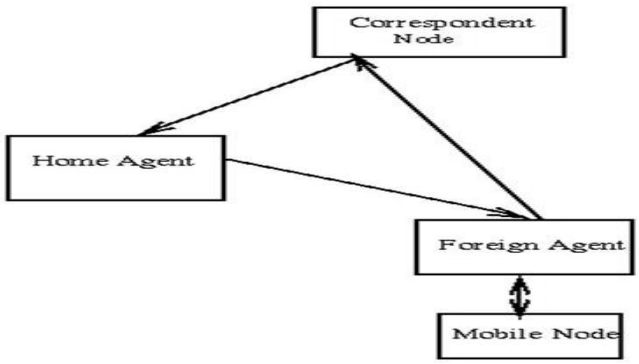
OR

What are the various optimizations techniques propose to solve the triangular routing problem in mobile IP?

OR

Explain how CN communicates to the MN when the mobile node changes its location suddenly.

In general if the data from CN wants to transmit to MN the following procedure takes place.



- First the data transfers from CN to HA and then from HA to COA or MN and then from MN to CN. This **process involves large amount of delay**. This **insufficient behaviour of a non-optimized mobile IP is called triangular routing.**
- In this non-optimized method the data from CN will travel to HA and from there to COA or FA which creates large overhead in all stages.
- This **drawback can be avoided by making to learn the CN where the MN is present currently by a technique called binding cache.**
- The place of the MN of current location should inform to CN by home agent only.

For this optimization mobile IP needs 4 additional messages

1. Binding request
2. Binding update
3. Binding Ack.
4. Binding warning

BINDING REQUEST: Any node that wants to know the current location of an MN can send a binding request to the HA. The HA can check if the MN has allowed dissemination

of its current location. If the HA is allowed to reveal the location it sends back binding update to CN.

BINDING UPDATE: This message sent by the HA to CN reveal the current location of MN. The message contains fixed IP address of the MN and the COA. The binding update can request for an ACK.

BINDING ACK: If requested a node returns this ACK after receiving a binding update message.

BINDING WARNING: If a node decapsulates a packet for an MN, but it is not the current FA for this MN, this node sends a binding warning. The warning contains MN's home address and a target node address. The recipient can be the HA, so the HA should now send a binding update to the node that obviously has a wrong COA for the MN.

The figure below shows the usage of 4 messages when the MN changes its location.

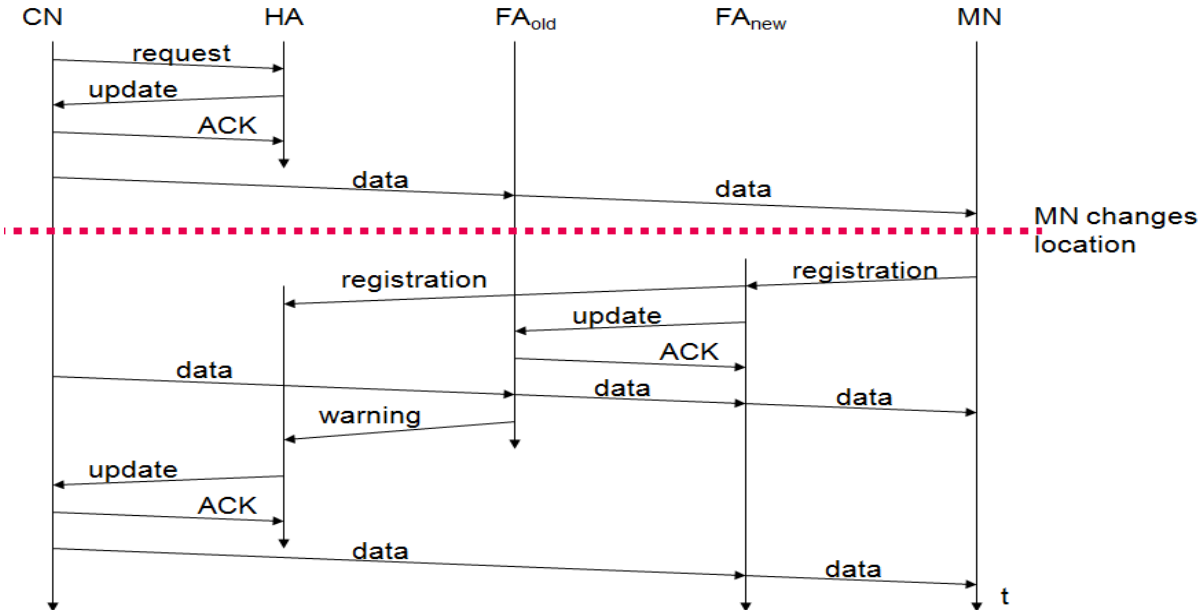
STEP 1: The CN can request the current location from the HA. If allowed by the MN, the HA returns the COA of the MN via an update message.

STEP 2: The CN acknowledges this update message and stores the mobility binding. Now the CN can send its data directly to the current foreign agent FA_{old}. FA_{old} forwards the packets to the MN. Encapsulation of data for tunneling to the COA is now done by the CN, not the HA.

STEP 3: The MN might now change its location and register with a new foreign agent, FAnew. This registration is also forwarded to the HA to update its location database.

STEP 4: FA_{new} informs FA_{old} about the new registration of MN. MN's registration message contains the address of FA_{old} for this purpose. Passing this information is achieved via an update message, which is acknowledged by FA_{old}.

STEP 5: Without the information provided by the new FA, the old FA would not get to know anything about the new location of MN. In this case, CN does not know anything about the new location, so it still tunnels its packets for MN to the old FA, FA_{old}.



STEP 6: This FA now notices packets with destination MN, but also knows that it is not the current FA of MN. FA_{old} might now forward these packets to the new COA of MN which is FA_{new} in this example. This forwarding of packets is another optimization of the basic Mobile IP providing **smooth handovers**.

Without this optimization, all packets in transit would be lost while the MN moves from one FA to another.

NOTE: Unfortunately, this optimization of mobile IP to avoid triangular routing causes several security problems (e.g., tunnel hijacking).

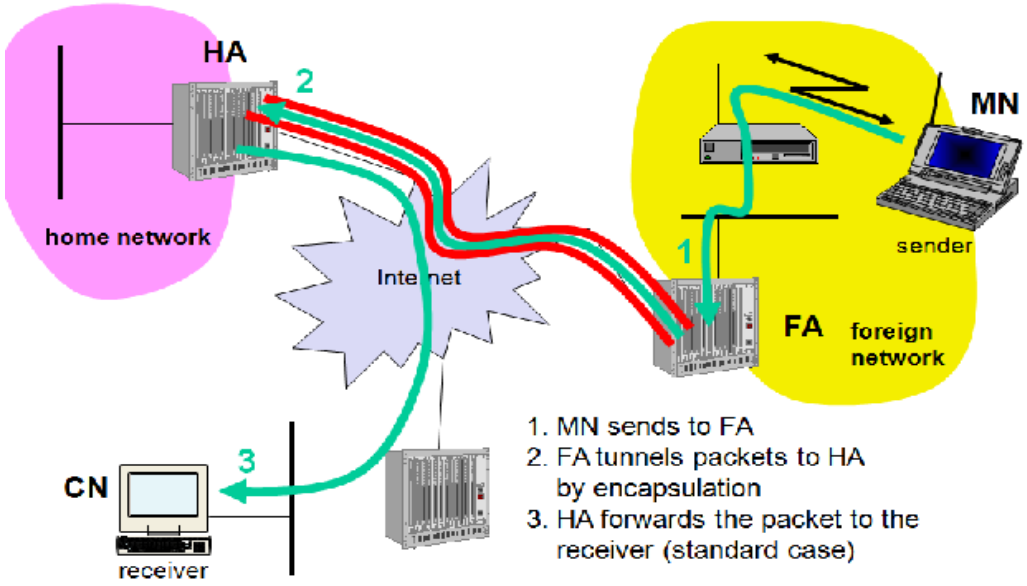
---

8. Explain the Reverse tunneling techniques used in WLAN.

OR

Explain the need for Reverse tunnel:

A **mobile** node can request a **reverse tunnel** between its foreign agent and its home agent when the **mobile** node registers. A **reverse tunnel** is a **tunnel** that starts at the **mobile** node's care-of address and terminates at the home agent.



But there are several severe problems associated with this simple solution.

● **Firewalls:**

Almost all companies and many other institutions secure their internal networks (intranet) connected to the internet with the help of a firewall. All data to and from the intranet must pass through the firewall. Besides many other functions, firewalls can be set up to filter out malicious **(intruder)** addresses from an administrator's point of view.

Quite often firewalls only allow packets with topologically correct addresses to pass. However, MN still sends packets with its fixed IP address as source which is not topologically correct in a foreign network.

● **Multi-cast:**

Reverse tunnels are needed for the MN to participate in a multicast group. While the nodes in the home network might participate in a multi-cast group, an MN in a foreign network cannot transmit multi-cast packets in a way that they emanate from its home network without a reverse tunnel.

● **TTL:**

Consider an MN sending packets with a certain TTL while still in its home network. The TTL might be low enough so that no packet is transmitted outside a certain region. If the MN now moves to a foreign network, this TTL might be too low for the packets to reach the same nodes as before.

A reverse tunnel is needed that represents only one hop, no matter how many hops are really needed from the foreign to the home network.

Hence, Reverse tunneling was added as an option to mobile IP in the new standard.

NOTE:

1. Obviously, **reverse tunneling now creates a triangular routing problem in the reverse direction.** All packets from an MN to a CN go through the HA.

2. Reverse tunneling also raises several security issues which have not been really solved up to now. For example, tunnels starting in the private network of a company and reaching out into the internet could be hijacked and abused for sending packets through a firewall.

---

9. Explain the features of IPv6 in mobile IP.

Need:

- When MN shifts its position from one location to another location in IPV4 registration request is required (i.e,) between Home Agent to Foreign Agent.
- In IPV6 no special mechanisms are required for updating the address information. **Address auto configuration** facility is has **in built.**
- Agent advertisement is not necessary in IPV6
- It has high security.
- Every IPV6 node can send binary updates to another node so that **MN can send** its **current care of address directly to CN** (Correspond Node) **and HA** (Home Agent).
- Soft handover is possible with IPV6
- No abrupt disconnection even a MN (Mobile Node) shifts to new network
- IPV6 can able to provide service without stopping the process.

Advantage:

- Foreign Agent is not needed anymore.
- CN(Correspond Node) itself able to process binding updates(it has cache memory).
- MN itself can able to receive packets and they itself send binding updates to CN directly.

Limitations:

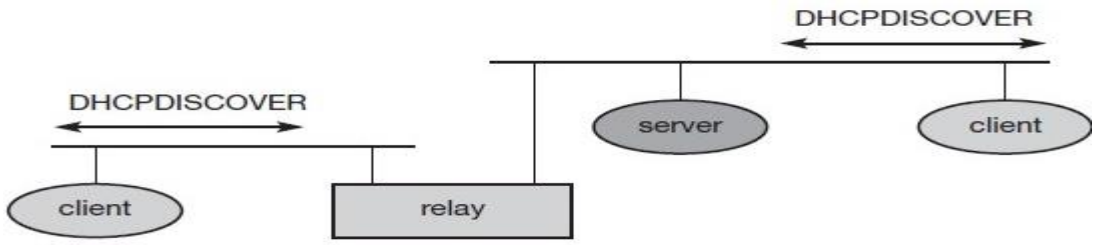
- IPV6 does not solve firewall problem.
- Keeping all these parameters/problems a new technology called Cellular IP was evolved which is known as micromobility.

---

10. State the concepts used in Dynamic host configuration protocol techniques.

The dynamic host configuration protocol is mainly used to simplify the installation and maintenance of networked computers.

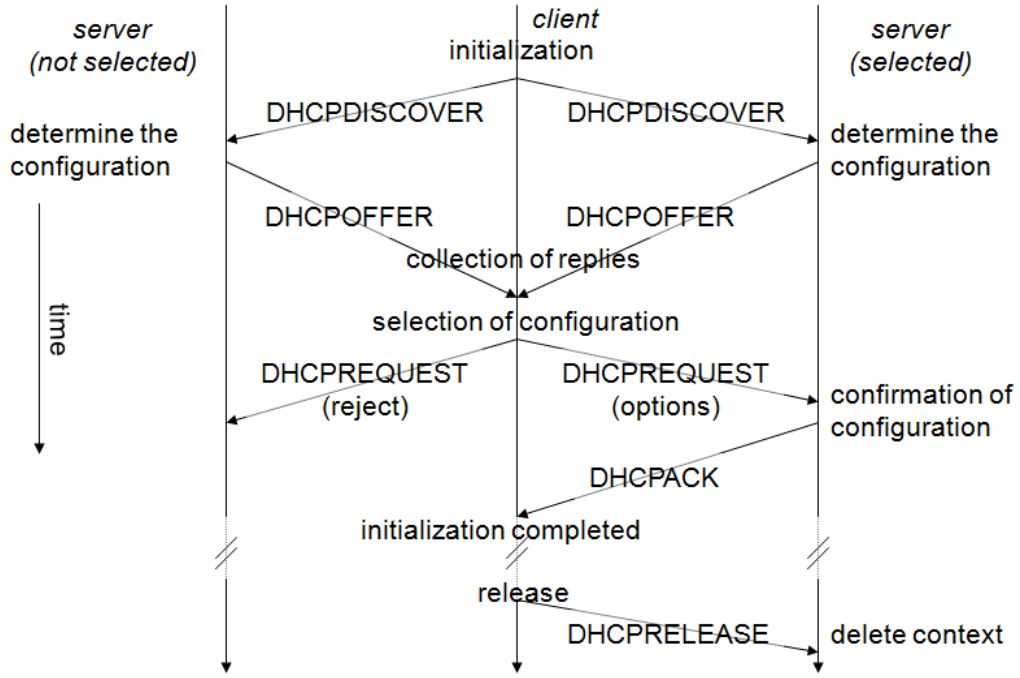
NEED: If a new computer is connected to a network, DHCP can provide it with all the necessary information for full system integration into the network, e.g., addresses of a DNS server and the default router, the subnet mask, the domain name, and an IP address. DHCP is based on a client/server model as shown in Figure below.



DHCP clients send a request to a server (DHCPDISCOVER in the example) to which the server responds. A client sends requests using MAC broadcasts to reach all devices in the LAN. A DHCP relay might be needed to forward requests across inter-working units to a DHCP server.

A typical initialization of a DHCP client is shown in Figure below. The figure shows one client and two servers. As described above, the client broadcasts a DHCPDISCOVER into the subnet.

There might be a relay to forward this broadcast. In the case shown, two servers receive this broadcast and determine the configuration they can offer to the client.



Servers reply to the client's request with DHCPOFFER and offer a list of configuration parameters. The client can now choose one of the configurations offered.

The client in turn replies to the servers, accepting one of the configurations and rejecting the others using DHCPREQUEST. If a server receives a DHCPREQUEST with a rejection, it can free the reserved configuration for other possible clients.

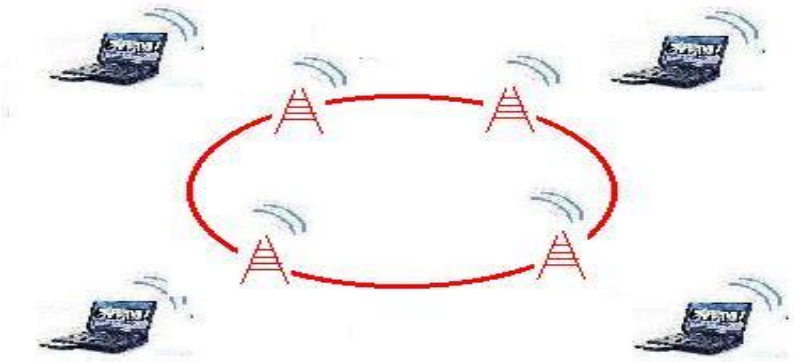
The server with the configuration accepted by the client now confirms the configuration with DHCPACK. This completes the initialization phase.

If a client leaves a subnet, it should release the configuration received by the server using DHCPRELEASE. Now the server can free the context stored for the client and offer the configuration again. The configuration a client gets from a server is only leased for a certain amount of time, it has to be reconfirmed from time to time.

-

MANET

- A mobile ad hoc network (**MANET**), also known as wireless Ad hoc network or Ad hoc wireless network is a **continuously self-configuring, infrastructure (**central device or Access point) **less** network where mobile devices are connected in wireless fashion.
- Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently.



Advantages:

1. Instant infrastructure: Unplanned meetings, spontaneous communications etc. cannot depend on any infrastructure. Infrastructures need planning and administration. It would take too long to set up this kind of infrastructure; therefore, in such cases this ad-hoc network will be helpful.

2. Disaster relief: Infrastructures typically break down in disaster areas. Hurricanes (cyclone) cut phone and power lines, floods destroy base stations, fires burn servers. In such cases ad-hoc network will be helpful.

3. Remote areas: Even if infrastructures could be planned ahead, it is sometimes too expensive to set up an infrastructure in sparsely (less no of people) living areas. Ad-hoc networks or satellite infrastructures can be a solution.

4. Effectiveness: Services provided by existing infrastructures will be too expensive for certain applications. If, for example, in a connection oriented cellular networks an application sends only a small status information every other minute, a cheaper ad-hoc packet-oriented network might be a better solution.

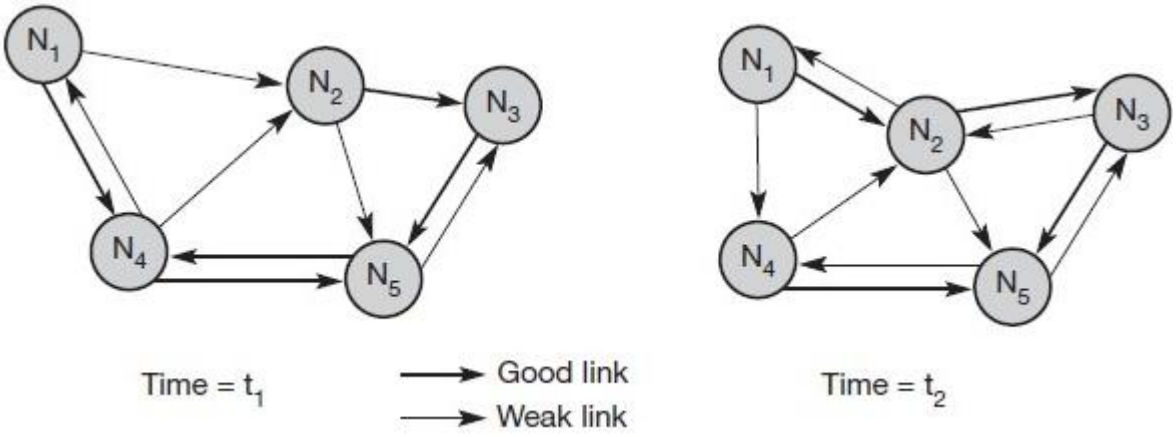
Registration procedures also consumes less time only in ad-hoc networks.

CHALLENGES FACED BY Ad-Hoc network:

(OR)

Why traditional routing algorithms cannot be employed for MANET?

In general the ultimate **objective of any network is routing (delivering) the data effectively between source and destination.** This routing in MANET involves multiple challenges due to multiple issues mentioned below:



Example for Ad-Hoc network

In figure shown above at time t1 the MANET structure will be as shown in figure left side, after some time at time t2 the structure changes as shown in figure right side. The **reasons** for this are **due to different antenna characteristics**. All antennas will not transmit with same power.

In figure shown above at time t1 N1 node receives weak signal from node N4 whereas at time t2 N1 does not receive any signal from N4. It means the **links are asymmetric between the two nodes.** The challenges are mentioned below:

1. **Asymmetric links:** The information transferred between two nodes will not always remain same as shown in figure above.

2. Redundant links: Wired networks have redundant (additional) links to survive for link failures problem. But this redundancy in wired networks can be controlled by a network administrator. In ad-hoc networks nobody controls redundancy, so there might be multiple redundant links. A high redundancy in ad-hoc can cause a large computational overhead for routing table updates.

3. Interference: In wired networks links exist only where a wire exists, and connections are planned by network administrators. This is not the case for wireless ad-hoc networks. **Links come and go depending on transmission characteristics**, one transmission might interfere with another. **Interference creates additional new problems.**

4. Dynamic topology: The greatest problem for routing arises due to dynamic topology. The mobile node changes its structure as shown in Figure at different time. These results in frequent changes in topology, so snapshots (structures) are valid only for a very short period of time.

Routing algorithms used **in wired networks** would either **react much too slowly or generate too many updates** for **changes in topology**. Routing table updates in fixed networks, for example, take place every 30 seconds. This updating frequency might be too low to be useful for ad-hoc networks. Some algorithms rely on a complete picture of the whole network. While this works in wired networks where changes are rare, it fails completely in ad-hoc networks. The topology changes during the distribution of the 'current' snapshot of the network, rendering the snapshot useless.

Let us go back to the example network in Figure shown above and assume that node N1 wants to send data to N3 and needs an acknowledgement. If N1 had a complete overview of the network at time t1, which is not always the case in ad-hoc networks, it would choose the path N1, N2, N3, for this requires only two hops (if we use hops as metric).

Acknowledgements cannot take the same path, N3 chooses N3, N5, N4, N1. Just a moment later, at time t2, the topology has changed. Now N3 cannot take the same path to send acknowledgements back to N1, while N1 can still take the old path to N3. Although already more complicated than fixed networks, this example still assumes that nodes can have a complete insight into the current situation.

The optimal knowledge for every node would be a description of the current connectivity between all nodes, the expected traffic flows, capacities of all links, delay of each link, and the computing and battery power of each node. While even in fixed networks traffic flows are not exactly predict table, for ad-hoc networks link capacities are additionally unknown.

The capacity of each link can change from 0 to the maximum of the transmission technology used. **In real ad-hoc networks no node knows all these factors, and establishing up-to-date snapshots of the network is almost impossible.**

Ad-hoc networks using mobile nodes face additional problems due to hardware

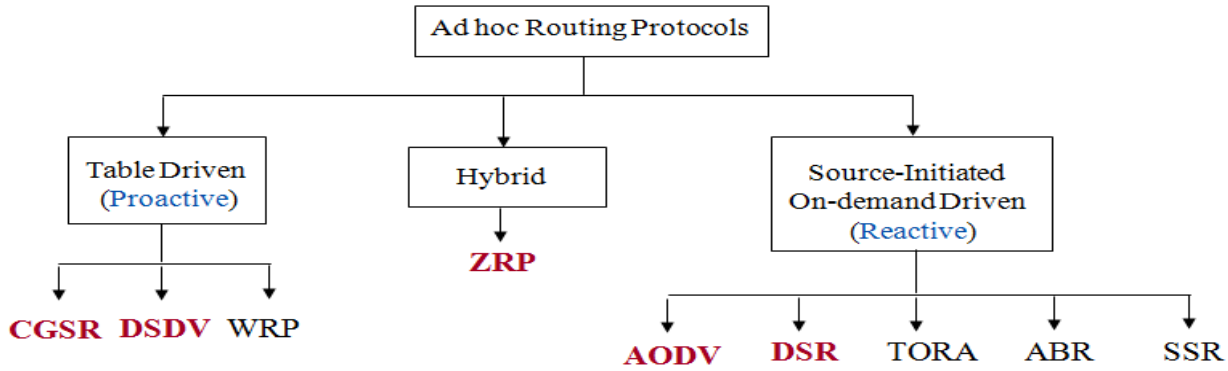
limitations. **Using the standard routing (traditional routing DVR, LSR) protocols with periodic updates wastes battery power without sending any user data. Periodic updates waste bandwidth.**

Due to the reasons mentioned above only traditional routing algorithms are not used in MANET.

CLASSIFICATIONS OF ROUTING ALGORITHMS IN MANET

Routing protocols can be classified into three types:

1. Proactive routing protocol 2. Reactive routing protocol 3. Hybrid protocols.



1. Proactive Routing Protocols (Table-driven)

- Proactive routing protocol **stores the routing information** and maintains (sharing) the information up to date by exchanging the control packet from their neighbours.
- This method **creates more overhead** since it updates the information often even if the node does not transmit also.
- The method **does not experience any delay** when the first node wishes to transmit.
- **More** amounts of **resources are wasted.**
- The **examples** of proactive routing protocols are **DSDV, OLSR, and WRP.**

2. Reactive Routing Protocols (Source-initiated on-demand)

- It does not store any routing information.
- It creates a path and updates the information to its neighbours whenever the node request to transfer data only.
- It creates less overhead.
- The method experiences more delay when the first node wishes to transmit since the updates were not started initially.
- Resources are not wasted.

- The examples of reactive routing protocols are **DSR, AODV**.

3. Hybrid Routing Protocols

It is the mixture of reactive and proactive routing protocols. The example of Hybrid routing protocols are ZRP, BGP, EIGRP.

Explain DSDV routing protocol or Explain Proactive routing protocol with a suitable example:

DESTINATION SEQUENCE DISTANCE VECTOR ROUTING **(DSDV)**

Need:

We have two problems associated with traditional routing algorithms like DVR Distance Vector routing are:

1. Count to infinity problem
2. Looping problem

To avoid both these problems we go for DSDV.

Characteristics of DSDV

- DSDV is Destination Based routing.
- **DSDV is Proactive** (Table Driven)
  - Here, each node maintains routing information for all known destinations.
  - Routing information will be updated periodically.
  - Traffic overhead exists even if there is no change in network topology.
  - Maintains routes which are never used also.
  - Guarantee Loop Freeness.

DSDV adds two things to the distance vector algorithm:

1. Sequence numbers:

- Each routing advertisement comes with a sequence number. Within ad-hoc networks, advertisements may propagate along many paths.
- **Sequence numbers** help to apply the advertisements in correct order. This **avoids the loops** that are occur in distance vector algorithm.
- **These Sequence number**s are originated from destination

Rules to set sequence number information

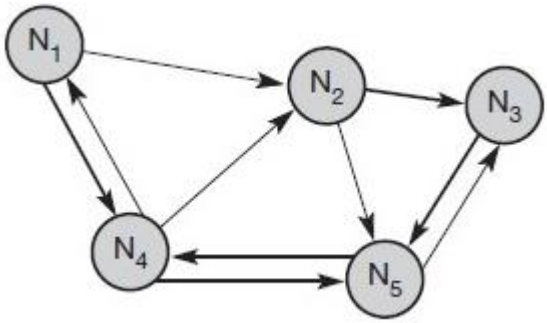
- On each advertisement increase own destination sequence number (use only even numbers)

- If a node is **no more reachable** (timeout) **increase sequence number of this node by 1 (odd sequence number)** and set metric = ∞

2. Damping:

Transient changes in topology of short duration should not destabilize the routing mechanisms. Advertisements containing changes in the current topology are stored.

A node waits with dissemination (information) if these changes are probably unstable. Waiting time depends on the time between the first and the best announcement of a path to a certain destination.



The routing table for N1 in Figure above would be as shown in Table below. For each node N1 stores the next hop toward this node, the metric (here number of hops), the sequence number of the last advertisement for this node, and the time at which the path has been installed first.

The table contains flags and a settling time that helps to decide when the path can be assumed stable. Router advertisements from N1 now contain data from the first, third, and fourth column: destination address, metric, and sequence number.

Destination	Next hop	Metric	Sequence no.	Instal time
N_1	N_1	0	S_1–321	T_4–001
N_2	N_2	1	S_2–218	T_4–001
N_3	N_2	2	S_3–043	T_4–002
N_4	N_4	1	S_4–092	T_4–001
N_5	N_4	2	S_5–163	T_4–002

Advantage:

- It does not have looping problem.
- DSDV requires low memory requirements.

- Converge quickly (finds the optimum path quickly).
- No latency (delay) caused due to route discovery.

Disadvantages:

- No sleeping nodes (it means all the nodes will be active at all time)
- Creates more overhead. It means most of the routing information are never used.

Explain Reactive routing protocol with a suitable example:

Need:

- It does not store any routing information.
- It creates a path and updates the information to its neighbours whenever the node request to transfer data only.
- It creates less overhead.
- The method experiences more delay when the first node wishes to transmit since the updates were not started initially.
- Resources are not wasted.
- The examples of reactive routing protocols are **DSR, AODV**.

1. Dynamic Source Routing (DSR).

Principle: Each router maintains a route cache in which it catches source routes that it has learnt. When one host sends a packet to another host, it first checks its route cache for a source route to the destination. If a route is found, the sender uses it to transmit the packet; else it may attempt to discover a route using route discovery protocol.

It divides the task of routing into two separate steps.

1. Route discovery: A node tries to discover a route to a destination only if it has to send something to that destination and if currently no known route are existing.

2. Route maintenance: If a node is continuously sending packets via a route, it checks the status of the route. As soon as a node detects problems with the current route, it will find an alternative route.

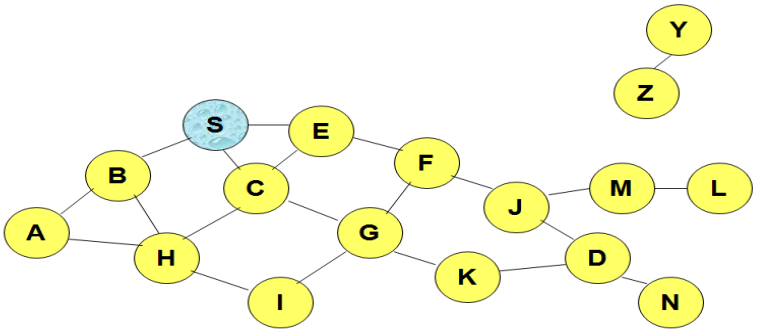
Steps involved in DSR

- If a node needs to discover a route, it broadcasts a route request (RREQ) with a unique identifier and the destination address as parameters.
- Any node that receives a route request does the following.

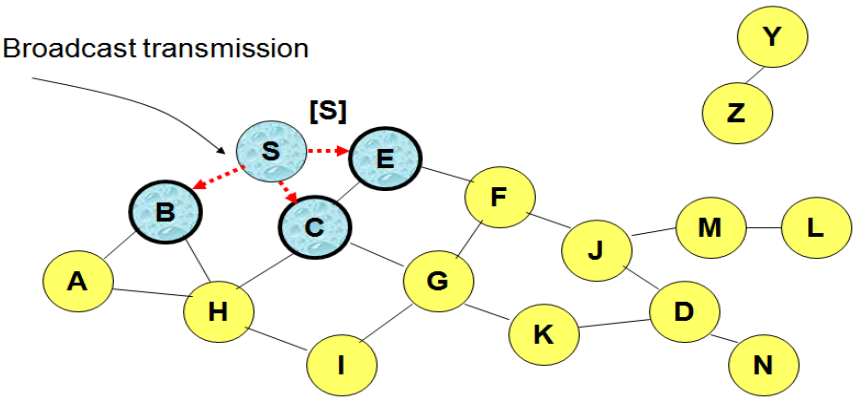
(i) If the node has already received the request (which is identified using the unique identifier), it drops the request packet.

(ii) If the node recognizes its own address as the destination, the request has reached its target.

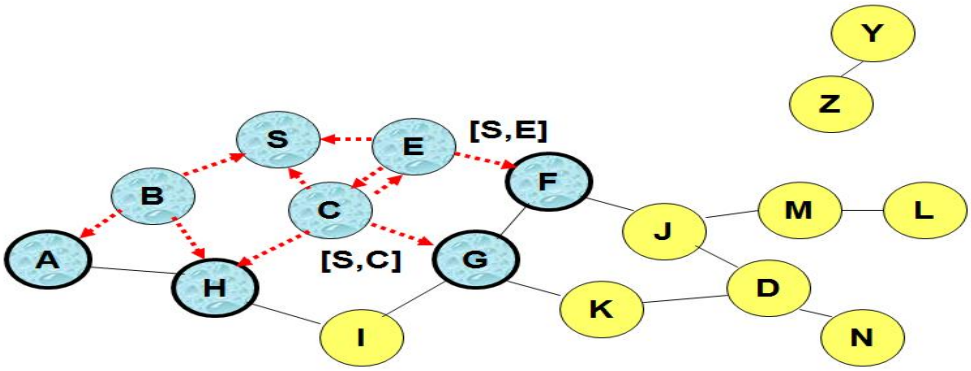
1. Route Discovery in DSR



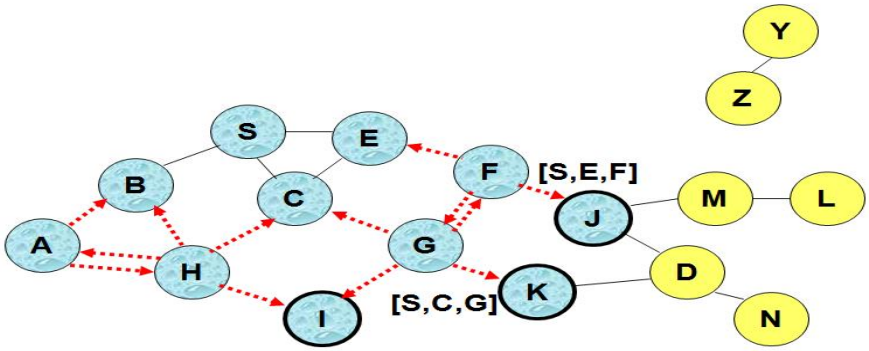
Represents a node that has received RREQ for D from S



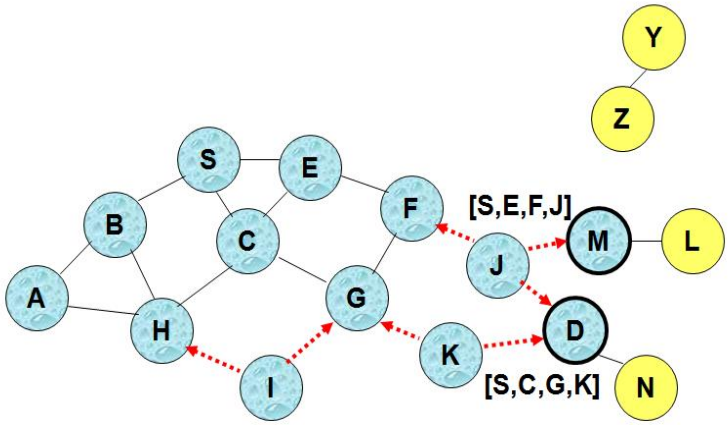
Represents transmission of RREQ



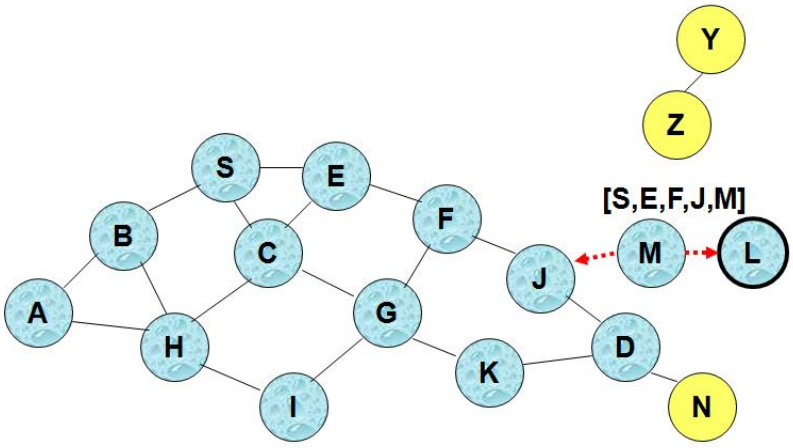
- Node H receives packet RREQ from two neighbors potential for collision



Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once.

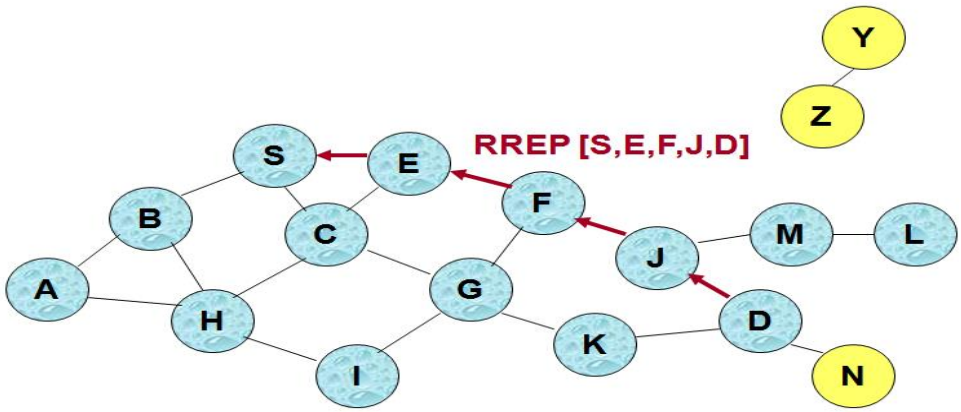


- Nodes J and K both broadcast RREQ to node D. Since nodes J and K are hidden from each other, their transmissions may collide.



- Node D does not forward RREQ, because node D is the intended target of the route discovery.
- Destination D on receiving the first RREQ, sends a Route Reply (RREP)
- RREP is sent on a route obtained by reversing the route appended to received RREQ.
- RREP includes the route from S to D on which RREQ was received by node D.

2. Route Reply in DSR



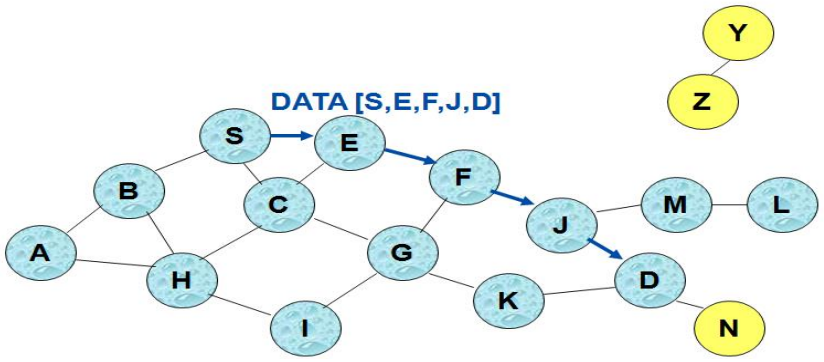
Represents RREP control message

- Route Reply can be sent by reversing the route in Route Request (RREQ) only if links are guaranteed to be bi-directional.

Advantage of DSR

- Node S on receiving RREP, **caches** (stores) the route included in the RREP.
- When node S sends a data packet to D, the entire route is included in the packet header
  - hence the name **source routing**
  - Intermediate nodes use the source route included in a packet to determine to whom a packet should be forwarded

3. Data Delivery in DSR

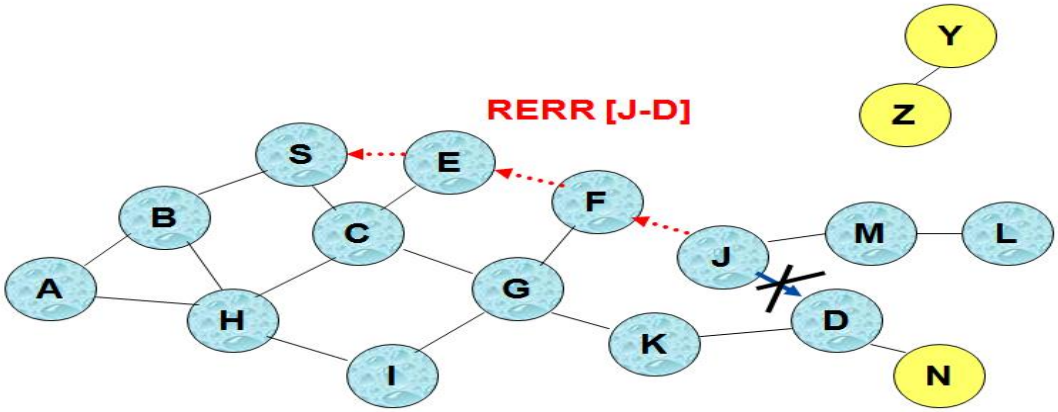


Packet header size grows with route length.

Use of Route Caching

- can speed up route discovery.
- can reduce propagation of route requests.

Route Error (RERR)



- J sends a route error to S along route J-F-E-S when its attempt to forward the data packet S (with route SEFJD) on J-D fails
- Nodes hearing RERR update their route cache to remove link J-D.

Advantages of DSR

- Routes are maintained only between nodes who need to communicate.
- Reduces overhead of route maintenance.
- Route caching can further reduce route discovery overhead.
- A single route discovery may yield many routes to the destination, due to intermediate nodes replying from local caches.

Disadvantages of DSR

- Packet **header size grows** with route length due to source routing.
- **Flood of route requests** may potentially **reach all nodes in** the **network**.
- **Care must be taken** to **avoid collisions** between route requests propagated by neighboring nodes.

Why DSR is called source based routing?

Note: DSR is called source routing because here the **entire route to the destination node D is identified by the source node S in step by step with the help of cache memory.** Hence it is called source based routing.

-

Ad-hoc On-Demand Distance Vector Routing (AODV)

It is an example for reactive routing.

- It improves DSDV by minimizing number of broadcasts by creating routes on-demand.
- It improves DSR by maintaining routing tables only at the nodes between source and destination.

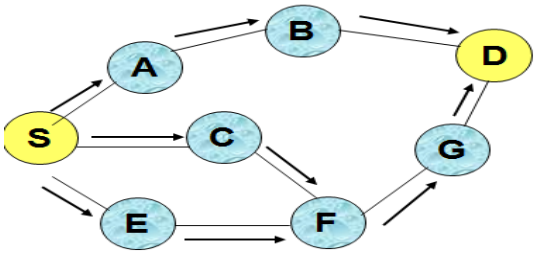
AODV uses two messages similar to DSR for route discovery and reply

1. RREQ –Route Request

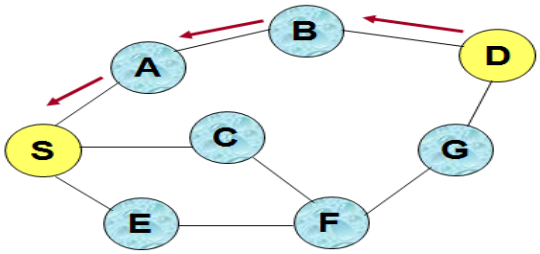
2. RREP – Route Reply

3. RERR – Route Error

AODV Route Discovery



Propagation of RREQ



Route Reply to Source

– Source **initiates a path** discovery process to locate the destination node by broadcasting a route request **(RREQ)** packet to its neighbors. The neighbors in turn forward the request to their neighbors and so on until destination is identified.

– **Destination sequence numbers are used to ensure that routes are loop free** and have the most recent route information.

– Each node maintains its own sequence number and broadcast ID (incremented with every RREQ the node initiates)

– Source sends RREQ (which includes sequence number for the destination) along with its own sequence number and broadcast ID.

– The intermediate node reply to RREQ only if

– sequence number of destination <= sequence number in the current RREQ

– When a node broadcasts a RREQ, a reverse path towards the source is created.

– Route reply uses the reverse path when RREQ is forwarded.

– A routing table entry containing reverse path is deleted after a sufficient timeout interval.

- A **routing table entry** containing forward path **is deleted if it is not activ**e for a **sufficient timeout interval.**
- A node is considered active if it participates in forwarding the packets.
- **Link failures are known to all active nodes using Route Error (RERR) messages**.
- When a **node cannot forward a packet** towards a destination, it generates a **RERR message**; increments sequence number for destination; includes this incremented destination sequence number in the RERR message.
- When a source receives the RERR, it initiates a new route discovery process for the destination using sequence number equal or greater than the destination sequence number in RERR message
- **Periodic Hello messages are used to ensure the links exist.**
- **A link failure occurs when no hello message are exchanged for a timeout interval**.

Advantage:

1. AODV creates routes only on demand, which greatly reduces the periodic control message overhead.

Drawback:

1. AODV queues data packets while discovering new routes and queued packets are sent out only when new routes are found.

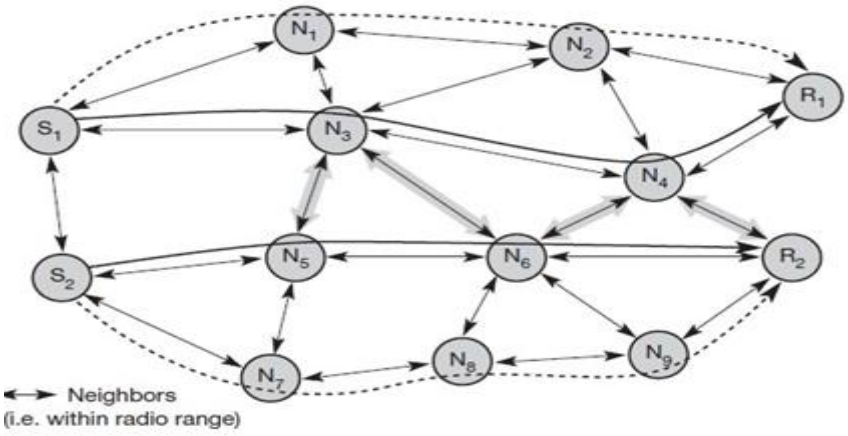
2. Latency exists when a new route is needed.

Explain the Alternative metrics used in Mobile IP layer:

Need: In general DSDV, DSR and AODV typically **use the number of hops** as routing metric. Although very simple, especially in wireless ad-hoc networks, this is not always the best choice.

Even for fixed networks, e.g., bandwidth can also be a factor for the routing metric. **Due to the varying link quality** and the fact that different transmissions can interfere, other metrics can be more useful.

One other metric, called **least interference routing** (LIR), takes possible interference into account. The figure shows below uses an ad-hoc network topology.



Sender S1 wants to send a packet to receiver R1, S2 to R2. Using the hop count as metric, S1 could choose three different paths with three hops, which is also the minimum. Possible paths are (S1, N3, N4, R1), (S1, N3, N2, R1), and (S1, N1, N2, R1). S2 would choose the only available path with only three hops (S2, N5, N6, R2).

Taking interference into account, this picture changes. To calculate the possible interference of a path, each node calculates its possible interference (interference is defined here as the number of neighbors that can overhear a transmission). Every node only needs local information to compute its interference.

In this example, the interference of node N3 is 6, that of node N4 is 5 etc. Calculating the costs of possible paths between S1 and R1 results in the following:

C1 = cost(S1, N3, N4, R1) = 16,
C2 = cost(S1, N3, N2, R1) = 15,
and C3 = cost(S1, N1, N2, R1) = 12.

All three paths have the same number of hops, but the last path has the lowest cost due to interference. Thus, S1 chooses (S1, N1, N2, R1). S2 also computes the cost of different paths, examples are C4 = cost(S2, N5, N6, R2) = 16 and C5 = cost(S2, N7, N8, N9, R2) = 15. S2 would, therefore, choose the path (S2, N7, N8, N9, R2), although this path has one hop more than the first one.

With both transmissions taking place simultaneously, there would have been interference between them as shown in Figure. In this case, least interference routing helped to avoid interference. Taking only local decisions and not knowing what paths other transmissions

take, this scheme can just lower the probability of interference. Interference can only be avoided if all senders know of all other transmissions (and the whole routing topology) and base routing on this knowledge.

Compare **IPv4 and IPv6**

Parameter	**IPv4**	**IPv6**
Size of IP address	32-Bit IP Address.	128 Bit IP Address.
Checksum	It has checksum fields	Does not have checksum fields
Network Configuration	Networks need to be configured either **manually** or with DHCP.	IPv6 support **auto configuration** capabilities.
SNMP Simple Network Management Protocol	SNMP support IPv4	SNMP does not support IPv6.
Security	Limited security	High security
Address configuration	Manual or via DHCP	Stateless address autoconfiguration using Internet Control Message Protocol version 6 (ICMPv6) or DHCPv6
Packet header	It does include flow label field for QoS handling.	Packet header contains Flow Label field that specifies packet flow for QoS handling
Broadcast	YES	NO

IPv4 and IPv6 cannot communicate with other but can exist together on the same network. This is known as **Dual Stack.**

SESSION INITIATION PROTOCOL (SIP)

Explain about Session Initiation Protocol:

- **SIP is** one of the most common protocol used in **VoIP** Voice over internet protocol technology.

- It is a signalling protocol used to create modify and terminate a **multimedia session** over the internet protocol.
- **Session:** Is a simple call or conversation between two end points. The end points can be smart phone, a laptop or any device that can receive and send multimedia over the internet.
- SIP takes the help of **SDP** session description protocol and **RTP** real time transport protocol for delivering voice and video over internet.

Applications of SIP:

- File transfer
- Instant messaging
- Video conferencing
- Online games
- Steaming multimedia distribution

Components or elements involved in SIP:

- User Agent
- Proxy Server
- Registration Server
- Redirect Server
- Location Server

User Agent: They are the endpoints (smart phone, laptop, etc.) and one of the most important network elements of a SIP network. These endpoints can initiate modify or terminate session.

It (UA) can be divided into two parts

- User Agent Client(UAC)- The entity that sends a request and receives a response.
- User Agent Server(UAS)-The entity that receives a request and sends a response.

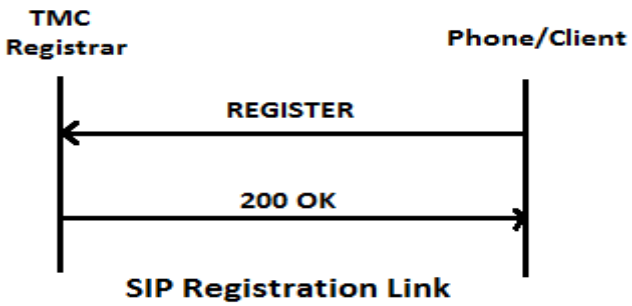
Proxy Server: It is the network element that takes a request from a user agent and forwards it to another user

- Basically the role of a proxy server is much like a router
- A proxy server sits in between two user agents
- There can be a maximum of 70 proxy server in between a source and a destination

Two types of proxy server:

- **Stateless proxy server**- It simply forwards the message received. This type of server does not store any information of a call or a transaction
- **Statefull proxy server**- This type of proxy server keeps track of every request and response received and can use it in future if required.

Registration Server: The registrar server accepts registration requests from user agents. It helps users to authenticate themselves within the network. It stores the URI and the location of users in a database to help other SIP servers within the same domain. Take a look at the following example that shows the process of a SIP Registration.



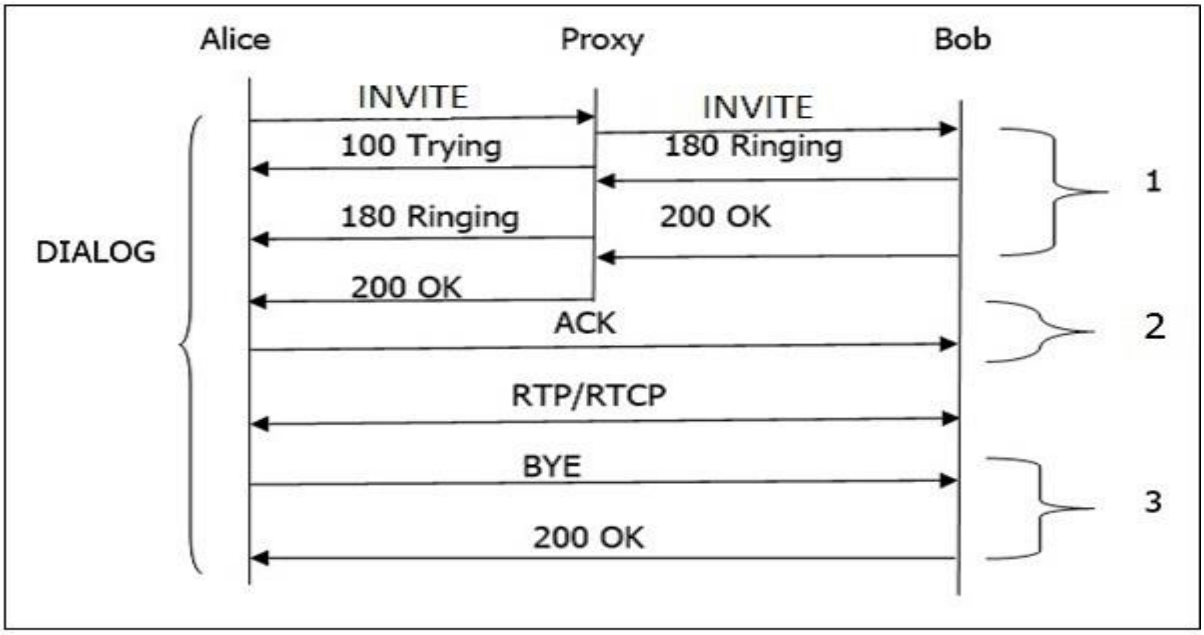
Here the caller wants to register with the TMC domain. So it sends a REGISTER request to the TMC's Registrar server and the server returns a 200 OK response as it authorized the client.

Location Server: The location server provides information about a caller's possible locations to the redirect and proxy servers. Only a proxy server or a redirect server can contact a location server.

The following figure depicts the roles played by each of the network elements in establishing a session.

The following image shows the basic call flow of a SIP session. Given below is a step-by-step explanation during the call flow.

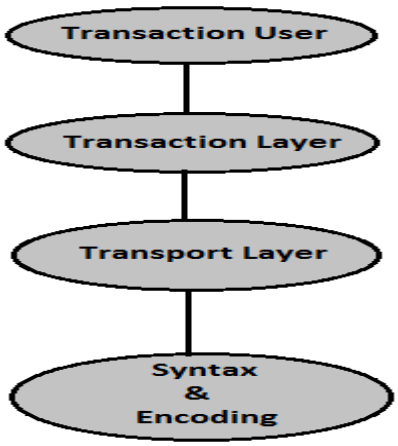
- An INVITE request that is sent to a proxy server is responsible for initiating a session.
- The proxy server sends a **100 trying** response immediately to the caller (Alice) to stop the re-transmissions of the INVITE request.
- The proxy server searches the address of Bob in the location server. After getting the address, it forwards the INVITE request further.
- Thereafter, **180 Ringing** (Provisional responses) generated by Bob is returned back to Alice.



- A **200 OK** response is generated soon after Bob picks the phone up.
- Bob receives an **ACK** from the Alice, once it gets **200 OK**.
- At the same time, the session gets established and RTP packets (conversations) start flowing from both ends.
- After the conversation, any participant (Alice or Bob) can send a **BYE** request to terminate the session.
- **BYE** reaches directly from Alice to Bob bypassing the proxy server.
- Finally, Bob sends a **200 OK** response to confirm the BYE and the session is terminated.
- In the above basic call flow, three **transactions** are (marked as 1, 2, 3) available.

The complete call (from INVITE to 200 OK) is known as a **Dialog**.

SIP – System Architecture:



- The lowest layer of SIP is its **syntax (procedure) and encoding**.
- At the second level is the **transport layer**. It defines how a Client sends requests and receives responses and how a Server receives requests and sends responses over the network. All SIP elements contain a transport layer.
- Next comes the **transaction layer**. A transaction is a request sent by a Client transaction to a Server transaction. Any task that a user agent client (UAC) accomplishes takes place using a series of transactions. **Stateless proxies** do not contain a transaction layer.
- The layer above the **transaction layer** is called the transaction user. Each of the SIP entities, except the **Stateless proxies**, is a transaction user.

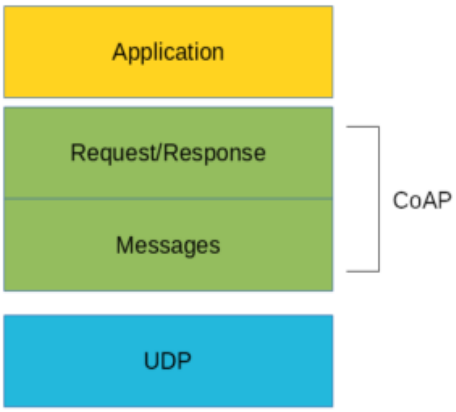
Write short notes on COAP:

- Constrained Application Protocol (COAP) is a web transfer protocol that is used for **constrained (specific) nodes or networks** such as IOT, M2M. Hence the name Constrained Application Protocol.
- This protocol is **developed for Internet of Things (IOT)** devices having less memory and less power specifications. Since it is designed for web applications it is also known as **"The Web of Things protocol'**
- It was designed by the Internet Engineering Task Force (IETF).

Features of CoAP:

- Web protocol used in M2M with constrained requirements.
- Asynchronous message exchange.

- Low overhead and very simple to use.
- It has Proxy and cache memory facility.
- **COAP protocol stack**



Two different layers are involved to create COAP protocol: Messages and Request/Response.

The Messages layer deals with UDP and with asynchronous messages. The Request/Response layer manages their interaction based on request/response messages.

Terminologies used in COAP

- **Sender**: The entity that sends a message.
- **Recipient**: The destination of a message.
- **Client**: The entity that **sends a request.**
- **Server**: The entity that **receives a request** from a client and sends back a response to the client.
- **Endpoint**: An entity that participates in the COAP protocol. Usually, an Endpoint is identified with a host.

COAP supports four different message types:

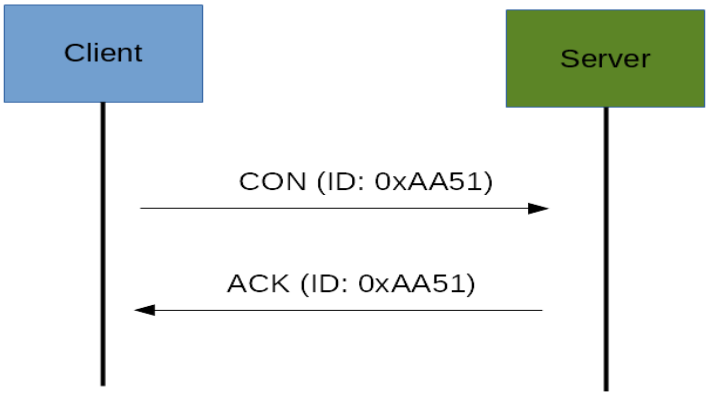
- Confirmable
- Non-confirmable
- Acknowledgment
- Reset

Confirmable message: A confirmable message is a **reliable message.** When exchanging messages between two endpoints, these messages can be reliable. In COAP, a reliable

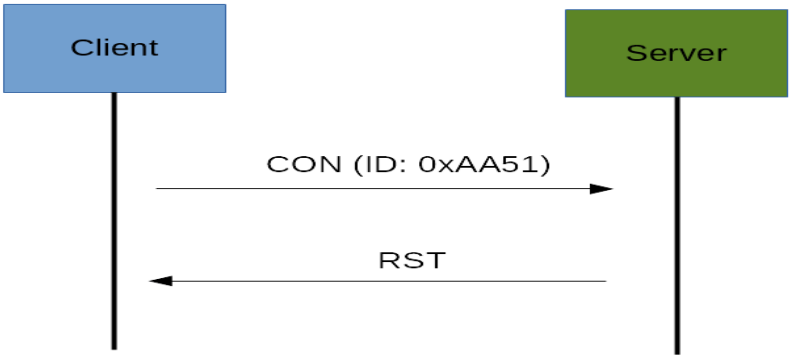
message is obtained using a **Confirmable message (CON)**. Using this kind of message, the client can be sure that the message will arrive at the server. A Confirmable message is sent again and again until the other party sends an **acknowledge message (ACK)**.

Note: The ACK message contains the same ID of the confirmable message (CON).

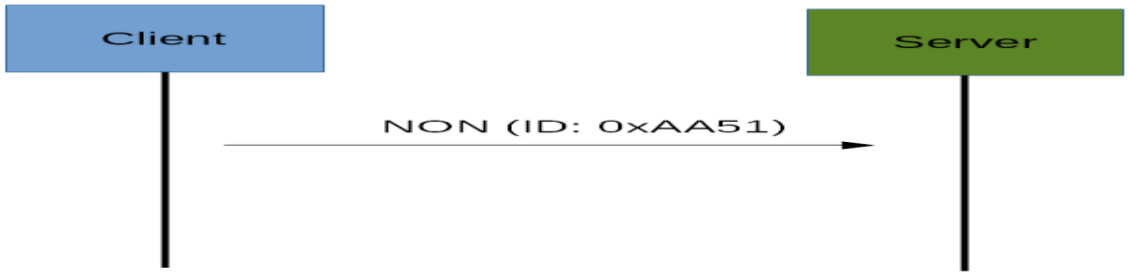
The picture below shows the message exchange process:



If the **server has troubles managing the incoming request**, it can **send** back a **Reset message (RST)** instead of the Acknowledge message (ACK).



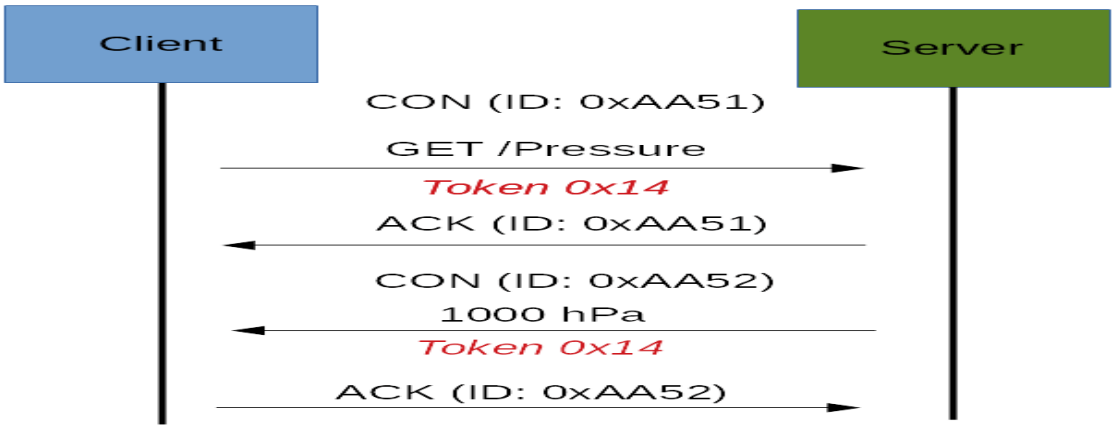
Non-confirmable message: The other message category is the Non-confirmable (NON) messages. These are messages that **don't require an Acknowledge by the server**. They are **unreliable messages** or in other words messages that do not contain critical information that must be delivered to the server.



COAP Request/Response Model: The COAP Request/Response is the second layer in the COAP protocol stack. The request is sent using a Confirmable (CON) or Non-Confirmable (NON) message. There are several scenarios depending on if the server can answer immediately to the client request or it can answer later if is not in a position to reply immediately.

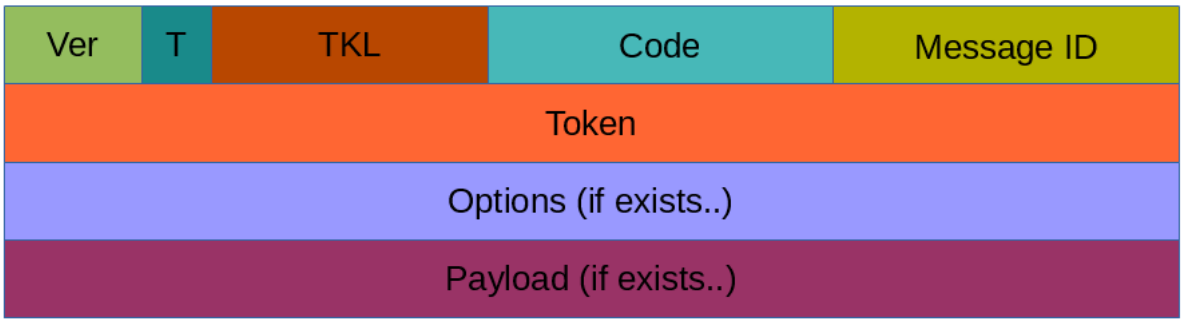
Scenario 1: If the **server can answer immediately** to the client request, then the request is carried using a Confirmable message (CON), the server sends back to the client an Acknowledge message containing the response.

As you can notice in the COAP message, there is a Token. The Token is different from the Message-ID and it is used to match the request and the response.



Scenario 2: If the **server can't answer** to the request coming from the client **immediately**, then it sends an Acknowledge message with an empty response **(No token in ACK)**. As soon as the response is available, then the server sends a new Confirmable message to the client containing the response. At this point, the client sends back an Acknowledge message. It is shown in above figure.

COAP Message Format: It includes version, type, token length, code and message ID.



Where:

- **Ver**: It is a 2 bit unsigned integer indicating the version
- **T**: it is a 2 bit unsigned integer indicating the message type: 0 confirmable, 1 non-confirmable
- **TKL**: Token Length is the token 4 bit length
- **Code**: It is the code response (8 bit length)
- **Message ID**: It is the message ID expressed with 16 bit

Advantages:

- It is a simple protocol and it uses less overhead due to operation over UDP.
- It has smaller packet sizes. This leads to faster communication cycles. Again, this allows batteries to last longer.

- Synchronous communication is not necessary in COAP protocol.
- It has lower latency compare to HTTP.
- It consumes less power than HTTP.

Disadvantages:

1. COAP is unreliable protocol due to use of UDP. Hence COAP messages reach to the destination in improper order and even some times it may get lost.
2. It is an unencrypted protocol.
3. COAP has communication issues for devices behind Network Address Translation.

MICROMOBILITY:

Need: In general we have following limitation in mobile IP. To solve this problem only we go for micro mobility concept.

Scenario 1: Consider a situation where a **mobile node shifts from one location** (FA) **to another location** (FA) for one time. When it shifts **to obtain its service continuously** without interruption it has to register with the new FA initially. To do this **registration it needs** some amount of binding (basic) information and also involves some amount of time which introduces a **latency (delay)** in the process.

Scenario 2: Consider a situation where a **mobile node shifts frequently**. Then as mentioned previously it needs multiple time registration procedure and more binding information which **creates more latency** (delay) and **over head** to the mobile station.

To avoid this drawback only we go for micro mobility.

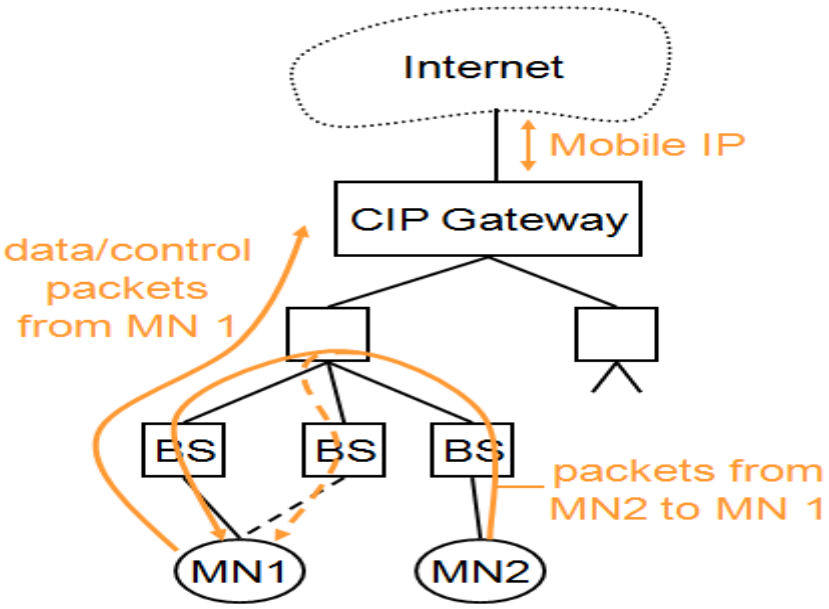
Principle involved in Micro-mobility: When the mobile node shifts frequently also the **local changes of the points of attachment are kept away from the home network** and the **information is given to the home agent only about major changes** (region change).

It can be achieved by three methods.

1. Cellular IP Gateway method
2. Hawaii
3. Hierarchical mobile IPv6 (HMIPv6)

1. Cellular IP Gateway method: In this method a **gateway** is maintained between the base station and the internet (outside world).The **gateway acts as a foreign agent** (intermediate) to the outside world (internet) and the home agent.

- The gateway will be having a **routing table** (look up table) which stores the address of each and every station connected in the network.
- As long as Mobile station is in the local region the gateway does not have any work.
- As shown in figure when the data move from MN2 to MN1 since it is connected adjacently the data are transferred through the corresponding base station (BS).
- When the data moves from MN1 to the outside world it is transferred to the CIP gateway.



Advantage:

Simple elegant and self configuring architecture.

Disadvantage/Limitation:

- **Security:** If cellular IP is not trusted, data can be transferred to multiple host.
- **Efficiency:** Additional load (routing table) is included on cellular IP gateway which may reduce the efficiency of the network.

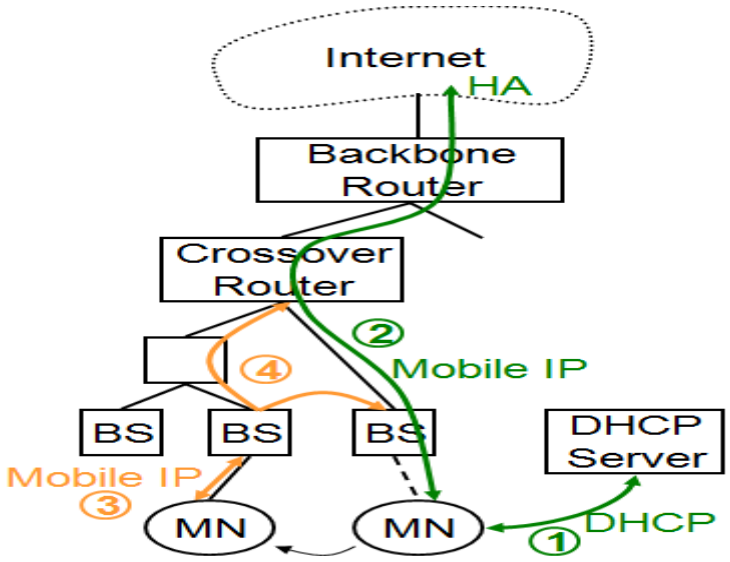
2. HAWAII (Hand-off Aware Wireless Access Internet

As, the name suggests Hand off aware it means a **transparency is maintained** between Home agent and Foreign agent when the mobile moves outside the region. It involves a **cross over router** which acts as a back bone between the MN and to the outside world.

Steps involved:

- As soon as a mobile node enters for transmission it obtains a temporary care of address.
- The MN then provides Registration request procedure to the Home agent.
- When the Mobile node shifts to new location inside the same foreign agent also it performs a registration request to the new base station.
- New BS update and sends the information to crossover router.
- When routing has been reconfigured successfully, the BS sends a registration reply to the MN.

Figure:



Advantage: Transparent to mobile node and home agent.

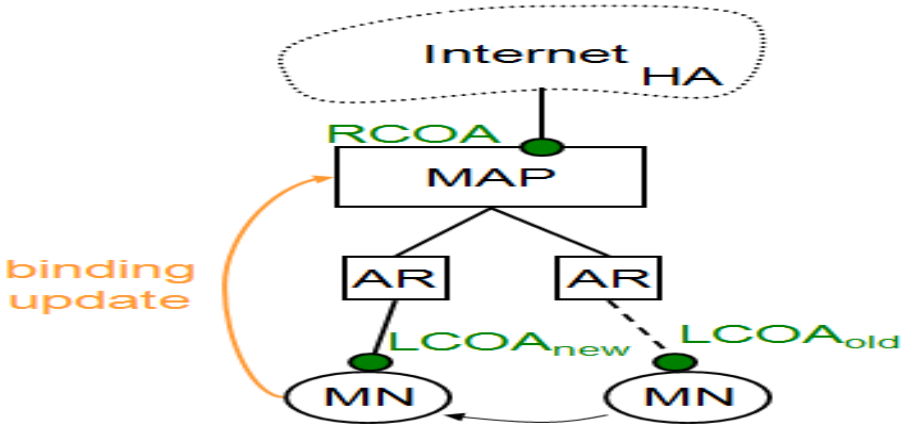
Limitation: No private address support is possible because of co-located COA.

3. HIERARCHICAL MOBILE IPV6 (HMIPV6)

- Here a **mobility anchor point (MAP)** is maintained between the Internet Home Agent and the Mobile Node.
- The MAP receives all packets on behalf of the MN, **encapsulates and forwards them directly to the MN's** current address (link COA, LCOA).
- As long as the MN stays within the local domain the LCOA does not change.
- **An access router (AR) defines** the boundaries of the mobility anchor point MAP.

- Regional care of address (RCOA) is a address which is necessary when the mobile node moves from one region to another region else local care of address Local care of address (LCOA) itself is enough.

Figure:



Limitation:

- Trusted mobile anchor point (MAP) is necessary.
- Security: It requires authentication and protection.

Difference between micro mobility and mobile IP

Micro mobility	Mobile IP
Local migration of mobile node will be handled locally and will keep away from home agent.	Each and every time (local migration also) it needs home agent and foreign agent update.
Local registration and binding updation not necessary.	Local registration and binding updation is necessary.
Reduced latency and less signalling overhead.	High latency and creates more signalling overhead.

Difference between routing cache and paging cache

Routing cache	Paging cache
It generally transfers the routing information between Mobile Node and cellular IP gateway.	It helps to find out idle hosts and updates continuously It refreshes in periodically
Here, entries are timeout after specific amount of period	These entries are maintained for a longer amount of time.

UNIT-3 OVERVIEW

Overview of UTMS Terrestrial Radio access network-UMTS Core network Architecture: 3GPP Architecture, User equipment, CDMA2000 overview- Radio and Network components, Network structure, Radio Network, TD-CDMA, TD – SCDMA.

1. Explain IMT 2000 family:

OR

Explain in detail about Third-Generation (3G) Wireless Systems.

NEED for 3G:

1. 2G networks were built for voice calls only.
2. 2G provides slow data transmission.
3. 2.5G or GPRS (General packet radio service) and 2.75G or EDGE (Enhanced data rate for GSM) technologies resulted in transition to 3G.

Features of 3G/Advantages of 3G:

1. 3G mobiles can operate on 2G and 3G technologies.
2. High security than 2G.
3. Supports video calls and video conferences.
4. We can watch videos online and can download huge files within less time.
5. Weather updating quickly.

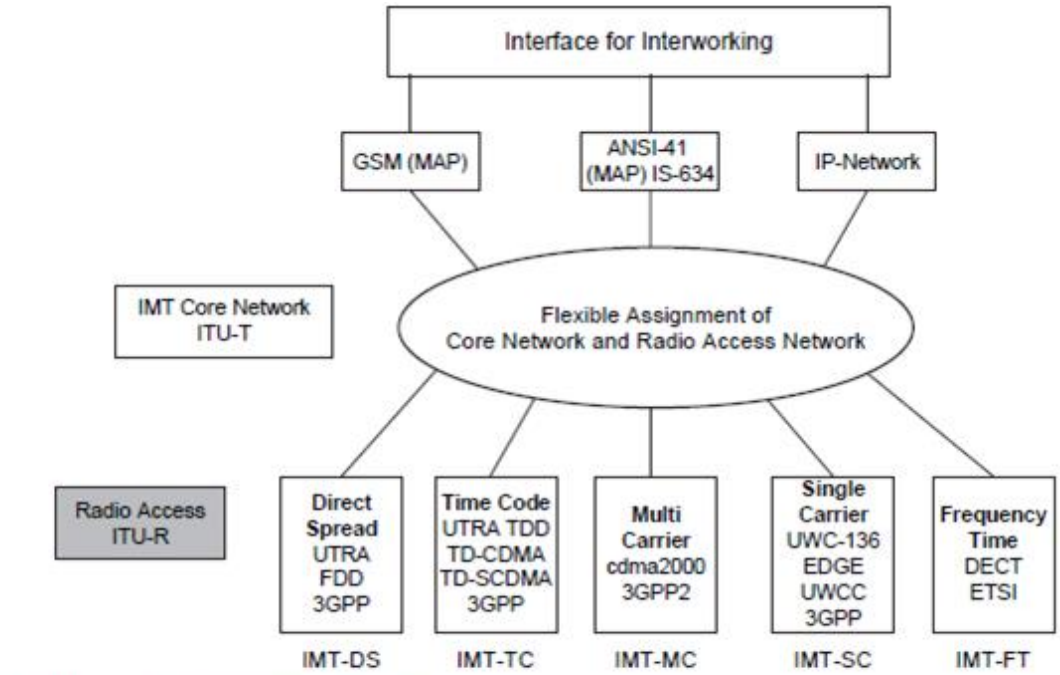
Challenges faced by 3G:

1. To upgrade the base station and infrastructure 3G requires very high costs.
2. To get license for 3G the 3G operator have to invest more amount.
3. High power consumption.

IMT family or IMT 2000:

The application of 3G increased worldwide. The ITU (International Telecommunication union) made a request for radio transmission by that IMT evolved. It was evolved in the year 2000 and the frequencies which are used around 2000 MHz.

- The IMT 2000 has been applied in environments such as indoor use, vehicles and satellites.
- Multiple proposals came from different countries to support IMT 2000.
- The European proposal for IMT 2000 prepared by ETSI is called UMTS.



ITU: International Telecommunication Union
MAP: Mobile Application Part
FDD: Frequency Division Duplex
3GPP: Third-Generation Partnership Project

The ITU standardized 5 groups of 3G radio access technologies:

IMT-DS: Direct spread technology includes wideband CDMA (WCDMA). It is uded for UTRA FDD and used by all European provides and the Japanese docomo for 3G wide area services.

IMT-TC: It involves time division CDMA (TD-CDMA). Later Chinese proposed TD-synchronous CDMA (TD-SCDMA) was added.

IMT-MC: It includes multicarrier technology.

IMT-SC: Is a single carrier technology. It is applied to enhance the 2G.

IMT-FT: Involves frequency time technology which is an enhanced version of cordless telephone system.

---

2. Explain UMTS reference architecture: (Apr-may2018) (Apr-may2017)

- **Universal Mobile Telecommunications System** (**UMTS**) is a **third generation** mobile cellular system for networks based on the GSM standard.
- It was **developed and maintained** by the **3GPP** (3rd Generation Partnership Project).
- UMTS is a component of the International Telecommunications Union IMT-2000 standard set.

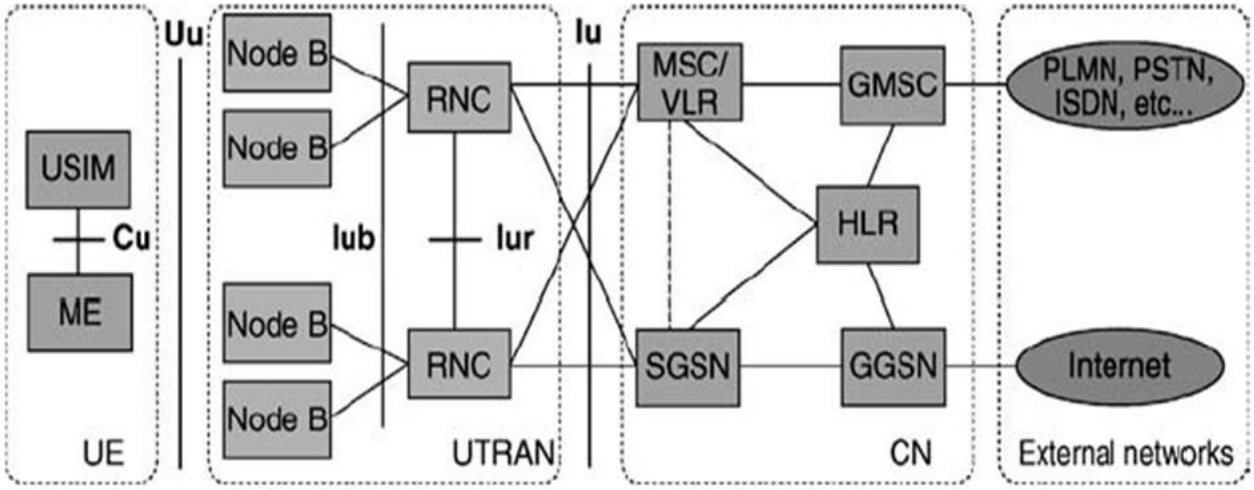
PRINCIPLE: UMTS uses **wideband code division multiple access (W-CDMA**) radio access technology to **offer greater spectral efficiency and bandwidth** to mobile network operators.

The UMTS Network architecture has three main entities (components):

1) User Equipment (UE)

2) UMTS Core Network (CN)

3) UMTS Terrestrial Radio Access Network (UTRAN)



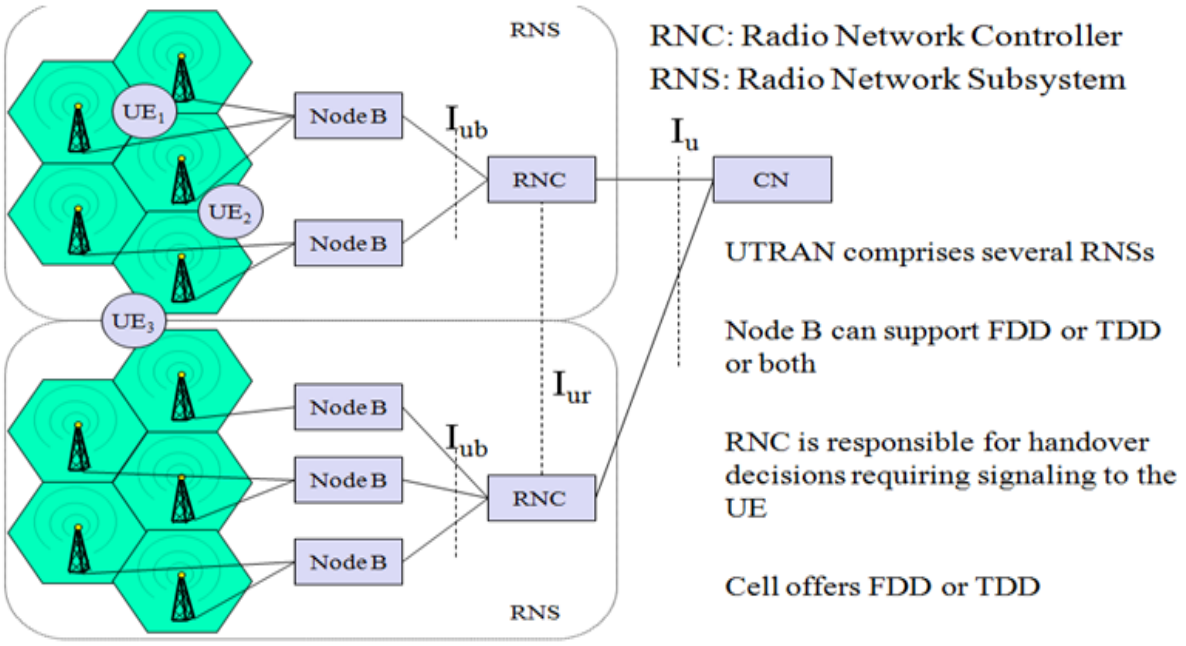
1. User equipment (UE): Is a device used directly by an end-user to communicate. It can be a hand-held telephone, a **laptop computer or any mobile device.** UE consists of two parts: ME and USIM.

(i) **Mobile Equipment (ME**): Is a device where all functions for radio transmission are done.

(ii) **Universal Subscriber Identity Module (USIM):**

- It is a smartcard that holds the subscriber identity.
- It performs encryption and decryption.

2. UTRAN: UMTS terrestrial Radio access Network (UTRAN): It **consists of multiple radio network subsystems (RNS)**. The RNS has two main elements: Node B and a Radio Network Controllers (RNC).



(i) Radio network controller (RNC):

- The RNC is responsible for **control of** the **radio resources** (electromagnetic signals) in its area. One RNC controls multiple nodes B.
- The **RNC** in UMTS provides **functions equivalent to** the **Base Station Controller (BSC)** functions **in GSM/GPRS** networks.
- The major difference is that **RNCs have more intelligence built-in** than their GSM/GPRS counterparts. For example, **RNCs can autonomously manage handovers.**

ii**. Node B:** A node B connects one or more antennas creating one or more cells. It is responsible for air-interface processing and some radio-resource management functions.

- The **Node B** in UMTS networks provides **functions equivalent to the base transceiver station (BTS) in GSM/GPRS** networks.
- The node B also measures connection qualities and signal strengths.
    - Inner loop power control to reduce near far effects.
    - Radio channel coding/decoding
    - Error detection on transport channels and indication to higher layers.
    - Frequency and time synchronization.
    - RF processing.

FUNCTIONS PROVIDED BY UTRAN (RNC + Node B)

1. Admission control: Is needed to **monitor the level of interference**. Here, the RNC calculates the traffic in each cell and decides any additional transmissions leads to increase in interference.

2. Congestion control: During packet oriented **data transmission**, **multiple stations share** the **available radio resources**. The **RNC allocates bandwidth** to each station **in a cyclic fashion**.

3. Radio channel encryption: The **RNC encrypts all data** arriving from the fixed network **before transmission over the wireless link** (and vice versa).

4. Handover: When the **user moves from old foreign agent to new foreign agent** the RNC informs the new cell and takes care of necessary transmission.

5. Radio resource control: RNC measures whether the resources (signal level) available is sufficient or not.

6. Channel coding: The CDMA codes used by a UE are selected by the RNC. These codes may vary during a transmission.

3) Core Network (CN): The major elements of CN are:

a) HLR (Home Location Register)

b) MSC/VLR (Mobile Services Switching Centre/Visitor Location Register)

c) GMSC (Gateway MSC)

d) SGSN (Serving GPRS (General Packet Radio Service Support Node)

e) GGSN (Gateway GPRS Support Node)

(a) HLR (Home Location Register):

It has a database located in user's home system that stores all user relevant information such as user's profile, roaming area information and call forwarding information. As soon as a mobile station leaves its current location area the information in the HLR is updated.

HLR database is similar to a **static database**.

(b) MSC/VLR (Mobile Services Switching Centre/Visitor Location Register)

The **MSC** performs the **switching of calls** between the mobile and other fixed or mobile network users, as well as the management of mobile services such as **registration, authentication, location updating, handovers, and call routing** to a roaming subscriber.

The **VLR** contains the exact location of all mobile subscribers currently present in the service area of the MSC. **VLR database** is a **dynamic database.**

Note:

Difference between HLR and VLR:

HLR: - Store data for the home customers or subscribers. Like if we buy SIM from Delhi residence then our data will store in Delhi HLR and it is *permanen*t store. It's Called **Home Locator Register.**

VLR:- It **store data of visiting location customers or subscribers**. If we have Delhi SIM card and we come to Tamilnadu then tamilnadu VLR will store our data *on temporary* basis for calls. But

still our data remains as Delhi HLR because **HLR data is permanent** and **VLR data is temporary**. It is called **Visitor Locator Register**.

(c) GMSC (Gateway MSC): Is a special kind of MSC that is **used to route calls outside the mobile network**. Whenever a call for a mobile subscriber comes from outside the mobile network or the subscriber wants to make a call to somebody outside the mobile network the call is routed through the GMSC.

(d) SGSN (Serving GPRS (General Packet Radio Service) Support Node): The Serving GPRS Support Node (**SGSN**) is a main component of the GPRS network, which **handles all packet switched data within the network**, e.g. the mobility management and authentication of the users. The **SGSN** performs the same **functions** as the MSC for voice traffic.

(e) GGSN (Gateway GPRS Support Node): The gateway GPRS support node (**GGSN**) is a main component of the GPRS network. The **GGSN** is responsible **for** the **internetworking between** the **GPRS network** and **external packet switched networks (**Internet)

---

3. Explain UMTS core network architecture: (Apr-may2017)

NEED: The 3G UMTS core network architecture is a migration of that used for GSM with further additional elements to provide the additional functionality demanded by UMTS.

In view of the different ways in which data may be carried, the UMTS core network may be split into two different areas:

1. Circuit switched elements: These elements a**re primarily based on the GSM network entities and** carry data **in a circuit switched manner, i.e. a** permanent channel **for the duration of the call.**

2. Packet switched elements: These network entities are **designed to carry packet data**. This enables much higher network usage as the capacity can be shared and data is carried as packets which are routed according to their destination.

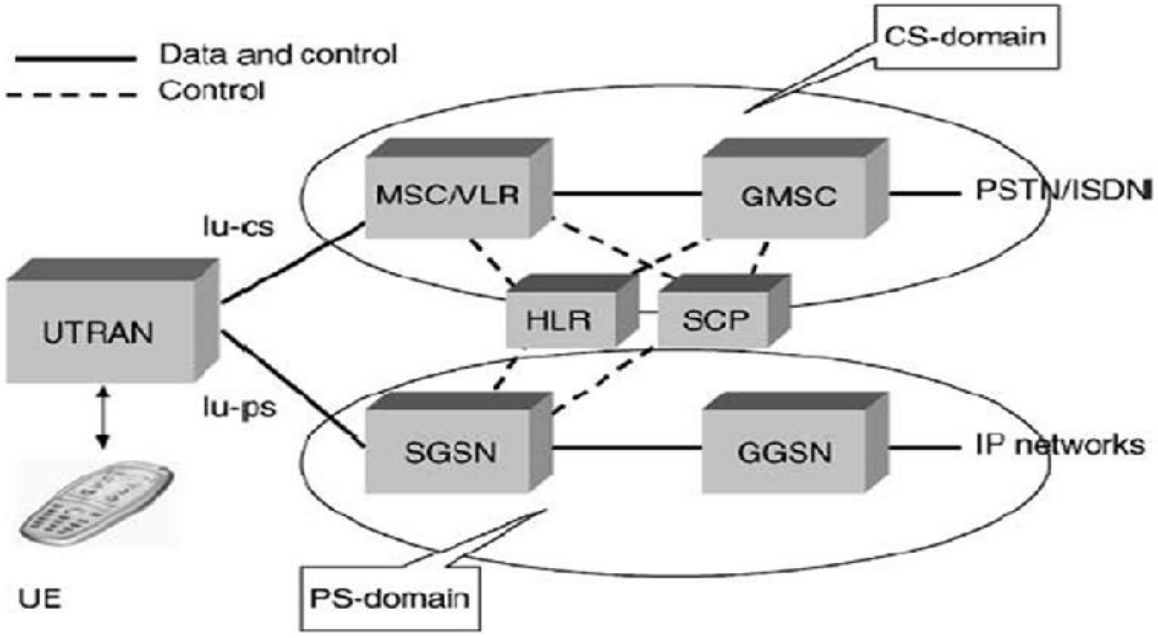
Some network elements, particularly those that are associated with registration are shared by both domains and operate in the same way that they did with GSM.

Circuit Switched Elements: The circuit switched elements of the UMTS core network architecture include the following network entities:

1. Mobile switching centre (MSC): The **MSC** performs the **switching of calls** between the mobile and other fixed or mobile network users, as well as the management of mobile services such as **registration, authentication, location updating, handovers, and call routing** to a roaming subscriber.

2. Gateway MSC (GMSC): **I**s a special kind of MSC that is **used to route calls outside the mobile network**. Whenever a call for a mobile subscriber comes from outside the mobile network or the subscriber wants to make a call to somebody outside the mobile network the call is routed through the GMSC.

.



Packet Switched Elements: The packet switched elements of the 3G UMTS core network architecture include the following network entities:

1. Serving GPRS Support Node (SGSN): **T**he Serving GPRS Support Node (**SGSN**) is a main component of the GPRS network, which **handles all packet switched data within the network**, e.g. the mobility management and authentication of the users. The **SGSN** performs the same **functions** as the MSC for voice traffic.

Mobility management (MM): When a UE enters into a new area the SGSN generates MM information based on the mobile's current location.

Session management: The SGSN manages the data sessions provides the required quality of service and also manage the channel (i.e) the pipes over which the data is sent.

Interaction with other areas of the network: The SGSN is able to manage its elements within the network only by communicating with other areas of the network, e.g. MSC and other circuit switched areas.

Billing: The SGSN is also responsible for billing. It **achieves** this **by monitoring the flow of** user **data across** the **GPRS network**.

2. Gateway GPRS Support Node (GGSN)*:* The gateway GPRS support node (**GGSN**) is a main component of the GPRS network. The **GGSN** is responsible **for** the **internetworking between** the **GPRS network** and **external packet switched networks (**Internet).

SHARED ELEMENT:

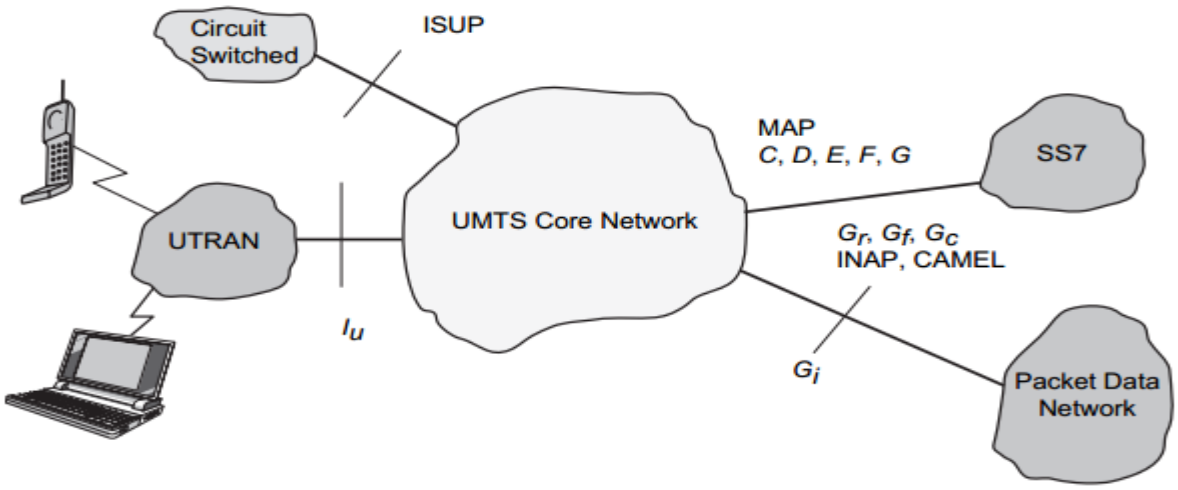
The shared elements of the 3G UMTS core network architecture include the following network entities.

1. Home location register (HLR): It has a database located in user's home system that stores the **master copy of user's service profile, roaming area information and call forwarding information**, as long as the subscription is active for the purpose of routing incoming transactions to UE.

2. Equipment identity register (EIR): The EIR is the entity that decides whether given UE equipment may be allowed onto the network. **Each UE** equipment **has** a number known as the **International Mobile Equipment Identity**. This number, as mentioned above, is installed in the equipment and is checked by the network during registration.

Authentication centre (AuC): The AuC is a protected database that contains the secret key also contained in the user's USIM card

The UMTS core architecture is shown in figure below:



1. 3G-MSC: Is the main core network element to provide **CS circuit switched services**. Its functions are listed below:

1. Mobility Management: Handles authentication, updates to HLR, relocation.

2. Call Management: Handles call set up messages from/to the UE.

3. Supplementary services: Call waiting.

4. Vocoding.

It also takes care of OAM (operation, administration and maintenance) agent function.

2. 3G-SGSN: Is the main core network element to provide **PS Packet switched services**. Its functions are listed below:

1. Session Management: Handles session setup messages from to the UE and takes care of QOS mechanisms.

2. SMS: It allows the user to send and receive SMS data.

3. Mobility Management: Handles authentication, updates to HLT, relocation.

4. Subscriber database functionality: This database is located within the 3G-SGSN and serves as intermediate storage for subscriber data to support subscriber mobility.

5. It also takes care of OAM (operation, administration and maintenance) agent function.

---

4. Explain UMTS terrestrial radio access network overview

OR

Explain UTRAN logical architecture:

UTRAN consist of Radio Network Subsystems (RNSs). The RNS has two main elements: Node B and a Radio Network Controllers (RNC).

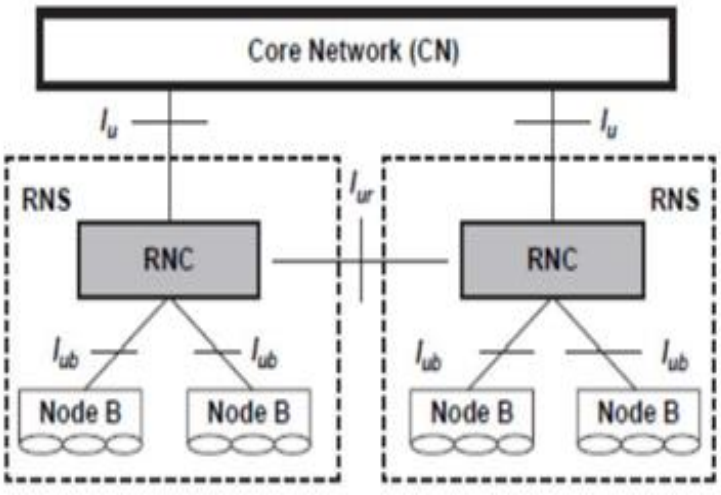
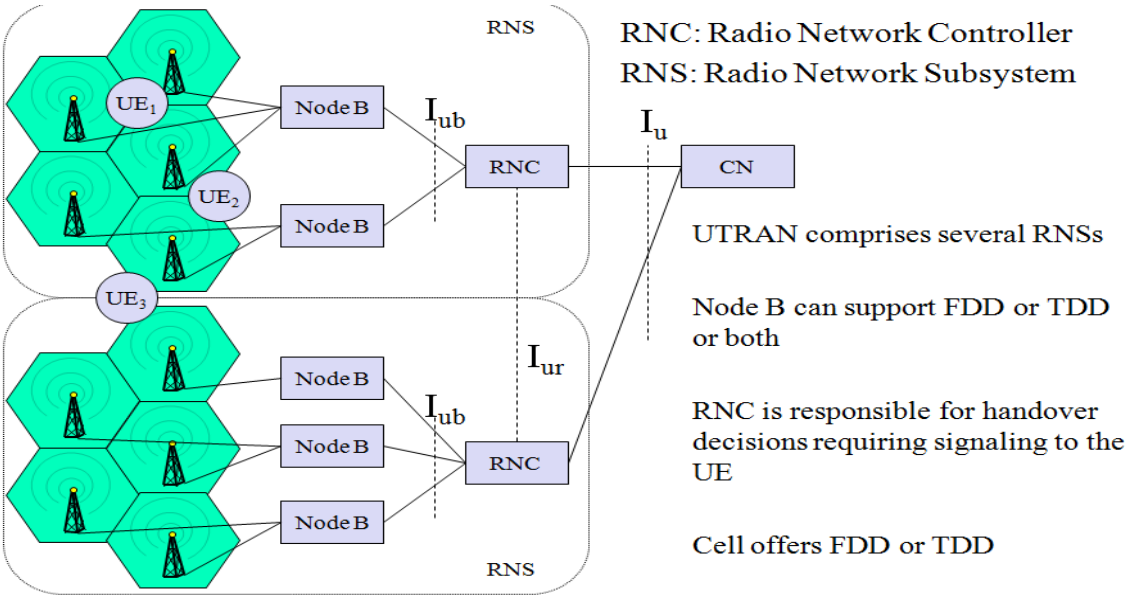


Fig 1 (text book diagram)

RNC-Rado Network Controller



RNS-Radio Network Subsystem

Fig 2 (net diagram for understanding purpose)

Note: Draw both diagrams because Fig 1 (text book diagram) and Fig 2 (net diagram for understanding purpose).

(i) Radio network controller (RNC):

- The RNC is responsible for **control of** the **radio resources** (electromagnetic signals) in its area. One RNC controls multiple nodes B.
- The **RNC** in UMTS provides **functions equivalent to** the **Base Station Controller (BSC)** functions **in GSM/GPRS** networks.
- The major difference is that **RNCs have more intelligence built-in** than their GSM/GPRS counterparts. For example, **RNCs can autonomously manage handovers.**

The other responsibilities are:

1. Intra UTRAN handover
2. Frame synchronization
3. Radio resource management
4. Outer loop power control
5. Frame selection/distribution for soft handover

ii**. Node B:** A node B connects one or more antennas creating one or more cells. It is responsible for air-interface processing and some radio-resource management functions.

- The **Node B** in UMTS networks provides **functions equivalent to the base transceiver station (BTS) in GSM/GPRS** networks.
- The node B also measures connection qualities and signal strengths.
    - Inner loop power control to reduce near far effects.
    - Radio environment survey
    - Radio channel coding/decoding
    - Error detection on transport channels and indication to higher layers.
    - Frequency and time synchronization.
    - Termination of I_{ub} interface from RNC.
    - Termination of U_u interface from UE.
    - RF processing.

FUNCTIONS PROVIDED BY UTRAN (RNC + Node B)

1. Admission control: Is needed to **monitor the level of interference**. Here, the RNC calculates the traffic in each cell and decides any additional transmissions leads to increase in interference.

2. Congestion control: During packet oriented **data transmission**, **multiple stations share** the **available radio resources**. The **RNC allocates bandwidth** to each station **in a cyclic fashion**.

3. Radio channel encryption: The **RNC encrypts all data** arriving from the fixed network **before transmission over the wireless link** (and vice versa).

4. Handover: When the **user moves from old foreign agent to new foreign agent** the RNC informs the new cell and takes care of necessary transmission.

5. Radio resource control: RC measures whether the resources (signal level) available is sufficient or not.

6. Channel coding: The CDMA codes used by a UE are selected by the RNC. These codes may vary during a transmission.

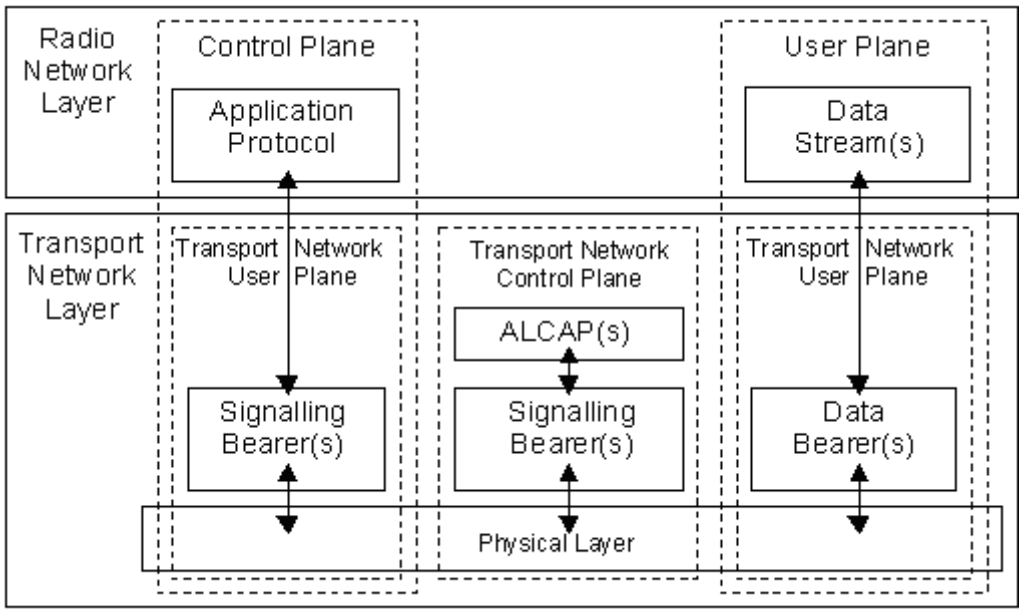
---

5. Explain UTRAN logical interfaces:

OR

Explain the features of UMTS interfaces

- In UTRAN protocol structure is designed so that layers and planes are logically independent of each other and, if required, parts of protocol structure can be changed in the future without affecting other parts.
- The protocol structure contains two main layers, the **radio network layer (RNL)** and the **transport network layer (TNL**). In the RNL, all UTRAN-related functions are visible, whereas the TNL deals with transport technology selected to be used for UTRAN.



1. User plane: From figure: (right side 3rd block)

The user plane **carriers the user information**. It includes data streams and data bearers for data streams.

2. Transport network control plane: **From figure** (Middle block)

The transport plane **lies between user plane and control plane**. The **addition of this transport plane in UTRAN allows** the application protocol in the radio network control plane to be totally **independent of the technology selected for user plane**.

It carries all **control signal** information. It has access link control application part **(ALCAP)** which is used to **carry the signaling information** for **user plane.**

The UMTS interfaces can be categorized as follows:

a. Uu :

- This is the interface between the user equipment and the network . That is, it is the UMTS air interface.

b. Iu: It is an interface between UTRAN and CN. It splits the function into two logical interfaces, **Iups** connecting the **packet switched domain** to the RNC and the **Iucs** connecting the **circuit switched domain** to the RNC. **Reference: Fig 1**

1. Iu –CS :

- This is the **circuit-switched** connection for carrying (typically) **voice** traffic and signalling between the UTRAN and the core voice network.
- The **main signalling protocol** used is Radio Access Network Application Part **(RANAP).**

2. Iu –PS :

- This is the **packet-switched** connection for carrying (typically) **data** traffic and signalling between the UTRAN and the core data GPRS network.
- The main signalling protocol used is RANAP.

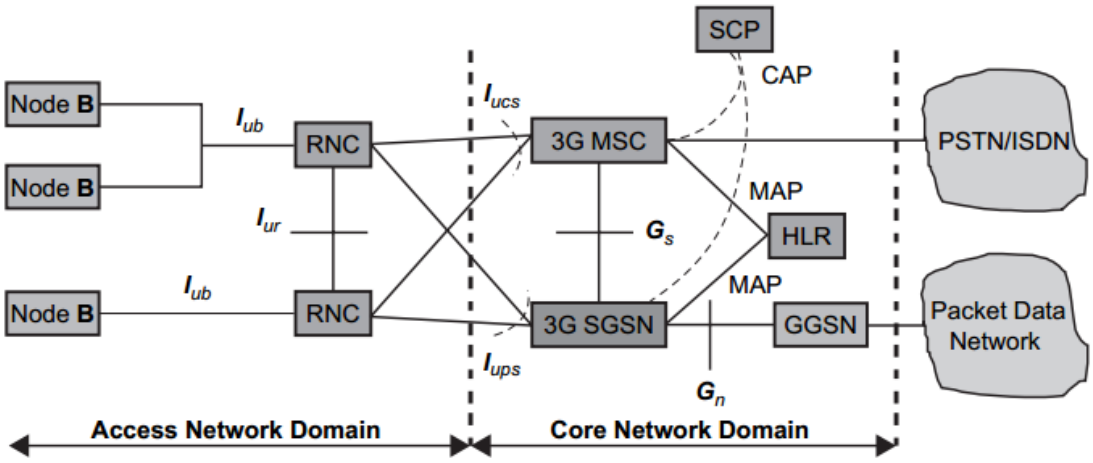


FIGURE 1

c. Iur: It is an interface which allows communication between two different RNC within the UTRAN. The primary purpose of the Iur interface is to support inter-MSC mobility. When a mobile subscriber moves between two different RNC the subscriber current data is now transferred to the new RNC via Iur.

- The **original RNC is known as the serving RNC** and the **new RNC** is known as the **drift RNC.**

It also carries information such as:

- User voice and packet data information on user plane

- Information for the control of radio resources

d. Iub : Reference: Fig 1

- This is the interface used by an RNC to control multiple Node B.
- The main signalling protocol used is Node B Application Part (NBAP).

---

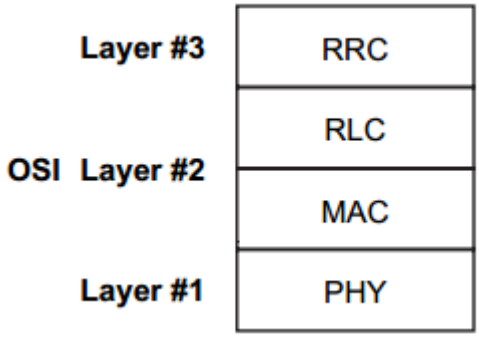
6. Explain about the channel structure in UMTS network.

(Nov-Dec 2018) (Apr-may2018)

The UMTS terrestrial radio access network (UTRAN) has an access layer and non access layer.

The **access layer** includes air interface and provides functions related to **OSI layer1, layer 2 and lower part of layer 3.**

The **non access layer** deals with communication **between user equipment (UE)** and **core network (CN)** and includes **OSI layer 3 (upper part) to layer 7.**



Layer #1 Physical layer

Layer #2 Upper part Radio Link Control (RLC)

Lower Part Medium Access control (MAC)

Layer #3 Radio resource control (RRC)

1. Physical layer functions:

- Modulation, spreading, demodulation, dispreading of physical channels.
- Multiplexing/mapping of services using dedicated physical codes.
- Signal measurements
- Forward error correction and bit-interleaving
- Frequency and time synchronization
- Fast closed loop power control

2. Medium Access control layer functions: It is responsible for efficiently transferring data

for both real time (circuit switching) and non-real time (packet switching) services to the physical layer. It also provides functions such as

- Priority handling in data flow between multiple users
- Selecting an appropriate format for delivering the data to physical layer
- Service multiplexing on random access channel (RACH), forward access channel (FACH) and dedicated channel (DCH)
- Access control on RACH and FACH
- Contention resolution on RACH

3. Radio link control functions: It sets up a logical link over the radio interface and is responsible for fulfilling QoS requirements. Its function also includes:

- Segmentation and reassembly of the data unit.
- Transfer of user data
- Error correction through retransmission
- Sequence integrity (order of the packets received checking)
- Duplication information (retransmitted packet data) detection
- Flow control of data

4. Radio resource control functions: This layer broadcasts system information, handover, and admission control and provides the required QoS.

---

1. Explain CDMA layer structure.

Introduction:

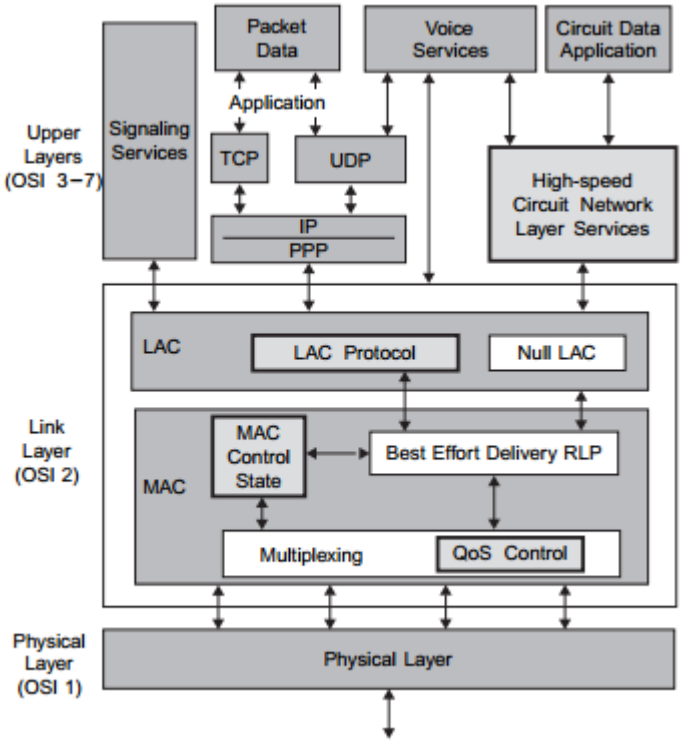
CDMA 2000 is a family of 3G mobile technology which uses CDMA channel to send voice, data and control signal between mobile phones and base station. It is also known as IMT MC (IMT Multi carrier). It was developed by third generation partnership project 2 which consists of five telecommunication standard bodies.

Protocol layers: It consists of three sections.

1. Physical layer
2. Link layer
3. Upper layers

1. PHYSICAL LAYER: It is responsible for transmitting and receiving bits through the physical medium. The bits have to be converted into waveforms by using suitable modulation technique.

It also provides multiplexing such as TDD and FDD.



2. LINK LAYER: It consists of medium access control (MAC) sublayer and link access control (LAC) sublayer.

MAC sublayer: The **service** provided by MAC is referred to as **best effort service.** It defines a **protocol called Radio Link Protocol (RLP)**.

Radio Link Protocol: RLP is an automatic repeat request **(ARQ)** protocol used in wireless environment. In general wireless environment are tuned to accept 1% packet loss is intolerable for certain applications. Keeping this in mind RLP is evolved.

RLP detects packet losses and performs retransmission so that packet los reduced to 0.01% or even 0.0001% which is suitable for TCP.

RLP operating modes: It operated in two modes Transparent mode and Non – transparent mode.

Transparent mode	Non Transparent mode
It does not retransmit missing segments.	It retransmits the data segments that are not transmitted properly.
It uses byte stream synchronization concept to alert the receiver about missing segments.	Byte stream synchronization concept is not needed since the missing segments are retransmitted.
It does not introduce delay and suitable for voice services.	It introduces delay and suitable for e-mail services.

Multiplexing and QOS control: It takes care providing required amount of QOS by appropriately prioritizing the access requests.

Link access control: The service provided by LAC is referred to as reliable service. To provide this service it depends on four sublayers.

1. Authentication sublayer: Authentication is applied when the mobile is first trying to access the network using common signalling channel. Once the mobile has made access it then uses the channel allocated and authentication is no longer required.

2. ARQ sublayer: It involves retransmission and positive or negative acknowledgment for missing segments.

3. Utility sublayer: It assembles (collects) the entire radio layer required functions and also provides padding if necessary.

4. Segmentation and Reassembly sublayer: On the transmitter side it performs required amount of segmentation through encapsulation technique and at the receiver side it performs the reverse operation.

3. UPPER LAYERS: It provides functions such as Voice services, Signaling and end user data bearing services.

---

2. Explain 3GPP architecture:

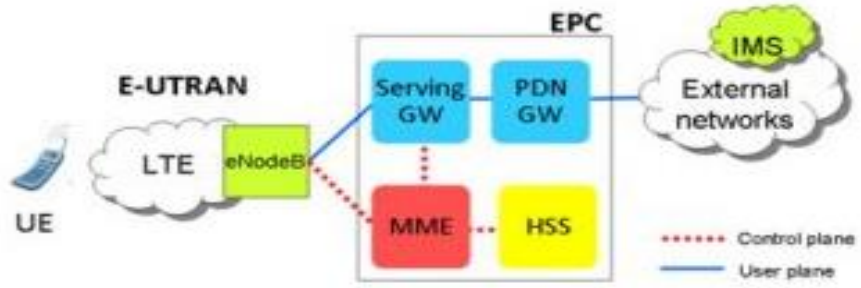
Objective: In GSM (2G) the architecture lies on circuit switching which helped for voice transmission. In GPRS (2.5G) packet switching involved which was suitable for data transmission.

In UMTS (3G) decided to use **IP internet protocol** as a a key for both voice and data services. This evolution is referred to as Evolved core network (EPC).

Circuit only	Circuit/packet	Packet only
Voice, SMS **GSM**	Voice, SMS **GPRS,UMTS**	Data, Voice, SMS **EPC**

Features:

It involves individual plane for user data and control signal transmission.



Components: It involves user equipment (UE), E-UTRAN, evolved packet core network and external network.

1. User equipment (UE): Is a device used directly by an end-user to communicate. It can be a hand-held telephone, a **laptop computer or any mobile device.** UE consists of two parts: ME and USIM.

(i) **Mobile Equipment (ME**): Is a device where all functions for radio transmission are done.

(ii) **Universal Subscriber Identity Module (USIM):**

- It is a smartcard that holds the subscriber identity.
- It performs encryption and decryption.

2. E-UTRAN: The E-UTRAN handles the radio communications between the mobile and the evolved packet core and it has one component, the evolved base stations, called **eNodeB** or **eNB**. Each eNB is a base station that controls the mobiles in one or more cells. The base station that is communicating with a mobile is known as its serving eNB.

LTE Mobile communicates with just one base station and one cell at a time.

The two main functions supported by eNB:

- The eNB sends and receives radio transmissions to all the mobiles using the analogue and digital signal processing functions of the LTE air interface.
- The eNB controls the low-level operation of all its mobiles, by sending them signalling messages such as handover commands.

3. The Evolved Packet Core (EPC) (The core network):

- The Home Subscriber Server **(HSS)** component is a **central database** that contains **information about** all the **network operator's subscribers**.
- The mobility management entity **(MME) controls the high-level operation of the mobile by** means of **signalling messages** and Home Subscriber Server (HSS).

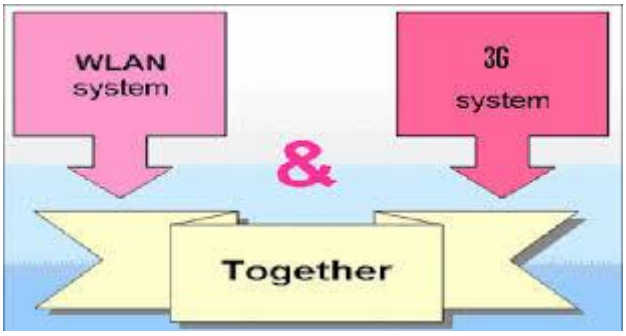
- The Packet Data Network (PDN) Gateway (P-GW) communicates with the outside world ie. packet data networks PDN, using SGi interface. Each packet data network is identified by an access point name (APN).
- The **serving gateway (S-GW) acts as a router**, and **forwards data between** the **base station and** the **PDN gateway.**

UNIT-4

INTERNETWORKING BETWEEN WLANS AND WWANS

Internetworking objectives and requirements, Schemes to connect WLANS and 3G Networks, Session Mobility, Internetworking Architecture for WLAN and GPRS, System Description, Local Multipoint Distribution Service, Multichannel Multipoint Distribution System.

What are the Requirements of interworking (connecting) WLAN and WWAN?



1. Common billing and customer care: Interconnecting the WLAN and WWAN provide a common bill and customer care for the subscribers which the subscriber feels more comfort.

2.3GPP access control and charging: **A**uthentication, **A**uthorization and **A**ccounting **(AAA)** for subscribers in the WLAN and same AAA procedures on WWAN provides more security.

3. **Service continuity**-To provide **Seamless** (Un interrupted) **service** when the mobile switch from WLAN to WWAN also.

4. Access to 3GPP circuit switched services: To allow the 3GPP (WWAN) operator to utilitize its **voice call** (circuit switched) **services** in WLAN environment.

5. Access to 3GPP packet switched services: To allow the 3GPP (WWAN) operator to utilitize its **data** (packet) **services** in WLAN environment.

Explain the various interworking schemes to connect WLAN and WWAN (3G Networks) (13 marks)

OR

Discuss briefly the various ways to achieve interworking between a WWAN and a WLAN.

OR

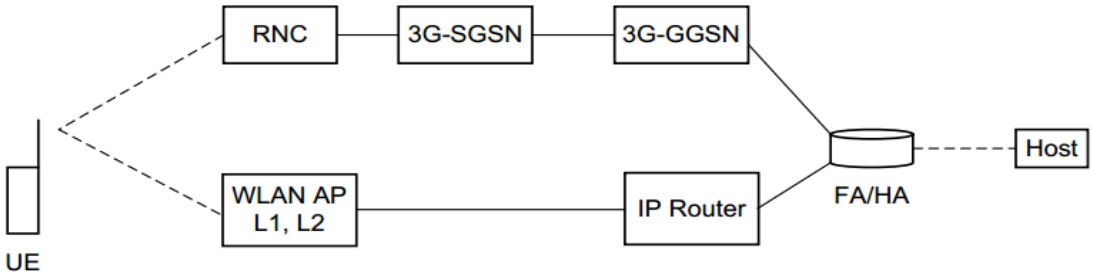
Explain the various approaches involved to achieve interworking between GPRS and a WLAN.

Need: Since we have multiple advantages such as **Common billing, uninterrupted service** and **AAA facility for subscribers** we go for interworking WLAN and WWAN. It can be achieved by three methods as mentioned below.

1. Mobile IP approach **(**Loose coupling)
2. Gateway approach
3. Emulator approach (Tight coupling)

1. MOBILE IP APPROACH (LOOSE COUPLING)

- Mobile IP is a protocol **developed to allow internetwork (connection) mobility (movement)** for **wireless nodes without** the need of **change in IP addresses.**
- The entire structure is divided in two halves. WLAN network and WWAN network. The **top section** which includes Radio Network Controller (RNC), 3G-Serving GPRS support node (SGSN) and 3G-Gateway GPRS support node **forms the WWAN** and the **lower section** Access point and router **forms the WLAN** network.
- The Foreign Agent and Home Agent are connected common to both the network.



- This approach can be implemented in the mobile nodes and this approach provides mobility during roaming between WLAN and 3G.

Limitations-Mobile IP approach

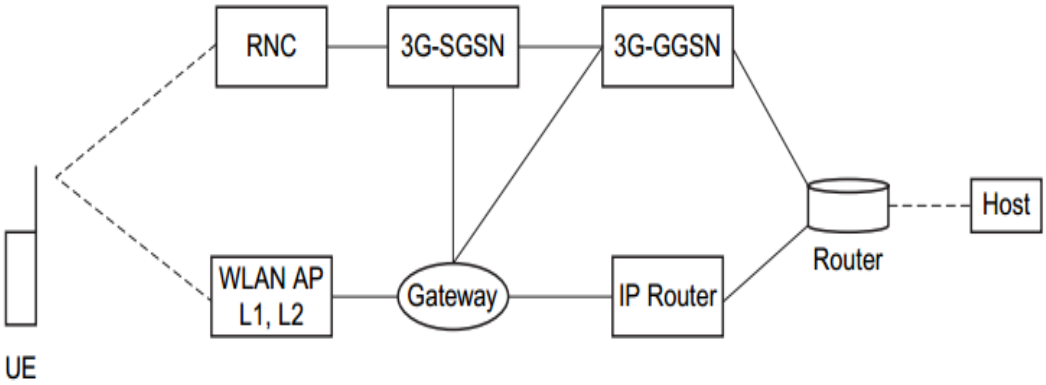
- 1. During **handoff** it requires registration hence there is a chance for **delay** and packet loss.
- 2. It may suffer due to **triangular routing.**

Mobile IP approach: Is also called **Loose coupling** approach. Coupling means **connection**.

Elements (nodes) or devices in the network are connected in such a way that **if any problem occurs in the network** also it **will not affect the whole network** or even if any devices want to be connected **addition or removal can be done easily**.

2. GATEWAY APPROACH: In this method new logical node called **Gateway** is connected **between two wireless networks** (WWAN and WLAN). The gateway acts as an internal device.

The new node exchanges necessary information between the two networks, converts signals and forwards the packets for roaming users.



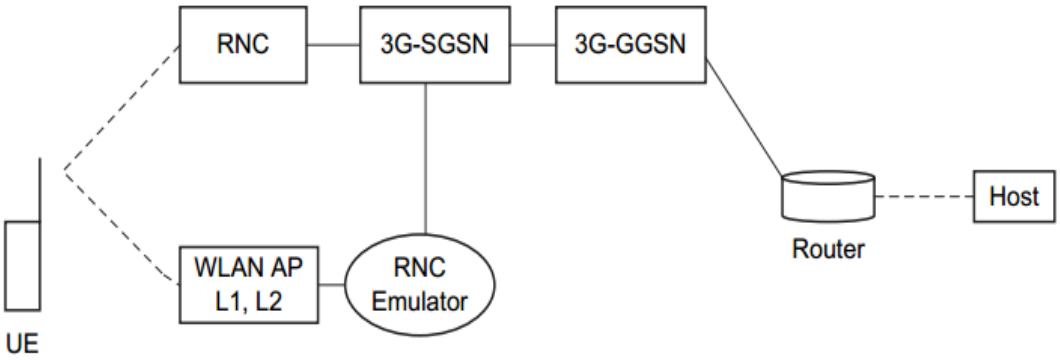
- A node (gateway) is connected between two networks.
- Gateway it acts as an interface between two networks.
- The gateway method makes **two networks to operate independently.**
- When a computer-server acts as a gateway, it also **operates as a firewall.**

Advantage-Gateway

- 1. Two networks operate independently.
- 2. During **handoff** delay will be reduced.
- 3. HA/FA is not necessary.
- 4. Packets while roaming directly travel through the gateway without processing by mobile IP so **triangular routing problem is also minimized.**

EMULATOR APPROACH (TIGHT COUPLING)

- The term "emulation" comes from the verb "emulate," which means to **imitate or reproduce**.
- This can be done using hardware, software, or a combination of the two.
- However, since hardware is expensive to reproduce, most emulation is done via software.
- In this method the **RNC emulator acts as a controller**.



- All packet routing and forwarding are processed by a core network. The WLAN terminal is a laptop or personal digital assistant.

Advantage:

- **Packet loss and delay can be avoided in this method.**
- Mobile IP is not required.

Emulator approach-Tight coupling

- Tight coupling is a coupling technique in which **hardware and software components are highly dependent on each other.**
- **Tight coupling** is also known as high coupling and strong coupling.

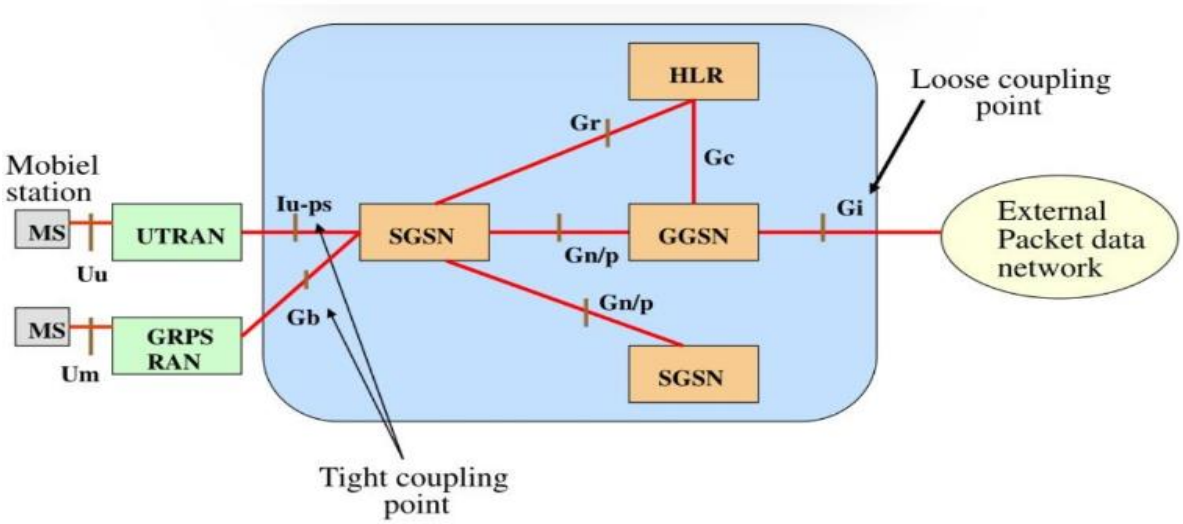
Limitation – Emulator approach

- **Flexibility** is very much **lacking** since two networks are tightly coupled.
- Gateway GPRS support node – GGSN is a **single point of contact to the internet**.
- All packets from the router have to enter the GGSN first and then only it can enter the other network so it experiences a **bottle neck**.

Comparison of Loose coupling and Tight coupling approach.

S.No	Loose coupling	Tight coupling
1	Here, the WLAN is connected to the external network directly.	The WLAN is initially connected to the GPRS (core network) which in turn connects to the external network.
2	It experiences **Less bottle neck** (congestion).	It experiences **High bottle neck** (congestion).
3	**Highly flexible** network	Flexibility is a lacking factor. (**Highly**

		rigid)
4	**Mobile IP** is used for hand over.	**RNC Emulator** is used here.
5	**HA/FA is involved** since mobile IP is involved.	HA/FA is **not involved**
6	It has **high delay**. Experiences **triangular routing problem**.	It has **less delay**.
7	If **any problem occurs in the network** it **will not affect the whole network** since it is a highly flexible network.	If any problem occurs in the network it will **affect the whole network** since it is highly inflexible.
8	**Coupling** is provided at **Gi** reference point.	Coupling is provided at **Gb** reference point.



Explain DEFACTO (Standard) WLAN SYSTEM:

De-facto: Is a **standard** that is **created** or based on facts **not formally recognized by any official body** or a de-facto standard is a one that has **become a standard since it is widely used** whereas **it was not officially approved by any govt or private sectors.**

Advantages:

1 High security and reliability

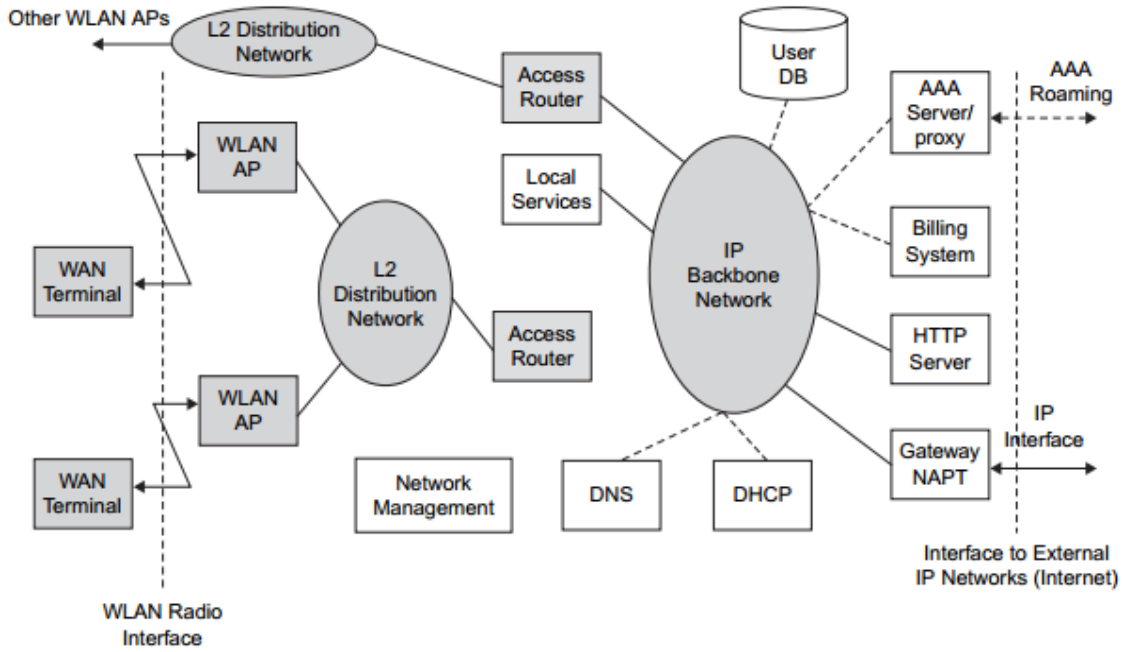
2. Good quality of service

3. Provides seamless (uninterrupted) service

4. Compatible to integrate WLAN and WWAN.

Standard Components involved in WLAN system architecture:

1. DHCP: Dynamic host configuration protocol. If a new computer is connected to a network, DHCP can **provide** it with **all** the **necessary information** for full system integration into the network, e.g., addresses of a DNS server and the default router, the subnet mask, the **domain name, and an IP address.**



2. DNS: Domain Name Server. It **translates** the **domain name into IP address** which computers can understand. Generally, humans can able to remember only domain name but system could not recognize domain name. Hence, the DNS translate (convert) those domain name to corresponding IP address.

3. Gateway/NAPT: Network address and port translation. Is a device which **acts as a firewall** between networks that are connected together. It provides a public address to a computer or group of companies inside a private network.

4. HTTP server: In general all requests from the user (client) transfers to the server using HTTP protocol only. Its primary function is to establish a connection with the server and send HTML pages back to the user browser.

5 AAA SERVER: Is a server that provides Authentication, Authorization and Accounting (AAA) services to the user. It can use a protocol called **"RADIUS".**

RADIUS: Remote Authentication Dial In User Service. Is a client/server protocol that enables remote access servers to communicate with a central server.

6. Network Management: Is the process of setting up and keeping track of connections in a network. It provides information about programs versions and updates installed in network computers. Network management helps the network to improve performance and solve any issues that arise.

7. WLAN terminal: Is typically a Laptop or a desktop computer.

8. WLAN AP: Is a central device that controls the station connected through the access point. The access points are similar to the base station which takes care when a mobile node moves from one foreign agent to other foreign agent.

9. User database: Is a system that holds the user information (user ID, password). The user database is accessed from the AAA server by using Light Weight Directory Access Protocol (LDAP).

10. Access Router: Is to connect multiple networks and forwards packets destined either for its own network or other networks.

Procedure involved in accessing browser:

Step1: User initiates web browser its first request into WLAN system.

Step2: Based on the request web page is displayed.

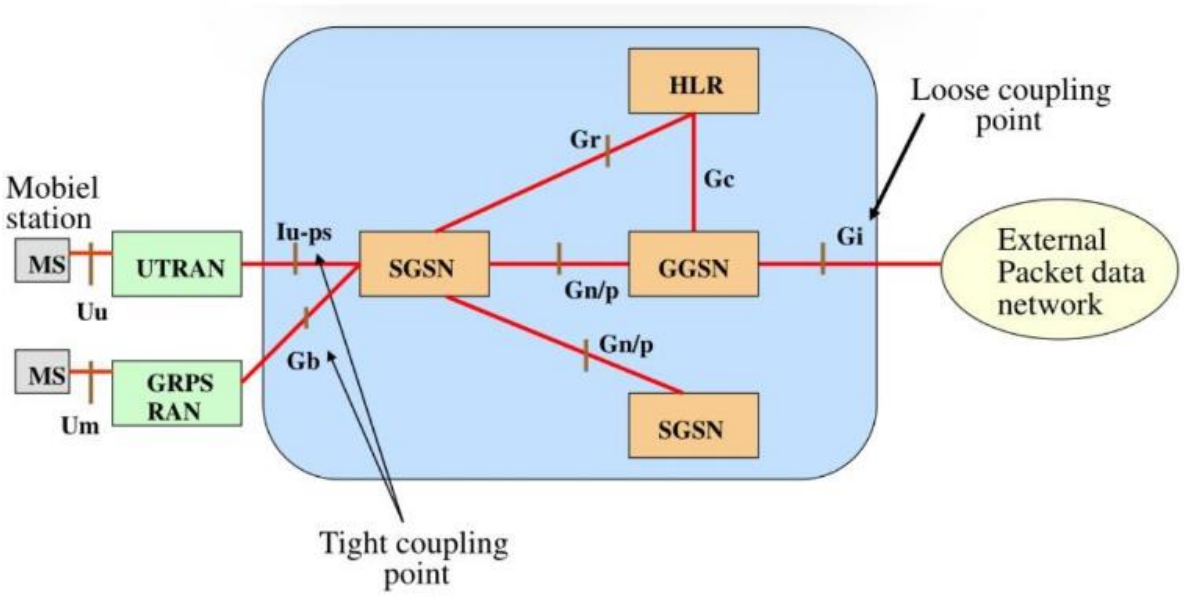
Step3: User is prompted to enter the login name and password.

Step4: The password can be static or even generated as OTP.

What are the internetworking architectures for WLAN and WWAN (GPRS)?

The two approaches widely used are:

1. Tight coupling approach (Emulator approach)
2. Loose coupling approach (Mobile IP approach)



HLR: Home location Register

SGSN: Serving GPRS support node

GGSN: Gateway GPRS support node

1.Tight coupling approach (Emulator approach): In this approach the **WLAN is initially connected to the core network and then to the external network.** Hence, all the traffic first goes through the core network. In tight coupling **WLAN** is **connected via G_b or Iu-ps reference points.**

2. Loose coupling approach (Mobile IP approach): In this approach **WLAN** is **connected** to the **external network directly**. It bypasses the GPRS network (core network).

The approach only utilizes the subscriber databases of the GPRS network but will not have any interface. The **interface junction** is indicated by **G_i** reference point.

Note: The trend is to follow the loose coupling approach and to use SIM or USIM based authentication and billing.

Advantages of tight coupling approach:

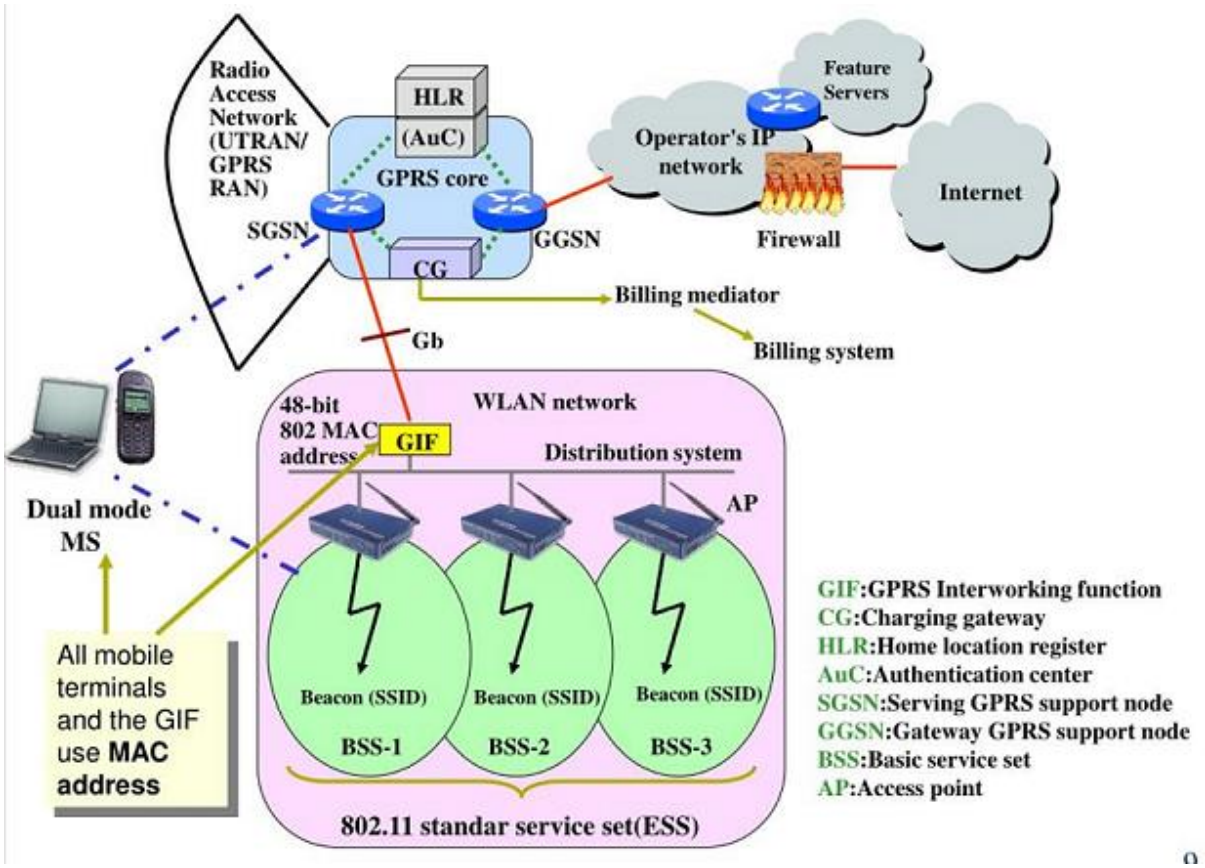
1. Seamless service continuation between WLAN and WWAN.
2. Increased security.
3. Common provision for billing and customer care.
4. SMS, location based service and MMS multimedia message services are handled easily in tight coupling approach.
5. Reuse of GPRS Infrastructure.
6. Reuse of GPRS AAA

Discuss tight coupling architecture between IEEE 802.11 WLAN and GPRS (3G) or WWAN. (13 marks)

Tight coupling approach: In this approach the **WLAN is initially connected to the core network and then to the external network.** Hence, all the traffic first goes through the core network. In tight coupling **WLAN** is **connected via G_b or Iu-ps reference points.**

The architecture consists of GPRS core (WWAN) network and WLAN network.

WLAN network: The WLAN consists of more number of access points (AP) which are connected to the individual basic service set (BSS). All the BSS are connected by a distribution system (DS) though AP. The DS can be a wired 802.3 Ethernet cable also.



- **BSS:** An **infrastructure formed with access point** is **referred to as basic service set**. **More number of BSS** which are **connected together** are **referred to as Extended Service Set (ESS).**

The AP behaves like a Base Station (BS) and all mobiles exchanges data through AP's only. The WLAN network looks like or it acts as an alternative Radio Access Network (RAN) and it connects to the core network (WWAN) through the standard G_b interface.

- The core network could not identify the WLAN as a separate network. It looks like another GPRS network only.
- It is achieved with the help of **GIF**. GPRS interworking function. It is the key element.
- GIF is connected between distribution system and to an SGSN via standard G_b interface.
- The **main function of GIF** is to **provide interface between WLAN and GPRS** and to **virtually hide the WLAN** and **to make WLAN as another GPRS** or routing area information or routing area update (RAU) system.

Scenario: Let us consider a mobile station was moved away from the WLAN area. Now, to connect to the WWAN the following steps are followed.

Step1: The WLAN enters into a passive scan mode (i.e) it scans a frequency band and searches for beacon (alert) signal.

Step 2: When a beacon signal is received the Service Set Identifier (SSID) is verified and compared against with already existing (pre-configured) SSID. The SSID serves as a WLAN identifier and can help mobile to attach to the correct WLAN.

Note: A user could use a unique SSID and request its stations to configure their mobiles to consider only that particular SSID alone.

Step 3: When an MS detects a valid SSID, it performs corresponding authentication and association procedure.

Step 4: The MS then enables its WLAN interface and further signalling is carried over its interface.

Dual mode MS: As shown in figure the mobile station operates in dual mode.

1. **When the MS enters into a WLAN area** a Routing area update (RAU) procedure take place and subsequent GPRS signalling and **data transmission carried over the WLAN interface**.
2. **When the MS moves away from WLAN** area another Routing area update (RAU) procedure take place and **GPRS interface is enabled.**

WLAN adaptation function (WAF): It is a layer connected to the GIF. Its primary function is it maps the GPRS and WLAN. As shown in figure of tight coupling architecture the MS can able to operate in two radio subsystems one for GPRS access and another for WLAN access.

Step1: The **WLAN adaption function identifies when the WLAN** radio **subsystem is to be enabled.** (i.e) when the MS associates with valid AP informs the LLC layer which subsequently redirects signalling and data traffic to the WLAN.

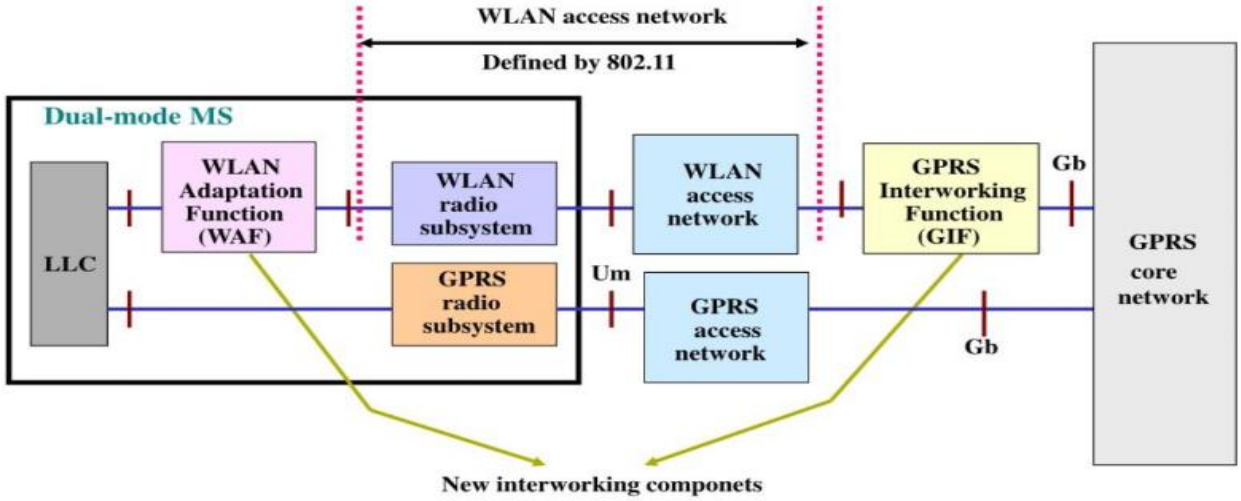
Step 2: WAF **supports the GIF/RAI discovery procedure** which is initiated by MS in order to discover the MAC address of GIF and routing area identity (RAI) of the WLAN.

Step 3: It supports the paging procedure on G_b interface when SGSN needs to page an MS. During this procedure, WAF sends an appropriate signalling message to MS in order to alert and respond to page.

Step 4: It **translates packet data unit (PDU)** between mobile and GIF.

Step 5: It **provides good QOS** by proper scheduling in GIF and MS.

Step 6: It transfers the **temporary logical link identifier (TLLI)** and QOS information in the WAF header. **TLLI is a temporary MS identifier used by the LLC layer for addressing purposes**.



What are the functions of WLAN adaptation function (WAF) in tight coupling architecture? Discuss briefly. (8 marks)

Note: Write answer mentioned above from WLAN adaptation function when asked separately.

Explain about GIF/RAI/RAU discovery procedure in tight coupling architecture. (13 or 8 marks)

GIF: GPRS interworking function. It is a key element which connects the distributed system (DS) in WLAN to the SGSN in core network (GPRS) or WWAN. Its main **function is to provide interface between WLAN and WWAN. (Ref. Fig in tight coupling architecture)**

GIF - Is a **component,** which interfaces WLAN and WWAN.	**RAI -** Is a procedure or process carried over by GIF

RAI: Routing area identity procedure. This procedure will takes place **when the MS** is **moved away from the WLAN region**. In such cases the GIF takes care of providing servicing by connecting with the SGSN directly.

People in GPRS will be assuming that they are connected to another GPRS network. **GIF virtually hides the WLAN absence.**

Steps involved in GIF/RAI discovery procedure;

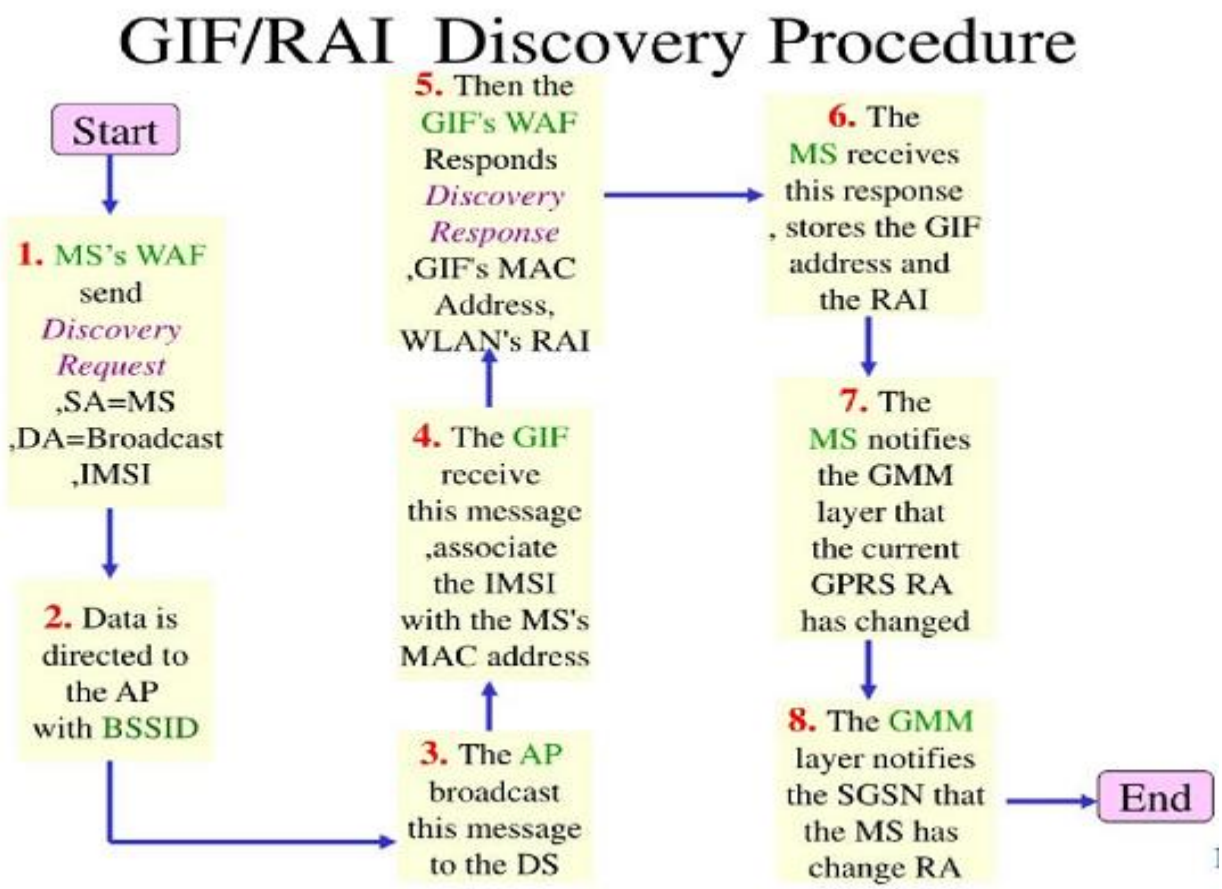
Step 1: To transfer the data from WLAN to WWAN through GIF we **need the MAC address of GIF**.

Step 2: The MAC address of GIF can be discovered by sending a request from mobile station of the corresponding WLAN through its access point by keeping mobile station (MS) source address as fixed and destination address as broadcast. This step is referred to as **GIF/RAI discovery request.**

Step 3: To achieve this process the data is transferred to the corresponding BSS AP.

Step4: The AP broadcast this message to the distribution system.

Step 5: The distribution system transfers this message to the GIF.



Note: To understand step 1 to step 5 (Ref. Fig in tight coupling architecture)

Step 6: The GIF's wireless adaptation function responds the corresponding MAC address. It is referred to as **GIF/RAI discovery response.**

Step 7: The mobile station receives this response stores the GIF MAC address and routing area identification (RAI) message.

Step 8: The **GPRS mobility management (GMM) layer notifies the GIF MAC address** and it uses the data to transfer directly from the mobile station.

How is authentication achieved in loose coupling architecture? Discuss briefly. (13 marks/ 8 marks)

Authentication: Generally, authentication is the process of verifying the identity of a user or a device.

Need: In loose coupling architecture it is essential since the WLAN is connected directly to the external network. The authentication is provided by using three protocols.

1. Extensive Authentication protocol (EAP)

2. RADIUS protocol

3. DIAMETER protocol

1. Extensive Authentication protocol (EAP): Generally authentication will be initiated by the client but the **special feature of EAP is here authentication is initiated by the server**. The steps involved in EAP authenticator is as follows.

Step 1: The authenticator (the server) sends a Request to authenticate the peer (the client).

Step 2: The client sends a Response packet in reply to a valid Request.

Step 3: The authenticator (server) sends an additional Request packet, and the client replies with a Response. The sequence of Requests and Responses continues as long as needed.

The authentication conversation can continue until the authenticator determines that successful authentication has occurred, in which case the authenticator must transmit an EAP Success.

2. RADIUS protocol: RADIUS stands for Remote Authentication Dial In User Service.

Is a protocol carrying authentication, authorization, and Administration (AAA) service. In general in larger network during roaming scenario, one or more proxy server will be involved. In such cases the RADIUS server protocol is commonly used.

It runs over UDP. Therefore, it is not that much reliable.

3. DIAMETER protocol:

1. It is an enhanced radius protocol
2. It uses TCP/SCTP (i.e. Stream Control Transmission Protocol).
3. It is a **reliable protocol.** All the messages will be acknowledged by the AAA server.
4. It is **suitable for 4G** network.
5. It is **suitable for IMS** network.

Difference between RADIUS and DIAMETER PROTOCOL

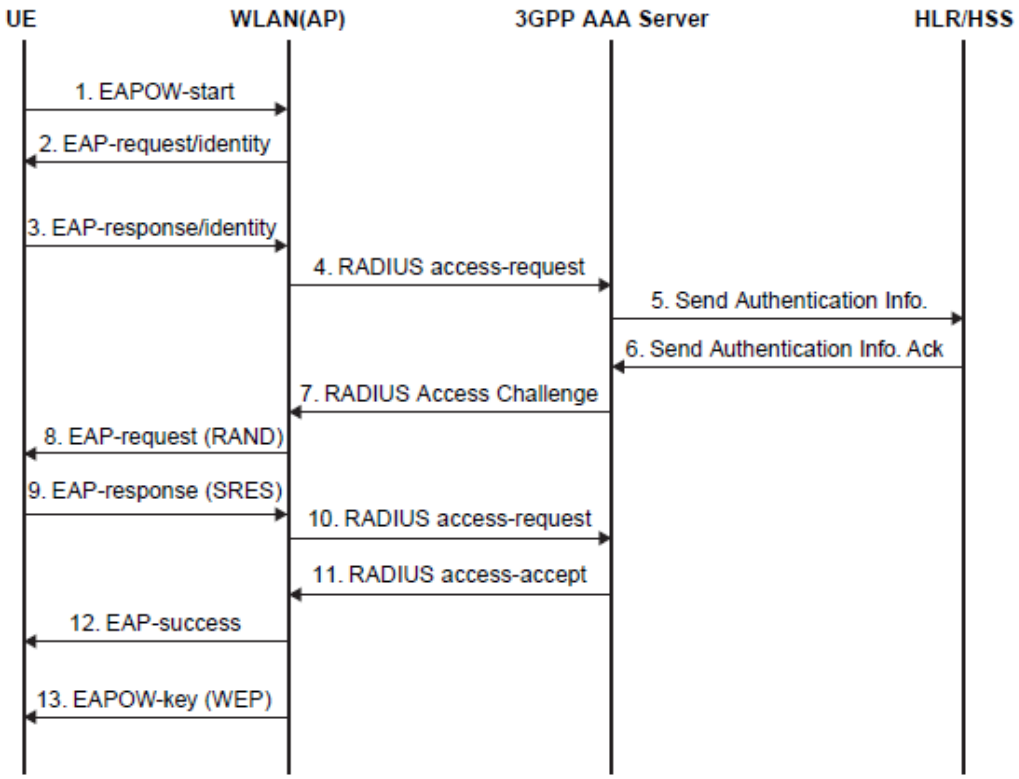
RADIUS Protocol	**DIAMETER Protocol**
Remote Authentication Dial In User Service	It is an enhanced radius protocol
It uses UDP.	It uses TCP/SCTP (i.e. Stream Control Transmission Protocol).
It is an unreliable protocol. It lacks in reliability, ordering and data integrity.	It is reliable protocol. All the messages will be acknowledged by the AAA server.
Not advisable for 4G network.	Suitable for 4G network.

Not suitable for IMS network	Suitable for IMS network

Process of Authentication:

Step 1: It starts once the user equipment (UE) is associated with an corresponding access point (AP). It is achieved with the help of **sending an EAP over WLAN (EAP-OW) start message from UE to the AP**.

Step 2: The access point responds the initiation by sending a request message to UE in order to know the identity to verify corresponding user or not.



Step 3: A UE provides the identification as response and it is validated by the AP.

Step 4: Since, the UE is validated (identified/authenticated) with some of the identification elements such as IMSI value stored in the SIM card the AP sends an RADIUS access request message to AAA server.

Step 5: The AAA server from the knowledge or information obtained from step 4 it generates additional authentication information and sends to the HLR register.

Step 6: In HLR already the database of UE is stored (user profile, basic information) it is validated then HLR provides an ACK to the AAA server.

Step 7: A RADIUS access challenge message is sent by AAA server to AP.

Step 8: The request is carried as EAP request to the UE. In both steps a random challenge (RAND) is sent as a request and an expected response (SRES) is obtained as authentication vector message.

Step 9: The SRES is transferred to AP.

Step 10: The SRES is transferred from AP to AAA server. In step 10 once the request is carried to AAA server the expected response (SRES) is compared against the corresponding (XRES) value received from HSS.

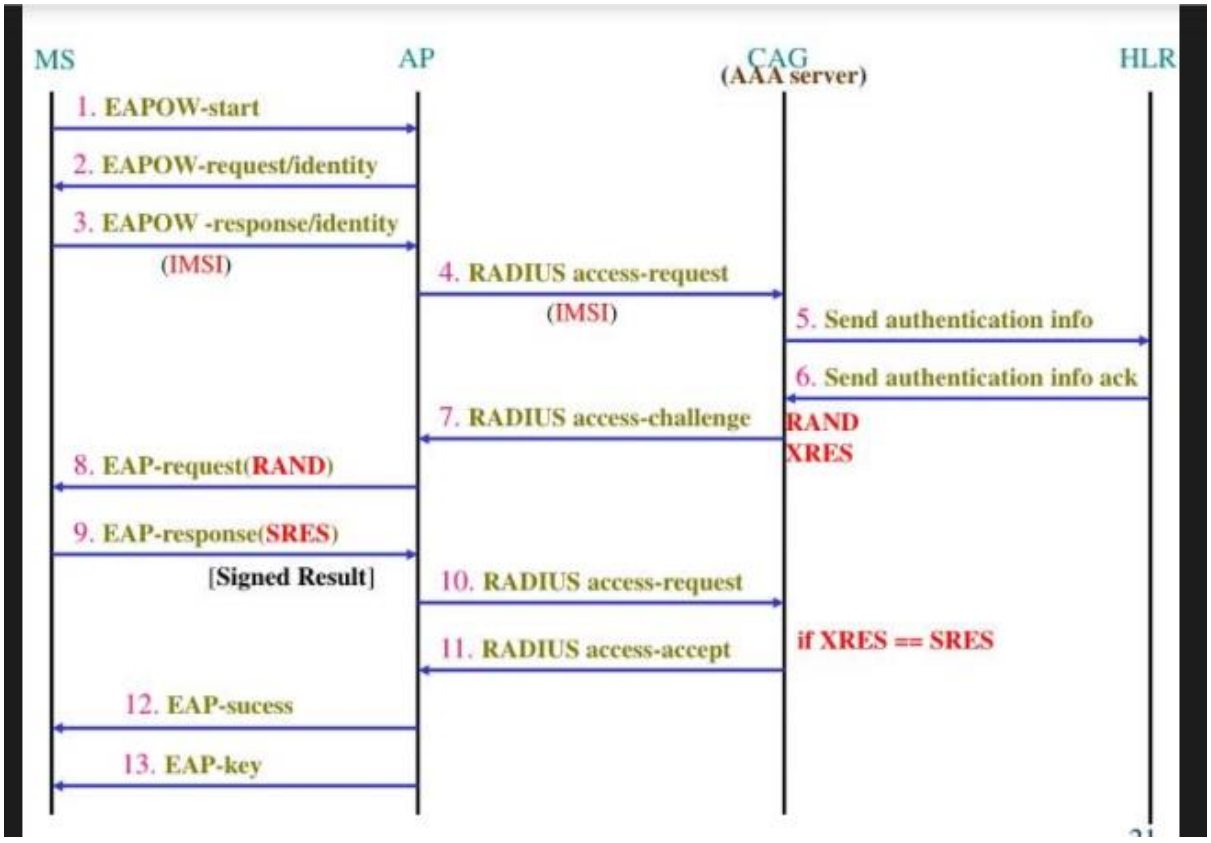
If these values match (i.e) **SRES = XRES** a **RADIUS access accept** is generated if not (i.e) **SRES ≠ XRES** match **RADIUS access reject** is generated.

Step 11: The RADIUS access accept generated is carried to WLAN (AP).

Step 12: Once the step 11 is successfully executed the WLAN AP sends an EAP success message to the UE.

Step 13: AN EAP-OW key message is generated and transferred from AP to the UE.

Through this process authentication is achieved successfully between UE and AAA server.



COMPARISON BETWEEN SIM AND USIM 2marks)

SIM	USIM
Subscriber identity module	Universal subscriber identity module
It supports only 2G	It supports 3G and 4G
Less security	High security
Limited storage capacity	High storage capacity
It provides global phone book	It provides global phone book and hidden phone book.

Explain LOCAL MULTIPOINT DISTRIBUTION SERVICE (LMDS):

Introduction

- It is a **stationary (fixed)** broadband **wireless** access technology **designed for** mass subscriber **(television)** market place. The meaning of fixed means **"stations" are immobile** (i.e) stations will not move anywhere.
- For these fixed stations wireless service is provided with help of antenna. **Ex:** Station-Television.
- It **operates @2.4 GHz** and above.

Objective: It was **designed for** wireless digital **television transmission**.

Features:

- It provides reliable two way (bidirectional) data and internet services.
- It is **cheaper than fiber or copper.**

The term **"Local"** in LMDS indicates that the signal in this technique propagates only for **short distance** (i.e) the transmitter can **cover only upto 5 miles.**

"Multipoint" in LMDS indicates that the signals can be transferred as point to point or even point to multipoint or as a **broadcast signal.**

Ex: For point to point data is transferred from subscriber to base station and point to multipoint is from base station to multiple subscribers.

The term **"Distribution"** in LMDS defines the **wide range of data (signals)** such as voice, or video can be transmitted to multiple receivers.

"Service" in LMDS explains the **relationship between customer and operator**. In LMDS the total service depends on operator service.

Characteristics:

1. The typical **data rate** is **45 Mbps.**
2. The **data access scheme** (technique) involved is **FDMA, TDMA or CDMA.**
3. **LMDS** signals are **strict to line of sight (LOS)** (i.e.) the reason LMDS is **suitable** where **antenna is present on** the **rooftop** system.
4. It can able to support all kinds of corporate network services such as video conference, file transfer and messaging.
5. LMDS signals are permitted at **different frequencies 24 GHz, 28 GHz, 31 GHz, and 38 GHz** and so on.

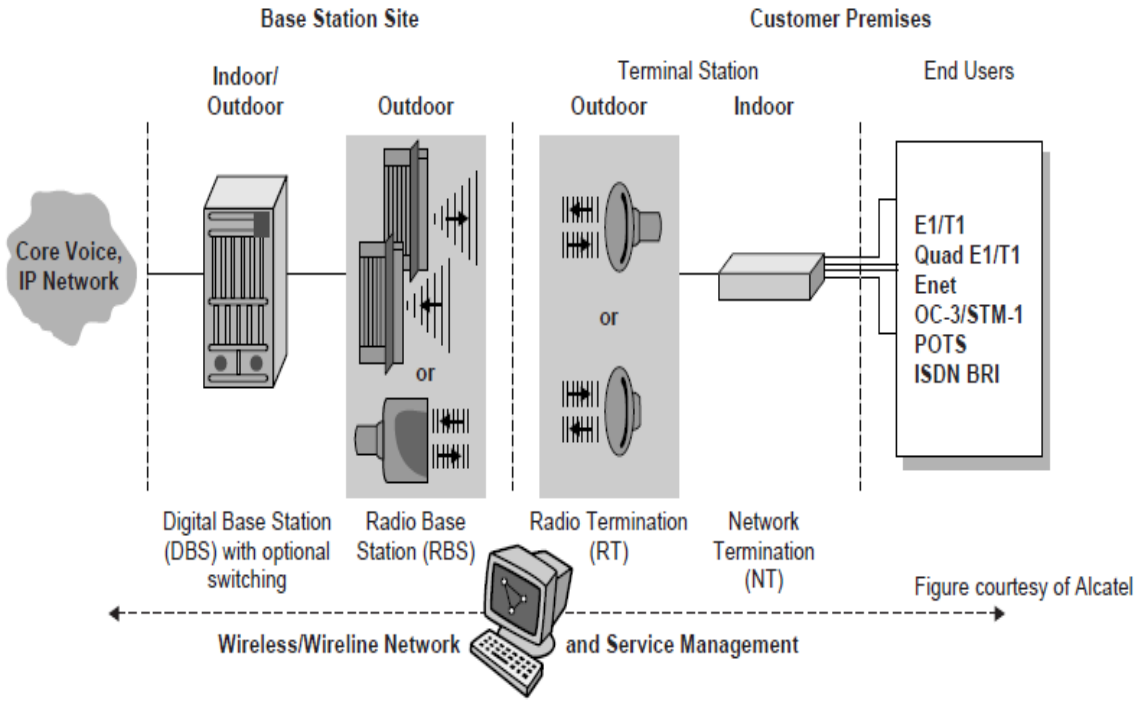
BLOCKS INVOLVED IN LMDS: Four components are involved in LMDS.

(i) Base station block

(ii) Customer premises block

(iii) Network Interface unit (NIU)

(iv) Fiber based Infrastructure



Customer Premise:

The customer premise block has one outdoor unit with transmitter and receiver antenna and an indoor unit which in-turn communicates with subscriber equipment such as telephones and PC's.

The **indoor unit** accepts the signal from the outdoor unit, demodulates and de multiplexes it and then interfaces with the connected subscriber equipment.

The customer premise equipment may attach to network using TDMA, FDMA or CDMA.

Base station site:

For downlink to customer premises the base station converts the digital bit stream voice, data and video information received from the core network into microwaves and is transmitted through a small antenna via outdoor unit to customer premises.

The **microwaves** are then **reconverted** back into **digital bit stream by the NIU** (Network Interface Unit) and delivered to the end user.

Fiber based Infrastructure

The fiber based infrastructure basically consists of SONET OC-12 OC-3 and DS-3 links, the ATM and IP switching systems, Interconnections with the PSTN, the central office equipment. The **conversion from fibered infrastructure to a wireless infrastructure happens at the base stations.**

Note: Local switching can also be present in the base station. If local switching is present then customers communicating in the same base station can communicate with each other without entering the fiber infrastructure.

Benefits of LMDS:

1. Network maintenance and managing involves less cost.
2. Major percentage of investment is shifted to CPE customer Permise Equipment (i.e) operator spends money on equipment only.
3. Scalable architecture (demand based build up).
4. Speed of network deployment is much quicker with wireless systems.

Limitations of LMDS:

1. Requires a direct LOS between buildings.
2. LMDS signals are susceptible to interference from rain, fog even walls and hills also.

MMDS:

Multichannel Multipoint Distribution System

- It is a new wireless technology evolved **especially for Internet service**.
- MMDS signals **have longer wavelength than LMDS** which can **travel** further **long distance** without losing significant power. The **increased power level** was **achieved** with the help of **repeaters.**

Features:

- It provides reliable two way (bidirectional) data and internet services.
- It is **cheaper than fiber or copper.**.

The term **"Multichannel"** in MMDS indicates that the signal in this technique propagates for **long distance** (i.e) the transmitter can **cover upto 35 miles.**

"Multipoint" in MMDS indicates that the signals can be transferred as point to point or even point to multipoint or as a **broadcast signal.**

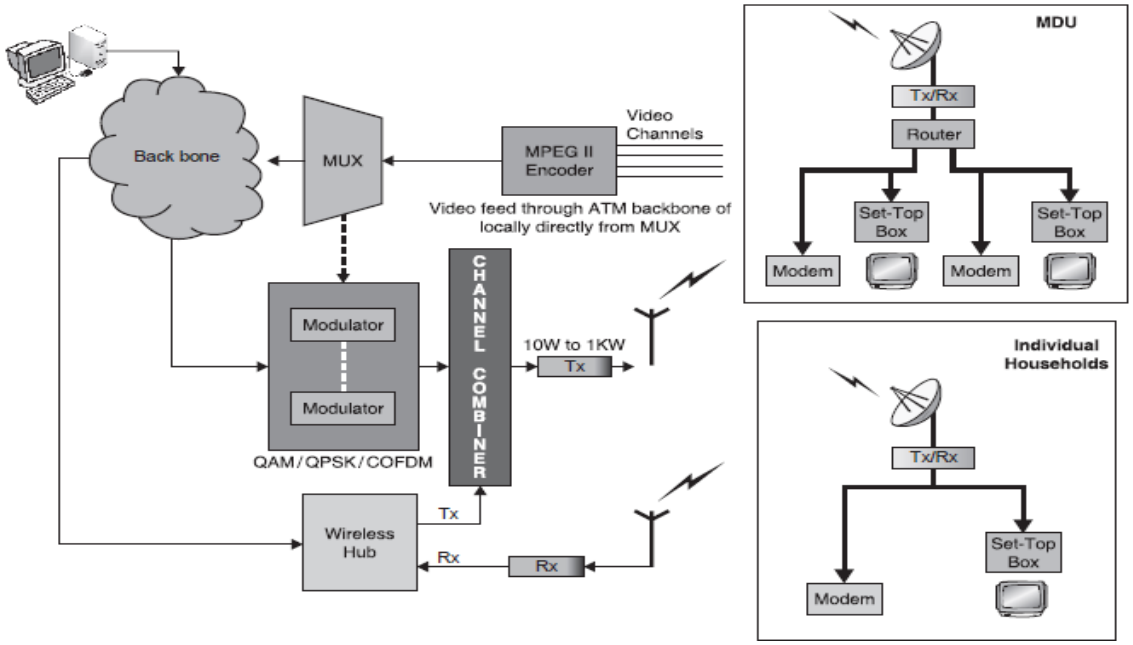
Ex: For point to point data is transferred from subscriber to base station and point to multipoint is from base station to multiple subscribers.

The term **"Distribution"** in MMDS defines the **wide range of data (signals)** such as voice, or video can be transmitted to multiple receivers.

"Service" in MMDS explains the **relationship between customer and operator**.

Characteristics of MMDS

- MMDS **signals are not blocked** easily **by objects** and are less susceptible to rain and smog.
- MMDS signals can **reach upto 35 miles.**
- MMDS signals **operate** only **@ 2.5 to 2.7 GHz.** (narrow spectrum).
- The typical **data rate** is **0.5 to 3 Mbps.**
- The **data access scheme** (technique) involved is **FDMA, TDMA or CDMA & OFDM.**
- Most of the MMDS are LOS system but non LOS system is also possible.
- The topology can be point to point or point to multipoint.



MDU: Multiple dwelling unit. It is a wireless internet service provider.

MODEM: The essential **function** of a **modem** is to create an easily transmitted and decoded signal that allows **digital data to be sent** from place to place **without the loss of information.**

MPEG II encoder: It enables users to **select their own level of compression,** and also offers a number of settings for adjusting both video and audio streams.

Multiplexer: It is a device that sends multiple signals on a carrier channel at the same time in the form of a single, complex signal to another device that recovers the separate signals at the receiving end.

Channel combiner: It is used **to cascade the output of several transmitters** into a common waveguide (transmission line).

Benefits of MMDS:

1. MMDS signals are less susceptible to interference from rain and fog.
2. It covers long distance.
3. Cheaper system to implement.

Limitations of MMDS:

1. Large upstream bandwidth in MMDS band requires careful planning, filtering etc.

Compare LMDS and MMDS.

Parameter	LMDS	MMDS

Frequency range	28-31 GHz	**2.5-2.7** GHz
Range (Coverage area)	Upto 5 miles	Upto 35 miles
Data rate	Typically upto 45 Mbps	Typically 0.5 to 3 Mbps
Propagation Characteristics	Strict to LOS	Non LOS is also permissible.
Topology	Point to point or point to multipoint.	Point to point or point to multipoint.
Access Scheme	FDMA, TDMA or CDMA	FDMA, TDMA or CDMA & OFDM
Target market	Large and medium Enterprises	Residential small enterprises
Wavelength	Shorter wavelength	Longer wavelength achieved using repeaters.
Cell architecture	Multiple and small microcells	Single large microcell
Cost of customer premises equipment	High	Low or medium compare to LMDS
Ability to support 2-way systems	Well suited due to small cell size, large bandwidth and high directive antennas.	Limited due to bandwidth, antenna characteristics and propagation characteristics
Link pathology	Long range and broad antenna beam ensure significant multipath.	Short range and highly directive antenna. It means no little multipath.

EC8004 WIRELESS NETWORKS VI SEM ECE-
UNIT 5

4G & BEYOND

Introduction – 4G vision – 4G features and challenges - Applications of 4G – 4G Technologies: Multicarrier Modulation, Smart antenna techniques, IMS Architecture, LTE, Advanced Broadband Wireless Access and Services, MVNO.

PART-A

1. Compare 3G and 4G systems.

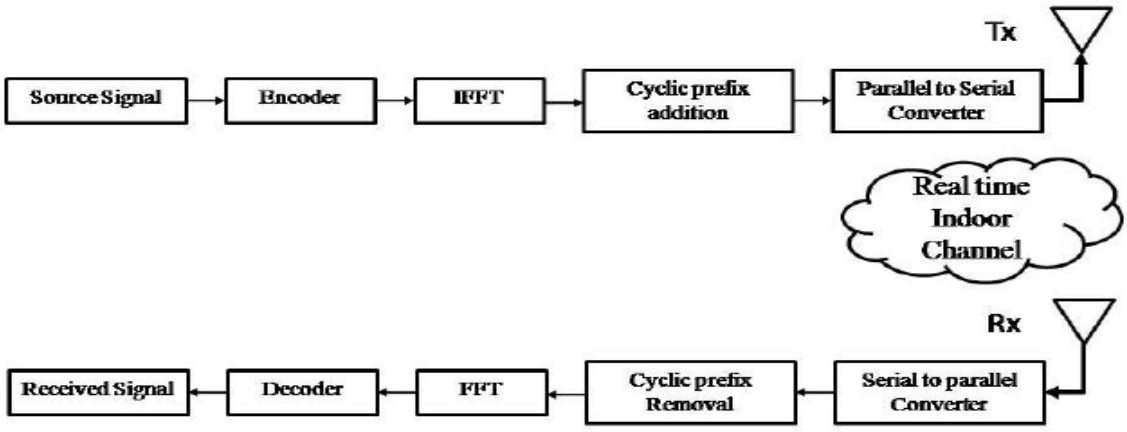
S.No	Parameters	3G	4G
1	Architecture	Wide area cell based network	Hybrid (Integration of WiFi, Bluetooth)
2	Speed	384 Kbps to 2 Mbps	20 to 100 Mbps
3	Frequency	1.8 to 2.4 GHz	2 to 8 GHz
4	Bandwidth	5 to 20 MHz	1000 MHz and more
5	Switching	Both circuit and packet	packet switching, message switching

---

2. How high spectral efficiency and increased throughput are achieved in the OFDM – MIMO system?

- **OFDM and MIMO can be combined** to achieve high spectral efficiency and increased throughput.

The OFDM MIMO system transmits independent OFDM modulated data from multiple antennas simultaneously. At the receiver after OFDM demodulation MIMO decodes each sub channel to extract data from all transmitted antennas on all the sub channels.

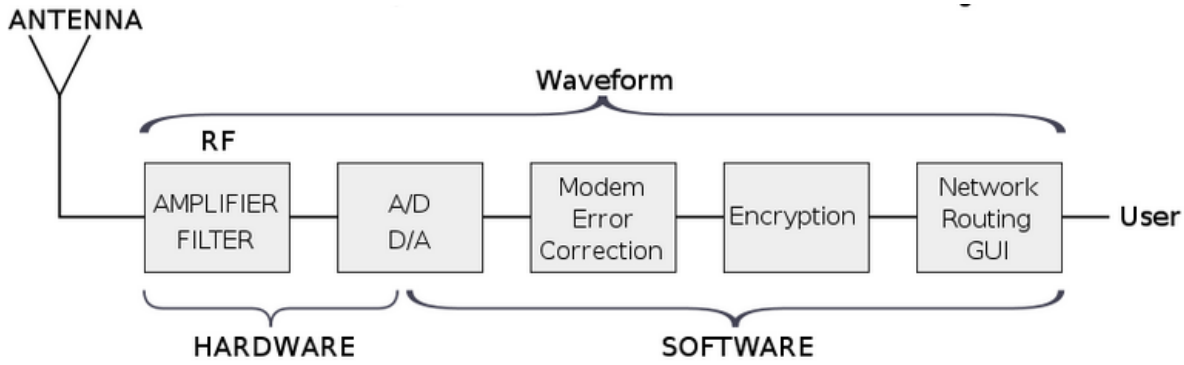


---

3. What is SDR?

A software-defined radio (SDR) system is a radio communication system which **uses software for the modulation and demodulation of radio signals**. An SDR performs significant amounts of signal processing in a general purpose computer.

Objective: To **produce a radio that** can **receive and transmit** a new form of radio protocol just **by running new software.**



---

4. Define 4G or what is 4G?

4G can defined as **MAGIC** also known as Mobile Broadband Everywhere

Mobile Multimedia

Anytime Anywhere

Global Mobility Support

Integrated Wireless Solution

Customized Personal Services

---

5. **What are the challenges faced while migrating to 4G?**

The main challenges are

a. Multimode user terminals

b. Wireless System Discovery and Selection

c. Terminal Mobility

d. Network Infrastructure and QoS Support

e. Security and Privacy

f. Fault tolerance and Survivability

g. Multiple Operators and Billing Systems

---

6. **List out the applications of 4G technologies.**

The applications of 4G technologies are:

a. Virtual Presence

b. Virtual Navigation

c. Tele-Medicine

d .Tele-Geo-Processing applications

e. Gaming

f. Education

---

7. **Define Multi Carrier Modulation (MCM) or what is MCM?**

PRINCIPLE:

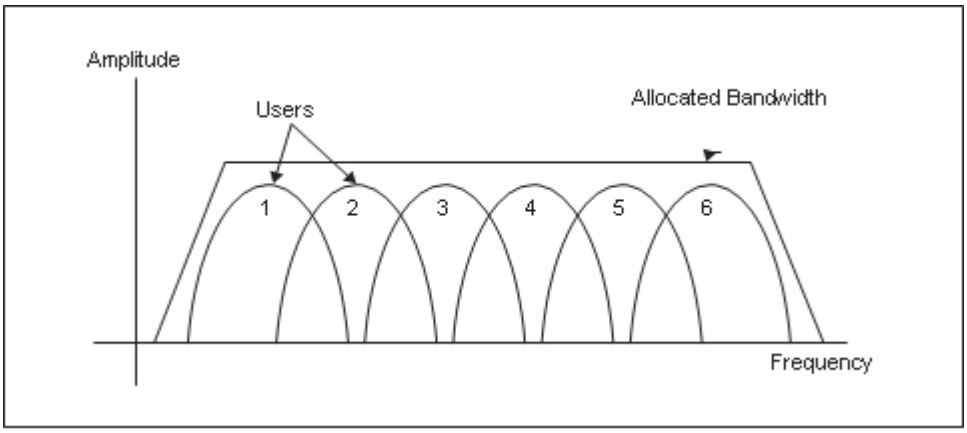
- Multi-carrier modulation (MCM) is a method of **transmitting data** by **splitting it into several components**, and sending **each** of these **components** through **separate carrier signals**.
- The **individual carriers** have **narrow bandwidth**, but the **composite signal** can have **broad bandwidth**.

Application: MCM was first used in analog military communications in the 1950s. Recently, MCM has attracted attention as a means of enhancing the bandwidth of digital communications over media.

---

8. **What is Smart Antenna? List the features of Smart Antenna.**

Smart antenna: Is a muti-element antenna where the signals received at each antenna element are intelligently combined to improve the performance of the wireless system.



Features:

a. Reduction Co-Channel Interference

b. Reduction in multipath interference

c. Fully controlled by software so less manual operation

d. Provides high security

e. Compatible: It can be applied to various multiple access techniques such as TDMA, FDMA and CDMA

---

9. **Compare MVNO and MNO.**

MVNO	**MVO**
A mobile virtual network operator (MVNO) is a mobile operator that **does not own radio spectrum or have its own network infrastructure**. A mobile virtual network operator (**MVNO**) is a **reseller for wireless communications services**. An **MVNO** leases wireless capacity from a third-party mobile network operator (MNO) at wholesale prices and resells it to consumers at reduced retail prices under its own business brand. **Ex: AEROVOYCE** is a MVNO established **in**	A mobile network operator (MVNO) is a mobile operator that **have its own radio spectrum and have its own network infrastructure**. Ex: Vodafone, Airtel, etc..

Tamilnadu.	

---

10. State the principle involved in Advanced Broadband Wireless Networks.

Objective: To provide broadband internet access to rural and remote area.

Principle: It involves wired optical network at back end and a wireless mesh network at front end.

---

11. Whether LTE and 4G are same? Justify.

No, LTE and 4G are different.

LTE	4G
It is the abbreviate form of Long Term Evolution. It does not qualify the terms of a new generation. So we may call it the **improved version of 3G but not 4 G.** It **allows 4G speed to advertise it, but it do not reach the standards. So it is an improvement.** It is designed to **provide** up to **10x (10 times) the speeds of 3G networks** for mobile devices such as smartphones, tablets, and wireless hotspots. Developed by the 3rd Generation Partnership Project (3GPP).	In 2008 ITU introduced the new version of signal boosting technology that is called 4G or fourth generation connectivity. **Features:** Full digital media on mobile gadgets Video streaming and multimedia High-speed music Higher download speed no worries about load time

---

12. State the features of IMP services.

IP Multimedia Subsystem is an architectural framework for delivering IP multimedia services.

It supports both real time (live conference) and non real time (store and forward-email) multimedia session services.

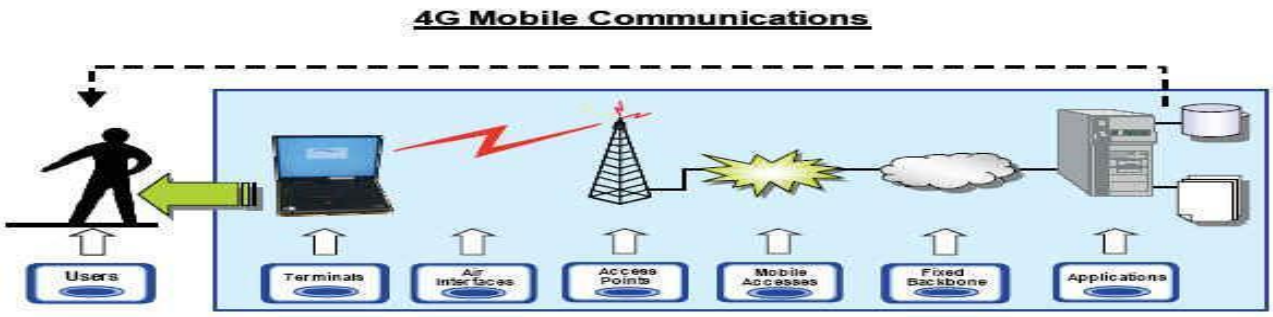
It supports fixed, mobile, UMTS and CDMA services.

PART-B

Explain or write short note on 4G VISION:

The 4G systems are projected to solve the still-remaining problems of 3G systems .They are designed to provide a wide variety of new services such as.

- High-quality voice, high-definition video at high-data-rate through wireless channels.
- The term 4G is used broadly to include several types of broadband wireless access communication systems, not only cellular systems.
- **4G is described as MAGIC:**
  - -Mobile multimedia
  - - Anytime anywhere
  - - Global mobility support
  - - Integrated wireless solution
  - -Customized personal service
- The **4G systems** will not only support the next generation mobile services, but **also will support the fixed wireless networks**.
- The 4G systems **provides seamless service** (without interruption) integrating terminals, networks, and applications **to satisfy** increasing **user demands.**



- Accessing information anywhere, anytime, with a seamless connection to a wide range of information and services, and **receiving a large volume of information, data, pictures, video, and so on, are the keys features of 4G.**

- The future 4G systems will consist of a set of various networks using IP as a common protocol. **4G systems will have broader bandwidth, higher data rate and quicker handoff** and will focus on ensuring seamless service across a multiple of wireless systems and networks.
- The key is to integrate the 4G capabilities with all the existing mobile technologies through the advanced techniques of digital communications and networking.

Explain the **APPLICATIONS OF 4G**

The following are some of the applications of the 4G system:

1. Virtual presence: 4G will provide user services at all times, even if the **user is off-line** without any interruption.

2. Virtual navigation: 4G will provide users with virtual navigation through which a user can **access a database of streets**, buildings, etc., of a large city. This requires high speed transmission.

3. Tele-medicine: 4G will support the **remote health monitoring** of patients via video conference assistance for a doctor at anytime and anywhere.

4. Tele-geo-processing applications: 4G will **combine** geographical information systems **(GIS**) and global positioning systems **(GPS)** to know simultaneous information from weather to traffic about current status.

5. Education: 4G will provide a good opportunity to people anywhere in the world to continue their education on-line in a cost-effective manner.

6. Gaming: High speed multi user gaming is possible with 4G.

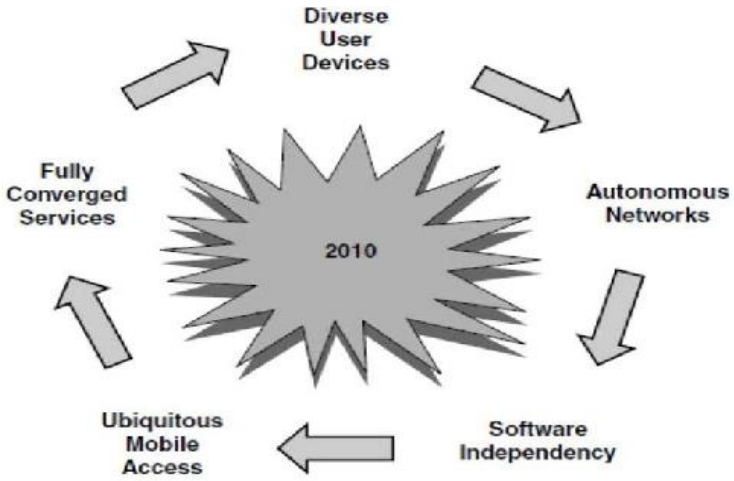
7. Cloud Computing: Safe and Secure cloud computing **(data storage)** is possible with 4G.

8. Crisis detection and prevention: Disasters both natural and man-made bring down communication and creates hurdle (difficult) in rescue operations. With 4G it is expected that in case of such crisis also it will be easier to restore communication at a fast rate.

Explain 4G FEATURES :

Some key features (primarily from users' points of view) of 4G mobile networks are as follows (see Figure):

1. IP-based heterogeneous networks: Anytime, anywhere, and with any technology.



2. Support for multimedia services at low transmission cost
3. Personalization
4. Integrated services
5. IP based mobile system
6. High speed, high capacity and low cost per bit.
7. Seamless switching and a high quality of service.
8. Better scheduling and call admission control techniques.
9. Better spectral efficiency.
10. Supports Ad-Hoc and Multi Hop networks.

List the CHALLENGES FACED BY 4G and their solutions

Need: Mobile communication is continuously one of the hottest areas that are developing at a booming speed, with advanced techniques emerging in all the fields of mobile and wireless communications. The **4G infrastructures** consist of a set of various **networks using IP**

(Internet protocol) as a common protocol so that users are in control because they are able to choose every application and environment.

Based on the developing trends of mobile communication, **4G have broader bandwidth, higher data rate, and quicker handoff** and it is focusing on **seamless service**.

Although 4G is an evolution in the wireless access technology but still it faces more challenges during its migration.

Challenges in migration to 4G Technology:

1. MULTIMODE USER TERMINAL:

Multimode user terminal is a device working in different modes supporting a wide variety of 4G services and wireless networks by re-configuring themselves to adapt to different wireless networks. They encounter several **design issues.**

Challenges faced: In the device size, cost, and power consumption.

Solution: One possible solution to this is the **use of SDR Software Defined Radio** which adapts itself to the wireless interface of the network.

2 WIRELESS NETWORK DISCOVERY:

Availing 4G services require the multimode user terminal to **discover and select the preferred wireless network.**

Challenge: Service discovery in 4G is much **more challenging then 3G because** of the **heterogeneity (different) of the networks** and their access protocols.

Solution: SDR approach has been proposed to counter this challenge. **SDR will scan** for the **available networks** and download the software required to interface with the selected network.

Software can be downloaded from a PC server, smart card or from over the air (OTA). Slow download speeds is one of the major problems faced by the SDR approach.

3. WIRELESS NETWORK SELECTION:

4G provide the users a choice to select a wireless network providing optimized performance and high QOS for a particular place, time and desired service (communication, multimedia).

Challenge: The parameters that define **high QOS** and optimized performance at particular instant **needs to be clearly defined** to make the network selection procedure efficient and transparent to the end user.

Solution: Possible considerations may be **available network resources,** network supported service types, cost and **user preference have to be mentioned**.

4. TERMINAL MOBILITY:

Terminal mobility is an **essential characteristic to fulfil the "Anytime Anywhere"** promise of 4G. It allows the mobile users to roam across the geographic boundaries of wireless networks.

Challenge: Two main issues in terminal mobility are **location and hand off management**.

(i) Location management involves tracking the location of the mobile users and maintaining information such as the authentication data, QoS capabilities, and the original and the current cell location

(ii) Handoff management is maintaining the ongoing communication when the terminal roams. Handoff can be horizontal or vertical depending on whether the user moves from one cell to another within the same wireless systems or across different wireless systems (WLAN to GSM).

5. NETWORK INFRASTRUCTURE AND QOS SUPPORT:

Unlike previous generation networks (2G and 3G), **4G is an integration of IP and non-IP based system.**

Challenge: Prior to 4G, QOS designs were made with a particular wireless system in mind.

Solution: But in 4G networks QOS designs should consider the integration of different wireless networks to guarantee QOS for the end-to-end services.

6. SECURITY:

Challenge: Most of the security schemes and the encryption/decryption protocols of the current generation networks were designed only for specific services. They seem to be very inflexible to be used across the heterogeneous architecture of 4G.

Solution: It dynamically reconfigurable, adaptive and lightweight security mechanism.

7. FAULT TOLERANCE:

Challenge: Wireless networks characterize a tree-like topology. Any failure in one of the levels can affect all the network elements at the levels below. This problem can be further aggravated because of the multiple tree topologies.

Solution: Adequate research work is required to devise a strategy for fault tolerance in wireless networks.

COMPARISON OF 3G AND 4G KEY PARAMETERS

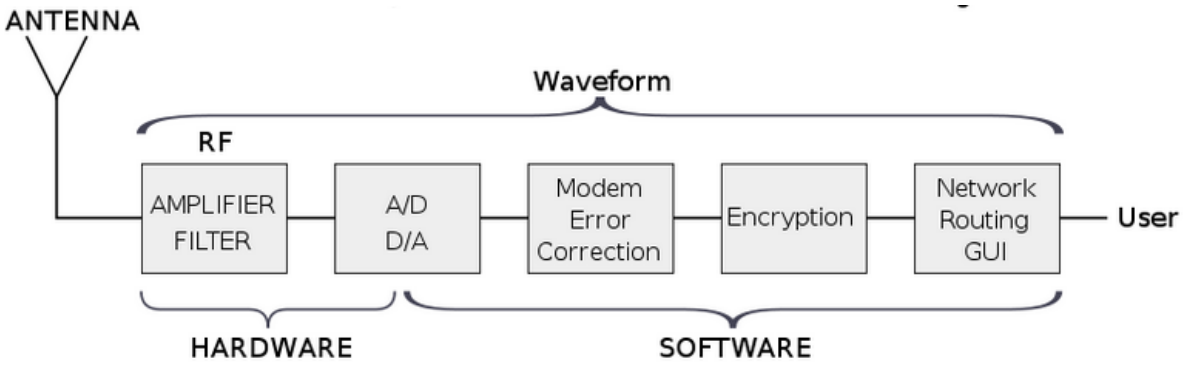
S.No	Parameters	3G	4G
1	Architecture	Wide area cell based network	Hybrid (Integration of WiFi, Bluetooth)
2	Speed	384 Kbps to 2 Mbps	20 to 100 Mbps
3	Frequency	1.8 to 2.4 GHz	2 to 8 GHz
4	Bandwidth	5 to 20 MHz	1000 MHz and more
5	Switching	Both circuit and packet	packet switching, message switching
6	Access technique	WCDMA, CDMA 2000	OFDM
7	Component Design	Optimized antenna design	Smart antenna, Software defined radio (SDR)
8	IP	IPv5	IPv6
9	Services and Application	CDMA 2000, UMTS and EDGE	LTE and Advanced
10	Forward error correction (FEC)	3G uses Turbo codes for error correction.	Concatenated codes are used for error corrections in 4G.

Explain about Software-Defined Radio.

A software-defined radio (SDR) system is a radio communication system which **uses software for the modulation and demodulation of radio signals**. An SDR performs significant amounts of signal processing in a general purpose computer.

Objective: To **produce a radio that** can **receive and transmit** a new form of radio protocol just **by running new software.**

Application: Software-defined radios have significant utility for cell phone services, which must serve a wide variety of changing radio protocols in real time.



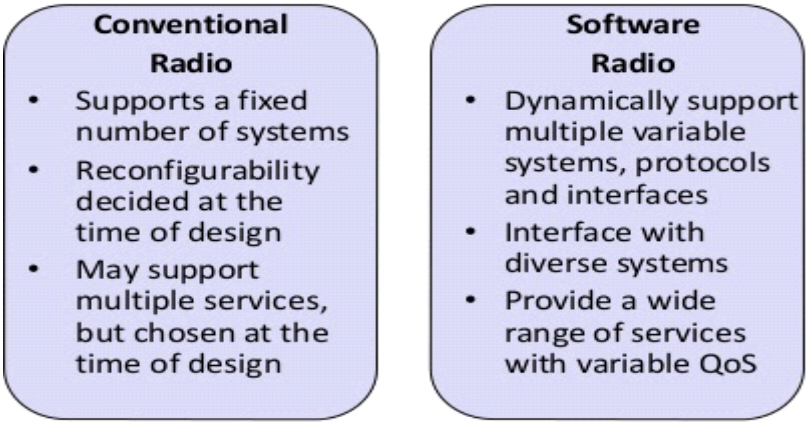
Construction: The hardware of a software- defined radio typically consists of a super heterodyne RF front end which converts RF signals from and to analog RF signals, and analog to digital converters and digital to analog converters which are used to convert digitized intermediate frequency (IF) signals from and to analog form, respectively.

Software-defined radio can currently be used to implement simple radio modem technologies. In the long run, SDR is expected to become the dominant technology in radio communications.

Features of SDR

- Software-defined radios can be **reconfigured "on-the-fly"** i.e., the **universal communication device that can reconfigure itself appropriately for the environment**. It could be a cordless phone one minute, a cell phone the next, a wireless Internet gadget the next, and a GPS receiver the next.
- Software-defined radios can be quickly and easily upgraded with enhanced features. In fact, the upgrade could be delivered over- the-air.
- Software-defined radios can talk and listen to multiple channels at the same time.

Difference between Software radio and Conventional radio networks:



Explain Multicarrier Modulation technique:

MULTI CARRIER MODULATION (MCM)

PRINCIPLE:

- Multi-carrier modulation (MCM) is a method of **transmitting data** by **splitting it into several components**, and sending **each** of these **components** through **separate carrier signals**.
- The **individual carriers** have **narrow bandwidth**, but the **composite signal** can have **broad bandwidth**.

Application: MCM was first used in analog military communications in the 1950s. Recently, MCM has attracted attention as a means of enhancing the bandwidth of digital communications over media.

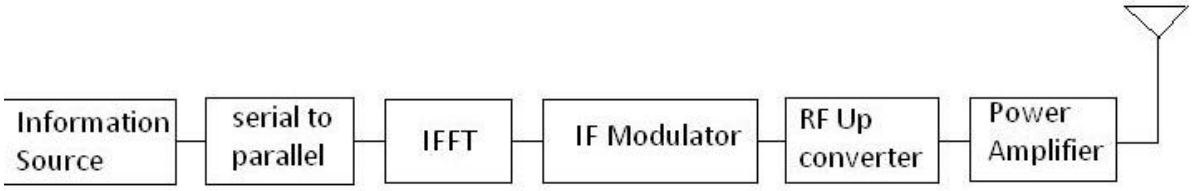
Before going in detail about MCM let us discuss about single carrier modulation:

NEED FOR MCM:

Multicarrier modulation techniques are particularly beneficial because :

- MCM provides a way of increasing the bandwidth while still being able to tolerate the varying fading conditions present.
- The scheme is used in audio broadcast services. The technology lends itself to digital television, and is used as a method of obtaining high data speeds in asymmetric digital subscriber line (ADSL) systems.

MULTI CARRIER MODULATION PROCESS



MCM uses multiple carriers spaced much closed over the band. Each of this carrier carry data bits as per modulation scheme employed. Hence OFDM delivers data rate is higher than the SC system. OFDM technique is used in WLAN and WIMAX broadband technologies.

MULTICARRIER MODULATION SCHEMES

- **Orthogonal frequency division multiplexing OFDM:** OFDM is possibly the most widely used form of multicarrier modulation. It uses multiple closely spaced carriers and as a result of their orthogonality, **mutual interference** between them is **avoided**.
- **Generalised Frequency Division Multiplexing (GFDM)**: GFDM is a multicarrier modulation scheme that **uses closed spaced non-orthogonal carriers** and provides flexible pulse shaping. It is therefore **attractive for** various applications such as **machine to machine communications.**

ADVANTAGES OF MCM:

1. Relative immunity to fading caused by transmission due to more than one path at a time (multipath fading) is avoided.
2. Less susceptibility than single carrier systems to interference caused by impulse noise.
3. Enhanced immunity to inter symbol interference.

LIMITATIONS OF MCM

- Difficult in synchronizing the carriers under marginal conditions.

MCM APPLICATIONS:

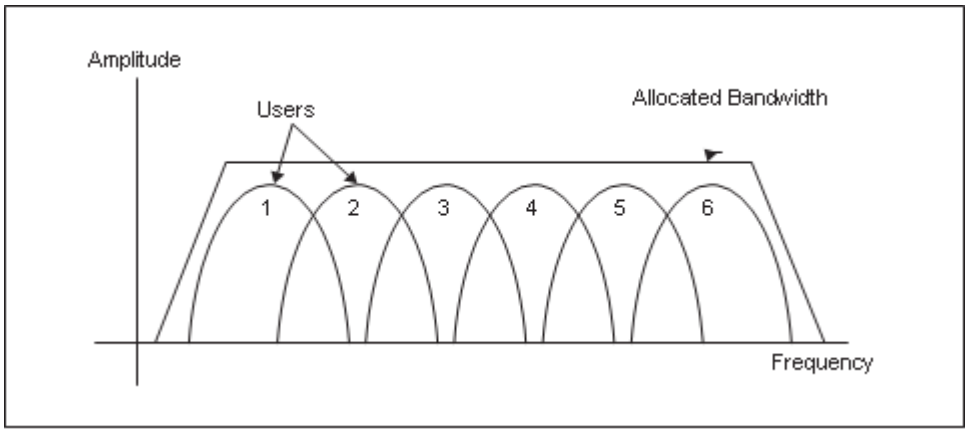
MCM has the elegant waveform properties that make it useful for a wide variety of applications.

- Digital transmission over telephone lines
- Applications in broadcasting
- Digital T.V.
- Wireless LANs

Explain about SMART antenna:

NEED: To increase the data throughput for mobile applications.

Example: **Multiple-input multiple-output** (MIMO) systems, it can **extend the capabilities of the 3G and 4G** systems.



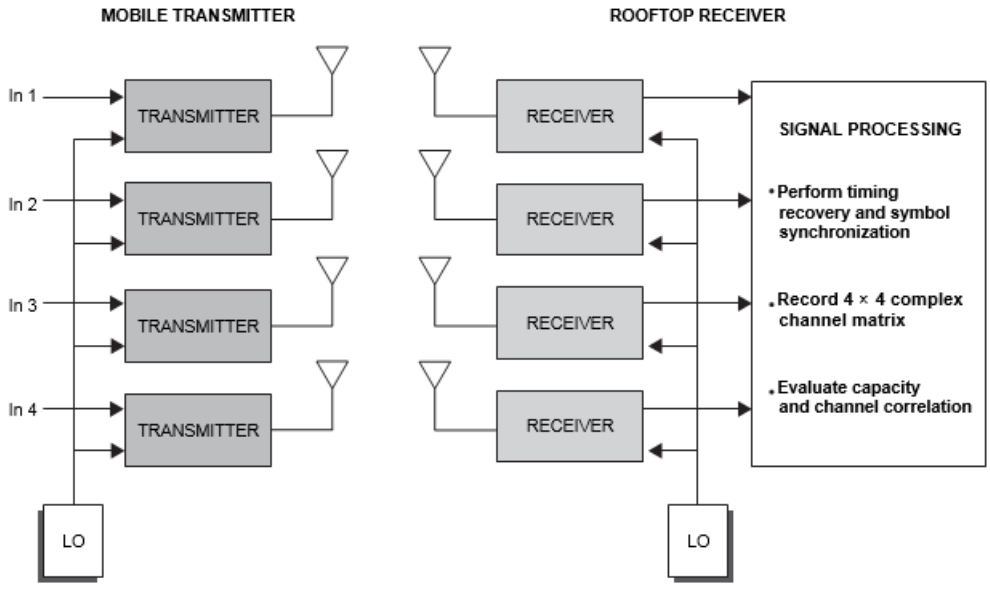
Overlapping sub channels

PRINCIPLE:

With MIMO, **different signals are transmitted** out of **each antenna simultaneously** in the **same bandwidth** and then separated at the receiver.

CONSTRUCTION:

MIMO systems use multiple antennas at both the transmitter and receiver to increase the capacity of the wireless channel to provide in excess of 1 Mbps for 2.5G wireless TDMA EDGE and as high as 20 Mbps for 4G systems.



With four antennas at the transmitter and receiver this has the potential to provide four times the data rate of a single antenna system without an increase in transmitting

power or bandwidth.

- MIMO techniques can support multiple independent channels in the same bandwidth, provided the multipath environment is rich enough. What this means is that high capacities are theoretically possible, unless there is a direct line of- sight between the transmitter and receiver.
- The number of transmitting antennas is *M*, and the number of receiving antennas is *N*

  where $N \geq M$.

We examine four cases:

- SISO - Single Input Single Output
- SIMO - Single Input Multiple output
- MISO - Multiple Input Single Output
- MIMO - Multiple Input multiple Output

Single-input, single-output (SISO): It has one antenna at the transmitter and at the receiver.. There is no diversity and no additional processing required.

Advantage: SISO system simple in construction

Drawback: Interference and fading will impact (affect) the system.

If the channel bandwidth is *B*, the transmitter power is *Pt*, the signal at the receiver has an average signal-to-noise ratio of SNR_0, then the Shannon limit on channel capacity *C* is

$$C=B\log_2(1+SNR_0)$$

Single-input, multiple-output (SIMO): The **transmitter** has a **single antenna** and the **receiver** has **multiple antennas**. This is also **known as receiver diversity**. It is often **used** to **enable** a **receiver** system that **receives signals** from a **number of independent sources** to combat (minimize) the effects of fading.

There are *N* antennas at the receiver.

Advantage: It is relatively easy to implement.

Drawback: For processing it consumes more time at the receiver since multiple antennas are involved.

Redundancy coding / processing is involved at receiver.

The overall increase in SNR will be:

$$SNR \approx \frac{N^2 \times (\text{signal power})}{N \times (\text{noise})} = N \times SNR_0$$

The capacity for this channel is approximately equal to

$$C \approx B \log_2 [1 + N \times SNR_0]$$

Multiple-input, single-output: MISO is also termed **transmit diversity**. In this case, the **same data** is **transmitted redundantly** (additionally) from the two transmitter antennas. The receiver is then able to receive the optimum (exact or appropriate) signal which it can then use to extract the required data.

Advantage:

1. Redundancy coding / processing is moved from the receiver to the transmitter.

2. Reducing the level of processing required in the receiver for the redundancy coding. This has a positive impact on size, cost and battery life as the lower level of processing requires less battery consumption.

We have *M* transmitting antennas. The total power is divided into *M* transmitter branches. Since there is only one receiving antenna, the noise level is same as SISO. The overall increase in SNR is approximately

$$\text{SNR} \approx \frac{M^2 \cdot [(\text{signal power})/M]}{\text{noise}} = M \times \text{SNR}_0$$

Multiple-input, multiple-output: Here, multiple antennas are involved at both transmitter and receiver.. MIMO can be used to provide improvements in both channel robustness as well as channel throughput.

MIMO systems can be viewed as a combination of MISO and SIMO channels. channel The channel capacity is equal to

$$C \approx B \log_2(1 + M \times N \times \text{SNR}_0)$$

Assuming $N \geq M$, we can send different signals using the same bandwidth and still be able to decode correctly at the receiver. Thus, we are creating a channel for each one of the transmitters. The capacity of each one of these channels is roughly equal to

$$C_{\text{single}} \approx B \log_2\left(1 + \frac{N}{M} \times \text{SNR}_0\right)$$

Since we have M of these channels (M transmitting antennas), the total capacity of the system is

$$C \approx MB \log_2\left(1 + \frac{N}{M} \times \text{SNR}_0\right)$$

We get a linear increase in capacity with respect to the transmitting antennas.

List some of the new technologies used in 4G system:

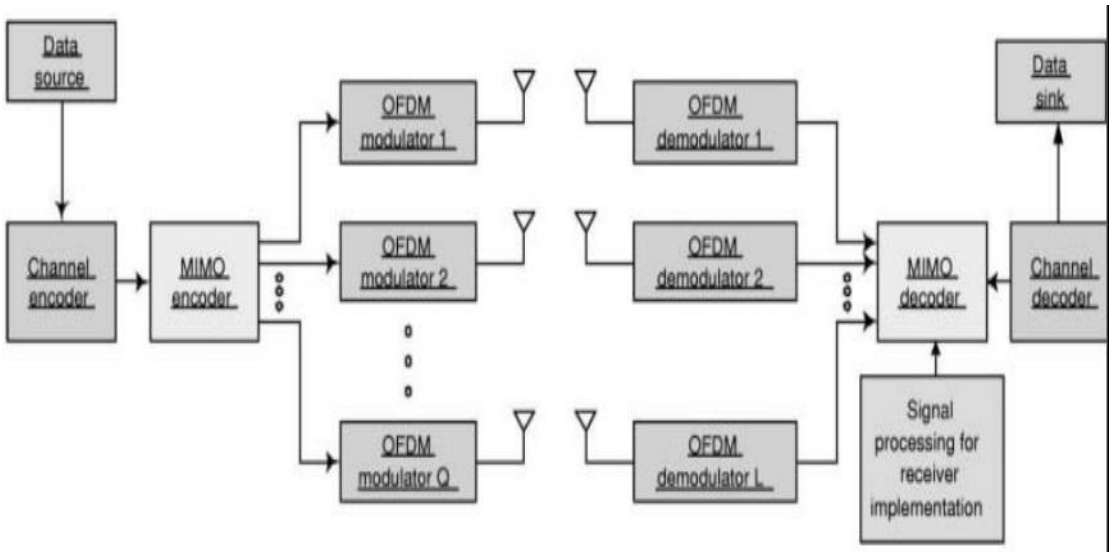
Ans: SDR and SMART ANTENNA

Explain briefly OFDM-MIMO system.

Multiple-input, multiple-output orthogonal frequency-division multiplexing (MIMO-OFDM) is the dominant air interface for 4G and 5G broadband wireless communications.

NEED: To provide more reliable communications at high speeds.

Principle: It combines multiple-input, multiple-output (MIMO) technology with OFDM to achieve high spectral efficiency.



MIMO OFDM Tx MIMO OFDM Rx

MIMO OFDM Transmitter

The source bit stream is encoded by the FEC encoder and the coded bit stream is mapped to a constellation by digital modulator, and encoded by the MIMO encoder. Each of the parallel output symbol streams are corresponded to a certain transmitting antenna.

MIMO OFDM Receiver

The received bit stream from different receiving antenna is first synchronized. Preamable bit and cyclic prefix (error codes) are extracted from received data. The remaining symbols are demodulated by FFT. Frequency pilots are extracted from the demodulated OFDM symbols and are used for channel estimation.

Estimated channel matrix aids the MIMO decoder and the estimated transmitted symbols are demodulated and then decoded.

Advantages of OFDM –MIMO systems are:

1. High spectral efficiency
2. Simple Implementation by FFT
3. Low receiver complexity
4. High flexibility

5. Robusteness to multipath fading

Applications of OFDM-MIMO systems are:

1. Wireless network

2. Power line control

3. Discrete multitone systems

4. Discrete multitone systems

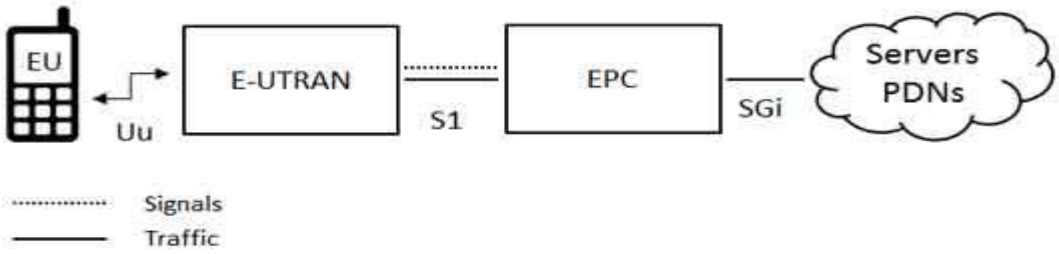
Explain LTE protocol architecture: (Apr-may2018)

LTE is an abbreviation for **L***ong* **T***erm* **E***volution*. LTE is a 4G wireless communications standard developed by the 3rd Generation Partnership Project (3GPP).

Objective: It is designed to **provide** up to **10x (10 times) the speeds of 3G networks** for mobile devices such as smartphones, tablets and wireless hotspots.

LTE is comprised of following three main components:

- The User Equipment (UE).
- The Evolved UMTS Terrestrial Radio Access Network (E-UTRAN).
- The Evolved Packet Core (EPC).



1. The User Equipment (UE): The internal architecture of the user equipment for LTE is identical to the one used by UMTS which is actually a Mobile Equipment (ME). The mobile equipment comprised of the following important modules:

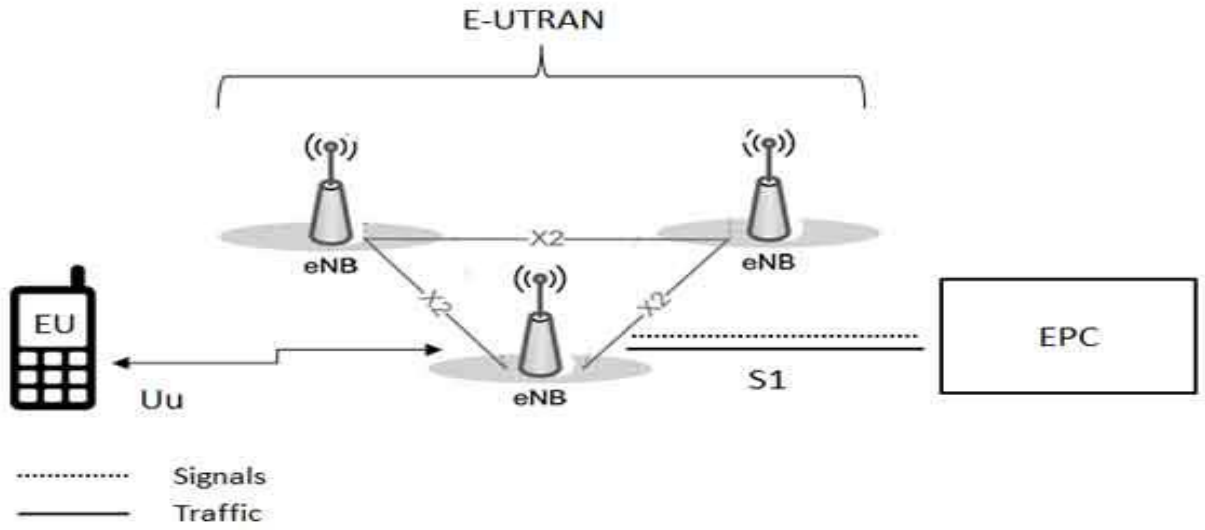
Mobile Termination (MT): This handles all the communication functions.

Terminal Equipment (TE): This terminates the data streams.

Universal Integrated Circuit Card (UICC): This is also known as the SIM card for LTE equipments. It runs an application known as the Universal Subscriber Identity Module (USIM).

A **USIM** stores user-specific data very similar to 3G SIM card. This keeps information about the user's phone number, home network identity and security keys etc.

2. The E-UTRAN (The access network): The architecture of evolved UMTS Terrestrial Radio Access Network (E-UTRAN) has been illustrated below.



The E-UTRAN handles the radio communications between the mobile and the evolved packet core and it has one component, the evolved base stations, called **eNodeB** or **eNB**. Each eNB is a base station that controls the mobiles in one or more cells. The base station that is communicating with a mobile is known as its serving eNB.

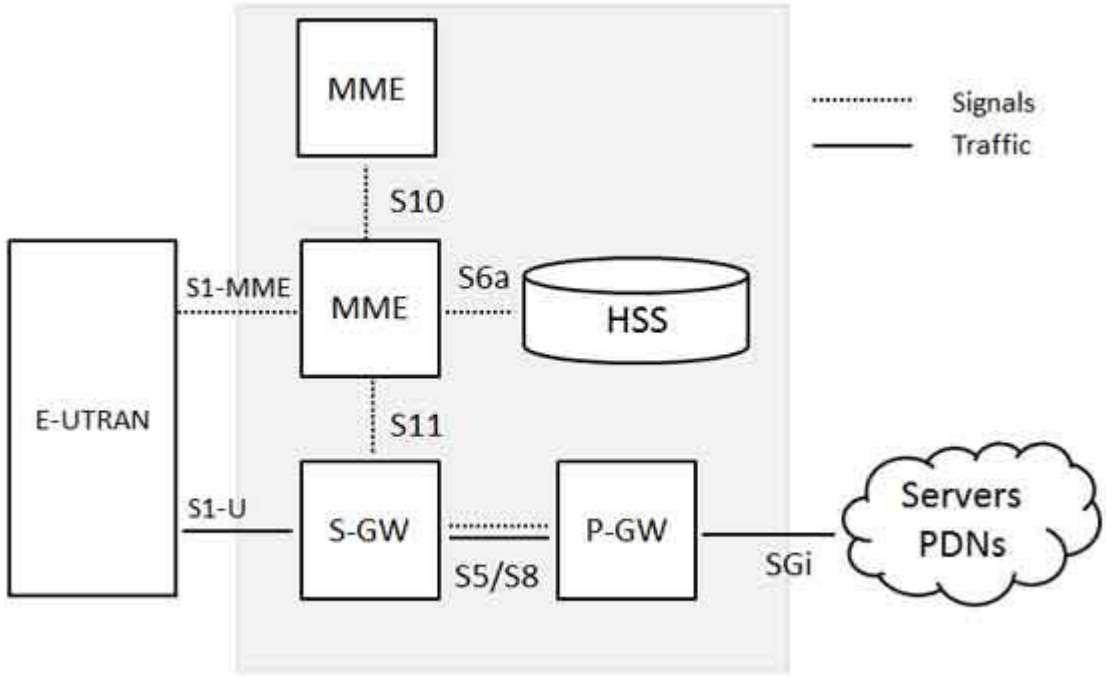
LTE Mobile communicates with just one base station and one cell at a time.

The two main functions supported by eNB:

- The eNB sends and receives radio transmissions to all the mobiles using the analogue and digital signal processing functions of the LTE air interface.
- The eNB controls the low-level operation of all its mobiles, by sending them signalling messages such as handover commands.

3. The Evolved Packet Core (EPC) (The core network):

The architecture of Evolved Packet Core (EPC) has been illustrated below.

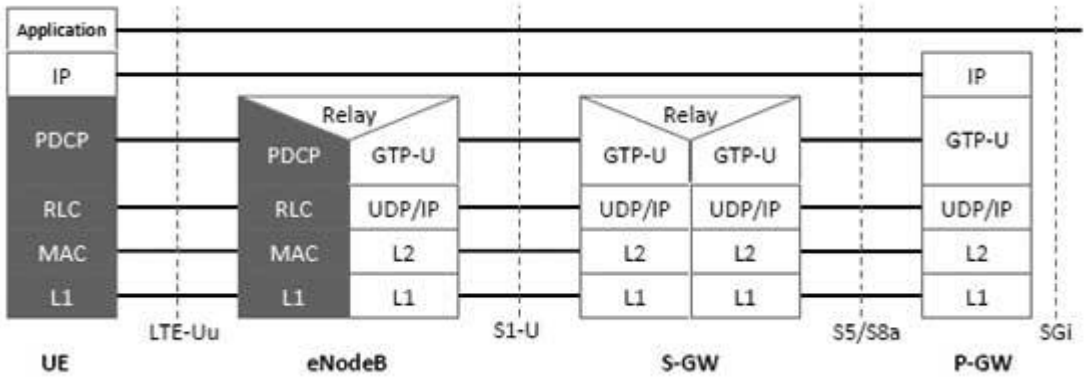


- The Home Subscriber Server **(HSS)** component is a **central database** that contains **information about** all the **network operator's subscribers**.
- The mobility management entity **(MME) controls the high-level operation of the mobile by** means of **signalling messages** and Home Subscriber Server (HSS).
- The Packet Data Network (PDN) Gateway (P-GW) communicates with the outside world ie. packet data networks PDN, using SGi interface. Each packet data network is identified by an access point name (APN).
- The **serving gateway (S-GW) acts as a router**, and **forwards data between** the **base station and** the **PDN gateway.**
- The **Policy Control and Charging Rules Function (PCRF)** is a component which is not shown in the above diagram but it is **responsible for policy control decision-making** which resides in the P-GW.

LTE protocol stack

1. Physical Layer (Layer 1)

Physical Layer carries all information from the MAC transport channels over the air interface. Takes care of **power control, cell search (for initial synchronization and handover** purposes)



2. Medium Access Layer (MAC)

MAC layer is responsible for **Mapping between logical channels and transport channels.**

1. Multiplexing and Demultiplexing.

2. Scheduling information, Error correction.

3. Priority handling between UEs by means of dynamic scheduling.

3. Radio Link Control (RLC) :

- Is responsible for duplicate detection (retransmitted data), and error detection.
- It also takes care of Concatenation, segmentation and reassembly.
- It operates in 3 modes of operation: Transparent Mode (TM), Unacknowledged Mode (UM), and Acknowledged Mode (AM).

4. Radio Resource Control (RRC)

The main services and functions of the RRC sublayer include:

1. Paging, establishment, maintenance and release of an RRC connection between the UE and E-UTRAN.

2.Security functions including key management, establishment, configuration and maintenance.

3. Broadcast of System Information. .

5. Packet Data Convergence Control (PDCP): It is responsible for

1. Header compression and decompression of IP data. Transfer of data between user plane and control plane.

2. Maintenance of PDCP Sequence Numbers (SNs) (In-sequence delivery).

3. Ciphering (encrypting) and deciphering (decrypting) of user plane data and control plane data.

4. Integrity protection and integrity verification of control plane data.

UNIT 1: FUNDAMENTALS & LINK LAYER

Overview of Data Communications- Networks – Building Network and its types– Overview of Internet - Protocol Layering - OSI Mode – Physical Layer – Overview of Data and Signals - introduction to Data Link Layer - Link layer Addressing- Error Detection and Correction

Overview of Data Communications:

The term telecommunication means communication at a distance. The word data refers to information presented in whatever form is agreed upon by the parties creating and using the data. Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable.

The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

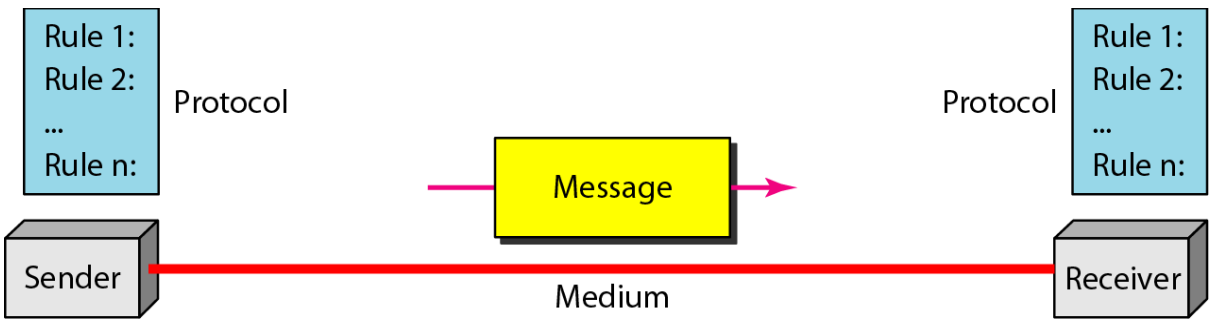
Delivery. The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.

Accuracy. The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.

Timeliness. The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called *real-time* transmission.

Jitter. Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets.

Components of a data communications system



Message. The **message** is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

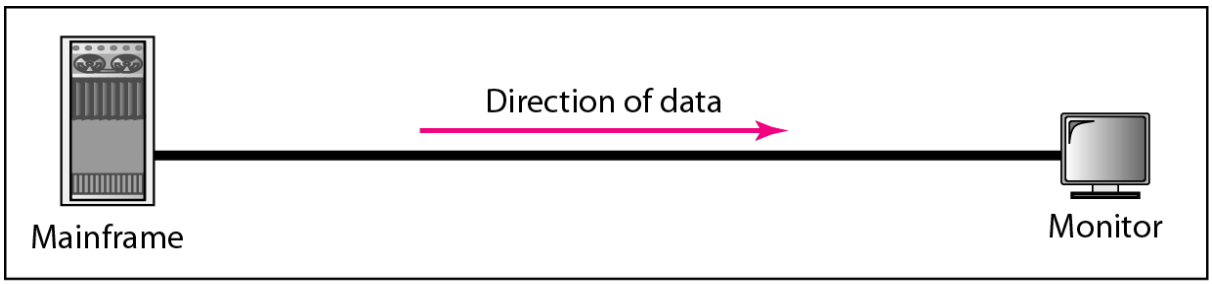
Sender. The **sender** is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

Receiver. The **receiver** is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

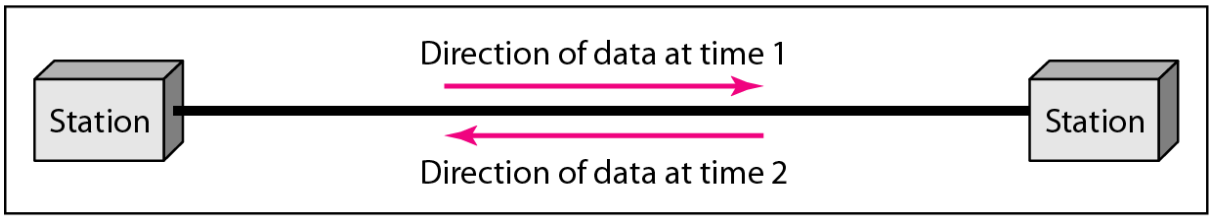
Transmission medium. The **transmission medium** is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

Protocol. A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

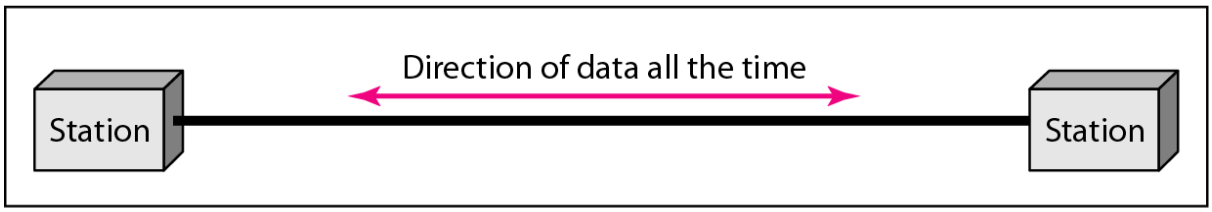
Data Flow



a. Simplex



b. Half-duplex



c. Full-duplex

Networks

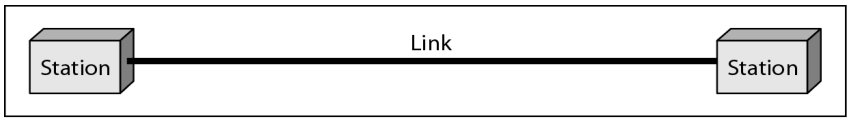
A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network. A link can be a cable, air, optical fiber, or any medium which can transport signal carrying information.

Network Criteria

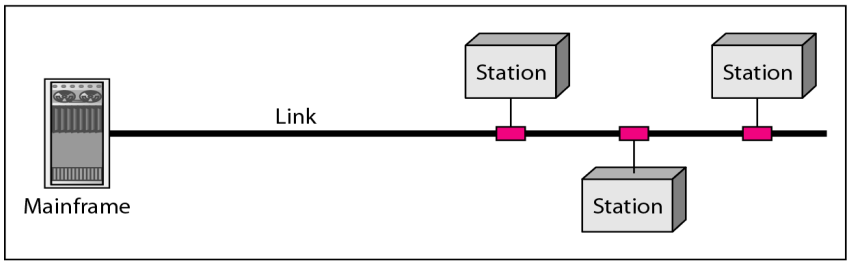
- ✓ Performance
  - Depends on Network Elements
  - Measured in terms of Delay and Throughput
- ✓ Reliability
  - Failure rate of network components
  - Measured in terms of availability/robustness
- ✓ Security
  - Data protection against corruption/loss of data due to:
    - ➢ Errors
    - ➢ Malicious users

Physical Structures

- ✓ Type of Connection
  - Point to Point - single transmitter and receiver
  - Multipoint - multiple recipients of single transmission

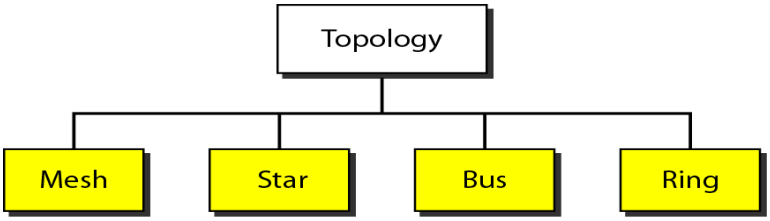


a. Point-to-point



b. Multipoint

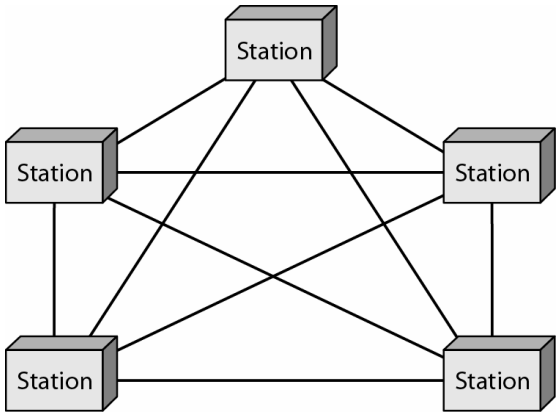
✓ Physical Topology



1. MESH:

- Each station has a point to point link to every other device.
- A fully connected mesh network requires n (n-1)/2 links.
- Each device should have n-1 input/output ports.

Where, n represents the number of stations.



Advantage:

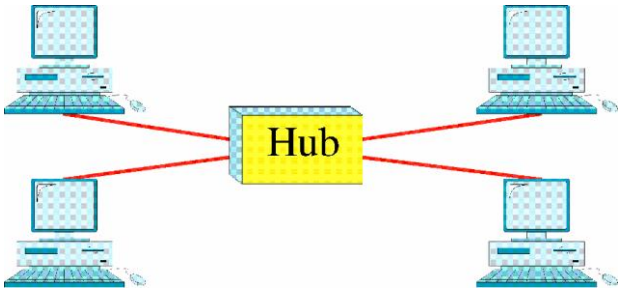
1. **Privacy/Security:** When message is sent from one station to other only the intended recipient receives it.
2. In this method if **one link becomes unusable**, it **does not disturb** the **entire system**.
3. Each link carries its own data and hence t**raffic problem** is **reduced.**
4. **Fault identification** and **rectification is easy** in this method.

Drawback:

1. Number of cables required and input/output ports required are more.
2. The hardware required to connect each link is more expensive.

2. STAR:

Each device has a point to point link only to a central controller called Hub. The devices are not directly linked to each other. If one device wants to send data to another it sends the data to the controller, it then relays the data to the other connected device.



Advantage:

1. Less expensive than mesh topology.
2. In star each device needs only one link and one I/O port to connect it to any number of other devices. This factor makes to install easily.
3. Less cable is required.
4. If one link fails only that link is affected. All other remains active. This factor makes easy fault identification and rectification.

Drawback:

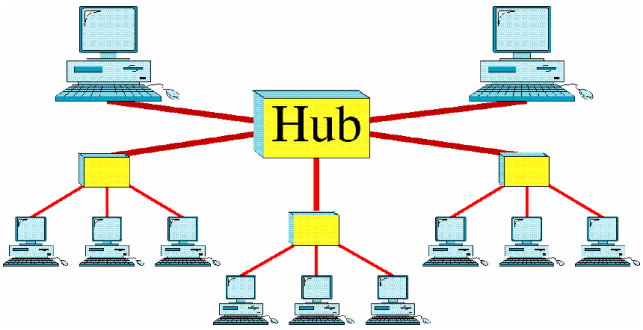
Since all the devices are connected to the hub it also requires more cable compared to bus topology.

3. TREE:

Is similar to star topology but not all the stations are connected to the central hub. The majority of the stations are connected to the secondary hubs that in turn connected to the primary hub.

The central hub in the tree is an active hub. An active hub contains repeater.

Repeater: Is a device which regenerates the original bit pattern before sending to the next device. The repeater increases the signal strength and the signal can be transmitted for long distances also.



Advantages:

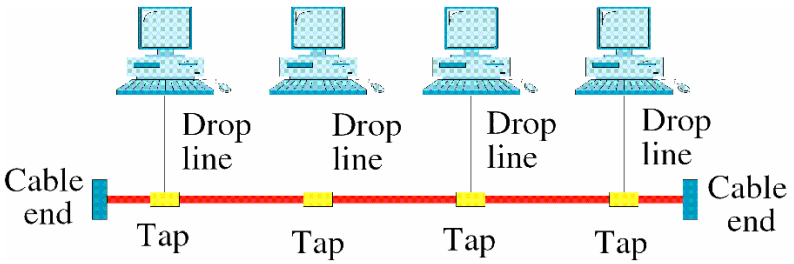
1. Since secondary hubs are used it allows more devices to connect to the central hub.

2. Since repeaters are used the signal can transmit from long distance also.
3. **Priority:** Stations attached to one secondary hub can be given priority over other stations attached to another secondary hub due to this advantage the system which wishes to transmit first can transfer the data and no need to wait for all other systems to transmit.

Ex: Cable TV technology. Here the main cable from the main office is divided into many branches and each branch is divided into smaller branches and so on.

4. BUS:

- Is a multipoint configuration.
- One long cable will be acting as backbone to link all the devices the network.
- All the stations are connected to the cable by means of drop line and tap.
- A drop line is a connection running between the device and the main cable.
- Tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core.



- When the signal is transmitted along the backbone of this cable some of its energy is transformed onto heat. Therefore, it becomes weaker and weaker when it travels far away.

Advantages:

1. Ease of installation
2. Uses less cable compared to mesh, star and ring topologies.

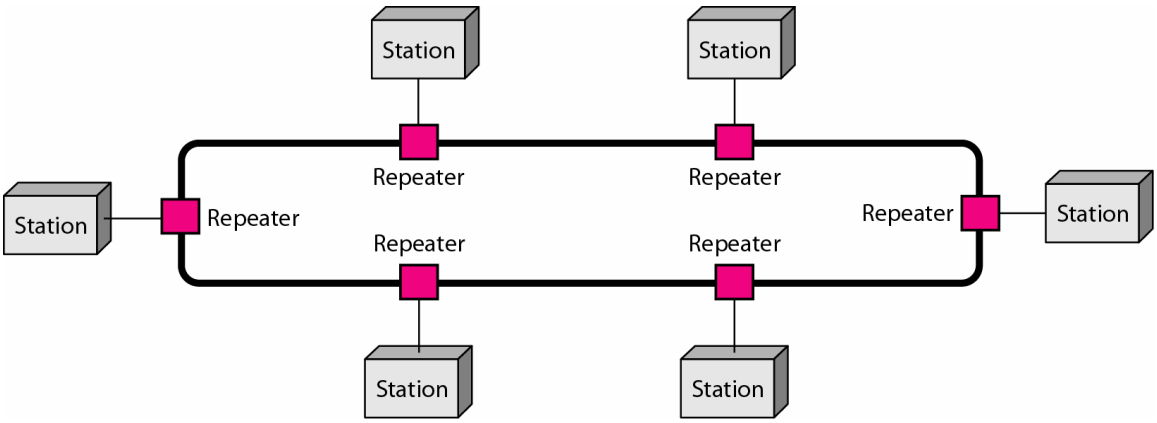
Drawback:

1. Fault identification is difficult.
2. The bus topology is designed to be optimum with number of devices at installation time and further devices cannot be attached or connected.
3. When any problem occurs in the backbone of the cable the entire cable should be replaced.

4. A fault or break in the bus cable stops all transmission. The damaged area reflects signals back in the direction of origin which creates noise in both directions.

5. RING:

A point o point link is established only between the two devices on either side of the station.



- The signal is passed along the ring in one direction from one station to other station until it reaches its destination.
- Each device in the ring incorporates a repeater.
- When a station receives a signal intended for another station its repeater regenerates the bits and passes them to the next device.

Advantages:

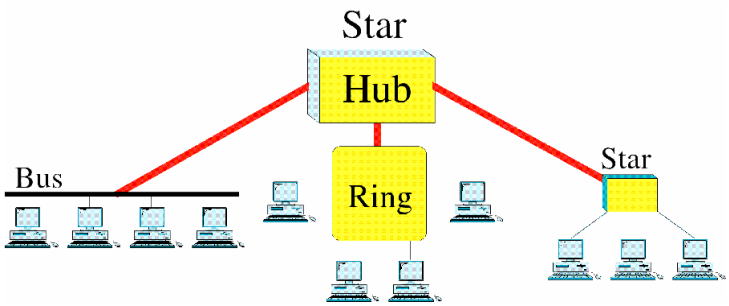
1. Easy to install
2. Each device is linked only to its immediate neighbors so to add or to delete a device it requires only two connections.
3. Fault isolation is easy. Therefore by keeping an alarm at each station when the signal is not received the alarm will sound hence faults can be identified easily.

Drawback:

1. **Unidirectional traffic:** A small break in the ring can disable the entire network.

HYBRID TOPOLOGY:

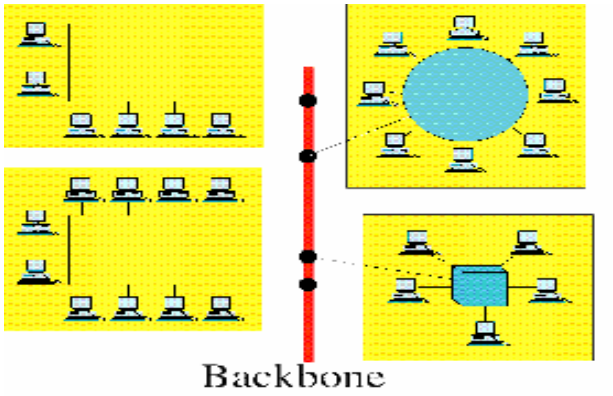
- The network combines several topologies as subnetworks linked together in a larger topology.



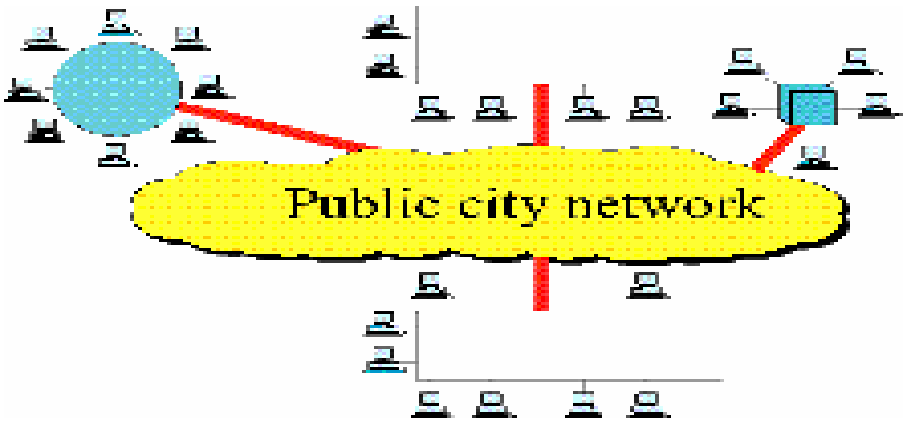
- **Ex:** One department of a business may have decided to use a bus topology while another department has a ring. The two can be connected to each other via a central controller in a star topology.

CATEGORIES OF NETWORKS:

a) LAN (Local Area Network): - A LAN is usually privately owned and links the devices in a single office, building or campus. LANs are designed to allow resources to be shared between personal computers are workstations.



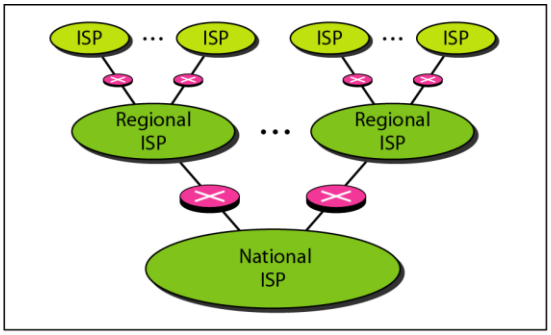
b) MAN (Metropolitan Area Network): - A MAN is designed to extend over an entire city. It may be a single n/w such as a cable TV n/w, or it may be means of connecting a number of LANs into a larger network so that resources may be shared LAN-to-LAN as well device-to-device.



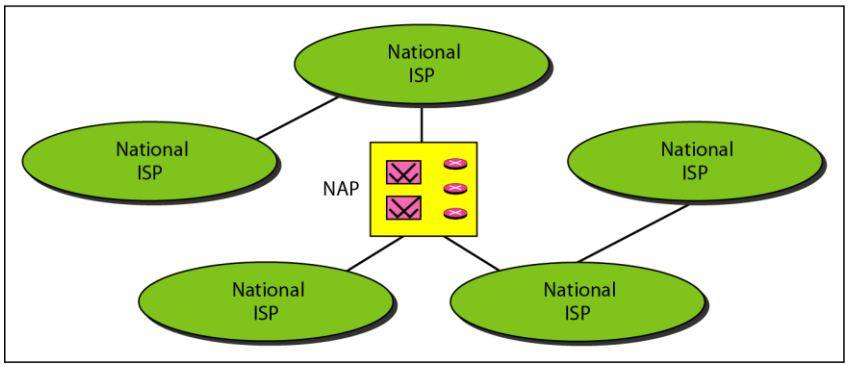
c) WAN (Wide Area Network): - WAN provides long distance transmission of data, voice, image and video information over large geographical areas that may comprise a country, or even the whole world.

Overview of Internet

The Internet has revolutionized many aspects of our daily lives. It has affected the way we do business as well as the way we spend our leisure time. The Internet is a communication system that has brought a wealth of information to our fingertips and organized it for our use.



a. Structure of a national ISP



b. Interconnection of national ISPs

Protocol Layering:

Protocol:

- Is a set of rules that govern data communication. It provides an agreement between the communicating devices. Without a protocol two devices may be connected but not communicated.

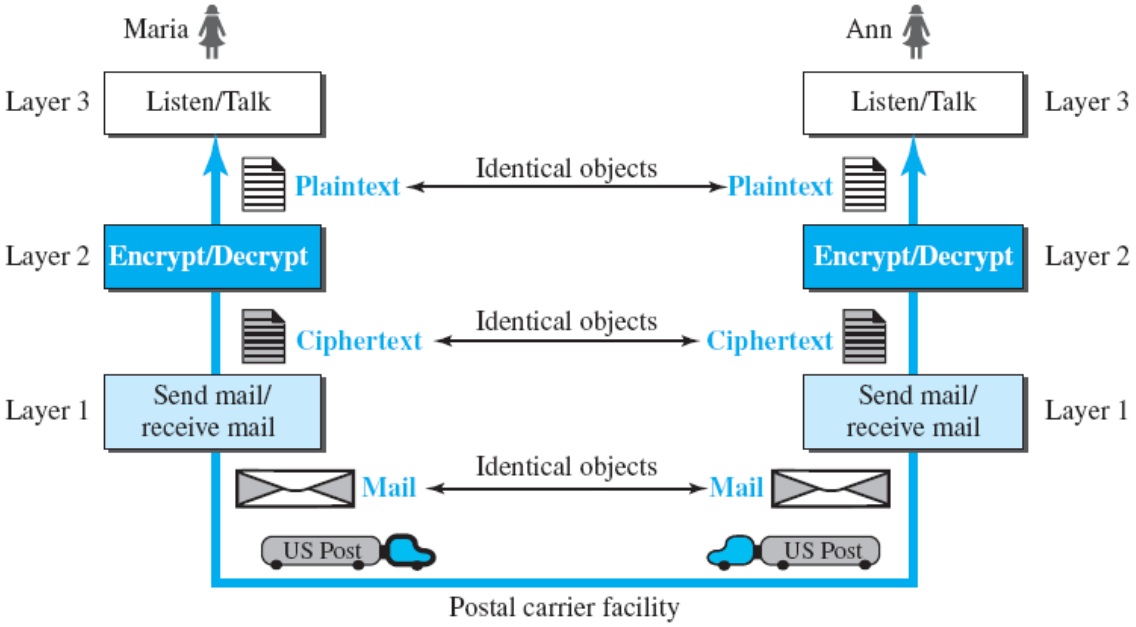
- In networks, communication occurs between the entities (users) in different systems. Two entities cannot just send bit streams to each other and expect to be understood. For communication, the entities must agree on a protocol.
- **Three basic key elements of a protocol**

Syntax: It **defines** about the **structure** or **format of** the **data.** Ex: In a group of data the first 8 bits may be sender address and the second 8 bits may be address of the receiver and the rest may be information or message.

Semantics: It **provides meaning** of each **section of bits**. That is if we consider any particular pattern how that pattern should interpreted and what is the action to be taken for the interpretation. These things will be defined by semantics.

Timing: It defines two characteristics: When data should be sent and how fast they can be sent. **Ex:** If a sender produces data at 100 Mbps, but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and data will be lost.

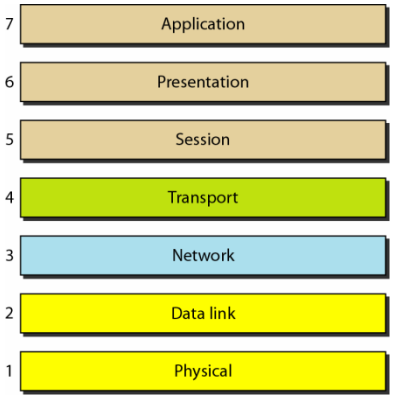
A three-layer Protocol:



OSI Model:

OSI- Open System Inter connection model. It was put forward by ISO.

Need for OSI: To communicate between two different systems without any independent of architecture. It consists of seven layers which are shown in figure below:



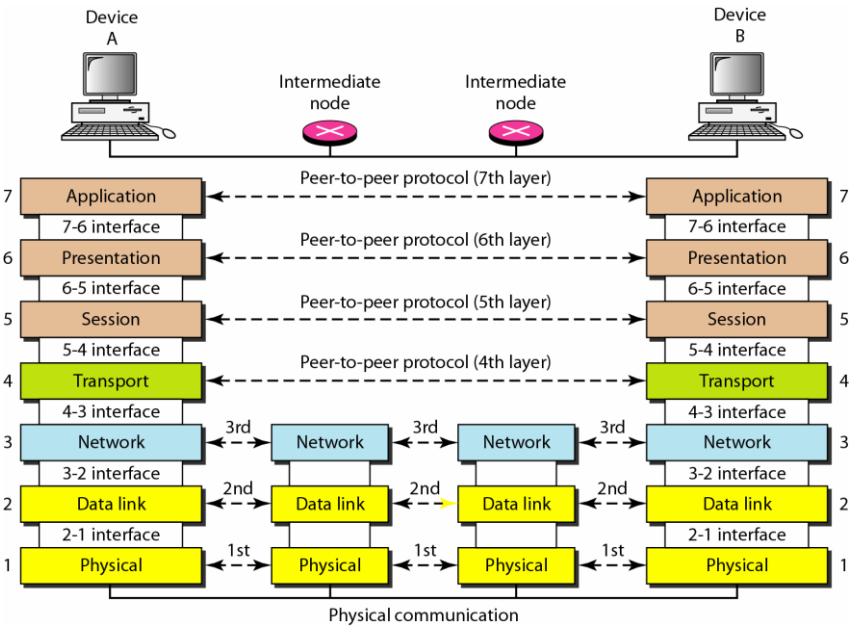
- The bottom most three layers physical data link and network are called network support layers.
- The top most three layers application, presentation and session are called user support layers.
- Transport layer is the one which links the network support layers and the user support layers.
- The upper OSI layers are almost implemented in software, whereas the lower layers are a combination of hardware and software except for the physical layer which is mostly hardware.

Layered architecture:

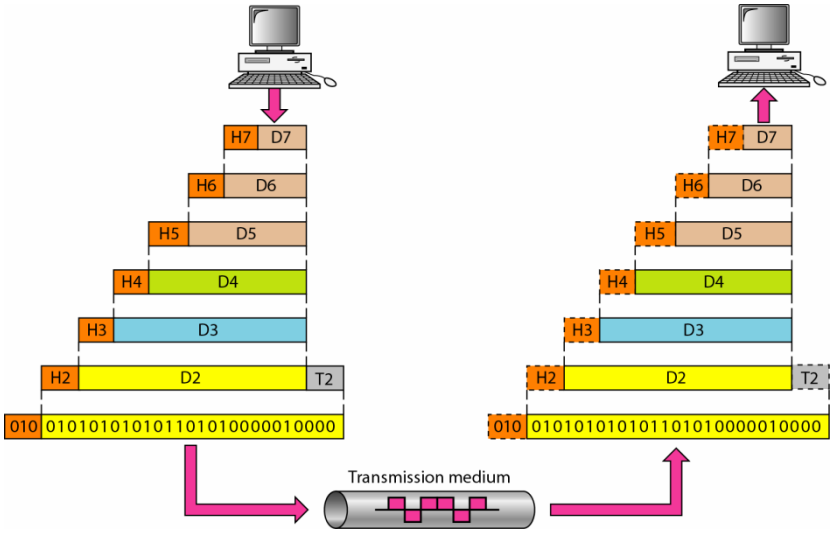
The below figure shows how the message is been transferred from device A to device B. As the message travels from A to B it may pass through many intermediate nodes. These intermediate nodes usually involve only the first three layers of the OSI model.

Peer to peer process:

The processes on each machine that communicate at a given layer are called peer to peer processes.



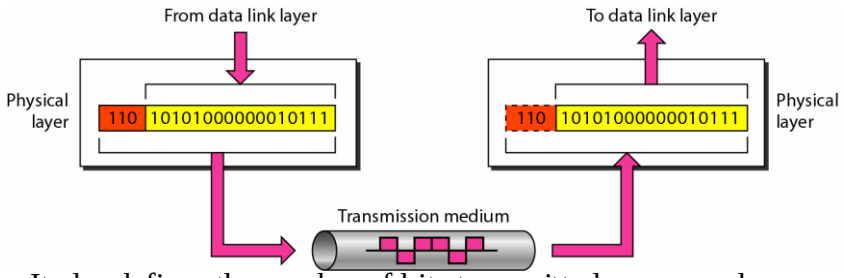
The below figure gives an overall view of the OSI layers. D7 means the data unit at layer 7, D6 means the data unit at layer6 and so on. The process starts at layer 7 (application layer), then moves from layer to layer in descending, sequential order. At each layer a **header** or possibly a **trailer** can be added to the data unit. In general the trailer is added at layer 2 only. When the formatted data unit passes through the physical layer it is changed into an electromagnetic signal and transported along a physical link.



1. PHYSICAL LAYER:

Is **responsible** for **movements** of **individual bits** from one hop (node) to the next. The functions of physical layer are given below:

1. Representation of bits: The physical layer contains a stream of bits. To be transmitted bits must be encoded into signals either electrical or optical. The physical layer defines the type of encoding.



2. Data rate: It also defines the number of bits transmitted per second.

3. Synchronization of bits: The sender and the receiver both should be synchronized at the bit level.

4. Line configuration: It also defines the type of configuration either point to point or multipoint.

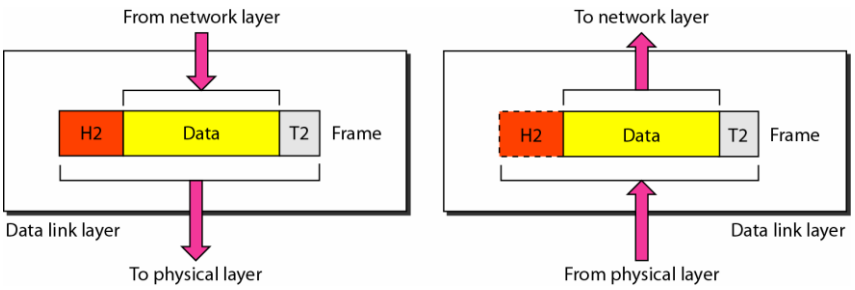
5. Topology: It defines the topology type also either mesh, star, tree or ring topology.

6. Transmission mode: It defines the direction of transmission between two devices (i.e.) simplex, half duplex or full duplex.

2. DATA LINK LAYER:

Is **responsible** for **moving frames** from one hop (node) to the next. The other functions are listed below:

1. **Framing:** The data link layer divides the stream of bits received from the network layer into a number of manageable data units called frames.
2. **Physical addressing:** If the frames are to be distributed to different systems on the network the data link layer adds a header to the frame to define the physical address of the sender and receiver address of the frame.
3. **Flow control:** If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender the data link layer imposes a flow control mechanism to prevent overflow of the receiver.

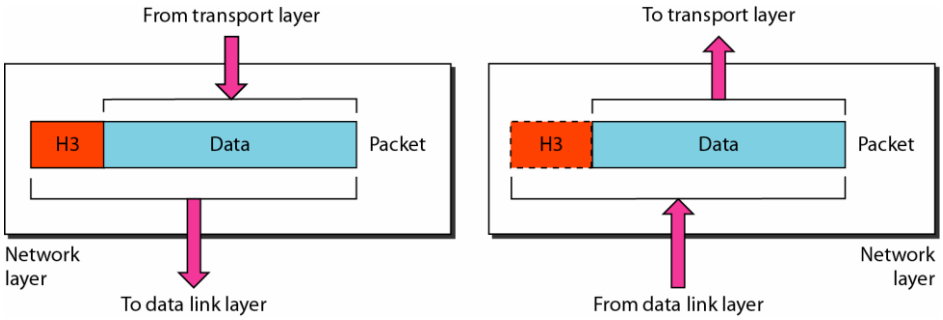


4. **Flow control:** It provides error detection and correction mechanism by retransmitting the damaged or lost frames.

5. **Access control:** When two or more devices are connected to the same link data link layer is used to determine which device has control over the link at a given time.

3. NETWORK LAYER:

Is **responsible** for the **delivery** of **individual packets** from the source host to the destination host. If two systems are connected to the same network then there is no need for network layer whereas if the two systems are connected to different network then network layer is used.

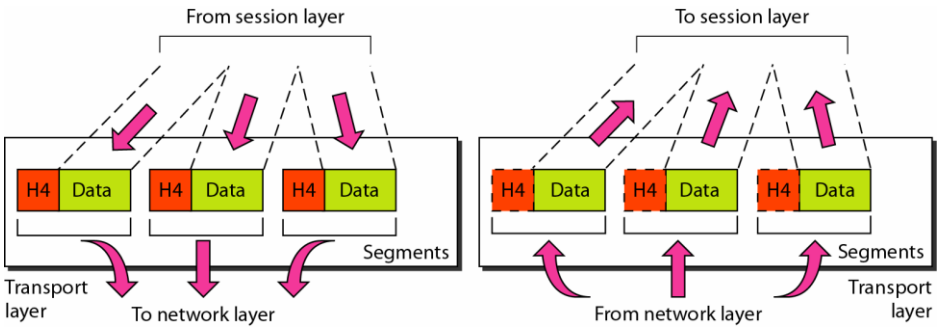


1. Logical addressing: If the packet has to be transferred from one network to another network then address should provide from where the data is coming and where it should reach that address is referred to a logical address.

2. Routing.: When independent networks or links are connected together to from an internetwork (large network) the routing devices like routers or gateways are used to route the packets to their final destination.

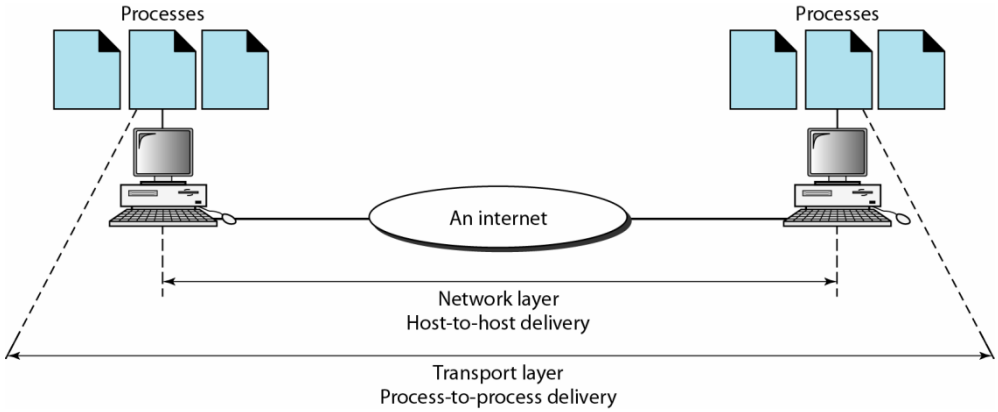
4. TRANSPORT LAYER:

Is responsible for **process to process (end to end) delivery** of the entire message. A process is an application program running on a host. The responsibilities are given below:



1. **Service point addressing:** When the programs which are under process (running program) have to deliver from one system to other system it requires an address to deliver from one system to other it is referred to as service point addressing.
2. **Segmentation and reassembly:** The message is divided into number of segments and for each segment a specific number is allotted. These numbers help for reassembling at the destination and to replace the packets if any is lost.
3. **Connection control:** The transport layer can either connection less or connection oriented. The connection oriented creates a connection before delivering the message and after the message is reached to the destination the connection is terminated.
4. **Flow control:** Similar to data link layer transport layer also provides flow control but here is end to end.
5. **Error control:** It also provides error control functions similar to data link layer but end to end and not a single message.

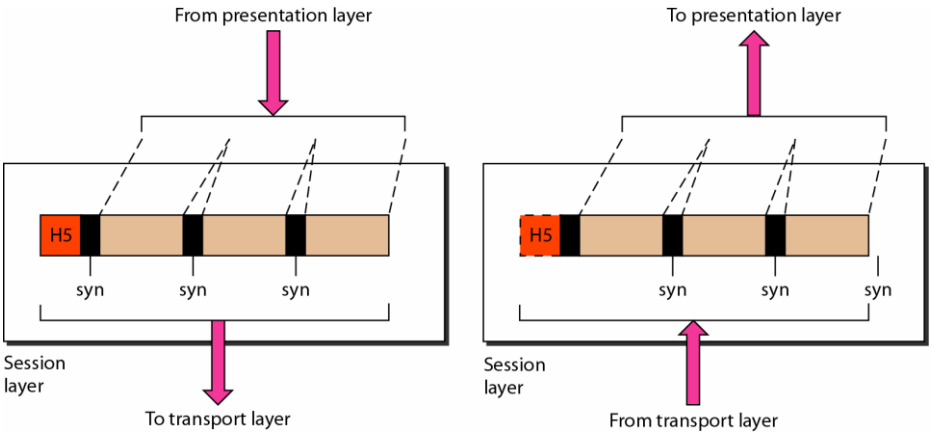
The figure below illustrates the process to process delivery of transport layer:



5. SESSION LAYER:

Is **responsible for dialog control and synchronization.**

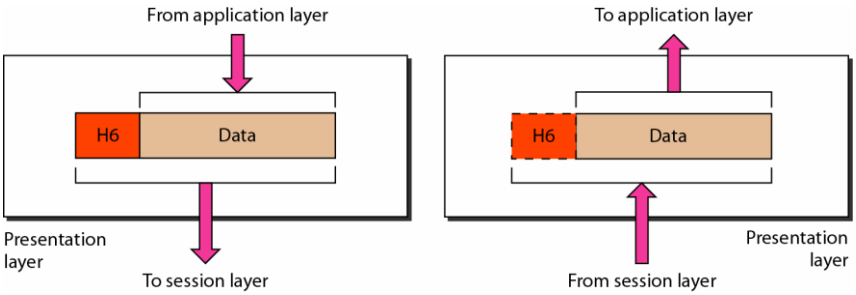
1. **Dialog control:** It allows two systems to communicate either in half duplex or full duplex mode.



2. Synchronization: It introduces **check points** into the stream of data. **Ex:** If a system is sending a file of 2000 pages it is advisable to insert check points after every 100 pages so that to ensure every 100 pages is received and acknowledged independently. In this case if a crash happens during the transmission of page 523 retransmission begins at page 501 only pages 1 to 500 need not be retransmitted again.

6. PRESENTATION LAYER: It deals with syntax and semantics of the information exchanged between two systems. The presentation layer is **responsible** for **translation, compression and encryption.**

1. Translation: Before transferring the message from source to destination the message is converted into stream of bits and then transmitted. (i.e.) in translation layer the message is converted to common format at the transmitter and at the receiver the common format is converted to receiver dependent format.

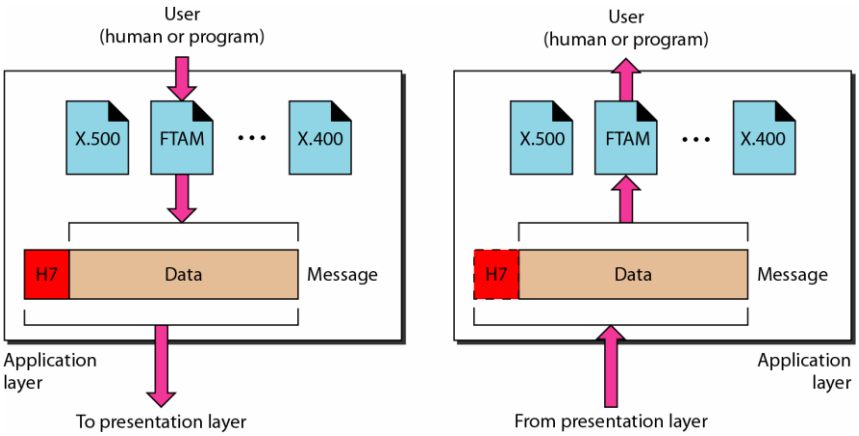


2. Encryption: To carry sensitive information the system should provide privacy; it is achieved by encryption technique at the sender.

3. Compression: Data compression it reduces the number of bits to be transmitted. Data compression is important in transmission of multimedia such as text, audio and video.

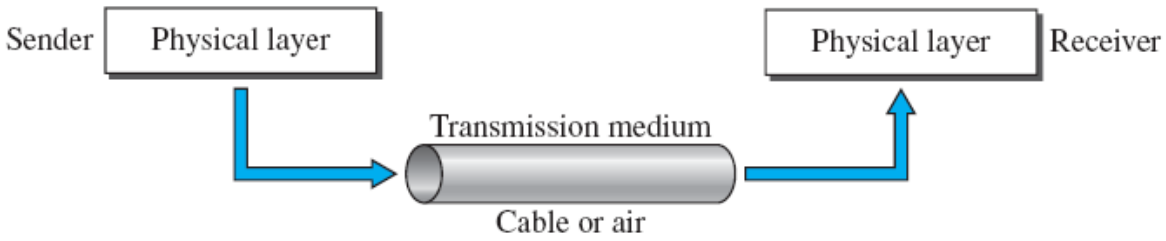
7. APPLICATION LAYER:

Is **responsible for providing services to** the **user.** The major functions are FTAM, Network virtual terminal and mail services.



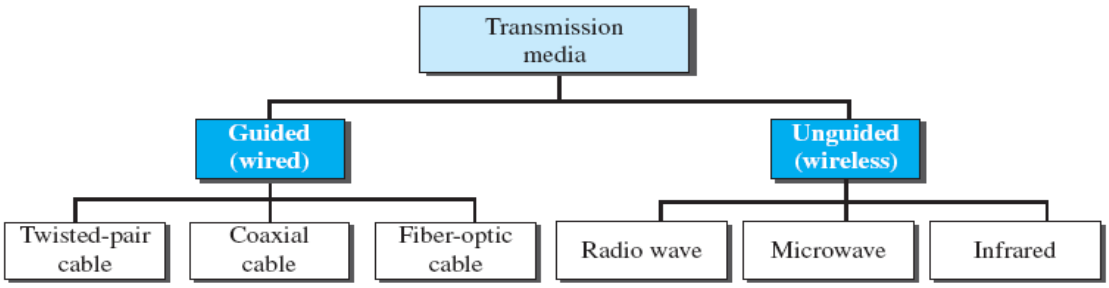
1. **Network virtual terminal:** It is a software version allows a user to log on to remote host. To do this the application layer creates a software terminal at the remote host. The users computers talk to the software terminal which in turn, talks to the host and vice versa.
2. **File transfer access and management (FTAM):** This allows the files to access at remote computer and to retrieve the files at the remote computer also.
3. **Mail services:** It provides application for email forwarding and storage.

Physical Layer



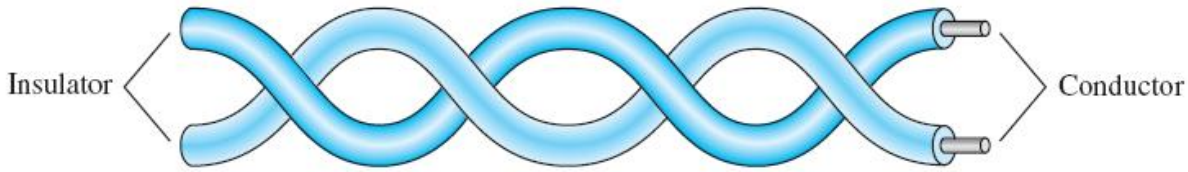
A **transmission medium** can be broadly defined as anything that can carry information from a source to a destination. For example, the transmission medium for two people having a dinner conversation is the air. The air can also be used to convey the message in a smoke signal or semaphore. For a written message, the transmission medium might be a mail carrier, a truck, or an airplane.

In data communications the definition of the information and the transmission medium is more specific. The transmission medium is usually free space, metallic cable, or fiber-optic cable. The information is usually a signal that is the result of a conversion of data from another form.



Guided media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable.

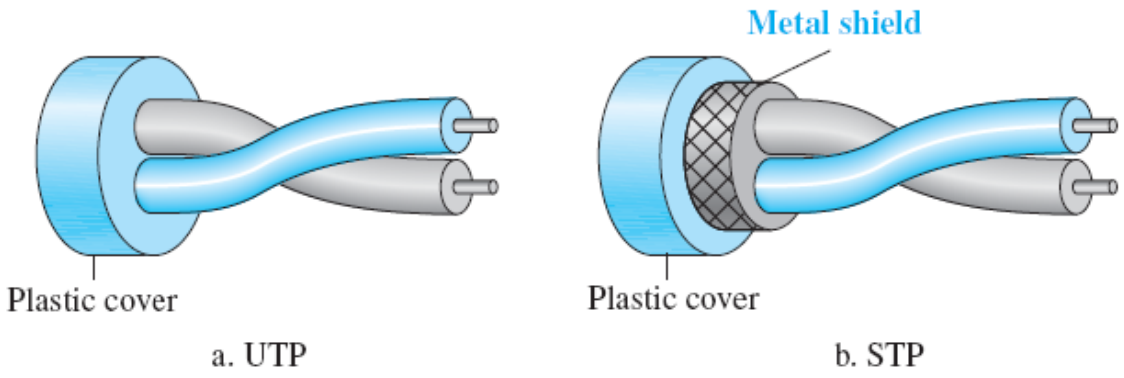
Twisted-pair cable



One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two. In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals.

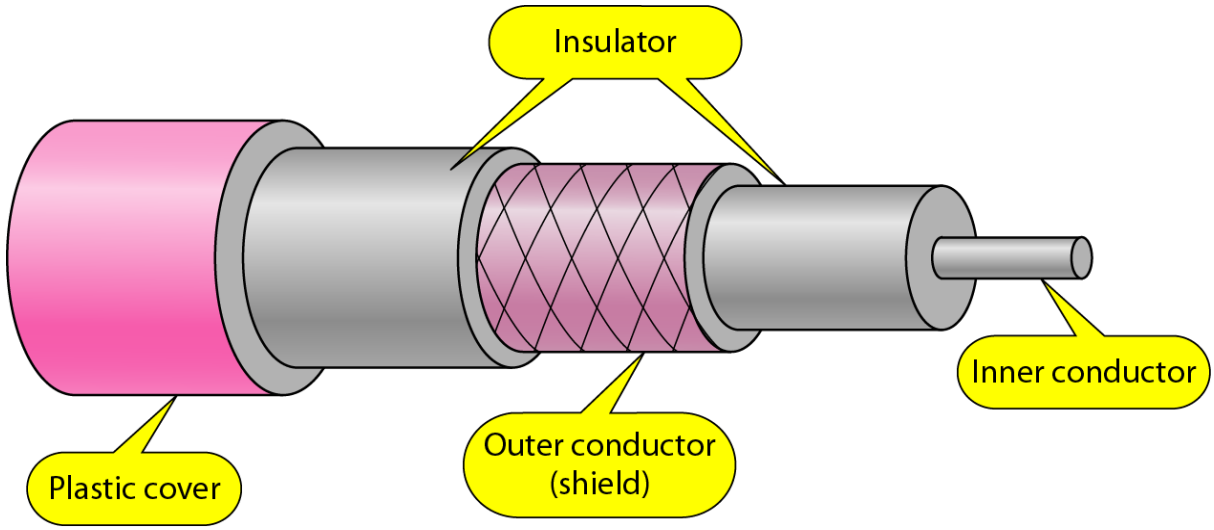
If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relative to the noise or crosstalk sources (e.g., one is closer and the other is farther). This results in a difference at the receiver.

Unshielded Versus Shielded Twisted-Pair Cable



Category	*Specification*	*Data Rate (Mbps)*	*Use*
1	Unshielded twisted-pair used in telephone	< 0.1	Telephone
2	Unshielded twisted-pair originally used in T-lines	2	T-1 lines
3	Improved CAT 2 used in LANs	10	LANs
4	Improved CAT 3 used in Token Ring networks	20	LANs
5	Cable wire is normally 24 AWG with a jacket and outside sheath	100	LANs
5E	An extension to category 5 that includes extra features to minimize the crosstalk and electromagnetic interference	125	LANs
6	A new category with matched components coming from the same manufacturer. The cable must be tested at a 200-Mbps data rate.	200	LANs
7	Sometimes called SSTP (shielded screen twisted-pair). Each pair is individually wrapped in a helical metallic foil followed by a metallic foil shield in addition to the outside sheath. The shield decreases the effect of crosstalk and increases the data rate.	600	LANs

Coaxial cable



Categories of coaxial cables

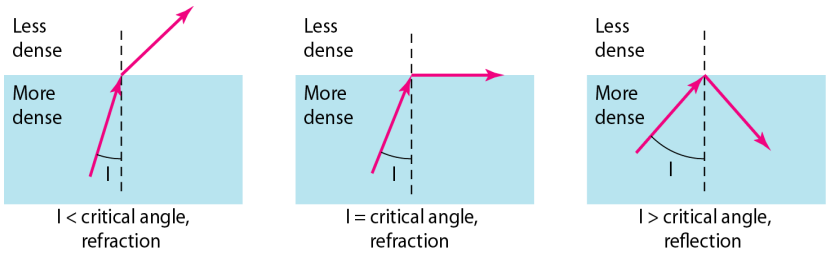
Category	*Impedance*	*Use*
RG-59	75 Ω	Cable TV
RG-58	50 Ω	Thin Ethernet
RG-11	50 Ω	Thick Ethernet

Coaxial cable (or *coax*) carries signals of higher frequency ranges than those in twisted pair cable, in part because the two media are constructed quite differently. Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two. The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit.

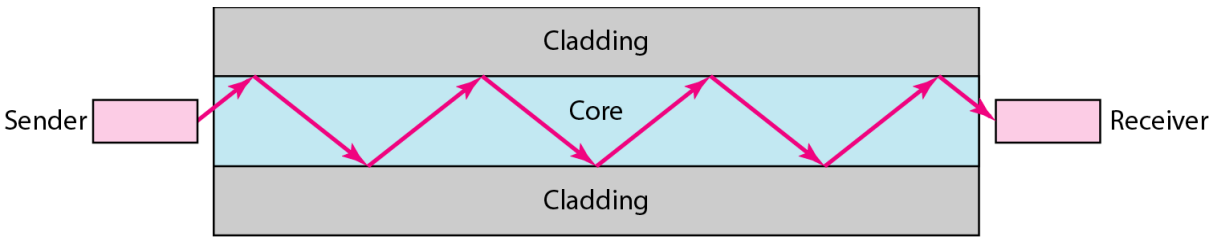
Fiber-optic Cable:

A fiber-optic cable is made of glass or plastic and transmits signals in the form of light. To understand optical fiber, we first need to explore several aspects of the nature of light.

Light travels in a straight line as long as it is moving through a single uniform substance. If a ray of light traveling through one substance suddenly enters another substance (of a different density), the ray changes direction.

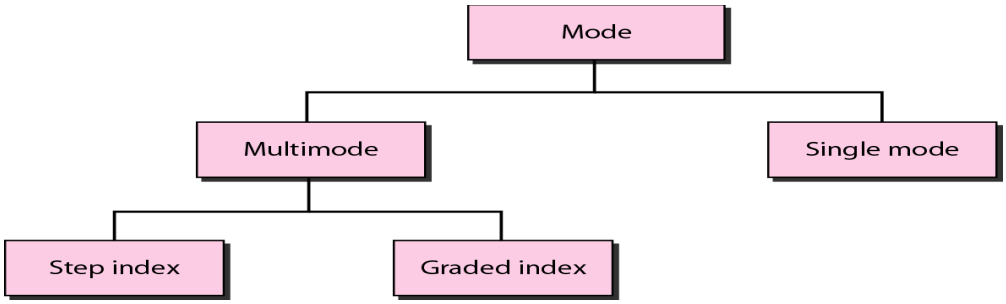


Optical fibers use reflection to guide light through a channel. A glass or plastic **core** is surrounded by a **cladding** of less dense glass or plastic. The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.

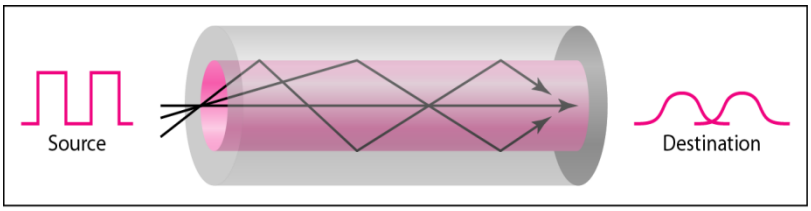


Propagation Modes

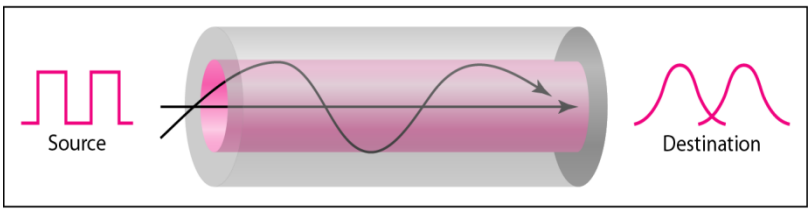
Current technology supports two modes (multimode and single mode) for propagating light along optical channels, each requiring fiber with different physical characteristics. Multimode can be implemented in two forms: step-index or graded-index.



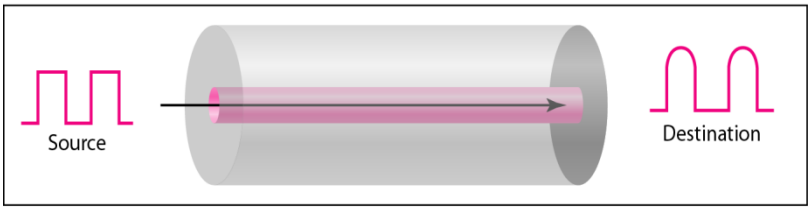
Modes



a. Multimode, step index



b. Multimode, graded index



c. Single mode

Advantages and Disadvantages of Optical Fiber

Advantages

Fiber-optic cable has several advantages over metallic cable (twisted-pair or coaxial).

- ✓ **Higher bandwidth.** Fiber-optic cable can support dramatically higher bandwidths (and hence data rates) than either twisted-pair or coaxial cable. Currently, data rates and bandwidth utilization over fiber-optic cable are limited not by the medium but by the signal generation and reception technology available.
- ✓ **Less signal attenuation.** Fiber-optic transmission distance is significantly greater than that of other guided media. A signal can run for 50 km without requiring regeneration. We need repeaters every 5 km for coaxial or twisted-pair cable.

- ✓ **Immunity to electromagnetic interference.** Electromagnetic noise cannot affect fiber-optic cables.
- ✓ **Resistance to corrosive materials.** Glass is more resistant to corrosive materials than copper.
- ✓ **Light weight.** Fiber-optic cables are much lighter than copper cables.
- ✓ **Greater immunity to tapping.** Fiber-optic cables are more immune to tapping than copper cables. Copper cables create antenna effects that can easily be tapped.

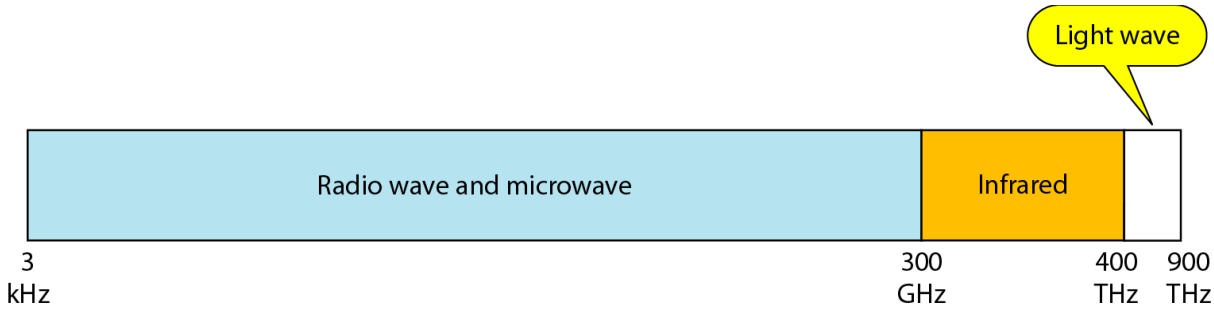
Disadvantages

There are some disadvantages in the use of optical fiber.

- ➢ **Installation and maintenance.** Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.
- ➢ **Unidirectional light propagation.** Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.
- ➢ **Cost.** The cable and the interfaces are relatively more expensive than those of other guided media. If the demand for bandwidth is not high, often the use of optical fiber cannot be justified.

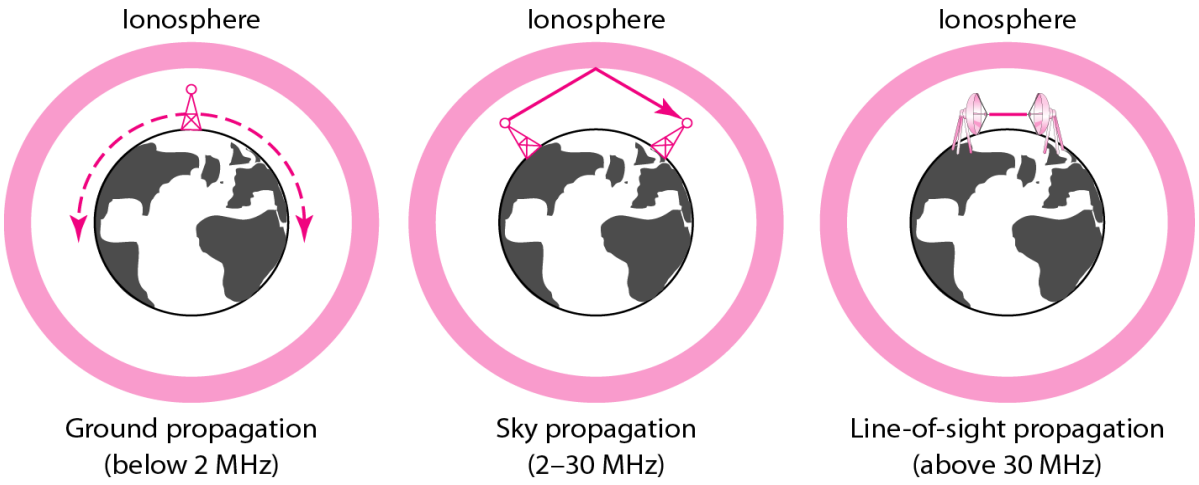
UNGUIDED MEDIA: WIRELESS

Unguided medium transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as ***wireless communication.*** Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.

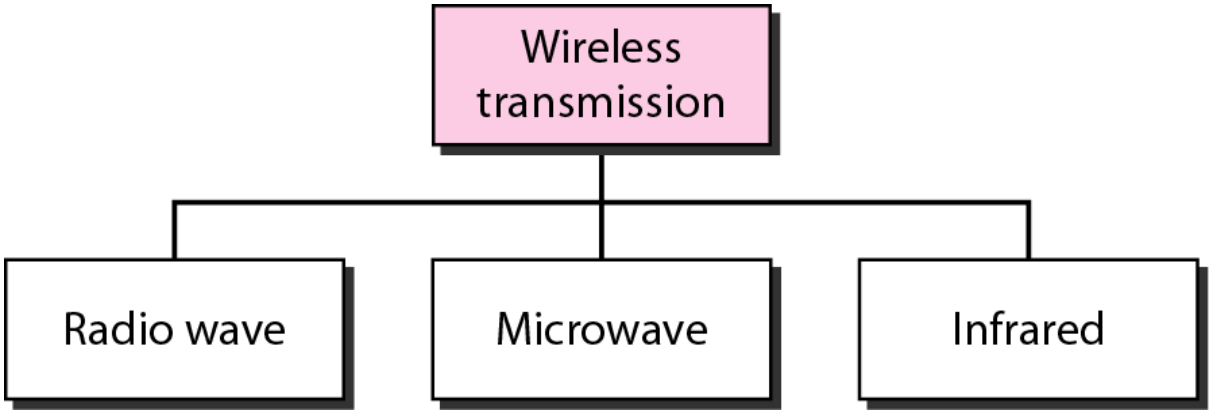


Electromagnetic spectrum for wireless communication

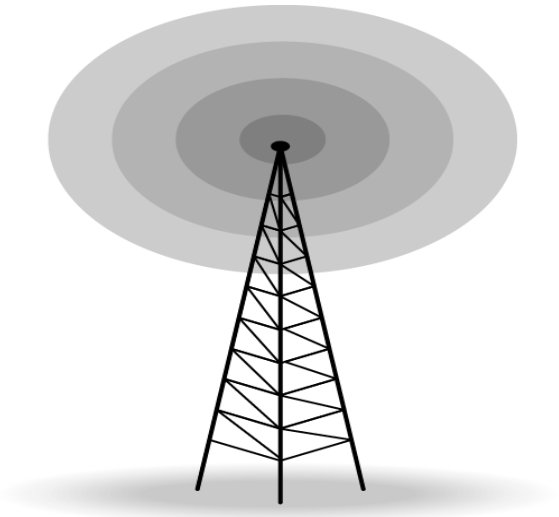
Propagation methods



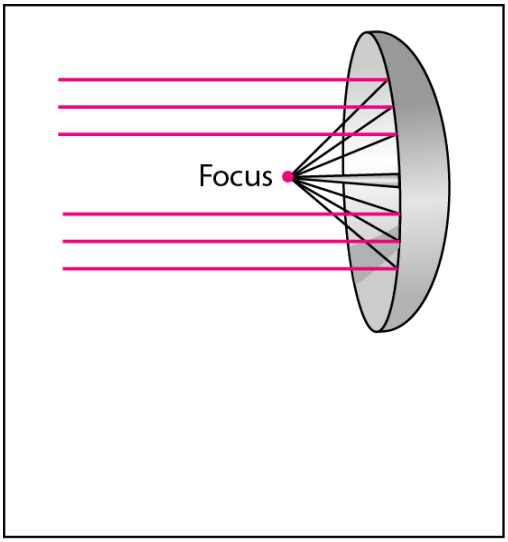
Wireless transmission waves



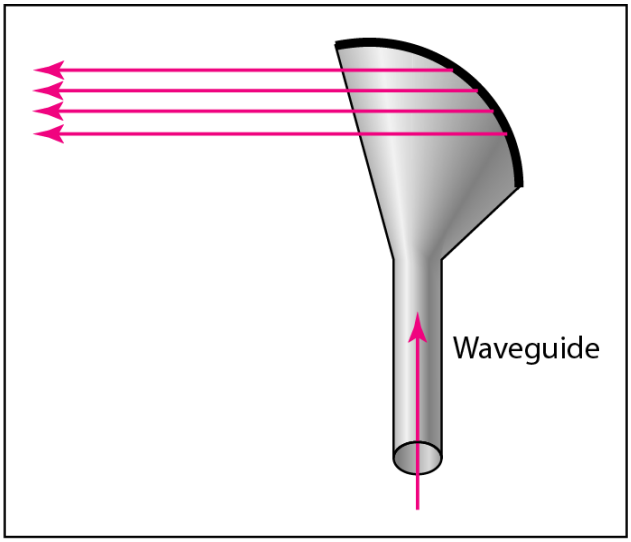
Radio waves are used for multicast communications, such as radio and television, and paging systems. They can penetrate through walls. Highly regulated. Use omni directional antennas



Microwaves are used for unicast communication such as cellular telephones, satellite networks, and wireless LANs. Higher frequency ranges cannot penetrate walls. Use directional antennas - point to point line of sight communications.



a. Dish antenna



b. Horn antenna

Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.

Overview of Data and Signals

Data can be analog or digital. The term analog data refers to information that is continuous; digital data refers to information that has discrete states. Analog data take on continuous values. Digital data take on discrete values.

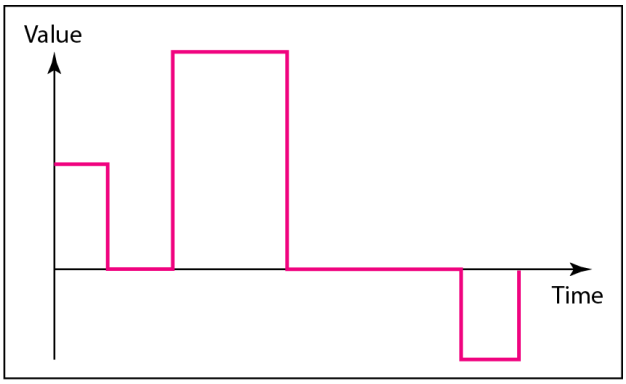
Analog and Digital Data

- Data can be analog or digital.
- Analog data are continuous and take continuous values.
- Digital data have discrete states and take discrete values.

Analog and Digital Signals

- Signals can be analog or digital.
- Analog signals can have an infinite number of values in a range.
- Digital signals can have only a limited number of values.

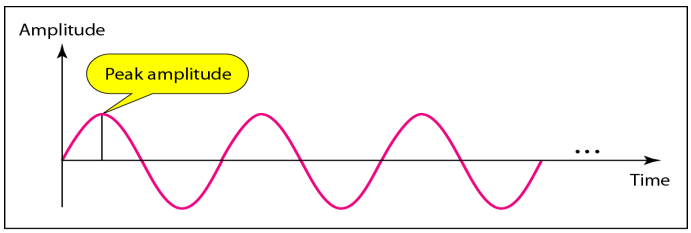
a. Analog signal



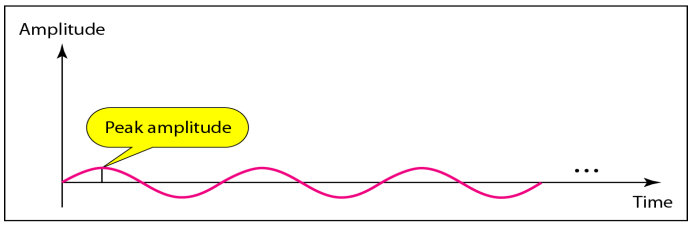
b. Digital signal

PERIODIC ANALOG SIGNALS

In data communications, we commonly use periodic analog signals and nonperiodic digital signals. Periodic analog signals can be classified as simple or composite. A simple periodic analog signal, a sine wave, cannot be decomposed into simpler signals. A composite periodic analog signal is composed of multiple sine waves.

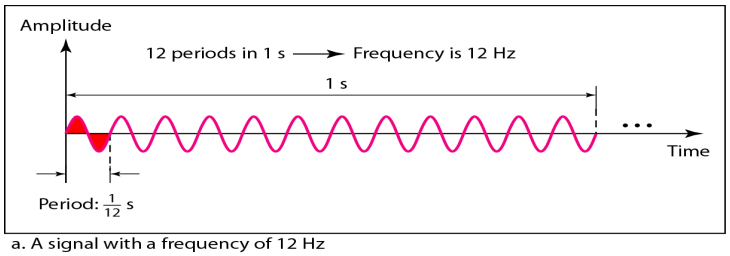


a. A signal with high peak amplitude

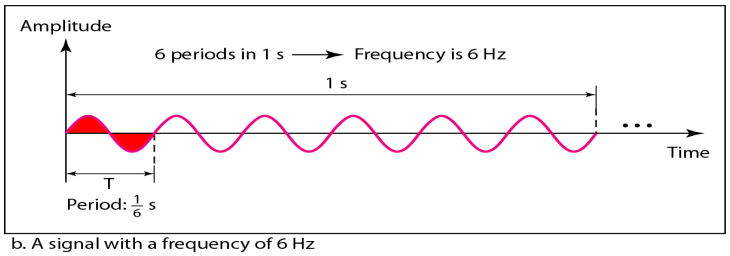


b. A signal with low peak amplitude

Frequency and period are the inverse of each other. $f = \frac{1}{T}$ and $T = \frac{1}{f}$



a. A signal with a frequency of 12 Hz



b. A signal with a frequency of 6 Hz

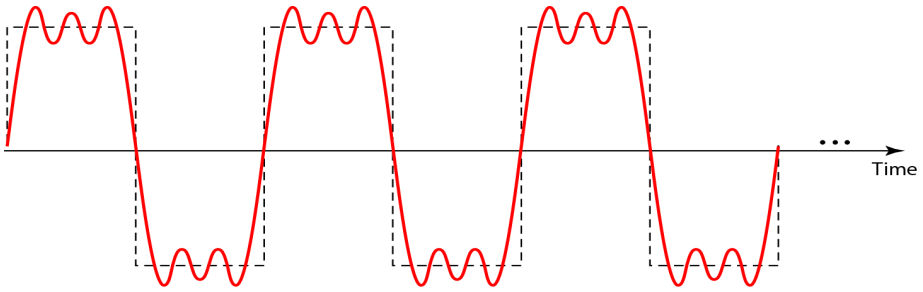
Unit	*Equivalent*	*Unit*	*Equivalent*
Seconds (s)	1 s	Hertz (Hz)	1 Hz
Milliseconds (ms)	10^{-3} s	Kilohertz (kHz)	10^{3} Hz
Microseconds (μs)	10^{-6} s	Megahertz (MHz)	10^{6} Hz
Nanoseconds (ns)	10^{-9} s	Gigahertz (GHz)	10^{9} Hz
Picoseconds (ps)	10^{-12} s	Terahertz (THz)	10^{12} Hz

Signals and Communication

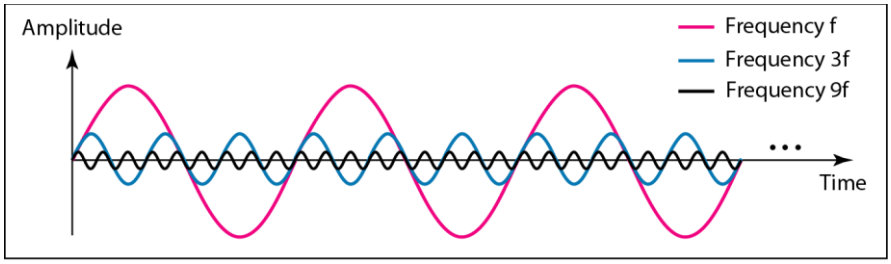
- A single-frequency sine wave is not useful in data communications
- We need to send a composite signal, a signal made of many simple sine waves.
- According to Fourier analysis, any composite signal is a combination of simple sine waves with different frequencies, amplitudes, and phases

Composite Signals and Periodicity

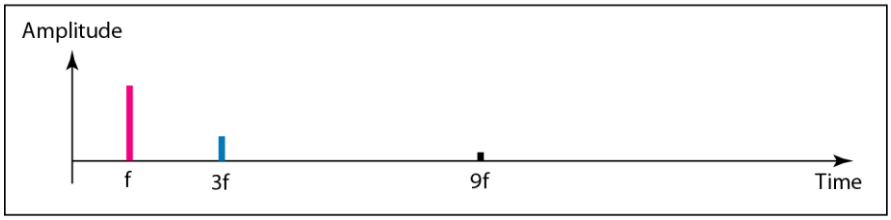
- If the composite signal is periodic, the decomposition gives a series of signals with discrete frequencies.
- If the composite signal is nonperiodic, the decomposition gives a combination of sine waves with continuous frequencies.



Decomposition of a composite periodic signal in the time and frequency domains



a. Time-domain decomposition of a composite signal



b. Frequency-domain decomposition of the composite signal

Introduction to Data Link Layer

HDLC Frame Types:

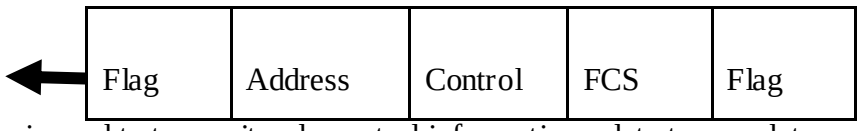
It has three types of frames

- Information frame
- Supervisory frame
- Unnumbered frame

Information frame (I – frame): -

❖ I – frame is used to transport user data and control information relating to user data.

Supervisory frame (S – frame): -

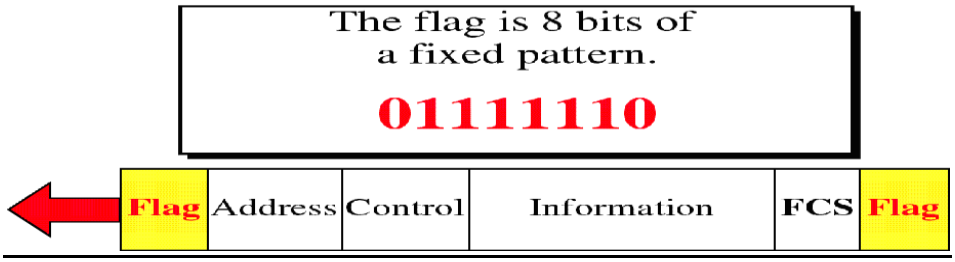


❖ S – Frame is used to transmit only control information relate to user data.

Unnumbered frame (U – frame): -

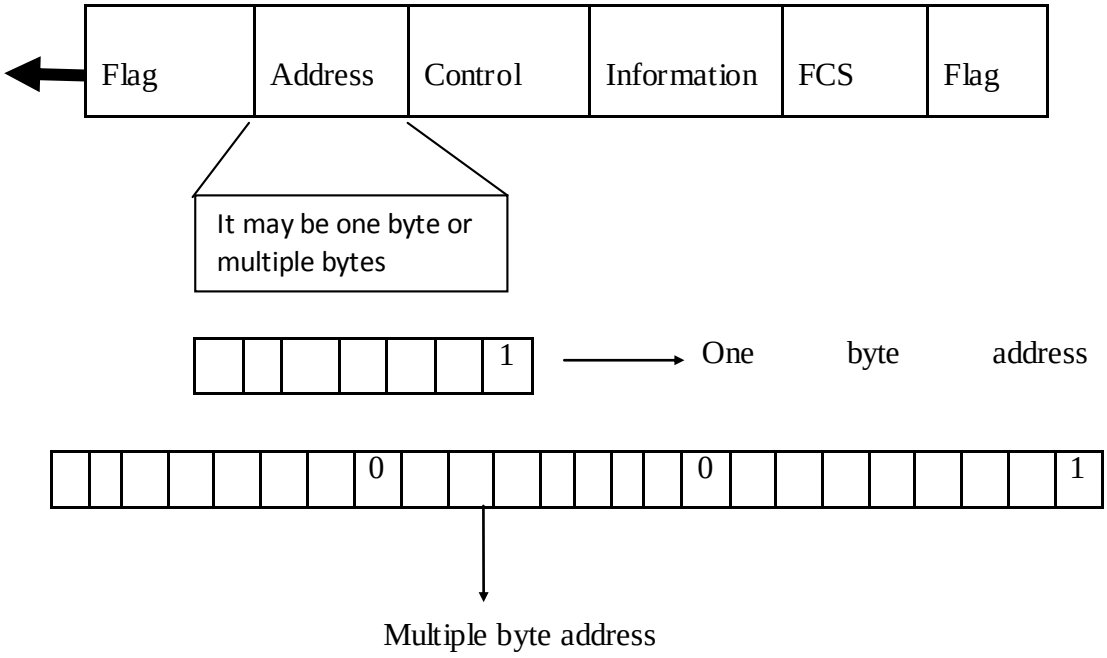
❖ U – Frame carries management information used for managing the network and it may or may not be present.

Flag field: -



- An HDLC frame contains two flag field. i.e. at the beginning and ending of the frame.
- So it provides synchronization pattern for the receiver.
- The eight bit sequence of the flag field is 0111 1110. So when a receiver identifies these bits it takes it as a flag field.
- But in this case we are having another problem as, when these bits come into data unit, the receiver takes it as flag field.
- Here the ending flag is the beginning of next frame.
- The problem of data transparency is solved. By using bit stuffing method.

Address field:

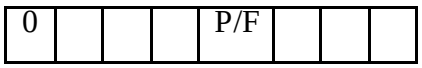


- In one byte address the last bit will be '1' always.
- In case of multiple bytes, the intermediate byte will be zero. And the last byte will be '1'.
- The address field is the 2nd field in HDLC frame format.

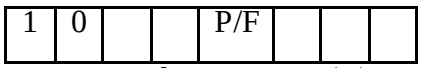
HDLC control Field:

- Control field also contains one byte, if requires two byte control field.
- Control field is separate for every frame.

I - frame

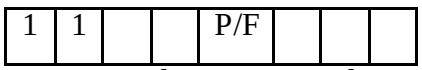


S - frame



Code	Command
00	RR Receive ready
01	REJ Reject
10	RNR Receive not ready
11	SREJ Selective-reject

U - frame



Code		Command	Response
00	001	SNRM	
11	011	SNRME	
11	000	SARM	DM
11	010	SARME	
11	100	SABM	
11	110	SABME	
00	000	UI	UI
00	110		UA
00	010	DISC	RD
10	000	SIM	RIM
00	100	UP	
11	001	RSET	
11	101	XID	XID
10	001		FRMR

P/F – poll / final bit

N(S) – sequence number of frame of frame sent

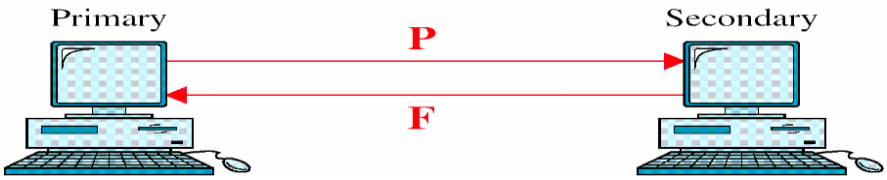
N(R) – sequence number of next frame expected

Code – code for supervisory or unnumbered frame

- If the **control field first bit** is **1 then** it is **I – frame.**
- In I – frame contains a 3 – bit flow and error control sequence called N(S) and N(R). N(S) specifies the number of the frame being sent. (Its own identifying number). N(R) indicates the number of frame expected i.e. it is acknowledgement field.
- If last frame received is error free then N(R) will be number of next frame expected. If it is damaged then N(R) will be the number of the same frame.
- If the **1st bit is 1 and second bit is 0 in** a **control field, it is S – frame**.

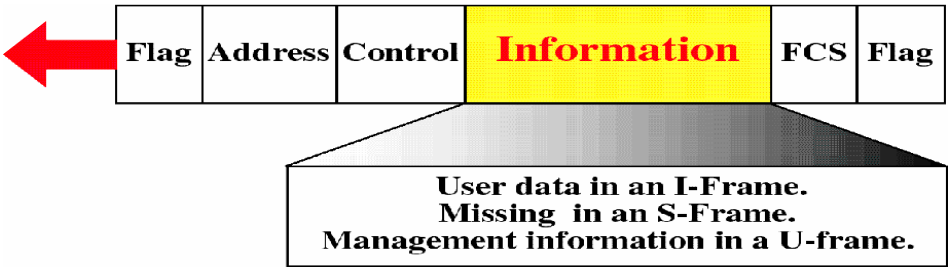
- The s – frame contain only N(R), not N(S), because S-frame is not consisting of an any data.
- S – Frame consists of a code (2 bit) which is used to carry error control information.
- **U –frame contains** the **first and second bit as 1.** i.e. both bits are '1'. It contains a two bit code and a 3 bit code.
- These codes are used to identify the type of U – frame and its function.
- All frames in control field use a one bit (P/F) bit which is poll /final bit. It is enabled only when (P/F) is '1'.

Poll/Final:



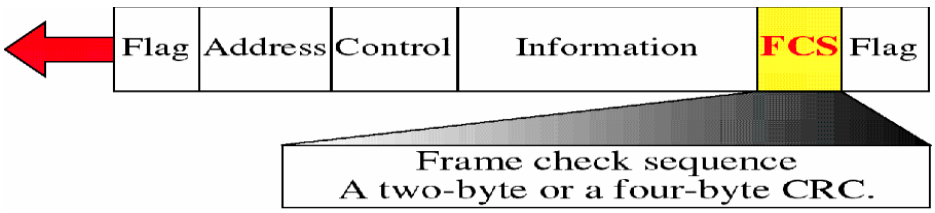
- Poll means the primary sends the frame to secondary.
- Final means the transmission of frame from secondary to primary.
- Depending upon the poll or final bit the transmission is occurred, in poll mode.
- We are having codes in s frame and u frame.
- In s frame we are having a 2 bit code. And for every code we are having a command.

Information Field:



- It contains user data in I – frame
- It does not exist in s – frame it contain management information in U – frame.
- Combining the data to be sent with control information is called as piggy backing.

FCS Field:



- Frame check sequence is the error detection field in HDLC frame.
- It may be either two – or – four byte CRC.
- In select response mode, the frame is set from primary to secondary.

The two main functions of the data link layer are :-
1-data link control (deals with the design and procedures for communication between two adjacent nodes: node-to-node communication).
2- media access control (deals how share the link).

Data link control functions include framing, flow and error control, and software implemented protocols that provide smooth and reliable transmission of frames between nodes.
To implement data link control, we need protocols.
protocol :- is a set of rules that need to be implemented in software and run by the two nodes involved in data exchange at the data link layer.

FRAMING

The data link layer needs to pack bits into frames, so that each frame is distinguishable from another. Our postal system practices a type of framing. The simple act of inserting a letter into an envelope separates one piece of information from another; the envelope serves as the delimiter.

Fixed-Size Framing – no boundaries for frames, size used as the delimeter
Variable-Size Framing – define begining and end of frame, character oriented or bit oriented approach

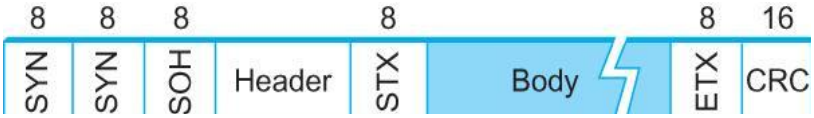
Framing in the data link layer separates a message from one source to a destination, or from other messages to other destinations, by adding a sender address and a destination address. The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt.

BYTE-ORIENTED PROTOCOLS

. The two different approaches are sentinel and the byte-counting.

Sentinel approach

Binary Synchronous Communication (BISYNC) protocol developed by IBM.



SYN-special synchronization bits indicating beginning of the frame

SOH-special sentinel character that indicates start of header

Header contains physical address of source, destination and other information

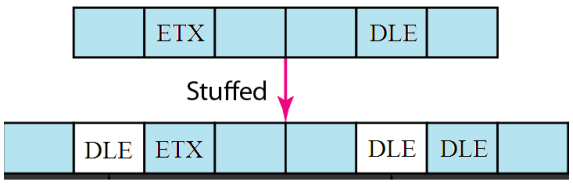
STX special sentinel character that indicates start of text/body

ETX special sentinel character that indicates end of text/body

CRC 16- bit code used to detect transmission error

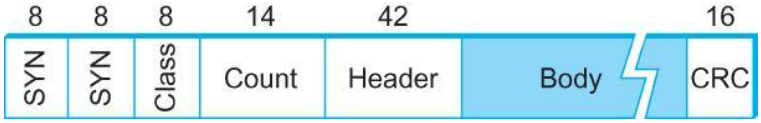
Character stuffing

- The problem with sentinel approach, is that the ETX character might appear in the data.
- In such case, ETX is preceded with a DLE (data-link-escape) character.
- If the data portion contains escape character, then it is preceded by another DLE.
- The insertion of DLE character onto the data is known as character stuffing.
- The receiver removes the additional escape characters and correctly interprets the frame.
- If ETX field is corrupted, then it is known as framing error. Such frames are discarded.



Byte-Counting Approach

- An alternative to detect end-of-frame is to include number of bytes in the frame body as part of the frame header.
- Digital Data Communication Message Protocol (DDCMP) uses the count approach.



- The Count field specifies how many bytes are contained in the frame's body.

- If Count field is corrupted, then it is known as framing error. The receiver comes to know of it when it comes across the SYN field of the next frame.

BIT-ORIENTED PROTOCOL

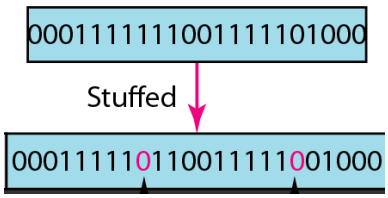
The bit-oriented protocols such as High-Level Data Link Control (HDLC) view the frame as a collection of bits. The frame format is given below:

The beginning and end of a frame has a distinguished bit sequence 01111110. Sequence is also transmitted when link is idle for synchronization

Bit Stuffing

- To prevent occurrence of bit pattern 01111110 as part of frame body, bit stuffing is used. In bit stuffing, if a 0 and five consecutive 1 bits are encountered, an extra 0 is added. This extra stuffed bit is eventually removed from the data by the receiver.
- The real flag 01111110 is not stuffed by the sender and is recognized by the receiver

If a bit such as 01111111 arrives, then an error has occurred and the frame is discarded.



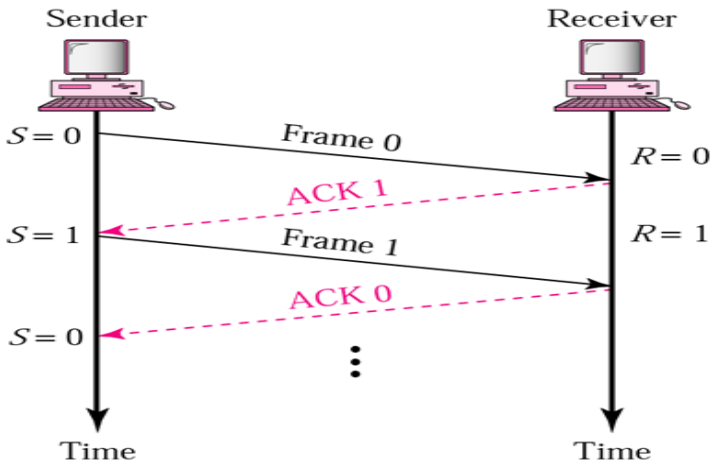
Flow Control Mechanism

- Flow control coordinates the amount of data that can be sent before receiving acknowledgement
- It is one of the most important functions of data link layer.
- Flow control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgement from the receiver.
- Receiver has a limited speed at which it can process incoming data and a limited amount of memory in which to store incoming data.
- Receiver must inform the sender before the limits are reached and request that the transmitter to send fewer frames or stop temporarily.
- Since the rate of processing is often slower than the rate of transmission, receiver has a block of memory (buffer) for storing incoming data until they are processed.

Various Flow Control Mechanisms

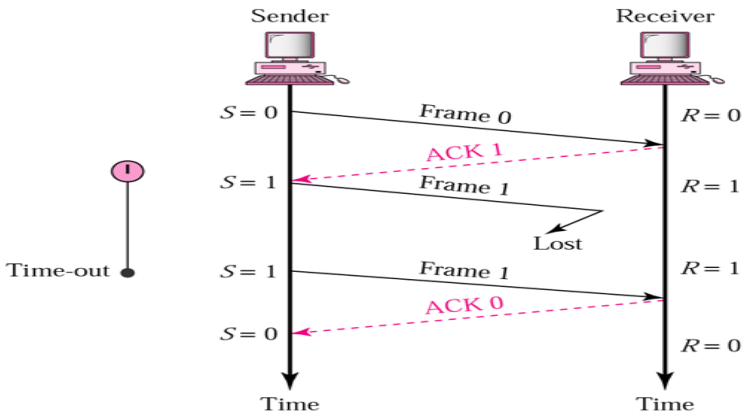
- Stop-and-Wait
- Go-Back-N ARQ
- Selective-Repeat ARQ

Stop-and-Wait



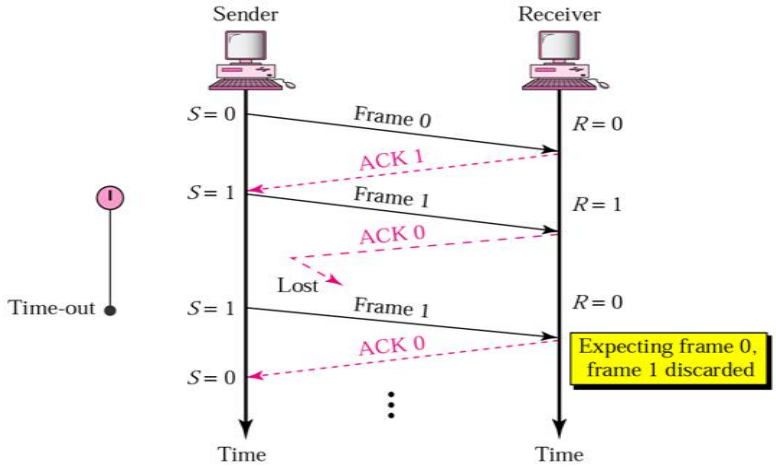
- Sender keeps a copy of the last frame until it receives an acknowledgement.
- For identification, both data frames and acknowledgements (ACK) frames are numbered alternatively 0 and 1.
- Sender has a control variable (S) that holds the number of the recently sent frame. (0 or 1)
- Receiver has a control variable ® that holds the number of the next frame expected (0 or 1).
- Sender starts a timer when it sends a frame. If an ACK is not received within a allocated time period, the sender assumes that the frame was lost or damaged and resends it
- Receiver send only positive ACK if the frame is intact.
- ACK number always defines the number of the next expected frame.

Stop-and-Wait ARQ, lost ACK frame



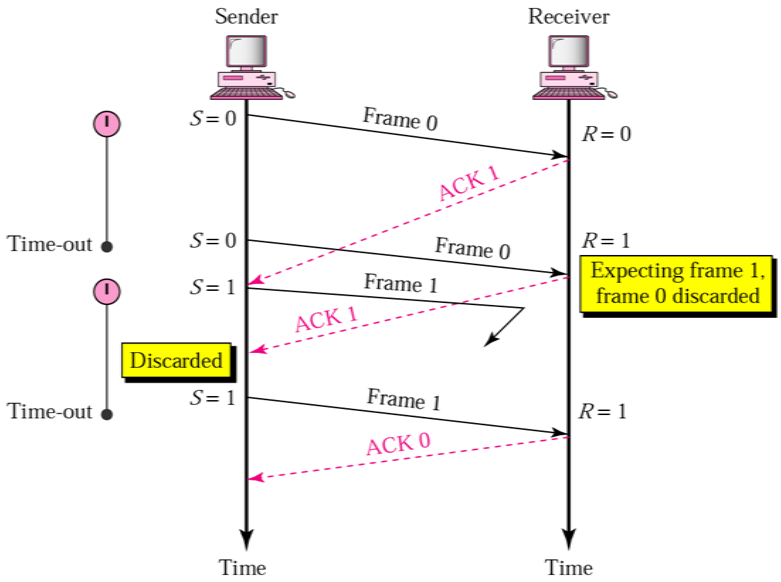
- When a receiver receives a damaged frame, it discards it and keeps its value of R.
- After the timer at the sender expires, another copy of frame 1 is sent.

Stop-and-Wait, lost ACK frame



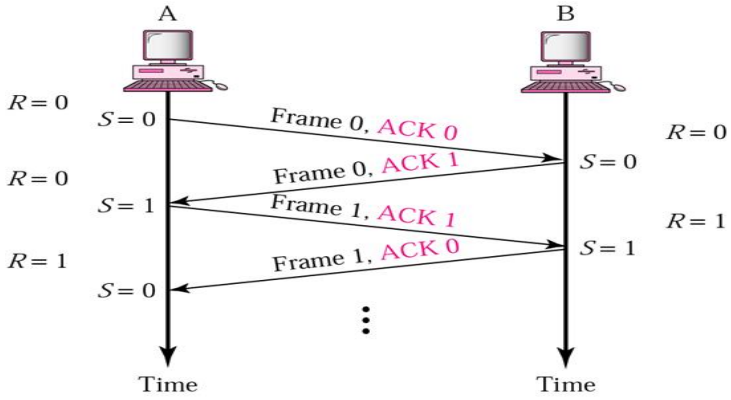
- If the sender receives a damaged ACK, it discards it.
- When the timer of the sender expires, the sender retransmits frame 1.
- Receiver has already received frame 1 and expecting to receive frame 0 (R=0). Therefore it discards the second copy of frame 1.

Stop-and-Wait, delayed ACK frame



- The ACK can be delayed at the receiver or due to some problem
- It is received after the timer for frame 0 has expired.
- Sender retransmitted a copy of frame 0. However, R =1 means receiver expects to see frame 1. Receiver discards the duplicate frame 0.
- Sender receives 2 ACKs, it discards the second ACK.

Piggybacking



- A method to combine a data frame with ACK.
- Station A and B both have data to send.
- Instead of sending separately, station A sends a data frame that includes an ACK.
- Station B does the same thing.
- Piggybacking saves bandwidth.

Disadvantage of Stop-and-Wait

- In stop-and-wait, at any point in time, there is only one frame that is sent and waiting to be acknowledged.
- This is not a good use of transmission medium.
- To improve efficiency, multiple frames should be in transition while waiting for

ACK.

Two protocol overcome the above drawback

- Go-Back-N ARQ

  Selective Repeat ARQ

Go-Back-N ARQ

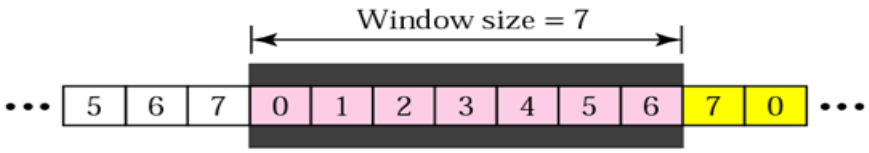
- We can send up to W frames before worrying about ACKs.
- We keep a copy of these frames until the ACKs arrive.
- This procedure requires additional features to be added to Stop-and-Wait ARQ.

Sequence Numbers

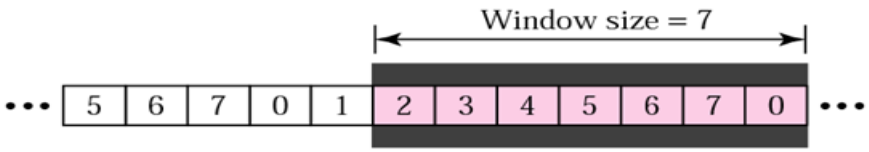
- Frames from a sender are numbered sequentially.
- We need to set a limit since we need to include the sequence number of each frame in the header.
- If the header of the frame allows m bits for sequence number, the sequence numbers range from 0 to $2^m - 1$. for m = 3, sequence numbers are: 1, 2, 3, 4, 5, 6, 7.
- We can repeat the sequence number.
- Sequence numbers are:

  0, 1, 2, 3, 4, 5, 6, 7, 0, 1, 2, 3, 4, 5, 6, 7, 0, 1, …

Sender Sliding Window



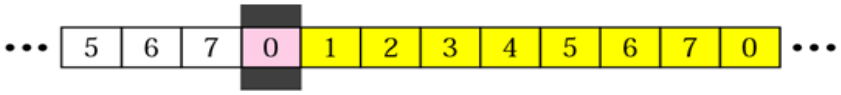
a. Before sliding



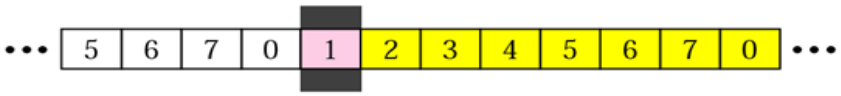
b. After sliding two frames

- At the sending site, to hold the outstanding frames until they are acknowledged, we use the concept of a window.
- The size of the window is at most 2^m -1 where m is the number of bits for the sequence number.
- Size of the window can be variable, e.g. TCP.
- The window slides to include new unsent frames when the correct ACKs are received

Receiver Sliding Window



a. Before sliding

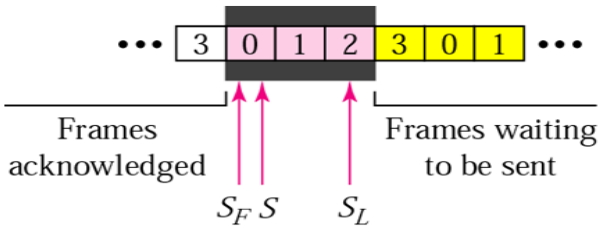


b. After sliding

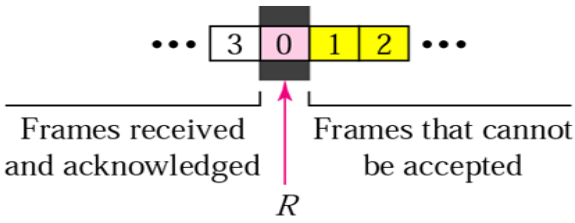
- Size of the window at the receiving site is always 1 in this protocol.
- Receiver is always looking for a specific frame to arrive in a specific order.
- Any frame arriving out of order is discarded and needs to be resent.
- Receiver window slides as shown in fig. Receiver is waiting for frame 0 in part a.

Control Variables

- Sender has 3 variables: S, S_F, and S_L
- S holds the sequence number of recently sent frame
- S_F holds the sequence number of the first frame
- S_L holds the sequence number of the last frame
- Receiver only has the one variable, R, that holds the sequence number of the frame it expects to receive. If the seq. no. is the same as the value of R, the frame is accepted, otherwise rejected.



a. Sender window



b. Receiver window

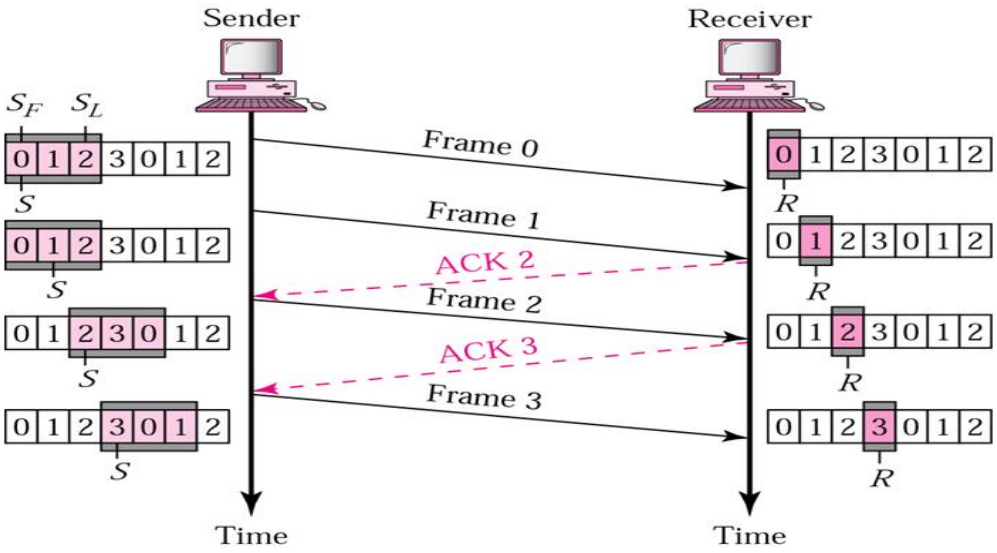
Acknowledgement

- Receiver sends positive ACK if a frame arrived safe and in order.
- If the frames are damaged/out of order, receiver is silent and discard all subsequent frames until it receives the one it is expecting.
- The silence of the receiver causes the timer of the unacknowledged frame to expire.
- Then the sender resends all frames, beginning with the one with the expired timer.
- For example, suppose the sender has sent frame 6, but the timer for frame 3 expires (i.e. frame 3 has not been acknowledged), then the sender goes back and sends frames 3, 4, 5, 6 again. Thus it is called Go-Back-N-ARQ

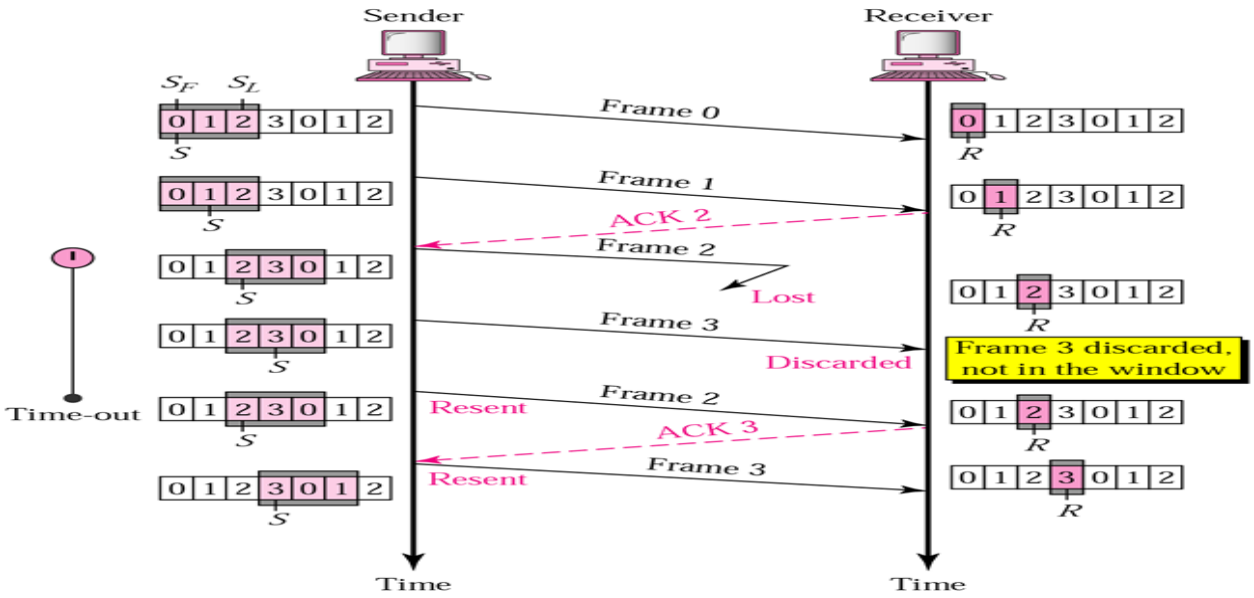
- The receiver does not have to acknowledge each frame received, it can send one cumulative ACK for several frames.

Go-Back-N ARQ, normal operation

The sender keeps track of the outstanding frames and updates the variables and windows as the ACKs arrive.



Go-Back-N ARQ, lost frame



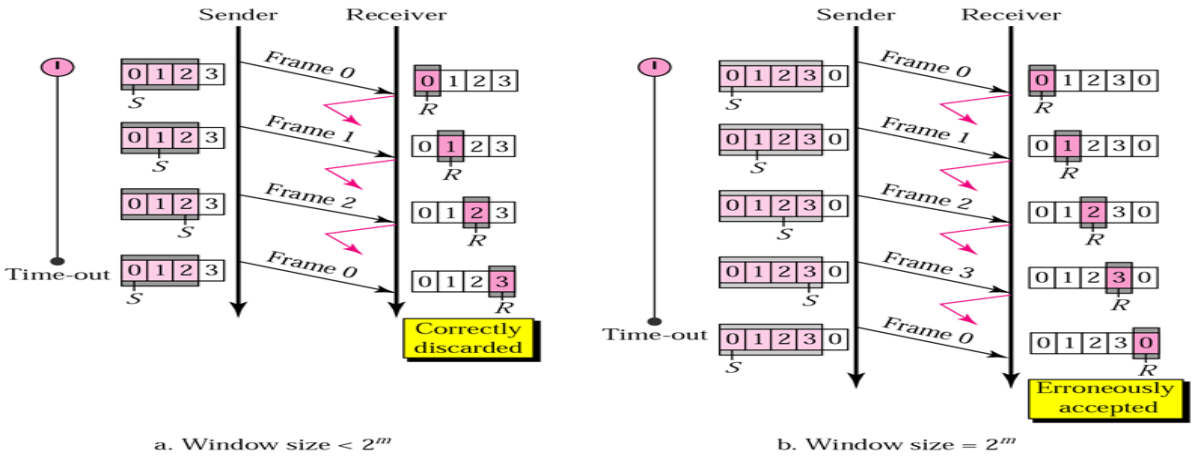
- Frame 2 is lost
- When the receiver receives frame 3, it discards frame 3 as it is expecting frame 2 (according to window). After the timer for frame 2 expires at the sender site, the sender sends frame 2 and 3. (go back to 2)

Go-Back-N ARQ, damaged/lost/delayed ACK

- If an ACK is damaged/lost, we can have two situations:
- If the next ACK arrives before the expiration of any timer, there is no need for retransmission of frames because ACKs are cumulative in this protocol.
- If ACK1, ACK2, and ACk3 are lost, ACK4 covers them if it arrives before the timer expires.
- If ACK4 arrives after time-out, the last frame and all the frames after that are resent.
- Receiver never resends an ACK.
- A delayed ACK also triggers the resending of frames

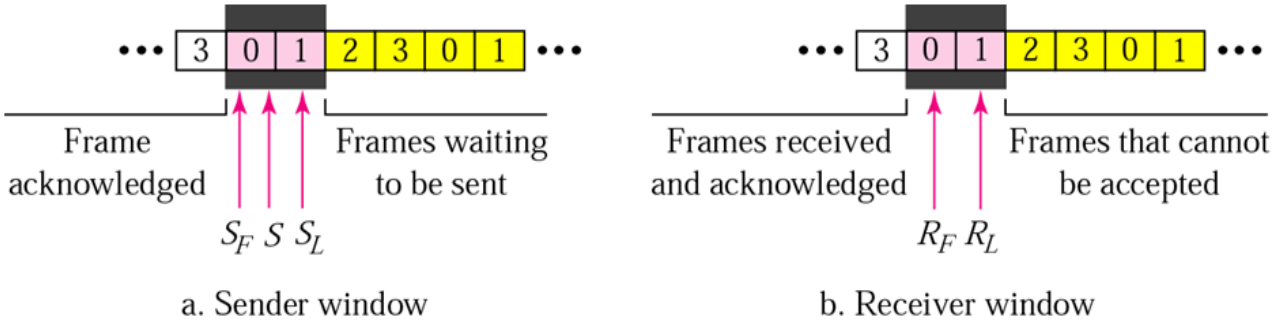
Go-Back-N ARQ, sender window size

- Size of the sender window must be less than 2^m. Size of the receiver is always 1. If m = 2, window size = $2^m - 1 = 3$.
- Fig compares a window size of 3 and 4.

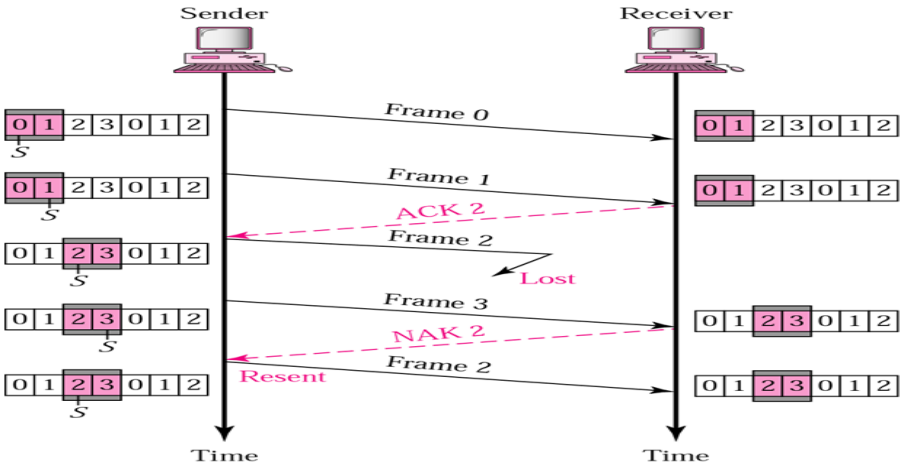


Selective Repeat ARQ, sender and receiver windows

- Go-Back-N ARQ simplifies the process at the receiver site. Receiver only keeps track of only one variable, and there is no need to buffer out-of-order frames, they are simply discarded.
- However, Go-Back-N ARQ protocol is inefficient for noisy link. It bandwidth inefficient and slows down the transmission.
- In Selective Repeat ARQ, only the damaged frame is resent. More bandwidth efficient but more complex processing at receiver.
- It defines a negative ACK (NAK) to report the sequence number of a damaged frame before the timer expires.



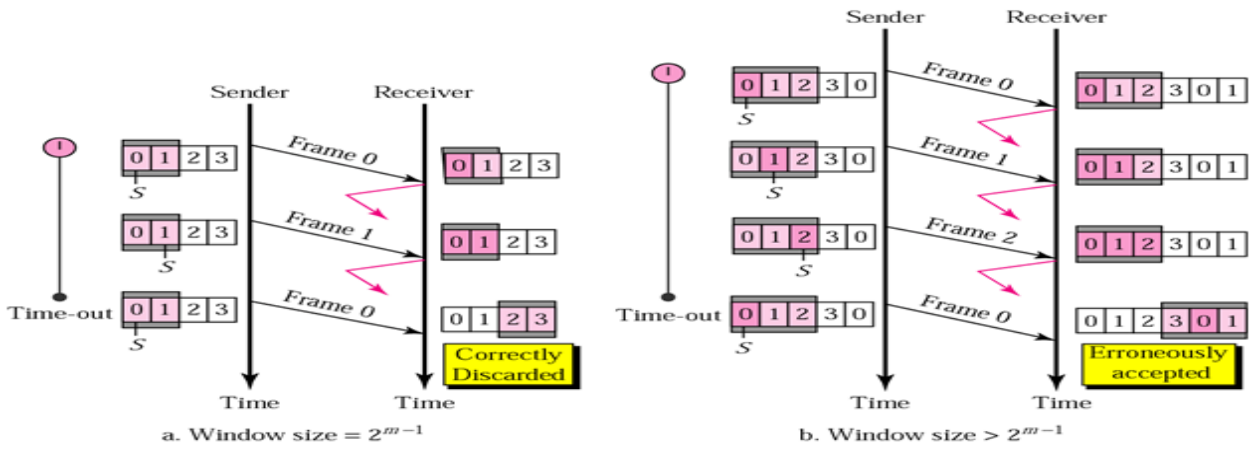
Selective Repeat ARQ, lost frame



- Frames 0 and 1 are accepted when received because they are in the range specified by the receiver window. Same for frame 3.
- Receiver sends a NAK2 to show that frame 2 has not been received and then sender resends only frame 2 and it is accepted as it is in the range of the window.

Selective Repeat ARQ, sender window size

- Size of the sender and receiver windows must be at most one-half of 2^m. If m = 2, window size should be $2^m/2 = 2$. Fig compares a window size of 2 with a window size of 3. Window size is 3 and all ACKs are lost, sender sends duplicate of frame 0, window of the receiver expect to receive frame 0 (part of the window), so accepts frame 0, as the 1st frame of the next cycle – an error.



Error Detection Methods

Error detection is only to see if any error has occurred. The basic idea behind any error detection scheme is to add redundant information to a frame that can be used to determine if errors have been introduced.

Two-Dimensional Parity

Data is divided into seven byte segments.

Even parity is computed for all bytes (Vertical Redundancy Check).

Even parity is also calculated for each bit position across each of the bytes (Longitudinal

Redundancy Check).

Thus a parity byte for the entire frame, in addition to a parity bit for each byte is sent.

The receiver recomputes the row and column parities. If parity bits are correct, the frame is accepted else discarded. Two-dimensional parity catches all 1, 2 and 3-bit errors, and most 4-bit errors.

Internet Checksum

The 16-bit checksum is not used at the link layer but by the upper layer protocols (UDP).

Sender

The data is divided into 16-bit words.

The initial checksum value is 0.

All words (incl. checksum) are summed using one's complement arithmetic.

Carries (if any) are wrapped and added to the sum.

The complement of sum is known as checksum and is sent with data

Receiver

The message (including checksum) is divided into 16-bit words.

All words are added using one's complement addition.

The sum is complemented and becomes the new checksum.

If the value of checksum is 0, the message is accepted, otherwise it is rejected.

7	0111		0111
11	1011		1011
12	1100		1100
6	0110		0110
Initial Checksum	0000	Received Checksum	**1001**
Sum	**10**0100	Sum	**10**1101
Carry	10	Carry	10
Sum	0110	Sum	1111
Checksum	**1001**	New Checksum	0000
Sender		Receiver	

Analysis

Checksum is **well-suited for software implementation** and is not strong as CRC. If value of one word is incremented and another word is decremented by the same amount, the errors are not detected because sum and checksum remain the same.

Cyclic Redundancy Check (CRC)

CRC developed by IBM uses the concept of finite fields.

A n bit message is represented as a polynomial of degree n - 1.

The message M(x) is represented as a polynomial by using the value of each bit in the message as coefficient for each term. For eg., 10011010 represents $x^7 + x^4 + x^3 + x$

For calculating a CRC, sender and receiver agree on a divisor polynomial, C(x) of degree k

such that k ” n – 1

PROCEDURE AND PROBLEM REFER CLASS NOTES

Error Correction Method

- The error correction process is done in the basis of finding the position of the error bit in the information sequence at receiver side.
- This technique adds the redundant bits with the information through some conditions. The sequence adding the redundant bit in the following manner.
- 2^0 = 1st position; 2^1 = 2nd position; 2^2 = 4th position; 2^3 = 8th position… and so on.
- Adding the redundant bits with information has done by using hamming code technique. In hamming code process, the redundant bits are added with the information through the following condition.,

2^r>=m+r+1

Where,

m – message or info. Bits count

r – redundant bits

Hamming code table

Message Bits (m)	Redundant Bits (r)	Total Bits (m+r) to be transmitted from the sender side
1	2	3
2	3	5
3	3	6
4	3	7
5	4	9
6	4	10
7	4	11 and so on...

EXAMPLE

Correct the error for the following information sequence 01101010

Soln:

Step 1 : Message bit count(m) = 8 bits

Step2 : Finding redundant bits with help of hamming code condition. (**2^r>=m+r+1)**

As per our example, the info consists of 8-bits. So we need to add 4 redundant bits with the information.

Step 3: Finding the redundant bits (r-bits). The r-bits are represented in the manner of r1 – 2^0 position, r2 – 2^1 position, r3 – 2^2 position, r4 – 2^3 position.

- **r1 – bits are find by last bit will be 1 (0001 – 1st position, 0011 – 3rd position and so on.)**
- Similarly for r2 – second bit will be 1 from the right most every position, ||ly r3 – third bit, r4 – fourth bit.

These bits are find by setting even or odd parity process. This example we used even parity to find r-bits.

				2^3				2^2		2^1	2^0
0	**1**	**1**	**0**	**r**	**1**	**0**	**1**	**r**	**0**	**r**	**r**
12 1100	11 1011	10 1010	9 1001	8 1000	7 0111	6 0110	5 0101	4 0100	3 0011	2 0010	1 0001

For our example,

r1=(1,3,5,7,9,11) = (r,0,1,1,0,1); r1=1

r2=(2,3,6,7,10,11)=(r,0,0,1,1,1); r2=1

r3=(4,5,6,7,12)=(r,1,0,1,0); r3=0

r4=(8,9,10,11,12)=(r,0,1,1,0); r4=0

There by the sender will send the information with its redundant bits as follows,

0	1	1	0	0	1	0	1	0	0	1	1

Receiver side

At the receiver side the original message receive without any error means all the r-bits will become 0.

0	1	1	0	0	1	0	1	0	0	1	1

r1=(1,3,5,7,9,11) = (1,0,1,1,0,1); r1=0

r2=(2,3,6,7,10,11)=(1,0,0,1,1,1); r2=0

r3=(4,5,6,7,12)=(0,1,0,1,0); r3=0

r4=(8,9,10,11,12)=(0,0,1,1,0); r4=0

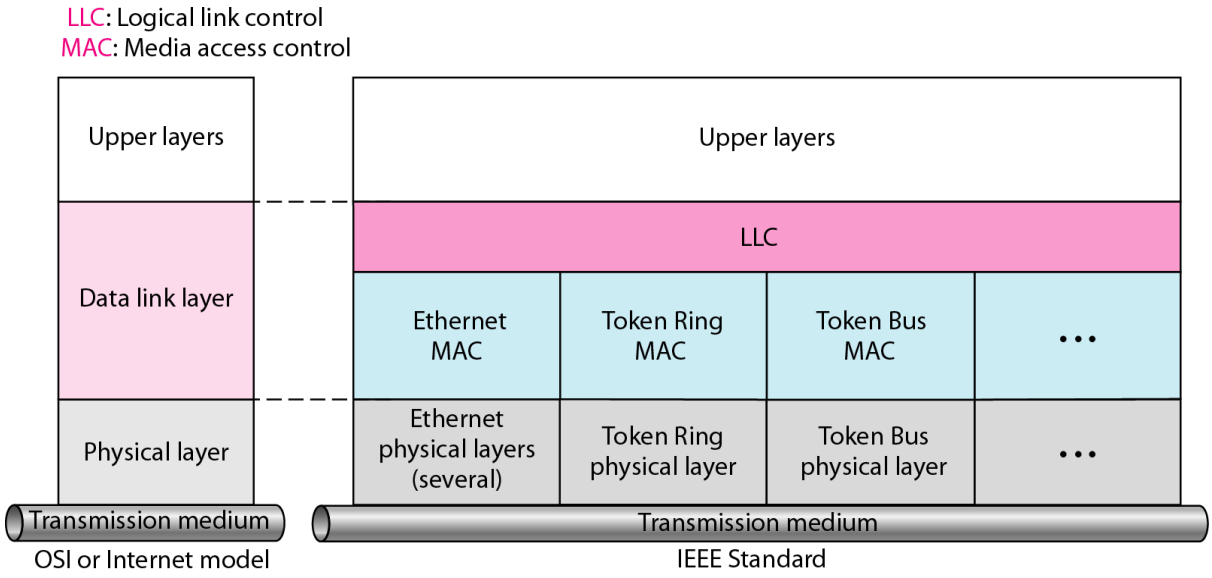
All the r-bits are zero means there is no error in the information.

UNIT 2: MEDIA ACCESS & INTERNETWORKING

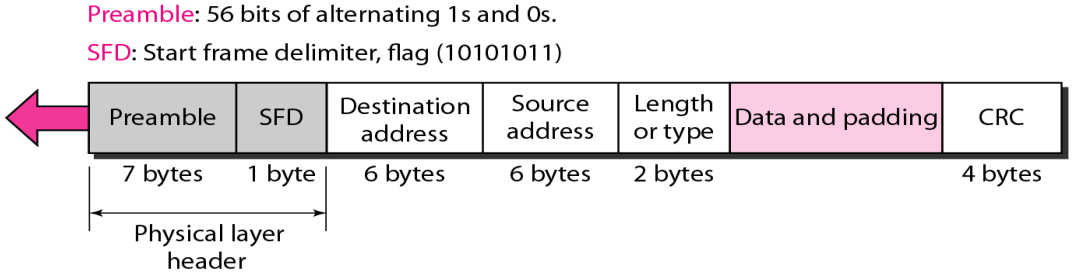
Overview of Data link Control and Media access control - Ethernet (802.3) - Wireless LANs – Available Protocols – Bluetooth – Bluetooth Low Energy – WiFi – 6LowPAN–Zigbee - Network layer services – Packet Switching – IPV4 Address – Network layer protocols (IP, ICMP, Mobile IP)

PART-A

1. **Compare 802 with OSI model.**



2. **Illustrate the operation of Ethernet format with neat sketch.**

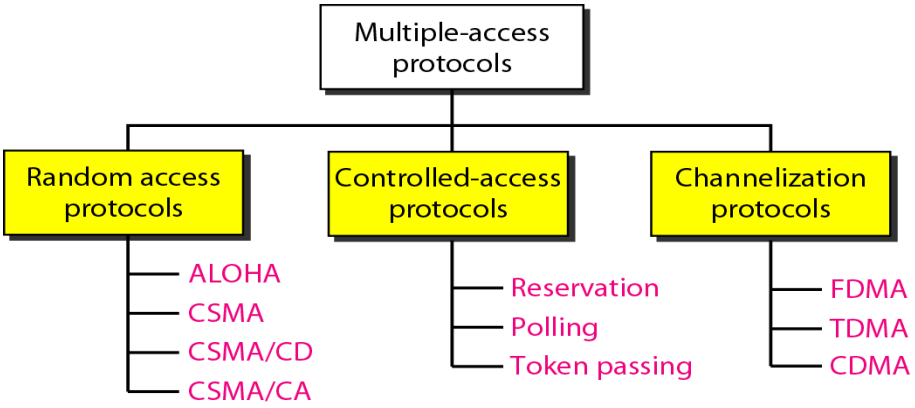


3. **List the types of stations in 802.11 architecture and explain each station operation.**

Station Types:

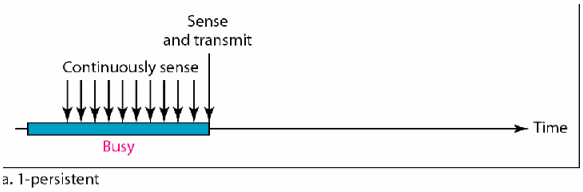
- **No transition:** The stations which share their information between the same BSS not to other BSS.
- **BSS transition:** The station which share their information from one BSS to other BSS but within the same ESS.
- **ESS transition:** The station which shares the information from one ESS to other.

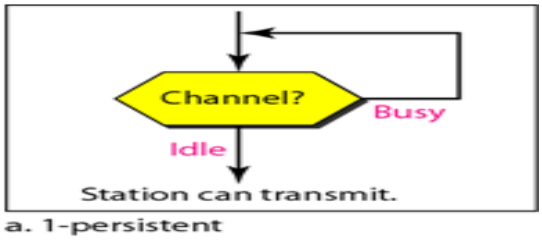
4. Categorize the media access in data link layer.



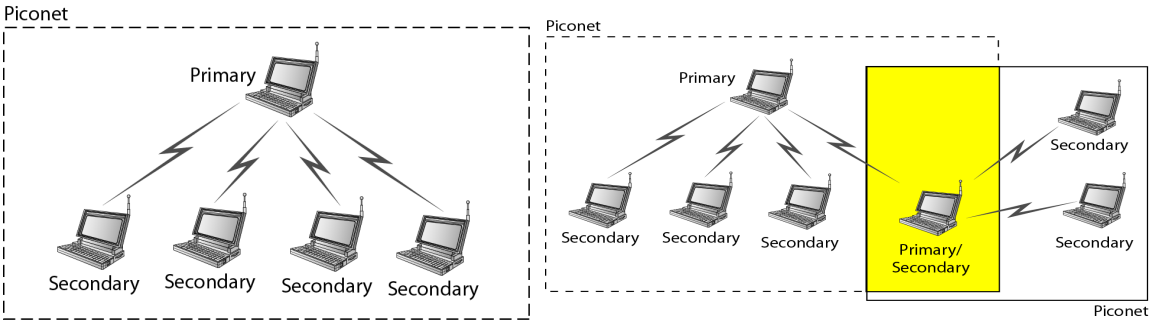
5. What do you mean by 1-persistant? Explain with a neat sketch.

In this scheme, transmission proceeds immediately if the carrier is idle. However, if the carrier is busy, then sender continues to sense the carrier until it becomes idle. The main problem here is that, if more than one transmitter is ready to send, a collision is GUARANTEED!!



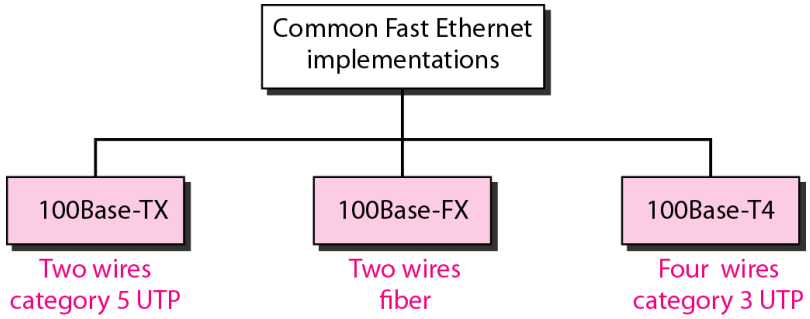


6. Examine the networks involved in Bluetooth architecture.

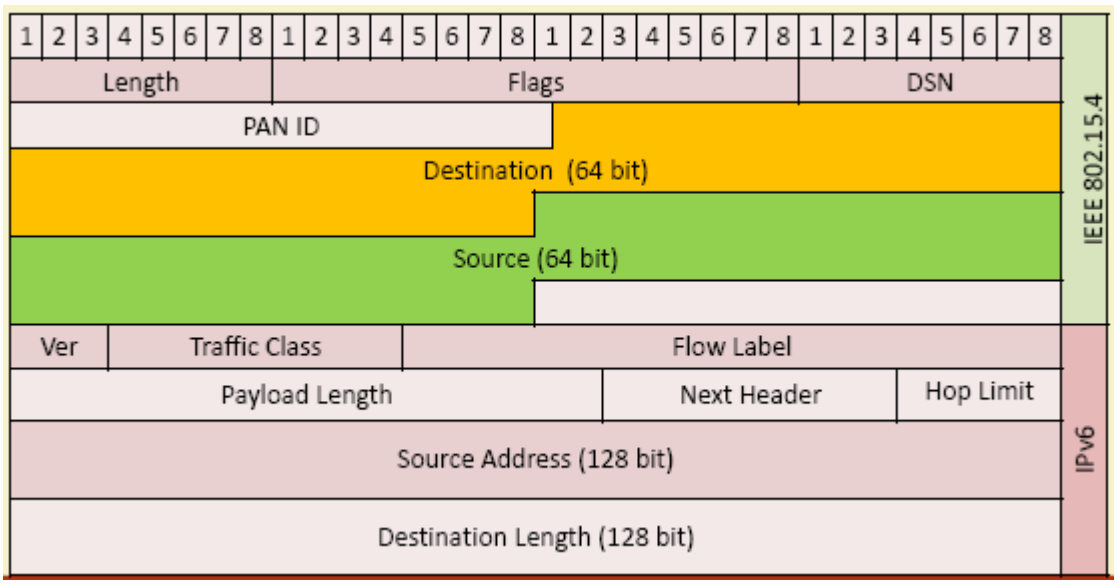


7. Write short notes on Fast Ethernet.

Fast Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel. IEEE created Fast Ethernet under the name 802.3. Fast Ethernet is backward-compatible with Standard Ethernet, but it can transmit data 10 times faster at a rate of 100 Mbps.



8. Construct the packet format for 6LowPAN.



9. List out the applications of Zigbee protocol.

- ✓ Building automation
- ✓ Remote control (RF4CE or RF for consumer electronics)
- ✓ Smart energy for home energy monitoring
- ✓ Health care for medical and fitness monitoring
- ✓ Home automation for control of smart homes
- ✓ Light Link for control of LED lighting
- ✓ Telecom services

10. Identify the error if any in the following IP address.

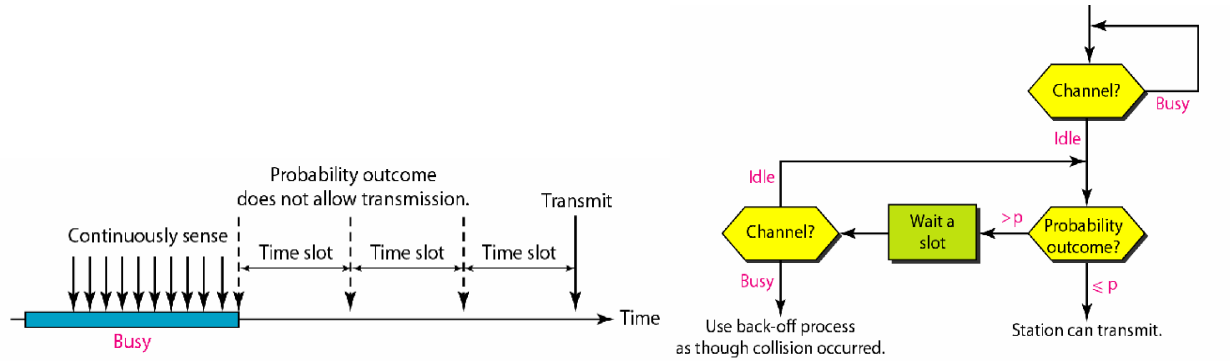
(i) **11.56.045.78 –** Error, The decimals in IP address should preceding with zero.

(ii) **75.45.301.14 –** Error, Each decimal value in IP address ranges from 0 – 255.

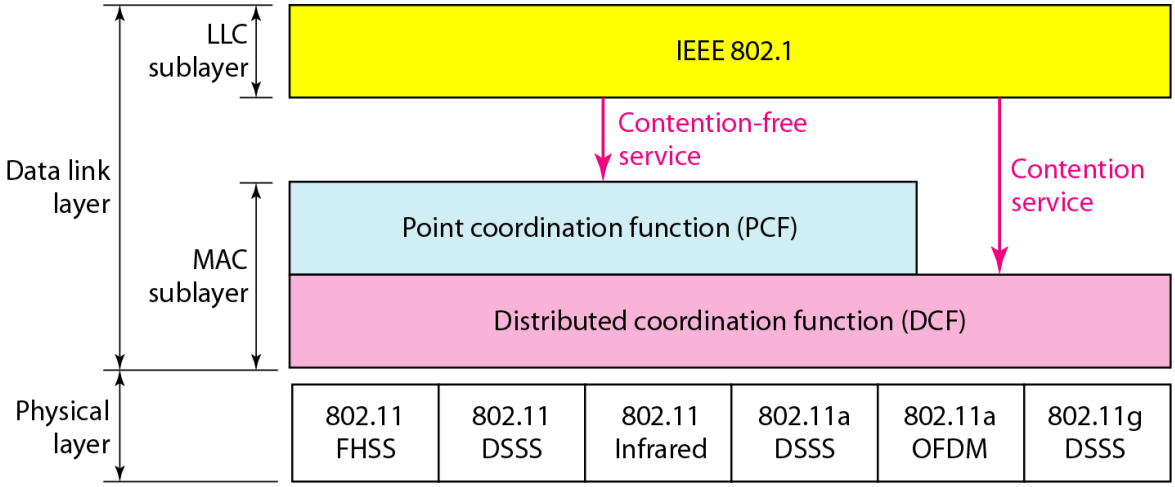
11. Explain the process of p-Persistent method with neat sketch.

Even if a sender finds the carrier to be idle, it uses a probabilistic distribution to determine whether to transmit or not. Put simply, "toss a coin to decide". If the carrier is idle, then transmission takes place with a probability p and the sender waits with a

probability 1-p. This scheme is a good trade off between the Non-persistent and 1-persistent schemes. So, for low load situations, p is high (example: 1-persistent); and for high load situations, p may be lower.



12. Show the protocol architecture of 802.11.



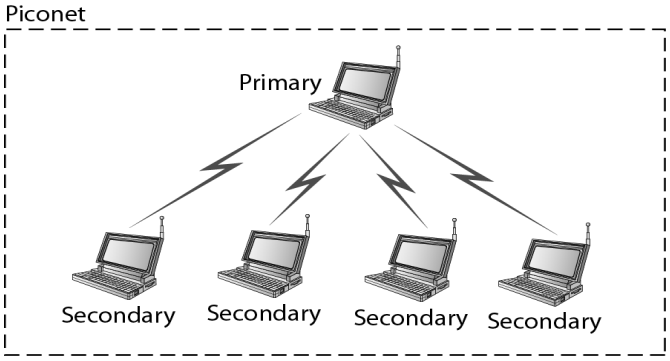
13. Write short notes on Pure Aloha.

• Each station transmits (access the medium) whenever it has data to send.
• Stations do not sense the medium (whether anyone else is sending data at the same time).
• Stations do not look for collisions (two stations transmitting at the same time).
• Reliability is achieved through acknowledgments. After transmitting, the station waits for an acknowledgment for twice the time it takes for the signal to travel the distance. If no acknowledgment arrives, then the station assumes that the message was lost, and after waiting a random amount of time, retransmits. The station will retry transmitting several times before giving up.

14. Inspect the operation of PICONET.

A Bluetooth network is called a piconet, or a small net. A piconet can have up to eight stations, one of which is called the primary; the rest are called secondary. All the secondary stations synchronize their clocks and hopping sequence with the primary. Note

that a piconet can have only one primary station. The communication between the primary and the secondary can be one-to-one or one-to-many.



15. Illustrate the routing protocols involved in 6LoWPAN.

Routing protocols used in 6LoWPAN are,

(i) LOADng - Derived from AODV and extended for use in IoT.

(ii) RPL - Distance Vector IPv6 **routing protocol for lossy and low power networks.**

16. A block of addresses is granted to a small organization. We know that one of the addresses is 205.16.37.39/28. What is the first address and last address in the block and also find the number of addresses?

N = 28,

Therefore mask of the network is, 255.255.255.240

Conversion of IP address in Dotted decimal to Binary,

205.16.37.39 – 11001101 00010000 00100101 00100111

First Address (Network Address):

IP address - 11001101 00010000 00100101 00100111

(And operation)

Mask - 11111111 11111111 11111111 11110000

First address – 11001101 00010000 00100101 00100000

First address in dotted decimal notation – 205.16.37.32

Last Address:

IP address - 11001101 00010000 00100101 00100111

(Or operation)

Mask - 00000000 00000000 00000000 00001111

Last address – 11001101 00010000 00100101 00101111

Last address in dotted decimal notation – 205.16.37.47

17. What do you meant by switching?

A switch is a *multi-input, multi-output* device, receives packets on one of its links and transmits them on one or more other links. This is known as *switching* or *forwarding*. Large networks can be built by *interconnecting* a number of switches. Hosts are connected to the switch using point-to-point link.

18. Identify the Class and represent the netid of the following IP Address:

(i) **110.34.56.45 –** Class A (Range of Class A addresses 0 – 127)
Net id – 110.0.0.0 (Mask of Class A is 255.0.0.0)

(ii) **212.208.63.23 –** Class C (Range of Class C; 192 – 223)
Net id – 212.208.63.0 (Mask of Class C is 255.255.255.0)

19. What do you understand by CSMA protocol?

In Carrier Sense Multiple Access (CSMA), each station first checks state of the medium using one of the persistence methods before sending. The possibility of collision still exists because of propagation delay. When a station sends a frame, it takes time for the first bit to reach every station.

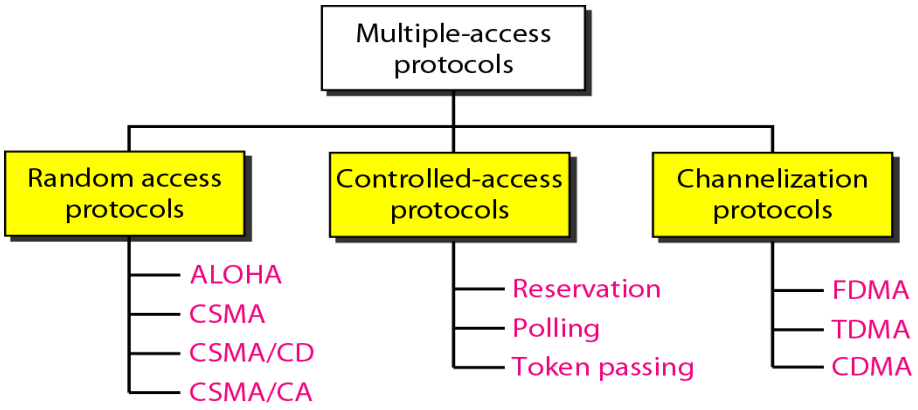
20. List the important components for ZIGBEE protocol.

(i) **Zigbee Device object (ZDO) –** Helps to Manage the device, maintain secrecy of the data, Providing QoS policies.

(ii) **Application Support Sublayer (APS) –** Interfacing and control services, bridge between network and other layers.

PART-B

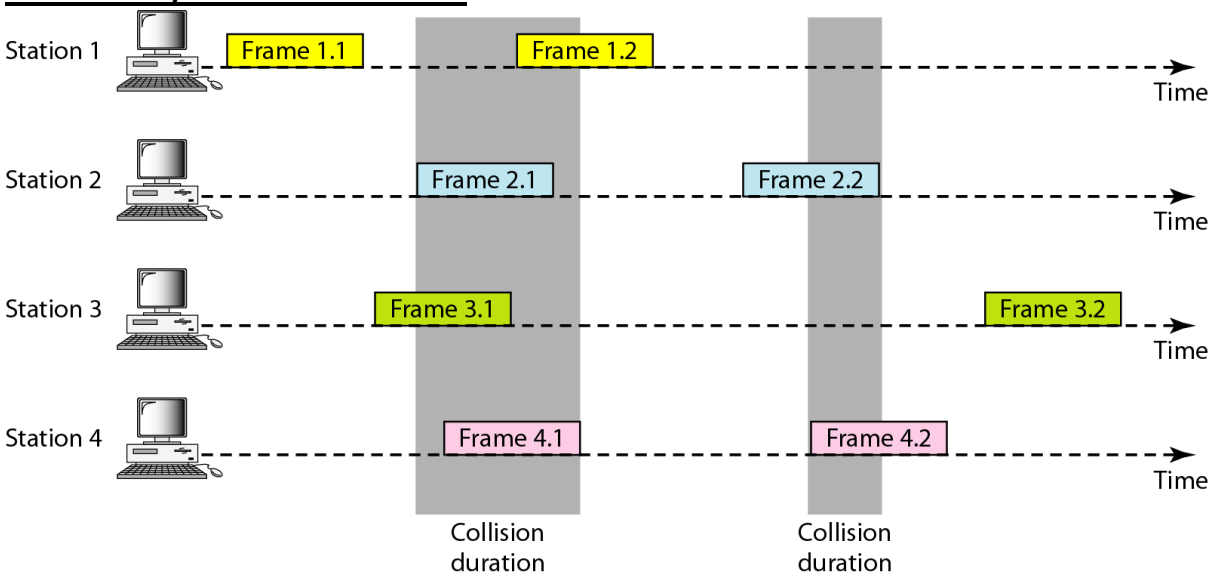
1. Explain in detail about MAC protocols.



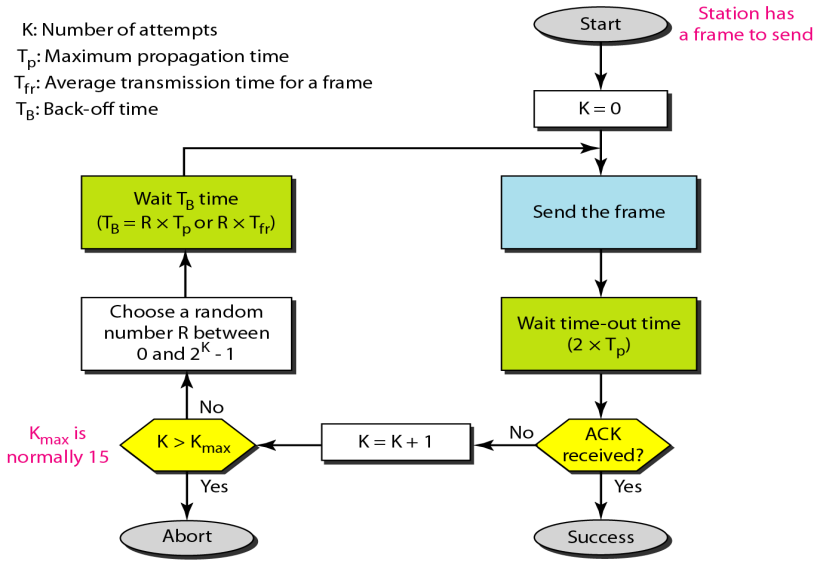
RANDOM ACCESS

In random access or contention methods, no station is superior to another station and none is assigned the control over another. No station permits, or does not permit, another station to send. At each instance, a station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send.

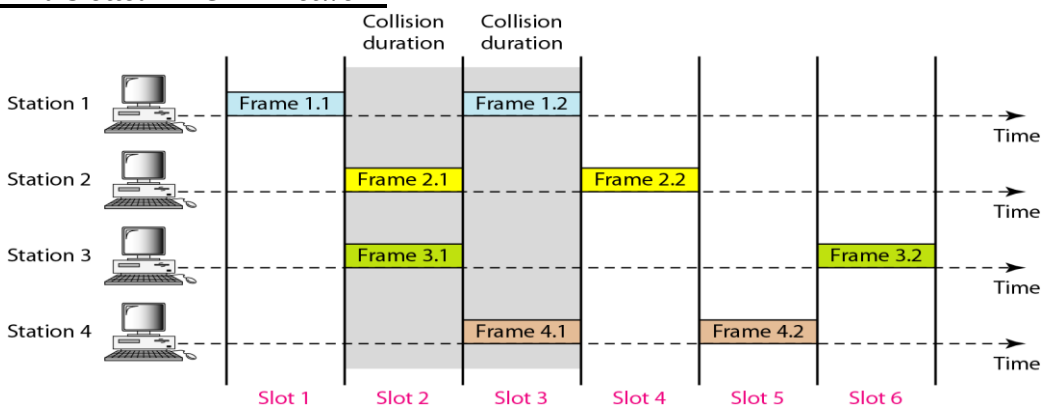
Frames in a pure ALOHA network



Procedure for pure ALOHA protocol

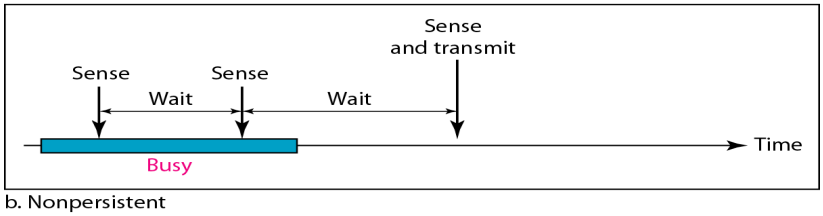


Frames in a slotted ALOHA network

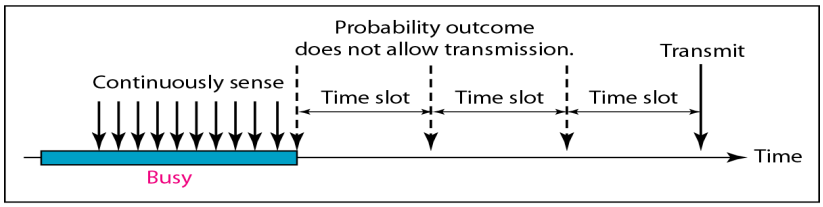


Behavior of three persistence methods

a. 1-persistent

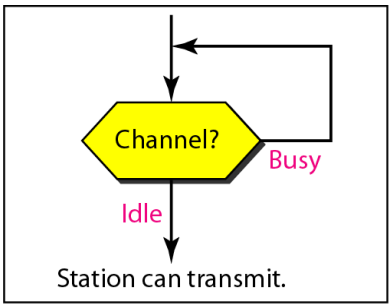


b. Nonpersistent

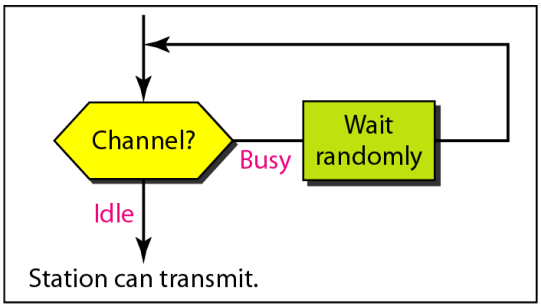


c. p-persistent

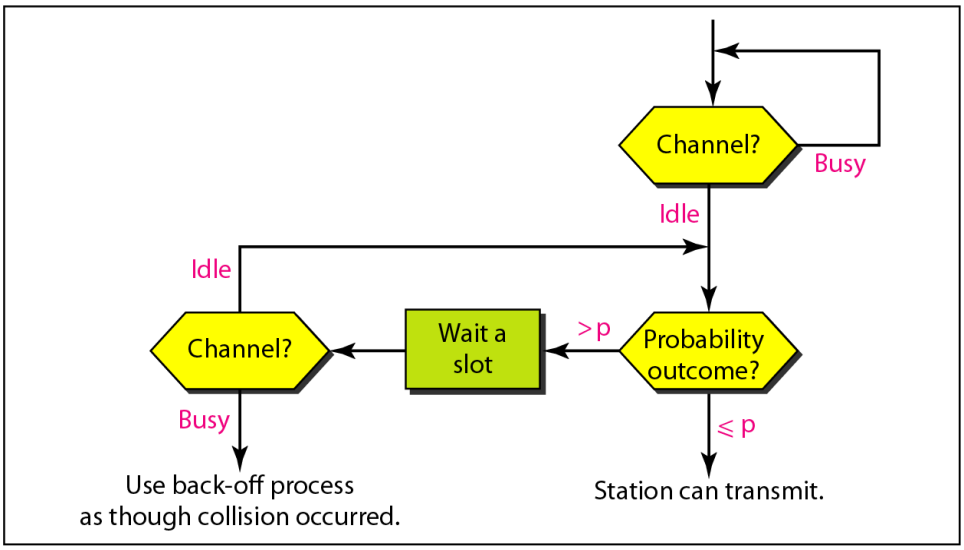
Flow diagram for three persistence methods



a. 1-persistent

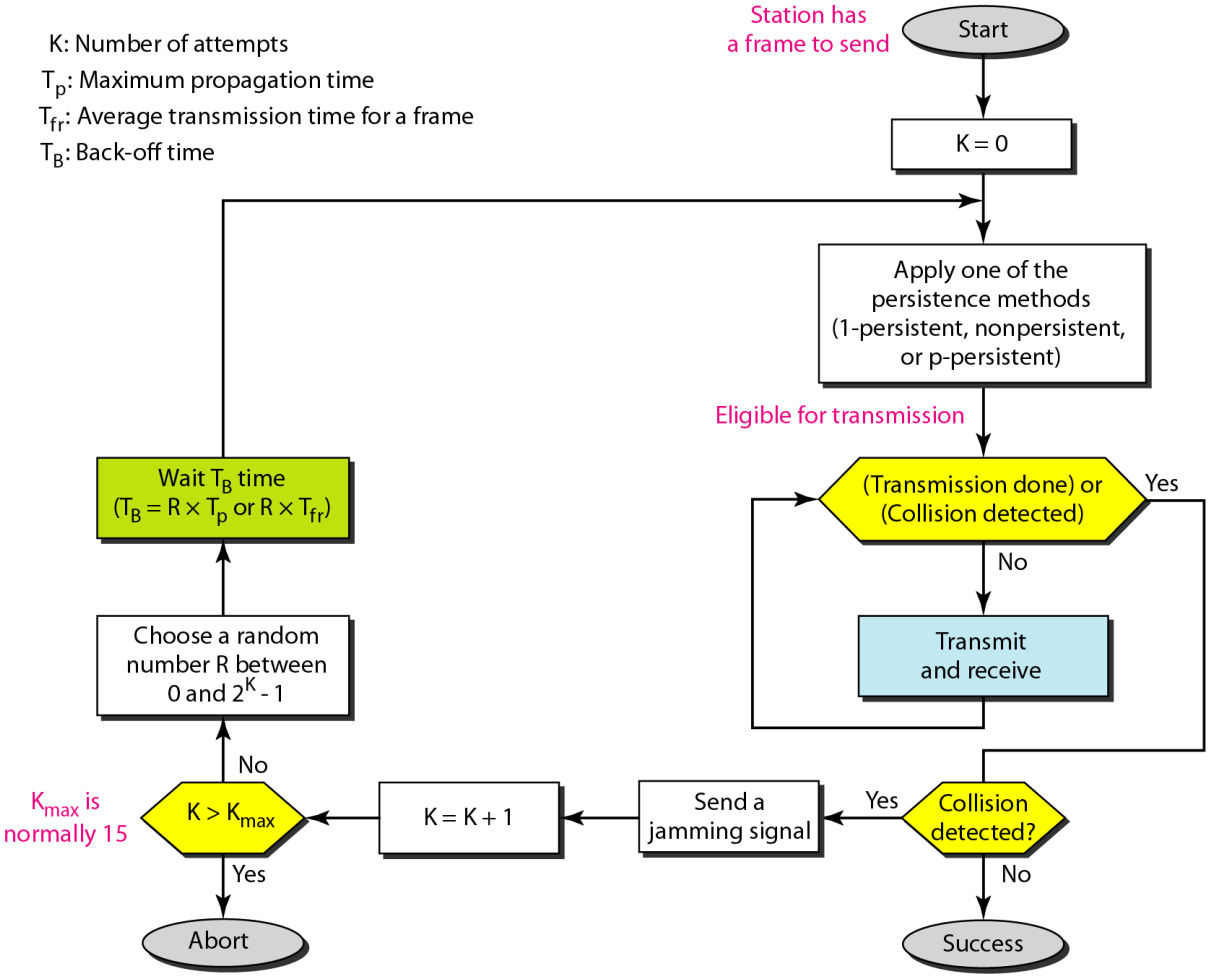


b. Nonpersistent

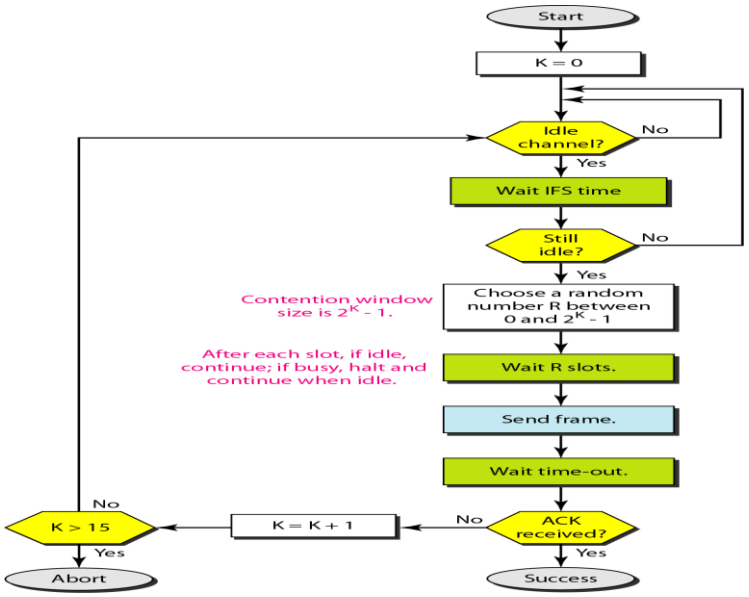


c. p-persistent

Flow diagram for the CSMA/CD



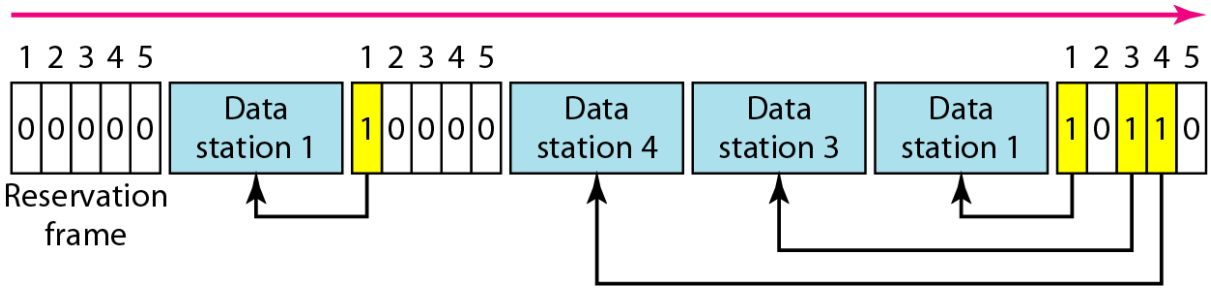
Flow diagram for CSMA/CA



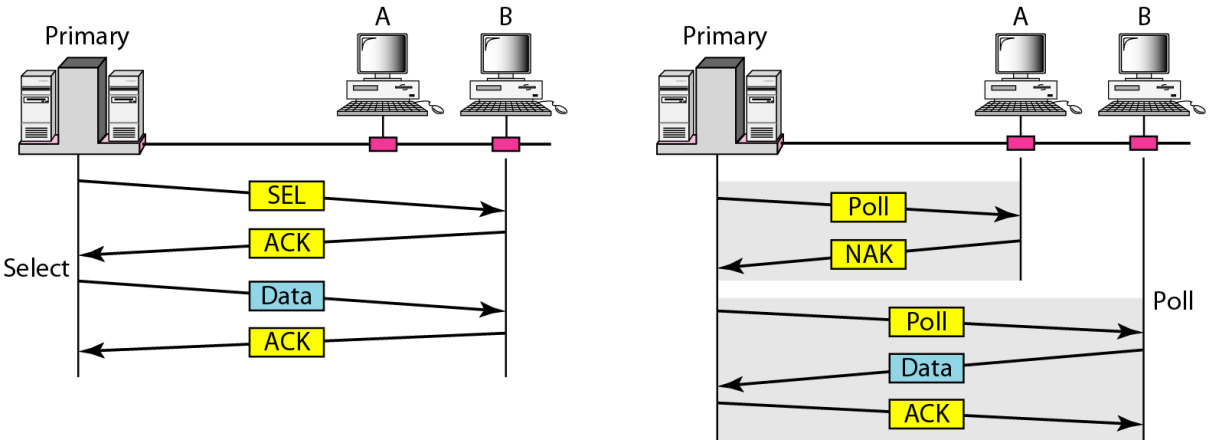
CONTROLLED ACCESS

In controlled access, the stations consult one another to find which station has the right to send. A station cannot send unless it has been authorized by other stations. We discuss three popular controlled-access methods.

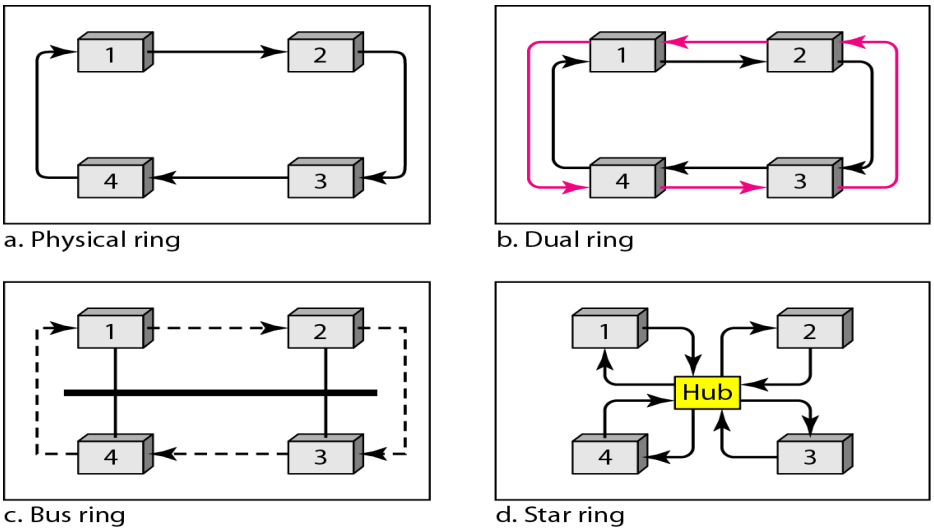
Reservation access method



Select and poll functions in polling access method



Logical ring and physical topology in token-passing access method

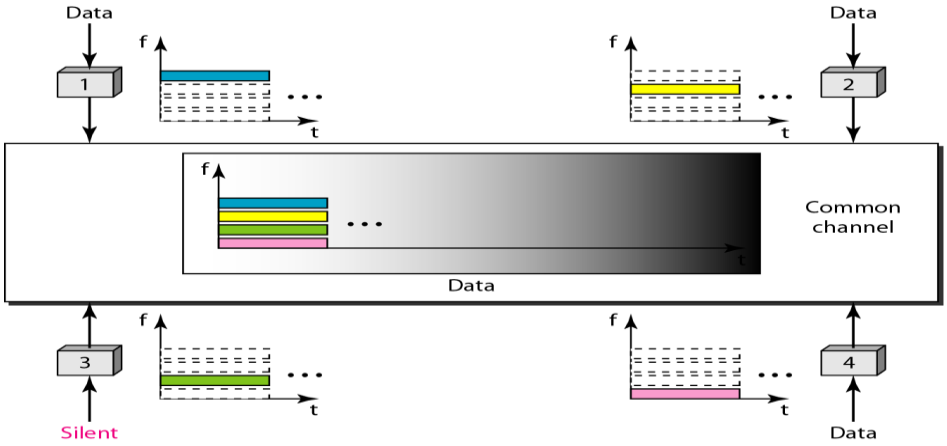


CHANNELIZATION

Channelization is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, between different stations. In this section, we discuss three channelization protocols.

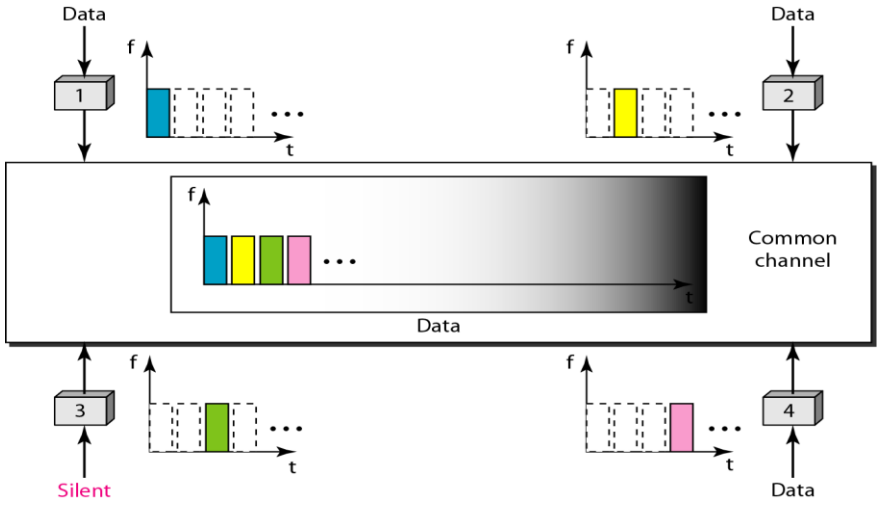
Frequency-division multiple access (FDMA)

In FDMA, the available bandwidth of the common channel is divided into bands that are separated by guard bands.



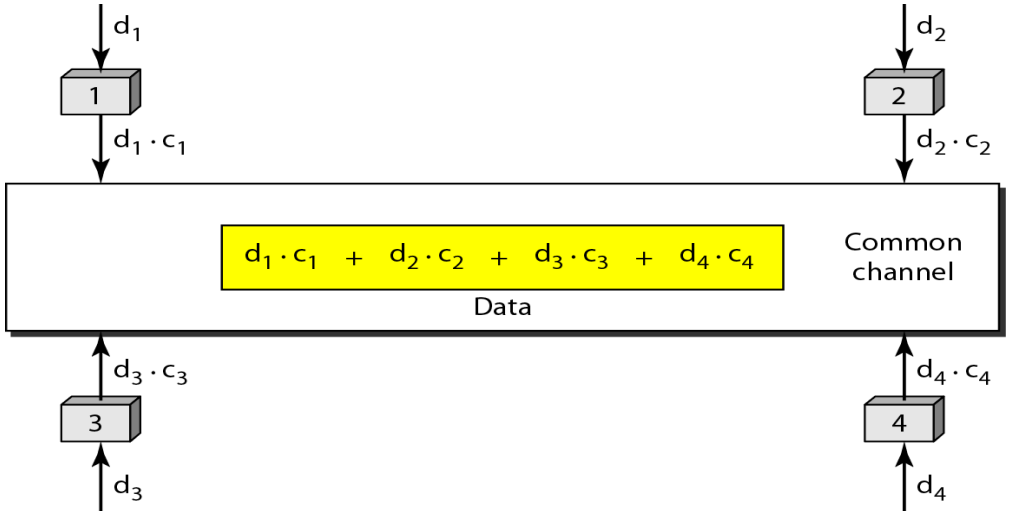
Time-division multiple access (TDMA)

In TDMA, the bandwidth is just one channel that is timeshared between different stations.



Code-division multiple access (CDMA)

In CDMA, one channel carries all transmissions simultaneously.



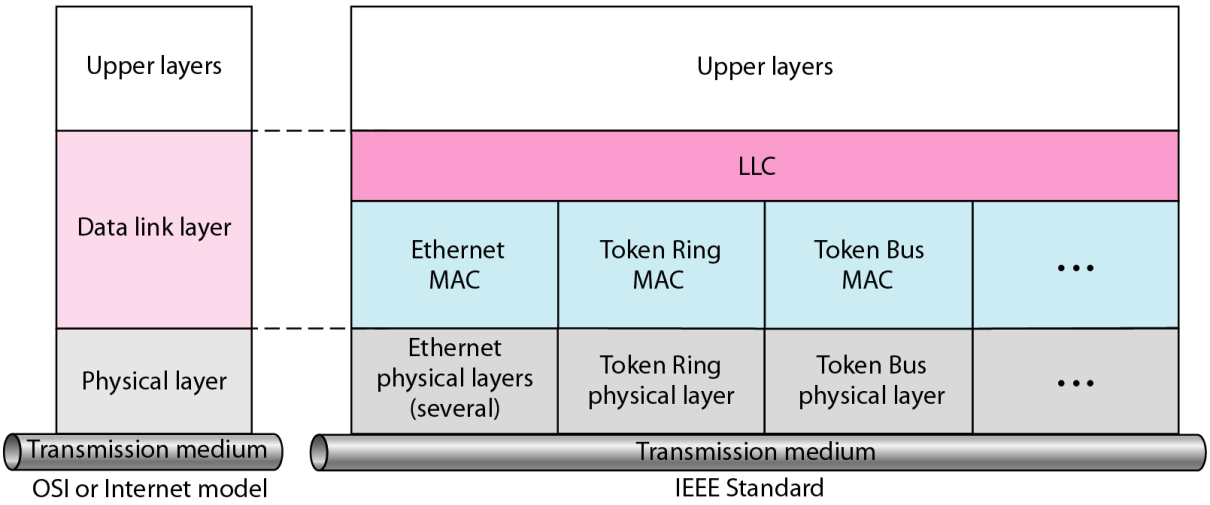
2. Explain in detail about Wired LAN (or) Ethernet.

Ethernet (802.3): (Wired LANS)

In 1985, the Computer Society of the IEEE started a project, called Project 802, to set standards to enable intercommunication among equipment from a variety of manufacturers. Project 802 is a way of specifying functions of the physical layer and the data link layer of major LAN protocols.

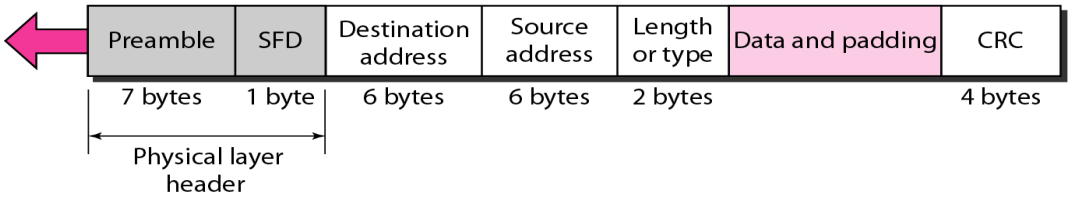
IEEE standard for LANs

LLC: Logical link control
MAC: Media access control



802.3 MAC frame

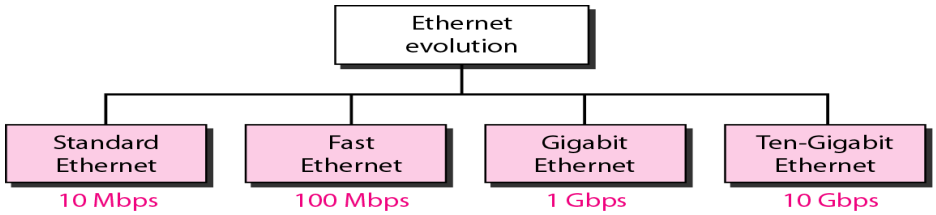
Preamble: 56 bits of alternating 1s and 0s.
SFD: Start frame delimiter, flag (10101011)



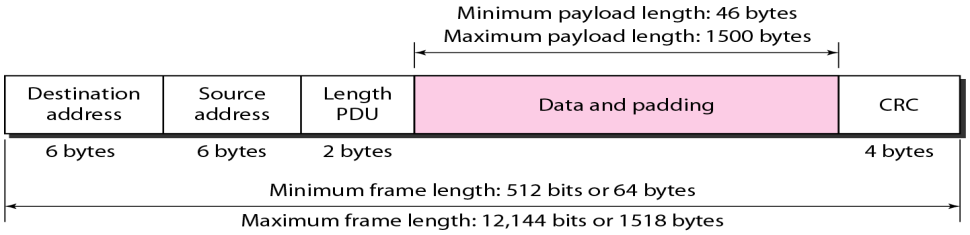
STANDARD ETHERNET

The original Ethernet was created in 1976 at Xerox's Palo Alto Research Center (PARC). Since then, it has gone through four generations.

Ethernet evolution through four generations



Minimum and maximum lengths

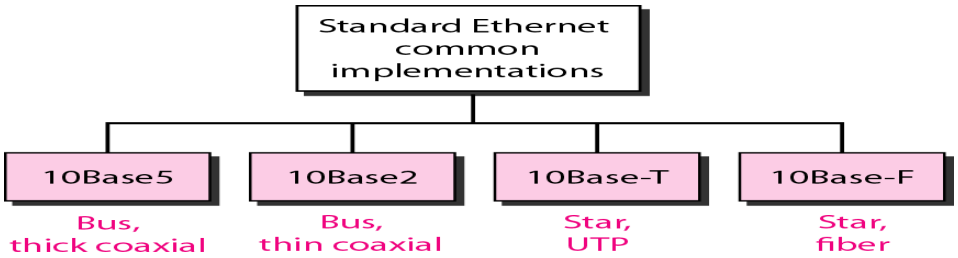


Example of an Ethernet address in hexadecimal notation

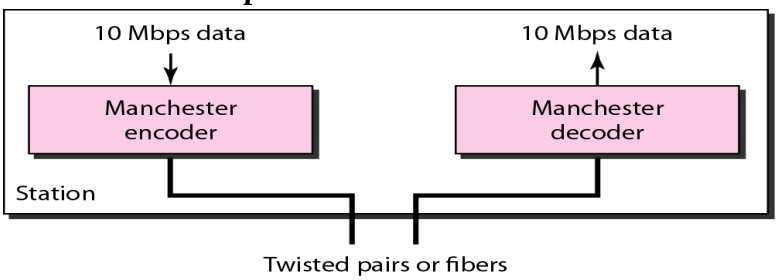
Unicast and multicast addresses

The broadcast destination address is a special case of the multicast address in which all bits are 1s. (***FF:FF:FF:FF:FF:FF)***

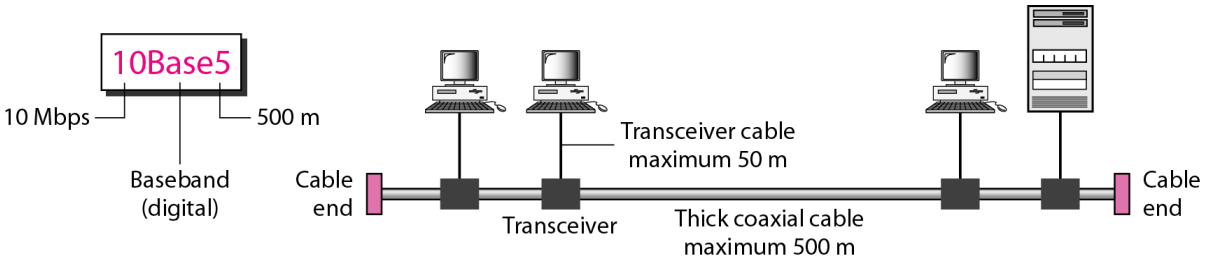
Categories of Standard Ethernet



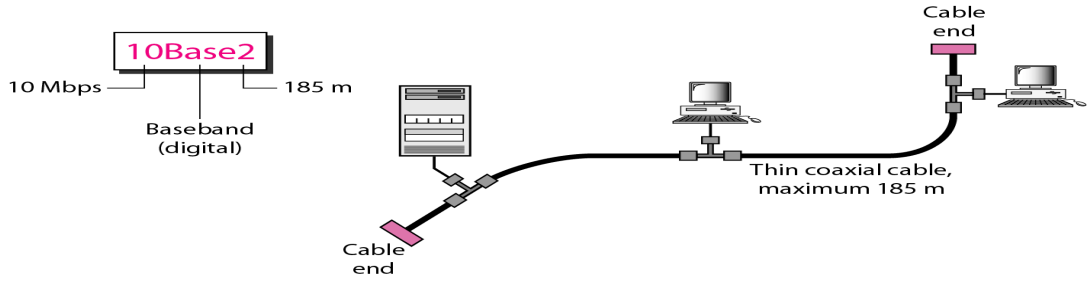
Encoding in a Standard Ethernet implementation



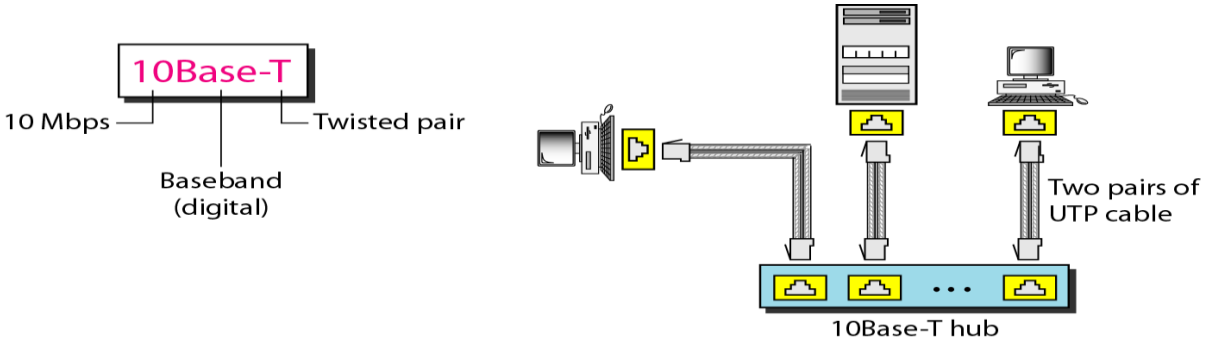
10Base5 implementation



10Base2 implementation



10Base-T implementation



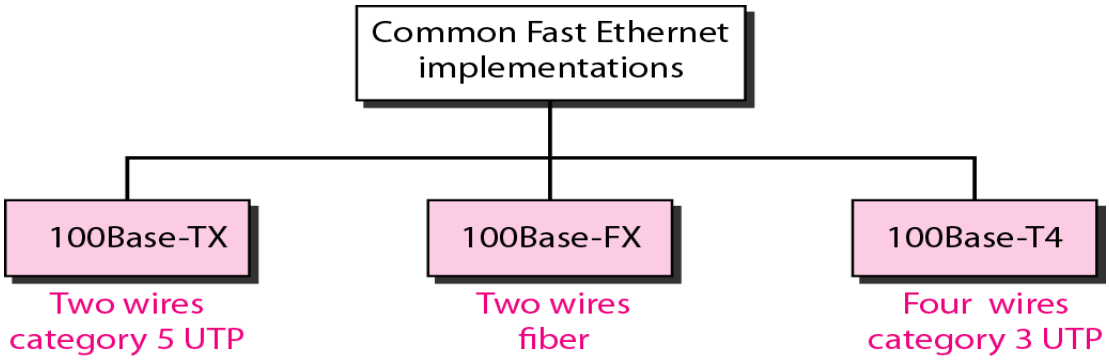
Summary of Standard Ethernet implementations

Characteristics	*10Base5*	*10Base2*	*10Base-T*	*10Base-F*
Media	Thick coaxial cable	Thin coaxial cable	2 UTP	2 Fiber
Maximum length	500 m	185 m	100 m	2000 m
Line encoding	Manchester	Manchester	Manchester	Manchester

FAST ETHERNET

Fast Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel. IEEE created Fast Ethernet under the name 802.3u. Fast Ethernet is backward-compatible with Standard Ethernet, but it can transmit data 10 times faster at a rate of 100 Mbps.

Fast Ethernet implementations



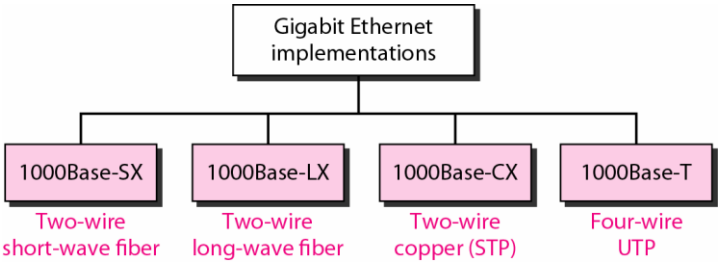
Summary of Fast Ethernet implementations

Characteristics	*100Base-TX*	*100Base-FX*	*100Base-T4*
Media	Cat 5 UTP or STP	Fiber	Cat 4 UTP
Number of wires	2	2	4
Maximum length	100 m	100 m	100 m
Block encoding	4B/5B	4B/5B	
Line encoding	MLT-3	NRZ-I	8B/6T

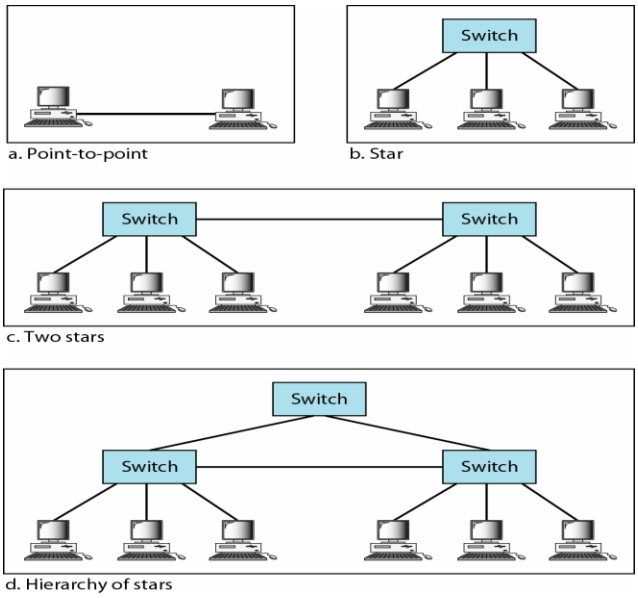
Gigabit Ethernet:

The need for an even higher data rate resulted in the design of the Gigabit Ethernet protocol (1000 Mbps).

In the full-duplex mode of Gigabit Ethernet, there is no collision; the maximum length of the cable is determined by the signal attenuation
in the cable.



Topologies of Gigabit Ethernet



- It has a data rate of100Mbps to1Gbps.

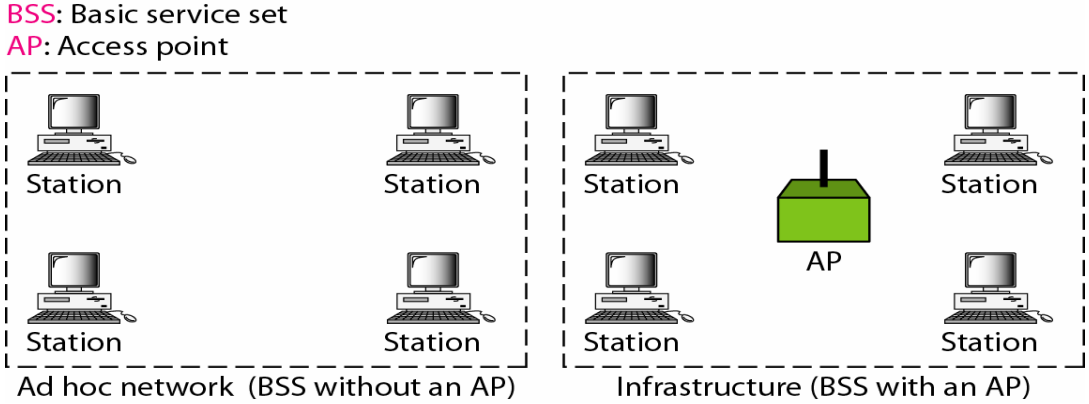
- It also having same design as in case of fast Ethernet. Only change in collisions domain &data rate.
- Gigabit Ethernet is the back bone of fast Ethernet .it may be use optical fiber or twisted pair cables.
- The implementations of gigabit Ethernet are: 1000Base LX, 1000 Base-SX.

Characteristics	*1000Base-SX*	*1000Base-LX*	*1000Base-CX*	*1000Base-T*
Media	Fiber short-wave	Fiber long-wave	STP	Cat 5 UTP
Number of wires	2	2	2	4
Maximum length	550 m	5000 m	25 m	100 m
Block encoding	8B/10B	8B/10B	8B/10B	
Line encoding	NRZ	NRZ	NRZ	4D-PAM5

3. Describe the architecture of 802.11.

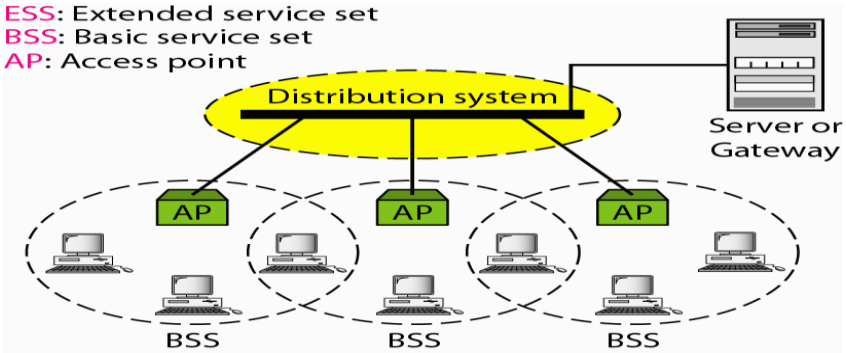
The 802.11 defines two kinds of services: Basic service set (BSS) and Extended service set (ESS).

Basic service sets (BSSs): Is made of stationary or, mobile wireless stations and a central base station known as Access point.



- A BSS without an AP is called an ad hoc network;
- A BSS with an AP is called an infrastructure network.

Extended service sets (ESS): Is made up of two or more BSS with an access point. In this case the BSS are connected through a distribution system which is usually a wired



LAN. The stations within one BSS can communicate without AP but stations from one BSS to other BSS can communicate only through AP.

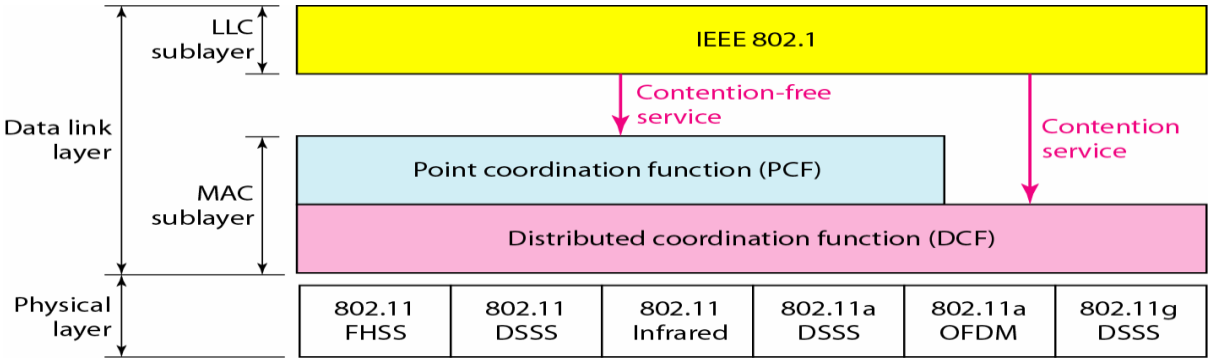
Station Types:

- **No transition:** The stations which share their information between the same BSS not to other BSS.
- **BSS transition:** The station which share their information from one BSS to other BSS but within the same ESS.
- **ESS transition:** The station which shares the information from one ESS to other.

Protocol architecture of 802.11: The IEEE 802.11 consists of physical layer and data link layer. The data link layer has two sublayers called MAC sublayer and LLC sublayer. The MAC has further two layers called point coordination function (PCF) and Distributed co-ordination function (DCF).

MAC layer: It regulates the frames properly to the exact radio frequency band so that station transmissions do not interfere with one another.

DCF: It uses CSMA/CA as the access method. Wireless LAN cannot implement CSM/CD due to the hidden station problem.



PCF: Used to provide contention free service. Higher priority traffic makes use of PCF.

LLC: It provides functions such as Error control.

Physical layer: Is been issued in three stages: first part issued in 1997 and the remaining two parts in 1999.

IEEE 802.11: It includes the MAC layer and three physical layer two in 2.4 GHz band and one in the infrared all operating at 1 and 2 Mbps.

IEEE 802.11a: Operates in the 5 GHz band at data rate up to 54 Mbps.

IEEE 802.11b: Operates in the 2.4 GHz band at data rate of 5.5 Mbps and 11 Mbps.

Three physical medias are defined in the original 802.11 standard. FHSS, DSSS and OFDM.

Spread spectrum: Involves the use of higher band width than the required data rate to minimize interference and to reduce the error rate.

FHSS (Frequency hopping spread spectrum): In this technique spread spectrum is achieved by frequency jumping from one carrier to another, if there is an interference at a given frequency it only affects a small fraction of transmission.

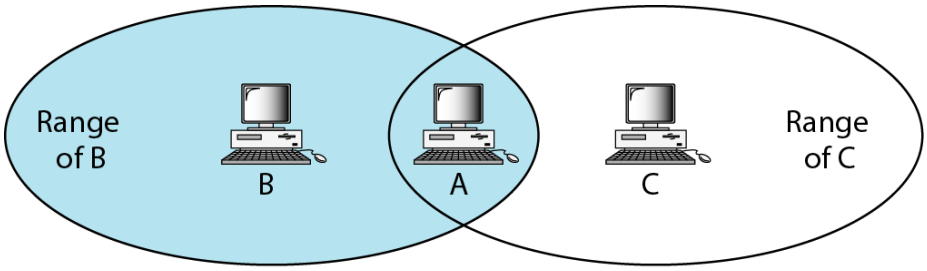
DSSS (Direct sequence spread spectrum): It increases the data rate of a signal by mapping each data bit into string of bits with one string used for binary 1 and other for binary 0.

OFDM (Orthogonal frequency division multiplexing): It uses multiple carrier signals at different frequencies; it is used in IEEE 802.11a with data rate from 6 to 54 Mbps.

4. Explain the problems in Wireless LAN and solution to solve the problem with an example.

Hidden station problem

In which a station may not be aware of another station's transmission due to some obstacles or range problems, collision may occur but not be detected.

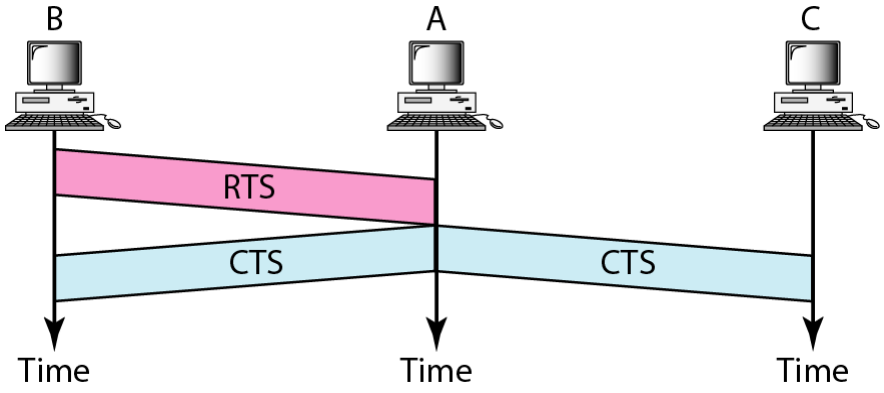


B and C are hidden from each other with respect to A.

Station B has a transmission range shown by the left oval (sphere in space); every station in this range can hear any signal transmitted by station B. Station C has a transmission range shown by the right oval (sphere in space); every station located in this range can hear any signal transmitted by C. Station C is outside the transmission range of B; likewise, station B is outside the transmission range of C. Station A, however, is in the area covered by both B and C; it can hear any signal transmitted by B or C. The figure also shows that the hidden station problem may also occur due to an obstacle.

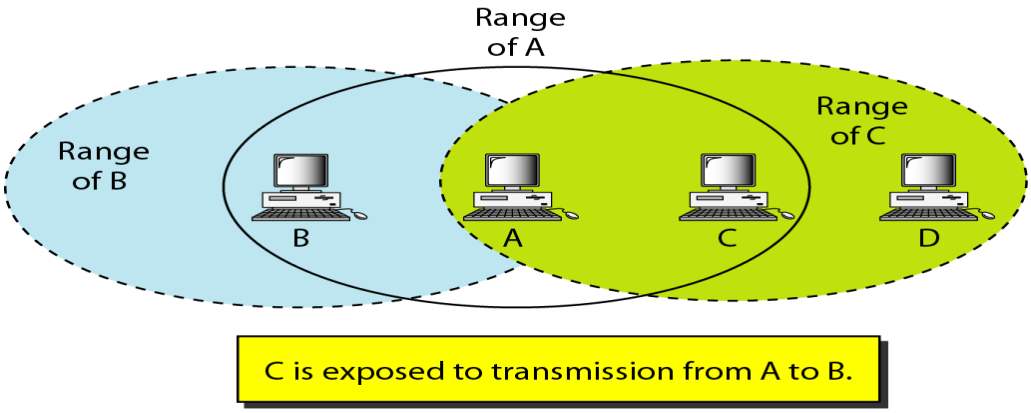
The CTS frame in CSMA/CA handshake can prevent collision from a hidden station.

Use of handshaking to prevent hidden station problem



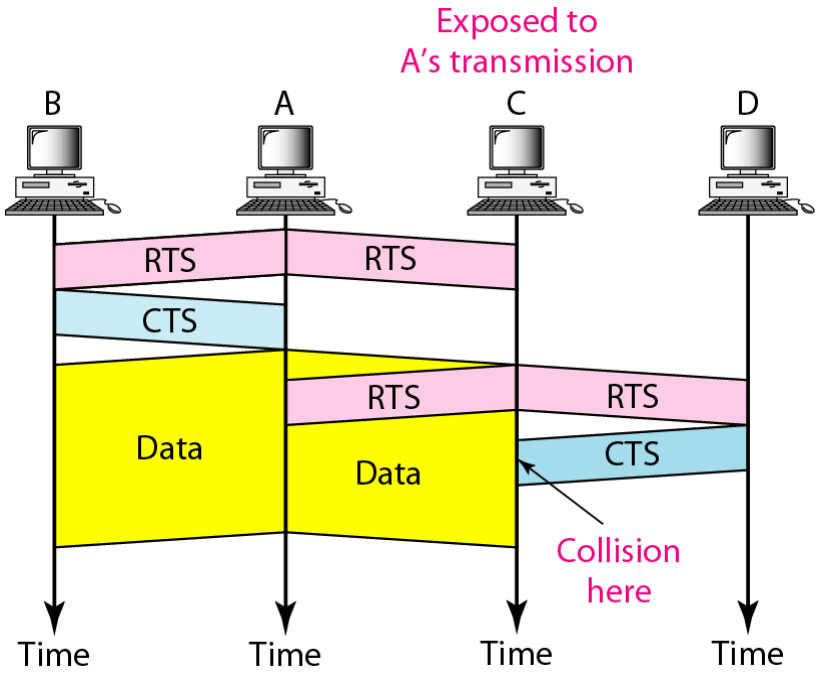
Exposed station problem

A similar problem is called the *exposed station problem*. In this problem a station refrains from using a channel when it is, in fact, available.



Station A is transmitting to station B. Station C has some data to send to station D, which can be sent without interfering with the transmission from A to B. However, station C is exposed to transmission from A; it hears what A is sending and thus refrains from sending. In other words, C is too conservative and wastes the capacity of the channel.

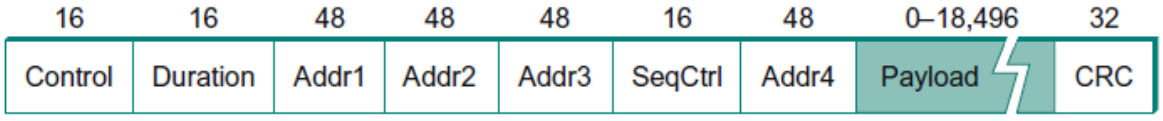
Use of handshaking in exposed station problem



5. Elaborate briefly about 802.11 frame format.

The 802.11 frame format which is depicted in the figure.

- ✓ The frame contains the source and destination node addresses, each of which is 48 bits long; up to 2312 bytes of data and 32-bit CRC.



- ✓ The Control field contains three subfields of interest

- 6 bit **Type** field: indicates whether the frame is an RTS or CTS frame or being used by the scanning algorithm
- pair of 1 bit fields : called **ToDS** and **FromDS**

✓ Frame contains four addresses, How these addresses are interpreted depends on the settings of the ToDS and FromDS bits in the frame's Control field

✓ This is to account for the possibility that the frame had to be forwarded across the distribution system.

✓ the original sender is not necessarily the same as the most recent transmitting node Same is true for the destination address

✓ Simplest case

- When one node is sending directly to another, both the DS bits are 0, Addr1 identifies the target node, and Addr2 identifies the source node

✓ Most complex case both DS bits are set to 1 Indicates that the message went from a wireless node onto the distribution system, and then from the distribution system to another wireless node

✓ ADDRESS REFERS

- Addr1 identifies the ultimate destination,
- Addr2 identifies the immediate sender (the one that forwarded the frame from the distribution system to the ultimate destination)
- Addr3 identifies the intermediate destination (the one that accepted the frame from a wireless node and forwarded across the distribution system)
- Addr4 identifies the original source

6. Explain in detail about Bluetooth.

Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers, cameras, printers, coffee makers, and so on. A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously.

Bluetooth technology has several applications. Peripheral devices such as a wireless mouse or keyboard can communicate with the computer through this technology. Monitoring devices can communicate with sensor devices in a small health care center. Home security devices can use this technology to connect different sensors to the main security controller.

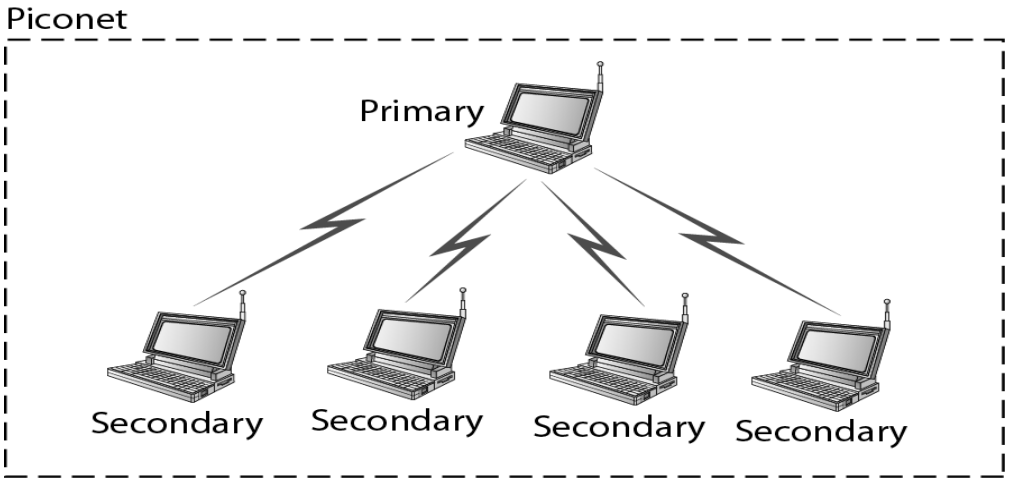
Bluetooth was originally started as a project by the Ericsson Company. It is named for Harald Blaatand, the king of Denmark (940-981) who united Denmark and Norway. *Blaatand* translates to *Bluetooth* in English.

Architecture

Bluetooth defines two types of networks: piconet and scatternet.

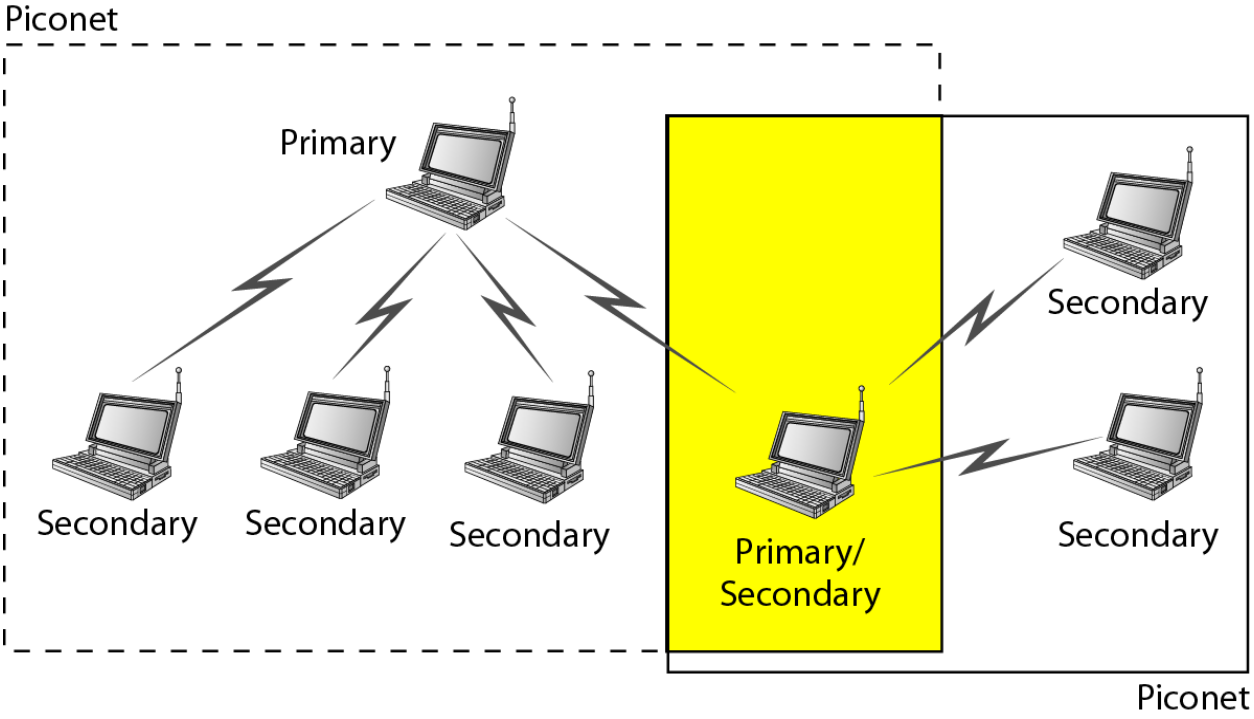
Piconets

A Bluetooth network is called a ***piconet,*** or a small net. A piconet can have up to eight stations, one of which is called the *primary;* the rest are called *secondaries.* All the secondary stations synchronize their clocks and hopping sequence with the primary. Note that a piconet can have only one primary station. The communication between the primary and secondary stations can be one-to-one or one-to-many.



Scatternet

Piconets can be combined to form what is called a ***scatternet.*** A secondary station in one piconet can be the primary in another piconet. This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet. A station can be a member of two piconets.

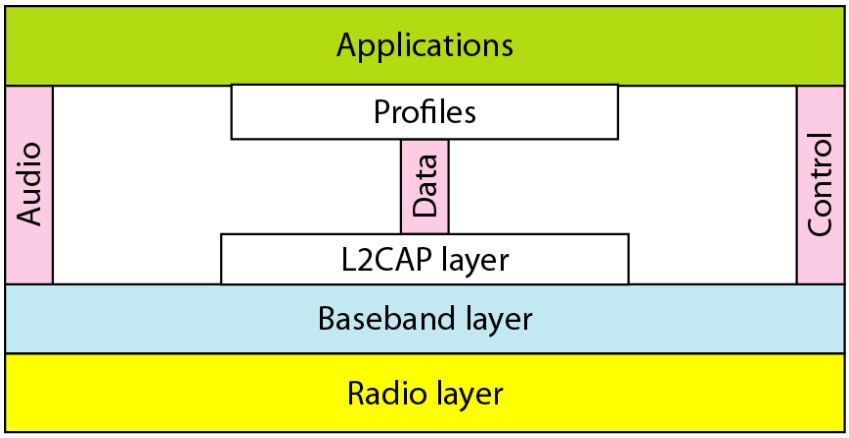


Bluetooth Devices

A Bluetooth device has a built-in short-range radio transmitter. The current data rate is 1 Mbps with a 2.4-GHz bandwidth. This means that there is a possibility of interference between the IEEE 802.11b wireless LANs and Bluetooth LANs.

Bluetooth Layers

Bluetooth uses several layers that do not exactly match those of the Internet model.



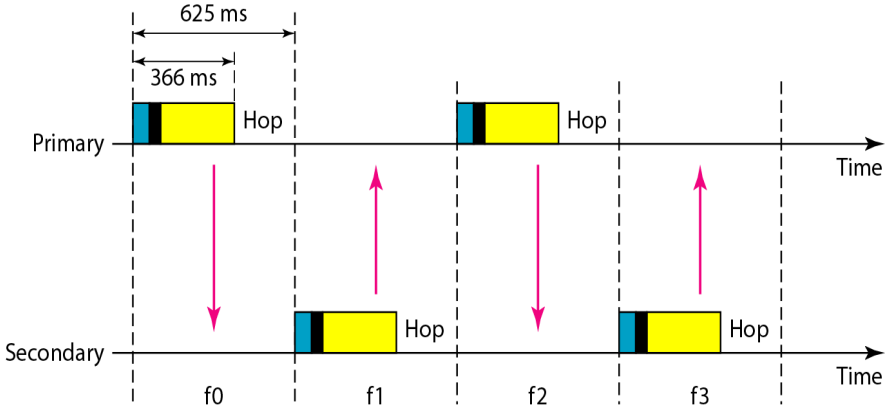
L2CAP

The **Logical Link Control and Adaptation Protocol,** or **L2CAP** (L2 here means LL), is roughly equivalent to the LLC sublayer in LANs. It is used for data exchange on an ACL link; SCO channels do not use L2CAP.

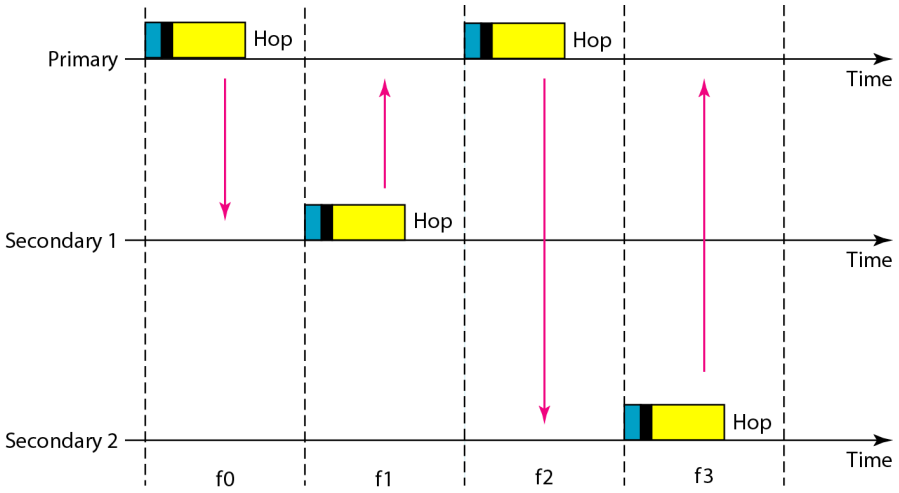
L2CAP data packet format

Bluetooth uses a form of TDMA that is called ***TDD-TDMA (time-division duplex TDMA).*** TDD-TDMA is a kind of half-duplex communication in which the sender and receiver send and receive data, but not at the same time (half-duplex); however, the communication for each direction uses different hops.

Single-Secondary Communication: If the piconet has only one secondary, the TDMA operation is very simple. The time is divided into slots of 625 µs. The primary uses even-numbered slots (0, 2, 4, . . .); the secondary uses odd-numbered slots (1, 3, 5, . . .). TDD-TDMA allows the primary and the secondary to communicate in half-duplex mode.



Multiple-Secondary Communication The process is a little more involved if there is more than one secondary in the piconet. Again, the primary uses the even-numbered slots, but a secondary sends in the next odd-numbered slot if the packet in the previous slot was addressed to it. All secondaries listen on even-numbered slots, but only one secondary sends in any odd-numbered slot.



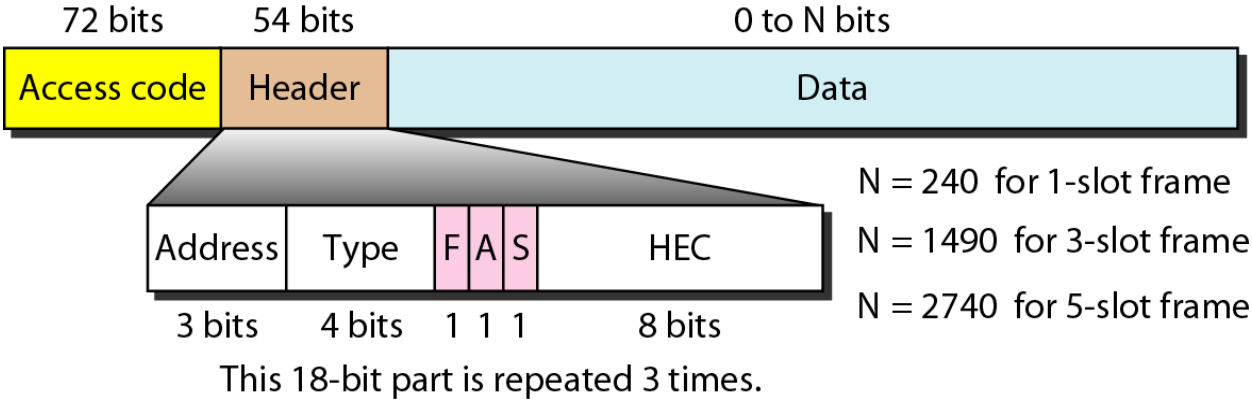
Frame Format

A frame in the baseband layer can be one of three types: one-slot, three-slot, or fiveslot.

A slot, as we said before, is 625 µs. However, in a one-slot frame exchange, 259 µs is needed for hopping and control mechanisms.

A three-slot frame occupies three slots. However, since 259 µs is used for hopping, the length of the frame is 3x625-259 = 1616 µs or 1616 bits.

A five-slot frame also uses 259 bits for hopping, which means that the length of the frame is 5x625-259 = 2866 bits.



The following describes each field:

Access code. This 72-bit field normally contains synchronization bits and the identifier of the primary to distinguish the frame of one piconet from that of another.

Header. This 54-bit field is a repeated 18-bit pattern. Each pattern has the following subfields:

a. *Address.* The 3-bit address subfield can define up to seven secondaries (1 to 7). If the address is zero, it is used for broadcast communication from the primary to all secondaries.

b. *Type.* The 4-bit type subfield defines the type of data coming from the upper layers. We discuss these types later.

c. *F*. This 1-bit subfield is for flow control. When set (1), it indicates that the device is unable to receive more frames (buffer is full).

d. *A*. This 1-bit subfield is for acknowledgment. Bluetooth uses Stop-and-Wait ARQ; 1 bit is sufficient for acknowledgment.

e. *S*. This 1-bit subfield holds a sequence number. Bluetooth uses Stop-and-Wait ARQ; 1 bit is sufficient for sequence numbering.

f. *HEC*. The 8-bit header error correction subfield is a checksum to detect errors in each 18-bit header section. The header has three identical 18-bit sections. The receiver compares these three sections, bit by bit. If each of the corresponding bits is the same, the bit is accepted; if not, the majority opinion rules.

Payload. This subfield can be 0 to 2740 bits long. It contains data or control information coming from the upper layers.

6. Discuss in detail about 6LoWPAN.

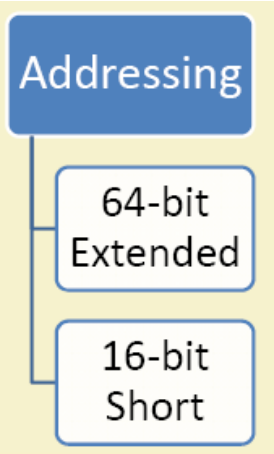
- Low-power Wireless Personal Area Networks over IPv6.
- Allows for the smallest devices with limited processing ability to transmit information wirelessly using an Internet protocol.
- Allows low-power devices to connect to the Internet.
- Created by the Internet Engineering Task Force (IETF) - RFC 5933 and RFC 4919.

Features of 6LoWPANs

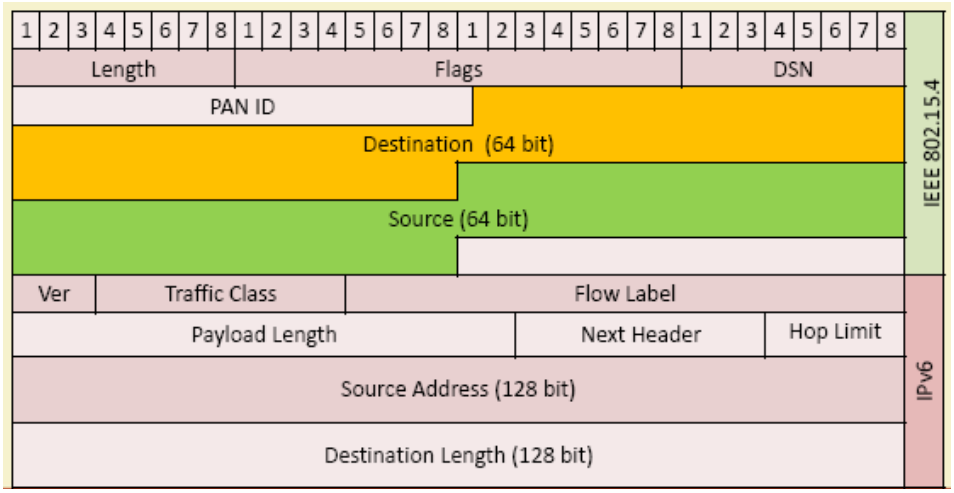
- ✓ Allows IEEE 802.15.4 radios to carry 128-bit addresses of Internet Protocol version 6 (IPv6).
- ✓ Header compression and address translation techniques allow the IEEE 802.15.4 radios to access the Internet.
- ✓ IPv6 packets compressed and reformatted to fit the IEEE 802.15.4 packet format.
- ✓ Uses include IoT, Smart grid, and M2M applications.

Addressing in 6LoWPAN

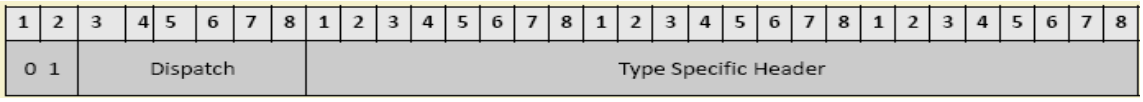
- 64-bit addresses: globally unique
- 16 bit addresses: PAN specific; assigned by PAN coordinator
- IPv6 multicast not supported by 802.15.4
- IPv6 packets carried as link layer broadcast frames.



6LowPAN Packet Format



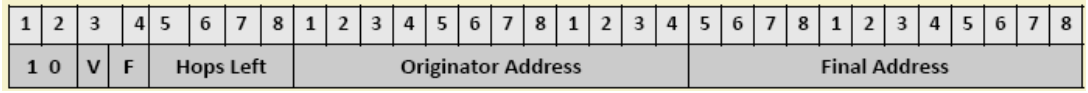
Header Type: Dispatch Header



Dispatch: Initiates communication

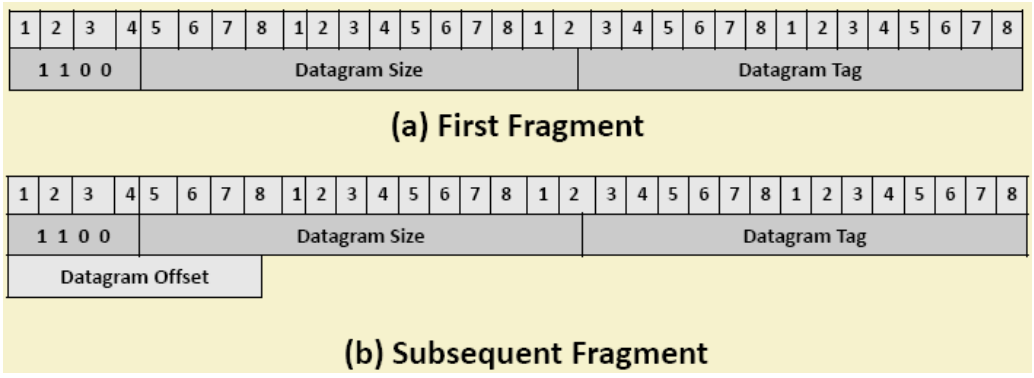
- **0,1**: Identifier for Dispatch Type
- **Dispatch**:
  - 6 bits
  - Identifies the next header type
- **Type Specific Header:**
  - Determined by Dispatch header

Header Type: Mesh Addressing Header

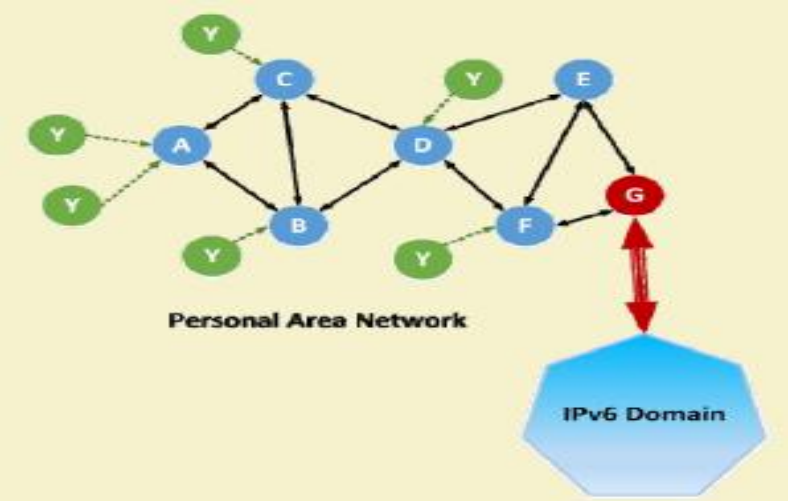


- **1,0**: ID for Mesh Addressing Header
- **V**: '0' if originator is 64-bit extended address, '1' if 16-bitaddress
- **F**: '0' if destination is 64-bit addr., '1' if 16-bit addr.
- **Hops Left**: decremented by each node before sending to next Hop

Header Type: Fragmentation Header



6LoWPAN Routing Considerations



- Mesh routing within the PAN space.
- Routing between IPv6 and the PAN domain.
- Routing protocols in use:
  - **LOADng**
  - **RPL**

LOADng Routing (*The Lightweight On-demand Ad hoc Distance-vector Routing Protocol - Next Generation)*

- Derived from AODV and extended for use in IoT.
- Basic operations of LOADng include:
  - Generation of **Route Requests (RREQs)** by a LOADng Router (originator) for discovering a route to a destination,
  - **Forwarding of such RREQs** until they reach the destination LOADng Router,
  - Generation of **Route Replies (RREPs)** upon receipt of an RREQ by the indicated destination, and unicast hop-by-hop forwarding of these RREPs towards the originator.
- If a route is detected to be broken, a **Route Error (RERR)** message is returned to the originator of that data packet to inform the originator about the route breakage.
- **Optimized flooding** is supported, reducing the overhead incurred by RREQ generation and flooding.
- Only the destination is permitted to respond to an RREQ.
- Intermediate LOADng Routers are explicitly prohibited from responding to RREQs, even if they may have active routes to the sought destination.
- RREQ/RREP messages generated by a given LOADng Router share a single unique, monotonically increasing sequence number.

RPL Routing

- Distance Vector IPv6 **routing protocol for lossy and low power networks.**
- Maintains routing topology using low rate beaconing.
- Beaconing rate increases on detecting inconsistencies (e.g. node/link in a route is down).
- Routing information included in the datagram itself.
- **Proactive**: Maintaining routing topology.
- **Reactive**: Resolving routing inconsistencies.

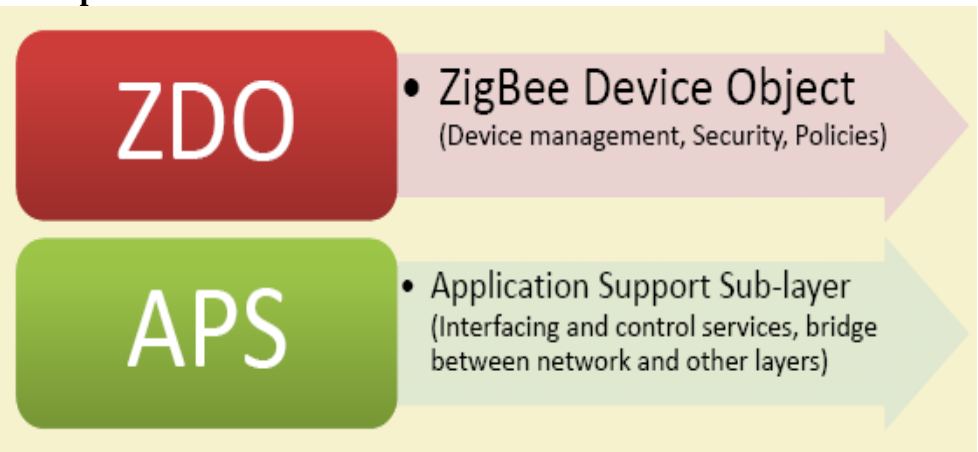
- RPL separates packet processing and forwarding from the routing optimization objective, which helps in Low power Lossy Networks (LLN).
- RPL supports message confidentiality and integrity.
- Supports Data-Path Validation and Loop Detection
- Routing optimization objectives include
  - minimizing energy
  - minimizing latency
  - satisfying constraints (w.r.t node power, bandwidth, etc.)
- RPL operations require bidirectional links.
- In some LLN scenarios, those links may exhibit asymmetric properties.
- It is required that the reachability of a router be verified before the router can be used as a parent.

7. Explain in detail about ZIGBEE.

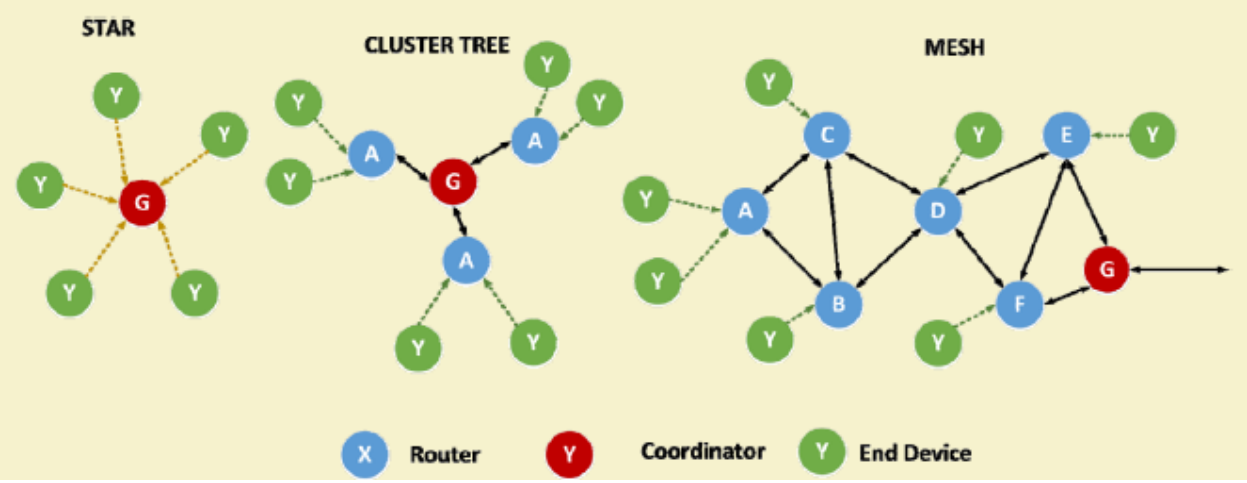
Features of ZigBee

- Most widely deployed enhancement of IEEE 802.15.4.
- The ZigBee protocol is defined by **layer 3 and above**. It works with the 802.15.4 layers 1 and 2.
- The standard uses layers 3 and 4 to define additional communication enhancements.
- These enhancements include authentication with valid nodes, encryption for security, and a data routing and forwarding capability that enables mesh networking.
- The most popular use of ZigBee is wireless sensor networks using the mesh topology.

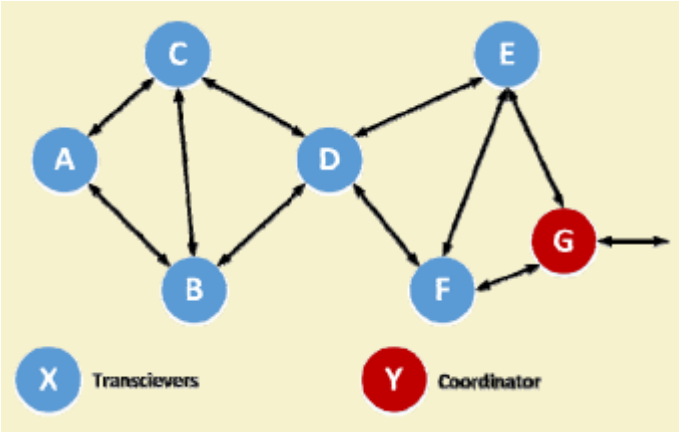
Important Components



ZigBee Topologies



ZigBee Mesh



- In a mesh, any node can communicate with any other node within its range.
- If nodes are not in range, messages are relayed through intermediate nodes.
- This allows the network deployment over large areas.
- Meshes have increased network reliability.
- For example, if nodes C and F are down, the message packets from A can still be relayed to G via B and E.
- ZigBee mesh networks are selfconfiguring and self-healing.

ZigBee Types

- *ZigBee Coordinator (ZC)*:
  - The Coordinator forms the root of the ZigBee network tree and might act as a bridge between networks.
  - There is a single ZigBee Coordinator in each network, which originally initiates the network.
  - It stores information about the network under it and outside it.
  - It acts as a Trust Center & repository for security keys.

ZigBee Types

- *ZigBee Router (ZR)*:
  - Capable of running applications, as well as relaying information between nodes connected to it.

- *ZigBee End Device (ZED)*:
    - It contains just enough functionality to talk to the parent node, and it cannot relay data from other devices.
    - This allows the node to be asleep a significant amount of the time thereby enhancing battery life.
    - Memory requirements and cost of ZEDs are quite low, as compared to ZR or ZC.

ZigBee Network Layer

- The network layer uses Ad Hoc On-Demand Distance Vector (AODV) routing.
- To find the final destination, the AODV broadcasts a route request to all its immediate neighbors.
- The neighbors relay the same information to their neighbors, eventually spreading the request throughout the network.
- Upon discovery of the destination, a low-cost path is calculated and informed to the requesting device via unicast messaging.

Applications

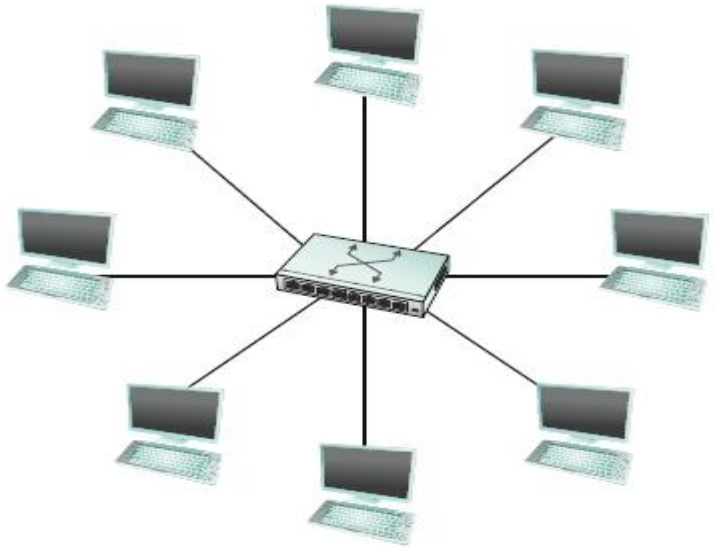
- ✓ Building automation
- ✓ Remote control (RF4CE or RF for consumer electronics)
- ✓ Smart energy for home energy monitoring
- ✓ Health care for medical and fitness monitoring
- ✓ Home automation for control of smart homes
- ✓ Light Link for control of LED lighting
- ✓ Telecom services

8. Discuss in detail about Switching with example.

A switch is a mechanism that allows us to **interconnect links to form a larger network**. A switch is a multi-input, multi-output device that transfers packets from an input to one or more outputs.

Thus, a switch adds the star topology in fig below to the point-to-point link, Bus (Ethernet), and ring topologies.

A star topology has several attractive properties:



A Switch provides a star topology

- Even though a switch has a fixed number of inputs and outputs, which limits the number of hosts that can be connected to a single switch, large networks can be built by interconnecting a number of switches.
- We can connect switches to each other and to hosts using point-to-point links, which typically means that we can build networks of large geographic scope.
- Adding a new host to the network by connecting it to a switch does not necessarily reduce the performance of the network for other hosts already connected.

For example, it is impossible for two hosts on the same 10-Mbps Ethernet segment to transmit continuously at 10 Mbps because they share the same transmission medium.

Host on a switched network has its own link to the switch, so it may be entirely possible for many hosts to transmit at the full link speed (bandwidth), providing high aggregate throughput is one of the design goals for a switch.

Switched networks are considered more ***scalable*** (i.e., more capable of growing to large numbers of nodes) than shared-media networks because of this ability to support many hosts at full speed.

A switch's primary job is to receive incoming packets on one of its links and to transmit them on some other link. This function is sometimes referred to as either *switching* or *forwarding.* Open Systems Interconnection (OSI) architecture, it is the main function of the network layer.

How does the switch decide which output link to place each packet on?

There are two common approaches.

Datagram* or *connectionless approach

Virtual circuit* or *connection-oriented approach

A third approach, ***source routing***, is less common than these other two, but it does have some useful applications.

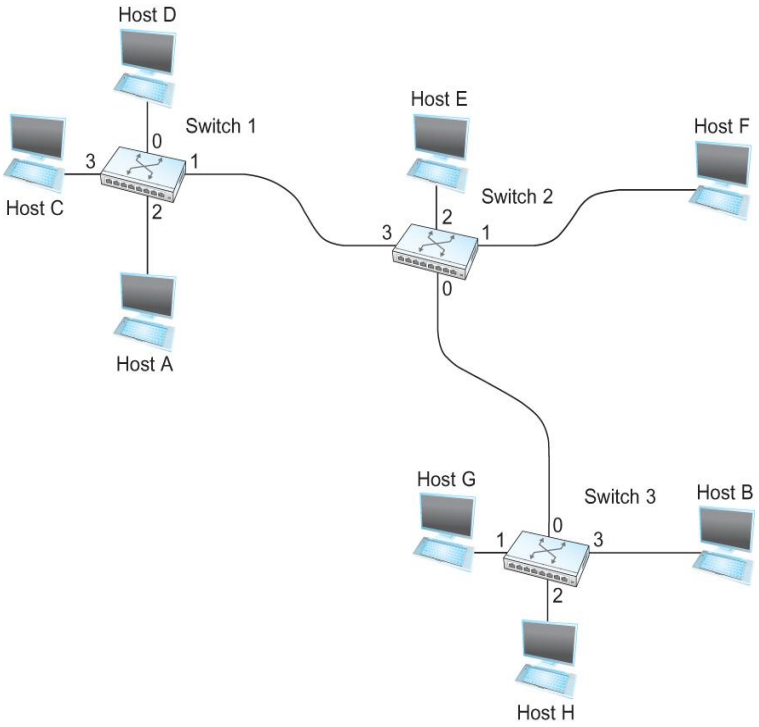
Each host has a globally unique address. There is some way to identify the input and output ports of each switch.

Datagram Approach

Key Idea of this approach

- ✓ Every packet contains enough information to enable any switch to decide how to get it to destination
- ✓ Every packet contains the complete destination address
- ✓ To decide how to forward a packet, a switch consults a ***forwarding table*** **(sometimes called a *routing table*)**

It is a lot harder to create the forwarding tables in large, complex networks with dynamically changing topologies and multiple paths between destinations. That harder problem is known as ***routing.***



Example Datagram network

Destination	Port
A	3
B	0
C	3
D	3
E	2
F	1
G	0
H	0

Forwarding Table for Switch 2

Characteristics of Connectionless (Datagram) Network

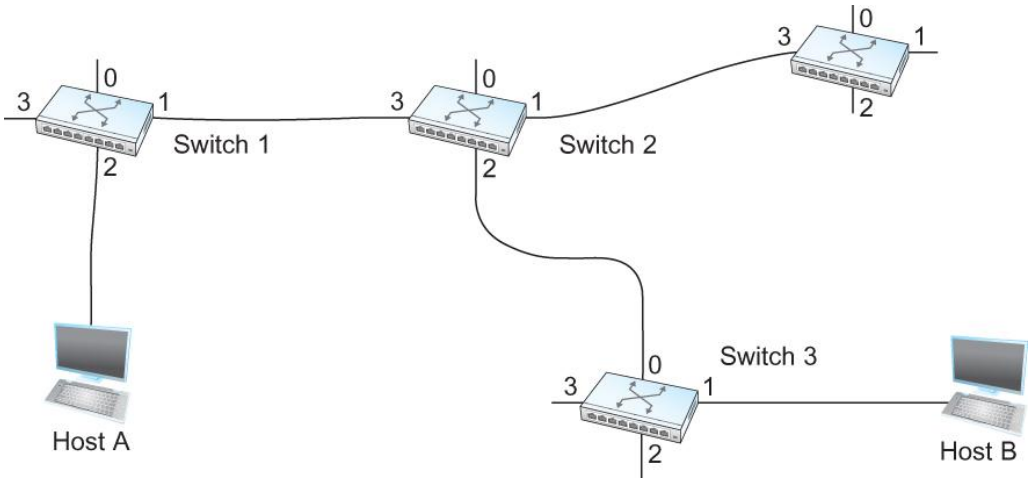
- A host can send a packet anywhere at any time, since any packet that turns up at the switch can be immediately forwarded (assuming a correctly populated forwarding table)
- When a host sends a packet, it has no way of knowing if the network is capable of delivering it or if the destination host is even up and running
- Each packet is forwarded independently of previous packets that might have been sent to the same destination.
- Thus two successive packets from host A to host B may follow completely different paths
- A switch or link failure might not have any serious effect on communication if it is possible to find an alternate route around the failure and update the forwarding table accordingly

Virtual Circuit Switching

This approach, which is called as virtual circuit (VC) also referred to as a *connection oriented model*, requires setting up a virtual connection from the source host to the destination host before any data is sent.

In fig where host A wants to send packets to host B it has two-stage process.

1. Connection setup
2. Data transfer



Example Virtual Circuit Network

In the connection setup phase, it is necessary to establish a "connection state" in each of the switches between the source and destination hosts.

The connection state for a single connection consists of an entry in a "VC table" in each switch through which the connection passes.

One entry in the VC table on a single switch contains:

- A ***virtual circuit identifier*** **(VCI)** that uniquely identifies the connection at this switch and which will be carried inside the header of the packets that belong to this connection
- An **incoming interface** on which packets for this VC arrive at the switch
- An **outgoing interface** in which packets for this VC leave the switch
- A **potentially different VCI** that will be used for outgoing packets

The semantics of one such entry is as follows:

If a packet arrives on the designated incoming interface and that packet contains the designated VCI value in its header, then that packet should be sent out the specified outgoing interface with the specified outgoing VCI value having been first placed in its header.

Note:

- The combination of the VCI of the packets as they are received at the switch and the interface on which they are received uniquely identifies the virtual connection
- There may be many virtual connections established in the switch at one time
- Incoming and outgoing VCI values are not generally the same
- VCI is not a globally significant identifier for the connection; rather it has significance only on a given link
- Whenever a new connection is created, we need to assign a new VCI for that connection on each link that the connection will traverse.

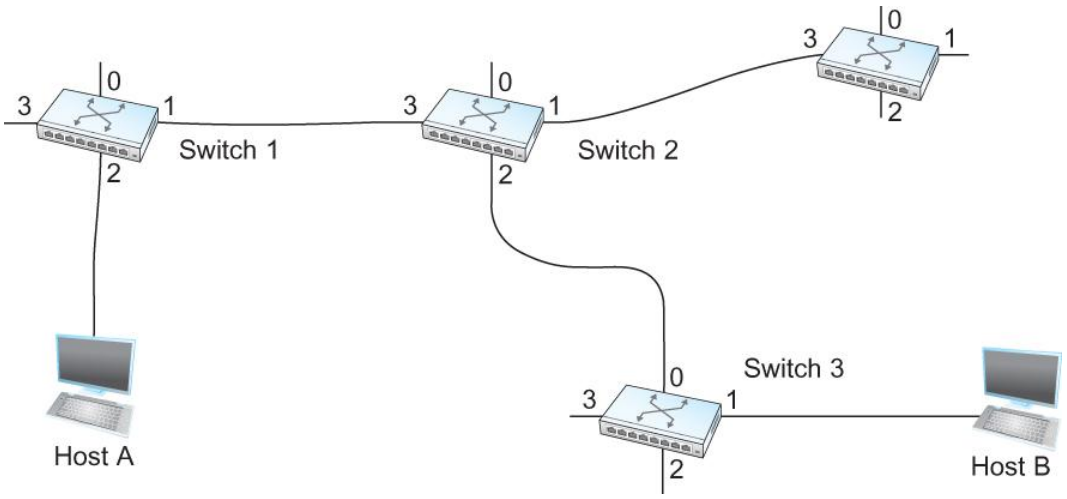
- We also need to ensure that the chosen VCI on a given link is not currently in use on that link by some existing connection.

Two broad classes of approach to establishing connection state

- Network Administrator will configure the state in which The virtual circuit is permanent (PVC)
- A host can send messages into the network to cause the state to be established
  - This is referred as signaling and the resulting virtual circuit is said to be switched (SVC)
  - A host may set up and delete such a VC dynamically without the involvement of a network administrator

Let's assume that a network administrator wants to manually create a new virtual connection from host A to host B

- ✓ First the administrator identifies a path through the network from A to B
- ✓ The administrator then picks a VCI value that is currently unused on each link for the connection



For our example,

- ✓ Suppose the VCI value 5 is chosen for the link from host A to switch 1
- ✓ 11 is chosen for the link from switch 1 to switch 2
- ✓ So the switch 1 will have an entry in the VC table

Incoming Interface	Incoming VC	Outgoing Interface	Outgoing VC
2	5	1	11

Virtual Circuit Table Entry for Table Switch 1

Similarly, suppose

VCI of 7 is chosen to identify this connection on the link from switch 2 to switch 3

VCI of 4 is chosen for the link from switch 3 to host B

Switches 2 and 3 are configured with the following VC table

Incoming Interface	Incoming VC	Outgoing Interface	Outgoing VC
3	11	2	7

Incoming Interface	Incoming VC	Outgoing Interface	Outgoing VC
0	7	1	4

For any packet that A wants to send to B, A puts the VCI value 5 in the header of the packet and sends it to switch 1

Switch 1 receives any such packet on interface 2, and it uses the combination of the interface and the VCI in the packet header to find the appropriate VC table entry.

The table entry on switch 1 tells the switch to forward the packet out of interface 1 and to put the VCI value 11 in the header

Packet will arrive at switch 2 on interface 3 bearing VCI 11.Switch 2 looks up interface 3 and VCI 11 in its VC table and sends the packet on to switch 3 after updating the VCI value appropriately. This process continues until it arrives at host B with the VCI value of 4 in the packet.To host B, this identifies the packet as having come from host A.

In real networks of reasonable size, the burden of configuring VC tables correctly in a large number of switches would quickly become excessive

- ✓ Thus, some sort of signaling is almost always used, even when setting up "permanent" VCs
- ✓ In case of PVCs, signaling is initiated by the network administrator
- ✓ SVCs are usually set up using signaling by one of the hosts.
- ✓ How does the signaling work
    - o To start the signaling process, host A sends a setup message into the network (i.e. to switch 1)
        - The setup message contains (among other things) the complete destination address of B.
        - The setup message needs to get all the way to B to create the necessary connection state in every switch along the way
        - It is like sending a datagram to B where every switch knows which output to send the setup message so that it eventually reaches B
        - Assume that every switch knows the topology to figure out how to do that
    - o When switch 1 receives the connection request, in addition to sending it on to switch 2, it creates a new entry in its VC table for this new connection
        - The entry is exactly the same shown in the previous table
        - Switch 1 picks the value 5 for this connection
    - o When switch 2 receives the setup message, it performs the similar process and it picks the value 11 as the incoming VCI
    - o Similarly switch 3 picks 7 as the value for its incoming VCI
        - Each switch can pick any number it likes, as long as that number is not currently in use for some other connection on that port of that switch
    - o Finally the setup message arrives at host B.

- Assuming that B is healthy and willing to accept a connection from host A, it allocates an incoming VCI value, in this case 4.
  - This VCI value can be used by B to identify all packets coming from A

✓ Now to complete the connection, everyone needs to be told what their downstream neighbor is using as the VCI for this connection

- Host B sends an acknowledgement of the connection setup to switch 3 and includes in that message the VCI value that it chose (4)
- Switch 3 completes the VC table entry for this connection and sends the acknowledgement on to switch 2 specifying the VCI of 7
- Switch 2 completes the VC table entry for this connection and sends acknowledgement on to switch 1 specifying the VCI of 11
- Finally switch 1 passes the acknowledgement on to host A telling it to use the VCI value of 5 for this connection.

✓ When host A no longer wants to send data to host B, it tears down the connection by sending a teardown message to switch 1

✓ The switch 1 removes the relevant entry from its table and forwards the message on to the other switches in the path which similarly delete the appropriate table entries

✓ At this point, if host A were to send a packet with a VCI of 5 to switch 1, it would be dropped as if the connection had never existed.

✓ **Characteristics of VC**

- Since host A has to wait for the connection request to reach the far side of the network and return before it can send its first data packet, there is at least one RTT of delay before data is sent
- While the connection request contains the full address for host B (which might be quite large, being a global identifier on the network), each data packet contains only a small identifier, which is only unique on one link.

✓ Thus the per-packet overhead caused by the header is reduced relative to the datagram model

✓ If a switch or a link in a connection fails, the connection is broken and a new one will need to be established.

✓ Also the old one needs to be torn down to free up table storage space in the switches

✓ The issue of how a switch decides which link to forward the connection request on has similarities with the function of a routing algorithm

SOURCE ROUTING

A third approach to switching uses neither virtual circuits nor conventional datagram's is known as ***source routing***.

The name derives from the fact that all the information about network topology that is required to switch a packet across the network is provided by the source host.There are various ways to implement source routing.

One would be to assign a number to each output of each switch and to place that number in the header of the packet.

For each packet that arrives on an input, the switch would read the port number in the header and transmit the packet on that output.

However, since there will in general be more than one switch in the path between the sending and the receiving host, the header for the packet needs to contain enough information to allow every switch in the path to determine which output the packet needs to be placed on.

This would be to put an ordered list of switch ports in the header and to rotate the list so that the next switch in the path is always at the front of the list.

Fig illustrates this idea.

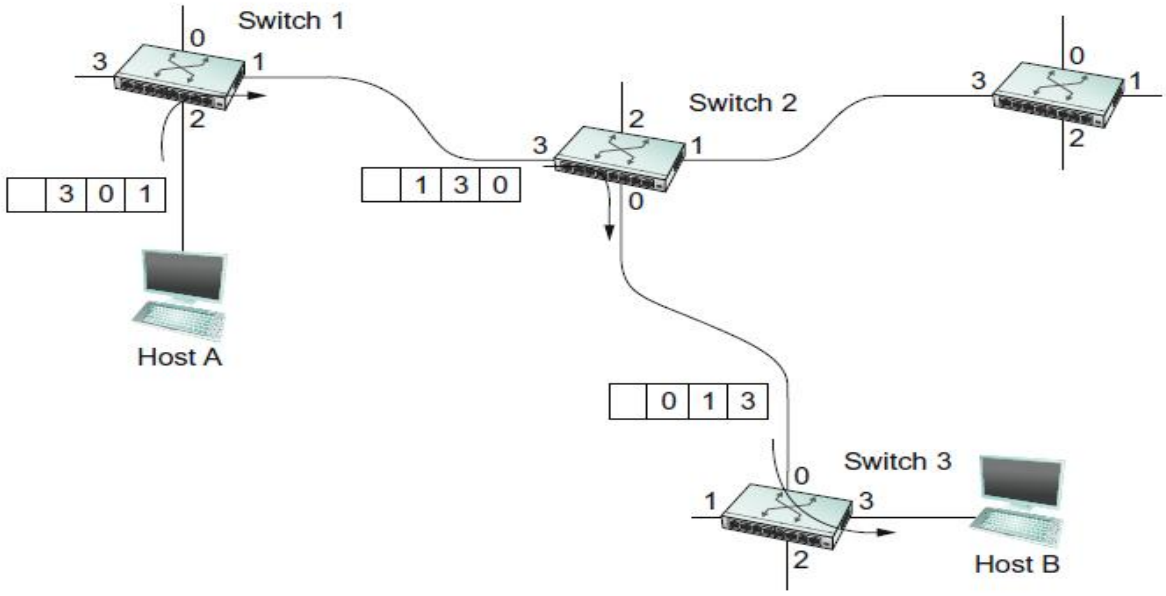
In this example,

The packet needs to traverse three switches to get from host A to host B.

At switch 1, it needs to exit on port 1, at the next switch it needs to exit at port 0, and at the third switch it needs to exit at port 3.

Thus, the original header when the packet leaves host A contains the list of ports (3, 0, 1), where we assume that each switch reads the rightmost element of the list.

To make sure that the next switch gets the appropriate information, each switch rotates the list after it has read its own entry. Thus, the packet header as it leaves switch 1 en route to switch 2 is now (1, 3, 0); switch 2 performs another rotation and sends out a packet with (0, 1, 3) in the header. Although not shown, switch 3 performs yet another rotation, restoring the header to what it was when host A sent it.

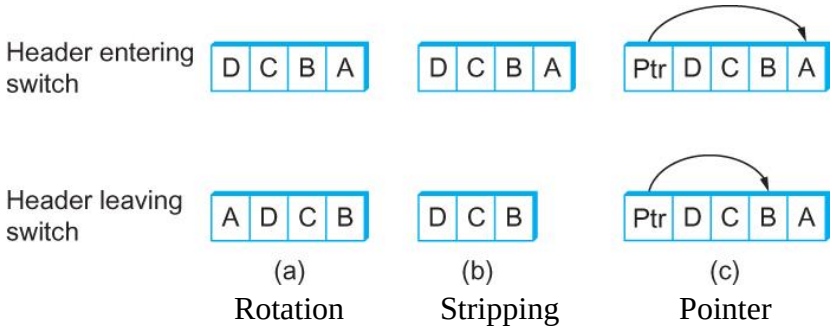


Source routing

There are several things to note about this approach.

1. Host A knows enough about the topology of the network to form header that direct every switch in the path.
2. We cannot predict how big the header needs to be, since it must be able to hold one word of information for every switch on the path.
3. It is different mechanism
   - Rotate the header; each switch could just strip the first element as it uses it.

- Rotation has an advantage over stripping, however: Host B gets a copy of the complete header, which may help it figure out how to get back to host A.
- The header carry a pointer to the current "next port" entry, so that each switch just updates the pointer rather than rotating the header



9. Illustrate about IPv4 addresses.

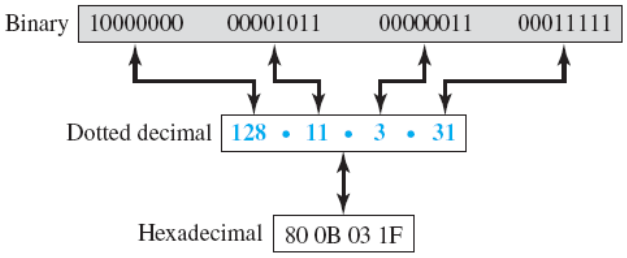
An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device (for example, a computer or a router) to the Internet.

Address Space

A protocol like IPv4 that defines addresses has an address space. An **address space** is the total number of addresses used by the protocol. If a protocol uses *b* bits to define an address, the address space is 2*b* because each bit can have two different values (0 or 1).

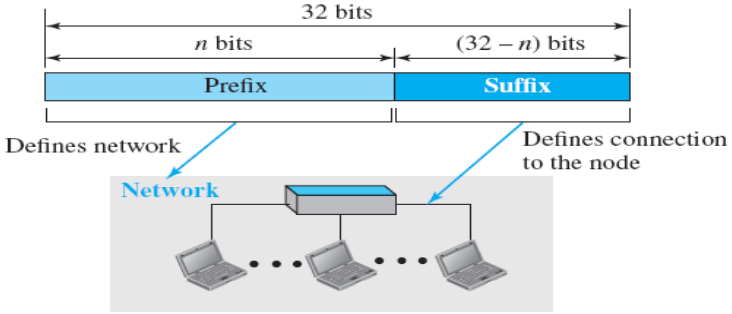
IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296 (more than four billion). If there were no restrictions, more than 4 billion devices could be connected to the Internet.

Three different notations in IPv4 addressing



Hierarchy in Addressing

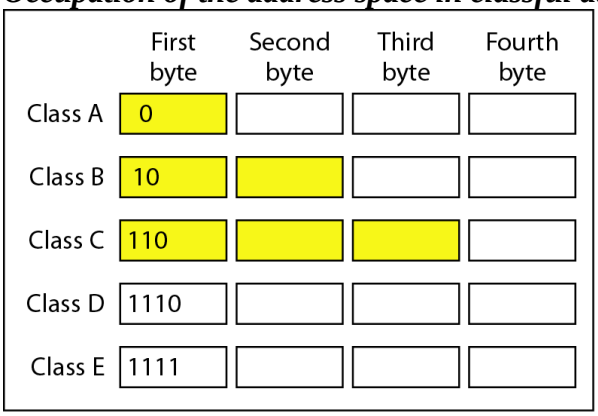
A 32-bit IPv4 address is also hierarchical, but divided only into two parts. The first part of the address, called the *prefix*, defines the network; the second part of the address, called the *suffix*, defines the node (connection of a device to the Internet).



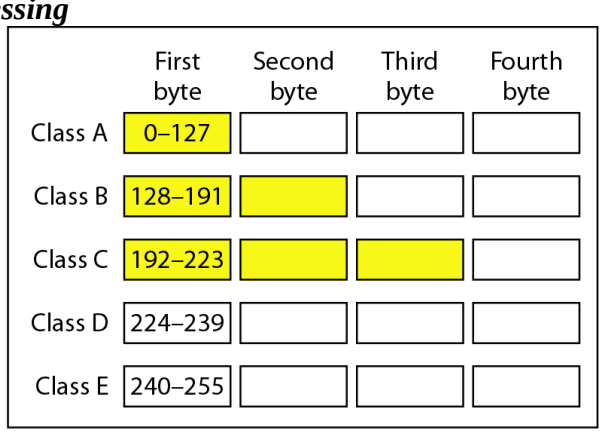
Classful Addressing

When the Internet started, an IPv4 address was designed with a fixed-length prefix, but to accommodate both small and large networks, three fixed-length prefixes were designed instead of one (n = 8, n = 16, and n = 24). The whole address space was divided into five classes (class A, B, C, D, and E). This scheme is referred to as **classful addressing.**

Occupation of the address space in classful addressing



a. Binary notation



b. Dotted-decimal notation

Address Depletion

The reason that classful addressing has become obsolete is address depletion. Since the addresses were not distributed properly, the Internet was faced with the problem of the addresses being rapidly used up, resulting in no more addresses available for organizations and individuals that needed to be connected to the Internet.

Number of blocks and block size in classful IPv4 addressing

Class	*Number of Blocks*	*Block Size*	*Application*
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved

Default masks for classful addressing

Class	*Binary*	*Dotted-Decimal*	*CIDR*
A	**11111111** 00000000 00000000 00000000	**255**.0.0.0	/8
B	**11111111 11111111** 00000000 00000000	**255.255**.0.0	/16
C	**11111111 11111111 11111111** 00000000	**255.255.255**.0	/24

Subnetting and Supernetting

To alleviate address depletion, two strategies were proposed and, to some extent, implemented: subnetting and supernetting.

In subnetting, a class A or class B block is divided into several subnets. Each subnet has a larger prefix length than the original network. For example, if a network in class A is divided into four subnets, each subnet has a prefix of $n_{sub} = 10$. At the same time, if all of the addresses in a network are not used, subnetting allows the addresses to be divided among several organizations. This idea did not work because most large organizations were not happy about dividing the block and giving some of the unused addresses to smaller organizations.

While subnetting was devised to divide a large block into smaller ones, supernetting was devised to combine several class C blocks into a larger block to be attractive to organizations that need more than the 256 addresses available in a class C block. This idea did not work either because it makes the routing of packets more difficult.

Advantage of Classful Addressing

Given an address, we can easily find the class of the address and, since the prefix length for each class is fixed, we can find the prefix length immediately. In other words, the prefix length in classful addressing is inherent in the address; no extra information is needed to extract the prefix and the suffix.

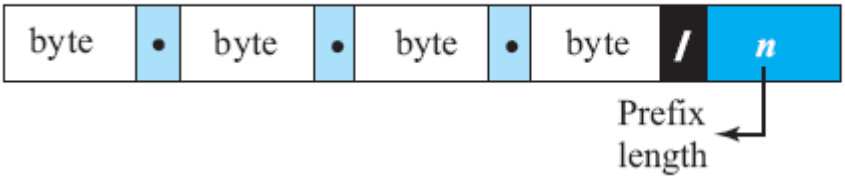
Classless Addressing

The short-term solution still uses IPv4 addresses, but it is called *classless addressing*. In other words, the class privilege was removed from the distribution to compensate for the address depletion.

In classless addressing, variable-length blocks are used that belong to no classes. We can have a block of 1 address, 2 addresses, 4 addresses, 128 addresses, and so on.

In classless addressing, the whole address space is divided into variable length blocks. The prefix in an address defines the block (network); the suffix defines the node (device). Theoretically, we can have a block of $2^0, 2^1, 2^2, \ldots, 2^{32}$ addresses.

In this case, the prefix length, *n*, is added to the address, separated by a slash. The notation is informally referred to as *slash notation* and formally as ***classless interdomain routing*** or ***CIDR*** (pronounced cider) strategy.



Examples:
12.24.76.8/8
23.14.67.92/12
220.8.24.255/25

Extracting Information from an Address

Given any address in the block, we normally like to know three pieces of information about the block to which the address belongs: the number of addresses, the first address in the block, and the last address. Since the value of prefix length, *n*, is given, we can easily find these three pieces of information,

1. The number of addresses in the block is found as $N = 2^{32-n}$

2. To find the first address, we keep the *n* leftmost bits and set the (32 - *n*) rightmost bits all to 0s.

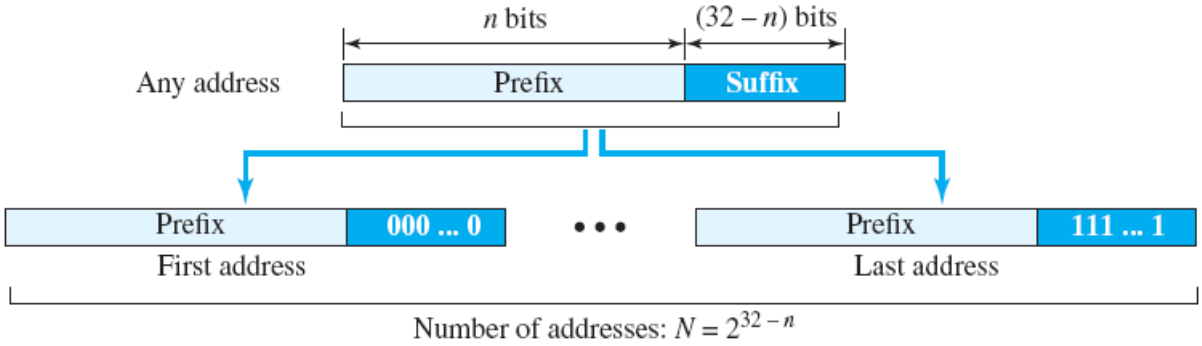
3. To find the last address, we keep the *n* leftmost bits and set the (32 - *n*) rightmost bits all to 1s.

Example 1:

A classless address is given as 167.199.170.82/**27**. We can find the above three pieces of information as follows.

The number of addresses in the network is $2^{32-n} = 2^5 = 32$ addresses.

Information extraction in classless addressing



The first address can be found by keeping the first 27 bits and changing the rest of the bits to 0s.

Address: 167.199.170.82/**27** 10100111 11000111 10101010 010**10010**

First address: 167.199.170.64/**27** 10100111 11000111 10101010 010**00000**

The last address can be found by keeping the first 27 bits and changing the rest of the bits to 1s.

Address: 167.199.170.82/**27** 10100111 11000111 10101010 010**11111**

Last address: 167.199.170.95/**27** 10100111 11000111 10101010 010**11111**

Example 2:

An ISP is granted a block of addresses starting with 190.100.0.0/16 (65,536 addresses). The ISP needs to distribute these addresses to three groups of customers as follows:

a. The first group has 64 customers; each needs 256 addresses.

b. The second group has 128 customers; each needs 128 addresses.

c. The third group has 128 customers; each needs 64 addresses.

Design the subblocks and find out how many addresses are still available after these allocations.

Solution

Group 1

For this group, each customer needs 256 addresses. This means that 8 (log2 256) bits are needed to define each host. The prefix length is then 32 − 8 = 24. The addresses are

1st Customer:	190.100.0.0/24	190.100.0.255/24
2nd Customer:	190.100.1.0/24	190.100.1.255/24
. . .		
64th Customer:	190.100.63.0/24	190.100.63.255/24
Total = 64 × 256 = 16,384		

Group 2

For this group, each customer needs 128 addresses. This means that 7 (log2 128) bits are needed to define each host. The prefix length is then 32 − 7 = 25. The addresses are

1st Customer:	190.100.64.0/25	190.100.64.127/25
2nd Customer:	190.100.64.128/25	190.100.64.255/25
. . .		
128th Customer:	190.100.127.128/25	190.100.127.255/25
Total = 128 × 128 = 16,384		

Group 3

For this group, each customer needs 64 addresses. This means that 6 ($\log_2 64$) bits are needed to each host. The prefix length is then 32 − 6 = 26. The addresses are

1st Customer:	190.100.128.0/26	190.100.128.63/26
2nd Customer:	190.100.128.64/26	190.100.128.127/26
. . .		
128th Customer:	190.100.159.192/26	190.100.159.255/26
Total = 128 × 64 = 8192		

Number of granted addresses to the ISP: 65,536

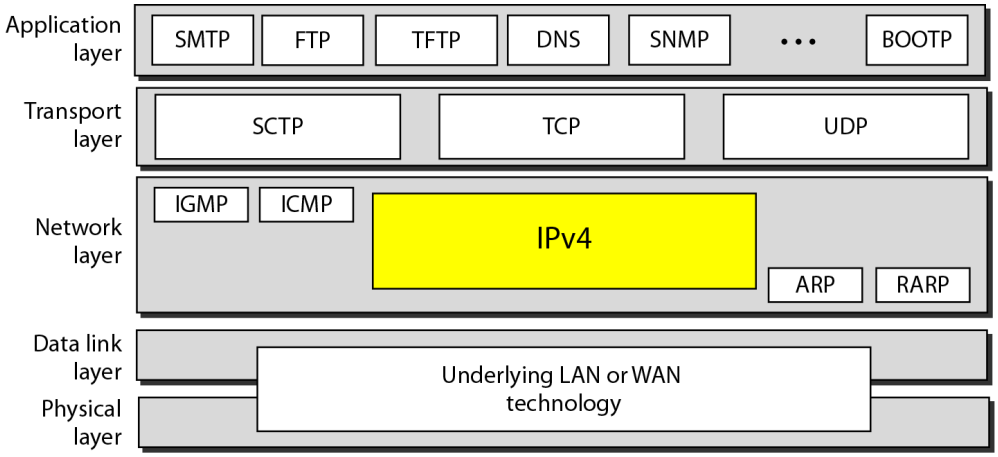
Number of allocated addresses by the ISP: 40,960

Number of available addresses: 24,576

10. Elaborate the Internet Protocol in detail.

The network layer in version 4 can be thought of as one main protocol and three auxiliary ones. The main protocol, Internet Protocol version 4 (IPv4), is responsible for packetizing, forwarding, and delivery of a packet at the network layer.

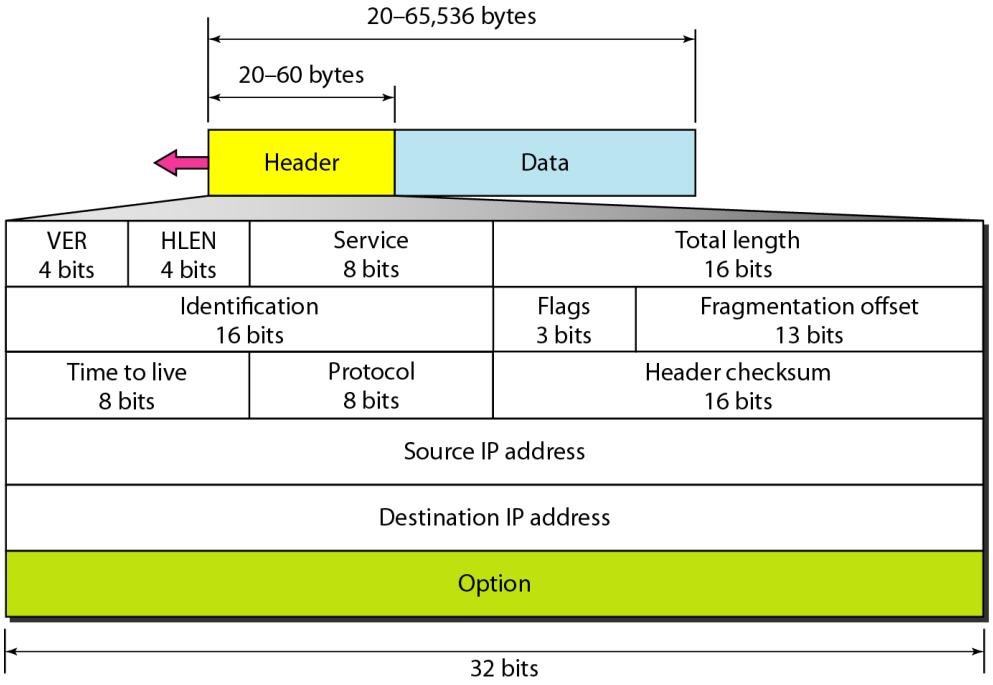
Position of IP and other network-layer protocols in TCP/IP protocol suite



IPv4 is an unreliable datagram protocol—a best-effort delivery service. The term *best-effort* means that IPv4 packets can be corrupted, be lost, arrive out of order, or be delayed, and may create congestion for the network. If reliability is important, IPv4 must be paired with a reliable transport-layer protocol such as TCP.

IPv4 is also a connectionless protocol that uses the datagram approach. This means that each datagram is handled independently, and each datagram can follow a different route to the destination. This implies that datagrams sent by the same source to the same destination could arrive out of order. Again, IPv4 relies on a higher-level protocol to take care of all these problems.

Datagram Format



- ✓ ***Version Number.*** The 4-bit version number (VER) field defines the version of the IPv4 protocol, which, obviously, has the value of 4.
- ✓ ***Header Length.*** The 4-bit header length (HLEN) field defines the total length of the datagram header in 4-byte words. The IPv4 datagram has a variable-length header. The

total length is divided by 4 and the value is inserted in the field. The receiver needs to multiply the value of this field by 4 to find the total length.

- ✓ ***Service Type.*** In the original design of the IP header, this field was referred to as type of service (TOS), which defined how the datagram should be handled. In the late 1990s, IETF redefined the field to provide *differentiated services* (DiffServ).
- ✓ ***Total Length.*** This 16-bit field defines the total length (header plus data) of the IP datagram in bytes. A 16-bit number can define a total length of up to 65,535 (when all bits are 1s).

Length of data = total length - (HLEN) x 4

- ✓ ***Identification, Flags, and Fragmentation Offset.*** These three fields are related to the fragmentation of the IP datagram when the size of the datagram is larger than the underlying network can carry.
- ✓ ***Time-to-live.*** Due to some malfunctioning of routing protocols (discussed later) a datagram may be circulating in the Internet, visiting some networks over and over without reaching the destination. This may create extra traffic in the Internet. The time-to-live (TTL) field is used to control the maximum number of hops (routers) visited by the datagram.
- ✓ ***Protocol.*** In TCP/IP, the data section of a packet, called the *payload,* carries the whole packet from another protocol. A datagram, for example, can carry a packet belonging to any transport-layer protocol such as UDP or TCP.

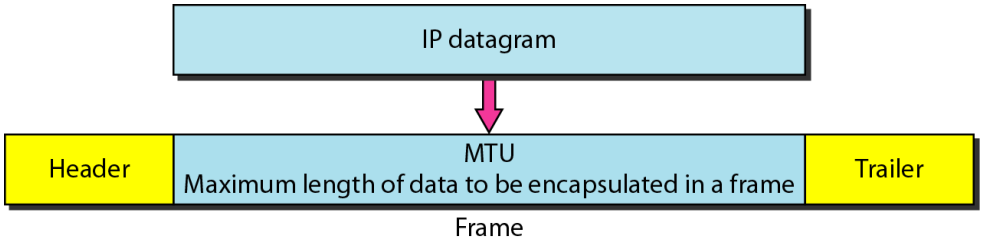
Fragmentation

A datagram can travel through different networks. Each router decapsulates the IP datagram from the frame it receives, processes it, and then encapsulates it in another frame. The format and size of the received frame depend on the protocol used by the physical network through which the frame has just traveled. The format and size of the sent frame depend on the protocol used by the physical network through which the frame is going to travel.

Flags used in fragmentation

Maximum Transfer Unit (MTU)

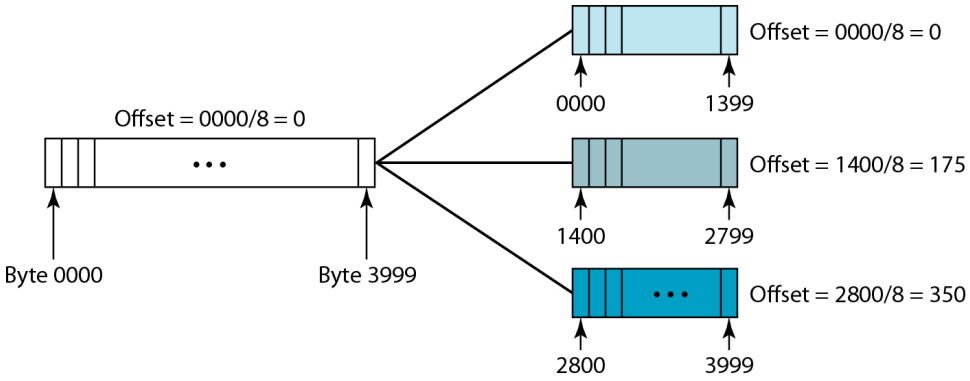
Each link-layer protocol has its own frame format. One of the features of each format is the maximum size of the payload that can be encapsulated. In other words, when a datagram is encapsulated in a frame, the total size of the datagram must be less than this maximum size, which is defined by the restrictions imposed by the hardware and software used in the network



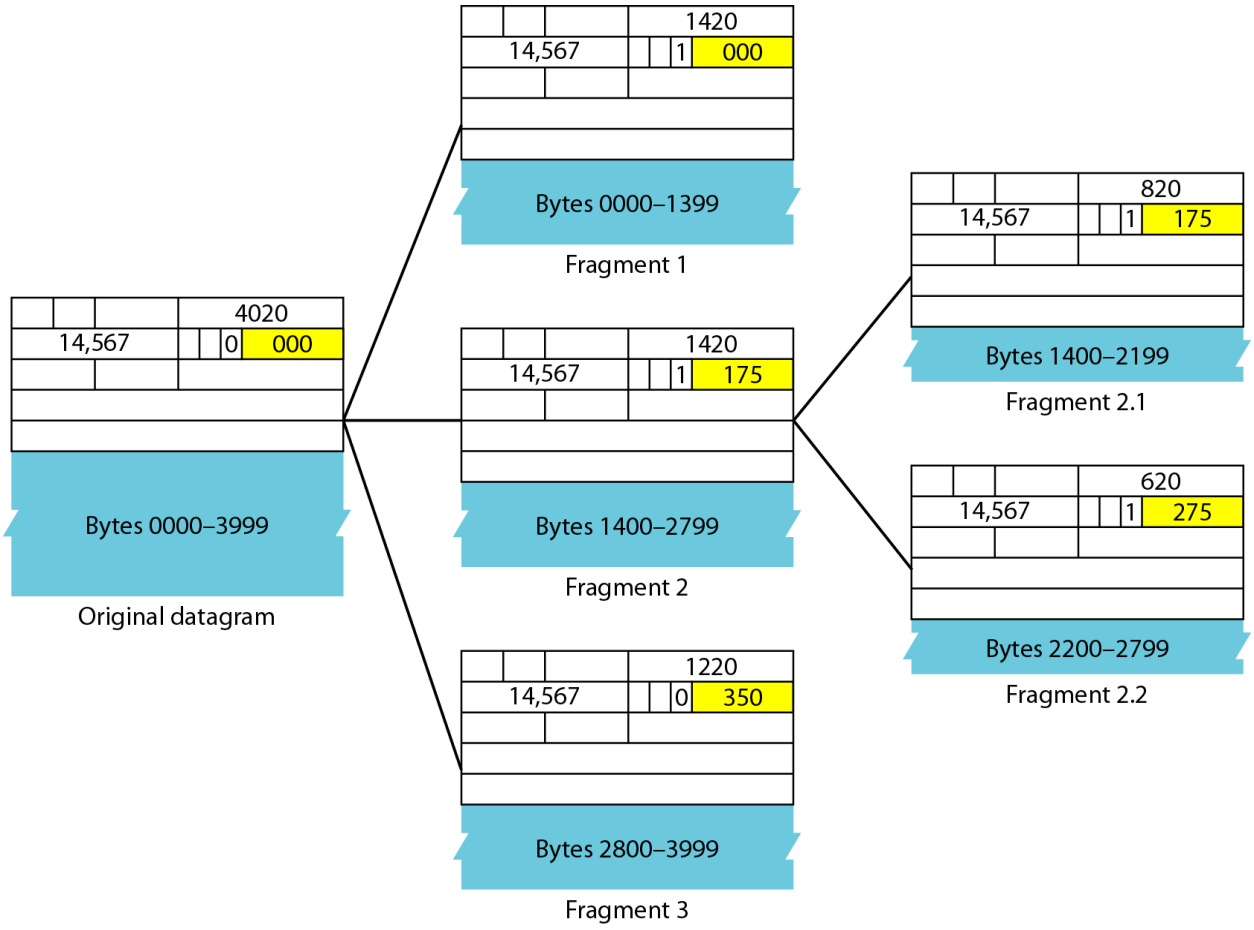
In order to make the IP protocol independent of the physical network, the designers decided to make the maximum length of the IP datagram equal to 65,535 bytes. This makes transmission more efficient if one day we use a link-layer protocol with an MTU of this size. However, for other physical networks, we must divide the datagram to make it possible for it to pass through these networks. This is called ***fragmentation.***

The ***reassembly*** of the datagram, however, is done only by the destination host, because each fragment becomes an independent datagram. Whereas the fragmented datagram can travel through different routes, and we can never control or guarantee which route a fragmented datagram may take, all of the fragments belonging to the same datagram should finally arrive at the destination host. So it is logical to do the reassembly at the final destination. An even stronger objection for reassembling packets during the transmission is the loss of efficiency it incurs.

Fragmentation Example:



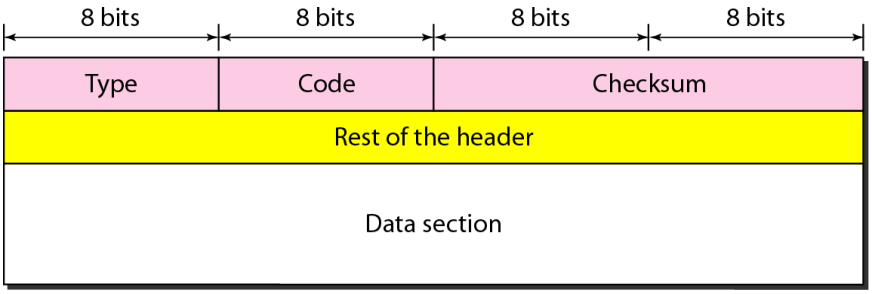
Detailed fragmentation example



11. Discuss in detail about ICMP.

The IP protocol has no error-reporting or error-correcting mechanism. The IP protocol also lacks a mechanism for host and management queries. The Internet Control Message Protocol (ICMP) has been designed to compensate for the above two deficiencies. It is a companion to the IP protocol.

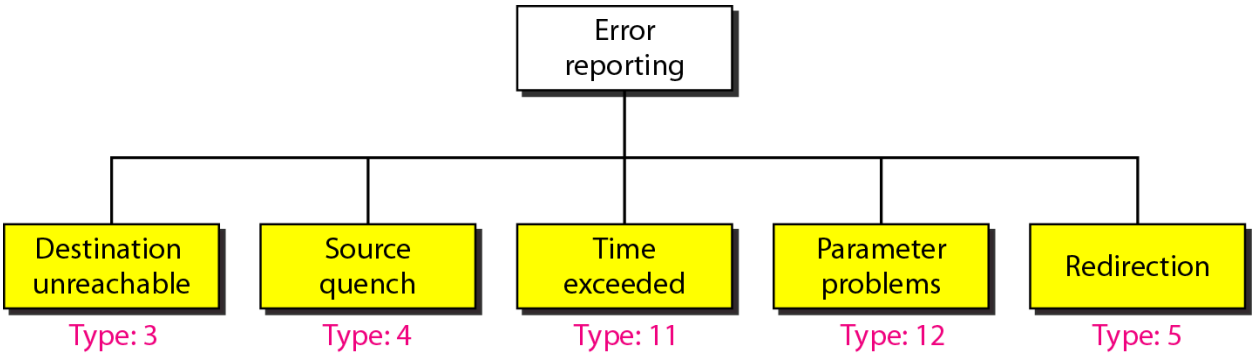
General format of ICMP messages



MESSAGES

- ICMP messages are divided into two broad categories: *error-reporting messages* and *query messages.*
- The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet.
- The query messages, which occur in pairs, help a host or a network manager get specific information from a router or another host.

Error-reporting messages



Destination Unreachable

The most widely used error message is the destination unreachable (type 3). This message uses different codes (0 to 15) to define the type of error message and the reason why a datagram has not reached its final destination.

Source Quench

Another error message is called the *source quench* (type 4) message, which informs the sender that the network has encountered congestion and the datagram has been dropped; the source needs to slow down sending more datagrams. In other words, ICMP adds a kind of congestion control mechanism to the IP protocol by using this type of message.

Time exceeded

When the TTL value becomes 0, the datagram is dropped by the visiting router and a *time exceeded* message (type 11) with code 0 is sent to the source to inform it about the situation. The

time-exceeded message (with code 1) can also be sent when not all fragments of a datagram arrive within a predefined period of time.

Redirection Message

The *redirection message* (type 5) is used when the source uses a wrong router to send out its message. The router redirects the message to the appropriate router, but informs the source that it needs to change its default router in the future. The IP address of the default router is sent in the message.

Parameter Problem

A *parameter problem message* (type 12) can be sent when either there is a problem in the header of a datagram (code 0) or some options are missing or cannot be interpreted (code 1).

Important points about ICMP error messages:

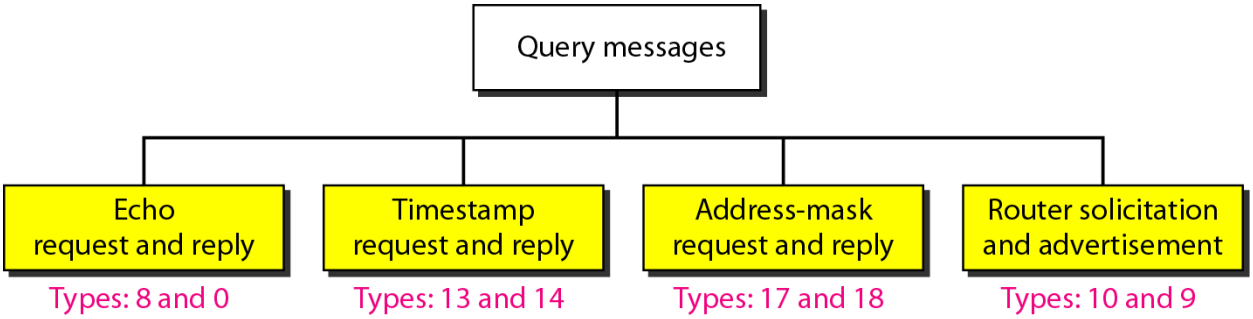
❏ No ICMP error message will be generated in response to a datagram carrying an ICMP error message.

❏ No ICMP error message will be generated for a fragmented datagram that is not the first fragment.

❏ No ICMP error message will be generated for a datagram having a multicast address.

❏ No ICMP error message will be generated for a datagram having a special address such as 127.0.0.0 or 0.0.0.0.

Query messages



Query messages are used to probe or test the liveliness of hosts or routers in the Internet, find the one-way or the round-trip time for an IP datagram between two devices, or even find out whether the clocks in two devices are synchronized. Naturally, query messages come in pairs: request and reply.

The *echo request* (type 8) and the *echo reply* (type 0) pair of messages are used by a host or a router to test the liveliness of another host or router. A host or router sends an echo request message to another host or router; if the latter is alive, it responds with an echo reply message.

The *timestamp request* (type 13) and the *timestamp reply* (type 14) pair of messages are used to find the round-trip time between two devices or to check whether the clocks in two devices are synchronized.

Address mask request and reply messages are not used today because their duties are done by the Dynamic Host Configuration Protocol (DHCP).

Router solicitation and advertisement messages are not used today because their duties are done by the Dynamic Host Configuration Protocol (DHCP).

12. Explain in detail about Mobile IP.

As mobile and personal computers such as notebooks become increasingly popular, we need to think about mobile IP, the extension of IP protocol that allows mobile computers to be connected to the Internet at any location where the connection is possible.

Addressing

The main problem that must be solved in providing mobile communication using the IP protocol is addressing.

Stationary Hosts

The original IP addressing was based on the assumption that a host is stationary, attached to one specific network. A router uses an IP address to route an IP datagram.

The IP addresses are designed to work with stationary hosts because part of the address defines the network to which the host is attached.

Mobile Hosts

When a host moves from one network to another, the IP addressing structure needs to be modified. Several solutions have been proposed.

Changing the Address

One simple solution is to let the **mobile host** change its address as it goes to the new network. The host can use DHCP to obtain a new address to associate it with the new network. This approach has several drawbacks.

First, the configuration files would need to be changed.

Second, each time the computer moves from one network to another, it must be rebooted.

Third, the DNS tables need to be revised so that every other host in the Internet is aware of the change.

Fourth, if the host roams from one network to another during a transmission, the data exchange will be interrupted.

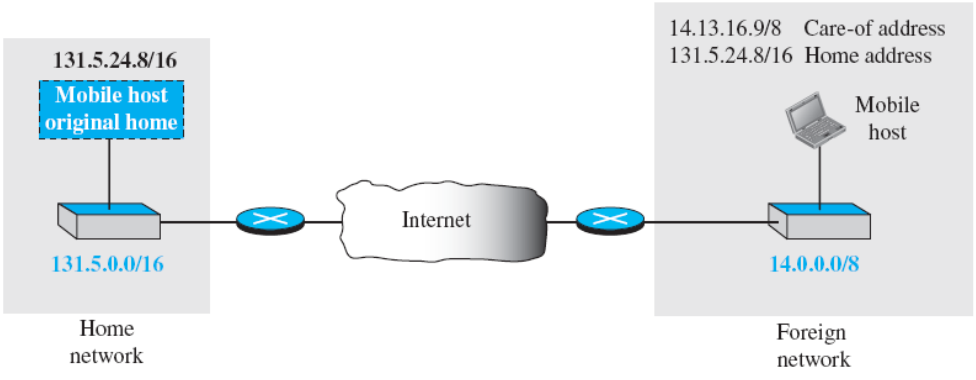
Two Addresses

The approach that is more feasible is the use of two addresses. The host has its original address, called the **home address,** and a temporary address, called the **care-of address.**

The home address is permanent; it associates the host with its **home network,** the network that is the permanent home of the host. The care-of address is temporary.

When a host moves from one network to another, the care-of address changes; it is associated with the **foreign network,** the network to which the host moves.

Home address and care-of address

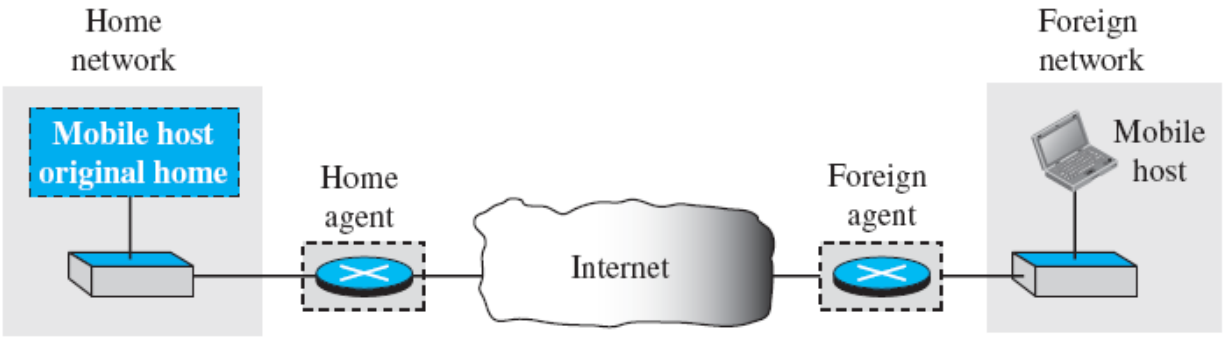


Mobile IP has two addresses for a mobile host: one home address and one care-of address. The home address is permanent; the care-of address changes as the mobile host moves from one network to another.

Agents

To make the change of address transparent to the rest of the Internet requires a **home agent** and a **foreign agent.**

Home agent and foreign agent



Home Agent

The home agent is usually a router attached to the home network of the mobile host. The home agent acts on behalf of the mobile host when a remote host sends a packet to the mobile host. The home agent receives the packet and sends it to the foreign agent.

Foreign Agent

The foreign agent is usually a router attached to the foreign network. The foreign agent receives and delivers packets sent by the home agent to the mobile host.

When the mobile host and the foreign agent are the same, the care-of address is called a collocated care-of address.

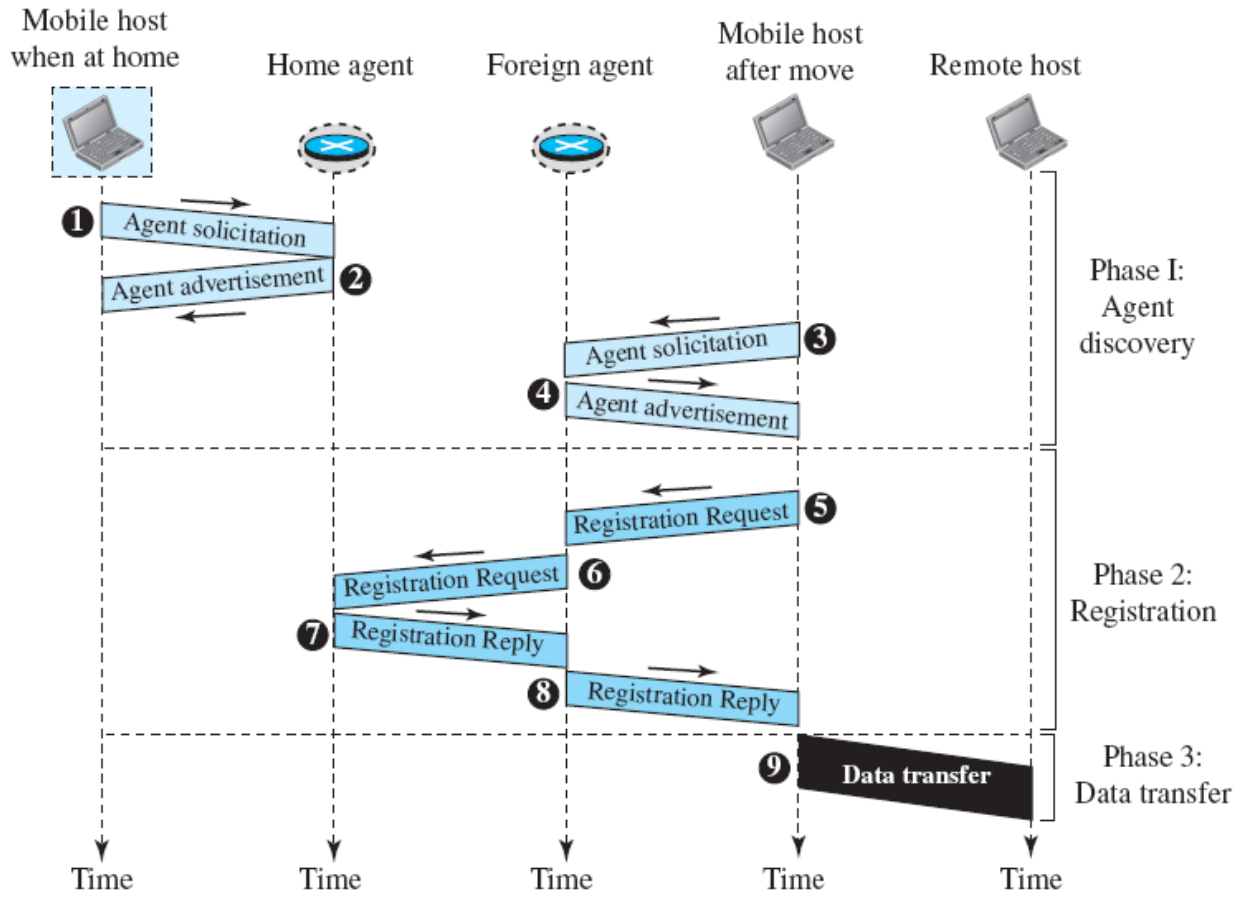
The advantage of using a collocated care-of address is that the mobile host can move to any network without worrying about the availability of a foreign agent.

The disadvantage is that the mobile host needs extra software to act as its own foreign agent.

Three Phases

To communicate with a remote host, a mobile host goes through three phases: agent discovery, registration, and data transfer

Remote host and mobile host communication



Agent Discovery

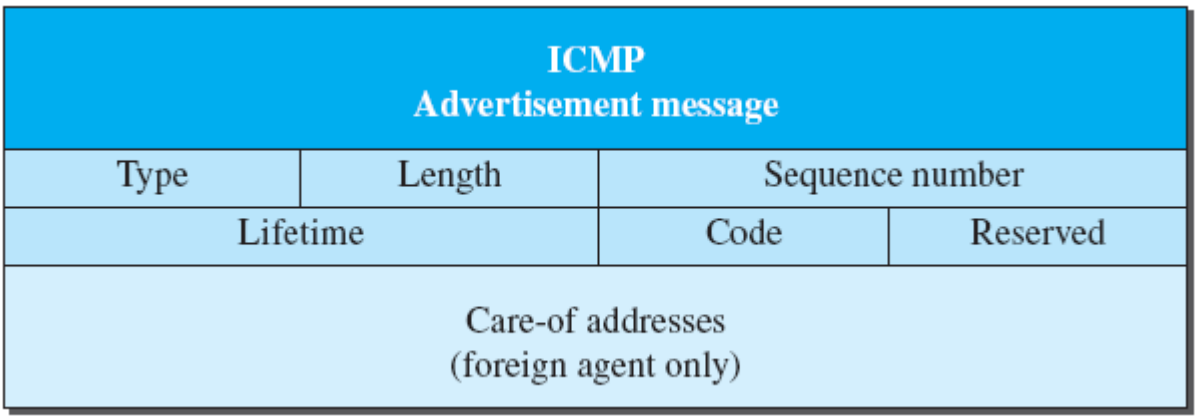
The first phase in mobile communication, *agent discovery*, consists of two subphases.

This discovery consists of learning the care-of address as well as the foreign agent's address. The discovery involves two types of messages: advertisement and solicitation.

Agent Advertisement

When a router advertises its presence on a network using an ICMP router advertisement, it can append an *agent advertisement* to the packet if it acts as an agent.

Mobile IP does not use a new packet type for agent advertisement; it uses the router advertisement packet of ICMP, and appends an agent advertisement message



The field descriptions are as follows:

- ***Type.*** The 8-bit type field is set to 16.
- ***Length.*** The 8-bit length field defines the total length of the extension message (not the length of the ICMP advertisement message).
- ***Sequence number.*** The 16-bit sequence number field holds the message number. The recipient can use the sequence number to determine if a message is lost.
- ***Lifetime.*** The lifetime field defines the number of seconds that the agent will accept requests. If the value is a string of 1s, the lifetime is infinite.
- ***Code.*** The code field is an 8-bit flag in which each bit is set (1) or unset (0).

Bit	*Meaning*
0	Registration required. No collocated care-of address.
1	Agent is busy and does not accept registration at this moment.
2	Agent acts as a home agent.
3	Agent acts as a foreign agent.
4	Agent uses minimal encapsulation.
5	Agent uses generic routing encapsulation (GRE).
6	Agent supports header compression.
7	Unused (0).

- ***Care-of Addresses.*** This field contains a list of addresses available for use as care of addresses. The mobile host can choose one of these addresses. The selection of this care-of address is announced in the registration request.

Agent Solicitation

When a mobile host has moved to a new network and has not received agent advertisements, it can initiate an *agent solicitation.* It can use the ICMP solicitation message to inform an agent that it needs assistance.

Mobile IP does not use a new packet type for agent solicitation; it uses the router solicitation packet of ICMP.

Registration

The second phase in mobile communication is *registration.* After a mobile host has moved to a foreign network and discovered the foreign agent, it must register. There are four aspects of registration:

1. The mobile host must register itself with the foreign agent.

2. The mobile host must register itself with its home agent. This is normally done by the foreign agent on behalf of the mobile host.

3. The mobile host must renew registration if it has expired.

4. The mobile host must cancel its registration (deregistration) when it returns home.

Request and Reply

To register with the foreign agent and the home agent, the mobile host uses a *registration request* and a registration reply

Registration Request A registration request is sent from the mobile host to the foreign agent to register its care-of address and also to announce its home address and home agent address. The foreign agent, after receiving and registering the request, relays the message to the home agent.

Registration request format

The field descriptions are as follows:

❑ ***Type.*** The 8-bit type field defines the type of message. For a request message the value of this field is 1.

❑ ***Flag.*** The 8-bit flag field defines forwarding information. The value of each bit can be set or unset.

Bit	*Meaning*
0	Mobile host requests that home agent retain its prior care-of address.
1	Mobile host requests that home agent tunnel any broadcast message.
2	Mobile host is using collocated care-of address.
3	Mobile host requests that home agent use minimal encapsulation.
4	Mobile host requests generic routing encapsulation (GRE).
5	Mobile host requests header compression.
6–7	Reserved bits.

❑ ***Lifetime.*** This field defines the number of seconds the registration is valid. If the field is a string of 0s, the request message is asking for deregistration. If the field is a string of 1s, the lifetime is infinite.

❑ ***Home address.*** This field contains the permanent (first) address of the mobile host.

❑ ***Home agent address.*** This field contains the address of the home agent.

❑ ***Care-of address.*** This field is the temporary (second) address of the mobile host.

❑ ***Identification.*** This field contains a 64-bit number that is inserted into the request by the mobile host and repeated in the reply message. It matches a request with a reply.

❑ ***Extensions.*** Variable length extensions are used for authentication. They allow a home agent to authenticate the mobile agent.

Registration Reply A registration reply is sent from the home agent to the foreign agent and then relayed to the mobile host. The reply confirms or denies the registration request. The fields are similar to those of the registration request with the following exceptions.

Encapsulation

Registration messages are encapsulated in a UDP user datagram. An agent uses the well-known port 434; a mobile host uses an ephemeral port.

Data Transfer

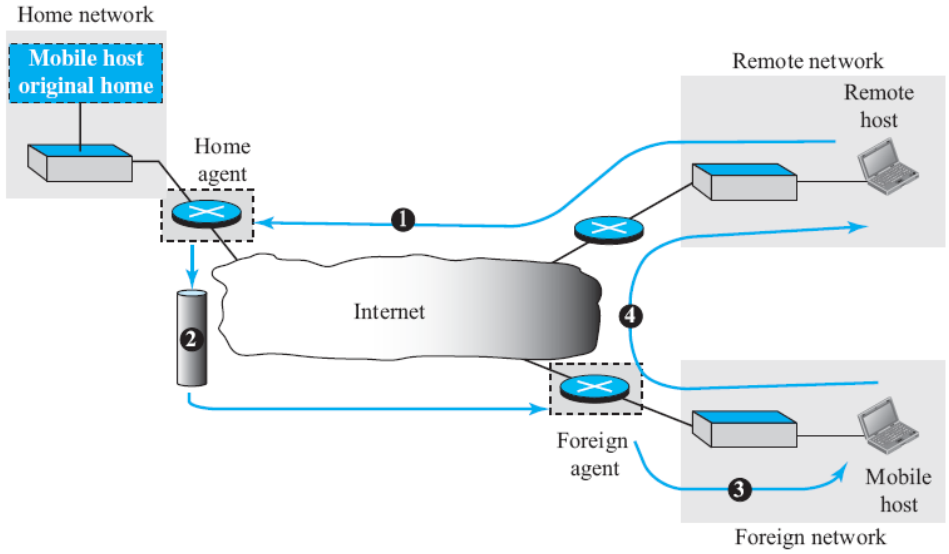
After agent discovery and registration, a mobile host can communicate with a remote host.

Registration reply format

Type	Code	Lifetime
Home address		
Home agent address		
Identification		
Extensions ...		

A registration request or reply is sent by UDP using the well-known port 434.

Data transfer

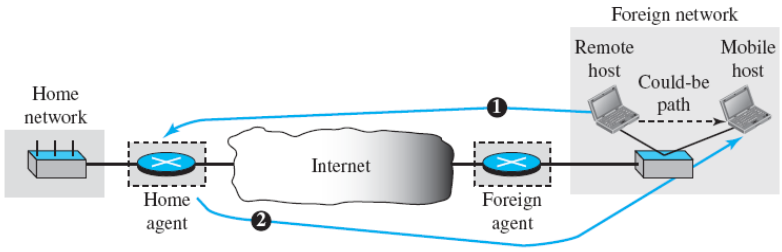


Inefficiency in Mobile IP

Communication involving mobile IP can be inefficient. The inefficiency can be severe or moderate. The severe case is called *double crossing* or *2X*. The moderate case is called *triangle routing* or *dog-leg routing*.

Double Crossing

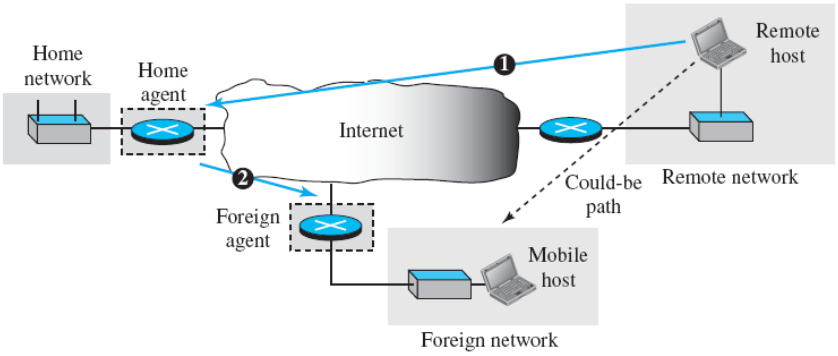
Double crossing occurs when a remote host communicates with a mobile host that has moved to the same network (or site) as the remote host.



When the mobile host sends a packet to the remote host, there is no inefficiency; the communication is local. However, when the remote host sends a packet to the mobile host, the packet crosses the Internet twice. Since a computer usually communicates with other local computers (principle of locality), the inefficiency from double crossing is significant.

Triangle Routing

Triangle routing, the less severe case, occurs when the remote host communicates with a mobile host that is not attached to the same network (or site) as the mobile host. When the mobile host sends a packet to the remote host, there is no inefficiency.



Solution

One solution to inefficiency is for the remote host to bind the care-of address to the home address of a mobile host.

UNIT 3: ROUTING

Routing - Unicast Routing – Algorithms – Protocols – Multicast Routing and its basics – Overview of Intradomain and interdomain protocols – Overview of IPv6 Addressing – Transition from IPv4 to IPv6

PART-A

1. **Define Routing.**

   It is defined as a process of transferring packets over a network from one host to another. This task is performed efficiently by making use of the devices are called **Routers**. In other words, It is a process of finding a path/route in a Network or group of Networks.

2. **What is Multicast Routing?**

   The process of sending a message to multiple receivers with a single sends operation is called **Multicasting**.

   To achieve multicasting, multiple receiver who are interested in receiving a multicast packet from a group.

   The member of group may join or leave a group. When a process joins a particular group, it informs about its membership to its host.

   The routers learn about group membership of their hosts in two ways,

   1. Host inform to their routers.
   2. Routers gets this information by asking their host Periodically.

3. **What are the metrics used by routing protocols?**

The metrics used by Routing protocols are as follows,

1. Number of Hops (hop count)
2. Path reliability
3. Path bandwidth
4. Speed of the path.

4. **What is Border Gateway Protocol (BGP)?**

   BGP is an inter autonomous system routing protocol. An autonomous system is a network or group of networks under common administration and with common routing policies.

   BGP is used to exchange routing information for the internet and is the protocol used between Internet Service Provider (ISP).

When BGP is used between Autonomous Systems (AS), the protocol is referred to External BGP (EBGP), if BGP is used to exchange information within an AS, then the protocol is referred to as Internal BGP (IBGP).

5. Define Intradomain multicast routing and Interdomain multicast routing.

Intradomain multicast routing

It is defined as the routing performed within an Autonomous System (AS). The different multicast routing protocols supporting the intradomain are Distance Vector Multicast Routing Protocols, Multicast Open Shortest Path First (OSPF).

Interdomain multicast routing

It is defined as the routing performed between the different autonomous systems. The protocols supported by interdomain multicasting are Multicast BGP (MBGP), Multicast Source Discovery Protocol (MSDP) etc.

6. Compare forwarding table and Routing table.

A forwarding table contains mapping between network number and outgoing interface as well as physical address of the next hop.

A routing table contains mapping between network number and logical address of next hop. It is built by routing algorithm.

7. Illustrate the concept of fragmentation and reassembly.

Fragmentation:

In internetworking, it is possible that a larger size packet can appear on a small size network. This is done by dividing the original packet into smaller fragments which are treated as independent packets are called fragmentation.

There are two strategies used for recombining the fragment into its original packet. They are as follows,

1. Transparent fragmentation
2. Non-transparent fragmentation

Reassembly:

The process of combining the small pieces of a single packet, in order to form an original packet is known as reassembly. It is the reverse process of fragmentation.

8. Why is IPv4 to IPv6 transition required?

IPv6 Addresses:

To overcome problems related to,

(i) Address depletion for the internet.

(ii) Lack of accommodation for real time audio and video transmission.

(iii) Data encryption and authentication.

9. Write short notes on Unicast Routing Protocol.

It refers to the transmission of data between single sender to single receiver. It is one to one communication (i.e., It has one source and one Destination). Hence unicast routing refers to routing of the data packets from source to destination using various algorithms and protocols.

There are three algorithms used in unicast protocol based on respective protocols.

- Distance Vector Routing algorithm (RIP)
- Link State Routing algorithm (OSPF)
- Path Vector Routing algorithm (BGP)

10. Explain about link state Algorithm.

Link state routing algorithm is a dynamic routing algorithm that takes into account the complete network topology, all delays and bandwidths when choosing routes. In this algorithm each router does the following,

- Learn about its neighbors and their addresses.
- Measure the line cost to each of its neighbors.
- Build packets containing information it learnt.
- Distributes packets to all other routers.
- Compute router, with shortest path to every other router.

11. Discuss about open shortest path first protocol.

An OSPF is a hierarchical interior gateway protocol for routing in Internet protocol using a link-state in the individual areas that make up the hierarchy. The area "0" represents the core or "backbone" region of an OSPF-enabled network. Other OSPF area numbers may be designated to serve other region of an enterprise. The backbone has an identifier as 0.0.0.0.

12. Discuss about RIP implementations.

RIP implements distance vector routing directly with some considerations:

1. In an Autonomous System (AS), we are dealing with routers and networks (links). The routers have routing tables; networks do not.
2. The destination in a routing table is a network, Which means the first column defines a Network address.

3. 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***
4. Infinity is defined as 16, which means that any route in an AS using RIP cannot have more than 15hops.
5. The next-node column defines the address of the router to which the packet is to be sent to reach its destination.

13. What is Flooding?

It is the method of sending a packet on every outgoing line except the line on which it has arrived without checking the address of the destination group.

The major drawback of flooding strategy is that the packet is even received by those host, which has not requested it.

Apart from this, the strategy even create loops due to which, a packet that was forwarded by a particular router may again receive it via., the same interface on another interface.

The issue of loop can be solved by maintaining a copy of the packet and discarding the duplicate packets.

14. Write short notes on IGMP.

It is a protocol to organize group membership of IP hosts. In a network these may be one or many multicast routers that allocate multicast packets to host routers. The information about membership status of these hosts and routers linked to network is provided to the multicast routers by IGMP protocol.

15. Classify different Routing algorithms.

The routing algorithm is the part of the network layer software called "Routing Protocol" that decides the path to be used for routing a packet from source to destination router. The classifications of routing algorithm are as follows,

(i) **Non-adaptive Routing algorithm** – These are *static routing algorithm*. In theses algorithms the routers are decided the route in advance.

(ii) **Adaptive Routing Algorithm** – These are *Dynamic routing algorithm*. Here, the routers decides a route based on network topology and traffic load.

The most popular adaptive routing algorithms are Distance vector routing (DVR) and Link state routing (LSR).

16. Explain about Count-to-Infinity Problem.

The DVR algorithm has serious problem when a link goes down or comes up. Otherwise it is works well, when all the nodes and links are always up.

The problem arises since the nodes exchange their updated distance vectors but hide how they compute the vectors, due to which the choice of next hop of downstream routers create loops. This problem is called ***Count-to-infinity*** problem.

17. List the Benefits of OSPF.

(i) Authentication of routing message

(ii) Additional Hierarchy

(iii) Load Balancing

18. Inspect the salient features of IPv6.

- Larger address space about 128 bits long.
- Address auto configuration
- Support for resource allocation
- Security capabilities

19. Compare IPv4 and IPv6.

BASIS OF COMPARISON	IPV4	IPV6
Address Configuration	Supports Manual and DHCP configuration.	Supports Auto-configuration and renumbering
Address Space	It can generate 4.29 x 10^9 addresses.	It can produce quite a large number of addresses, i.e., 3.4 x 10^{38}.
Security features	Security is dependent on application	IPSEC is inbuilt in the IPv6 protocol
Address length	32 bits (4 bytes)	128 bits (16 bytes)
Address Representation	In decimal	In hexadecimal
Fragmentation performed by	Sender and forwarding routers	Only by the sender

BASIS OF COMPARISON	IPV4	IPV6
Encryption and Authentication	Not Provided	Provided

20. Identify the error is present or not in the following IPv6 Addresses:

(i) A456:04FF::F678:001F – No error; it's a compact way of represent the IPv6 Address.

(ii) **0000:::FFFF – Error;** There should not be three semicolon in the representation of IPv6 Addresses.

21. What is multicast addressing?

Range of IP address is reserved for multicasting (Class D in IPv4). Multicast addresses are associated with an abstract group, whose members are dynamic. If not for multicast addressing, a host would have to send a separate packet with the identical data to each member of the group.

In IPv4, there are 28 bits of possible multicast addresses, ignoring the prefix.

22. Define IP multicasting.

- IP multicast supports both source-specific multicast (one-to-many) and any source multicast (many-to-many), where each group has its own IP multicast address.
- Hosts that are members of a group receive copies of any packet sent to that group's multicast address.
- IP multicast allows any host to send multicast traffic, it needn't even be a member. IP multicast is more scalable because it eliminates redundant traffic.

23. State the drawbacks of IPv4.

- Despite all short-term solutions, such as subnetting, classless addressing, and NAT, address depletion is still a long-term problem.
- Internet must accommodate real-time audio and video transmission that requires minimum delay strategies and reservation of resources.
- Internet must provide encryption and authentication of data for some applications.

24. Define dual-stack operation and tunneling.

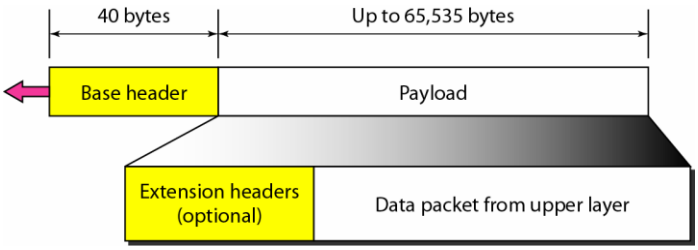
In dual-stack, nodes run both IPv6 and IPv4, uses Version field to decide which stack should process an arriving packet. IPv6 packet is encapsulated with an IPv4 packet as it travels through

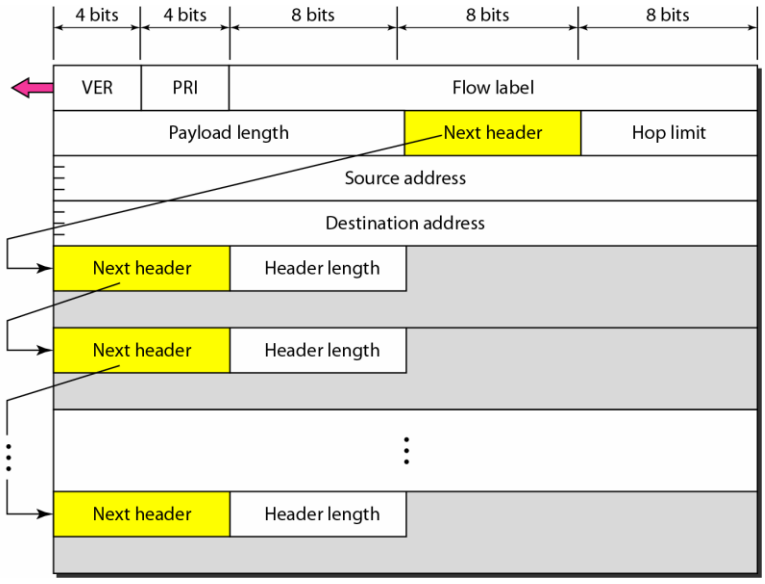
an IPv4 network. This is known as tunneling and packet contains tunnel endpoint as its destination address.

PART-B

1. Draw the IPv6 packet format:

The IPv6 packet is shown in figure below. Each packet is composed of based header followed by the payload. The payload consists of two parts: optional extension headers and data from an upper layer. The base header occupies 40 bytes, whereas the extension headers and data from upper layer contain up to 65,535 bytes of information.





The figure above shows the base header with its eight fields. These fields are as follows:

- **Version:** This 4 bit field defines the version number of the IP. For IPv6, the value is 6.
- **Priority:** This 4 bit field defines the priority of the packet with respect to traffic congestion.
- **Flow label:** The flow label is a 3 byte (24-bit) field that is designed to provide some special functions for a particular flow of data.
  - A flow label is used to speed up the processing of a packet by a router. When a router receives a packet, instead of consulting the routing table and going through a routing algorithm to define the address of the next hop, it can easily look in a flow label for the next hop.

- A flow label can be used to support the transmission of real time audio and video. Real time audio or video particularly in digital form requires resources such as high bandwidth, large buffers, long processing time

- **Next header:** The next header is an 8 bit field defining the header that follows the base header in the datagram. The next header is either one of the optional extension headers used by the IP or the header of an encapsulated packet such as UDP or TCP.
- **Hop limit:** This 8 bit hop limit field serves the same purpose as the TTL field in IPv4.
- **Source address:** The source address field is a 16 byte (128 bit) that defines the original source of the datagram.
- **Destination address:** The destination address field is a 16 byte that defines the final destination of the datagram.

Priority: The priority field of the IPv6 packet defines the priority of each packet with respect to other packets from the same source. For ex: if one of two consecutive datagrams must be discarded due to congestion, the datagram with the lower priority will be discarded. IPv6 divides traffic into two broad categories: congestion controlled and non congestion controlled traffic.

Congestion-controlled traffic: Here, the source adapts itself to traffic slowdown when there is congestion, the traffic is referred to as congestion-controlled traffic. Here, the packets may arrive delayed, lost or out of order.

Noncongestion-controlled traffic: Here, the source does not reduce the traffic even in congestion situation also. Discarding of packets is not desirable. Retransmission in most cases is impossible. Real time audio and video are examples of this type of traffic.

2. Compare IPv4 and IPv6 headers:

1. The header length field is eliminated in IPv6 because the length of the header is fixed in this version.

2. The service type field is eliminated in IPv6. The priority and flow labels together take over the function of the service type field.

3. The total length field is eliminated in IPv6 and replaced by the payload length field.

4. The identification, flag and offset fields are eliminated from the base header in IPv6. They are included in the fragmentation extension header.

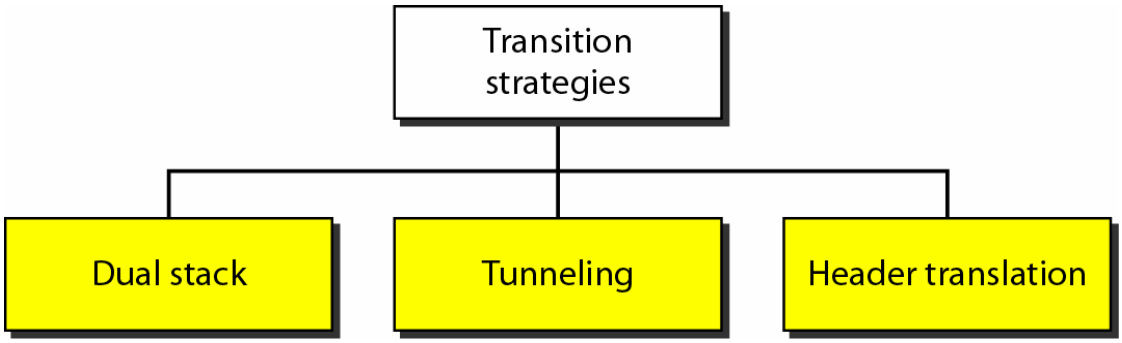
5. The TTL field is called hop limit in IPv6.

6. The protocol field is replaced by the next heard field.

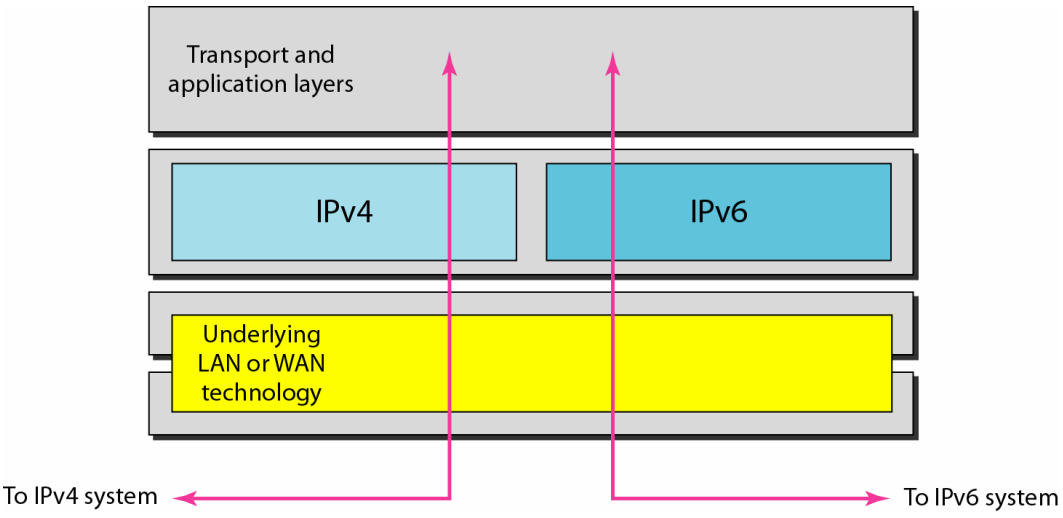
7. The header check sum is eliminated because the check sum is provided by the upper layer protocols; it is therefore not needed at this level.

3. Explain the transition from IPv4 to IPv6 or what are the strategies involved in transition from IPv4 to IPv6?

Need for transition: Because of the huge number of systems on the internet, the transition from IPv4 to IPv6 cannot happen suddenly. It takes a considerable amount of time before every system in the internet can move from IPv4 to Ipv6. The transition must be smooth to prevent any problems between IPv4 and IPv6 systems. Three strategies have been devised by the IETF to help the transition.

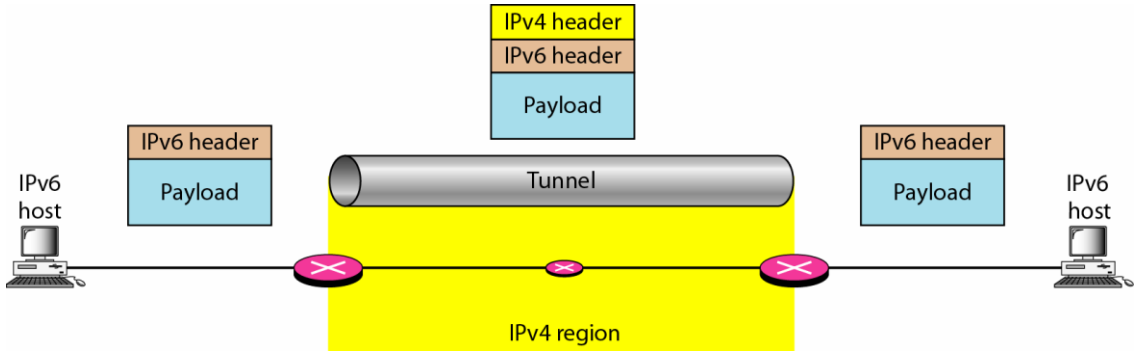


1. Dual stack: It is recommended that all hosts, before migrating completely to version 6, have a dual stack of protocols. That is, each station must run IPv4 and IPv6 simultaneously until all the internet uses IPv6.



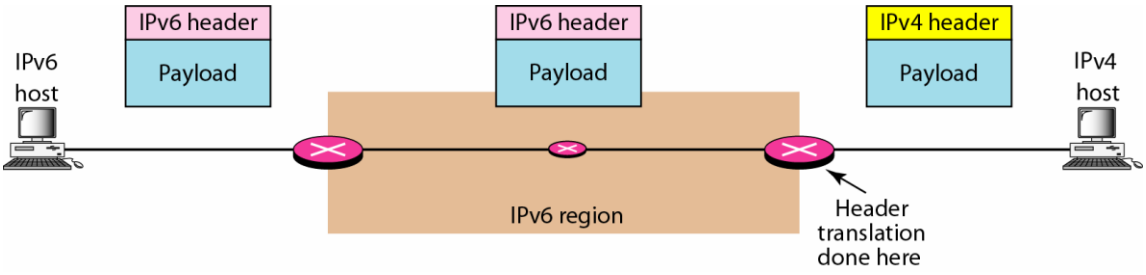
To determine which version to use when sending a packet to a destination, the source host queries the DNS. If the DNS returns an IPv4 address, the source host sends an IPv4 packet. If the DNS returns an IPv6 address, the source host sends an IPv6 packet.

2. Tunneling: Is used when two computers using IPv6 want to communicate with each other and the packet must pass through a region that uses IPv4.



To pass through this region, the packet must have an IPv4 address. So the IPv6 packet is encapsulated in an IPv4 packet when it enters the region, and it leaves its capsule when it exists the region.

3. Header translation: Is necessary when the majority of the internet has moved to IPv6 but some systems still use IPv4 in such situations. For ex: the sender wants to use IPv6, but the receiver does not understand IPv6. Tunneling does not work in this situation because the packet must be in the IPv4 format to be understood by the receiver.



In this case, the header format must be totally changed through header translation. The header of the IPv6 packet is converted to an IPv4 header.

4. Compare distance vector routing and link state routing:

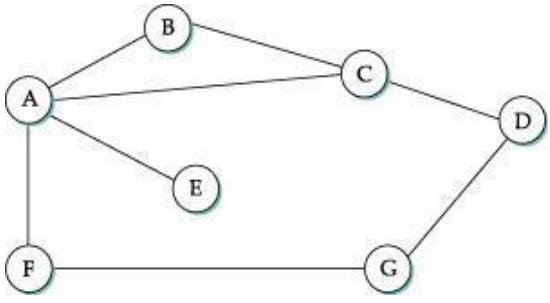
Distance vector Routing	Link state Routing
Bellman ford algorithm used to calculate the shortest path	Dijkstras algorithm used to calculate link state cost
Sends message to their neighbours.	Sends message to every other node in the network.
It is decentralized routing algorithm.	It is centralized global routing algorithm.
Sends larger updates only to neighbouring routers	Sends small updates every where.
Protocol ex: RIP	Protocol ex: OSPF
Requires less CPU power and memory space	Requires more CPU power and memory space
Simple to implement and support.	Expensive to implement and support.
Convergence is less	Convergence is more

5. Explain distance vector routing (or) Routing Information Protocol with an example.

Distance vector routing is distributed, i.e., algorithm is run on all nodes.

Each node knows the distance (cost) to each of its directly connected neighbors. Infinite cost is assigned if link is down. Each node constructs a vector (Destination, Cost, NextHop) to reach all other nodes and distributes the vector to its neighbors.

Nodes compute routing table of minimum distance to every other node via NextHop using information obtained from its neighbors.



Initial State

In given network, cost of each link is 1 hop.

Each node sets a distance of 1 (hop) to its immediate neighbor and cost to itself as 0.

Distance for non-neighbors is marked as unreachable with value (infinity).

For node A, nodes B, C, E and F are reachable, whereas nodes D and G are unreachable.

Destination	Cost	NextHop
A	0	A
B	1	B
C	1	C
D		—
E	1	E
F	1	F
G		

Node A's initial table

Destination	Cost	NextHop
A	1	A
B	1	B
C	0	C
D	1	D
E		
F		
G		

Node C's initial table

Destination	Cost	NextHop
A	1	A
B		
C		
D		
E		
F	0	F
G	1	G

Node F's initial table

Sharing & Updation

Each node sends its initial table (distance vector) to neighbors and receives their estimate. Node A sends its table to nodes B, C, E & F and receives tables from nodes B, C, E & F. Each node updates its routing table by comparing with each of its neighbor's table

For each destination, Total Cost is computed as:

Total Cost = Cost(Node to Neighbor) + Cost(Neighbor to Destination)

Node A learns from C's table to reach node D and from F's table to reach node G.

- Total Cost to reach node D via C = Cost (A to C) + Cost(C to D) = 1 + 1 = 2.
  Since 2 < , entry for destination D in A's table is changed to (D, 2, C)
- Total Cost to reach node G via F = Cost(A to F) + Cost(F to G) = 1 + 1 = 2
  Since 2 < , entry for destination G in A's table is changed to (G, 2, F)

Each node builds complete routing table after few exchanges with its neighbors.

Destination	Cost	NextHop
A	0	A
B	1	B
C	1	C
D	2	C
E	1	E
F	1	F
G	2	F

Node A's final routing table

System stabilizes when all nodes have complete routing information, i.e., convergence. Routing tables are exchanged periodically (every 30 sec.) and in case of triggered update.

Triggered Update

Link failure is assumed, if a node does not receive periodic updates from its neighbor. When a node's routing table changes, it updates its neighbors, neighbors update their neighbors and so on. This is known as triggered update.

Assume that node F detects that its link to G has failed.

o Node F sets distance to G as and shares its table with A.

o Node A updates its distance to G as ∞.

o Meanwhile, node A receives periodic update from C with distance to G as 2 hops.

o Node A updates its distance to G as 3 hops via C.

o Eventually node F is updated to reach G via A in 4 hops.

Loop Instability

Suppose link from node A to E goes down. Node A advertises a distance of to E, meanwhile B and C advertise a distance of 2 to E. o Node B updated by C, concludes that E can be reached in 3 hops via C.

- Node B advertises to A as 3 hops to reach E
- Node A in turn updates C with a distance of 4 hops to E and so on.

Thus nodes update each other until cost to E reaches infinity. Convergence does not occur. This problem is called **loop instability or count to infinity**. It is avoided by redefining infinity to a small number or by using poison reverse.

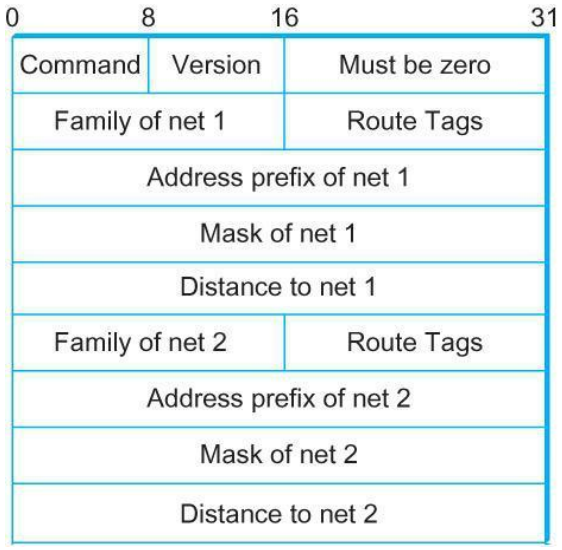
6. Write short note on Routing Information Protocol (RIP)

RIP is an intra-domain routing protocol based on distance-vector algorithm. **Here, routers advertise the cost of reaching networks, instead of reaching other routers**. Cost of each link is 1. The metric in RIP is hop count.

Routers update cost and next hop information for each network number. **Infinity is defined as 16**, i.e., any route within an autonomous system cannot have more than 15 hops.

RIP is limited to run on small-sized networks only.

Routers send their advertisements every 30 seconds or in case of triggered update. RIPv2 packet format contains (network address, distance) pair.



List the solutions for count-to-infinity or loop instability problem.

Infinity is redefined to a small number. Most implementations define 16 as infinity. Thus distance vector routing cannot be used in large networks.

When a node updates its neighbors, it does not send those routes it learned from each neighbor back to that neighbor. This is known as split horizon.

Split horizon with poison reverse allows nodes to advertise back to the sender but with a warning message.

7. Explain link state routing (or) OSPF with an example.

Each node knows the state of link to its neighbors and the cost involved.

Link-state routing protocols rely on two mechanisms:

(i) Reliable dissemination of link-state information to all nodes

(ii) Route calculation from the accumulated link-state knowledge

Each node creates an update packet called link-state packet (LSP) that includes:

(i) ID of the node

(ii) List of neighbors for that node and associated cost

(iii) Sequence number

(iv) Time to live

Sequence number and Time to live fields are used in flooding whereas the other two fields are used for route calculation.

Reliable Flooding

Each node sends its LSP out on each of its directly connected links. Transmission of LSPs between adjacent routers is made reliable using acknowledgment. When a node receives LSP of another node, checks if it has one for that node.

- If not, it stores and forwards the LSP on all other links except the incoming one.
- Otherwise, if the received LSP has a bigger sequence number, then it is stored and forwarded. The older one is discarded.

Thus recent LSP of a node eventually reaches all nodes, i.e., reliable flooding.

LSP is generated either periodically or when there is a change in the topology.

Link-state routing stabilizes quickly without generating much traffic and is dynamic.

Amount of information stored (LSP for each node) at nodes is large.

Flooding of LSP in a small network

Reducing Overhead

Flooding creates traffic and overhead for the network. Mechanisms to reduce are:

- o Timer using long timers, in terms of hours for periodic generation.
- o Sequence number 64-bit sequence does not wrap around soon and is used to discard old LSPs since nodes increment its sequence number for each new LSP it creates.
- o Time to live When TTL reaches 0, the node re-floods that LSP, which signals nodes to delete their stored LSP for that ID.

Route Calculation

- Each node knows the entire topology, once it has LSP from every other node.
- Routing table is determined from the LSPs using a variation of Dijkstra algorithm called forward search algorithm
- Each node maintains two lists namely Tentative and Confirmed with entries of the form (Destination, Cost, NextHop).

Forward Search algorithm

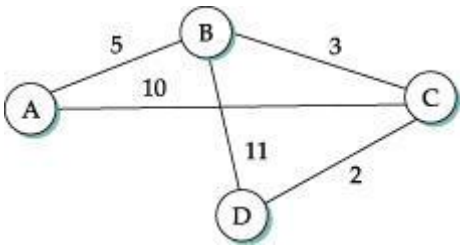
Initialize the Confirmed list with an entry for the Node and Cost = 0.

The node just added to Confirmed list, is called Next and select its LSP.

For each neighbor of Next, calculate cost to reach each neighbor as Cost(Node to Next) + Cost(Next to Neighbor).

If Neighbor is currently on neither Confirmed nor Tentative list, then add (Neighbor, Cost, NextHop) to Tentative list.

- o Neighbor is currently on Tentative list, and the Cost is less than currently listed cost for Neighbor, then replace the entry with (Neighbor, Cost, NextHop).
- o If Tentative list is empty then Stop, otherwise select least cost entry from Tentative list and move it to Confirmed list. Go to Step 2.



For the given network, the process of building routing table for node D is tabulated

Step	Confirmed	Tentative	Comment
1	(D, 0, –)		D is moved to Confirmed list initially
2	(D, 0, –)	(B, 11, B) (C, 2, C)	Based on D's LSP, its immediate neighbors B and C are added to Tentative list
3	(D, 0, –) (C, 2, C)	(B, 11, B)	The lowest-cost member C of Tentative list is moved onto Confirmed list. C's LSP is to be examined next.
4	(D, 0, –) (C, 2, C)	(B, 5, C) (A, 12, C)	Cost to reach B through C is 5, so the entry (B,11,B) is replaced. C's neighbor A is also added to Tentative list
5	(D, 0, –) (C, 2, C) (B, 5, C)	(A, 12, C)	The lowest-cost member B is moved to the Confirmed list. B's LSP is to be examined next
6	(D, 0, –) (C, 2, C) (B, 5, C)	(A, 10, C)	Since A could be reached B at a lower cost than the existing one, the Tentative list entry (A,12,C) is replaced to (A,10,C).
7	(D, 0, –) (C, 2, C) (B, 5, C) (A, 10, C)		The lowest-cost and only member A is moved to Confirmed list. Processing is over.

8. Write short notes on Open Shortest Path First Protocol (OSPF)

OSPF is a non-proprietary widely used link-state routing protocol.

Features added to link state routing include:

(i) **Authentication of routing messages**: Malicious host can collapse a network by advertising to reach every host with cost 0. Such disasters are averted by mandating routing updates to be authenticated.

(ii) **Additional hierarchy**: Domain is partitioned into areas, i.e., a router need not know the complete network, instead only its area.

- Load balancing Allows multiple routes to the same place to be assigned the same cost for traffic to be distributed evenly.

OSPF Header

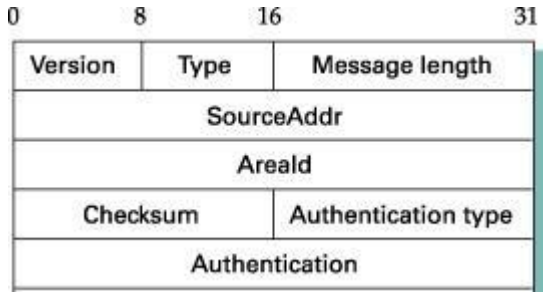
- Version represents the current version, i.e., 2.
- Type represents the type value (1–5) of OSPF message.
  - Type 1 known as hello message to find out whether its neighbors are alive. o

Other types are used to request, send and acknowledge link-state messages.

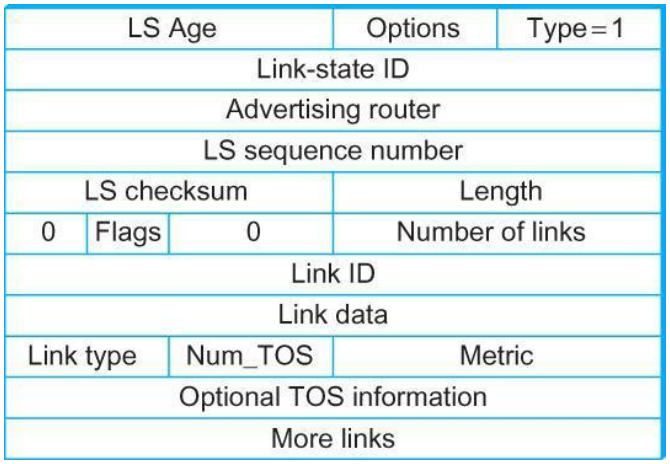
- o SourceAddr identifies the sender
- o AreaId 32-bit identifier of the area in which the node is located o

Checksum 16-bit checksum

- o Authentication type has value 0 if no authentication is used, 1 for simple password and 2 for cryptographic authentication checksum.
- o Authentication contains password or cryptographic checksum



Link State Advertisement



- ✓ LS Age is incremented at each node until it reaches a maximum
- ✓ Type defines type of LSA. Type1 LSAs advertise the cost of links between routers.
- ✓ Link-state ID 32-bit identifier that identifies the router.
- ✓ LS sequence number used to detect old or duplicate packets
- ✓ LS checksum covers all fields except LS Age
- ✓ Length indicates length of the LSA in bytes
- ✓ Link ID and Link Data identify a link Metric specifies cost of the link.
- ✓ Link Type specifies type of link (for example, point-to-point)

- ✓ TOS allows OSPF to choose different routes based on the value in TOS field

9. Discuss Interdomain routing (or) Border Gateway Protocol.

Internet is divided into autonomous systems (AS), since no routing protocol can update the routing tables of all routers.

Interdomain routing involves sharing set of IP address reachable through an AS with other autonomous systems.

Goal of interdomain routing should be reachability and not optimality.

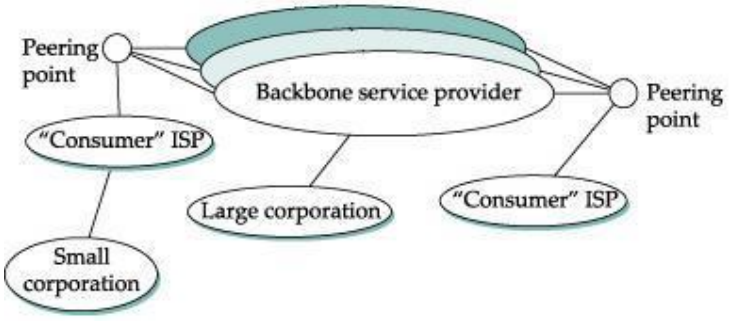
Border Gateway Protocol has replaced EGP as the major interdomain routing protocol Challenges

Each autonomous system has an intradomain routing protocol, its own policy and metric. For example, an AS may refuse to carry transit traffic.

An internet backbone must be able to route packets to the destination that complies with policies of autonomous system along the path and is loop-less.

Service providers have trust deficit and may not trust route advertisements by other AS.

Internet Structure



Internet consists of multiple backbone networks and sites connected to each other. Providers connect at a peering point.

Traffic on the internet is of two types:

- o traffic within an autonomous system is called local.

  traffic that passes through an autonomous system is called transit.

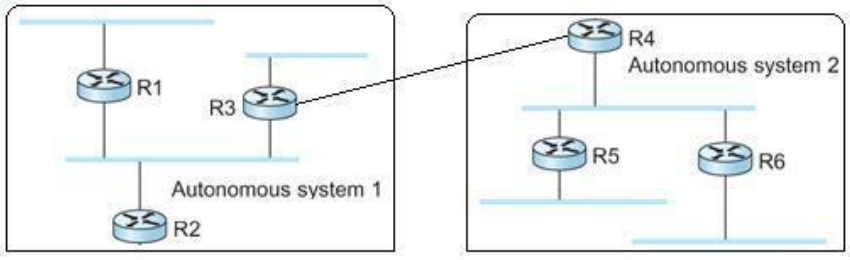
Autonomous Systems (AS) are classified as:

- o Stub AS is connected to only one another autonomous system and can carry local traffic only (e.g. Small corporation).
- o Multihomed AS has connections to multiple autonomous systems but refuses to carry transit traffic (e.g. Large corporation).
- o Transit AS has connections to multiple autonomous systems and is designed to

carry both transit and local traffic (e.g. Backbone service provider).

10. Write short note on Border Gateway Protocol (BGP-4)

BGP views internet as a set of autonomous systems interconnected arbitrarily.



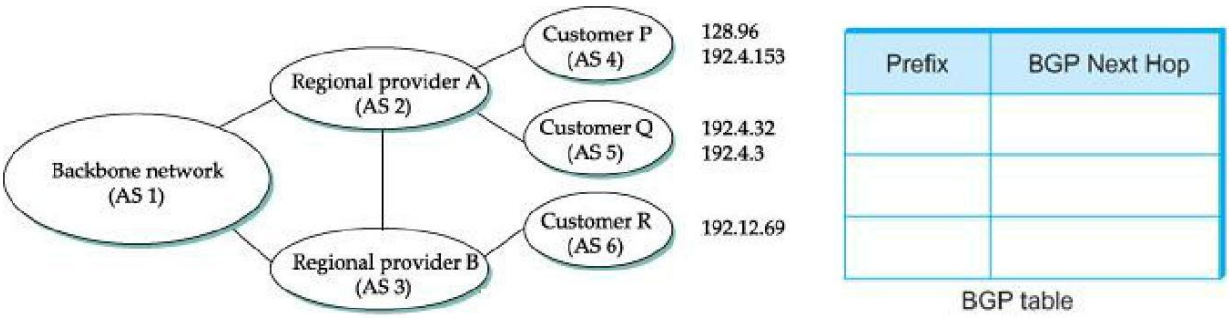
Each AS have a border router (gateway), by which packets enter and leave that AS. In above figure, R3 and R4 are border routers.

One of the nodes in each autonomous system is designated as BGP speaker.

BGP Speaker exchange reachability information with other BGP speakers, known as external BGP session.

BGP advertises complete path as enumerated list of AS (path vector) to reach a particular network. Paths must be without any loop, i.e., AS list is unique.

- For example, backbone network advertises that networks 128.96, 192.4.153, 192.4.32, and 192.4.3 can be reached along the path <AS1, AS2, AS4>.
- AS3 receiving advertisement from AS1, advertises that to AS2 as <AS3, AS1, AS2, AS4>. Since AS2 is part of the path, i.e., loop, it is not used by AS2.



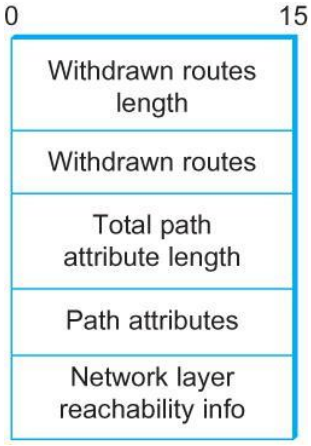
If there are multiple routes to a destination, BGP speaker chooses one based on policy. Speakers need not advertise any route to a destination, even if one exists.

Advertised paths can be cancelled, if a link/node on the path goes down. This negative advertisement is known as withdrawn route. Attributes in a path can be well known or optional.

Designed for classless addressing with prefix of any length.

TCP s used by BGP to ensure reliability.

Routes are not repeatedly sent. If there is no change, keep alive messages are sent.



BGP-4 update packet format

Policies

Provider-Customer Provider advertises the routes it knows to the customer and advertises the routes learnt from customer to everyone.

Customer-Provider advertise own pre xes and routes learned from customers to provider, advertise routes learned from provider to customers, but doesn't advertise routes learned from one provider to another provider.

Peer Two providers access to each other's customers without having to pay.

Integrating inter and intra domain

Any network that has not been explicitly advertised in the intradomain protocol is reachable through the border router.

Variant of BGP known as interior BGP (iBGP) is used by routers to update routing information learnt from other speakers to routers inside the autonomous system. iBGP enables router in an AS to learn the best border router to use.

Each router in an AS knows how to reach each border router using intra domain protocol. Combining these information, each router in the AS is able to determine the appropriate next hop for all prefixes.

11. How routing algorithms are classified?

The routing algorithms may be classified as follows:

Adaptive Routing Algorithm: These algorithms change their routing decisions to reflect changes in the topology and in traffic as well. These get their routing information from adjacent routers or from all routers. This can be further classified as follows:

Non-Adaptive Routing Algorithm: These algorithms do not base their routing decisions on measurements and estimates of the current traffic and topology. Instead the route to be taken in going from one node to the other is computed in advance when the network is booted. This is also known as **static routing.** This can be further classified as:

1. Flooding: Flooding adapts the technique in which every incoming packet is sent on every outgoing line except the one on which it arrived. One problem with this method is that packets may go in a loop. As a result of this a node may receive several copies of a particular packet which is undesirable. Some techniques adapted to overcome these problems are as follows:

(a) Sequence Numbers: Every packet is given a sequence number. When a node receives the packet it sees its source address and sequence number. If the node finds that it has sent the same packet earlier then it will not transmit the packet and will just discard it.

(b) Hop Count: Every packet has a hop count associated with it. This is decremented (or incremented) by one by each node which sees it. When the hop count becomes zero (or a maximum possible value) the packet is dropped.

© Spanning Tree: The packet is sent only on those links that lead to the destination by constructing a spanning tree routed at the source. This avoids loops in transmission but is possible only when all the intermediate nodes have knowledge of the network topology.

Flooding is not practical for general kinds of applications. But in cases where high degree of robustness is desired such as in military applications, flooding is of great help.

12. Write short note on Interior Gateway Protocols (IGP):

IGP is a type of protocols used by the routers in an autonomous system to exchange network reachability and routing information. Some of IGPs are given below.

Routing Information Protocol (RIP): This is one of the most widely used IGP. It was developed at Berkeley. This is also known by the name of the program that implements it, routed .This implements Distance Vector algorithm.

Features of RIP:

- RIP uses a hop count metric to measure the distance to a destination. To compensate for differences in technologies, many RIP implementations allow managers to configure artificially high hop counts when advertising connections to slow networks. All routing updates are broadcast. This allows all hosts on the network to know about the routes.
- To prevent routes from oscillating between two or more equal cost paths, RIP specifies that existing routes should be retained until a new route has strictly lower cost.

- To prevent instabilities, RIP must use a low value for the maximum possible distance. RIP uses 16 as the maximum hop count. This restricts the maximum network diameter of the system to 16.

To solve the slow convergence problem arising due to slow propagation of routing information, RIP uses Hold Down. If a particular link is down, any new information about that link is not accepted till some time. This is because the router must wait till the information about the link being down propagates to another router before accepting information from that router about that down link.

13. Discuss the notation, representation and address space of IPv6.

CIDR and subnetting could not solve address space exhaustion faced by IPv4.

IPv6 was evolved to solve address space problem and offered set of services that include: o Support for real-time services

Security support, Auto configuration, Support for mobile hosts

Addresses Space Allocation

IPv6 provides a 128-bit address space to handle up to 3.4×10^{38} nodes. IPv6 uses classless addressing, but classification is based on MSBs.

Prefix	**Usage**
00...0 (128 bits)	Unspecified
00...1 (128 bits)	Loopback
1111 1111	Multicast addresses
1111 1110 10	Link local use addresses
1111 1110 11	Site local use addresses
Everything else	Global unicast

IPv4's classes A, B and C start with 001 prefix. Multicast address serves the purpose of class D address. Unicast IPv6 address has prefix 001.

Large chunks (87%) of address space are left unassigned for future use. IPv6 defines local addresses for private networks. It is classified into

- Link local enables a host to construct an address that need not be globally unique.
- Site local allows valid local address for use in a isolated site with several subnets. Reserved addresses start with prefix of eight 0s. It is classified into

unspecified address is used when a host does not know its address

o loopback address is used for testing purposes before connected to network

o compatible address is used when IPv6 hosts communicate through IPv4 network o mapped address is used when a IPv6 host communicates with a IPv4 host.

Address Notation

Standard representation of IPv6 is x:x:x:x:x:x:x:x where x is a 16-bit hexadecimal address separated by colon (:)

47CD:1234:4422:ACO2:0022:1234:A456:0124

IPv6 address with contiguous 0 bytes can be written compactly. For example,

47CD:0000:0000:0000:0000:0000:A456:0124 47CD::A456:0124

IPv4 address can be mapped to IPv6 address by prefixing the 32-bit IPv4 address with 2 bytes of 1s and then zero-extending the result to 128 bits. For example,

128. 96.33.81 ::FFFF:128.96.33.81

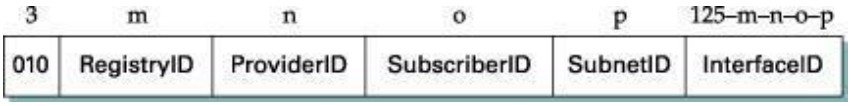
Address Aggregation

Goal of IPv6 address allocation plan is to provide aggregation of routing information to reduce the burden on routers.

Aggregation is done by assigning prefixes at continental level.

For example, if all addresses in Europe have a common prefix, then routers in other continents would need one routing table entry for all networks in Europe.

Format for provider-based unicast address aggregation is:



o RegistryID contains identifier assigned to the continent. It is either INTERNIC (North America), RIPNIC (Europe) or APNIC (Asia and Pacific)

o ProviderID identifies the provider for Internet access such as an ISP. o SubscriberID specifies the assigned subscriber identifier

o SubnetID defines a specific subnet under the territory of subscriber. o InterfaceID contains the link level or physical address.

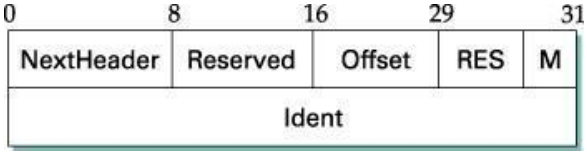
Extension Headers

Extension header provides greater functionality to IP. Base header can be followed by up to six extension headers in the specified order.

Each extension header contains a NextHeader field to identify the header following it. Last extension header is followed by transport layer header.

1. Hop-by-Hop—source host passes information to all routers visited by the packet
2. Source Routing—routing information (strict/loose) provided by the source host.

3. Fragmentation—In IPv6, only the source host can fragment. Source uses a path MTU discovery technique to find smallest MTU on the path.
4. Authentication—used to validate the sender and ensures data integrity.
5. Encrypted Security Payload—provides confidentiality against eavesdropping.
6. Destination—source host information passed only to the destination.



Advanced Capabilities

Longer address format helps in providing auto or stateless configuration of IP address to hosts without the need for a server.

Anycast addressing in IPv6 is used to specify topological entity such as backbone provider. Packet with anycast address is delivered to only one member of anycast group.

Enhanced routing support for mobile hosts is provided by using anycast addressing in the routing header.

Advantages

Address space IPv6 has 128 address space. The address space is so huge, that 1500 address can be allocated for each sqft of earth surface.

Header format In IPv6, options are separated from the base header. Each router thus need not process unwanted addition information.

Options IPv6 has new options to allow additional functionalities such as enhanced routing functionality, support for mobile hosts, etc.

Extensible IPv6 is designed to allow extension of protocol, if required by new technologies or applications.

Resource allocation In IPv6, flow label has been added to enable the source to request special handling of the packet such as real-time audio and video.

Security The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

Auto configuration IPv6 allows a host to be connected to a network without the help of a DHCP server.

14. Explain Multicast routing in detail.

- ✓ In multicast routing, each involved router needs to construct a shortest path tree for each group.

Multicast Applications

Multicasting has many applications today, such as access to distributed databases, information dissemination, teleconferencing, and distance learning.

❑ ***Access to Distributed Databases.*** Most of the large databases today are distributed. That is, the information is stored in more than one location, usually at the time of production. The user who needs to access the database does not know the location of the information. A user's request is multicast to all the database locations, and the location that has the information responds.

❑ ***Information Dissemination*****.** Businesses often need to send information to their customers. If the nature of the information is the same for each customer, it can be multicast. In this way a business can send one message that can reach many customers. For example, a software update can be sent to all purchasers of a particular software package. In a similar manner, news can be easily disseminated through multicasting.

❑ ***Teleconferencing*****.** Teleconferencing involves multicasting. The individuals attending a teleconference all need to receive the same information at the same time. Temporary or permanent groups can be formed for this purpose.

❑ ***Distance Learning*****.** One growing area in the use of multicasting is distance learning. Lessons taught by one professor can be received by a specific group of students. This is especially convenient for those students who find it difficult to attend classes on campus.

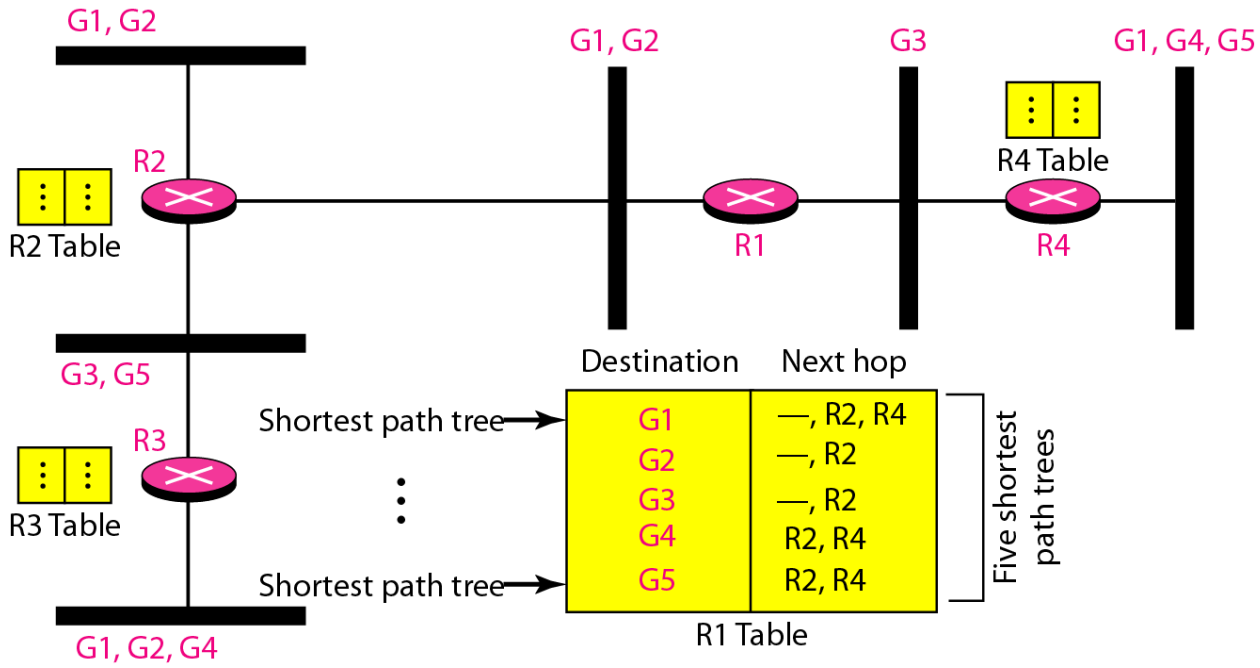
Two Approaches to Multicasting

Two different approaches in multicast routing have been developed:

- ➢ Routing using source-based trees and
- ➢ Routing using group-shared trees.

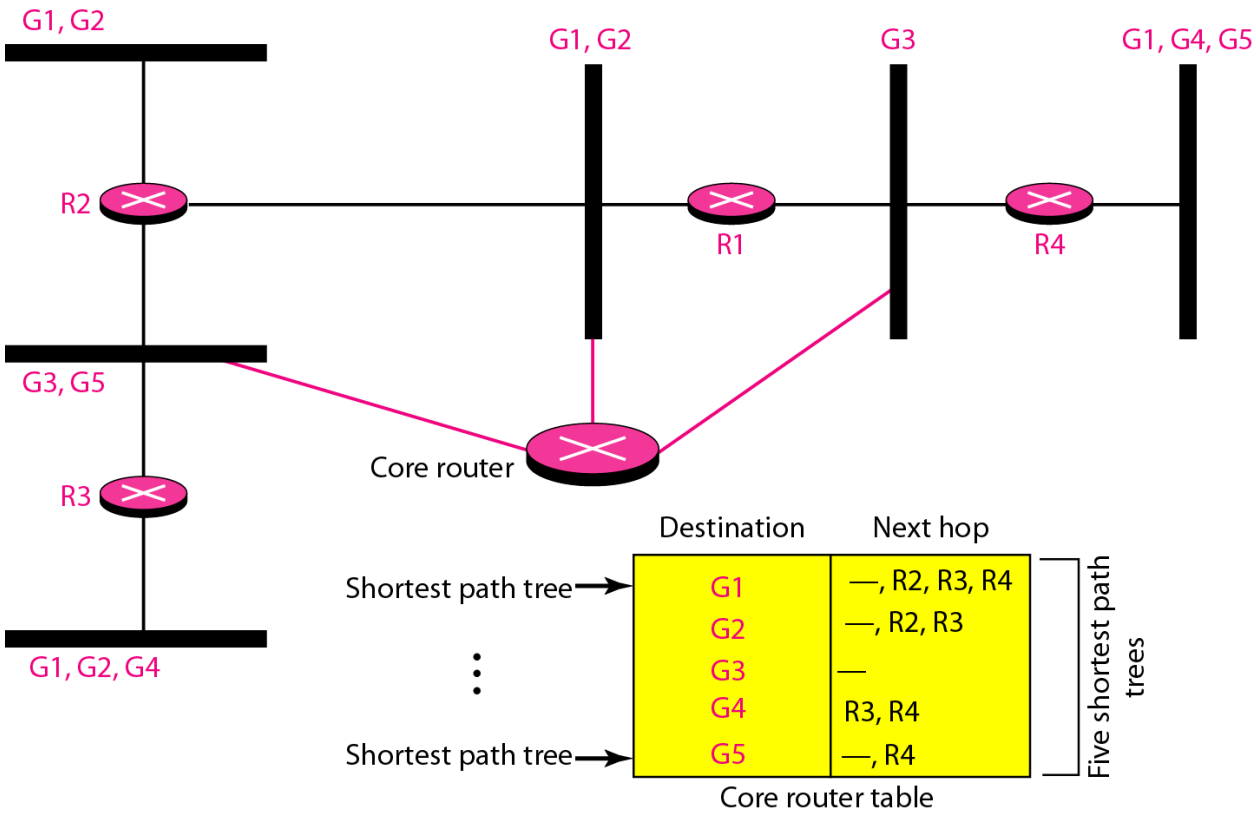
Source-based tree approach

In the **source-based tree** approach to multicasting, each router needs to create a separate tree for each source-group combination. In other words, if there are *m* groups and *n* sources in the internet, a router needs to create ($m \times n$) routing trees. In each tree, the corresponding source is the root, the members of the group are the leaves, and the router itself is somewhere on the tree.



Group-shared tree approach

In the **group-shared tree** approach, we designate a router to act as the phony source for each group. The designated router, which is called the *core* router or the *rendezvouspoint* router, acts as the representative for the group. Any source that has a packet to send to a member of that group sends it to the core center (unicast communication) and the core center is responsible for multicasting.



15. Explain Multicast routing protocols in detail.

To support multicasting, routers additionally have multicast forwarding tables. Multicast forwarding table is a tree structure, known as multicast distribution trees.

Internet multicast is implemented on physical networks that support broadcasting by extending forwarding functions.

Multicast routing is the process by which multicast distribution trees are determined. Prominent multicast routing protocols are:

- o Distance-Vector Multicast (DVMRP)
- o Protocol Independent Multicast (PIM)

Distance-Vector Multicast (DVMRP)

Distance vector routing for unicast is extended to support multicast routing. Each router maintains a table of (Destination, Cost, NextHop) for all destination through exchange of distance vectors.

Multicasting is added to distance-vector routing in two stages.

- o Reverse Path Broadcast mechanism that floods packets to other networks
- o Reverse Path Multicasting that prunes end networks that do not have hosts belonging to a multicast group.
- o DVMRP is also known as flood-and-prune protocol.

Reverse-Path Broadcasting

Router on receiving a multicast packet from source S to a Destination from NextHop, forwards the packet on all out-going links, since it comes from shortest path.

Packet is flooded but not looped back to S. The drawbacks are:

- o It floods a network, even if it has no members for that group.
- o Packets are forwarded by each router connected to a LAN (duplicate flooding).

Duplicate flooding is avoided by

- o Designating a router as parent router for each link.
- o Router that has the shortest path to source S, is selected as parent router.
- o Only parent router forwards multicast packets from source S to that LAN.

Routers maintain a bit indicating whether it is the parent for that source/link pair or not.

Reverse-Path Multicasting

Multicasting is achieved by pruning networks that do not have members for a group G. This is done in two stages.

Step 1: Identify a leaf network which has only one router (parent).

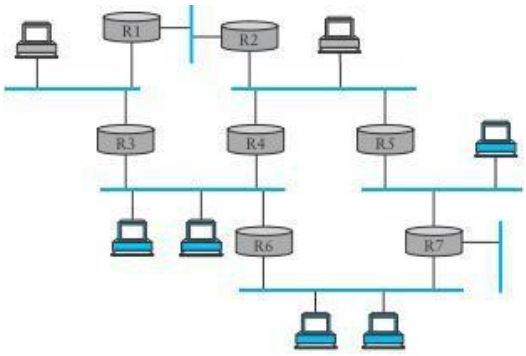
Leaf network is monitored to determine if it has any members for group G, by having hosts periodically announce to which group it belongs to.

Router uses information from hosts to decide whether or not to forward packets addressed to group G over that LAN.

Step 2: Propagate the information "no members of G here" up the shortest path tree.

- Routers augment the (Destination, Cost) pairs it sends to its neighbors with the set of groups for which the leaf network is interested in receiving multicast packets.
- This information is propagated amongst routers so that a router knows for what groups it should forward on each of its links.

Including all this information in a routing update is expensive.



Example internet with members of group G in color

Protocol Independent Multicast (PIM)

Existing multicast routing protocols such as DVMRP did not scale well.

PIM divides multicast routing problem into sparse and dense mode.

PIM sparse mode (PIM-SM) is widely used multicast routing protocol. PIM does not rely on any type of unicast routing protocol, hence protocol independent.

Routers explicitly join and leave multicast group using PIM Join and Prune messages.

A router is designated as rendezvous point (RP) for each group in a domain to receive PIM messages.

Routers in the domain know the IP address of RP for each group.

A multicast forwarding tree is built as a result of routers sending Join messages to RP.

Initially the tree is shared by multiple senders and depending on traffic it may be source-specific to a sender.

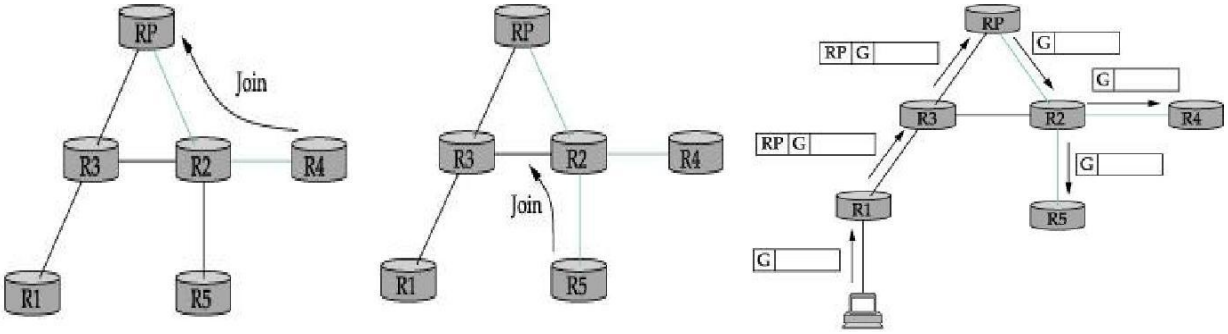
Shared Tree

When a router sends Join message for group G to RP, it goes through a set of routers. o Join message is wildcarded (*), i.e., it is applicable to all senders.

- Router create an entry (*, G) in its forwarding table for the shared tree.
- Interface on which the Join arrived is marked to forward packets for that group. o Forwards Join towards RP on an interface where packets for that group arrive.

Eventually, the message arrives at RP. Thus a shared tree with RP as root is formed.

Example



Join from R4 Join from R5 Multicast message to group G

Router R4 sending Join message for group G to rendezvous router RP.

Join message is received by router R2. R2 makes an entry (*, G) in its table and forwards the message to RP.

As routers send Join message for a group, branches are added to the tree, i.e., shared.

When R5 sends Join message for group G, R2 does not forwards the Join. It adds an outgoing interface to the forwarding table created for that group.

Hosts create a packet with multicast address and send to designated router for its network Suppose router R1, receives a message to group G.

- R1 has no state for group G.
- It encapsulates the multicast packet in a PIM Register message addressed to RP
- Multicast packet is tunneled along the way to RP.

RP decapsulates the packet and sends multicast packet onto the shared tree, towards R2. R2 forwards the multicast packet to routers R4 and R5 that have members for group G.

Source-specific tree.

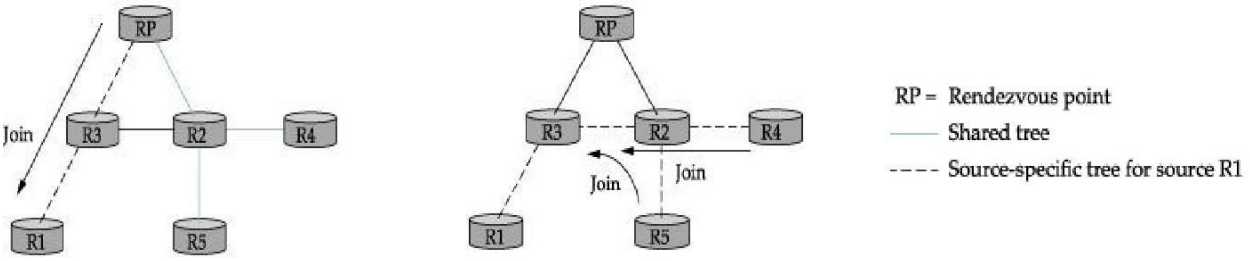
RP can force routers to know about group G, by sending Join message to the sending host, so that tunneling can be avoided.

Intermediary routers create sender-specific entry (S, G) in their tables. Thus a source-specific route from R1 to RP is formed.

If there is high rate of packets sent from a sender to a group G, then shared-tree is replaced

by source-specific tree with sender as root.

Example



Source-specific Join from RP. Routers switch to Source tree

Rendezvous router RP sends a Join message to the host router R1.

Router R3 learns about group G through the message sent by RP.

Router R4 send a source-specific Join due to high rate of packets from source.

Router R2 learns about group G through the message sent by R4.

Eventually a source-specific tree is formed with R1 as root.

Analysis

PIM is protocol independent because, tree maintenance is based on Join messages that come via the shortest path.

Shared trees are more scalable than source-specific trees. Source-specific trees enable efficient routing than shared trees. PIM-SM protocol is used within a domain, not across domains.

UNIT 4: TRANSPORT LAYER

Introduction to Transport layer –Protocols- User Datagram Protocols (UDP) and Transmission Control Protocols (TCP) –Services – Features – TCP Connection – State Transition Diagram – Flow, Error and Congestion Control - Congestion avoidance (DECbit, RED) – QoS – Application requirements

PART-A

1. Distinguish between network and transport layer

Network layer	Transport layer
Responsible for host-to-host delivery	Responsible for process-to-process delivery
Host address is required for delivery	Host IP, port number is required for delivery
Flow control is not done	Flow control is not done
Multicasting capability is not inbuilt	Support for multicasting is embedded

2. List the features desired of a transport layer protocols.

- Guaranteed and in-order delivery of the message.
- Supports multiple application processes on each host.
- It supports synchronization between sender and receiver.
- It allows receiver to apply flow control at the sender.
- Transport layer protocols are UDP, TCP and RTP.

3. What are the services provided by transport layer?

- Process-to-process Communication.
- Stream delivery.
- Sending and receiving buffers.
- Segments.
- Full-Duplex Communication.
- Connection-oriented service.
- Reliable service.

4. Define process and port number?

Processes are programs that run on hosts. It could be either server or client. These processes communicate with TCP with the help of a concept called port number. The port number is 16-bit unique number allocated to a particular application or process. on that host.

Server processes operate at well-known ports (0–1023), assigned by IANA.

Client processes are assigned ephemeral ports (49152–65535) by operating system.

5. Distinguish between connection-less and connection-oriented protocol in transport layer.

UDP (Connection-less)	TCP (Connection-oriented)
Datagram model (connection-less)	Byte-stream service (connection-oriented)
Unreliable delivery	Reliable delivery using acknowledgement
No flow control	Supports flow control
No congestion control	Built-in congestion control mechanism
Light overhead	Heavy overhead
Data is collected in order of receipt	Segments are ordered using sequence number

6. Define Congestion or when congestion occurs? Or what is congestion?

- Congestion occurs if load on the network (the number of packets sent) is greater than capacity of the network (the number of packets a network can handle).
- When load is less than network capacity, throughput increases proportionally.
- When the load exceeds capacity, the queues become full and the routers discard some packets and throughput declines sharply.

7. Distinguish between flow control and congestion control:

- Flow control prevents a fast sender from overrunning the capacity of slow receiver.
- Congestion control prevents too much data from being injected into the network, thereby causing switches or links overloaded beyond its capacity.
- Flow control is an end-to-end issue, whereas congestion control is interaction between hosts and network.

8. How is urgent data delivered in TCP?

- A process may send *urgent* data. For example, abort a process by Ctrl + C keystroke.
- Sending TCP inserts the urgent data at *beginning* of the segment and sets URG flag.
- When TCP receives a segment with URG bit set, it delivers urgent data *out of order* to the receiving application.

9. What is push operation in TCP?

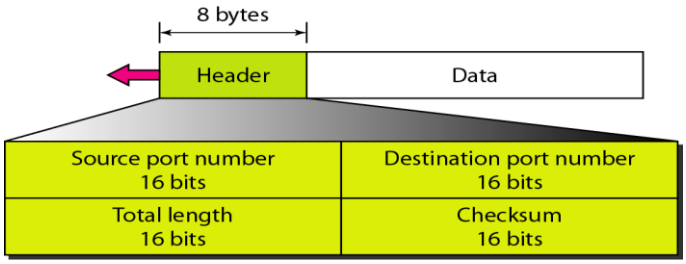
Receiving TCP buffers the data and delivers when process is ready. When a process issues *Push* operation, the sending TCP sets the PUSH flag, which forces the TCP to create a segment and send it immediately.

When TCP receives a segment with PUSH flag set, it is delivered immediately.

10. What is the function of multiplexing in transport layer?

The job of gathering data chunks at the source host from different sockets, encapsulating each data chunks with header information to create segments, and hassing the segments to the network layer is called multiplexing.

11. Draw the UDP header format with neat sketch.



12. List the flags used in TCP header?

1. URG
2. ACK
3. PSH
4. RST
5. SYN
6. FIN

13. What is silly window syndrome?

In a network either a sending application program creates data slowly or the receiving application program consumes data slowly or both. This problem is called the silly window syndrome.

14. Identify the source port number and destination port number from the following dump of a UDP header in hexadecimal format.

06	32	00	0D	00	1C	E2	17

To find the source port and destination port number convert the hexadecimal into decimal. Source port number: $(06\ 32)_{16}$ =1586; Destination port number: $(00\ 0D)_{16}$ =13.

15. Define traffic shaping.

Is a mechanism to control the amount and rate of the traffic sent to the network. Two techniques to shape the traffic are:

1. Leaky bucket 2. Token Bucket

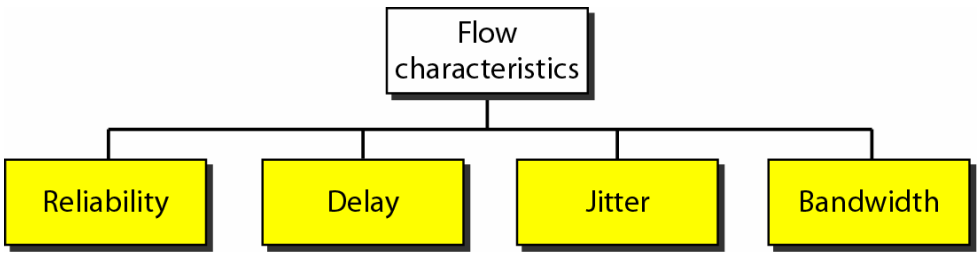
16. What are the four general techniques to improve QOS?

The various methods to improve the QOS are:

1. Scheduling
2. Traffic Shaping
3. Resource Reservation
4. Admission control

17. Define QoS?

The Quality of Service (QOS) defines a set of attributes related to the performance of the network. The four attributes to be satisfied for a good QOS are:



1. **Reliability:** An email, file transfer should have more reliable than audio conference or video conferencing.
2. **Delay:** Audio or video conference should have minimum delay whereas file transfer or email can have acceptable delay.
3. **Jitter:** Is the variation in delay for packets belonging to the same flow. Real time audio and video cannot tolerate high jitter.
4. **Bandwidth:** Different applications need different bandwidths. In video conferencing we need to send millions of bits per second while the total number of bits in an e-mail may not reach even a million.

18. What is the advantage of RED algorithm?

In this technique a **router discards one or more incoming packets before the output buffer is completely full** in order to improve the performance of the network.

The technique adopted by RED is referred to as **Proactive packet discard** technique.

19. How random early detection helps in congestion avoidance?

- RED is designed to **avoid congestion** rather than react to it.
- Thus **RED must detect the onset of congestion** to maintain the network **in a region of low delay** and high throughput.

20. How random early detection helps in Global Synchronization avoidance?

- When the onset of congestion is recognized, the router must decide which connection should be removed.
- By detecting congestion early and notifying only as many connections as necessary, global synchronization is avoided.

21. What is the difference between Differentiated and Integrated Services?

Integrated services: Is concerned with providing an integrated or collective service to the set of traffic demands placed on a given domain.

Differentiated Services: The traffic is classified into number of classes (groups)

- Each class traffic is handled differently.
- It does not handle the over all traffic (integrated) and also it does not attempt to reserve network in advance.

22. What are the various functions performed by ISA to manage congestion and to Provide QOS transport?

- Admission control
- Routing algorithm
- Queuing discipline
- Discard Policy

23. What are the key elements of Guaranteed Service?

The key elements of the guaranteed service are as follows:

1. The service provides assured capacity level, or data rate.
2. There is a specified upper bound on the queuing delay through the network.
3. There are no queuing losses. That is, no packets are lost due to buffer overflow; packets may be lost due to failures in the network or changes in routing paths.

24. What are the key elements of Controlled load Service?

The key elements of the controlled load service are:

1. There is no specified upper bound on the queuing delay through the network.
2. A very high percentage of transmitted packets will be successfully delivered (i.e. almost no queuing loss)

Under unloaded conditions the service will be best (i.e.) overloaded means network leads to losing of packets.

25. What can you say about the TCP segment in which the value of the control field is one of the following?

a. **000001 –** Terminating the Connection
b. **000000 –** No control over segment
c. **010001 –** ACK+FIN, Terminating with acknowledgement.

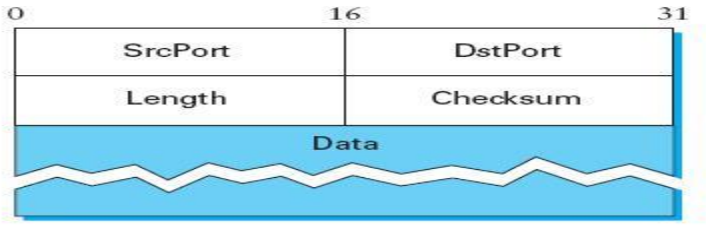
PART-B

1. UDP (Simple Demultiplexer) / Users Datagram protocol

Simple Demultiplexer (UDP)

- The simplest possible transport protocol is one that extends the host-to-host delivery service of the underlying network into a process-to-process communication service.
- Demultiplexing is allowing multiple application processes on each host to share the network.
- The Internet's User Datagram Protocol (UDP) is an example of such a transport protocol.
- The common approach, and the one used by UDP, is for processes to indirectly identify each other using an abstract locator, often called a **port or mailbox.**
- The basic idea is for a source process to send a message to a port and for the destination process to receive the message from a port.

- The header for an end-to-end protocol that implements this demultiplexing function contains an identifier (port) for both the sender (source) and the receiver (destination) of the message.



Format for UDP Header

A client process initiates a message exchange with a server process.

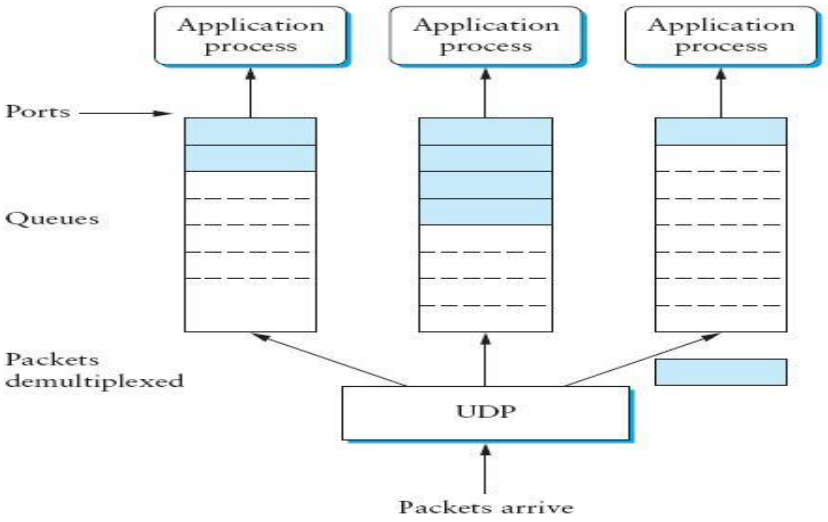
- Once a client has contacted a server, the server knows the client's port and can reply to it.

A common approach is for the server to accept messages at a **well-known port.**

- That is, each server receives its messages at some fixed port that is widely published.
- Ex: the Domain Name Server (DNS) receives messages at well-known port 53 on each host, the mail service listens for messages at port 25, and the Unix talk program accepts messages at well-known port 517, and so on.
- An alternative strategy is to use only a single well-known port—the one at which the **"Port Mapper"** service accepts messages.

- A client would send a message to the Port Mapper's well-known port asking for the port it should use to talk to the "whatever" service, and the Port Mapper returns the appropriate port.
- This strategy makes it easy to change the port associated with different services over time, and for each host to use a different port for the same service.

A port is implemented by a **message queue**, is shown below :



UDP message queue

- When a message arrives, the protocol (e.g., UDP) appends the message to the end of the queue.
- If the queue is full, the message is discarded.
- There is no flow-control mechanism that tells the sender to slow down.
- When an application process wants to receive a message, one is removed from the front of the queue.
- If the queue is empty, the process blocks until a message becomes available.
- UDP does not implement flow control or reliable/ordered delivery,
- UDP ensures the correctness of the message by the use of a checksum.
- UDP computes its checksum over the UDP header, the contents of the message body, and something called the **pseudoheader**.
- The pseudoheader consists of three fields from the IP header
    - protocol number
    - source IP address
    - destination IP address + the UDP length field.

- The pseudoheader is to verify that this message has been delivered between the correct two endpoints.

Applications :

- Used for management processes such as SNMP. Used for route updating protocols such as RIP. It is a suitable transport protocol for multicasting.
- UDP is suitable for a process with internal flow and error control mechanisms such as Trivial File Transfer Protocol (TFTP).

2. Reliable Byte Stream (TCP)

- TCP guarantees the reliable, in-order delivery of a stream of bytes.
- It is a full-duplex protocol, meaning that each TCP connection supports a pair of byte streams, one flowing in each direction.
- It also includes a flow-control mechanism for each of these byte streams that allows the receiver to limit how much data the sender can transmit at a given time.
- Finally, like UDP, TCP supports a demultiplexing mechanism that allows multiple application programs on any given host to simultaneously carry on a conversation with their peers.

End-to-End Issues (Important points about TCP)

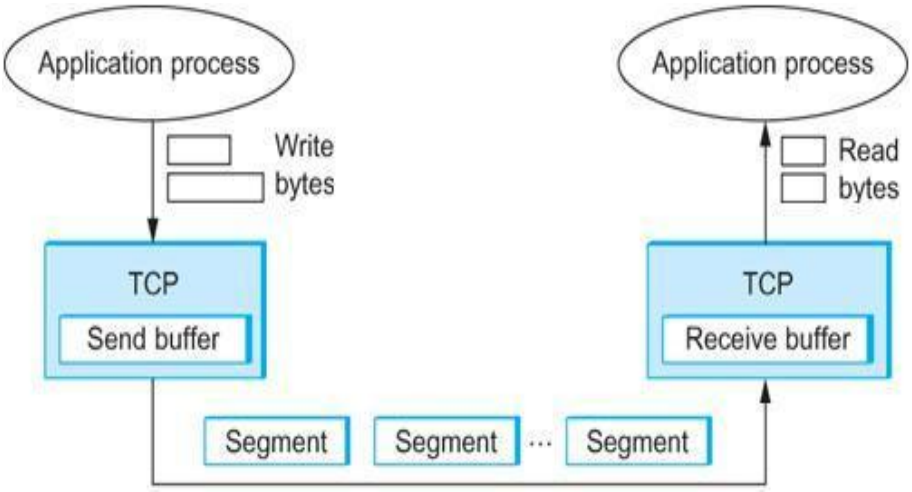
- At the heart of TCP is the **sliding window algorithm**.
- TCP runs over the Internet rather than a point-to-point link.
- The sliding window algorithm runs over a single physical link that always connects the same two computers.
- TCP supports logical connections between processes that are running on any two computers in the Internet.
- This means that TCP needs an connection establishment phase during which the two sides of the connection agree to exchange data with each other.
- A single physical link that always connects the same two computers has a fixed RTT, TCP connections are likely to have widely different round-trip times.
- Packets may be reordered as they cross the Internet.
- Packets that are slightly out of order do not cause a problem since the sliding window algorithm can reorder packets correctly using the sequence number.
- TCP uses flow control and congestion-control mechanisms.
- Flow control involves preventing senders from overrunning the capacity of receivers.

- Congestion control involves preventing too much data from being injected into the network, thereby causing switches or links to become overloaded.

TCP manages a byte stream.

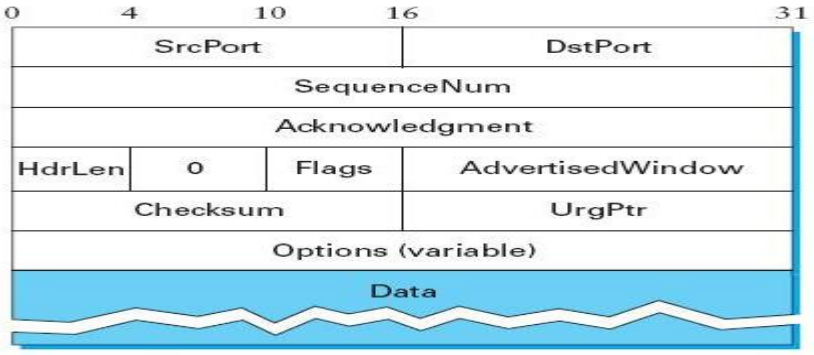
- TCP is a byte-oriented protocol, which means that the sender writes bytes into a TCP connection and the receiver reads bytes out of the TCP connection.
- TCP on the source host buffers enough bytes from the sending process to fill a reasonably sized packet and then sends this packet to its peer on the destination host.
- TCP on the destination host then empties the contents of the packet into a receive buffer, and the receiving process reads from this buffer at its leisure.
- A single TCP connection supports byte streams flowing in both directions.
- The packets exchanged between TCP peers are called **segments** since each one carries a segment of the byte stream.

The following diagrams shows data flowing in only one direction from TCP connection.



TCP Segment Format:

- Each TCP segment contains the entries shown in the above figure.
- The SrcPort and DstPort fields identify the source and destination ports, respectively,just as in UDP.
- The Acknowledgment, SequenceNum, and AdvertisedWindow fields are all involved in TCP's sliding window algorithm.
- Each byte of data has a sequence number; the SequenceNum field contains the sequence number for the first byte of data carried in that segment.



- The Acknowledgment and AdvertisedWindow fields carry information about the flow of data going in the other Direction .
- The 6-bit Flags field is used to relay control information between TCP peers.
- The possible flags include SYN, FIN, RESET, PUSH, URG, and ACK.
- The SYN and FIN flags are used when establishing and terminating a TCP connection, respectively.
- The ACK flag is set any time the Acknowledgment field is valid, implying that the receiver should pay attention to it.
- The URG flag signifies that this segment contains urgent data. When this flag is set, the UrgPtr field indicates where the nonurgent data contained in this segment begins. The PUSH flag signifies that the sender invoked the push operation, which indicates to the receiving side of TCP that it should notify the receiving process of this fact.
- The RESET flag signifies that the receiver has become confused.

3. TCP Connection Management:

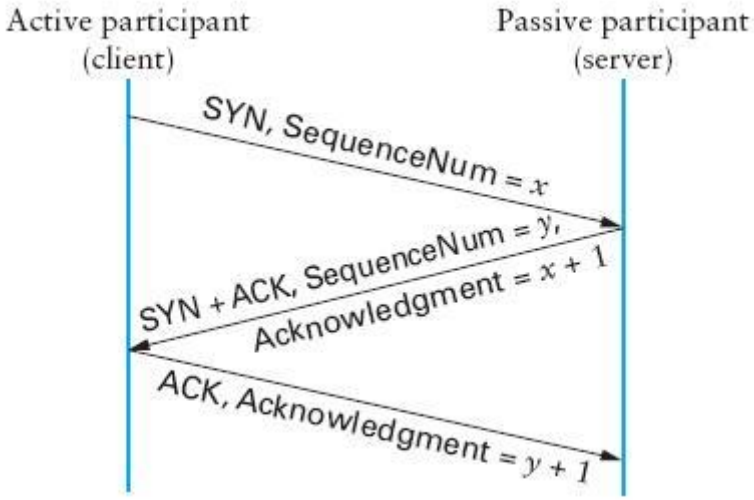
- A TCP connection begins with a client (caller) doing an active open to a server (callee).
- Assuming that the server had earlier done a passive open, the two sides engage in an exchange of messages to establish the connection.
- Only after this connection establishment phase is over do the two sides begin sending data.
- As soon as a participant is done sending data, it closes one direction of the connection, which causes TCP to initiate a round of connection termination messages.

Three-Way Handshake :

- The algorithm used by TCP to establish and terminate a connection is called a three- way handshake.

- The three-way handshake involves the exchange of three messages between the client and the server.
- First, the client (the active participant) sends a segment to the server (the passive participant) stating the initial sequence number it plans to use (Flags = SYN, SequenceNum = x).
- The server then responds with a single segment that both acknowledges the client's sequence number (Flags = ACK, Ack = x + 1) and states its own beginning sequence number (Flags = SYN, SequenceNum = y). That is, both the SYN and ACK bits are set in the Flags field of this second message.

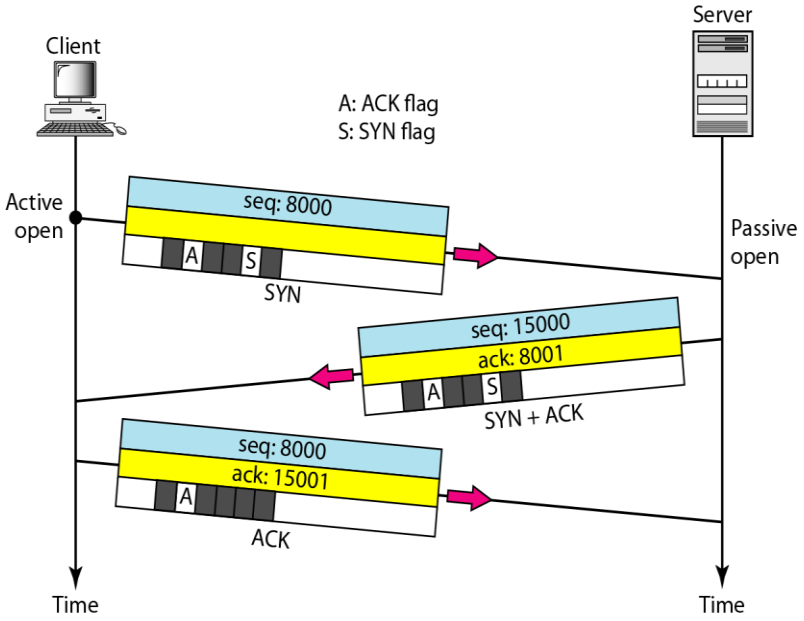
The diagrammatic representation of three way handshaking algorithm is shown below:



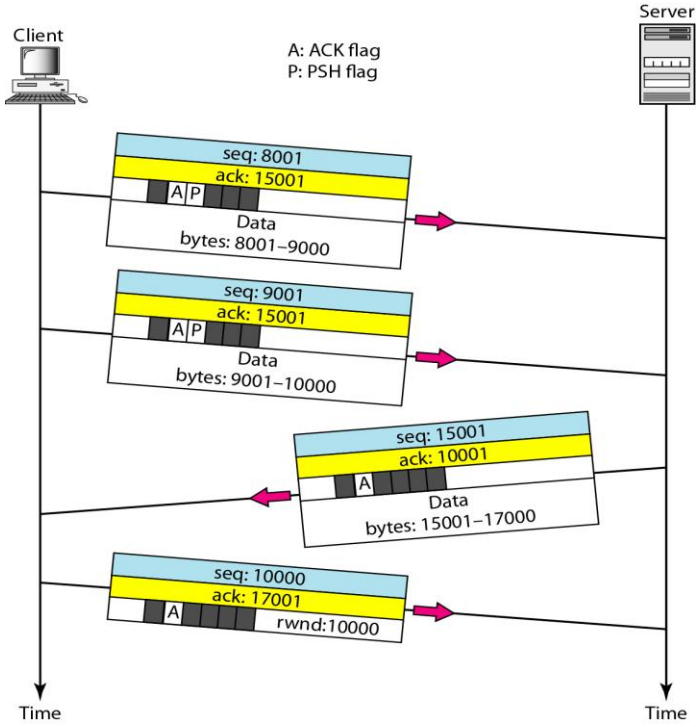
Timeline for three-way handshake algorithm.

- Finally, the client responds with a third segment that acknowledges the server's sequence number (Flags = ACK, Ack = y + 1).
- The reason that each side acknowledges a sequence number that is one larger than the one sent is that the Acknowledgment field actually identifies the "next sequence number expected."

Connection establishment using three-way handshaking:



Data transfer:



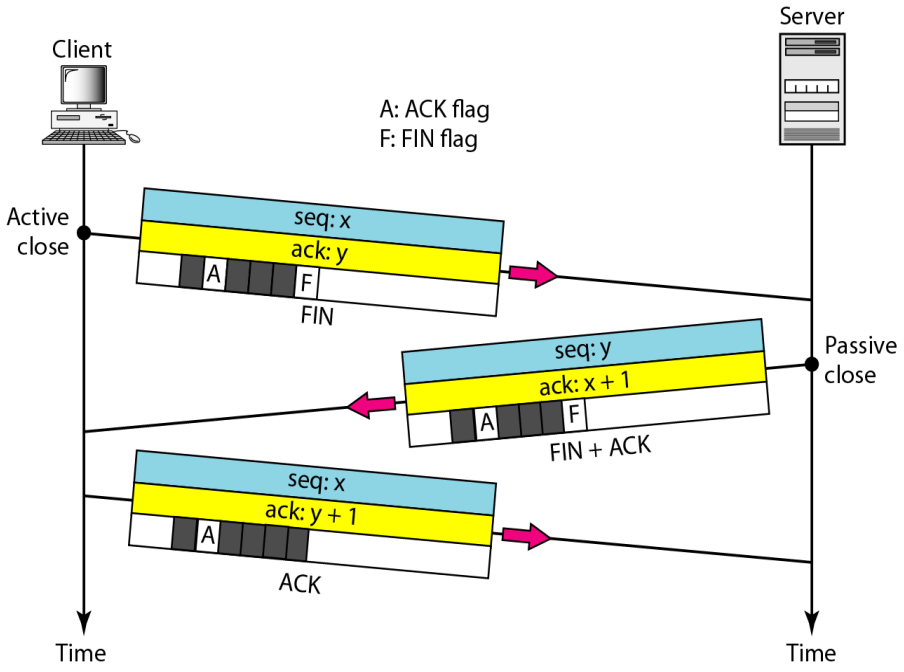
Connection Termination:

- Connection termination or teardown is symmetric. It can be done in two ways
- **Three-way close** : Both client and server close simultaneously. Client sends a FIN segment. The FIN segment can include last chunk of data. Server responds with FIN + ACK segment to inform its closing. Finally, client sends an ACK segment.
- **Half-Close:** One end can stop sending while still receiving data, known as half-close.

Client half-closes the connection by sending a FIN segment.

- Server accepts the half-close by sending the ACK segment. Data transfer from client to the server *stops*.
- After sending all data, server sends a FIN segment to the client, which is acknowledged by the client.

Connection termination using three-way handshaking:



4. TCP State Transition Diagram

States involved in opening and closing a connection is shown above and below **ESTABLISHED** state respectively.

Operation of sliding window is hidden in the ESTABLISHED state

***Opening*:**

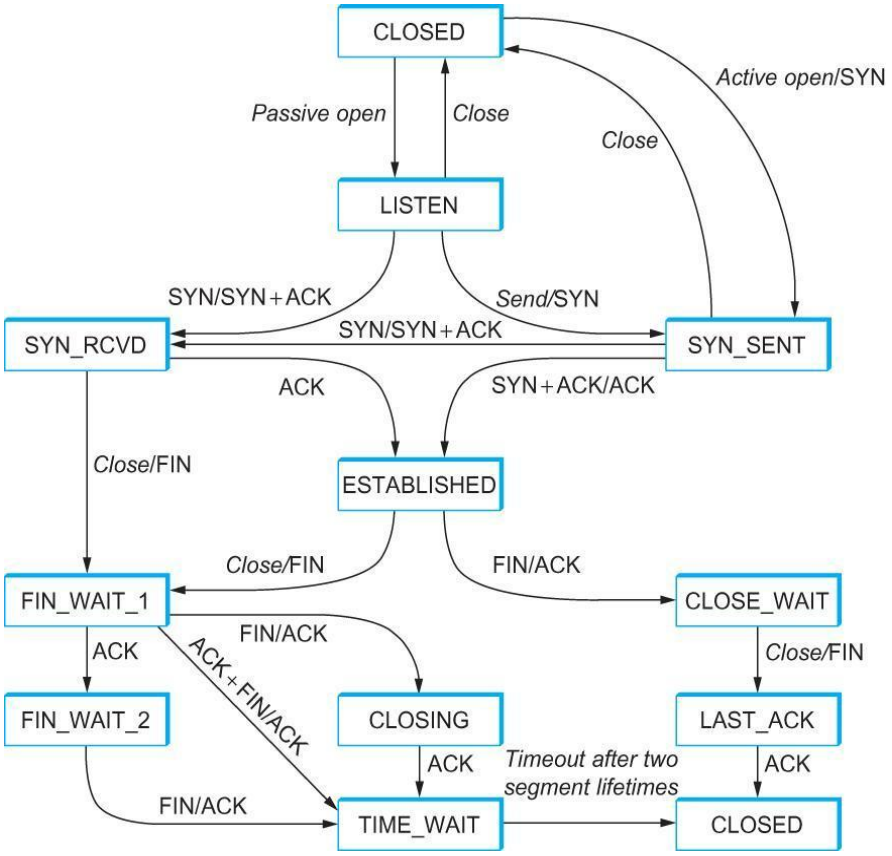
- Server invokes a *passive* open on TCP, which causes TCP to move to LISTEN state
- Later, the client does an *active* open, which causes its end of the connection to send a SYN segment to the server and to move to the SYN_SENT state.
- When SYN segment arrives at the server, it moves to SYN_RCVD state and *responds* with a SYN + ACK segment.
- Arrival of SYN + ACK segment causes the client to move to ESTABLISHED state and sends an ACK to the server.
- When ACK arrives, the server finally moves to ESTABLISHED state.

- Even if the client's ACK gets lost, sever will move to ESTABLISHED state when the first data segment from client arrives.

***Closing*:**

- Process on both sides of the connection can independently close its half of the connection or simultaneously.
- Transitions from ESTABLISHED to CLOSED state are:
- *One side closes*: ESTABLISHED FIN_WAIT_1 FIN_WAIT_2 TIME_WAIT CLOSED *Other side closes*: ESTABLISHED CLOSE_WAIT LAST_ACK CLOSED
- *Simultaneous close*: ESTABLISHED FIN_WAIT_1 CLOSING TIME_WAIT CLOSED

The following figure describes the state transition diagram during opening and closing connection:



TCP state transition diagram

5. Explain the Congestion Control mechanism in TCP:

OR

Explain slow start, additive increase and multiplicative decrease in TCP:

Need: To avoid the congestion this occurs in the network or at the receiver.

The Sender's window size is determined by two factors:

(i) Receiver window size

(ii) Congestion Window size

Actual window size = minimum (rwnd, cwnd)

Where, rwnd is the receiver window and cwnd is the congestion window size.

- In TCP congestion is handled by three phases:

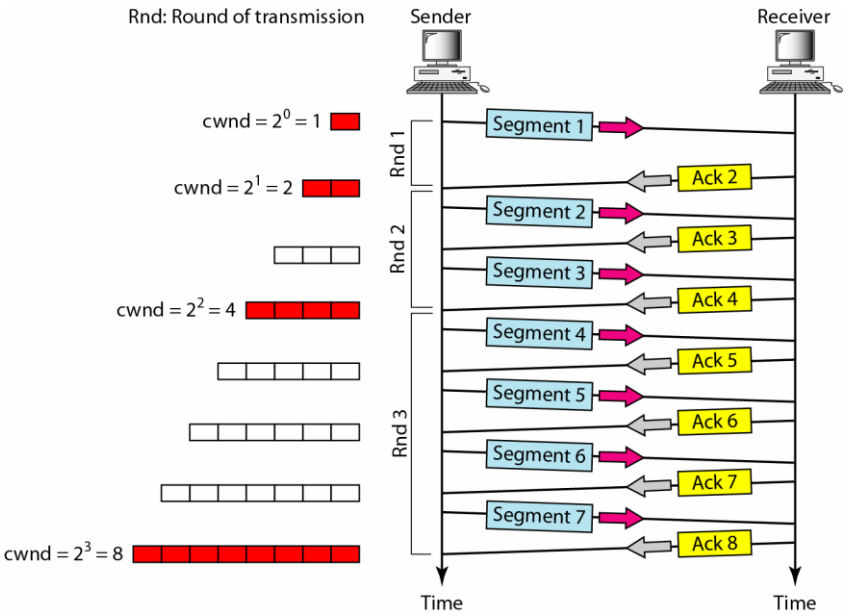
(i) Slow start phase

(ii) Congestion avoidance phase

(iii) Congestion detection phase

(i) Slow start, exponential increase:

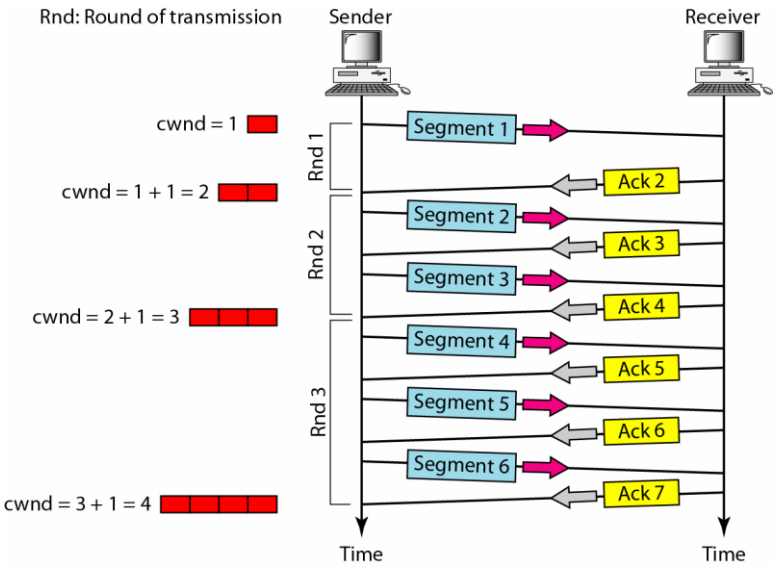
- In the slow-start algorithm, the size of the **congestion window increases exponentially until it reaches a threshold.**
- At the beginning of the connection, TCP sets the congestion window size to the maximum segment size.
- For each segment that is ACK, TCP increases the size of the congestion window by one segment size until it reaches a threshold of one half of the allowable window size. This is referred to as slow start, because the process is not slow at all.
- The size of the congestion window increases exponentially.



Ex: If the sender sends one segment, receives the ACK, increases the size to two segments, sends two segments, receiving ACK for two segments, increases the size to 4 segments, sends 4 segments receives ACK for 4 segments, increases the size to 8 segments and so on.

(ii) Congestion avoidance, additive increase:

To avoid congestion before it happens the exponential growth should be slow down.

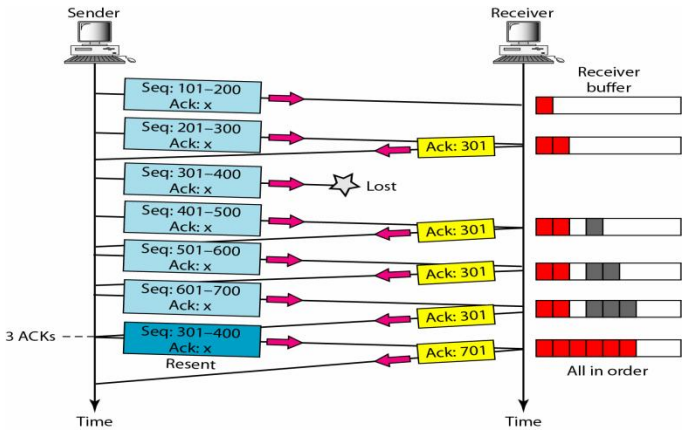


- After the window size reaches the threshold, the size is increased one segment for each ACK even if an ACK is for several segments.
- **In the congestion avoidance algorithm, the size of the congestion window increases additively until congestion is detected.**

(iii) Congestion Detection: (**Multiplicative Decrease):**

- If **congestion occurs**, the **cwnd size must be decreased.**

The only way the sender can guess that congestion has occurred is through a lost segment. When a segment has been lost retransmission occurs.

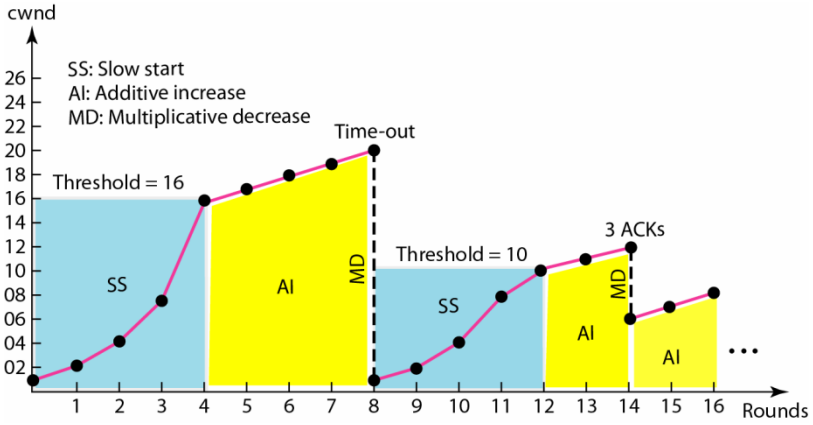


Retransmission occurs in two cases:

(i) When a timer times out.

(ii) When three ACK's are received.

Solution: In both cases the **size of the threshold is dropped to one half, a multiplicative decrease.**



Let us assume the maximum window size is 32 segments. The threshold is set to 16 segments (one half of the maximum window size). In the slow start phase the size of the window size starts from 1 and grows exponentially until it reaches threshold.

After it reaches the threshold, the congestion avoidance (additive increase) procedure allows the window size to increase linearly until a time out occurs or the maximum window size is reached.

In the figure shown above the time out occurs when the window size is 20. At this moment, the multiplicative decrease procedure takes over and reduces the threshold to one half of the previous window size.

The previous window size was 20 when the time out happened so the new threshold is now 10. TCP moves to slow start again and starts with a window size of 1, and TCP moves to additive increase when the new threshold is reached. When the window size is 12, three ACKs even happens.

The multiplicative decrease procedure takes over again. The threshold is set to 6 and TCP goes to the additive increase phase this time. It remains in this phase until another time out or another three ACKs happen.

6. Compare TCP and UDP

TCP	**UDP**
Connection oriented.	Connectionless.
Connection is byte stream	Connection is message stream.
Does not support multicasting and broadcasting.	Support broadcasting.
It provides error control and flow control.	It does not provide error control and flow control.

Supports full duplex communication.	Does not support full duplex communication.
Reliable protocol.	Unreliable protocol.
Packet is called segment.	Packet is called user datagram.

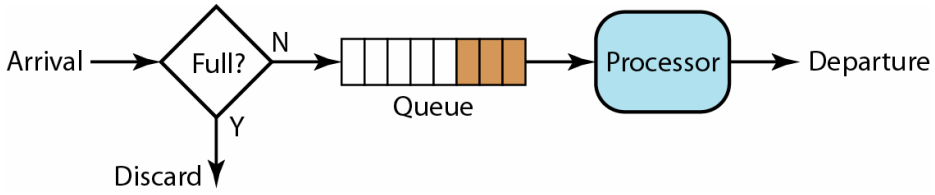
7. What are the various methods or techniques to improve the QOS?

The various methods to improve the QOS are:

1. Scheduling
2. Traffic Shaping
3. Resource Reservation
4. Admission control

(I) SCHEDULING

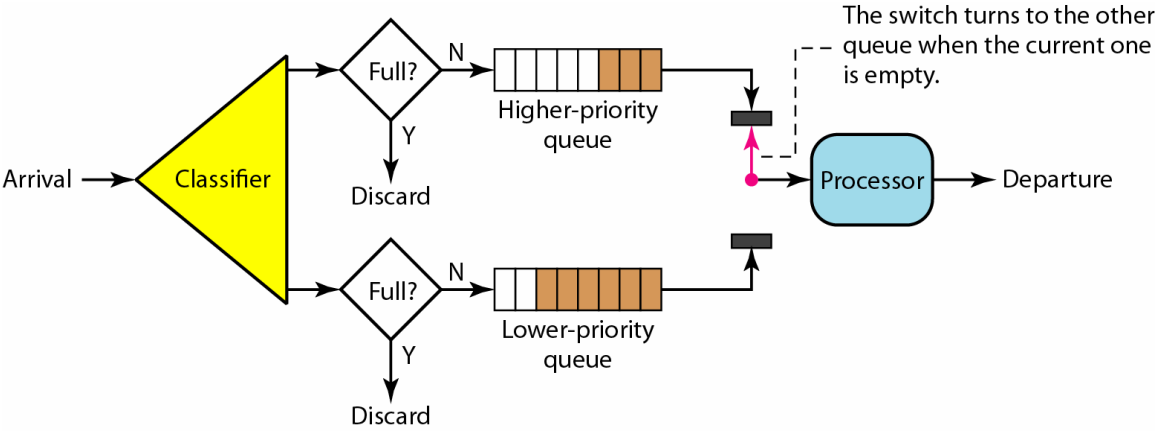
1. **FIFO Queuing:** In FIFO packets wait in a buffer (queue) until the node (router or switch) is ready to process them. If the arrival rate is higher than the average processing rate, the queue will fill up and new packets will be discarded.



Drawback:

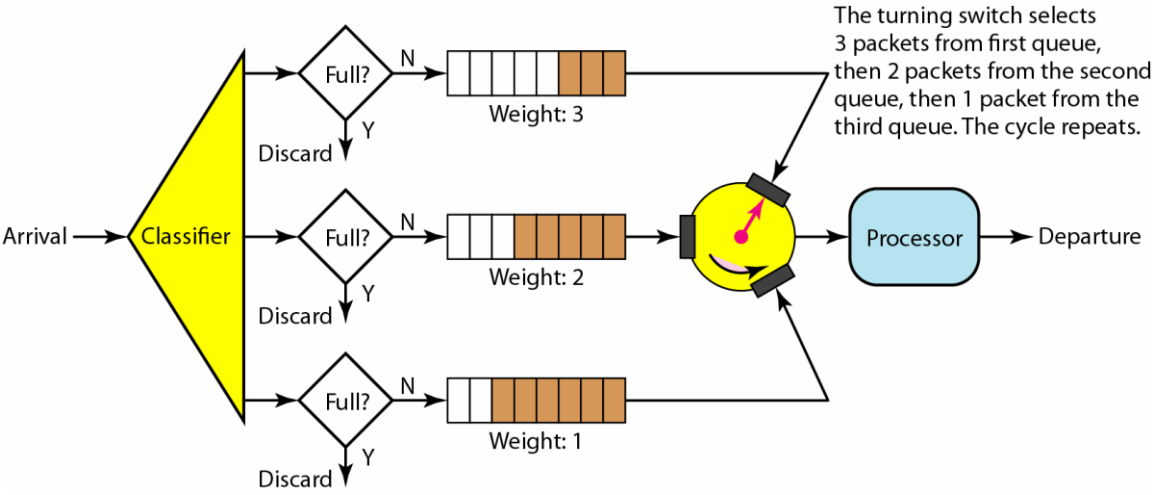
No special treatment is given to packets that are of higher priority and to packets those are more delay sensitive. If a number of packets from different flows are ready to forward, they are handled strictly in FIFO order.

2. Priority Queuing: In priority queuing packets are first assigned to a priority class. Each priority class has its own queue. The packets in the highest priority queue are processed first. Packets in the lowest priority queue are processed last.



Drawback: If there is a continuous flow in a high priority queue the packets in the lower priority queues will never have a chance to be processed.

3. Weighed Fair Queuing: In this technique the packets are still assigned to different classes and admitted to different queues. The **queues,** however, are **weighted based on the priority of the queues; higher priority means a higher weight**.



The system processes packets in each queue in a round robin fashion with the number of packets selected from each queue based on the corresponding weight. For example if the weights are 3, 2 and 1 three packets are processed from the first queue, two from the second queue, and one from the third queue.

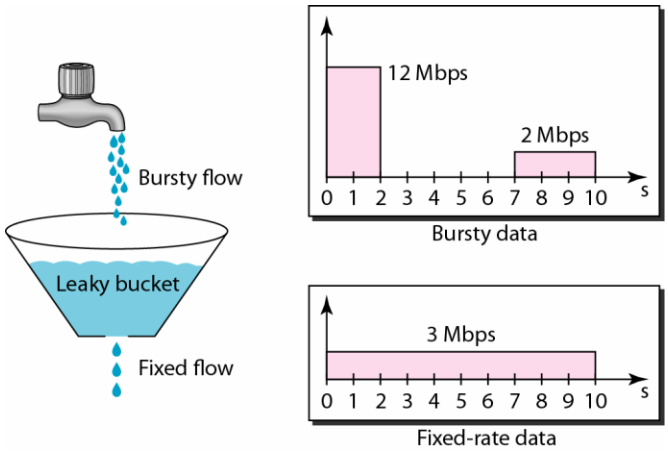
(II) TRAFFIC SHAPING:

TRAFFIC SHAPING: It is a mechanism used to control the amount and the rate of the traffic sent to the network.

1. Leaky Bucket:

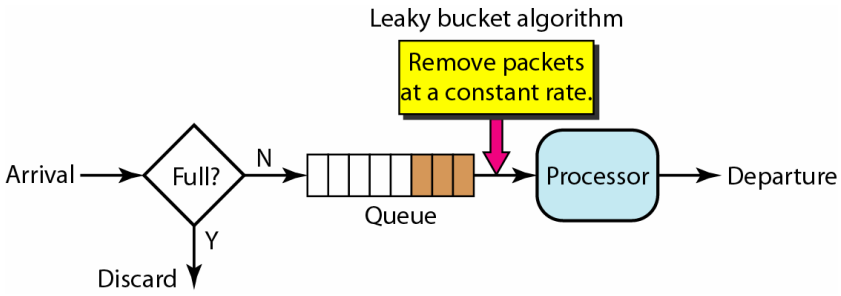
- If a bucket has a small hole at the bottom the water leaks from the bucket at a constant rate as long as there is water in the bucket. The rate at which the water leaks does not depend on the rate at which the water is input to the bucket.
- The input rate can vary but the output rate remains constant.

Similarly, in networking a technique called leaky bucket can smooth out bursty traffic.



- In the figure shown below the host sends a burst of data at the rate of 12 Mbps for 2s, for a total of 24 Mega bits of data. The host is silent for 5s and then sends data at a rate of 2 Mbps for 3s, for a total of 6 Mega bits of data.
- Totally the host has sent 30 Mega bits of data in 10s. The leaky bucket smooths the traffic by sending out data at a rate of 3 Mbps during the same 10s. Without the leaky bucket, the beginning burst may have hurt the network by consuming more bandwidth than is set aside for this host.

Leaky Bucket Implementation: A simple leaky bucket implementation is shown in figure:

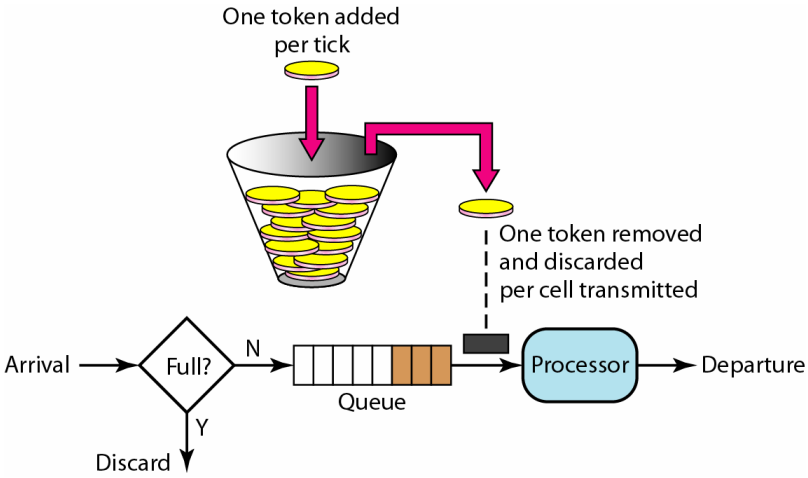


2. Token Bucket:

<u>Need</u>:

- The leaky bucket is very restrictive. It does not credit on idle host. For ex: if a host is not sending for a while, its bucket becomes empty.
- Now, if the host has bursty data, the leaky bucket allows only on average rate. The time when the host was idle is not taken into account.

In token bucket the idle hosts accumulate credit for the future in the form of tokens. For each tick of the clock, the system sends n tokens to the bucket. The system removes one token for every cell (or byte) of data sent.



For ex: if n is 100 and the host is idle for 100 ticks, the bucket collects 10,000 tokens. Now the host can consume all these tokens in one tick with 10,000 cells or the host takes 1000 ticks with 10 cells per tick.

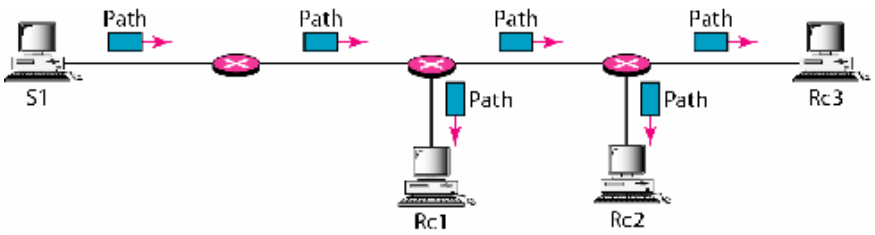
Advantage: Token bucket can send bursty data of long as the bucket is not empty.

(III) Resource Reservation: A flow of data needs resources such as buffer, bandwidth etc. The QOS is improved if these resources are reserved before itself.

RSVP uses two basic message types: Resv and Path.

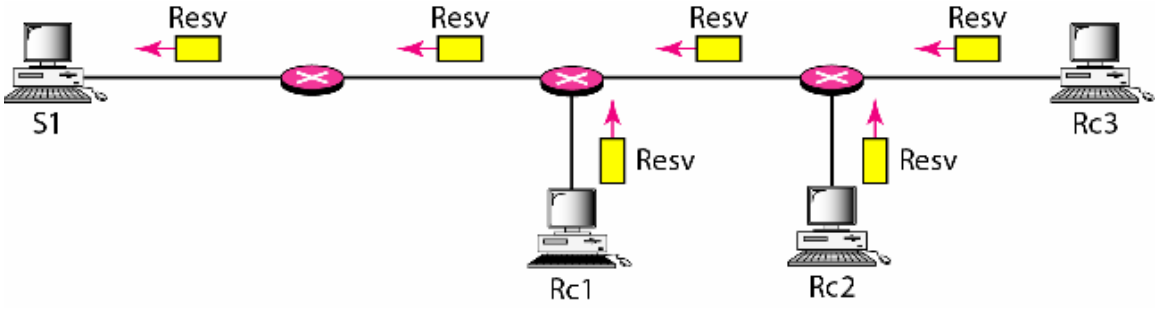
Path messages:

A path message travels from the sender and reaches all receivers in the multicast path. On the way the path message stores the necessary information for the receivers.



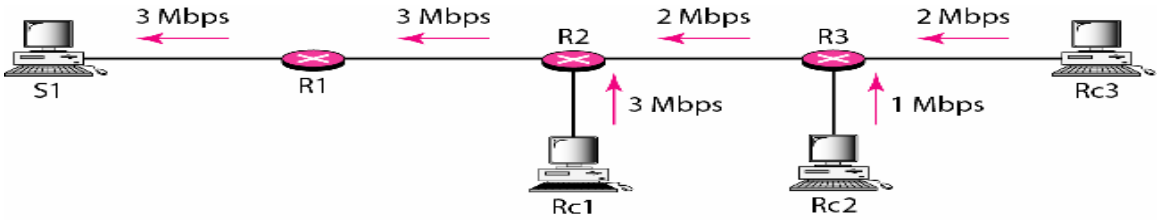
Resv messages:

After receiver has received a path message it sends a Resv message. The Resv message travels toward the sender (upstream) and makes a resource reservation on the routers that support RSVP.

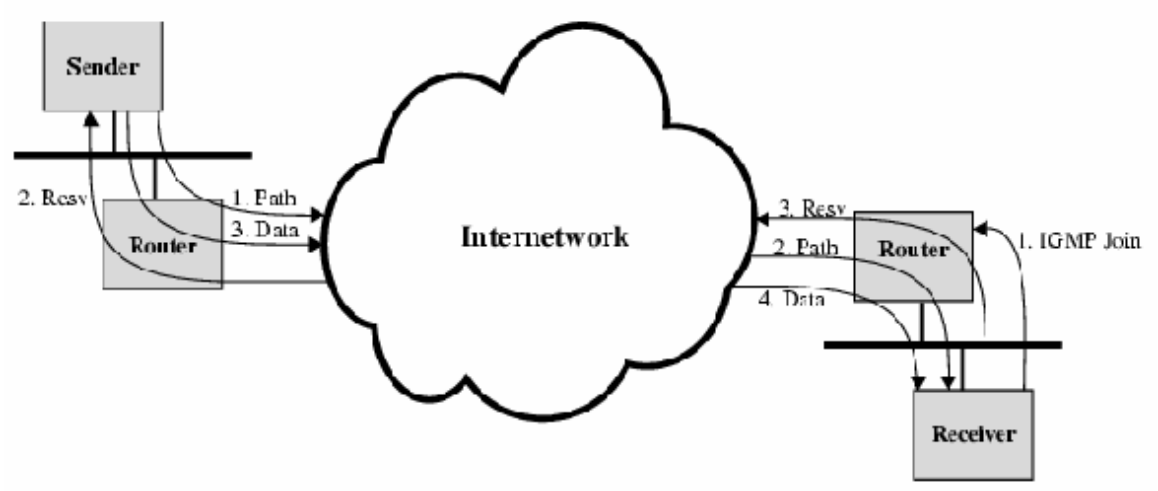


Reservation Merging:

In RSVP the resources are not reserved for each receiver in a flow; the reservation is merged. In the below figure RC3 request a 2- Mbps bandwidth while RC2 requests a 1- Mbps bandwidth. Router R3 which needs to make a bandwidth reservation merges the two requests. The reservation is made for 2- Mbps, the larger the two because a 2- Mbps input reservation can handle both requests.



The figure illustrates the operation of the protocol from the host perspective. The following events occur:

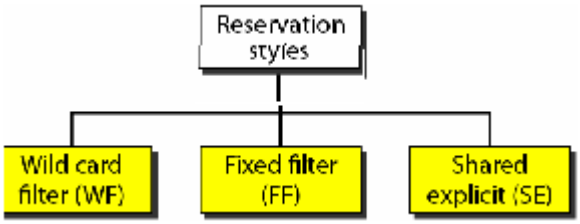


- A receiver joins a multicast group by sending an IGMP (Internet Group Message Protocol) join message to a neighboring router.
- A potential sender issues a path message to the multicast group address.
- A receiver receives a path message identifying a sender.
- Now that the receiver has reverse path information, it may begin sending Resv messages, specifying the desired flow descriptors.
- The Resv message propagates through the internet and is delivered to the sender.
- The sender starts sending data packets.
- The receiver starts receiving data packets.

Different types of reservation styles defined in RSVP:

Need for Reservation

When there is more than one flow the router needs to make a reservation to accommodate all of them. RSVP defines three types of reservation styles:



Wild card filter (WF) style:

- In this style, the **router creates a single reservation to all senders.** The reservation is based on the largest request.
- This type of style is used when the **flows from different senders do not occur at the same time**.

Fixed filter style:

- In this style the router creates a **distinct reservation** for **each sender** (i.e.) if there are n senders n different reservations are made.
- This type of style is **used when the flows from different senders occurs at the same time.**

Shared explicit style:

- In this style the router creates a single reservation which can be shared among explicit list of senders.

(IV) Admission Control: It refers to the mechanism used by the router or a switch to accept or reject a flow.

8. Explain RED algorithm in detail:

- Is one of the technique in order to prevent the congestion. The method is referred to as proactive packet discard technique.
- In this technique a router discards one or more incoming packets before the output buffer is completely full, in order to improve the performance of the network.

Motivations:

When there is a surge of congestion on a network router buffers fill up and routes begin to drop packets. For TCP traffic this is a signal to enter the slow start phase, which reduces the load on the network and relives the congestion. Two drawbacks are present due to this effect:

(i) Lost packets should be retransmitted.

(ii) Global synchronization

The solution is to use bigger buffers at each router to reduce the probability of dropping packets. This is a bad solution for two reasons. First as these big buffers fills up the delays suffered by all connections increase dramatically, second we cannot build buffers big enough. Big buffers arrive one after another so that congestion is sustained and the buffer requirements grow. A better solution would be to anticipate the onset of congestion and tell one TCP connection at a time to slow down. Then measure the effect of that one slow down before if necessary slowing down another connection. In this fashion as congestion begins the brakes are gradually applied to reduce traffic load gently, with minimal impact on TCP connections and without global synchronization. RED provides this solution.

RED design goals:

(i) **Congestion avoidance:** RED is designed to avoid congestion rather than react to it. Thus RED must detect the onset of congestion to maintain the network in a region of low delay and high throughput.

(ii) **Global synchronization avoidance:** When the onset of congestion is recognized, the router must decide which connection or connections to notify to bakeoff. By detecting congestion early and notifying only as many connections as necessary, global synchronization is avoided.

(iii) **Avoidance of bias against burst traffic:** The onset of congestion is likely to occur with the arrival of a burst of traffic from one or a few sources. This burst adds to the

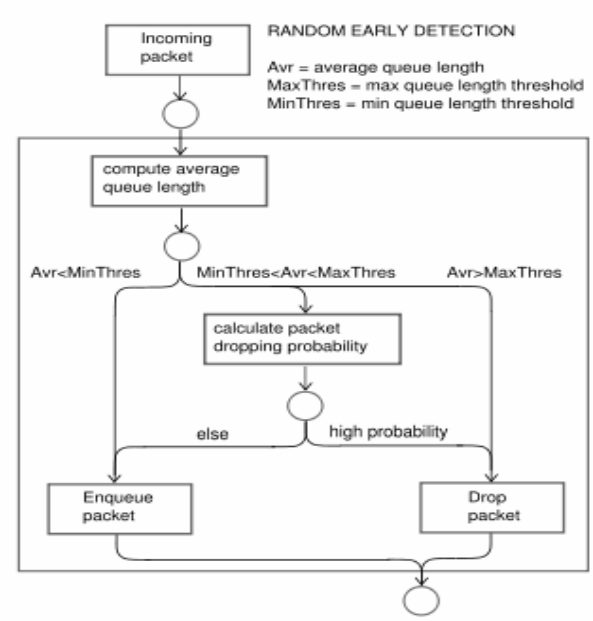
burden already supported at the router. If only arriving packets are selected for dropping then it is likely that the discard algorithm will be biased against burst sources as compared to smooth sources with the same average traffic.

(iv) Bound on average queue length: RED should be able to control the average queue size and therefore control the average delay.

Algorithm: The algorithm performs two functions each time a new packet arrives at a FIFO output queue.

1. The first step is to compute the average queue length, avg. This average queue length is compared to two thresholds. If avg is less than a lower threshold TH_{min}, congestion is assumed to be minimal or non existent, and the packet is placed in the queue.
2. If avg is greater than or equal to an upper threshold TH_{max}, congestion is assumed to be serious and the packet is discarded.
3. If avg is between the two thresholds, then we are in an area that might indicate the onset of congestion. In this region a probability P_a is calculated that depends on the exact value of avg and that increases the closer avg gets to the upper threshold. When the queue is in this region, the packet is discarded with probability P_a and queued with probability $1-p_a$.

Flowchart:



RED algorithm

calculate the average queue size, *avg*

if *avg* < *THmin*

queue the packet

else if $THmin \leq avg < THmax$

calculate probability *Pa*

with probability *Pa*

discard the packet

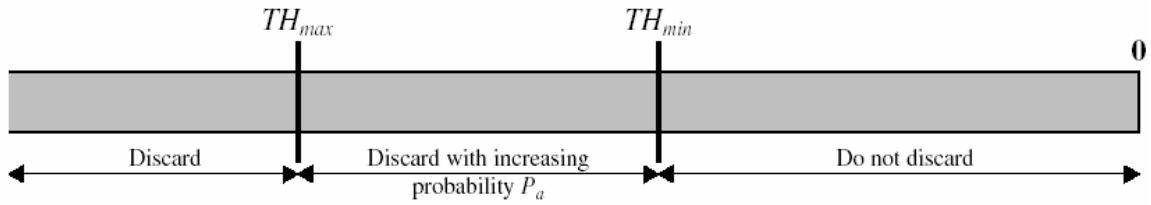
else with probability $1 - Pa$

queue the packet

else if $avg \geq THmax$

discard the packet

The first part of the algorithm (calculate queue size) determines the degree of burstiness to be allowed, and the second part of the algorithm (determine packet discard) determines the frequency of dropped packets given the current level of congestion.



Determining packet discard:

If avg is less than $TH_{min,}$ the incoming packet is queued, and avg is greater than or equal to TH_{max}, the incoming, the incoming packet is automatically discarded. The critical region is for a value of avg between the two thresholds. In this region, RED assigns a probability of discard to an incoming packet that depends on two factors:

(i) The closer avg is to TH_{max}, the higher the probability of discard.

As long as avg is in the critical range we keep a count of how many consecutive packets escape discard: the higher the value of count, the higher the probability of discard.

UNIT 5: APPLICATION LAYER

Application Layer Paradigms – Client Server Programming – World Wide Web and HTTP – DNS - Electronic Mail (SMTP, POP3, IMAP, MIME) – Introduction to Peer to Peer Networks – Need for Cryptography and Network Security – Firewalls.

PART-A

1. What is Domain Name Service?

DNS is a client server application that identifies each host on the internet with a user friendly name.

2. List the two types of DNS messages:

1. Query message: It consists of header and the question record.

2. Response message: It consists of header, questions record, answer record, authoritative record and additional records.

3. Why do HTTP, SMTP and POP3 run on top of TCP rather than on UDP?

Since TCP is a connection oriented protocol which requires for the applications HTTP, FTP, SMTP and POP3 they are run on top of TCP rather than on UDP.

4. What are the three domains of DNS?

Generic domain, Country domain and Inverse domain.

5. What is the purpose of the inverse domain?

The inverse domain finds a domain name for a given IP address. This is called address to name resolution.

6. What are the three types of web documents?

Static document Active document and Dynamic document.

7. What is the difference between active document and a dynamic document?

A dynamic document is the product of a program run by a server as requested by a browser. An active document is the product of a program sent from the server to the client and run at the client site.

8. What is the purpose of Domain Name System?

Domain Name System can map a name to an address and conversely an address to name.

9. Discuss the three main division of the domain name space:

Domain name space is divided into three different sections: generic domains, country domains & inverse domain.

Generic domain: Define registered hosts according to their generic behavior, uses generic suffixes.

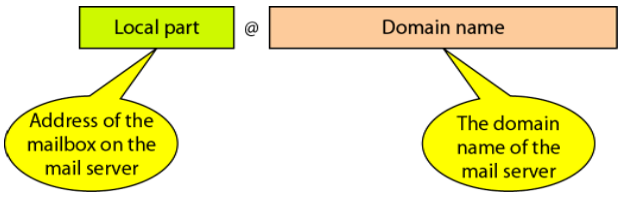
Country domain: Uses two characters to identify a country as the last suffix.
Inverse domain: Finds the domain name given the IP address.

10. Define SMTP.

Is a protocol that supports e-mail on the internet is called Simple Mail Transfer Protocol.

11. What are the two parts of addressing system used in SMTP?

The addressing system used by SMTP consists of two parts: a local part and a domain name separated by a @ sign.



12. What is an Electronic mail?

e-mail is a popular application in which a user or a computer sends a memo to one or more receivers.

13. What are the functions of e-mail?

Compose, transfer, reporting and displaying.

14. What is MIME?

MIME – Multipurpose Internet Mail Extension:

Need:

- SMTP cannot support Non ASCII characters such as French, German, Russian, Chinese and Japanese.
- SMTP cannot be used to send binary files or to send video or audio data also.

Hence, for such applications MIME protocol is used.

15. What is Post office protocol (POP)?

Need: SMTP expects the destination host, the mail server receiving the mail, to be on-line all the time; else a TCP connection cannot be established. For this reason, it is not practical to establish an SMTP session with a desktop computer because desktop computer are usually powered down at the end of the day.

16. What are the four types or groups of HTTP header?

1. General Header
2. Entity Header
3. Request Header
4. Response Header

17. Define www or World Wide Web.

The WWW today is a distributed client/server service, in which a client using a browser can access a service using a server. However, the service provided is distributed over many locations called sites.

18. List the advantages of IMAP over POP.

User can check the e-mail header prior to downloading.

User can search e-mail for a specific string of characters prior to downloading.

User can download partially, very useful in case of limited bandwidth.

User can create, delete, or rename mailboxes on the mail server.

19. What is hypertext?

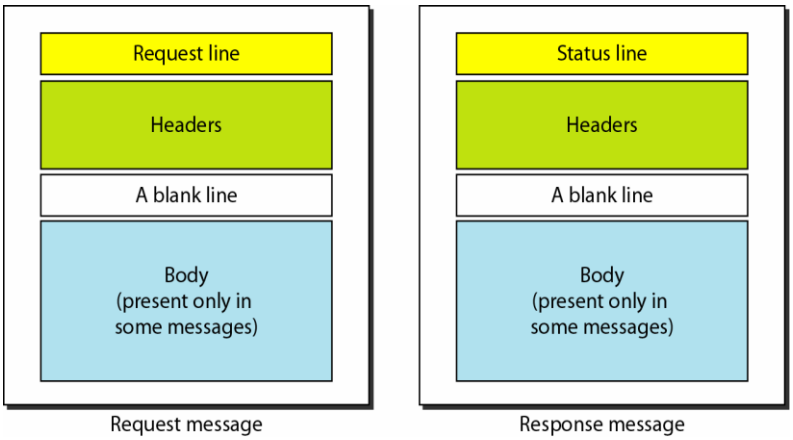
Hypertext is a text that contains embedded URL known as links.

When hypertext is clicked, browser opens a new connection, retrieves file from the server and displays the file.

20. **Distinguish between application programs and application protocol.**

- Application program are client process that run on hosts, such as Chrome, Firefox, etc.
- Application protocols control client/server communication, such as FTP, HTTP, SMTP.
- Different applications might be use the same protocol. For example, web browsers use HTTP to retrieve web pages from a web server.

21. What are the two messages used by HTTP?



22. What is non persistent connection in HTTP?

Non Persistent connection: In non persistent connection one TCP connection is made for each request/response. The following steps are involved in non persistent connection:

1. The client opens a TCP connection and sends a request.
2. The server sends the response and closes the connection.
3. The client reads the data until it encounters an end of file marker; it then closes the connection.

Therefore, for N different pictures in different files, the connection must be opened and closed N times.

Drawback: The nonpersistent strategy imposes high overhead on the server because the server needs N different buffers and requires a slow start procedure each time a connection is opened.

23. **What is persistent connection in HTTP?**

- HTTP version 1.1 specifies persistent connection.
- In persistent connection the server leaves the connection open for more requests after sending a response.
- The server can close the connection at the request of a client or if a time-out has been reached.

24. What is the function of proxy server in HTTP?

- A proxy server is a computer that keeps copies of responses to recent requests.
- The HTTP client sends a request to the proxy server. The proxy server checks its cache.
- If the response is not stored in the cache, the proxy server sends the request to the corresponding server.
- Incoming responses are sent to the proxy server and stored for future request from other clients.

Advantage: The proxy server reduces the load on the original server and reduces the delay.

25. What is encryption and decryption?

- Encryption means the sender transforms the original information to another form and sends the resulting unintelligible message out over the network.
- Decryption reverses the encryption process in order to transform the message back in to its original form.

26. What is the relation between plaintext and cipher text?

- The sender uses an encryption algorithm and a key to transform the plain text (original message) in to a cipher text (encrypted message).
- The receiver uses decryption algorithm and a key to transform the cipher text back to the original form.

27. Define cryptography. State the types of cryptographic algorithms? [April-05]

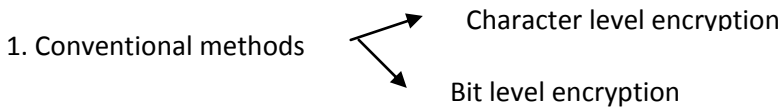
Cryptography is a technique of encoding (i.e. encrypting) and decoding (i.e. decrypting) messages. The types are: 1. Secret key encryption (or) private key symmetric encryption. **E.g.** Data encryption standard (DES). 2. Public key encryption **E.g.**: RSA Algorithm.

28. What are the categories of encryption (or) Decryption methods?

(OR)

What are the classifications of encryption methods? [April-04]

The categories of encryption /Decryption are



2. Public key encryption

- In conventional method encryption and decryption key are same.
- In public key method encryption key is same but decryption algorithm is kept secret.

29. What is monoalphabetic and polyalphabetic substitution?

(OR)

Define the types of substitution encryption?

- The monoalphabetic encryption algorithm simply adds a number to the ASCII code of the character; the decryption algorithm simply subtracts the same number from the ASCII code.
- In poly alphabetic substitution each occurrence of a character can have a different substitute .it finds the position of the character in the text and uses the character in the text and use that value in the key.

30. What is transpositional encryption?

In Transpositional encryption the characters retain their plain text form but change their position to create the cipher text. The text is organized in to a two dimensional table, and the columns are interchanged according to the key.

31. Contrast straight compressed and expanded permutation:

- In straight permutation the number of bits in the input and output are preserved only the positions are interchanged.
- In compressed permutation the number of bits is reduced.
- In expanded permutation the number of bits is increased.

32. What is DES? (OR) For private key encryption, discuss the keys and their ownership:

- DES is the data encryption standard was designed by IBM and adopted by the U.S government as the standard encryption method.
- Here only one key is used and the same key is used for encryption and decryption and both parties must agree the key before any transmission begins.

33. What is RSA encryption? (OR) Write about public key encryption?

- The RSA algorithm is the best technique used for public key encryption. It is Rivest, Shamir, Adleman (RSA) encryption.
- Here one party uses a public key the other party uses a secret key. i.e. one key is used for the encryption and only the other key must be used for decryption.

34. What is reciprocity of RSA?

The RSA algorithm is reciprocal. This means the bank can use the same secret key, K_S to send a reply to the customer and the customer can decrypt the message using his own private key.

35. What are the three types of permutations in P-Box?

(i) Straight Permutation (ii) Compressed Permutation and Expansion permutation

36. Name four factors needed for a secure network.

Privacy: The sender and the receiver expect confidentiality.

Authentication: The receiver is sure of the sender's identity and that an imposter has not sent the message.

Integrity: The data must arrive at the receiver exactly as it was sent.

Non-Reputation: The receiver must able to prove that a received message came from a specific sender.

37. What is a digital signature?

Digital signature is a method to authenticate the sender of a message. It is similar to that of signing transactions documents when you do business with a bank. In network transactions, you can create an equivalent of an electronic or digital signature by the way you send data.

38. List out the services/ Factors for Secured Network?

- Message Confidentiality
- Message Integrity
- Message Authentication
- Message Non-repudiation
- Entity Authentication.

39. What are the criteria for Hash function?

- ✓ One-wayness
- ✓ Weak collision resistance
- ✓ Strong collision resistance

40. Explain briefly about Firewall.

To control access to a system, we need firewalls. A firewall is a device installed between the internal network of an organization and the rest of the Internet. It is designed to forward some packets and filter (not forward) others.

PART-B

1. Explain Domain Name System (DNS).

Domain Name System is a client server application that identifies each host on the Internet.

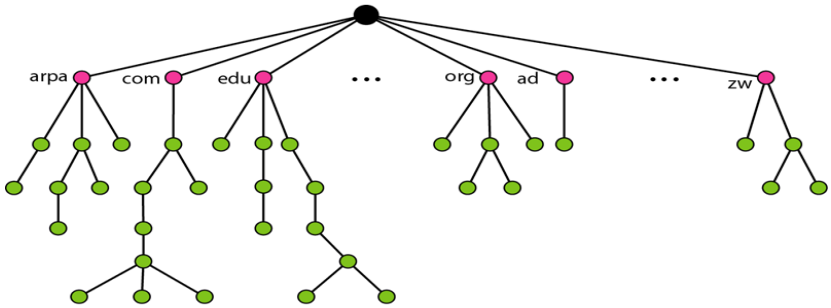
Need:

- To identify an entity (user) TCP/IP protocols use the IP address, this uniquely identifies the connection of a host to the Internet.
- However, people prefer to use names instead of addresses. Therefore we need a system that can map a name to an address and conversely an address to a name.

Flat Name Space: Here, a name is assigned to an address. A name in this space is a sequence of characters without structure. The major drawback in flat name space is that it cannot be used in a large system such as internet.

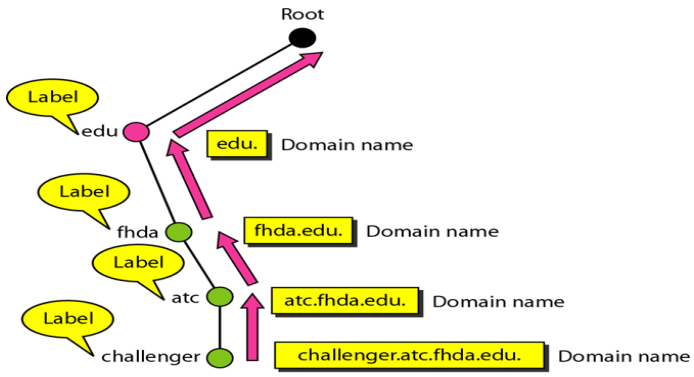
Hierarchical Name Space: A name is made of several parts. The first part define the structure of an organization, the second part define the name of an organization and the third part define departments in the organization.

DOMAIN NAME SPACE: To have a hierarchical name space, a domain name space was designed. In this design the names are defined in an inverted-tree structure with the root at the top. The tree can have only 128 levels: level 0 (root) to level 127.

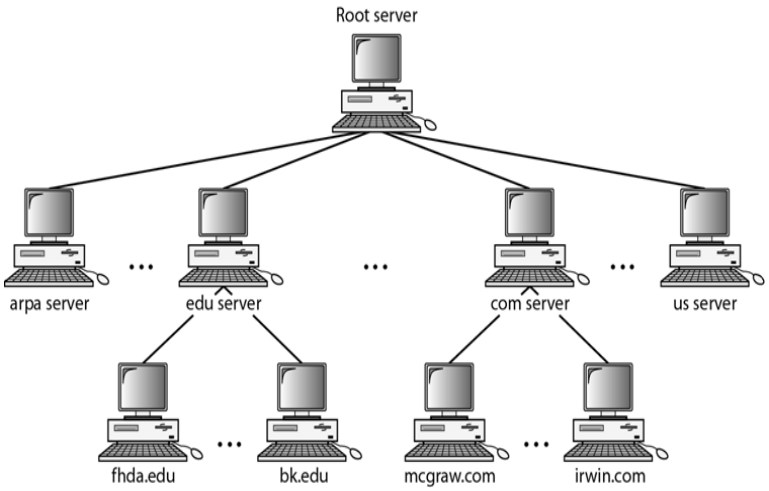


Label: Each node in the tree has a label which is a string with maximum 63 characters.

Domain Name: Each node in the tree has a domain name. A full domain name is a sequence of labels separated by dots (.).

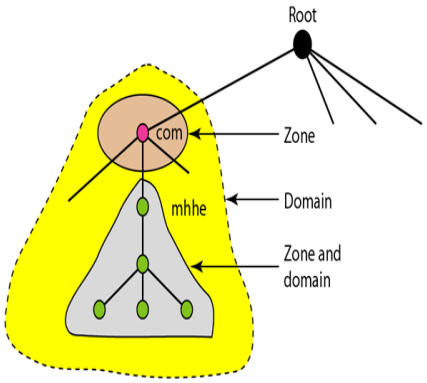


DISTRIBUTION OF NAME SPACE: The information contained in the domain name space must be stored. However, it is very inefficient and also unreliable to have just one computer store such a huge amount of information. The solution to these problems is to distribute the information among many computers called DNS servers.



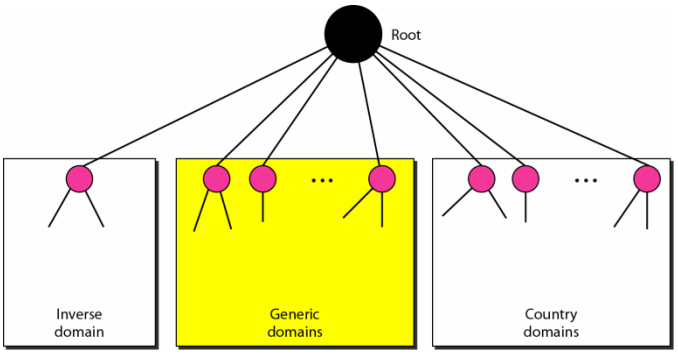
Zone: When a server is responsible or has authority over a service means then the server is referred to as zone.

Root server: Is a server whose zone consists of the whole tree.

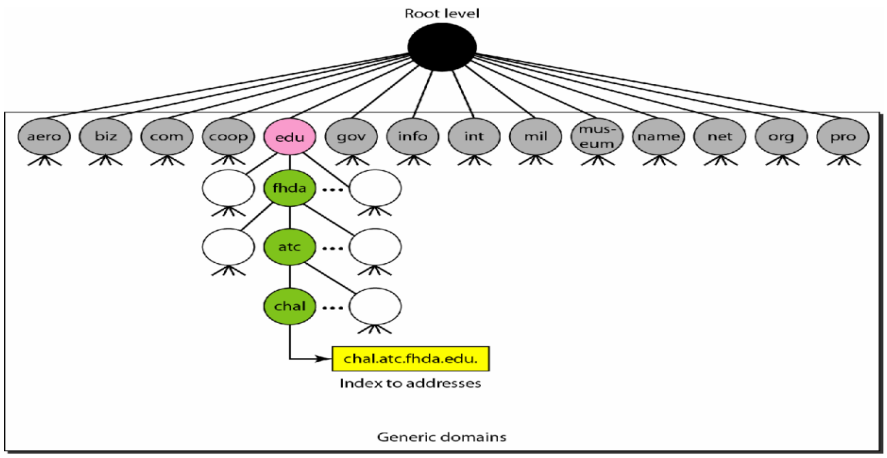


Primary and Secondary Servers: A primary server loads all information from the disk file; the secondary server loads all information from the primary server. When the secondary downloads information from the primary, it is called zone transfer.

DNS in the Internet: In the Internet, the domain name space (tree) is divided into three different sections: Generic domain, country domains and inverse domains.



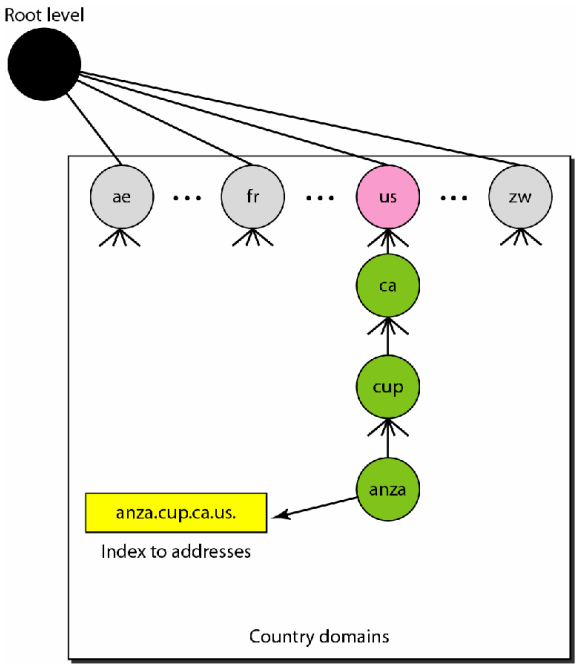
Generic Domain: According to the generic behavior registered hosts are defined by the generic domains.



The generic domain allows three character labels. These labels describe the organization types listed below in the table.

Label	*Description*
aero	Airlines and aerospace companies
biz	Businesses or firms (similar to "com")
com	Commercial organizations
coop	Cooperative business organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International organizations
mil	Military groups
museum	Museums and other nonprofit organizations
name	Personal names (individuals)
net	Network support centers
org	Nonprofit organizations
pro	Professional individual organizations

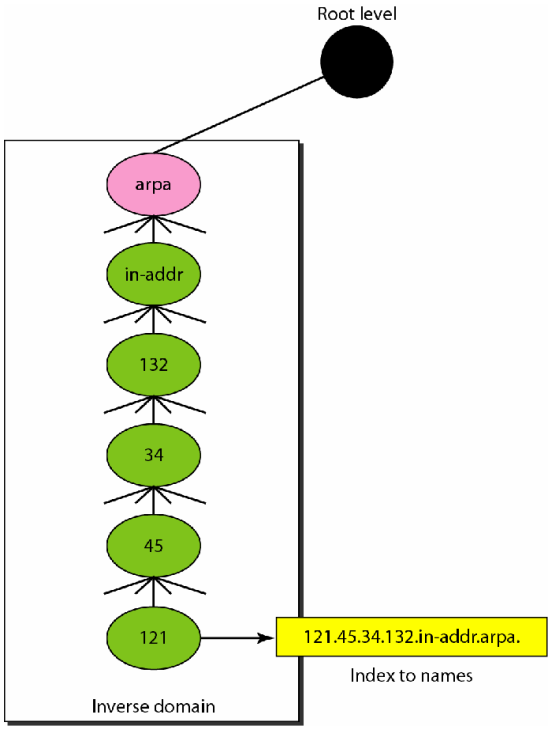
Country domain: It is similar to the generic domains but uses two character country abbreviations (e.g., "US" for United states).



The figure shows the country domain section. The address anza.cup.ca.us can be translated to DE Anza College in Cupertino in California in the United States.

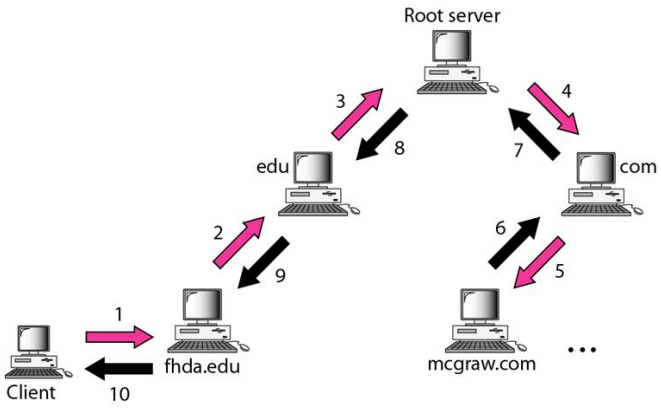
Inverse Domain: It is used to map an address to a name. It is used in situations such as when a server has received a request from a client to do a task. Whereas the server has a file that

contains a list of authorized clients, the server lists only the IP address of the client (extracted from the received IP packet).



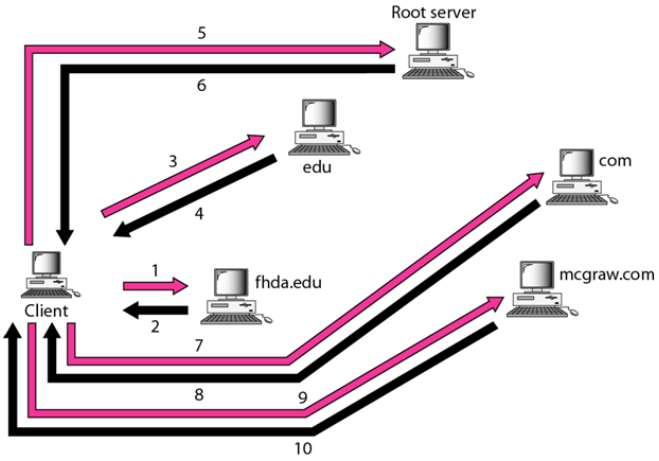
Resolver: A host that needs to map an address to a name or a name to an address calls a DN client called a resolver.

Recursive Resolution: The client (resolver) can ask for a recursive answer from a name server. This means the resolver expects the server to supply the final answer. If the server is the authority the resolver expects the server to supply the final answer.



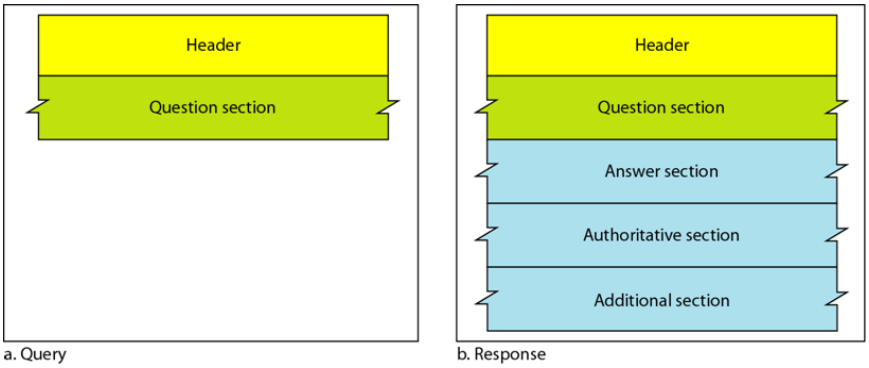
If the server is not the authority, it sends the request to another server and waits for the response. When the query is finally resolved the response travels back until it finally reaches the requesting client. This is called recursive resolution.

Iterative resolution: If the client does no ask for a recursive answer, the mapping can be done iteratively. If the server is an authority for the name, it sends the answer. If it is not it returns the IP address of the server that it thinks can resolve the query.



The client is responsible for repeating the query to this second server. If the newly addressed server can resolve the problem it answers the query with the IP address; else it returns the IP address of a new server to the client. Now the client must repeat the query to the third server. This process is called iterative resolution.

DNS MESSAGES: DNS has two types of messages: query and response. Both types have the same format. The query message consists of a header and question records; the response message consists of a header, question records, answer records, authoritative records and additional records.



Identification	Flags
Number of question records	Number of answer records (all 0s in query message)
Number of authoritative records (all 0s in query message)	Number of additional records (all 0s in query message)

Identification: Used to match client query exactly.

Flags: It defines the type of message and type of answer.

No of question: This record contains no of queries in the question section of message.

No of answers: This record contains no of answers in the response section of message.

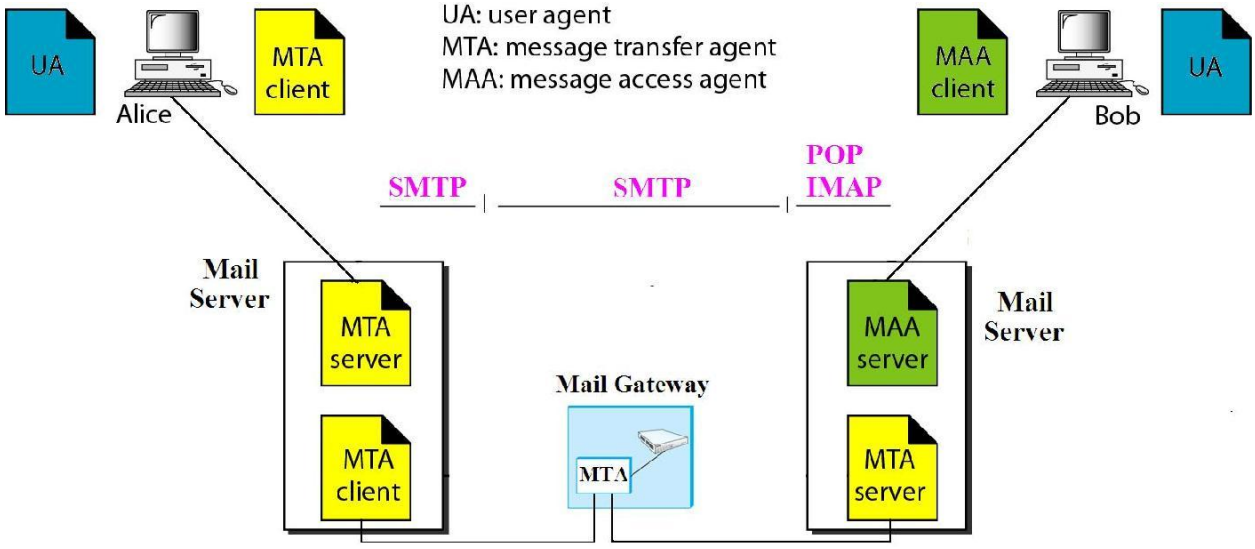
Authority: The record comes from a certain manager anybody that it is an authorized record or not. It will be checked by this field.

2. Discuss the components of an email system and the protocols used.

OR

Explain electronic mail (e - mail) or SMTP, MIME, POP.

One of the most popular Internet services is electronic mail (e-mail).The TCP/IP protocol that supports electronic mail on the Internet is called Simple Mail Transfer Protocol (SMTP).



Features of SMTP:

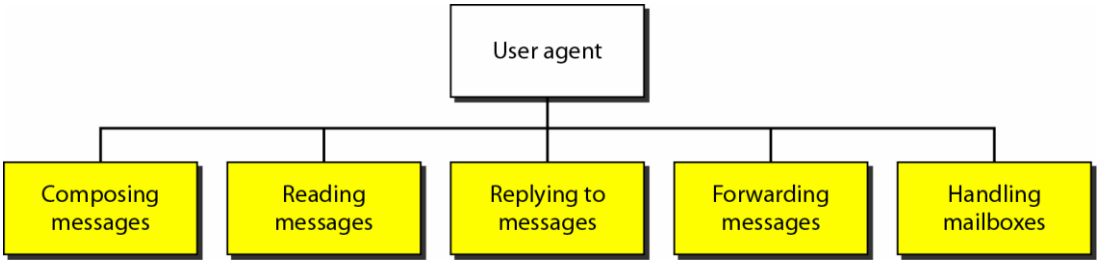
1. It is used to exchange the mail between users on the same or different computers.
2. Sending a single message to one or more recipients.
3. Sending messages that include text, voice, video or graphics.
4. Sending messages to users on networks outside the Internet.

The SMTP it consists of two basic components: User agent and Message transfer agent (MTA).

UA: It prepares the message, creates the envelope and puts the message in the envelope.

MTA: It transfers the mail across the Internet.

Services of user agent: The services provided are listed below:



Composing Messages: A user agent is responsible for composing the e-mail message to be sent out. Most user agents provide a template on the screen to be filled in by the user.

Reading messages: When a user invokes a user agent it first checks the mail in the incoming mail box. Most user agents will show a one line summary of each received mail which contains the following fields.

1. A number field
2. A flag field that shows if the mail is new, already read, but not replied, read and replied and so on.
3. The size of the message.
4. The sender.
5. The subject field if the subject line in the message is not empty.

Replying messages: After reading a message a user can use the user agent to reply to a message. A user agent allows the user to reply to the original sender or to reply to all recipients of the message.

Forwarding messages: That is sending the message to a third party.

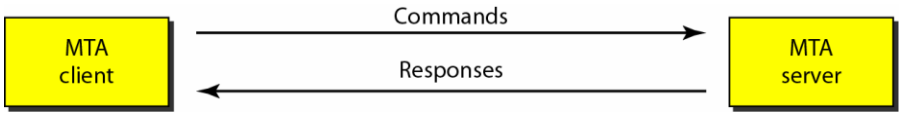
Handling mail boxes: A user agent creates two mail boxes: Inbox and Outbox. The inbox keeps all the received e-mails until they are deleted by the user. The outbox keeps all the sent e-mails until the user deletes them.

E-mail address: To deliver mail, a mail handling system must use a unique addressing system. The addressing system used by SMTP consists of two parts: a local part and a domain name separated by an @ symbol.

Local Part: The local part defines the name of a special file called the user mailbox, where all the mail received for a user is stored for retrieval by the user agent.

Domain Name: The second part of the address is domain name. An organization usually selects one or more hosts to receive and send e-mail; they are sometimes called mail exchangers.

Message Transfer Agent (MTA): To send a mail a system must have a client MTA and to receive a mail a system must have a server MTA. To send a message we need a client SMTP and server SMTP.

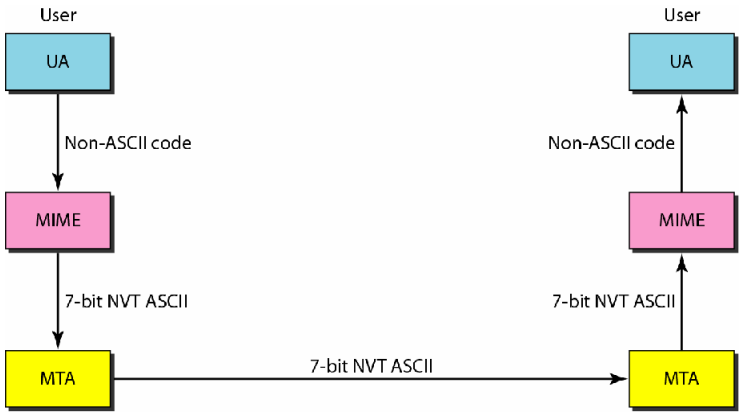


SMTP uses commands and responses to transfer messages between an MTA client and MTA server

MIME – MULTIPURPOSE INTERNET MAIL EXTENSION:

Need:

- SMTP cannot support Non ASCII characters such as French, German, Russian, Chinese and Japanese.
- SMTP cannot be used to send binary files or to send video or audio data also.

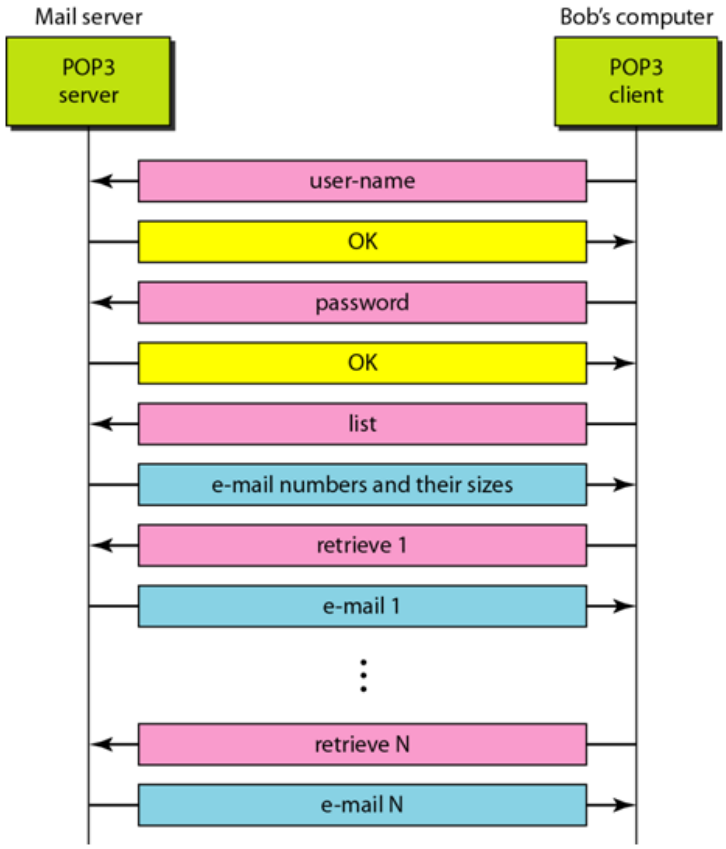


MIME allows non ASCII data to be sent through SMTP. MIME is not a protocol and cannot replace SMTP; it is only an extension to SMTP.MIME transforms non ASCII data at the sender side to ASCII data and delivers it to the client SMTP to be sent through the Internet. The server SMTP at the receiver side receives the ASCII data and delivers it to MIME to be transformed back to the original data.

POST OFFICE PROTOCOL (POP):

Need: SMTP expects the destination host, the mail server receiving the mail, to be on-line all the time; else a TCP connection cannot be established. For this reason, it is not practical to establish an SMTP session with a desktop computer because desktop computer are usually powered down at the end of the day.

Solution: In many organizations mail is received by an SMTP server that is always on-line. This SMTP server provides a mail drop service. The server receives the mail on behalf of every host in the organization. Workstations interact with the SMTP host to retrieve messages by using a client-server protocol such as Post Office Protocol (POP), version 3 (POP3).

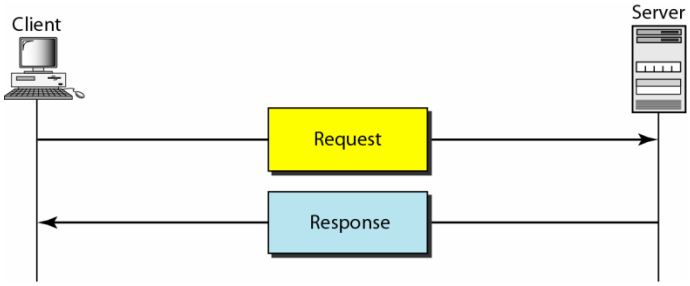


Although POP3 is used to download messages from the server, the SMTP client is still needed on the desktop to forward messages from the workstation user to its SMTP mail server.

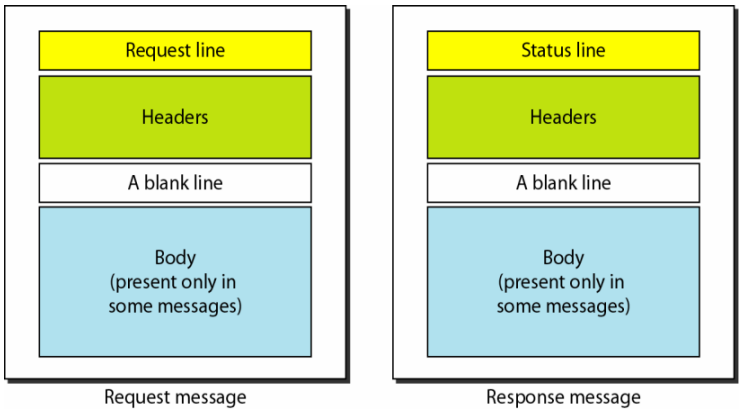
3. Write short notes on HTTP:

- Hypertext Transport Protocol (HTTP) is a protocol used mainly to access data on the World Wide Web.
- HTTP uses the services of TCP on well-known port 80.
- HTTP uses only one TCP connection.

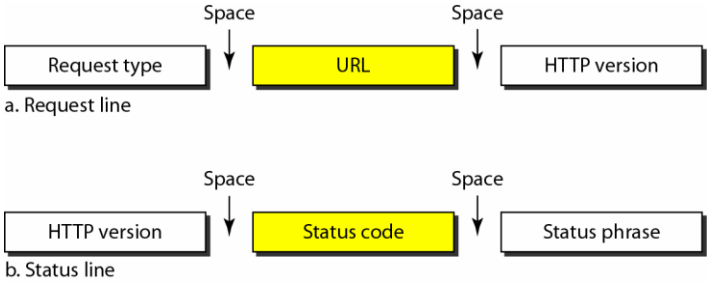
HTTP transaction: The figure illustrates the HTTP transaction between the client and server. The client initializes the transaction by sending a request message. The server replies by sending a response.



Messages: The formats of the request and response messages are similar: both are shown in figure. A request message consists of a request line, a header and sometimes a body.



Request and Status Lines: The first line in a request message is called a request line; the first line in the response message is called the status line.



Request type: This field is used in the request message.

Method	*Action*
GET	Requests a document from the server
HEAD	Requests information about a document but not the document itself
POST	Sends some information from the client to the server
PUT	Sends a document from the server to the client

Version: The most current version of HTTP is 1.1.

Status code: This field is used in the response message. It consists of three digits.

Status phrase: This field is used in the response message. It explains the status code in text form.

Header: The header exchanges additional information between the client and the server. For ex: the client can request that the document be sent in a special format or the server can send extra information about the document. The three types of header available are request header, Response header and entity header.

General Header: It gives information about the message and can be present in both a request and response.

Request header: It can be present only in a request message. It specifies the client's configuration.

Response header: It will be present only in a response message. It specifies the server's configuration and special information about the request.

Entity Header: The entity header gives the information about the body of the document.

Body: The body can be present in a request or response message.

Persistent versus Non persistent Connection:

Non Persistent connection: In non persistent connection one TCP connection is made for each request/response. The following steps are involved in non persistent connection:

1. The client opens a TCP connection and sends a request.
2. The server sends the response and closes the connection.
3. The client reads the data until it encounters an end of file marker; it then closes the connection.

Therefore, for N different pictures in different files, the connection must be opened and closed N times.

Drawback: The nonpersistent strategy imposes high overhead on the server because the server needs N different buffers and requires a slow start procedure each time a connection is opened.

Persistent connection: HTTP version 1.1 specifies persistent connection. In persistent connection the server leaves the connection open for more requests after sending a response. The server can close the connection at the request of a client or if a time-out has been reached.

Proxy Server: HTTP supports proxy server. A proxy server is a computer that keeps copies of responses to recent requests. The HTTP client sends a request to the proxy server. The proxy server checks its cache. If the response is not stored in the cache, the proxy server sends the

request to the corresponding server. Incoming responses are sent to the proxy server and stored for future request from other clients.

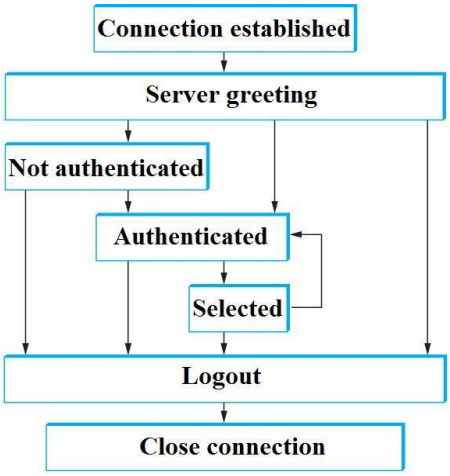
Advantage: The proxy server reduces the load on the original server and reduces the delay.

4. Write short note on Internet Message Access Protocol (IMAP)

- IMAP is a client/server protocol running over TCP.
- Current version is IMAP4.
- Client is authenticated in order to access the mailbox.
- LOGIN, AUTHENTICATE, SELECT, EXAMINE, CLOSE, LOGOUT, FETCH, STORE, DELETE, etc., are some commands that the client can issue.
- Server responses are OK, NO (no permission), BAD (incorrect command), etc.

When user asks to FETCH a message, server returns it in MIME format and the mail reader decodes it. Message attributes such as size are also exchanged.

Flags (Seen, Answered, Deleted, Recent) are used by client to report about user actions.



IMAP4 State transition

5. Define Encryption/ Decryption and write their types with examples:

Encryption means the sender transforms the original information to another form and sends the results.

Decryption reverses the encryption process in order to transform the message back to its original form.

Encryption and Decryption is classified as i) Conventional methods (ii) Public Key methods

(i)Conventional methods: - In this method, the encryption key (k_e) and the decryption key (k_d) are the same and secret. The conventional methods are again classified as:

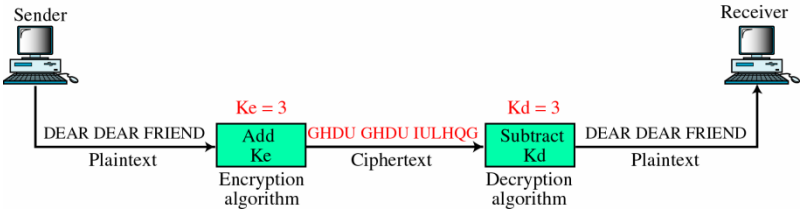
i) Character level encryption.

ii) Bit level encryption

CHARACTER LEVEL ENCRYPTION: In this encryption is done at character level. This character level encryption is again classified as, substitutional and Transpositional

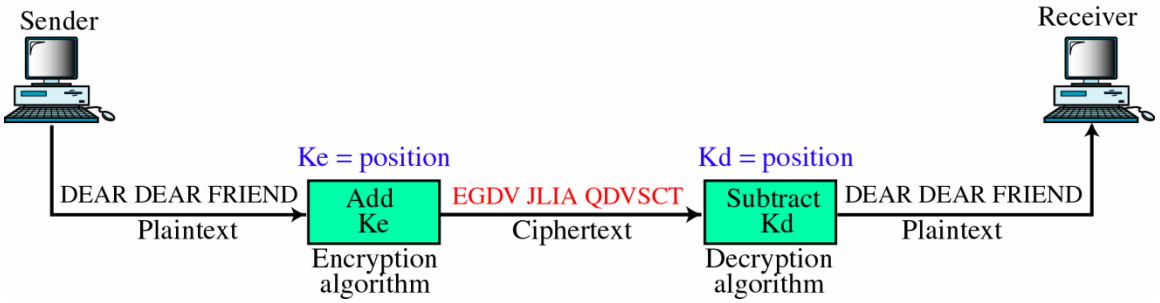
Substitutional: The simplest form of character level encryption is substitutional. Two types are: Monoalphabetic substitution and Polyalphabetic substitution.

Monoalphabetic substitution: In this the encryption algorithm simply adds a number to ASCII code of the character. The decryption algorithm simply subtracts the same number from the ASCII code.



Here we are adding 3 & subtracting 3.i.e. D + 3 =g, g-3=d but the code can broken by snoopers.

Polyalphabetic substititution: Each occurrence of a character can have a different substitute.

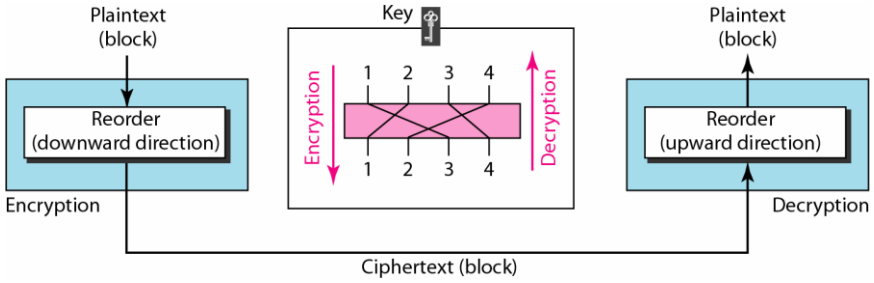


Here we are adding and subtracting the numbers as D + 1, E+ 2, = E, G

E – 1, G- 1 = D, E.

Still we are having the problem of snoopers.

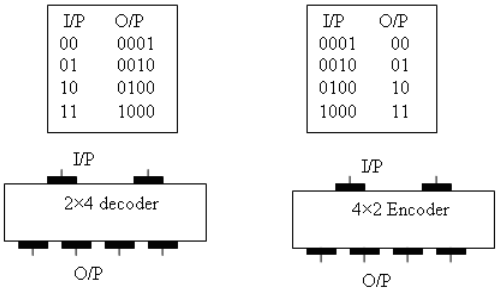
Transposition: In transposition cipher, there is no substitution of characters; instead their locations change. A transposition cipher reorders (permutes) symbols in a block of symbols.



In encryption we move the character at position 2 to position 1, the character at position 4 to position 2 and so on. In decryption we do the reverse. In the figure shown above the encryption applies it from downward while decryption applies it upward.

BIT – LEVEL ENCRYPTION: In this data as text, graphics audio or video are first divided in to a block of bits. Then it is altered by using encoding / decoding, permutation, substitution, and XOR, rotation techniques etc

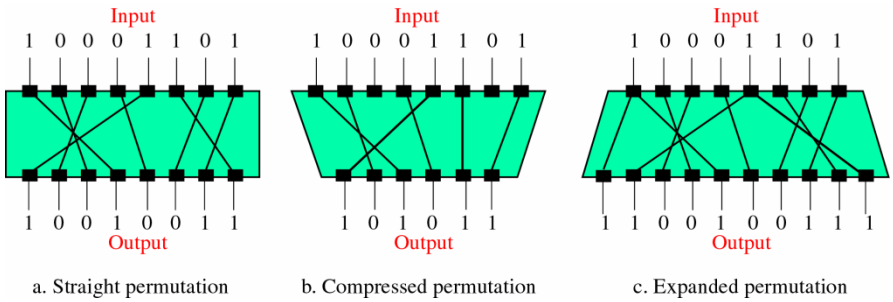
Encoding / Decoding: The decoder changes n bits in to 2^n bits o/p, and encoder changes 2^n bits into only n outputs.



So we are using encoder/ decoder for changing plaintext in to cipher text and again cipher text into plaintext.

Permutation: Permutation ia transposition at the bit level.

1. Straight permutation: Here only the positions of the bits are interchanged. So the plain text is changed in to cipher text by simply interchanging the position of bits.

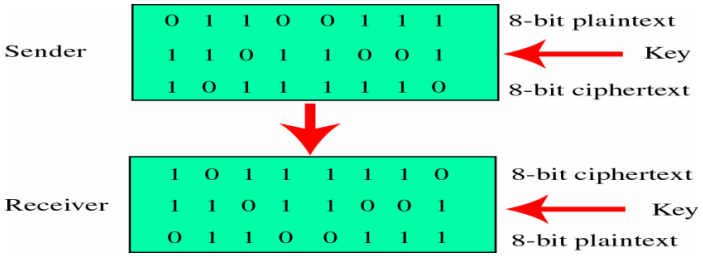


a. Straight permutation b. Compressed permutation c. Expanded permutation

Substitution: The permutation is called. P- Boxes. Substitution is the combination of P-boxes, encoders and decoder i.e. called as s- boxes.

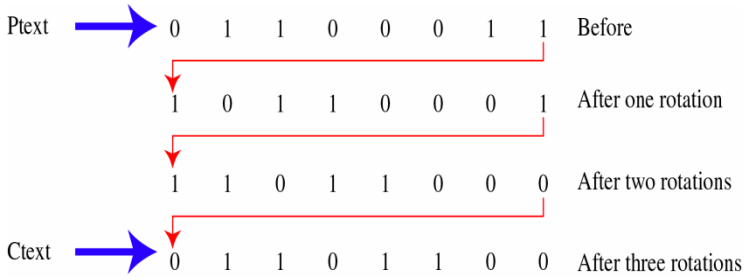
Product: Combination of P boxes and S boxes is called the product. The product converts the plain text into cipher text.

Exclusive OR: It is using Ex – OR table in order to convert the plain text to cipher text and cipher text to plain text.



Rotation: Another way of encrypt a bit pattern is to rotate bit pattern is to rotate bits to the right or left. The key is the number of bits to be rotated. The figure shows the plaintext rotated to create ciphertext

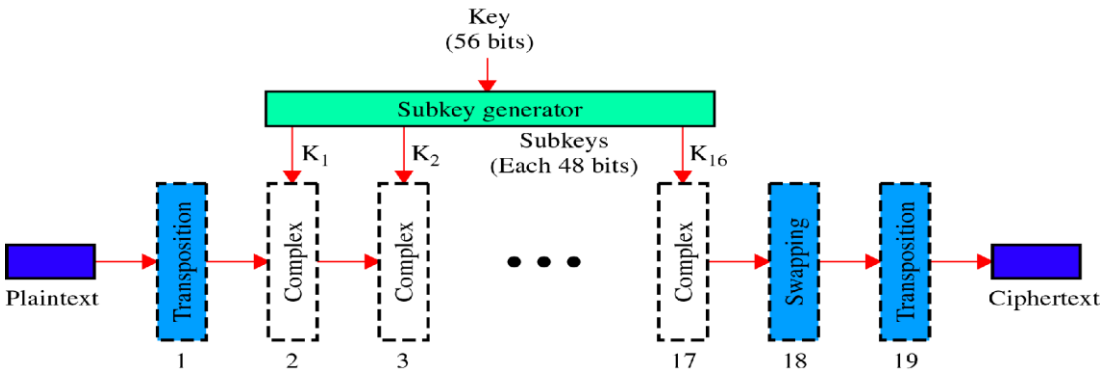
.



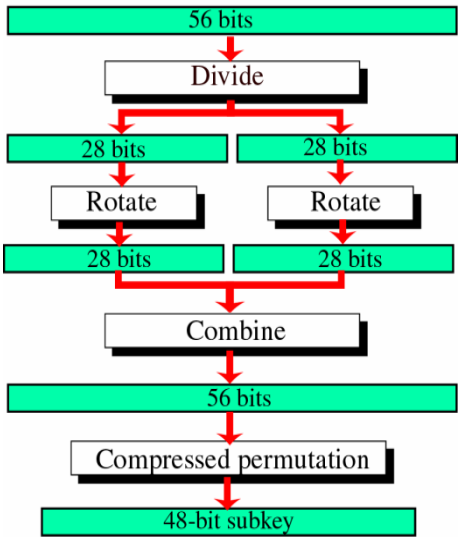
6. Explain in detail DES encryption scheme with an example and what are the drawbacks of DES algorithms? [NOV-04] OR Explain symmetric key cryptography with a suitable example:

DES algorithm:

- The data encryption standard (DES) is the best example of bit level encryption.
- This algorithm encrypts a 64 bit plain text using a 56 bit key.
- The steps followed for this is very complex and it is of 19 different steps.



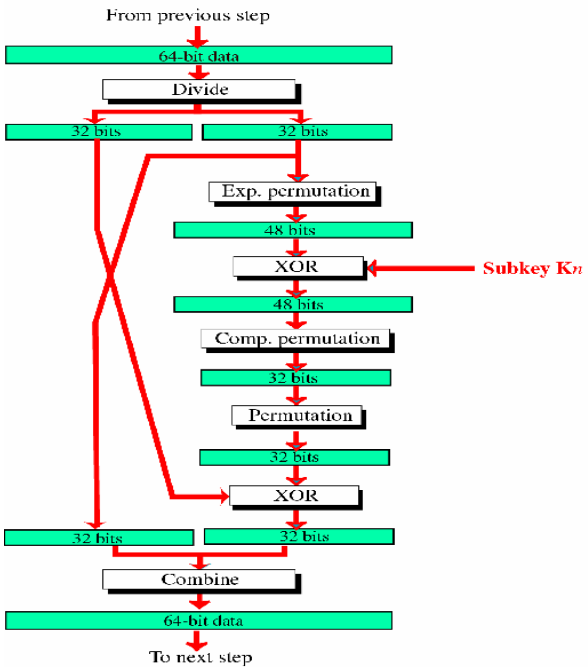
The **sub key generator** is of 48 bits which is derived from 56 bit sub key generator.



- Every step uses a separate key.
- For generating the 48 bit sub key from 56 bits, first we are dividing the 56 bits in to 28 bits.
- Then we are providing rotation and then the combined 56 bits are again compressed in to 48 bit sub key.

For example if we take one of the steps in DES algorithm

Eg: One of the 16 steps in DES



From the above eg: the 64 bit data is divided in to 32 bits and each 32 bits are expanded to 48 bits and uses 48 bit sub key and the result is compressed using compressed permutation and again they are combined to form 64 bit data and forwarded to next step.

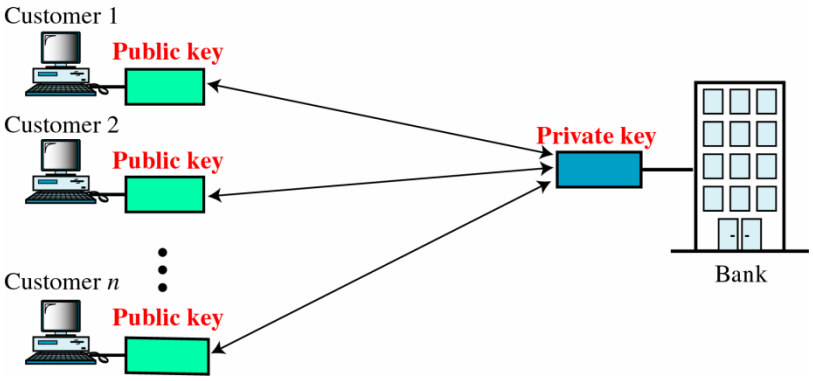
Drawbacks: This encryption / decryption process uses the same key. So if anyone identifies the key can deduce and decrypt the algorithm. This is the draw back in this system.

7. Explain the principle of RSA algorithm and how the public and secret keys are derived? [April -04] OR Explain asymmetric key cryptography with suitable example:

To overcome the disadvantages in conventional methods, we are using public key methods. In this the entire process is kept secret.

- For eg: Imagine that a bank wants to give customers remote access to their accounts. for each customer they have to use separate encryption and decryption algorithms to overcome this we are using public key methods
- In this the user can encrypt the message by using same encryption algorithm. But only an authorized receiver can decrypt it. It is not the inverse of the encryption algorithm.
- One of the public key method is RSA algorithm

RSA algorithm: This technique is called as Rivest, Shamir, and Adleman (RSA) algorithm. Here we are using two keys, one is public key (K_P), the other party uses secret key (K_S).



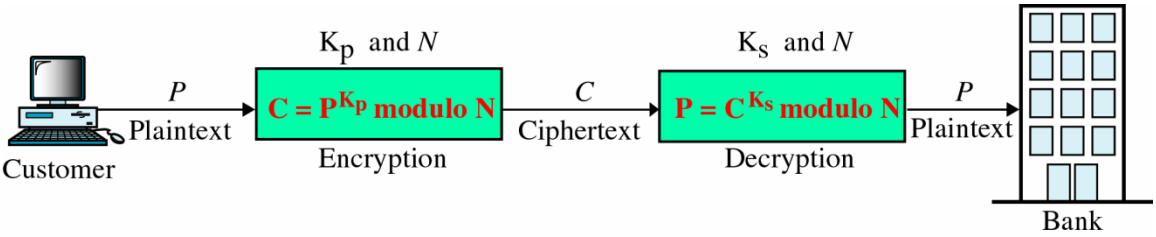
The encryption algorithm follows these steps

- Encode the data to be encrypted as a number to create the plain text P.
- Calculate the cipher text C as $C = P^{K_P}$ module N (modulo means divide P^{K_P} by N and keep only the remainder).
- Send C as the cipher text.

The decryption algorithm follows the steps:

- Receive C, the cipher text.

- Calculate plaintext $P=C^{K_S}$ modulo N.
- Decode P to the original data.



So by using RSA any one can encrypt, but the authorized person only able to decrypt the message

- For eg: We will take one eg: to discuss the public and secret keys.
  Choose K_P = 5, K_S = 77, and N=119 by selecting p =7 and q=17

Steps to calculate the value of K_P, K_S and N

- First choose the prime numbers (a prime number is divisible only by1 & itself), p & q .for e.g.(7 & 17)
- Calculate p×q = N (so from our eg; N = 7×17 =119)
- Select K_P such that it is not a factor of (p-1) ×(q-1).
  (From our e.g. (7-1) (17-1) =96. The factors of 96 are 2, 2, 2, 2, & 3. So we take 5 Which is not a factor of 96).
- Select K_S such that (K_P× K_S) modulo (p-1) ×(q-1) =1. (So choose 77 for eg. So it will be 5×77 modulo 96. So 385/96 =4; remainder 1).
- Finally K_P =5, K_S =77, N=119.
- Now if you are transmitting a letter F then (A to Z) is (1 to 26). So F=6 and
  6 K_P modulo 119 is C. Therefore C = 6^5 modulo119 = 41 will be transmitted & P = 41^5 modulo 119 will be the original plain text again.
- The security will be obtained by using prime numbers because the snoopers cannot calculate the prime numbers.

8. Distinguish between conventional and public key encryption

	Conventional Encryption	Public key encryption
1.	In this method the encryption key (K_e) and decryption key (K_d) are same.	Here encryption key is same decryption key is secret and Different.
2.	It uses character level encryption, bit level encryption.	Only public key encryption
3.	Used in DES algorithm.	Used in RSA algorithm
4.	The key is kept secret for both encryption and decryption.	The encryption key is publicly announced. But decryption key is kept secret.
5.	The snooper can easily break the letters.	The snoopers cannot be able to identify the prime numbers.
6.	It is also called as private key symmetric encryption	It is also called as asymmetric cryptography.

9. Discuss in detail about Client/ Server Programming.

- The place to start when implementing **a network application is the interface exported by the network**.
- Since most network protocols are implemented in software (especially those high in the protocol stack), and **nearly all computer systems implement their network protocols as part of the operating system**, when we refer to the interface "exported by the network,"
- We are generally referring to the interface that the **OS provides to its networking subsystem. This interface is often called the network *application programming interface* (API).**
- Each protocol **provides a certain set of *services*, and the API provides a *syntax* by which those services** can be invoked in this particular OS.
- The implementation is then responsible for **mapping the tangible set of operations and objects defined by the API onto the abstract set of services** defined by the protocol.
- The interface defines operations for **creating a socket, attaching the socket to the network, sending/receiving messages through the socket, and closing the socket.**
- The first step is to ***create a socket***, which is done with the following operation:

int socket(int domain, int type, int protocol)

- The ***domain argument*** specifies the protocol *family* that is going to be used:
  PF_INET denotes the Internet family,
  PF_UNIX denotes the Unix pipe facility, and
  PF_PACKET denotes direct access to the network interface (i.e., it bypasses the TCP/IP protocol stack).
- The ***type argument*** indicates the semantics of the communication.
  SOCK_STREAM is used to denote a byte stream.
  SOCK_DGRAM is an alternative that denotes a message-oriented service, such as that provided by UDP.
- The ***protocol argument*** identifies the specific protocol that is going to be used. In our case, this argument is **UNSPEC** because the combination of PF_INET and SOCK_STREAM implies TCP.

➢ The next step depends on whether you are a client or a server. On a server machine, the application process performs a *passive* open—the server says that it is prepared to accept connections, but it does not actually establish a connection.

➢ The server does this by invoking the following three operations:

int bind(int socket, struct sockaddr *address, int addr len)
int listen(int socket, int backlog)
int accept(int socket, struct sockaddr *address, int *addr len)

- The *bind* operation, as its name suggests, **binds the newly created socket** to the specified address.
- The *listen* operation then **defines how many connections** can be pending on the specified socket.
- Finally, the *accept* operation **carries out the passive open**. It is a blocking operation that does not return until a remote participant has established a connection

➢ On the client machine, the application process performs an *active* open; that is, it says who it wants to communicate with by invoking the following single operation:

int connect(int socket, struct sockaddr *address, int addr len)

➢ This operation does not return until TCP has successfully established a connection, at which time the application is free to begin sending data. In this case, address contains the remote participant's address.

➢ Once a connection is established, the application processes invoke the following two operations to send and receive data:

int send(int socket, char *message, int msg len, int flags)
int recv(int socket, char *buffer, int buf len, int flags)

- The first operation **sends the given message over the specified socket**,
- while the second operation **receives a message from the specified socket** into the given buffer.

Example Application

Client:

```
#include <stdio.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>
#define SERVER_PORT 5432
#define MAX_LINE 256
int
main(int argc, char * argv[])
{
FILE *fp;
struct hostent *hp;
struct sockaddr_in sin;
char *host;
char buf[MAX_LINE];
int s;
int len;
if (argc==2) {
host = argv[1];
}
else {
fprintf(stderr, "usage: simplex-
talk host\n");
exit(1);
}
/* translate host name into
peer's IP address */
hp = gethostbyname(host);
if (!hp) {
fprintf(stderr, "simplex-talk:
unknown host: %s\n", host);
exit(1);
}
/* build address data structure
*/
bzero((char *)&sin,
sizeof(sin));
sin.sin_family = AF_INET;
bcopy(hp->h_addr, (char
*)&sin.sin_addr, hp->h_length);
sin.sin_port =
htons(SERVER_PORT);
/* active open */
if ((s = socket(PF_INET,
SOCK_STREAM, 0)) < 0) {
perror("simplex-talk: socket");
exit(1);
}
if (connect(s, (struct sockaddr
*)&sin, sizeof(sin)) < 0) {
perror("simplex-talk: connect");
close(s);
exit(1);
}
/* main loop: get and send lines
of text */
while (fgets(buf, sizeof(buf),
stdin)) {
buf[MAX_LINE-1] = '\0';
len = strlen(buf) + 1;
send(s, buf, len, 0);
}
}
```

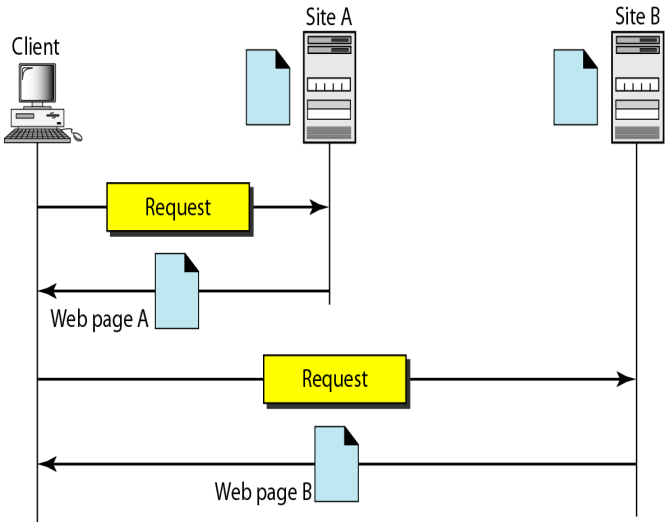
Server:

```
#include <stdio.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>
#define SERVER_PORT 5432
#define MAX_PENDING 5
#define MAX_LINE 256
int
main()
{
struct sockaddr_in sin;
char buf[MAX_LINE];
int len;
int s, new_s;
/* build address data structure
*/
bzero((char *)&sin,
sizeof(sin));
sin.sin_family = AF_INET;
sin.sin_addr.s_addr =
INADDR_ANY;
sin.sin_port =
htons(SERVER_PORT);
/* setup passive open */
if ((s = socket(PF_INET,
SOCK_STREAM, 0)) < 0) {
perror("simplex-talk: socket");
exit(1);
}
if ((bind(s, (struct sockaddr
*)&sin, sizeof(sin))) < 0) {
perror("simplex-talk: bind");
exit(1);
}
listen(s, MAX_PENDING);
/* wait for connection, then
receive and print text */
while(1) {
if ((new_s = accept(s, (struct
sockaddr *)&sin, &len)) < 0){
perror("simplex-talk: accept");
exit(1);
}
while (len = recv(new_s, buf,
sizeof(buf), 0))
fputs(buf, stdout);
close(new_s);
}
}
```

10. Explain in detail about WWW.

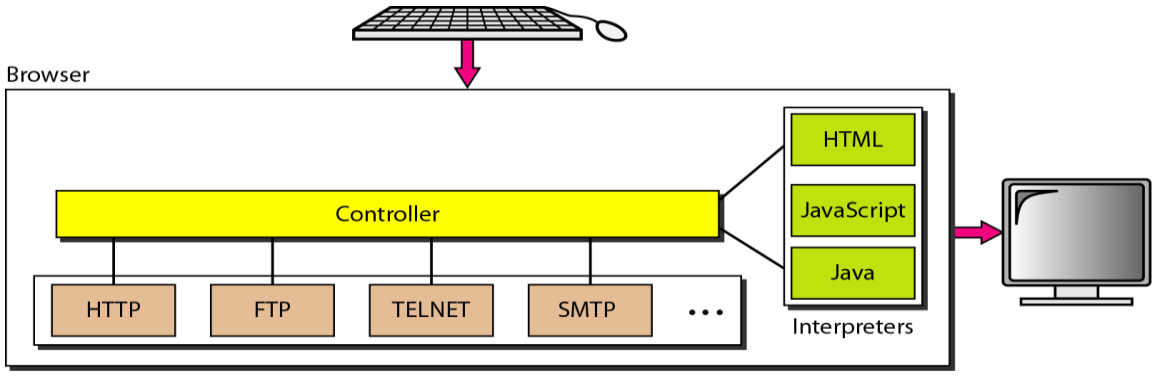
- The idea of the Web was first proposed by Tim Berners-Lee in 1989 at *CERN*†, the European Organization for Nuclear Research, to allow several researchers at different locations throughout Europe to access each others' researches. The commercial Web started in the early 1990s.
- The Web today is a repository of information in which the documents, called ***web pages,*** are distributed all over the world and related documents are linked together.
- The popularity and growth of the Web can be related to two terms in the above statement: ***distributed*** **and** ***linked*****.**
- **Distribution allows the growth of the Web.** Each web server in the world can add a new web page to the repository and announce it to all Internet users without overloading a few servers.
- **Linking allows one web page to refer to another web page stored in another server somewhere else in the world.** The linking of web pages was achieved using a concept called ***hypertext,*** which was introduced many years before the advent of the Internet.

Architecture



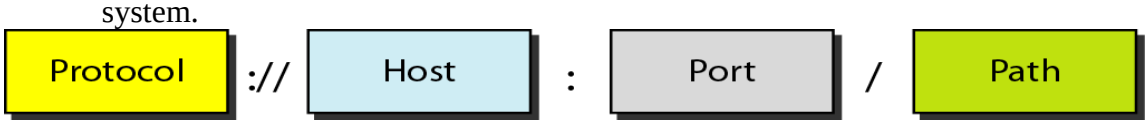
Web Client (Browser)

- A variety of vendors offer commercial **browsers** that interpret and display a web page, and all of them use nearly the same architecture. Each browser usually consists of three parts: **a controller, client protocols, and interpreters**.



URL

- A web page, as a file, needs to have a unique identifier to distinguish it from other web pages. To define a web page, we need three identifiers: *host, port,* and *path*. However, before defining the web page, we need to tell the browser what client-server application we want to use, which is called the *protocol*.
  - ***Protocol*:** The first identifier is the abbreviation for the client-server program that we need in order to access the web page.
  - ***Host*:** The host identifier can be the IP address of the server or the unique name given to the server.
  - ***Port*:** The port, a 16-bit integer, is normally predefined for the client-server application.
  - ***Path*:** The path identifies the location and the name of the file in the underlying operating system. The format of this identifier normally depends on the operating system.

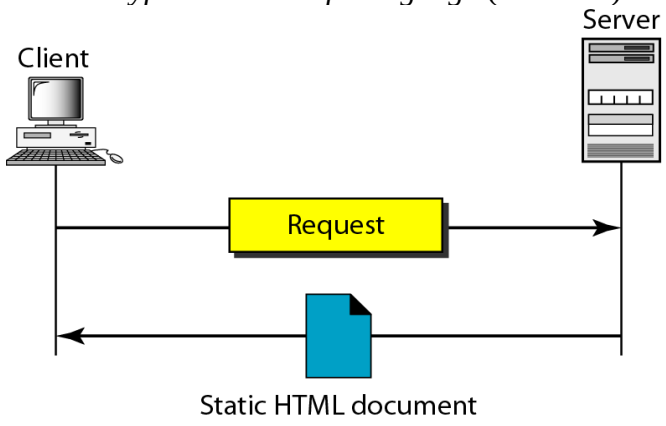


WEB DOCUMENTS

- The documents in the WWW can be grouped into three broad categories: static, dynamic, and active. The category is based on the time at which the contents of the document are determined.

Static Documents

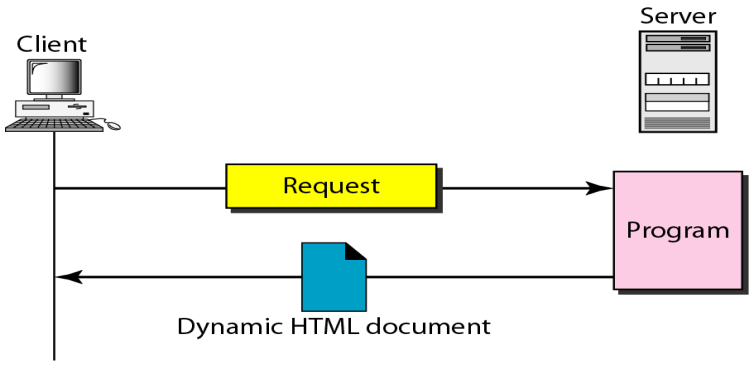
- **Static documents** are fixed-content documents that are created and stored in a server. The client can get a copy of the document only. In other words, the contents of the file are determined when the file is created, not when it is used. The user can then use a browser to see the document.
- Static documents are prepared using one of several languages: *HyperText Markup Language* (HTML), *Extensible Markup Language* (XML), *Extensible Style Language* (XSL), and *Extensible Hypertext Markup Language* (XHTML).



Dynamic Documents

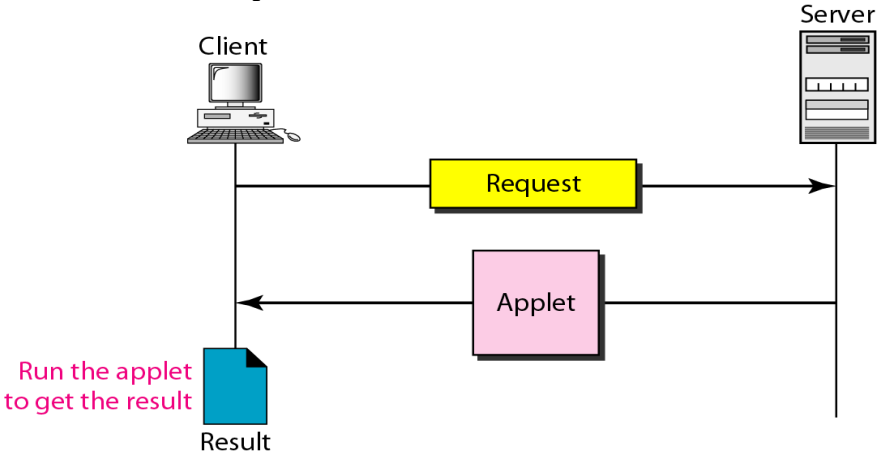
- A **dynamic document** is created by a web server whenever a browser requests the document. When a request arrives, the web server runs an application program or a script that creates the dynamic document.

- A very simple example of a dynamic document is the retrieval of the time and date from a server. Time and date are kinds of information that are dynamic in that they change from moment to moment.
- Although the *Common Gateway Interface* (*CGI*) was used to retrieve a dynamic document in the past, today's options include one of the scripting languages such as *Java Server Pages* (*JSP*), which uses the Java language for scripting, or *Active Server Pages* (*ASP*), a Microsoft product that uses Visual Basic language for scripting, or *ColdFusion*, which embeds queries in a Structured Query Language (SQL) database in the HTML document.



Active Documents

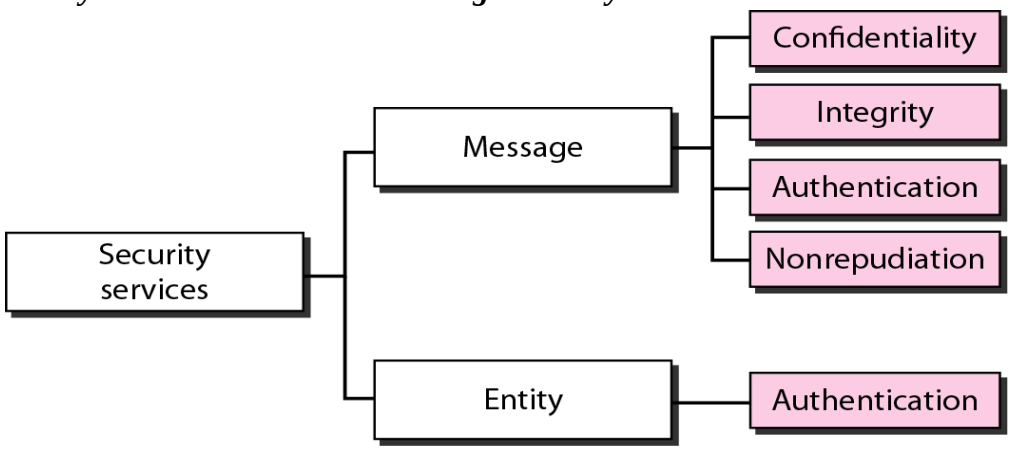
- For many applications, we need a program or a script to be run at the client site. These are called ***active documents*.**
- One way to create an active document is to use *Java applets*, a program written in Java on the server. It is compiled and ready to be run.
- The document is in byte code (binary) format. Another way is to use *JavaScripts* but download and run the script at the client site.



10. Discuss in detail about Network Security.

Network security can provide five services. Four of these services are related to the message exchanged using the network. The fifth service provides entity authentication or identification.

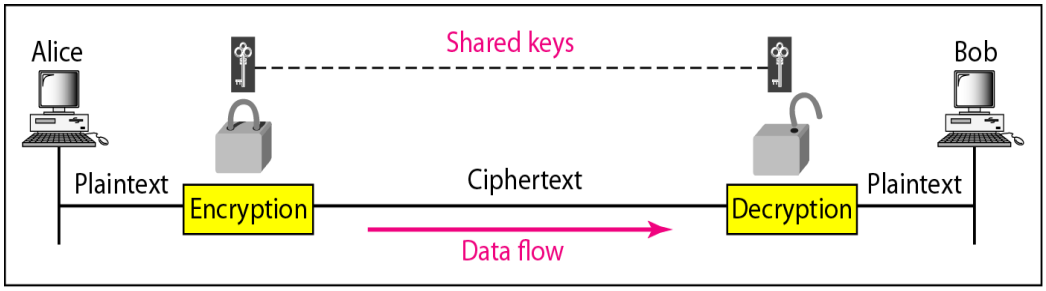
Security services related to the message or entity



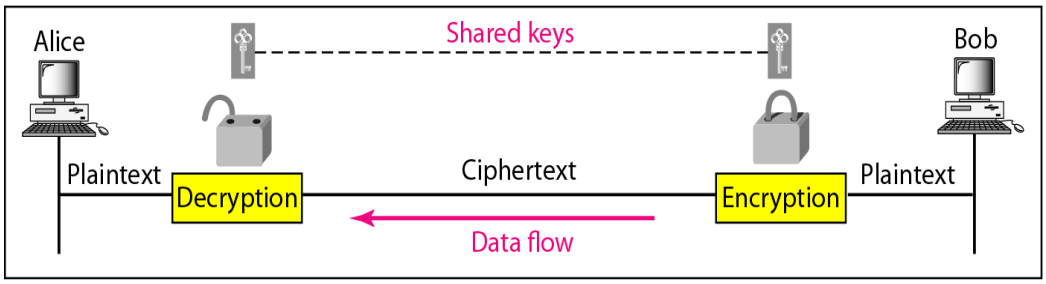
MESSAGE CONFIDENTIALITY

The concept of how to achieve message confidentiality or privacy has not changed for thousands of years. The message must be encrypted at the sender site and decrypted at the receiver site. This can be done using either symmetric-key cryptography or asymmetric-key cryptography.

Message confidentiality using symmetric keys in two directions



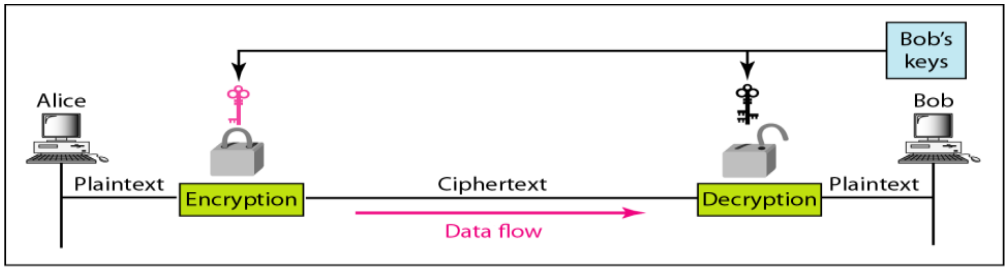
a. A shared secret key can be used in Alice-Bob communication



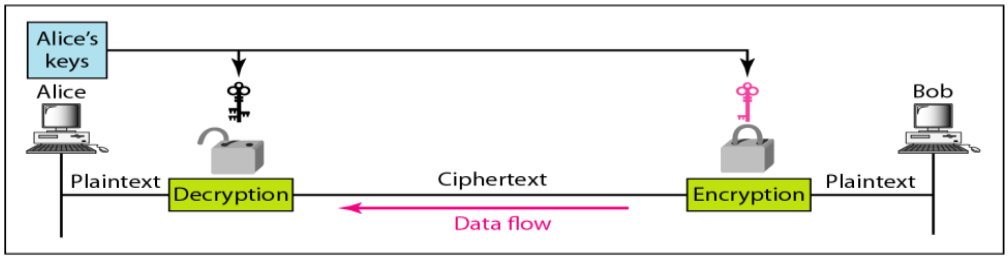
b. A different shared secret key is recommended in Bob-Alice communication

To provide confidentiality with symmetric-key cryptography, a sender and a receiver need to share a secret key. In the past when data exchange was between two specific persons (for example, two friends or a ruler and her army chief), it was possible to personally exchange the secret keys.

Message confidentiality using asymmetric keys



a. Bob's keys are used in Alice-Bob communication



b. Alice's keys are used in Bob-Alice communication

The problem we mentioned about key exchange in symmetric-key cryptography for privacy culminated in the creation of asymmetric-key cryptography. Here, there is no key sharing; there is a public announcement.

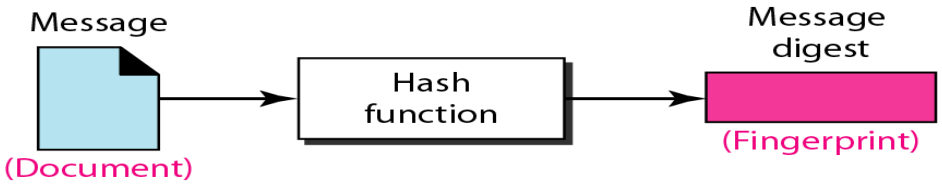
The public key is used only for encryption; the private key is used only for decryption. The public key locks the message; the private key unlocks it.

MESSAGE INTEGRITY

Encryption and decryption provide secrecy, or confidentiality, but not integrity. However, on occasion we may not even need secrecy, but instead must have integrity. To preserve the integrity of a document, both the document and the fingerprint are needed.

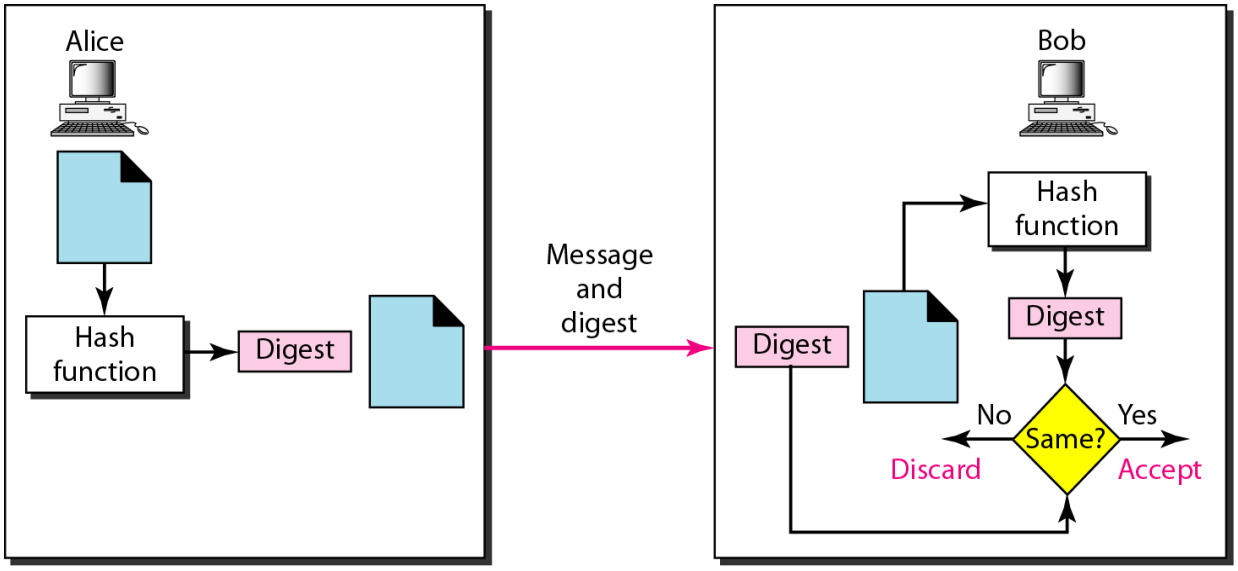
Message and message digest

The electronic equivalent of the document and fingerprint pair is the message and message digest pail: To preserve the integrity of a message, the message is passed through an algorithm called a hash function. The hash function creates a compressed image of the message that can be used as a fingerprint.



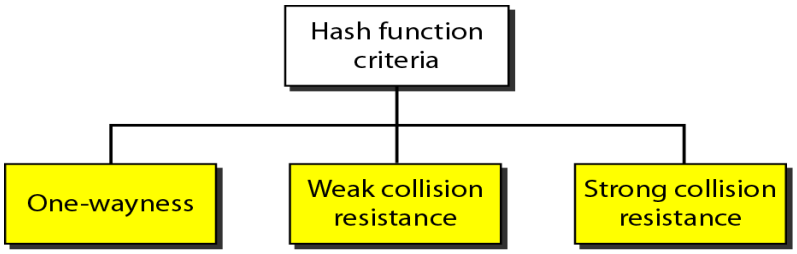
The two pairs document/fingerprint and message/message digest are similar, with some differences. The document and fingerprint are physically linked together; also, neither needs to be kept secret. The message and message digest can be unlinked (or sent) separately and, most importantly, the messages digest needs to be kept secret.

Checking integrity



The message digest is created at the sender site and is sent with the message to the receiver. To check the integrity of a message, or document, the receiver creates the hash function again and compares the new messages digest with the one received. If both are the same, the receiver is sure that the original message has not been changed.

Criteria of a hash function



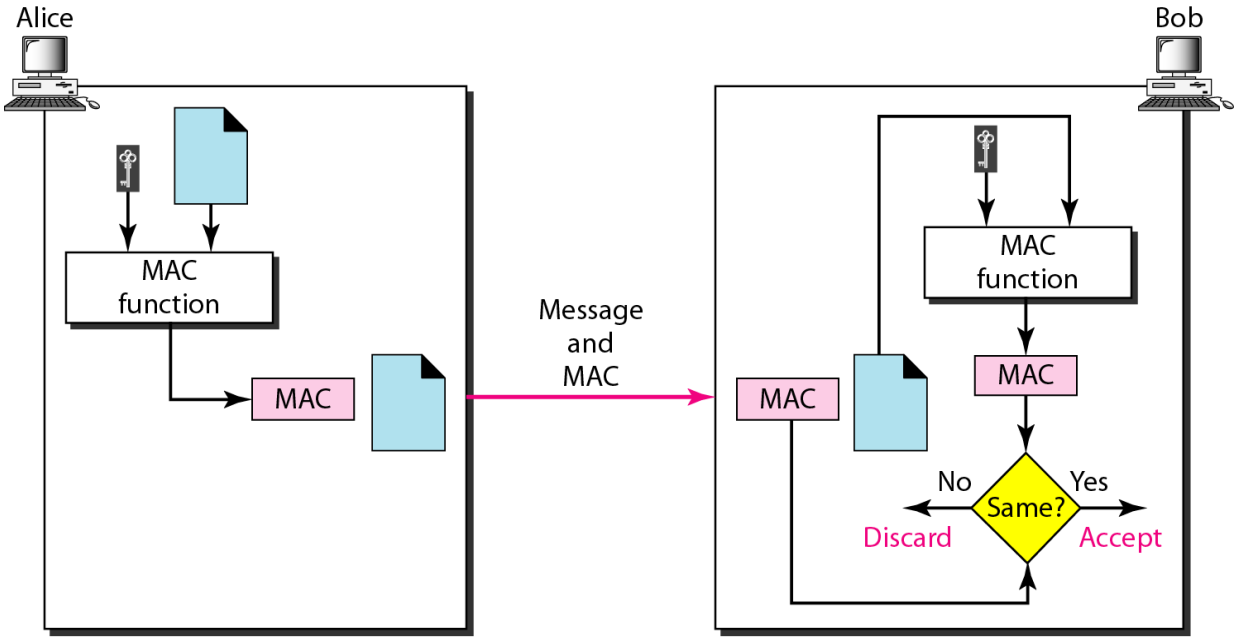
- A hash function must have **one-wayness;** a message digest is created by a one-way hashing function. We must not be able to recreate the message from the digest.
- The second criterion, weak collision resistance, ensures that a message cannot easily be forged. In other words, given a specific message and its digest, it is impossible (or at least very difficult) to create another message with the same digest.
- The third criterion, strong collision resistance, ensures that we cannot find two messages that hash to the same digest. This type of collision is called strong because the probability of collision is higher than in the previous case. An adversary can create two messages that hash to the same digest.

MESSAGE AUTHENTICATION

A hash function guarantees the integrity of a message. It guarantees that the message has not been changed. A hash function, however, does not authenticate the sender of the message.

To provide message authentication, we need to change a modification detection code to a message authentication code (MAC). An MDC uses a keyless hash function; a MAC uses a keyed hash function. A keyed hash function includes the symmetric key between the sender and receiver when creating the digest.

MAC, created by Alice and checked by Bob

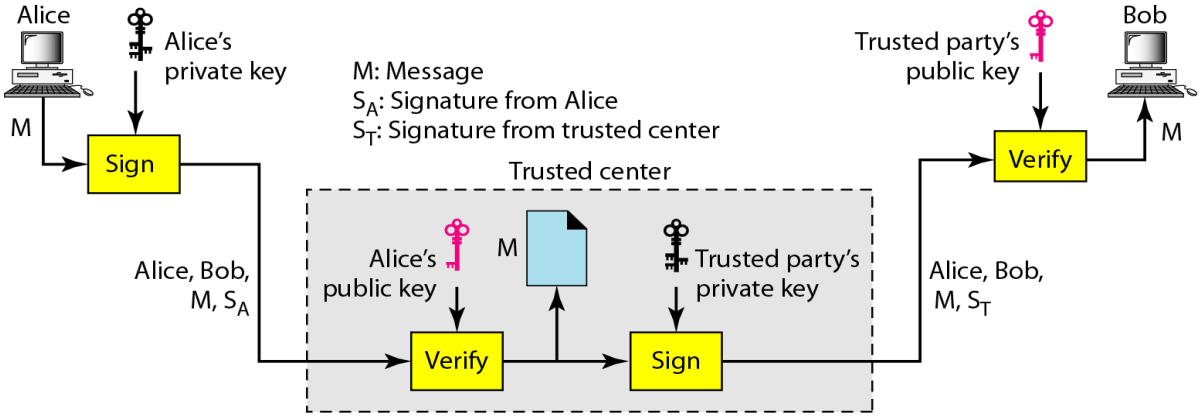


MESSAGE NONREPUDIATION

If Alice sends a message to a bank (Bob) and asks to transfer $10,000 from her account to Ted's account, can Alice later deny that she sent this message? With the scheme we have presented so far, Bob might have a problem. Bob must keep the signature on file and later use Alice's public key to create the original message to prove the message in the file and the newly created message are the same.

This is not feasible because Alice may have changed her private/public key during this time; she may also claim that the file containing the signature is not authentic. One solution is a trusted third party. People can create a trusted party among themselves.

Using a trusted center for nonrepudiation



ENTITY AUTHENTICATION

Entity authentication is a technique designed to let one party prove the identity of another party. An entity can be a person, a process, a client, or a server. The entity whose identity needs to be proved is called the claimant; the party that tries to prove the identity of the claimant is called the verifier.

In entity authentication, the claimant must identify herself to the verifier. This can be done with one of three kinds of witnesses: *something known*, *something possessed*, or *something inherent.*

- *Something known.* This is a secret known only by the claimant that can be checked by the verifier. Examples are a password, a PIN number, a secret key, and a private key.
- *Something possessed.* This is something that can prove the claimant's identity. Examples are a passport, a driver's license, an identification card, a credit card, and a smart card.
- *Something inherent.* This is an inherent characteristic of the claimant. Examples are conventional signature, fingerprints, voice, facial characteristics, retinal pattern, and handwriting.

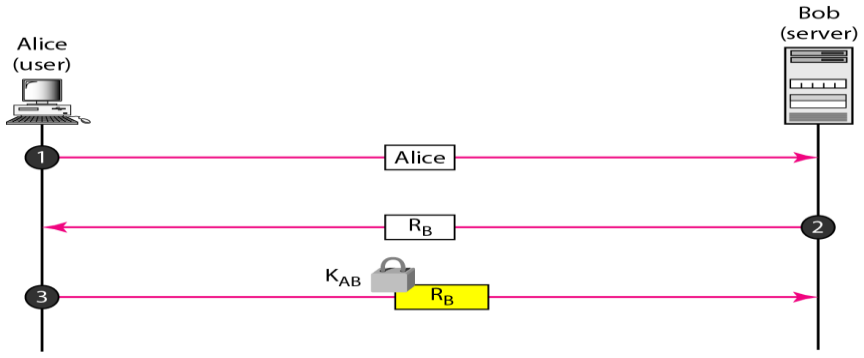
Passwords

A password is used when a user needs to access a system to use the system's resources (log-in). Each user has a user identification that is public and a password that is private. We can divide this authentication scheme into two separate groups: the fixed password and the one-time password.

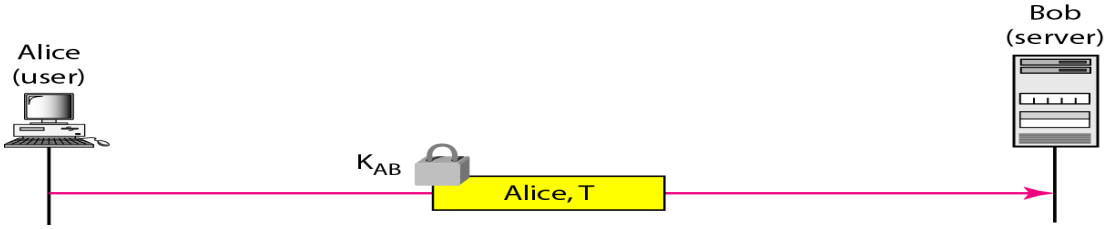
Challenge-Response

In challenge-response authentication, the claimant proves that she knows a secret without revealing it.The challenge is a time-varying value sent by the verifier; the response is the result of a function applied on the challenge.

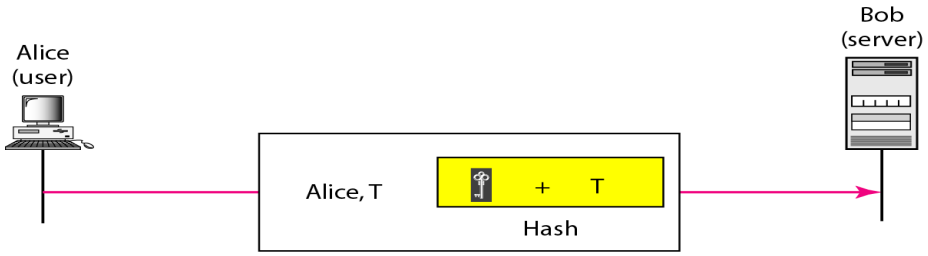
Challenge/response authentication using a nonce



Challenge-response authentication using a timestamp

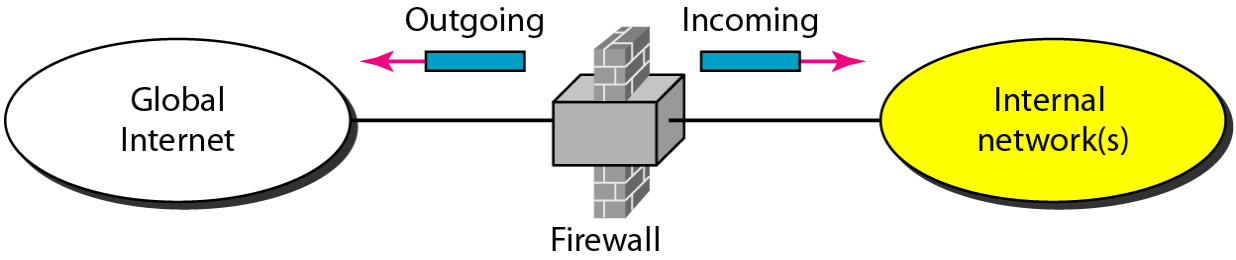


Challenge-response authentication using a keyed-hash function



11. Elaborate about Firewall.

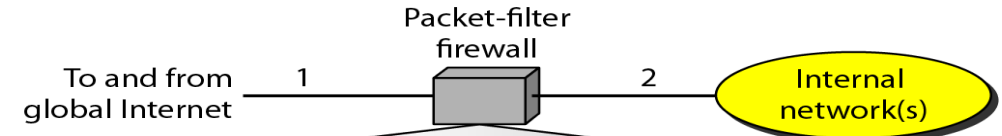
All previous security measures cannot prevent Eve from sending a harmful message to a system. To control access to a system, we need firewalls. A **firewall** is a device (usually a router or a computer) installed between the internal network of an organization and the rest of the Internet. It is designed to forward some packets and filter (not forward) others.



A firewall is usually classified as a packet-filter firewall or a proxy-based firewall.

Packet-filter firewall

A firewall can be used as a packet filter. It can forward or block packets based on the information in the network layer and transport layer headers: source and destination IP addresses, source and destination port addresses, and type of protocol (TCP or UDP). A packet-filter firewall is a router that uses a filtering table to decide which packets must be discarded (not forwarded).



Interface	Source IP	Source port	Destination IP	Destination port
1	131.34.0.0	*	*	*
1	*	*	*	23
1	*	*	194.78.20.8	*
2	*	80	*	*

Proxy firewall

The packet-filter firewall is based on the information available in the network layer and transport layer headers (IP and TCP/UDP). However, sometimes we need to filter a message based on the information available in the message itself (at the application layer).

A packet-filter firewall is not feasible because it cannot distinguish between different packets arriving at TCP port 80 (HTTP). Testing must be done at the application level (using URLs).

One solution is to install a proxy computer (sometimes called an application gateway), which stands between the customer (user client) computer and the corporation computer.