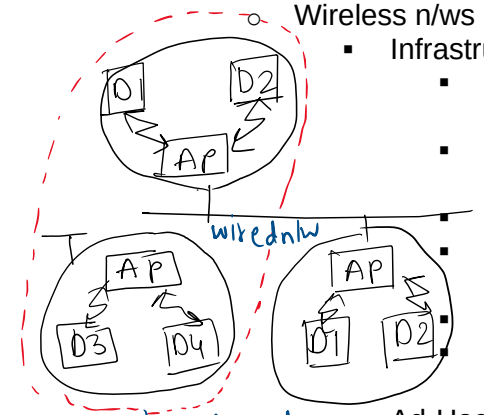
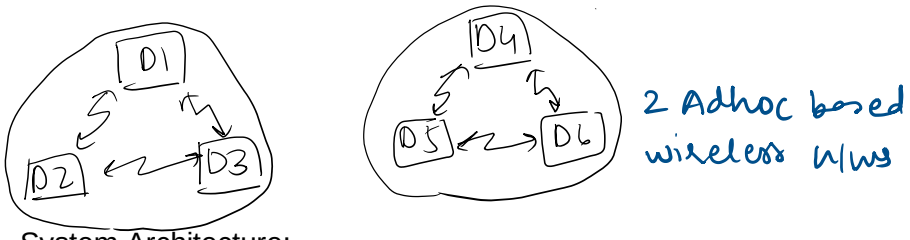
IEEE 802.11

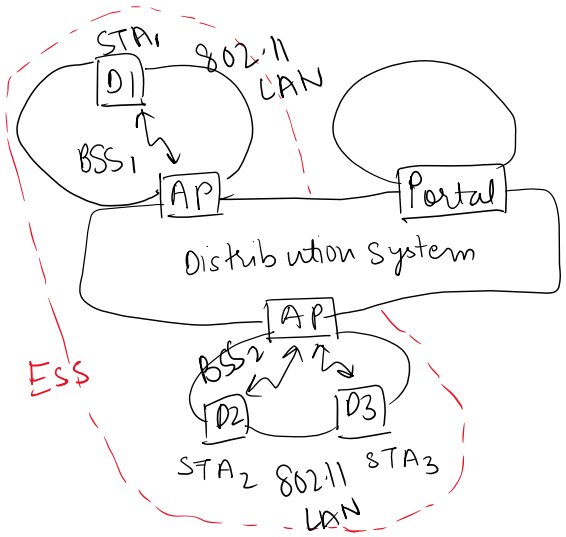
- Primary goal: MAC address should be able to operate with multiple physical layers.
- Each physical layer exhibiting a different medium sense and transmission characteristics.
- Additional features:
  - Support of power management
  - Handling hidden nodes
  - Worldwide accessibility
- Frequency: 2.4GHz of IMS band
- Data Rate: 1 Mbit/sec mandatory and 2 Mbit/sec optional.
- System Architecture:
  - Wireless n/ws exhibits 2 different basic system architecture:
    - Infrastructure:
      - Communication takes place only between the wireless nodes and the access points.
      - Access points control medium access, and also acts as a bridge to other wireless or wired networks.
      - Most hardware functionality lies within access points.
      - They cannot be used for disaster relief in case where no infrastructure is left.
      - Cellular phones are infrastructure-based n/w for wide area.
      - Note: Infrastructure does not necessary imply a wired fixed network.



    - Ad-Hoc Network:
      - Do not need any infrastructure to work
      - Each node can directly communicate with other node, so no access points controlling medium access is necessary.



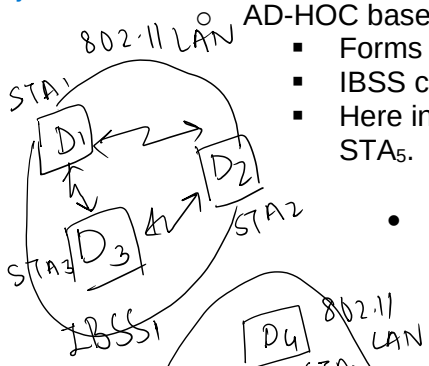
- System Architecture:
  - Infrastructure based architecture:
    - Several nodes, called stations (STA), connected to access points (AP).
    - Stations and AP which are within the same radio coverage from a Basic Service Set (BSS).
    - So, BSS_1 and BSS_2 are connected, via a distributed system.
    - These BSSs are connected via a Access Poins to form Extended Service Set (ESS).
    - Sation selects an AP and associates with it.
    - APs supports roaming between different AP.
    - The distributed system handles data transfer between different APs.
    - AP provides synchronization within a BSS
    - Also supports power management,
    - Control medium access to support time-bounded services.



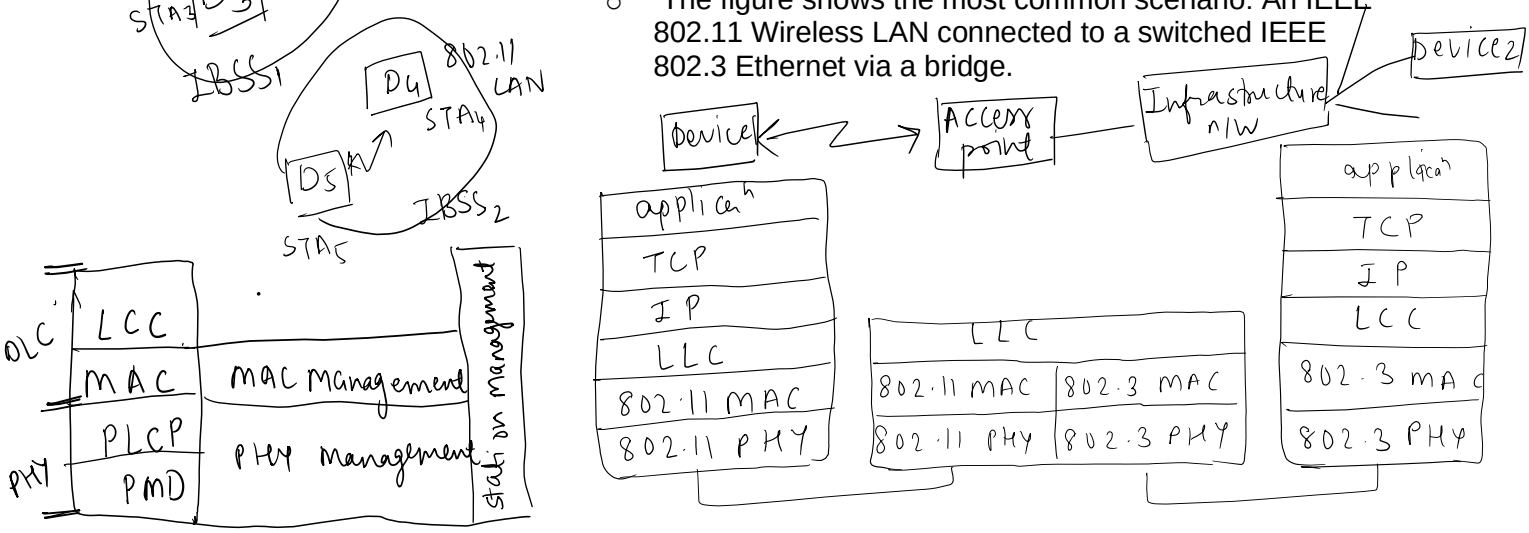
Functions of AP

@jiisanda

- AD-HOC based wireless LAN Architecture:
  - Forms one or more independent BSSs (IBSS) as shown.
  - IBSS comprises of group of stations using the same radio frequency.
  - Here in figure: STA_1 and STA_3 can communicate directly, but nit with STA_5.



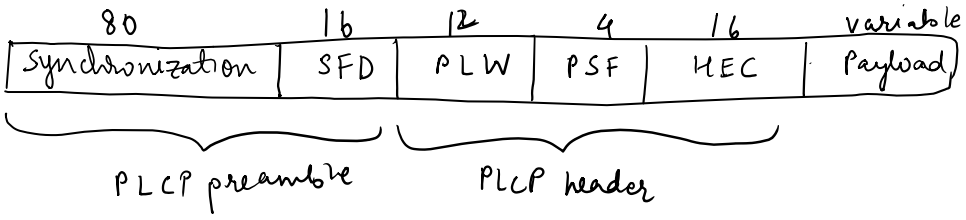
- **Protocol Architecture:**
  - The figure shows the most common scenario: An IEEE 802.11 Wireless LAN connected to a switched IEEE 802.3 Ethernet via a bridge.



  - The IEEE 802.11 standards only covers the physical layer PHY and medium access layer MAC.
  - Physical layer is sub divided into 2
    - PLCP (Physical Layer Convergence Protocol)
      - This sublayer provides carrier sense signal c/d Clear Channel Assessment (CCA);
      - Also provides a common PHY service access point (SAP)
    - PMD (Physical Medium Dependent)
      - This sublayer handles modulation and encoding/decoding of signals.
  - Basic tasks of MAC layer:
    - Medium Access
    - Fragmentation of User data
    - Encryption
  - MAC Management:
    - It supports association and re-association of a station to an access point;
    - It supports roaming b/w different access points;
    - It also controls authentication mechanism, encryption, synchronization of station with regard to an access point.
    - Power management to save battery
  - PHY management:
    - Main tasks include channel tunning
  - Station Management:
    - Interacts with both management layers
    - Responsible for additional higher layer functions (e.g., control of bridging, etc)

- **Physical Layer:**
  - IEEE 802.11 supports 3 different types of physical layer: One layer based on infrared and Two layers based on radio transmission.

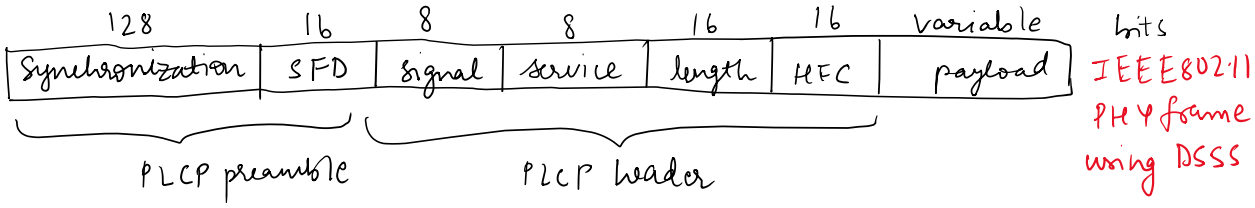
- All variants include property of the clear channel assessment (CCA), which is needed for MAC controlling medium access and indicates if the medium is currently ideal.
- The PHY layer offers service access point (SAP) with 1 or 2 Mbit/sec of transfer rate to MAC layer.
- Three versions of a PHY layer defined are:
  - *Frequency Hopping Spread Spectrum (FHSS)*:
    - Physical layer based on Radio Transmission**.**
    - This allows coexistence of multiple networks in same area by separating different n/ws using different hopping sequence.
    - These introduced low-cost devices for lower rate.
    - The following is the frame of physical layer used with FHSS:



IEEE 802.11 PHY frame using FHSS

      - The frame consists of two parts, PLCP part (preamble and header) and the payload part.
      - PLCP is to be transmitted at 1 Mbit/s, payload i.e., MAC data, can use 1 or 2 Mbit/s.
      - Also, MAC data is scrambled using the polynomial $s(z) = z^7+z^4+1$ for whitening the spectrum.
      - The frame fields, have the following functions:
        - *Synchronization*:
          - 80 bits, with 010101010… bit pattern
          - This pattern is used for synchronization of potential receivers and signal detection by CCA.
        - *Start Frame Delimiter (SFD):*
          - 16 bits, indicates start of frame
          - Provides frame synchronization
          - Pattern is 0000110010111101.
        - *PLCP_PDU length word (PLW):*
          - First fields of PLCP header,
          - Indicates the length of payload in bytes, including 32 bit CRC at the end of payload.
        - *PLCP Signalling Field (PSF):*
          - 4 bits field
          - Indicates the data rate of the payload
            - 0000 -> lowest data rate of 1 M bit/sec
            - 0010 -> 2Mbit/sec
            - 1111 -> Maximum 8.5 Mbit/sec
          - Does not accommodate today's high data rates.
        - *HEC (Header Error Check):*
          - PLCP header is protected by a 16-bit checksum
  - *Direct Sequence Spread Spectrum (DSSS):*
    - This method is separated by code not by frequency.
    - IEEE 802.11 DSSS, spreading is achieved using 11-chip Beaker sequence (+1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1).
    - Key characteristics: Robustness against interfaces and its insensitivity of multipath propagation.
    - Implementation is complex as compared to FHSS.

- Uses 2.4 GHz ISM band, and offers 1 and 2 Mbit/s data rates.
- The following is the frame of physical layer using DSSS:

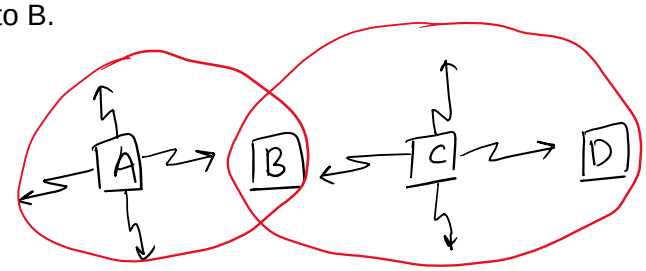


- The fields of the frame have the following functions:
  - Synchronization:
    - First 128 bits
    - Used for:
      - Synchronization
      - Gain setting, energy detection
      - Frequency offset compensation
      - Only consists of scrambled 1 bit
  - Start Frame Delimiter (SFD):
    - 16-bit field
    - Used for synchronization at the beginning of frame
  - Signal:
    - Indicates the data rate of the payload
    - 8 bits
  - Service:
    - Field is reserved for future use
    - 8 bits
  - Length:
    - 16 bits
    - Used for length indication of the payload
  - Header Error Checksum (HSC):
    - Signal, Service, and length fields are protected by this checksum.

Medium Access Control Layer:

1) Functions of MAC Layer
   - Control medium access
   - support roaming
   - authentication
   - power conservation
2) The basic services provided are:
   - Mandatory *asynchronous data service* [offered by ad-hoc and infrastructure both]
   - Optional *time-bounded service* [offered by infrastructure only]
3) Most wired LANs, uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) as a MAC protocol.
4) Carrier Sense means the station will listen before it transmits. If there is already someone transmitting, then the station waits and tries again later. If no one is transmitting then station goes ahead and sends what it has. But when more than one station tries to transmit, the transmission will collide and the information will be lost. This where Collision Detection comes into play. This technique works well for wired LANs but wireless medium presents some unique challenges as:
   - The wireless LANs are vulnerable to unwanted interception leading to security problem.
   - Hidden Station and Exposed Station Problems
     - **Hidden Station Problem:**

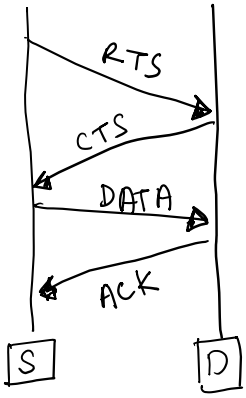
- Problem of station not been able to detect a potential competitor for the medium because the competitors is far away is refer to as Hidden Station Problem.
- Consider a situation when A is transmitting to B, if C senses the medium, it will not hear anything because it is out of range, and thus falsely conclude that no transmission is going on and will start transmit to B.



C is hidden station to A.
Hidden station problem

- **Exposed Station Problem:**
  - Consider a situation when B is transmitting to A, C sense the medium and detects the ongoing transmission between B and A. C falsely concludes that it cannot transmit to D, when the fact that it will not cause any problem.
  - A transmission can cause problem only when the destination is zone between B and C. This problem is Exposed Station Problem.

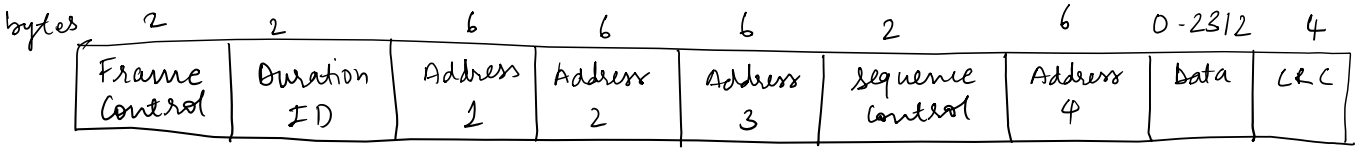
5) The solution to these problems is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)



4 way handshake protocol

- Steps can be summarised as
  - Sender sends a short frame called request (RTS)[20 bytes] to destination. RTS also contain the length of data frame.
  - Destination responds with a short [14 bytes] clear to send (CTS) frame.
  - After receiving the CTS, the sender starts sending the data frame.
  - If collusion occurs, CTS frame is not received within a certain time frame.

6) MAC Frames



IEEE 802.11 MAC packet structure

- The above figure shows the basic structure of an IEEE 802.11 MAC data frame.
- **Frame Control:**
  - 2 bytes
  - Contains several subfields like, *Protocol version, Type, Subtype, Power Management*
- **Duration/ID:**
  - Field value is less than 32,768
  - This field contains the value indicating the period of time in which the medium is occupied (in µs)
- **Address 1 to 4:**

    - The four address fields contain standard IEEE 802 MAC Addresses (48 bits each)
- **Sequence Control:**
    - Due to acknowledgement mechanism, frames may be duplicated, so sequence control is used to filter duplicates.
- **Data:**
    - MAC frame must contain arbitrary data (max 2,312 bytes), which is transferred transparently from sender to receiver(s).
- **Checksum (CRC):**
    - 32-bit checksum
    - Used to protect the frame.

Comparison of S/T/F/CDMS:

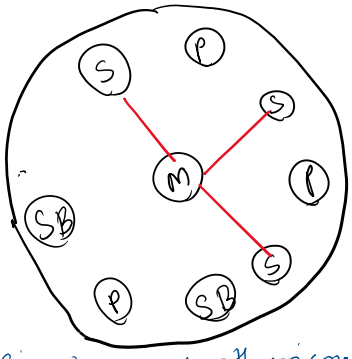
- In real systems, MAC schemes always occur in combinations. A very common combination is SDMA/TDMA/FDMA as used in PAC phones; CDMA/SDMA is used in satellite systems.

Approach	SDMA	TDMA	FDMA	CDMA
Full Forms	Space Division Multiple Access	Time Division Multiple Access	Frequency Division Multiple Access	Code Division Multiple Access
Idea	Segment space into cells/sectors	Segment sending time into disjoint time-slots, demand driven or fixed pattern	Segment the frequency band into disjoint sub-bands	Spread the spectrum using orthogonal codes
Terminals	Only one terminal can be active in one cell/one sector	All terminals are active for short periods of time on the same frequency.	Every terminal has its own frequency uninterrupted	All terminals can be active at same place at the same moment, uninterrupted
Signal separation	Cell structure directed antennas	Synchronization in the time domain	Filtering in the frequency domain	Code plus special receivers
Advantages	Very simple; increases capacity per km^2	Established; fully digital; very flexible	Simple; established; robust	Flexible; less planning needed; soft handover
Disadvantages	Inflexible; antennas typically fixed	Guard space needed (multi-path propagation); synchronization difficult	Inflexible; frequencies are a scarce resource	Complex receivers; needs more complicated power control for senders
Comment	Only in combination with TDMA, FDMA or CDMA useful	Standard in fixed networks, together with FDMA/SDMA used in many mobile networks	Typically combined with TDMA, and SDMA	Used in many 3G systems, higher complexities, lowered expectations; integrated with TDMA/FDMA.

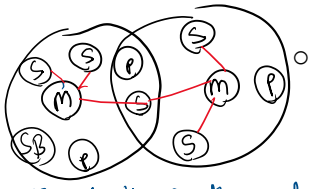
Bluetooth

- Aims for ad-hoc piconets, which are local area networks.
- They have limited coverage
- Do not need infrastructure.
- Need to connect different small devices in close proximity.
- **Architecture:**
  - Networking:
    - Bluetooth operates on 79 channels in 2.4Ghz band with 1MHz carrier spacing.
    - Each device performs hoping with 1600 hops/sec.
    - In a piconet 1 act as master, all other devices connected must act as slaves.
    - Each piconet has one master and up to seven slaves.
    - More than 200 can be parked.
    - The upper limit is 8 active devices, because of the 3 bit address used in Bluetooth.
    - One slave in the piconet can switch to park mode to allow the parked device to switch to active mode.
    - Extension of piconet is scatternet i.e., when nodes can communicate with each other piconets.
    - Master can also leave its piconet and act as a slave in another piconet.

m - master
s - slave
P - parked
SB - stand by

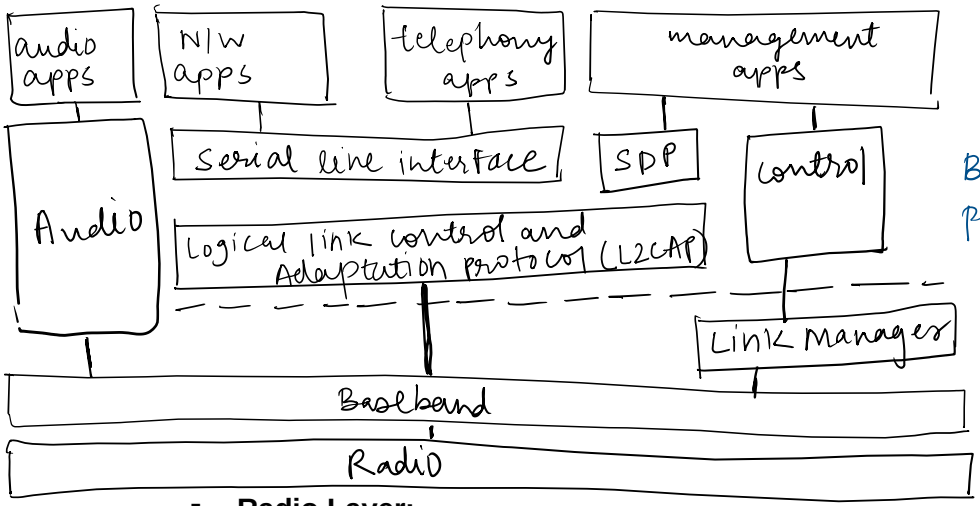


Simple bluetooth piconet



Bluetooth scatternet

  - Protocol Stack:
    - The core protocols of Bluetooth comprise the following elements:
      - Radio
      - Baseband
      - Link manager protocol
      - Logical link control and adaptation protocol (L2CAP)
      - Service discovery protocol

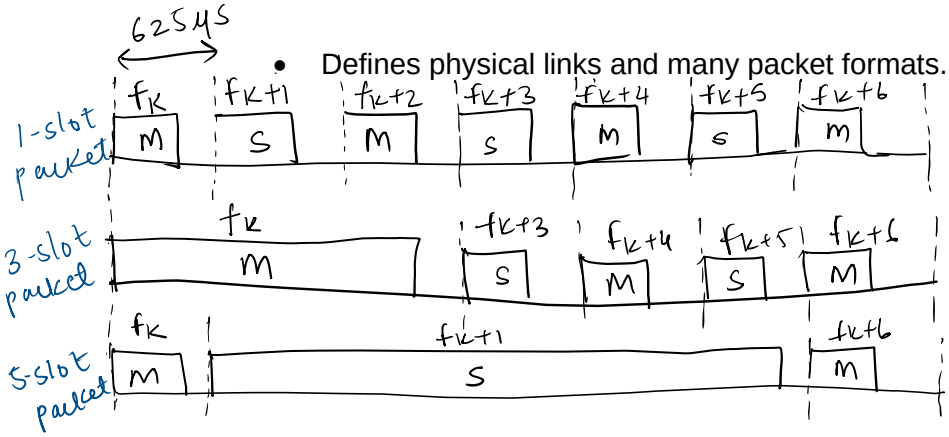


Bluetooth protocol stack

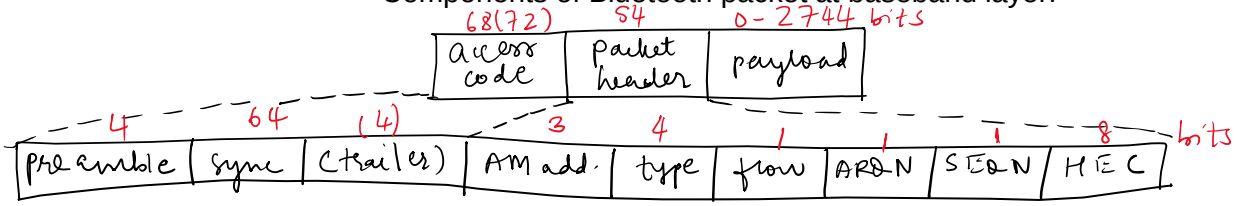
    - **Radio Layer:**
      - Specification of air interface.
      - Defines carrier frequency and output power.
      - Bluetooth uses license free frequency band at 2.4GHz.
      - Fast hopping rates of 1600 hops/sec.
      - Time b/w hops is c/d slots, which is interval of 625µs.
      - After worldwide harmonization, Bluetooth devices can be used (almost) anywhere.
    - **Baseband Layer:**
      - Performs frequency hopping for medium access.

@jiisanda

- Defines physical links and many packet formats.



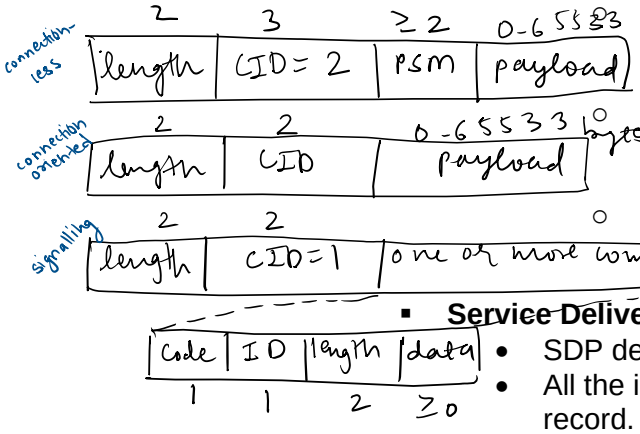
- Components of Bluetooth packet at baseband layer.



- **Link manager protocol:**
  - Functions:
    - Authentication, pairing and encryption
    - Synchronization
    - Capability negotiation
    - Quality of Service negotiation
      - Master can limit the no. of slots available for slave answer to increase its own bandwidth.
      - Depending on this signal level the device can direct the sender of the measured signal to increase or decrease it transmit power.
    - Link Supervision
      - LMP may setup a new SCO (synchronous connection oriented) link or may declare the failure of a link.
    - State and transmission mode change:
      - Devices may switch the master/slave role,
      - Detach themselves from connection
      - Change operating mode
  - To save battery power Bluetooth devices can go into one of three low power states:
    - Sniff State:
      - Highest power consumption
      - Device listens to the piconet at reduced rate
      - Master reduces the no. of slots for transmission to slave
      - Device keeps its AMA (Active Member Address)
    - Hold State:
      - Devices does not release its AMA, but stops its async connection link (ACL) transmission.
      - Slave may still exchange SCO packets.
    - Parked State:
      - Lowest duty cycle
      - Lowest power consumption

- Releases its AMA and receives parked member address (PMA).
- Device is still in piconet, but gives room for another device to become active.

- **L2CAP**:
  - Logical link control and adaptation protocol.
  - Data link control protocol on top of the baseband layer
  - Offers logical channels b/w Bluetooth devices with QoS properties:



    - Connectionless:
      - Unidirectional
      - Used for broadcasts from master to its slave(s)
    - Connection Oriented:
      - Channel is bidirectional
      - Supports QoS for both directions
    - Signalling:
      - Used in exchanging signalling messages b/w L2CAP entities.

- **Service Delivery Protocol:**
  - SDP defines only discovery of services, not their usage.
  - All the information an SDP server services is in a service record. This consists of list of service attributes.
  - Service attribute consists of an attribute ID (16-bit) and an attribute value (UUID).
  - Example

1G Technology:

- 1st Generation of wireless telephone
- Completed in early 1990s.
- Speed up to 2.4kbps.
- Allows voice calls in one country.
- N/w uses Analog Signal
- Drawbacks:
  - Poor Voice quality
  - Poor Battery Life
  - Large Phone Size
  - No Security
  - Limited Capacity
  - Poor Handoff Reliability

2G Technology

- 2nd Generation, based on GSM.
- Launched in Finland, 1991
- Uses digital signals
- Data Speed: 64 kbps
- Features:
  - Enables text messages, picture messages and MMS (Multi Media Message)
  - Provides better quality and capacity
- Drawbacks
  - Requires strong digital signals
  - Unable to handle complex data as videos

2.5G Technology

- Technology between the 2G and 3G.
- Sometimes describes as 2G Cellular Technology combined with GPRS.

- Features:
    - Phone Calls
    - Send/Receive Email messages
    - Web Browsing
    - Speed:64-144kbps
    - Camera Phones
    - Take a time of 6-9 mins. to download a 3 mins. Mp3 song

3G Technology

- 3rd Generation, introduced in 2000s.
- Data Transmission speed: 144kbps-2Mbps
- Typically called Smart Phones.
- Features:
    - Providing Faster Communication
    - Send/Receives Large Email Messages
    - High Speed Web / More Security
    - Video Conferencing / 3D Gaming
    - TV Streaming / Mobile TV / Phone Calls
    - Large Capacities and Broadband Capabilities
    - 11sec – 1.5 min time to download a 3min Mp3 song
- Drawbacks:
    - Expensive fees for 3G licenses service
    - It will challenge to build the infrastructure for 3G
    - High Bandwidth requirement
    - Expensive 3G Phones
    - Large Cell phones.

4G Technology (Anytime Anywhere)

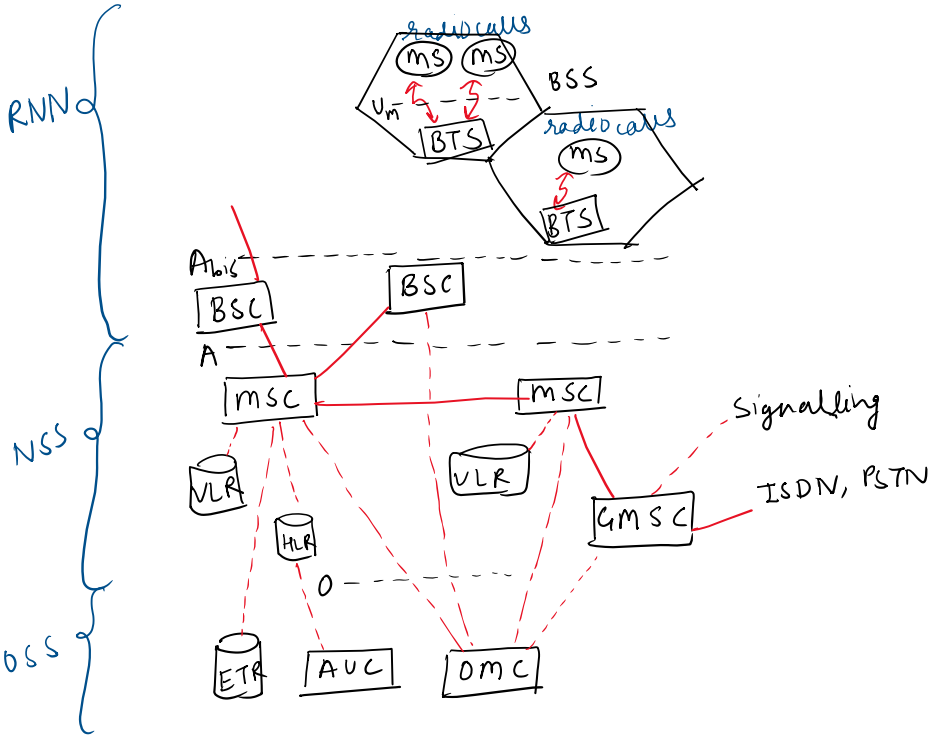
- 4th Generation, late 2000s
- Data Speed: 100Mbps – 1Gbps
- Also described as MAGIC:
    - Mobile Multimedia
    - Anytime Anywhere
    - Global Mobility Support
    - Integrated Wireless Solution
    - Customized Personal Service
- Also known as Mobile Broadband Everywhere
- Features:
    - High QoS
    - High Security
    - High Speed
    - High Capacity
    - Low cost per bit
- Drawbacks:
    - More Battery uses
    - Hard to implement
    - Need complicated hardware
    - Expensive equipment required.

Comparison between 3G and 4G

Technology	**3G**	**4G**
Data Transfer Rate	3.1 MB/sec	100 MB/sec
Internet Service	Broadband	Ultra broadband
Mobile TV Resolution	Low	High
Bandwidth	1.6-2GHz	2-8GHz
Download & Upload	5.8 Mbps	14Mbps

GSM:

- Groupe Special Mobile (GSM)
  Or latter known as
  Global System for Mobile Communication
- Typically, the 1st generation system
- Mobile Service provided by GSM:
  - Bearer Services
  - Tele Services
  - Supplementary Services
- **Bearer Services**
  - Bearer services permits transparent and non-transparent, synchronous or asynchronous data transmission.
- **Tele Services**
  - Main Service of GSM is telephony
  - i.e., to provide high-quality digital voice transmission
  - Another service offered by GSM is emergency numbers
  - SMS (Short Message Service) was in GSM standard from the beginning.
- **Supplementary Services**
  - Offers various enhancement for the standard telephony services
  - Typically, services are user identification, call redirection or forwarding of ongoing calls.
- **System Architecture of GSM:**
  - A GSM system consists of three subsystems
    - Radio Subsystem (RSS)
    - Network Subsystem (NSS)
    - Operational Subsystems (OSS)

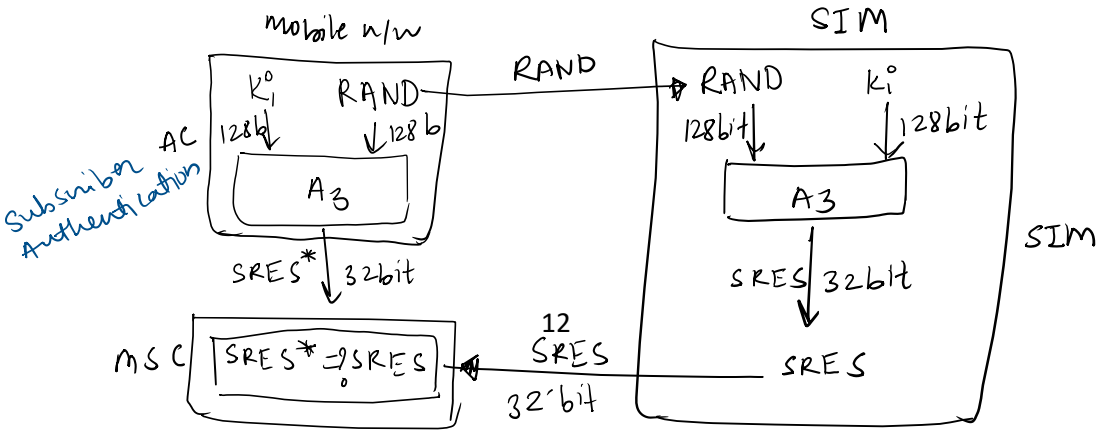


  - **Radio Subsystem (RSS):**
    - As the name implies, the RSS comprises all radio specific entities, i.e., the mobile stations (MS) and the base station subsystem (BSS).
    - **Basic Station Subsystem (BSS):**
      - GMS n/w contains many BSSs, each controlled by Base Station Controller (BSC).

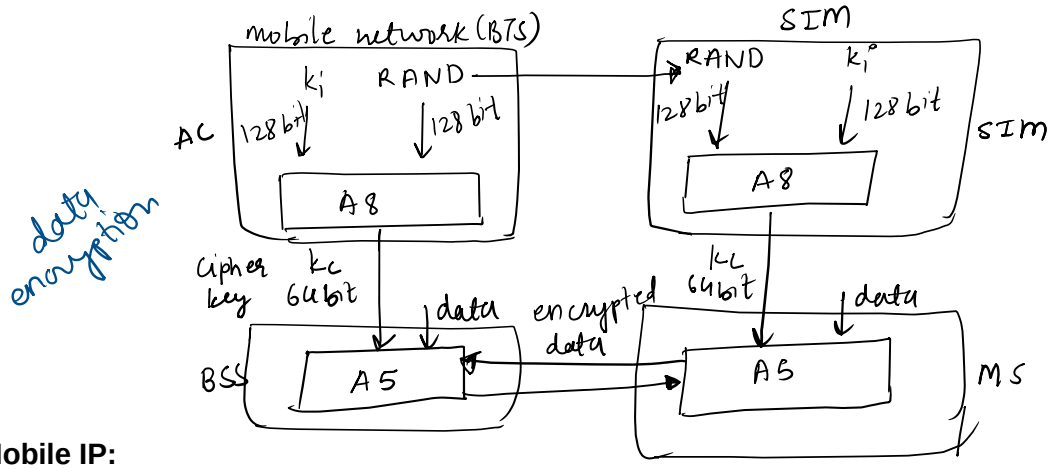
@jiisanda

        - BSS performs all function necessary to maintain radio connection to an MS (Mobile Station).
        - Beside BSC, the BSS contains several BTSs.
    - **Base Transceiver Station (BTS):**
        - BTS contains all radio equipment i.e., antennas, signal processing, amplifiers necessary for radio transmission.
    - **Base Station Controller (BSC):**
        - BSC manages the BTSs,
        - Performs paging of the MS.
- **Network and switching Subsystem (NSS):**
    - Heart of the GSM.
    - NSS connects the wireless n/w with standard public networks, performs handover between different BSSs.
- **Operation Subsystems (OSS):**
    - Contains the necessary functions for network operations and maintenance.
    - The OSS posses network entities of its own and access other entities.

- Security Services provided by GSM
    - GSM offers several security services using confidential information stored in the individual SIM. The SIM stores personal, secret data and is protected with a PIN against unauthorized use.
        - Access control and authentication:
            - The first step includes authentication of valid user for the SIM.
            - The user needs a secret PIN to access the SIM.
            - The next step is subscriber authentication.
        - Confidentiality:
            - All user-related is encrypted. After authentication, BTS and MS apply encryption to voice, data and signalling.
        - Anonymity:
            - To provide user anonymity, all data is encrypted before transmission, and user identifiers are not used over the air.
    - Three algorithms are specified to provide security services in GSM:
        - Algorithm A3 used for authentication
        - A5 for encryption
        - A8 for generation of cipher key
    - <u>Authentication:</u>
        - User must be authenticated, before a subscriber use any service from GSM.
        - Authentication is based on SIM, which stores the individual authentication key K_i, the user identification IMSI.
        - The algorithm used for authentication A3.
        - Authentication is based on challenge-response method: the access control AC generates a random number RAND as a challenge, and the SIM within the MS answers with SRES (Signed Response) as response.



- Encryption:
  - To ensure privacy, all messages containing user-related information are encrypted in GSM over the air interface.
  - After authentication, MS and BSS can start using encryption by applying the cipher key K_c.
  - K_c is generated using the individual key K_i and a random value by applying the algorithm A8.



Mobile IP:

- If Mobile IP is not used, you will not receive a single packet as soon as you leave your home network, i.e., the n/w you are configured for, and reconnect your computer at another place.
- One might think the quick solution can be to assign the computer a new IP address. i.e., moving to a new location would mean assigning a new IP address. The problem is nobody knows about this new address. It's almost impossible to find a (mobile) host on the internet which has just changed its address.
- There is a severe problem with higher layer protocols like TCP which rely on IP addresses. Changing the IP address while still having a TCP connection open means breaking the connection. A TCP connection is identified by the tuple (source IP address, source port, destination IP address, destination port), also known as socket pair (a socket consists of address and ports). Therefore, a TCP connection cannot survive any address change. Breaking a TCP connection is not an option, the mobile node would also have to notify all communication partners about the new address.
- **Requirements that led to Mobile IP**:
  - Compatibility:
    - A new standard cannot introduce changes for applications or network protocols already in use.
    - Mobile IP has to be integrated into existing operating systems.
    - Router should not require other software.
    - Mobile IP must not require special media or MAC/LLC protocol.
  - Transparency:
    - Mobility should remain 'invisible' for many higher layer protocols.
  - Scalability and efficiency:
    - Introducing the 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.
    - Mobile IP is expected to be scalable over a large number of participants in the whole internet, worldwide.
  - Security:
    - Mobility poses many security problems; the minimum requirement is that of all messages related to the management of Mobile IP are authenticated.

        - The IP layer must be sure that if it forwards a packet to a mobile host that this host receives the packet.
    - The goal of 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.'
- Entities and Technology:

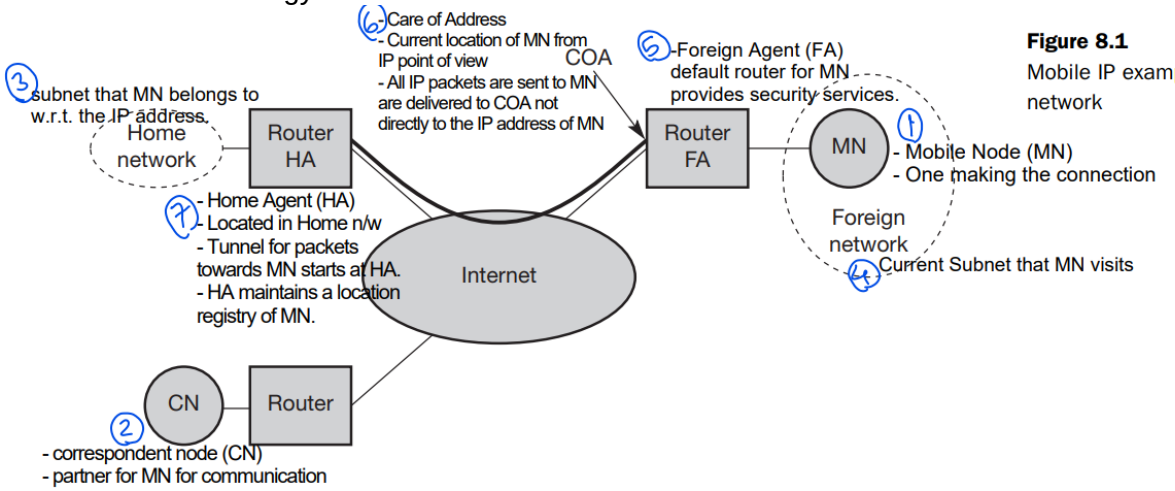
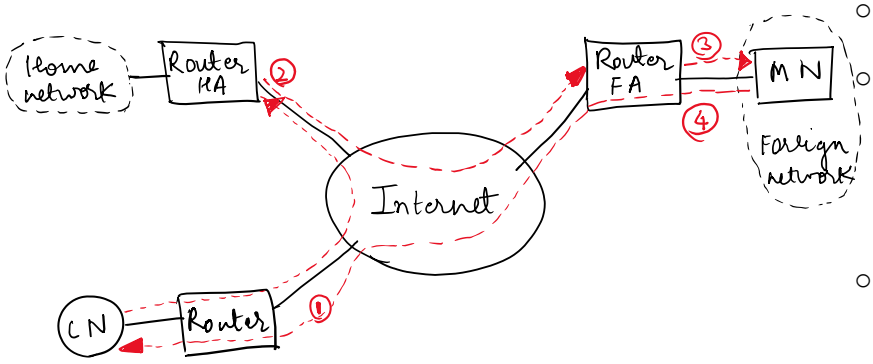


Figure 8.1 Mobile IP example network

- **IP Packet Delivery**

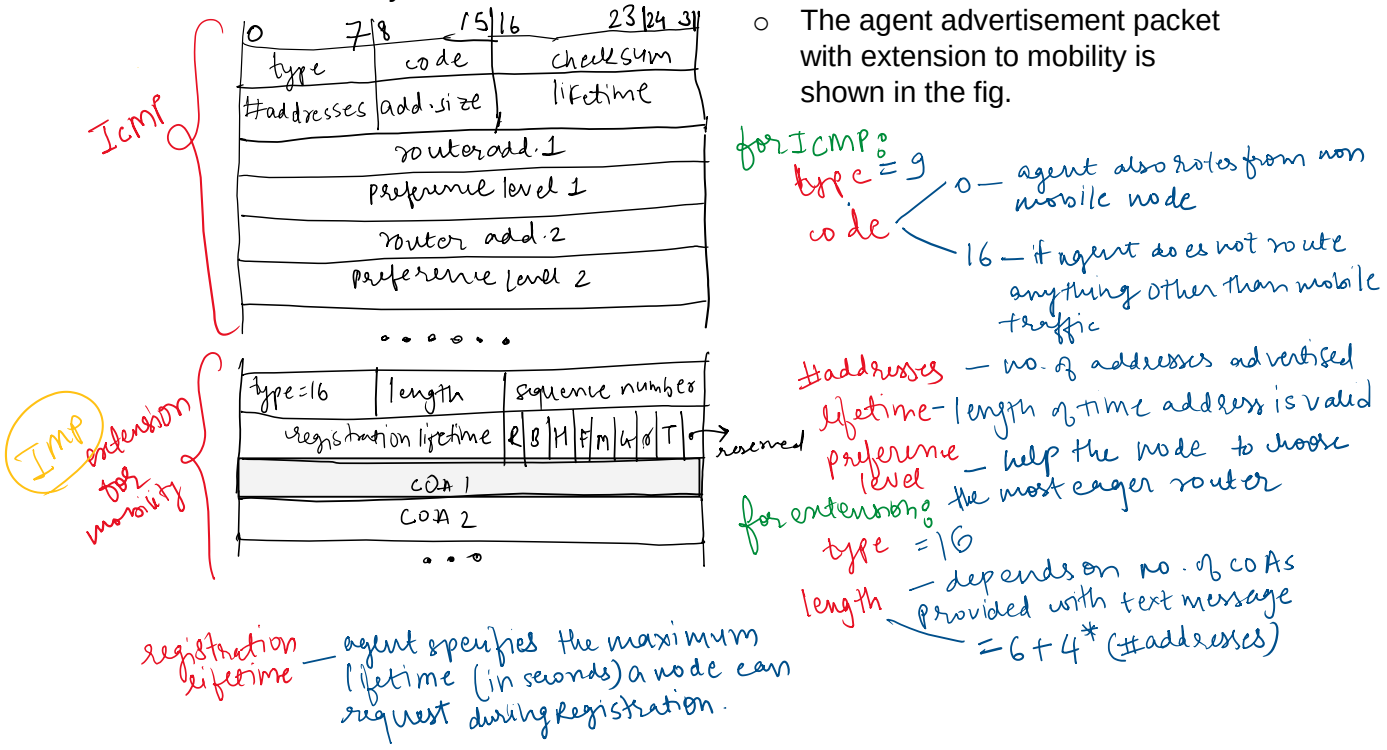


    - Correspondent node (CN) wants to send an IP packet to the MN.
    - Requirement of mobile IP:
        - Support hiding the mobility of the MN.
        - CN does not need to know anything about MN's current location,
    - So, CN sends an IP packet with MN as a destination address and CN as a source address. (Step 1)
    - The internet, not having information on the current location of MN, routes the packet to the router responsible for the home network of MN.
    - The HA now intercepts the packet, knowing that MN is currently not in its home network. So, packet will not be forwarded into the usual subnet, but it is encapsulated and tunnelled to the COA.
    - Now, new header is put in front of old IP address showing the COA as new destination as HA as a source of the encapsulated packet. (Step 2)
    - The FA now decapsulated the packet, and forwards the original packet with CN as a source and MN as destination to the MN. (Step 3)
    - Note, MN's mobility is not Visible. It receives the packet with the same sender and receiver address as it would have in the home network.
    - The MN sends the packet as usual with its own IP address as a source and CN's address as destination. (Step 4)
    - The router with FA acts as default router and forwards the packet in the same way as it would do for any other node in the foreign network. As long as CN is a fixed node the remainder is in the fixed internet as usual. If CN was also a mobile node residing in foreign network, the same mechanism as described in step 1 to 3 would apply now in the other direction.
- **Agent Discovery**

One of the problems of MN is how to find a foreign agent. How does the MN discover that it has moved? For this mobile IP have 2 methods *agent advertisement* and *agent solicitation*.

Agent advertisement

- In this method, foreign agents and home agents advertise their presence periodically using special agent advertisement messages.
- These messages can be seen as the beacon broadcast into the subnet.
- For this Internet Control message protocol (ICMP) messages are used with some mobility extensions.



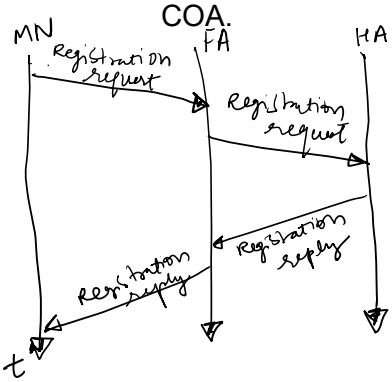
- The agent advertisement packet with extension to mobility is shown in the fig.
- The following bits specify the characteristics of agent in detail.
  - R -> registration bit, shows if a registration with this agent is required
  - B -> is set if the agent is currently too busy to accept new registrations
  - H -> is set if the agent offers services as a home agent
  - F -> is set if the agent offers services as a foreign agent.
  - M & G -> type of encapsulation
    - M -> Minimal encapsulation
    - G -> Generic routing encapsulation
  - r -> set to zero and must be ignored.
  - T -> indicates reverse tunning is supported by FA

Agent Solicitation

- If no agent advertisements are present, the mobile node must send agent solicitation.
- Care should be taken that these solicitation messages should not flood the network, but basically an MN can search for an FA endlessly sending out solicitation messages.
- Typically, a mobile node can send upto 3 solicitation messages per second, as soon as it enters a new network.
- If a node does not receive an answer to its solicitations, it must decrease the rate of solicitations exponentially to avoid network flooding.
- The next step is registration with HA if MN is in foreign network.

- **Registration:**

Having receiving the COA, MN must register with HA. The main purpose of the registration, is to inform the HA of the current location for correct forwarding of packet. Registration can be done in 2 different ways depending on the location of the COA.



- If COA is at the FA, registration is done as the following figure.
  - The MN sends its registration request containing the COA to the FA which is forwarding the request to the HA.
  - The HA now sets up a *mobility binding* contining the mobile node's home IP address and the current COA.
  - Aditionally, mobility binding contains the lifetime of the registration, negotiated during the registration process.
  - The registration gets deleted after the lifetime automatically, so MN should reregister before the expiration.
  - After setting up the mobility binding, the HA sends a reply message back to the FA which forwards it to MN.

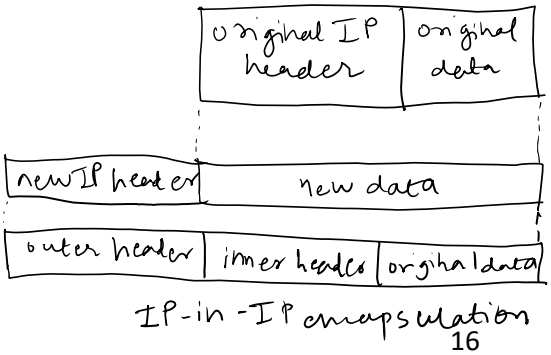
- If COA is co-located, registration can be simpler, shown in figure.
  - The MN can send the request directly to the HA and vice versa.
  - This is also a process of registation for MN when it returns back to the home agent.
- UDP packets are used for registration requests.
- IP source address is set to the interface address of the MN, UDP destination address is that of FA or HA (based on location of COA)
- The UDP destination port is set to 434.
- UDP is used because of low overheads and better performance, compared to TCP in wireless environment.
- A registration reply, which is conveyed in a UDP packet.

- **Tunnelling and encapsulation**

Mechanisms used for forwarding packets between HA and COA (Step 2). Tunnelling i.e., sending a packet through a tunnel, is achieved by using encapsulation. Encapsulation is a 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 data part of another part, is called decapsulation.

IP-in-IP encapsulation:

- Mandatory encapsulation method used for mobile IP is IP-in-IP encapsulation.
- The figure describes what the HA at the tunnel entry does.
- The HA takes the original packet with the MN as destination, puts it into the data part of a new packet and sends the new IP address in such a way that the packet is routed to COA.

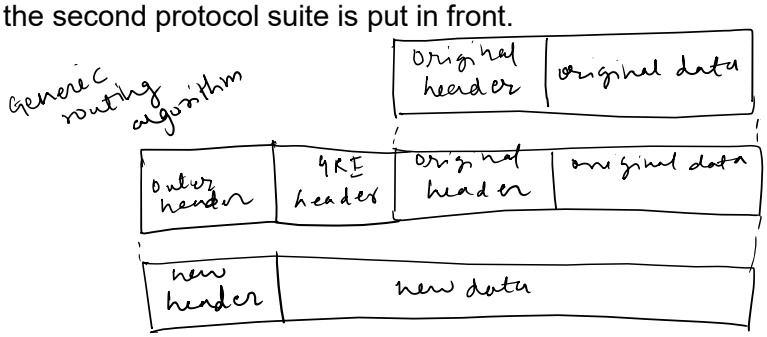


Minimal Encapsulation

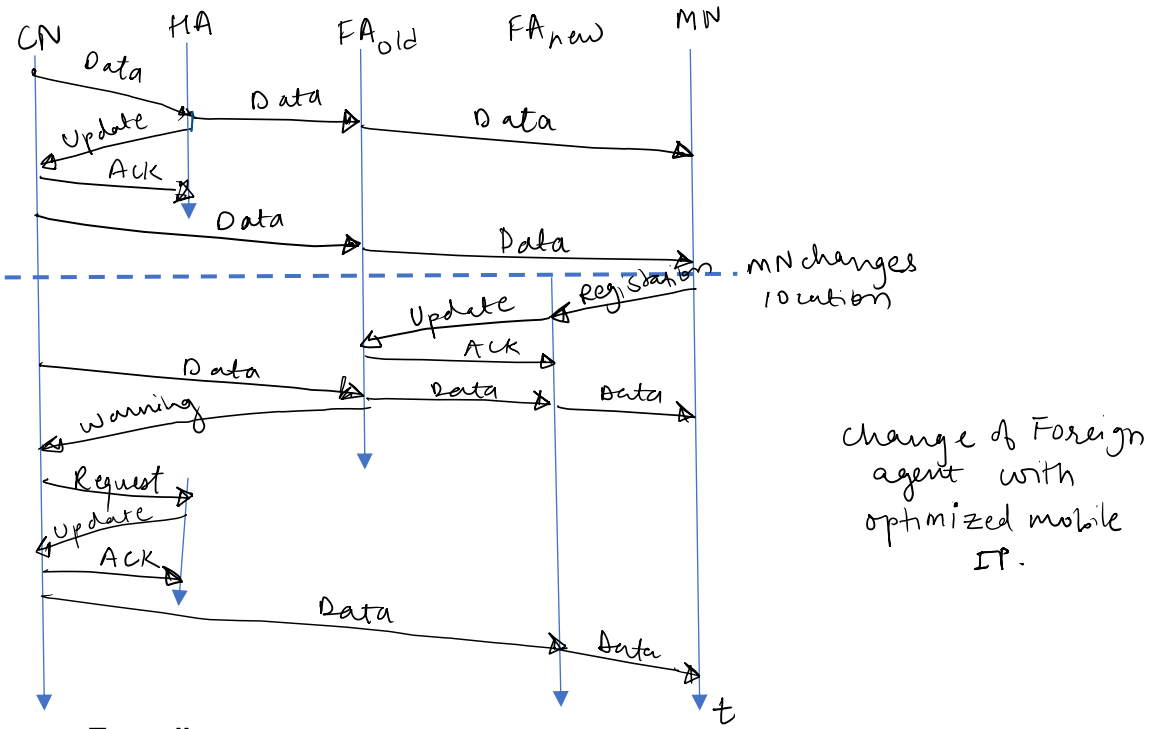
- Optional encapsulation method for a mobile IP.
- Tunnel entry points and endpoint are specified.
- The inner header is different for minimal encapsulation

Generic Routing Encapsulation

- While IP-in-IP only works for IP, the following encapsulation scheme also supports other network layer protocols in addition to IP.
- Generic Routing Encapsulation (GRE) allows the encapsulation of packet of one protocol suite into payload portion of packet of another protocol suit.
- Fig. shows the procedure. The packet of one protocol suite with the original packet header and data is taken and a new GRE header is prepended. Together this forms the new data part of the new packet. Finally, the header of the second protocol suite is put in front.



- **Optimization**
  - Example, Imagine the following situation, Japanese and German meet at a conference on Hawaii. Both uses their laptops for exchanging data, both run mobile IP for mobility support. So, if the Japanese sends a packet to the German, his computer sends the data to the HA of the German, i.e., from Hawaii to Germany. The HA in Germany now encapsulates the packet and tunnels them to the COA of the German laptop on Hawaii. That means although the computers are just meters away, the packet travel around the world! This inefficient behavior of non-optimized mobile IP is called *triangular routing.* The triangular is made of 3 segments CN-HA, HA-COA/MN, MN back to CN.
  - One way to optimize route is to inform the Cn of the current location of MN, the CN can learn the location of MN by caching it in *binding cache*. The appropriate entity to inform the location of MN to CN is HA.
  - The optimized mobile IP protocol needs four additional messages:
    - Binding request: Any node that wants to know the current location, of an MN, sends a binding request to HA. The HA checks if the MN has allowed dissemination of its current location, if yes HA sends back the binding update.
    - Binding Update: The message is sends by HA to CNs reveling the current location of an MN. The message contains the fixed IP address of MN and the COA. The binding update can request an acknowledgement.
    - Binding Acknowledgement: If requested, the node returns its acknowledgement after receiving the binding update message.
    - Binding Warning: If the node decapsulates a packet for an MN, bit it is not the current FA for this MN, this node sends a binding warning.
  - The figure explains the additional four messages together with the case of MN changing its FA.
  - This provides smooth handovers.
  - Without this optimization, all packets in transit would be lost while MN moves from one FA to another.



- **Reverse Tunneling**
  - The return from MN to CN in IP Packet Delivery fig, looks simple, i.e., the MN can directly send its packet to the CN as in any other standard IP situation. The destination address in the packets is that of CN. But there are several sever problems with this simple solution.
    - Firewalls:
      - This provides at least a first and simple protection against misconfigured system of unknown addresses.
      - Firewalls often filter packets coming from outside containing a source address from computers of internal networks. This avoids other computers that could use internal addresses and claim to be internal computers.
      - This means that not only the destination address matters for forwarding IP packets, but also the source address due to security concerns.
    - Multi-cast:
      - Reverse tunneling is needed for the MN to participate in multi-cast group.
      - While the node in the HN might participate in multi-cast group, an MN in a foreign network cannot transmit multi-cast packet in a way that they emanate from its home network without a reverse tunnel.
      - The foreign network might not even provide the technical infrastructure for multi-cast communication.
    - 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.

- Mobile IP is no longer transparent if a user has to adjust the TTL while moving. 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.

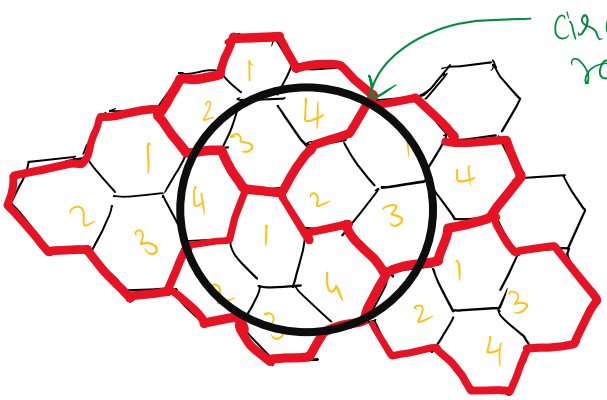
- **IPv6**
  - While mobile IP was originally designed for IPv4, IPv6 makes life much easier.
  - Several mechanisms that had to be specified specifically for mobility support comes free in IPv6.
  - One issue is security with regards to authentication, which is now a required feature for all IPv6 nodes.
  - No special mechanisms as add-ons are needed for securing mobile IP registration.
  - The mechanisms for acquiring a COA are already build in.
  - Neighbor discovery as a mechanism mandatory for every node is also included in specification.
  - Special foreign agents are no longer needed to advertise services.
  - Every IPv6 node can send binding update to another node, so the MN can send its current COA directly to the CN and HA. These mechanisms are integral part of IPv6.
  - A soft handover is possible with IPv6.
  - A CN only has to be able to process binding updates, i.e., to create or to update an entry in the routing cache.
  - However, IPv6 does not solve any firewall or privacy problems. Additional mechanisms on higher layer are needed for this.

TCP over 2.5/3G Wireless

The following characteristics have to be considered when deploying applications over 2.5G/3G wireless links:
- Data rates
- Latency
- Jitter
- Packet loss

Based on these characteristics, the following configuration parameters to adapt TCP to wireless environments:
- Large windows
- Limited transmit
- Large MTU (Maximum Transfer Unit)
- Selective Acknowledgement
- Explicit Congestion Notification
- Timestamp
- No header compression

Frequency Resue
In a cellular system, each cell has a base transceiver. The transmission power is carefully controlled to allow communication within the cell using given frequency while limiting the power at that the frequency that escapes the cell into adjacent ones.
The objective is to use same frequency in other nearby cells thus allowing the frequency to be used for multiple simultaneous conversations.



In characterizing frequency reuse, the following parameters are commonly used:

D = minimum dist. b/w centers of cells that use the same band of frequency.

R = radius of a cell

d = distance between centers of adjacent cells ($d = \sqrt{3}R$)

N = no. of cells in a repetitions pattern, (reuse factor)

In hexagonal cell pattern,

$$N = I^2 + J^2 + (I \times J), \quad I, J = 0, 1, 2, 3, \ldots$$

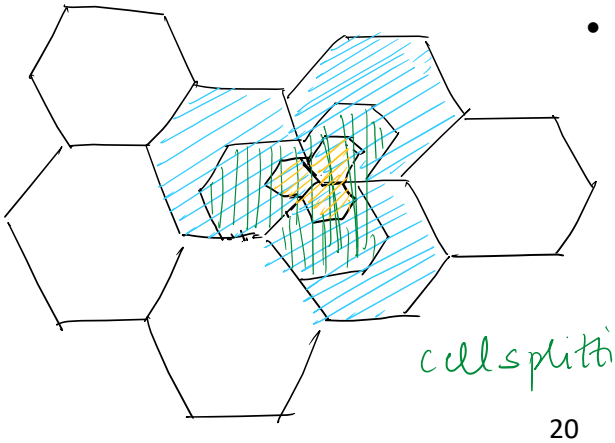
$\therefore N = 1, 3, 4, 7, 9, 12, \ldots$

∴ relationship is $\frac{D}{R} = \sqrt{3N} \Rightarrow \frac{D}{d} = \sqrt{N}$

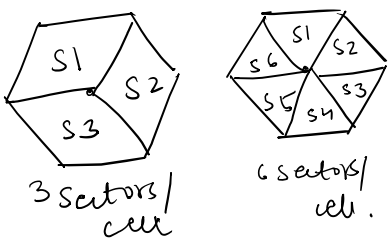
Increasing Capacity [**Improving Coverage and Capacity of cellular network**]

In time, as more customers use the system, traffic may build up so that there are not enough frequencies assigned to a cell to handle its cells. The following are approaches:

- Adding new channels: Growth and expansion can be managed in an orderly fashion by adding new channels.
- Frequency borrowing: In simplest case, frequencies are taken from adjacent cells by congested cells.
- Cell Splitting: In practice, the distribution of traffic is not uniform, and this presents opportunity for capacity increase. Generally, the original cells are 6.5 to 13 km in size. 1.5km cells are close to the practical minimum.
    - As the cell gets smaller, the handoffs become much frequent.
    - The radius reduction by a factor of F reduces the coverage area and increases the required number of base stations, by a factor of F^2.



- Cell Sectoring:
    - With cell sectoring the cell is divided into wedge shaped sectors, each with its own set of channels, typically three or six sectors per cell.



- Microcells:
    - As cell becomes smaller, antennas move from tops of tall buildings or hills, to top of small buildings or the sides of large buildings, and finally on lamp posts, where they form microcells.
    - Microcells are useful in city streets in congested area, along highways, and inside large public buildings.

Channel Assignment Strategies

Channel assignment strategies affect the performance of the system especially when it comes to handoffs. There are several channel assignment strategies, two of them are:

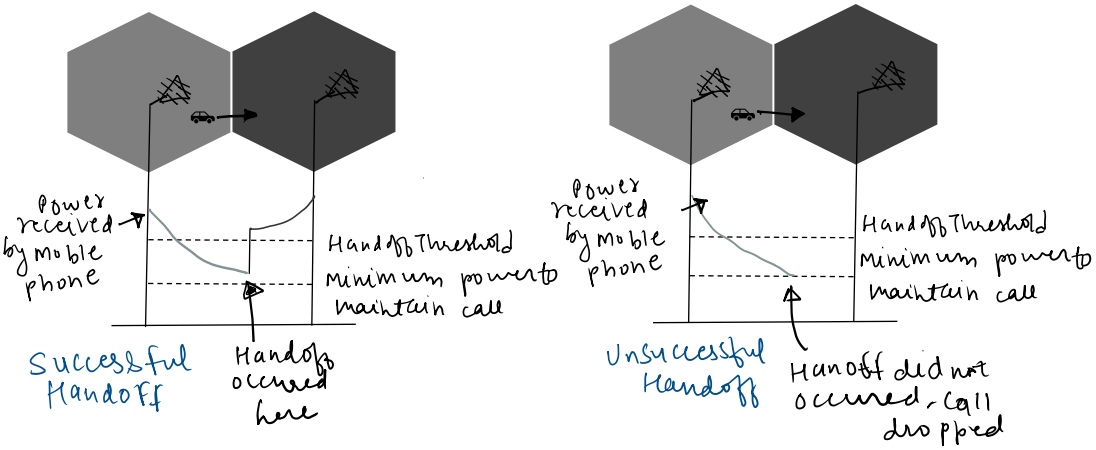
- Fixed Channel Assignment
  In this channel assignment, channels are pre-allocated to different cells meaning that each cell is assigned a specific number of channels and the frequencies of these channels are set. Such a channel assignment has the following aspects:
  1. Any call attempts in a cell after all channels of that cell become occupied gets BLOCKED (meaning that the caller gets a signal indicating that all channels are occupied).
  2. Very simple and requires least amount of processing.
  3. A variation of this method is the Borrowing Strategy:
     a. Cells in this strategy are allowed to borrow channels from adjacent cells if their channels are fully occupied while adjacent cells have free channels,
     b. MSC (Mobile Switching Center) monitors the process and gives permission to borrowing cell to borrow channels putting in mind
        (i) donating cell is not affected by the borrowing process,
        (ii) no interference will occur by moving the channel from one cell to another.
- Dynamic Channel Assignment:
  In this channel assignment, channels are NOT pre-allocated to any cells meaning that any channel can be allocated to any desired cell during the operation of the system. Such a channel assignment has the following aspects:
  1. MSC monitors all cells and all channels,
  2. 2. Each time a call request is made, serving BS requests a channel from the MSC,
  3. 3. MSC runs an algorithm that takes into account:
     a. Possibility of future blocking in cells
     b. Frequency being used for channel
     c. The reuse distance of the channel
  4. MSC assigns a channel only if it is not used and if it will not cause co-channel interference with any cell in range,
  5. This algorithm provides higher capacity (less blocking),
  6. It requires huge computational power,
  7. MSC collects real-time data of channel occupancy, traffic distribution, and radio signal strengths indicators (RSSI).

Handoff Strategies

- The process of transferring an active call from one cell to another as a mobile unit moves from first cell to other cell without disconnecting the call.
- The amount of power received by mobile phone or tower or both usually used to determine whether handoff is necessary or not.
- Following points are put into mind:

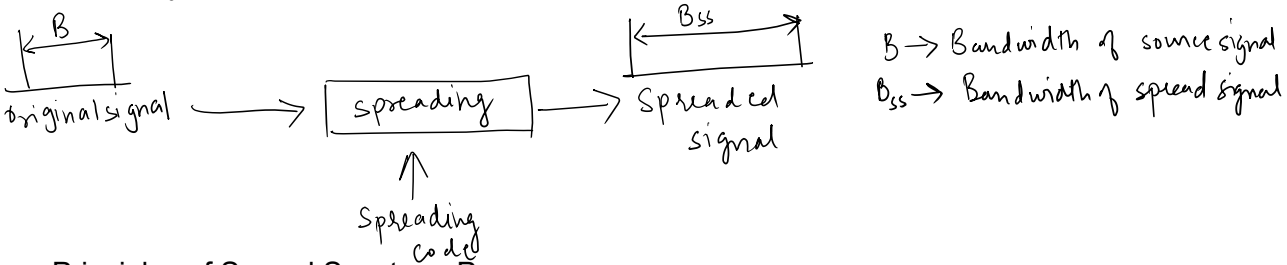
- Most system give higher priority to handoff over call initiation (it is mor annoying to have an active call disconnected than new call blocked)
- Handoffs must be completed successfully as much as possible as infrequently as possible and must be unnoticeable to the user.

- To meet these requirements, two power levels are defined:
  - Minimum acceptable signal to maintain the call $P_{\text{minimum to maintain call}}$: This is the minimum power received by the mobile phone or tower that allows the call to continue. Once the signal drops below this level, it becomes impossible to maintain the active call, because the cell because the signal is too weak.
  - Handoff Threshold $P_{\text{Threshold}}$: This power is usually selected to be few dB's (5dB to 10dB) above the minimum acceptable signal to maintain the call level.
  - The margin $\Delta = P_{\text{Threshold}} - P_{\text{Minimum to maintain call}}$ should not be too large or too small. If it is:
    - Too large, unnecessary handoffs will occur because the handoff threshold is high.
    - Too small, calls may get dropped before a successful handoff takes place because not enough time is available for the handoff.
  - The following figures shows two handoff situations. In first situation, a successful handoff takes place where the mobile phone is switched from one tower to another while in the second case, the signal power drops to the minimum value needed for maintaining a call and the call is dropped without handoff.



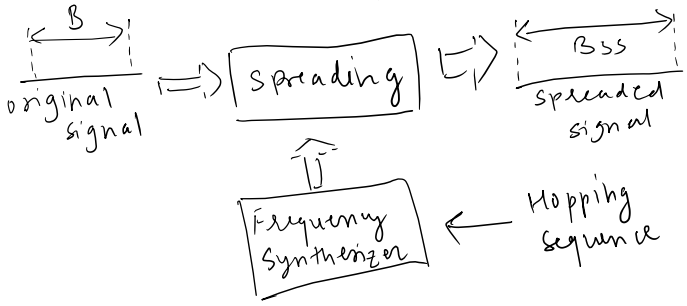
Spread Spectrum Techniques

- In spread spectrum, signals from different sources are combined to fit into larger bandwidth.
- Spread Spectrum Techniques helps in transmission of radio signals because they can easily reduce the noise and other issues that are data resistant.



- Principles of Spread Spectrum Process:
  - To allow redundancy. It is necessary that the bandwidth allocated to each station should be much larger than needed.

    - The spreading process occurs after the signal, is created by the source.
- Characteristics of Spread Spectrum:
    - Ability to resist multipath propagation
    - They are resistant to jamming.
    - Spread Spectrum offers multiple access capabilities.
- Two types of techniques for Spread Spectrum:
    - Frequency Hopping Spread Spectrum (FHSS)
    - Direct Sequence Spread Spectrum (DSSS)
- Frequency Hopping Spread Spectrum (FHSS):
    - In FHSS, different carrier frequencies are modulated by the source signal. At one moment signal modulates one carrier frequency and at the subsequent moment, it modulates other carrier frequencies.



    - Advantages of FHSS:
        - Synchronization is not dependent on distance
        - Processing Gain is higher than DSSS.
    - Disadvantages of FHSS:
        - The bandwidth of the FHSS system is too large
        - Complex and expensive Digital frequencies synthesizers are required.
- Direct Sequence Spread Spectrum (DSSS):
    - In DSSS the bandwidth of the original is also expanded by a different technique.
    - Here each data bit is replaced with n bits using a spreading code called chips, and the bit rate of the chip is called chip rate.