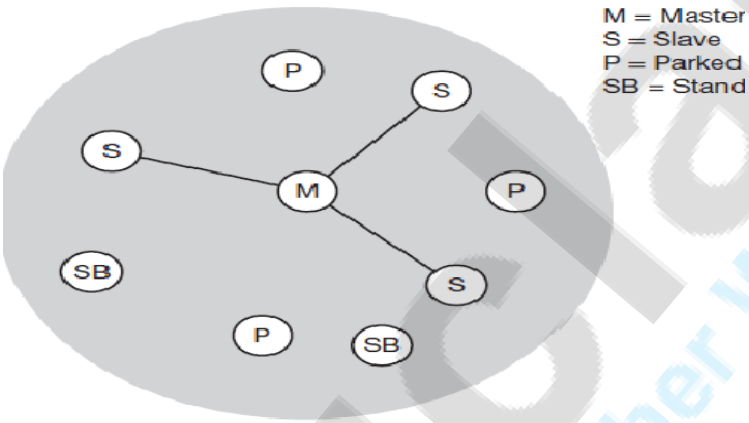
December 2012

Q2. WHAT IS PICONET AND SCATTERNET? EXPLAIN VARIOUS PROTOCOLS SUPPORTED BY BLUETOOTH PROTOCOL ARCHITECTURE. [20M]

Answer:

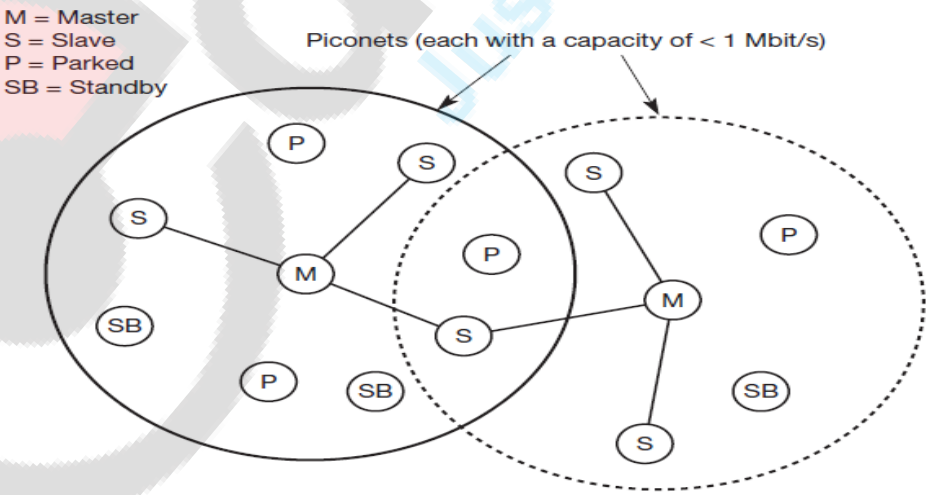
PICONET:

A piconet is a network that is created using a wireless Bluetooth connection.
A **piconet** consists of two or more devices occupying the same physical channel (synchronized to a common clock and hopping sequence).



SCATTERNET:

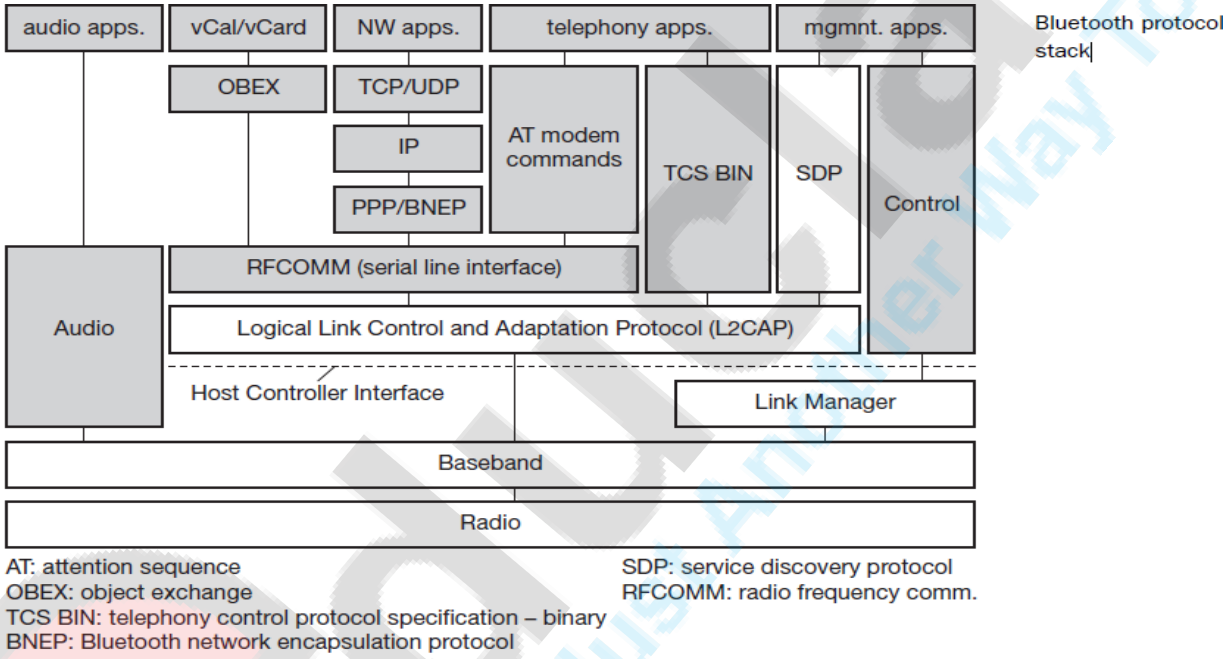
A **scatternet** is a type of ad hoc computer network consisting of two or more **piconets**.
The terms '**scatternet**' and '**piconet**' are typically applied to Bluetooth wireless technology.



ARCHITECTURE:

Like IEEE 802.11b, Bluetooth operates in the 2.4 GHz ISM band. However, MAC, physical layer and the offered services are completely different. After presenting the overall architecture of Bluetooth and its specialty, the piconets, the following sections explain all protocol layers and components in more detail.

Protocol stack



The Bluetooth specification already comprises many protocols and components.

The **core protocols** of Bluetooth comprise the following elements:

- **Radio:** Specification of the air interface, i.e., frequencies, modulation, and transmit power .
- **Baseband:** Description of basic connection establishment, packet formats, timing, and basic QoS parameters

● **Link manager protocol:** Link set-up and management between devices including security functions and parameter negotiation
● **Logical link control and adaptation protocol (L2CAP):** Adaptation of higher layers to the baseband .
● **Service discovery protocol:** Device discovery in close proximity plus querying of service characteristics.

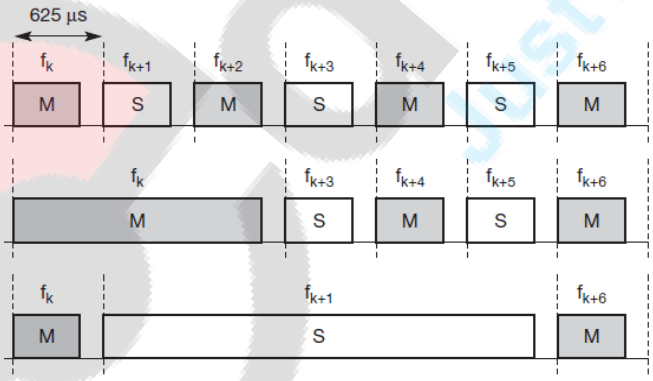
On top of L2CAP is the **cable replacement protocol** RFCOMM that emulates

- **Radio layer**

Several limitations had to be taken into account when Bluetooth's radio layer was designed. Bluetooth devices will be integrated into typical mobile devices and rely on battery power.
This requires small, low power chips which can be built into handheld devices.

- **Baseband layer**

The functions of the baseband layer are quite complex as it not only performs frequency
hopping for interference mitigation and medium access, but also defines physical links and many packet formats. Below figure shows several examples of frequency selection during data transmission. Remember that each device participating in a certain piconet hops at the same time to the same carrier frequency .



Frequency selection during data transmission (1, 3, 5 slot packets)

- **Link manager protocol:**

The link manager protocol (LMP) manages various aspects of the radio link between a master and a slave and the current parameter setting of the devices. The following groups of functions are covered by the LMP:

● **Authentication, pairing, and encryption:**
Although basic authentication is handled in the baseband, LMP has to control the exchange of random numbers and signed responses. The pairing service is needed to establish an initial
trust relationship between two devices that have never communicated before. The result of pairing is a link key. This may be changed, accepted or rejected. LMP is not directly involved in the encryption process, but sets the encryption mode (no encryption, point-to-point, or broadcast), key size, and random speed.

● **Synchronization:**
Precise synchronization is of major importance within a Bluetooth network. The clock offset is updated each time a packet is received from the master. Additionally, special synchronization packets can be received. Devices can also exchange timing information related to the time differences (slot boundaries) between two adjacent piconets.

● **Capability negotiation:**
Not only the version of the LMP can be exchanged but also information about the supported features. Not all Bluetooth devices will support all features that are described in the standard, so devices have to agree the usage of, e.g., multi-slot packets, encryption, SCO
links, voice encoding, park/sniff/hold mode (explained below), HV2/HV3 packets etc.

● **Quality of service negotiation:**
Different parameters control the QoS of a Bluetooth device at these lower layers. The poll interval, i.e., the maximum time between transmissions from a master to a particular slave, controls the latency and transfer capacity. Depending on the quality of the channel, DM
or DH packets may be used (i.e., 2/3 FEC protection or no protection). The number of repetitions for broadcast packets can be controlled. A master can also limit the number of slots available for slaves' answers to increase its own bandwidth.

● **Power control:**
A Bluetooth device can measure the received signal strength. Depending on this signal level the device can direct the sender of the measured signal to increase or decrease its transmit power.

● **Link supervision:**
LMP has to control the activity of a link, it may set up new SCO links, or it may declare the failure of a link.

● **State and transmission mode change:**
Devices might switch the master/slave role, detach themselves from a connection, or change the operating mode. Every device, which is currently not participating in a piconet (and not
switched off), is in **standby** mode. This is a low-power mode where only the native clock is running. The next step towards the **inquiry** mode can happen in two different ways. Either a device wants to establish a piconet or a device just wants to listen to see if something is going on.

- A device wants to establish a piconet: A user of the device wants to scan for other devices in the radio range. The device starts the inquiry procedure by sending an inquiry access code (IAC) that is common to all Bluetooth devices. The IAC is broadcast over 32 so-called wake-up carriers in turn.
- Devices in standby that listen periodically: Devices in standby may enter the inquiry mode periodically to search for IAC messages on the wake-up carriers.

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

- **Sniff state:**
  The sniff state has the highest power consumption of the low power states. Here, the device listens to the piconet at a reduced rate (not on every other slot as is the case in the active state).
- **Hold state:**
  The device does not release its AMA but stops ACL transmission. A slave may still exchange SCO packets. If there is no activity in

the piconet, the slave may either reduce power consumption or participate in another piconet.

- **Park state:**
  In this state the device has the lowest duty cycle and the lowest power consumption. The device releases its AMA and receives a parked member address (PMA). The device is still a member of the piconet, but gives room for another device to become active (AMA is only 3 bit, PMA 8 bit).

➢ **L2CAP:**

The **logical link control and adaptation protocol (L2CAP)** is a data link control protocol on top of the baseband layer offering logical channels between Bluetooth devices with QoS properties. L2CAP is available for ACLs only. Audio applications using SCOs have to use the baseband layer directly. L2CAP provides three different types of logical channels that are transported via the ACL between master and slave:

● **Connectionless:**
These unidirectional channels are typically used for broadcasts from a master to its slave(s).

● **Connection-oriented:**
Each channel of this type is bi-directional and supports QoS flow specifications for each direction. These flow specs follow RFC 1363 (Partridge, 1992) and define average/peak data rate, maximum burst size, latency, and jitter.

● **Signaling:**
This third type of logical channel is used to exchanging signaling messages between L2CAP entities. Each channel can be identified by its **channel identifier (CID)**. Signaling channels always use a CID value of 1, a CID value of 2 is reserved for connectionless channels.

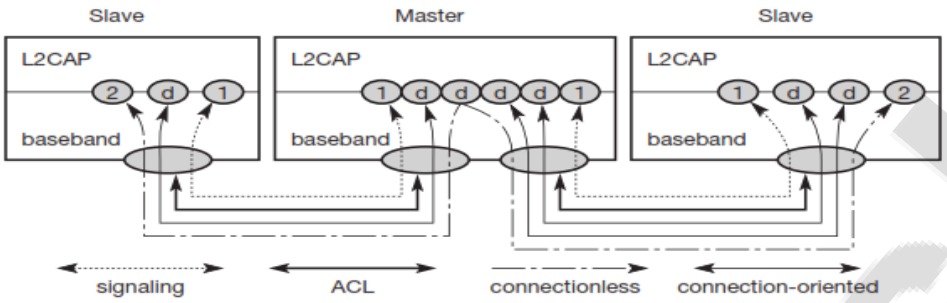


Figure gives an example for logical channels

The three packet types belonging to the three logical channel types. The **length** field indicates the length of the payload (plus PSM for connectionless PDUs). The **CID** has the multiplexing /demultiplexing function a. For connectionless PDUs a **protocol/service multiplexor (PSM)** field is needed to identify the higher layer recipient for the payload. For connection-oriented PDUs the CID already fulfills this function. Several PSM values have been defined, e.g., 1 (SDP), 3 (RFCOMM), 5 (TCS-BIN). Values above 4096 can be assigned dynamically. The payload of the signaling PDU contains one or more **commands**. Each command has its own **code** (e.g.,
for command reject, connection request, disconnection response etc.) and an **ID** that matches a request with its reply. The **length** field indicates the length of the **data** field for this command.

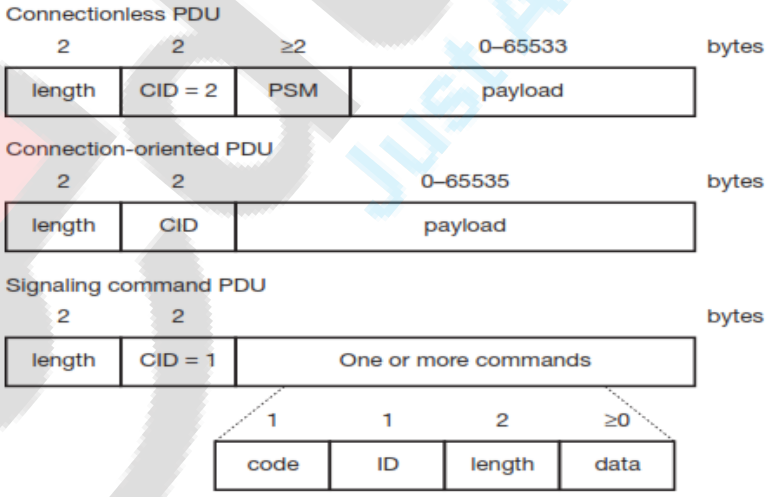


FIG:L2CAP PACKET FORMAT

Besides protocol multiplexing, flow specification, and group management,

the L2CAP layer also provides segmentation and reassembly functions. Depending on the baseband capabilities, large packets have to be chopped into smaller segments. DH5 links, for example, can carry a maximum of 339 bytes while the L2CAP layer accepts up to 64 kbyte.

Q.3) How spreading of the spectrum is advantageous in wireless transmission? Explain the technique of frequency hopping.
(10 m)

Spread spectrum uses wideband, noise-like signals that are hard to detect, intercept, or demodulate. Additionally, spread-spectrum signals are harder to jam (interfere with) than narrow band signals. These low probability of intercept (LPI) and anti-jam (AJ) features are why the military has used spread spectrum for so many years. Spread-spectrum signals are intentionally made to be a much wider band than the information they are carrying to make them more noise-like.

Spread-spectrum transmitters use similar transmit power levels to narrowband transmitters. Because spread-spectrum signals are so wide, they transmit at a much lower spectral power density, measured in watts per hertz, than narrow band transmitters. This lower transmitted power density characteristic gives spread-spectrum signals a big plus. Spread-spectrum and narrowband signals can occupy the same band, with little or no interference. This capability is the main reason for all the interest in spread spectrum today.

The use of special pseudo noise (PN) codes in spread-spectrum communications makes signals appear wide band and noise-like. It is this very characteristic that makes spread-spectrum signals possess a low LPI. Spread-spectrum signals are hard to detect on narrow band equipment because the signal's energy is spread over a bandwidth of maybe 100 times the information bandwidth**(Figure 1)**.

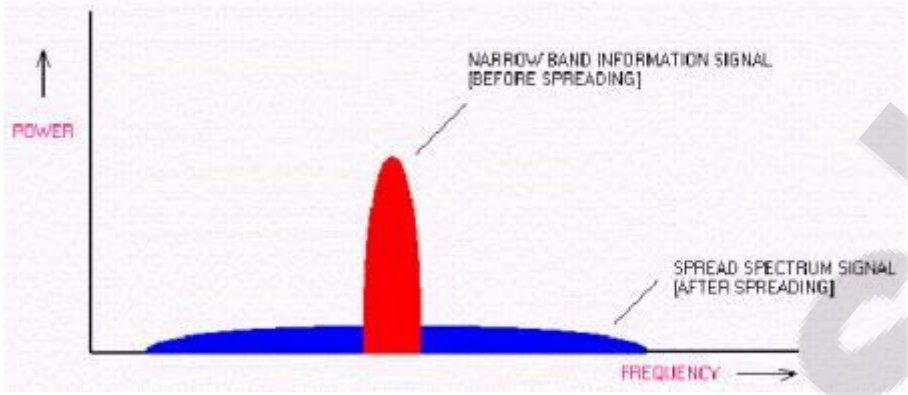


Figure 1: In a spread-spectrum system, signals are spread across a wide bandwidth, making them difficult to intercept, demodulate, and intercept.

The spread of energy over a wide band, or lower spectral power density, also makes spread-spectrum signals less likely to interfere with narrowband communications. Narrowband communications, conversely, cause little to no interference to spread spectrum systems because the correlation receiver effectively integrates over a very wide bandwidth to recover a spread spectrum signal. The correlator then "spreads" out a narrowband interferer over the receiver's total detection bandwidth.

Since the total integrated signal density or signal-to-noise ratio (SNR) at the correlator's input determines whether there will be interference or not. All spread spectrum systems have a threshold or tolerance level of interference beyond which useful communication ceases. This tolerance or threshold is related to the spread-spectrum processing gain, which is essentially the ratio of the RF bandwidth to the information bandwidth.

Frequency Hopping:

Frequency-hopping systems achieve the same results provided by direct-sequence systems by using different carrier frequency at different time. The frequency-hop system's carrier will hop around within the band so that hopefully it will avoid the jammer at some frequencies.

A frequency-hopping signal is shown in **Figure 5**.

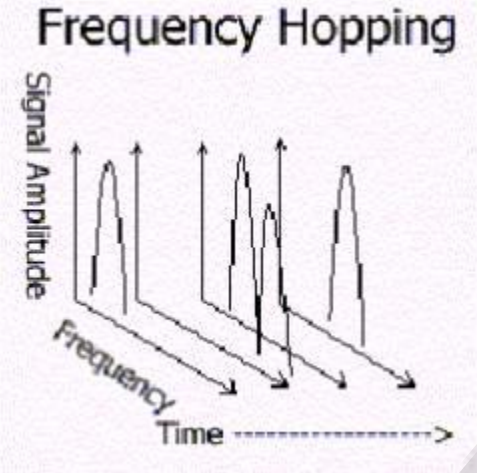


Figure 5: Diagram showing how a frequency-hop system works.

The frequency-hopping technique does not spread the signal, as a result, there is no processing gain. The processing gain is the increase in power density when the signal is de-spread and it will improve the received signal's Signal-to-noise ratio (SNR). In other words, the frequency hopper needs to put out more power in order to have the same SNR as a direct-sequence radio.

The frequency hopper, however, is more difficult to synchronize. In these architectures, the receiver and the transmitter must be synchronized in time and frequency in order to ensure proper transmission and reception of signals. In a direct-sequence radio, on the other hand, only the timing of the chips needs to be synchronized.

The frequency hopper also needs more time to search the signal and lock to it. As a result, the latency time is usually longer. While a direct-sequence radio can lock in the chip sequence in just a few bits.

To make the initial synchronization possible, the frequency hopper will typically park at a fixed frequency before hopping or communication begin. If the jammer happens to locate at the same frequency as the parking frequency, the hopper will not be able to hop at all. And once it hops, it will be very difficult, if not impossible to re-synchronize if the receiver ever lost the sync.

The frequency hopper, however, is better than the direct-sequence radio when dealing with multipath. Since the hopper does not stay at the same frequency and a null at one frequency is usually not a null at another frequency if it is not too close to the original frequency. So a hopper can usually deal with multipath fading issues better than direct-sequence radio.

Slow and Fast Hopping

There are two kinds of frequency hopping

- Slow Frequency Hopping (SFH)
  In this case one or more data bits are transmitted within one hop. An advantage is that coherent data detection is possible. Often, systems using slow hopping also employ (burst) error control coding to restore loss of (multiple) bits in one hop.
- Fast Frequency Hopping (FFH)
  One data bit is divided over multiple hops. In fast hopping, coherent signal detection is difficult, and seldom used. Mostly, FSK or MFSK modulation is used.

Q4: What are convolution codes? Draw an encoder with k=1, n=2, K=3. Give example of its usage.(15m)

Answer:

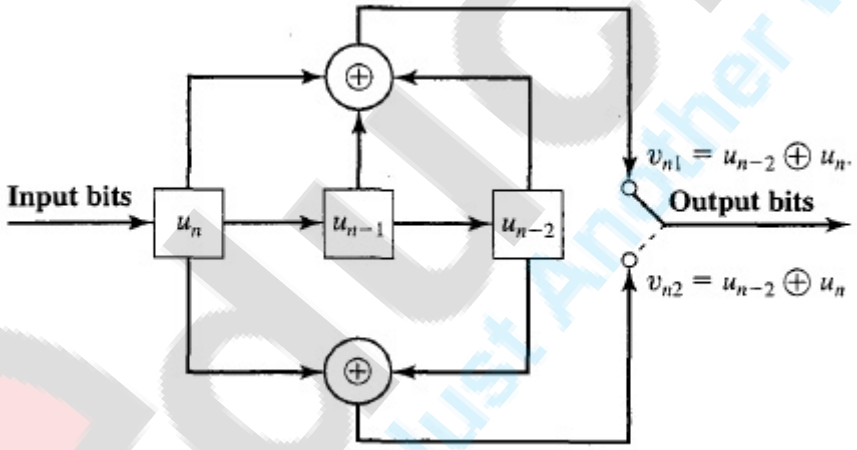
Convolution code:

Block codes are one of the two widely used categories of error correcting codes for wireless transmission; the other is convolutional codes. An *(n, k)* block code process data in
blocks of *k* bits at a time, producing a block of *n* bits *(n > k)* as output for every block of *k* bits as input. If data are transmitted and received in a more or less continuous stream, a block code, particularly one with a large value of *n*, may not be as convenient as a code that generates redundant bits continuously so that error checking and correcting are carried out continuously. This is the function of convolution codes.

A convolutional code is defined by three parameters: *n, k,* and *K.* An *(n, k, K)* code

processes input data *k* bits at a time and produces an output of *n* bits for each incoming *k* bits. So far this is the same as the block code. In the case of a convolutional code, nand *k* are generally quite small numbers. The difference is that convolutional codes have memory, which is characterized by the *constraint factor K*. In essence, the current *n-bit* output of an *(n, k, K)* code depends not only on the value of the current block of *k* input bits but also on the previous *K* – 1 blocks of *k* input bits. Hence, the current output of *n* bits is a function of the last *K* X *k* input bits. Convolutional codes are best understood by looking at a specific example For an *(n, k, K)* code, the shift register contains the most recent *K* X *k* input bits; the register is initialized to all zeros. The encoder produces *n* output bits, after which the oldest *k* bits from the register are discarded and *k* new bits are shifted in. Thus, although the output of *n* bits depends on *K* X *k* input bits, the rate of encoding is *n* output bits per *k* input bits. As in a block code, the code rate is therefore *kin*. The most commonly used binary encoders have *k* = 1 and hence a shift register length of *K*.

Our example is of a (2, 1,3) code (Figure).



In this example, the encoder converts an input bit U_n into two output bits V_{nl} and V_{n2}, using the three most recent bits. The first output bit produced is from the upper logic circuit $(V_{nl} = U_n \oplus U_{n-l} \oplus U_{n-2})$, and the second output bit from the lower logic circuit $(V_{n2} = U_n \oplus U_{n-2})$. For any given input of *k* bits, there are $2k(K-l)$ different functions that map the *k* input bits into *n* output bits. Which function is used depends on the history of the last $(K - 1)$ input blocks of *k* bits each. We can therefore represent a convolutional code using a finite-state machine. The machine has $2k(K-l)$ states, and the transition from one state to another is determined by the most recent *k* bits of inputs and produces *n* output bits. The initial state of the

machine corresponds to the all-zeros state. For our example (Figure) there are 4 states, one for each possible pair of values for the last two bits. The next input bit causes a transition and produces an output of two bits. For example, if the last two bits were 10 ($U_{n-1} = 1$, $U_{n-2} = 0$) and the next bit is 1 ($U_n = 1$), then the current state is state b (10) and the next state is d (11).

The output is $V_{n1} = U_n \oplus U_{n-1} \oplus U_n = 0 \oplus 1 \oplus 1 = 0$ $V_{n2} = 0 \oplus 1 = 1$

Q.6. Explain GSM architecture. What is the role of mobile switching center in roaming?

Answer:

GSM architecture:

GSM is a PLMN (Public Land Mobile Network).

A GSM system consists of three subsystems, the radio sub system (RSS), the network and switching subsystem (NSS), and the operation subsystem (OSS).

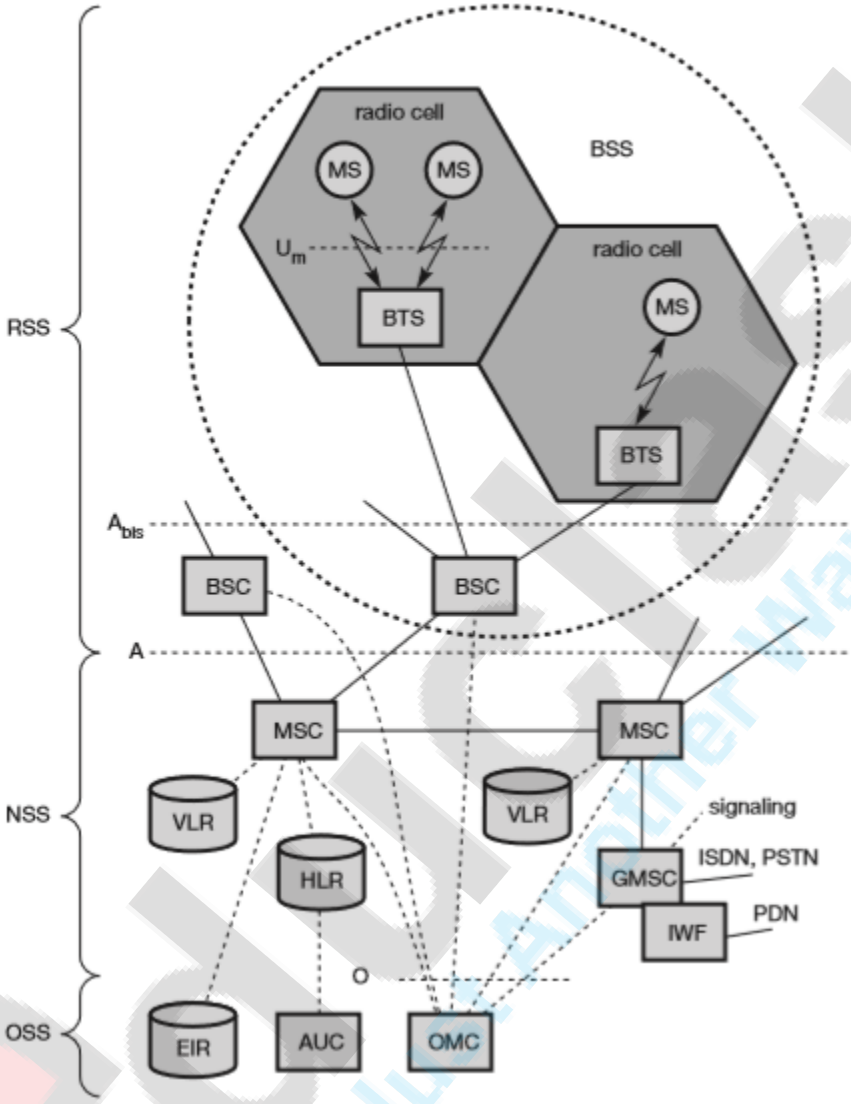


Fig: Functional architecture of GSM.

1) Radio subsystem (RSS)
   The radio subsystem (RSS) comprises all radio specific entities, i.e., the mobile stations (MS) and the base station subsystem (BSS).
   The connection between the RSS and the NSS via the A inter- face (solid lines) and the connection to the OSS via the O interface (dashed lines).

The A interface is typically based on circuit-switched PCM-30 systems (2.048 Mbit/s), carrying up to 30 64 kbit/s connections, whereas the O interface uses the Signalling System No. 7 (SS7) based on X.25 carrying management data to/from the RSS.

- Base station subsystem (BSS): A GSM network comprises many BSSs, each controlled by a base station controller (BSC). The BSS performs all functions necessary to maintain radio connections to an MS, coding/decoding of voice, and rate adaptation to/from the wireless network part. Besides a BSC, the BSS contains several BTSs.
- Base transceiver station (BTS): A BTS comprises all radio equipment, i.e., antennas, signal processing, amplifiers necessary for radio transmission. A BTS can form a radio cell or, using sectorized antennas, several cells and is connected to MS via the Um interface (ISDN U interface for mobile use), and to the BSC via the Abis interface. The Um interface contains all the mechanisms necessary for wireless transmission (TDMA, FDMA etc.). The Abis interface consists of 16 or 64 kbit/s connections. A GSM cell can measure between some 100 m and 35 km depending on the environment (buildings, open space, mountains etc.) but also expected traffic.
- Base station controller (BSC): The BSC basically manages the BTSs. It reserves radio frequencies, handles the handover from one BTS to another within the BSS, and performs paging of the MS. The BSC also multiplexes the radio channels onto the fixed network connections at the A interface.
- Mobile station (MS): The MS comprises all user equipment and software needed for communication with a GSM network. An MS consists of user independent hard- and software and of the subscriber identity module (SIM), which stores all user-specific data that is relevant to GSM. While an MS can be identified via the international mobile equipment identity (IMEI), a user can personalize any MS using his or her SIM, i.e., user-specific mechanisms like charging and authentication are based on the

SIM, not on the device itself. Device-specific mechanisms, e.g., theft protection, use the device specific IMEI. Without the SIM, only emergency calls are possible. The SIM card contains many identifiers and tables, such as card-type, serial number, a list of subscribed services, a personal identity number (PIN), a PIN unblocking key (PUK), an authentication key Ki, and the international mobile subscriber identity (IMSI). The PIN is used to unlock the MS. Using the wrong PIN three times will lock the SIM. In such cases, the PUK is needed to unlock the SIM. The MS stores dynamic information while logged onto the GSM system, such as, e.g., the cipher key Kc and the location information consisting of a temporary mobile subscriber identity (TMSI) and the location area identification (LAI). Apart from the telephone interface, an MS can also offer other types of interfaces to users with display, loudspeaker, microphone, and programmable soft keys.

2) Network and switching subsystem(NSS)

The "heart" of the GSM system is formed by the network and switching sub-system (NSS). The NSS connects the wireless network with standard public networks, performs handovers between different BSSs, comprises functions for worldwide localization of users and supports charging, accounting, and roaming of users between different providers in different countries. The NSS consists of the following switches and databases:

- Mobile services switching center (MSC): MSCs are high-performance digital ISDN switches. They set up connections to other MSCs and to the BSCs via the A interface, and form the fixed backbone network of a GSM system. Typically, an MSC manages several BSCs in a geographical region. A gateway MSC (GMSC) has additional connections to other fixed networks, such as PSTN and ISDN. Using additional interworking functions (IWF), an MSC can also connect to public data networks (PDN) such as X.25. An MSC handles all signaling needed for connection setup, connection release and handover of

connections to other MSCs. An MSC also performs all functions needed for supplementary services such as call forwarding, multi-party calls, reverse charging etc.

- Home location register (HLR): The HLR is the most important database in a GSM system as it stores all user-relevant information. This comprises static information, such as the mobile subscriber ISDN number (MSISDN), sub- scribed services (e.g., call forwarding, roaming restrictions, GPRS), and the international mobile subscriber identity (IMSI). Dynamic information is also needed, e.g., the current location area (LA) of the MS, the mobile sub- scriber roaming number (MSRN), the current VLR and MSC. As soon as an MS leaves its current LA, the information in the HLR is updated. This information is necessary to localize a user in the worldwide GSM network. All these user-specific information elements only exist once for each user in a single HLR, which also supports charging and accounting. HLRs can manage data for several million customers and contain highly specialized data bases which must fulfill certain real-time requirements to answer requests within certain time-bounds.
- Visitor location register (VLR): The VLR associated to each MSC is a dynamic database which stores all important information needed for the MS users currently in the LA that is associated to the MSC (e.g., IMSI, MSISDN, HLR address). If a new MS comes into an LA the VLR is responsible for, it copies all relevant information for this user from the HLR. This hierarchy of VLR and HLR avoids frequent HLR updates and long-distance signaling of user information. Some VLRs in existence, are capable of managing up to one million customers.

3) Operation subsystem(OSS)

The third part of a GSM system, the operation subsystem (OSS), contains the necessary functions for network operation and maintenance. The OSS

possesses network entities of its own and accesses other entities via SS7 signaling. The following entities have been defined:

- Operation and maintenance center (OMC): The OMC monitors and controls all other network entities via the O interface. Typical OMC management functions are traffic monitoring, status reports of network entities, subscriber and security management, or accounting and billing. OMCs use the concept of telecommunication management network (TMN) as standardized by the ITU-T.
- Authentication centre (AuC): As the radio interface and mobile stations are particularly vulnerable, a separate AuC has been defined to protect user identity and data transmission. The AuC contains the algorithms for authentication as well as the keys for encryption and generates the values needed for user authentication in the HLR. The AuC may, in fact, be situated in a special protected part of the HLR.
- Equipment identity register (EIR): The EIR is a database for all IMEIs, i.e., it stores all device identifications registered for this network. As MSs are mobile, they can be easily stolen. With a valid SIM, anyone could use the stolen MS. The EIR has a blacklist of stolen (or locked) devices. In theory an MS is useless as soon as the owner has reported a theft. Unfortunately, the blacklists of different providers are not usually synchronized and the illegal use of a device in another operator's network is possible (the reader may speculate as to why this is the case). The EIR also contains a list of valid IMEIs (white list), and a list of malfunctioning devices (gray list).

Role of Mobile Switching Center(MSC) in Roaming:

- The HLR always contains information about the current location (only the location area, not the precise geographical location), and the VLR currently responsible for the MS informs the HLR about location changes.
- As soon as an MS moves into the range of a new VLR (a new location area), the HLR sends all user data needed to the new VLR.

- Changing VLRs with uninterrupted availability of all services is also called **roaming**.
- Roaming can take place within the network of one provider, between two providers in one country (national roaming is, often not supported due to competition between operators), but also between different providers in different countries (international roaming).

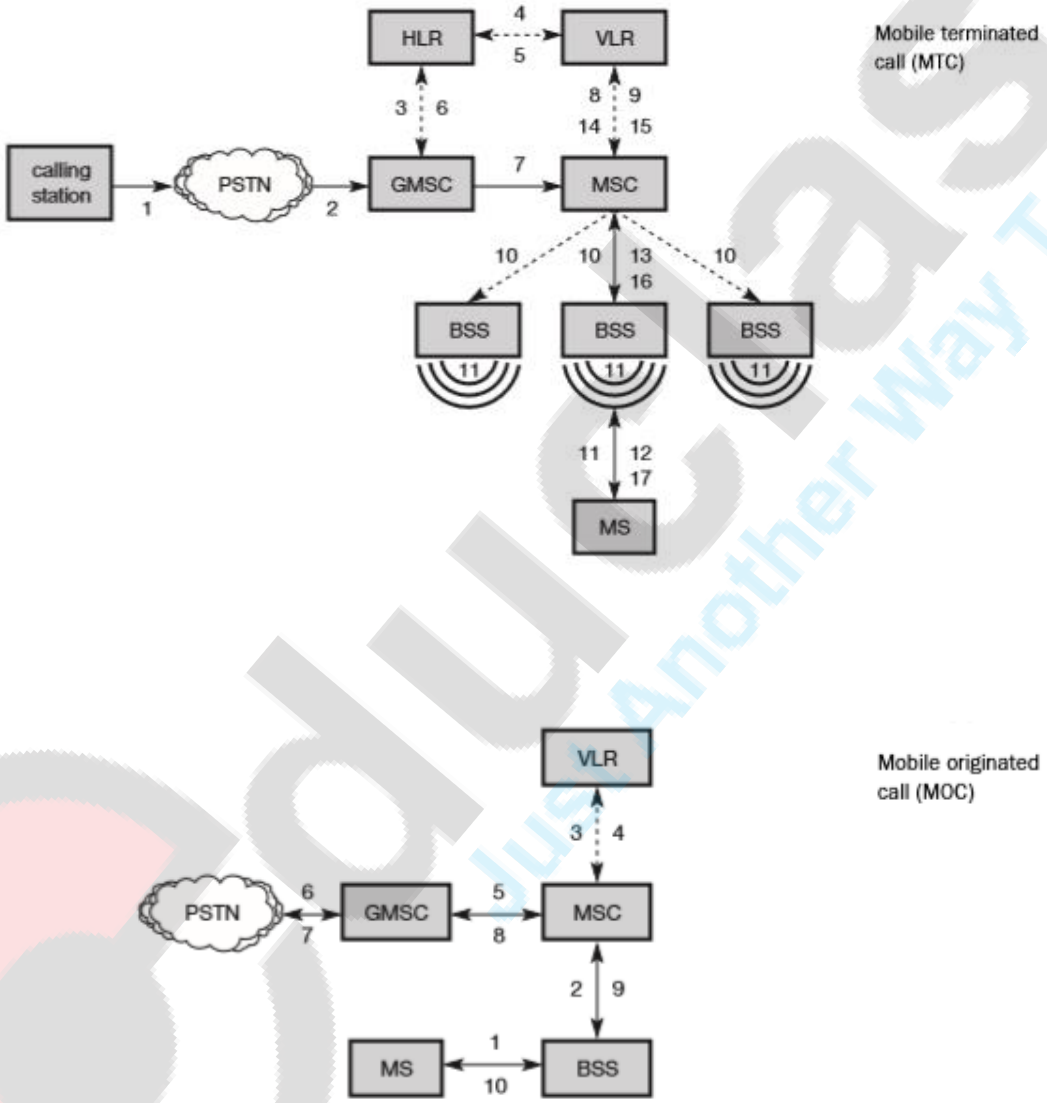
Mobile Terminated Call (MTC)

- MTC is a situation in which a station calls a mobile station (the calling station could be outside the GSM network or another mobile station). Below figure shows the basic steps needed to connect the calling station with the mobile user.

1) A user dials the phone number of a GSM subscriber.
2) The fixed network (PSTN) notices (looking at the destination code) that the number belongs to a user in the GSM network and forwards the call setup to the Gateway MSC.
3) The GMSC identifies the HLR for the subscriber (which is coded in the phone number) and signals the call setup to the HLR.
4) The HLR now checks whether the number exists and whether the user has subscribed to the requested services, and requests an MSRN from the current VLR.
5) & 6) After receiving the MSRN, the HLR can determine the MSC responsible for the MS and forwards this information to the GMSC.
7) The GMSC can now forward the call setup request to the MSC indicated.
8) From this point on, the MSC is responsible for all further steps. First, it requests the current status of the MS from the VLR.
9) & 10) If the MS is available, the MSC initiates paging in all cells it is responsible for (i.e. the location area, LA), as searching for the right cell would be too time consuming (but this approach puts some load on the signaling channels so optimizations exist).
11) The BTSs of all BSSs transmit this paging signal to the MS.

12) & 13) If the MS answers, the VLR has to perform security checks (set up encryption etc.).

14-17) The VLR then signals to the MSC to set up a connection to the MS.



Mobile Originated Call (MOC)

It is much simpler to perform a mobile originated call (MOC) compared to a MTC.

1) The MS transmits a request for a new connection
2) The BSS forwards this request to the MSC.
3) & 4) The MSC then checks if this user is allowed to set up a call with the requested service and checks the availability of resources through the GSM network and into the PSTN. If all resources are available, the MSC sets up a connection between the MS and the fixed network.

Q.7) Describe WIMAX network reference model along with its features.(10 m)

The network reference model envisions a unified network architecture for supporting fixed, nomadic, and mobile deployments and is based on an IP service model. Below is simplified illustration of an IP-based WiMAX network architecture. The overall network may be logically divided into three parts:

- Mobile Stations (MS) used by the end user to access the network.
- The access service network (ASN), which comprises one or more base stations and one or more ASN gateways that form the radio access network at the edge.
- Connectivity service network (CSN), which provides IP connectivity and all the IP core network functions.

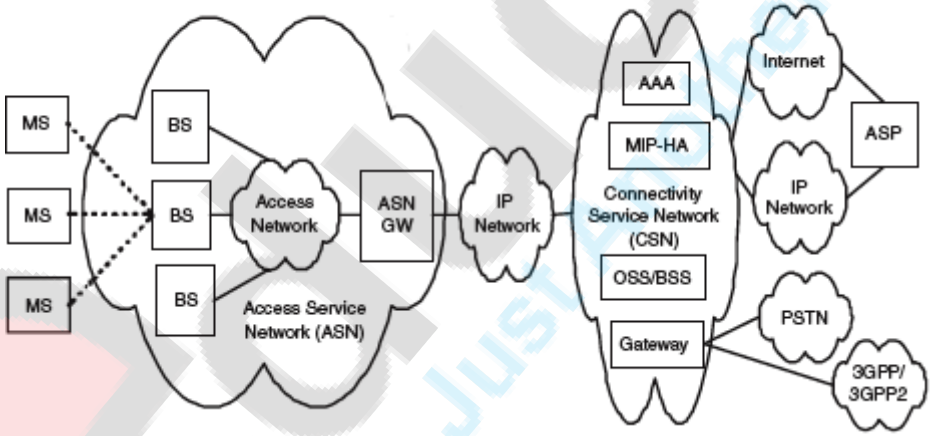
The network reference model developed by the WiMAX Forum NWG defines a number of functional entities and interfaces between those entities. Fig below shows some of the more important functional entities.

- **Base station (BS):** The BS is responsible for providing the air interface to the MS. Additional functions that may be part of the BS are micromobility management functions, such as handoff triggering and tunnel establishment, radio resource management, QoS policy enforcement, traffic classification, DHCP

(Dynamic Host Control Protocol) proxy, key management, session management, and multicast group management.

- **Access service network gateway (ASN-GW):** The ASN gateway typically acts as a layer 2 traffic aggregation point within an ASN. Additional functions that may be part of the ASN gateway include intra-ASN location management and paging, radio resource management, and admission control, caching of subscriber profiles, and encryption keys, AAA client functionality, establishment, and management of mobility tunnel with base stations, QoS and policy enforcement, foreign agent functionality for mobile IP, and routing to the selected CSN.
- **Connectivity service network (CSN):** The CSN provides connectivity to the Internet, ASP, other public networks, and corporate networks. The CSN is owned by the NSP and includes AAA servers that support authentication for the devices, users, and specific services. The CSN also provides per user policy management of QoS and security. The CSN is also responsible for IP address management, support for roaming between different NSPs, location management between ASNs, and mobility and roaming between ASNs.

IP-Based WiMAX Network Architecture



The WiMAX architecture framework allows for the flexible decomposition and/or combination of functional entities when building the physical entities. For example, the ASN may be decomposed into base station transceivers (BST), base station controllers (BSC), and an ASNGW analogous to the GSM model of BTS, BSC, and Serving GPRS Support Node (SGSN).

WiMAX is a wireless broadband solution that offers a rich set of features with a lot of flexibility in terms of deployment options and potential service offerings. Some of the more salient features that deserve highlighting are as follows:

1) OFDM-based physical layer:

Orthogonal frequency division multiple access (OFDM)

The WiMAX physical layer (PHY) is based on orthogonal frequency division multiplexing, a scheme that offers good resistance to multipath, and allows WiMAX to operate in NLOS conditions.

2) Very high peak data rates:

WiMAX is capable of supporting very high peak data rates. In fact, the peak PHY data rate can be as high as 74Mbps when operating using a 20MHz wide spectrum.

More typically, using a 10MHz spectrum operating using TDD scheme with a 3:1 downlink-to-uplink ratio, the peak PHY data rate is about 25Mbps and 6.7Mbps for the downlink and the uplink, respectively.

3) Scalable bandwidth and data rate support:

WiMAX has a scalable physical-layer architecture that allows for the data rate to scale easily with available channel bandwidth.

For example, a WiMAX system may use 128, 512, or 1,048-bit FFTs (fast fourier transforms) based on whether the channel bandwidth is 1.25MHz, 5MHz, or 10MHz, respectively. This scaling may be done dynamically to support user roaming across different networks that may have different bandwidth allocations.

4) Adaptive modulation and coding (AMC):

WiMAX supports a number of modulation and forward error correction (FEC) coding schemes and allows the scheme to be changed on a per user and per frame basis, based on channel conditions.

AMC is an effective mechanism to maximize throughput in a time-varying channel.

5) Link-layer retransmissions:

WiMAX supports automatic retransmission requests (ARQ) at the link layer for connections that require enhanced reliability. ARQ-enabled connections require each transmitted packet to be acknowledged by the receiver; unacknowledged packets are assumed to be lost and are retransmitted.

6) Support for TDD and FDD:

IEEE 802.16-2004 and IEEE 802.16e-2005 supports both time division duplexing and frequency division duplexing, as well as a half-duplex FDD, which allows for a low-cost system implementation.

7) WiMAX uses OFDM:

Mobile WiMAX uses Orthogonal frequency division multiple access (OFDM) as a multiple-access technique, whereby different users can be allocated different subsets of the OFDM tones.

8) Flexible and dynamic per user resource allocation:

Both uplink and downlink resource allocation are controlled by a scheduler in the base station. Capacity is shared among multiple users on a demand basis, using a burst TDM scheme.

9) Support for advanced antenna techniques:

The WiMAX solution has a number of hooks built into the physical-layer design, which allows for the use of multiple-antenna techniques, such as beamforming, space-time coding, and spatial multiplexing.

10) Quality-of-service support:

The WiMAX MAC layer has a connection-oriented architecture that is designed to support a variety of applications, including voice and multimedia services.

WiMAX system offers support for constant bit rate, variable bit rate, real-time, and non-real-time traffic flows, in addition to best-effort data traffic.

WiMAX MAC is designed to support a large number of users, with multiple connections per terminal, each with its own QoS requirement.

11) Robust security:

WiMAX supports strong encryption, using Advanced Encryption Standard (AES), and has a robust privacy and key-management protocol.

The system also offers a very flexible authentication architecture based on Extensible Authentication Protocol (EAP), which allows for a variety of user credentials, including username/password, digital certificates, and smart cards.

12) Support for mobility:

The mobile WiMAX variant of the system has mechanisms to support secure seamless handovers for delay-tolerant full-mobility applications, such as VoIP.

13) IP-based architecture:

The WiMAX Forum has defined a reference network architecture that is based on an all-IP platform. All end-to-end services are delivered over an IP architecture relying on IP-based protocols for end-to-end transport, QoS, session management, security, and mobility.

Q.10) Write short notes on:
a) Mobile IP
b) GPRS
c) Antenna
d) WCDMA

Answer:

A) Mobile IP:

- A standard that allows users with mobile devices whose IP addresses are associated with one network to stay connected when moving to a network with a different IP address.
- When a user leaves the network with which his device is associated (home network) and enters the domain of a foreign network, the foreign network uses the Mobile IP protocol to inform the home network of a care-of address to which all packets for the user's device should be sent.
- Mobile IP is most often found in wireless WAN environments where users need to carry their mobile devices across multiple LANs with different IP addresses.

Requirements for Mobile IP:

- **Transparency**
  - Mobile end-systems keep their IP address
  - Continuation of communication after interruption of link possible
  - Point of connection to the fixed network can be changed
- **Compatibility**
  - Support of the same layer 2 protocols as IP
  - No changes to current end-systems and routers required
  - Mobile end-systems can communicate with fixed systems
- **Security**
  - Authentication of all registration messages
- **Efficiency and scalability**
  - Only little additional messages to the mobile system required (connection typically via a low bandwidth radio link)
  - World-wide support of a large number of mobile systems in the whole Internet

Terminologies used in Mobile IP:

- **Mobile Node (MN)**
  - System (node) that can change the point of connection to the network without changing its IP address
- **Home Agent (HA)**
  - System in the home network of the MN, typically a router

- Registers the location of the MN, tunnels IP datagrams to the COA

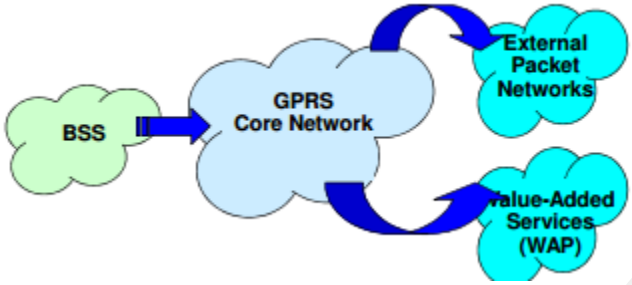
- **Foreign Agent (FA)**
  - System in the current foreign network of the MN, typically a router
  - Forwards the tunneled datagrams to the MN, typically also the default router for the MN
- **Care-of Address (COA)**
  - Address of the current tunnel end-point for the MN (at FA or MN)
  - Actual location of the MN from an IP point of view
  - Can be chosen, e.g., via DHCP
- **Correspondent Node (CN)**
  - Communication partner

Problems with Mobile IP :

- **Security**
  - Authentication with FA problematic, for the FA typically belongs to another organization
  - No protocol for key management and key distribution has been standardized in the Internet
  - Patent and export restrictions
- **Firewalls**
  - Typically mobile IP cannot be used together with firewalls, special set-ups are needed (such as reverse tunneling)
- **Qos**
  - Many new reservations in case of RSVP
  - Tunneling makes it hard to give a flow of packets a special treatment needed for the qos

B) GPRS:

- GPRS provides mobile users worldwide access to
  - Value-added WAP services and
  - Different external packet networks (e.g. Internet or intranets)

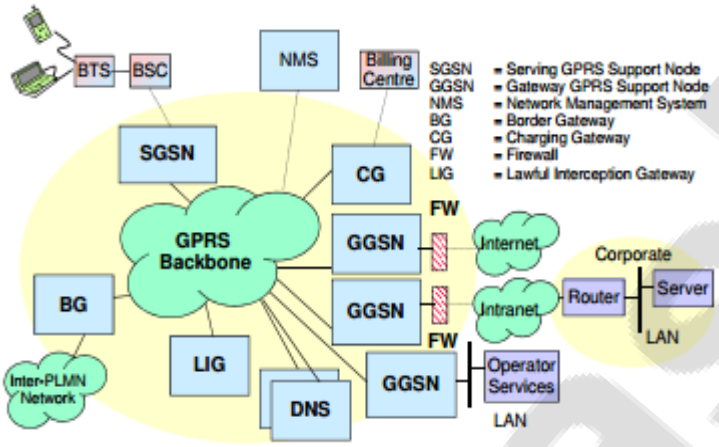


- GPRS uses a packet-based technique which will enhance GSM data services significantly, especially for bursty Internet/intranet traffic.
- Technology which permits mobile data communication using packet switching techniques
- **GSM allows circuit switched (CS) data transfer**
    - Data transfer on a dedicated channel (connection oriented)
    - Connection setup procedure needed as in modem
    - Subscriber charged according to time of connection
    - TS is held for duration of connection - waste of resources
- **GPRS designed as an extension to digital cellular networks**
    - Connectionless packet switched (PS) data service
    - Standardised by ETSI
    - Radio resources shared between CS and PS data
    - New terminals are required

<u>GPRS network elements:</u>

- ‰ GSN (GPRS Support Nodes): GGSN and SGSN
- ‰ GGSN (Gateway GSN)
    - interworking unit between GPRS and PDN (Packet Data Network)
- ‰ SGSN (Serving GSN)
    - supports the MS (location, billing, security)
- GR (GPRS Register)
    - user addresses

GPRS Architecture



Advantages:

- The main advantages of GPRS for users:
  - Instant access to data as if connected to an office LAN
  - Charging based on amount of data transferred (not the time connected)
  - Higher transmission speeds
- The main advantages for operators:
  - Fast network roll-out with minimum investment
  - Excess voice capacity used for GPRS data
  - Smooth path to 3G services

C) Antenna

Antennas**:**

- Helps to get rid of wires.
- Transmits signals through space without guidance
- Couple the energy from the transmitter to the outside world and vice versa.

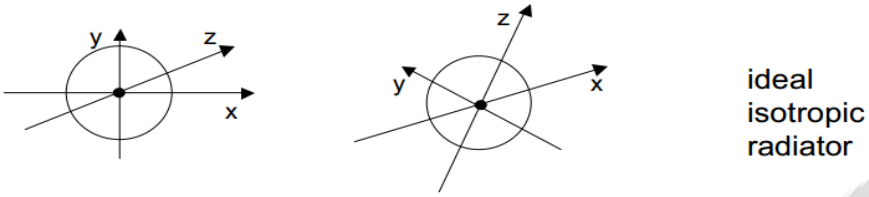
Antennas couple electromagnetic energy to and from space to and from wire or a coaxial cable.

Antennas transform wire propagated waves into space propagated waves.

They receive electromagnetic waves and pass them onto a receiver or they transmit electromagnetic waves which have been produced by a transmitter.

Antennas: isotropic radiator

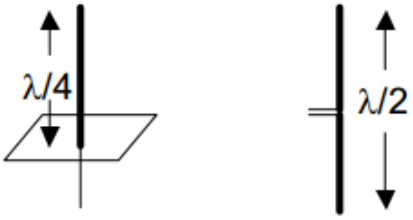
- A theoretical reference antenna is the isotropic radiator, a point in space radiating equal power in all directions, i.e. all points with equal power are located on a sphere with the antenna as its center.
- The radiation pattern is symmetric in all directions.



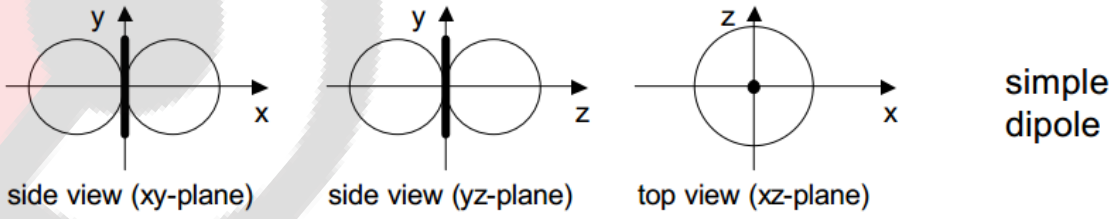
ideal isotropic radiator

Antennas: simple dipoles

Real antennas are not isotropic radiators, they exhibit directive effects, i.e., the intensity of radiation is not the same in all directions from the antenna.
The simplest real antenna is a thin, center-fed dipole, also called Hertzian dipole.



The dipole consists of two collinear conductors of equal length, separated by a small feeding gap.
The length of the dipole is not arbitrary but for example, half the wavelength l of the signal to transmit results in a very efficient radiation of the energy.
It mounted on the root of car; the length of l/4 is efficient. This is also known as Marconi antenna.
A l/2 dipole has a uniform or Omni-directional radiation pattern in one plane and a figure eight pattern in the other two planes as shown in following figure.

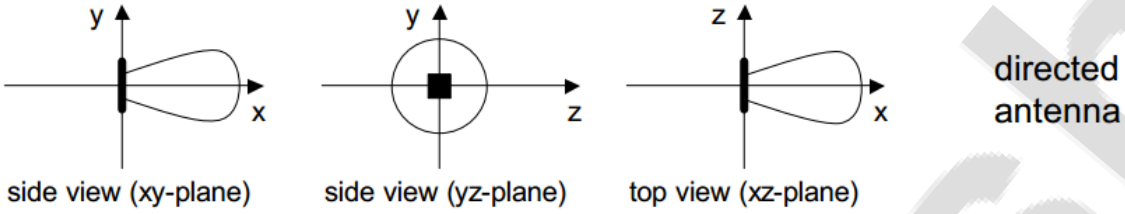


side view (xy-plane) side view (yz-plane) top view (xz-plane)

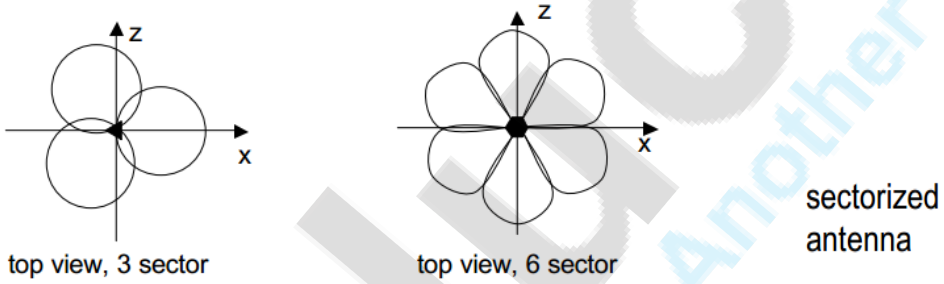
simple dipole

Antennas: directed and sectorized

If an antenna is positioned, an omnidirectional radiation pattern is not very useful.

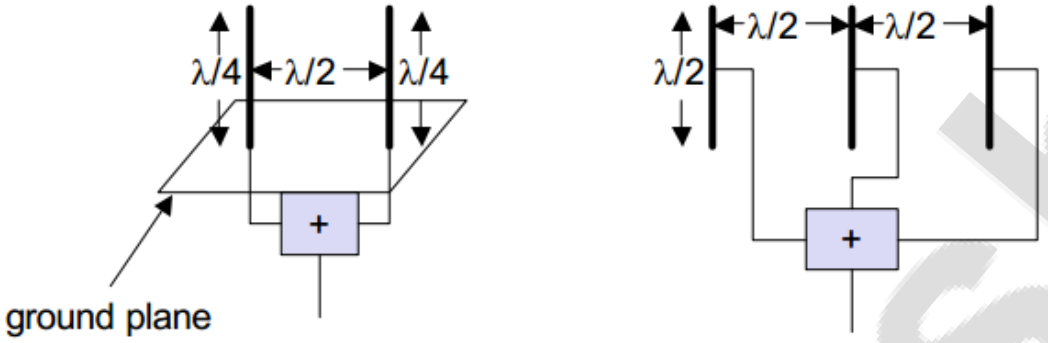


Directed antennas are typically applied in cellular systems as presented in above section.
Several directed antennas can be combined on a single pole to construct a sectorized antenna.
A cell can be sectorized into 3 or 6 sectors, thus enabling frequency reuse as explained in above section.
Below figure shows the radiation patterns of these sectorized antennas.



Antennas: diversity

- Grouping of 2 or more antennas :
  - multi-element antenna arrays
- Antenna diversity
  - switched diversity, selection diversity
    - receiver chooses antenna with largest output
  - diversity combining
    - combine output power to produce gain
    - cophasing needed to avoid cancellation

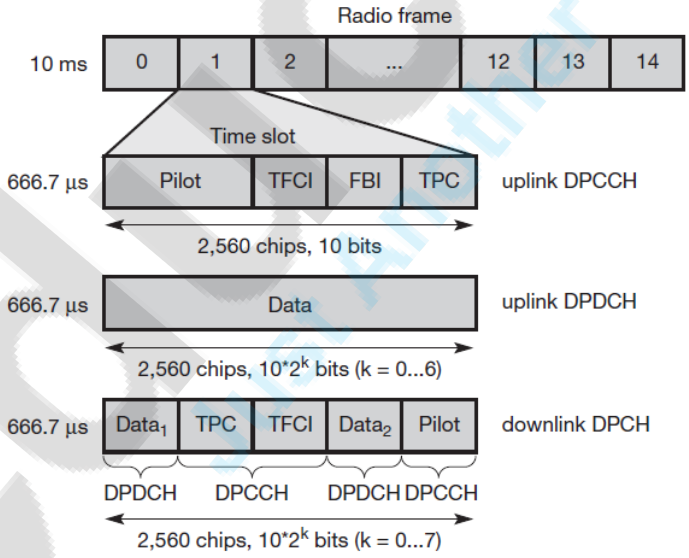


D) WCDMA:

The FDD mode for UTRA uses wideband CDMA (W-CDMA) with direct sequence spreading. As implied by FDD, uplink and downlink use different frequencies.

Time slots in W-CDMA are not used for user separation but to support periodic functions.

Figure 4.28
UTRA FDD (W-CDMA) frame structure



Back to the frame structure shown in Figure 4.28. Similar to GSM, UMTS defines many logical and physical channels, and their mapping. The figure shows three examples of physical channels as they are used for data transmission.

Two physical channels are shown for the uplink.

- **Dedicated physical data channel (DPDCH):** This channel conveys user or signaling data. The spreading factor of this channel can vary between 4 and 256.

This directly translates into the data rates this channel can offer: 960 kbit/s (spreading factor 4, 640 bits per slot, 15 slots per frame, 100 frames per second), 480, 240, 120, 60, 30, and 15 kbit/s (spreading factor 256). This also shows one of the problems of using OVSF for spreading: only certain multiples of the basic data rate of 15 kbit/s can be used. If, for example, 250 kbit/s are needed the device has to choose 480 kbit/s, which wastes bandwidth. In each connection in layer 1 it can have between zero and six DPDCHs. This results in a theoretical maximum data rate of 5,740 kbit/s (UMTS describes UEs with a maximum of 1,920 kbit/s only). Table 4.7 shows typical user data rates together with the required data rates on the physical channels.

● **Dedicated physical control channel (DPCCH):** In each connection layer 1 needs exactly one DPCCH. This channel conveys control data for the physical layer only and uses the constant spreading factor 256. The **pilot** is used for channel estimation. The **transport format combination identifier (TFCI)** specifies the channels transported within the DPDCHs. Signaling for a soft handover is supported by the **feedback information field (FBI)**. The last field, **transmit power control (TPC)** is used for controlling the transmission power of a sender. Power control is performed in each slot, thus 1,500 power control cycles are available per second. Tight power control is necessary to mitigate near-far-effects as explained in chapter 2. Six different DPCCH bursts have been defined which differ in the size of the fields.

● **Dedicated physical channel (DPCH):** The downlink time multiplexes control and user data. Spreading factors between 4 and 512 are available. Again, many different burst formats (17 altogether) have been defined which differ in the size of the field shown in Figure 4.28. The available data rates for data channels (DPDCH) within a DPCH are 6 (SF=512), 24, 51, 90, 210, 432, 912,and 1,872 kbit/s (SF=4).

User data rate [kbit/s]	12.2 (voice)	64	144	384
DPDCH [kbit/s]	60	240	480	960
DPCCH [kbit/s]	15	15	15	15
Spreading	64	16	8	4

Table 4.7 Typical UTRA–FDD uplink data rates

While no collisions can occur on the downlink (only the base station sends on the downlink), medium access on the uplink has to be coordinated. A **physical random access channel (PRACH)** is used for this purpose. UTRA-FDD defines 15 random access slots within 20 ms; within each access slot 16 different access preambles can be used for random access. Using slotted Aloha, a UE can access an access slot by sending a preamble. The UE starts with the lowest available transmission power to avoid interfering with other stations. If no positive acknowledgement is received, the UE tries another slot and another preamble with the next higher power level (power ramping). The number of available access slots can be defined per cell and is transmitted via a broadcast channel to all UEs. A UE has to perform the following steps during the **search for a cell** after power on:

- **Primary synchronization:** A UE has to synchronize with the help of a 256 chip primary synchronization code. This code is the same for all cells and helps to synchronize with the time slot structure.
- **Secondary synchronization:** During this second phase the UE receives a secondary synchronization code which defines the group of scrambling codes used in this cell. The UE is now synchronized with the frame structure.
- **Identification of the scrambling code:** The UE tries all scrambling codes within the group of codes to find the right code with the help of a correlator. After these three steps the UE can receive all further data over a broadcast channel.