Name of the Subject: **WIRELESS COMMUNICATIONS & NETWORKS**

Class : **IV B.Tech I Sem**

Branch: **Electronics and Communication Engineering**

**Prepared By**

Dr K RIYAZUDDIN

Associate Professor

Department of ECE

# UNIT I

## INTRODUCTION TO WIRELESS COMMUNICATIONS AND MULTIPLE ACCESS TECHNIQUES

# Evolution of Mobile Radio Communications

Wireless communication is having its fastest growth period in history, due to enabling technologies.

Growth in the mobile communication field has started slowly associated with technological improvements.

Bell Laboratories developed the cellular concept in the 1960's and 1970's.

Till that the ability to provide wireless communications to an entire population was not even conceived.

# Major Wireless Standards

- Wireless WLANs and PANs
  - HIPERLANs,
  - IEEE 802.15 (Bluetooth)
- Fixed Broadcast Systems
  - DVB(digital video broadcasting), DAB(Digital audio broadcasting)
  - Satellite radio
  - Local Multipoint Distribution Service(26-32 GHz)
- Cellular Systems
- Cordless Phones

# Why Wireless?

- **Benefits**
  - Mobility: Ability to communicate anywhere!!
  - Easier configuration, set up and lower installation cost
- **Difficulties**
  - Communication medium: Free space
    - Noisy and unpredictable channel
    - Broadcast channel, more user ->less BW per user
  - Higher equipment cost
  - Need backbone systems in order to function properly

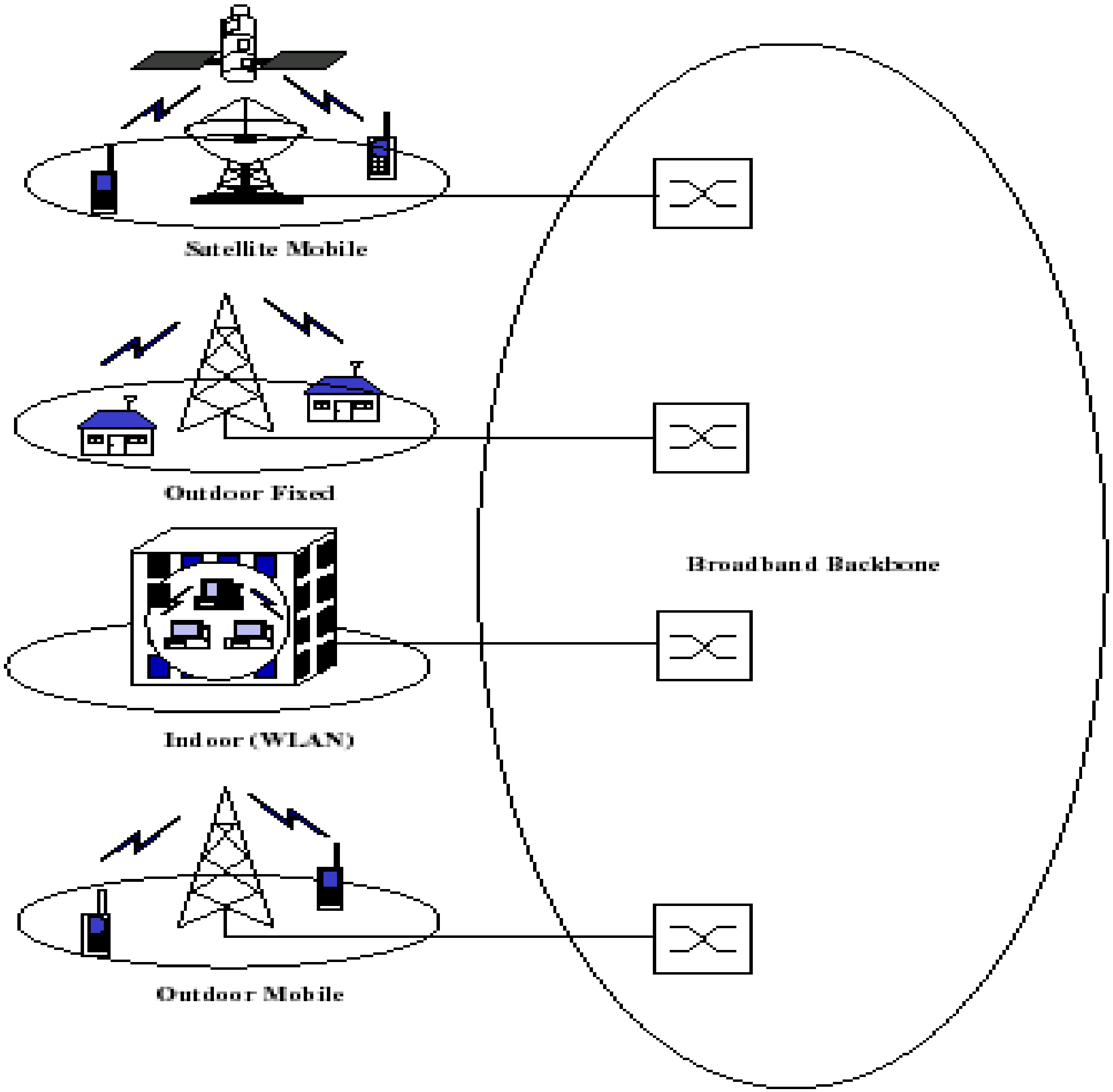
# Wireless Services

Satelite

Outdoor Fixed

Indoor (WLAN)

Outdoor Mobile



# Market penetration

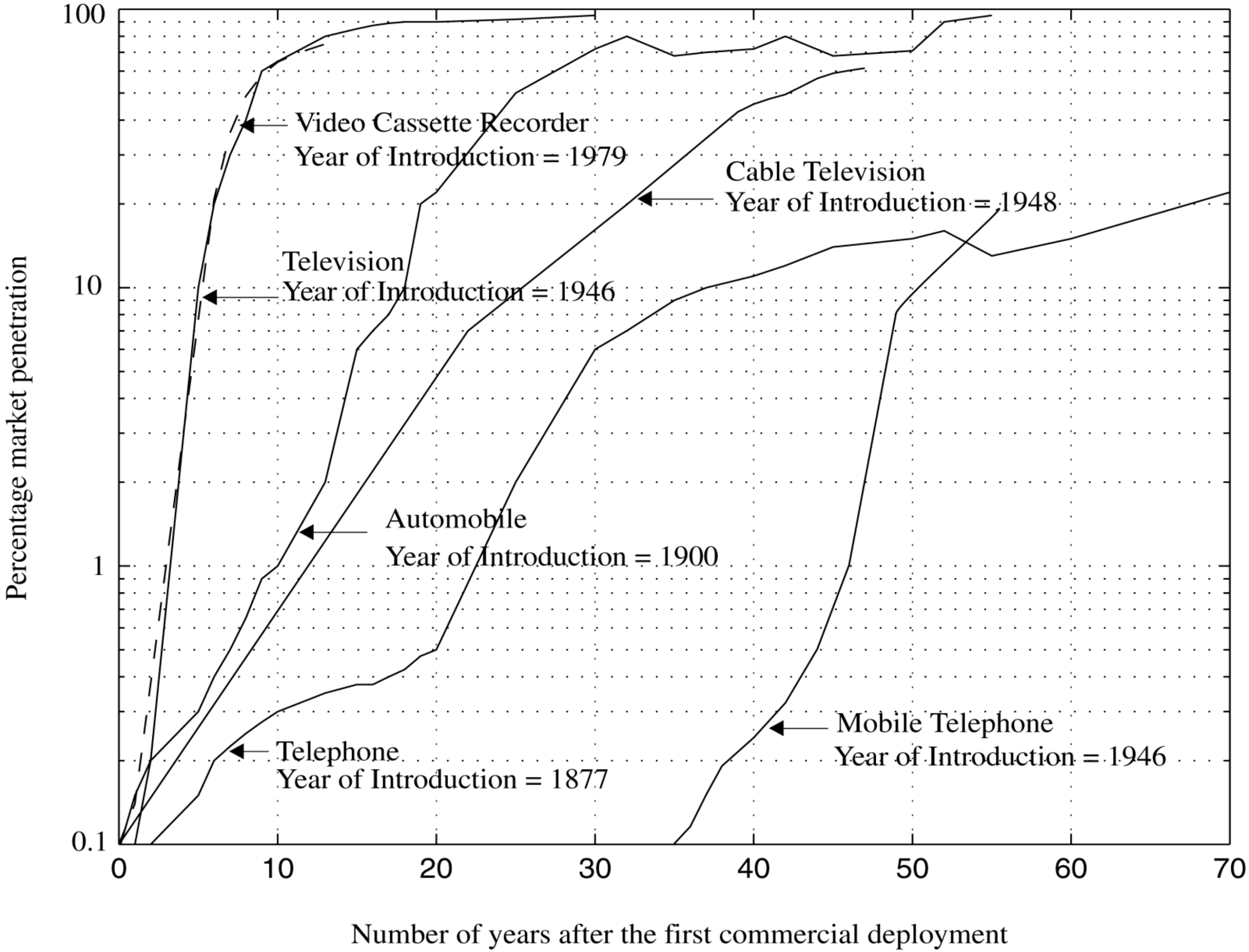



Figure 1.1 The growth of mobile telephony as compared with other popular inventions of the 20th century.

# EXAMPLES OF WIRELESS COMMUNICATION SYSTEMS

- Most people are familiar with a number of mobile radio communication systems used in everyday life.
- Remote controllers for home equipment, cordless telephones, walkie-talkies, pagers and cellular telephones are all examples of mobile radio communication systems.
- However, the cost, complexity, performance and types of services are vastly different.
- The term mobile has been used to classify any radio terminal that could be moved during operation.

# Wireless Communications System Definitions

- **Base Station -** A fixed station in a mobile radio system used for radio communication with mobile stations. Base stations are located at the center or on the edge of a coverage region and consist of radio channels and transmitter and receiver antennas mounted on a tower.
- **Control Channel -** Radio channels used for transmission of call setup, call request, call initiation, and other beacon or control purposes.
- **Forward Channel -** Radio channel used for transmission of information from the base station to the mobile.
- **Full Duplex Systems -** Communication systems which allow simultaneous two-way communication. Transmission and reception is typically on two different channels (FDD) although new cordless/PCS systems are using TDD.
- **Half Duplex Systems -** Communication systems which allow two-way communication by using the same radio channel for both transmission and reception. At any given time, the user can only either transmit or receive information.

- **Mobile Switching Center -** Switching center which coordinates the routing of calls in a large service area. In a cellular radio system, the MSC connects the cellular base stations and the mobiles to the PSTN. An MSC is also called a mobile telephone switching office (MTSO).
- **Page -** A brief message which is broadcast over the entire service area, usually in a simulcast fashion by many base stations at the same time.
- **Reverse Channel -** Radio channel used for transmission of information from the mobile to base station.
- **Roamer -** A mobile station which operates in a service area (market) other than that from which service has been subscribed.
- **Simplex Systems -** Communication systems which provide only one-way communication.
- **Subscriber -** A user who pays subscription charges for using a mobile communications system.
- **Transceiver -** A device capable of simultaneously transmitting and receiving radio signals.

- **Handoff -** The process of transferring a mobile station from one channel or base station to another.
- **Mobile Station -** A station in the cellular radio service intended for use while in motion at unspecified locations. Mobile stations may be hand-held personal units (portables) or installed in vehicles (mobiles).

# 1. Paging Systems

Paging systems are communication systems that send brief messages to a subscriber. Depending on the type of service, the message may be either a numeric message, an alphanumeric message, or a voice message.

Paging systems are typically used to notify a subscriber of the need to call a particular telephone number or travel to a known location to receive further instructions.

The issued message is called a page.

# Paging system

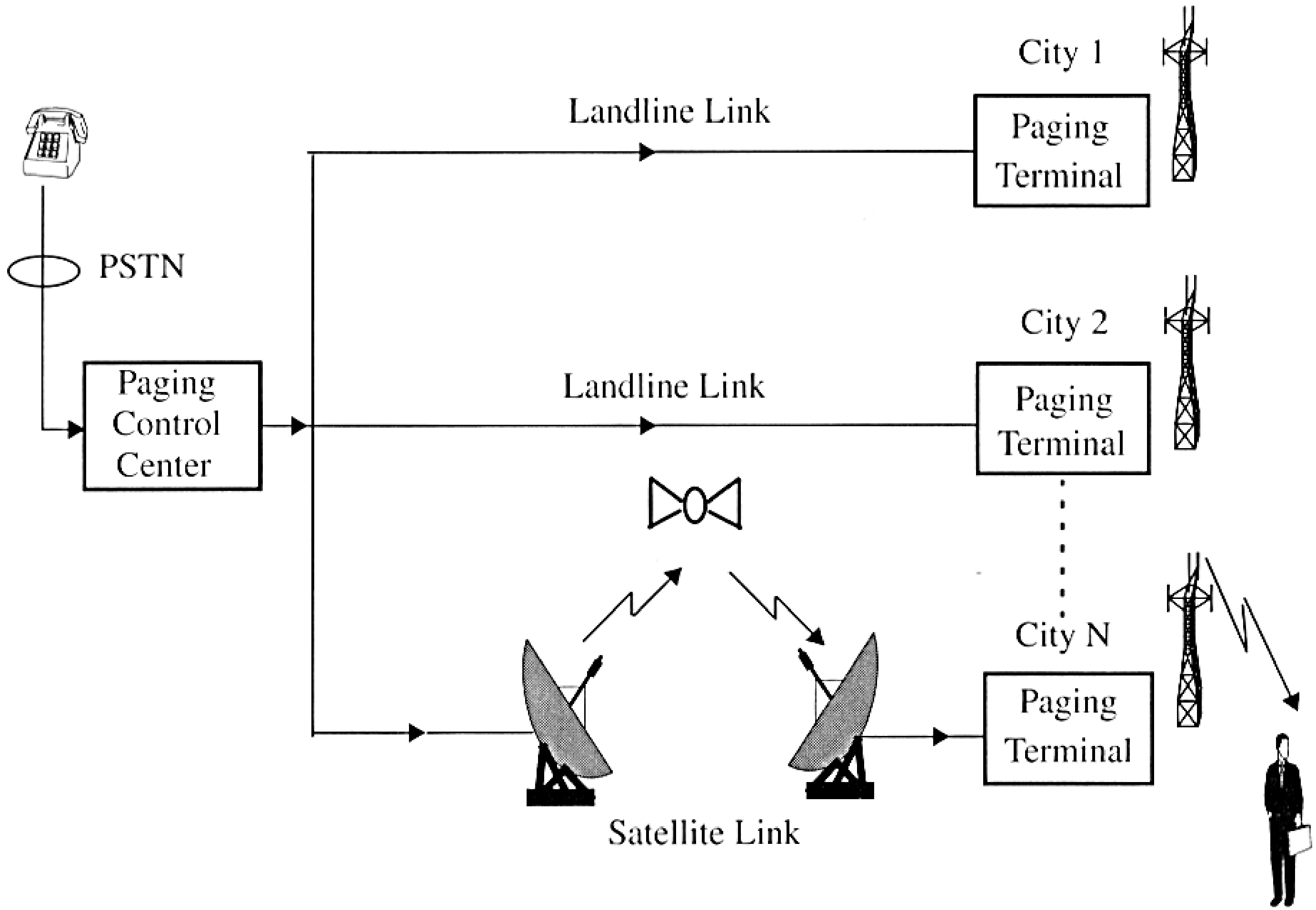



**Figure 1.3** A wide area paging system. The paging control center dispatches pages received from the PSTN throughout several cities at the same time.

# 2. Cordless telephone system

- Cordless telephone systems are full duplex communication systems that use radio to connect a portable handset to a base station, which is then connected to a telephone line with a specific telephone number on the PSTN.
- In First generation – the portable unit communicates only to the base unit of over few meters.
- In Second generation – allows subscribers to use their handsets in outdoor locations with urban centers.

# Cordless telephone system

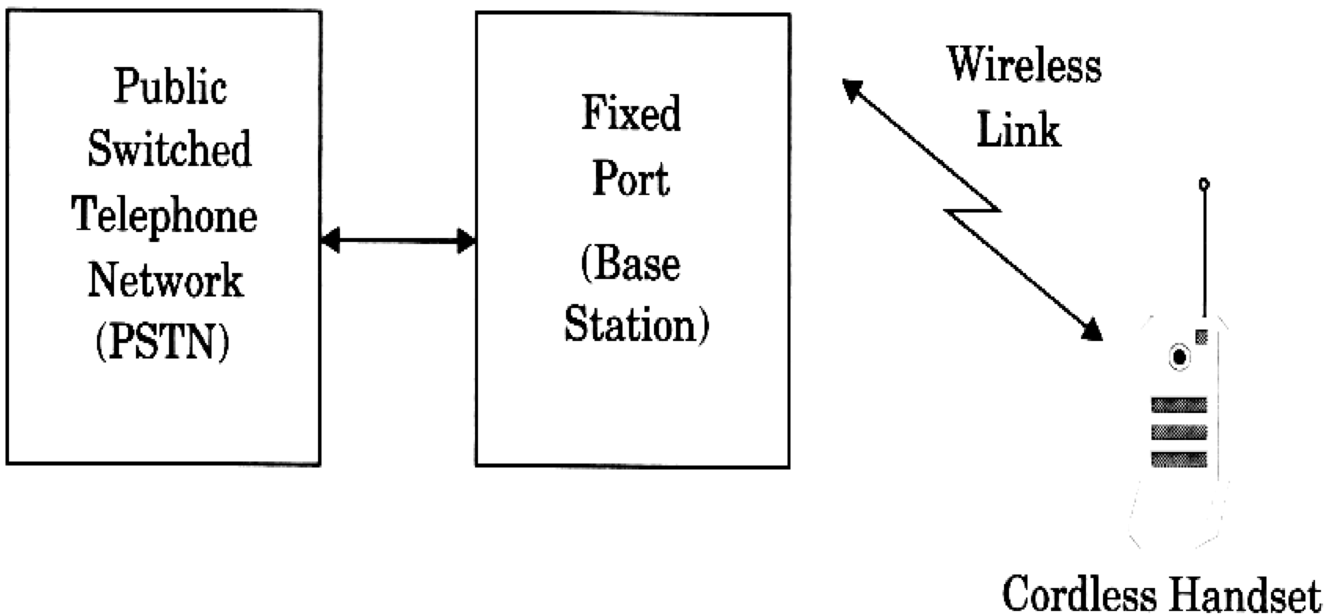



**Figure 1.4** A cordless telephone system.

# 3. Cellular telephone system

- A cellular telephone system provides a wireless connection to the PSTN for any user location within the radio range of the system.
- Cellular systems accommodate a large number of users over a large geographic area, within a limited frequency spectrum.
- A sophisticated switching technique called a **handoff** enables a call to proceed uninterrupted when the user moves from one cell to another.

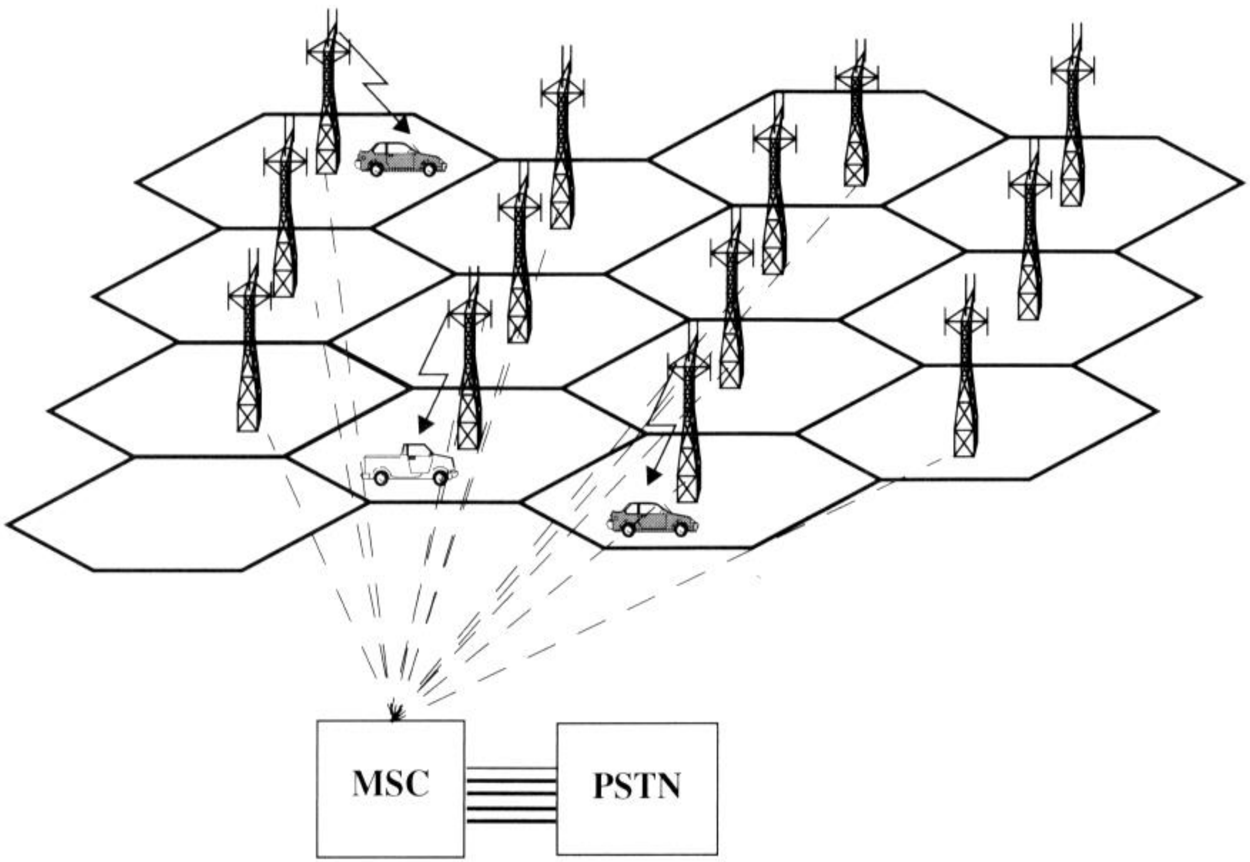



**Figure 1.5** A cellular system. The towers represent base stations which provide radio access between mobile users and the mobile switching center (MSC).

- Figure 1.5 shows a basic cellular system which consists of mobile stations, base stations and a mobile switching center (MSC).
- The Mobile Switching Center is sometimes called a mobile telephone switching office (MTSO), since it is responsible for connecting all mobiles to the PSTN in a cellular system.
- Each mobile communicates via radio with one of the base stations and may be handed-off to any number of base stations throughout the duration of a call.

- Communication between the base station and the mobiles is defined by a standard common air interface (CAI) that specifies four different channels.
- The channels used for voice transmission from the base station to mobiles are called forward voice channels (FVC) and the channels used for voice transmission from mobiles to the base station are called reverse voice channels (RVC).
- The two channels responsible for initiating mobile calls are the forward control channels (FCC) and reverse control channels (RCC).

# How a Cellular Telephone Call is Made

- When a cellular phone is turned on, but is not yet engaged in a call, it first scans the group of forward control channels to determine the one with the strongest signal, and then monitors that control channel until the signal drops below a usable level.
- At this point it again scans the control channels in search of the strongest base station signal.
- The mobile identification number (MIN), which is the subscriber's telephone number, is then broadcast as a paging message over all of the forward control channels throughout the cellular system.

- The mobile receives the paging message sent by the base station which it monitors, and responds by identifying itself over the reverse control channel.
- The base station relays the acknowledgment sent by the mobile and informs the MSC of the handshake.
- Then, the MSC instructs the base station to move the call to an unused voice channel within the cell.
- Once a call is in progress, the MSC adjusts the transmitted power of the mobile and changes the channel of the mobile unit and base stations in order to maintain call quality as the subscriber moves in and out of range of each base station. This is called a **handoff.**

# Comparison of Common Mobile Radio Systems

Table 1.5 Comparison of Mobile Communication Systems — Mobile Station

| Service | Coverage Range | Required Infra-structure | Complexity | Hardware Cost | Carrier Frequency | Functionality |
|---|---|---|---|---|---|---|
| TV Remote Control | Low | Low | Low | Low | Infra-red | Transmitter |
| Garage Door Opener | Low | Low | Low | Low | < 100 MHz | Transmitter |
| Paging System | High | High | Low | Low | < 1 GHz | Receiver |
| Cordless Phone | Low | Low | Moderate | Low | < 100 MHz | Transceiver |
| Cellular Phone | High | High | High | Moderate | < 1 GHz | Transceiver |

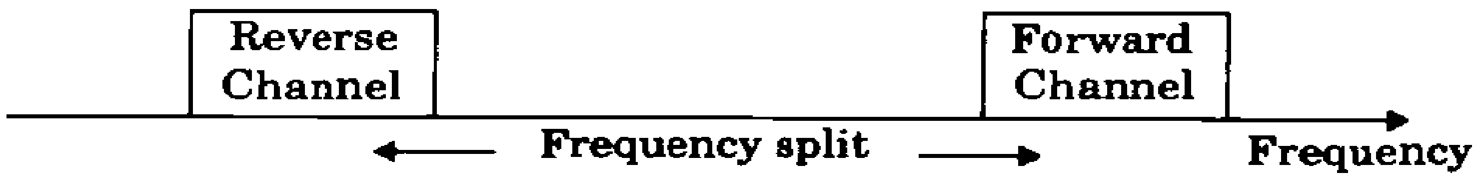
Table 1.6 Comparison of Mobile Communication Systems — Base Station

| Service | Coverage Range | Required Infra-structure | Complexity | Hardware Cost | Carrier Frequency | Functionality |
|---|---|---|---|---|---|---|
| TV Remote Control | Low | Low | Low | Low | Infra-red | Receiver |
| Garage Door Opener | Low | Low | Low | Low | < 100 MHz | Receiver |
| Paging System | High | High | High | High | < 1 GHz | Transmitter |
| Cordless Phone | Low | Low | Low | Moderate | < 100 MHz | Transceiver |
| Cellular Phone | High | High | High | High | < 1 GHz | Transceiver |

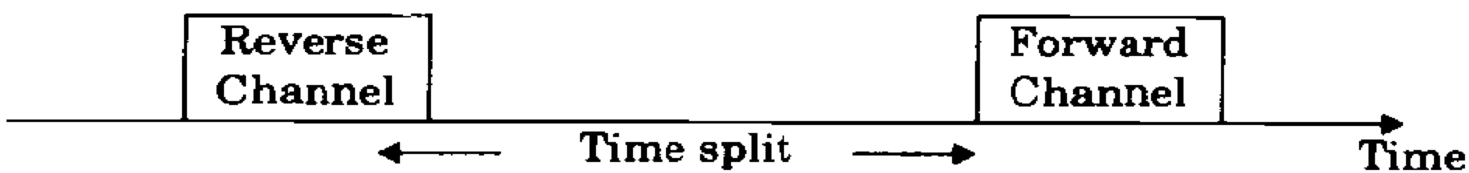
# INTRODUCTION TO MULTIPLE ACCESS

- In wireless communications systems, it is often desirable to allow the subscriber simultaneously to send and receive information to and from the base station.
- Duplexing may be done using frequency or time domain techniques.
- **Frequency division duplexing (FDD)** provides two distinct bands of frequencies for every user.
- The forward band provides traffic from the base station to the mobile, and the reverse band provides traffic from the mobile to the base

- **Time division duplexing (TDD)** uses time instead of frequency to provide both a forward and reverse link




(a)




(b)

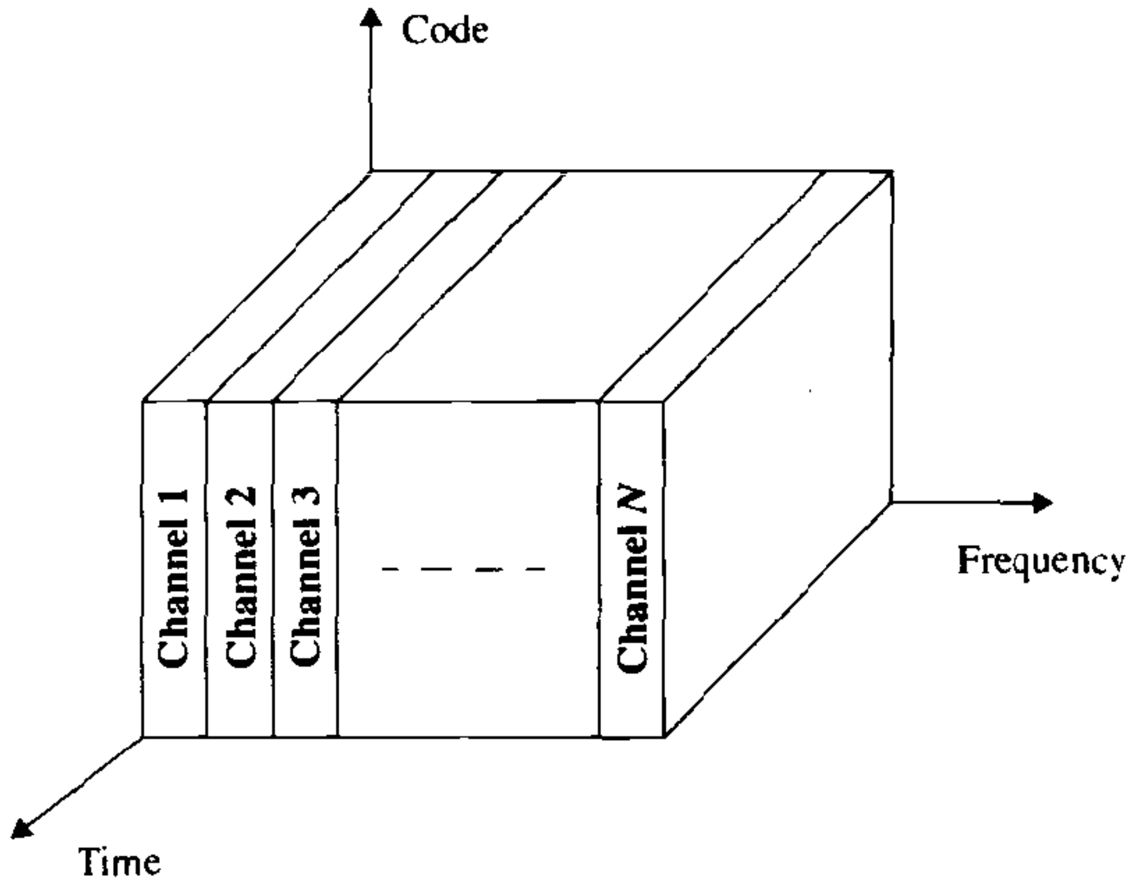
- Frequency division multiple access (**FDMA**), time division multiple access (**TDMA**), and code division multiple access (**CDMA**) are the three major access techniques used to share the available bandwidth in a wireless communication system.
- These techniques can be grouped as narrowband and wideband systems, depending upon how the available bandwidth is allocated to the users.
- **Narrowband Systems** — In a narrowband multiple access system, the available radio spectrum is divided into a large number of narrowband channels. The channels are usually operated using FDD.

- In **wideband multiple access systems**, the users are allowed to transmit in a large part of the spectrum.
- A large number of transmitters are also allowed to transmit on the same channel.
- TDMA allocates time slots to many transmitters on the same channel and allows only one transmitter to access the channel at any instant of time, whereas spread spectrum CDMA allows all of the transmitters to access the channel at the same time.
- TDMA and CDMA systems may use either FDD or TDD multiplexing techniques.

- In addition to FDMA, TDMA, and CDMA, two other multiple access schemes are used for wireless communications.
- They are packet radio (**PR**) and space division multiple access (**SDMA**)

# Frequency Division Multiple Access (FDMA)

- Frequency division multiple access (FDMA) assigns individual channels to individual users.
- It can be seen from Figure, that each user is allocated a unique frequency band or channel.
- These channels are assigned on demand to users who request service.
- During the period of the call, no other user can share the same frequency band.
- In FDD systems, the users are assigned a channel as a pair of frequencies; one frequency is used for the forward channel, while the other frequency is used for the reverse channel.




**FDMA where different channels are assigned different frequency bands.**

The features of FDMA are as follows:

- The FDMA channel carries only one phone circuit at a time.
- If an FDMA channel is not in use, then it remains idle and cannot be used by other users to increase or share capacity. It is essentially a wasted resource.
- After the assignment of a voice channel, the base station and the mobile transmit simultaneously and continuously.
- The bandwidths of FDMA channels are relatively narrow (30 kHz) as each channel supports only one circuit per carrier. That is, FDMA is usually implemented in narrowband systems.

- The complexity of FDMA mobile systems is lower when compared to TDMA systems, though this is changing as digital signal processing methods improve for TDMA.
- Since FDMA is a continuous transmission scheme, fewer bits are needed for overhead purposes (such as synchronization and framing bits) as compared to TDMA.
- FDMA systems have higher cell site system costs as compared to TDMA systems, because of the single channel per carrier design, and the need to use costly bandpass filters to eliminate false radiation at the base station.
- The FDMA mobile unit uses duplexers since both the transmitter and receiver operate at the same time. This results in an increase in the cost of FDMA subscriber limits and base stations.
- FDMA requires RF filtering to minimize adjacent channel interference.

- The number of channels that can be simultaneously supported in a FDMA system is given by

$$N = \frac{B_t - 2B_{guard}}{B_c}$$

where $B_t$ is the total spectrum allocation, $B_{guard}$ is the guard band allocated at the edge of the allocated spectrum, and $B_c$ is the channel bandwidth.

## Example 8.2

If $B_t$ is 12.5 MHz, $B_{guard}$ is 10 kHz, and $B_c$ is 30 kHz, find the number of channels available in an FDMA system.

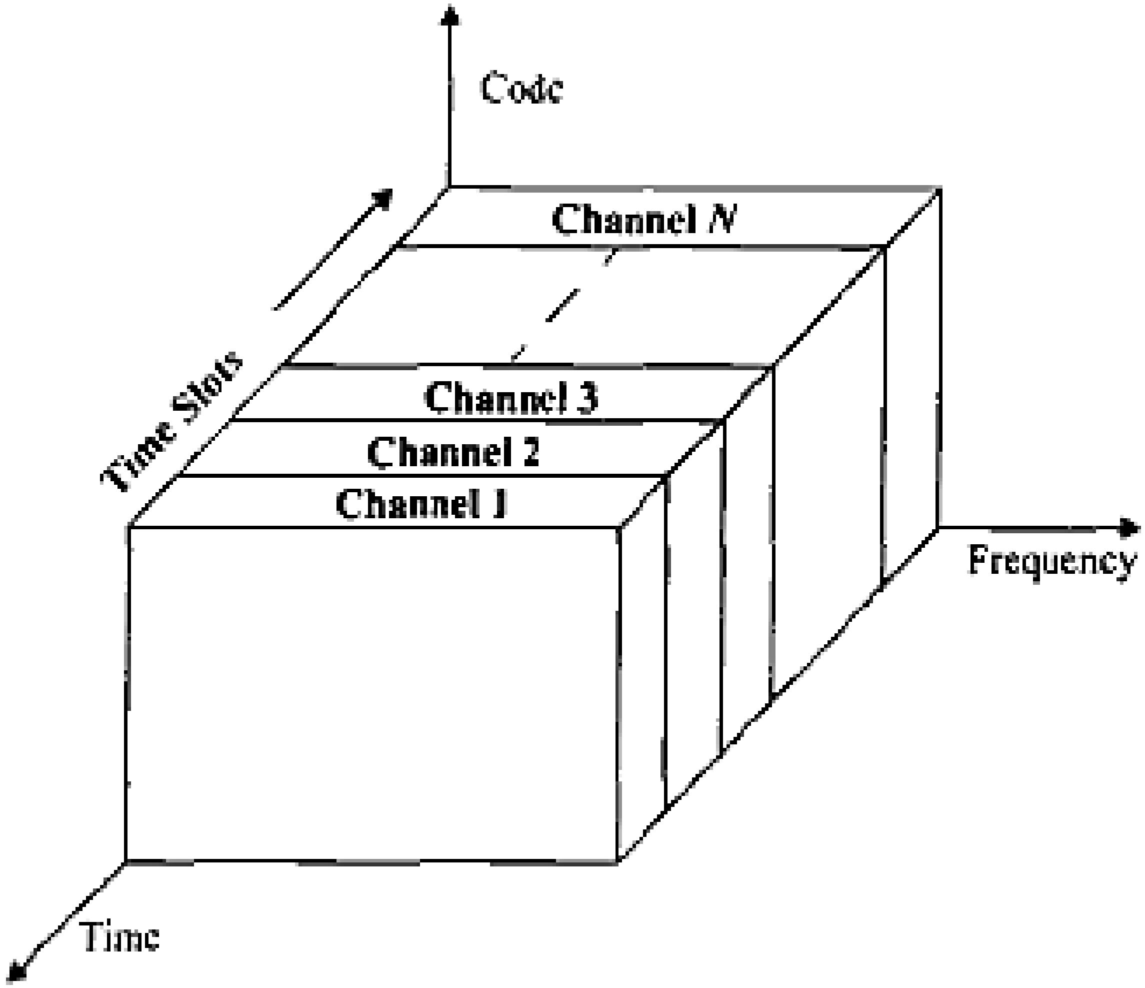
### Solution to Example 8.2

The number of channels available in the FDMA system is given as

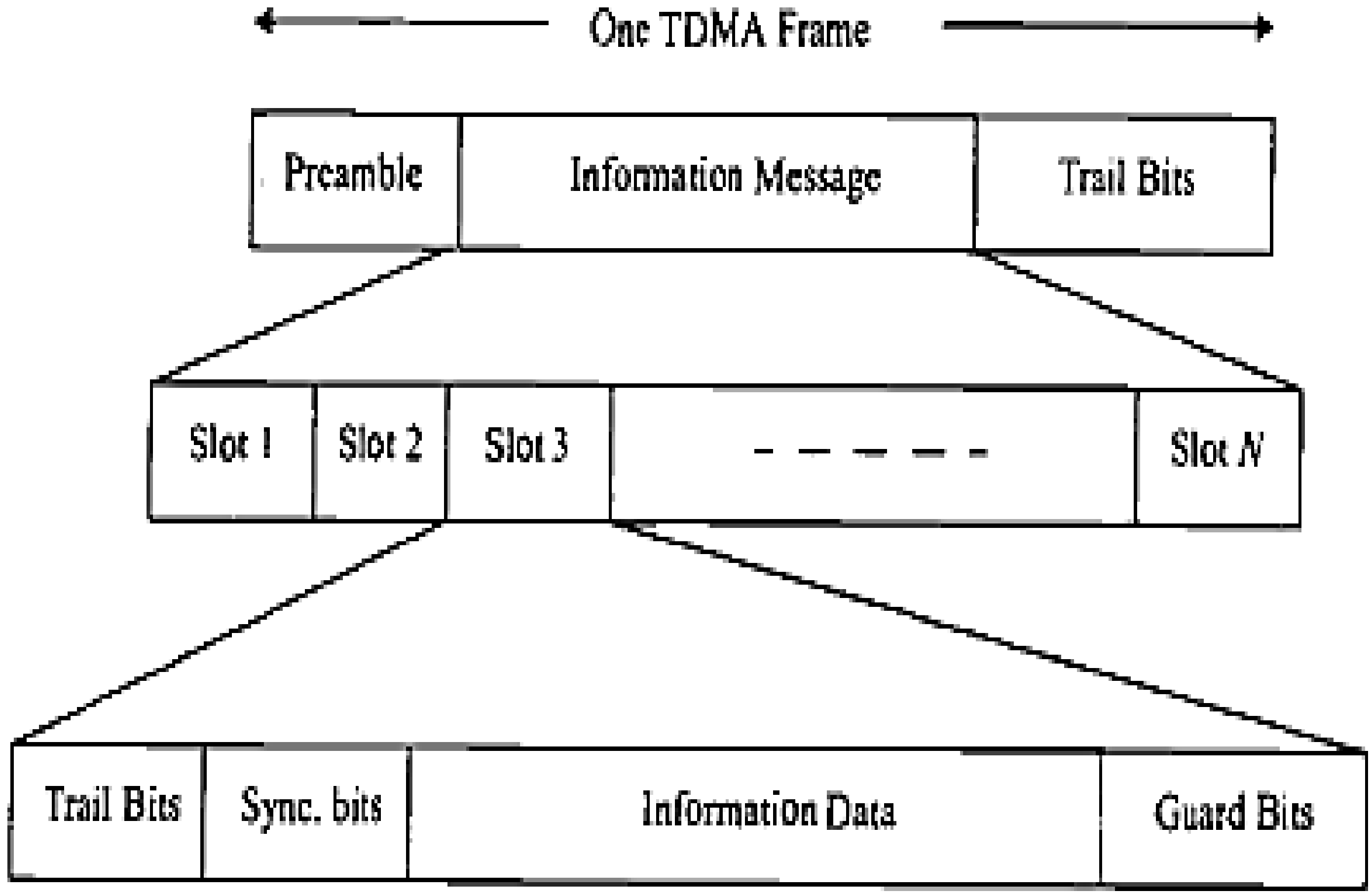
$$N = \frac{12.5 \times 10^6 - 2(10 \times 10^3)}{30 \times 10^3} = 416$$

# Time Division Multiple Access (TDMA)

- TDMA systems divide the radio spectrum into time slots, and in each slot only one user is allowed to either transmit or receive.
- It can be seen from Figure, that each user occupies a cyclically repeating time slot, so a channel may be thought of as particular time slot that reoccurs every frame, where N time slots comprise a frame.
- Unlike in FDMA systems which accommodate analog FM, digital data and digital modulation must be used with TDMA




TDMA scheme where each channel occupies a cyclically repeating time slot.




**TDMA frame structure**

- TDMA shares a single carrier frequency with several users, where each user makes use of nonoverlapping time slots. The number of time slots per frame depends on several factors, such as modulation technique, available bandwidth, etc.
- • Data transmission for users of a TDMA system is not continuous, but occurs in bursts. This results in low battery consumption, since the subscriber transmitter can be turned off when not in use (which is most of the time).
- • Because of discontinuous transmissions in TDMA, the handoff process is much simpler for a subscriber unit, since it is able to listen for other base stations during idle time slots. An enhanced link control, such as that provided by mobile assisted handoff (MAHO)

- **Efficiency of TDMA** — The efficiency of a TDMA system is a measure of the percentage of transmitted data The frame efficiency, is the percentage of bits per frame which contain transmitted data
- The frame efficiency can be found as follows

$$b_{OH} = N_r b_r + N_t b_p + N_t b_g + N_r b_g$$

- where,
- $N_r$ is the number of reference bursts per frame,
- $N_t$ is the number of traffic bursts per frame,
- $b_r$ is the number of overhead bits per reference burst,
- $b_p$ is the number of overhead bits per preamble in each slot, and

- $b_g$ is the number of equivalent bits in each guard time interval.
- The total number of bits per frame , $b_T$ is

$$b_T = T_f R$$

  - where $T_f$ is the frame duration, and R is the channel bit rate. The frame efficiency $\eta_f$ is thus given as

$$\eta_f = \left(1 - \frac{b_{OH}}{b_T}\right) \times 100\%$$

- **Number of channels in TDMA system** — The number of TDMA channel slots that can be provided in a TDMA system is found by multiplying the number of TDMA slots per channel by the number of channels available, and it is given by

$$N = \frac{m\,(B_{tot} - 2B_{guard})}{B_c}$$

  - where m is the maximum number of TDMA users supported on each radio channel.

# Example:

**Ques:** Consider Global System for Mobile, which is a TDMA/FDD system that uses 25 MHz for the forward link, which is broken into radio channels of 200 kHz. If 8 speech channels are supported on a single radio channel, and if no guard band is assumed, find the number of simultaneous users that can be accommodated in GSM.

**Solution:**

The number of simultaneous users that can be accommodated in GSM is given as

$$N = \frac{25\ \text{MHz}}{(200\ \text{kHz})/8} = 1000$$

Thus, GSM can accommodate 1000 simultaneous users.

# Example: 2

- **Ques:** If GSM uses a frame structure where each frame consists of S time slots, and each time slot contains 156.25 bits, and data is transmitted at 270.833 kbps in the channel, find (a) the time duration of a bit, (b) the time duration of a slot, (c) the time duration of a frame, and (d) how long must a user occupying a single time slot must wait between two simultaneous transmissions.

**Solution**

- (a) The time duration of a bit, $T_b = \frac{1}{270.833 \text{ kbps}} = 3.692\ \mu\text{s}.$
- (b) The time duration of a slot, $T_{slot} = 156.25 \times T_b = 0.577 \text{ ms}.$
- (c) The time duration of a frame, $T_f = 8 \times T_{slot} = 4.615 \text{ ms}.$
- (d) A user has to wait 4.615 ms, the arrival time of a new frame, for its next transmission.

# Example 3

**Ques.:** If a normal GSM time slot consists of 6 trailing bits, 8.25 guard bits, 26 training bits, and 2 traffic bursts of 58 bits of data, find the frame efficiency.

**Solution:**

A time slot has $6 + 8.25 + 26 + 2(58) = 156.25$ bits.

A frame has $8 \times 156.25 = 1250$ bits/frame.

The number of overhead bits per frame is given by

$$b_{OH} = 8(6) + 8(8.25) + 8(26) = 322 \text{ bits}$$

Thus, the frame efficiency

$$\eta_f = \left[1 - \frac{322}{1250}\right] \times 100 = 74.24\ \%$$

# Spread Spectrum Multiple Access

- Spread spectrum multiple access (SSMA) uses signals which have a transmission bandwidth that is several orders of magnitude greater than the minimum required RF bandwidth.
- SSMA is not very bandwidth efficient when used by a single user. However, since many users can share the same spread spectrum bandwidth without interfering with one another, spread spectrum systems become bandwidth efficient in a multiple user environment.
- There are two main types of spread spectrum multiple access techniques; frequency hopped multiple access **(FH)** and direct sequence multiple access **(DS). Direct sequence** multiple access is **also called code division multiple access (CDMA).**

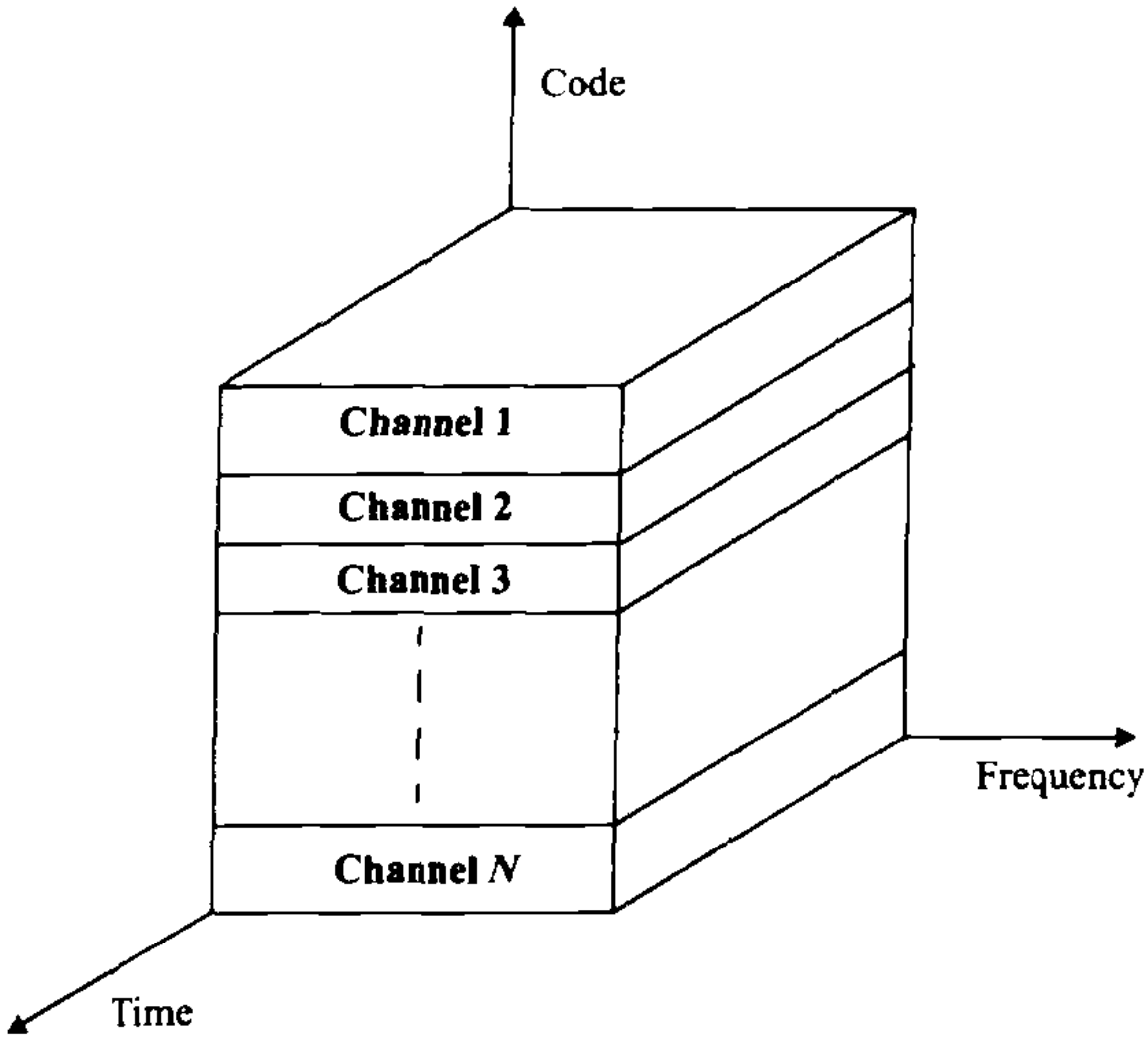
# Frequency Hopped Multiple Access (FHMA)

- Frequency hopped multiple access (FHMA) is a digital multiple access system in which the carrier frequencies of the individual users are varied in a pseudorandom fashion within a wideband channel.
- The digital data is broken into uniform sized bursts which are transmitted on different carrier frequencies.
- The difference between FHMA and a traditional FDMA system is that the frequency hopped signal changes channels at rapid intervals.
- If the rate of change of the carrier frequency is greater than the symbol rate then the system is referred to as a **fast frequency hopping** system.
- If the channel changes at a rate less than or equal to the symbol rate, it is called **slow frequency hopping.**

- Error control coding and interleaving can also be combined to guard against Errors which can occur when two or more users transmit on the same channel at the same time.

## Code Division Multiple Access (CDMA)

- In code division multiple access (CDMA) systems, the narrowband message signal is multiplied by a very large bandwidth signal called the spreading signal.
- All users in a CDMA system, use the same carrier frequency and may transmit simultaneously.
- Each user has its own pseudorandom codeword which is approximately orthogonal to all other codewords




**CDMA in which each channel is assigned a unique PN code which is orthogonal to PN codes used by other users.**

- The near-far problem occurs when many mobile users share the same channel.
- In general, the strongest received mobile signal will capture the demodulator at a base station.
- To combat the near-far problem, power control is used in most CDMA implementations.
- Power control is provided by each base station in a cellular system and assures that each mobile within the base station coverage area provides the same signal level to the base station receiver.

The **features of CDMA** including the following:

- Many users of a CDMA system share the same frequency. Either TDD or FDD may be used.
- Unlike TDMA or FDMA, CDMA has a soft capacity limit. Increasing the number of users in a CDMA system raises the noise floor in a linear manner.

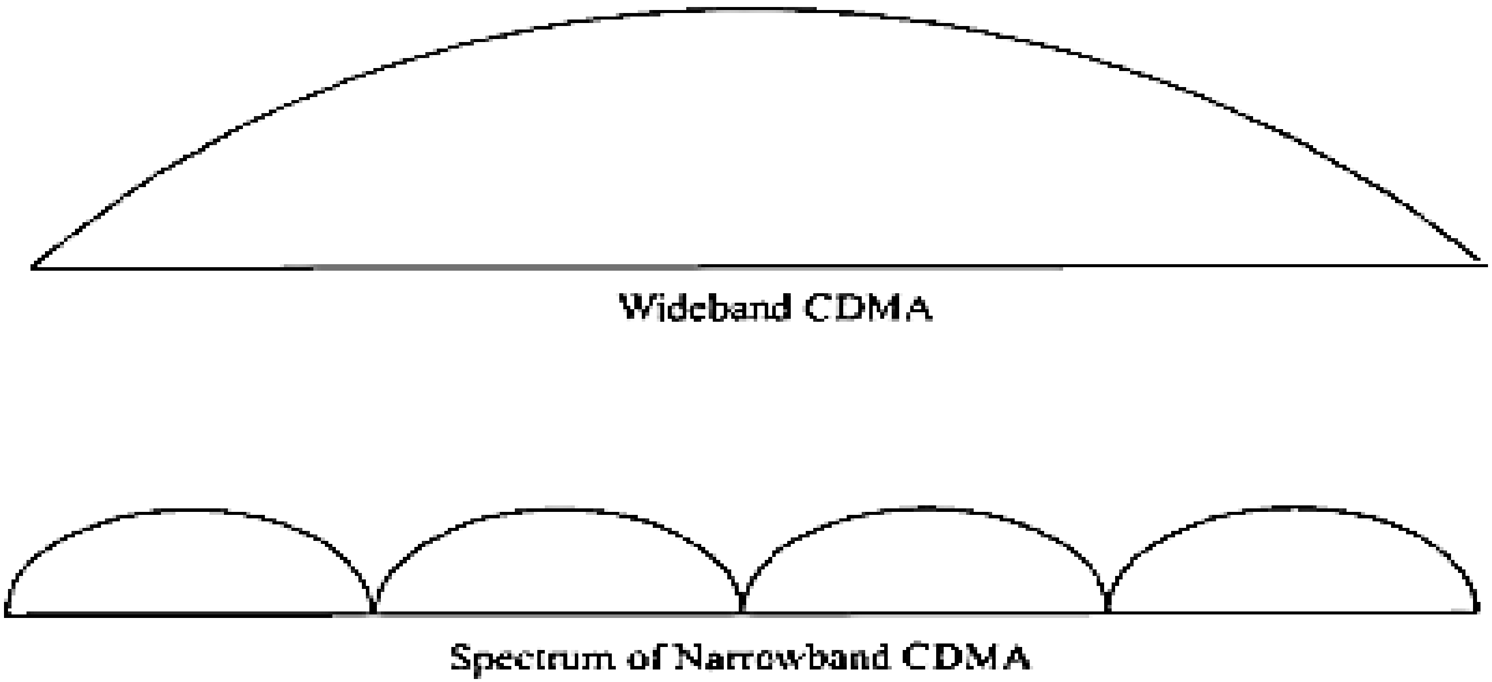
- Thus, there is no absolute limit on the number of users in CDMA.
- Multipath fading may be substantially reduced because the signal is spread over a large spectrum.
- Channel data rates are very high in CDMA systems.
- Since CDMA uses co-channel cells, it can use macroscopic spatial diversity to provide soft handoff. Soft handoff is performed by the MSC, which can simultaneously monitor a particular user from two or more base stations.
- Self-jamming is a problem in CDMA system. Self-jamming arises from the fact that the spreading sequences of different users are not exactly orthogonal.
- The near-far problem occurs at a CDMA receiver if an undesired user has a high detected power as compared to the desired user.

# Hybrid Spread Spectrum Techniques

- There are certain other hybrid combinations that provide certain advantages. These hybrid technique types are,

**Hybrid FDMA/CDMA (FCDMA):**

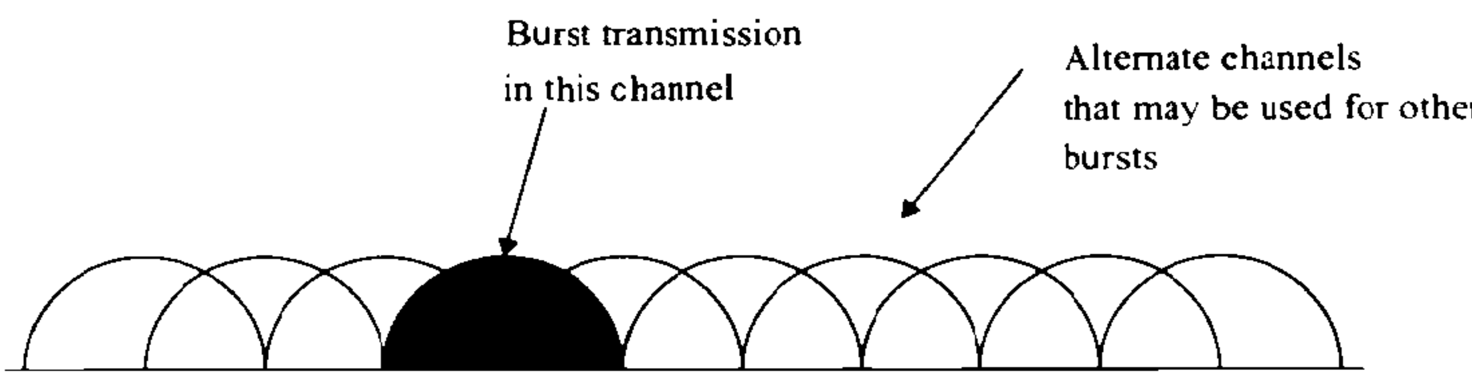
- This technique can be used as an alternative to the DS-CDMA techniques discussed above.
- Figure, shows the spectrum of this hybrid scheme.
- The available wideband spectrum is divided into a number of subspectras with smaller bandwidths.
- Each of these smaller subchannels becomes a narrowband CDMA system.
- This hybrid system has an advantage in that the required bandwidth need not be contiguous and different users can be allotted different subspectrum bandwidths depending on their requirements.




**Spectrum of wideband CDMA compared to the spectrum of a hybrid, frequency division, direct sequence multiple access.**

## Hybrid Direct Sequence/Frequency Hopped Multiple Access (DS/FHMA)

- This technique consists of a direct sequence modulated signal whose center frequency is made to hop periodically in a pseudorandom fashion.
- Figure, shows the frequency spectrum of such a signal.
- Direct sequence, frequency hopped systems have an advantage in that they avoid the near-far effect.



## Time Division CDMA (TCDMA)

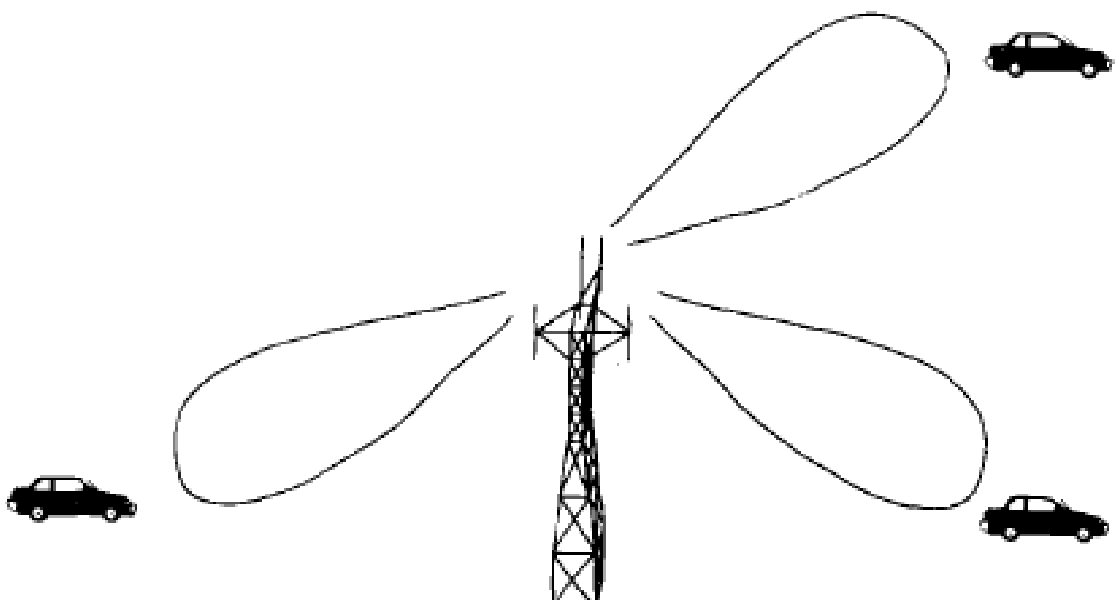
- In a TCDMA (also called TDMA/CDMA) system, different spreading codes are assigned to different cells.
- Within each cell, only one user per cell is allotted a particular time slot.
- Thus at any time, only one CDMA user is transmitting in each cell.

## Time Division Frequency Hopping (TDFH)

- This technique has been adopted for the GSM standard.
- Where the hopping sequence is predefined and the subscriber is allowed to hop only on certain frequencies which are assigned to a cell.
- This scheme also avoids co-channel interference problems between neighboring cells.

# Space Division Multiple Access (SDMA)

- Space division multiple access (SDMA) controls the radiated energy for each user in space.
- It can be seen from Figure, that SDMA serves different users by using spot beam antennas.
- These different areas covered by the antenna beam may be served by the same frequency (in a TDMA or CDMA system) or different frequencies (in an FDMA system).



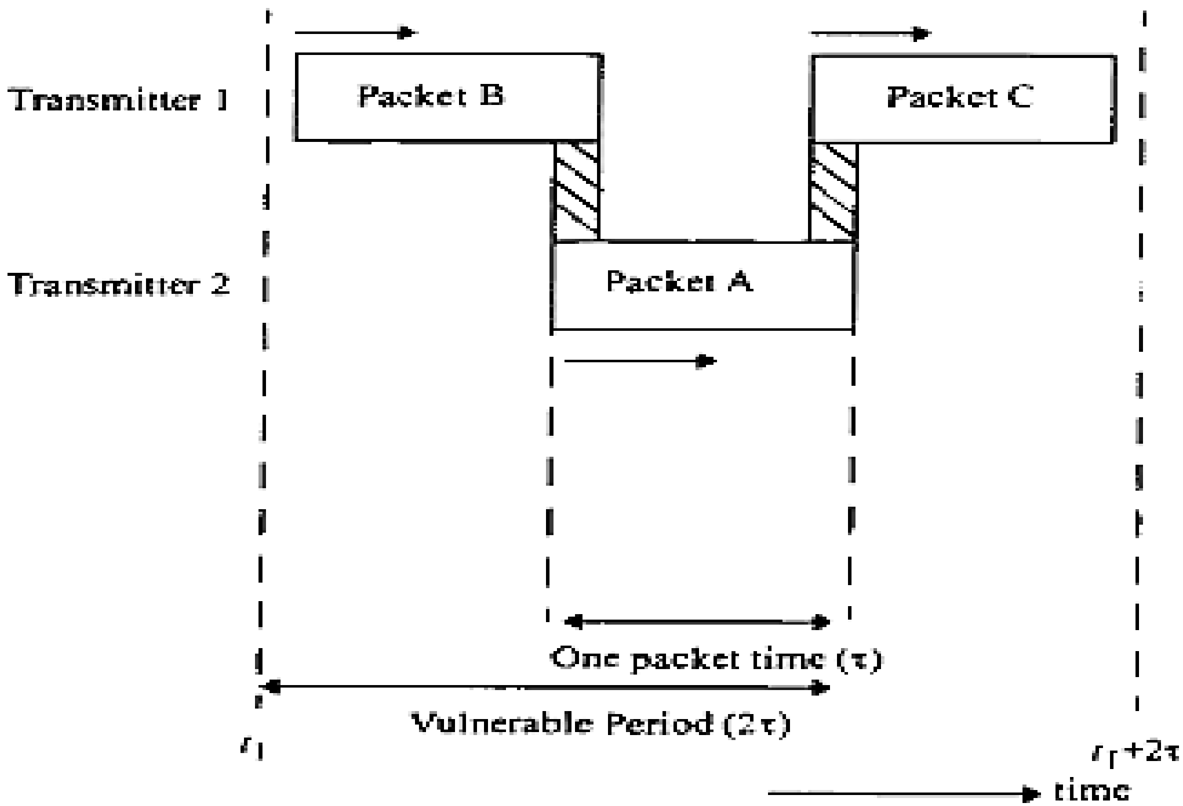
- First, the base station has complete control over the power of all the transmitted signals on the forward link.
- However, because of different radio propagation paths between each user and the base station, the transmitted power from each subscriber unit must be dynamically controlled to prevent any single user from driving up the interference level for all other users.
- Second, transmit power is limited by battery consumption at the subscriber unit, therefore there are limits on the degree to which power may be controlled on the reverse link.

## Packet Radio

- In packet radio (PR) access techniques, many subscribers attempt to access a single channel in an uncoordinated (or minimally coordinated) manner.
- Transmission is done by using bursts of data.
- Collisions from the simultaneous transmissions of multiple transmitters are detected at the base station receiver, in which case an ACK or NACK signal is broadcast by the base station to alert the desired user (and all other users) of received transmission.

# Packet Radio Protocols

- In order to determine the throughput, it is important to determine the **vulnerable period, Vp,** which is **defined** as the time interval during which the packets are susceptible to collisions with transmissions from other users.




**Packet A will collide with packets B and C because of overlap in transmission time.**

- If $\tau$ is the packet duration in seconds, then the traffic occupancy or throughput R of a packet radio network is given by

$$R = \lambda\tau$$

- The normalized throughput is given as the total offered load times the probability of successful transmission,

$$T = R\Pr[no\ collision] = \lambda\tau\Pr[no\ collision]$$

- The probability that n packets are generated by the user population during a given packet duration interval is assumed to be Poisson distributed and is given as

$$Pr(n) = \frac{R^n e^{-R}}{n!}$$

- The probability that zero packets are generated (i.e., no collision) during this interval is given by

$$Pr(0) = e^{-R}$$

**Pure ALOHA :**

- The pure ALOHA protocol is a random access protocol used for data transfer.
- A user accesses a channel as soon as a message is ready to be transmitted.
- After a transmission, the user waits for an acknowledgment.
- In case of collisions, (i.e., when a NACK is received), the terminal waits for a random period of time and retransmits the message.

- As the number of users increase, a greater delay occurs because the probability of collision increases.
- For the ALOHA protocol, the vulnerable period is double the packet duration.
- Thus, the probability of no collision during the interval of $2\tau$ is found by evaluating Pr (n) given as

$$Pr(n) = \frac{(2R)^n e^{-2R}}{n!} \text{ at } n = 0$$

- One may evaluate the mean of above equation to determine the average number of packets sent during $2\tau$ .

- The probability of no collision $Pr(0) = e^{-2R}$.
- The throughput of the ALOHA protocol is found by using

$$T = Re^{-2R}$$

**Slotted ALOHA :**

- In slotted ALOHA, time is divided into equal time slots of length greater than the packet duration $\tau$.
- The subscribers each have synchronized clocks and transmit a message only at the beginning of a new time slot, thus resulting in a discrete distribution of packets.
- This prevents partial collisions, where one packet collides with a portion of another.

- The vulnerable period for slotted ALOHA is only one packet duration, since partial collisions are prevented through synchronization.
- The throughput for the case of slotted ALOHA is thus given by

$$T = Re^{-R}$$

**Carrier Sense Multiple Access (CSMA) Protocols :**

- ALOHA protocols do not listen to the channel before transmission, and therefore do not exploit information about the other users.

- ALOHA protocols do not listen to the channel before transmission, and therefore do not exploit information about the other users.
- By listening to the channel before engaging in transmission, greater efficiencies may be achieved.
- CSMA protocols are based on the fact that each terminal on the network is able to monitor the status of the channel before transmitting information.
- If the channel is idle (i.e., no carrier is detected), then the user is allowed to transmit a packet based on a particular algorithm.

- In CSMA protocols, detection delay and propagation delay are two important parameters.
- Detection delay is a function of the receiver hardware and is the time required for a terminal to sense whether or not the channel is idle.
- Propagation delay is a relative measure of how fast it takes for a packet to travel from a base station to a mobile terminal.
- Propagation delay is important, since just after a user begins sending a packet, another user may be ready to send and may be sensing the channel at the same time.

- the propagation delay $t_d$, can be expressed as

$$t_d = \frac{t_p R_b}{m}$$

- where $t_p$ - propagation time in seconds,

  $R_b$ - channel bit rate, and

  m - expected number of bits in a data packet

There exist several variations of the CSMA strategy

- **1-persistent CSMA** — The terminal listens to the channel and waits for transmission until it finds the channel idle. As soon as the channel is idle, the terminal transmits its message with probability one.
- **Non-persistent CSMA** — In this type of CSMA strategy after receiving a negative acknowledgment the terminal waits a random time before retransmission of the packet.
- **p-persistent CSMA** — p-persistent CSMA is applied to slotted channels. When a channel is found to be idle, the packet is transmitted in the first available slot with probability p or in the next slot with probability i-p.
- **CSMA/CD** — In CSMA with collision detection (CD), a user monitors its transmission for collisions. If two or more terminals start a transmission at the same time, collision is detected, and the transmission is immediately aborted in midstream.

- **Data sense multiple access (DSMA)** — DSMA is a special type of CSMA that relies on successfully demodulating a forward control channel before broadcasting data back on a reverse channel.

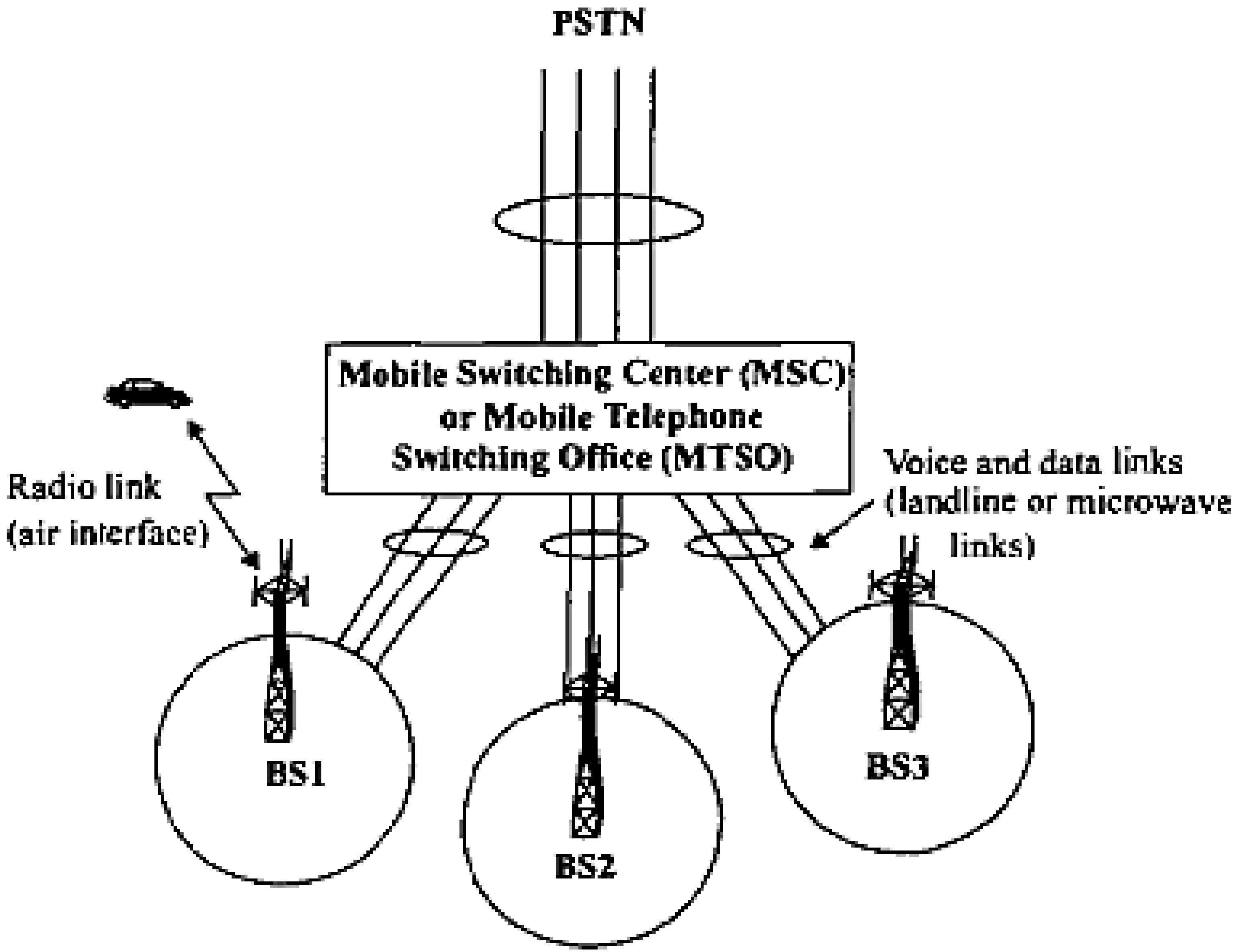
**Reservation Protocols :**

**Reservation ALOHA**

- Reservation ALOHA is a packet access scheme based on time division multiplexing.
- In this protocol, certain packet slots are assigned with priority, and it is possible for users to reserve slots for the transmission of packets.
- Slots can be permanently reserved or can be reserved on request.

## Packet Reservation Multiple Access (PRMA)

- PRMA uses a discrete packet time technique similar to reservation ALOHA and combines the cyclical frame structure of TDMA in a manner that allows each TDMA time slot to carry either voice or data, where voice is given priority.



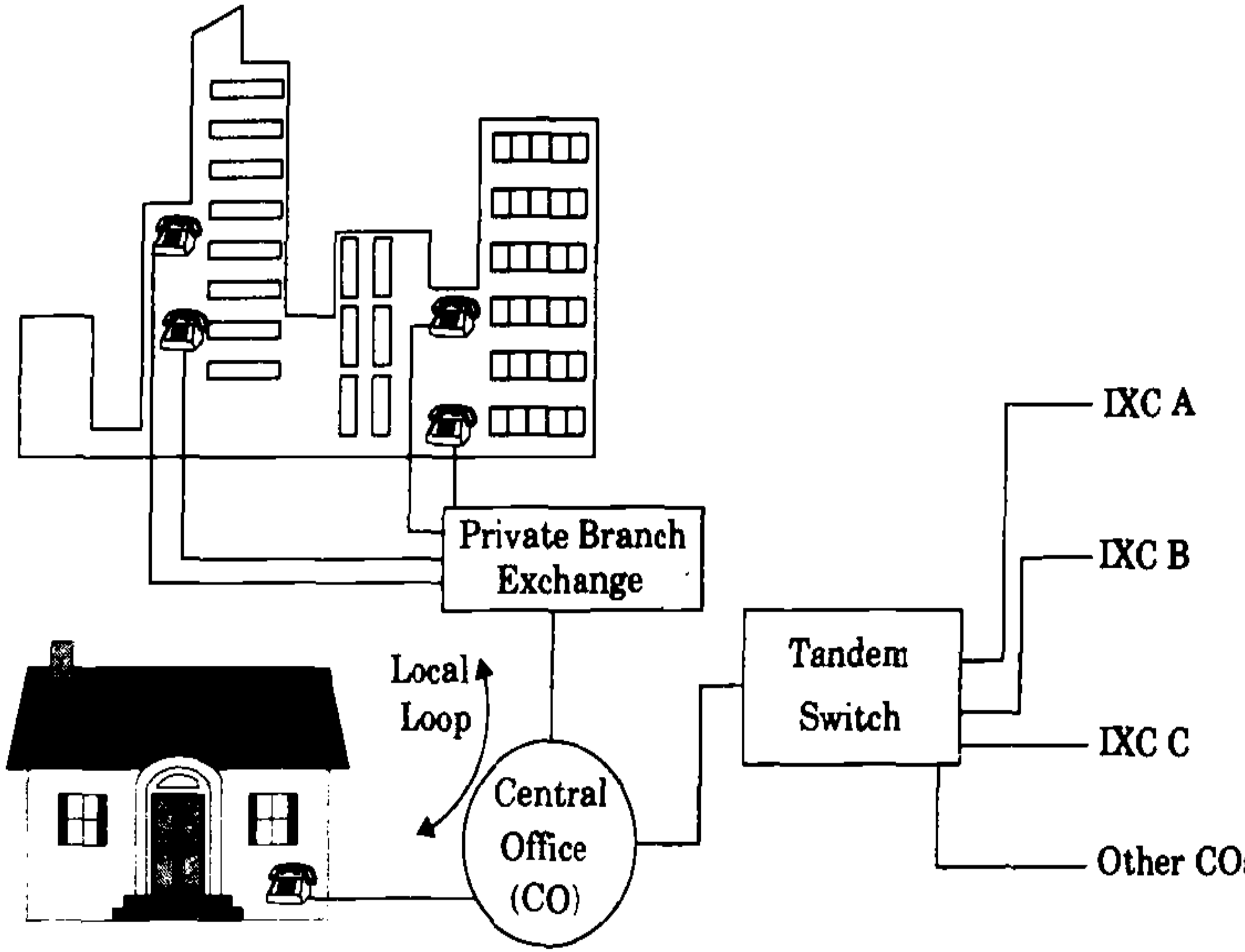

**Block diagram of a cellular system**

## Differences Between Wireless and Fixed Telephone Networks

- Transfer of information in the public switched telephone network (PSTN) takes place over landline trunked lines (called trunks) comprised of fiber optic cables, copper cables, microwave links, and satellite links.

## The Public Switched Telephone Network (PSTN)

- The PSTN is a highly integrated communications network that connects over 70% of the world's inhabitants.
- In early 1994, the International Telecommunications Union estimated that there were 650 million public landline telephone numbers, as compared to 30 million cellular telephone numbers.
- While landline telephones are being added at a 3% rate, wireless subscriptions are growing at greater than a 50% rate.




**Local landline telephone network**

# Limitations in Wireless Networking

- As compared with the local, fixed telephone network, where all end-users are static, a wireless communications system is extremely complex.
- First, the wireless network requires an air interface between base stations and subscribers to provide telephone grade communications under a wide range of propagation conditions and for any possible user location.
- To assure adequate area coverage, the deployment of many (sometimes hundreds) of base stations throughout a market is necessary, and each of these base stations must be connected to the MSC.
- Furthermore, the MSC must eventually provide connection for each of the mobile users to the PSTN.

- A problem unique to wireless networks is the extremely hostile and random nature of the radio channel, and since users may request service from any physical location while traveling over a wide range of velocities, the MSC is forced to switch calls randomly between base stations throughout the system.

## Merging Wireless Networks and the PSTN

- Until the mid 1980s, most analog landline telephone links throughout the world sent signaling information along the same trunked lines as voice traffic.

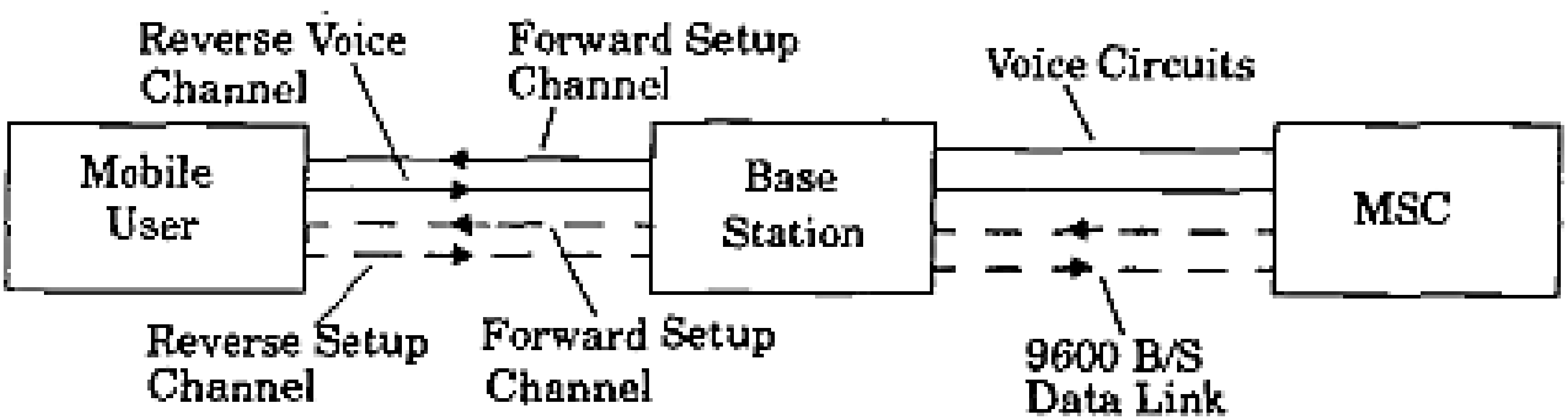
- A single physical connection was used to handle both signaling traffic and voice traffic for each user.

- The advantage of a separate but parallel signaling channel allows the voice trunks to be used strictly for voice traffic, and supports many more users on each trunked line.
- Thus, during the mid 1980s, the PSTN was transformed into two parallel networks — one dedicated to user traffic, and one dedicated to call signaling traffic.
- This technique is called common channel signaling.
- Common channel signaling is used in all modern telephone networks. Most recently, dedicated signaling channels have been used by cellular MSCs to provide global signaling interconnection.

# Development of Wireless Networks

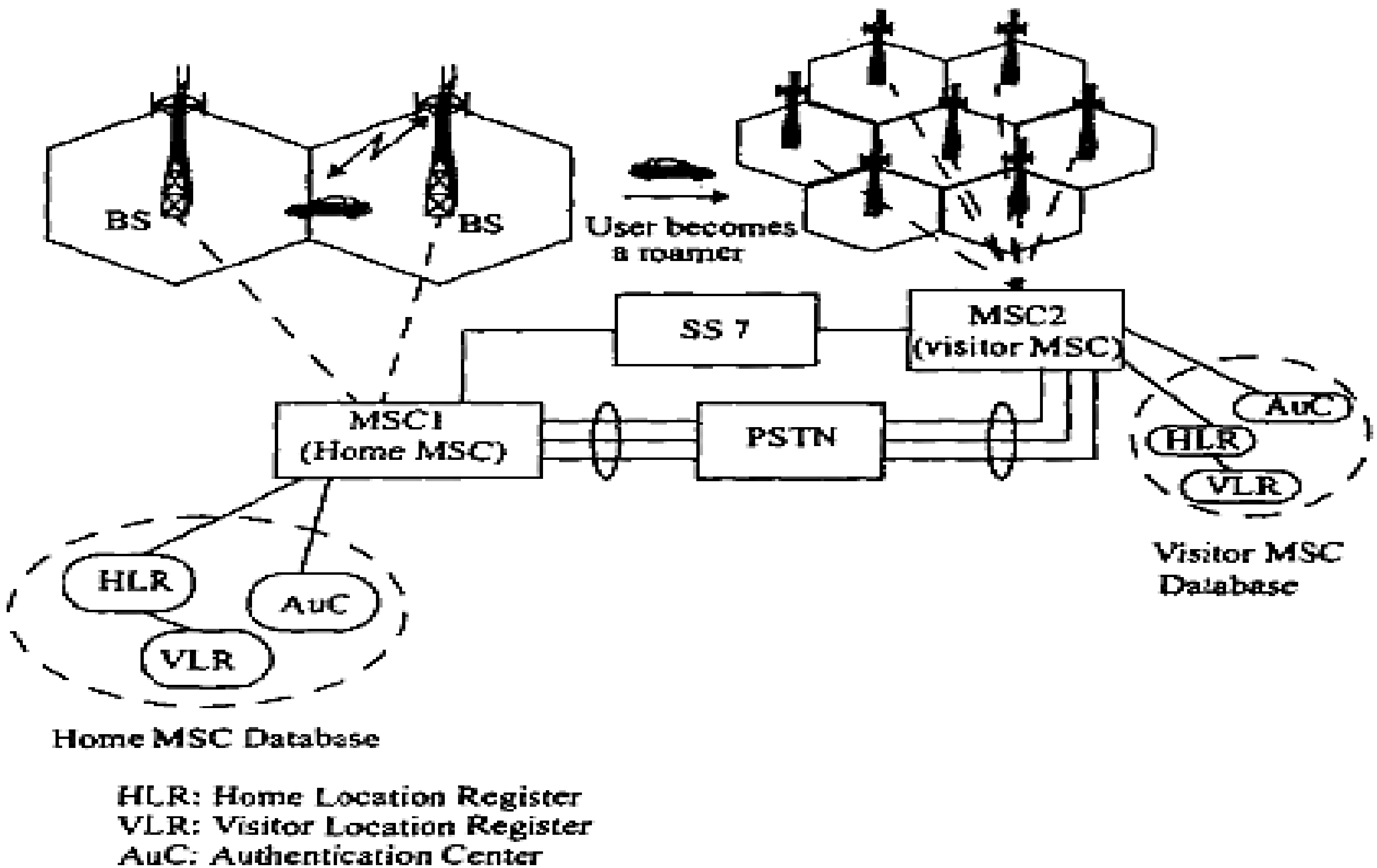
## First Generation Wireless Networks

- First generation cellular and cordless telephone networks are based on analog technology.
- All first generation cellular systems use FM modulation, and cordless telephones use a single base station to communicate with a single portable terminal.

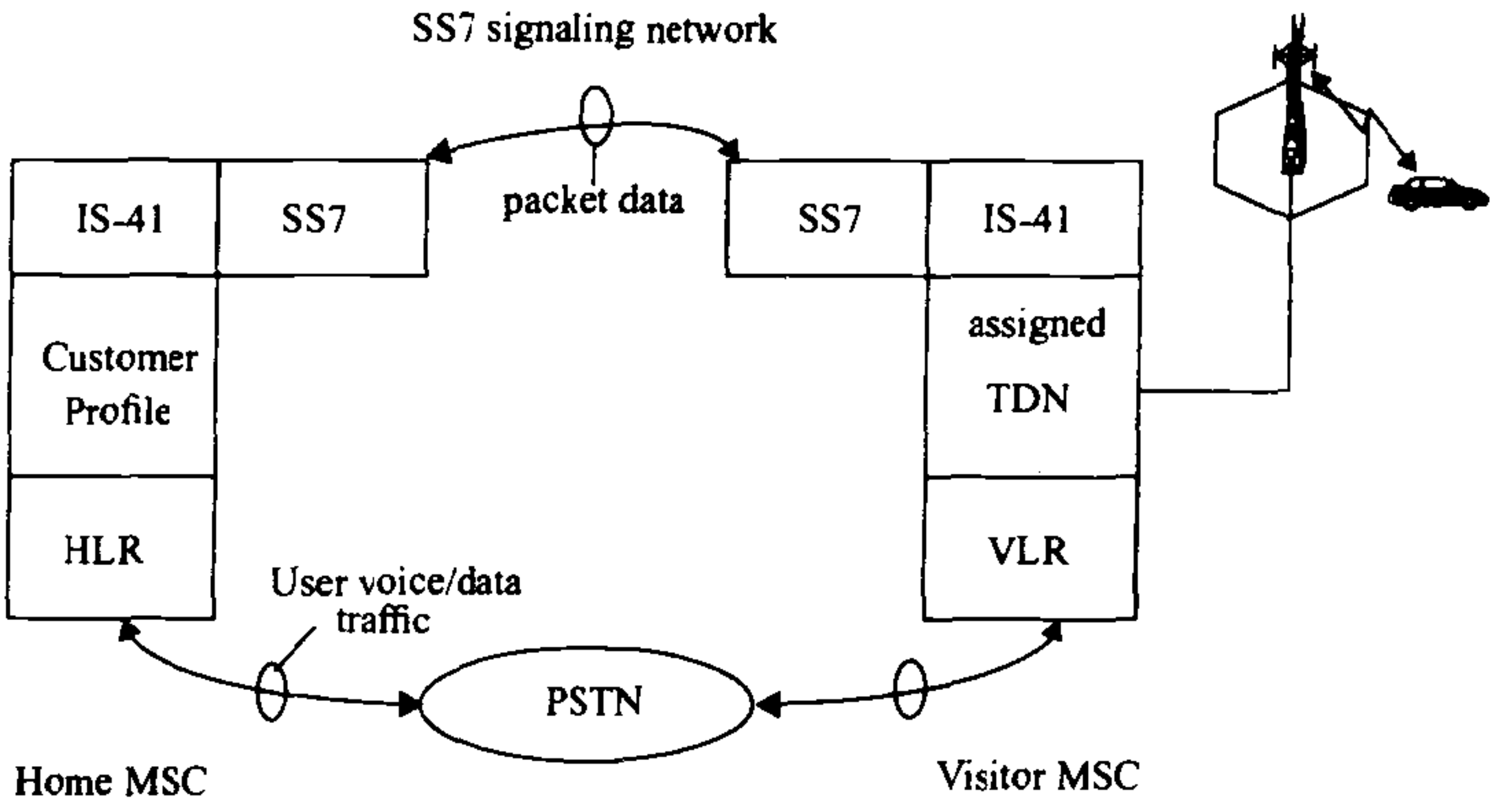



**Communication signaling between mobile, base station, and MSC in first generation wireless networks.**

- The figure, shows a diagram of a first generation cellular radio network, which includes the mobile terminals, the base stations, and MSCs.
- In first generation cellular networks, the system control for each market resides in the MSC, which maintains all mobile related information and controls each mobile handoff.



- When the user roams into a new market covered by a different service provider, the wireless network must register the user in the new area and cancel its registration with the previous service provider so that calls may be routed to the roamer as it moves through the coverage areas of different MSCs.




**The North American Cellular Network architecture used to provide user traffic and signaling traffic between MSCs**

## Second Generation Wireless Networks

- Second generation wireless systems employ digital modulation and advanced call processing capabilities. Examples of second generation wireless systems include the **Global System for Mobile** (GSM).
- All second generation systems use **digital voice coding and digital modulation**.
- The systems employ dedicated control channels within the air interface for simultaneously exchanging voice and control information between the subscriber, the base station and the MSC while a call is in progress.

## Third Generation Wireless Networks

- The aim of third generation wireless networks is to provide a **single set of standards** that can meet a wide range of wireless applications and provide universal access throughout the world.
- In third generation wireless systems, the distinctions between cordless telephones and cellular telephones will disappear, and a universal personal communicator (a personal handset) will provide access to a variety of **voice, data, and video communication services.**
- Third generation systems will use the Broadband Integrated Services Digital Network (**B-ISDN**) to provide access to information networks, such as the Internet and other public and private databases.

- Third generation networks will carry many types of information (voice, data, and video), will operate in varied regions.
- The terms Personal Communication System **(PCS)** and Personal Communication Network **(PCN)** are used to imply emerging third generation wireless systems for hand-held devices.
- Other names for PCS include Future Public Land Mobile Telecommunication Systems **(FPLMTS)** for worldwide use which has more recently been called International Mobile Telecommunication **(IMT-2000),** and Universal Mobile Telecommunication System **(UMTS)** for advanced mobile personal services.

# Traffic Routing in Wireless Networks

- The amount of traffic capacity required in a wireless network is highly dependent upon the type of traffic carried.
- Two general routing services are provided by networks. These are
  - connection- oriented services (virtual circuit routing), and
  - connectionless services (datagram services).

- In **connection-oriented routing**, the communications path between the message source and destination is fixed for the entire duration of the message, and a call set-up procedure is required to dedicate network resources to both the called and calling parties.

- Connectionless routing, on the other hand, does not establish a firm connection for the traffic, and instead relies on packet-based transmissions.

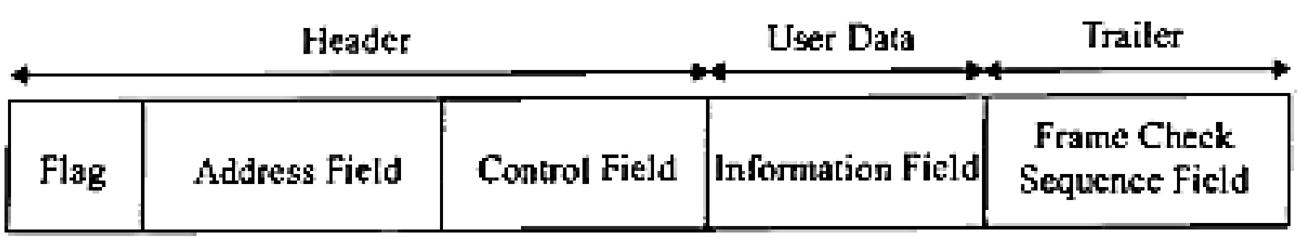
## Circuit Switching

- First generation cellular systems provide connection-oriented services for each voice user.
- Circuit switching establishes a dedicated connection (a radio channel between the base and mobile, and a dedicated phone line between the MSC and the PSTN) for the entire duration of a call.
- Wireless data networks are not well supported by circuit switching

# Packet Switching

- Packet switching (also called virtual switching) is the most common technique used to implement connectionless services and allows a large number of data users to remain virtually connected to the same physical channel in the network.


**Packet data format**




**Fields in a typical packet of data.**

# Wireless Data Services

- U.S. cellular industry developed the cellular digital packet data (CDPD) standard to coexist with the conventional voice only cellular system.
- In the 1980s, two other data-only mobile services called ABDIS and RMD were developed to provide packet radio connectivity throughout a network.

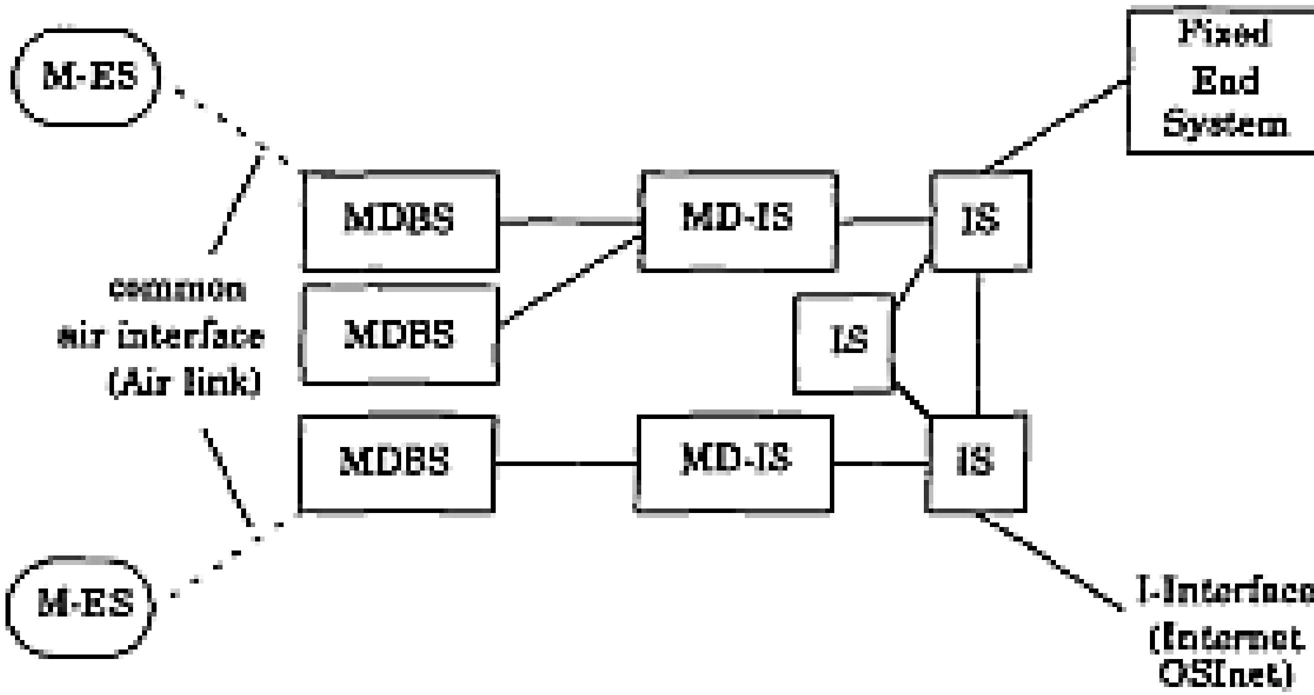
## Cellular Digital Packet Data (CDPD)

- CDPD is a data service for first and second generation U.S. cellular systems and uses a full 30 kHz AMPS channel on a shared basis.
  - The mobile data link protocol (MDLP)
  - Radio resource management protocol (RRMP)

Table 9.2 Link Layer Characteristics for CDPD

| | |
|---|---|
| Protocols | MDLP, RRMP, X.25 |
| Channel Data Rate (bps) | 19,200 |
| Channel Bandwidth (kHz) | 30 |
| Spectrum Efficiency (b/Hz) | 0.64 |
| Random Error Strategy | cover with burst protect |
| Burst Error Strategy | RS 63,47 (6 bits per symbol) |
| Fading Performance | withstands 2.2 ms fade |
| Channel Access | slotted DSMA/CD |

# CDPD Network




**M-ES** : Mobile End Station
**MDBS** : Mobile Data Base Station
**MD-IS** : Intermediate Server for CDPD traffic

## Advanced Radio Data Information Systems (ARDIS)

- Advance Radio Data Information Systems (ARDIS) is a private network service provided by Motorola and IBM.
- ARDIS provides 800 MHz two-way mobile data communications for short-length radio messages in urban and in-building environments, and for users traveling at low speeds.

## RAM Mobile Data (RMD)

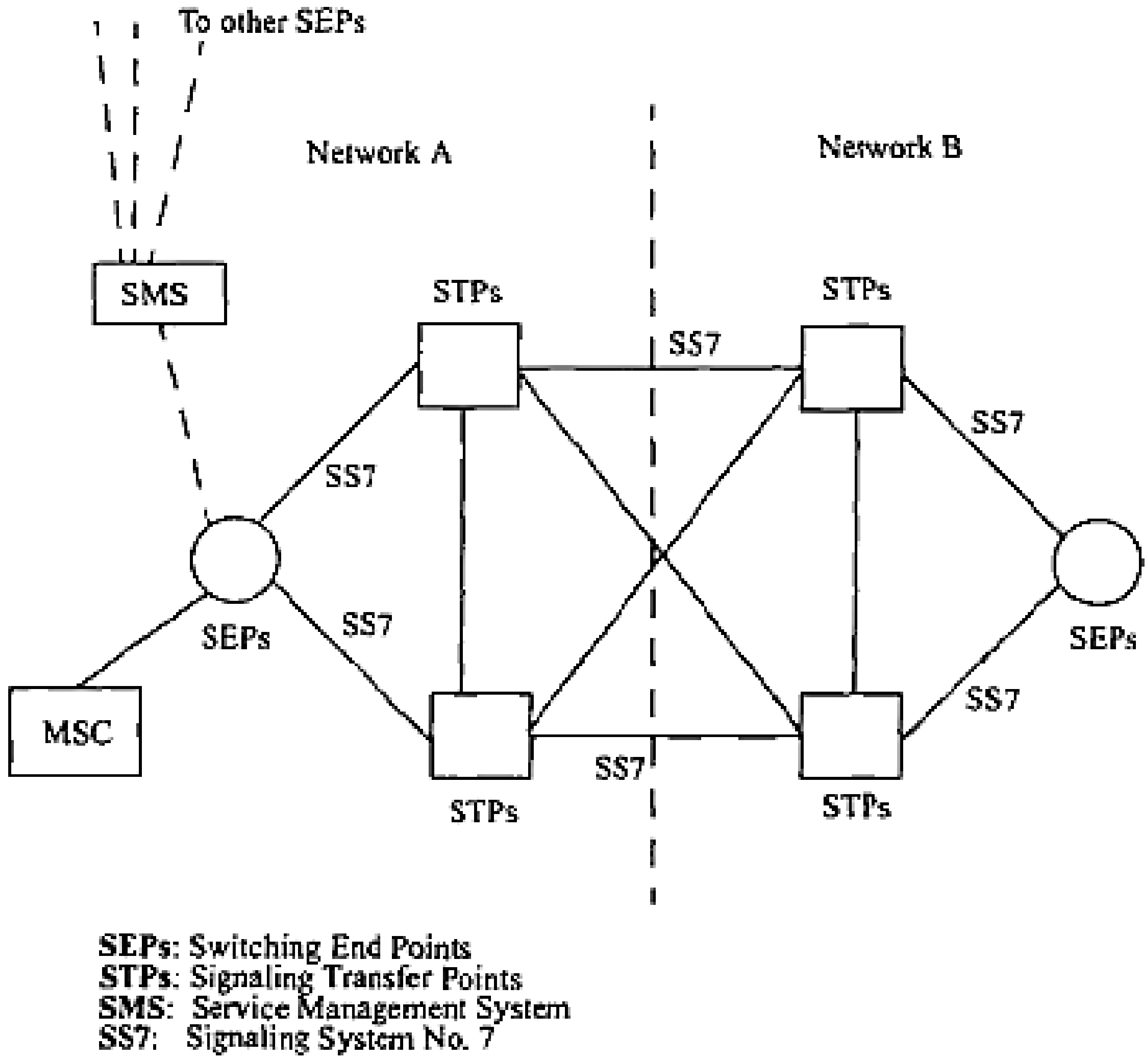
- RAMMobile Data (RMD) is a public, two-way data service based upon the Mobitex protocol developed by Ericsson.
- RAM provides street level coverage for short and long messages for users moving in an urban environment.

# Common Channel Signaling (CCS)

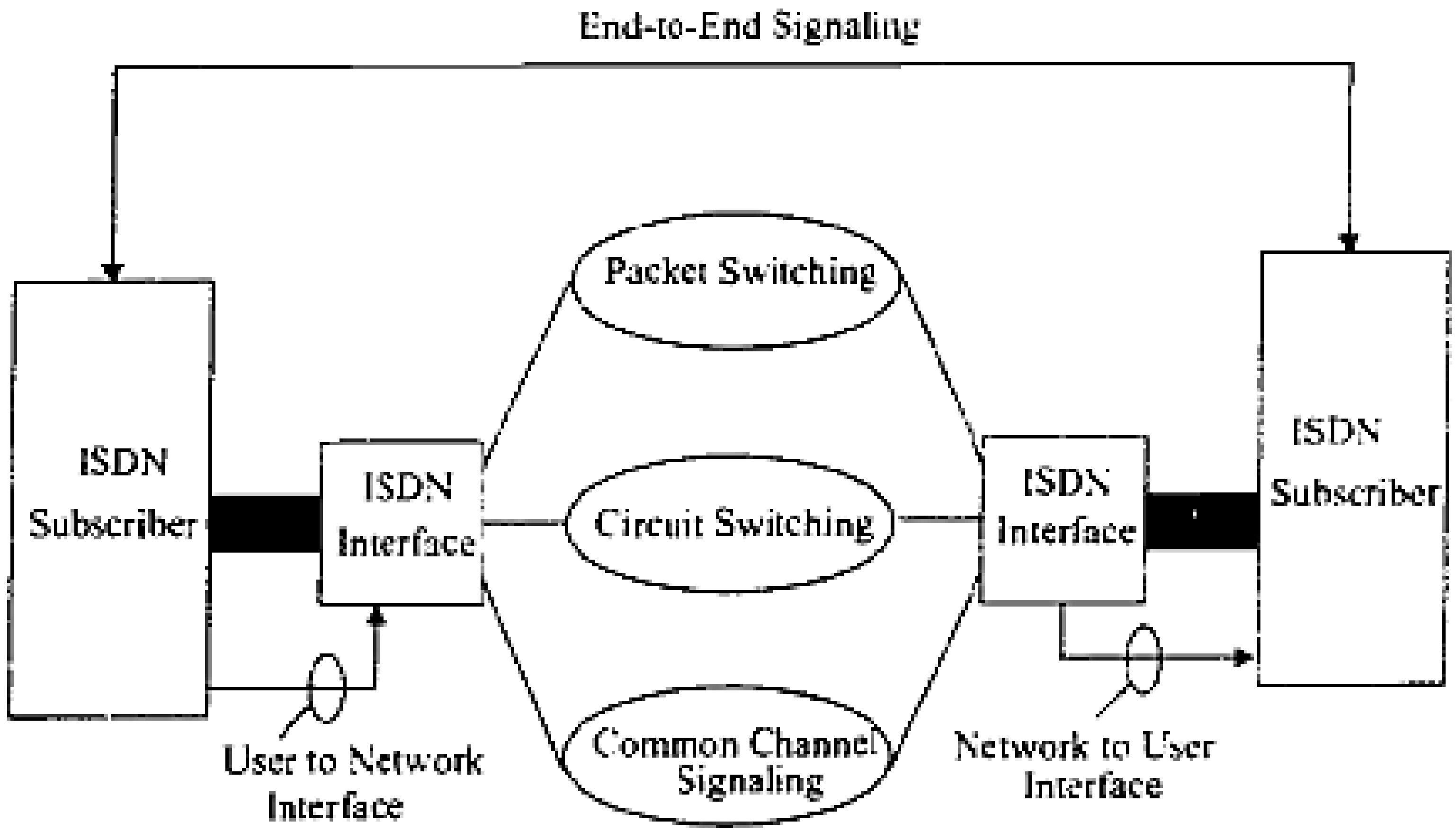
- Common channel signaling (CCS) is a digital communications technique that provides simultaneous transmission of user data, signaling data, and other related traffic throughout a network.

- This is accomplished by using out-of-band signaling channels which logically separate the network data from the user information (voice or data) on the same channel.

# The Distributed Central Switching Office for CCS

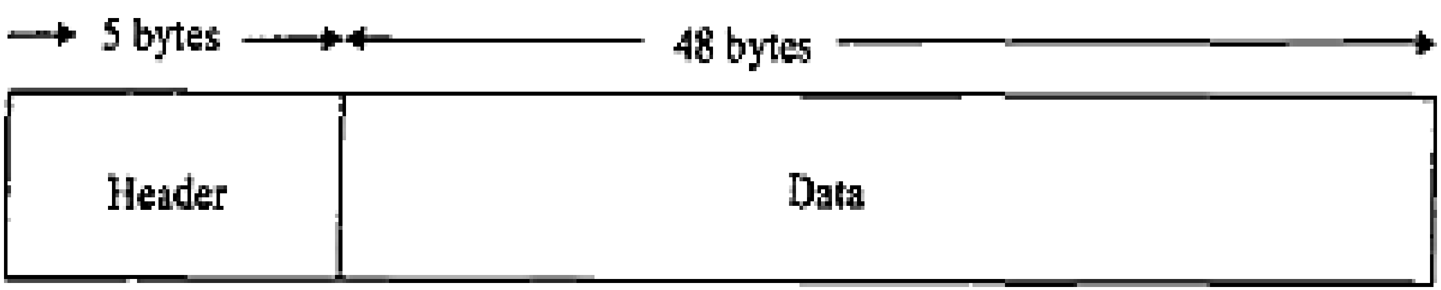


# Integrated Services Digital Network (ISDN)



## Broadband ISDN and ATM

- Recent work has defined ISDN interface standards that increase the end-user transmission bandwidth to several Mb/s.
- This emerging networking technique is known as broadband ISDN (B-ISDN) and is based on asynchronous transfer mode (ATM) technology which allows packet switching rates up to 2.4 Gbps

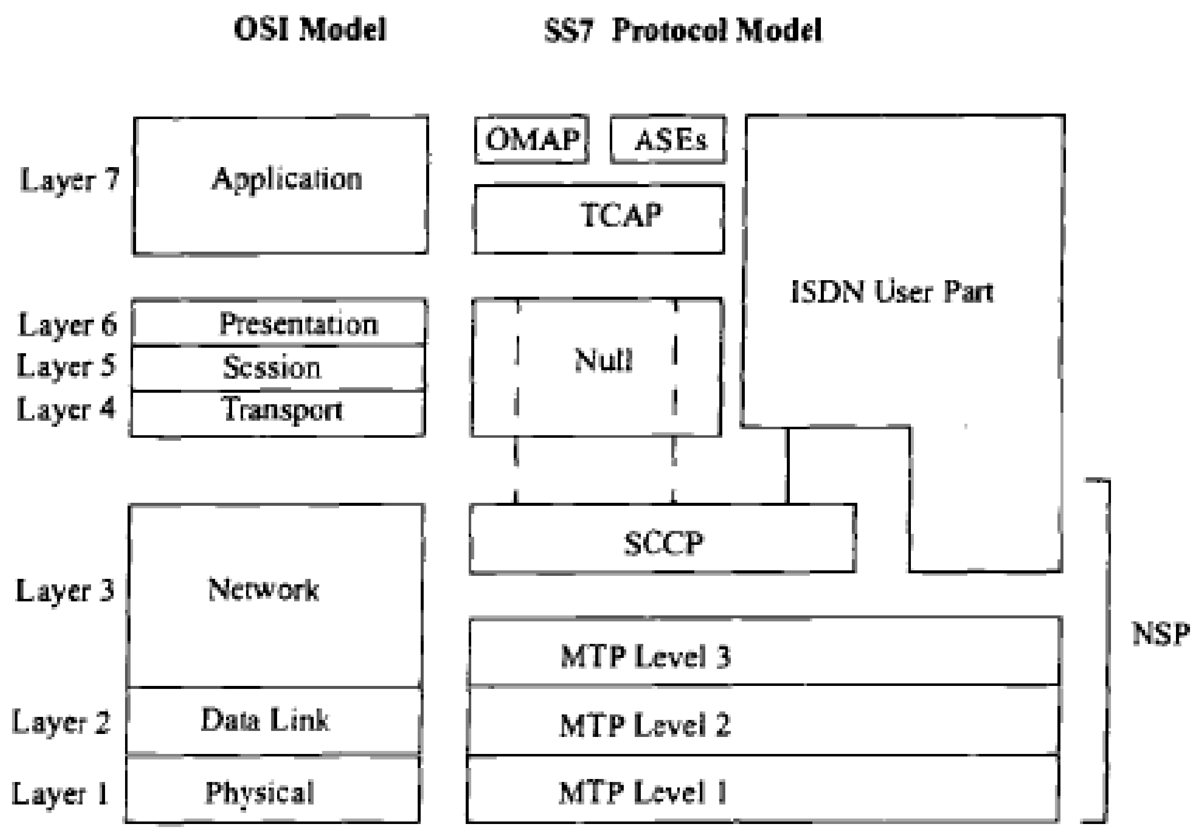


# Signaling System No. 7(SS7)

- The SS7 signaling protocol is widely used for common channel signaling between interconnected networks.

**Network Services Part (NSP) of SS7**

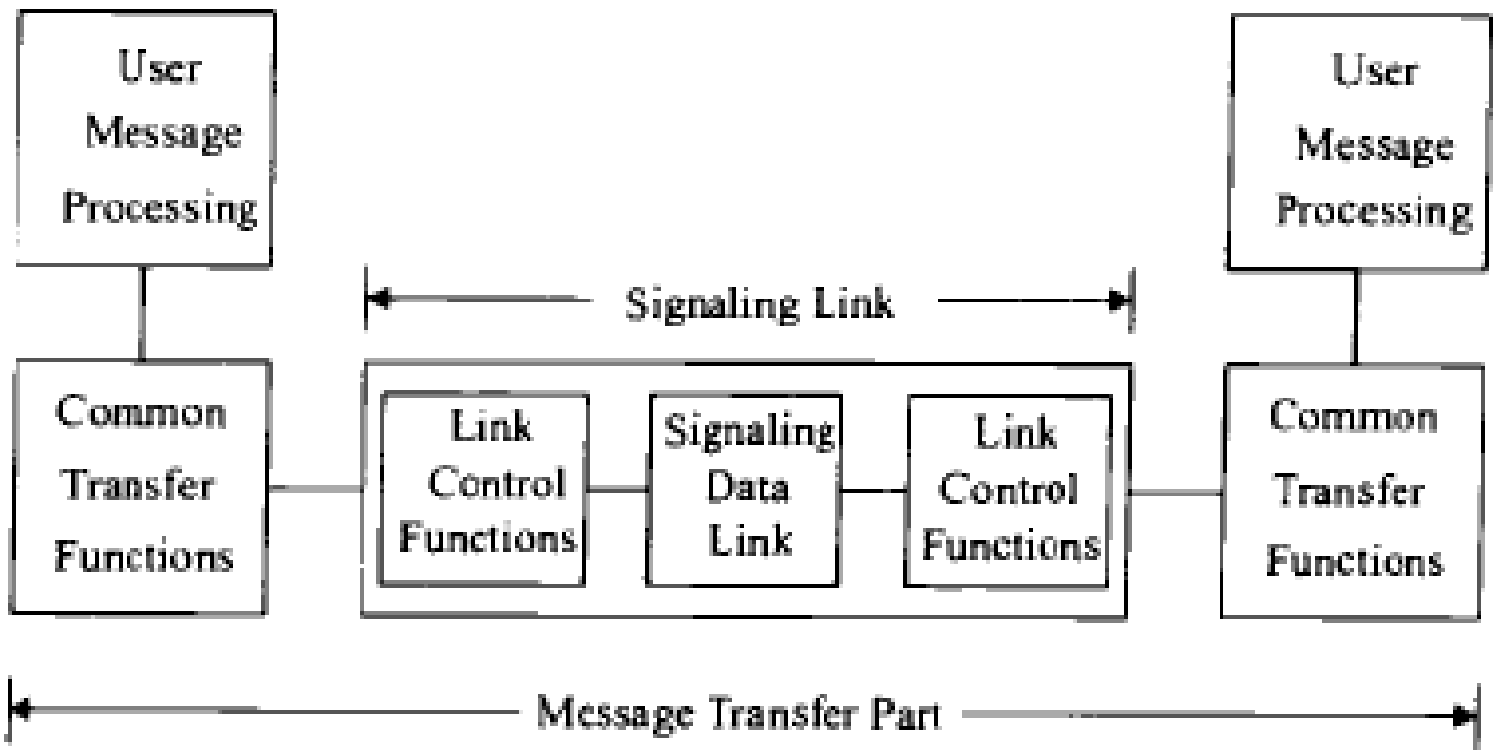
- The NSP provides ISDN nodes with a highly reliable and efficient means of exchanging signaling traffic using connectionless services. The SCCP in SS7 actually supports packet data network interconnections as well as connection oriented networking to virtual circuit networks




**OMAP**: Operations Maintenance and Administration Part
**ASE**: Application Service Element
**TCAP**: Transaction Capabilities Application Part
**SCCP**: Signaling Connection Control Part
**MTP**: Message Transfer Part
**NSP**: Network Service Part

# SS7 protocol architecture

- Signaling data link functions (MTP Level 1) provide an interface to the actual physical channel over which communication takes place.
- Signaling link functions (MTP Level 2) correspond to the second layer in the OSI reference model and provide a reliable link for the transfer of traffic between two directly connected signaling points.
- Signaling network functions (MTP Level 3) provide procedures that transfer messages between signaling nodes. As in ISDN, there are two types of MTP Level 3 functions.




**Functional diagram of message transfer part**

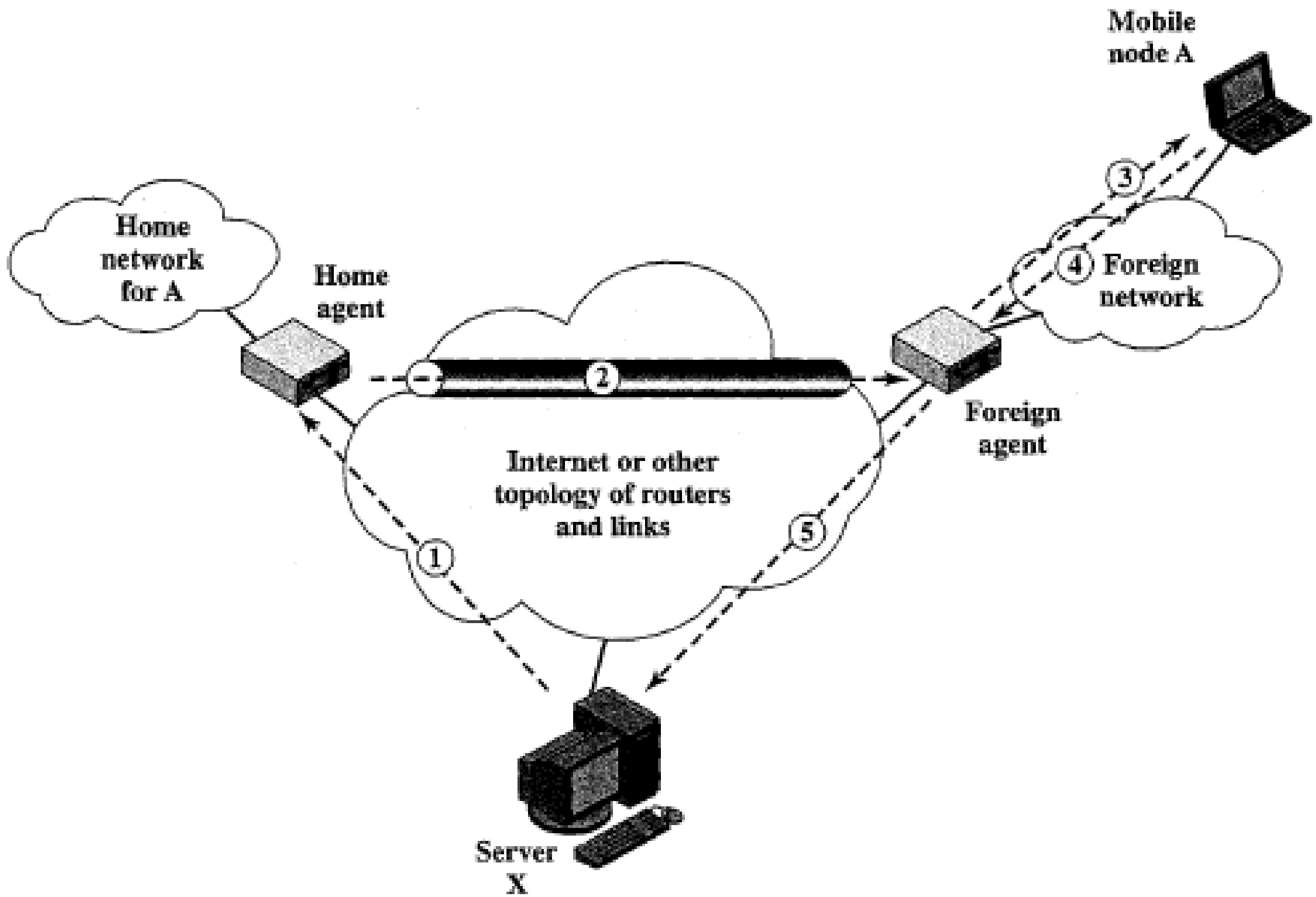
# MOBILE IP

- The term mobile in this context implies that a user is connected to one or more applications across the Internet, that the user's point of attachment changes dynamically, and that all connections are automatically maintained despite the change.

# Operation of Mobile IP

- Routers make use of the IP address in an IP datagram to perform routing.
- In particular, the **network portion** of an IP address is used by routers to move a datagram from the source computer to the network to which the target computer is attached.
- Then the final router on the path, which is attached to the same network as the target computer, uses the **host portion** of the IP address to deliver the IP datagram to the destination.

- A mobile node is assigned to a particular network, known as its **home network.** Its IP address on that network, known as its **home address,** is static.
- When the mobile node moves its attachment point to another network, that network is considered a **foreign network** for this host.
- Once the mobile node is reattached, it makes its presence known by registering with a network node, typically a router, on the foreign network known as a **foreign agent**.
- The mobile node then communicates with a similar agent on the user's home network, known as a **home agent**, giving the home agent the **care-of address** of the mobile node.

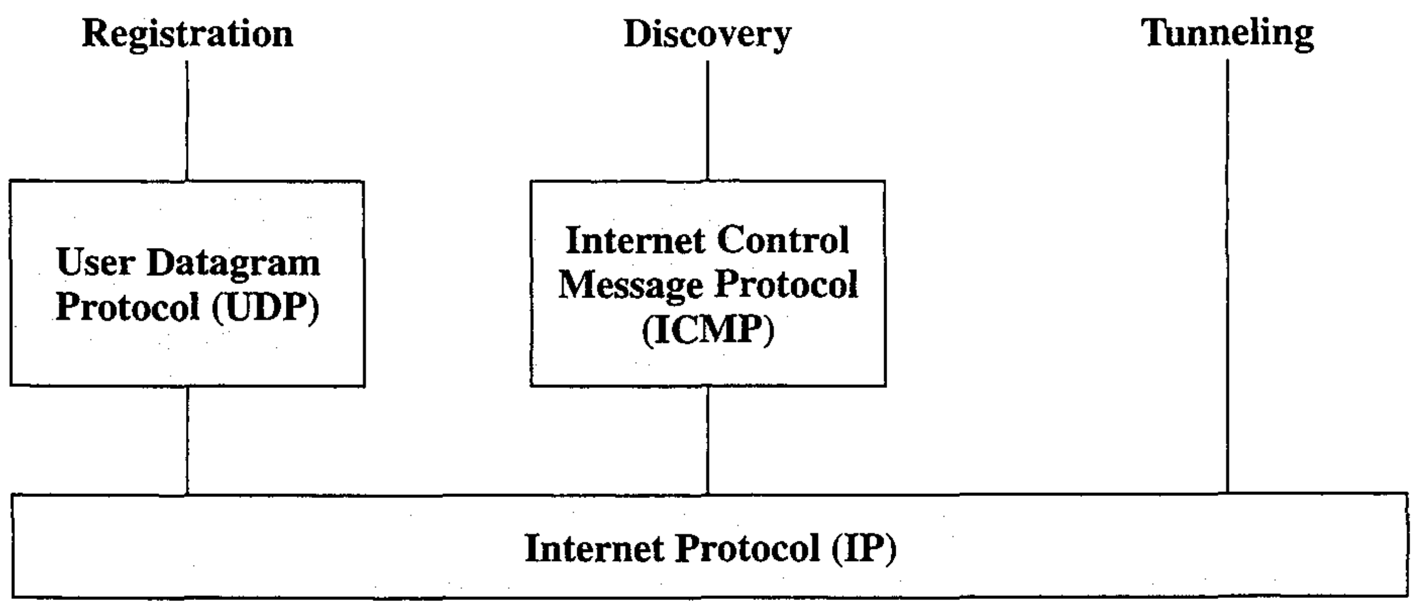



**Mobile IP Scenario**

- To support the operations Mobile IP includes three basic capabilities:
    - **Discovery:** A mobile node uses a discovery procedure to identify prospective home agents and foreign agents.
    - **Registration:** A mobile node uses an authenticated registration procedure to inform its home agent of its care-of address.
    - **Tunneling:** Tunneling is used to forward IP datagrams from a home address to a care-of address.

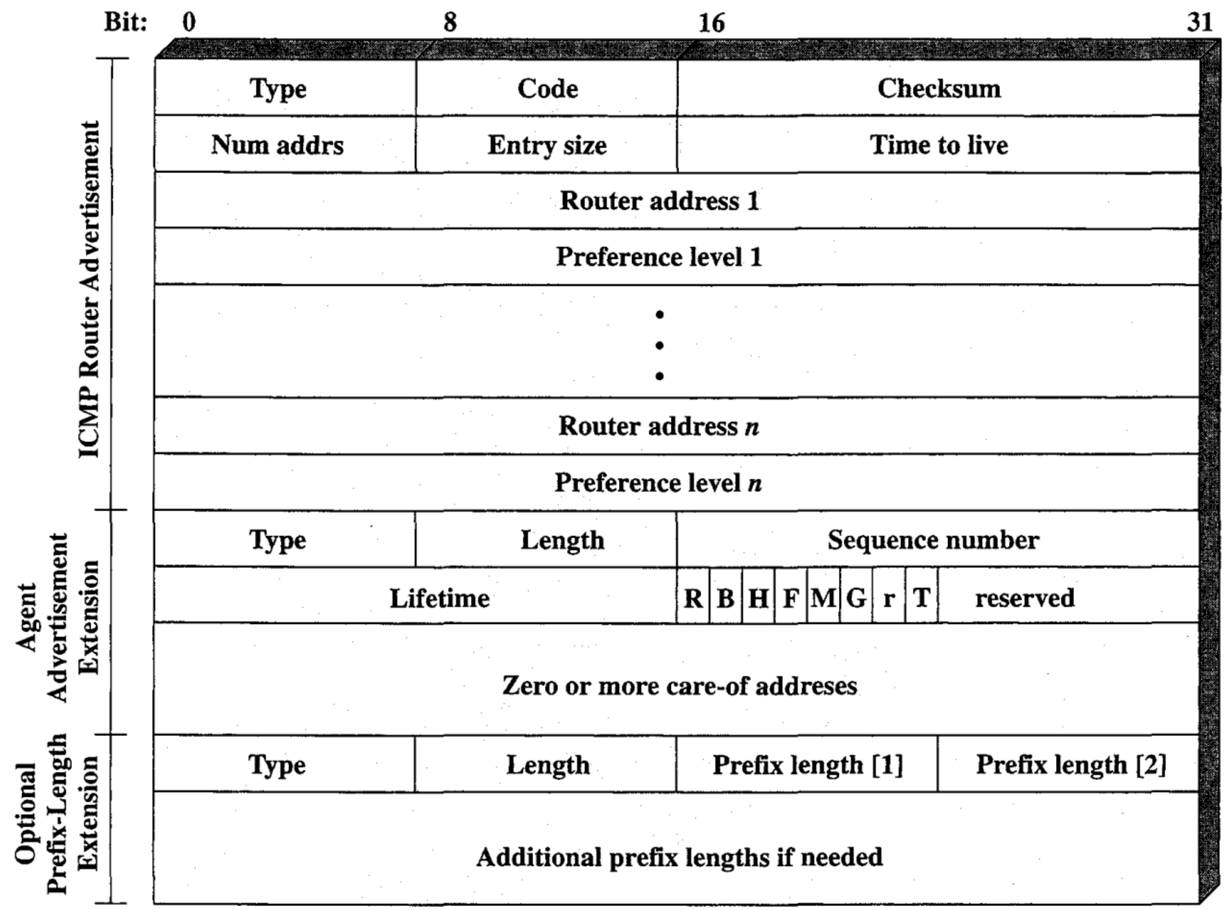
# Discovery

- The discovery process in Mobile IP is very similar to the router advertisement process defined in ICMP **(Internet Control Message Protocol).** Accordingly, agent discovery makes use of ICMP router advertisement messages, with one or more extensions specific to Mobile IP.




**Protocol Support for Mobile IP**

- The router advertisement portion of the message includes the IP address of the router.
- The advertisement extension includes additional information about the router's role as an agent.
- A mobile node listens for these agent advertisement messages.



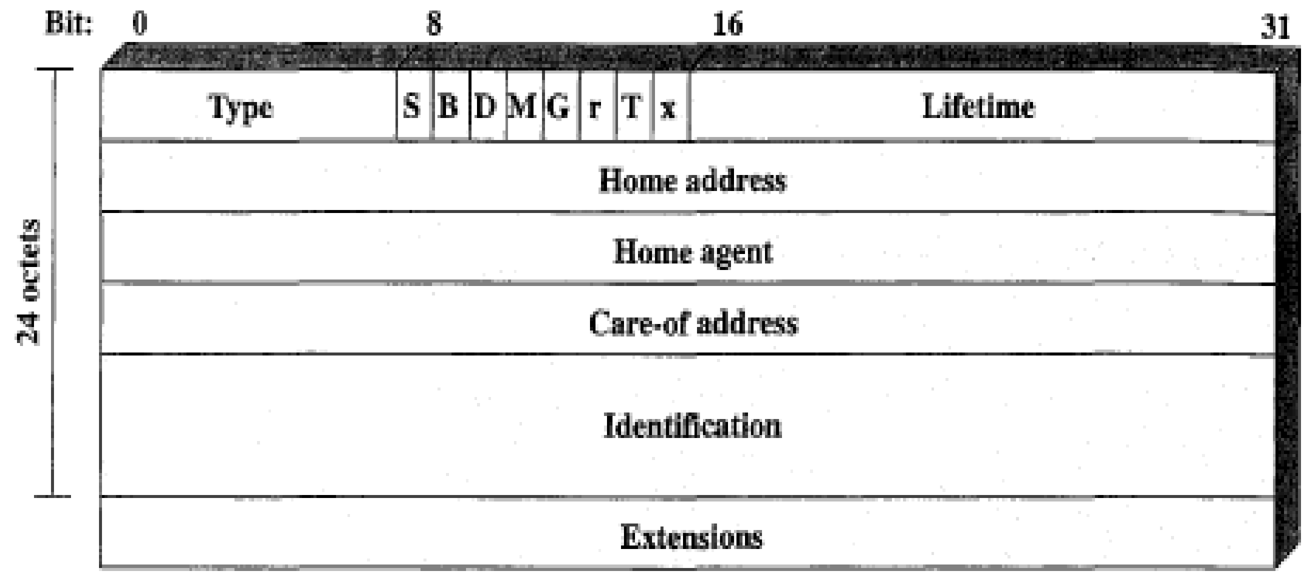

**Mobile IP Agent Advertisement Message**

- The agent advertisement extension follows the ICMP router advertisement fields and consists of the following fields.
- • **Type**: 16, indicates that this is an agent advertisement.
- • **Length**: Number of bytes in the extension, excluding the Type and Length fields.
- • **Sequence Number**: The count of agent advertisement messages sent since the agent was initialized.
- • **Lifetime**: The longest lifetime, in seconds, that this agent is willing to accept a registration request from a mobile node.
- • **R**: Registration with this foreign agent is required. Even those mobile nodes that have already acquired a care-of address from this foreign agent must re-register.
- **B:** Busy. The foreign agent will not accept registrations from additional mobile nodes.
- • **H:** This agent offers services as a home agent on this network.
- • **F:** This agent offers services as a foreign agent on this network.

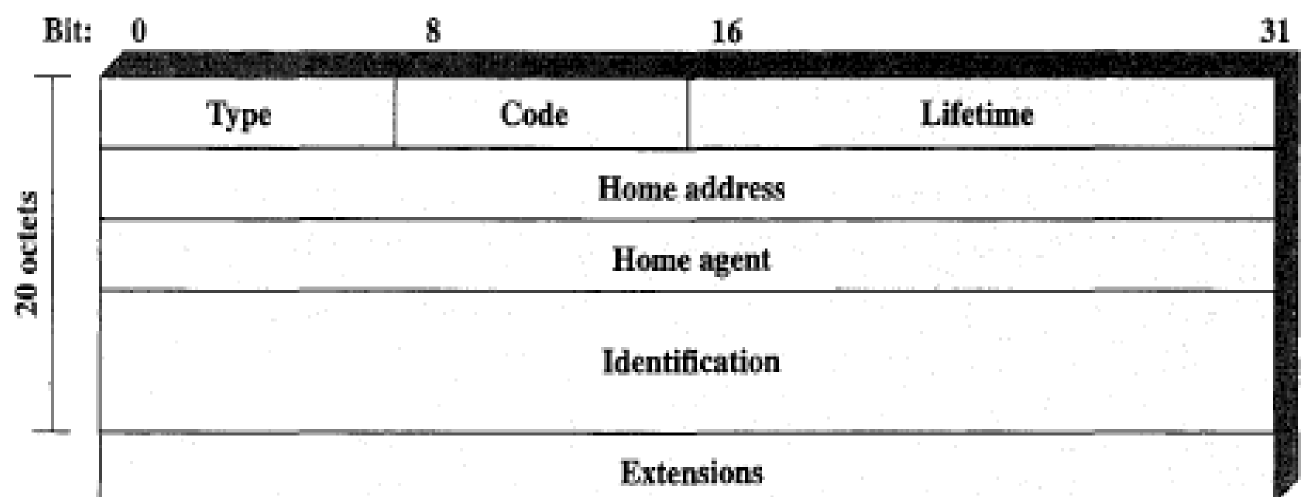
- • **M:** This agent can receive tunneled IP datagrams that use minimal encapsulation
- • **G:** This agent can receive tunneled IP datagrams that use GRE encapsulation.
- • **r:** reserved.
- • **T:** Foreign agent supports reverse tunneling.
- • **Care-Of Address:** The care-of address or addresses supported by this agent on this network.

## Registration

- The registration process involves four steps:
- 1. The mobile node requests the forwarding service by sending a registration request to the foreign agent.
- 2. The foreign agent relays this request to the mobile node's home agent.
- 3. The home agent either accepts or denies the request and sends a registration reply to the foreign agent.
- 4. The foreign agent relays this reply to the mobile node.




(a) Registration request message




(b) Registration reply message

# Mobile IP Registration Messages

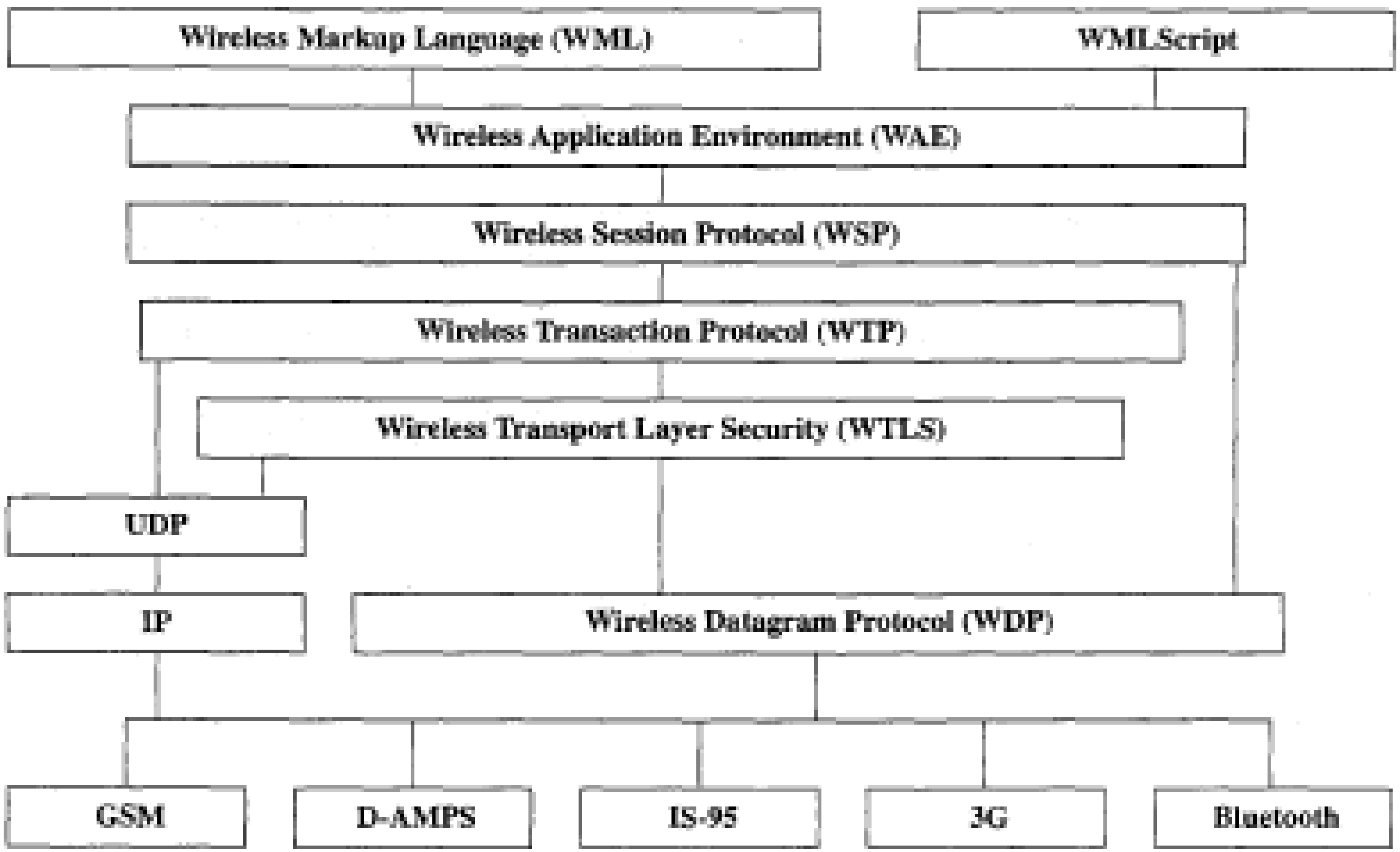
**Tunneling**

- Once a mobile node is registered with a home agent, the home agent must be able to intercept IP datagrams sent to the mobile node's home address so that these datagrams can be forwarded via tunneling.
- The standard does not mandate a specific technique for this purpose but references ARP (Address Resolution Protocol) as a possible mechanism.

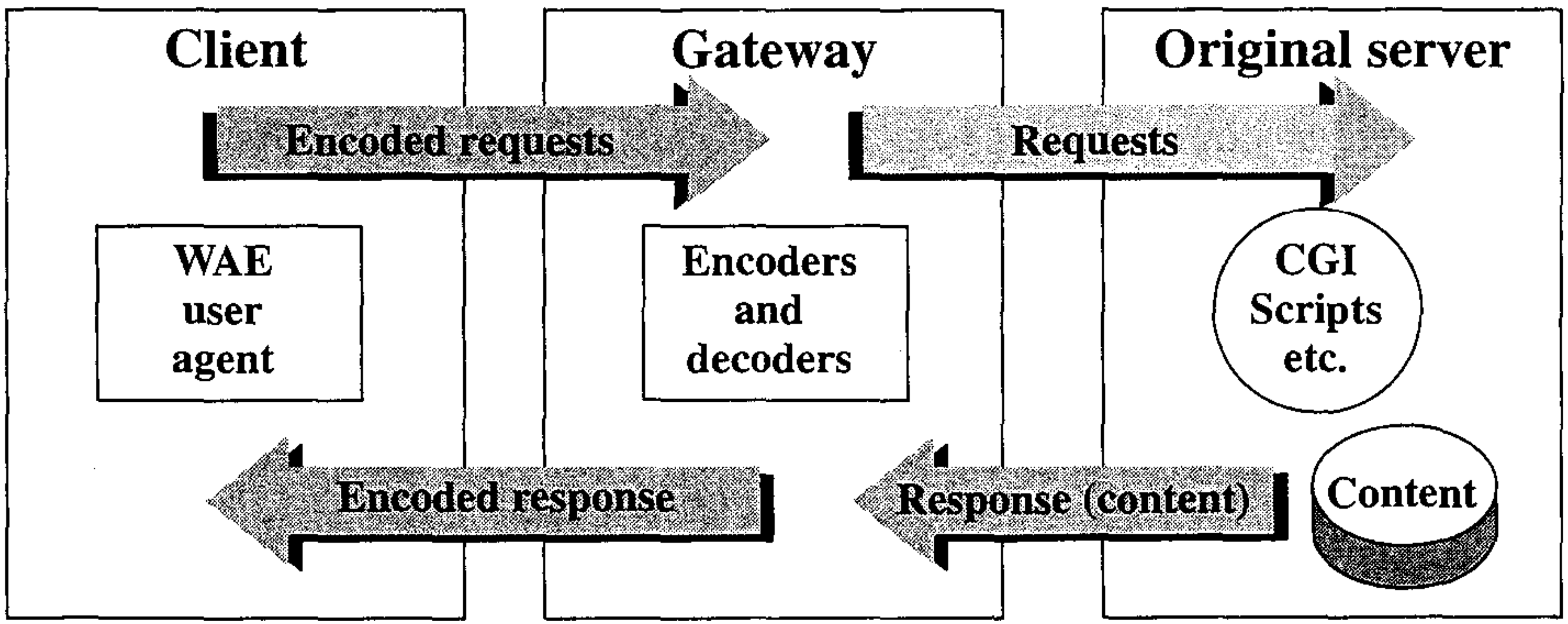
# WIRELESS APPLICATION PROTOCOL

- The Wireless Application Protocol (WAP) is a universal, open standard developed by the WAP Forum to provide mobile users of wireless phones and other wireless terminals .
- WAP is designed to work with all wireless network technologies (e.g., GSM, CDMA, and TDMA).

- The WAP specification includes
- • A programming model based on the WWW Programming model
- A markup language, the Wireless Markup Language, adhering to XML
- A specification of a small browser suitable for a mobile, wireless terminal
- A lightweight communications protocol stack
- • A framework for wireless telephony applications (WTAs)




**WAP Protocol Stack**


Client
Gateway
Original server
Encoded requests
Requests
WAE
user
agent
Encoders
and
decoders
CGI
Scripts
etc.
Encoded response
Response (content)
Content

# Wireless Markup Language

- WML was designed to describe content and format for presenting data on devices with limited bandwidth, limited screen size, and limited user input capability.
- It is designed to work with telephone keypads, styluses, and other input devices common to mobile, wireless communication.
- Text and image support: Formatting and layout commands are provided for text and limited image capability.
- Support for navigation among cards and decks: WML includes provisions for event handling, which is used for navigation or executing scripts.

# WML Script

- WML Script is a scripting language with similarities to JavaScript.
- It is designed for defining script-type programs in a user device with limited processing power and memory.

| Tag | Description |
|---|---|
| | **Deck Structure** |
| <access> | Access control |
| <card> | Card definition |
| <head> | Deck-level information (meta, access, template) |
| <meta> | Meta information |
| <template> | Deck-level event bindings |
| <wml> | Deck definition |
| | **Content** |
| <img> | Image |
| <p> | Paragraph, visible content |
| <table> | Table |
| <td> | Table data |
| <tr> | Table row |
| | **Formatting** |
| <b> | Bold |
| <big> | Large font |
| <br> | Line break |
| <em> | Emphasis |
| <i> | Italic |
| <small> | Small font |
| <strong> | Strong font |
| <u> | Underline |

| Tag | Description |
|---|---|
| | **User Input** |
| <fieldset> | Data entry items grouping |
| <input> | Data entry |
| <optgroup> | Subset of a choice list |
| <option> | Single choice in a list |
| <select> | Choice list |
| | **Variables** |
| <postfield> | Set an http request variable |
| <setvar> | Set a variable in a task |
| | **Timers** |
| <Timer> | Set a timer |
| | **Tasks** |
| <go> | Go to a URL |
| <noop> | No action |
| <prev> | Go to previous card |
| <refresh> | Screen redraw |
| | **Task/Event Bindings** |
| <a> | Abbreviated anchor |
| <anchor> | Anchor |
| <do> | Response to user button press |
| <onevent> | Intrinsic event binding |

**WML Tags**

| Statement | Description |
| --- | --- |
| = | Assignment |
| break | Terminate the current loop |
| continue | Current loop iteration |
| for | Indexed loop |
| function | Function declaration |
| if..else | Conditional test |
| return | Exit the current function |
| var | Variable declaration |
| while | Boolean-controlled loop |

**WML Script Statements**

# Wireless Session Protocol

- WSP provides applications with an interface for two session services.
- The connection oriented session service operates above the reliable transport protocol WTP, and the connectionless session service operates above the unreliable transport protocol WDP.
- WSP Service In general, a connection-mode WSP provides the following services:
- Establish a reliable session from client to server and release that session in an orderly manner.
- Agree on a common level of protocol functionality using capability negotiation.
- Exchange content between client and server using compact encoding.

- Suspend and resume a session.
- Push content from server to client.
- Session establishment

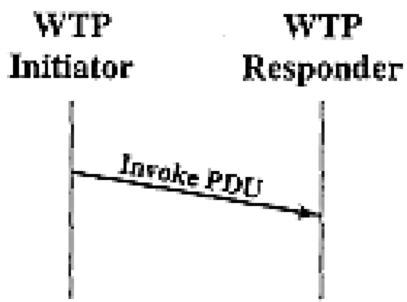
- **Server address:** The peer with which the session is to be established.
- **Client address:** The originator of the session.
- **Client headers:** Contain attribute information that can be used for application level parameters to be communicated to the peer.

# Wireless Transaction Protocol

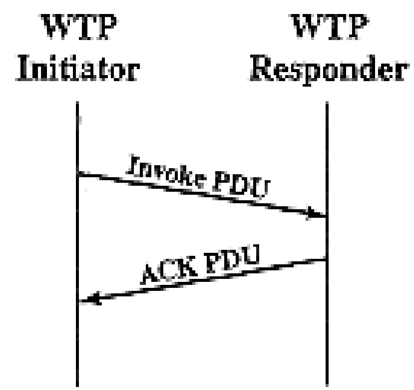
- WTP manages transactions by conveying requests and responses between a user agent (such as a WAP browser) and an application server for such activities as browsing and e-transactions.
- WTP includes the following features:
- Three classes of transaction service.
- Optional user-to-user reliability: WTP user triggers the confirmation of each received message.
- Optional out-of-band data on acknowledgments.
- Asynchronous transactions.

**WTP Transaction Classes**

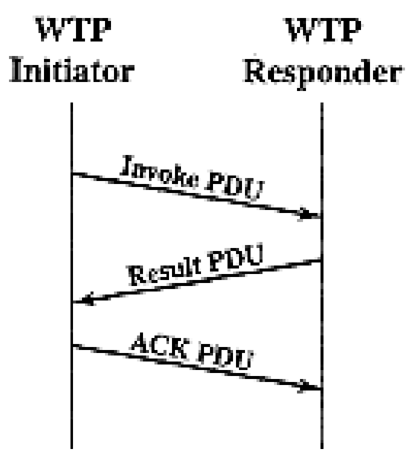
- WTP provides three transaction classes that may be invoked by WSP or another higher layer protocol:
- **Class 0:** Unreliable invoke message with no result message
- **Class 1:** Reliable invoke message with no result message
- **Class 2:** Unreliable invoke message with one reliable result message



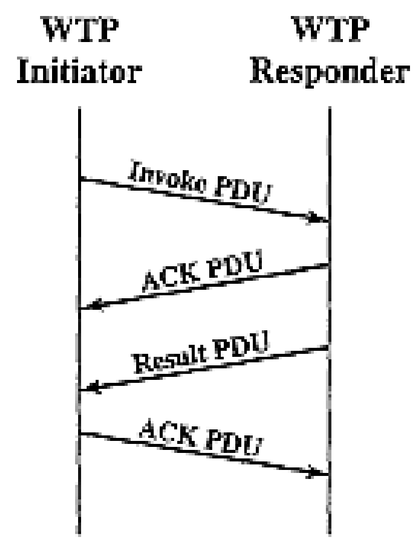

(a) Basic Class 0 transaction




(b) Basic Class 1 transaction




(c) Basic Class 2 transaction




(d) Class 2 transaction with "hold on" acknowledgment

# Wireless Datagram Protocol

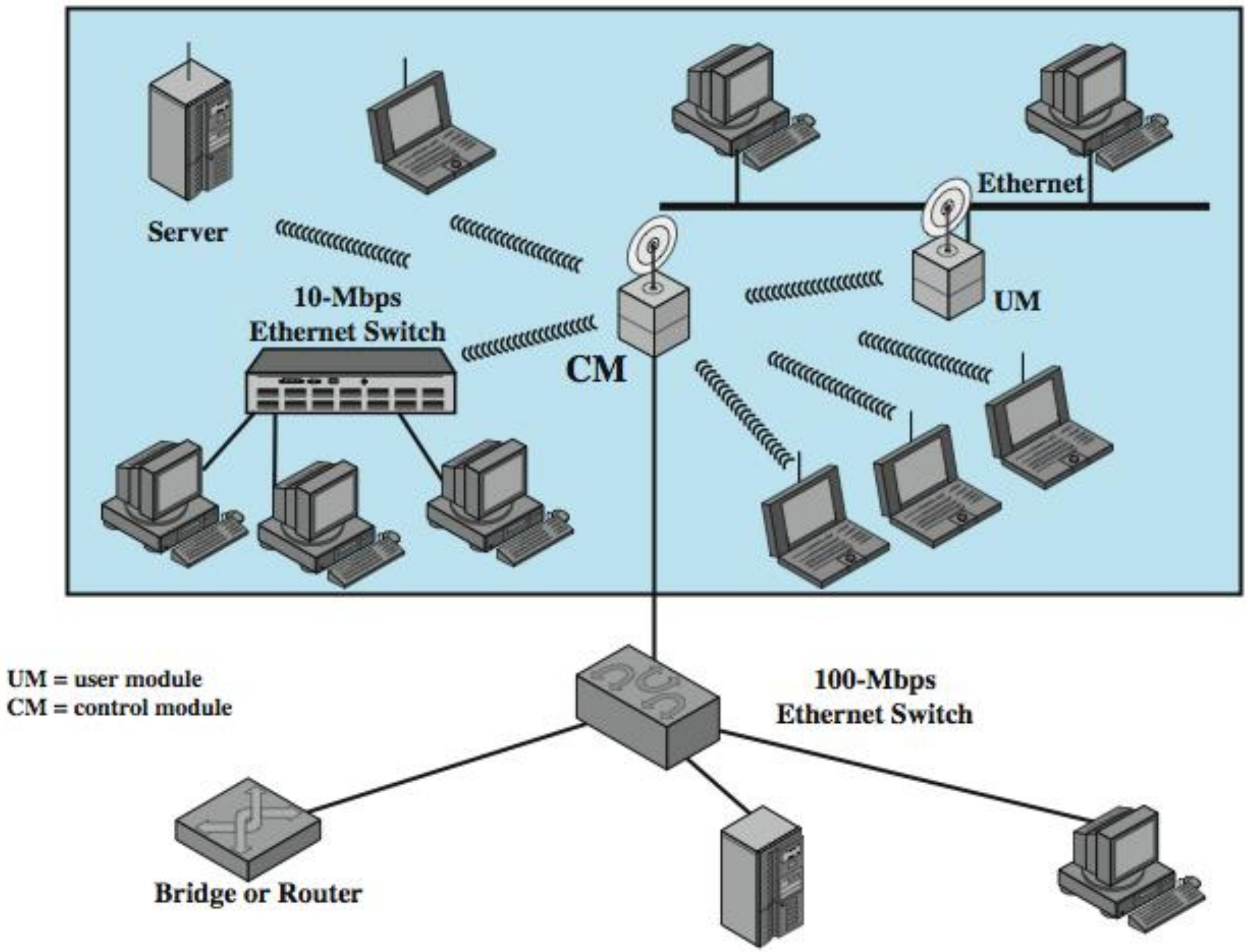
- WDP is used to adapt a higher-layer WAP protocol to the communication mechanism (called the bearer) used between the mobile node and the WAP gateway.
- service with the following parameters:
- • **Source address**: Address of the device making a request to the WDP layer
- • **Source port:** Application address associated with the source address
- • **Destination address:** Destination address for the data submitted to WDP
- • **Destination port:** Application address associated with the destination address
- • **User data:** User data from the next higher layer, submitted to WDP for transmission to the destination port

- The following fields are necessary in a WDP PDU:
- • Header length (1 byte): Length of header.
- • Port numbers identifier (1 byte)
- • Port numbers length (1 byte)
- • Destination port (2 bytes)
- • Source port (2 bytes)
- SAR identifier (1 byte)
- SAR length (1 byte)
- Datagram reference number (1 bytes)
- Number of segments (1 byte)
- Segment count
- User data (1 to n bytes)

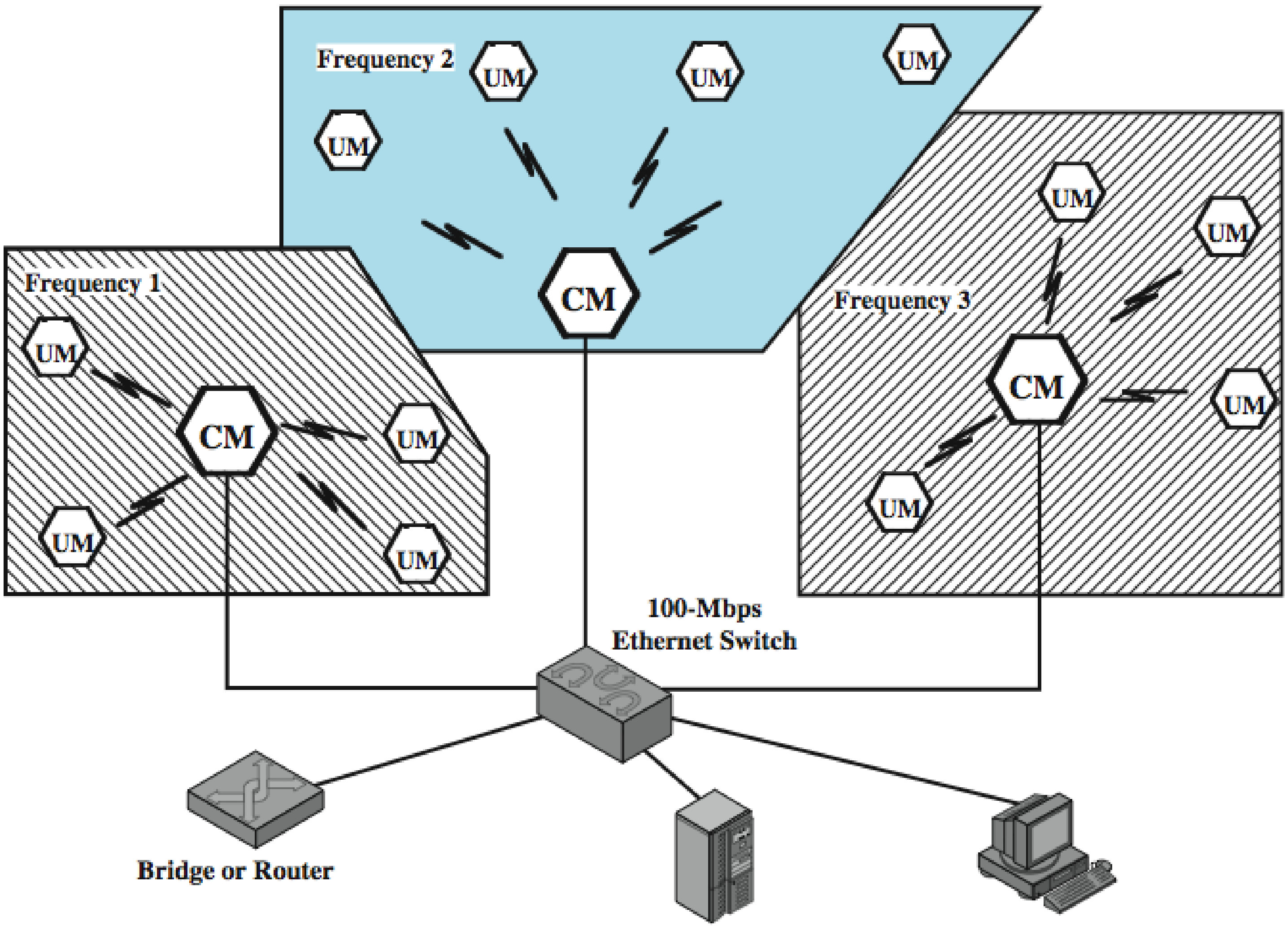
# Overview of Wireless LANs

- use wireless transmission medium
- issues of high prices, low data rates, occupational safety concerns, & licensing requirements now addressed
- key application areas:
  - LAN extension
  - cross-building interconnect
  - ad hoc networking

# Single Cell LAN Extension



# Multi Cell LAN Extension



# Infrared LANs

- constructed using infrared portion of spectrum
- strengths
  - spectrum virtually unlimited hence high rates possible
  - unregulated spectrum
  - infrared shares some properties of visible light
  - inexpensive and simple
- weaknesses
  - background radiation, e.g. sunlight, indoor lighting
  - power limited by concerns for eye safety and power consumption

# Infrared LANs Transmission Techniques

- directed-beam IR
  - point-to-point links
  - range depends on power and focusing
  - for indoor use can set up token ring LAN
  - IR transceivers positioned so data circulates in ring
- omnidirectional
  - single base station with line of sight to other stations
  - acts as a multiport repeater
  - other stations use directional beam to it
- diffused configuration
  - stations focused / aimed at diffusely reflecting ceiling

# Spread Spectrum LAN Configuration

- usually use multiple-cell arrangement
- adjacent cells use different center frequencies
- configurations:
  - hub
    - connected to wired LAN
    - connect to stations on wired LAN and in other cells
    - may do automatic handoff
  - peer-to-peer
    - no hub
    - MAC algorithm such as CSMA used to control access
    - for ad hoc LANs

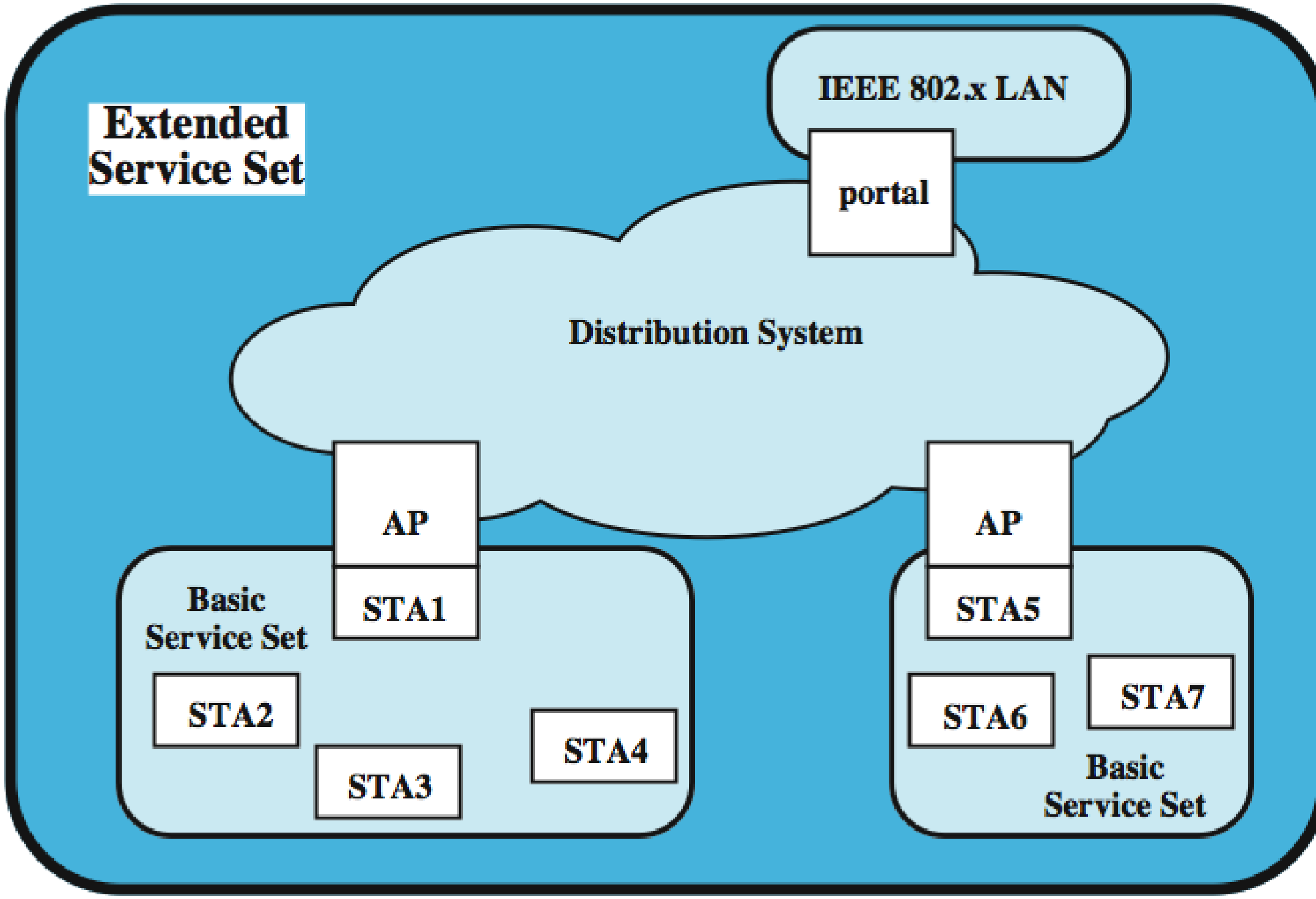
# Spread Spectrum LANs Transmission Issues

- licensing regulations differ between countries
- USA FCC allows in ISM band:
  - spread spectrum (1W), very low power (0.5W)
    - 902 - 928 MHz (915-MHz band)
    - 2.4 - 2.4835 GHz (2.4-GHz band)
    - 5.725 - 5.825 GHz (5.8-GHz band)
  - 2.4 GHz also in Europe and Japan
- interference
  - many devices around 900 MHz: cordless telephones, wireless microphones, and amateur radio

# IEEE 802 Terminology

| | |
|---|---|
| Access point (AP) | Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations |
| Basic service set (BSS) | A set of stations controlled by a single coordination function |
| Coordination function | The logical function that determines when a station operating within a BSS is permitted to transmit and may be able to receive PDUs |
| Distribution system (DS) | A system used to interconnect a set of BSSs and integrated LANs to create an ESS |
| Extended service set (ESS) | A set of one or more interconnected BSSs and integrated LANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs |
| MAC protocol data unit (MPDU) | The unit of data exchanged between two peer MAC entites using the services of the physical layer |
| MAC service data unit (MSDU) | Information that is delivered as a unit between MAC users |
| Station | Any device that contains an IEEE 802.11 conformant MAC and physical layer |

# IEEE 802.11 Architecture




STA = station
AP = access point

# IEEE 802.11 - BSS

- basic service set (BSS) building block
- may be isolated
- may connect to backbone distribution system (DS) through access point (AP)
- BSS generally corresponds to cell
- DS can be switch, wired network, or wireless network
- have independent BSS (IBSS) with no AP

# Extended Service Set (ESS)

- possible configurations:
  - simplest is each station belongs to single BSS
  - can have two BSSs overlap
  - a station can participate in more than one BSS
  - association between station and BSS dynamic
- ESS is two or more BSS interconnected by DS
- appears as single logical LAN to LLC

# Services - Message Distribution

- distribution service
  - primary service used by stations to exchange MAC frames when frame must traverse DS
  - if stations in same BSS, distribution service logically goes through single AP of that BSS
- integration service
  - enables transfer of data between 802.11 LAN station and one on an integrated 802.x LAN

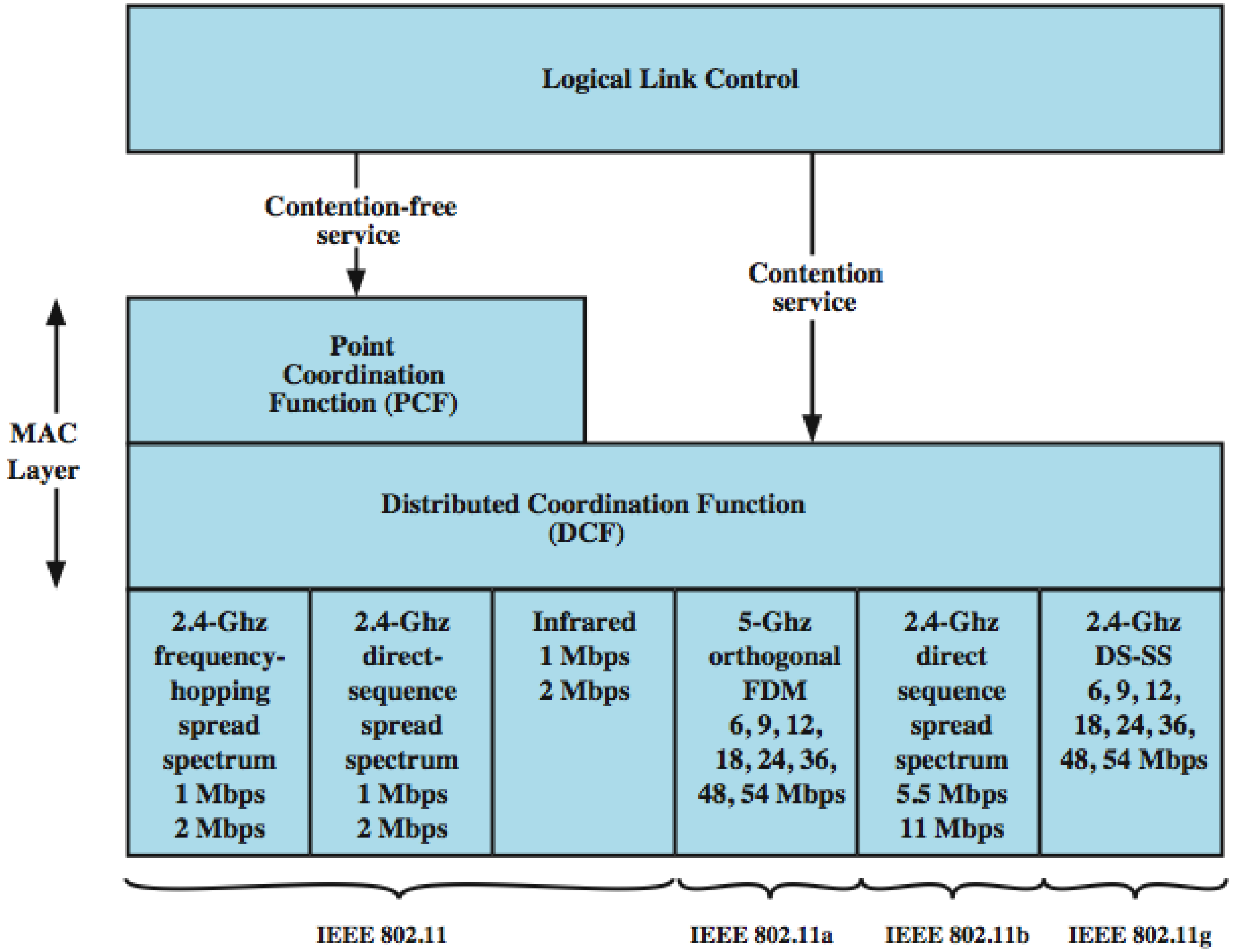
# Medium Access Control

- MAC layer covers three functional areas
  - reliable data delivery
  - access control
  - security

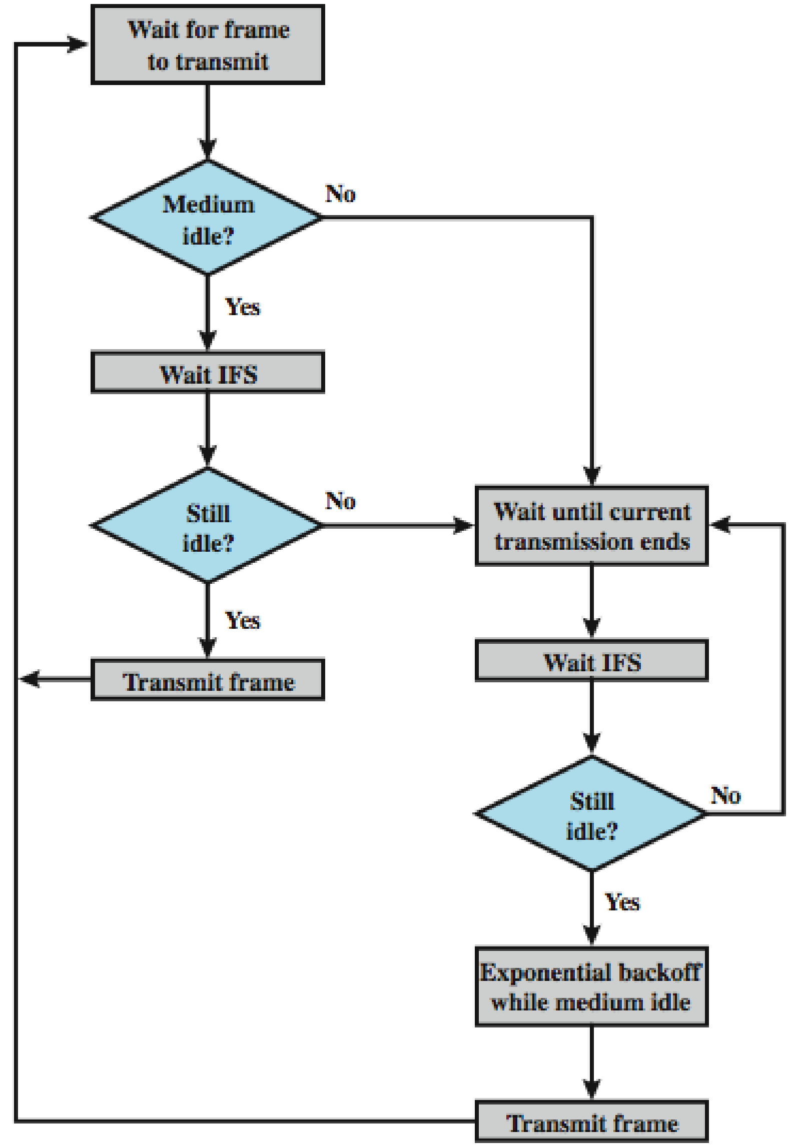
# Reliable Data Delivery

- 802.11 physical / MAC layers unreliable
  - noise, interference, and other propagation effects result in loss of frames
  - even with error-correction codes, frames may not successfully be received
- can be dealt with at a higher layer, e.g. TCP
- more efficient to deal with errors at MAC level
- 802.11 includes frame exchange protocol
  - station receiving frame returns acknowledgment (ACK) frame
  - exchange treated as atomic unit
  - if no ACK within short period of time, retransmit

# Media Access Control



# IEEE 802.11 Medium Access Control Logic



# IEEE 802.11 MAC Frame Format

| octets | 2 | 2 | 6 | 6 | 6 | 2 | 6 | 0 to 2312 | 4 |
|---|---|---|---|---|---|---|---|---|---|
| | FC | D/I | Address | Address | Address | SC | Address | Frame body | CRC |

FC = Frame control
D/I = Duration/Connection ID
SC = Sequence control

# Bluetooth

- Bluetooth is designed to operate in an environment of many users.
- Up to eight devices can communicate in a small network called a **piconet.**
- Ten of these piconets can coexist in the same coverage range of the Bluetooth radio.
- To provide security, each link is encoded and protected against eavesdropping and interference.

- Bluetooth provides support for three general application areas using short-range wireless connectivity:

- **Data and voice access points:** Bluetooth facilitates real-time voice and data transmissions by providing effortless wireless connection of portable and stationary communications devices.
- **Cable replacement:** Bluetooth eliminates the need for numerous, often proprietary, cable attachments for connection of practically any kind of communication device.
- **Ad hoc networking:** A device equipped with a Bluetooth radio can establish instant connection to another Bluetooth radio as soon as it comes into range.

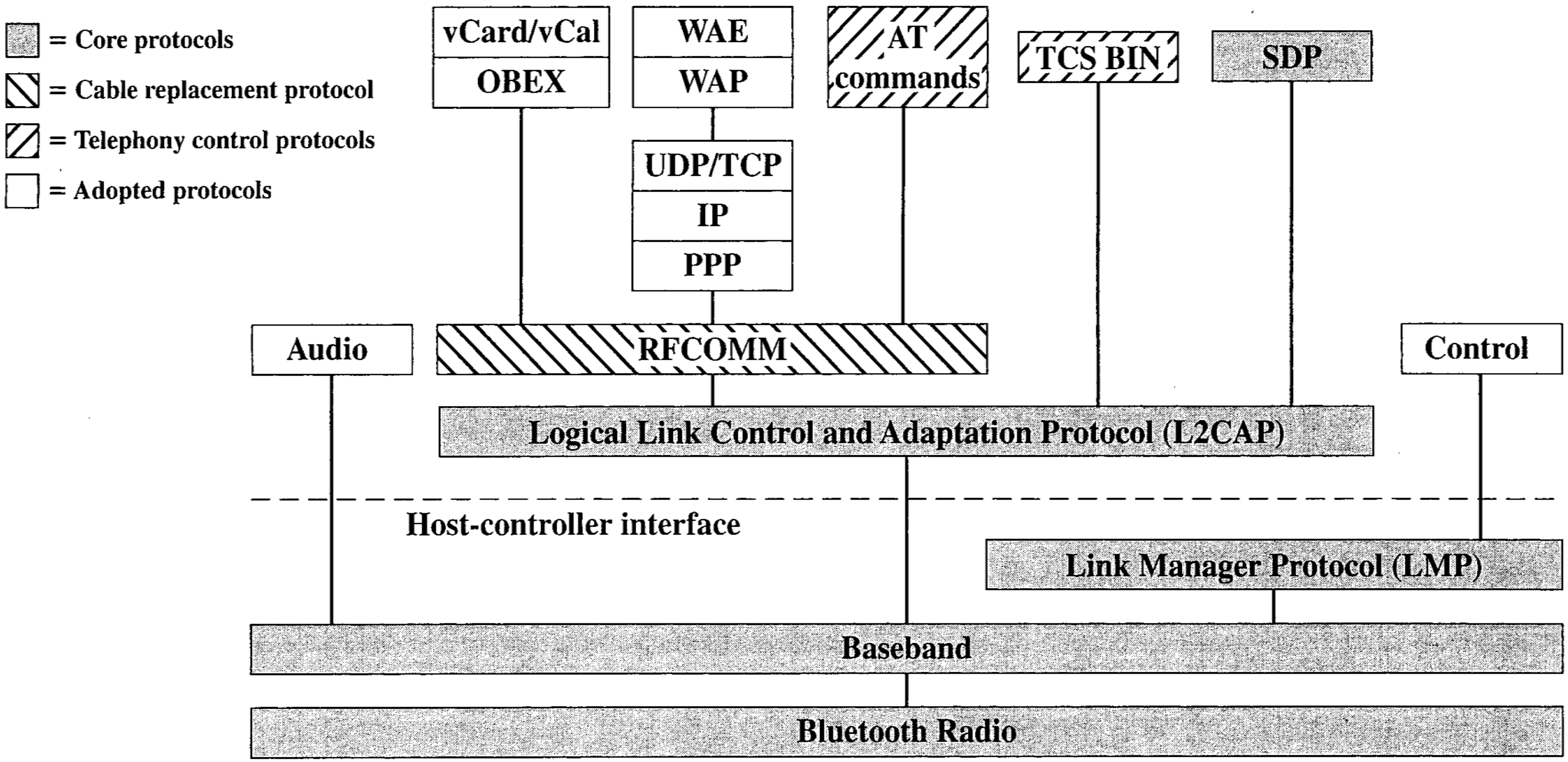
# Protocol Architecture

- The **core protocols** form a five-layer stack consisting of the following elements:

- **Radio:** Specifies details of the air interface, including. frequency, the use of frequency hopping, modulation scheme, and transmit power.
- • **Baseband:** Concerned with connection establishment within a piconet, addressing, packet format, timing, and power control.
- **Link manager protocol (LMP):** Responsible for link setup between Bluetooth devices and ongoing link management.

- **Logical link control and adaptation protocol** (L2CAP**):** Adapts upper-layer protocols to the baseband layer. L2CAP provides both connectionless and connection-oriented services.
- **Service discovery protocol (SDP):** Device information, services, and the characteristics of the services can be queried to enable the establishment of a connection between two or more Bluetooth devices.

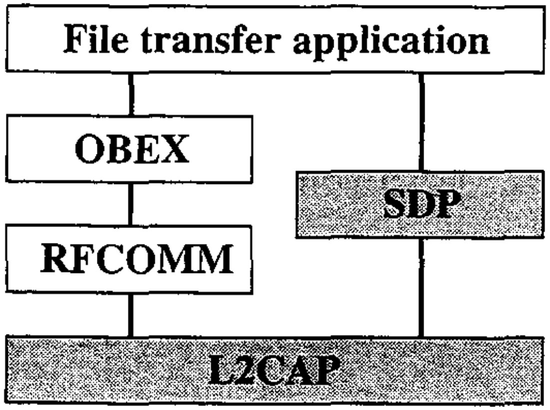
# Bluetooth Protocol Stack



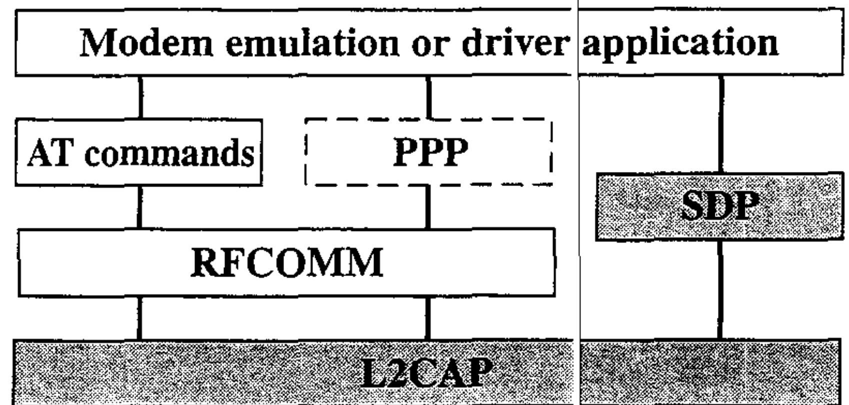

| | | | |
|---|---|---|---|
| AT | = attention sequence (modem prefix) | TCS BIN | = telephony control specification—binary |
| IP | = Internet Protocol | UDP | = User Datagram Protocol |
| OBEX | = Object Exchange Protocol | vCal | = virtual calendar |
| PPP | = Point-to-Point Protocol | vCard | = virtual card |
| RFCOMM | = radio frequency communications | WAE | = wireless application environment |
| SDP | = Service Discovery Protocol | WAP | = Wireless Application Protocol |
| TCP | = Transmission Control Protocol | | |

# Usage Models

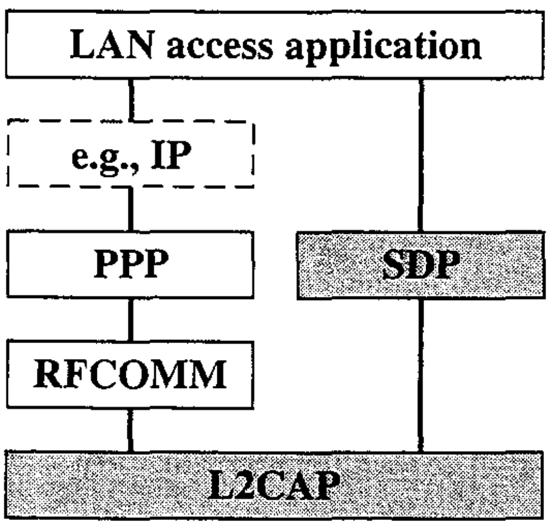
- **File transfer:** The file transfer usage model supports the transfer of directories, files, documents, images, and streaming media formats. This usage model also includes the capability to browse folders on a remote device.
- **Internet bridge:** With this usage model, a PC is wirelessly connected to a mobile phone or cordless modern to provide dial-up networking and fax capabilities.



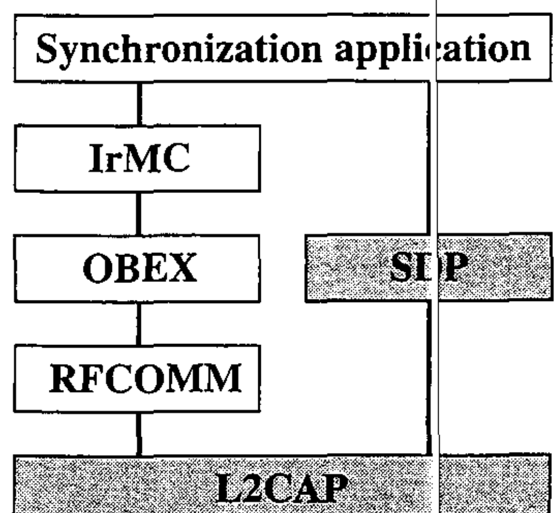

(a) File transfer



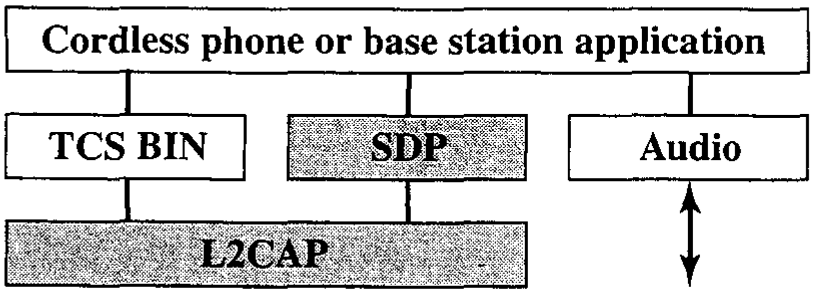

(b) Dial-up networking



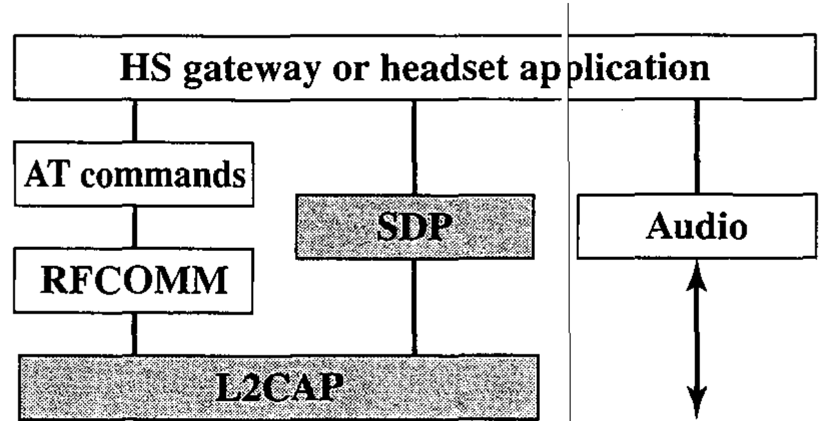

(c) LAN access




(d) Synchronization




(e) Cordless phone and intercom

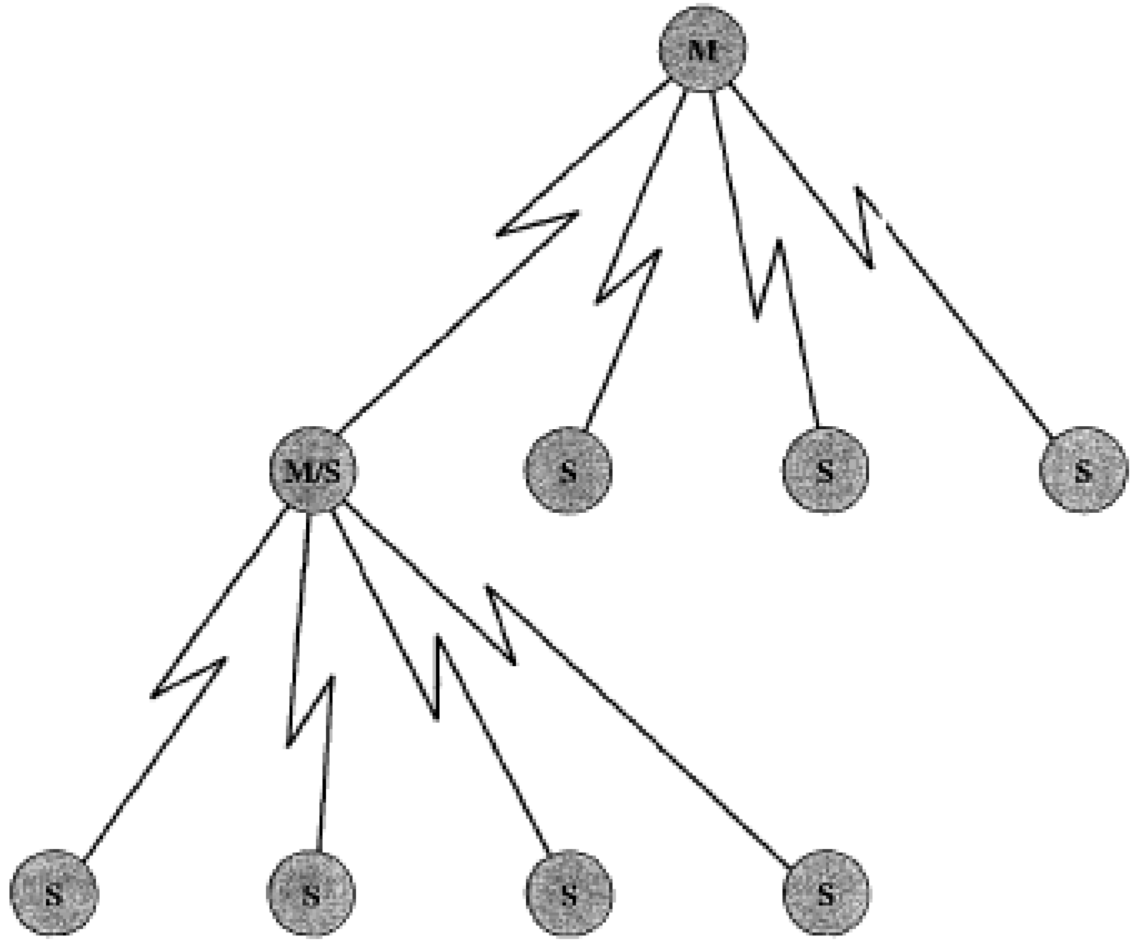



(f) Headset

**LAN access:** This usage model enables devices on a piconet to access a LAN. Once connected, a device functions as if it were directly connected (wired) to the LAN.

**Synchronization:** This model provides a device-to-device synchronization of PIM (personal information management) information, such a phone book, calendar, message, and note information.

- **Three-in-one phone:** Telephone handsets that implement the usage model may act as a cordless phone connecting to a voice base station, s an intercom device for connecting to other telephones, and as a cellular phone.
- **Headset:** The headset can act as a remote device's audio input and output interface.




**Master/Slave Relationships**

# RADIO SPECIFICATION

- The Bluetooth radio specification is a short document that gives the basic details of radio transmission for Bluetooth devices.

**Table 15.2** Bluetooth Radio and Baseband Parameters

| | |
|---|---|
| Topology | Up to 7 simultaneous links in a logical star |
| Modulation | GFSK |
| Peak data rate | 1 Mbps |
| RF bandwidth | 220 kHz (−3dB), 1 MHz (−20dB) |
| RF band | 2.4 GHz, ISM band |
| RF carriers | 23/79 |
| Carrier spacing | 1 MHz |
| Transmit power | 0.1 W |
| Piconet access | FH-TDD-TDMA |
| Frequency hop rate | 1600 hops/s |
| Scatternet access | FH-CDMA |

- **Class 1:** Outputs 100 mW (+20 dBm) for maximum range, with a minimum of 1 mW (0 dBm). In this class, power control is mandatory, ranging from 4 to 20 dBm. This mode provides the greatest distance.
- **Class 2:** Outputs 2.4 mW (+4 dBm) at maximum, with a minimum of 0.25 mW (-6 dBm). Power control is optional.
- **Class 3:** Lowest power. Nominal output is 1 mW.

- Modulation for Bluetooth is Gaussian FSK, with a binary one represented by a positive frequency deviation and a binary zero represented by a negative frequency deviation from the center frequency.
- The minimum deviation is 115 kHz.

# BASEBAND SPECIFICATION

Table 15.3 International Bluetooth Frequency Allocations

| Area | Regulatory Range | RF Channels |
|---|---|---|
| U.S., most of Europe, and most other countries | 2.4 to 2.4835 GHz | $f = 2.402 + n$ MHz, $n = 0, \ldots, 78$ |
| Japan | 2.471 to 2.497 GHz | $f = 2.473 + n$ MHz, $n = 0, \ldots, 22$ |
| Spain | 2.445 to 2.475 GHz | $f = 2.449 + n$ MHz, $n = 0, \ldots, 22$ |
| France | 2.4465 to 2.4835 GHz | $f = 2.454 + n$ MHz, $n = 0, \ldots, 22$ |

# LINK MANAGER SPECIFICATION

- LMP manages various aspects of the radio link between a master and a slave.
- The protocol involves the exchange of messages in the form of LMP PDUs (protocol data units) between the LMP entities in the master and slave.

- **Authentication:** Authentication is defined in the baseband specification but involves the exchange of two LMP PDUs, one containing the random number and one containing the signed response.
- **Pairing:** This service allows mutually authenticated users to automatically establish a link encryption key.

- **Change link key:** If two devices are paired and use a combination key, then that key can be changed. One side generates a new key and sends it to the other side XORed with the old link key.
- **Change current link key:** The current link key can be changed temporarily.
- **Encryption:** LMP is not directly involved in link encryption but provides services to manage the encryption process.
- **Clock offset request:** When a slave receives the FRS packet, the difference is computed between its own clock and the master's clock value included in the payload of the FRS packet.
- **Slot offset information:** An initiating device can transmit a message that describes timing differences (time difference between slot boundaries) between two adjacent piconets.

# LOGICAL LINK CONTROL AND ADAPTATION PROTOCOL

- Logical Link Control (LLC) in the IEEE 802 specification, L2CAP provides a link-layer protocol between entities across a shared-medium network.
- **Connectionless service:** This is a reliable datagram style of service.
- **Connection-mode service:** This service is similar to that offered by RDLC. A logical connection is set up between two users exchanging data, and flow control and error control are provided.

| Octets: | 2 | 2 | ≥ 2 | 0 to 65533 |
|---|---|---|---|---|
| | Length | Channel ID (0x0002) | PSM | Information |

(a) Connectionless PDU

| 2 | 2 | 0 to 65535 |
|---|---|---|
| Length | Channel ID | Information |

(b) Connection-oriented PDU

| 2 | 2 | |
|---|---|---|
| Length | Channel ID (0x0001) | 1 or more commands |

(c) Signaling command PDU

| 1 | 1 | 2 | ≥ 0 |
|---|---|---|---|
| Code | Iden-tifier | Length | Data |

(d) Command format

Figure 15.15 L2CAP Formats

## Quality of Service

- The flow specification consists of the following parameters:

- Service type
- Token rate (bytes/second)
- Token bucket size (bytes)
- Peak bandwidth (bytes/second)
- Latency (microseconds)
- Delay variation (microseconds)

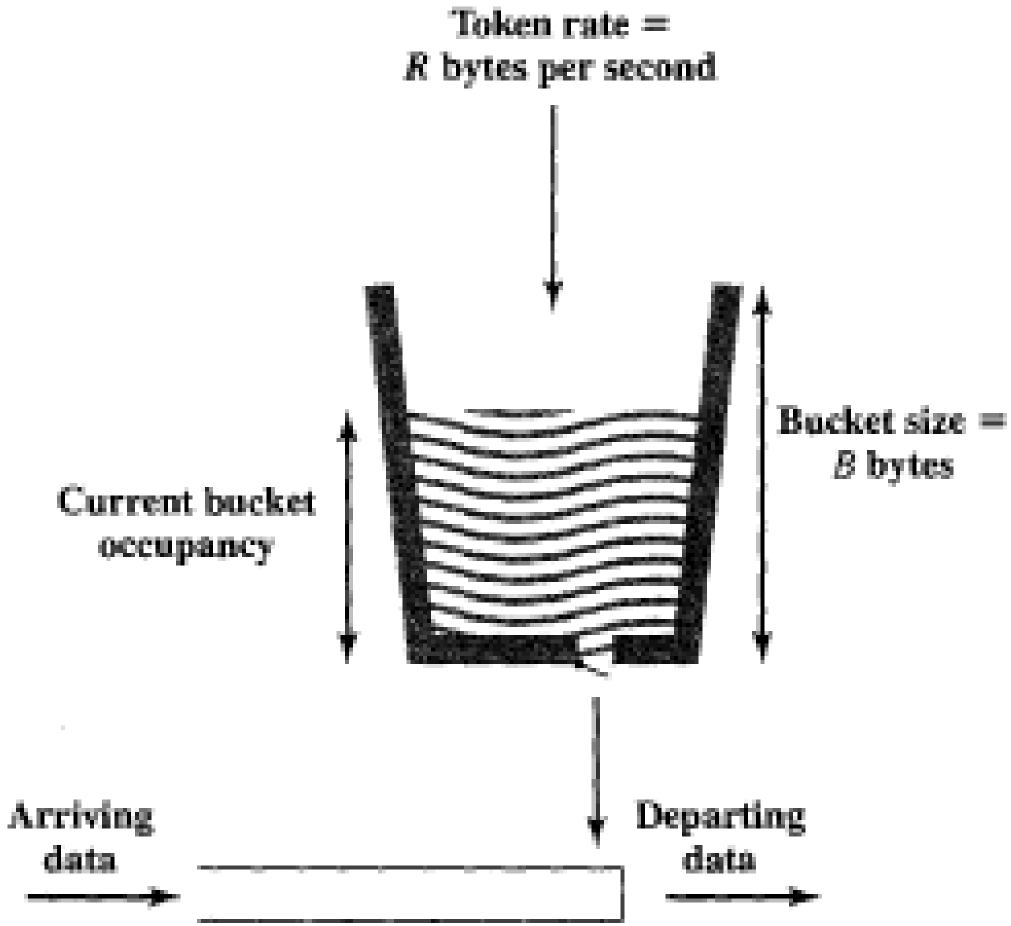



Figure 15.16 Token Bucket Scheme

- The **peak bandwidth,** expressed in bytes per second, limits how fast packets may be sent back-to-back from applications. Some intermediate systems can take advantage of this information, resulting in more efficient resource allocation.

# UNIT V

# MOBILE DATA NETWORKS AND HIPER LAN

## CDPD NETWORK

### Introduction

As we know, the AMPS (Advanced Mobile Phone System) cellular network was developed for voice communication in the 1980s. Due to long-established setup times and modem handshaking requirements, packet data communication was not natively supported by AMPS.



In order to support packet data, CDPD was introduced in 1993. Cellular Digital Packet Data (CDPD) is a technology that revolutionized wireless data communication by allowing data to be transmitted over existing cellular networks.

CDPD was developed to facilitate efficient and reliable data transmission, leveraging the infrastructure of analog cellular networks.

This tutorial delves into the key features, network architecture, applications, advantages, and disadvantages of CDPD.

### What is CDPD (Cellular Digital Packet Data)?

CDPD stands for Cellular Digital Packet Data. Though it has its own infrastructure, it utilizes unused channels or gaps between the channels in an analog cellular network for packet communication.

CDPD architecture co-exists with the AMPS network architecture.

It supports both data and voice communication, making it a cost-effective solution for mobile data services. By utilizing existing cellular infrastructure, CDPD provided a significant boost to mobile data communication without requiring major network overhauls.



### Key Features of CDPD

Following are the features of CDPD (Cellular Digital Packet Data):

- Communication between BS (Base station i.e. MDBS) and MS (i.e. M-ES) is full duplex.
- It utilizes or seizes a 30 KHz channel from existing AMPS/GSM networks for transmitting data at 19.2 Kbps. The net data rate is 9.2 Kbps due to the large amount of overhead.
- It utilizes the same frequency band as used by AMPS, i.e., 824 MHz and 894 MHz for uplink and downlink. Both uplink and downlink are separated using FDMA.
- There are two types of handsets or phones available: single mode and dual mode. A single-mode phone can initiate a data call or voice call. In contrast, a dual-mode phone can switch between data calls and voice calls due to simultaneous registration on both AMPS and CDPD networks.
- It utilizes the DSMA (Digital Sense Multiple Access) technique. In this technique, the CDPD mobile checks for a flag bit in the downlink channel, which informs whether the uplink slot is

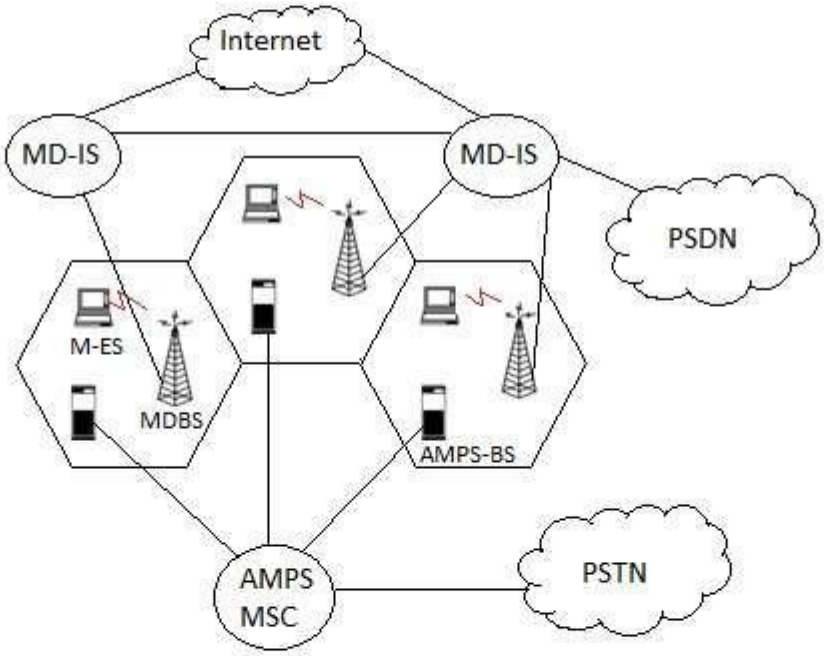
idle or busy. If idle, it utilizes it for transmission. If busy, it waits for a random period instead of transmitting in the next time slot.

- It supports different types of services and has access to the internet backbone.

Best smartphone

**CDPD Network Architecture**

The figure depicts CDPD architecture in mobile computing. As shown, it consists of three major system elements: M-ES, MDBS, and MD-IS. Moreover, CDPD co-exists with the AMPS network and hence will fall back to AMPS for voice calls. The figure shows AMPS-BS and AMPS-MSC, which are part of the AMPS network connected with PSTN for voice connectivity.




CDPD Network Architecture

There are three CDPD interfaces: E-interface, I-interface, and A-interface.

- The E-interface exists between CDPD and a fixed network external to CDPD.
- The I-interface exists between two CDPD networks.
- The A-interface exists between BS and MS. It is also known as the Air interface.

Let us understand the network elements used in the CDPD architecture.

- **M-ES**: It functions similarly to a subscriber or mobile unit used in any cellular system. It requires a SIM for operation, which can be housed in a laptop, mobile, or PDA. It interfaces with radio equipment at 19.2 Kbps. Each M-ES has a unique NEI (Network Equipment Identifier) which is associated with its home MD-IS.
- **MDBS**: It functions similarly to a Base Station. It broadcasts available channels for M-ES. It takes care of radio activities such as channel allocation, usage, etc. These MDBSs co-exist with AMPS Base Stations and hence share the same antenna and site together.

- **MD-IS**: It provides connectivity with the internet and PSDN. It has the functionalities of both a frame relay switch and a packet router. It does buffering of packets routed for M-ES. It also supports roaming management as it contains a registration directory.

**CDPD Applications**

Following are the applications of CDPD.

- **Mobile Internet Access:** CDPD enabled early mobile internet access, allowing users to browse the web, check emails, and access online services on the go.
- **Telematics:** CDPD was widely used in telematics applications, including vehicle tracking, fleet management, and remote monitoring of assets.
- **Point of Sale Systems:** CDPD facilitated wireless point of sale (POS) systems, allowing businesses to process transactions from virtually any location.
- **Remote Monitoring and Control:** CDPD was utilized for remote monitoring and control of various systems, such as utility meters, vending machines, and industrial equipment.
- **Emergency Services:** CDPD provided reliable data communication for emergency services, enabling quick and efficient coordination during critical situations.

**Advantages of CDPD**

Following are the benefits or advantages of CDPD:

- It utilizes existing channels of the AMPS network and hence is easy to install and start using the existing channels if not in use. By leveraging existing cellular infrastructure, CDPD reduces the need for additional investments in network hardware, making it a cost-effective solution for mobile data services.
- The use of packet-switched technology and idle channels enhances network efficiency, allowing more data to be transmitted without impacting voice communication.
- It has a cellular-like architecture and hence can support larger capacity due to ease in upgrading the network.
- There is no delay in establishing a data call as the CDPD phone is already registered with the CDPD network.
- CDPD incorporates error correction mechanisms to ensure data integrity and reliability during transmission. This feature is crucial for maintaining high-quality data communication in mobile environments.
- CDPD includes encryption and authentication features to protect data transmission from unauthorized access and ensure secure communication.
- CDPD supports seamless handoffs between cells, allowing uninterrupted data communication as users move across different coverage areas.

**Limitations of CDPD**

Following are the limitations or disadvantages of CDPD:

- There is no mesh connectivity in CDPD. Hence, M-ES and M-ES cannot communicate directly. Communication between them occurs via MDBS.
- CDPD cell size is limited to less than 10 miles.

- CDPD offered relatively low data transmission speeds compared to modern standards. The typical data rates were around 19.2 kbps, which are insufficient for many contemporary data-intensive applications.
- CDPD relied on the infrastructure of analog cellular networks (AMPS), which were phased out in favor of digital cellular technologies. As analog networks were decommissioned, the availability of CDPD services declined.
- The use of idle channels in the analog cellular network limited the available bandwidth for CDPD. This restriction impacted the overall data throughput and capacity of the system.
- Due to the nature of packet-switched technology and the dynamic allocation of idle channels, CDPD could experience higher latency compared to dedicated circuit-switched data connections.
- Operating in the analog spectrum, CDPD was susceptible to interference from various sources, which could degrade signal quality and data transmission reliability.
- While CDPD included basic encryption and authentication features, the security mechanisms were not as robust as those found in later digital mobile data technologies. This made CDPD less secure against sophisticated attacks.
- CDPD shared resources with voice communication channels. During peak voice call times, the availability of idle channels for data transmission could be significantly reduced, leading to potential data transmission delays and reduced service quality.
- The implementation of CDPD required modifications to existing cellular infrastructure, including the installation of additional equipment and upgrades to support packet-switched data. This added complexity and cost for network operators.
- The emergence of digital cellular technologies, such as GPRS, EDGE, and later, 3G, 4G, and 5G networks, offered significantly higher data rates, better efficiency, and more robust security. These newer technologies quickly outpaced CDPD in terms of performance and capabilities.

## GPRS AND HIGHER DATA RATES:

GPRS (General Packet Radio Service) is an expansion of GSM (Global System for Mobile Communications) networks that offer packet-switched data services. The GPRS architecture consists of different network components and interfaces that work together to provide data services. In this article, we will discuss everything about GPRS architecture.

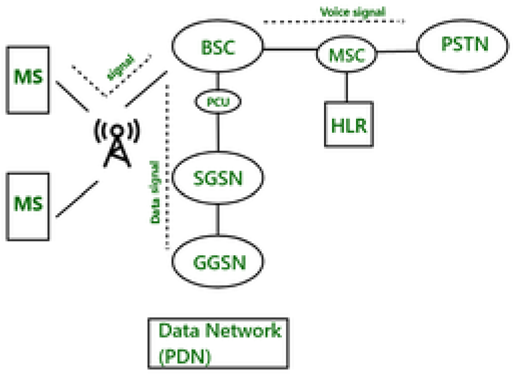
### What is GPRS?

**GPRS** stands for General Packet Radio Service. It is the modified version of GSM architecture. GPRS is a packet-oriented mobile data mechanism, that can carry data packets as well. In GSM architecture, only voice signals can be transported, so being an enhanced version GPRS can transmit voice as well as data packets. It uses the same physical radio channel as GSM does, the only difference is it has a new logic defined for the radio channel.

### GPRS Network Architecture

GPRS tries to make maximum use of the existing physical structure of GSM. It has introduced a new entity named GPRS support nodes(GSN) whose responsibility is to route and deliver a data packet. GSN is of two types:

- Serving GPRS Support Node (SGSN)
- Gateway GPRS Support Node (GGSN)




GPRS Architecture

**Components of GPRS Architecture**

**1. Mobile Station(MS)**

GPRC requires enhanced mobile stations, as existing mobile stations were designed according to the GSM network, and they were unable in handling enhanced data packets. A variety of high-speed mobile stations are available to support enhanced data packets. These mobile stations are also capable of handling the GSM architecture to make voice calls.

**2. Base Station Controller (BSC)**

In GSM architecture there is one component called BSC. But in GPRS there is one component is added to BSC called PCU. PCU stands for Packet Control Unit. If the signal comes to BSC and that signal contains data, then PCU routes to the SGSN. The interface is used between BSC and PCU is the FRI interface. After the signal comes to SGSN, it delivers the data packet to the GGSN. GGSN routes the data packet to the data network (PDN- Predefined Data Network).

**3. GPRS Support Nodes**

GPRS support nodes are of two types:

(a) **Serving GPRS Support Node (SGSN)**: It is responsible for the following tasks:

- Packet Delivery
- Mobility management
  - apply/ sign off of terminals
  - localization
- LLC (Logical Link Control) management
- Authentication
- Billing

**(b) Gateway GPRS Support Node (GGSN)**: It is responsible for the following tasks:

- Mediator between GPRS between backbone and external data networks.
- Saves current data for the SGSN address of the participant as well as their profile and data for authentication and invoice.

**4. Internal Backbone Network**

It is an IP-based network that is used to support the working of GPRS and this is responsible to carry new packets between different GSNs. The tunneling is used between SGSNs and GGSNs to exchange information without informing the internal backbone.

**5. Mobility Support**

GPRS has the following mechanism to support mobility in the network:

- Attachment Procedure
- Location and Handoff Management

**6. Routing Area**

This is similar to the location area in GSM the only difference is routing area use fewer cells as routing areas are smaller than the location area.

**7. SMS in GSM**

GSM introduced a mechanism of Short Messaging Service(SMS) which is similar to peer-to-peer Instant messaging.

**Benefits Of GPRS**

- **Mobility:** The capacity to keep up consistent voice and information interchanges while moving.
- **Cost Efficient:** Communication via GPRS is cheaper than through the regular GSM network.
- **Immediacy:** Allows customers to obtain connectivity when needed, regardless of location and without a lengthy login session.
- **Localization:** Enables customers to acquire data applicable to their present area.
- **Easy Billing:** GPRS packet transmission offers an easier to use billing than that offered by circuit switched administrations.

**Short messaging service in GSM**

In the SMS network operated by GSM service providers four layers of transport is used (Figure 1.):

SM-AL (Application Layer)
SM-TL (Transfer Layer)
SM-RL (Relay Layer)
SM-LL (Lower Layers)

Ozeki Message Server is located in the SM-AL layer. When sending an SMS the software creates protocol data units (PDU's) transported by the SM-TL layer. When a GSM phone attached to the PC receives an SMS, the message is also encoded according the SM-TL layer PDU specification. Ozeki Message Server decodes this PDU and makes the message readable for computer programs and computer users.

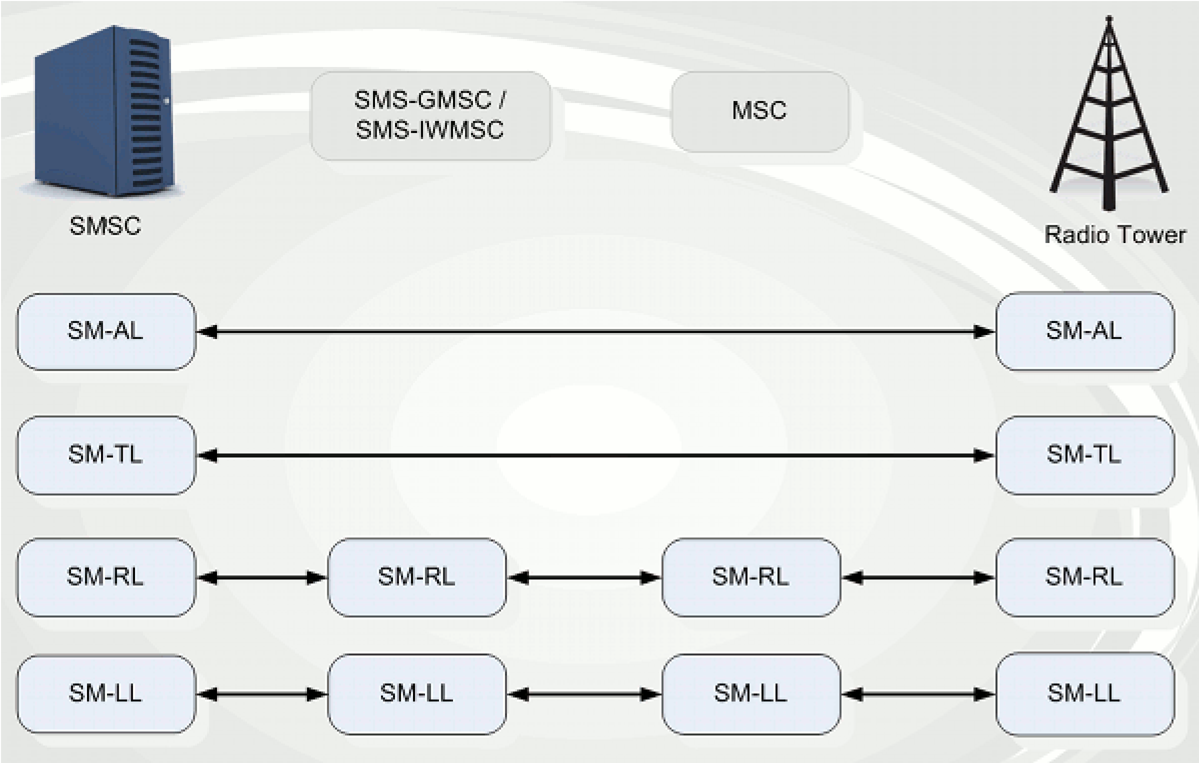



Figure 1 - SMS network layers

To understand how the SMS travels from the mobile phone to the SMSC please take a look at Figure 2. On this figure you can see which protocols are used and which GSM network entities take place in the communication process. As you can see, the mobile phone (Mobile station) transmits the SMS message to the GSM base station (BTS) through a wireless link. After this the message goes through the backbone network of the service provider. The Mobile Switching Center (MSC), the Home Location Register (HLR) and optionally the Visitor Location Register (VLR) is used to find out the appropriate Short Message Service Center (SMSC) that will store and forward the message when the receiving party becomes available.

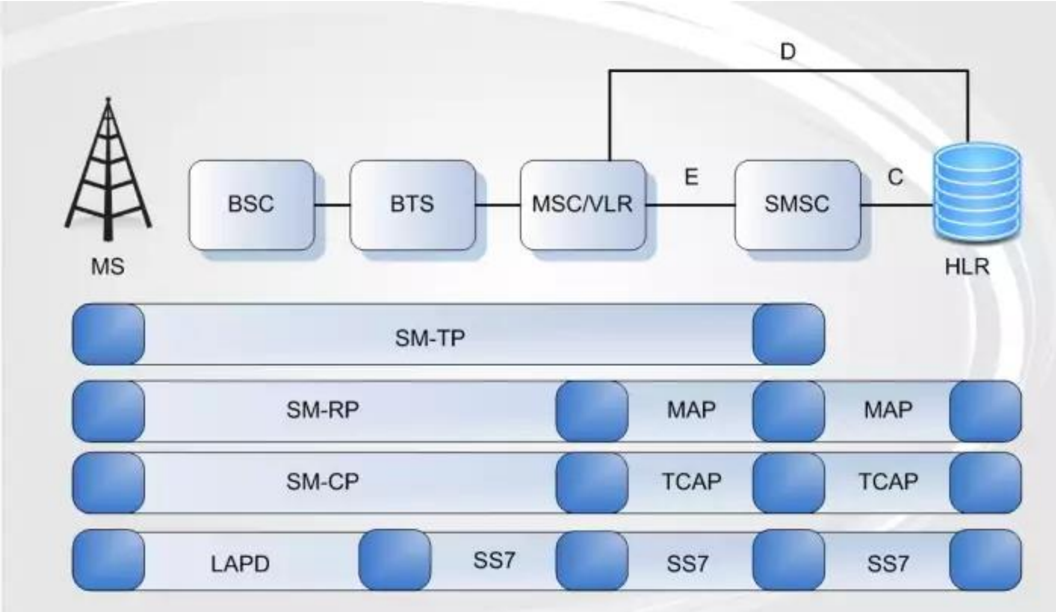
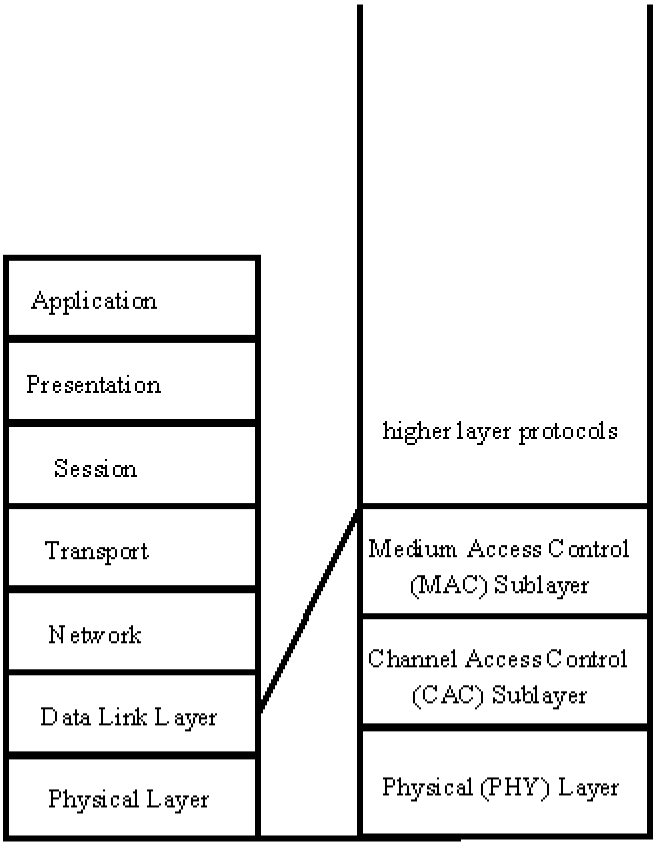



Figure 2 - SMS transportation

**HIPERLAN**

HIPERLAN is a European family of standards on digital high speed wireless communication in the 5.15-5.3 GHz and the 17.1-17.3 GHz spectrum developed by ETSI. The committee responsible for HIPERLAN is RES-10 which has been working on the standard since November 1991.

The standard serves to ensure the possible interoperability of different manufacturers' wireless communications equipment that operate in this spectrum. The HIPERLAN standard only describes a common air interface including the physical layer for wireless communications equipment, while leaving decisions on higher level configurations and functions open to the equipment manufacturers.




**OSI Reference** **HIPERLAN Reference**

The choice of frequencies allocated to HIPERLAN was part of the 5-5.30 GHz band being allocated globally to aviation purposes. The Aviation industry only used the 5-5.15GHz frequency, thus making the 5.15-5.30 frequency band accessible to HIPERLAN standards.

HIPERLAN is designed to work without any infrastructure. Two stations may exchange data directly, without any interaction from a wired (or radio-based) infrastructure. The simplest HIPERLAN thus consists of two stations. Further, if two HIPERLAN stations are not in radio contact with each other, they may use a third station (i.e. the third station must relay messages between the two communicating stations).

Products compliant to the HIPERLAN 5 GHz standard shall be possible to implement on a PCMCIA Type III card. Thus the standard will enable users to truly take computing power on the road.

The HIPERLAN standard has been developed at the same time as the development of the SUPERnet standard in the United States.

**HIPERLAN requirements**

- Short range - 50m
- Low mobility - 1.4m/s
- Networks with and without infrastructure
- Support isochronous traffic
- audio 32kbps, 10ns latency

- video 2Mbps, 100ns latency
- Support asynchronous traffic
- data 10Mbps, immediate access

**Quality of service**

Performance is one of the most important factors when dealing with wireless LANs. In contrast to other radio-based systems, data traffic on a local area network has a randomized bursty nature, which may cause serious problems with respect to throughput.

Many factors have to be taken into consideration, when quality of service is to be measured. Among these are:

- The topography of the landscape in general
- Elevations in the landscape that might cause shadows, where connectivity is unstable or impossible.
- Environments with many signal-reflection surfaces
- Environments with many signal-absorbing surfaces
- Quality of the wireless equipment
- Placement of the wireless equipment
- Number of stations
- Proximity to installations that generate electronic noise
- and many more

The sheer number of factors to take into consideration means, that the physical environment will always be a factor in trying to asses the usefulness of using a wireless technology like HIPERLAN.

Simulations show that the HIPERLAN MAC can simultaneously support

- 25 audio links at 32kbit/s, 10ms delivery
- 25 audio links at 16kbit/s, 20ms delivery
- 1 video link at 2Mbit/s, 100ms delivery
- Asynch file transfer at 13.4Mbit/s