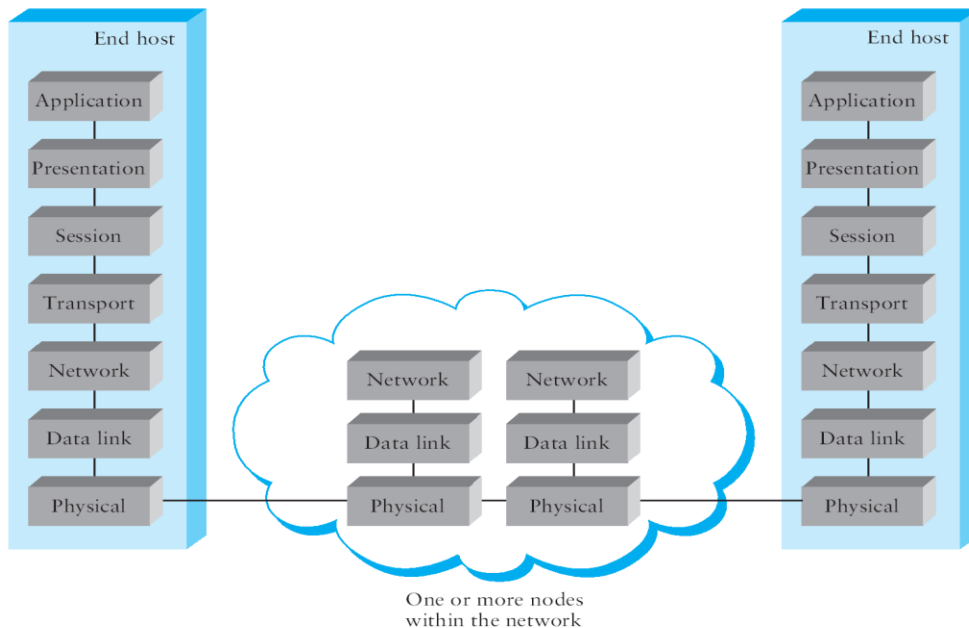


## OSI Architecture

- ISO defines a common way to connect computer by the architecture called Open System Interconnection(OSI) architecture.
- Network functionality is divided into seven layers.



### Organization of the layers

The 7 layers can be grouped into 3 subgroups

#### 1. Network Support Layers

Layers 1,2,3 - Physical, Data link and Network are the network support layers. They deal with the physical aspects of moving data from one device to another such as electrical specifications, physical addressing, transport timing and reliability.

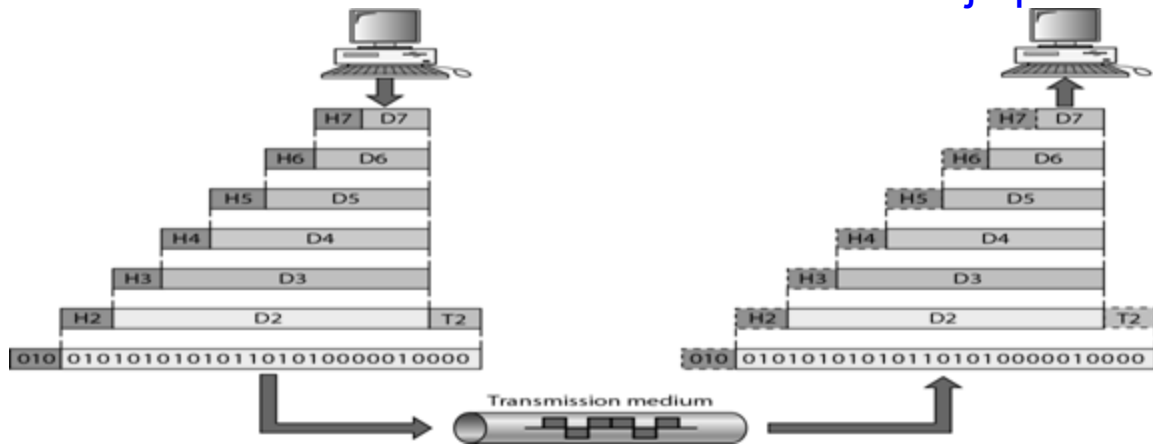
#### 2. Transport Layer

Layer4, transport layer, ensures end-to-end reliable data transmission on a single link.

#### 3. User Support Layers

Layers 5,6,7 – Session, presentation and application are the user support layers. They allow interoperability among unrelated software systems

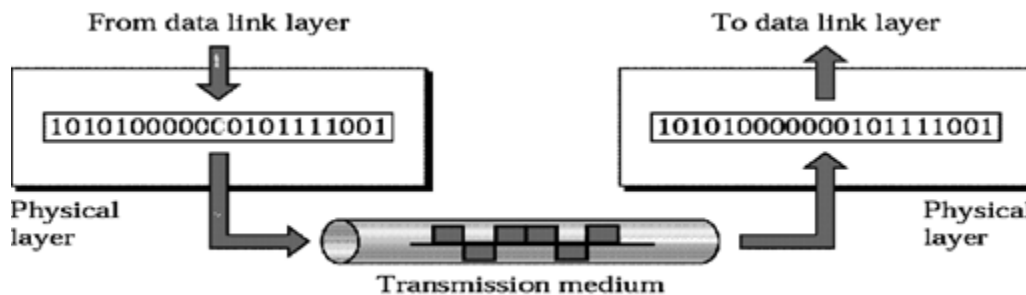
### An Data exchange using the OSI model



## Functions of the Layers

### 1. Physical Layer

The physical layer coordinates the functions required to transmit a bit stream over a physical medium.

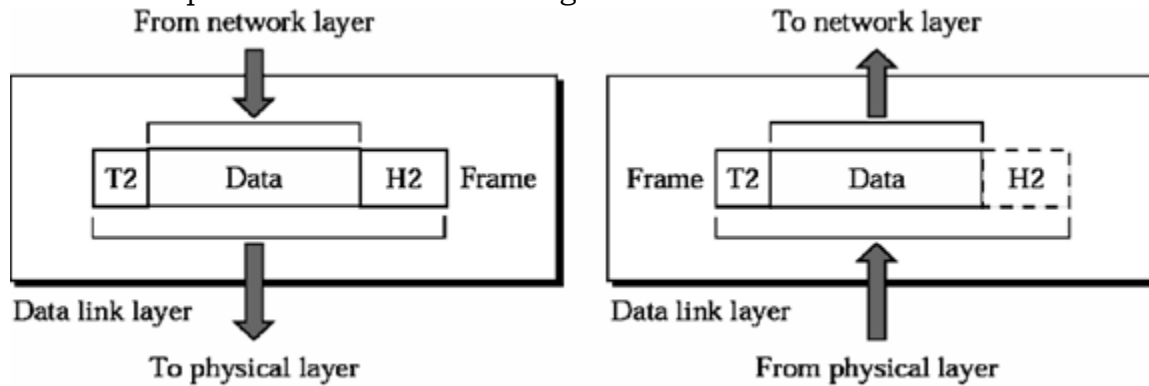


The physical layer is concerned with the following:

- **Physical characteristics of interfaces and media** - The physical layer defines the characteristics of the interface between the devices and the transmission medium.
- **Representation of bits** - To transmit the stream of bits, it must be encoded to signals. The physical layer defines the type of encoding.
- **Data Rate or Transmission rate** - The number of bits sent each second – is also defined by the physical layer.
- **Synchronization of bits** - The sender and receiver must be synchronized at the bit level. Their clocks must be synchronized.
- **Line Configuration** - In a point-to-point configuration, two devices are connected together through a dedicated link. In a multipoint configuration, a link is shared between several devices.
- **Physical Topology** - The physical topology defines how devices are connected to make a network. Devices can be connected using a mesh, bus, star or ring topology.
- **Transmission Mode** - The physical layer also defines the direction of transmission between two devices: simplex, half-duplex or full-duplex.

### 2. Data Link Layer

It is responsible for transmitting frames from one node to next node.

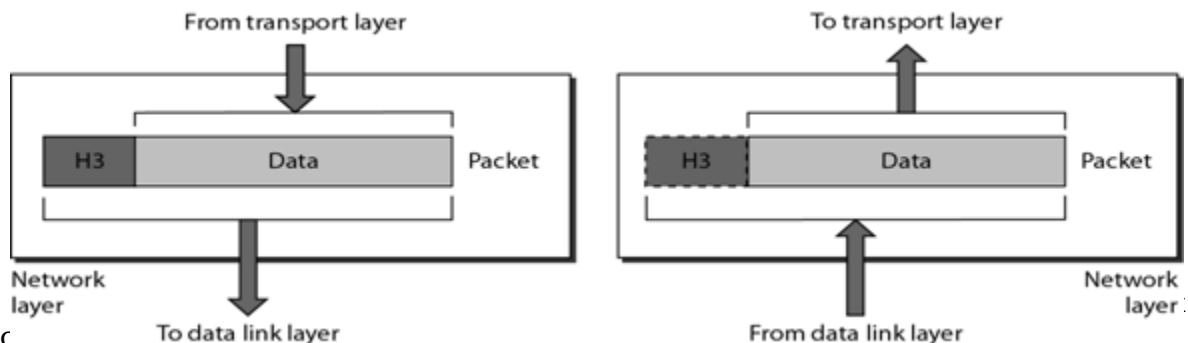


The other responsibilities of this layer are

- **Framing** - Divides the stream of bits received into data units called frames.
- **Physical addressing** – If frames are to be distributed to different systems on the n/w , data link layer adds a header to the frame to define the sender and receiver.
- **Flow control**- If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender ,the Data link layer imposes a flow ctrl mechanism.
- **Error control**- Used for detecting and retransmitting damaged or lost frames and to prevent duplication of frames. This is achieved through a trailer added at the end of the frame.
- **Access control** -Used to determine which device has control over the link at any given time.

### 3. NETWORK LAYER

This layer is responsible for the delivery of packets from source to destination.



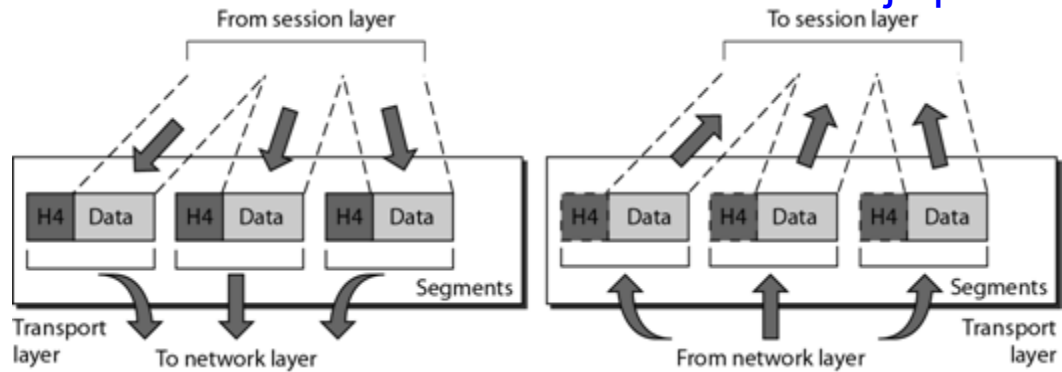
to and

The other responsibilities of this layer are

- **Logical addressing** - If a packet passes the n/w boundary, we need another addressing system for source and destination called logical address.
- **Routing** – The devices which connects various networks called routers are responsible for delivering packets to final destination.

### 4. TRANSPORT LAYER

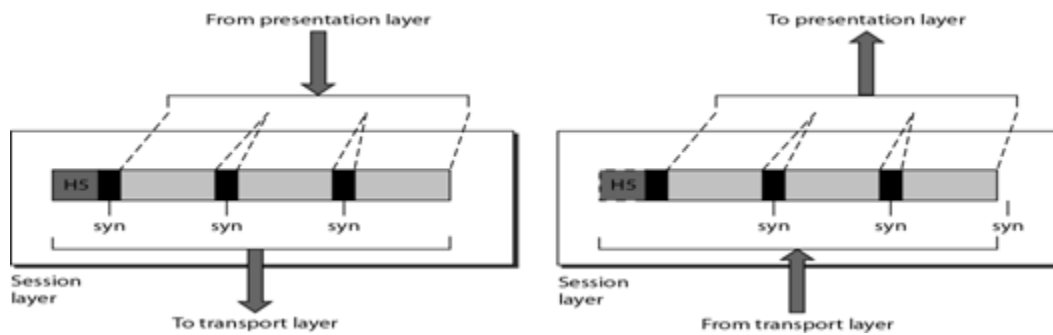
- It is responsible for **Process to Process** delivery.
- It also ensures whether the message arrives in order or not.



The other responsibilities of this layer are

- **Port addressing** - The header in this must therefore include a address called port address. This layer gets the entire message to the correct process on that computer.
- **Segmentation and reassembly** - The message is divided into segments and each segment is assigned a sequence number. These numbers are arranged correctly on the arrival side by this layer.
- **Connection control** - This can either be **connectionless or connection-oriented**. The connectionless treats each segment as a individual packet and delivers to the destination. The connection-oriented makes connection on the destination side before the delivery. After the delivery the termination will be terminated.
- **Flow and error control** - Similar to data link layer, but process to process take place.

## 5. SESSION LAYER



This layer establishes, manages and terminates connections between applications.

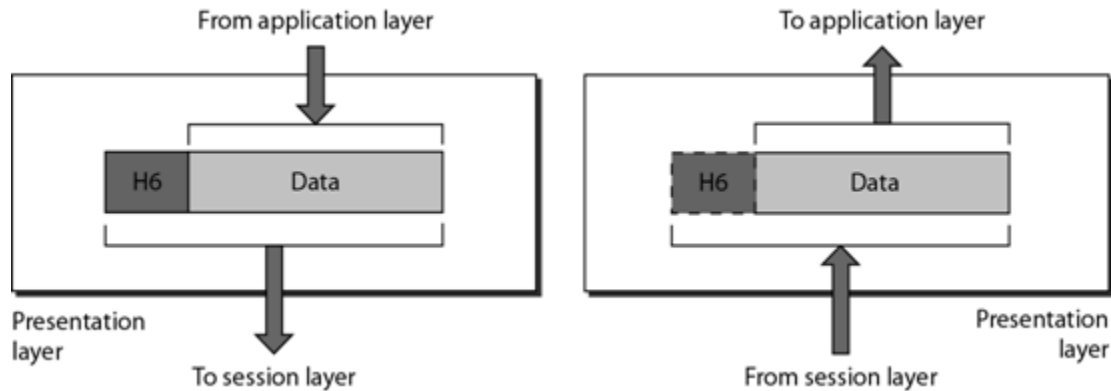
The other responsibilities of this layer are

- **Dialog control** - This session allows two systems to enter into a dialog either in half duplex or full duplex.
- **Synchronization** - This allows to add checkpoints into a stream of data.

## 6. PRESENTATION LAYER

It is concerned with the syntax and semantics of information

exchanged between two systems.

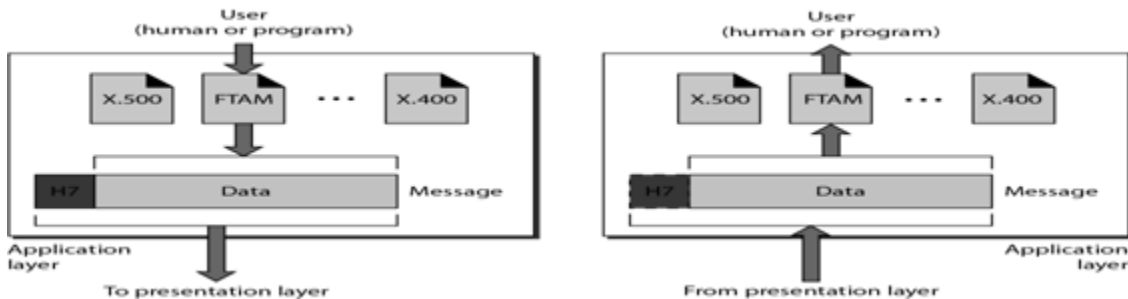


The other responsibilities of this layer are

- **Translation** – Different computers use different encoding system, this layer is responsible for interoperability between these different encoding methods. It will change the message into some common format.
- **Encryption and decryption**-It means that sender transforms the original information to another form and sends the resulting message over the n/w. and vice versa.
- **Compression and expansion**-Compression reduces the number of bits contained in the information particularly in text, audio and video.

## 7 APPLICATION LAYER

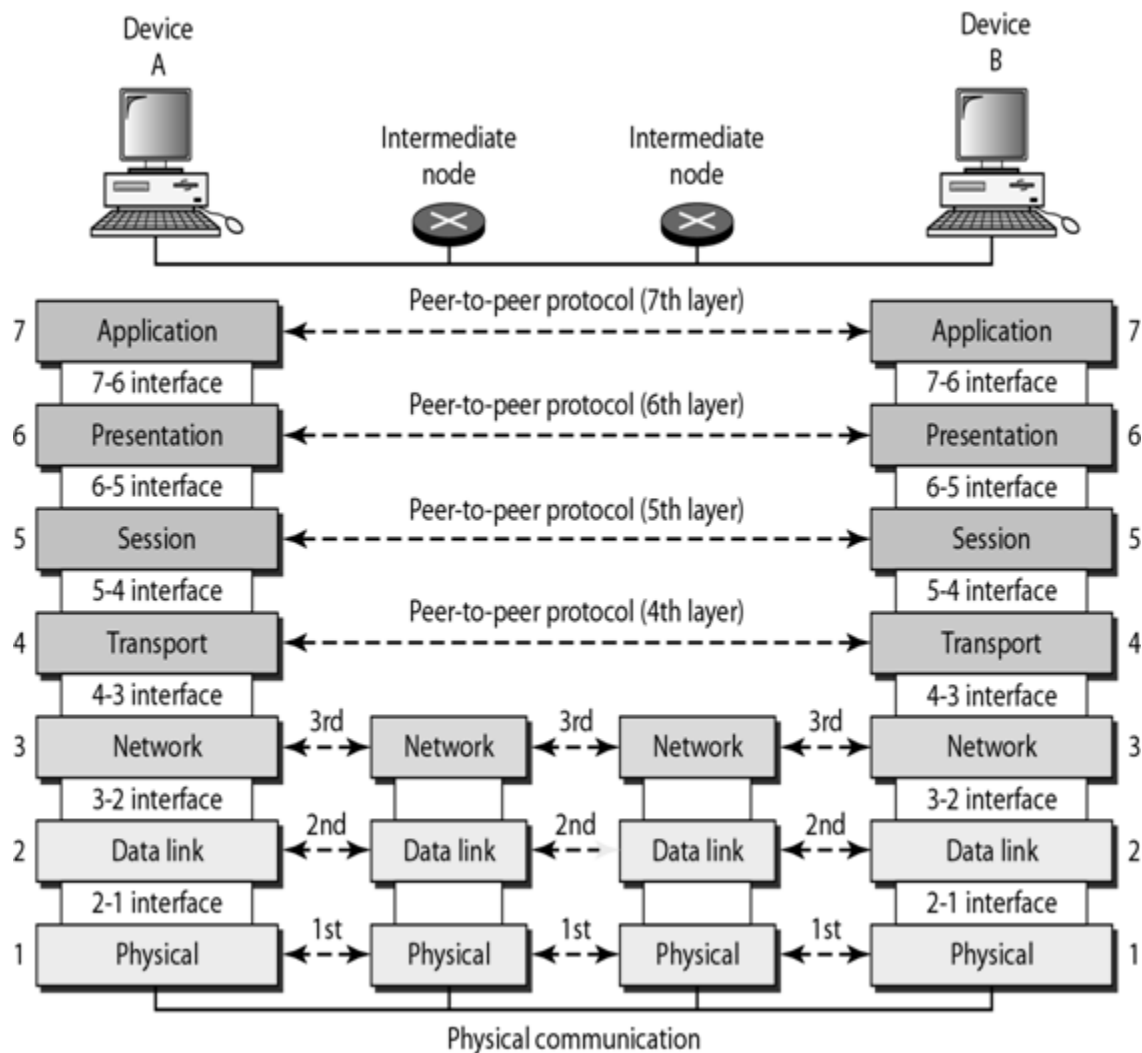
This layer enables the user to access the n/w. This allows the user to log on to remote user.



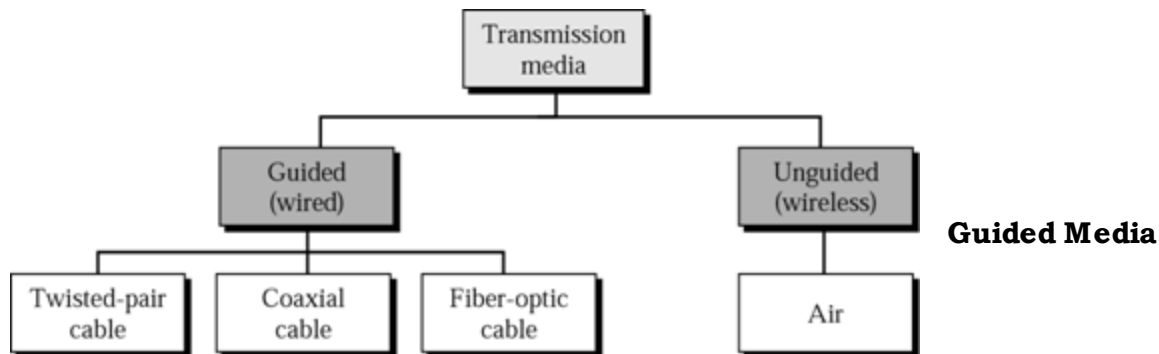
other responsibilities of this layer are

- **FTAM(file transfer,access,mgmt)** - Allows user to access files in a remote host.
- **Mail services** - Provides email forwarding and storage.
- **Directory services** - Provides database sources to access information about various sources and objects.

## The interaction between layers in the OSI model



## Transmission Media



Guided media conduct signals from one device to another include Twisted-pair cable, Coaxial Cable and Fiber-optic cable. A signal traveling along any of these media is directed and contained by the physical limits of the medium.

Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. Optical fiber is a glass cable that accepts and transports signals in the form of light.

### Twisted Pair Cable

A twisted pair consists of two conductors (normally copper) each with its own plastic insulation, twisted together.

- One of the wires is used to carry signals to the receiver
- Other is used as ground reference



Interference and cross talk may affect both the wires and create unwanted signals, if the two wires are parallel.

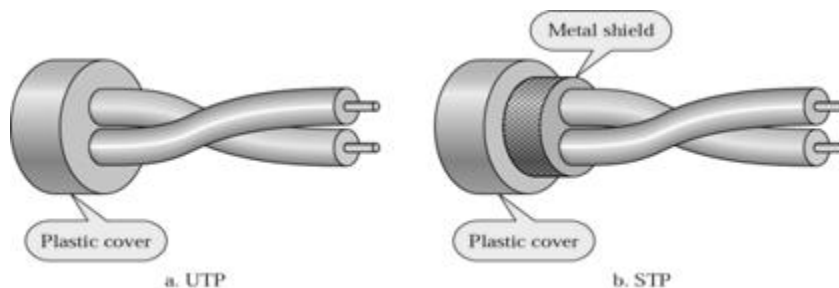
By twisting the pair, a balance is maintained. Suppose in one twist one wire is closer to noise and the other is farther in the next twist the reverse is true. Twisting makes it probable that both wires are equally affected by external influences.

Twisted Pair Cable comes into two forms:

- **Unshielded**
- **Shielded**

### Unshielded versus shielded Twisted-Pair Cable

- Shielded Twisted-Pair (STP) Cable has a metal foil or braided-mesh covering that encases each pair of insulated conductors.
- Metal casing improves that quality of cable by preventing the penetration of noise or cross talk.
- It is more expensive. The following figure shows the difference between UTP and STP



### Applications

- Twisted Pair cables are used in telephone lines to provide voice and data channels.
- Local area networks also use twisted pair cables.

### Connectors

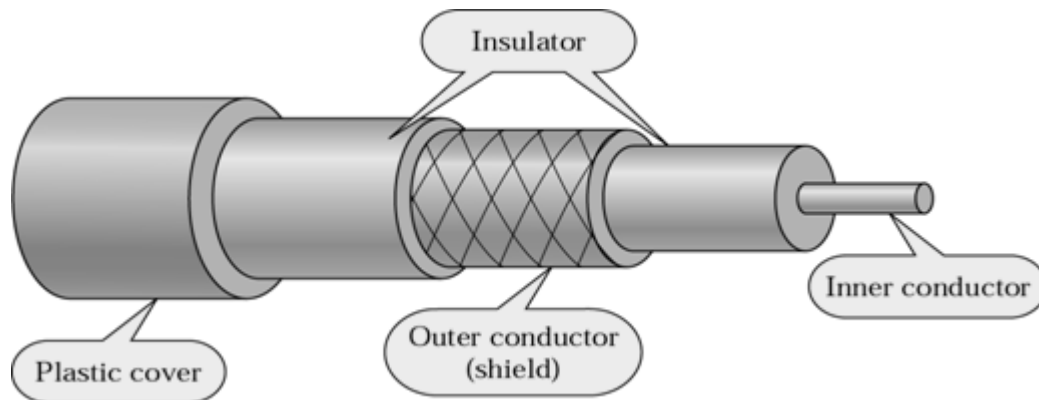
The most common UTP connector is RJ45.

### Coaxial Cable

Coaxial cable (coax) carries signals of higher frequency ranges than twisted pair cable.

Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, and with outer conductor of metal foil.

The outer metallic wrapping serves both as a shield against noise and as the second conductor and the whole cable is protected by a plastic cover.



### Categories of coaxial cables

| Category | Impedance | Use            |
|----------|-----------|----------------|
| RG-59    | 75        | Cable TV       |
| RG-58    | 50        | Thin Ethernet  |
| RG-11    | 50        | Thick Ethernet |

### Applications

- It is used in analog and digital telephone networks
- It is also used in Cable TV networks
- It is used in Ethernet LAN

### Connectors



- BNC connector – to connect the end of the cable to a device
- BNC T - to branch out network connection to computer
- BNC terminator - at the end of the cable to prevent the reflection of the signal.

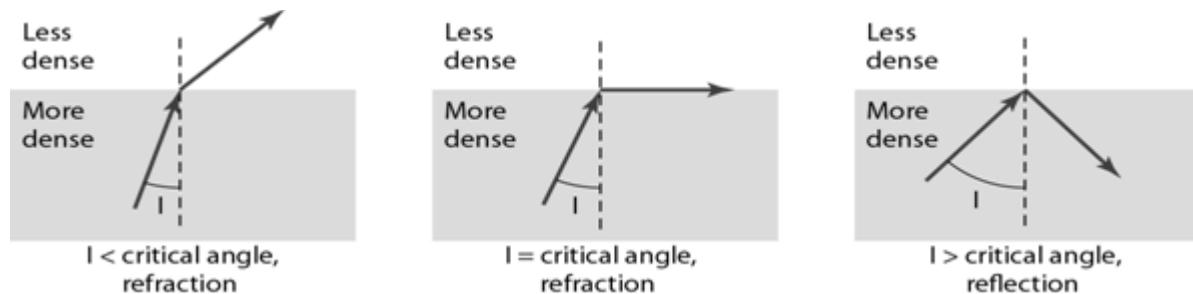
### Fiber Optic Cable

A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.

### Properties of light

- Light travels in a straight line as long as it moves through a single uniform substance. If traveling through one substance suddenly enters another, ray changes its direction.

### Bending of light ray

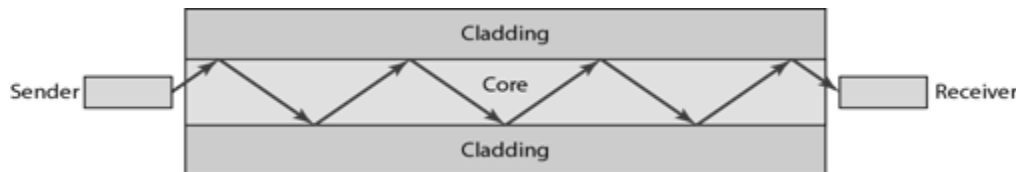


If the angle of incidence (the angle the ray makes with the line perpendicular to the interface between the two media) is less than the critical angle, the ray refracts and moves closer to the surface.

If the angle of incidence is equal to the critical angle, the light bends along the interface.

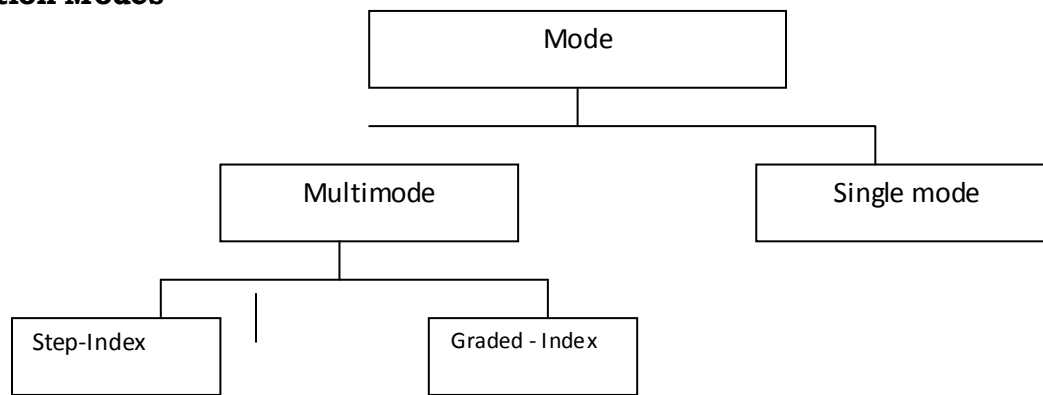
If the angle of incidence is greater than the critical angle, the ray reflects and travels again in the denser substance. Critical angle differs from one medium to another medium.

Optical fibers use reflection to guide light through a channel.



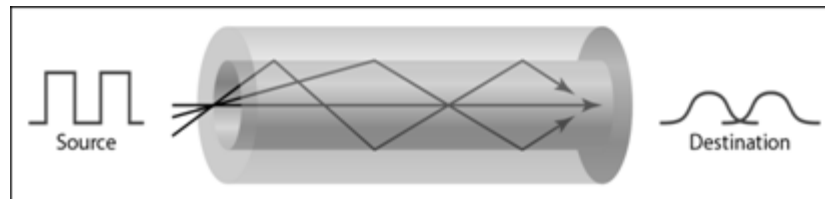
A glass or plastic core is surrounded by a cladding of less dense glass or plastic.

## Propagation Modes

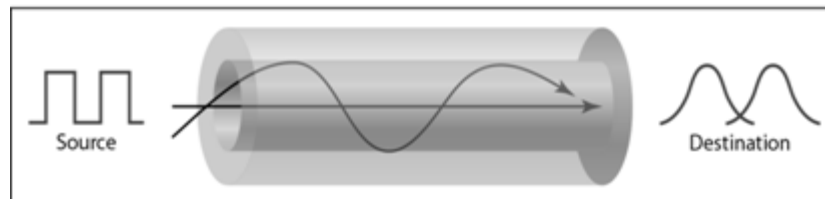


## Multimode

In the multiple mode, multiple light beams from a source move through the core in different paths.



a. Multimode, step index



b. Multimode, graded index



c. Single mode

- **Multimode-Step-index fiber:** The density of core remains constant from the centre to the edge.

A ray of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding. At the interface there is an abrupt change to a lower density that changes the angle of the beam's motion.

- **Multimode- Graded -Index fiber:** The density is varying. Density is highest at the centre of the core and decreases gradually to its lowest at the edge.

## Single Mode

- Single mode uses step-index fiber and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal.

- The single mode fiber itself is manufactured with a much smaller diameter than that of multimedia fiber.

### Connectors

- **Subscriber channel (SC) connector** is used for cable TV.
- **Straight-tip (ST) connector** is used for connecting cable to networking devices.

### Advantages of Optical Fiber

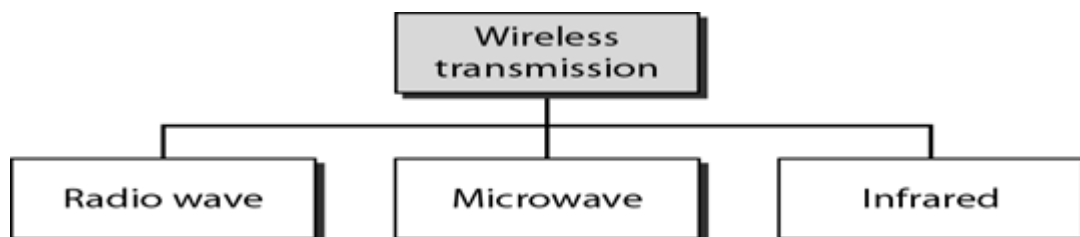
- Noise resistance
- Less signal attenuation
- Light weight

### Disadvantages

- Cost
- Installation and maintenance
- Unidirectional
- Fragility (easily broken)

### Unguided media

- Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication.
- Signals are normally broadcast through air and thus available to anyone who has device capable of receiving them.
- Unguided signals can travel from the source to destination in several ways:
- **Ground propagation** – waves travel through lowest portion on atmosphere.
- **Sky propagation** – High frequency waves radiate upward into ionosphere and reflected back to earth.
- **Line-of-sight propagation** – Very high frequency signals travel in a straight line



### Radio Waves

Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves.

## Properties

- Radio waves are omnidirectional. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned.
- A sending antenna sends waves that can be received by any receiving antenna.
- Radio waves, particularly those of low and medium frequencies, can penetrate walls.

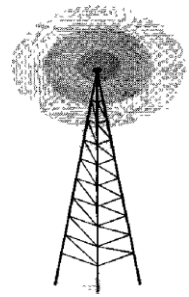


Fig: Omnidirectional antenna

## Disadvantages

- The omnidirectional property has a disadvantage, that the radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band.
- As Radio waves can penetrate through walls, we cannot isolate a communication to just inside or outside a building.

## Applications

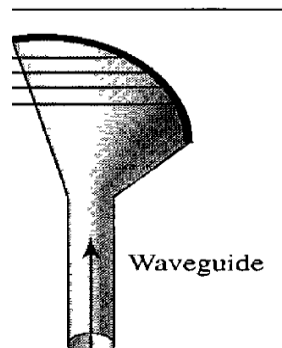
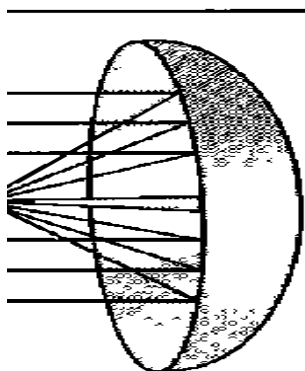
Radio waves are used for multicast communications, such as radio and television, and paging systems.

## Microwaves

Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves.

## Properties

- Microwaves are unidirectional.
- Sending and receiving antennas need to be aligned
- Microwave propagation is line-of-sight
- Very high-frequency microwaves cannot penetrate walls



a) ParabolicDish antenna

b)Horn antenna

- Parabolic Dish antenna focus all incoming waves into single point
- Outgoing transmissions are broadcast through a horn aimed at the dish.

### **Disadvantage**

- If receivers are inside buildings, they cannot receive these waves

### **Applications**

- Microwaves are used for unicast communication such as cellular telephones, satellite networks, and wireless LANs.

### **Infrared**

- Electromagnetic waves with frequencies from 300 GHz to 400 THz are called infrared rays
- Infrared waves, having high frequencies, cannot penetrate walls.

### **Applications**

- Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.

### **Channel Access on links**

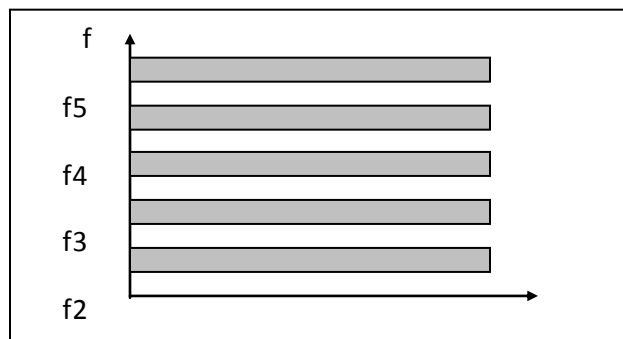
#### **Multiple Access Techniques**

Various multiple access techniques are

- Frequency Division Multiple Access(FDMA)
- Time Division Multiple Access (TDMA)
- Code Division Multiple Access(CDMA)

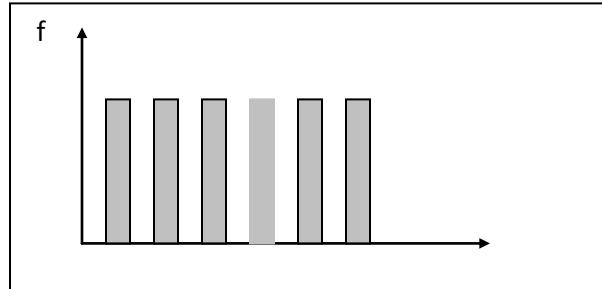
#### **Frequency Division Multiple Access**

- In frequency-division multiple access (FDMA), the available bandwidth is divided into frequency bands.
- Each station is allocated a band to send its data.
- In this method when any one frequency level is kept idle and another is used frequently leads to inefficiency.



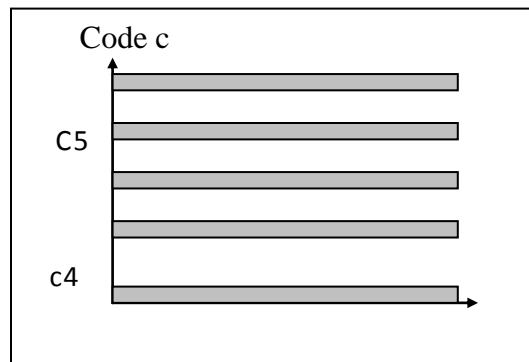
#### **Time Division Multiple Access**

- In time-division multiple access (TDMA), the stations share the bandwidth of the channel in time.
- Each station is allocated a time slot during which it can send data.
- The main problem with TDMA lies in achieving synchronization between the different stations.
- Each station needs to know the beginning of its slot and the location of its slot.



### Code Division Multiple Access

- CDMA differs from FDMA because only one channel occupies the entire bandwidth of the link.
- It differs from TDMA because all stations can send data at the same time without timesharing.
- CDMA simply means communication with different codes.
- CDMA is based on coding theory. Each station is assigned a code, which is a sequence of numbers called chips.
- Chips will be added with the original data and it can be transmitted through same medium.



## Issues in the data link layer

### Framing

To transmit frames over the node it is necessary to mention start and end of each frame. There are three techniques to solve this frame

- Byte-Oriented Protocols (BISYNC, PPP, DDCMP)
- Bit-Oriented Protocols (HDLC)
- Clock-Based Framing (SONET)

### Byte Oriented protocols

In this, view each frame as a collection of bytes (characters) rather than a collection of bits. Such a byte-oriented approach is exemplified by the **BISYNC** (Binary Synchronous Communication) protocol and the **DDCMP** (Digital Data Communication Message Protocol)

### Sentinel Approach

The BISYNC protocol illustrates the sentinel approach to framing; its frame format is

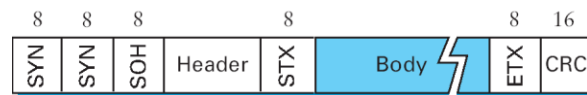


Fig: BISYNC Frame format

- The beginning of a frame is denoted by sending a special SYN (synchronization) character.
- The data portion of the frame is then contained between special sentinel characters: STX (start of text) and ETX (end of text).
- The SOH (start of header) field serves much the same purpose as the STX field.
- The frame format also includes a field labeled CRC (cyclic redundancy check) that is used to detect transmission errors.

The problem with the sentinel approach is that the ETX character might appear in the data portion of the frame. BISYNC overcomes this problem by “escaping” the ETX character by preceding it with a DLE (data-link-escape) character whenever it appears in the body of a frame; the DLE character is also escaped (by preceding it with an extra DLE) in the frame body. This approach is called **character stuffing**.

### Point-to-Point Protocol (PPP)

The more recent Point-to-Point Protocol (PPP). The format of PPP frame is

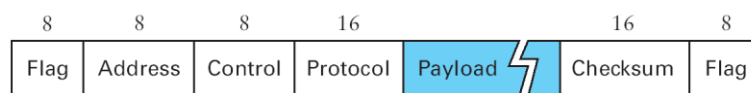


Fig: PPP Frame Format

- The Flag field has 01111110 as starting sequence.

- The Address and Control fields usually contain default values
- The Protocol field is used for demultiplexing.
- The frame payload size can be negotiated, but it is 1500 bytes by default.
- The PPP frame format is unusual in that several of the field sizes are negotiated rather than fixed.
- Negotiation is conducted by a protocol called LCP (Link Control Protocol).
- LCP sends control messages encapsulated in PPP frames—such messages are denoted by an LCP identifier in the PPP Protocol.

### Byte-Counting Approach

The number of bytes contained in a frame can be included as a field in the frame header. DDCMP protocol is used for this approach. The frame format is

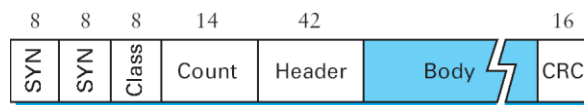


Fig: DDCMP frame format

- COUNT Field specifies how many bytes are contained in the frame's body.
- Sometime count field will be corrupted during transmission, so the receiver will accumulate as many bytes as the COUNT field indicates. This is sometimes called a **framing error**.
- The receiver will then wait until it sees the next SYN character.

### Bit-Oriented Protocols (HDLC)

In this, frames are viewed as collection of bits. High level data link protocol is used. The format is



Fig: HDLC Frame Format

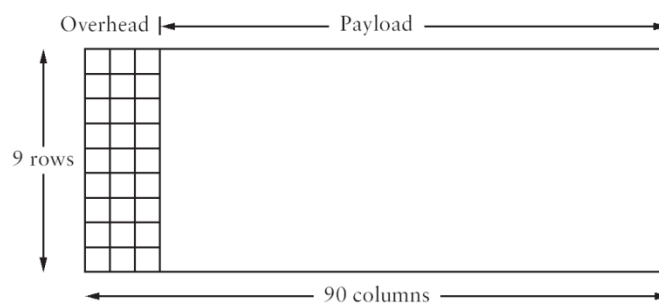
- HDLC denotes both the beginning and the end of a frame with the distinguished bit sequence 01111110.
- This sequence might appear anywhere in the body of the frame, it can be avoided by bit stuffing.
- On the sending side, any time five consecutive 1's have been transmitted from the body of the message (i.e., excluding when the sender is trying to transmit the distinguished 01111110 sequence), the sender inserts a 0 before transmitting the next bit.



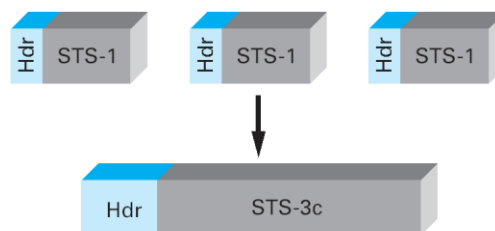
- On the receiving side, five consecutive 1's arrived, the receiver makes its decision based on the next bit it sees (i.e., the bit following the five is).
- If the next bit is a 0, it must have been stuffed, and so the receiver removes it. If the next bit is a 1, then one of two things is true, either this is the end-of-frame marker or an error has been introduced into the bit stream.
- By looking at the next bit, the receiver can distinguish between these two cases:  
If it sees a 0 (i.e., the last eight bits it has looked at are 01111110), then it is the end-of-frame marker.  
If it sees a 1 (i.e., the last eight bits it has looked at are 01111111), then there must have been an error and the whole frame is discarded.

### **Clock-Based Framing (SONET)**

- Synchronous Optical Network Standard is used for long distance transmission of data over optical network.
- It supports multiplexing of several low speed links into one high speed links.
- An STS-1 frame is used in this method.



- It is arranged as nine rows of 90 bytes each, and the first 3 bytes of each row are overhead, with the rest being available for data.
- The first 2 bytes of the frame contain a special bit pattern, and it is these bytes that enable the receiver to determine where the frame starts.
- The receiver looks for the special bit pattern consistently, once in every 810 bytes, since each frame is  $9 \times 90 = 810$  bytes long.



- The STS-N frame can be thought of as consisting of N STS-1 frames, where the bytes from these frames are interleaved; that is, a byte from the first frame is transmitted, then a byte from the second frame is transmitted, and so on.
- Payload from these STS-1 frames can be linked together to form a larger STS-N payload, such a link is denoted STS-Nc. One of the bits in overhead is used for this purpose.

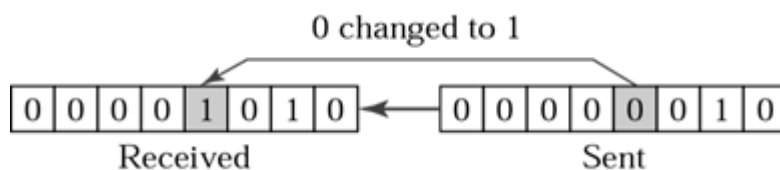
### **Error Detection and Correction**

Data can be corrupted during transmission. For reliable communication, errors must be detected and corrected.

#### **Types of Errors**

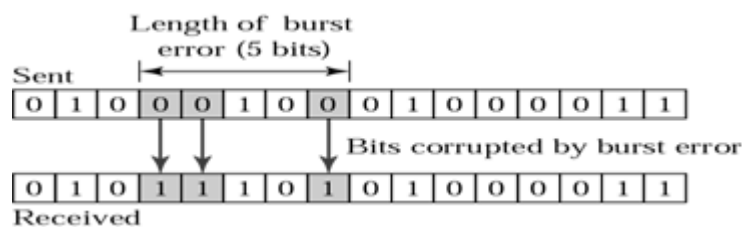
##### **Single-bit error**

The term Single-bit error means that only one bit of a given data unit (such as byte, character, data unit or packet) is changed from 1 to 0 or from 0 to 1.



##### **Burst Error**

The term Burst Error means that two or more bits in the data unit have changed from 1 to 0 or from 0 to 1.



##### **Redundancy**

One method is to send every data twice, so that receiver checks every bit of two copies and detect error.

##### **Drawbacks**

- Sends n-redundant bits for n-bit message.
  - Many errors are undetected if both the copies are corrupted.
- Instead of adding entire data, some bits are appended to each unit.

This is called redundant bit because the bits added will not give any new information. These bits are called error detecting codes.

The three error detecting techniques are:

- Parity check
- Check sum algorithm
- Cyclic Redundancy Check

## Parity Check

### Simple parity check

Only one redundant bit, called parity bit is added to every data unit so that the total number of 1's in unit become even (or odd)

### Two Dimensional Parity

- It is based on simple parity.
- It performs calculation for each bit position across each byte in the frame.
- This adds extra parity byte for entire frame, in addition to a parity bit for each byte.

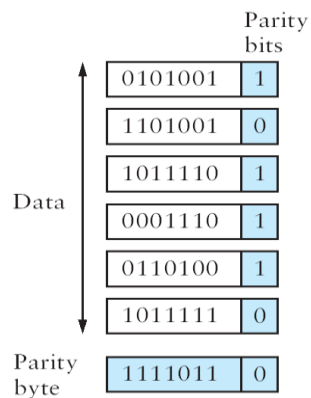


Fig: Two-dimensional parity

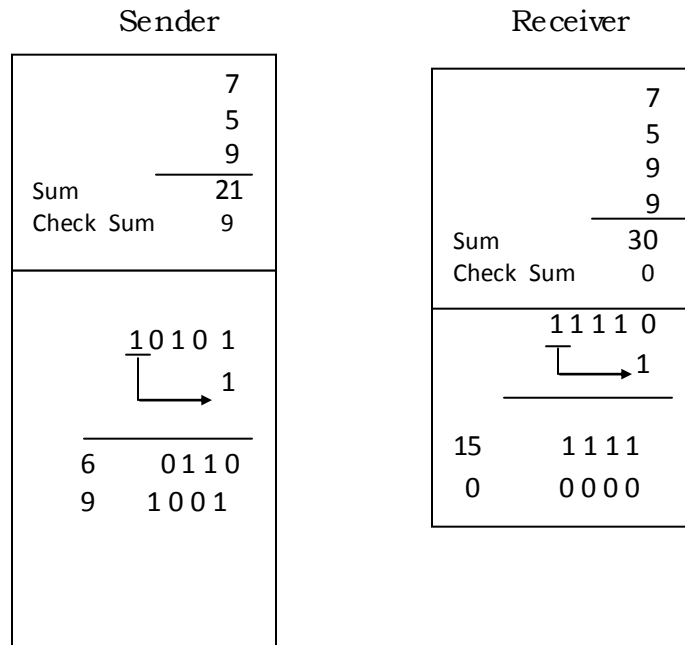
For example frame containing 6 bytes of data. In this third bit of the parity byte is 1 since there are an odd number of 1's is in the third bit across the 6 bytes in the frame.

In this case, 14 bits of redundant information are added with original information.

### Check sum algorithm

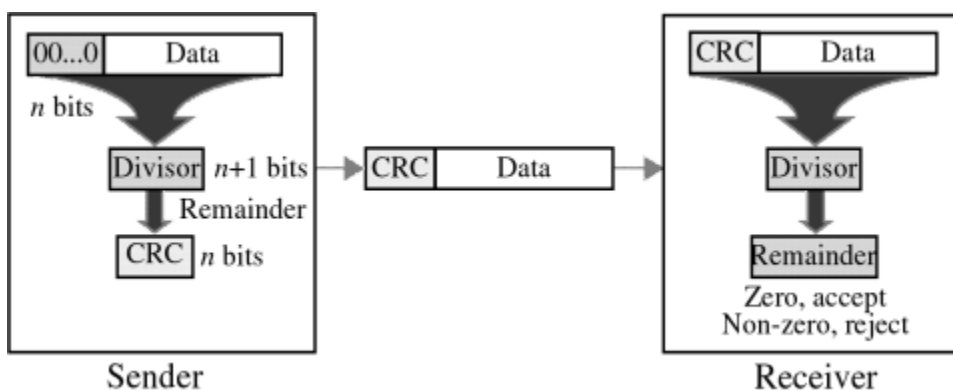
- In the sender side all the words are added and then transmit the result of sum called checksum with the data.
- The receiver performs the same calculation on the received data and compares the result with the received checksum.

- If any transmitted data, including the checksum itself, is corrupted, then the results will not match, so the receiver knows that an error occurred.
- Instead of sending the checksum as such, one's complement of that sum will be sent to the receiver. If the receiver gets the result as zero then it will be the correct one.
- In this, we can represent unsigned number from 0 to  $2^n$  using  $n$  bits.
- If the number has more than  $n$  bits, the extra leftmost bits need to be added to the  $n$  rightmost bits.
- Data can be divided in to 16 bit word and the Checksum is initialized to zero.



### Cyclic Redundancy Check

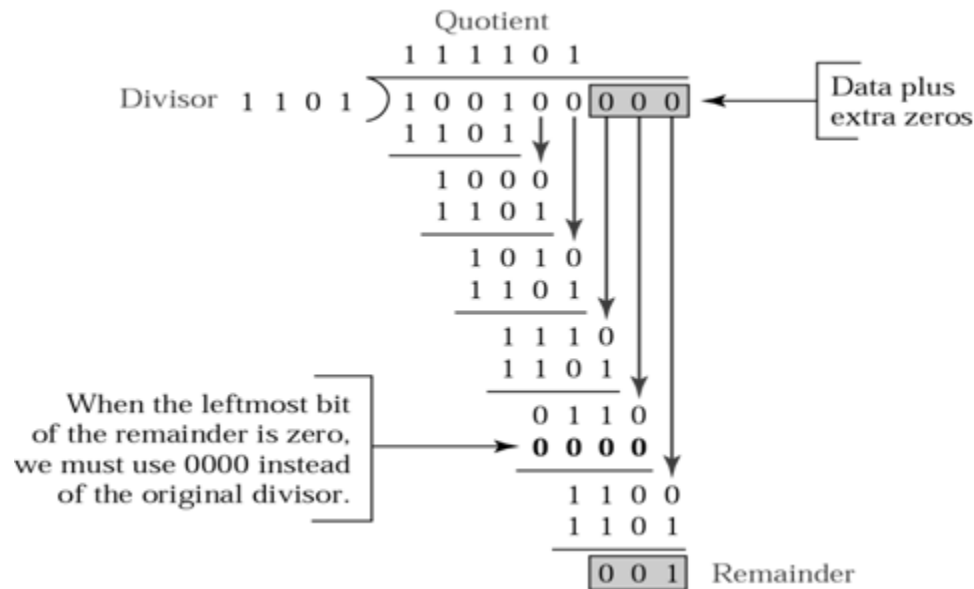
- It uses small number of redundant bits to detect errors.
  - Divisor is calculated by the polynomial functions under two conditions
    - It should not be divisible by  $x$
    - It should be divisible by  $x+1$
- 8 Consider the original message as  $M(x) - n+1$  bits
- 9 Divisor  $C(x) - K$  bits
- 10 Original sent message =  $M(x) + k-1$  bits



## Steps

- Append  $k-1$  zeros with  $M(x) - P(x)$
- Divide  $P(x)$  by  $C(x)$
- Subtract the remainder from  $T(x)$
- Subtraction is made by making XOR operation

Eg: 100100 by 1101



## Error Correction

Error Correction can be handled in two ways

1. When an error is discovered, the receiver can have the sender to retransmit the entire data unit.
2. A receiver can use an error correcting code, which automatically correct certain errors.

Error correcting codes are more sophisticated than error-detection codes and require more redundancy bits.

In single bit error detection only two states are sufficient.

1) error

2) no error

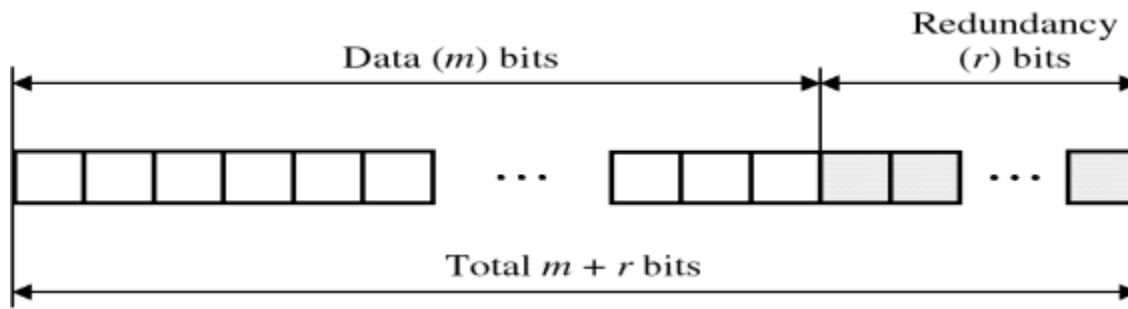
Two states are not enough to detect an error but not to correct it.

## Redundancy Bits

- To calculate the number of redundancy bit( $r$ ) required to correct a given number of data bits ( $m$ ), we must find a relationship between  $m$  and  $r$ .

- Add  $m$  bits of data with  $r$  bits. The length of the resulting code is  $m+r$ .

### Data and Redundancy bits



- If the total number of bits are  $m+r$ , then  $r$  must be able to indicate at least  $m+r+1$  different states.  $r$  bits can indicate  $2^r$  different states. Therefore,  $2^r$  must be equal to or greater than  $m+r+1$

$$2^r \geq m+r+1$$

- For example if the value of  $m$  is 7 the smallest  $r$  value that can satisfy this equation is 4.

### Relationship between data and redundancy bits

| Number of Data Bits (m) | Number of redundancy Bits(r) | Total bits (m+r) |
|-------------------------|------------------------------|------------------|
| 1                       | 2                            | 3                |
| 2                       | 3                            | 5                |
| 3                       | 3                            | 6                |
| 4                       | 3                            | 7                |
| 5                       | 4                            | 9                |
| 6                       | 4                            | 10               |
| 7                       | 4                            | 11               |

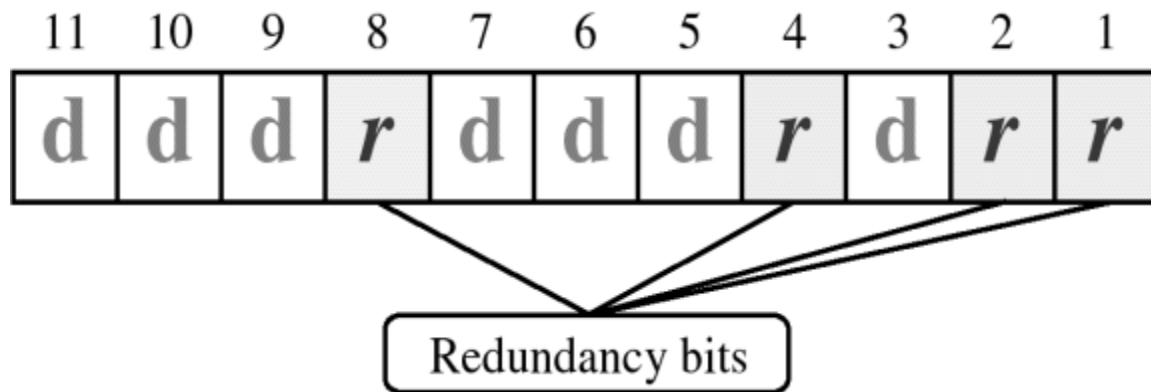
### Hamming Code

R.W. Hamming provides a practical solution for the error correction.

### Positioning the Redundancy Bits

For example, a seven-bit ASCII code requires four redundancy bits that can be added to the end of the data or intersperse with the original data bits. These redundancy bits are placed in positions 1, 2, 4 and 8. We refer these bits as  $r_1$ ,  $r_2$ ,  $r_3$  and  $r_4$

### Position of redundancy bits in Hamming code



The combination used to calculate each of the four *r* values for a seven-bit data sequence are as follows

- The *r*<sub>1</sub> bit is calculated using all bits positions whose binary representation include a 1 in the rightmost position
- *r*<sub>2</sub> is calculated using all bit position with a 1 in the second position and so on

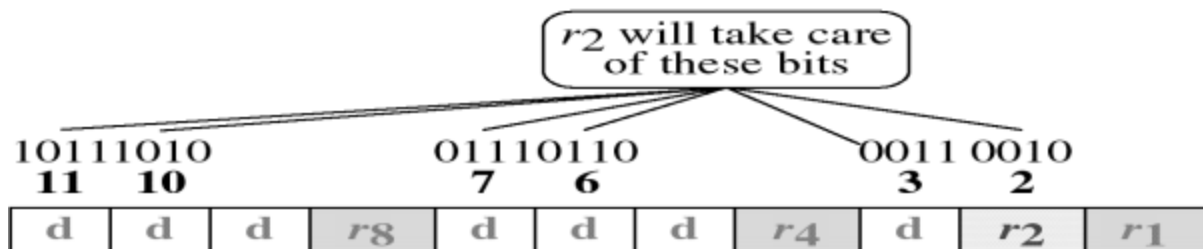
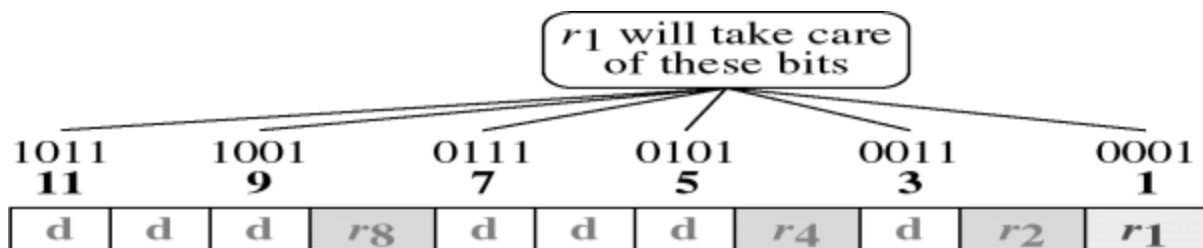
*r*<sub>1</sub>: bits 1,3,5,7,9,11

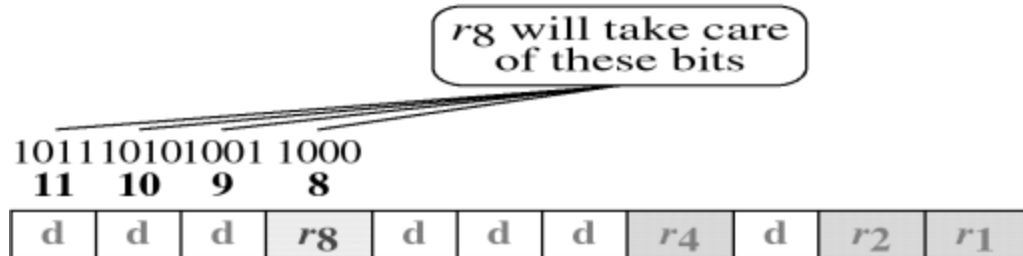
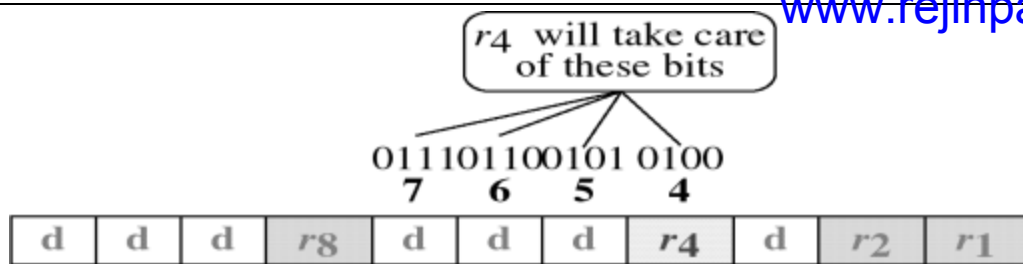
*r*<sub>2</sub>: bits 2, 3, 6, 7, 10, 11

*r*<sub>3</sub>: bits 4, 5, 6, 7

*r*<sub>4</sub>: bits 8, 9, 10, 11

### Redundancy bits calculation





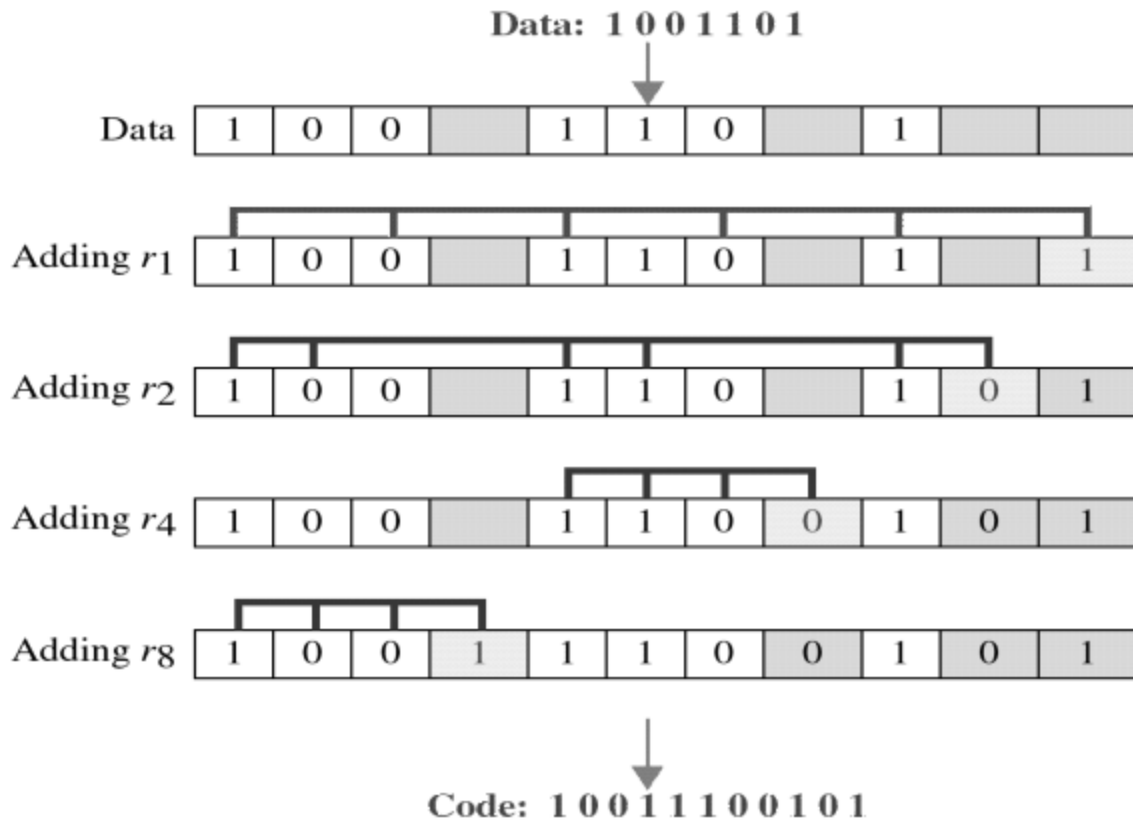
### Calculating the r values

- Place each bit of the original character in its appropriate position in the 11-bit unit.
- Calculate the even parities for the various bit combination.
- The parity value for each combination is the value of the corresponding r bit.

### For example,

- The value of r<sub>1</sub> is calculated to provide even parity for a combination of bits 3,5,7,9 and 11.
- The value of r<sub>2</sub> is calculated to provide even parity with bits 3, 6, 7, 10 and 11.
- The value of r<sub>3</sub> is calculated to provide even parity with bits 4,5,6 and 7.
- The value of r<sub>4</sub> is calculated to provide even parity with bits 8,9,10 and 11.

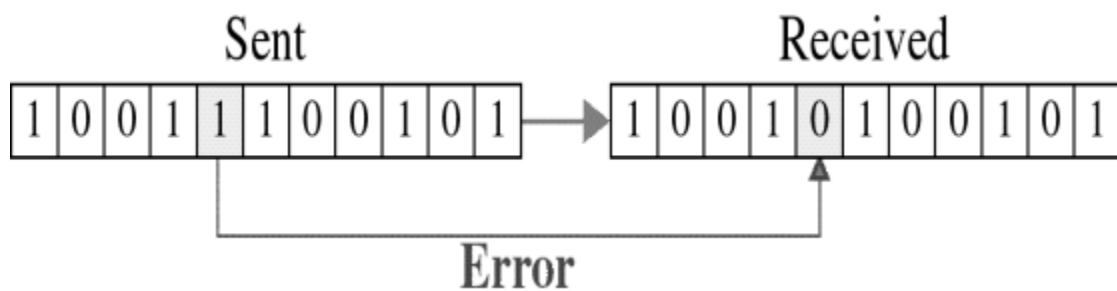




### Error Detection and Correction

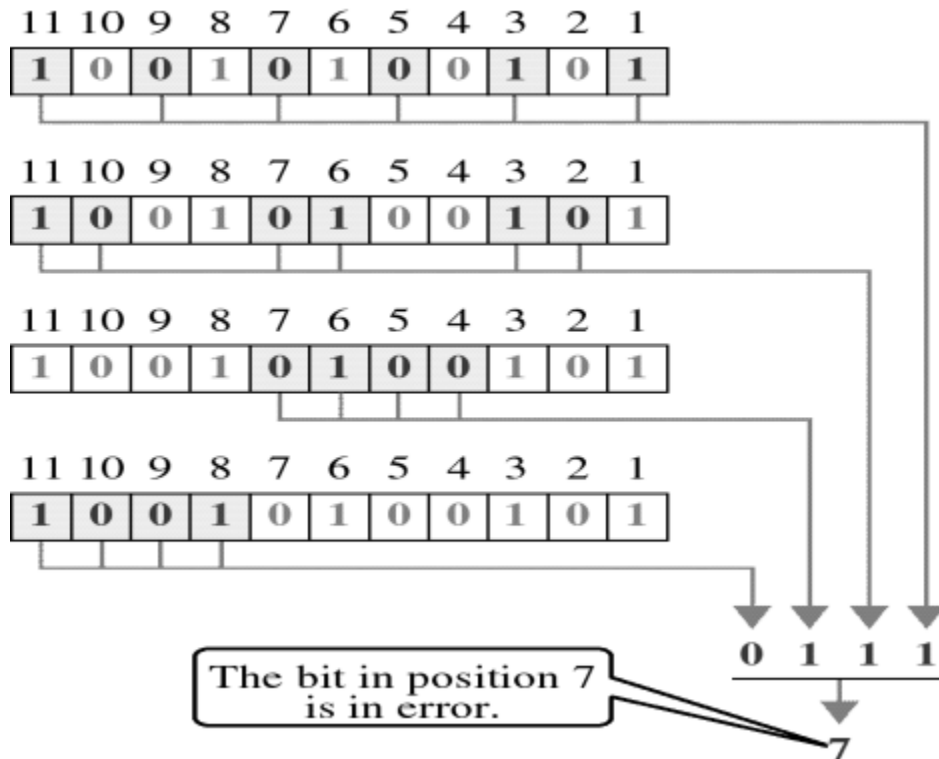
Now imagine the received data has 7th bit changed from 1 to 0.

#### Single-bit error



The receiver takes the transmission and recalculates four new data using the same set of bits used by the sender plus the relevant parity (r) bit for each set.

#### Error detection



- Then it assembles the new parity values into a binary number in order of  $r$  position ( $r_8, r_4, r_2, r_1$ ).
- This step gives us the binary number 0111(7 in decimal) which is the precise location of the bit in error.
- Once the bit is identified, the receiver can reverse its value and correct the error.

## Hamming Distance

One of the central concepts in coding for error control is the idea of the Hamming distance.

- The Hamming distance between two words (of the same size) is the number of differences between the corresponding bits. The Hamming distance between two words  $x$  and  $y$  is  $d(x, y)$ .
- The Hamming distance can be found by applying the XOR operation on the two words and count the number of 1's in the result.
- In a set of words, the minimum Hamming distance is the smallest Hamming distance between all possible pairs. We use  $d_{min}$  to define the minimum Hamming distance in a coding scheme.

# GSM

# Global System for Mobile Communication

# GSM: Overview

## □ GSM

- formerly: Groupe Spéciale Mobile (founded 1982)
- now: Global System for Mobile Communication
- Pan-European standard (ETSI, European Telecommunications Standardisation Institute)

## □ Today many providers all over the world use GSM

(219 countries in Asia, Africa, Europe, Australia, America)

- more than 4,2 billion subscribers in more than 700 networks
- more than 75% of all digital mobile phones use GSM
- over 29 billion SMS in Germany in 2008, (> 10% of the revenues for many operators) [be aware: these are only rough numbers...]
- See e.g. [www.gsmworld.com/newsroom/market-data/index.htm](http://www.gsmworld.com/newsroom/market-data/index.htm)

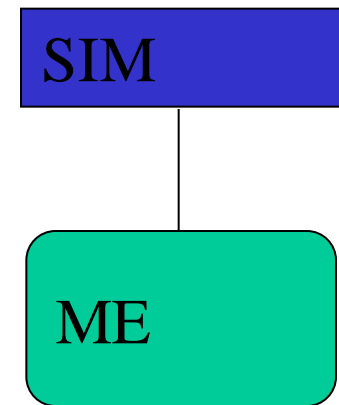
# Disadvantages of GSM

- ❑ There is no perfect system!!
  - no end-to-end encryption of user data
  - no full ISDN bandwidth of 64 kbit/s to the user, no transparent B-channel
- ❑ reduced concentration while driving
- ❑ electromagnetic radiation
- ❑ abuse of private data possible
- ❑ roaming profiles accessible
- ❑ high complexity of the system
- ❑ several incompatibilities within the GSM standards

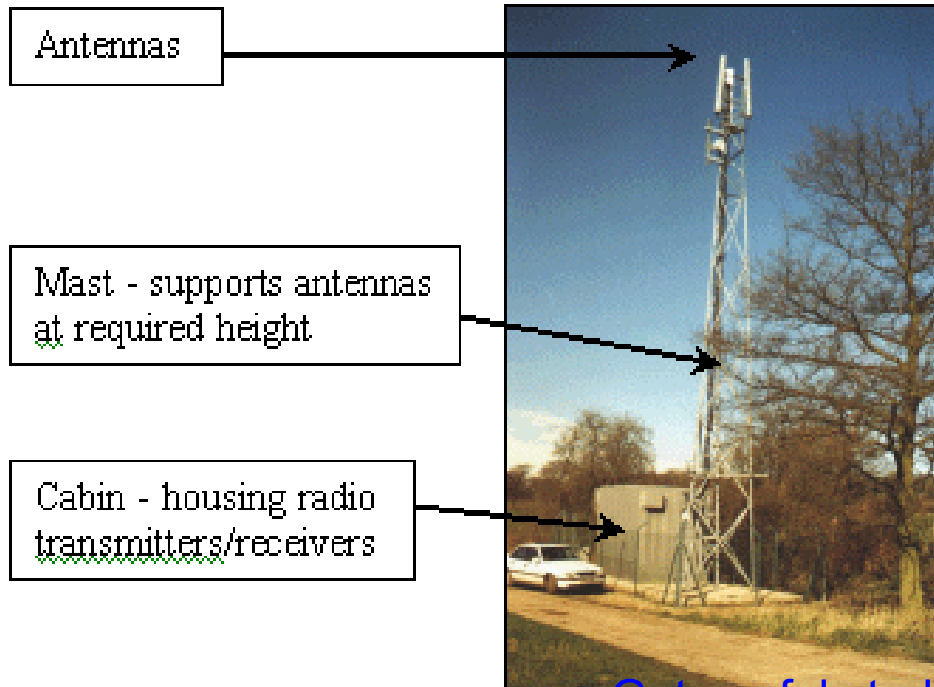
# GSM user equipment

- ❑ User equipment: Mobile equipment (ME) + SIM card
  - Subscriber Identity Module (SIM) contains encryption key and personal data
  - The user is uniquely identified through "International Mobile Subscriber Identity" (IMSI)
  - The mobile equipment is uniquely identified through "International Mobile Equipment Identity" (IMEI)
  - Both equipment and user uniquely identified

SIM =  
Subscriber Identity Module



# Some base station equipment

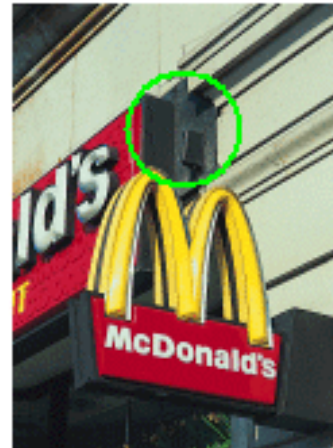




# Some more base station equipment



Typical macro cell



Typical micro cell

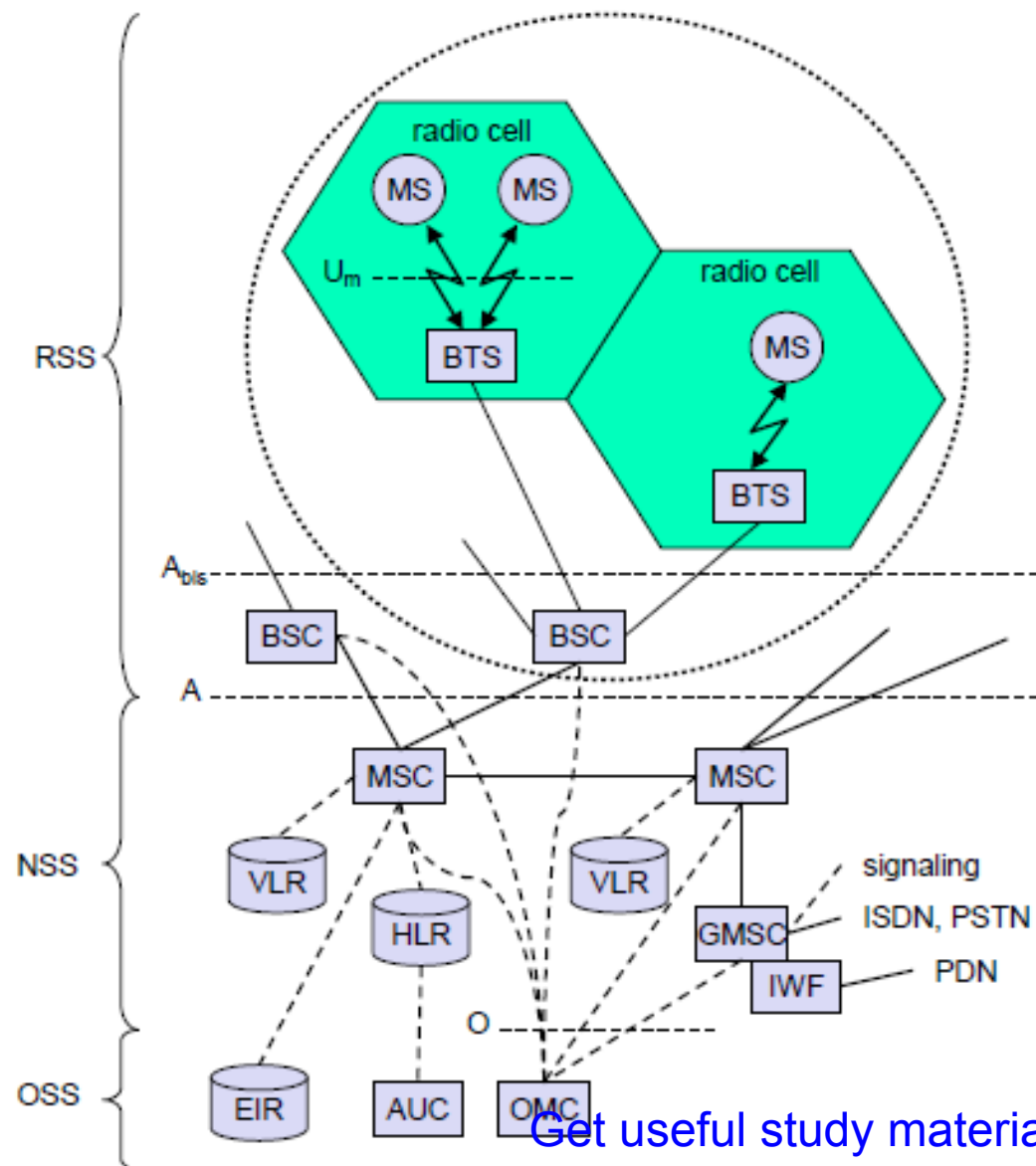
# Architecture of the GSM system

- ❑ GSM is a PLMN (Public Land Mobile Network)
  - several providers setup mobile networks following the GSM standard within each country
  - components
    - MS (mobile station)
    - BS (base station)
    - MSC (mobile switching center)
    - LR (location register)
  - subsystems
    - RSS (radio subsystem): covers all radio aspects
    - NSS (network and switching subsystem): call forwarding, handover, switching
    - OSS (operation subsystem): management of the network

## The Radio Station Subsystem The Wireless Part

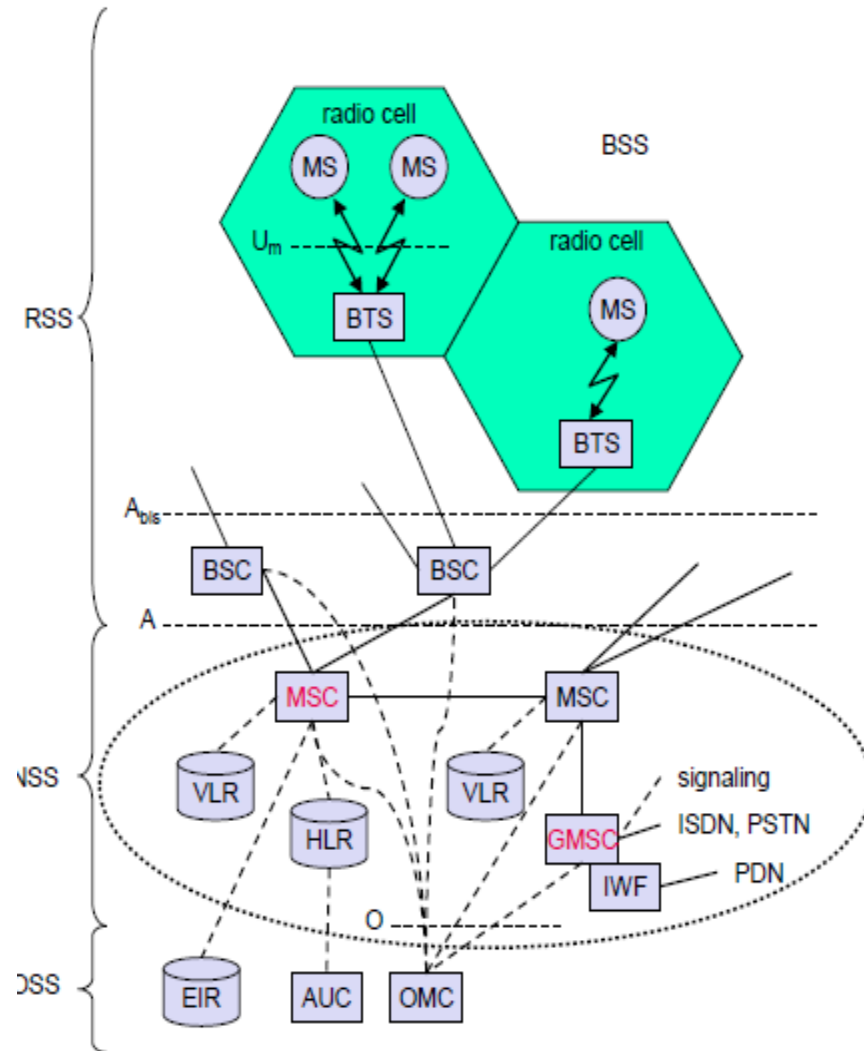
**Base Transceiver Station (BTS)**  
cell coverage, comprises radio functions

**Base Station Controller (BSC)**  
controls several BTSs, the switch center for radio channels



### Functions

|  |
|--|
| Management of radio channels               |
| Frequency hopping (FH)                     |
| Management of terrestrial channels         |
| Mapping of terrestrial onto radio channels |
| Channel coding and decoding                |
| Rate adaptation                            |
| Encryption and decryption                  |
| Paging                                     |
| Uplink signal measurements                 |
| Traffic measurement                        |
| Authentication                             |
| Location registry, location update         |
| Handover management                        |



The Network Switching Subsystem (NSS) -

The Mobile Switching Centre (MSC) manages a large number of BSCs

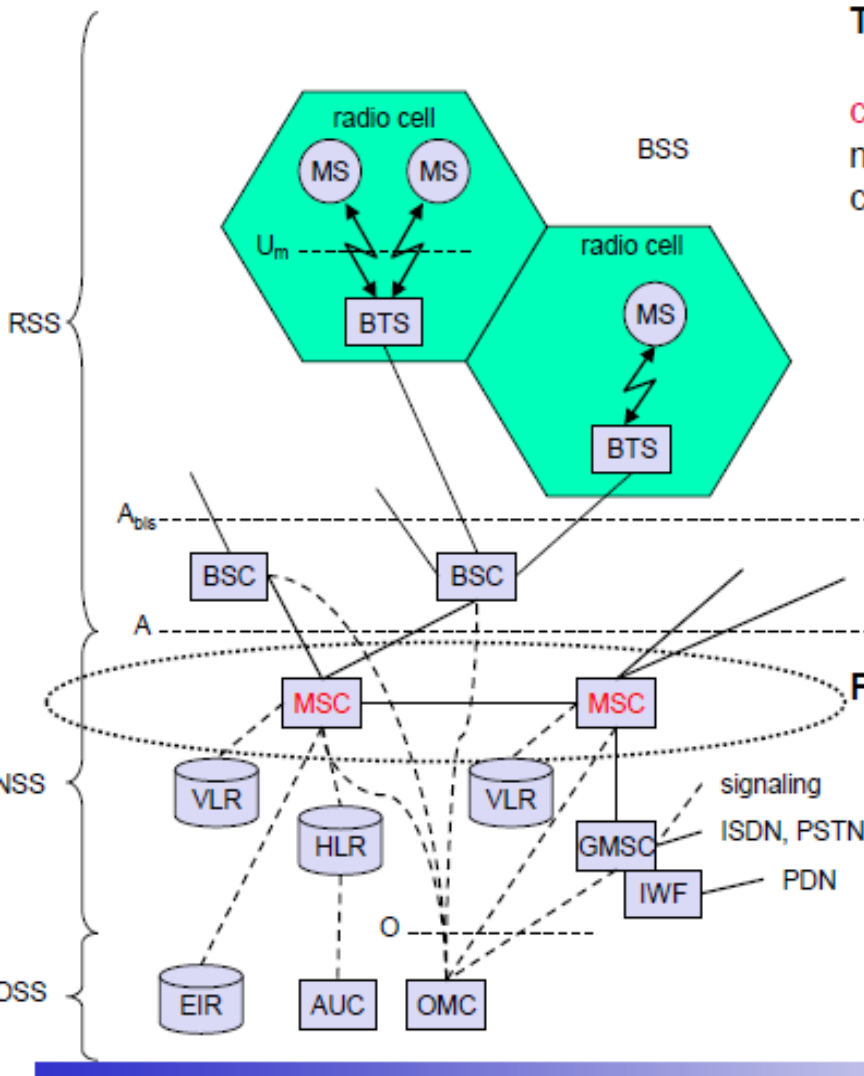
Gateway Mobile Switching Centre (GMSC) is the gateway to other networks

Various Registers (data bases)

Signalling messages and data base accesses are transported by the Signalling System Nr. 7 (SS7) using the Mobile Application Part (MAP)



# GSM: elements and interfaces



## The MSC plays a central role in GSM

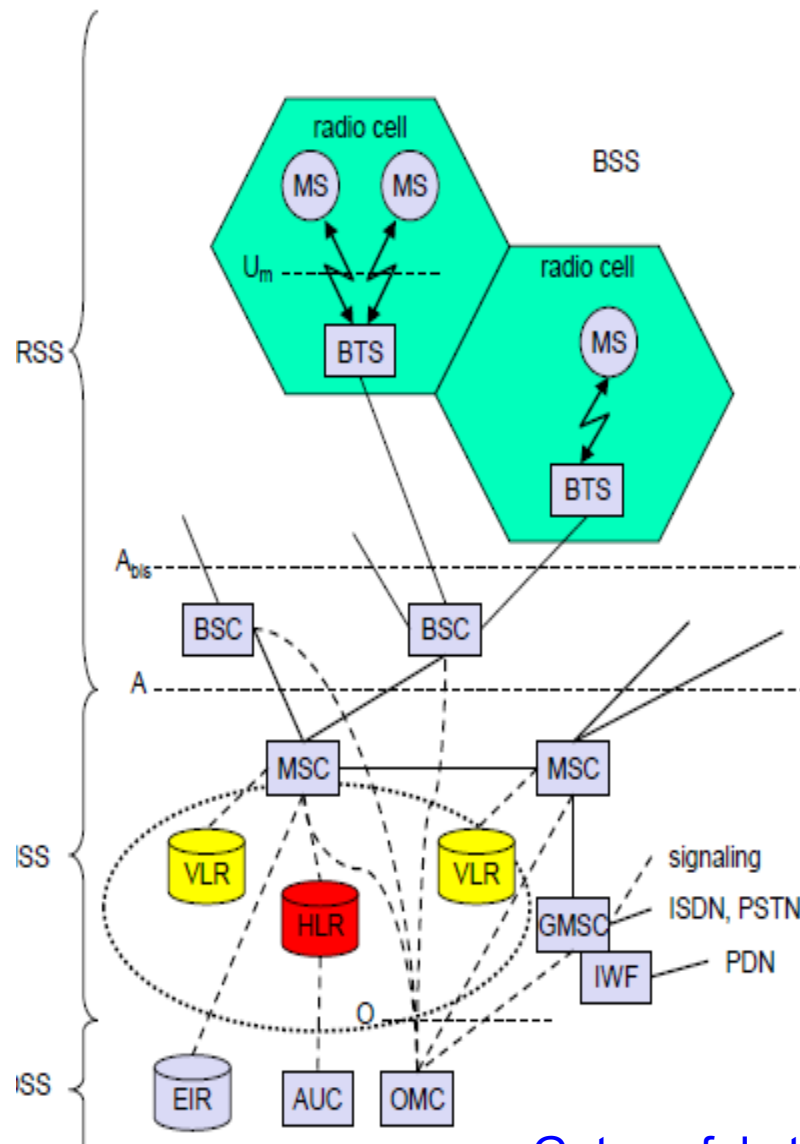
**controls all connections** via a separated network to/from a mobile terminal within the domain of the MSC - several BSC can belong to a MSC

- switching functions
- additional functions for mobility support
- management of network resources
- interworking functions via Gateway MSC (GMSC)
- integration of several databases

## Functions of a MSC

- specific functions for paging and call forwarding
- mobility specific signaling
- location registration and forwarding of location information
- support of short message service (SMS)
- generation and forwarding of accounting and billing information





## Home Location Register (HLR)

Central master database containing user data, permanent and semi-permanent data of all subscribers assigned to the HLR

- \* usually one HLR per provider
- \* primarily a data base for subscriber data.
- \* Subscriber identifiers service profiles, etc.
- \* Localization information (current VLR, MSC)
- \* Is a platform for all kinds of services

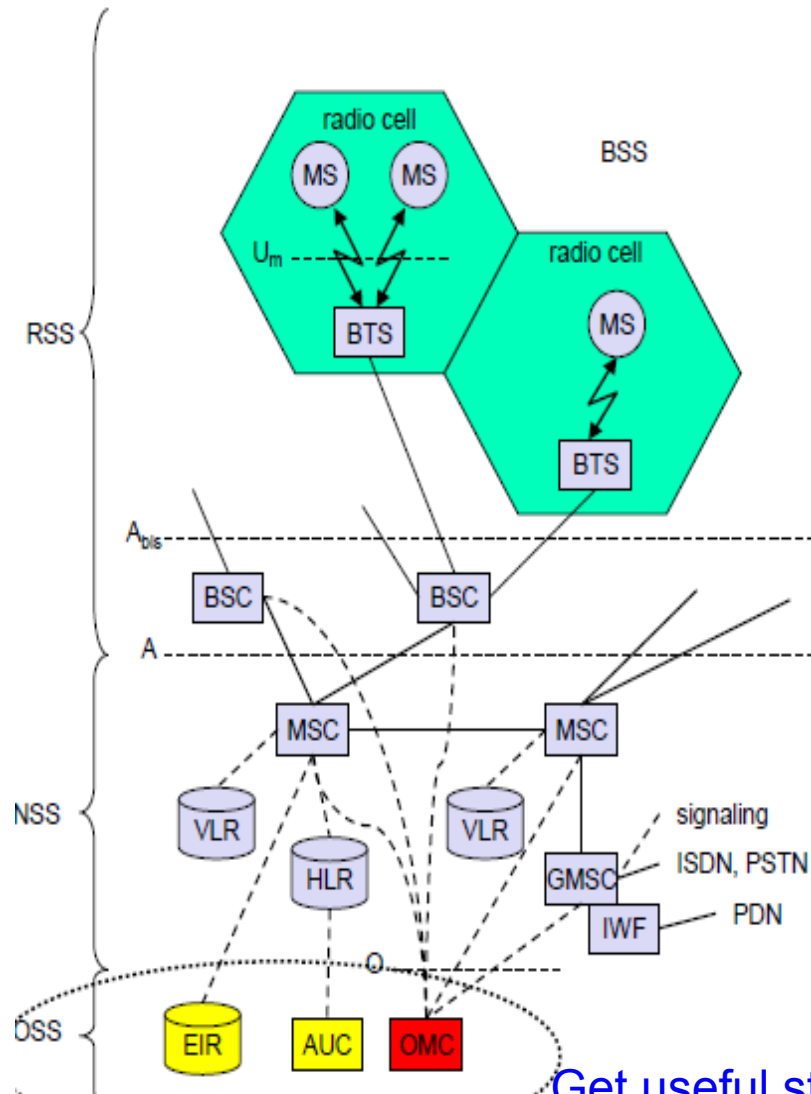
## Visitor Location Register (VLR)

local database for a subset of user data, including data about all user currently in the domain of the VLR

- \* usually one VLR per MSC
- \* stores all relevant data of visiting MS



# System Architecture



The OSS (Operation Subsystem) enables centralized operation, management, and maintenance of all GSM subsystems

## □ Components

Authentication Center (AUC)

Equipment Identity Register (EIR)

Operation and Maintenance Center (OMC)  
different control capabilities for the radio  
subsystem and the network subsystem



# Ingredients 1: Mobile Phones, PDAs, etc



The visible but **smallest** part of the network!



# GSM radio interface - Main characteristics

## ❑ Frequency bands:

### ○ GSM 900:

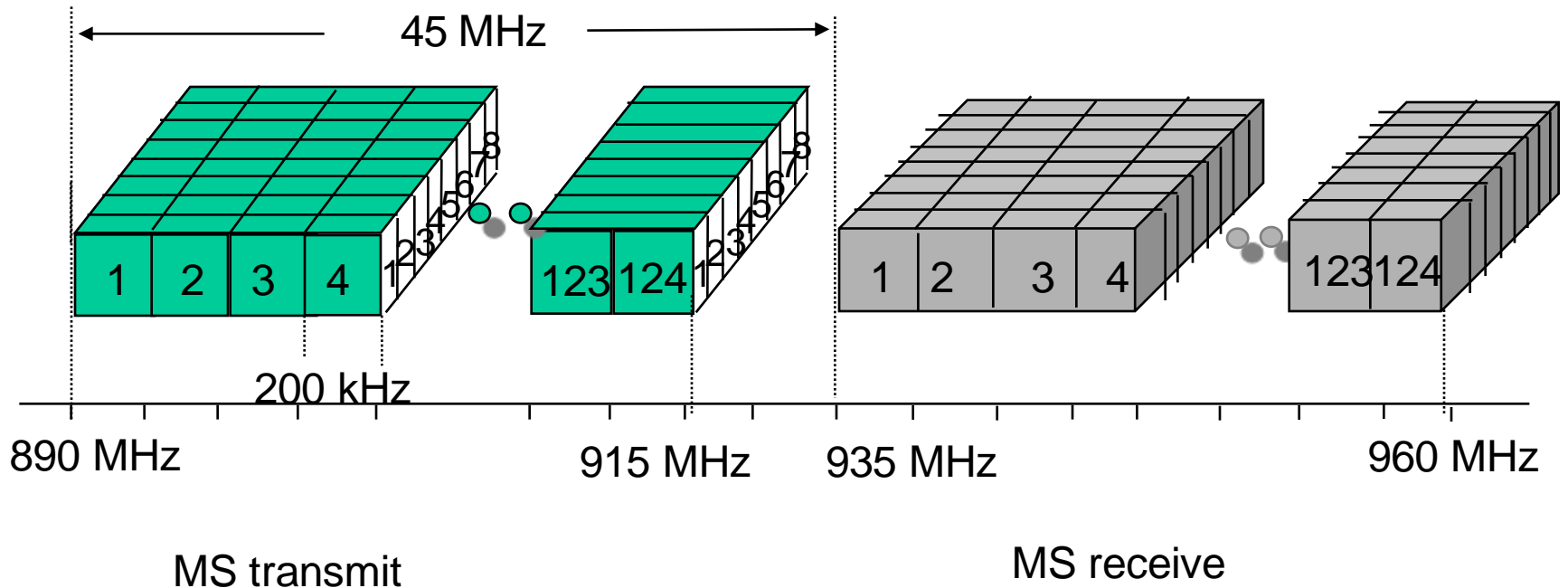
- 890 - 915 MHz: Uplink (MS transmit)
- 935 - 960 MHz: Downlink (MS receive)

### ○ GSM 1800:

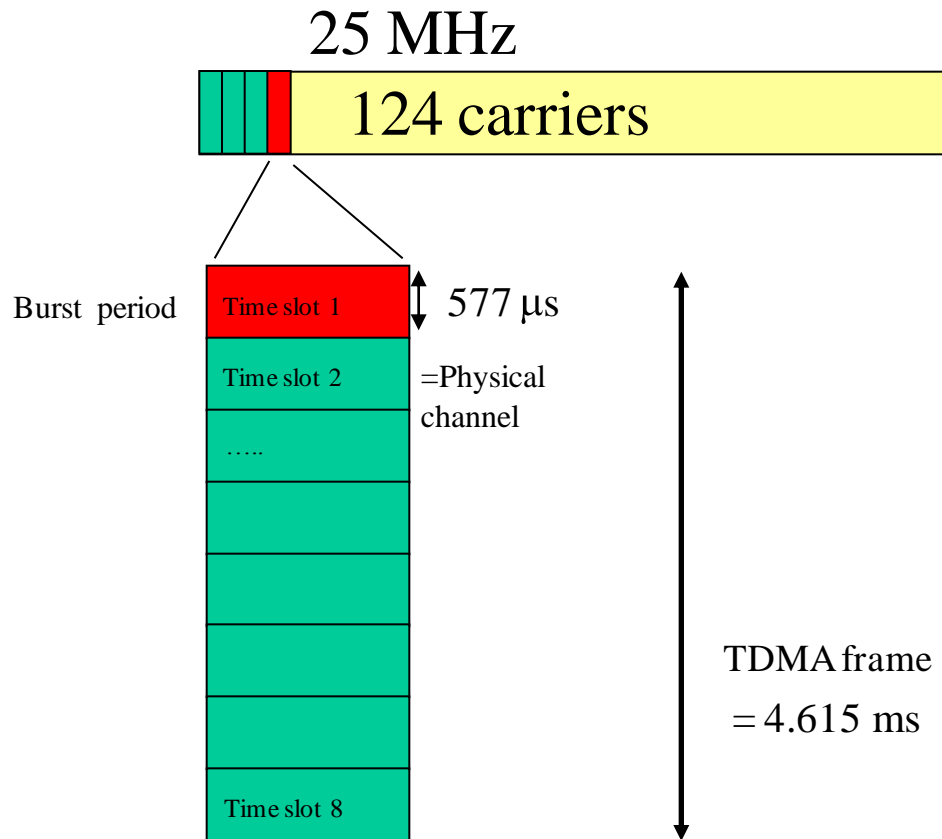
- 1710 - 1885 MHz: Uplink
- 1805 - 1880 MHz: Downlink

|                              |                |
|------------------------------|----------------|
| ❑ Carrier bandwidth:         | 200 kHz        |
| ❑ Channels / carrier:        | 8              |
| ❑ Multiple access:           | TDMA / FDMA    |
| ❑ Duplex:                    | FDD            |
| ❑ Gross bit rate pr carrier: | 270,833 kbit/s |
| ❑ Modulation:                | GMSK           |
| ❑ Spectrum efficiency:       | 1.35 bps/Hz    |

# Channels in GSM900



# GSM Channel structure



- ❑ Logical channels built up of physical channels
  - Control channels
  - Traffic channels
  
- ❑ Logical channels divided between:
  - Dedicated channels
  - Common channels

# GSM frequency bands (examples)

[www.rejinpaul.com](http://www.rejinpaul.com)

| Type                             | Channels  | Uplink [MHz]                  | Downlink [MHz]                |
|----------------------------------|---|-------------------------------|-------------------------------|
| GSM 850                          | 128-251   | 824-849                       | 869-894                       |
| GSM 900<br>classical<br>extended | 0-124, 955-1023<br>124 channels<br>+49 channels | 876-915<br>890-915<br>880-915 | 921-960<br>935-960<br>925-960 |
| GSM 1800                         | 512-885   | 1710-1785                     | 1805-1880                     |
| GSM 1900                         | 512-810   | 1850-1910                     | 1930-1990                     |
| GSM-R<br>exclusive               | 955-1024, 0-124<br>69 channels                  | 876-915<br>876-880            | 921-960<br>921-925            |

- Additionally: GSM 400 (also named GSM 450 or GSM 480 at 450-458/460-468 or 479-486/489-496 MHz)
- Please note: frequency ranges may vary depending on the country!
- Channels at the lower/upper edge of a frequency band are typically not used

Get useful study materials from [www.rejinpaul.com](http://www.rejinpaul.com)

# Base Transceiver Station and Base Station Controller

- ❑ Tasks of a BSS are distributed over BSC and BTS
- ❑ BTS comprises radio specific functions
- ❑ BSC is the switching center for radio channels

| Functions                                  | BTS | BSC |
|--|-----|-----|
| Management of radio channels               |     | X   |
| Frequency hopping (FH)                     | X   | X   |
| Management of terrestrial channels         |     | X   |
| Mapping of terrestrial onto radio channels |     | X   |
| Channel coding and decoding                | X   |     |
| Rate adaptation                            | X   |     |
| Encryption and decryption                  | X   | X   |
| Paging                                     | X   | X   |
| Uplink signal measurements                 | X   |     |
| Traffic measurement                        |     | X   |
| Authentication                             |     | X   |
| Location registry, location update         |     | X   |
| Handover management                        |     | X   |

# Network and switching subsystem

- ❑ NSS is the main component of the public mobile network GSM
  - switching, mobility management, interconnection to other networks, system control
- ❑ Components
  - Mobile Services Switching Center (MSC)  
controls all connections via a separated network to/from a mobile terminal within the domain of the MSC - several BSC can belong to a MSC
  - Databases (important: scalability, high capacity, low delay)
    - Home Location Register (HLR)  
central master database containing user data, permanent and semi-permanent data of all subscribers assigned to the HLR (one provider can have several HLRs)
    - Visitor Location Register (VLR)  
local database for a subset of user data, including data about all user currently in the domain of the VLR

# Mobile Services Switching Center

- ❑ The MSC (mobile services switching center) plays a central role in GSM
  - switching functions
  - additional functions for mobility support
  - management of network resources
  - interworking functions via Gateway MSC (GMSC)
  - integration of several databases
- ❑ Functions of a MSC
  - specific functions for paging and call forwarding
  - termination of SS7 (signaling system no. 7)
  - mobility specific signaling
  - location registration and forwarding of location information
  - provision of new services (fax, data calls)
  - support of short message service (SMS)
  - generation and forwarding of accounting and billing information

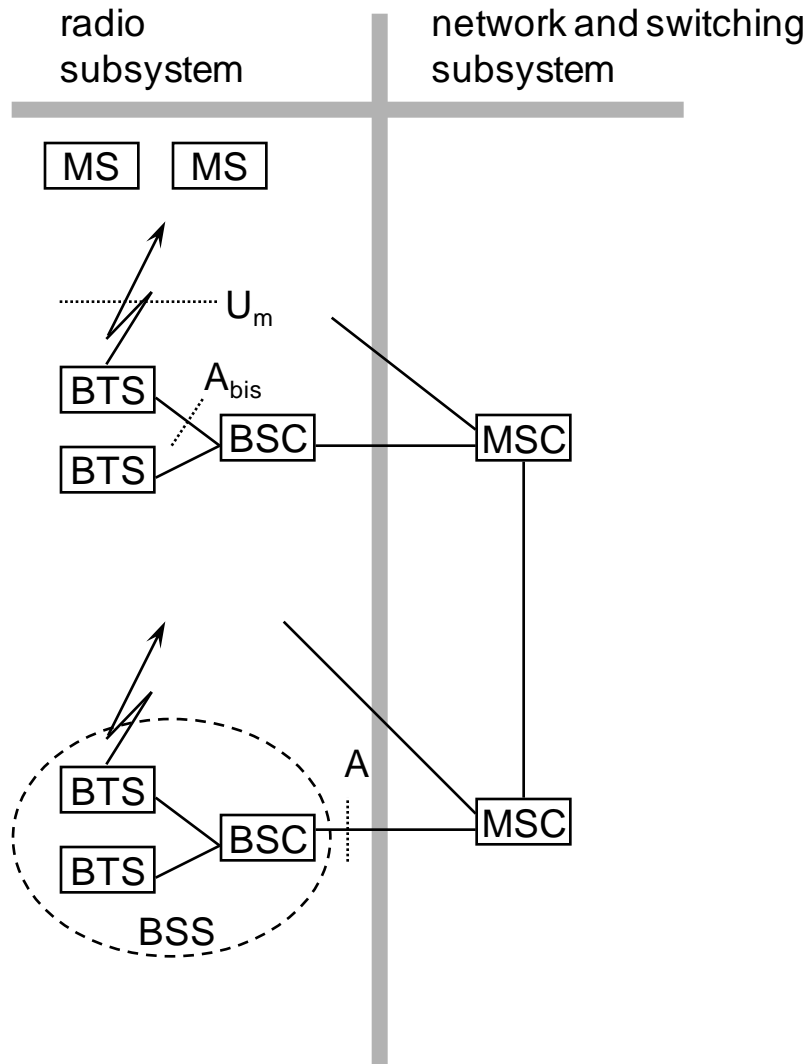
# Operation subsystem

- ❑ The OSS (Operation Subsystem) enables centralized operation, management, and maintenance of all GSM subsystems
- ❑ Components
  - Authentication Center (AUC)
    - generates user specific authentication parameters on request of a VLR
    - authentication parameters used for authentication of mobile terminals and encryption of user data on the air interface within the GSM system
  - Equipment Identity Register (EIR)
    - registers GSM mobile stations and user rights
    - stolen or malfunctioning mobile stations can be locked and sometimes even localized
  - Operation and Maintenance Center (OMC)
    - different control capabilities for the radio subsystem and the network subsystem



# Radio Interfaces

# System architecture: radio subsystem



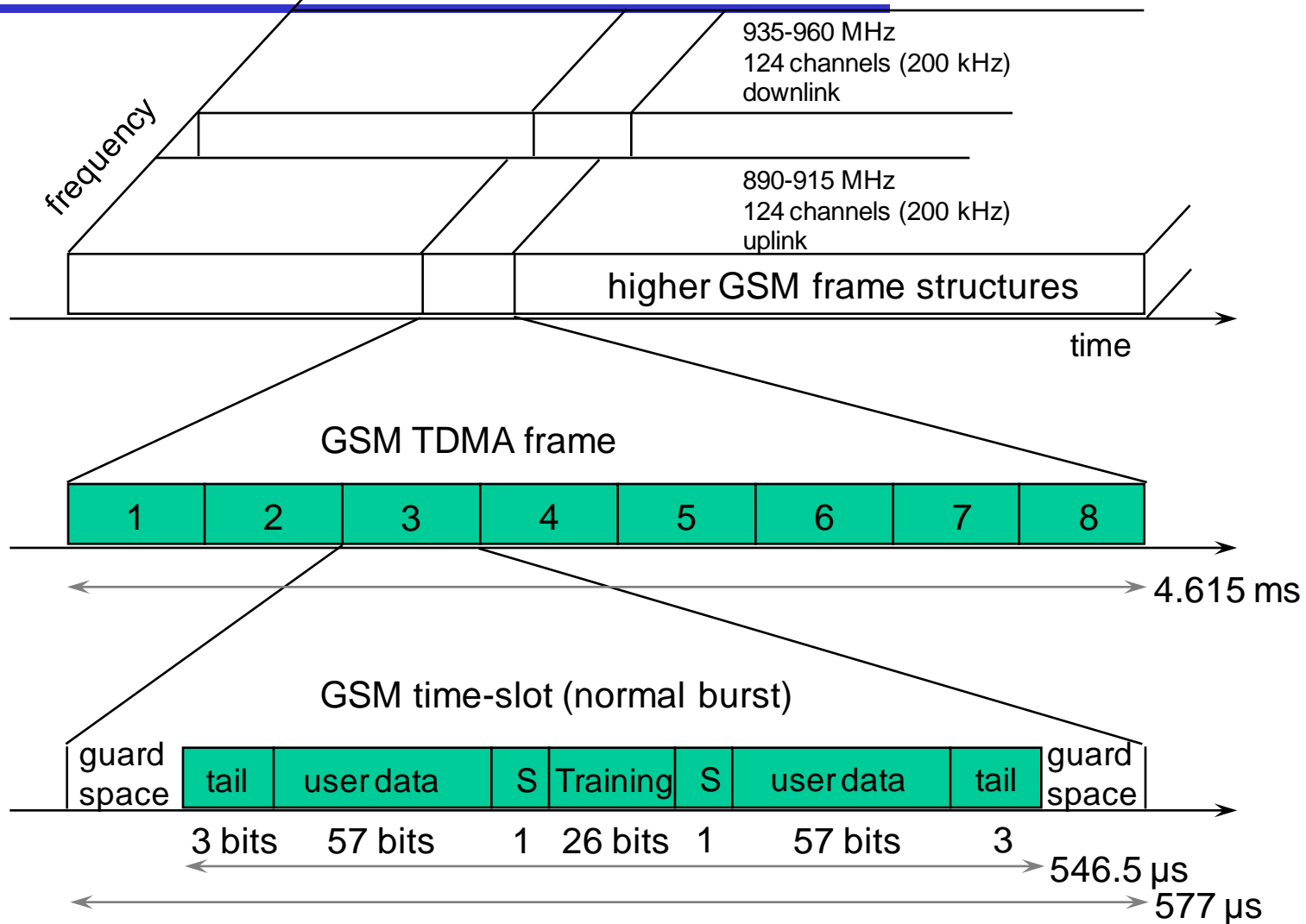
## Components

- **MS** (Mobile Station)
- **BSS** (Base Station Subsystem): consisting of
  - **BTS** (Base Transceiver Station): sender and receiver
  - **BSC** (Base Station Controller): controlling several transceivers

## Interfaces

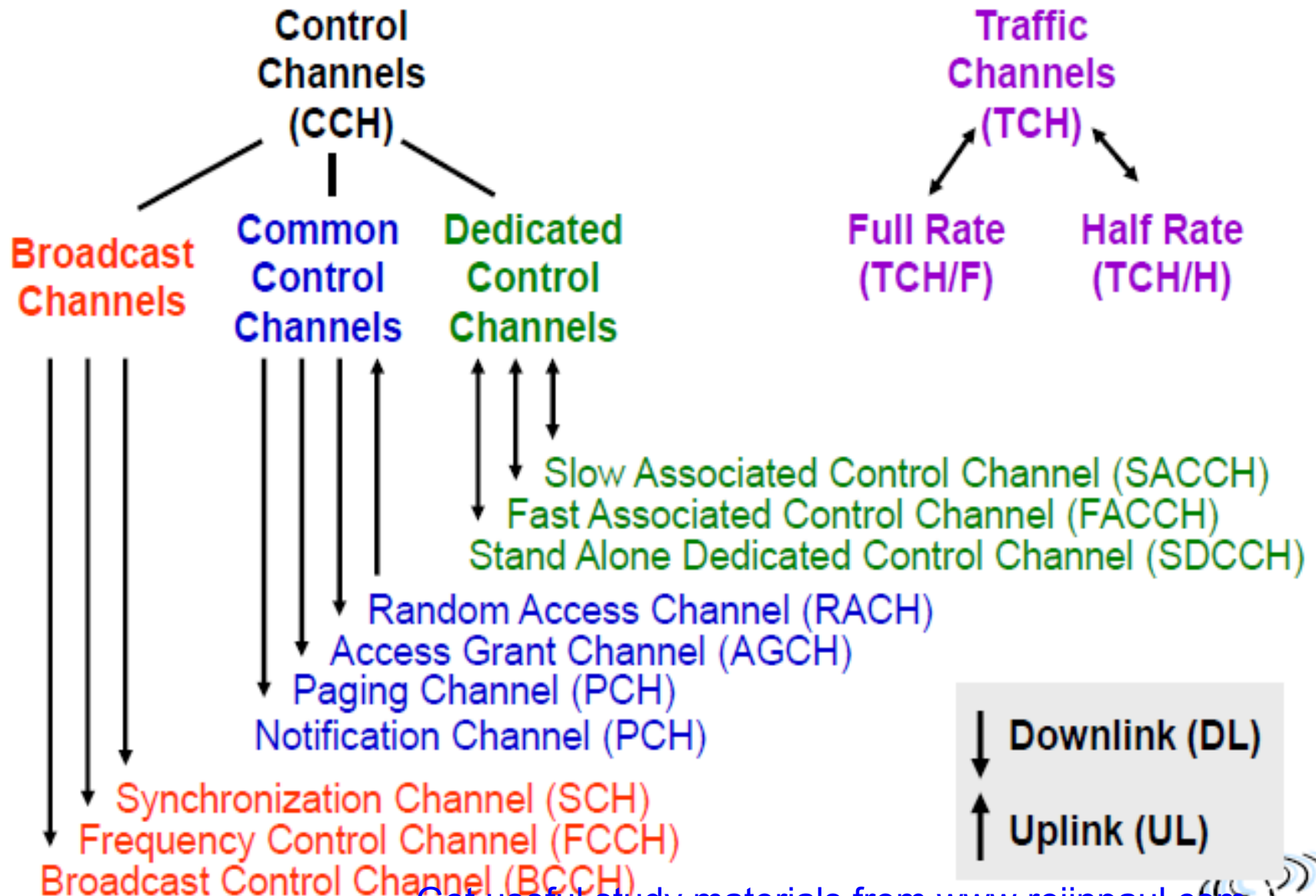
- $U_m$ : radio interface
- $A_{bis}$ : standardized, open interface with 16 kbit/s user channels
- $A$ : standardized, open interface with 64 kbit/s user channels

# GSM - TDMA/FDMA

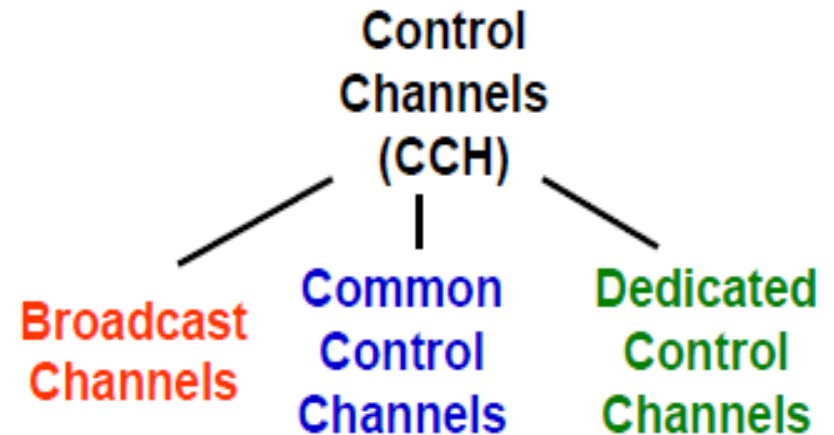


## Five Different Types of Burst

- ❑ Normal Burst - Traffic and Control Payload
- ❑ Frequency Correction Burst - All Zeroes Sequence
- ❑ Synchronization Burst - Special Fixed Sequence
- ❑ Access Burst - Extended Guard Period of 68.25 Bits (252  $\mu$ s)
- ❑ Dummy Burst



Broadcast Channels are used for synchronisation purposes and broadcasting of cell-specific information in the downlink from BTS to MS



## Frequency Correction Channel (FCCH)

carries information for frequency correction of the MS

## Synchronization Channel (SCH)

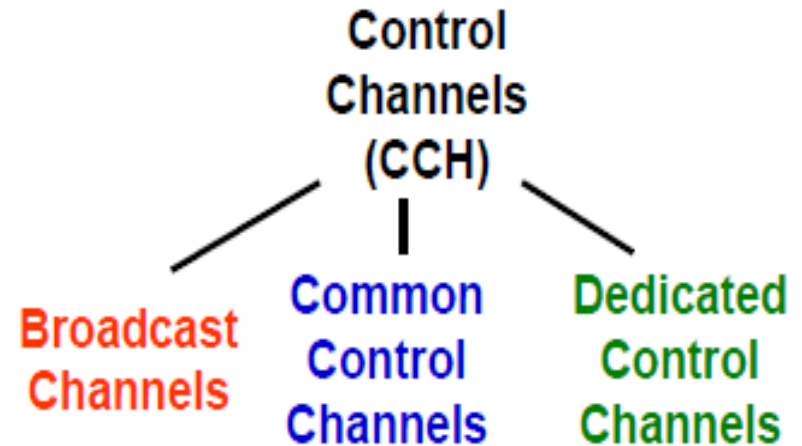
carries information for frame synchronization of the MS (e.g. TDMA frame number FN) and for identification of the BTS (e.g. Base Station Identity Code BSIC)

## Broadcast Control Channel (BCCH)

broadcasts general information on the BTS as well as cell-specific information like control channel organisation, frequency hopping sequences, cell identification, etc.



Common Control Channels  
are point-to-multipoint  
channels used mainly for  
access control



**Paging Channel (PCH)** - downlink only

used by the BTS for paging and localizing the MS

**Random Access Channel (RACH)** - uplink only

used by any MS to request allocation of a signalling channel (SDCCH). A slotted Aloha protocol is used, so collisions among concurring MS are quite possible.

**Access Grant Channel (AGCH)** - downlink only

used to allocate a SDCCH or directly a TCH

**Notification Channel (NCH)** - downlink only

used to notify MS of voice group and voice broadcast calls (ASCI feature)





**Broadcast  
Channels**

**Common  
Control  
Channels**

**Dedicated  
Control  
Channels**

Dedicated Control Channels are bidirectional point-to-point channels, that allow authentication, signalling, handover and the exchange of measurement values.

## Stand Alone Dedicated Control Channel (SDCCH)

used for call setup (authentication, signalling, assignment of actual TCH), localisation updates and **SMS**

## Slow Associated Control Channel (SACCH)

is always coupled with a SDCCH or TCH and is used for the exchange of measurement values and control parameters

- Downlink : Control of MS Power Level and MS Timing Advance
- Uplink : Measurement reports (MS reception levels) used by the BTS for its handover-decisions

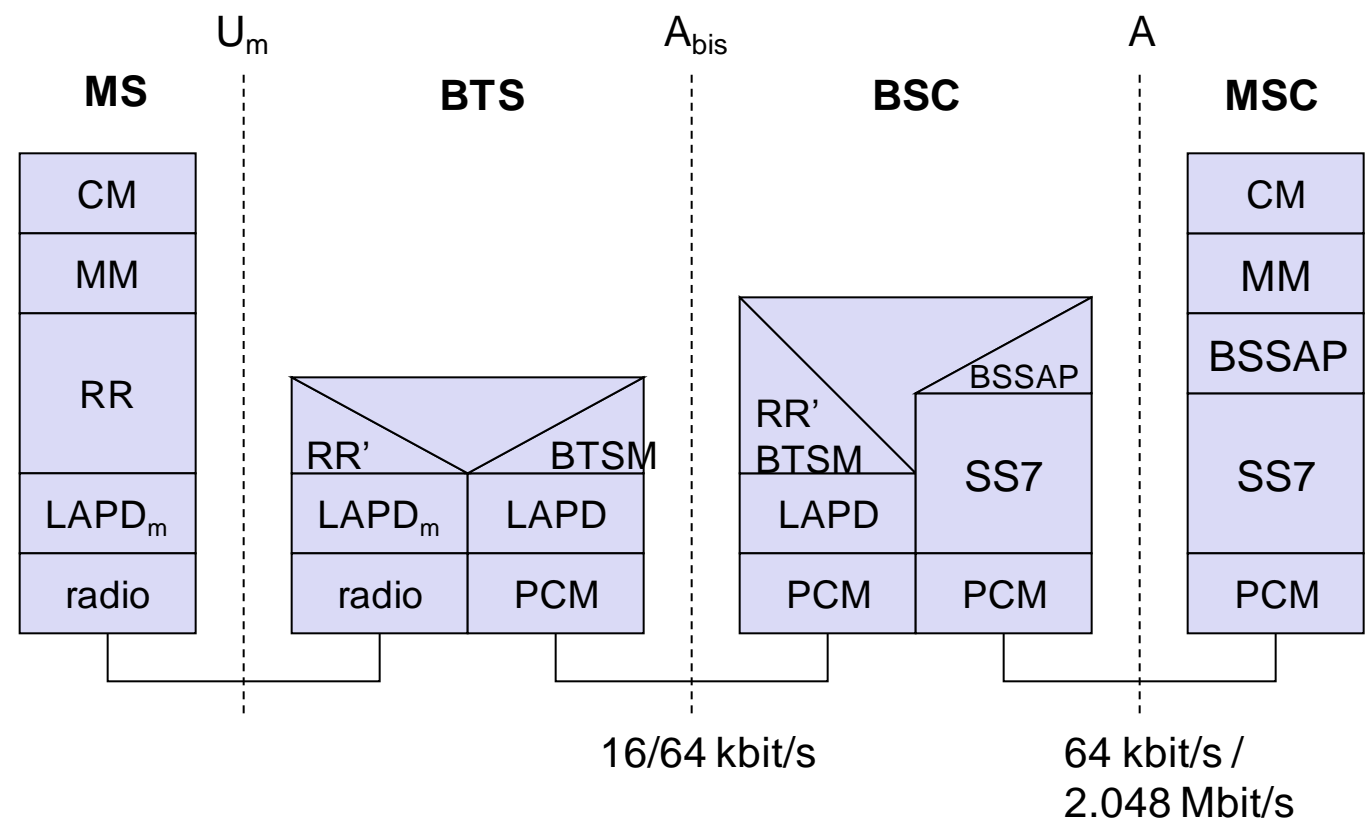
## Fast Associated Control Channel (FACCH)

is activated in case of increased signalling demand e.g. during handover. Bandwidth is stolen from associated TCH

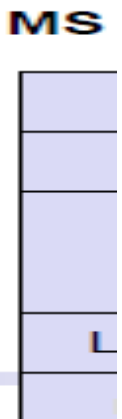




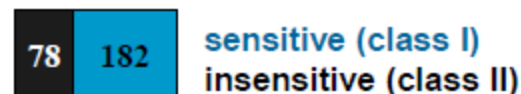
# GSM protocol layers for signaling



- creation of bursts – 5 different formats
- multiplexing of bursts into TDMA frames
- synchronisation with the BTS (see next slide)
- detection of idle channels
- measurements of channel quality at downlink
- the physical layer at Um uses GMSK modulation
- performs encryption/decryption of data



Channel coding and error detection/correction!

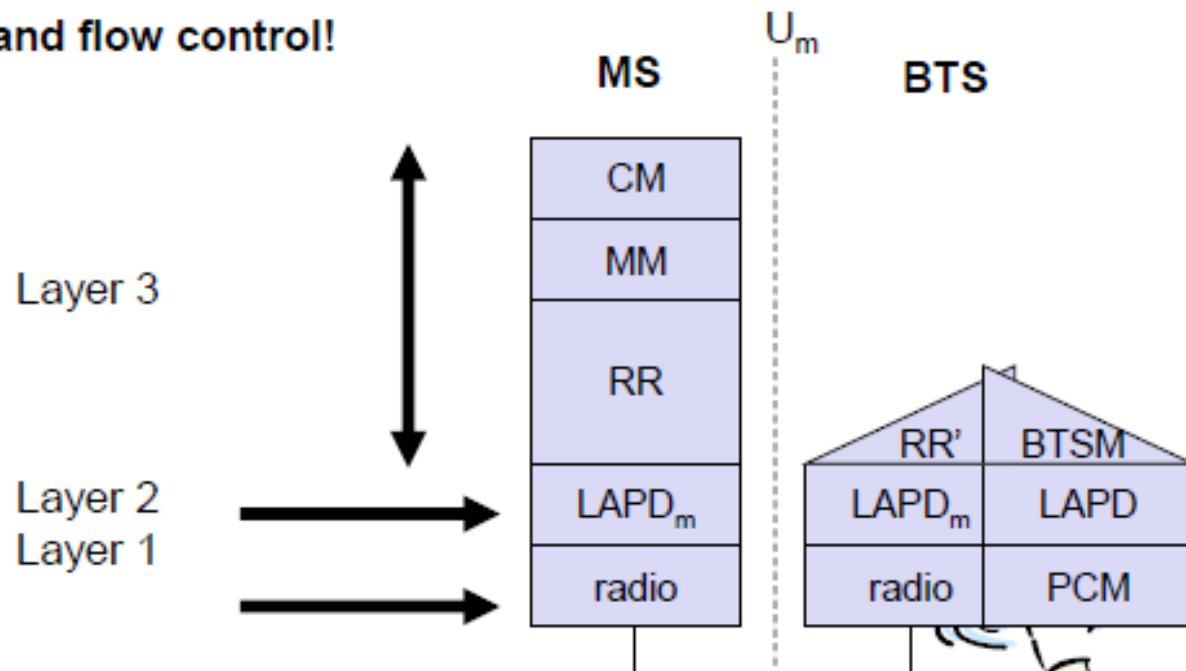


# Layer 2 (data link) - LAPDm [www.rejinpaul.com](http://www.rejinpaul.com)

It is said to be a lightweight LAPD protocol as it does not handle error correction/detection.

It handles:

- segmentation and reassembly of data and acknowledges/unacknowledged data transfer
- re-sequencing of data frames and flow control!



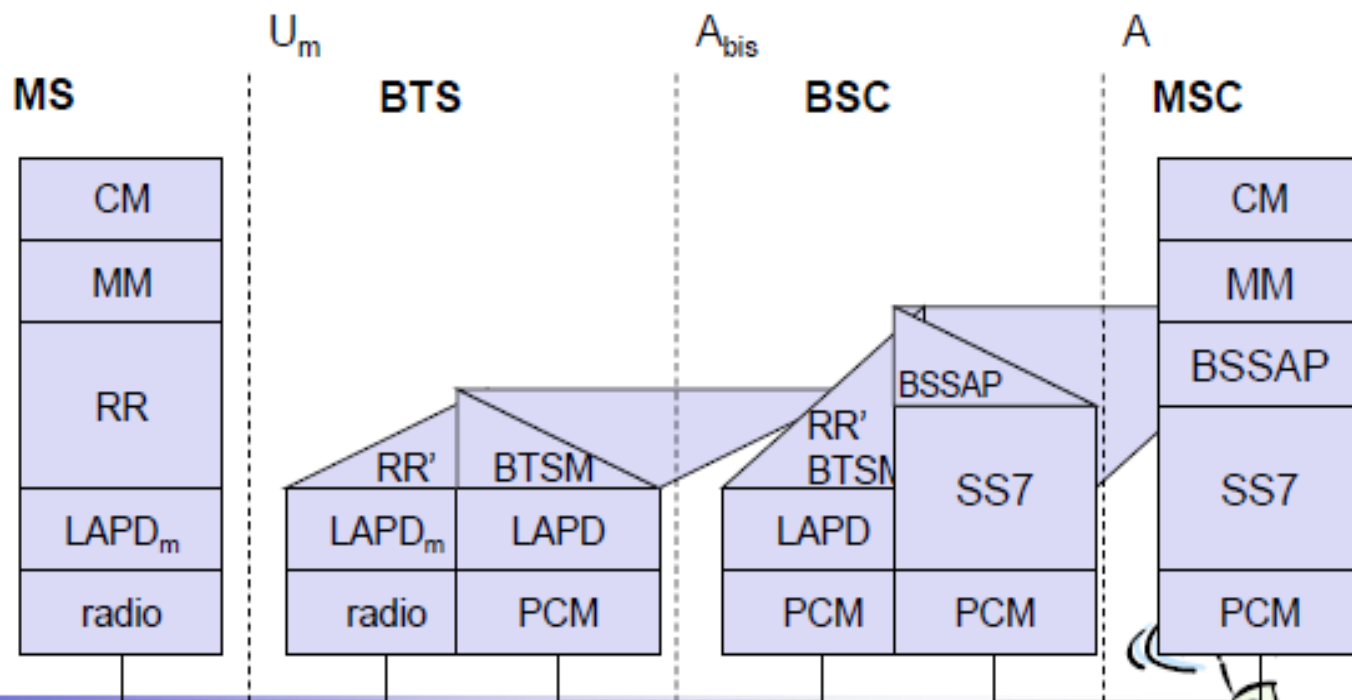
# The network layer in GSM comprises several sublayers!

[www.rejinpaul.com](http://www.rejinpaul.com)

The lowest sublayer is the **Radio Resource Management (RR)**!

Just a part of it is implemented in the BTS, the remainder in the BSC!

Setup,  
maintenance and  
release  
of radio channels



Get useful study materials from [www.rejinpaul.com](http://www.rejinpaul.com)

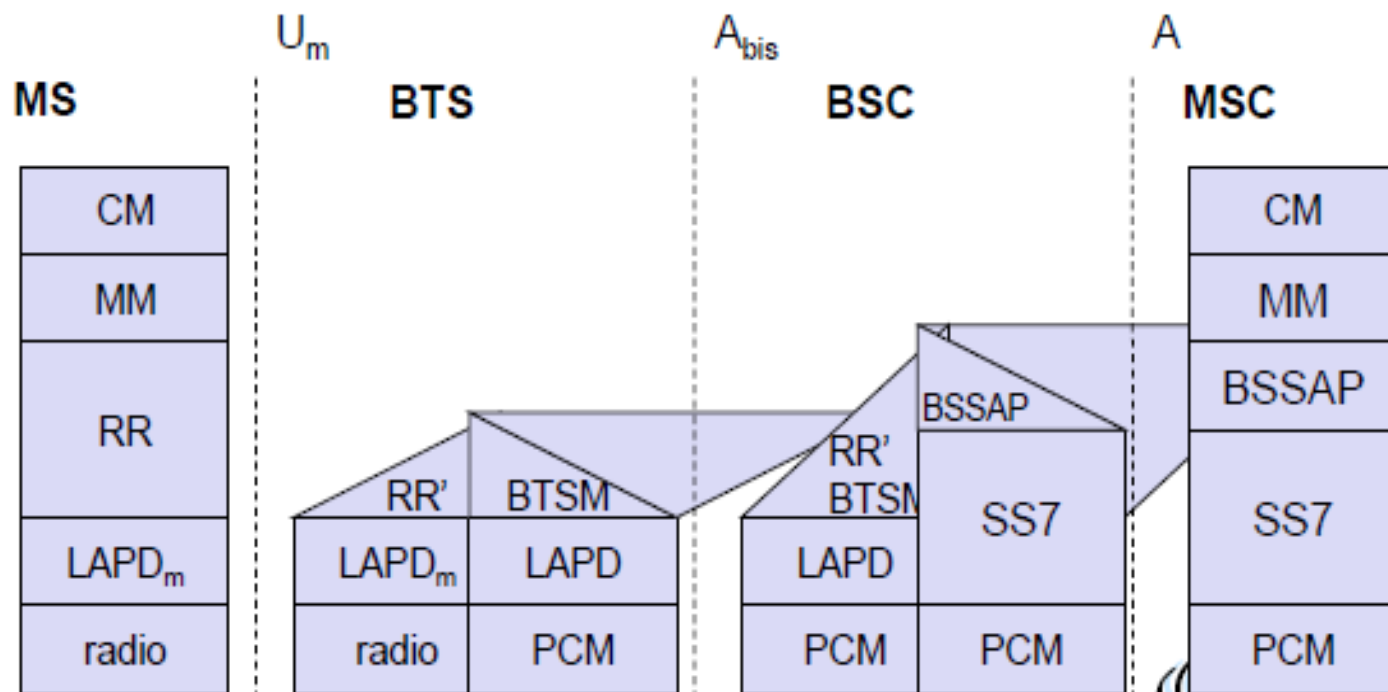
# The network layer in GSM comprises several sublayers!

[www.rejinpaul.com](http://www.rejinpaul.com)

**Mobility Management (MM)** contains functions for

registration  
authentication  
location update

It also provides a **temporary mobile subscriber identity (TMSI)** that replaces the **international mobile subscriber identity (IMSI)** which hides the real identity of an MS user over the air interface.



Get useful study materials from [www.rejinpaul.com](http://www.rejinpaul.com)

16/64 kbit/s

64 kbit/s

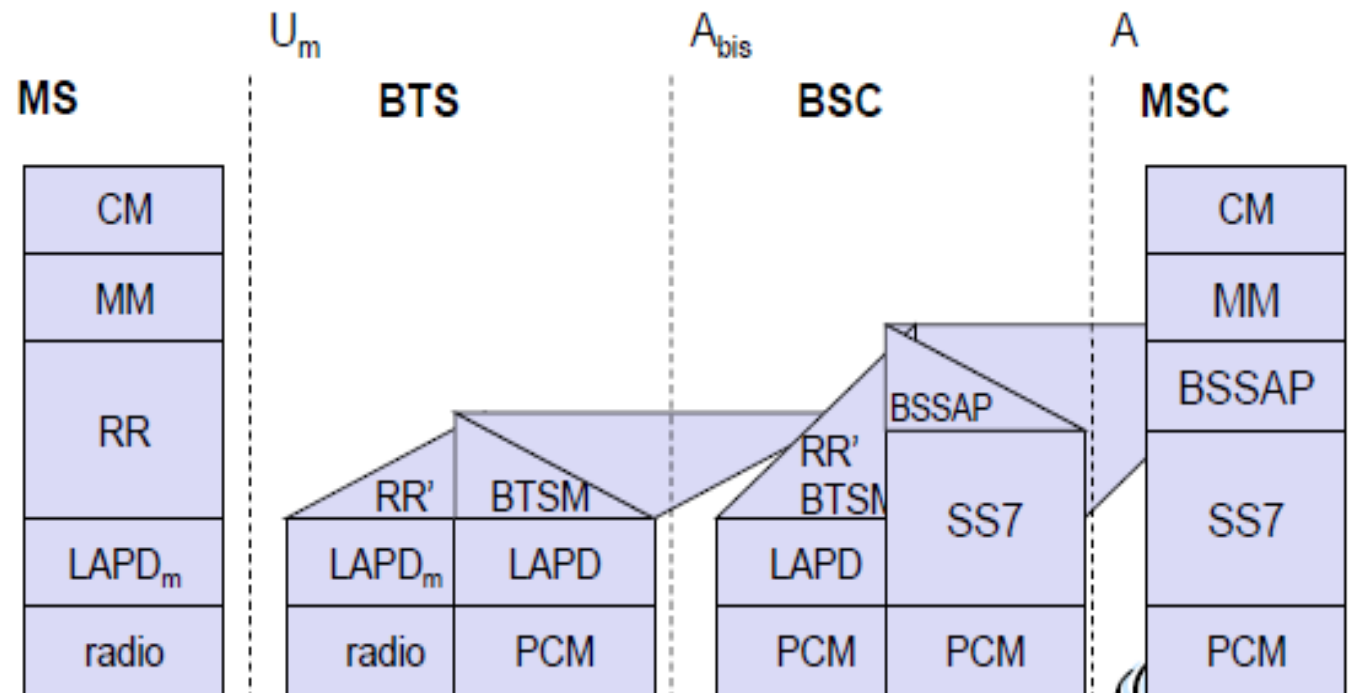
# The network layer in GSM comprises several sublayers!

**Call Management (CM)** contains functions for:

call control (CC): point-to point connection between two terminals  
 call establishment, call clearing, etc.

short message service (SMS): using control channels SDCCH and SACCH

supplementary services (SS): user identification, forwarding, etc.

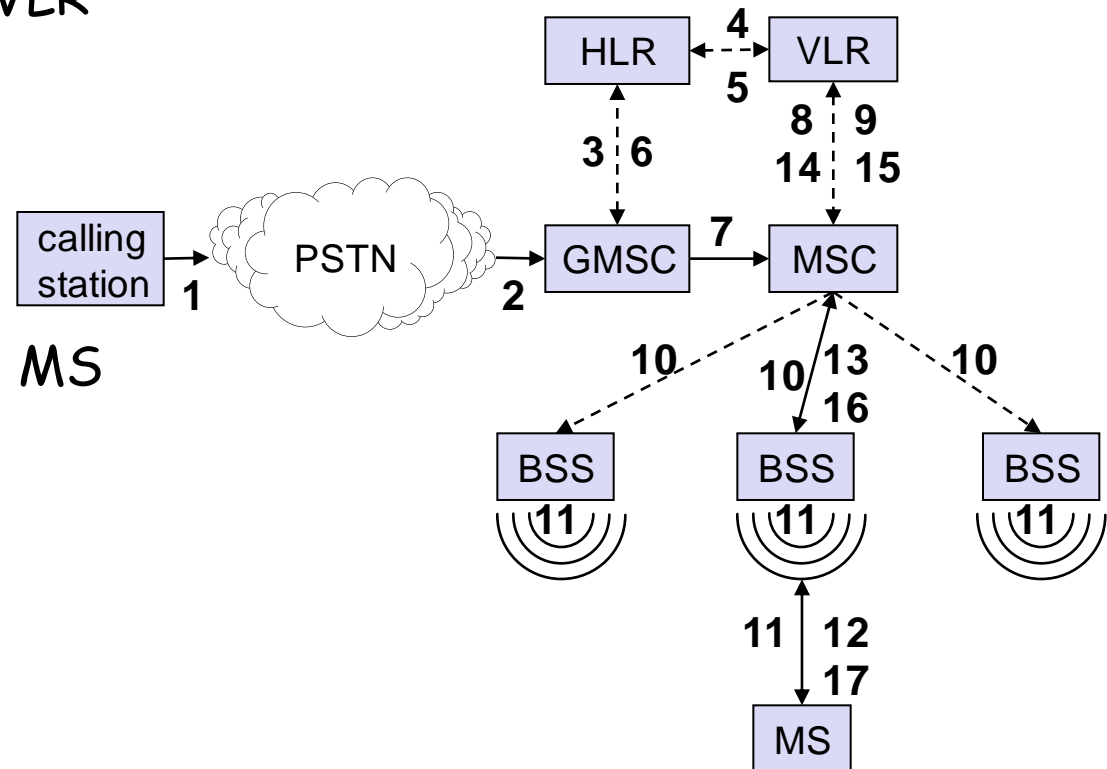


# Localization and Calling

- ❑ Roaming
- ❑ Mobile station international ISDN number
  - ❑ Country code, National Destination code and Subscriber number
- ❑ International mobile subscriber identity
  - ❑ Mobile country code, mobile network code, mobile subscriber identification number
- ❑ Temporary mobile subscriber identity
- ❑ Mobile station roaming number
  - ❑ Visitor country code, visitor national destination code.

# Mobile Terminated Call

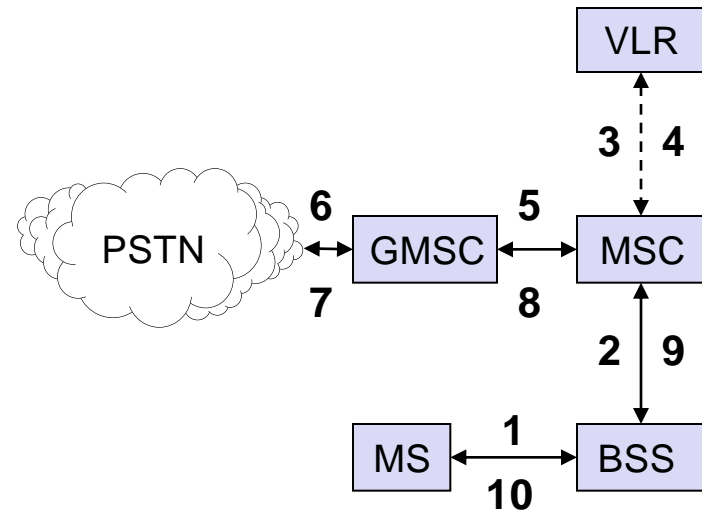
- ❑ 1: calling a *GSM* subscriber
- ❑ 2: forwarding call to *GMSC*
- ❑ 3: signal call setup to *HLR*
- ❑ 4, 5: request *MSRN* from *VLR*
- ❑ 6: forward responsible *MSC* to *GMSC*
- ❑ 7: forward call to current *MSC*
- ❑ 8, 9: get current status of *MS*
- ❑ 10, 11: paging of *MS*
- ❑ 12, 13: *MS* answers
- ❑ 14, 15: security checks
- ❑ 16, 17: set up connection



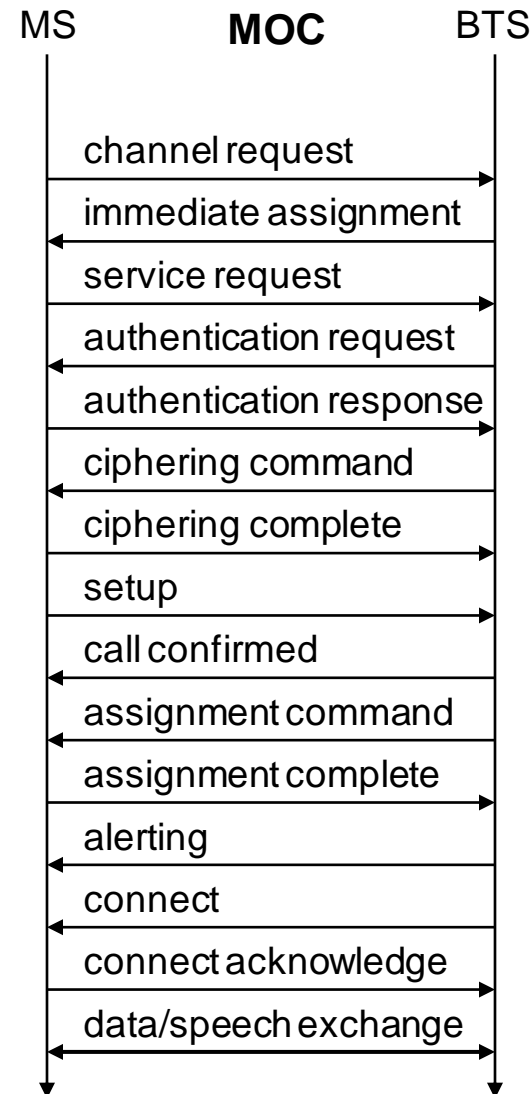
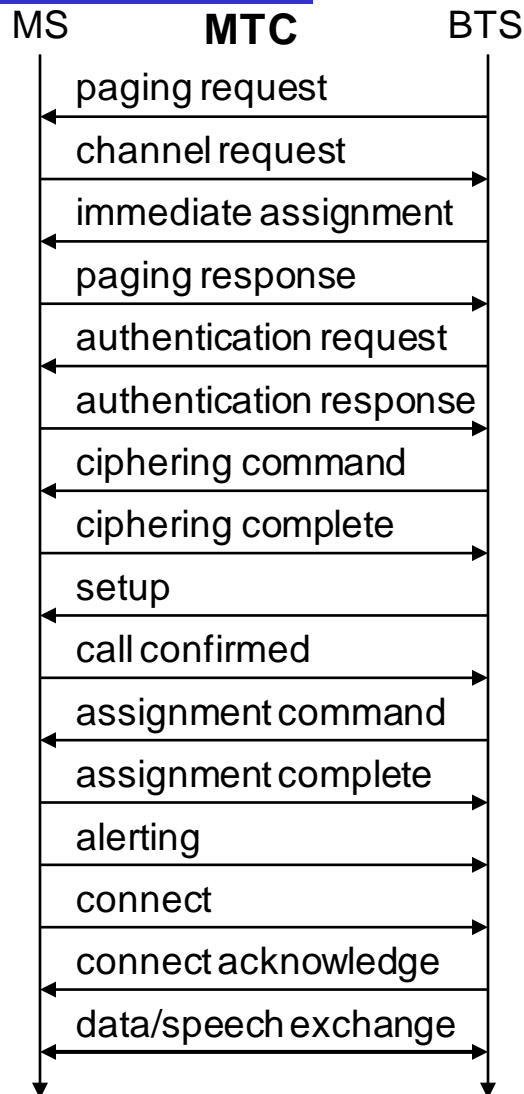


# Mobile Originated Call

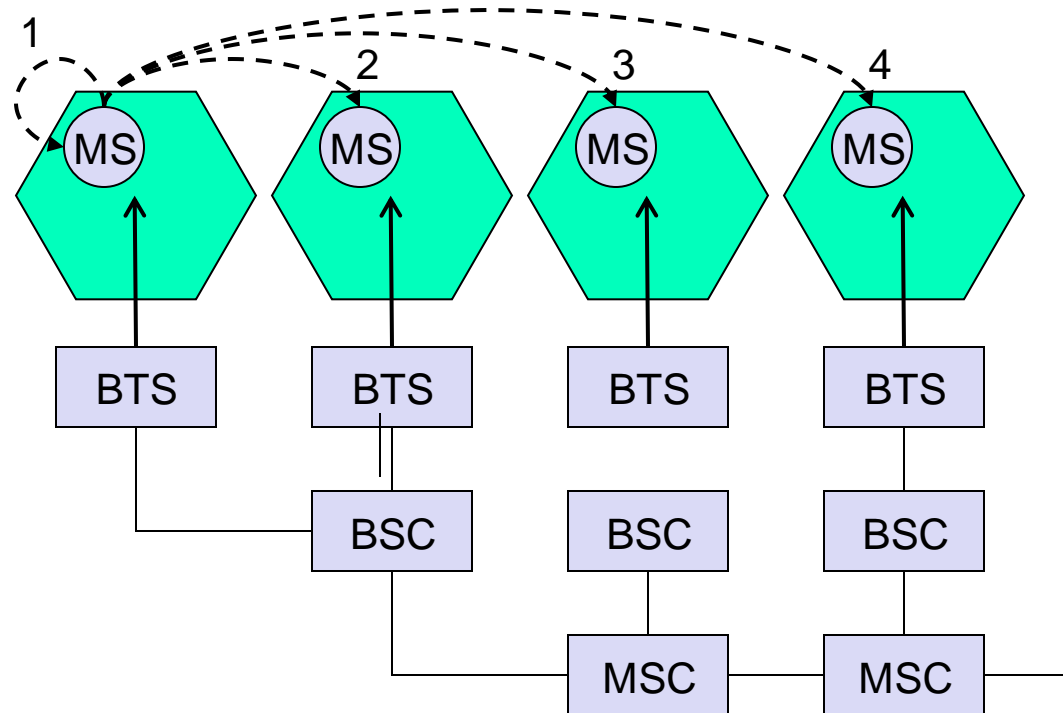
- ❑ 1, 2: connection request
- ❑ 3, 4: security check
- ❑ 5-8: check resources (free circuit)
- ❑ 9-10: set up call



# MTC/MOC

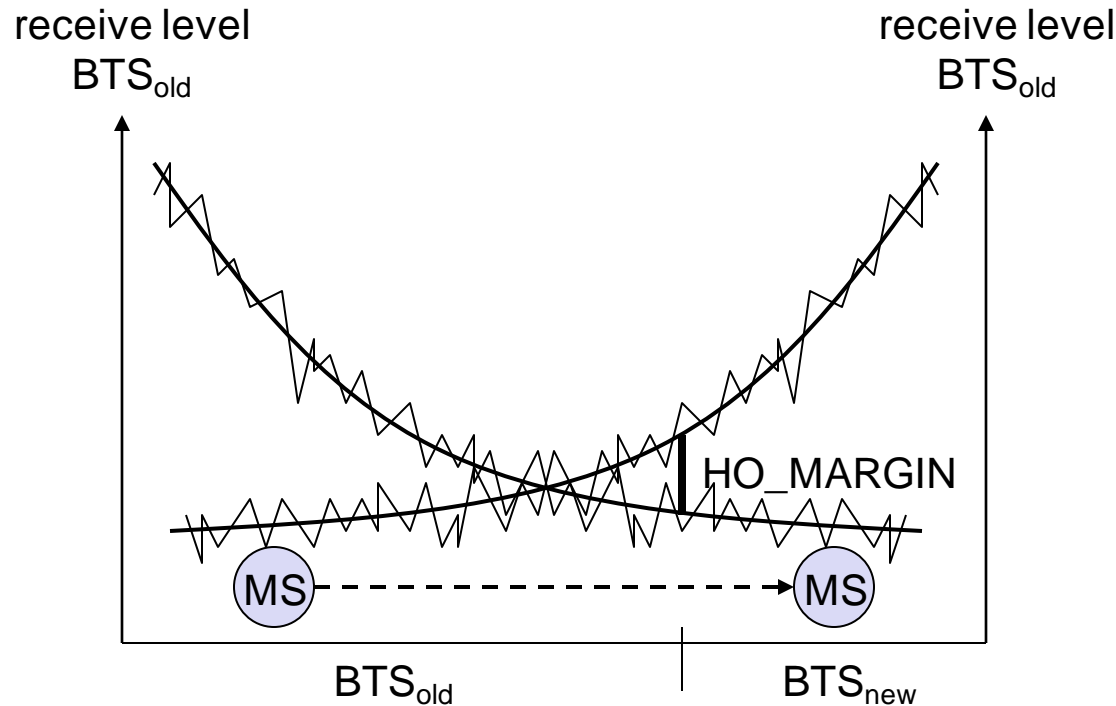


# 4 types of handover

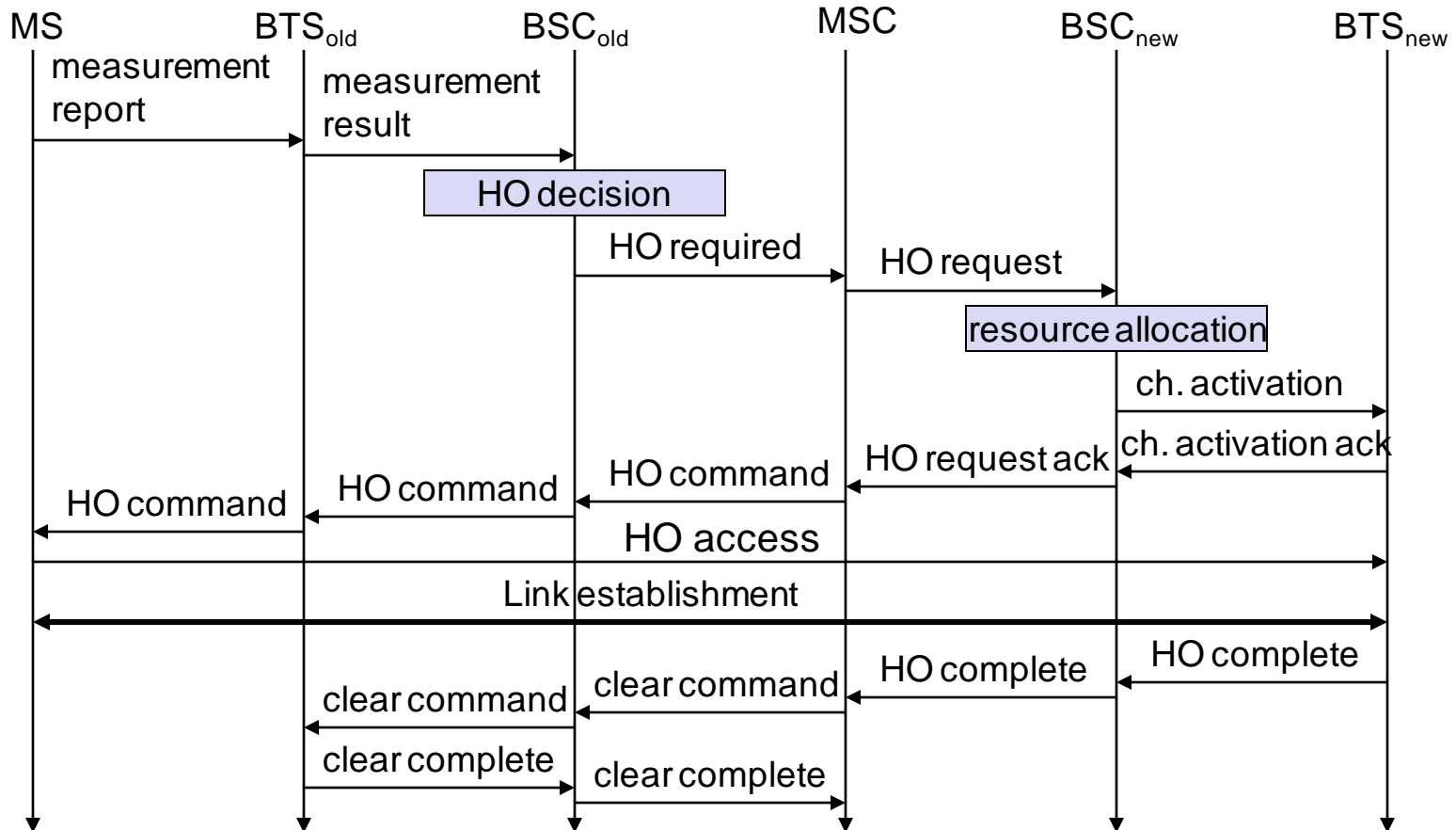


- ☐ Intracell handover
- ☐ Inter cell intra BSC handover
- ☐ Inter BSC intra MSC handover
- ☐ Inter MSC Handover

# Handover decision



# Handover procedure



# Security in GSM

## □ Security services

- access control/authentication
  - user  $\leftrightarrow$  SIM (Subscriber Identity Module): secret PIN (personal identification number)
  - SIM  $\leftrightarrow$  network: challenge response method
- confidentiality
  - voice and signaling encrypted on the wireless link (after successful authentication)
- anonymity
  - temporary identity TMSI (Temporary Mobile Subscriber Identity)
  - newly assigned at each new location update (LUP)
  - encrypted transmission

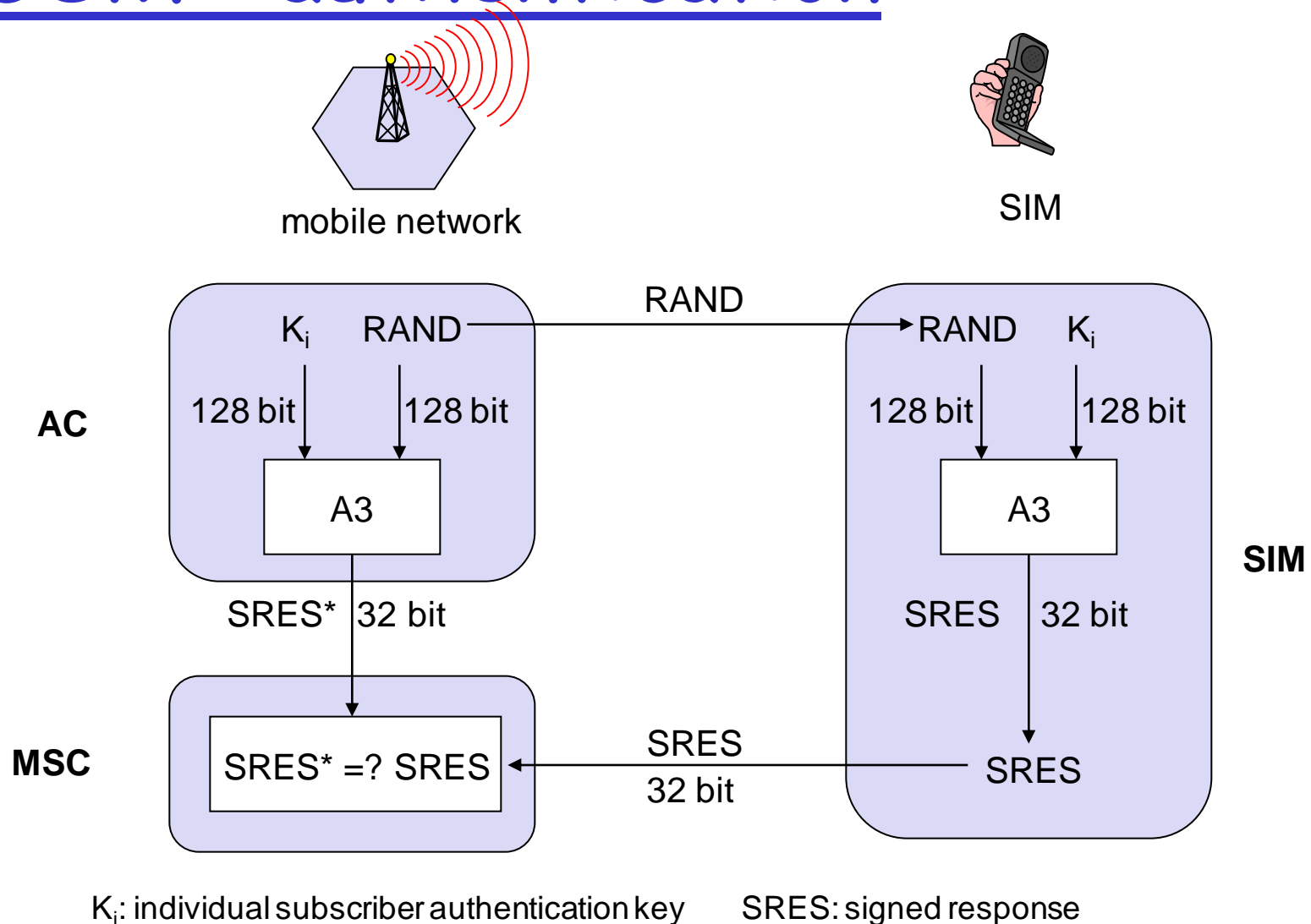
## □ 3 algorithms specified in GSM

- A3 for authentication ("secret", open interface)
- A5 for encryption (standardized)
- A8 for key generation ("secret", open interface)

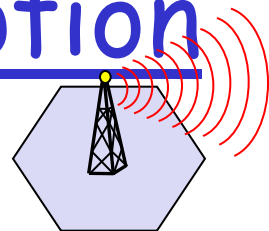
"secret":

- A3 and A8 available via the Internet
- network providers can use stronger mechanisms

# GSM - authentication



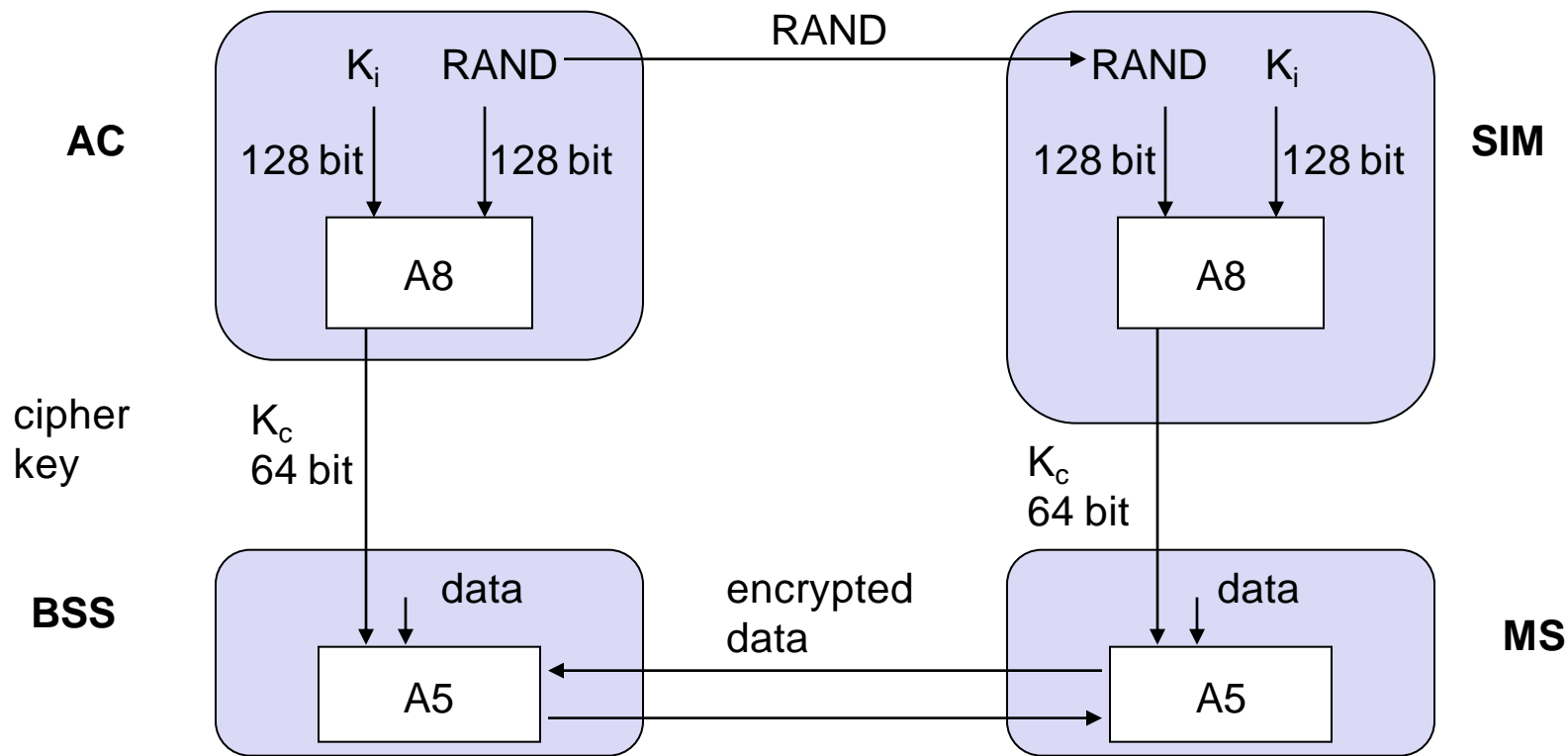
# GSM - key generation and encryption



mobile network (BTS)



MS with SIM





# Data services in GSM I

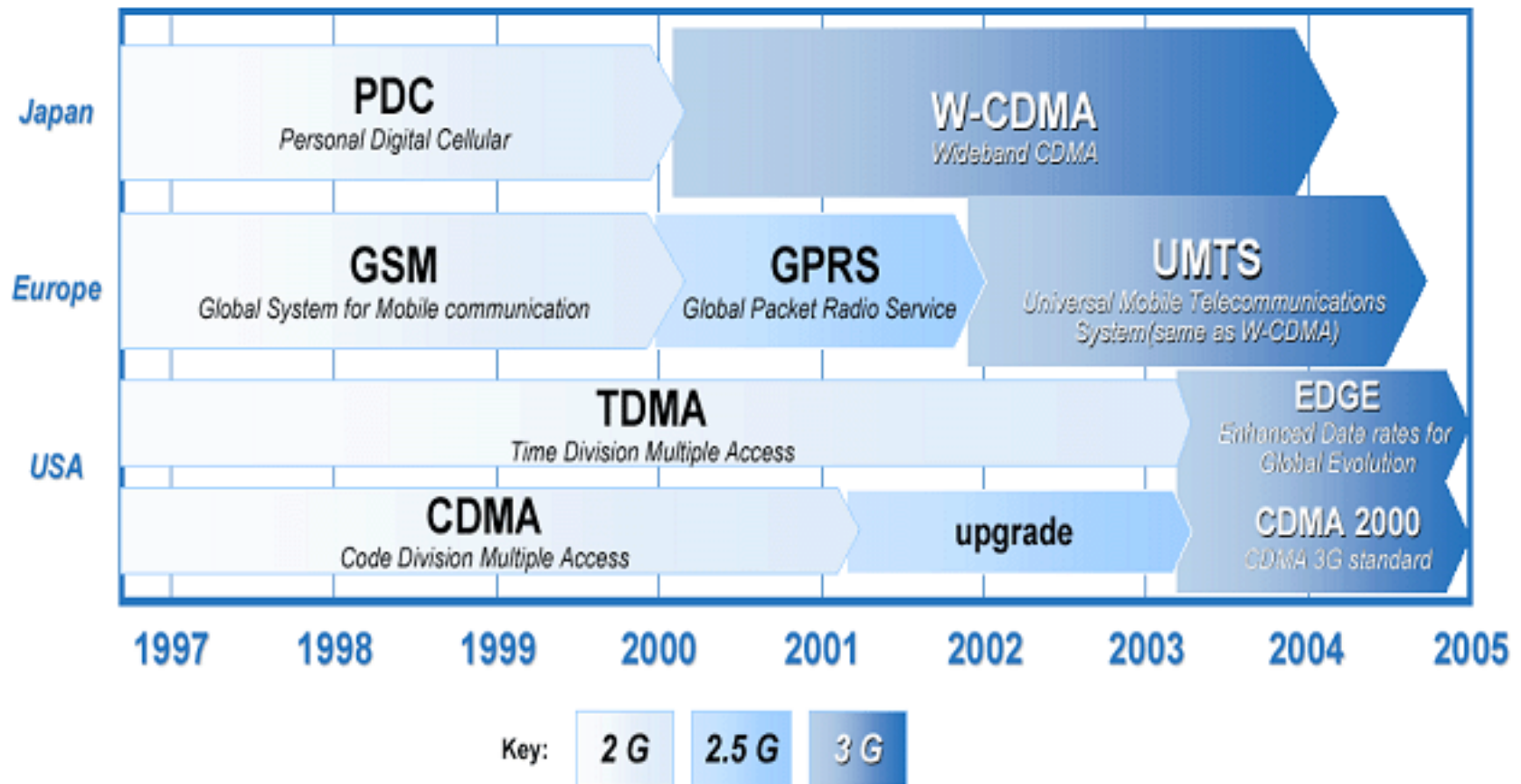
- ❑ Data transmission standardized with only 9.6 kbit/s
  - advanced coding allows 14.4 kbit/s
  - not enough for Internet and multimedia applications
- ❑ HSCSD (High-Speed Circuit Switched Data)
  - mainly software update
  - bundling of several time-slots to get higher AIUR (Air Interface User Rate, e.g., 57.6 kbit/s using 4 slots @ 14.4)
  - advantage: ready to use, constant quality, simple
  - disadvantage: channels blocked for voice transmission

| AIUR [kbit/s] | TCH/F4.8 | TCH/F9.6 | TCH/F14.4 |
|---------------|----------|----------|-----------|
| 4.8           | 1        |          |           |
| 9.6           | 2        | 1        |           |
| 14.4          | 3        |          | 1         |
| 19.2          | 4        | 2        |           |
| 28.8          |          | 3        | 2         |
| 38.4          |          | 4        |           |
| 43.2          |          |          | 3         |
| 57.6          |          |          | 4         |

# Data services in GSM II

- ❑ GPRS (General Packet Radio Service)
  - packet switching
  - using free slots only if data packets ready to send (e.g., 50 kbit/s using 4 slots temporarily)
  - standardization 1998, introduction 2001
  - advantage: one step towards UMTS, more flexible
  - disadvantage: more investment needed (new hardware)
- ❑ GPRS network elements
  - GSN (GPRS Support Nodes): GGSN and SGSN
  - GGSN (Gateway GSN)
    - interworking unit between GPRS and PDN (Packet Data Network)
  - SGSN (Serving GSN)
    - supports the MS (location, billing, security)
  - GR (GPRS Register)
    - user addresses

# Timeline of Technology Evolution



# GPRS quality of service

| Reliability class | Lost SDU probability | Duplicate SDU probability | Out of sequence SDU probability | Corrupt SDU probability |
|-------------------|----------------------|---------------------------|---------------------------------|-------------------------|
| 1                 | $10^{-9}$            | $10^{-9}$                 | $10^{-9}$                       | $10^{-9}$               |
| 2                 | $10^{-4}$            | $10^{-5}$                 | $10^{-5}$                       | $10^{-6}$               |
| 3                 | $10^{-2}$            | $10^{-5}$                 | $10^{-5}$                       | $10^{-2}$               |

| Delay class | SDU size 128 byte |               | SDU size 1024 byte |               |
|-------------|-------------------|---------------|--------------------|---------------|
|             | mean              | 95 percentile | mean               | 95 percentile |
| 1           | < 0.5 s           | < 1.5 s       | < 2 s              | < 7 s         |
| 2           | < 5 s             | < 25 s        | < 15 s             | < 75 s        |
| 3           | < 50 s            | < 250 s       | < 75 s             | < 375 s       |
| 4           | unspecified       |               |                    |               |

# Examples for GPRS device classes

[www.rejinpaul.com](http://www.rejinpaul.com)

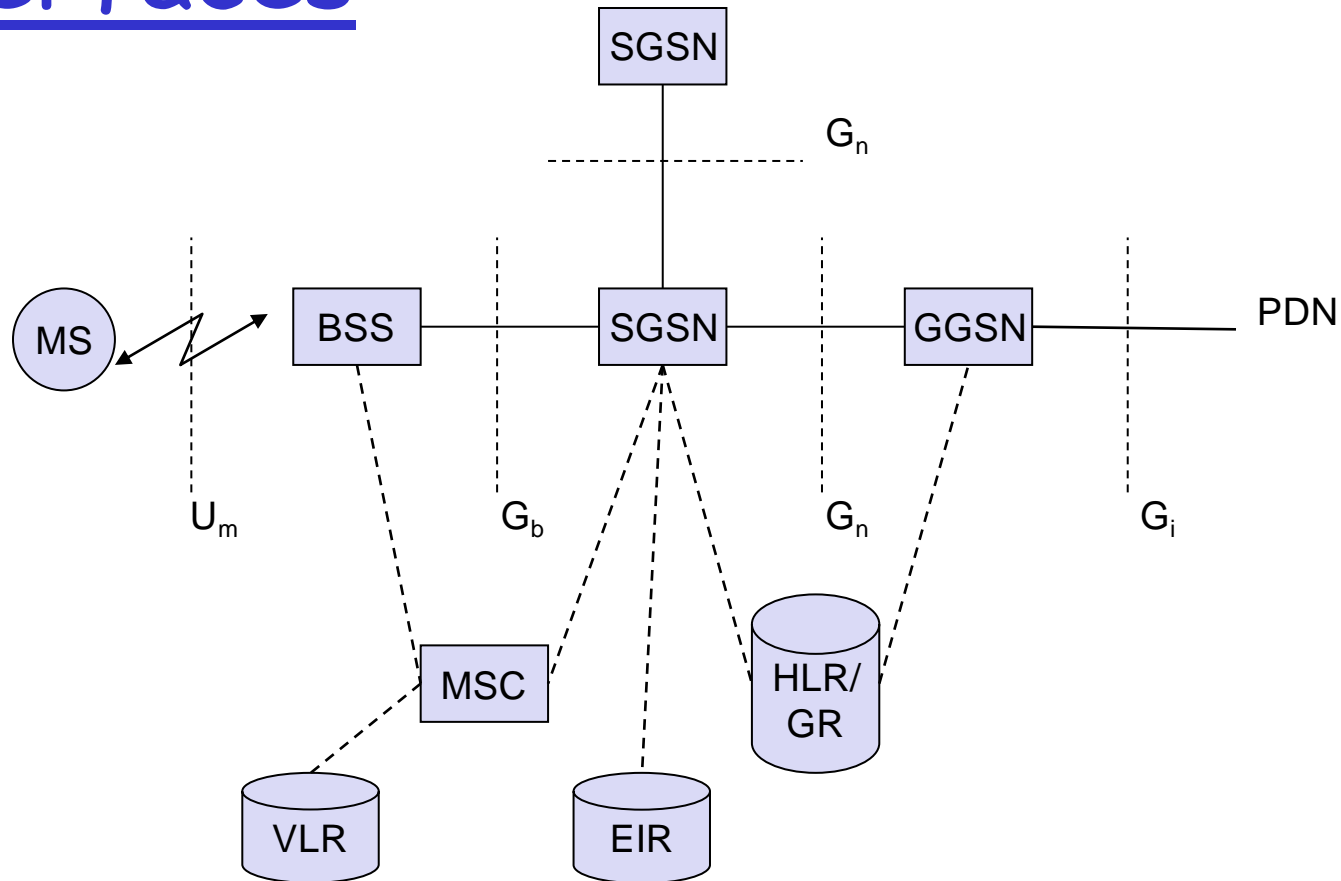
| <b>Class</b> | <b>Receiving slots</b> | <b>Sending slots</b> | <b>Maximum number of slots</b> |
|--------------|------------------------|----------------------|--------------------------------|
| 1            | 1                      | 1                    | 2                              |
| 2            | 2                      | 1                    | 3                              |
| 3            | 2                      | 2                    | 3                              |
| 5            | 2                      | 2                    | 4                              |
| 8            | 4                      | 1                    | 5                              |
| 10           | 4                      | 2                    | 5                              |
| 12           | 4                      | 4                    | 5                              |

# GPRS user data rates in kbit/s

| <b>Coding scheme</b> | <b>1 slot</b> | <b>2 slots</b> | <b>3 slots</b> | <b>4 slots</b> | <b>5 slots</b> | <b>6 slots</b> | <b>7 slots</b> | <b>8 slots</b> |
|----------------------|---------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|
| CS-1                 | 9.05          | 18.1           | 27.15          | 36.2           | 45.25          | 54.3           | 63.35          | 72.4           |
| CS-2                 | 13.4          | 26.8           | 40.2           | 53.6           | 67             | 80.4           | 93.8           | 107.2          |
| CS-3                 | 15.6          | 31.2           | 46.8           | 62.4           | 78             | 93.6           | 109.2          | 124.8          |
| CS-4                 | 21.4          | 42.8           | 64.2           | 85.6           | 107            | 128.4          | 149.8          | 171.2          |

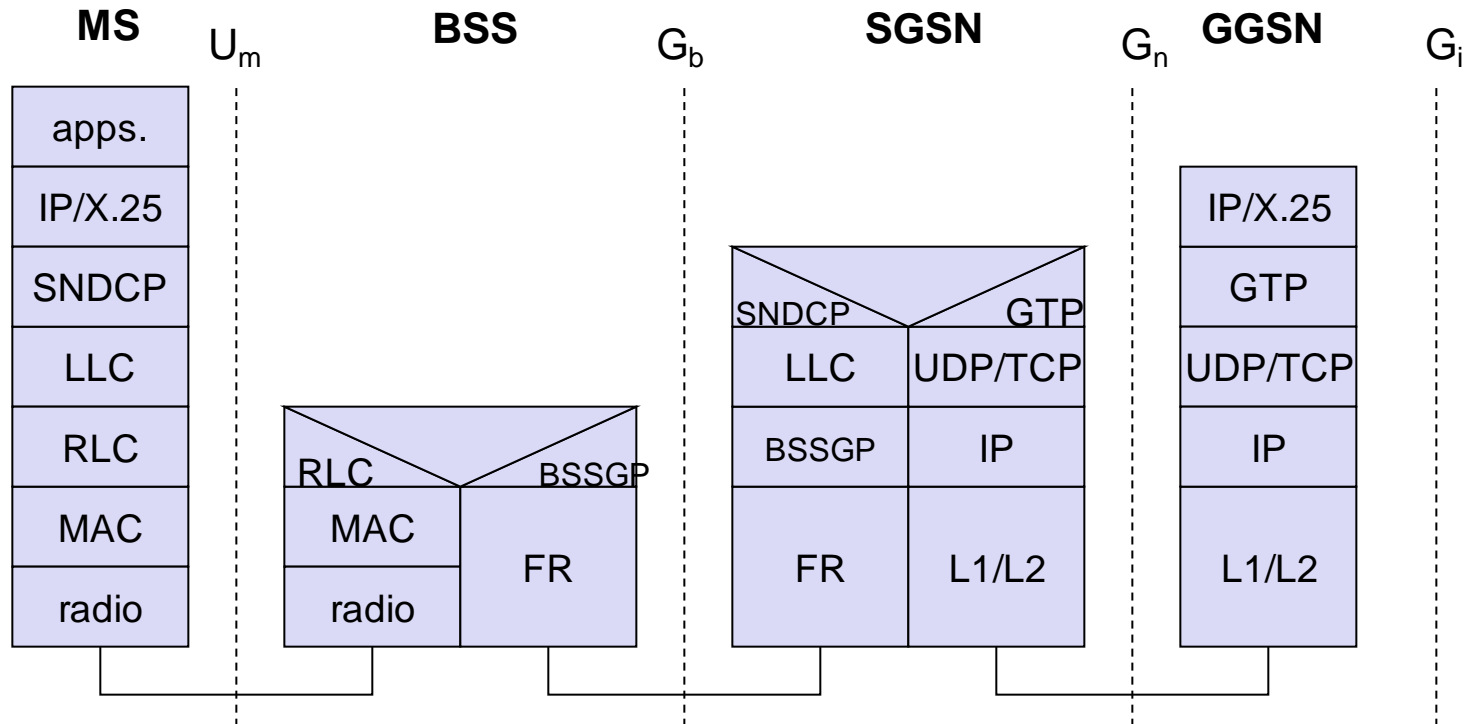
# GPRS architecture and interfaces

[www.rejinpaul.com](http://www.rejinpaul.com)



Get useful study materials from [www.rejinpaul.com](http://www.rejinpaul.com)

# GPRS protocol architecture

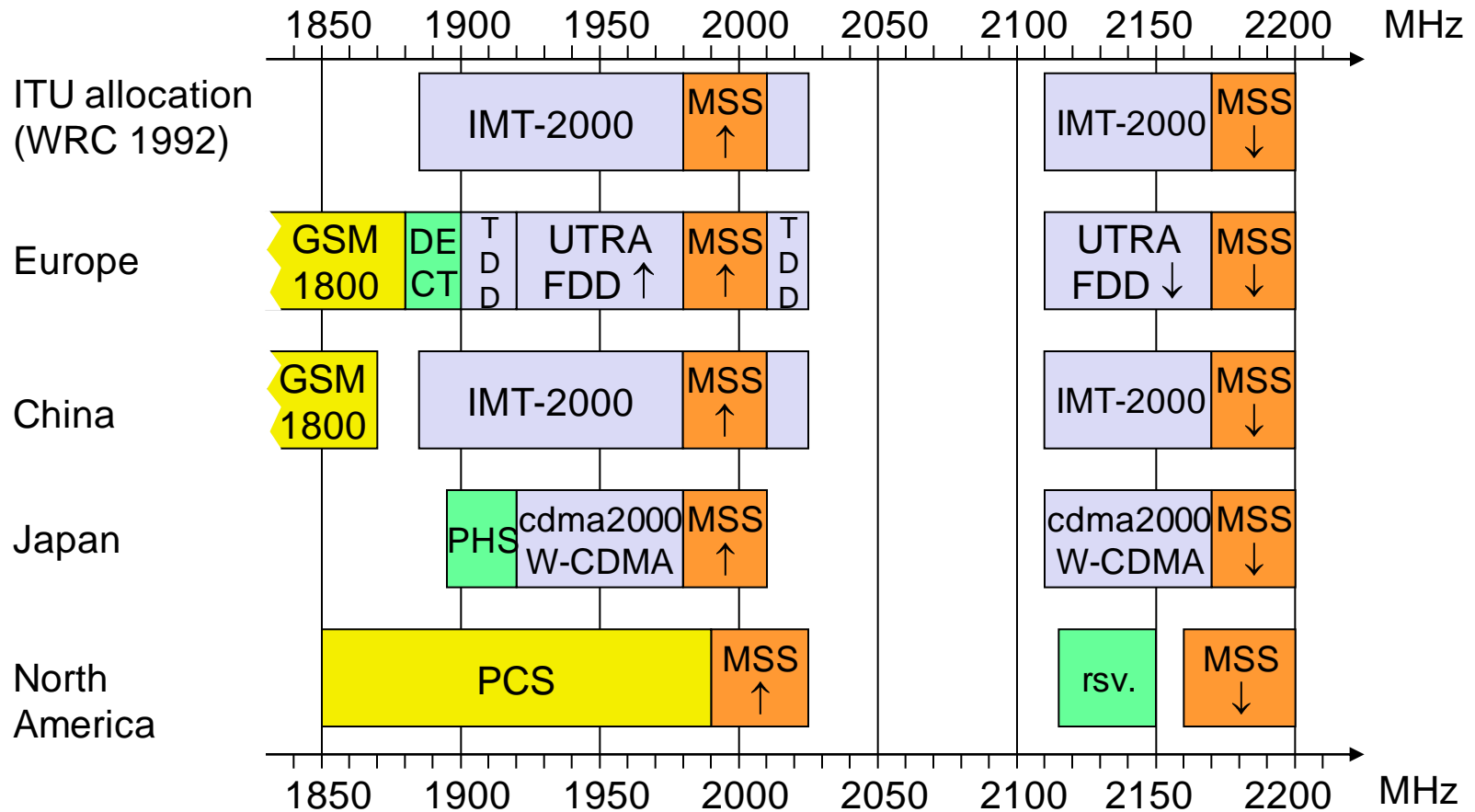




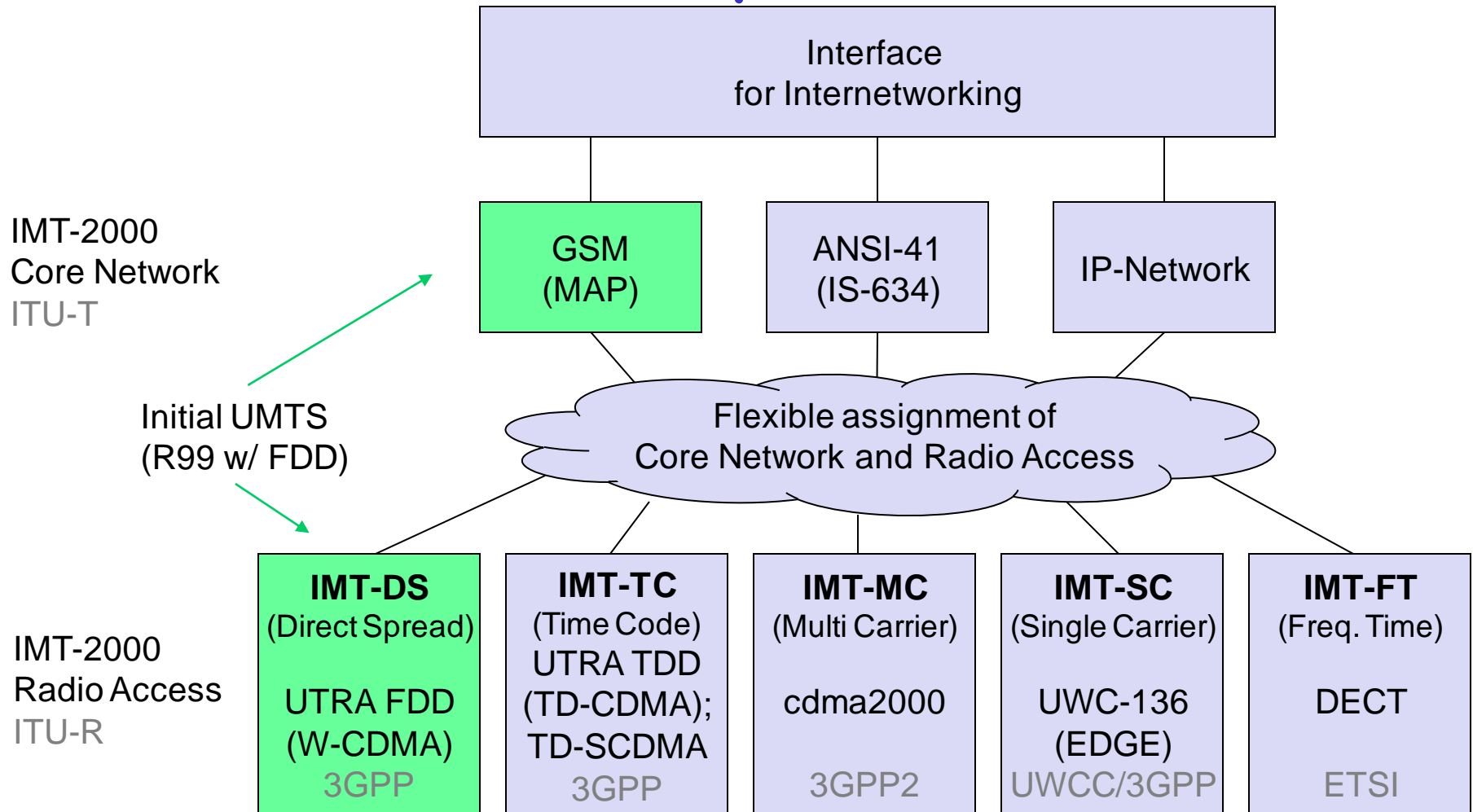
# UMTS and IMT-2000

- ❑ Proposals for IMT-2000 (International Mobile Telecommunications)
  - UWC-136, cdma2000, WP-CDMA
  - UMTS (Universal Mobile Telecommunications System) from ETSI
- ❑ UMTS
  - UTRA (was: UMTS, now: Universal Terrestrial Radio Access)
  - enhancements of GSM
    - EDGE (Enhanced Data rates for GSM Evolution): GSM up to 384 kbit/s
    - CAMEL (Customized Application for Mobile Enhanced Logic)
    - VHE (virtual Home Environment)
  - fits into GMM (Global Multimedia Mobility) initiative from ETSI
  - requirements
    - min. 144 kbit/s rural (goal: 384 kbit/s)
    - min. 384 kbit/s suburban (goal: 512 kbit/s)
    - up to 2 Mbit/s urban

# Frequencies for IMT-2000



# IMT-2000 family



# GSM and UMTS Releases

## □ Stages

- (0: feasibility study)
- 1: service description from a service-user's point of view
- 2: logical analysis, breaking the problem down into functional elements and the information flows amongst them
- 3: concrete implementation of the protocols between physical elements onto which the functional elements have been mapped
- (4: test specifications)

## □ Note

- "Release 2000" was used only temporarily and was eventually replaced by "Release 4" and "Release 5"

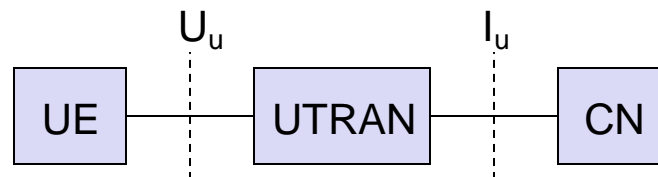
## □ Additional information:

- [www.3gpp.org/releases](http://www.3gpp.org/releases)
- [www.3gpp.org/ftp/Specs/html-info/SpecReleaseMatrix.htm](http://www.3gpp.org/ftp/Specs/html-info/SpecReleaseMatrix.htm)

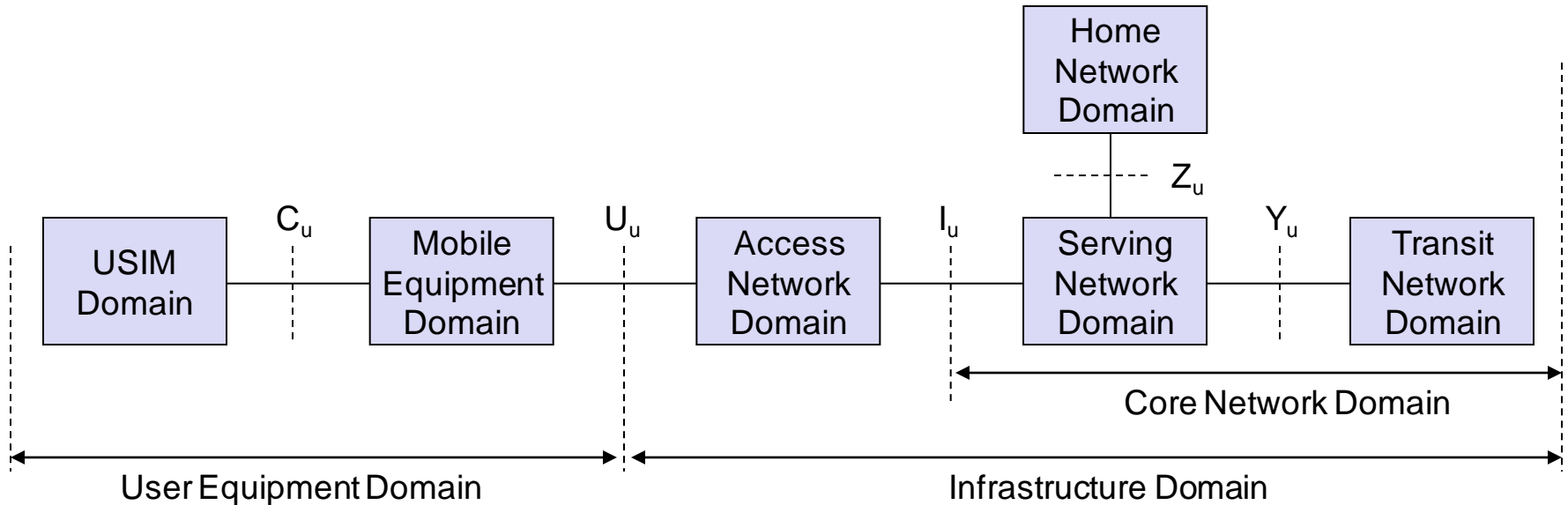
| Rel    | Spec version number | Functional freeze date, indicative only  |
|--------|---------------------|--|
| Rel-10 | 10.x.y              | Stage 1 ?<br>Stage 2 ?<br>Stage 3 ?  |
| Rel-9  | 9.x.y               | Stage 1 freeze December 2008<br>Stage 2 June 2009?<br>Stage 3 freeze December 2009?            |
| Rel-8  | 8.x.y               | Stage 1 freeze March 2008<br>Stage 2 freeze June 2008<br>Stage 3 freeze December 2008          |
| Rel-7  | 7.x.y               | Stage 1 freeze September 2005<br>Stage 2 freeze September 2006<br>Stage 3 freeze December 2007 |
| Rel-6  | 6.x.y               | December 2004 - March 2005   |
| Rel-5  | 5.x.y               | March - June 2002  |
| Rel-4  | 4.x.y               | March 2001   |
| R00    | 4.x.y               | see note 1 below   |
|        | 9.x.y               |  |
| R99    | 3.x.y               | March 2000   |
|        | 8.x.y               |  |
| R98    | 7.x.y               | early 1999   |
| R97    | 6.x.y               | early 1998   |
| R96    | 5.x.y               | early 1997   |
| Ph2    | 4.x.y               | 1995   |
| Ph1    | 3.x.y               | 1992   |

# UMTS architecture (Release 99 used here!)

- ❑ UTRAN (UTRA Network)
  - Cell level mobility
  - Radio Network Subsystem (RNS)
  - Encapsulation of all radio specific tasks
- ❑ UE (User Equipment)
- ❑ CN (Core Network)
  - Inter system handover
  - Location management if there is no dedicated connection between UE and UTRAN



# UMTS domains and interfaces I



## ❑ User Equipment Domain

- Assigned to a single user in order to access UMTS services

## ❑ Infrastructure Domain

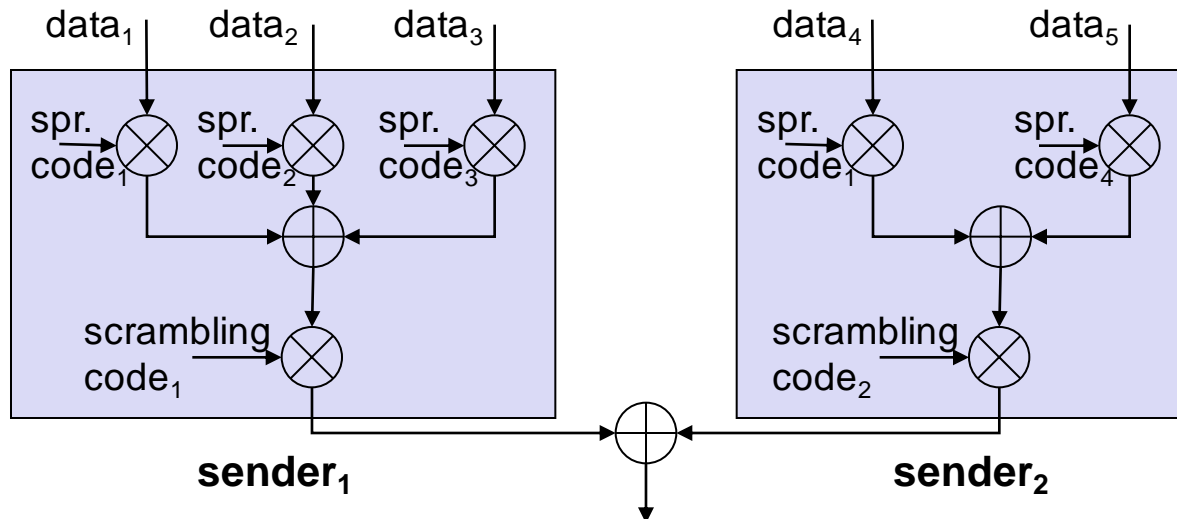
- Shared among all users
- Offers UMTS services to all accepted users

# UMTS domains and interfaces II

- ❑ Universal Subscriber Identity Module (USIM)
  - Functions for encryption and authentication of users
  - Located on a SIM inserted into a mobile device
- ❑ Mobile Equipment Domain
  - Functions for radio transmission
  - User interface for establishing/maintaining end-to-end connections
- ❑ Access Network Domain
  - Access network dependent functions
- ❑ Core Network Domain
  - Access network independent functions
  - Serving Network Domain
    - Network currently responsible for communication
  - Home Network Domain
    - Location and access network independent functions

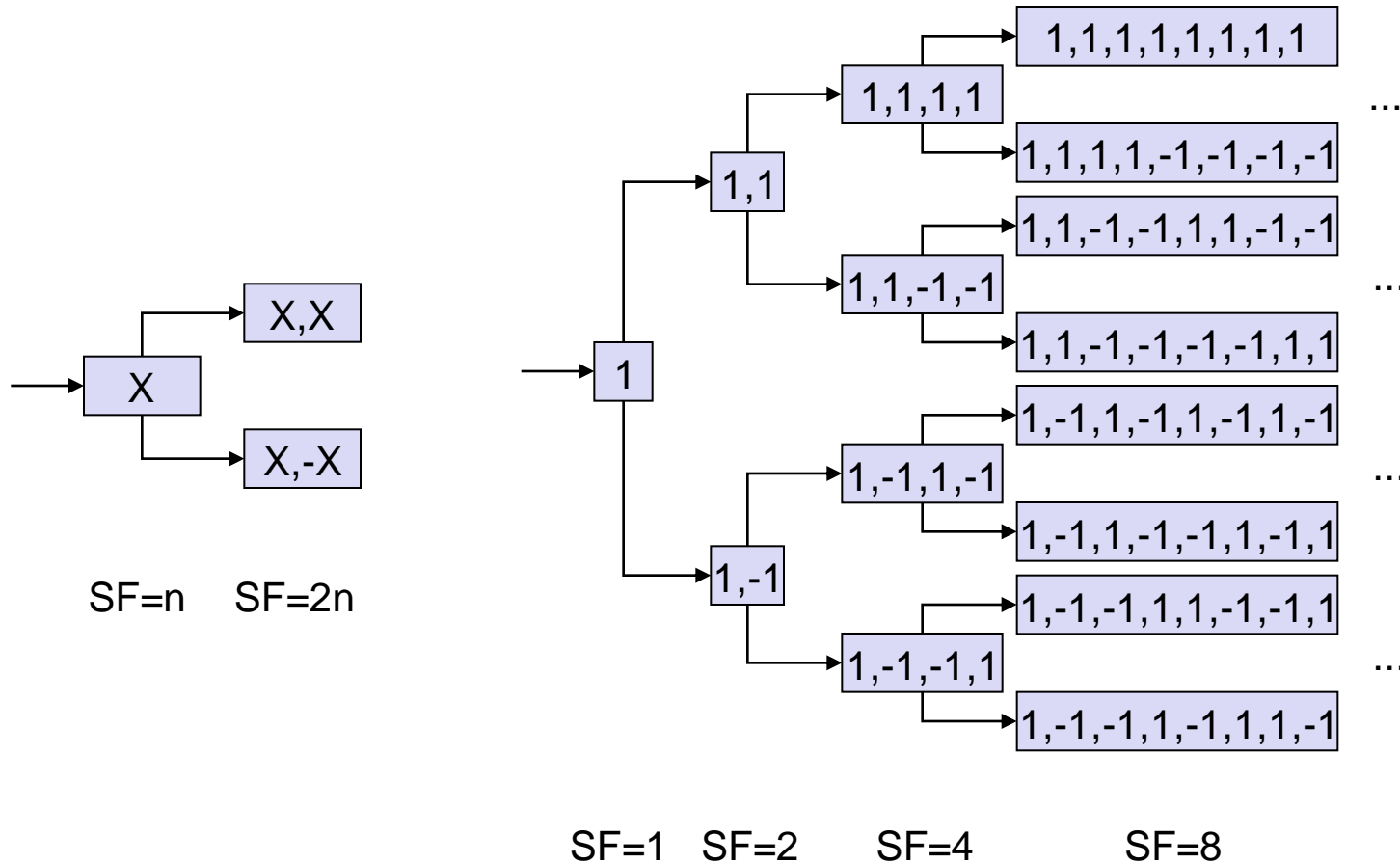
# Spreading and scrambling of user data

- ❑ Constant chipping rate of 3.84 Mchip/s
- ❑ Different user data rates supported via different spreading factors
  - higher data rate: less chips per bit and vice versa
- ❑ User separation via unique, quasi orthogonal scrambling codes
  - users are not separated via orthogonal spreading codes
  - much simpler management of codes: each station can use the same orthogonal spreading codes
  - precise synchronization not necessary as the scrambling codes stay quasi-orthogonal



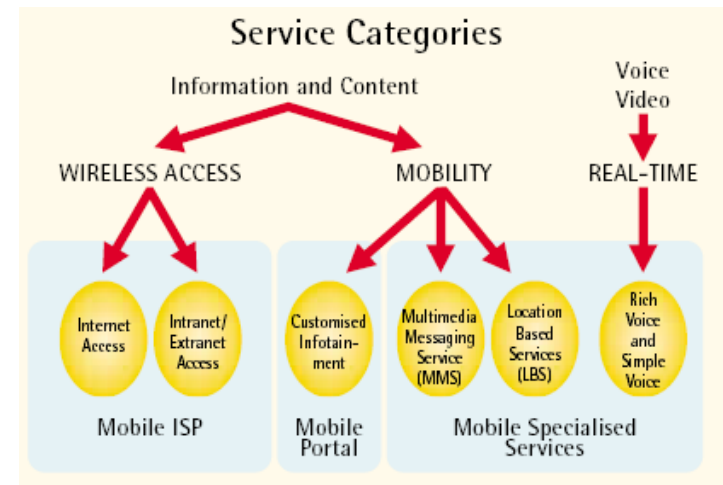


# OSVF coding



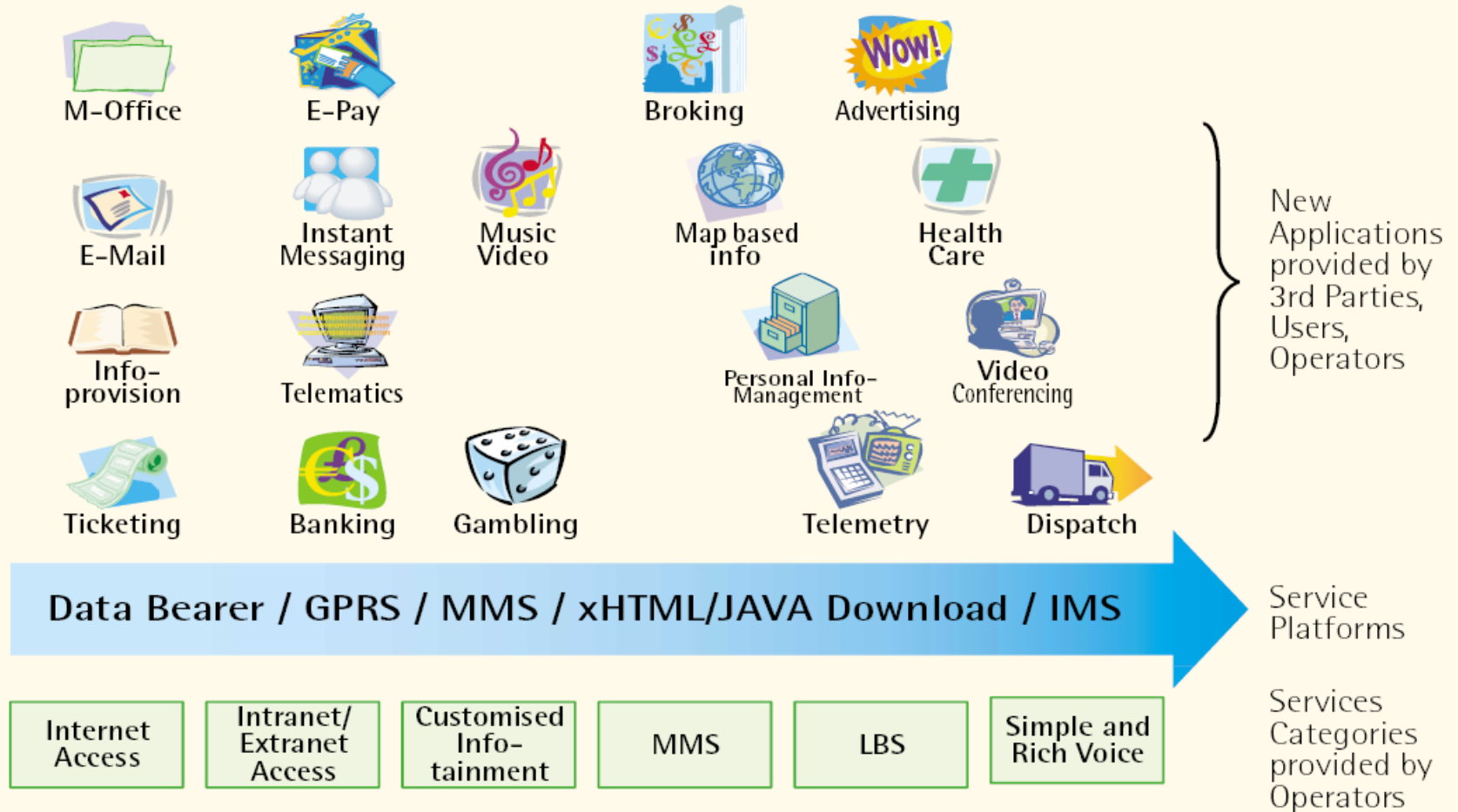
# Services

- ❑ In shaping future mobile services, the following characteristics should be taken into consideration: mobility, interactivity, convenience, ubiquity, easy access, immediacy, personalization, multimedia
- ❑ Services for 3G will evolve within 3 different areas:
  - Personal Communication
  - Wireless Internet
  - Mobile Media (e.g. music, sports, news services)
- ❑ Voice traffic will remain the primary business of 3G mobile networks



# Services

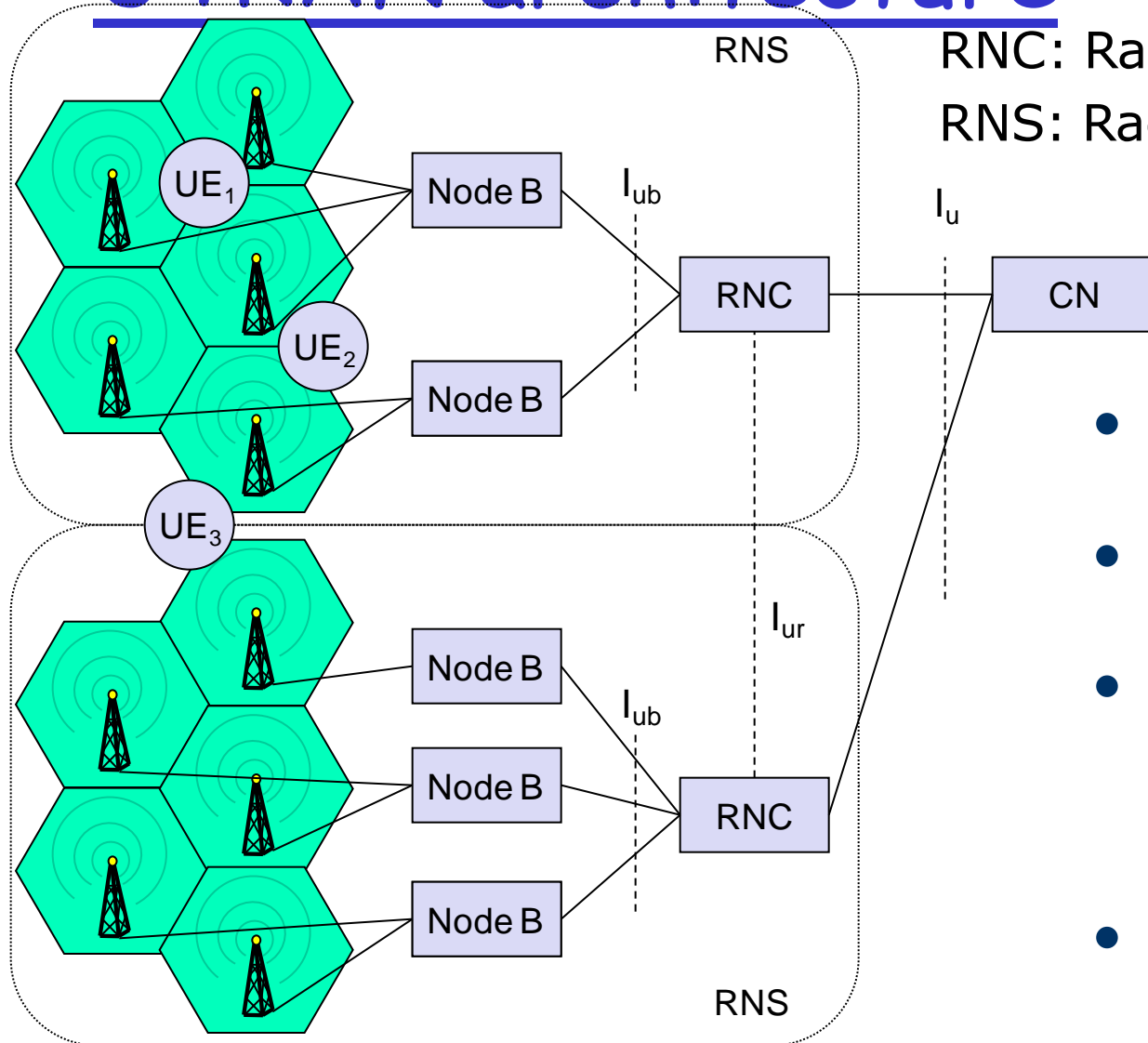
## Network Services provide Platforms for Applications



# Typical UTRA-FDD uplink data rates

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

# UTRAN architecture



RNC: Radio Network Controller

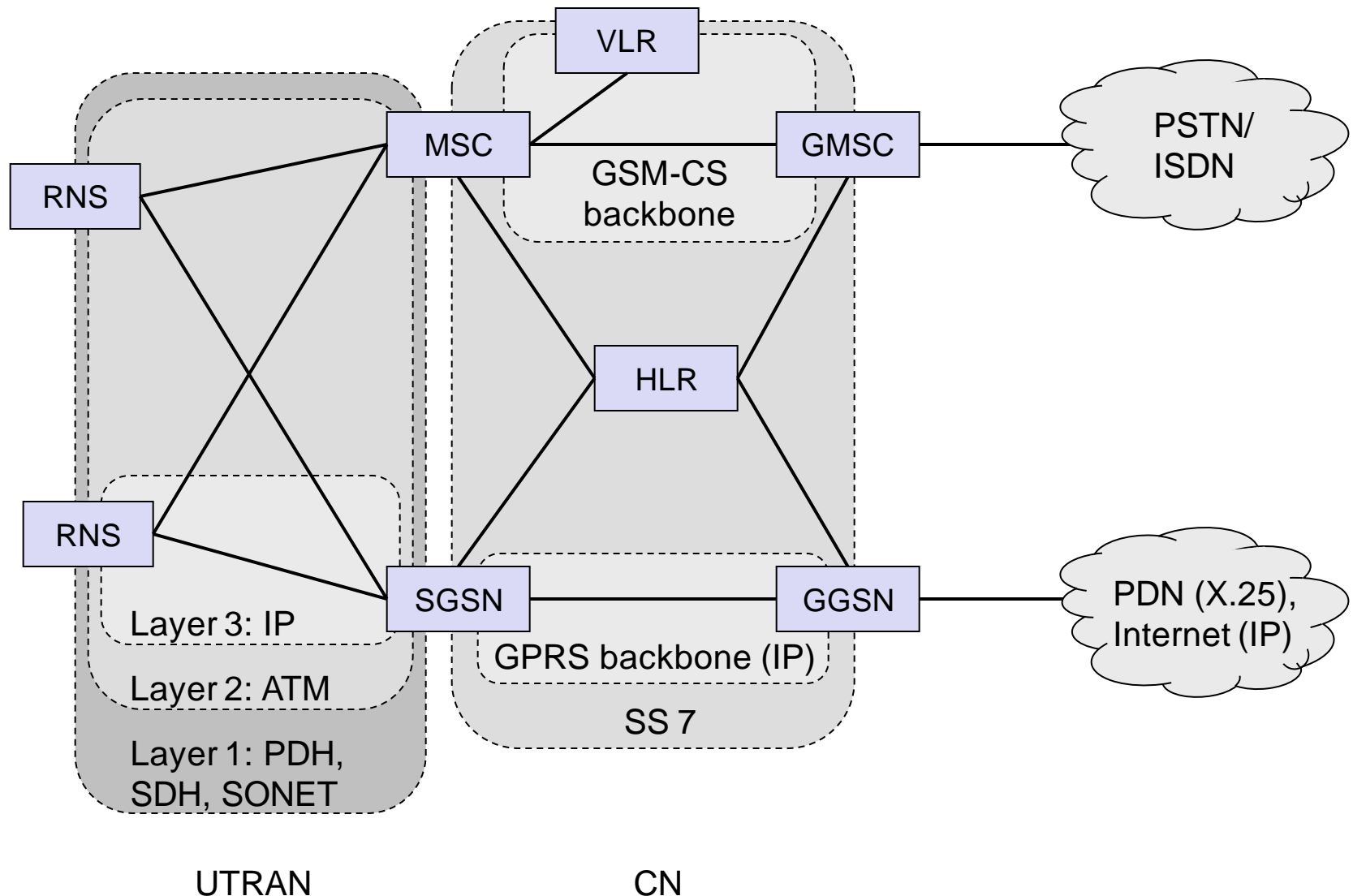
RNS: Radio Network Subsystem

- UTRAN comprises several RNSs
- Node B can support FDD or TDD or both
- RNC is responsible for handover decisions requiring signaling to the UE
- Cell offers FDD or TDD

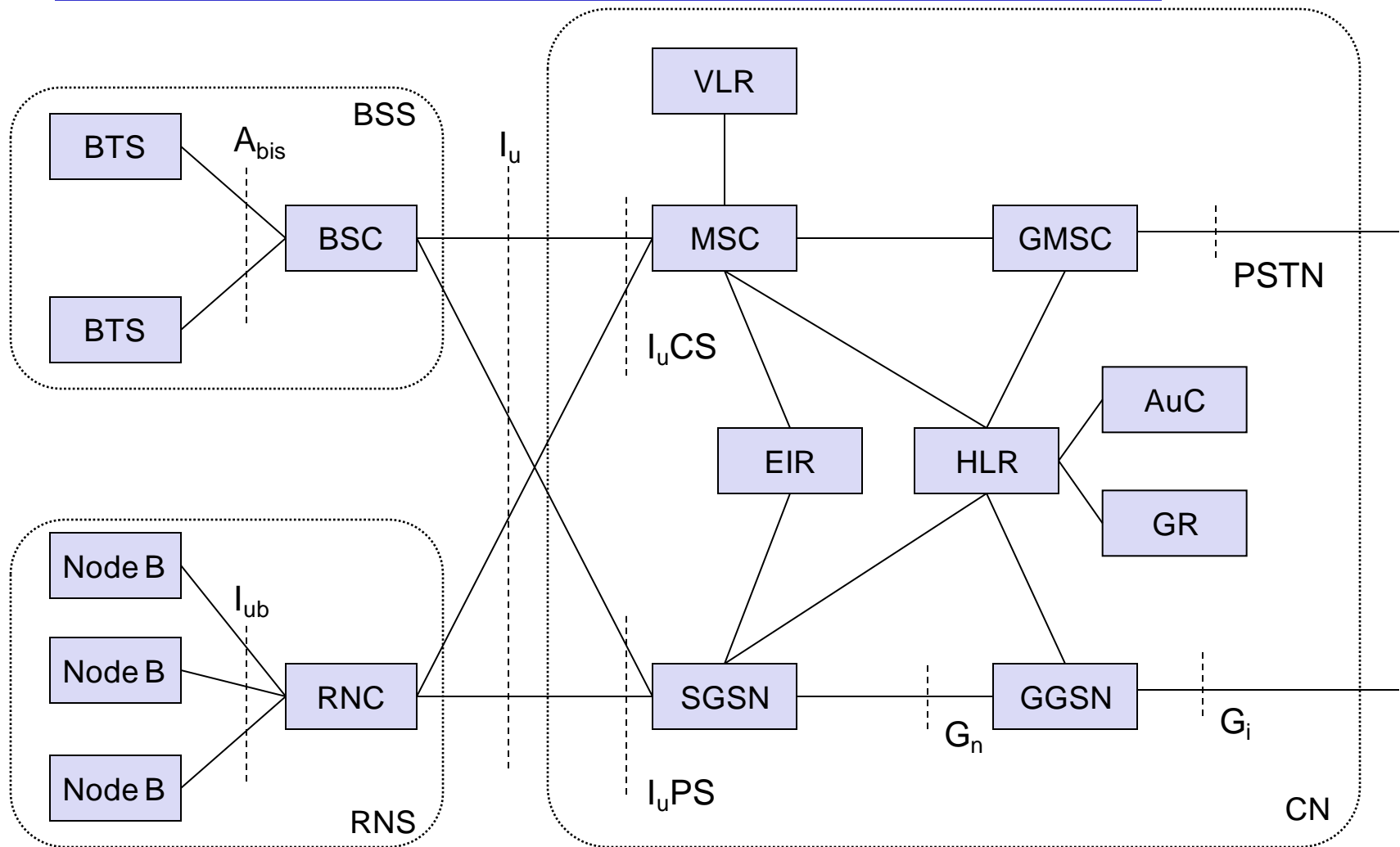
# UTRAN functions

- ☐ Admission control
- ☐ Congestion control
- ☐ System information broadcasting
- ☐ Radio channel encryption
- ☐ Handover
- ☐ SRNS moving
- ☐ Radio network configuration
- ☐ Channel quality measurements
- ☐ Macro diversity
- ☐ Radio carrier control
- ☐ Radio resource control
- ☐ Data transmission over the radio interface
- ☐ Outer loop power control (FDD and TDD)
- ☐ Channel coding
- ☐ Access control

# Core network: protocols



# Core network: architecture



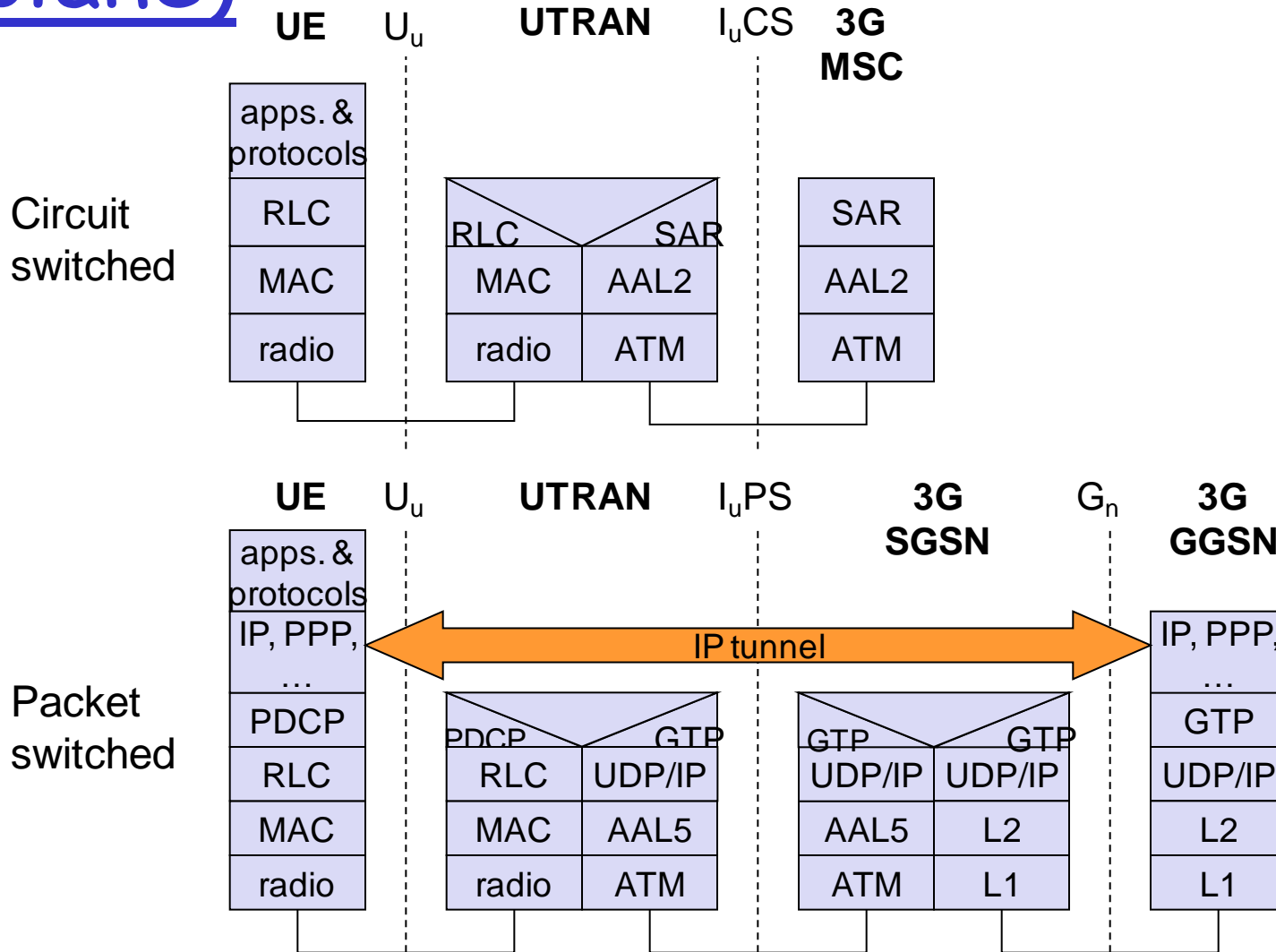


# Core network

- ❑ The Core Network (CN) and thus the Interface  $I_u$ , too, are separated into two logical domains:
- ❑ Circuit Switched Domain (CSD)
  - Circuit switched service incl. signaling
  - Resource reservation at connection setup
  - GSM components (MSC, GMSC, VLR)
  - $I_{uCS}$
- ❑ Packet Switched Domain (PSD)
  - GPRS components (SGSN, GGSN)
  - $I_{uPS}$
- ❑ Release 99 uses the GSM/GPRS network and adds a new radio access!
  - Helps to save a lot of money ...
  - Much faster deployment
  - Not as flexible as newer releases (5, 6)

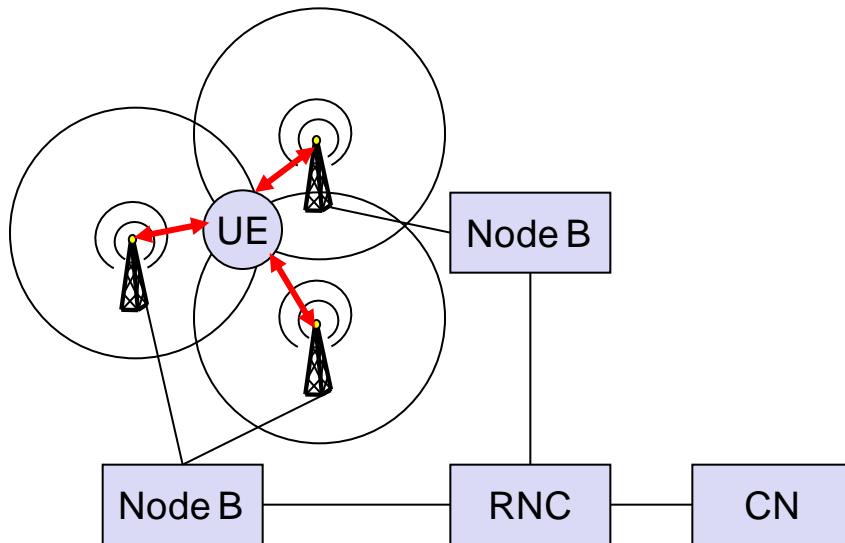
# UMTS protocol stacks (user plane)

[www.rejinpaul.com](http://www.rejinpaul.com)



Get useful study materials from [www.rejinpaul.com](http://www.rejinpaul.com)

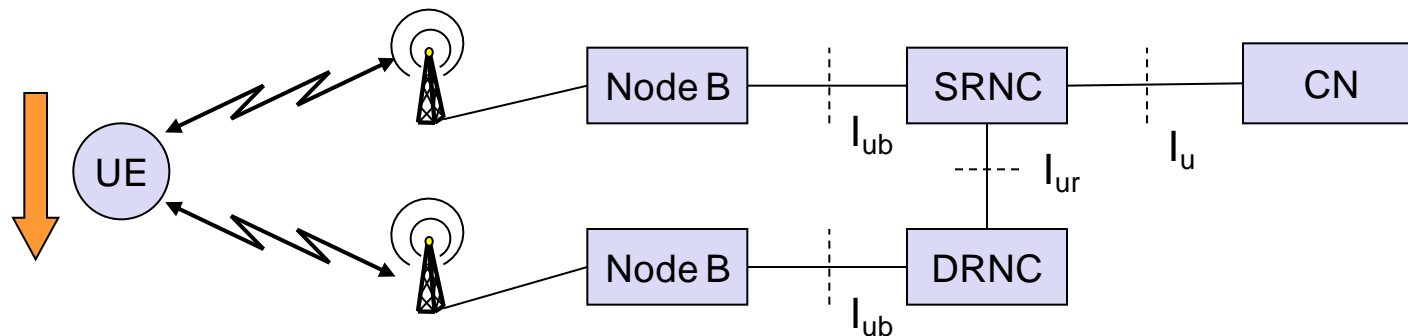
# Support of mobility: macro diversity



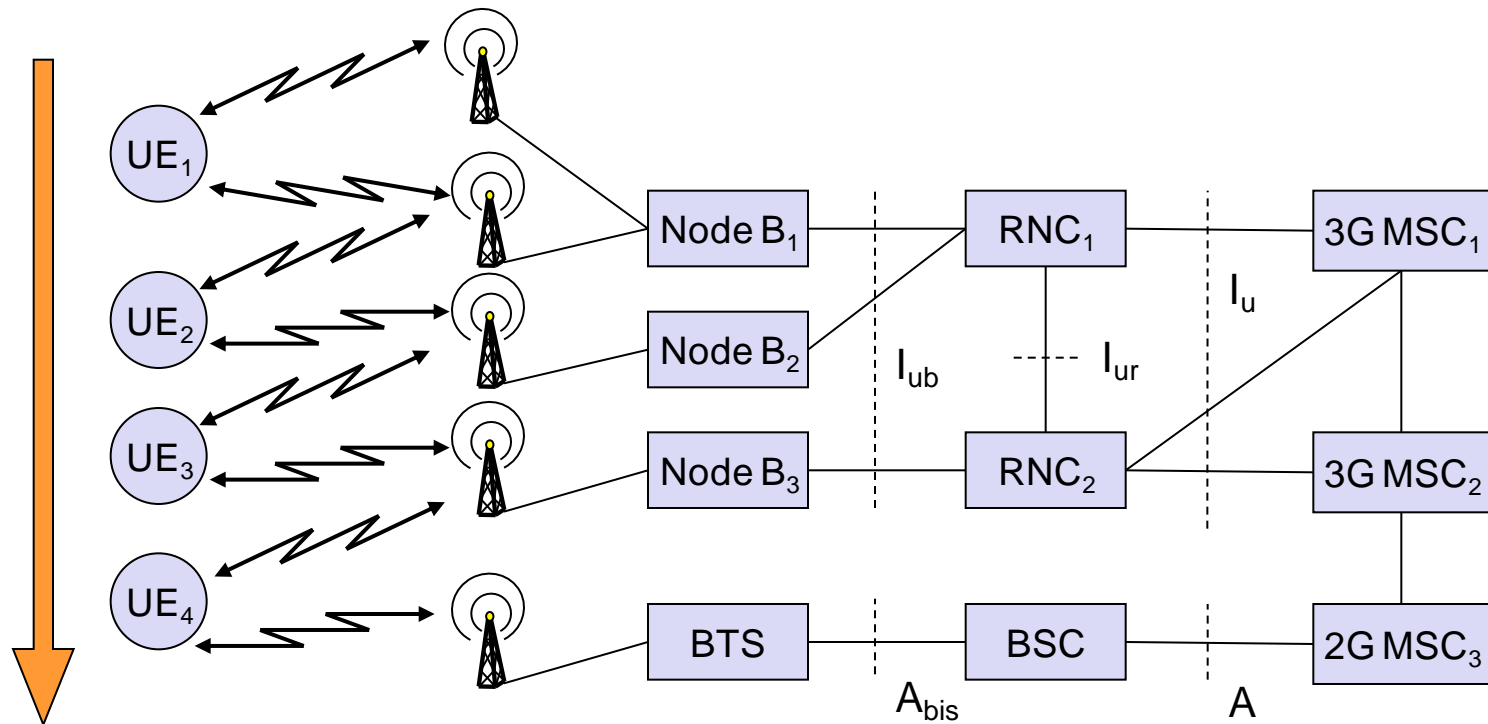
- ❑ Multicasting of data via several physical channels
  - Enables soft handover
  - FDD mode only
- ❑ Uplink
  - simultaneous reception of UE data at several Node Bs
  - Reconstruction of data at Node B, SRNC or DRNC
- ❑ Downlink
  - Simultaneous transmission of data via different cells
  - Different spreading codes in different cells

# Support of mobility: handover

- ❑ From and to other systems (e.g., UMTS to GSM)
  - This is a must as UMTS coverage will be poor in the beginning
- ❑ RNS controlling the connection is called SRNS (Serving RNS)
- ❑ RNS offering additional resources (e.g., for soft handover) is called Drift RNS (DRNS)
- ❑ End-to-end connections between UE and CN only via  $I_u$  at the SRNS
  - Change of SRNS requires change of  $I_u$
  - Initiated by the SRNS
  - Controlled by the RNC and CN



# Example handover types in UMTS/GSM



# Breathing Cells

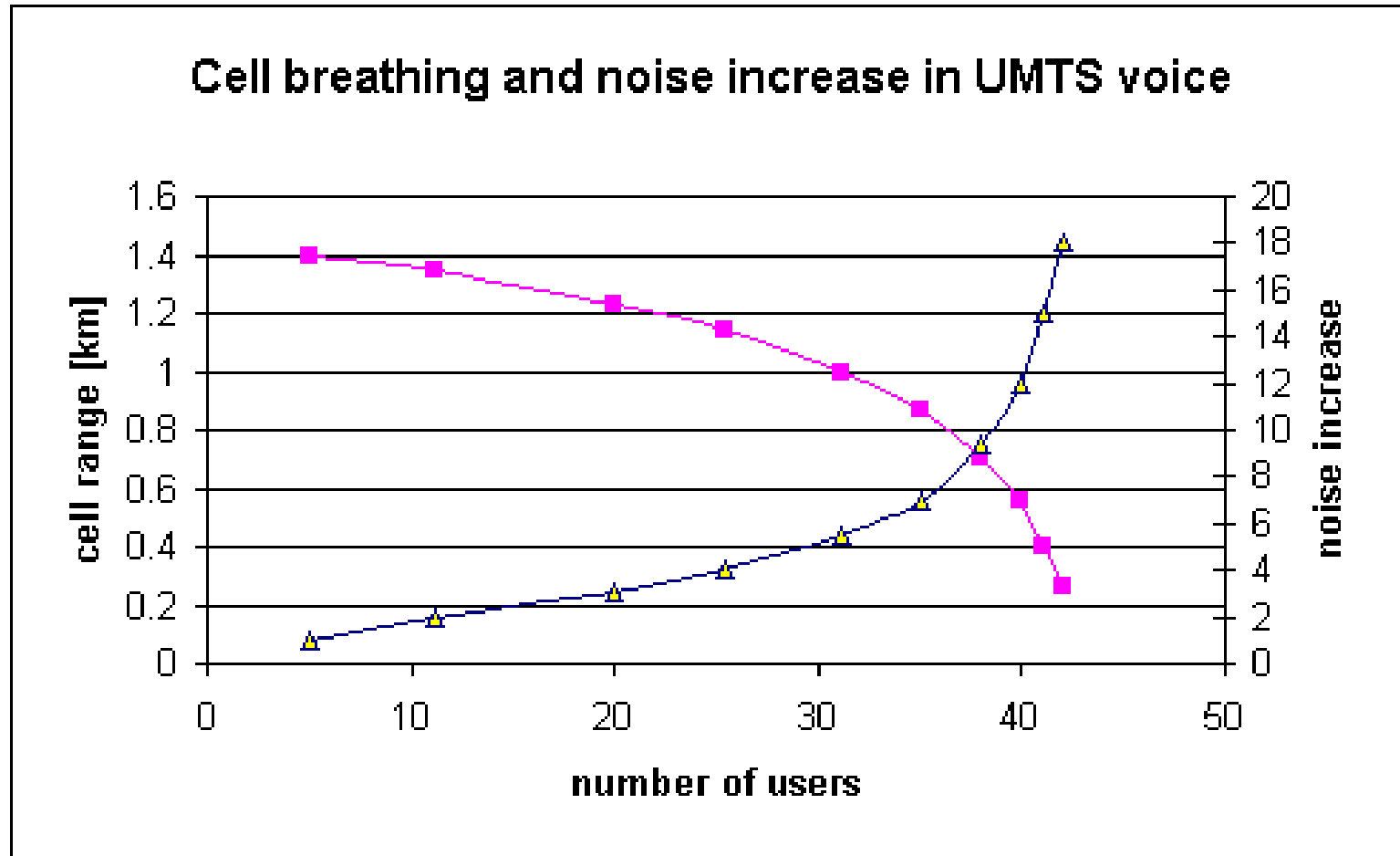
## ❑ GSM

- Mobile device gets exclusive signal from the base station
- Number of devices in a cell does not influence cell size

## ❑ UMTS

- Cell size is closely correlated to the cell capacity
- Signal-to-noise ratio determines cell capacity
- Noise is generated by interference from
  - other cells
  - other users of the same cell
- Interference increases noise level
- Devices at the edge of a cell cannot further increase their output power (max. power limit) and thus drop out of the cell  
⇒ no more communication possible
- Limitation of the max. number of users within a cell required
- Cell breathing complicates network planning

# Breathing Cells: Example



# UMTS services (originally)

## □ Data transmission service profiles

| Service Profile     | Bandwidth   | Transport mode   |                                |
|---------------------|-------------|------------------|--------------------------------|
| High Interactive MM | 128 kbit/s  | Circuit switched | Bidirectional, video telephone |
| High MM             | 2 Mbit/s    | Packet switched  | Low coverage, max. 6 km/h      |
| Medium MM           | 384 kbit/s  | Circuit switched | asymmetrical, MM, downloads    |
| Switched Data       | 14.4 kbit/s | Circuit switched |                                |
| Simple Messaging    | 14.4 kbit/s | Packet switched  | SMS successor, E-Mail          |
| Voice               | 16 kbit/s   | Circuit switched |                                |

## □ Virtual Home Environment (VHE)

- Enables access to personalized data independent of location, access network, and device
- Network operators may offer new services without changing the network
- Service providers may offer services based on components which allow the automatic adaptation to new networks and devices
- Integration of existing TN services



# Some current enhancements

## □ GSM

### ○ EMS/MMS

- EMS: 760 characters possible by chaining SMS, animated icons, ring tones, was soon replaced by MMS (or simply skipped)
- MMS: transmission of images, video clips, audio
  - see WAP 2.0 / chapter 10

### ○ EDGE (Enhanced Data Rates for Global [was: GSM] Evolution)

- 8-PSK instead of GMSK, up to 384 kbit/s
- new modulation and coding schemes for GPRS → EGPRS
  - MCS-1 to MCS-4 uses GMSK at rates 8.8/11.2/14.8/17.6 kbit/s
  - MCS-5 to MCS-9 uses 8-PSK at rates 22.4/29.6/44.8/54.4/59.2 kbit/s

## □ UMTS

### ○ HSDPA (High-Speed Downlink Packet Access)

- initially up to 10 Mbit/s for the downlink, later > 20 Mbit/s using MIMO- (Multiple Input Multiple Output-) antennas
- can use 16-QAM instead of QPSK (ideally > 13 Mbit/s)
- user rates e.g. 3.6 or 7.2 Mbit/s

### ○ HSUPA (High-Speed Uplink Packet Access)

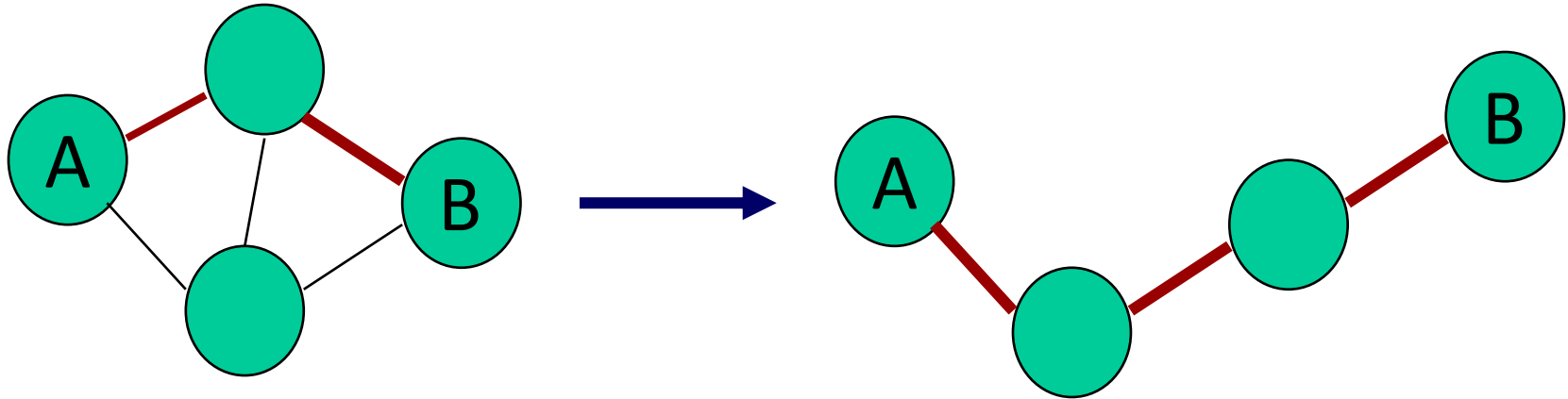
- initially up to 5 Mbit/s for the uplink
- user rates e.g. 1.45 Mbit/s

- **MOBILE AD HOC  
NETWORKS**

# What Are MANETs ?

- Interconnected collection of wireless nodes
- Nodes enter and leave over time
- Nodes also act as routers; forward packets
- No pre-established network infrastructure
- No centralized administration
- Communication using BlueTooth and WAP

# Characteristics Of MANETs



- Dynamic Topologies and node memberships
- Host movement frequent
- Topology change frequent
- Data must be routed via intermediate nodes
- Bandwidth constraints
- Many Transmission Errors
- Energy-constrained operation

# Why Ad Hoc Networks ?

- Setting up of fixed access points and backbone infrastructure is not always viable
  - Infrastructure may not be present in a disaster area or war zone
  - Infrastructure may not be practical for short-range radios; Bluetooth (range ~ 10m)
- Ad hoc networks:
  - Do not need backbone infrastructure support
  - Are easy to deploy
  - Useful when infrastructure is absent, destroyed or impractical

# Where Could We Use MANETs ?

- Industrial and commercial networks
- 'Anywhere' communication
- Military applications
- Robust alternatives to cellular networks
- Wearable and Ubiquitous computing
- Remote satellite - based communication

# Many Applications

- **Personal area networking**
  - cell phone, laptop, ear phone, wrist watch
- **Military environments**
  - soldiers, tanks, planes
- **Civilian environments**
  - taxi cab network
  - meeting rooms
  - sports stadiums
  - boats, small aircraft
- **Emergency operations**
  - search-and-rescue
  - policing and fire fighting

# Challenges in Mobile Environments

- **Limitations of the Wireless Network**
  - packet loss due to transmission errors
  - variable capacity links
  - frequent disconnections/partitions
  - limited communication bandwidth
  - Broadcast nature of the communications
- **Limitations Imposed by Mobility**
  - dynamically changing topologies/routes
  - lack of mobility awareness by system/applications
- **Limitations of the Mobile Computer**
  - short battery lifetime
  - limited capacities



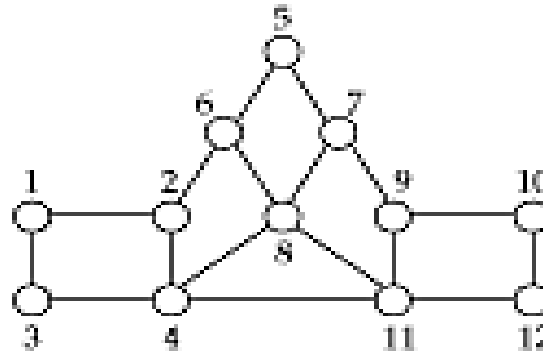
# Effect of mobility on the protocol stack

- **Application**
  - new applications and adaptations
- **Transport**
  - congestion and flow control
- **Network**
  - addressing and routing
- **Link**
  - media access and handoff
- **Physical**
  - transmission errors and interference

# Routing Protocols

# Traditional Routing

- A *routing protocol* sets up a *routing table* in *routers*



ROUTING TABLE AT 1

| Destination | Next hop | Destination | Next hop |
|-------------|----------|-------------|----------|
| 1           | —        | 7           | 2        |
| 2           | 2□       | 8□          | 2□       |
| 3           | 3□       | 9□          | 2□       |
| 4           | 3□       | 10□         | 2□       |
| 5           | 2□       | 11□         | 3□       |
| 6           | 2        | 12          | 3        |

- A node makes a *local* choice depending on *global* topology

# Routing and Mobility

- Finding a path from a source to a destination
- Issues
  - Frequent route changes
    - amount of data transferred between route changes may be much smaller than traditional networks
  - Route changes may be related to host movement
  - Low bandwidth links
- Goal of routing protocols
  - decrease routing-related overhead
  - find short routes
  - find “stable” routes (despite mobility)

# Routing Protocols

- **Proactive protocols**
  - Traditional distributed shortest-path protocols
  - Maintain routes between every host pair at all times
  - Based on periodic updates; High routing overhead
  - Example: DSDV (destination sequenced distance vector)
- **Reactive protocols**
  - Determine route if and when needed
  - Source initiates route discovery
  - Example: DSR (dynamic source routing)
- **Hybrid protocols**
  - Adaptive; Combination of proactive and reactive
  - Example : ZRP (zone routing protocol)

# Protocol Trade-offs

- **Proactive protocols**
  - Always maintain routes
  - Little or no delay for route determination
  - Consume bandwidth to keep routes up-to-date
  - Maintain routes which may never be used
- **Reactive protocols**
  - Lower overhead since routes are determined on demand
  - Significant delay in route determination
  - Employ flooding (global search)
  - Control traffic may be bursty
- Which approach achieves a better trade-off depends on the traffic and mobility patterns

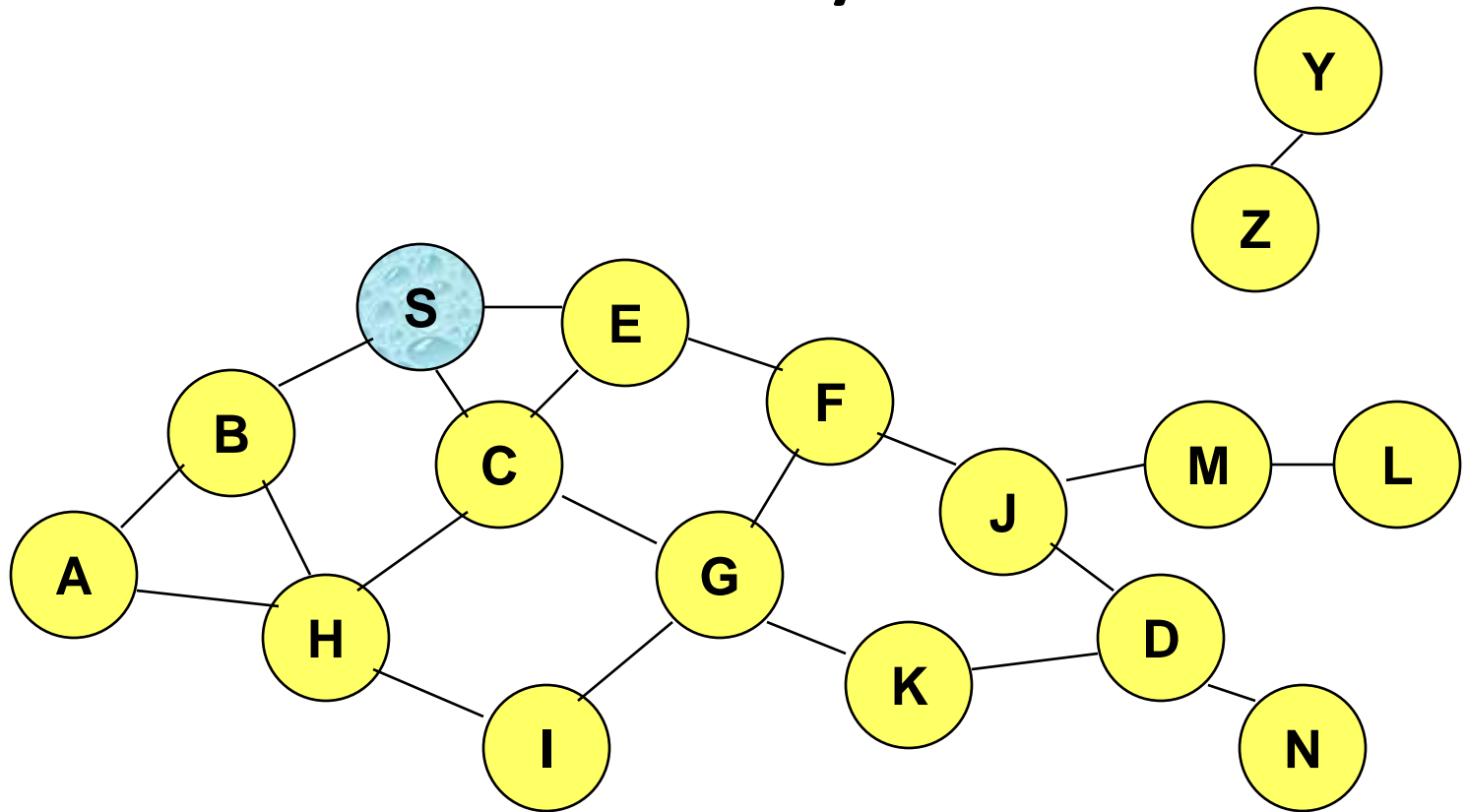
# Reactive Routing Protocols

# Dynamic Source Routing (DSR)

- When node S wants to send a packet to node D, but does not know a route to D, node S initiates a **route discovery**
- Source node S floods **Route Request (RREQ)**
- Each node *appends own identifier* when forwarding RREQ



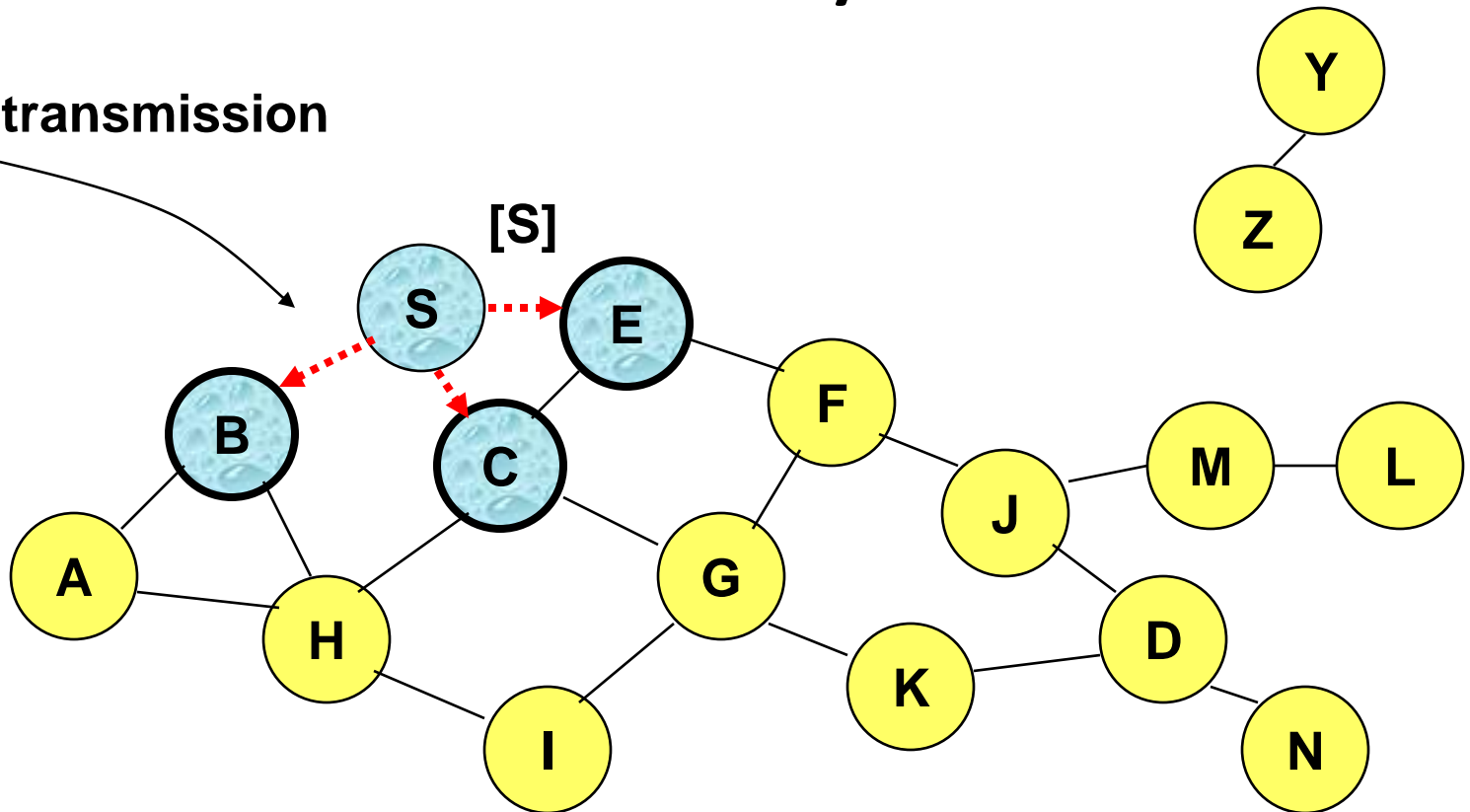
# Route Discovery in DSR



**Represents a node that has received RREQ for D from S**

# Route Discovery in DSR

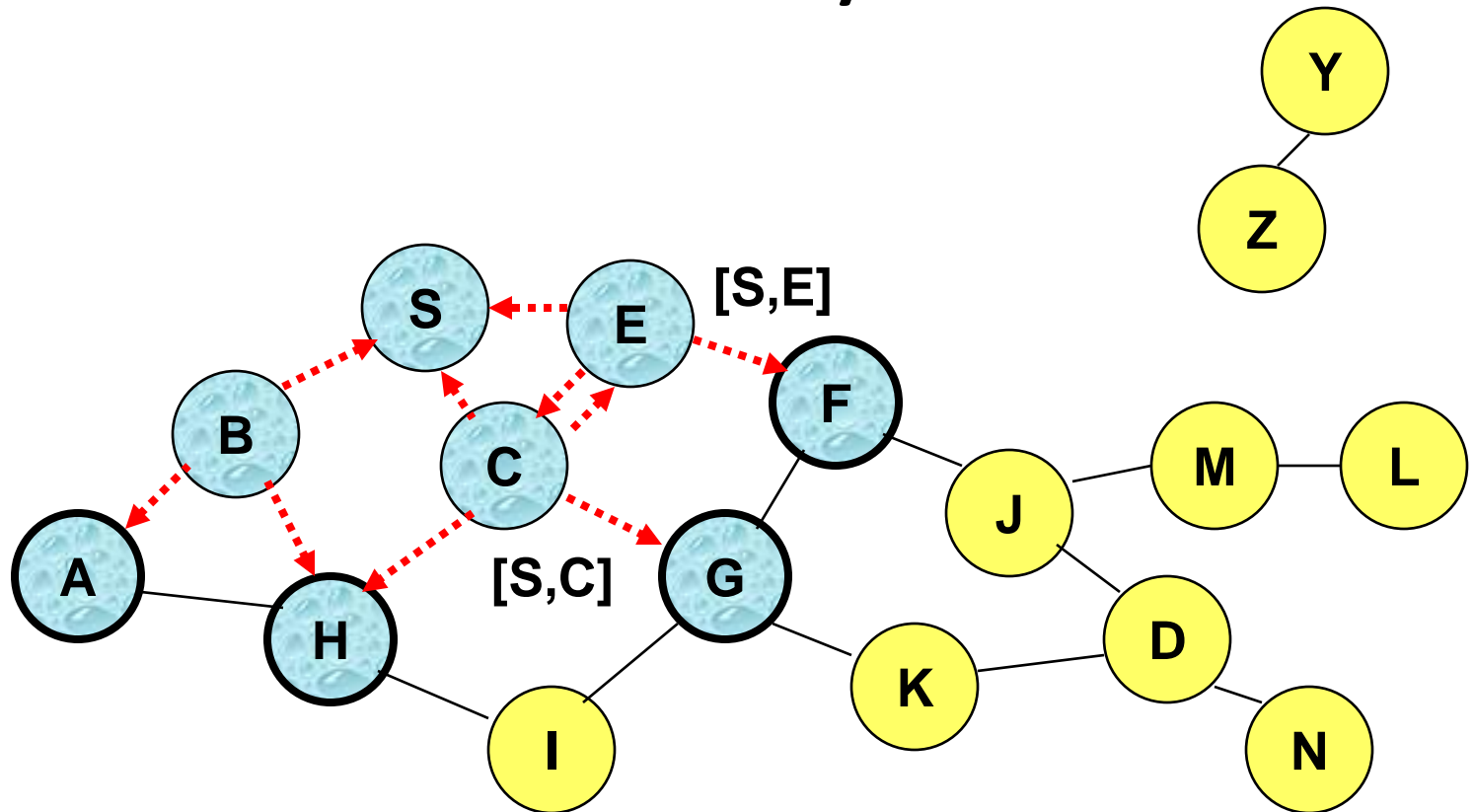
Broadcast transmission



.....→ Represents transmission of RREQ

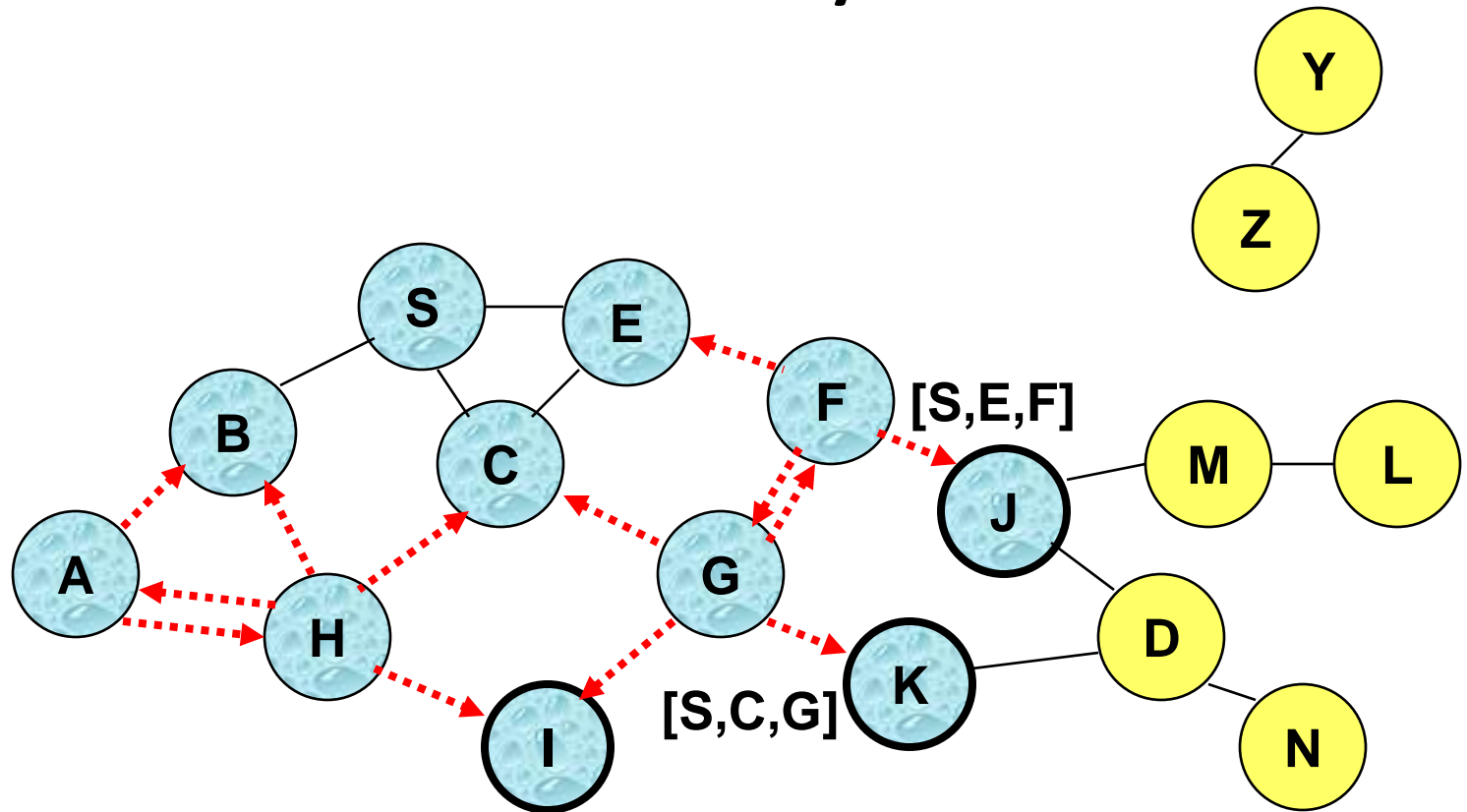
[X,Y] Represents list of identifiers appended to RREQ

# Route Discovery in DSR



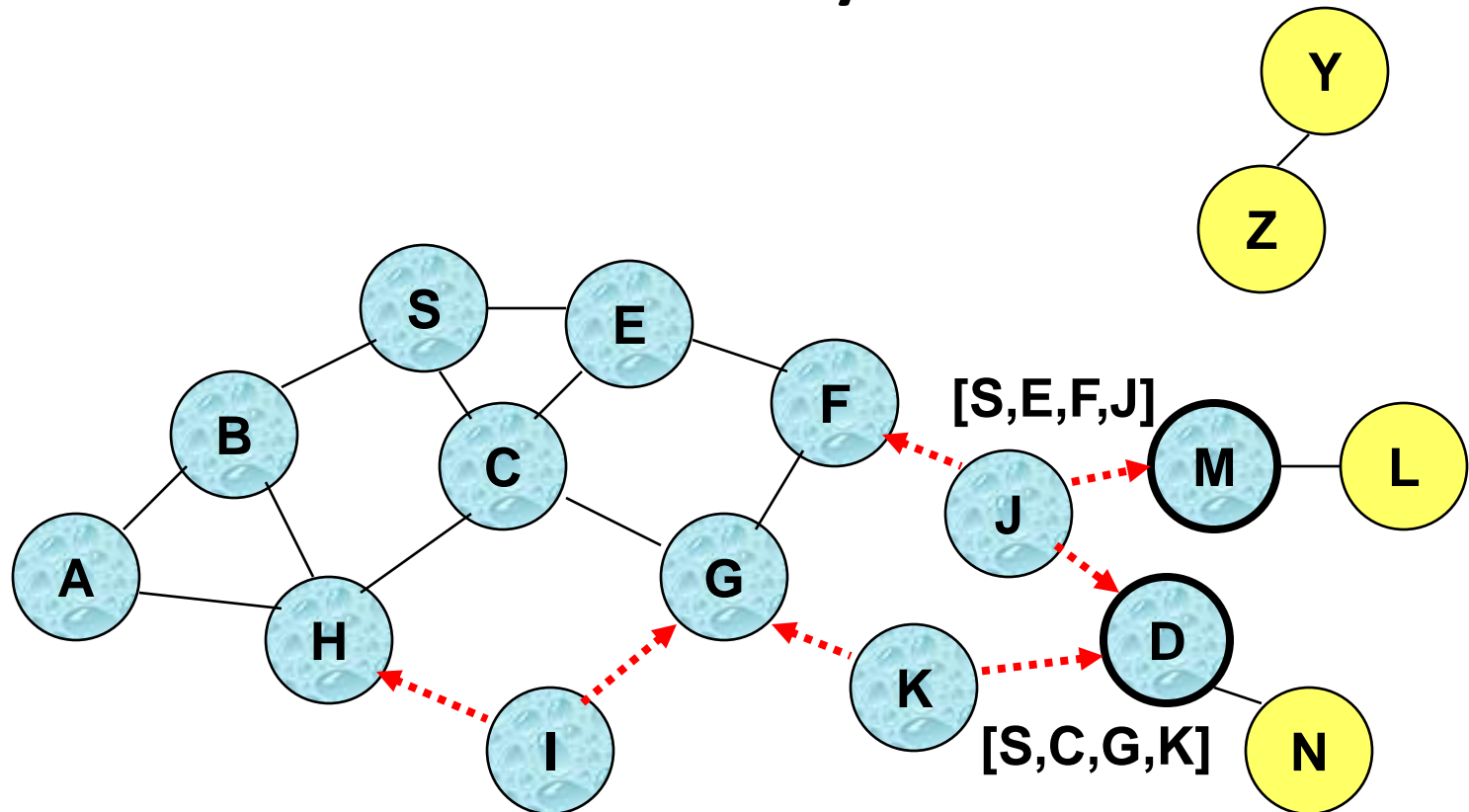
- **Node H receives packet RREQ from two neighbors:  
potential for collision**

# Route Discovery in DSR



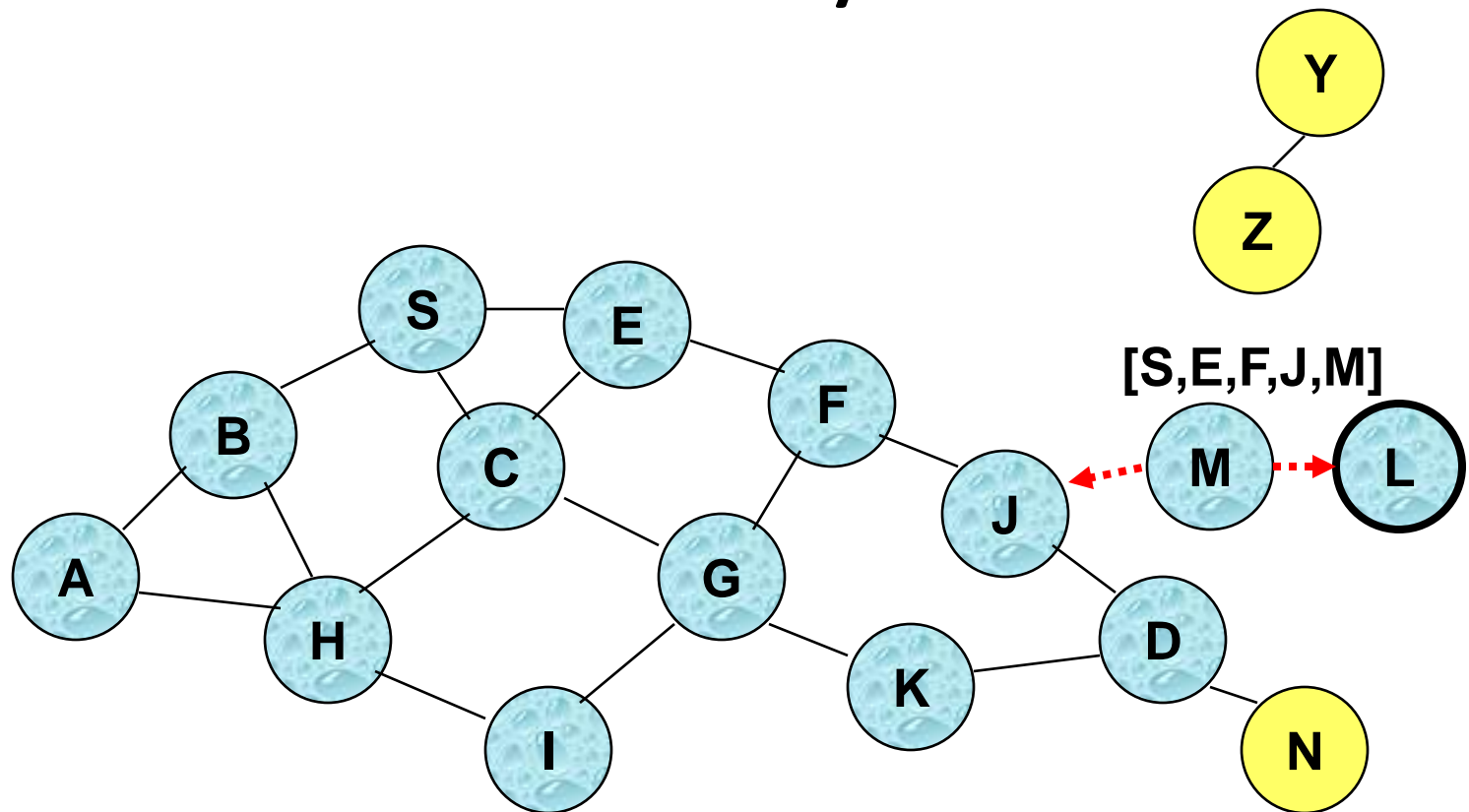
- Node C receives RREQ from G and H, but does not forward it again, because node C has **already forwarded RREQ** once

# Route Discovery in DSR



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

# Route Discovery in DSR

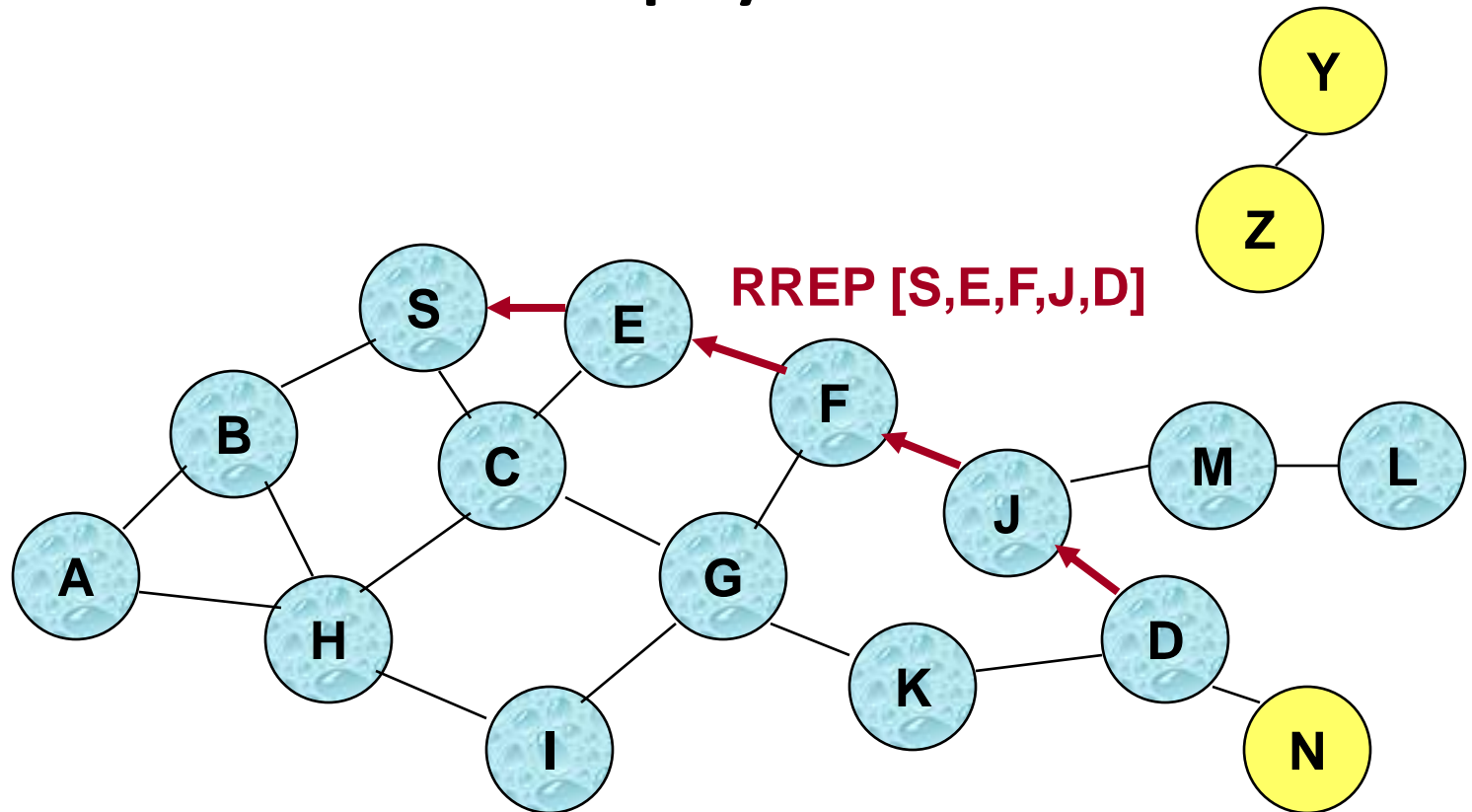


- Node D **does not forward** RREQ, because node D is the **intended target** of the route discovery

# Route Discovery in DSR

- Destination D on receiving the first RREQ, sends a **Route Reply (RREP)**
- RREP is sent on a route obtained by **reversing** the route appended to received RREQ
- RREP **includes the route** from S to D on which RREQ was received by node D

# Route Reply in DSR



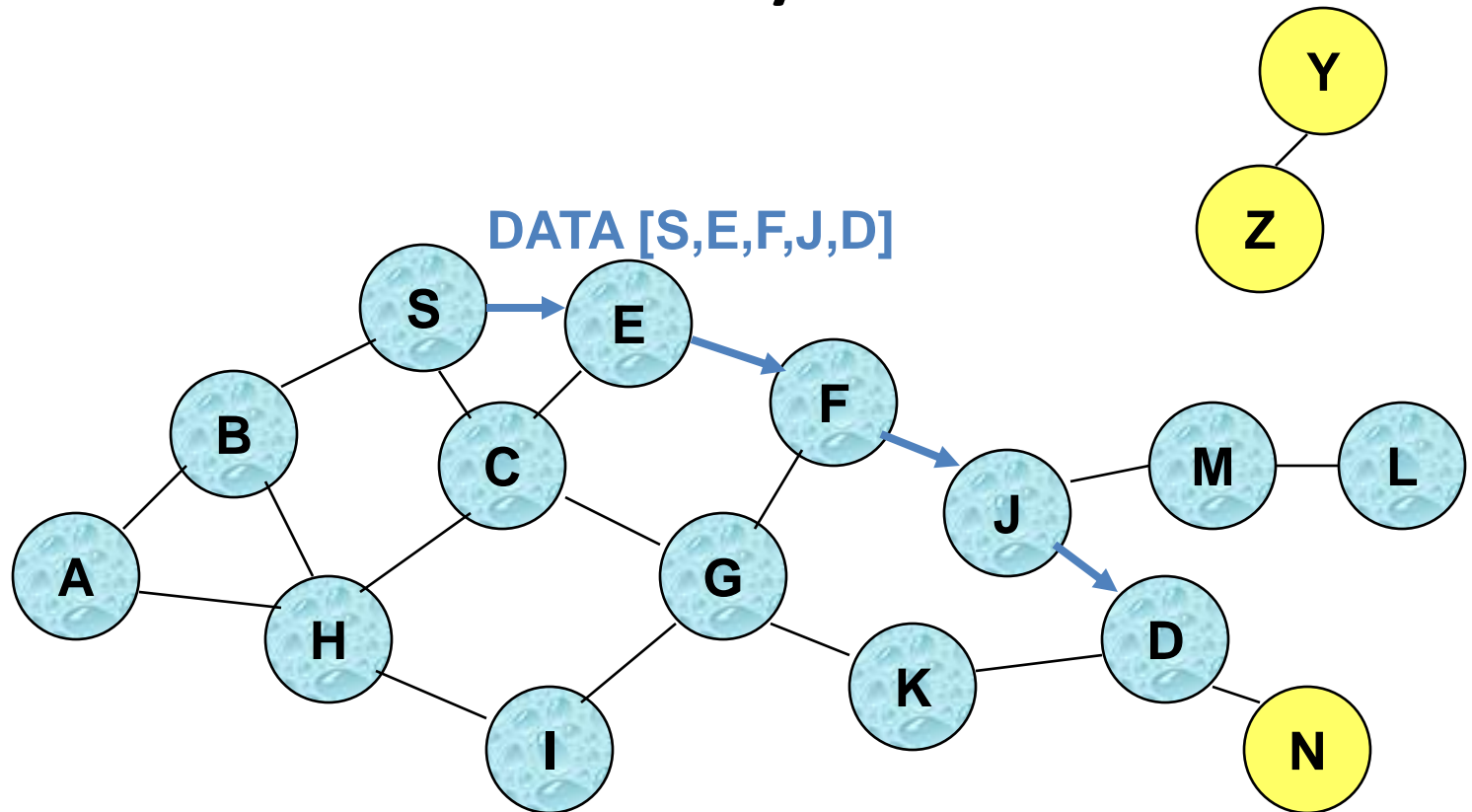
← Represents RREP control message



# Dynamic Source Routing (DSR)

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

# Data Delivery in DSR



**Packet header size grows with route length**

# DSR Optimization: Route Caching

- Each node caches a new route it learns by *any means*
- When node S finds route [S,E,F,J,D] to node D, node S also learns route [S,E,F] to node F
- When node K receives Route Request [S,C,G] destined for node, node K learns route [K,G,C,S] to node S
- When node F forwards Route Reply RREP [S,E,F,J,D], node F learns route [F,J,D] to node D
- When node E forwards Data [S,E,F,J,D] it learns route [E,F,J,D] to node D

# Dynamic Source Routing: Advantages

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

# Dynamic Source Routing: Disadvantages

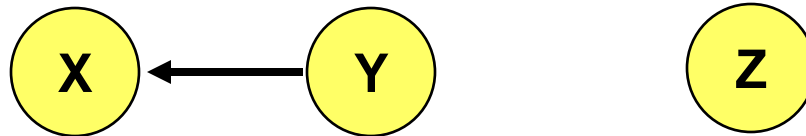
[www.rejinpaul.com](http://www.rejinpaul.com)

- Packet header size grows with route length due to source routing
- Flood of route requests may potentially reach all nodes in the network
- Potential collisions between route requests propagated by neighboring nodes
  - insertion of random delays before forwarding RREQ
- Increased contention if too many route replies come back due to nodes replying using their local cache
  - Route Reply *Storm* problem

# Proactive Routing Protocols

# Destination-Sequenced Distance-Vector (DSDV)

- When X receives information from Y about a route to Z
  - Let destination sequence number for Z at X be  $S(X)$ ,  $S(Y)$  is sent from Y



- If  $S(X) > S(Y)$ , then X ignores the routing information received from Y
- If  $S(X) = S(Y)$ , and cost of going through Y is smaller than the route known to X, then X sets Y as the next hop to Z
- If  $S(X) < S(Y)$ , then X sets Y as the next hop to Z, and  $S(X)$  is updated to equal  $S(Y)$

# DSDV Protocol

- Packets are transmitted between the nodes using route tables stored at each node.
- Each **route table** lists all available destinations and the number of hops to each destination.
- For each destination, a node knows which of its neighbours leads to the shortest path to the destination.



# DSDV Protocol

- Consider a source node S and a destination node D.
- Each route table entry in S is tagged with a sequence number that is originated by the destination node.
- For example, the entry for D is tagged with a sequence number that S received from D (may be through other nodes).

# DSDV Protocol

- We need to maintain the consistency of the route tables in a dynamically varying topology.
- Each node periodically transmits updates. This is done by each node when significant new information is available.

# DSDV Protocol

- The route-update messages indicate which nodes are accessible from each node and the number of hops to reach them.
- We consider the hop-count as the distance between two nodes. However, the DSDV protocol can be modified for other metrics as well.

# Route Advertisements

- The DSDV protocol requires each mobile node to advertise its own route table to all of its current neighbours.
- Since the nodes are mobile, the entries can change dynamically over time.
- The route advertisements should be made whenever there is any change in the neighbourhood or periodically.

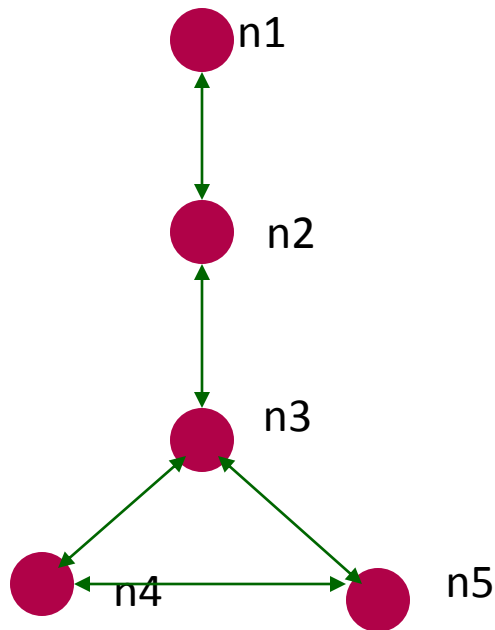
# Route Advertisements

- Each mobile node agrees to forward route advertising messages from other mobile nodes.
- This forwarding is necessary to send the advertisement messages all over the network.
- In other words, route advertisement messages help mobile nodes to get an overall picture of the topology of the network.

# Route Table Entry Structure

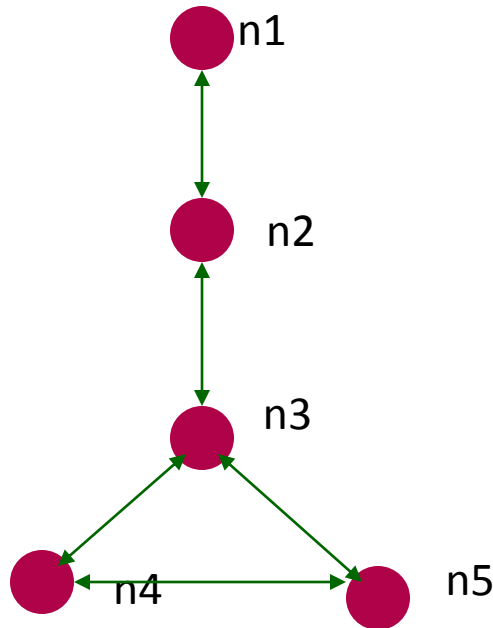
- The route advertisement broadcast by each mobile node has the following information for each new route :
  - The destination's address
  - The number of hops to the destination
  - The sequence number of the information received from that destination. This is the original sequence number assigned by the destination.

# An Example of Route Update



- At the start, each node gets route updates only from its neighbour.
- For **n4**, the distances to the other nodes are :  
**n5=1, n3=1, n2=  $\infty$**   
**n1 =  $\infty$**
- All nodes broadcast with a sequence number **1**

# An Example of Route Update



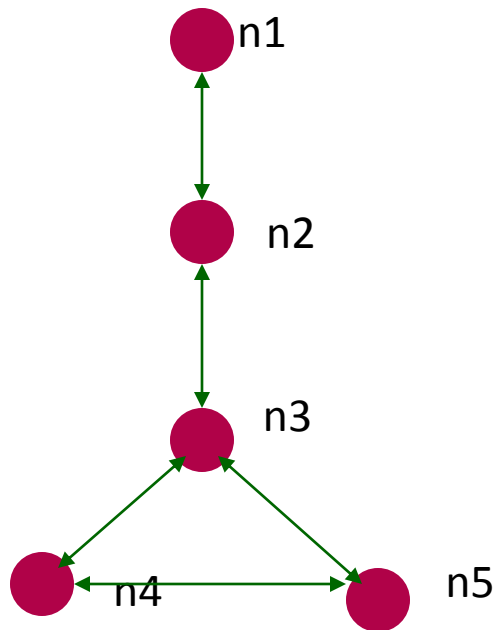
- After this, nodes forward messages that they have received earlier.
- The message that **n2** sent to **n3** is now forwarded by **n3**
- For **n4**, the distances are now :

**n5=1, n3=1, n2=2, n1=  $\infty$**

All messages have sequence number **1**



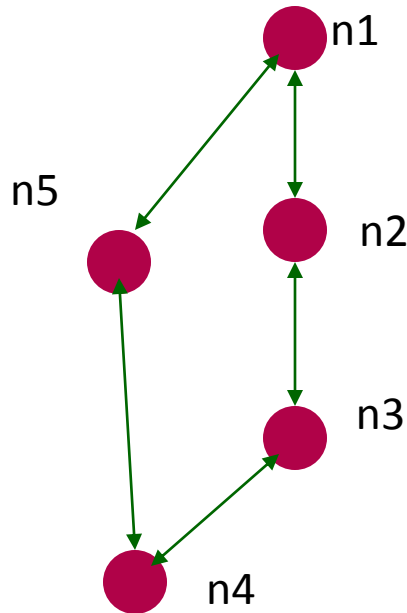
# An Example of Route Update



- Finally, after second round of forwarding, **n4** gets the following distances :

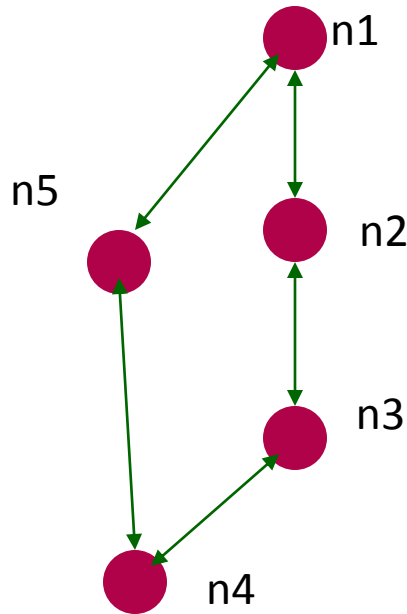
**n5=1, n3=1, n2=2, n1=3**

# An Example of Route Update



- Suppose **n5** has moved to its new location.
- Also, **n5** receives a new message from **n1** with a sequence number **2**
- This message is forwarded by **n5** to **n4**
- Two distances to **n1** in **n4**

# An Example of Route Update



- Distance **3** with sequence number **1**, and
- Distance **2** with sequence number **2**
- Since the latter message has a more recent sequence number, **n4** will update the distance to **n1** as **2**

## AD-HOC NETWORK ROUTING PROTOCOLS

### PROACTIVE ( table driven) ROUTING PROTOCOLS-

Each node in the network has routing table for the broadcast of the data packets and want to establish connection to other nodes in the network. These nodes record for all the presented destinations, number of hops required to arrive at each destination in the routing table.

The routing entry is tagged with a sequence number which is created by the destination node. To retain the stability, each station broadcasts and modifies its routing table from time to time.

How many hops are required to arrive that particular node and which stations are accessible is result of broadcasting of packets between nodes.

Each node that broadcasts data will contain its new sequence number and for each new route, node contains the following information:

- 1 – How many hops are required to arrive that particular destination node
- 2 – Generation of new sequence number marked by the destination
- 3 – The destination address

The proactive protocols are appropriate for less number of nodes in networks, as they need to update node entries for each and every node in the routing table of every node. It results more Routing overhead problem. There is consumption of more bandwidth in routing table..

Example of Proactive Routing Protocol is Destination Sequenced Distance Vector (DSDV).

### REACTIVE ( On Demand) ROUTING PROTOCOL-

Reactive Protocol has lower overhead since routes are determined on demand. It employs flooding (global search) concept. Constantly updation of route tables with the latest route topology is not required in on demand concept.

**Reactive** protocol searches for the route in an on-demand manner and set the link in order to send out and accept the packet from a source node to destination node. Route discovery process is used in on demand routing by flooding the route request (**RREQ**) packets throughout the network.

Examples of reactive routing protocols are the dynamic source Routing (DSR), and on-demand distance vector routing (AODV).

### DESTINATION SEQUENCE DISTANCE VECTOR (DSDV) ROUTING PROTOCOL-

The Destination-Sequenced Distance-Vector (DSDV) Routing Algorithm is based on the idea of the classical Bellman-Ford Routing Algorithm. Routing Loop problem is solved which is present in Bellman-Ford algorithm. To solve the routing loop problem, this routing makes use of sequence numbers.

Each mobile node maintains a routing table that includes the number of hops to reach the destination, all available destinations and the sequence number tagged by the destination node. The sequence number is used to distinguish stale routes from new ones and thus avoid the formation of loops. So, the update is both time-driven and event-driven. A "full dump" or an incremental update technique is used to update the routing table.

A full dump sends the full routing table to the neighbors and could span many packets whereas in an incremental update only those entries from the routing table are sent that has a metric change since the last update and it must fit in a packet. When the network is relatively stable, incremental updates are sent to avoid extra traffic and full dump are relatively infrequent. If there is space in the incremental update packet then those entries may be included whose sequence number has changed. DSDV protocol guarantees loop free paths and Count to infinity problem is reduced in DSDV.

### DYNAMIC SOURCE ROUTING PROTOCOL (DSR)

DSR uses source routing concept. When packets are flooded by a source node, the sender node caches complete hop-by-hop route to the receiver node. These route lists are caches in a *route cache*.

The data packets carry the source route in the packet header. DSR uses Route Discovery process to send the data packets from sender to receiver node for which it does not already know the route, it uses a **route discovery** process to dynamically determine such a route. In Route discovery DSR works by flooding the data packets in network with **route request (RREQ)** packets.

RREQ packets are received by every neighbor nodes and continue this flooding process by retransmissions of **RREQ** packets, unless it gets destination or its route cache consists a route for destination. Such a node replies to the RREQ with a **route reply (RREP)** packet that is routed back to real source node. source routing uses RREQ and RREP packets.

The RREQ builds up the path traversed across the network. The RREP routes itself back to the source by traversing this path toward the back. The source caches backward route by RREP packets for upcoming use. If any connection on a source route is wrecked, a *route error* (RERR) packet is notified to the source node.

### ADHOC ON DEMAND DISTANCE VECTOR ROUTING (AODV)-

AODV uses a very special technique to maintain routing information. AODV protocol is both an on-demand and a table-driven protocol. It adopts flat routing tables, one entry per destination.

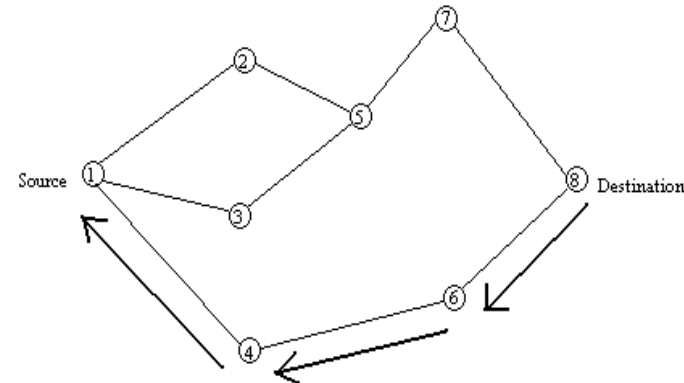
It is in difference to DSR, which can maintain multiple route cache entries for every one destination.

Unlike DSR The packet size in AODV is uniform. In AODV there is no need for system-wide broadcasts due to local changes, unlike DSDV. AODV has multicasting and uncasing routing protocol property within a uniform framework. *Source node, destination node and next hops* are addressed using *IP addressing*. AODV builds routes using a *route request /route reply cycle*.

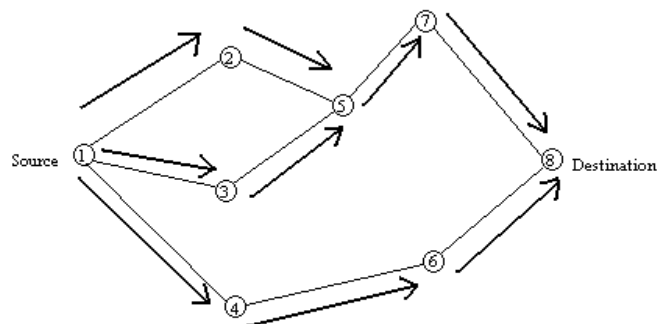
To determine freshness of routing information and to prevent routing loops, AODV uses sequence numbers maintained at each destination. Sequence number for both destination and source are used. These sequence numbers are carried by all routing packets. Maintenance of timer-based states in each node, regarding use of individual routing table entries is an important feature of AODV. If routing table entry is not used recently then routing table entry is *expired*.

When the next-hop link breaks nodes are notified with RERR packets. Each predecessor node, forwards the RERR to its own set of predecessors, thus effectively erasing all routes using the broken link.. Route error propagation in

AODV can be visualized conceptually as a tree whose root is the node at the point of failure and all sources using the failed link as the leaves. It is loop free, self starting, and scales to large numbers of mobile nodes.



(b) Path taken by the Route Reply (RREP) Packet



(a) Propagation of Route Request (RREQ) Packet

**CS2402 MOBILE AND PERVASIVE COMPUTING**  
**2 MARKS QUESTION AND ANSWER**  
**Unit –IV**

**1.What are the three Low Power States provided by Bluetooth?**

PARK state HOLD state SNIFF state

**2.What is SCO?**

SCO-stands for Synchronous Connection Oriented Link Standard telephone (voice) connection require symmetrical, circuit-switched, point-topoint connections. For this type of link, the master reserves two consecutive slots at fixed intervals.

**3.What are the three phases in EY-NPMA?**

i. Prioritization: Determine the highest priority of a data packet ready to be sent on competing nodes. ii. Contention: Eliminate all but one of the contenders, if more than one sender has the highest current priority. iii. Transmission: Finally, transmit the packet of the remaining node.

**4. What are the system integration functions of MAC management?**

• Synchronization • Power management • Roaming • Management information base (MIB)

**5. What do you meant by roaming?.**

Moving between access point is called roaming. Even wireless networks may require more than one access point to cover all rooms. In order to provide uninterrupted service, we require roaming when the user moves from one access point to another.

**6. What is mobile routing?**

Even if the location of a terminal is known to the system, it still has to route the traffic through the network to the access point currently responsible for the wireless terminal. Each time a user moves to a new access point, the system must reroute traffic. This is known as **mobile** routing.

**7. What are the functions which support service and connection control?**

Access point control function  
Call control and connection control function  
Network security agent  
Service control function  
Mobility management function

**8. What are the examples for service scenarios identified in WATM ?**

Office environments

Universities, schools, training, centers  
Industry  
Hospitals  
Home  
Networked vehicles

### **9. What is BRAN?**

The broadband radio access networks(BRAN) which have been standardized by European Telecommunications Standard Institute(ETSI) are a possible choice for an RAL for WATM. Although BRAN has been standardized independently from WATM, there is co-operation between the two to concentrate the common efforts on one goal. The main motivation behind BRAN is the deregulation and privatization of the telecommunication sector in Europe.

### **10. What are the different network types of BRAN?**

Hyperlan1  
Hyperlan2  
Hyper access  
Hyperlink

### **11. What is the main problem for WATM during handover?**

The main problem for WATM during the handover is rerouting of all connections and maintaining connection quality.

### **12. What are the different segments in ATM end-to-end connection?**

An ATM end-to-end connection is separated into different segments. A fixed segment is a part of the connection that is not affected by the handover . Handover segment is affected by the handover and is located completely within a handover domain.

### **13. What is anchor point?**

The Anchor point is the boundary between a handover segment and a fixed segment.

### **14. What are different types of handover?**

Hard handover  
Terminal initiated  
Network initiated  
Network initiated, terminal assisted  
Network controlled  
Backward handover  
Forward handover the extended TCP is called SCPS-transport protocols.(SCPS-TP).

### **15) What are Advantage and Disadvantage of Mobile TCP?**

**Advantages:** i. M-TCP maintains the TCP end-to-end semantics. The SH does not send any ACK itself but forwards the ACKs from the MH. ii. If the MH is disconnected, M-TCP avoids useless retransmissions, slow starts or breaking connections by simply shrinking the sender's window to 0; iii. Since M-TCP does not buffer data in the SH as I-TCP does, it is not necessary to forward buffers to a new SH. Lost packets will be automatically retransmitted to the new SH.

**Disadvantages:** i. As the SH does not act as proxy as in I-TCP, packet loss on the wireless link due to bit errors is propagated to the sender. M-TCP assumes low bit error rates, which is not always a valid assumption. ii. A modified TCP on the wireless link not only requires modification to the MH protocol software but also new network elements like the bandwidth manager.

### **16) What is mobile routing?**

Even if the location of a terminal is known to the system, it still has to route the traffic through the network to the access point currently responsible for the wireless terminal. Each time a user moves to a new access point, the system must reroute traffic. This is known as mobile routing.

### **17) What are the functions which support service and connection control?**

Access point control function  
Call control and connection control function  
Network security agent > Service control function  
Mobility management function

### **18) What are the examples for service scenarios identified in WATM ?**

Office environments  
Universities, schools, training, centres  
Industry  
Hospitals  
Home  
Networked vehicles

### **19) What are the different segments in ATM end-to-end connection?**

An ATM end-to-end connection is separated into different segments. > A fixed segment is a part of the connection that is not affected by the handover > Handover segment is affected by the handover and is located completely within a handover domain.

### **21) What is anchor point? .**

The Anchor point is the boundary between a handover segment and a fixed segment.



**22) What is mobile terminal and wireless terminal?.**

Mobile terminal is a standard ATM terminal with the additional capability of reconnecting after access point change. the terminal can be moved between different access point within a certain domain. Wireless terminal is accessed via a wireless link, but the terminal itself is fixed, i.e., the terminal keeps its access point to the network.

**23) What is generic routing encapsulation?**

Generic routing encapsulation (GRE) is an encapsulation scheme which supports other network protocols in addition to IP. It allows the encapsulation of packets of one protocol suite into the payload portion of a packet of another protocol suite.

**24) Define COA.**

The COA (care of address) defines the current location of the MN from an IP point of view. All IP packets sent to the MN are delivered to the COA, not directly to the IP address of the MN. Packet delivery toward the MN is done using the tunnel.

**25) What is meant by Transparency?**

Mobility should remain invisible for many higher layer Protocols and applications. The only affects of mobility should be a higher delay and lower bandwidth which are natural in the case of mobile networks.

**26) What is Generic Routing encapsulation?**

Generic Routing encapsulation (GRE) allows the encapsulation of packets of one protocol suite into the payload portion of a packet of another protocol suit.

**27)What is Binding Request?**

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

**28) What are the possibilities for the location of care-of-address (COA)?**

The two possibilities for the location of care-of-address are: i.Foreign agent COA ii.Co-related COA

**29) What are the requirements for the development of mobile IP standard?**

The requirements are: a.Compatibility b.Transparency c.Scalability and efficiency d.Security

**30) What is Dynamic source Routing?**

Dynamic Source Routing eliminates all periodic routing updates. If a node needs to discover a route, it broadcast a route request with a unique identifier and the destination address as parameters. Any node that receives a route request gives a list of addresses representing a possible path on its way toward the destination.

**31) Why is need of routing?**

Routing is to find the path between source and destination and to forward the packets appropriately.

**32) Define Mobile node:**

A mobile node is an end-system or router that can change its point of attachment to the Internet using mobile IP. The MN keeps its IP address and can continuously with any other system in the Internet as long as link layer connectivity is given.

**PART – B (16 MARKS) UNIT IV**

1. a. What are the requirements of a mobile IP? (8)  
b. Describe Dynamic host configuration protocol. (8)
2. a. Discuss the routing algorithm in ad-hoc network (8)  
b. What are the entities in mobile IP? (8)
3. a. Discuss how optimization in achieved in mobile IP (8).  
b. Explain tunneling and encapsulation in mobile IP. (8)
4. .Explain how dynamic source routing protocols handles routing with an example (16)

## **Introduction**

*Pervasive Computing* is a technology that pervades the users' environment by making use of multiple independent information devices (both fixed and mobile, homogeneous or heterogeneous) interconnected seamlessly through wireless or wired computer communication networks which are aimed to provide a class of computing / sensory /communication services to a class of users, preferably transparently and can provide personalized services while ensuring a fair degree of privacy / non-intrusiveness. It may also be seen as the as *the technology* that is a combination of Personal computing technology *and* one or more of the following:

- Internetworking technology
- Invisible computing technology
- Wearable computing technology
- Mobile Computing Technology

### **1.1 Elements of Pervasive Computing Systems**

Components of Infrastructure for Pervasive Computing include Mobile computing devices, Fixed computing devices, Multimode RF Mobile communication infrastructure

*<Fixed-to-Mobile and Mobile-to-Fixed communication system interfaces>*, Trust system (*security and privacy*), Protocol stacks and Personalized service frameworks. What should the Infrastructure provide?

- Pervasive Computing Infrastructure has to comprise of computing elements, communicating elements, sensors, actuators, and interface devices.

- Computation to be available widely and freely (not free of cost).

- Intermittent connectivity has to be a supported feature due to physical limitations pertaining to power, cost, bandwidth and network congestion.

- Bluetooth and other choices address small-distance networking issues and allow intermittent connection.

- The infrastructure has to offer seamless connectivity to the devices /entities / services.

- It has to support placement and location of uniquely identifiable “information tags / track able tags” to all devices / entities in the Pervasive Computing environment.

- User’s environment must be able to be aware of the user’s context.

Roaming Environment: An environment that allows connectivity and communication to the services outside the home zone is called a Roaming Environment.

Some sample devices that may involve Roaming-based access <fixed / mobile roaming>:

- PDAs / Palmtops / Pocket PCs / Cell phones / Smart phones / WAP Phones
  - Laptops / Tablet PCs / Notebook PCs
  - Desktop PCs / Servers / Web TVs
  - Kiosks
  - Invisible computing devices / Smart interactive posters
  - Wearable computers
- 1.2 Pervasive Computing Devices

Basic Aspects Device Technology for Pervasive Computing include Power-provisioning technologies, Display technologies, Memory technologies, Communication technologies, Processor technologies, Interfacing technologies, Sensor Technologies and Authentication Technologies.

**Technology Aspects Low-power Device Technologies** Since many of the devices involved in the pervasive computing environment may have to be small in size and may have to live on their battery / power units, consumption of lower power, extension of power provisioning period etc. assume critical significance. In addition, prevention from excessive heating also requires attention. Power requirements can be reduced by several means right from material selection and chip-level designing to software designing and communication system designing. Power provisioning technology including the Battery design technology plays a very important role in the process.

**Batteries as Power Provisioning Devices**

- Key issue: Size and weight of the batteries versus the power capacity and price
- Bottleneck: Relatively slower advances in the battery technology compared to those in other fields like display and storage technologies
- Major choices available: Nickel-Cadmium (NiCd: 12-27 hrs. standby time), Nickel-Metal-Hydride (NiMH: 16-37 hrs. standby time), Lithium-Ion (Li-ion: 21-50 hrs. standby time), Lithium-Polymer Cell based batteries (> 60 hrs. standby time, flexible shapes) etc.

**Display Device Technologies** Not all pervasive computing devices need display elements but those needing them may have a range of different requirements in terms of: – Display-size – Display-shape – Display-resolution – Display-colour richness – Display viewing angles to be supported – Display power provisioning constraints – Display refresh rates etc.

**Major Display Device Technologies**

- Cathode Ray Tube

based Displays (CRTs) •Liquid Crystal Displays (LCDs) Active Matrix Displays  
§Thin Film Transistor Displays (TFTs) Passive Matrix displays §Single Scan  
Displays (Colour Super-Twist Nematic: CSTNs) §Dual Scan Displays (Dual  
Super-Twist Nematic: DSTN) §High-Performance Addressing displays (HPAs)  
•Light Emitting Diode based Displays (LEDs)

Organic LED based Displays (OLEDs)

Light-Emitting Polymer based Displays (LEPs)

- Chip-on-Glass Displays (CoGs)
- Liquid Crystal on Glass Displays (LCoGs)

Connectivity Aspects Role of communication architectures in pervasiveness

- The pervasive computing system needs at least two basic elements to be pervading everywhere they are required to pervade: O Computing elements to take care of computational needs; and, O Communication elements to interconnect these computing elements either through wires or wirelessly (with / without mobility).

- From the end user's perspective and in many a practical situations, the wireless communication based mobile computing is becoming increasingly important.

- From the back-end systems' viewpoint, however, due to its sheer traffic volume, low error rates, better noise immunity and low cost, the wire line communication based computing still remains an attractive option.

- Therefore, hybrid architectures will possibly continue to exist even though end users may not be even aware of it. Identifying multi-technology mobile communication architectures of relevance

- Several generations

- Gradual enhancements

- Coexistence & transition Generations of Wireless Communication Networking Standards

- First Generation Global Mobile Radio standard : 1G Only voice, No data

- Second Generation Global Mobile Radio standard : 2G oGSM:9.6 Kbps <circuit switched voice / data> O Enhanced Second Generation Global Mobile Radio standard : 2.5G§GSM-GPRS <combination of circuit and packet switched voice / data> §GPRS-136: <100Kbps <packet switched>

- Third Generation Global Mobile Radio standard: 3G oCDMA2000,=< 2Mbps <packet switched voice / data>

- Fourth Generation Global Mobile Radio standard : 4G (near future) 20-40 Mbps <packet switched voice / data> Inside the GSM Network Subsystem



- MSC (Mobile Services Switching Center) acts like a normal switching node and provides the connection to the fixed networks (such as the PSTN or ISDN).

- HLR (Home Location Register ) contains information of each subscriber registered in the corresponding GSM network, along with the current location of the mobile. There is logically one HLR per GSM network

- VLR (Visitor Location Register) contains selected information from the HLR, necessary for call control and provision of the subscribed services and each mobile currently located in the geographical area controlled by the VLR.

- EIR (The Equipment Identity Register) is a database that contains a list of all valid mobile equipment on the network,

- AuC (The Authentication Center) is a protected database: secret key of SIM

GSM uses TDMA/FDMA to share the limited radio spectrum wherein the FDMA part divides frequency of the not more than 25 MHz B/W into 124 carrier frequencies spaced 200 kHz apart.; and Each of these carrier frequencies is then divided in time, using a TDMA scheme. GSM is a circuit-switched digital network. SGSN (the Serving GPRS Support Node) keeps track of the location of the mobile within its service area and send/receive packets from the mobile , passing them on, or receiving them from the GGSN. GGSN (Gateway GPRS Support Node) converts the GSM packets into other packet protocols (e.g. IP /X.25) and sends them out into another network.

- GPRS users can share the resource (Radio link) which is used only when users are actually sending or receiving data.

- GPRS is based on GMSK which is a modulation technique known as Gaussian minimum-shift keying. It can support a theoretical upper limit of speed up to 171.2kbps as against the GSM „s9.6Kbps.

- In GPRS, a channel that is 200kHz wide, is divided into 8 separate data streams, each carrying maximum 20kbps(14.4kbps typical) whereas in GSM we use only one channel.

The 3G:

- 3G Stands for the Third Generation,
- Used in the context of new wireless mobile communication systems /services,
- Leverages the progress made in cellular technologies with the advances made in the Internet-based communication / services and the fixed wire line communication technologies,
- Is a general-purpose communication network / service architecture,
- Allows freedom to end users from being aware of location of request /provision of services,

- Puts more emphasis on the services than on the underlying delivery technologies,
- Aims to play a key role in aiding the On-Demand service paradigm.

- Is not a single -technology architecture; instead allows a multi-technology solution. Processor technologies

- Intel's SpeedStep processor technology Intel's Speedstep™ technology based processors and their successors are capable of:

- Changing the internal clock frequencies
- Adapting core voltage to changes in power supply
- Switching of selective parts of the CPU cores / CPU on or off depending on whether the current calculations require them to be available

- Using the reduced the clock rate and voltage of the processor core while on batteries, leading to significant power saving.

- Switching between these modes is transparent to user and is usually fast <however, while the system is connected to external power supply, the full clock rate and core voltage is available to processor resulting into maximum performance>

- Transmeta's Crusoe processor technology
- Total number of transistors are reduced in an attempt to save the power consumption

- Software replaces the functionalities which otherwise would have been provided in hardware by the eliminated set of transistors

- Software dynamically translates the original instructions into another set of instruction for the processor

- A technology called LongRun™ reduces the power consumption even more by reducing the processor's voltage on the fly when processor is idle

- Motorola's Dragon Ball processor technology

- Deprecated now!

- Intel's X-Scale processor technology

- This is next generation of ARM-processors that have replaced the Intel StrongARM series Memory Technologies

- Register class elements

- Cache memory elements

- Primary Memory elements

RAM

SRAM

DRAM

Ut-RAM

MRAM

FRAM

MBM

ROM

- Secondary Memory

Flash Disks

Magnetic Disks

Optical Disks

Magenta-Optical Storages

Magnetic Tape Storage

## **1.2 Operating System Aspects**

Operating Systems for Pervasive Computing Environments

- Types of Operating Systems

Classification based on location of functionalities:

Centralised Ses

Networked Ses

Distributed Ses

Support for security through full encryption and certificate management, secure protocols (HTTPS, SSL and TLS), WIM framework and certificate-based application installation o Support for content development options for C++, Java (J2ME) WAP etc.; Support for variety of user inputs – generic input mechanism

supporting full keyboard, 0-9\*# (numeric mobile phone keypad), voice, handwriting recognition and predictive text input.

- Variants of Microsoft Windows O Windows XP Embedded O WinCE

Memory management:

Support for protected Virtual Memory Management (upto 32 MB per process), special heap-support for File System / Registry / Object Store <max. size of Object Store:256 MB>

**Security:** Support for cryptography with a Crypto Library+ Crypto API, support for SD and Smart Cards

**Footprint:** About 400 kb for the OS Core / Kernel §About 3 MB with Kernel + all modules About 8 MB with Kernel + all modules + MS Word / PowerPoint / IE etc.

**User-interface:** Simple, intuitive, generally consistent, Menu-driven, Iconic

**User management:** Designed for single user support only

**Energy-awareness aspects:** Support for energy-saving enabled at the kernel level

- Variants of Linux ARM -Linux BlueCat Embedded Linux RT-Linux

- PalmOS

- QNX Neutrino

- Variants of JavaOS

JavaOS Java for Business

- BeOS Major constraints specific to recognition accuracy of Speech Recognition Systems as components of pervasive computing environment:
- Resource availability in terms of processing power, memory and available time for each instance of recognition
- Complexity due to isolated and continuous recognition needs,
- Secondary storage's capability to store required supporting data affecting dictionary and other data
- Context-variance implications
- Complexity arising out of Speaker-dependent and Speaker-independent device requirements
- Extent of training needed and its regulation
- Security and other implications

### **1.3 Interfacing Aspects**

Interfacing technologies Respective significance of Fitaly, Tegic T9, Octave methods of keyboards vis-à-vis traditional QWERTY layout based keyboards / keypads, in the context of mobile handheld devices: §Fitaly: •Merit / Significance: Speeds up input of text, letters selected as per likely occurrence frequencies and ensuring minimization of inter-letter travel distance (to no more than 2 positions), supports 220 ANSI/ISO Latin- 1 character set, supports accents, available in on-screen as well as mechanical forms

•**Demerit:** Specific to English language's estimated usage patterns, needs to be practiced for a while before use, needs to learn „sliding“ for accents' use etc.  
§Tegic T9:

•**Merit / Significance:** Requires lesser number of keystrokes for textual input due to support for predictive text by combining use of dictionary and linguistic rules' embedding, resolution of word-ambiguity is supported through prompts, available in on-screen as well as mechanical forms

•**Demerit:** Requires sizeable software support and computing resources (instruction cycles and memory)

#### **Octave:**

•**Merit / Significance:** Commands available to support multiple language dictionaries, available in on-screen as well as mechanical forms although second form is more popular, gesture-based iconic support for certain insertions, word-recognition supported by dictionary, ability to resolve stroke-ambiguity with the help of dictionary

•**Demerit:** Requires sizeable software support and computing resources (instruction cycles and memory)

#### **Traditional QWERTY:**



•**Merit / Significance:** Simplicity in design and use, available in on-screen as well as mechanical forms •**Demerit:** Requires more space and may be difficult in use in case of devices with very small form-factor Major Interfacing technologies:

- Navigation technologies
- Haptic interfacing technologies
- On-screen / Touch-panel technologies
- Voice interfacing technologies
- Video-interfacing technologies
- Handwriting-based interfacing technologies
- Hybrid interfacing technologies)