MOBILE COMPUTING

The terms mobile and wireless as used throughout the mobile computing should be defined. There are two different kinds of mobility 1.user mobility 2. Device portability

User mobility: it refers to a user who has access to the same or similar telecommunication services at different places. i.e. the user can be mobile and the services will follow him/her.

Divice portability: the communication device moves (with/without a user). Many machanisms in the network and inside the device have to make sure that communication is still possible while the device is moving where the system itself hands the device from one radio transmitter to the next if the signal becomes too weak.

Most of the scenarios described in this contains both user mobility and device portability at the same time.

With this regard to devices the term wireless is used this only describes the way of accessing and network or other communication partners i.e. without a wire. The wire is replaced by transmission of electromagnetic waves through the air(although wireless transmission doesn't need any medium)

A communication device can exhibit one of the following characteristics

1. **fixed and wired:**

This configuration describes the typical desktop computers in an office neither weight nor power consumption of the devices allow for mobile usage. These devices use fixed networks for performance reasons.

2. **Mobile and wired:**

Many of today's laptops will fall into this category. user's can carry the laptop from one hotel to the next reconnecting to the companies network via telephone network and a modem

3. **Fixed and wireless:**

This mode is used for installing networks Eg. historical buildings to avoid damage by installing wires.

4. **mobile and wireless:**

This is the most interesting case. No cable restricts the user who can roam between different wireless networks. Most technologies discuss in this deal with this type of device and networks supporting them.

Mobile computing technology:

Mobile Computing is a technology that allows transmission of data, voice and video via a computer or any other wireless enabled device without having to be connected to a fixed physical link. The main concept involves −

- Mobile communication
- Mobile hardware
- Mobile software

Mobile communication

The mobile communication in this case, refers to the infrastructure put in place to ensure that seamless and reliable communication goes on. These would include devices such as protocols, services, bandwidth, and portals necessary to facilitate and support the stated services. The data format is also defined at this stage. This ensures that there is no collision with other existing systems which offer the same service.

Since the media is unguided/unbounded, the overlaying infrastructure is basically radio wave-oriented. That is, the signals are carried over the air to intended devices that are capable of receiving and sending similar kinds of signals.

Mobile Hardware

Mobile hardware includes mobile devices or device components that receive or access the service of mobility. They would range from portable laptops, smartphones, tablet Pc's, Personal Digital Assistants.

These devices will have a receptor medium that is capable of sensing and receiving signals. These devices are configured to operate in full- duplex, whereby they are capable of sending and receiving signals at the same time. They don't have to wait until one device has finished communicating for the other device to initiate communications.

Above mentioned devices use an existing and established network to operate on. In most cases, it would be a wireless network.

Mobile software

Mobile software is the actual program that runs on the mobile hardware. It deals with the characteristics and requirements of mobile applications. This is the engine of the mobile

device. In other terms, it is the operating system of the appliance. It's the essential component that operates the mobile device.

Since portability is the main factor, this type of computing ensures that users are not tied or pinned to a single physical location, but are able to operate from anywhere. It incorporates all aspects of wireless communications

In today's computing world, different technologies have emerged. These have grown to support the existing computer networks all over the world. With mobile computing, we find that the need to be confined within one physical location has been eradicated. We hear of terms such as telecommuting, which is being able to work from home or the field but at the same time accessing resources as if one is in the office..

The advent of portable computers and laptops, Personal Digital Assistants (PDA), PC tablets and smartphones, has in turn made mobile computing very convenient. The portability of these devices ensure and enable the users to access all services as if they were in the internal network of their company. For example, the use of Tablet PC and iPads. This new technology enables the users to update documents, surf the internet, send and receive e-mail, stream live video files, take photographs and also support video and voice conferencing.

The constant and ever increasing demand for superior and robust smart devices has been a catalyst for market share. Each manufacturer is trying to carve a niche for himself in the market. These devices are invented and innovated to provide state-of-the-art applications and services. For instance, different manufacturers of cellular phones have come up with unique smartphones that are capable of performing the same task as computers and at the same processing speed. The market share for different competitors is constantly being fought for. For example, the manufacturers of Apple's iPhone OS, Google's Android' Microsoft Windows Mobile, Research In Motion's Blackberry OS, are constantly competing to offer better products with each release.

The need for better, portable, affordable, and robust technology has made these vendors to constantly be innovative. Market figure and statistics show an ever growing need to purchase and use such devices for either professional or personal use. It is in this light that services to suit long-term implementation are developed or innovated. It has also pushed other industry vendors to adopt services that will provide better services. For example, cellular service providers are forced to improve and be innovative to capture more subscribers. This can be in terms of superior services such as high speed internet and data access, voice and video service etc. Hence the adoption of different generations of networks like of 2G, 2.5G, 3G, 4G network services.

The essence of mobile computing is to be able to work from any location. The use of iPads, tablets, smartphones, and notebooks, have pushed the demand for these devices. Modern day workers have such devices that enable them to carry out their work from the confines of their own location. These devices are configured to access and store large amounts of vital data. Executive and top management can take decisions based on ready information without going to the office. For example, sales reports and market forecasts can be accessed through these devices or a meeting can take place via video or audio conferencing through these devices. With such features being high in demand, manufacturers are constantly coming up with applications geared to support different services in terms of mobile computing

Applications of Mobile Computing

Mobile working infrastructure can deliver real time business benefits, companies of all sizes are walking up to the fact that they can improve productivity and increase profits by giving employees remote access to mission critical corporate IT system. The importance of Mobile Computers has been highlighted in many fields of which a few are described below:

1. For Estate Agents:

Estate agents can work either at home or out in the field. With mobile computers they can be more productive. They can obtain current real estate information by accessing multiple listing services, which they can do from home, office or car when out with clients. They can provide clients with immediate feedback regarding specific homes or neighborhoods, and with faster loan approvals, since applications can be submitted on the spot. Therefore, mobile computers allow them to devote more time to clients.

2. Emergency Services:

Ability to receive information on the move is vital where the emergency services are involved. Information regarding the address, type and other details of an incident can be dispatched quickly, via a Cellular Digital Packet Data (CDPD) system using mobile computers, to one or several appropriate mobile units, which are in the vicinity of the incident.

3. In courts:

Defense counsels can take mobile computers in court. When the opposing counsel references a case which they are not familiar, they can use the computer to get direct, real-time access to on-line legal database services, where they can gather information on the case and related precedents. Therefore mobile computers allow immediate access to a wealth of information, making people better informed and prepared.

4. In companies:

Managers can use mobile computers in, say, critical presentations to major customers. They can access the latest market share information. At a small recess, they can revise the presentation to take advantage of this information. They can communicate with the office about possible new offers and call meetings for discussing responds to the new proposals. Therefore, mobile computers can leverage competitive advantages.

5. Credit Card Verification:

At Point of Sale (POS) terminals in shops and supermarkets, when customers use credit cards for transactions, the intercommunication is required between the bank central computer and the POS terminal, in order to effect verification of the card usage, can take place quickly and securely over cellular channels using a mobile computer unit. This can speed up the transaction process and relieve congestion at the POS terminals.

Limitations of mobile computing:

1. Insufficient Bandwidth:

Mobile Internet access is generally slower than direct cable connections, using technologies such as GPRS and EDGE, and more recently 3Gnetworks. These networks are usually available within range of commercial cell phone towers. Higher speed wireless LANs are inexpensive but have very limited range.

2. Security Standards:

When working mobile, one is dependent on public networks, requiring careful use of Virtual Private Network (VPN). Security is a major concern while concerning the mobile computing standards on the fleet. One can easily attack the VPN through a huge number of networks interconnected through the line.

3. Power consumption:

When a power outlet or portable generator is not available, mobile computers must rely entirely on battery power. Combined with the compact size of many mobile devices, this often means unusually expensive batteries must be used to obtain the necessary battery life.

4. Transmission interferences:

Weather, terrain, and the range from the nearest signal point can all interfere with signal reception. Reception in tunnels, some buildings, and rural areas is often poor.

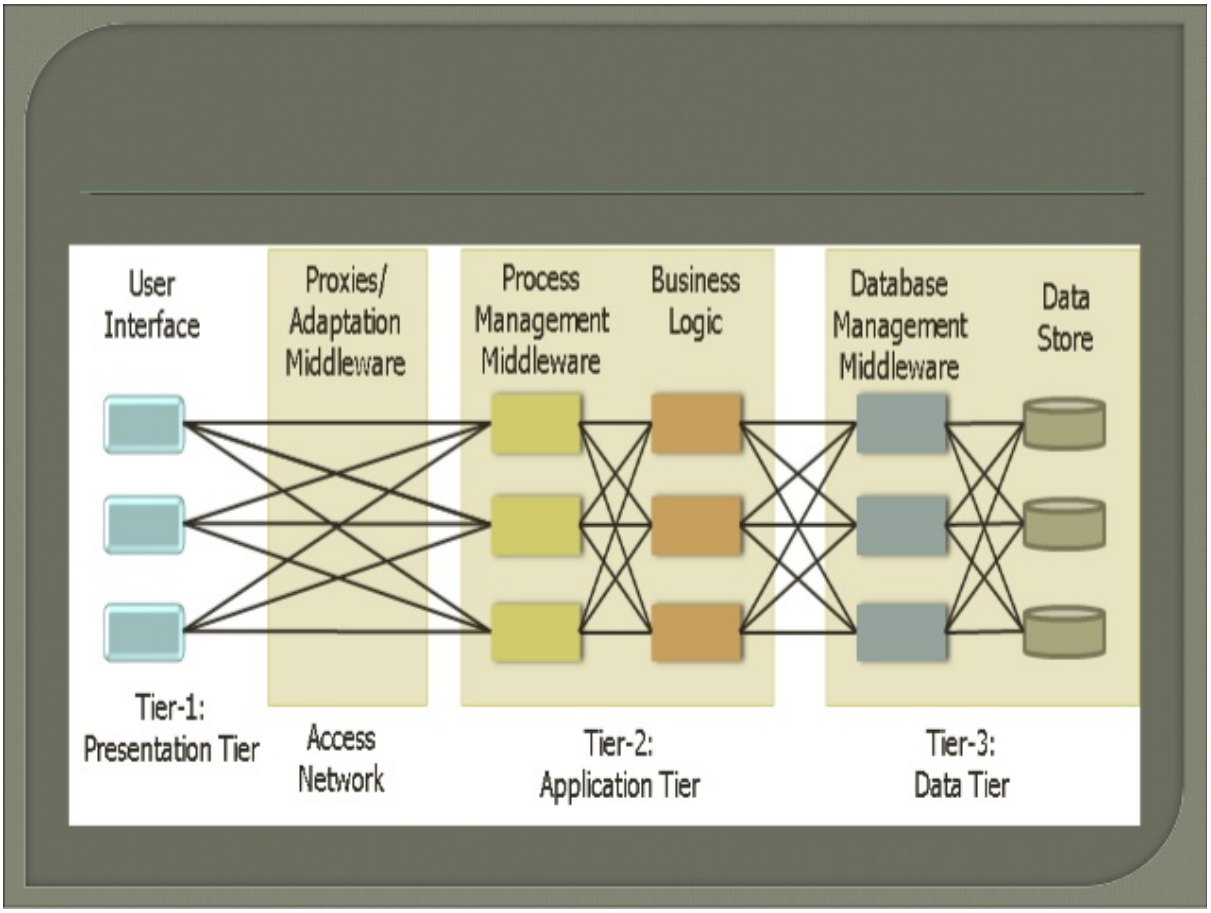
5. Potential health hazards:

People who use mobile devices while driving are often distracted from driving are thus assumed more likely to be involved in traffic accidents. Cell phones may interfere with sensitive medical devices. There are allegations that cell phone signals may cause health problems.

6. Human interface with device:

Screens and keyboards tend to be small, which may make them hard to use. Alternate input methods such as speech or handwriting recognition require training.

Mobile computing Architecture:



GSM :

Gsm is the most successful digital mobile telecommunication system in the world today it is used by over 800 million people more than 180 countries with different carrier frequencies. The primary goal of gsm is to provide mobile phone system that allows users to roam throughout Europe and provides voice services compatible to ISDN and other PSTN systems. Gsm standardization aims at adopting as much as possible.

Mobile Services:

Gsm permits the integration of different voice and data services and interworking with existing networks. A mobile station MS is connected to the gsm public land mobile network (PLMN) via the Um interface(GSM PLMN is the infrastructure needed for the GSM network and this is connected to transit network). There might be an additional network, the source/destination network before another terminal TE is connected. Interfaces like U,S and R in case of ISDN have not been defined for all networks so, it depends on the specific network which interface is used as a reference for the transparent transmission of data.

Within the mobile station MS the mobile termination MT performs all network specific task and offers and interface for data transmission to the terminal TE. Depending on the capabilities of TE further interfaces may be needed.

Gsm as defined three different categories of services

1. **Bearer services :**

Bearer services now comprise all services that enable the transparent transmission of data between the interfaces to the network. These services permit transparent and non transparent, synchronous or asynchronous data transmission. Transparent bearer services only use the functions of physical layer to transmit data. Data transmission has a constant delay and throughput if no transmission error occurs. the only mechanism to increase transmission quality is the use of forward error correction FEC which codes redundancy into the data string and helps to reconstructs the original data in case of transmission errors. Transparent bearer services do not try to recover lost data.

Non transparent use protocols of layers two and three to implement error correction and flow control. These services use the transparent bearer services adding a radio link protocol RLP. Data transmission can be full- duplex, synchronous with data rates of 1.2, 2.4, 4.8, 9.6 k bits/s or full- duplex, asynchronous from 300-9600 bits/s.

2. **Tele services:**

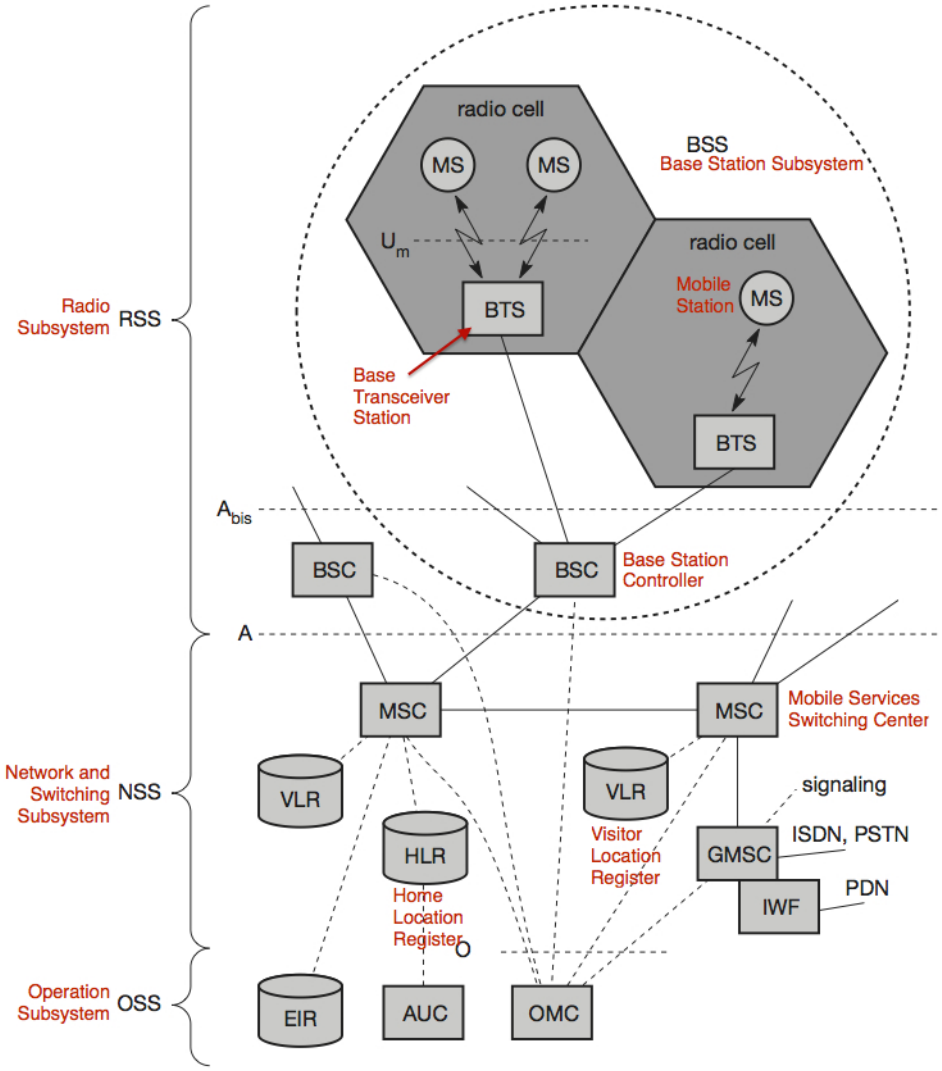
GSM mainly focuses on voice oriented tele-services. These comprises encrypted voice transmission, message services and basic data communication with terminals as known from PSTN /ISDN as the main service is telephony the primary goal of GSM was the provision of high quality digital voice transmission offering at least the typical bandwidth of 3.1 kHz of analog phone systems. Special codecs (coder/decoder) are used for voice transmission while other codecs are used for transmission of analog data for communication with traditional computer modems eg. Fax machine.

Another service offered by GSM is the emergency number. The same number can be used throughout the Europe. This service is mandatory for all providers and free of charge. A useful service for very simple message transfer is the short message service (SMS), which

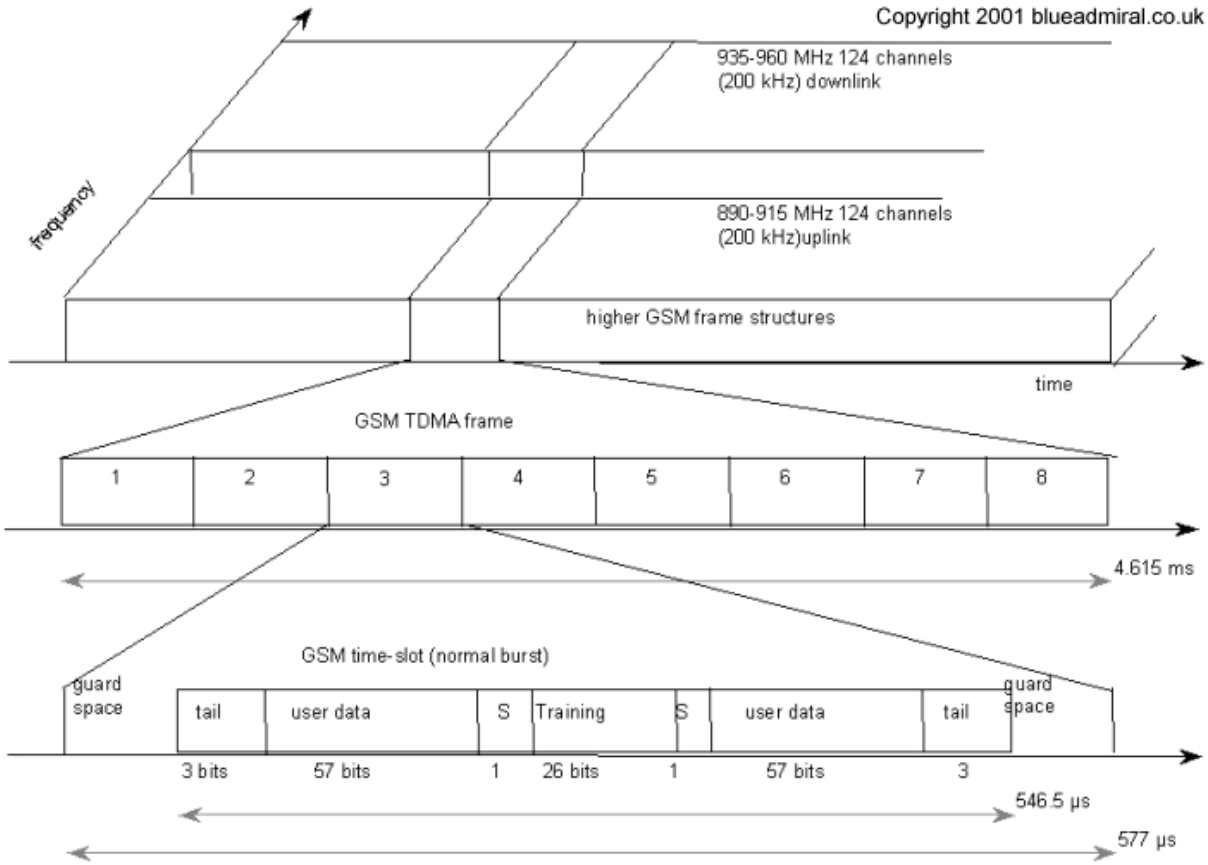
offers transmission of messages of up to 160 characters. Sending and receiving of SMS is possible during data/voice transmission.

3. **Supplementary services**

System Architecture:



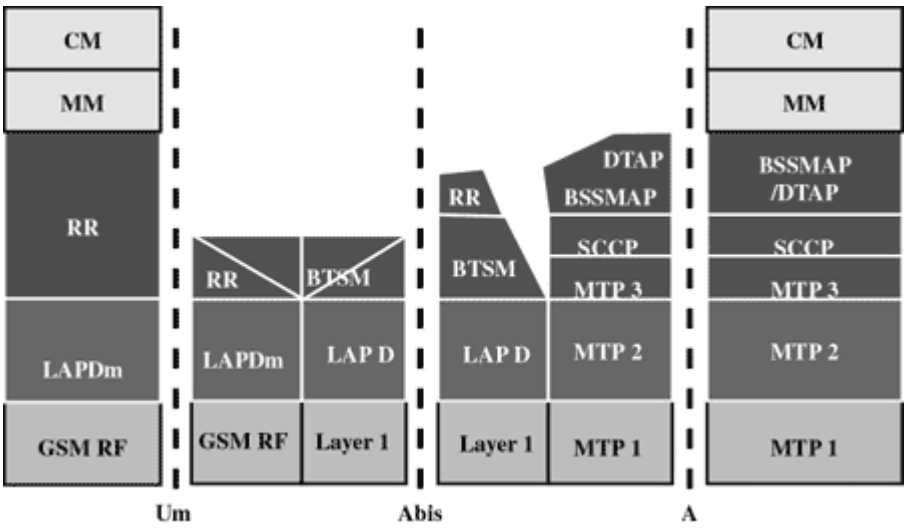
Radio Interface:



Protocals:

Um Interface:

1. Handles all radio specific functions.
2. Creation of bursts
   i) Multiplexing of bursts into TDMA frame
   ii) Synchronization with BTS
   iii) Detection of idle channels
   iv) Measurement of channel quality on downlink
   v) Uses GMSK(Gaussian Minimum shift keying) for digital modulation



LAPD:

- It is a lightweight LAPD
- Offers reliable data transfer
- Re-sequencing of data frames
- Flow control
- Segmentation
- Reassembly of data
- Acknowledged data transfer

RR:

- Setup
- Maintenance
- Release of radio channels
- Accesses physical layer

MM:

- Registration
- Authentication
- Identification
- Location Updating
- Provision of TMSI

CM:

- Call control(CC)
- Short Message Service(SMS)
- Supplementary Service(SS)

Localization and calling:

One of the main features of GSM system is the automatic, worldwide localization of it's users. The GSM system always knows where a user is currently located, and the same phone number is valid worldwide. To have this ability the GSM system performs periodic location updates, even if the user does not use the MS, provided that the MS is still logged on to the GSM network and is not completely switched off. The HLR contains information about the current location, and the VLR that is currently responsible for the MS informs the HLR about the location of the MS when it changes. Changing VLRs with uninterrupted availability of all services is also called roaming. Roaming can take place within the context of one GSM service provider or between two providers in one country, however this does not normally happen but also between different service providers in different countries, known as international roaming.

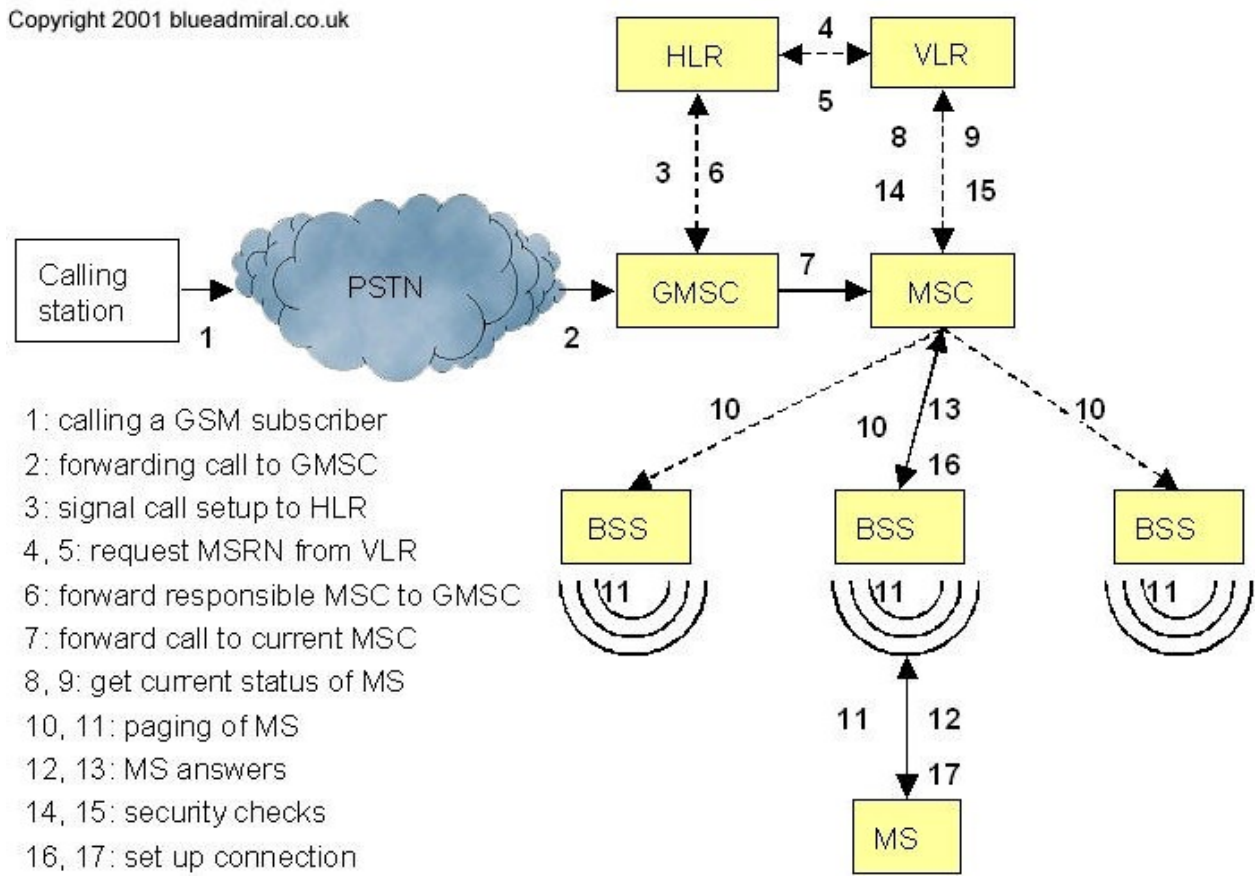
To locate an MS and to address the MS, several numbers are needed:

MSISDN (Mobile Station International ISDN Number) The only important number for the user of GSM is the phone number, due to the fact that the phone number is only associated with the SIM, rather than a certain MS. The MSISDN follows the E.164, this standard is also used in fixed ISDN networks.

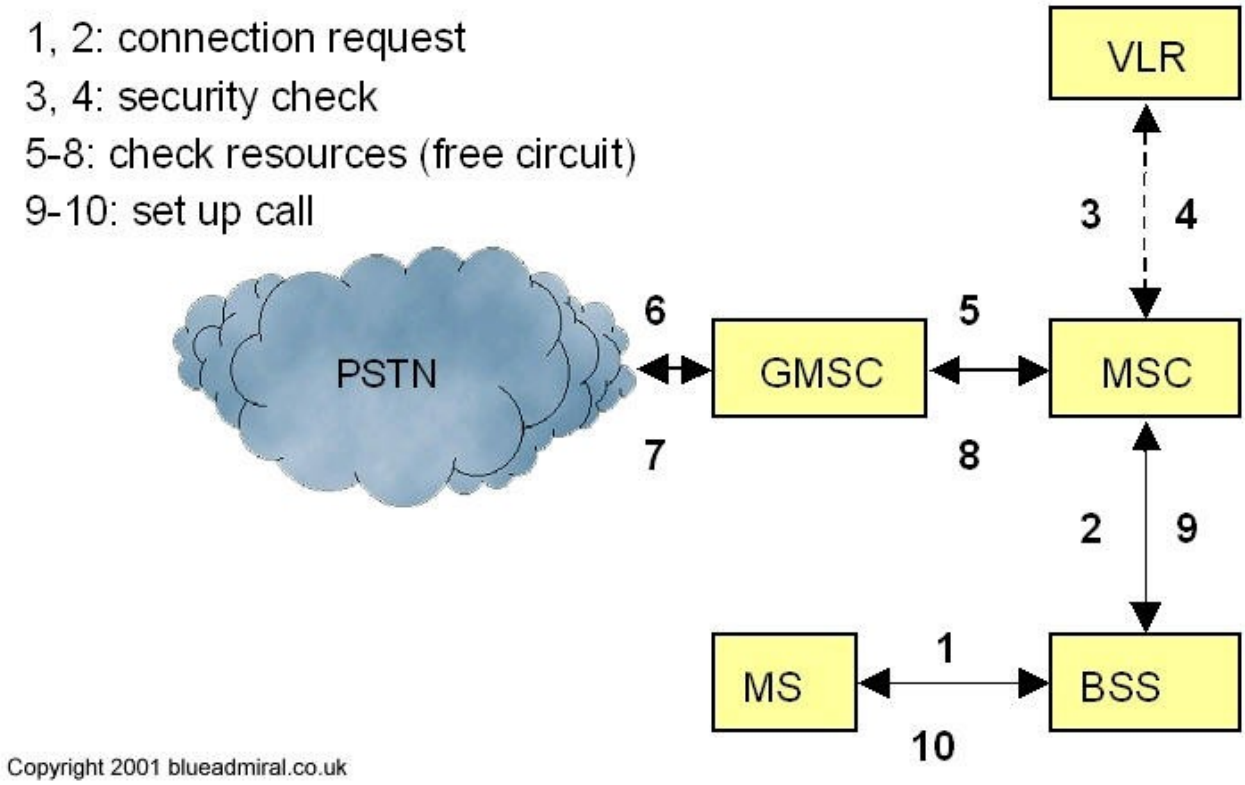
IMSI(International Mobile Subscriber Identity). GSM uses the IMSI for internal unique identification of a subscriber.
TMSI(Temporary Mobile Subscriber Identity). To disguise the IMSI that would give the exact identity of the user which is signaling over the radio air interface, GSM uses the 4 byte TMSI for local subscriber identification. The TMSI is selected by the VLR and only has temporary validity within the location area of the VLR. In addition to that the VLR will change the TMSI periodically.

MSRN (Mobile Station [Subscriber] Roaming Number). This is another temporary address that disguises the identity and location of the subscriber. The VLR generates this address upon request from the MSC and the address is also stored in the HLR. The MSRN is comprised of the current VCC (Visitor Country Code), the VNDC (Visitor National Destination Code) and the identification of the current MSC together with the subscriber number, hence the MSRN is essential to help the HLR to find a subscriber for an incoming call.

All the numbers described above are needed to find a user within the GSM system, and to maintain the connection with a mobile station. The following scenarios below shows a MTC (Mobile Terminate Call) and a MOC (Mobile Originated Call).



Mobile Terminated Call



GSM HANDOVER:

One of the key elements of a mobile phone or cellular telecommunications system, is that the system is split into many small cells to provide good frequency re-use and coverage. However as the mobile moves out of one cell to another it must be possible to retain the connection. The process by which this occurs is known as handover or handoff. The term handover is more widely used within Europe, whereas handoff tends to be use more in North America. Either way, handover and handoff are the same process.

GSM systems require a procedure known as a Handover to maintain the continuity of the call. This is because a single cell does not cover the whole service area e.g. a whole city or country. However a single cell has a maximum service area of approximately 23 miles (35

km) for each antenna . The smaller the size of the cell and the faster the movement of the MS through the cells (Up to 155 mph (250 kph) for GSM), the more handovers of ongoing calls are required, but a handover should not cause the a call drop. Basically there are two main reasons for handovers, however the GSM Specification identifies 40 reasons.

The MS moves out of coverage of the serving BTS thus the signal level becomes lower continuously until it falls beneath the minimal requirements for communications. Or the error rate may grow due to interference, the distance to the BTS may be do high. All these effects may diminish the quality of the radio link and make transmission impossible in the near future.
The wired infrastructure i.e. the MSC, BSC may decide that the traffic in one cell is too high thus introducing congestion and hence decides to shift some MSs to other cells with a lower level of traffic, if that is possible. Thus, handovers can be used as a method of controlling traffic through load balancing to relieve localised congestion.

Figure 11 shows four possible handover scenarios with in the GSM system.

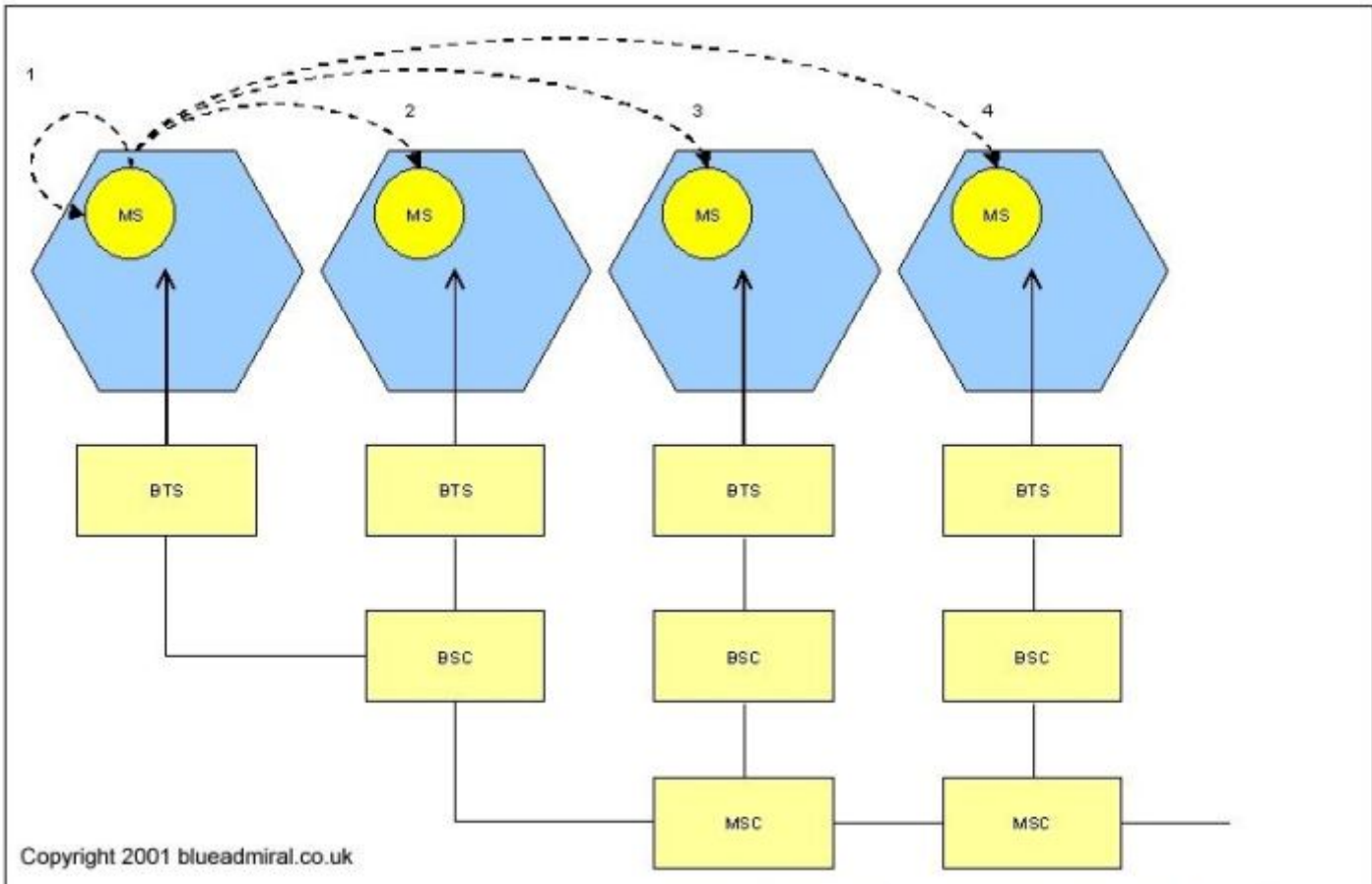


Figure 11 Types of handover within a GSM system

1. Intra Cell Handover : This happens when within a cell, when narrowband interference could make transmission at a certain frequency impossible. The BSC could then decide to change the carrier frequency.
2. Inter Cell, intra BSC handover : This type of handover is a typical handover within the GSM system and occurs when the MS moves from one BTS to another but stays within the

control of same BSC. The BSC performs the handover and assigns a new radio channel in the new BTS, then releases the old BTS.
3. Inter BSC, Intra MSC handover : Since a BSC controls a limited number of BTSs, the GSM system has to perform handovers between BSCs. This form of handover is controlled by the MSC.
4. Inter MSC handover : A handover could also be required between two BTSs that belong to two different MSCs, now both MSCs perform the handover together.

GSM SECURITY:

GSM is the most secured cellular telecommunications system available today. GSM has its security methods standardized. GSM maintains end-to-end security by retaining the confidentiality of calls and anonymity of the GSM subscriber.

Temporary identification numbers are assigned to the subscriber’s number to maintain the privacy of the user. The privacy of the communication is maintained by applying encryption algorithms and frequency hopping that can be enabled using digital systems and signalling.

This chapter gives an outline of the security measures implemented for GSM subscribers.

Mobile Station Authentication:

The GSM network authenticates the identity of the subscriber through the use of a challenge-response mechanism. A 128-bit Random Number (RAND) is sent to the MS. The MS computes the 32-bit Signed Response (SRES) based on the encryption of the RAND with the authentication algorithm (A3) using the individual subscriber authentication key (Ki). Upon receiving the SRES from the subscriber, the GSM network repeats the calculation to verify the identity of the subscriber.

The individual subscriber authentication key (Ki) is never transmitted over the radio channel, as it is present in the subscriber's SIM, as well as the AUC, HLR, and VLR databases. If the received SRES agrees with the calculated value, the MS has been successfully authenticated and may continue. If the values do not match, the connection is terminated and an authentication failure is indicated to the MS.

The calculation of the signed response is processed within the SIM. It provides enhanced security, as confidential subscriber information such as the IMSI or the individual subscriber authentication key (Ki) is never released from the SIM during the authentication process.

Signalling and Data Confidentiality:

The SIM contains the ciphering key generating algorithm (A8) that is used to produce the 64-bit ciphering key (Kc). This key is computed by applying the same random number (RAND) used in the authentication process to ciphering key generating algorithm (A8) with the individual subscriber authentication key (Ki).

GSM provides an additional level of security by having a way to change the ciphering key, making the system more resistant to eavesdropping. The ciphering key may be changed at regular intervals as required. As in case of the authentication process, the computation of the ciphering key (Kc) takes place internally within the SIM. Therefore, sensitive information such as the individual subscriber authentication key (Ki) is never revealed by the SIM.

Encrypted voice and data communications between the MS and the network is accomplished by using the ciphering algorithm A5. Encrypted communication is initiated by a ciphering mode request command from the GSM network. Upon receipt of this command, the mobile station begins encryption and decryption of data using the ciphering algorithm (A5) and the ciphering key (Kc).

Subscriber Identity Confidentiality:

To ensure subscriber identity confidentiality, the Temporary Mobile Subscriber Identity (TMSI) is used. Once the authentication and encryption procedures are done, the TMSI is sent to the mobile station. After the receipt, the mobile station responds. The TMSI is valid in the location area in which it was issued. For communications outside the location area, the Location Area Identification (LAI) is necessary in addition to the TMSI.

GSM NEW DATA SERVICES

The main data service used in modern GSM systems is the GPRS. Therefore, the major part of this chapter is devoted to GPRS. However, HSCSD is also of importance. HSCSD was available earlier than GPRS and was therefore chosen by some network providers in order to provide higher data rate services in GSM as fast as possible and it is still used in many networks. A third important aspect of providing improved data rates in GSM systems is EDGE, which helps to increase the data rate of both GPRS and HSCSD by allowing for higher-order modulation schemes when the signal strength is sufficiently high. Let us now first focus on GPRS in the following.

GPRS

Packet data transmission has already been standardized in GSM phase 2, offering access to the Packet Switched Public Data Network (PSPDN). However, on the air interface such access occupies a complete circuit switched traffic channel for the entire call period. In the case of bursty traffic (e.g. Internet traffic), such access leads to a highly inefficient resource utilization. It is obvious that in this case, packet switched bearer services result in a much better utilization of the traffic channels. This is because a packet channel will only be allocated when needed and will be released after the transmission of the packets. With this principle, multiple users can share one physical channel (statistical multiplexing).

UNIT 2

-

(Wireless) Medium Access Control: Motivation for a specialized MAC (Hidden and exposed terminals, Near and far terminals), SDMA, FDMA, TDMA, CDMA.

The **Media Access Control** (**MAC**) data communication protocol sub-layer, also known as the Medium Access Control, is a sublayer of the Data Link Layer specified in the seven-layer OSI model (layer 2). The hardware that implements the MAC is referred to as a **Medium Access Controller**. The MAC sub-layer acts as an interface between the Logical Link Control (LLC) sublayer and the network's physical layer.

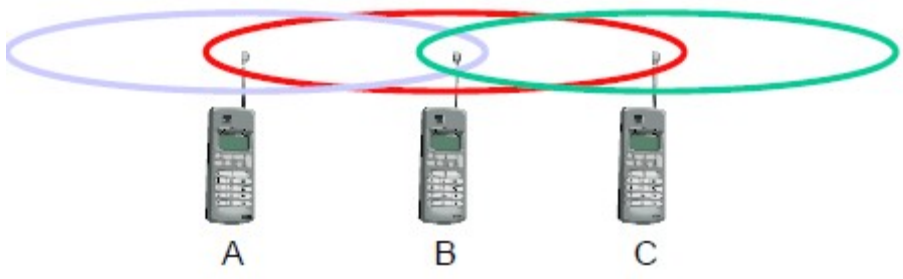
Motivation for a specialized MAC:

One of the most commonly used MAC schemes for wired networks is carrier sense multiple access with collision detection (CSMA/CD). In this scheme, a sender senses the medium (a wire or coaxial cable) to see if it is free. If the medium is busy, the sender waits until it is free. If the medium is free, the sender starts transmitting data and continues to listen into the medium. If the sender detects a collision while sending, it stops at once and sends a jamming signal. But this scheme doest work well with wireless networks. The problems are:

- Signal strength decreases proportional to the square of the distance
- The sender would apply CS and CD, but the collisions happen at the receiver
- It might be a case that a sender cannot “hear” the collision, i.e., CD does not work
- Furthermore, CS might not work, if for e.g., a terminal is “hidden”

Hidden and Exposed Terminals:

Consider the scenario with three mobile phones as shown below. The transmission range of A reaches B, but not C (the detection range does not reach C either). The transmission range of C reaches B, but not A. Finally, the transmission range of B reaches A and C, i.e., A cannot detect C and vice versa.



Hidden terminals:

- A sends to B, C cannot hear A
- C wants to send to B, C senses a “free” medium (CS fails) and starts transmitting
- Collision at B occurs, A cannot detect this collision (CD fails) and continues with its transmission to B
- A is “hidden” from C and vice versa

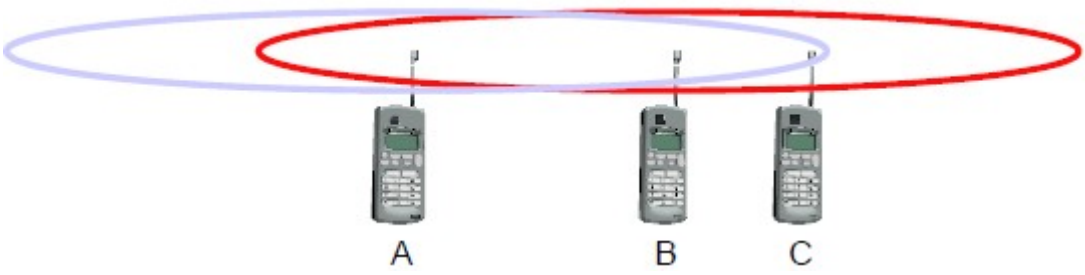
Exposed terminals:

- B sends to A, C wants to send to another terminal (not A or B) outside the range
- C senses the carrier and detects that the carrier is busy.
- C postpones its transmission until it detects the medium as being idle again
- but A is outside radio range of C, waiting is **not** necessary
- C is “exposed” to B

Hidden terminals cause collisions, where as Exposed terminals causes unnecessary delay.

Near and far terminals:

Consider the situation shown below. A and B are both sending with the same transmission power.



- Signal strength decreases proportional to the square of the distance
- So, B's signal drowns out A's signal making C unable to receive A's transmission
- If C is an arbiter for sending rights, B drown out A's signal on the physical layer making C unable to hear out A.

The **near/far effect** is a severe problem of wireless networks using CDM. All signals should arrive at the receiver with more or less the same strength for which Precise power control is to be implemented.

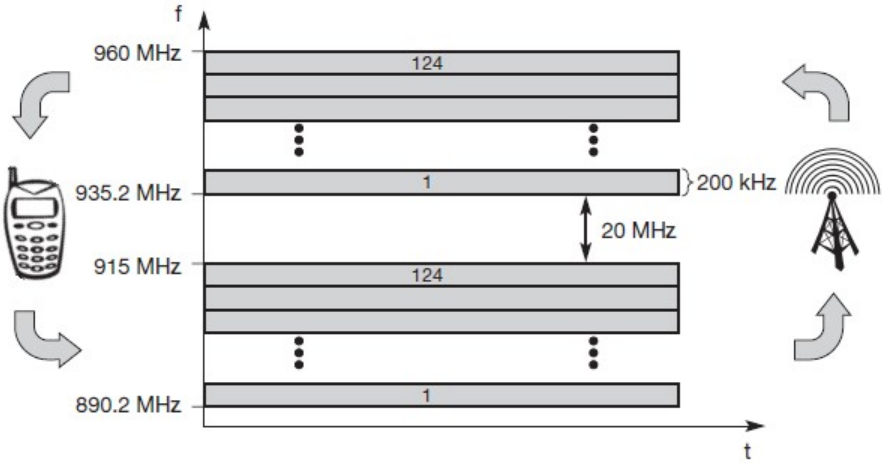
SDMA:

Space Division Multiple Access (SDMA) is used for allocating a separated space to users in wireless networks. A typical application involves assigning an optimal base station to a mobile phone user. The mobile phone may receive several base stations with different quality. A MAC algorithm could now decide which base station is best, taking into account which frequencies (FDM), time slots (TDM) or code (CDM) are still available. The basis for the SDMA algorithm is formed by cells and sectorized antennas which constitute the infrastructure implementing **space division multiplexing (SDM).** SDM has the unique advantage of not requiring any multiplexing equipment. It is usually combined with other multiplexing techniques to better utilize the individual physical channels.

FDMA:

Frequency division multiplexing (FDM) describes schemes to subdivide the frequency dimension into several non-overlapping frequency bands.

Frequency Division Multiple Access is a method employed to permit several users to transmit simultaneously on one satellite transponder by assigning a specific frequency within the channel to each user. Each conversation gets its own, unique, radio channel. The channels are relatively narrow, usually 30 KHz or less and are defined as either transmit or receive channels. A full duplex conversation requires a transmit & receive channel pair. FDM is often used for simultaneous access to the medium by base station and mobile station in cellular networks establishing a duplex channel. A scheme called **frequency division duplexing (FDD)** in which the two directions, mobile station to base station and vice versa are now separated using different frequencies.



FDM for multiple access and duplex:

The two frequencies are also known as **uplink**, i.e., from mobile station to base station or from ground control to satellite, and as **downlink**, i.e., from base station to mobile station or from satellite to ground control. The basic frequency allocation scheme for GSM is fixed and regulated by national authorities. All uplinks use the band between 890.2 and 915 MHz, all downlinks use 935.2 to 960 MHz. According to FDMA, the base station, shown on the right side, allocates a certain frequency for up- and downlink to establish a duplex channel with a mobile phone. Up- and downlink have a fixed relation. If the uplink frequency is fu = 890 MHz + n·0.2 MHz, the downlink frequency is fd = fu + 45 MHz, i.e**., fd = 935 MHz + n·0.2**

MHz for a certain channel n. The base station selects the channel. Each channel (uplink and downlink) has a bandwidth of 200 kHz.

This scheme also has disadvantages. While radio stations broadcast 24 hours a day, mobile communication typically takes place for only a few minutes at a time. Assigning a separate frequency for each possible communication scenario would be a tremendous waste of (scarce) frequency resources. Additionally, the fixed assignment of a frequency to a sender makes the scheme very inflexible and limits the number of senders.

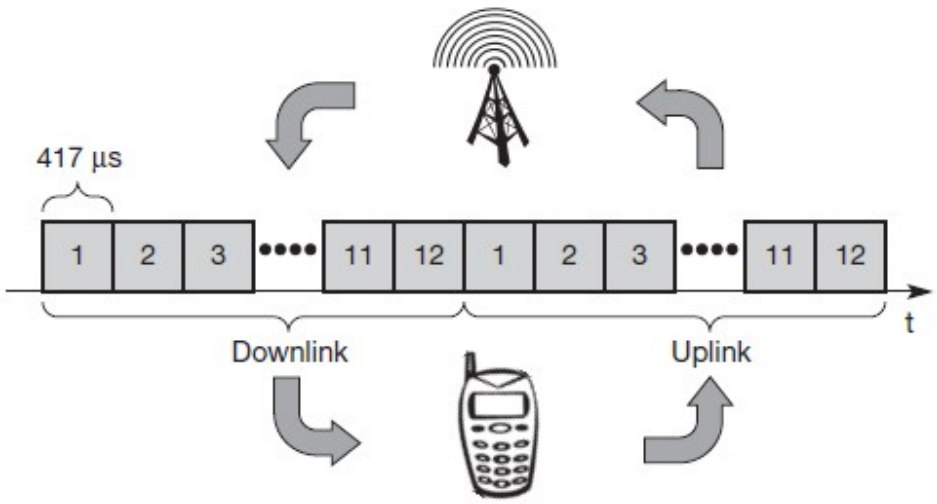
TDMA:

A more flexible multiplexing scheme for typical mobile communications is time division multiplexing (TDM). Compared to FDMA, time division multiple access (TDMA) offers a much more flexible scheme, which comprises all technologies that allocate certain time slots for communication. Now synchronization between sender and receiver has to be achieved in the time domain. Again this can be done by using a fixed pattern similar to FDMA techniques, i.e., allocating a certain time slot for a channel, or by using a dynamic allocation scheme.

Listening to different frequencies at the same time is quite difficult, but listening to many channels separated in time at the same frequency is simple. Fixed schemes do not need identification, but are not as flexible considering varying bandwidth requirements.

Fixed TDM:

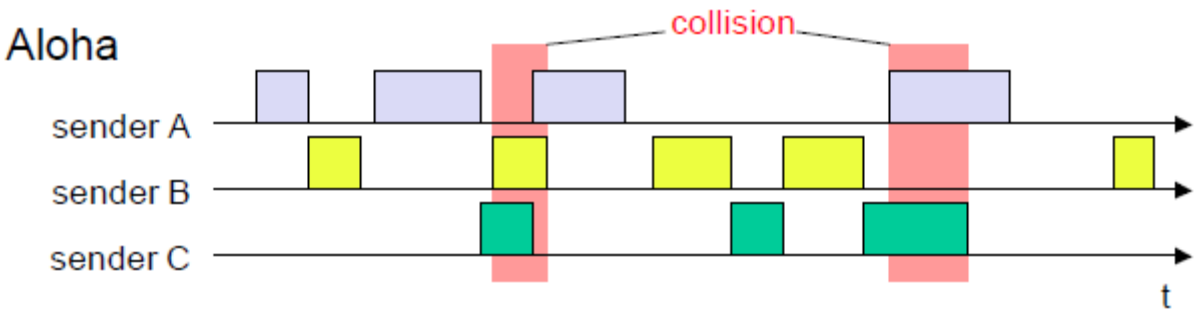
The simplest algorithm for using TDM is allocating time slots for channels in a fixed pattern. This results in a fixed bandwidth and is the typical solution for wireless phone systems. MAC is quite simple, as the only crucial factor is accessing the reserved time slot at the right moment. If this synchronization is assured, each mobile station knows its turn and no interference will happen. The fixed pattern can be assigned by the base station, where competition between different mobile stations that want to access the medium is solved.



The above figure shows how these fixed TDM patterns are used to implement multiple access and a duplex channel between a base station and mobile station. Assigning different slots for uplink and downlink using the same frequency is called **time division duplex (TDD)**. As shown in the figure, the base station uses one out of 12 slots for the downlink, whereas the mobile station uses one out of 12 different slots for the uplink. Uplink and downlink are separated in time. Up to 12 different mobile stations can use the same frequency without interference using this scheme. Each connection is allotted its own up- and downlink pair. This general scheme still wastes a lot of bandwidth. It is too static, too inflexible for data communication. In this case, connectionless, demand-oriented TDMA schemes can be used

Classical Aloha:

In this scheme, TDM is applied without controlling medium access. Here each station can access the medium at any time as shown below:

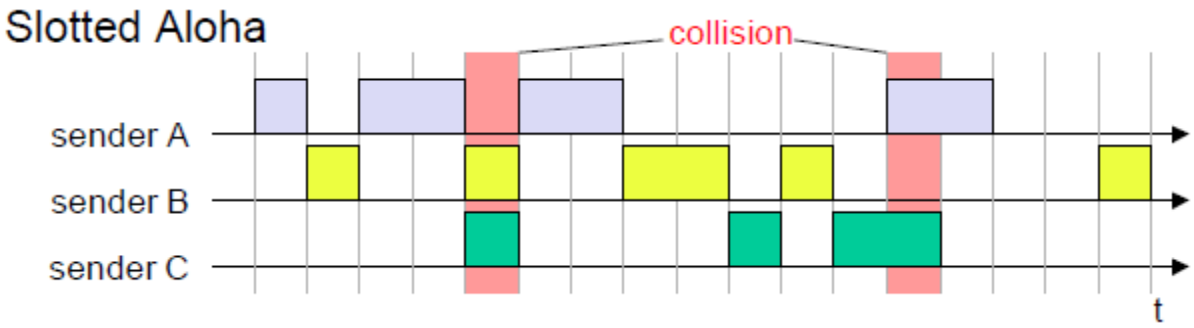


This is a random access scheme, without a central arbiter controlling access and without coordination among the stations. If two or more stations access the medium at the same time,

a **collision** occurs and the transmitted data is destroyed. Resolving this problem is left to higher layers (e.g., retransmission of data). The simple Aloha works fine for a light load and does not require any complicated access mechanisms.

Slotted Aloha:

The first refinement of the classical Aloha scheme is provided by the introduction of time slots (**slotted Aloha**). In this case, all senders have to be **synchronized**, transmission can only start at the beginning of a **time slot** as shown below.



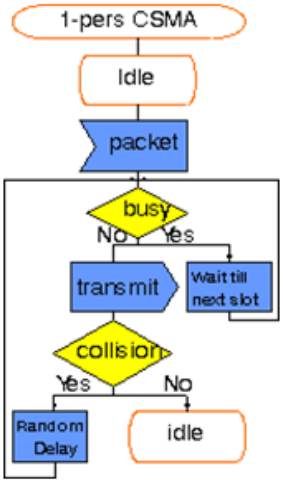
The introduction of slots raises the throughput from 18 per cent to 36 per cent, i.e., slotting doubles the throughput. Both basic Aloha principles occur in many systems that implement distributed access to a medium. Aloha systems work perfectly well under a light load, but they cannot give any hard transmission guarantees, such as maximum delay before accessing the medium or minimum throughput.

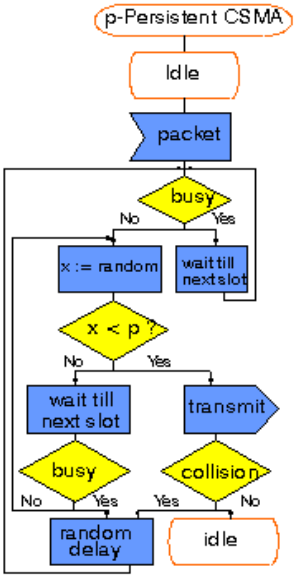
Carrier sense multiple access:

One improvement to the basic Aloha is sensing the carrier before accessing the medium. Sensing the carrier and accessing the medium only if the carrier is idle decreases the probability of a collision. But, as already mentioned in the introduction, hidden terminals cannot be detected, so, if a hidden terminal transmits at the same time as another sender, a collision might occur at the receiver. This basic scheme is still used in most wireless LANs. The different versions of CSMA are:

- **1-persistent CSMA**: Stations sense the channel and listens if its busy and transmit immediately, when the channel becomes idle. It's called 1-persistent CSMA because the host transmits with a probability of 1 whenever it finds the channel idle.
- **non-persistent CSMA**: stations sense the carrier and start sending immediately if the medium is idle. If the medium is busy, the station pauses a random amount of time before sensing the medium again and repeating this pattern.
- **p-persistent CSMA**: systems nodes also sense the medium, but only transmit with a probability of p, with the station deferring to the next slot with the probability 1-p, i.e., access is slotted in addition

CSMA with collision avoidance (**CSMA/CA**) is one of the access schemes used in wireless LANs following the standard IEEE 802.11. Here sensing the carrier is combined with a back-off scheme in case of a busy medium to achieve some fairness among competing stations.



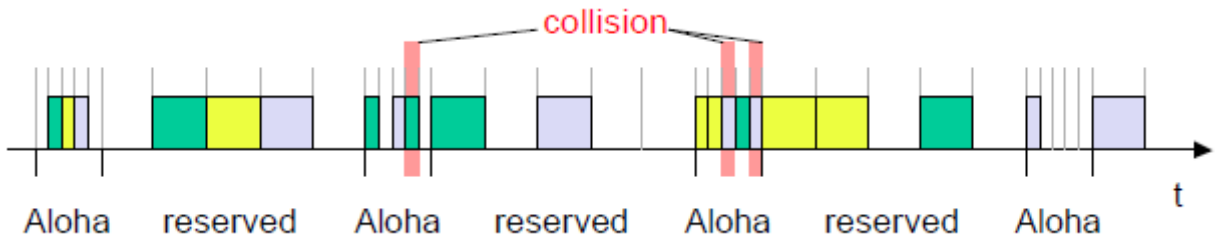


Demand assigned multiple access:

Channel efficiency for Aloha is 18% and for slotted Aloha is 36%. It can be increased to 80% by implementing reservation mechanisms and combinations with some (fixed) TDM patterns. These schemes typically have a reservation period followed by a transmission period. During the reservation period, stations can reserve future slots in the transmission period. While, depending on the scheme, collisions may occur during the reservation period, the transmission period can then be accessed without collision.

One basic scheme is **demand assigned multiple access (DAMA)** also called **reservation Aloha**, a scheme typical for satellite systems. It increases the amount of users in a pool of satellite channels that are available for use by any station in a network. It is assumed that not all users will need simultaneous access to the same communication channels. So that a call can be established, DAMA assigns a pair of available channels based on requests issued from a user. Once the call is completed, the channels are returned to the pool for an assignment to another call. Since the resources of the satellite are being used only in proportion to the occupied channels for the time in which they are being held, it is a perfect environment for voice traffic and data traffic in batch mode.

- It has two modes as shown below.
-

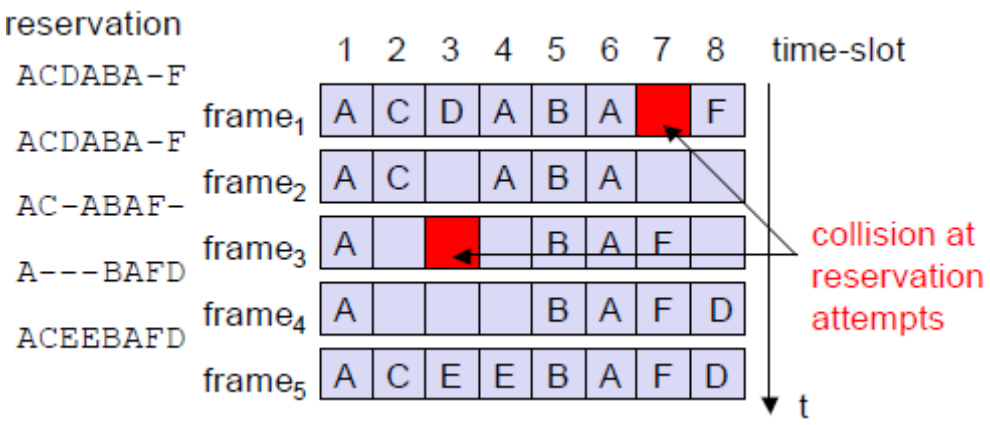


During a contention phase following the slotted Aloha scheme; all stations can try to reserve future slots. Collisions during the reservation phase do not destroy data transmission, but only the short requests for data transmission. If successful, a time slot in the future is reserved, and no other station is allowed to transmit during this slot. Therefore, the satellite collects all successful requests (the others are destroyed) and sends back a reservation list indicating access rights for future slots. All ground stations have to obey this list. To maintain the fixed TDM pattern of reservation and transmission, the stations have to be synchronized from time to time. DAMA is an **explicit reservation** scheme. Each transmission slot has to be reserved explicitly.

PRMA packet reservation multiple access:

It is a kind of implicit reservation scheme where, slots can be reserved implicitly. A certain number of slots form a frame. The frame is repeated in time i.e., a fixed TDM pattern is applied. A base station, which could be a satellite, now broadcasts the status of each slot to all

mobile stations. All stations receiving this vector will then know which slot is occupied and which slot is currently free.

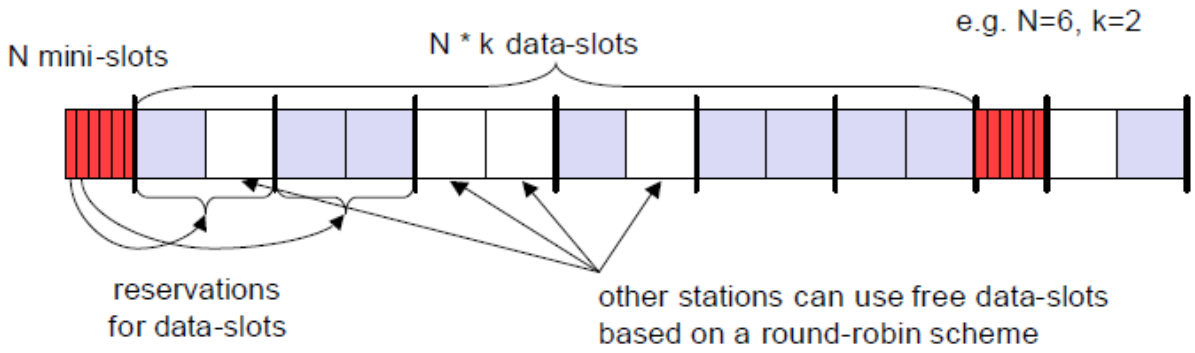


The base station broadcasts the reservation status 'ACDABA-F' to all stations, here A to F. This means that slots one to six and eight are occupied, but slot seven is free in the following transmission. All stations wishing to transmit can now compete for this free slot in Aloha fashion. The already occupied slots are not touched. In the example shown, more than one station wants to access this slot, so a collision occurs. The base station returns the reservation status 'ACDABA-F', indicating that the reservation of slot seven failed (still indicated as free) and that nothing has changed for the other slots. Again, stations can compete for this slot. Additionally, station D has stopped sending in slot three and station F in slot eight. This is noticed by the base station after the second frame. Before the third frame starts, the base station indicates that slots three and eight are now idle. Station F has succeeded in reserving slot seven as also indicated by the base station.

As soon as a station has succeeded with a reservation, all future slots are implicitly reserved for this station. This ensures transmission with a guaranteed data rate. The slotted aloha scheme is used for idle slots only; data transmission is not destroyed by collision.

Reservation TDMA:

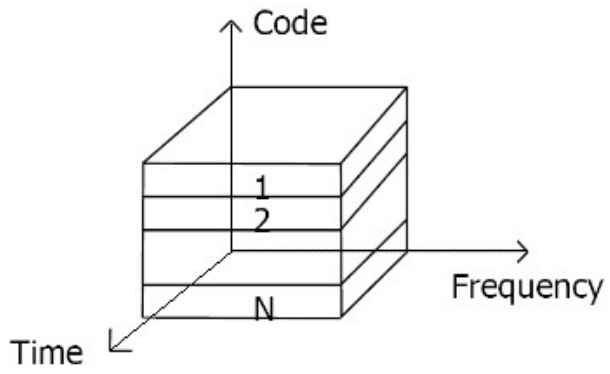
In a fixed TDM scheme N mini-slots followed by N·k data-slots form a frame that is repeated. Each station is allotted its own mini-slot and can use it to reserve up to k data-slots.



This guarantees each station a certain bandwidth and a fixed delay. Other stations can now send data in unused data-slots as shown. Using these free slots can be based on a simple round-robin scheme or can be uncoordinated using an Aloha scheme. This scheme allows for the combination of, e.g., isochronous traffic with fixed bitrates and best-effort traffic without any guarantees.

CDMA:

Code division multiple access systems apply codes with certain characteristics to the transmission to separate different users in code space and to enable access to a shared medium without interference.



All terminals send on the same frequency probably at the same time and can use the whole bandwidth of the transmission channel. Each sender has a unique random number, the sender XORs the signal with this random number. The receiver can “tune” into this signal if it knows the pseudo random number, tuning is done via a correlation function

Disadvantages:

- Higher complexity of a receiver (receiver cannot just listen into the medium and start receiving if there is a signal)
- All signals should have the same strength at a receiver

Advantages:

- all terminals can use the same frequency, no planning needed
- huge code space compared to frequency space
- interferences is not coded
- forward error correction and encryption can be easily integrated

Comparison SDMA/TDMA/FDMA/CDMA

Approach	SDMA	TDMA	FDMA	CDMA
Idea	segment space into cells/sectors	segment sending time into disjoint time-slots, demand driven or fixed patterns	segment the frequency band into disjoint sub-bands	spread the spectrum using orthogonal codes
Terminals	only one terminal can be active in one cell/one sector	all terminals are active for short periods of time on the same frequency	every terminal has its own frequency, uninterrupted	all terminals can be active at the same place at the same moment, uninterrupted
Signal separation	cell structure, directed antennas	synchronization in the time domain	filtering in the frequency domain	code plus special receivers
Advantages	very simple, increases capacity per km²	established, fully digital, flexible	simple, established, robust	flexible, less frequency planning needed, soft handover
Dis-advantages	inflexible, antennas typically fixed	guard space needed (multipath propagation), synchronization difficult	inflexible, frequencies are a scarce resource	complex receivers, needs more complicated power control for senders
Comment	only in combination with TDMA, FDMA or CDMA useful	standard in fixed networks, together with FDMA/SDMA used in many mobile networks	typically combined with TDMA (frequency hopping patterns) and SDMA (frequency reuse)	still faces some problems, higher complexity, lowered expectations; will be integrated with TDMA/FDMA

UNIT 3

MOBILE IP:

The IP addresses are designed to work with stationary hosts because part of the address defines the network to which the host is attached.

A host cannot change its IP address without terminating on-going sessions and restarting them after it acquires a new address. Other link layer mobility solutions exist but are not sufficient enough for the global Internet.

Mobility is the ability of a node to change its point-of-attachment while maintaining all existing communications and using the same IP address.

Nomadicity allows a node to move but it must terminate all existing communications and then can initiate new connections with a new address.

Mobile IP is a network layer solution for homogenous and heterogeneous mobility on the global Internet which is scalable, robust, secure and which allows nodes to maintain all ongoing communications while moving.

Design Goals:

Mobile IP was developed as a means for transparently dealing with problems of mobile users. Mobile IP was designed to make the size and the frequency of required routing updates as

small as possible. It was designed to make it simple to implement mobile node software. It was designed to avoid solutions that require mobile nodes to use multiple addresses.

Requirements: There are several requirements for Mobile IP to make it as a standard. Someof them are:

1.Compatibility:

The whole architecture of internet is very huge and a new standard cannot introduce changes to the applications or network protocols already in use. Mobile IP is to be integrated into the existing operating systems. Also, for routers also it may be possible to enhance its capabilities to support mobility instead of changing the routers which is highly impossible. Mobile IP must not require special media or MAC/LLC protocols, so it must use the same interfaces and mechanisms to access the lower layers as IP does. Finally, end-systems enhanced with a mobile IP implementation should still be able to communicate with fixed systems without mobile IP.

2.Transparency:

Mobility remains invisible for many higher layer protocols and applications. Higher layers continue to work even if the mobile computer has changed its point of attachment to the network and even notice a lower bandwidth and some interruption in the service. As many of to day's applications have not been designed to use in mobile environments, the effects of mobility will be higher delay and lower bandwidth.

3.Scalability and efficiency:

The efficiency of the network should not be affected even if a new mechanism is introduced into the internet. Enhancing IP for mobility must not generate many new messages flooding the whole network. Special care is necessary to be taken considering the lower bandwidth of wireless links. Many mobile systems have a wireless link to an attachment point. Therefore, only some additional packets must be necessary between a mobile system and a node in the network. It is indispensable for a mobile IP to be scalable over a large number of participants in the whole internet, throughout the world.

4.Security:

Mobility possesses many security problems. A minimum requirement is the authentication of all messages related to the management of mobile IP. It must be sure for the IP layer if it forwards a packet to a mobile host that this host really is the receiver of the packet. The IP layer can only guarantee that the IP address of the receiver is correct. There is no way to prevent faked IP addresses and other attacks.

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

Entities and terminology:

The following defines several entities and terms needed to understand mobile IP

Mobile Node (MN):

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 communicate with any other system in the internet as long as link-layer connectivity is given. Examples are laptop, mobile phone, router on an aircraft etc.

Correspondent node (CN):

At least one partner is needed for communication. In the following the CN represents this partner for the MN. The CN can be a fixed or mobile node.

Home network(HN):

The home network is the subnet the MN belongs to with respect to its IP address. No mobile IP support is needed within the home network.

Foreign networ(FN):

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

Foreign agent (FA):

The FA can provide several services to the MN during its visit to the foreign network. The FA can have the COA, acting as tunnel endpoint and forwarding packets to the MN. The FA can be the default router for the MN. FAs can also provide security services because they belong to the foreign network as opposed to the MN which is only visiting. FA is implemented on a router for the subnet the MN attaches to.

Care-of address (COA):

The COA defines the current location of the MN from an IP point of view. All IP packets sent to the MN are delivered to the COA, not directly to the IP address of the MN. Packet delivery toward the MN is done using a tunnel, i.e., the COA marks the tunnel endpoint, i.e., the address where packets exit the tunnel. There are two different possibilities for the location of the COA:

Foreign agent COA:

The COA could be located at the FA, i.e., the COA is an IP address of the FA. The FA is the tunnel end-point and forwards packets to the MN. Many MN using the FA can share this COA as common COA.

Co-located COA:

The COA is co-located if the MN temporarily acquired an additional IP address which acts as COA. This address is now topologically correct, and the tunnel endpoint is at the MN.Co-located addresses can be acquired using services such as DHCP.

Home agent (HA):

The HA provides several services for the MN and is located in the home network. The tunnel for packets toward the MN starts at the HA. The HA maintains a location registry, i.e., it is informed of the MN's location by the current COA. Three alternatives for the implementation of an HA exist.

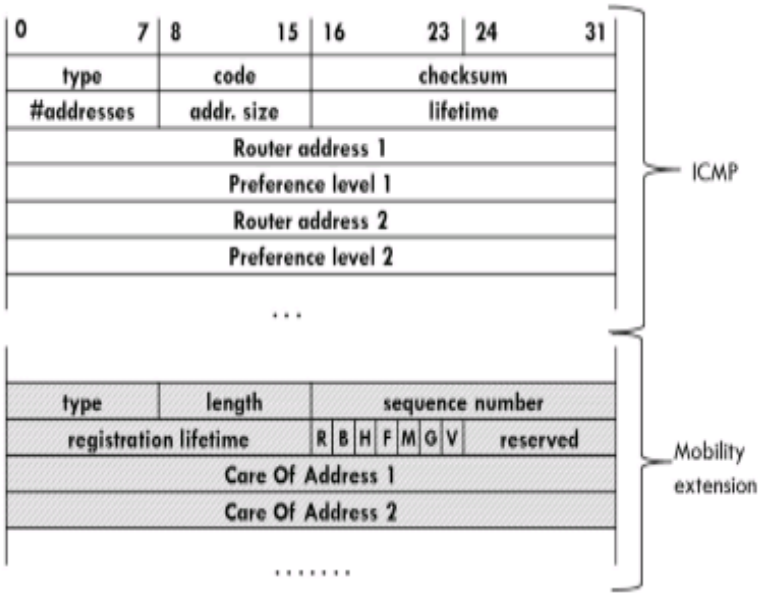
1. The HA can be implemented on a router that is responsible for the home network. This is obviously the best position, because without optimizations to mobile IP, all packets for the MN have to go through the router anyway.

2. If changing the router's software is not possible, the HA could also be Implemented on an arbitrary node in the subnet. One disadvantage of this solution is the double

Agent Advertisement:

- Over here the HA and FA periodically advertise their presence by using special advertisements messages.
- Usually, the FA periodically broadcasts the IRDP message in its own network to let the visited MN know the FA is here and what services the FA provides (Agent Advertisement). Thus, the MN knows which network it belongs to.
- In case the MN does not receive this message, it can request the service by sending a solicitation message to inform the FA directly (Agent Solicitation).
- These advertisements can be seen as beacon broadcast to the subnets.
- Here we use ICMP messages according to RFC 1256. The agent advertisement packet is show alongside.
- In the figure the upper half is the ICMP packet while the lower half is the extension needed for mobility
- The IP destination address (not in fig.) can be set to 224.0.0.1 (which is the standard address for multicast) or 255.255.255.255 (broadcast address)
- Some of the fields used are as follows:
-
    - Type → set to 9
    - Code → 0 if agent routes traffic from non-mobile nodes as well or else 16
    - Check sum → The 16-bit one's complement of the one's complement sum of the ICMP /IRDP message
    - #addresses → The number of router addresses advertised in this message

- Addr. Size → The number of 32-bit words of information per each router address
- Lifetime → The maximum number of seconds that the router addresses may be considered valid.
- Router Address [i=1,2,3..] → The sending router's IP address on the ith interface from which this message is sent.
- Prefernce level [i=1,2,…] →The preferability of each Router Address[i]



- Till now what was done is standard ICMP procedure. After this we move to the extra extension created i.e. mobility extension. The fields in it are:

  - Type → 16 (Mobility advertisement extension)
  - Length → 6+ 4*(number of addresses)
  - Sequence number → The count of Agent Advertisement messages sent since the agent was initialized.
  - Registration lifetime → maximum lifetime in seconds a node can request during registration

Agent Registration:

- Having received a COA, the MN has to register with the HA. The main purpose of the registration is to inform the HA of the current location for correct forwarding of packets. Registration can be done in two different ways depending on the location of the COA.

- If the COA is at the FA, the MN sends its registration request containing the COA to the FA which forwards the request to the HA. The HA now sets up a mobility binding, containing the mobile node's home IP address and the current COA.

- It also contains the lifetime of the registration which is negotiated during the registration process. Registration expires automatically after the lifetime and is deleted; so, an MN should reregister before expiration. This mechanism is necessary to avoid mobility bindings which are no longer used. After setting up the mobility binding, the HA sends a reply message back to the FA which forwards it to the MN.
- Registration of a mobile node via the FA or directly with the HA

- If the COA is co-located, registration can be simpler, the MN sends the request directly to the HA and vice versa. This is also the registration procedure for MNs returning to their home network to register directly with the HA.

- UDP packets are used for the registration requests using the port no 434. The IP source address of the packet is set to the interface address of the MN, the IP destination address is that of the FA or HA.

Registration Request:

- The first field type is set to 1 for a registration request. With the S bit an MN can specify if it wants the HA to retain prior mobility bindings. This allows for simultaneous bindings. Setting the B bit generally indicates that an MN also wants to receive the broadcast packets which have been received by the HA in the home network. If an MN uses a co-located COA, it also takes care of the decapsulation at the tunnel endpoint. The D bit indicates this behavior. As already defined for agent advertisements, the bits M and G denote the use of minimal encapsulation or generic routing encapsulation, respectively.
- T indicates reverse tunneling,
- R and x are set to zero.
- Lifetime denotes the validity of the registration in seconds. A value of zero indicates deregistration; all bits set indicates infinity. Thehome address is the fixed IP address of the MN, home agent is the IP address of the HA, and
- COA represents the tunnel endpoint. The64 bit identification is generated by the MN to identify a request and match it with registration replies. This field is used for protection against replay attacks of registrations.The extensions must at least contain parameters for authentication A registration reply, which is conveyed in a UDP packet, contains a type field set to3 and a code indicating the result of the registration request.

Registration Reply:

- The lifetime field indicates how many seconds the registration is valid if it was successful. Home address and home agent are the addresses of the MN and the HA, respectively. The64-bitidentification is used to match registration requests with replies. The value is based on the identification field from the registration and the authentication method. Again, the extension must at least contain parameters for authentication.

Tunnelling and encapsulation:

A tunnel establishes a virtual pipe for data packets between a tunnel entry and a tunnel endpoint. Packets entering a tunnel are forwarded inside the tunnel and leave the tunnel unchanged. Tunneling, i.e., sending a packet through a tunnel is achieved by using encapsulation.
Mobile IP tunneling Encapsulation is the mechanism of taking a packet consisting of packet header and data and putting it into the data part of a new packet. The reverse operation, taking a packet out of the data part of another packet, is called decapsulation.

Encapsulation and decapsulation are the operations typically performed when a packet is transferred from a higher protocol layer to a lower layer or from a lower to a higher layer respectively. The HA takes the original packet with the MN as destination, puts it into the data part of a new packet and sets the new IP header so that the packet is routed to the COA. The new header is called outer header.

DHCP:

Traditional TCP:

UNIT 4

Hoarding Techniques:

Caching invalidation mechanisms:

In order to maintain the relevance of cached data, based on time, user or other variables, the data will have to be invalidated or removed from the cache. Dyna cache provides different methods for performing cache invalidation. There are four methods to invalidate the cache.

- Time based invalidation
- Command based invalidation
- Dynacache API and CACHEIVL table invalidation
- Group based invalidation

Time based invalidation:

Time-based invalidation is useful when the cache entries cannot be invalidated by any other mechanism , or they should be refreshed after a set period. This method can be accomplished by specifying the *<timeout>value</timeout>* sub-element with a cache-entry in the cachespec.xml file. Value is the amount of time, in seconds , the cache entry is kept in the cache. The default value for this element is 0, which indicates this entry never expires.

An example in which time-based invalidation makes sense to use is caching of a e-Marketing Spot. In general e-Marketing Spots should not be cached because the page output is generated dynamically based on personalized data. But in the case that the store admin is willing to sacrifice function for performance, then the e-Marketing spot JSP pages can be cached with a timeout sub-element, so that the output can be reused for a certain period of time.
There is also an inactivity sub element which is used to specify a time-to-live (TTL) value for the cache entry based on the last time that the cache entry was accessed. It is a sub element of the cache-id element. <inactivity>value<inactivity> where value is the amount of time, in seconds, to keep the cache entry in the cache after the last cache hit. This is especially useful for user dependent cache entries where the an average user session duration can be specified as an inactivity timeout.

Command based invalidation:

Invalidation occurs upon execution of a command, based on invalidation rules, that extends from the WebSphere Commerce Command Framework API. Invalidation IDs for command-based invalidation are constructed based on methods and fields provided by the commands.
To allow a command call to be intercepted by the dynamic cache, the command must be written to the WebSphere Command Framework within its implementation class extending from CacheableCommandImpl (in the com.ibm.websphere.command package). To simplify command writing for command-based invalidation, WebSphere Commerce has updated the abstract classes, ControllerCommandImpl and TaskCommandImpl. They extend from CacheableCommandImpl so that any commands extend from these abstract classes would also extend from CacheableCommandImpl, and therefore, be eligible for command-based invalidation.
When building the command-based invalidation policies in cachespec.xml, keep in mind the following restrictions:

- Only the methods invoked by the command that return the input instance variables can be used in the method component.
- All the methods that are used to construct the invalidation IDs, must be provided in the command interface and be implemented.
- The request attributes component type cannot be used.

Dynacache API and CACHEIVL table invalidation:

WebSphere Application Server dynamic caching provides the following Java classes to support programmatic invalidation

- com.ibm.websphere.cache.DistributedMap
- com.ibm.wsspi.cache.Cache
- com.ibm.websphere.cache.Cache

WebSphere Commerce provides a **DynaCacheInvalidation** command, which is called by the **scheduler** periodically to process the records in the **CACHEIVL** table and call the above WebSphere Application Server dynamic cache Java classes to invalidate the specified cache entries. By default, the schedule interval is every ten minutes.

Group based invalidation:

Using dependency trees you can to create conceptual groupings of your cache-entries, and invalidate based on those groups.

You can specify additional cache group identifiers to associate multiple cache entries the same group identifier in cachespec.xml. There is no limit on the number of such identifiers -- dependency IDs, that can be defined in a cache entry. You can define more than one dependency ID on the same cache entry and the same dependency identifier can be reused on another cache entry. This mechanism provides a convenient way to remove all related cache entries at the same time by means of a single rule.

The following shows an example in which the same dependency ID and storeId, has been defined on each of the catalog page cache entries. Also, at the end, an invalidation rule is provided in which the invalidation ID is generated in a way that maps to that of the dependency ID when the rule intercepts the command call to StoreStyleUpdateCmd. At execution time, after dynamic cache generates the invalidation ID, it will compare the ID to each of the dependency IDs for the same identifier and value from the cache entries. All catalog page cache entries that are grouped under the dependency ID will be removed.

client server computing with adaptation:

Power aware computing:

The main goal of power aware computing is to conserve energy for routing messages from source to destination. The current era is world of wireless network where the nodes communicate with each other in multi hop fashion. There are different data transmission protocol are used in this technology. Different routing methods will consume more battery power. Power aware routing metrics has provided important role in power aware computing.

There are two types of traffic considered under power aware computing.

- Unicast: Data packets are travels towards single receiver.
- Broadcast: Data packets are travels towards several network nodes.

In unicast, with respect to power consumption there are five Different Routing metrics defined.

- Energy Consumed By one packet.
- Time for Network partition.
- Variance in power level across mobiles
- Cost for one packet
- Maximum mobile cost

To save energy, it is important to minimize all metrics except the time parameter and it has to maximize.

Power Aware Computing Methods:

Data caching: Data are cached at mobile device.
Cache invalidation mechanism: If the data is invalid due to expiry date or modification, then server notify to all the client devices about data invalidation.
Normalization of records: Before transmitting the data, the records should be normalized as example Duplicate records should be suppressed and not transmitted.

Context aware computing:

Context-aware computing or pervasive computing is a mobile computing mechanism in which software applications can discover and take advantage of contextual information such as user location, time of day, nearby users, devices, and user activity.

Some other definitions are:

What it is…

Context-aware computing is:
"software that examines and reacts to an individual's changing context."
By- Schilit, Adams, & Want 1994

"aware of its user's state and surroundings , and help it adaptits behavior"
By- Satyanarayanan 2000
What is context?

"any information that can be used to characterize the situation of an entity."
(Dey et al., 2000)

Classification of context:
- Identity (Who)

- Activity (What)
- Time (When)
- Location (Where)

Application of context:

They proposes three basic functions that should be implemented by any context-aware application.

- Presentation of information and services.

Presentation of information and services means that either it present context information to the user, or use context help the user for selections of actions.

Examples: According to the context, it provides the user's location on the map and nearby sites of interest.

- Automatic execution of services.

Examples: A navigation system that provides you direction when the user misses a turn.

- Storage (and retrieval) of context information.

Example: A context aware system that provides the data related to meeting as who was there, when the meeting occurred and where it was located.

Context-aware applications:

- Context-aware browser (CAB)
- Context-based workplace awareness
- ConaMSN: A context-aware messenger
- InCarMusic: Context-aware music recommendations
- HEP: Context-aware communication service provision

Security and privacy issues :

There are two main security concerns with context-aware systems.

- Ensuring privacy of location and identity information.
- Ensuring secure communications

transactional models: