**AIMAN COLLEGE OF ARTS & SCIENCE FOR WOMEN,TIRUCHIRAPPALLI**

**Class : I M.Sc Computer Science – II Semester**

**Subject Title : Mobile Communications (unit 2 ,3)**

**Subject Code : P16CSE1A**

**Staff Name : A. Gurshith Begum**

**Designation : Asst. Professor**

**Mobile Communications – Unit II – Cheatsheet**

Telecommunications System: **Digital cellular networks** are the segment of the market for mobile and wireless devices which are growing most rapidly. They are the wireless extensions of traditional PSTN or ISDN networks and allow for seamless roaming with the same mobile phone nation or even worldwide. Today, these systems are mainly used for voice traffic. However, data traffic is continuously growing.

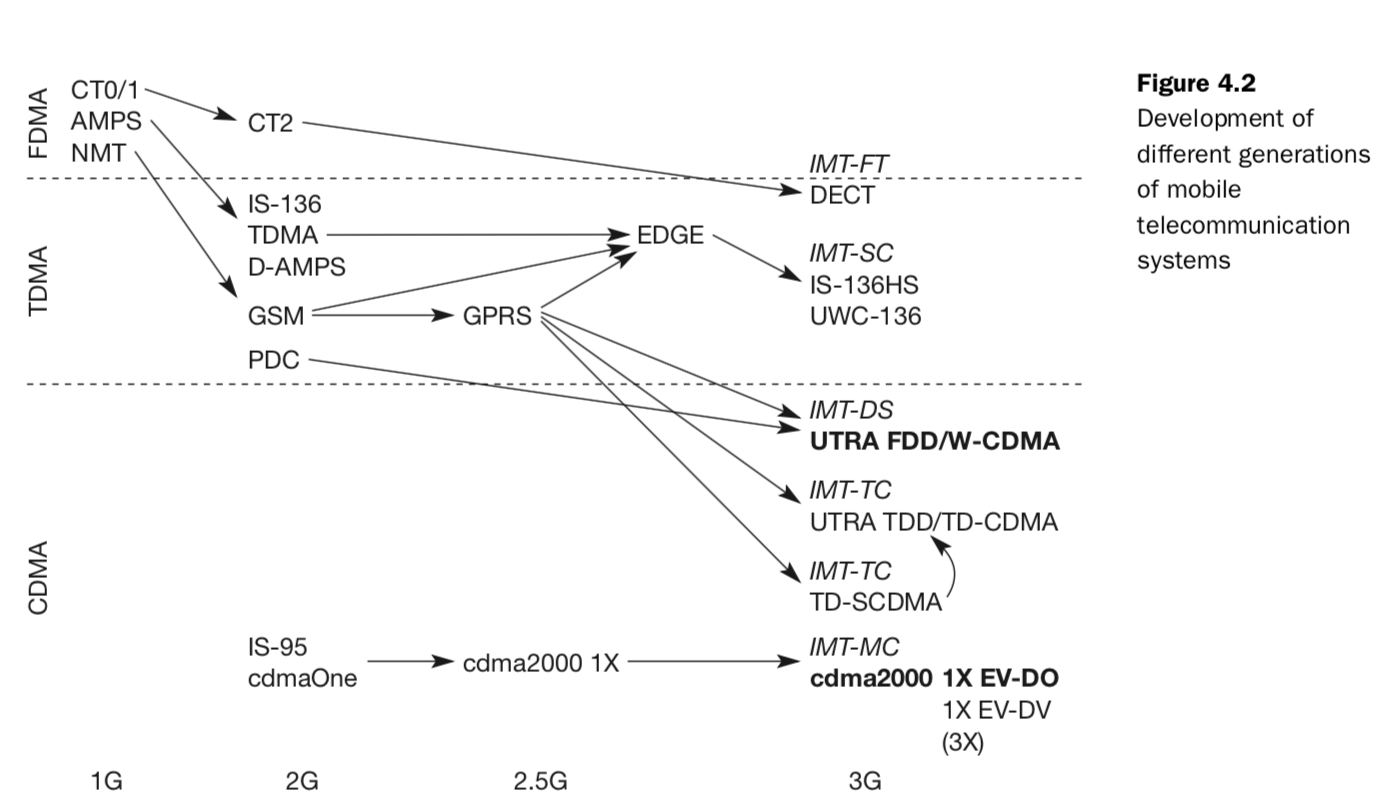
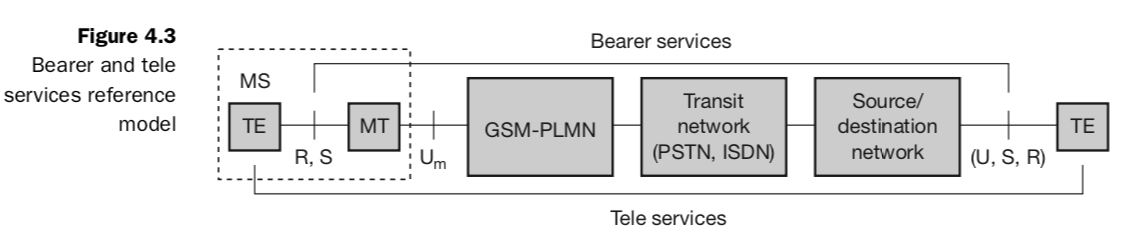


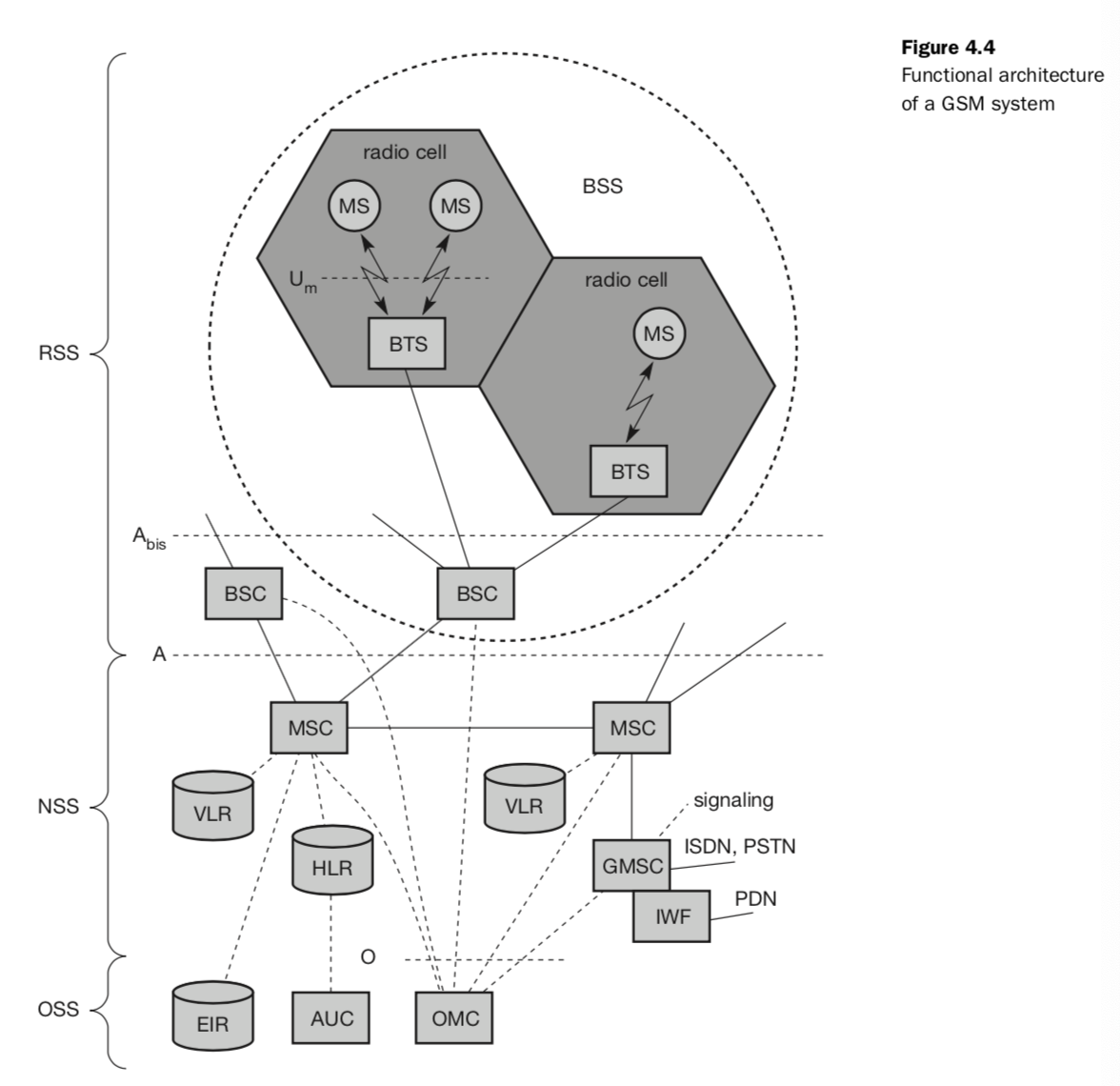
Figure 4.2 shows several development and migration paths for different mobile telecommunication systems. The diagram is divided into the three main multiplexing schemes, FDMA, TDMA, and CDMA. The figure classifies the technologies into three generations. The first generation comprises analog systems, which typically rely on FDMA. The first 2G systems hit the market in the early nineties. In the US **D-AMPS** was a digital successor of **AMPS**, in Europe **GSM** was developed as a replacement for several versions of **NMT**, and **PDC** was introduced in Japan. All these 2G systems introduced a TDMA mechanism in addition to FDMA, which is still used for channel separation. With cdmaOne the first CDMA technology was available in the US as a competitor to the TDMA technologies. Between the second and third generation there is no real revolutionary step. The systems evolved over time: **GPRS** introduced a packet-oriented service and higher data rates to GSM (but can also be used for TDMA systems in general), **EDGE** proposes a new modulation scheme, and **cdmaOne** was enhanced to **cdma2000 1x** offering higher data rates. These systems are often called 2.5G systems. Most systems added CDMA technology to become 3G systems. Cordless telephone systems started with CT0 and CT1, became digital with CT2, and ended in Europe in the fully digital standard **DECT**. This standard has even been chosen as one of the candidates for a 3G system (IMT-FT).

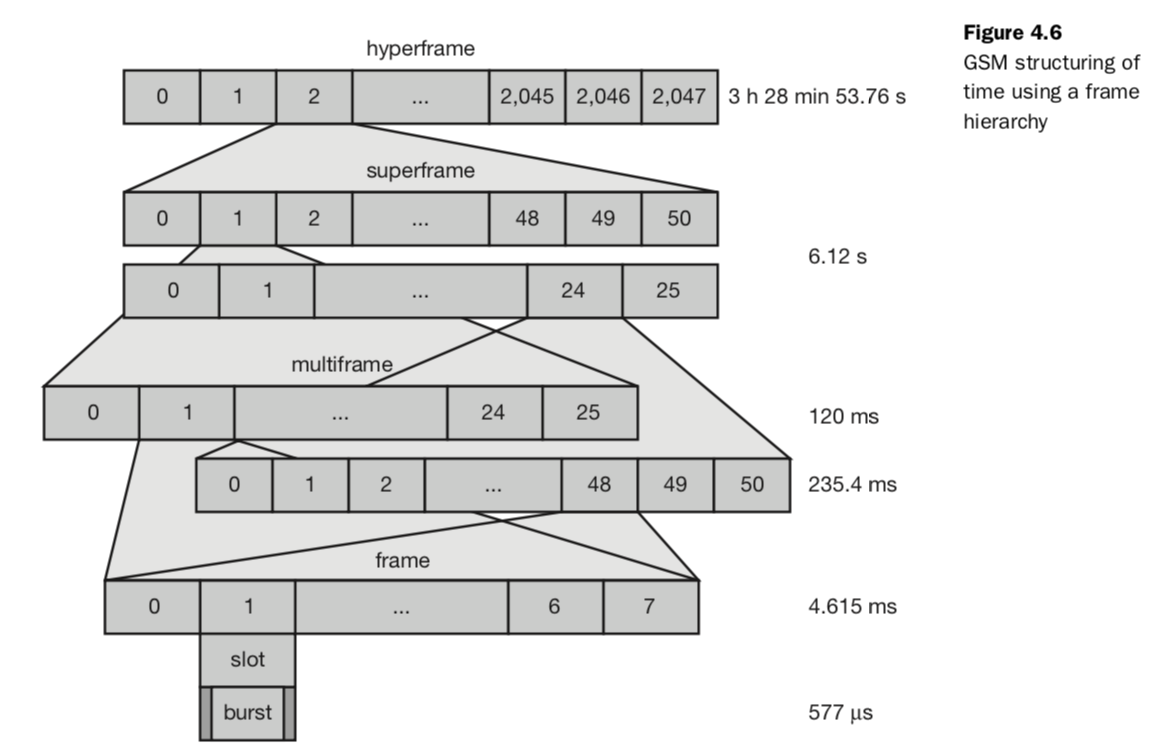
GSM: GSM is the most successful digital mobile telecommunication system in the world today. It is used by over 800 million people in more than 190 countries. In the early 1980s, Europe had numerous coexisting analog mobile phone systems, which were often based on similar standards (e.g., NMT 450), but ran on slightly different carrier frequencies. To avoid this situation for a second generation fully digital system, the groupe spéciale mobile (GSM) was founded in 1982. This system was soon named the global system for mobile communications (GSM), with the specification process lying in the hands of ETSI. In the context of UMTS and the creation of 3GPP (Third generation partnership project) the whole development process of GSM was transferred to 3GPP and further development is combined with 3G development. The primary goal of GSM was to provide a mobile phone system that allows users to roam throughout Europe and provides voice services compatible to ISDN and other PSTN systems. GSM is a typical second generation system, replacing the first generation analog systems, but not offering the high worldwide data rates that the third generation systems, such as UMTS, are promising. GSM has initially been deployed in Europe using 890–915 MHz for uplinks and 935–960 MHz for downlinks – this system is now also called **GSM 900** to distinguish it from the later versions. These versions comprise GSM at 1800 MHz (1710–1785 MHz uplink, 1805–1880 MHz downlink), also called **DCS (digital cellular system) 1800**, and the GSM system mainly used in the US at 1900 MHz (1850–1910 MHz uplink, 1930–1990 MHz downlink), also called **PCS (personal communications service) 1900**. **Mobile Services:** GSM permits the integration of different voice and data services and the inter- working with existing networks. Services make a network interesting for customers. GSM has defined three different categories of services: bearer, tele, and supplementary services.



Bearer services permit transparent and non-transparent, synchronous or asynchronous data transmission. **Transparent bearer services** only use the functions of the physical layer (layer 1) to transmit data. Data transmission has a constant delay and throughput if no transmission errors occur. **Non-transparent bearer services** 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)**. Using transparent and non-transparent services, GSM specifies several bearer services for interworking with PSTN, ISDN, and packet switched public data networks (PSPDN) like X.25, which is available worldwide. GSM mainly focuses on voice-oriented tele services. These comprise encrypted voice transmission, message services, and basic data communication with terminals as known from the PSTN or ISDN (e.g., fax). A useful service for very simple message transfer is the **short message service (SMS)**, which offers transmission of messages of up to 160 characters. SMS messages do not use the standard data channels of GSM but exploit unused capacity in the signalling channels. Sending and receiving of SMS is possible during data or voice transmission. In addition to tele and bearer services, GSM providers can offer **supplementary services**. Similar to ISDN networks, these services offer various enhancements for the standard telephony service, and may vary from provider to provider. Typical services are user **identification**, call **redirection**, or **forwarding** of ongoing calls. Standard ISDN features such as **closed user groups** and **multi-party** communication may be available. Closed user groups are of special interest to companies because they allow, for example, a company-specific GSM sub-network, to which only members of the group have access.

Architecture: As with all systems in the telecommunication area, GSM comes with a hierarchical, complex system architecture comprising many entities, interfaces, and acronyms. Figure 4.4 gives a simplified overview of the GSM system as specified in ETSI (1991b). A GSM system consists of three subsystems, the **radio sub system (RSS)**, the **network and switching subsystem (NSS)**, and the **operation subsystem (OSS)**. Each subsystem will be discussed in more detail in the follow- ing sections. Generally, a GSM customer only notices a very small fraction of the whole network – the mobile stations (MS) and some antenna masts of the base transceiver stations (BTS).

As the name implies, the **radio subsystem (RSS)** comprises all radio specific entities, i.e., the **mobile stations (MS)** and the **base station subsystem (BSS)**. Figure 4.4 shows the connection between the RSS and the NSS via the **A inter- face** (solid lines) and the connection to the OSS via the **O interface** (dashed lines). ● Base station subsystem (**BSS**): A GSM network comprises many BSSs, each controlled by a base station controller (BSC). The BSS performs all functions necessary to maintain radio connections to an MS, coding/decoding of voice, and rate adaptation to/from the wireless network part. Besides a BSC, the BSS contains several BTSs. ● Base transceiver station (**BTS**): A BTS comprises all radio equipment, i.e., antennas, signal processing, amplifiers necessary for radio transmission. A BTS can form a radio cell or, using sectorized antennas, several cells, and is connected to MS via the Um interface (ISDN U interface for mobile use), and to the BSC via the Abis interface. The Um interface contains all the mechanisms necessary for wireless transmission (TDMA, FDMA etc.) and will be discussed in more detail below. The Abis interface consists of 16 or 64 kbit/s connections. A GSM cell can measure between some 100 m and 35 km depending on the environment (buildings, open space, mountains etc.) but also expected traffic. ● Base station controller (**BSC**): The BSC basically manages the BTSs. It reserves radio frequencies, handles the handover from one BTS to another within the BSS, and performs paging of the MS. The BSC also multiplexes the radio channels onto the fixed network connections at the A interface. ● Mobile station **(MS)**: The MS comprises all user equipment and software needed for communication with a GSM network. An MS consists of user independent hard- and software and of the **subscriber identity module (SIM)**, which stores all user-specific data that is relevant to GSM.3 While an MS can be identified via the **international mobile equipment identity (IMEI). Network and switching subsystem (NSS):** The “heart” of the GSM system is formed by the **network and switching sub- system (NSS)**. The NSS connects the wireless network with standard public networks, performs handovers between different BSSs, comprises functions for worldwide localization of users and supports charging, accounting, and roaming of users between different providers in different countries. The NSS consists of the following switches and databases: ● **Mobile services switching center (MSC)**: MSCs are high-performance digital ISDN switches. They set up connections to other MSCs and to the BSCs via the A interface, and form the fixed backbone network of a GSM system. Typically, an MSC manages several BSCs in a geographical region. A **gateway MSC (GMSC)** has additional connections to other fixed networks, such as **PSTN** and **ISDN**. ●  **Home location register (HLR)**: The HLR is the most important database in a GSM system as it stores all user-relevant information. This comprises static information, such as the **mobile subscriber ISDN number (MSISDN)**, sub- scribed services (e.g., call forwarding, roaming restrictions, GPRS), and the **international mobile subscriber identity (IMSI)**. ●  **Visitor location register (VLR)**: The VLR associated to each MSC is a dynamic database which stores all important information needed for the MS users currently in the LA that is associated to the MSC (e.g., IMSI, MSISDN, HLR address). ●  **Visitor location register (VLR)**: The VLR associated to each MSC is a dynamic database which stores all important information needed for the MS users currently in the LA that is associated to the MSC (e.g., IMSI, MSISDN, HLR address). **Operating SubSystem (OSS)**: The third part of a GSM system, the operation subsystem (OSS), contains the necessary functions for network operation and maintenance. The OSS possesses network entities of its own and accesses other entities via SS7 signalling. The following entities have been defined: ● **Operation and maintenance center (OMC)**: The OMC monitors and con- trols all other network entities via the O interface (SS7 with X.25). Typical OMC management functions are traffic monitoring, status reports of net- work entities, subscriber and security management, or accounting and billing. OMCs use the concept of **telecommunication management net- work (TMN).** ● **Authentication centre (AuC**)**:** As the radio interface and mobile stations are particularly vulnerable, a separate AuC has been defined to protect user identity and data transmission. ● **Equipment identity register (EIR):** The EIR is a database for all IMEIs, i.e., it stores all device identifications registered for this network. As MSs are mobile, they can be easily stolen. With a valid SIM, anyone could use the stolen MS. The EIR has a blacklist of stolen (or locked) devices. **Radio Interface:** The most interesting interface in a GSM system is Um, the radio interface, as it comprises many mechanisms presented in chapters 2 and 3 for multiplexing and media access. GSM implements SDMA using cells with BTS and assigns an MS to a BTS. Furthermore, FDD is used to separate downlink and uplink. Media access combines TDMA and FDMA. In GSM 900, 124 channels, each 200 kHz wide, are used for FDMA, whereas GSM 1800 uses, 374 channels. Due to technical reasons, channels 1 and 124 are not used for transmission in GSM 900. Typically, 32 channels are reserved for organizational data; the remaining 90 are used for customers. Each BTS then manages a single channel for organizational data and, e.g., up to 10 channels for user data. The following example is based on the GSM 900 system, but GSM works in a similar way at 1800 and 1900 MHz. Data is transmitted in small portions, called **bursts**.



Protocols:

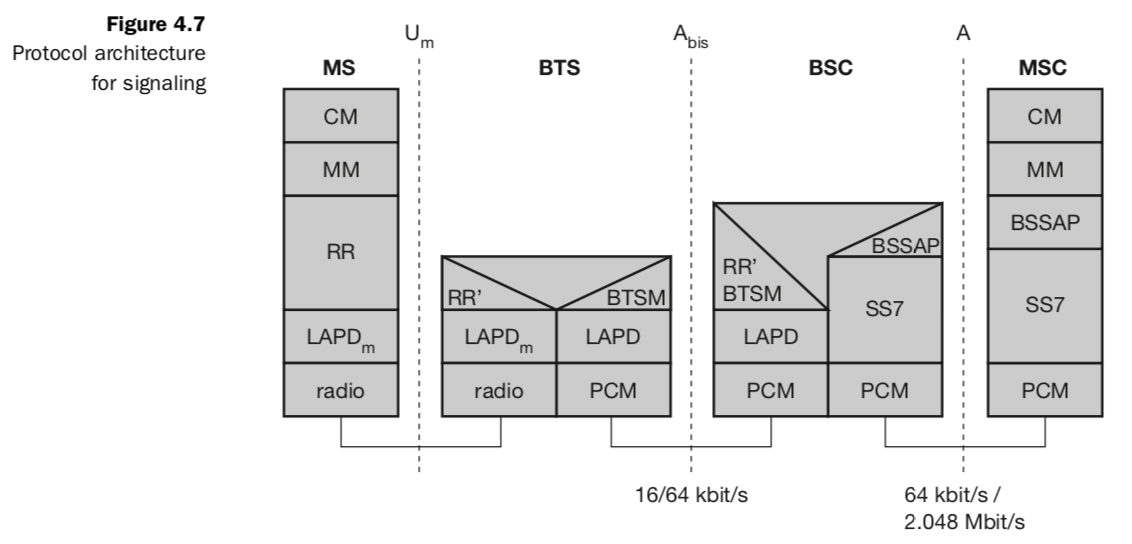
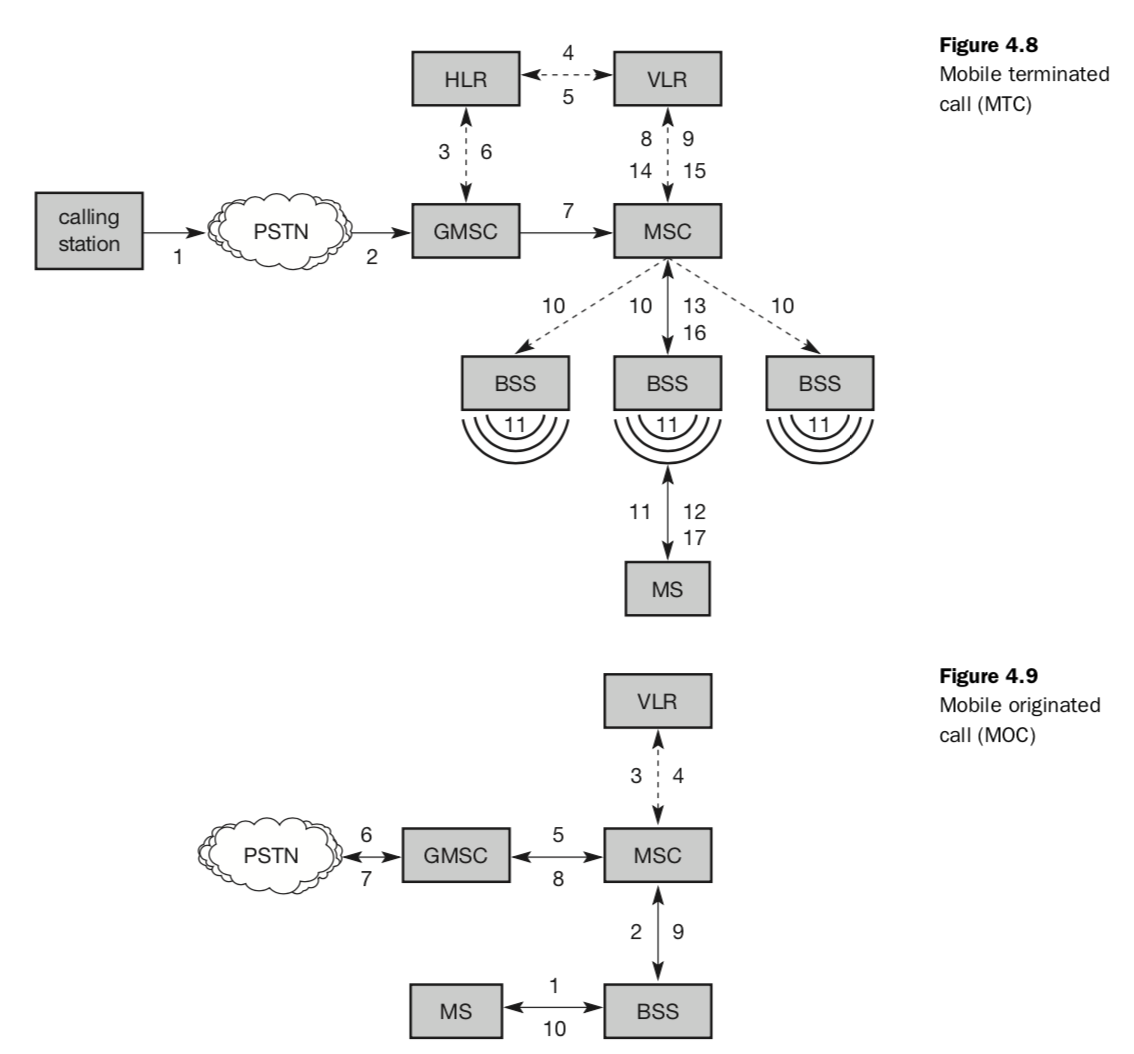
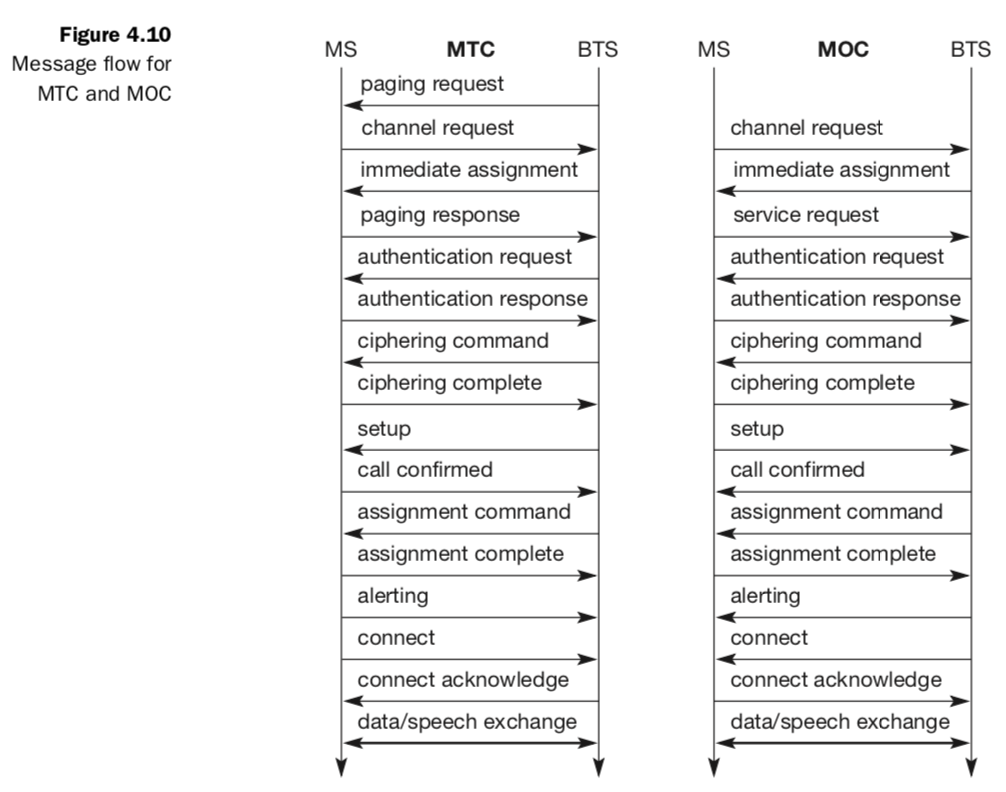
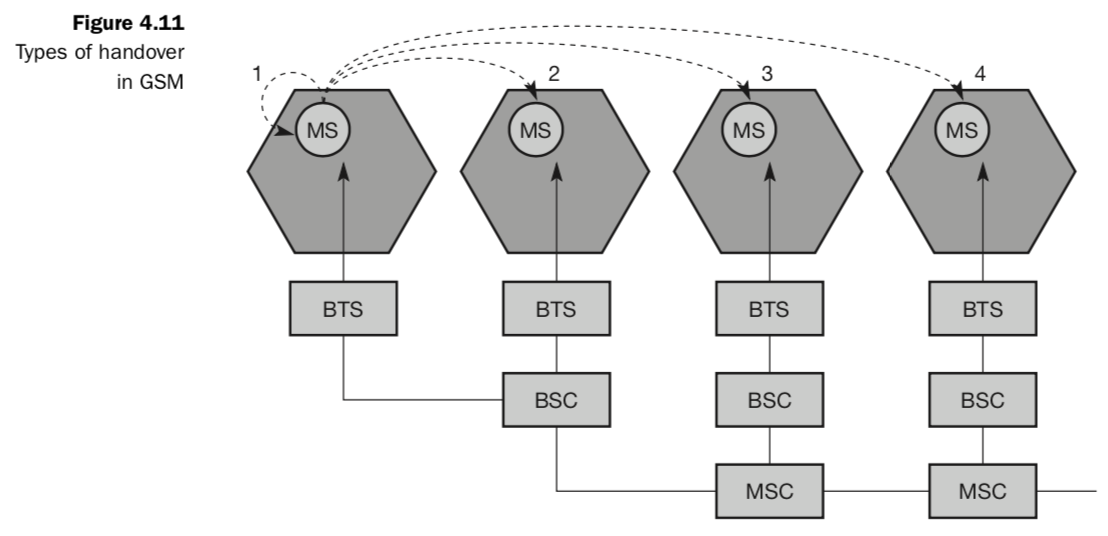


Figure 4.7 shows the protocol architecture of GSM with signalling protocols, interfaces, as well as the entities already shown in Figure 4.4. The main interest lies in the Um interface, as the other interfaces occur between entities in a fixed network. **Layer 1**, the physical layer, handles all **radio**-specific functions. This includes the creation of bursts according to the five different formats, **multi- plexing** of bursts into a TDMA frame, **synchronization** with the BTS, detection of idle channels, and measurement of the **channel qualit**y on the downlink. The physical layer at Um uses GMSK for digital **modulation** and performs **encryption/decryption** of data, i.e., encryption is not performed end-to-end, but only between MS and BSS over the air interface. Synchronization also includes the correction of the individual path delay between an MS and the BTS. All MSs within a cell use the same BTS and thus must be synchronized to this BTS. The BTS generates the time-structure of frames, slots etc. Adjusting the access is controlled via the variable **timing advance**, where a burst can be shifted up to 63 bit times earlier, with each bit having a duration. The main tasks of the physical layer comprise **channel coding** and **error detection/correction**, which is directly combined with the coding mechanisms. Channel coding makes extensive use of different **forward error correction (FEC)** schemes. As voice was assumed to be the main service in GSM, the physical layer also contains special functions, such as **voice activity detection (VAD)**, which transmits voice data only when there is a voice signal. The network layer in GSM, **layer three**, comprises several sublayers. The lowest sublayer is the **radio resource management (RR)**. The functions of RR’ are supported by the BSC via the **BTS management (BTSM)**. **Mobility management (MM)** contains functions for registration, authentication, identification, location updating, and the provision of a **temporary mobile subscriber identity (TMSI)** that replaces the **international mobile subscriber identity (IMSI)** and which hides the real identity of an MS user over the air interface. Finally, the **call management (CM)** layer contains three entities: **call control (CC)**, **short message service (SMS)**, and **supplementary service (SS)**. SMS allows for message transfer using the control channels SDCCH and SACCH (if no signalling data is sent). Layer also provides functions to send in-band tones, called **dual tone multiple frequency (DTMF)**, over the GSM network. Data transmission at the physical layer typically uses **pulse code modulation (PCM)** systems.



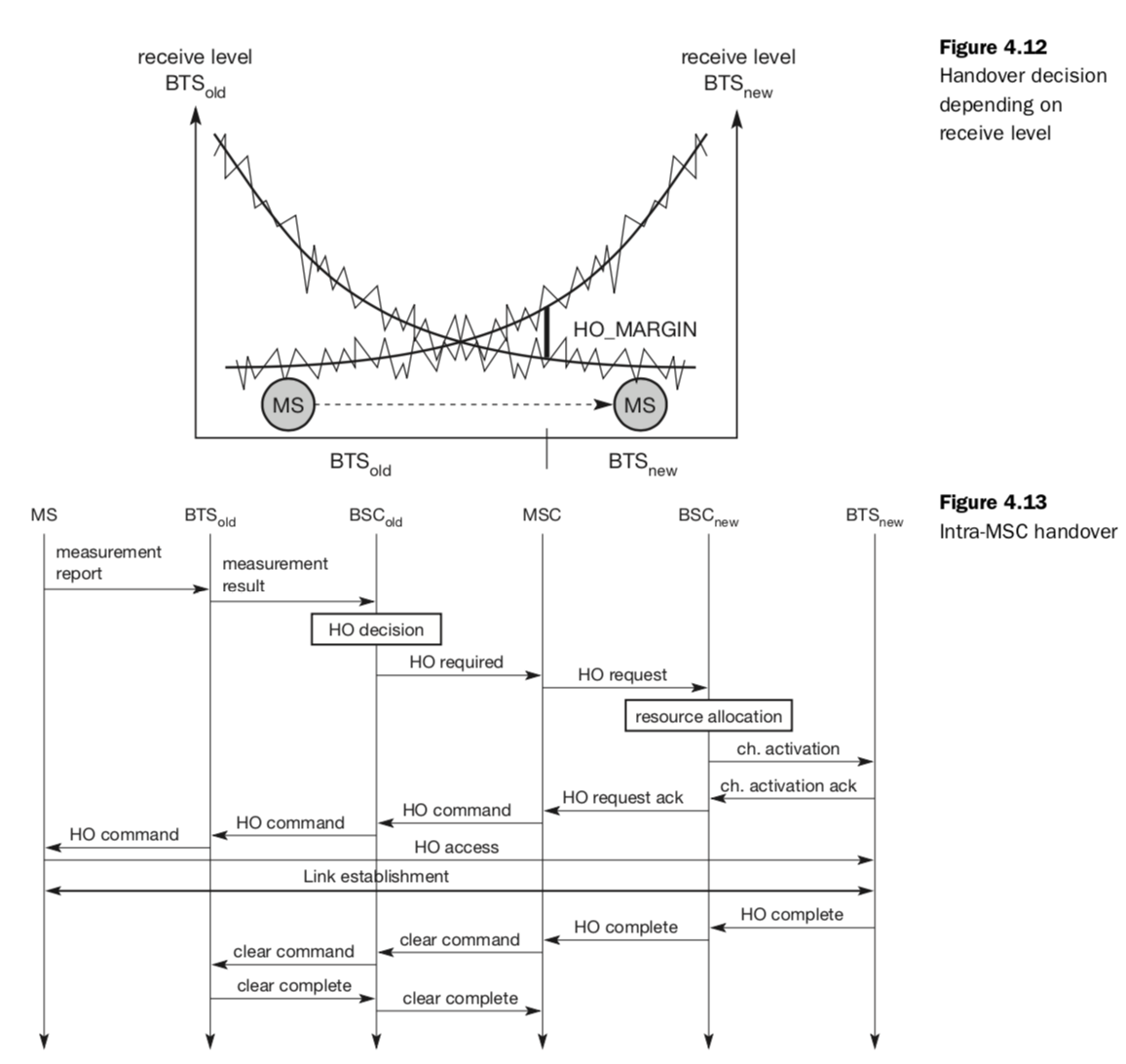


Hand over:

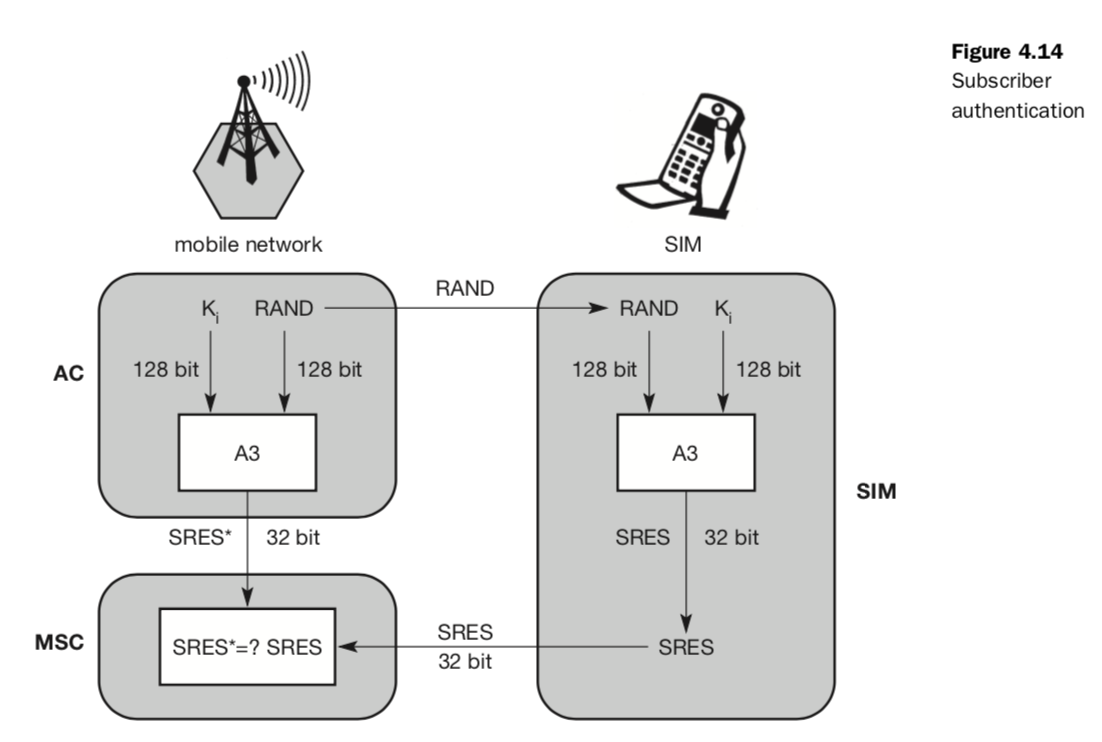


Cellular systems require **handover** procedures, as single cells do not cover the whole service area, but, e.g., only up to 35 km around each antenna on the countryside and some hundred meters in cities (Tripathi, 1998). The smaller the cell size and the faster the movement of a mobile station through the cells (up to 250 km/h for GSM), the more handovers of ongoing calls are required. However, a handover should not cause a cut-off, also called **call drop**. GSM aims at maximum handover duration of 60 ms.

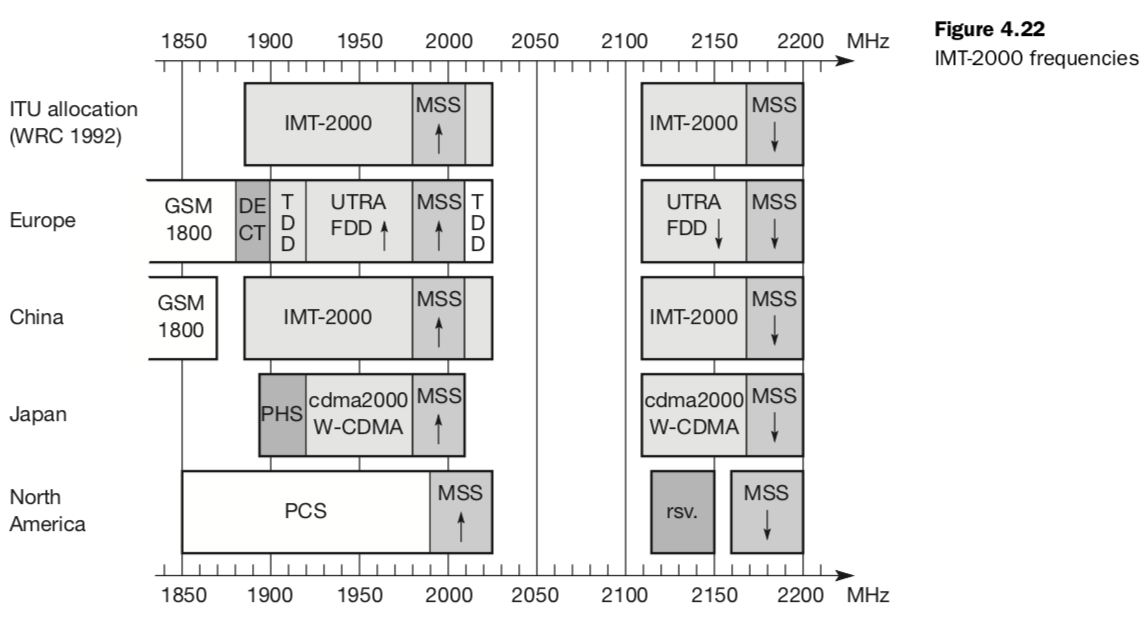
There are two basic reasons for a handover (about 40 have been identified in the standard): ●  The mobile station **moves out of the range** of a BTS or a certain antenna of a BTS respectively. The received **signal level** decreases continuously until it falls below the minimal requirements for communication. The **error rate** may grow due to interference, the distance to the BTS may be too high (max. 35 km) etc. – all these effects may diminish the **quality of the radio link** and make radio transmission impossible in the near future. ●  The wired infrastructure (MSC, BSC) may decide that the **traffic in one cell is too high** and shift some MS to other cells with a lower load (if possible). Handover may be due to **load balancing**. Figure 4.11 shows four possible handover scenarios in GSM: ●  **Intra-cell handover:** Within a cell, narrow-band interference could make transmission at a certain frequency impossible. The BSC could then decide to change the carrier frequency (scenario 1). ●  **Inter-cell, intra-BSC handover:** This is a typical handover scenario. The mobile station moves from one cell to another, but stays within the control of the same BSC. The BSC then performs a handover, assigns a new radio channel in the new cell and releases the old one (scenario 2). ●  I**nter-BSC, intra-MSC handover:** As a BSC only controls a limited number of cells; GSM also has to perform handovers between cells controlled by differ- ent BSCs. This handover then has to be controlled by the MSC (scenario 3). ●  **Inter MSC handover:** A handover could be required between two cells belonging to different MSCs. Now both MSCs perform the handover together (scenario 4).

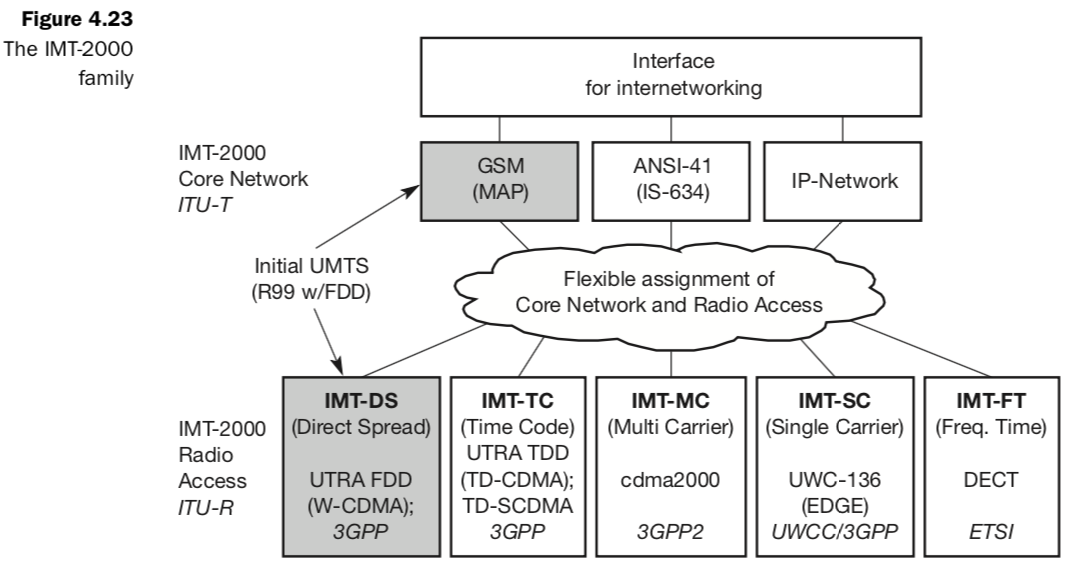


Security: GSM offers several security services using confidential information stored in the AuC and in the individual SIM (which is plugged into an arbitrary MS). The SIM stores personal, secret data and is protected with a PIN against unauthorized use. (For example, the secret key Ki used for authentication and encryption procedures is stored in the SIM.) The security services offered by GSM are explained below: ●  **Access control and authentication:** The first step includes the authentication of a valid user for the SIM. The user needs a secret PIN to access the SIM. The next step is the subscriber authentication (see Figure 4.10). This step is based on a challenge-response scheme. ●  **Confidentiality:** All user-related data is encrypted. After authentication, BTS and MS apply encryption to voice, data, and signalling as shown in section 4.1.7.2. This confidentiality exists only between MS and BTS, but it does not exist end-to-end or within the whole fixed GSM/telephone network. ●  **Anonymity:** To provide user anonymity, all data is encrypted before trans- mission, and user identifiers (which would reveal an identity) are not used over the air. Instead, GSM transmits a temporary identifier (TMSI), which is newly assigned by the VLR after each location update. Additionally, the VLR can change the TMSI at any time. Three algorithms have been specified to provide security services in GSM. **Algorithm A3** is used for **authentication**, **A5** for **encryption**, and **A8** for the **generation of a cipher key**. In the GSM standard only algorithm A5 was publicly available, whereas A3 and A8 were secret, but standardized with open interfaces. Both A3 and A8 are no longer secret, but were published on the inter- net in 1998. This demonstrates that security by obscurity does not really work. As it turned out, the algorithms are not very strong. However, network providers can use stronger algorithms for authentication – or users can apply stronger end-to-end encryption. Algorithms A3 and A8 (or their replacements) are located on the SIM and in the AuC and can be proprietary. Only A5 which is implemented in the devices has to be identical for all providers.

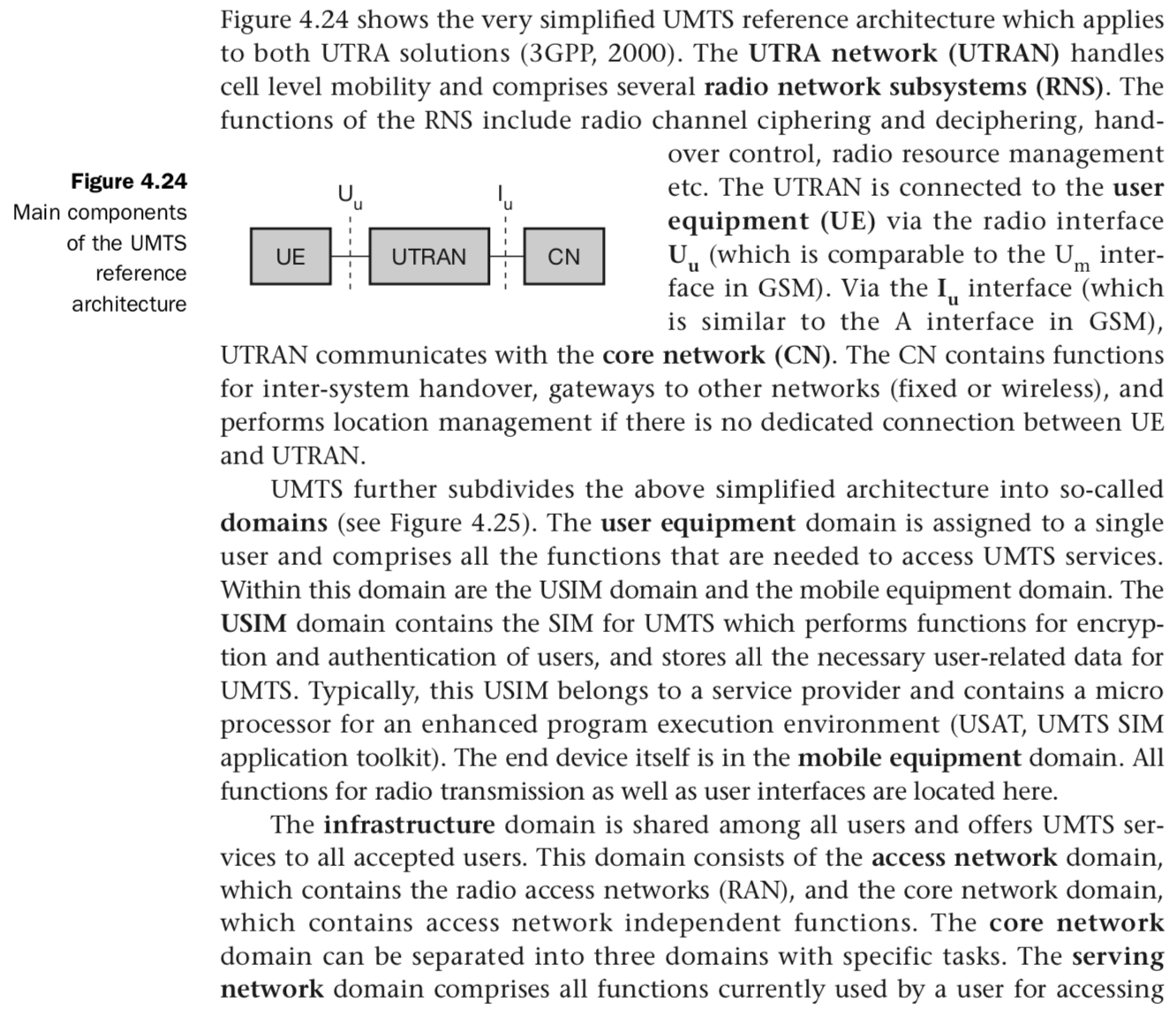


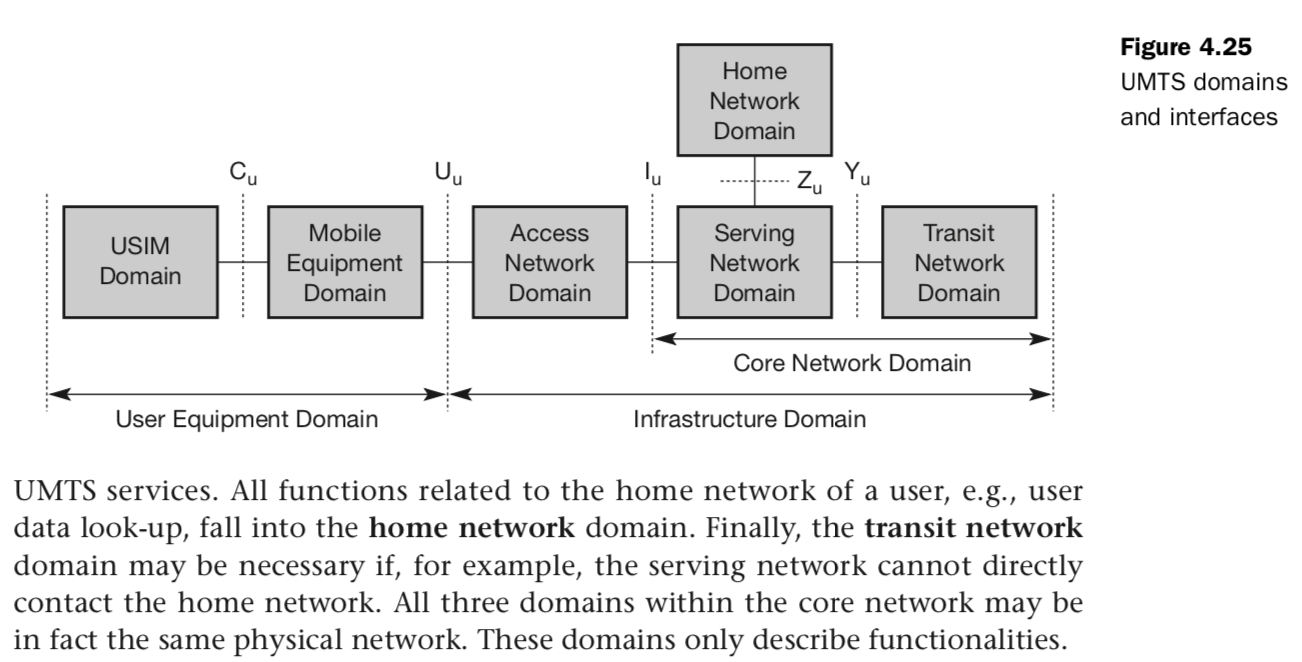
UMTS and IMT 2000: the International Telecommunication Union (ITU) made a request for proposals for radio transmission technologies (RTT) for the **international mobile telecommunications (IMT) 2000** program. IMT-2000, formerly called future public land mobile telecommunication system (FPLMTS), tried to establish a common worldwide communication system that allowed for terminal and user mobility, supporting the idea of universal per- sonal telecommunication (UPT). Within this context, ITU has created several recommendations for FPLMTS systems, e.g., network architectures for FPLMTS (M.817), Requirements for the Radio Interface(s) for FPLMTS (M.1034), or Framework for Services Supported by FPLMTS (M.816). The number 2000 in IMT-2000 should indicate the start of the system (year 2000+x) and the spectrum used (around 2000 MHz). IMT-2000 includes different environments such as indoor use, vehicles, satellites and pedestrians. The world radio conference (WRC) 1992 identified 1885–2025 and 2110–2200 MHz as the frequency bands that should be available worldwide for the new IMT-2000 systems (Recommendation ITU-R M.1036). Within these bands, two times 30 MHz have been reserved for mobile satellite services (MSS).



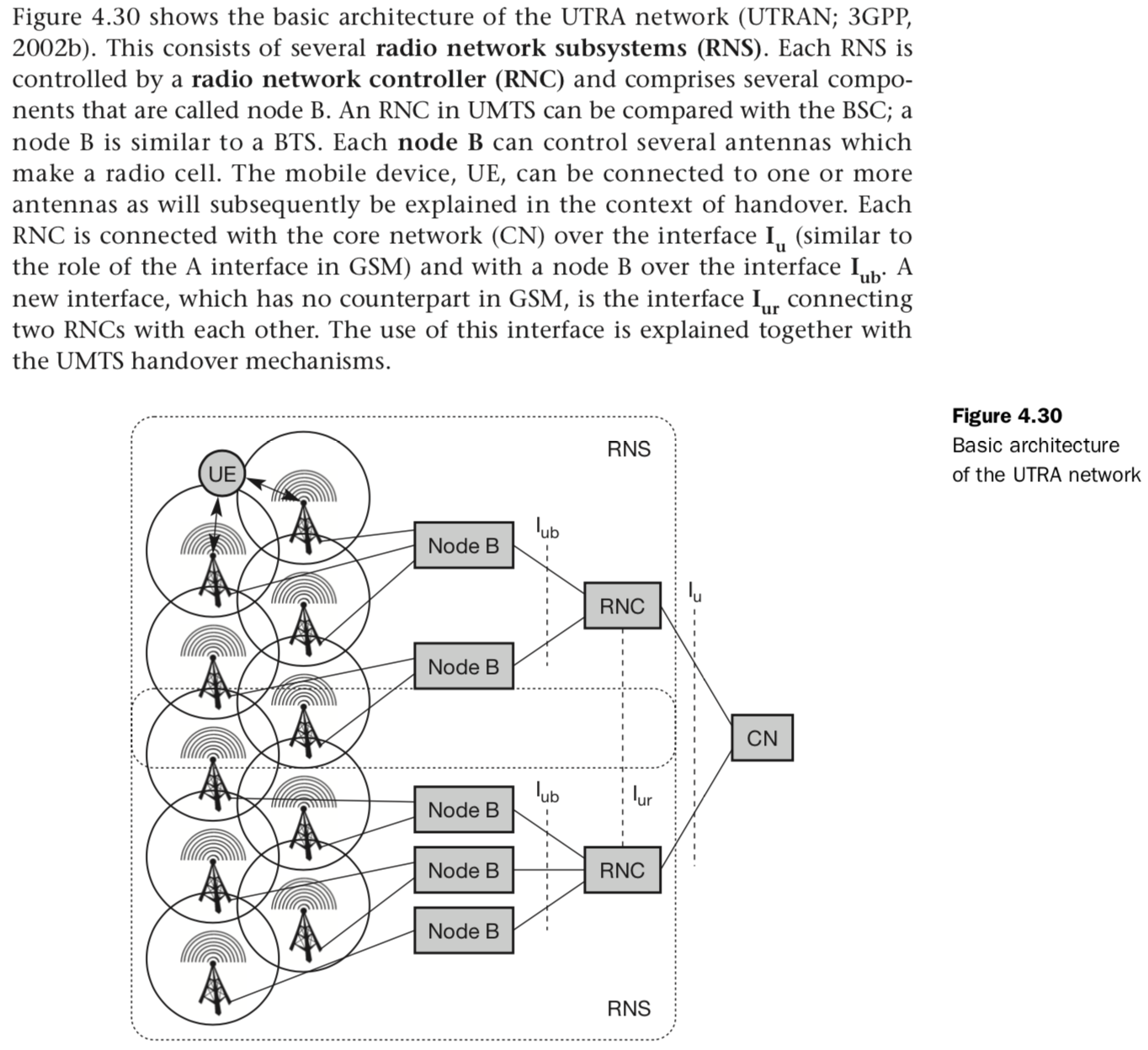


UMTS System Architecture:

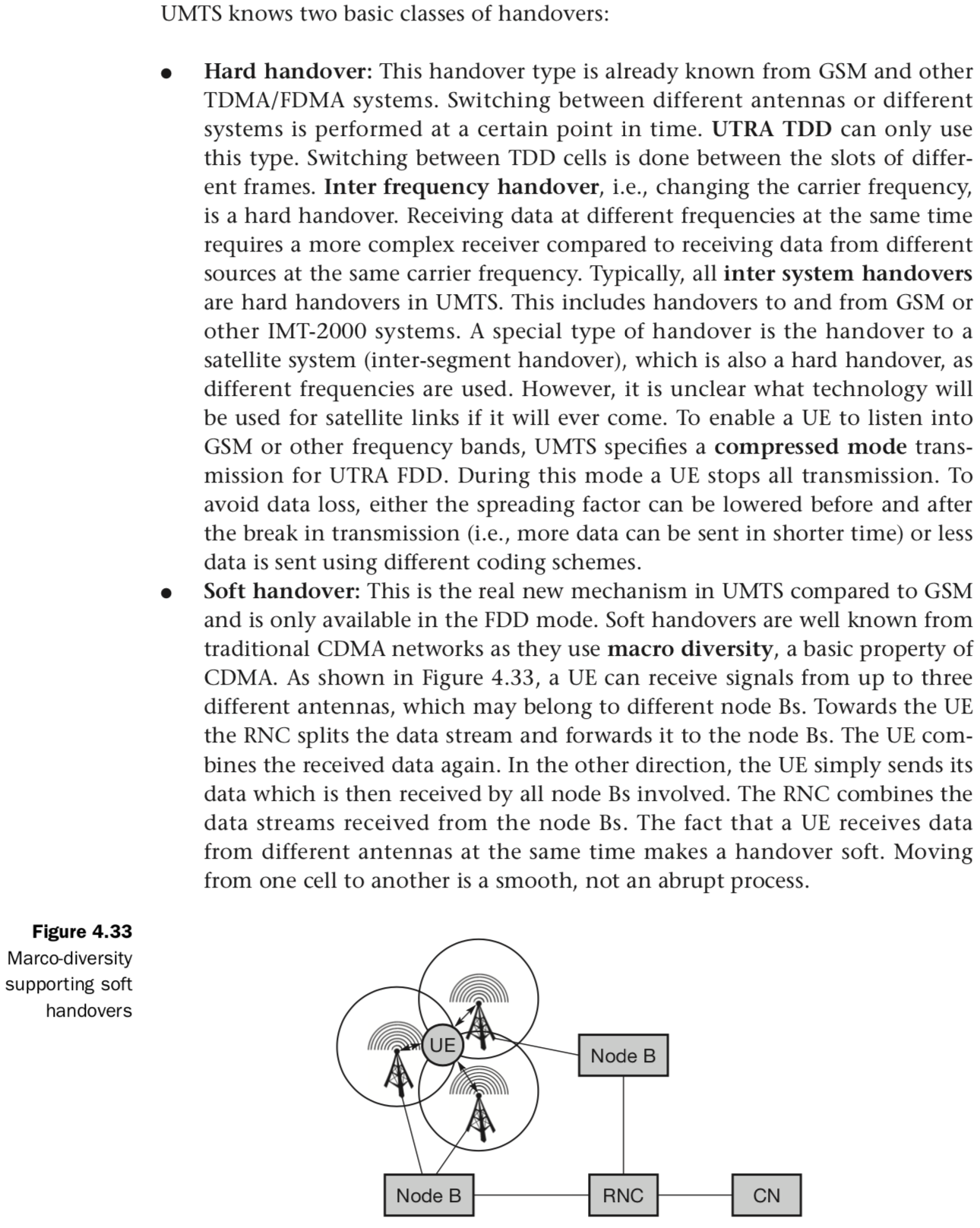


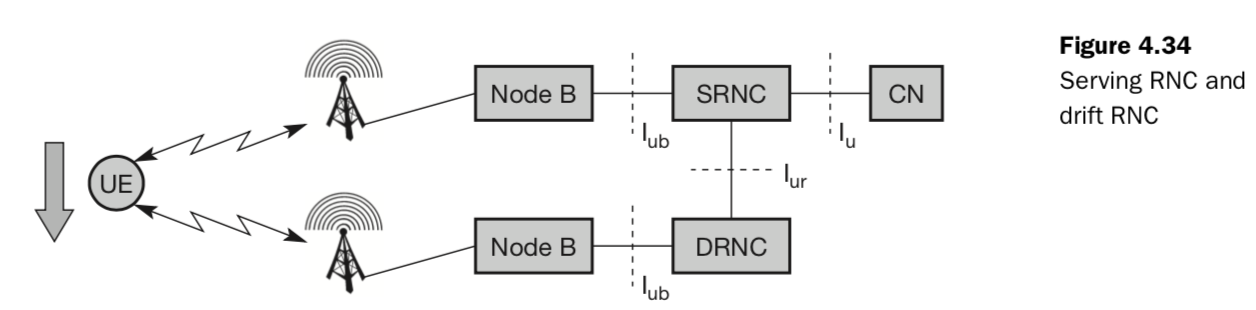


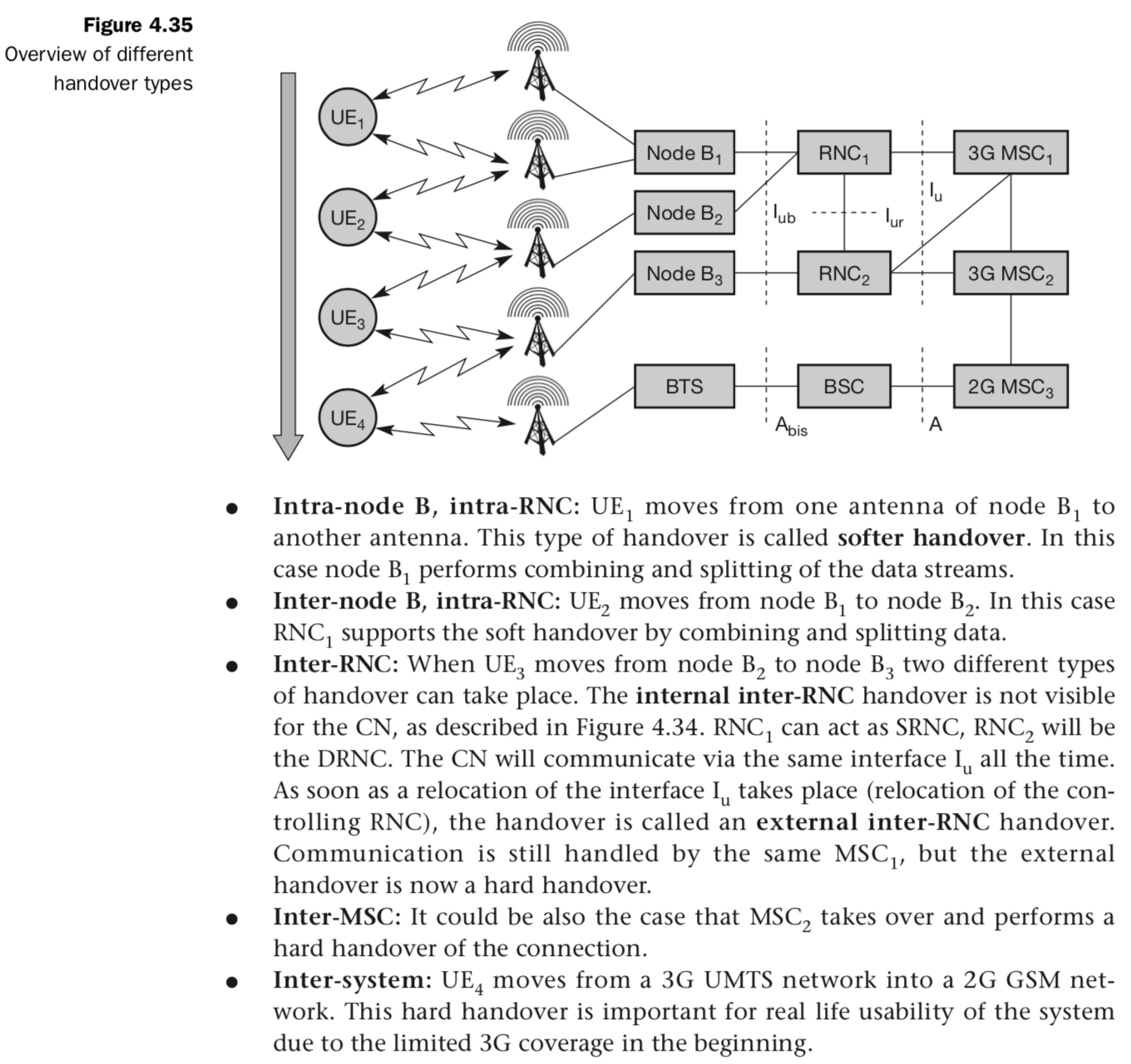
UTRAN Core Network:



Handover & Satellite System:







**===End of Unit II===**

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.

**Requirements for GSM handover**

The process of handover or handoff within any cellular system is of great importance. It is a critical process and if performed incorrectly handover can result in the loss of the call. Dropped calls are particularly annoying to users and if the number of dropped calls rises, customer dissatisfaction increases and they are likely to change to another network. Accordingly GSM handover was an area to which particular attention was paid when developing the standard.

**Types of GSM handover**

Within the GSM system there are four types of handover that can be performed for GSM only systems:

* ***Intra-BTS handover:***   This form of GSM handover occurs if it is required to change the frequency or slot being used by a mobile because of interference, or other reasons. In this form of GSM handover, the mobile remains attached to the same base station transceiver, but changes the channel or slot.
* ***Inter-BTS Intra BSC handover:***   This for of GSM handover or GSM handoff occurs when the mobile moves out of the coverage area of one BTS but into another controlled by the same BSC. In this instance the BSC is able to perform the handover and it assigns a new channel and slot to the mobile, before releasing the old BTS from communicating with the mobile.
* ***Inter-BSC handover:***   When the mobile moves out of the range of cells controlled by one BSC, a more involved form of handover has to be performed, handing over not only from one BTS to another but one BSC to another. For this the handover is controlled by the MSC.
* ***Inter-MSC handover:***   This form of handover occurs when changing between networks. The two MSCs involved negotiate to control the handover.

**GSM handover process**

Although there are several forms of GSM handover as detailed above, as far as the mobile is concerned, they are effectively seen as very similar. There are a number of stages involved in undertaking a GSM handover from one cell or base station to another.

In GSM which uses TDMA techniques the transmitter only transmits for one slot in eight, and similarly the receiver only receives for one slot in eight. As a result the RF section of the mobile could be idle for 6 slots out of the total eight. This is not the case because during the slots in which it is not communicating with the BTS, it scans the other radio channels looking for beacon frequencies that may be stronger or more suitable. In addition to this, when the mobile communicates with a particular BTS, one of the responses it makes is to send out a list of the radio channels of the beacon frequencies of neighbouring BTSs via the Broadcast Channel (BCCH).

The mobile scans these and reports back the quality of the link to the BTS. In this way the mobile assists in the handover decision and as a result this form of GSM handover is known as Mobile Assisted Hand Over (MAHO).

The network knows the quality of the link between the mobile and the BTS as well as the strength of local BTSs as reported back by the mobile. It also knows the availability of channels in the nearby cells. As a result it has all the information it needs to be able to make a decision about whether it needs to hand the mobile over from one BTS to another.

If the network decides that it is necessary for the mobile to hand over, it assigns a new channel and time slot to the mobile. It informs the BTS and the mobile of the change. The mobile then retunes during the period it is not transmitting or receiving, i.e. in an idle period.

A key element of the GSM handover is timing and synchronisation. There are a number of possible scenarios that may occur dependent upon the level of synchronisation.

* ***Old and new BTSs synchronised:***   In this case the mobile is given details of the new physical channel in the neighbouring cell and handed directly over. The mobile may optionally transmit four access bursts. These are shorter than the standard bursts and thereby any effects of poor synchronisation do not cause overlap with other bursts. However in this instance where synchronisation is already good, these bursts are only used to provide a fine adjustment.
* ***Time offset between synchronised old and new BTS:***   In some instances there may be a time offset between the old and new BTS. In this case, the time offset is provided so that the mobile can make the adjustment. The GSM handover then takes place as a standard synchronised handover.
* ***Non-synchronised handover:***   When a non-synchronised cell handover takes place, the mobile transmits 64 access bursts on the new channel. This enables the base station to determine and adjust the timing for the mobile so that it can suitably access the new BTS. This enables the mobile to re-establish the connection through the new BTS with the correct timing.

**Inter-system handover**

With the evolution of standards and the migration of GSM to other 2G technologies including to 3G UMTS / WCDMA as well as HSPA and then LTE, there is the need to handover from one technology to another. Often the 2G GSM coverage will be better then the others and GSM is often used as the fallback. When handovers of this nature are required, it is considerably more complicated than a straightforward only GSM handover because they require two technically very different systems to handle the handover.

These handovers may be called intersystem handovers or inter-RAT handovers as the handover occurs between different radio access technologies.

The most common form of intersystem handover is between GSM and UMTS / WCDMA. Here there are two different types:

* ***UMTS / WCDMA to GSM handover:***   There are two further divisions of this category of handover:
  + Blind handover:   This form of handover occurs when the base station hands off the mobile by passing it the details of the new cell to the mobile without linking to it and setting the timing, etc of the mobile for the new cell. In this mode, the network selects what it believes to be the optimum GSM based station. The mobile first locates the broadcast channel of the new cell, gains timing synchronisation and then carries out non-synchronised intercell handover.
  + Compressed mode handover:   using this form of handover the mobile uses the gaps I transmission that occur to analyse the reception of local GSM base stations using the neighbour list to select suitable candidate base stations. Having selected a suitable base station the handover takes place, again without any time synchronisation having occurred.
* ***Handover from GSM to UMTS / WCDMA:***   This form of handover is supported within GSM and a "neighbour list" was established to enable this occur easily. As the GSM / 2G network is normally more extensive than the 3G network, this type of handover does not normally occur when the mobile leaves a coverage area and must quickly find a new base station to maintain contact. The handover from GSM to UMTS occurs to provide an improvement in performance and can normally take place only when the conditions are right. The neighbour list will inform the mobile when this may happen.

GSM is a second generation or 2G mobile phone system. Originally introduced in 1991, it is still used for many voice calls and some low data rate services that require its use.

The acronym for GSM originally meant Groupe Speciale Mobile, but this changed to Global System for Mobile Communications as the system spread on a global basis.

The use of GSM grew beyond all the original expectations. Initially it had been conceived as a European system, but its use spread globally and by 2004 there were over a billion subscriptions - a milestone achievement as it had taken over 100 years for landlines to reach this point.

Although technology has moved on significantly since the introduction of GSM as a 2G technology, it is still in widespread use as phones are low cost, and battery usage small enabling battery charge intervals to be often a week or more.

## What is GSM - system overview

The GSM system was designed as a second generation (2G) cellular phone technology. One of the basic aims was to provide a system that would enable greater capacity to be achieved than the previous first generation analogue systems. GSM achieved this by using a digital TDMA (time division multiple access approach).

By adopting this technique more users could be accommodated within the available bandwidth. In addition to this, ciphering of the digitally encoded speech was adopted to retain privacy. Using the earlier analogue cellular technologies it was possible for anyone with a scanner receiver to listen to calls and a number of famous personalities had been "eavesdropped" with embarrassing consequences.

#### Note on the History of Mobile Phone Technology:

Mobile phone technology has developed every year. From the first introductions of cellular phone systems in the 1980s to current day, new technology development has steadily improved the systems available. Starting with the first generation analogues systems, new 2G digital systems were introduced and these have moved on so that 5G technology is now being developed.

## GSM services

Speech or voice calls are obviously the primary function for the GSM cellular system. To achieve this the speech is digitally encoded and later decoded using a vocoder. A variety of vocoders are available for use, being aimed at different scenarios.

In addition to the voice services, GSM cellular technology supports a variety of other data services. Although their performance is nowhere near the level of those provided by 3G, they are nevertheless still important and useful. A variety of data services are supported with user data rates up to 9.6 kbps. Services including Group 3 facsimile, videotext and teletex can be supported.

One service that has grown enormously is the short message service. Developed as part of the GSM specification, it has also been incorporated into other cellular technologies. It can be thought of as being similar to the paging service but is far more comprehensive allowing bi-directional messaging, store and forward delivery, and it also allows alphanumeric messages of a reasonable length. This service has become particularly popular, initially with the young as it provided a simple, low fixed cost.

## GSM basics

The GSM cellular technology had a number of design aims when the development started:

* It should offer good subjective speech quality
* It should have a low phone or terminal cost
* Terminals should be able to be handheld
* The system should support international roaming
* It should offer good spectral efficiency
* The system should offer ISDN compatibility

The resulting GSM cellular technology that was developed provided for all of these. The overall system definition for GSM describes not only the air interface but also the network or infrastructure technology.

By adopting this approach it is possible to define the operation of the whole network to enable international roaming as well as enabling network elements from different manufacturers to operate alongside each other, although this last feature did not fully work out, especially with older items.

The RF or air interface of GSM cellular technology uses 200 kHz RF channels. These are time division multiplexed to enable up to eight users to access each carrier. In this way it is a TDMA / FDMA system.

The base transceiver stations (BTS) are organised into small groups, controlled by a base station controller (BSC) which is typically co-located with one of the BTSs. The BSC with its associated BTSs is termed the base station subsystem (BSS).

Further into the core network is the main switching area. This is known as the mobile switching centre (MSC). Associated with it is the location registers, namely the home location register (HLR) and the visitor location register (VLR) which track the location of mobiles and enable calls to be routed to them. Additionally there is the Authentication Centre (AuC), and the Equipment Identify Register (EIR) that are used in authenticating the mobile before it is allowed onto the network and for billing. The operation of these are explained in the following pages.

Last but not least is the mobile itself. Often termed the ME or mobile equipment, this is the item that the end user sees. This element of the overall network architecture introduced some new items and it fuelled the growth of the overall mobile phone ecosystem.

One important feature that was first implemented on GSM was the use of a Subscriber Identity Module. This card carried with it the users identity and other information to allow the user to upgrade a phone very easily, while retaining the same identity on the network. It was also used to store other information such as "phone book" and other items.

The introduction of the SIM has enabled people to change phones very easily, and this has fuelled the phone manufacturing industry and enabled new phones with additional features to be launched. This has allowed mobile operators to increase their average revenue per user (ARPU) by ensuring that users are able to access any new features that may be launched on the network requiring more sophisticated phones.

Battery life was another important aspect, and using GMSK meant that the RF transmitter amplifier deficiency could be high, allowing battery life times to be in excess of several days, especially as battery technology improved.

## GSM SMS Messages

Another capability of GSM that took off in a manner that was not expected was that of texting. SMS messaging was used for the first time on 3 December 1992, when Neil Papworth, used a personal computer to send the text message "Merry Christmas" via the UK Vodafone GSM network.

Although the principle of text messaging was established in 1992, it was not until 1994 that the Finnish network provider Radiolinja became the first to offer a commercial person-to-person SMS text messaging service.

Once text messaging became established it soon took off as it provider a much cheaper way of sending messages than making a call. As a result many you people used it as mobile phone usage had spread and the younger generation could manage costs much better by sending texts.

As a result of the usage of SMS messaging on the GSM network, it became adopted by other 2G systems as it provided additional revenue for the network providers, and a cheap form of communications fo the users.

## GSM system overview

The table below summarises the main points of the GSM system specification, showing some of the highlight features of technical interest.

| **SPECIFICATION SUMMARY FOR GSM CELLULAR SYSTEM** | |
| --- | --- |
| Multiple access technology | FDMA / TDMA |
| Duplex technique | FDD |
| Uplink frequency band | 890 - 915 MHz (basic 900 MHz band only) |
| Downlink frequency band | 933 -960 MHz (basic 900 MHz band only) |
| Channel spacing | 200 kHz |
| Modulation | GMSK |
| Speech coding | Various - original was RPE-LTP/13 |
| Speech channels per RF channel | 8 |
| Channel data rate | 270.833 kbps |
| Frame duration | 4.615 ms |

## Further developments of GSM

GSM was a particularly successful mobile telecommunications system. Initially it had been intended for use within Europe, but within a relatively short while the system was being used well beyond the borders of Europe, becoming an internationally accepted system.

In addition to its success as a voice communications system, it was developed beyond the basic voice capability to be able to carry data. With the Internet becoming more widely used, GSM was developed to start to meet these needs.

* ***GPRS:***   GPRS, the General Packet Radio Service was an evolution of the GSM 2G cellular telecommunications system. Using packet data rather than circuit switched data circuits, it enabled speeds similar to those experienced using dial up networking services to be achieved under ideal conditions. However data speeds were very slow by comparison with the systems used today.

#### Note on 2G GPRS:

GPRS - General Packet Radio System introduced packet data to the GSM cell phone system. Although data was slow by current standards, it enabled data to become a main part of the system.

* ***GSM EDGE :***   GSM EDGE, Enhanced Data rates for GSM Evolution, was the evolution of GSM, & GPRS which used 8PSK modulation to achieve data transfer rates up to 384 kbps. Although this provided a significant increase over GPRS, data speeds were still very slow.

#### Note on 2G GSM EDGE:

GSM EDGE - Enhanced Data rates for GSM Evolution provided for an increase in the data rates achievable by the 2G GSM based system. By using packet data (already used on GPRS) and changing the modulation format to 8PSK, considerable increases in data Read performance were obtained.

As GSM evolved providing more than just voice calls as it started to carry data, it started to show the way that mobile communications technology would develop.

Top of Form

Although it took some years, GSM steadily became the dominant 2G mobile phone system. Ground-breaking attributes like the SIM card enabling the same number and account to be retained when the phone was upgraded along with aspects like international roaming gave it a significant lead over other systems.

Even many years later the basic GSM network and the GSM upgrade technologies and architecture are being used to provide legacy service for many systems that relay on a basic technology. Although operators have reduced the spectrum available to it, GSM is still likely to be maintained for quite a number of years to come.

The GSM network architecture provided a simple and yet effective architecture to provide the services needed for a 2G cellular or mobile communications system.

There were four main elements to the overall GSM network architecture and these could often be further split. Elements like the base station controller, MSC, AuC, HLR, VLR and the like are brought together to form the overall system.

The 2G GSM network architecture, although now superseded gives an excellent introduction into some of the basic capabilities required to set up a mobile communications phone network and how all the entities operate together.



A base station antenna carrying 2G GSM signals

**GSM network architecture elements**

In order that the GSM system operates together as a complete system, the overall network architecture brings together a series of data network identities, each with several elements.

The GSM network architecture is defined in the GSM specifications and it can be grouped into four main areas:

* Network and Switching Subsystem (NSS)
* Base-Station Subsystem (BSS)
* Mobile station (MS)
* Operation and Support Subsystem (OSS)

The different elements of the GSM network operate together and the user is not aware of the different entities within the system.

As the GSM network is defined but the specifications and standards, it enables the system to operate reliably together regardless of the supplier of the different elements.

A basic diagram of the overall system architecture for the 2G GSM mobile communications system includes four major elements which are shown below:

Simplified GSM Network Architecture Diagram

Within this diagram the different network areas can be seen - they are grouped into the four areas that provide different functionality, but all operate to enable reliable mobile communications to be achieved.

The overall network architecture provided to be very successful and was developed further to enable 2G evolution to carry data and then with further evolutions to allow 3G to be established.

**Network Switching Subsystem (NSS)**

The GSM system architecture contains a variety of different elements, and is often termed the core network. It is essentially a data network with a various entities that provide the main control and interfacing for the whole mobile network. The major elements within the core network include:

* ***Mobile Services Switching Centre (MSC):***   The main element within the core network area of the overall GSM network architecture is the Mobile switching Services Centre (MSC). The MSC acts like a normal switching node within a PSTN or ISDN, but also provides additional functionality to enable the requirements of a mobile user to be supported. These include registration, authentication, call location, inter-MSC handovers and call routing to a mobile subscriber. It also provides an interface to the PSTN so that the mobile communications calls can be routed from the mobile network to a phone connected to a landline. Interfaces to other MSCs are provided to enable calls to be made to mobiles on different networks.
* ***Home Location Register (HLR):***   This database contains all the administrative information about each subscriber along with their last known location. In this way, the GSM network is able to route calls to the relevant base station for the MS. When a user switches on their phone, the phone registers with the network and from this it is possible to determine which BTS it communicates with so that incoming calls can be routed appropriately. Even when the phone is not active (but switched on) it re-registers periodically to ensure that the network (HLR) is aware of its latest position. There is one HLR per network, although it may be distributed across various sub-centres to for operational reasons.
* ***Visitor Location Register (VLR):***   This contains selected information from the HLR that enables the selected services for the individual subscriber to be provided. The VLR can be implemented as a separate entity, but it is commonly realised as an integral part of the MSC, rather than a separate entity. In this way access is made faster and more convenient.
* ***Equipment Identity Register (EIR):***   The EIR is the entity that decides whether a given mobile equipment may be allowed onto the network. Each mobile equipment has a number known as the International Mobile Equipment Identity. This number, as mentioned above, is installed in the equipment and is checked by the network during registration. Dependent upon the information held in the EIR, the mobile may be allocated one of three states - allowed onto the network, barred access, or monitored in case its problems.
* ***Authentication Centre (AuC):***   The AuC is a protected database that contains the secret key also contained in the user's SIM card. It is used for authentication and for ciphering on the radio channel.
* ***Gateway Mobile Switching Centre (GMSC):***   The GMSC is the point to which a ME terminating call is initially routed, without any knowledge of the MS's location. The GMSC is thus in charge of obtaining the MSRN (Mobile Station Roaming Number) from the HLR based on the MSISDN (Mobile Station ISDN number, the "directory number" of a MS) and routing the call to the correct visited MSC. The "MSC" part of the term GMSC is misleading, since the gateway operation does not require any linking to an MSC.
* ***SMS Gateway (SMS-G):***   The SMS-G or SMS gateway is the term that is used to collectively describe the two Short Message Services Gateways defined in the GSM standards. The two gateways handle messages directed in different directions. The SMS-GMSC (Short Message Service Gateway Mobile Switching Centre) is for short messages being sent to an ME. The SMS-IWMSC (Short Message Service Inter-Working Mobile Switching Centre) is used for short messages originated with a mobile on that network. The SMS-GMSC role is similar to that of the GMSC, whereas the SMS-IWMSC provides a fixed access point to the Short Message Service Centre.

These entities were the main ones used within the GSM network. They were typically co-located, but often the overall core network was distributed around the country where the network was located. This gave some resilience in case of failure.

Although the GSM system was essential a voice system, the core network was a data network as all signals were handled digitally.

**Base Station Subsystem (BSS)**

The Base Station Subsystem (BSS) section of the 2G GSM network architecture that is fundamentally associated with communicating with the mobiles on the network.

It consists of two elements:

* ***Base Transceiver Station (BTS):***   The BTS used in a GSM network comprises the radio transmitter receivers, and their associated antennas that transmit and receive to directly communicate with the mobiles. The BTS is the defining element for each cell. The BTS communicates with the mobiles and the interface between the two is known as the Um interface with its associated protocols.
* ***Base Station Controller (BSC):***   The BSC forms the next stage back into the GSM network. It controls a group of BTSs, and is often co-located with one of the BTSs in its group. It manages the radio resources and controls items such as handover within the group of BTSs, allocates channels and the like. It communicates with the BTSs over what is termed the Abis interface.

The base station subsystem element of the GSM network utilised the radio access technology to enable a number of users to access the system concurrently. Each channel supported up to eight users and by enabling a base station to have several channels, a large number of subscribers could be accommodated by each base station.

Base stations are carefully located by the network provider to enable complete coverage of an area. The area being covered bay a base station often being referred to as a cell.

As it is not possible to prevent overlap of the signals into the adjacent cells, channels used in one cell are not used in the next. In this way interference which would reduce call quality is reduced whilst still maintaining sufficient frequency re-use.

It is important to have the different BTSs linked with the BSS and the BSSs linked back to the core network.

A variety of technologies were used to achieve this. As data rates used within he GSM network were relatively low, E1 or T1 lines were often used, especially for linking the BSS back to the core network.

As more data was required with increasing usage of the GSM network, and also as other cellular technologies like 3G became more widespread, many links used carrier grade Ethernet.

Often remote BTSs were linked using small microwave links as this could reduce the need for the installation of specific lines if none were available. As base stations often needed to be located to provide good coverage rather than in areas where lines could be installed, the microwave link option provided an attractive method for providing a data link for the network.

**Mobile station**

Mobile stations (MS), mobile equipment (ME) or as they are most widely known, cell or mobile phones are the section of a GSM mobile communications network that the user sees and operates. In recent years their size has fallen dramatically while the level of functionality has greatly increased. A further advantage is that the time between charges has significantly increased.

There are a number of elements to the cell phone, although the two main elements are the main hardware and the SIM.

The hardware itself contains the main elements of the mobile phone including the display, case, battery, and the electronics used to generate the signal, and process the data receiver and to be transmitted.

The mobile station, or ME also contains a number known as the International Mobile Equipment Identity (IMEI). This is installed in the phone at manufacture and "cannot" be changed. It is accessed by the network during registration to check whether the equipment has been reported as stolen.

The SIM or Subscriber Identity Module contains the information that provides the identity of the user to the network. It contains are variety of information including a number known as the International Mobile Subscriber Identity (IMSI). As this is included in the SIM, and it means that by moving the SIM card from one mobile to another, the user could easily change mobiles. The ease of changing mobiles whilst keeping the same number meant that people would regularly upgrade, thereby creating a further revenue stream for network providers and helping to increase the overall financial success of GSM.

**Operation and Support Subsystem (OSS)**

The OSS or operation support subsystem is an element within the overall GSM mobile communications network architecture that is connected to components of the NSS and the BSC. It is used to control and monitor the overall GSM network and it is also used to control the traffic load of the BSS. It must be noted that as the number of BS increases with the scaling of the subscriber population some of the maintenance tasks are transferred to the BTS, allowing savings in the cost of ownership of the system.

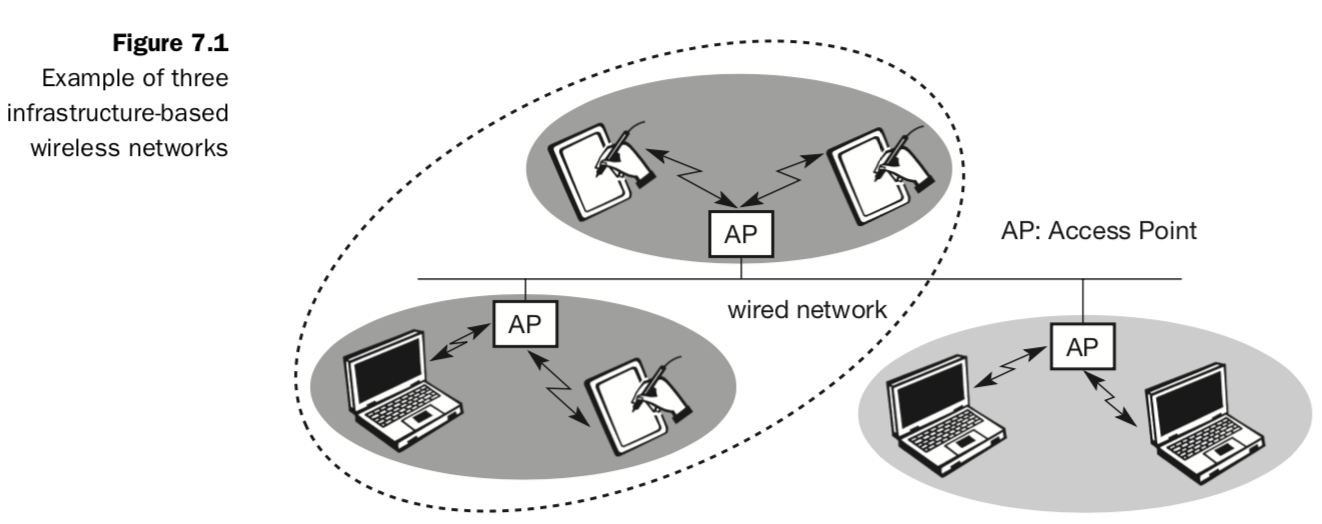
The 2G GSM network architecture follows a logical method of operation. It is far simpler than current mobile phone network architectures which use software defined entities to enable very flexible operation. However the 2G GSM architecture does show the voice and operational basic functions that are needed and how they fit together. As the GSM system was all digital, the network was a data network.

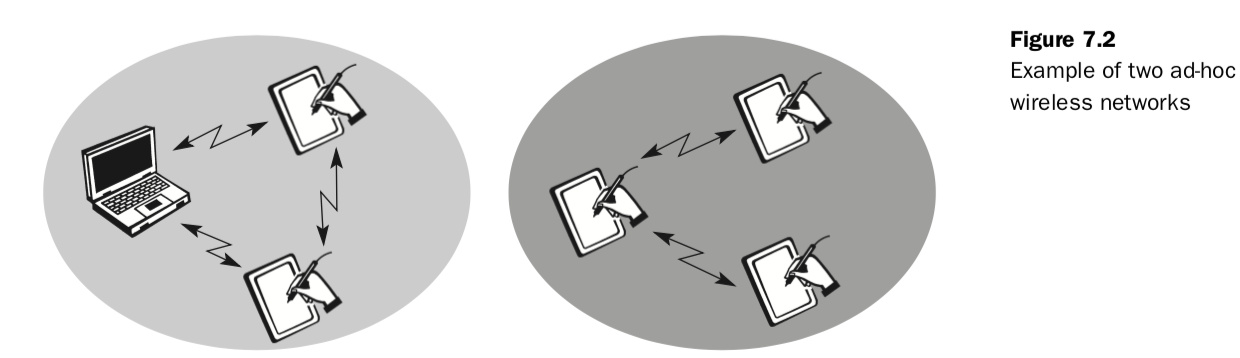
**Mobile Communications – Unit III – Cheatsheet**

Wireless LAN: WLANs are typically restricted in their diameter to buildings, a campus, single rooms etc. and are operated by individuals, not by large-scale network providers. The global goal of WLANs is to replace office cabling, to enable tetherless access to the internet and, to introduce a higher flexibility for ad-hoc communication in, e.g., group meetings. Some **advantages** of WLANs are: ●  **Flexibility:** Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls, senders and receivers can be placed anywhere (also non-visible, e.g., within devices, in walls etc.). Sometimes wiring is difficult if firewalls separate buildings (real firewalls made out of, e.g., bricks, not routers set up as a firewall). Penetration of a firewall is only permitted at certain points to prevent fire from spreading too fast. ●  **Planning:** Only wireless ad-hoc networks allow for communication without previous planning, any wired network needs wiring plans. As long as devices follow the same standard, they can communicate. For wired net- works, additional cabling with the right plugs and probably interworking units (such as switches) have to be provided. ●  **Design:** Wireless networks allow for the design of small, independent devices which can for example be put into a pocket. Cables not only restrict users but also designers of small PDAs, notepads etc. Wireless senders and receivers can be hidden in historic buildings, i.e., current networking technology can be introduced without being visible. ●  **Robustness:** Wireless networks can survive disasters, e.g., earthquakes or users pulling a plug. If the wireless devices survive, people can still communicate. Networks requiring a wired infrastructure will usually break down completely. ●  **Cost:** After providing wireless access to the infrastructure via an access point for the first user, adding additional users to a wireless network will not increase the cost. This is, important for e.g., lecture halls, hotel lobbies or gate areas in airports where the numbers using the network may vary significantly. Using a fixed network, each seat in a lecture hall should have a plug for the network although many of them might not be used permanently. Constant plugging and unplugging will sooner or later destroy the plugs. Wireless connections do not wear out. But WLANs also have several **disadvantages**: ●  **Quality of service:** WLANs typically offer lower quality than their wired counterparts. The main reasons for this are the lower bandwidth due to limitations in radio transmission (e.g., only 1–10 Mbit/s user data rate instead of 100–1,000 Mbit/s), higher error rates due to interference (e.g., 10–4 instead of 10–12 for fiber optics), and higher delay/delay variation due to extensive error correction and detection mechanisms. ●  **Proprietary solutions:** Due to slow standardization procedures, many companies have come up with proprietary solutions offering standardized functionality plus many enhanced features (typically a higher bit rate using a patented coding technology or special inter-access point protocols). However, these additional features only work in a homogeneous environment, i.e., when adapters from the same vendors are used for all wireless nodes. At least most components today adhere to the basic standards IEEE 802.11b or (newer) 802.11a. ●  **Restrictions:** All wireless products have to comply with national regulations. Several government and non-government institutions worldwide regulate the operation and restrict frequencies to minimize interference. Consequently, it takes a very long time to establish global solutions like, e.g., IMT-2000, which comprises many individual standards (see chapter 4). WLANs are limited to low-power senders and certain license-free frequency bands, which are not the same worldwide. ●  **Safety and security:** Using radio waves for data transmission might interfere with other high-tech equipment in, e.g., hospitals. Senders and receivers are operated by laymen and, radiation has to be low. Special pre- cautions have to be taken to prevent safety hazards. The open radio interface makes eavesdropping much easier in WLANs than, e.g., in the case of fiber optics. All standards must offer (automatic) encryption, privacy mechanisms, support for anonymity etc. Otherwise more and more wireless networks will be hacked into as is the case already.

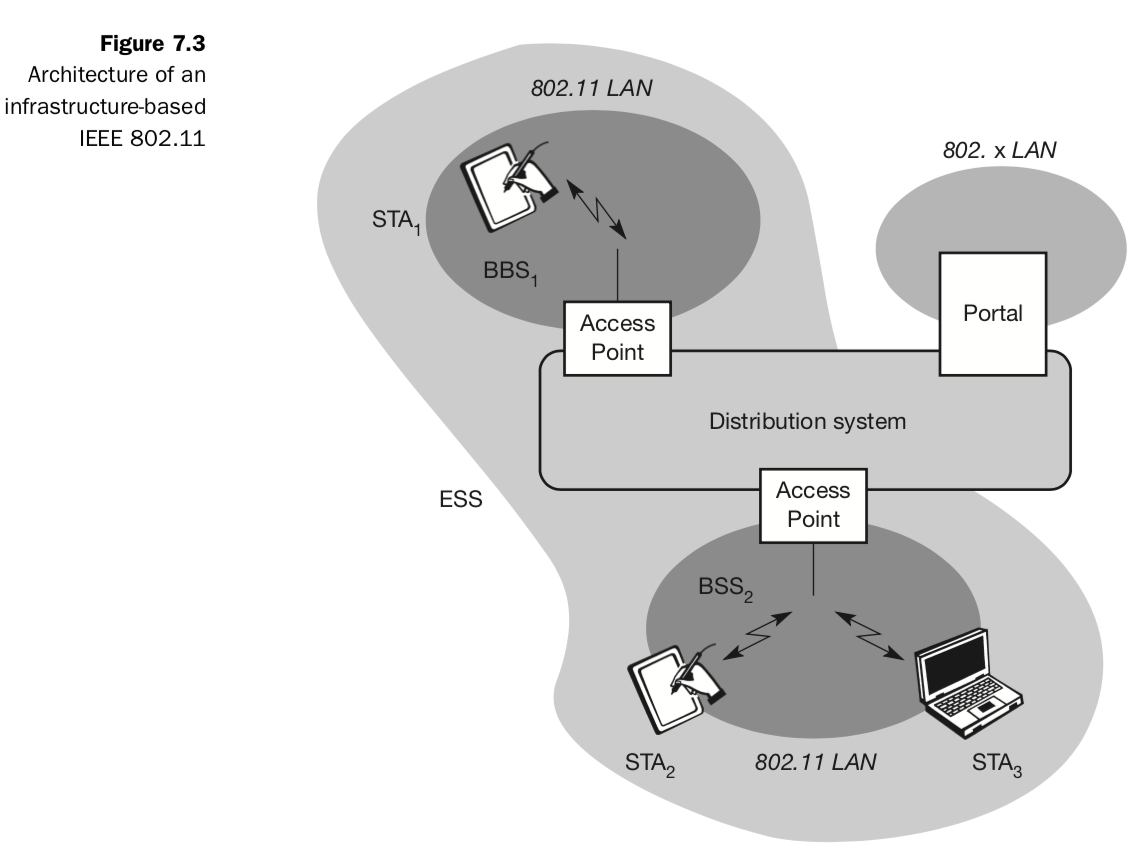
**Infra-red vs radio transmission:** Today, two different basic transmission technologies can be used to set up WLANs. One technology is based on the transmission of infra-red light (e.g., at 900 nm wavelength), the other one, which is much more popular, uses radio transmission in the GHz range (e.g., 2.4 GHz in the license-free ISM band). Both technologies can be used to set up ad-hoc connections for work groups, to connect, e.g., a desk- top with a printer without a wire, or to support mobility within a small area. ●  The main **advantages** of infra-red technology are its simple and extremely cheap senders and receivers which are integrated into nearly all mobile devices available today. PDAs, laptops, notebooks, mobile phones etc. have an infra-red data association (IrDA) interface. Version 1.0 of this industry standard implements data rates of up to 115 kbit/s, while IrDA 1.1 defines higher data rates of 1.152 and 4 Mbit/s. No licenses are needed for infra-red technology and shielding is very simple. Electrical devices do not interfere with infra-red transmission. ●  **Disadvantages** of infra-red transmission are its low bandwidth compared to other LAN technologies. Typically, IrDA devices are internally connected to a serial port limiting transfer rates to 115 kbit/s. Even 4 Mbit/s is not a particularly high data rate. However, their main disadvantage is that infra-red is quite easily shielded. Infra-red transmission cannot penetrate walls or other obstacles. Typically, for good transmission quality and high data rates a LOS, i.e., direct connection, is needed.

Almost all networks described in this book use **radio** waves for data transmission, e.g., GSM at 900, 1,800, and 1,900 MHz, DECT at 1,880 MHz etc. ●  **Advantages** of radio transmission include the long-term experiences made with radio transmission for wide area networks (e.g., microwave links) and mobile cellular phones. Radio transmission can cover larger areas and can penetrate (thinner) walls, furniture, plants etc. Additional coverage is gained by reflection. Radio typically does not need a LOS if the frequencies are not too high. Furthermore, current radio-based products offer much higher transmission rates (e.g., 54 Mbit/s) than infra-red (directed laser links, which offer data rates well above 100 Mbit/s. These are not considered here as it is very difficult to use them with mobile devices). ●  Again, the main advantage is also a big **disadvantage** of radio transmission. Shielding is not so simple. Radio transmission can interfere with other senders, or electrical devices can destroy data transmitted via radio. Additionally, radio transmission is only permitted in certain frequency bands. Very limited ranges of license-free bands are available worldwide and those that are available are not the same in all countries. However, a lot of harmonization is going on due to market pressure.

Many WLANs of today need an **infrastructure** network. Infrastructure networks not only provide access to other networks, but also include forwarding functions, medium access control etc. In these infrastructure-based wireless networks, communication typically takes place only between the wireless nodes and the access point (see Figure 7.1), but not directly between the wireless nodes.



IEEE 802.11: The IEEE standard 802.11 (IEEE, 1999) specifies the most famous family of WLANs in which many products are available. As the standard’s number indicates, this standard belongs to the group of 802.x LAN standards, e.g., 802.3 Ethernet or 802.5 Token Ring. This means that the standard specifies the physical and medium access layer adapted to the special requirements of wire- less LANs, but offers the same interface as the others to higher layers to maintain interoperability. The primary goal of the standard was the specification of a simple and robust WLAN which offers time-bounded and asynchronous services. The MAC layer should be able to operate with multiple physical layers, each of which exhibits a different medium sense and transmission characteristic. Candidates for physical layers were infra-red and spread spectrum radio transmission techniques. System Architecture of IEEE 802.11:



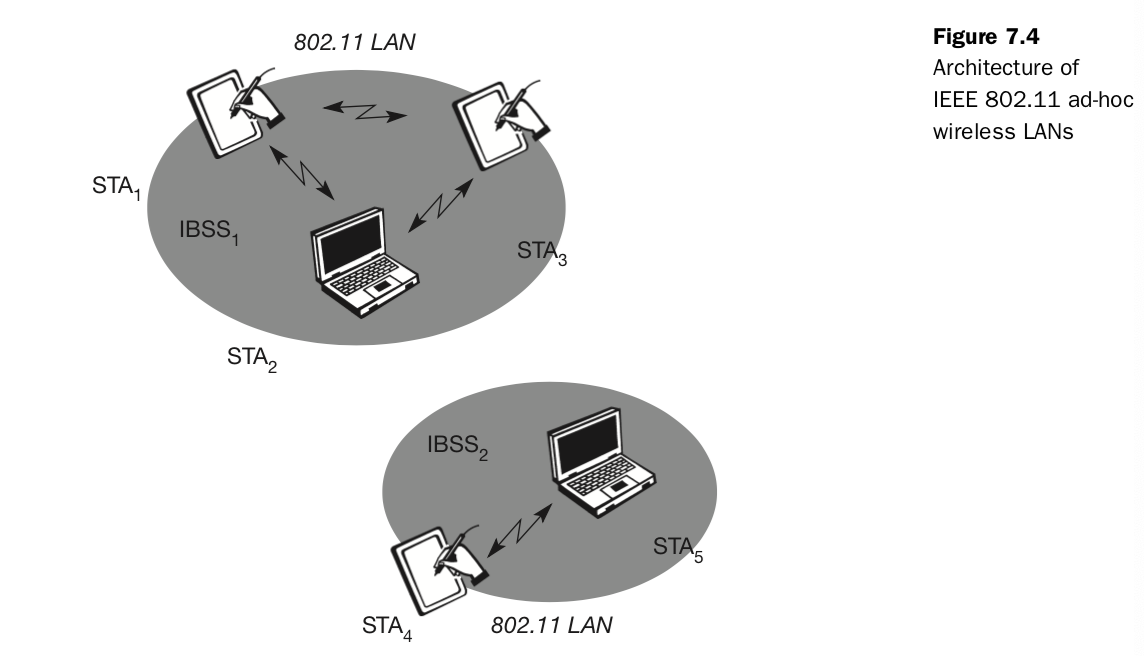
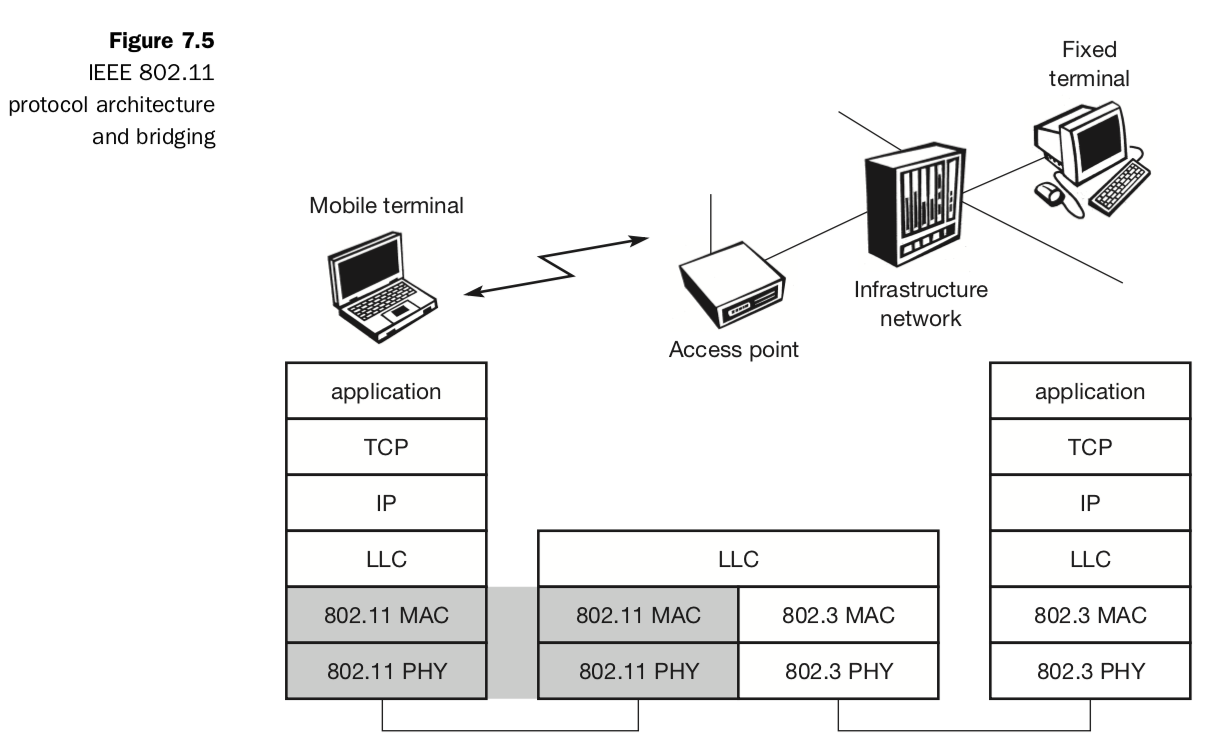
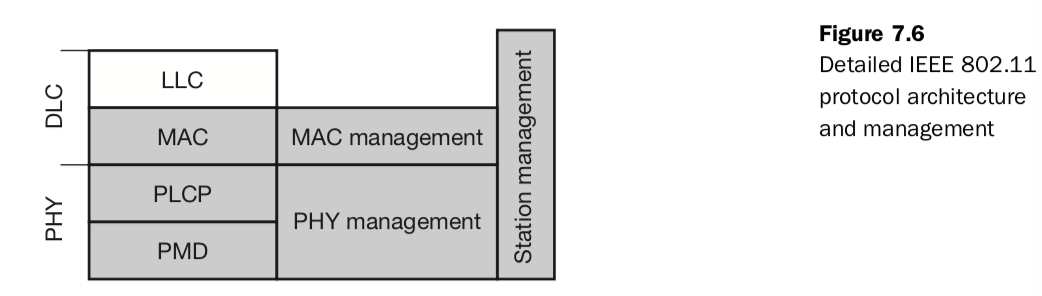
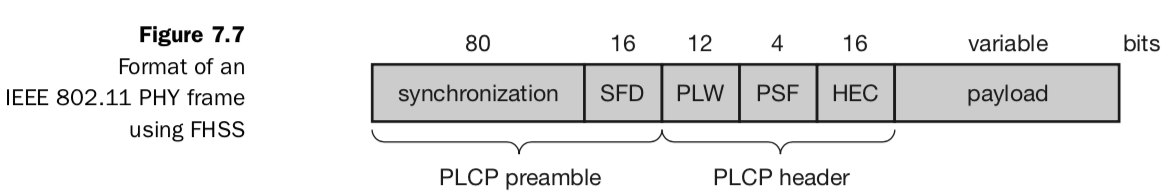


Figure 7.3 shows the components of an infrastructure and a wireless part as specified for IEEE 802.11. Several nodes, called **stations (STAi)**, are connected to **access points (AP)**. Stations are terminals with access mechanisms to the wireless medium and radio contact to the AP. The stations and the AP which are within the same radio coverage form a **basic service set (BSSi)**. The example shows two BSSs – BSS1 and BSS2 – which are connected via a **distribution system**. A distribution system connects several BSSs via the AP to form a single network and thereby extends the wireless cover- age area. This network is now called an **extended service set (ESS)** and has its own identifier, the ESSID. The ESSID is the ‘name’ of a network and is used to separate different networks. Without knowing the ESSID (and assuming no hacking) it should not be possible to participate in the WLAN. The distribution system connects the wireless networks via the APs with a **portal**, which forms the interworking unit to other LANs.

IEEE 802.11 Protocol Architecture: As indicated by the standard number, IEEE 802.11 fits seamlessly into the other 802.x standards for wired LANs. Figure 7.5 shows the most common scenario: an IEEE 802.11 wireless LAN connected to a switched IEEE 802.3 Ethernet via a bridge. Applications should not notice any difference apart from the lower bandwidth and perhaps higher access time from the wireless LAN. The WLAN behaves like a slow wired LAN. Consequently, the higher layers (application, TCP, IP) look the same for wireless nodes as for wired nodes. The upper part of the data link control layer, the logical link control (LLC), covers the differences of the medium access control layers needed for the different media. In many of today’s networks, no explicit LLC layer is visible.

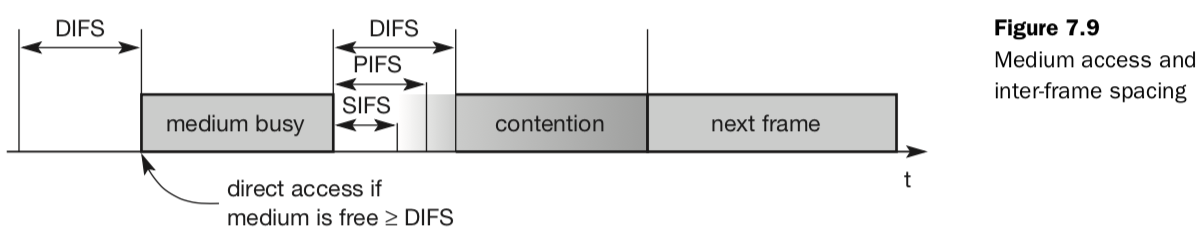




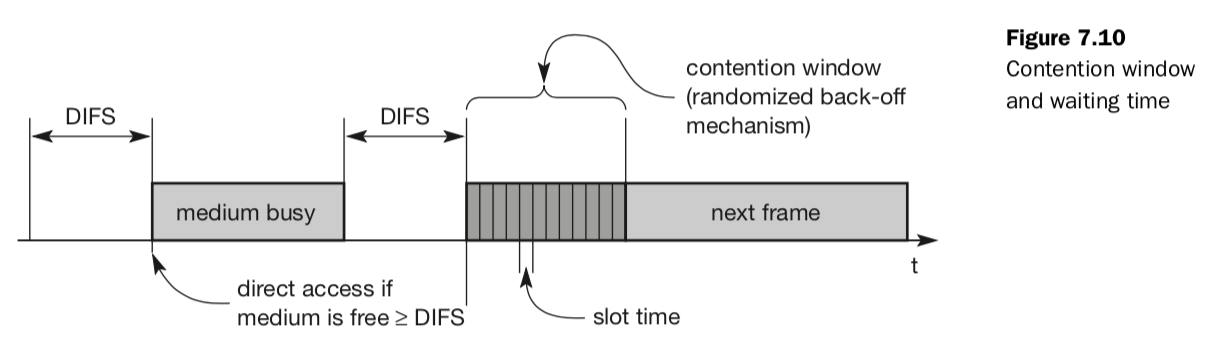


The IEEE 802.11 standard only covers the physical layer **PHY** and medium access layer **MAC** like the other 802.x LANs do. The physical layer is subdivided into the **physical layer convergence protocol (PLCP)** and the **physical medium dependent** sublayer **PMD** (see Figure 7.6). The basic tasks of the MAC layer comprise medium access, fragmentation of user data, and encryption. The PLCP sublayer provides a carrier sense signal, called clear channel assessment (CCA), and provides a common PHY service access point (SAP) independent of the transmission technology. Finally, the PMD sublayer handles modulation and encoding/decoding of signals. The **MAC management** supports the association and re-association of a station to an access point and roaming between different access points. It also controls authentication mechanisms, encryption, synchronization of a station with regard to an access point, and power management to save battery power. MAC management also maintains the MAC management information base (MIB). The main tasks of the **PHY management** include channel tuning and PHY MIB maintenance. Finally, **station management** interacts with both management layers and is responsible for additional higher layer functions (e.g., control of bridging and interaction with the distribution system in the case of an access point).

Medium Access Control Layer: The MAC layer has to fulfill several tasks. First of all, it has to control medium access, but it can also offer support for roaming, authentication, and power con- servation. The basic services provided by the MAC layer are the mandatory **asynchronous data service** and an optional **time-bounded service**. While 802.11 only offers the asynchronous service in ad-hoc network mode, both ser- vice types can be offered using an infrastructure-based network together with the access point coordinating medium access. The asynchronous service sup- ports broadcast and multi-cast packets, and packet exchange is based on a ‘best effort’ model, i.e., no delay bounds can be given for transmission. The following three basic access mechanisms have been defined for IEEE 802.11: the mandatory basic method based on a version of CSMA/CA, an optional method avoiding the hidden terminal problem, and finally a con- tention-free polling method for time-bounded service. The first two methods are also summarized as **distributed coordination function (DCF)**, the third method is called **point coordination function (PCF**). DCF only offers asyn- chronous service, while PCF offers both asynchronous and time-bounded service but needs an access point to control medium access and to avoid con- tention. The MAC mechanisms are also called **distributed foundation wireless medium access control (DFWMAC)**.

●  **Short inter-frame spacing (SIFS):** The shortest waiting time for medium access (so the highest priority) is defined for short control messages, such as acknowledgements of data packets or polling responses. For DSSS SIFS is 10 *μ*s and for FHSS it is 28 *μ*s. The use of this parameter will be explained in sections 7.3.4.1 through 7.3.4.3. ●  **PCF inter-frame spacing (PIFS):** A waiting time between DIFS and SIFS (and thus a medium priority) is used for a time-bounded service. An access point polling other nodes only has to wait PIFS for medium access (see sec- tion 7.3.4.3). PIFS is defined as SIFS plus one slot time. ●  **DCF inter-frame spacing (DIFS):** This parameter denotes the longest wait- ing time and has the lowest priority for medium access. This waiting time is used for asynchronous data service within a contention period (this para- meter and the basic access method are explained in section 7.3.4.1). DIFS is defined as SIFS plus two slot times.

The mandatory access mechanism of IEEE 802.11 is based on **carrier sense mul- tiple access with collision avoidance** (CSMA/CA), which is a random access scheme with carrier sense and collision avoidance through random backoff. The basic CSMA/CA mechanism is shown in Figure 7.10. If the medium is idle for at least the duration of DIFS (with the help of the CCA signal of the physical layer), a node can access the medium at once. This allows for short access delay under light load. But as more and more nodes try to access the medium, ad- ditional mechanisms are needed.

**MAC Frame:**

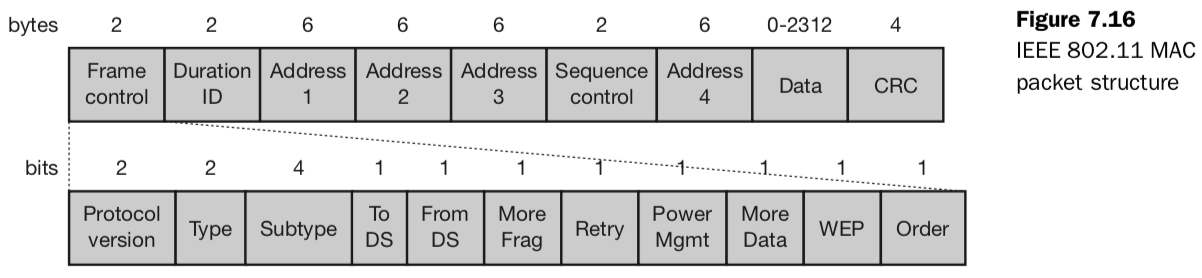
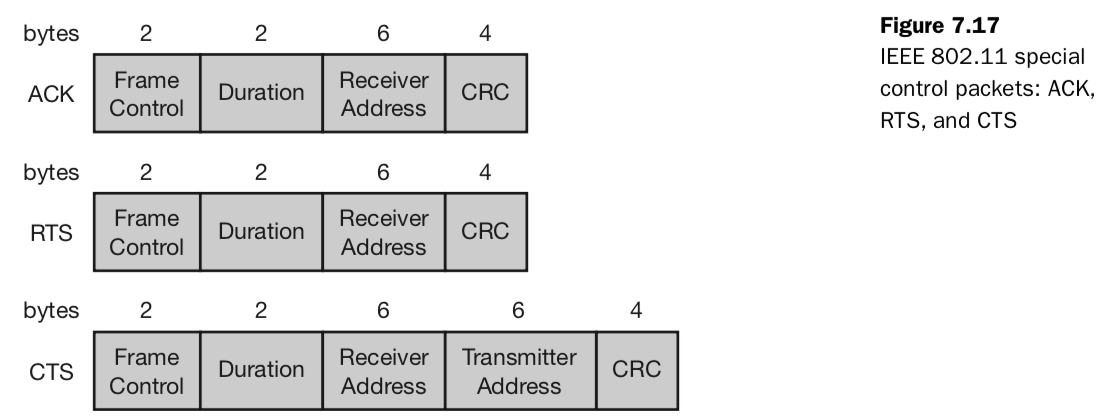
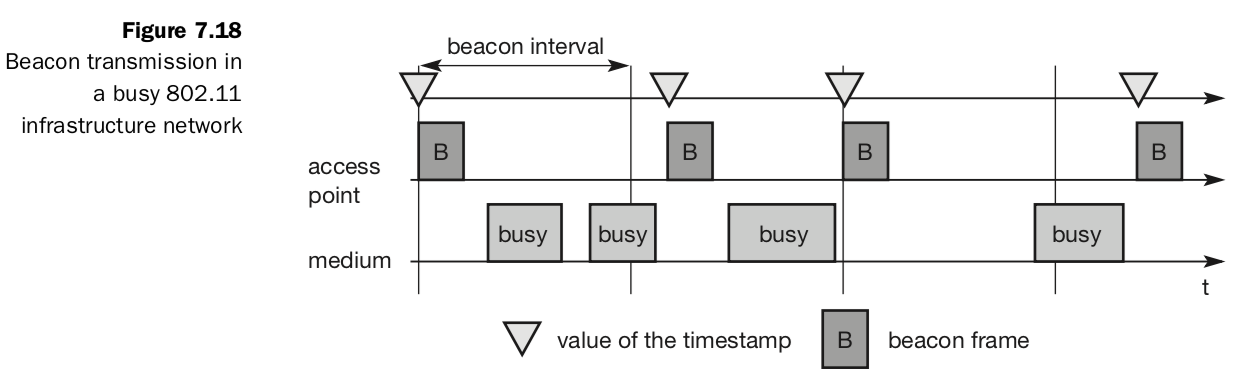


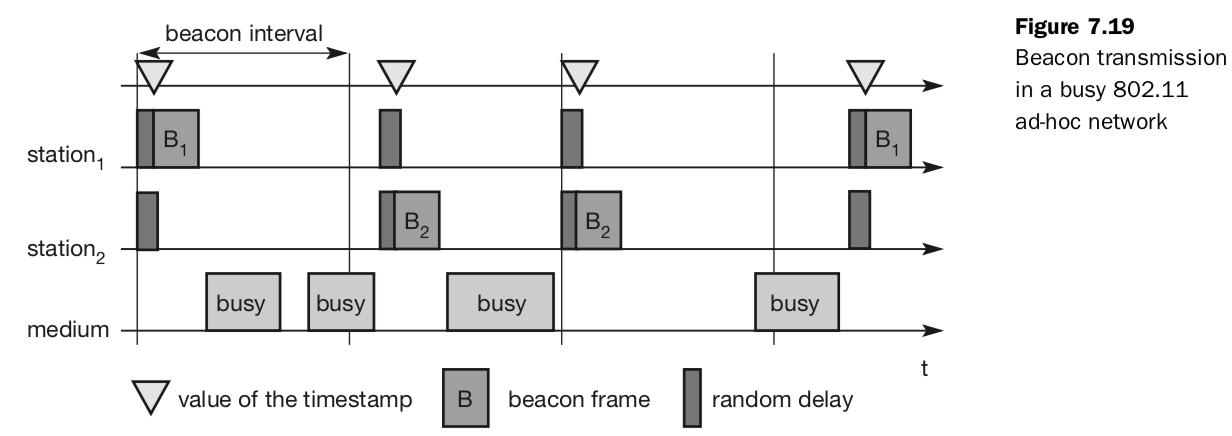
Figure 7.16 shows the basic structure of an IEEE 802.11 MAC data frame together with the content of the frame control field. The fields in the figure refer to the following: ●  **Frame control:** The first 2 bytes serve several purposes. They contain several sub-fields as explained after the MAC frame. ●  **Duration/ID:** If the field value is less than 32,768, the duration field contains the value indicating the period of time in which the medium is occupied (in *μ*s). This field is used for setting the NAV for the virtual reservation mechanism using RTS/CTS and during fragmentation. Certain values above 32,768 are reserved for identifiers. ●  **Address 1 to 4:** The four address fields contain standard IEEE 802 MAC addresses (48 bit each), as they are known from other 802.x LANs. The meaning of each address depends on the DS bits in the frame control field and is explained in more detail in a separate paragraph. ●  **Sequence control:** Due to the acknowledgement mechanism frames may be duplicated. Therefore a sequence number is used to filter duplicates. ●  **Data:** The MAC frame may contain arbitrary data (max. 2,312 byte), which is transferred transparently from a sender to the receiver(s). ●  **Checksum (CRC):** Finally, a 32 bit checksum is used to protect the frame as it is common practice in all 802.x networks.

The frame control field shown in Figure 7.16 contains the following fields: ●  **Protocol version:** This 2 bit field indicates the current protocol version and is fixed to 0 by now. If major revisions to the standard make it incompatible with the current version, this value will be increased. ●  **Type:** The type field determines the function of a frame: management (=00), control (=01), or data (=10). The value 11 is reserved. Each type has several subtypes as indicated in the following field. ●  **Subtype:** Example subtypes for management frames are: 0000 for association request, 1000 for beacon. RTS is a control frame with subtype 1011, CTS is coded as 1100. User data is transmitted as data frame with subtype 0000. All details can be found in IEEE, 1999. ●  **To DS/From DS:** Explained in the following in more detail. ●  **More fragments:** This field is set to 1 in all data or management frames that have another fragment of the current MSDU to follow. ●  **Retry:** If the current frame is a retransmission of an earlier frame, this bit is set to 1. With the help of this bit it may be simpler for receivers to eliminate duplicate frames. ●  **Power management:** This field indicates the mode of a station after successful transmission of a frame. Set to 1 the field indicates that the station goes into power-save mode. If the field is set to 0, the station stays active. ●  **More data:** In general, this field is used to indicate a receiver that a sender has more data to send than the current frame. This can be used by an access point to indicate to a station in power-save mode that more packets are buffered. Or it can be used by a station to indicate to an access point after being polled that more polling is necessary as the station has more data ready to transmit. ●  **Wired equivalent privacy (WEP):** This field indicates that the standard security mechanism of 802.11 is applied. However, due to many weaknesses found in the WEP algorithm higher layer security should be used to secure an 802.11 network (Borisov, 2001). ●  **Order:** If this bit is set to 1 the received frames must be processed in strict order.

Figure 7.17 shows three control packets as examples for many special pack- ets defined in the standard. The **acknowledgement packet (ACK)** is used to acknowledge the correct reception of a data frame as shown in Figure 7.12. The receiver address is directly copied from the address 2 field of the immediately previous frame.

MAC Management: It plays a central role in an IEEE 802.11 station as it more or less controls all functions related to system integration, i.e., integration of a wireless station into a BSS, formation of an ESS, synchronization of stations etc. The following functional groups have been identified and will be discussed in more detail in the following sections: ●  **Synchronization:** Functions to support finding a wireless LAN, synchronization of internal clocks, generation of beacon signals. ●  **Power management:** Functions to control transmitter activity for power conservation, e.g., periodic sleep, buffering, without missing a frame. ●  **Roaming:** Functions for joining a network (association), changing access points, scanning for access points. ●  **Management information base (MIB):** All parameters representing the current state of a wireless station and an access point are stored within a MIB for internal and external access. A MIB can be accessed via standardized protocols such as the simple network management protocol (SNMP).

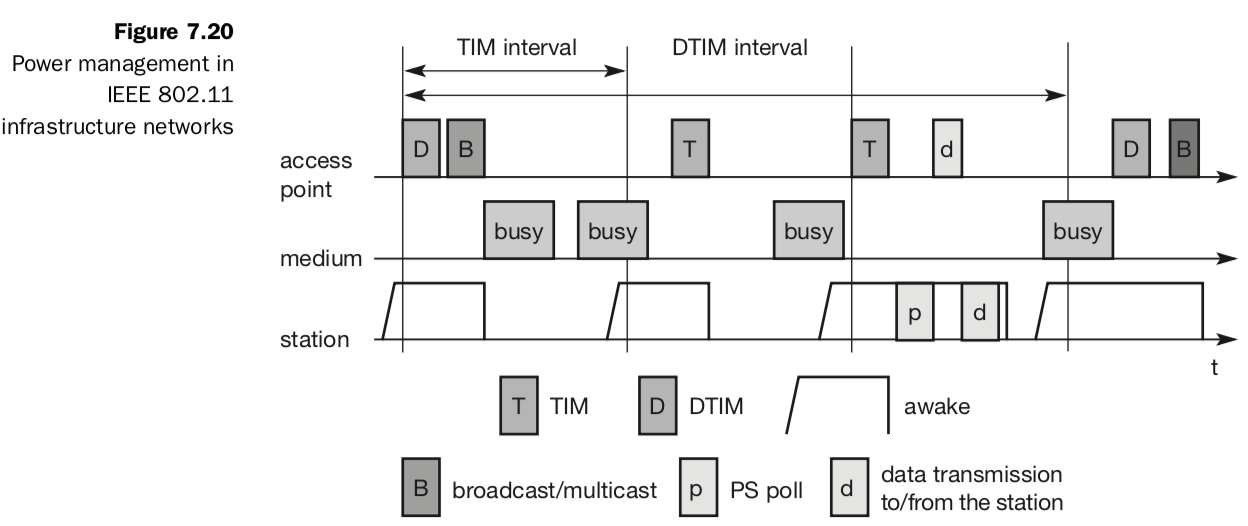


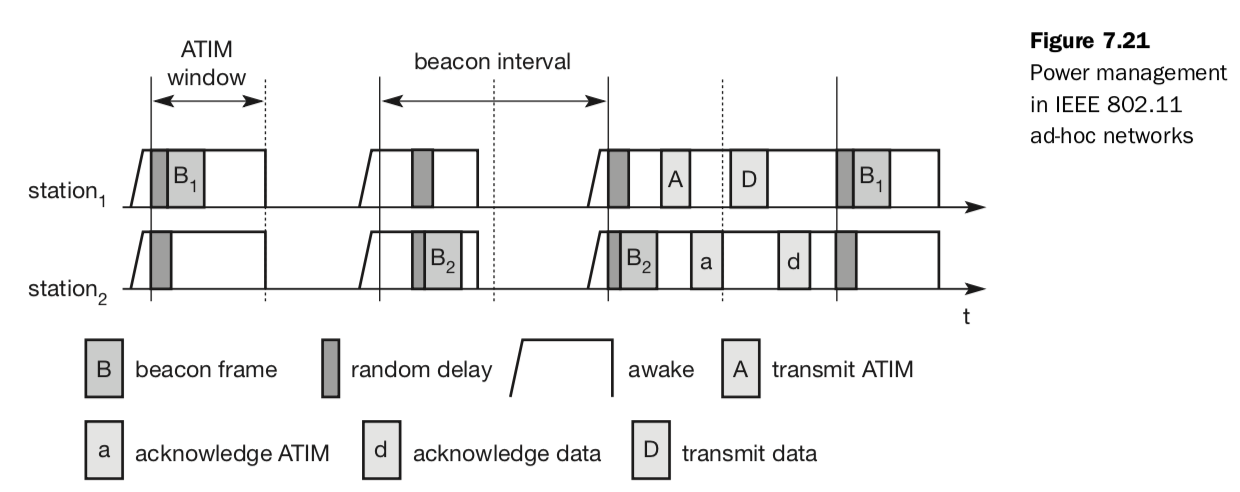


Within a BSS, timing is conveyed by the (quasi)periodic transmissions of a beacon frame. A **beacon** contains a timestamp and other management information used for power management and roaming (e.g., identification of the BSS). The timestamp is used by a node to adjust its local clock. The node is not required to hear every beacon to stay synchronized; however, from time to time internal clocks should be adjusted. The transmission of a beacon frame is not always periodic because the beacon frame is also deferred if the medium is busy.

Within **infrastructure-based** networks, the access point performs synchronization by transmitting the (quasi)periodic beacon signal, whereas all other wireless nodes adjust their local timer to the time stamp.

**Power Management:**





The basic idea of power saving includes two states for a station: **sleep** and **awake**, and buffering of data in senders. If a sender intends to communicate with a power-saving station it has to buffer data if the station is asleep. The sleeping station on the other hand has to wake up periodically and stay awake for a certain time. During this time, all senders can announce the destinations of their buffered data frames. If a station detects that it is a destination of a buffered packet it has to stay awake until the transmission takes place. Waking up at the right moment requires the **timing synchronization function (TSF).**

Power management in **infrastructure**-based networks is much simpler com- pared to ad-hoc networks. The access point buffers all frames destined for stations operating in power-save mode. With every beacon sent by the access point, a **traffic indication map (TIM)** is transmitted.

Roaming: Typically, wireless networks within buildings require more than just one access point to cover all rooms. Depending on the solidity and material of the walls, one access point has a transmission range of 10–20 m if transmission is to be of decent quality. Each storey of a building needs its own access point(s) as quite often walls are thinner than floors. If a user walks around with a wireless station, the station has to move from one access point to another to provide uninterrupted service. Moving between access points is called **roaming**. The term “handover” or “handoff” as used in the context of mobile or cellular phone systems would be more appropriate as it is simply a change of the active cell. However, for WLANs roaming is more common.

The steps for roaming between access points are: ●  A station decides that the current link quality to its access point AP1 is too poor. The station then starts **scanning** for another access point. ●  Scanning involves the active search for another BSS and can also be used for setting up a new BSS in case of ad-hoc networks. IEEE 802.11 specifies scanning on single or multiple channels (if available at the physical layer) and differentiates between passive scanning and active scanning. **Passive scanning** simply means listening into the medium to find other networks, i.e., receiving the beacon of another network issued by the synchronization function within an access point. **Active scanning** comprises sending a **probe** on each channel and waiting for a response. Beacon and probe responses contain the information necessary to join the new BSS. ●  The station then selects the best access point for roaming based on, e.g., signal strength, and sends an **association request** to the selected access point AP2. ●  The new access point AP2 answers with an **association response**. If the response is successful, the station has roamed to the new access point AP2. Otherwise, the station has to continue scanning for new access points. ●  The access point accepting an association request indicates the new station in its BSS to the distribution system (DS). The DS then updates its database, which contains the current location of the wireless stations. This database is needed for forwarding frames between different BSSs, i.e. between the different access points controlling the BSSs, which combine to form an ESS (see Figure 7.3). Additionally, the DS can inform the old access point AP1 that the station is no longer within its BSS.

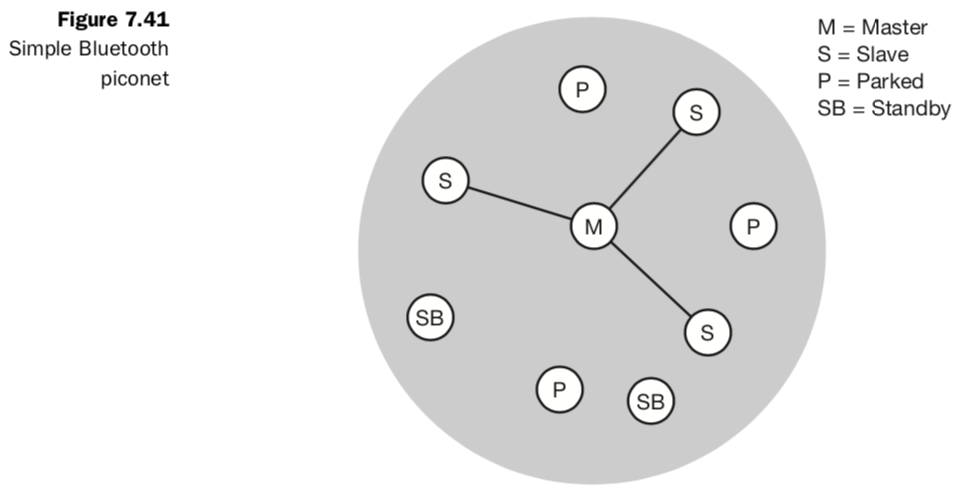
**802.11b:** As standardization took some time, the capabilities of the physical layers also evolved. Soon after the first commercial 802.11 products came on the market some companies offered proprietary solutions with 11 Mbit/s. To avoid market segmentation, a common standard, **IEEE 802.11b** (IEEE 1999) soon followed and was added as supplement to the original standard (Higher-speed physical layer extension in the 2.4 GHz band). This standard describes a new PHY layer and is by far the most successful version of IEEE 802.11 available today. Do not get confused about the fact that 802.11b hit the market before 802.11a. The standards are named according to the order in which the respective study groups have been established. As the name of the supplement implies, this standard only defines a new PHY layer. All the MAC schemes, management procedures etc. explained above are still used.

**802.11a:** Initially aimed at the US 5 GHz U-NII (Unlicensed National Information Infrastructure) bands **IEEE 802.11a** offers up to 54 Mbit/s using OFDM (IEEE, 1999). The first products were available in 2001 and can now be used (after some harmonization between IEEE and ETSI) in Europe. The physical layer of IEEE 802.11a and the ETSI standard HiperLAN2 has been jointly developed, so both physical layers are almost identical. Most statements and explanations in the following, which are related to the transmission technology are also valid for HiperLAN2. However, HiperLAN2 differs in the MAC layer, the PHY layer packet formats, and the offered services (quality of service, real time etc.).

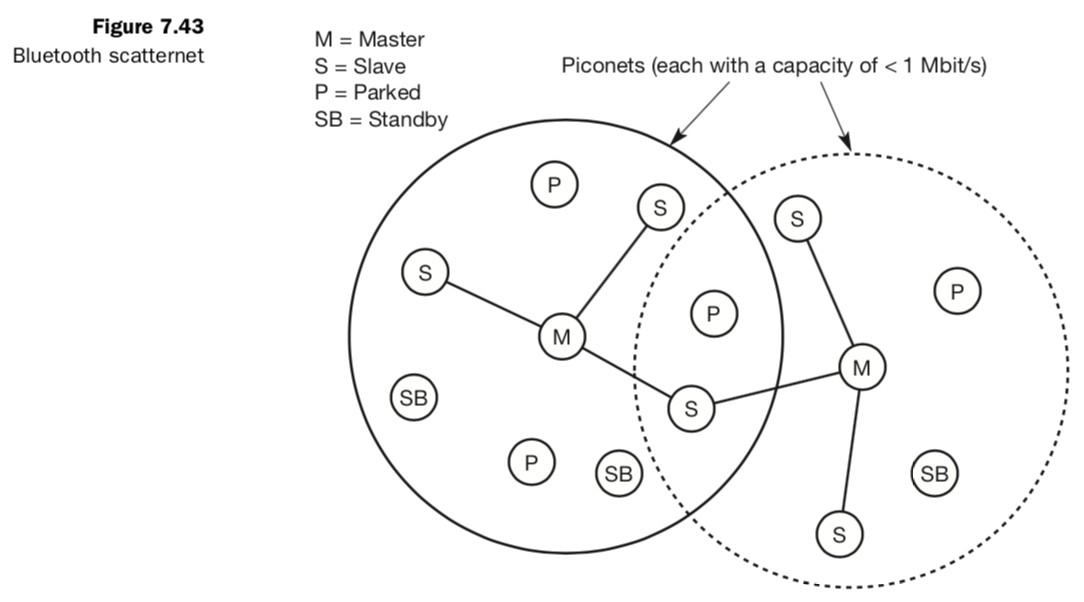
**Bluetooth:** Compared to the WLAN technologies, the Bluetooth technology discussed here aims at so-called **ad-hoc piconets**, which are local area networks with a very limited coverage and without the need for an infrastructure. This is a different type of network is needed to connect different small devices in close proximity (about 10 m) without expensive wiring or the need for a wireless infrastructure. The envisaged gross data rate is 1 Mbit/s, asynchronous (data) and synchronous (voice) services should be available. The necessary transceiver components should be cheap. At the same time the Bluetooth development started, a study group within IEEE 802.11 discussed **wireless personal area networks (WPAN)** under the following five criteria: ●  **Market potential:** How many applications, devices, vendors, customers are available for a certain technology? ●  **Compatibility:** Compatibility with IEEE 802. ●  **Distinct identity:** Originally, the study group did not want to establish a second 802.11 standard. However, topics such as, low cost, low power, or small form factor are not addressed in the 802.11 standard. ●  **Technical feasibility:** Prototypes are necessary for further discussion, so the study group would not rely on paper work. ●  **Economic feasibility:** Everything developed within this group should be

cheaper than other solutions and allow for high-volume production.

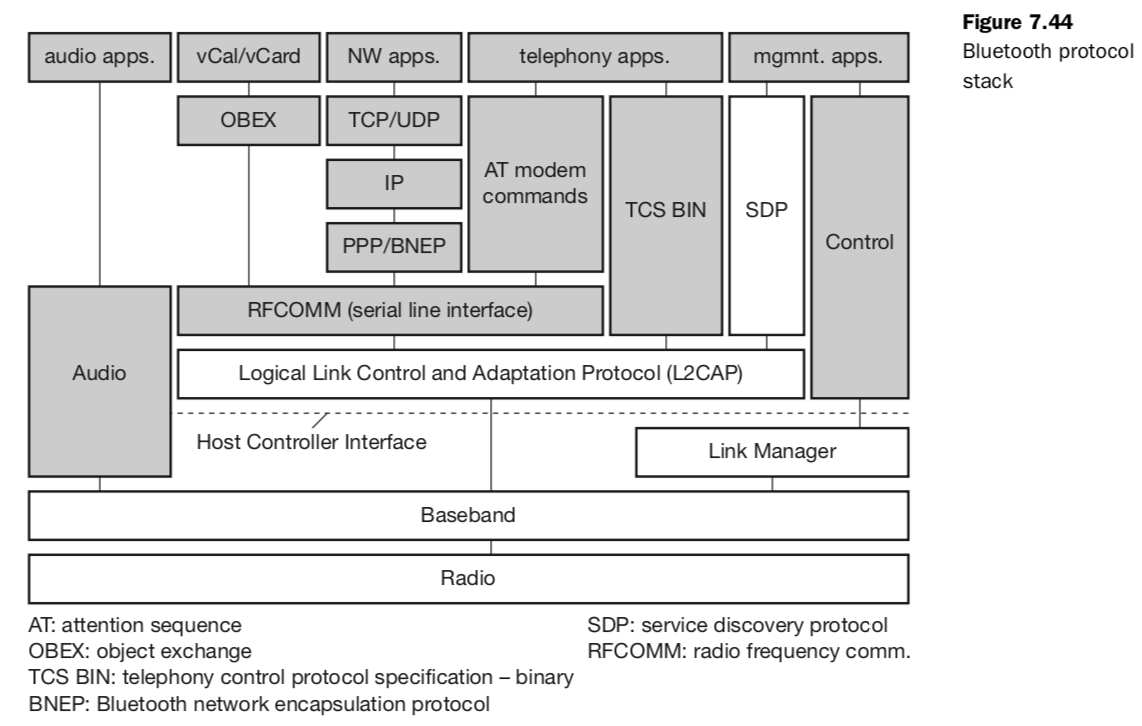
Architecture: Like IEEE 802.11b, Bluetooth operates in the 2.4 GHz ISM band. However, MAC, physical layer and the offered services are completely different.



To understand the networking of Bluetooth devices a quick introduction to its key features is necessary. Bluetooth operates on 79 channels in the 2.4 GHz band with 1 MHz carrier spacing. Each device performs frequency hopping with 1,600 hops/s in a pseudo random fashion. Bluetooth applies FHSS for interference mitigation (and FH-CDMA for separation of networks). A very important term in the context of Bluetooth is a **piconet**. A piconet is a collection of Bluetooth devices which are synchronized to the same hopping sequence. Figure 7.41 shows a collection of devices with different roles. One device in the piconet can act as **master** (M), all other devices connected to the master must act as **slaves** (S). The master determines the hopping pattern in the piconet and the slaves have to synchronize to this pattern. Each piconet has a unique hopping pattern. If a device wants to participate it has to synchronize to this. Two additional types of devices are shown: parked devices (P) cannot actively participate in the piconet (i.e., they do not have a connection), but are known and can be reactivated within some milliseconds. The phase in the hopping pattern is deter- mined by the master’s clock. After adjusting the internal clock according to the master a device may participate in the piconet. All active devices are assigned a 3-bit **active member address** (AMA). All parked devices use an 8-bit **parked member address** (PMA). Devices in stand-by do not need an address.



**Protocol Stack:**



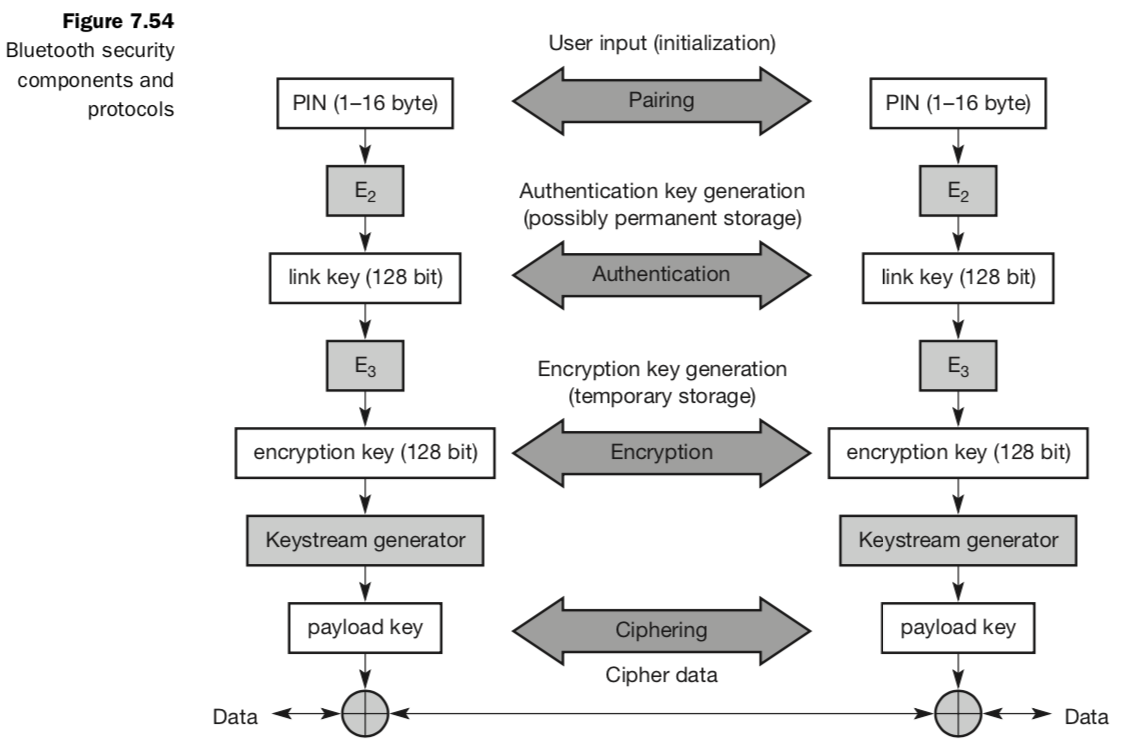
As Figure 7.44 shows, the Bluetooth specification already comprises many proto- cols and components. Starting as a simple idea, it now covers over 2,000 pages dealing with not only the Bluetooth protocols but many adaptation functions and enhancements. The Bluetooth protocol stack can be divided into a **core specification**, which describes the protocols from physical layer to the data link control together with management functions, and **profile specifications** (Bluetooth, 2001b). The latter describes many protocols and functions needed to adapt the wireless Bluetooth technology to legacy and new applications.

The **core protocols** of Bluetooth comprise the following elements: ●  **Radio:** Specification of the air interface, i.e., frequencies, modulation, and transmit power.●  **Baseband:** Description of basic connection establishment, packet formats, timing, and basic QoS parameters. ●  **Link manager protocol:** Link set-up and management between devices including security functions and parameter negotiation. ●  **Logical link control and adaptation protocol (L2CAP):** Adaptation of higher layers to the baseband (connectionless and connection-oriented services. ●  **Service discovery protocol:** Device discovery in close proximity plus querying of service characteristics.

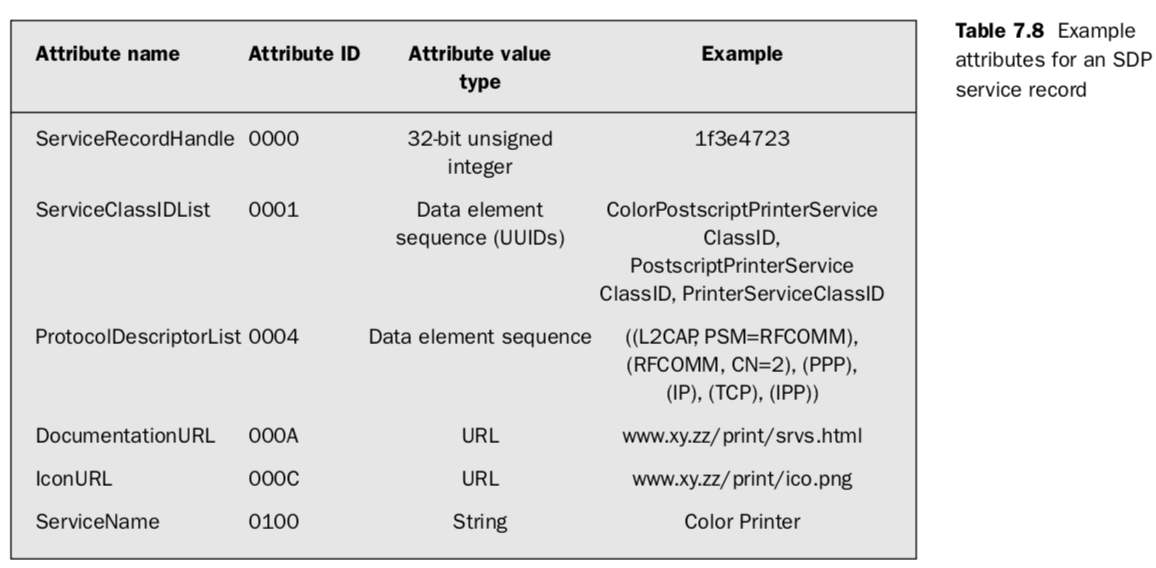
Link Manager Protocol: The link manager protocol (LMP) manages various aspects of the radio link between a master and a slave and the current parameter setting of the devices. LMP enhances baseband functionality, but higher layers can still directly access the baseband. The following groups of functions are covered by the LMP: ●  **Authentication, pairing, and encryption:** Although basic authentication is handled in the baseband, LMP has to control the exchange of random numbers and signed responses. The pairing service is needed to establish an initial trust relationship between two devices that have never communicated before. The result of pairing is a link key. This may be changed, accepted or rejected. LMP is not directly involved in the encryption process, but sets the encryption mode (no encryption, point-to-point, or broadcast), key size, and random speed. Section 7.5.7 gives an overview of Bluetooth’s security mechanisms. ●  **Synchronization:** Precise synchronization is of major importance within a Bluetooth network. The clock offset is updated each time a packet is received from the master. Additionally, special synchronization packets can be received. Devices can also exchange timing information related to the time differences (slot boundaries) between two adjacent piconets. ●  **Capability negotiation:** Not only the version of the LMP can be exchanged but also information about the supported features. Not all Bluetooth devices will support all features that are described in the standard, so devices have to agree the usage of, e.g., multi-slot packets, encryption, SCO links, voice encoding, park/sniff/hold mode (explained below), HV2/HV3 packets etc. ●  **Quality of service negotiation:** Different parameters control the QoS of a Bluetooth device at these lower layers. The poll interval, i.e., the maximum time between transmissions from a master to a particular slave, controls the latency and transfer capacity. Depending on the quality of the channel, DM or DH packets may be used (i.e., 2/3 FEC protection or no protection). The number of repetitions for broadcast packets can be controlled. A master can also limit the number of slots available for slaves’ answers to increase its own bandwidth. ●  **Power control:** A Bluetooth device can measure the received signal strength. Depending on this signal level the device can direct the sender of the measured signal to increase or decrease its transmit power. ●  **Link supervision:** LMP has to control the activity of a link, it may set up new SCO links, or it may declare the failure of a link. ●  **State and transmission mode change:** Devices might switch the master/slave role, detach themselves from a connection, or change the operating mode.

**To save battery power**, a Bluetooth device can go into one of three low power states: ●  **Sniff state:** The sniff state has the highest power consumption of the low power states. Here, the device listens to the piconet at a reduced rate (not on every other slot as is the case in the active state). The interval for listening into the medium can be programmed and is application dependent. The master designates a reduced number of slots for transmission to slaves in sniff state. However, the device keeps its AMA. ●  **Hold state:** The device does not release its AMA but stops ACL trans- mission. A slave may still exchange SCO packets. If there is no activity in the piconet, the slave may either reduce power consumption or participate in another piconet. ●  **Park state:** In this state the device has the lowest duty cycle and the lowest power consumption. The device releases its AMA and receives a parked member address (PMA). The device is still a member of the piconet, but gives room for another device to become active (AMA is only 3 bit, PMA 8 bit). Parked devices are still FH synchronized and wake up at certain beacon intervals for re-synchronization. All PDUs sent to parked slaves are broadcast.

Security and Link Management:



A radio interface is by nature easy to access. Bluetooth devices can transmit private data, e.g., schedules between a PDA and a mobile phone. A user clearly does not want another person to eavesdrop the data transfer. Just imagine a scenario where two Bluetooth enabled PDAs in suitcases ‘meet’ on the conveyor belt of an airport exchanging personal information! Bluetooth offers mechanisms for authentication and encryption on the MAC layer, which must be implemented in the same way within each device. The main security features offered by Bluetooth include a challenge- response routine for authentication, a stream cipher for encryption, and a session key generation. Each connection may require a one-way, two-way, or no authentication using the challenge-response routine. All these schemes have to be implemented in silicon, and higher layers should offer stronger encryption if needed. The security features included in Bluetooth only help to set up a local domain of trust between devices. The security algorithms use the public identity of a device, a secret private user key, and an internally generated random key as input parameters. For each transaction, a new random number is generated on the Bluetooth chip. Key management is left to higher layer software. The first step, called **pairing**, is necessary if two Bluetooth devices have never met before. To set up trust between the two devices a user can enter a secret PIN into both devices. This PIN can have a length of up to 16 byte. Based on the PIN, the device address, and random numbers, several keys can be computed which can be used as link key for **authentication**. Based on the link key, values generated during the authentication, and again a random number an encryption key is generated during the **encryption** stage of the security architecture. This key has a maximum size of 128 bits and can be individually generated for each transmission. Based on the encryption key, the device address and the current clock a payload key is generated for ciphering user data. The payload key is a stream of pseudo-random bits. The **ciphering** process is a simple XOR of the user data and the payload key.



Bluetooth devices should work together with other devices in unknown environments in an ad-hoc fashion. It is essential to know what devices, or more specifically what services, are available in radio proximity. To find new services, Bluetooth defined the **service discovery protocol (SDP)**. SDP defines only the discovery of services, not their usage. Discovered services can be cached and gradual discovery is possible. Devices that want to offer a service have to instal an SDP server. For all other devices an SDP client is sufficient.

All the information an SDP server has about a service is contained in a **service record**. This consists of a list of service attributes and is identified by a 32-bit service record handle. SDP does not inform clients of any added or removed services. There is no service access control or service brokerage. A **service attribute** consists of an attribute ID and an attribute value. The 16-bit **attribute ID** distinguishes each service attribute from other service attributes within a service record. The attribute ID also identifies the semantics of the associated attribute value. The **attribute value** can be an integer, a UUID (universally unique identifier), a string, a Boolean, a URL (uniform resource locator) etc. Table 7.8 gives some example attributes.

**===End of Unit III===**