Chapter

4

The *M* in FMC

Give me a place to stand, and I will move the earth.

—Archimedes (287–212 B.C.)

Without a good understanding of fixed networks, which you already should have acquired by reading the preceding chapter, it would be quite difficult to fully appreciate the aspects of mobility we are going to delve into in this chapter. Indeed, much of the fundamental functionality and many architectural aspects of fixed networks have been borrowed and extended to create the core of modern mobile networks.

For instance, termination of a voice call in a mobile environment requires an interaction with a database storing subscriber profiles, the Home Location Register (HLR), much like the interaction that occurs in fixed networks with an SCP in order to route a toll-free phone call to the correct call center's call distributors. This example well illustrates how lessons learned and concepts invented for fixed environments are reapplied in a mobile setting, albeit with the necessary adaptations.

In this chapter we will identify these similarities and differences, and explore the most common cellular and noncellular radio access systems that may commonly be part of FMC solutions. The knowledge acquired in this and the preceding chapter will then make it possible for you to fully appreciate the ensuing discussion on convergence.

In the end, *fixed* and *mobile* communications can be seen (and they are) as two different facets of the same technology, which indeed have never been totally independent, so convergence for them is a consequential natural course of evolution. Thus, sooner or later, fixed and mobile networks will come together—the process already evident in the industry with the launch of services allowing use of a mobile phone at fixed-line rates, and using fixed-line access, when in the home—with FMC being one of the technologies hastening this "homecoming." To paraphrase Archimedes' famous statement: "Give me a fixed network and I can build mobile networks around that."

Mobility

While mobility is not only about wireless or radio access systems (as we have established in earlier chapters, there is quite a good distinction between *wireless* and *mobile,* wireless referring to the type of access and mobile to the type of service), wireless systems are usually at the core of mobile communications, so in this chapter most of the discussion in fact revolves around such solutions. It should be noted that many wireless access systems such as Wi-Fi do not natively support mobility. In fact, most of today's applications have relied on Wi-Fi mainly for "cord cutting" while accessing fixed networks; that is, this has held true until the recently introduced uses of Wi-Fi for metro data coverage and wireless VoIP broadened its scope, albeit without the support for macromobility allowed by cellular systems.

In the future it is also likely that Wi-Fi and other technologies such as WiMAX will be used to connect to mobile packet cores (à la 3GPP TS 23.234 [82]), which is not surprising given their broadening support on cellular phones. Before turning to Wi-Fi, however, in the sections that follow we will first address cellular systems and then introduce WiMAX access, paying special attention to its mobile version.

Mobile Communications Systems Fundamentals

One of the fundamental characteristics of mobile systems is that, like fixed systems, they include a core network, the elements of which act as an anchor for mobility. The core network also contains points of interworking with other (fixed and mobile) networks and connects to an access network needed to support the radio interface technology that characterizes a specific mobile system.

Core and Access

Note that different mobile systems, defined by various radio interfaces and access networks, may still share the same core network. For instance, it is possible to use the same core network to support the Global System for Mobile Communications (GSM—originally an acronym for *Groupe Spécial Mobile* and now the most widespread cellular technology) and the Universal Mobile Telecommunications System (UMTS).

Core Network Functions The core network normally includes the "intelligence" necessary to make the system operate. The core provides the admission control to wireless services via access authentication and stores subscriber profiles, letting the core determine the specific service set and treatment to be applied to a user. These are examples of the questions the core can decide on:

- Is the user allowed to roam to another network?
- Are there areas where the user cannot receive service?
- Is the user in and out of a "home zone"?
- What Quality of Service (QoS) for packet data services is the user is entitled to?
- What calls is the user entitled to receive or place, and which are barred?

The core also provides *mobility management* of the mobile terminal in idle mode, that is, at times when it is not engaged in a voice call or in the active transmission and reception of data. The mobility management function allows tracking the user's whereabouts, by means of location updates the terminal issues periodically or when it crosses boundaries of "location areas" as the user moves.

Further, the core participates in call control for speech services and session control for multimedia services as well as providing infrastructure that is ancillary to the delivery of services (such as location information). The core network is also the main source of charging information.[1] Finally, mandated services like lawful interception rely on the core network to provide support for tracking the location and specific behavior of a user, log its activity types, and deliver the content of communications to the authorized agencies.

All this intelligent functionality (typically supported by different servers and network elements) can be quite computationally intensive, and concentrating these in centralized locations provides efficiency gains in large part for statistical reasons (not all users will need to use the same resources at the same time, so centralizing some functions will increase efficiency). Another reason for centralization is the need to provide a "point of access" for external networks to the mobile system services. Examples of this include scalable call termination and roaming interfaces (on roaming interfaces, it is in fact necessary to minimize the number of peering relationships to simplify roaming operations).

Access Network Functions Typical functions of the radio access network are Physical-layer termination and Link-layer termination of radio interface protocols, ciphering and header compression,[2] mobility management within the radio access, paging, broadcast information distribution, and scheduling.

---

[1] In some systems, like in UMTS, the RAN cooperates with the core by delivering unsent data volume reports, but this feature is most likely to be discontinued in future systems, as it either was not implemented in most cases by vendors or was not used by providers, and of course the increase of data rates will make the value per bit unsent smaller, so it will be less important to count unsent data.

[2] In some technologies like GSM, ciphering and header compression for data sessions are done in the core network.

It should also be understood that for a mobile system to provide a satisfactory user experience, it must offer extensive coverage over large geographical areas. There is also the need to keep the transmission power of terminals and the complexity of receivers low to allow for longer battery life and lower terminal cost. To assist in that goal, the reach of the base transceiver stations (BTSs, which include the antennas in the network, radiating signals to mobiles and receiving signals from them) has to be limited (also to allow for frequency reuse, as explained later in the chapter), so the number of elements in a typical radio access network is much higher than in the core, and this is where most of the capital investment is needed.

Since BTSs represent the largest number of elements in a mobile radio access network, the functions in the BTS tend to be kept to the bare minimum necessary to provide radio access. However, with the introduction of high-speed wireless data services, there is a trend to offload some of the functions that were suitably kept in the access nodes higher up in the radio access network hierarchy down to the BTS. There is a host of technical reasons behind this, mostly linked to the delay introduced by the traversal of a backhaul network to a controller, which would make, for instance, running some retransmission algorithms less effective.

This trend of assigning additional functions in the BTS to handle data access has been taken to the extreme by the introduction of the concept of "Home BTS" or *femtocell,* which is promising the delivery of "personalized" wireless coverage in residential or business premises not reachable by the existing WAN infrastructure of BTSs. This technology is driving the use of IP connectivity to the BTS in order to reuse the infrastructure already available in those premises, and the simplification of the protocol layers supported on the interface between the core and the *femtocells,* to minimize the cost of backhaul.

Circuit and Packet

Mobile networks, like fixed networks, can provide a variety of services, including circuit-switched (CS) and packet-switched (PS) services.

Circuit services include speech, video, and circuit-switched data (akin to landline modem dial-up—fast becoming a thing of the past with the rise of broadband—based on dialing a circuit connection to a remote access server (RAS) and running PPP over it).

Packet services include high-speed data used for access to Internet and private networks, portal access, Web browsing, instant messaging and presence, and other innovative services, including IMS, multicast, and broadcast.

Circuit-switched services are supported by all traditional *cellular* systems, whether digital or analog (the latter actually have been discontinued globally, with possibly a few rare exceptions). However, not every *mobile* communication system supports circuit services. For instance, the evolution of the 3GPP system foresees that all services will be packet based and, more specifically, IP based. Other mobile systems such as WiMAX and CDMA EV-DO revA were built as packet only from the ground up.

On the other hand, packet-switched services were not supported by analog systems or by initial releases of digital systems, as at the times these systems were introduced, the demand for data services was not sufficient to justify the additional effort to define packet data support in cellular systems. This functionality was added in subsequent system releases as an evolution of both the radio and the core network of these systems.

The need to support both packet- and circuit-switched services requires the core and access of a mobile-system to support features that are often very different in nature. The mobile-system features dedicated to CS services are often identified as the "CS domain," whereas the set of features devoted to the support of PS services are defined as the "PS domain."

Having thus explained the fundamental differences between PS and CS, we are now ready to proceed with an overview of the specific mobile systems, starting with the discussion of the traditional cellular infrastructure.

Cellular Systems: The Sky Is the Limit

The concept of *cellular* has been invented to cope with one fundamental issue in wireless transmission technologies operating in a licensed spectrum.[3] The issue is the scarcity (and cost!) of the radio frequency (RF) bandwidth. When an operator is allowed to provide wireless service, a regulatory authority assigns it portions of the RF spectrum (known as "bands") to use for radiating and receiving signals from its subscribers.

Sometimes operators engage in fierce bidding to buy some of this spectrum, which results in staggering amounts of money being transferred to the government (or, in some cases, to previous owners of the spectrum bands). Therefore, the need to maximize the efficiency when using this precious resource, as well as the need to overcome basic physical limitations of wireless transmission, has led to the invention of what is called *frequency reuse.* With frequency reuse, multiple transmitters can use *the same* radio frequency to send and receive data as long as they are "sufficiently remote" so as to avoid interference. That is, a given (RF) channel can be used over and over again and thus cover an extremely wide area and support a very high number of simultaneous transmissions.

The concept of "sufficiently remote" requires some degree of clarification here. It is a common experience for everyone that the coverage of a radio station can be quite broad even without repeaters. The reason for this is that the radio station transmits at high power levels. In cellular systems, by contrast, the goal is to control the power of transmission so that interference is avoided between areas where the same frequency is reused. So, the concept of "sufficiently remote" is relative to the possible reach of a signal transmitted at a given power level. One of the most important characteristics of frequency reuse is the *reuse distance.* Intercell interference can be limited by changing

[3] Licensed spectrum is spectrum for which an operator needs to obtain authorization from a regulatory authority for the use of the radio frequency (RF) it needs for the operation of the wireless service.

the reuse distance and the power levels of BTS transmission. The resulting combination of power control and frequency planning is used to fine-tune the cellular network in a given area.

The elementary area of coverage in a cellular system roughly centered around the BTS is called a *cell.* Each BTS can use a subset of the RF channels the operator is allowed to operate. These channels cannot be reused in any neighboring and potentially interfering cells (that is, any cell within the "reuse distance"). With the introduction of cellular systems based on Code Division Multiple Access (CDMA) technology, there have been ways to advance the use of digital technology to reduce interference while allowing for greater reuse levels and thus increased capacity. Also, other techniques such as cell "sectorization" (using directional antennas, thus adding space division to frequency division, in order to maximize frequency reuse) and dynamic channel assignment to cells (thus introducing the concept of time division in addition to frequency division) have made it possible to further increase capacity by allowing higher reuse factors and availability of more channels per BTS.

In summary, the cellular systems have made it commercially viable to support mobility of a large number of subscribers in a wide area at a reasonable cost practically without any limitations as long as a sufficient number of base stations is installed. It is no surprise that, given the relative ease and speed of deployment allowed by cellular systems, and the reach of customers in even the remotest areas at reasonable costs, cellular communication is now a dominant and growing sector of the telecommunications industry. This sector is, however, relatively nascent in comparison with fixed networking (it is only a few decades old, compared to the more than one-hundred-year history of public wireline telephony), but it has dramatically changed the way we communicate. Its evolution has also been quite rapid from the early days of analog cellular telephony to the recent days of high-speed wireless data. The next section summarizes this evolution.

Cellular Generations

The evolution of cellular communication systems has been commonly identified via a series of generations (1G, 2G, 3G, and, by implication, 4G and yet further generations). This evolution has been somewhat linked to the evolution of computing. When digital computing was expensive, it was considered unfeasible to digitally process speech and use digital transmission of digitally encoded voice over the radio interface, in large part due to the high handset power requirements and limited memory capabilities. Therefore, the natural choice was to keep wireless telephony entirely in the analog domain.

1G Analog cellular systems are commonly known as 1G (or first-generation) cellular systems. 1G was introduced in the late 1970s and early 1980s. These systems delivered almost exclusively speech services; albeit some low-bit-rate data services were available as dial-up connections via wireless modems.

Analog systems are almost everywhere being phased out, and those that are not will probably be retired very soon. From a practical standpoint, the investment in these systems has stopped on both vendors' and operators' sides, and for this reason they are not considered in the scope of convergence, which mostly lies in an area where the industry is going to develop.

Typical 1G systems include:

- **AMPS** Advanced Mobile Phone Service, adopted mainly in the America, using FDMA transmission in the 800 MHz band.
- **TACS** Total Access Communication System, adopted mostly in Europe. TACS was similar to the AMPS system. There were various flavors of it; for instance, in the UK, ETACS (Extended TACS) operated in the 871–904/916–949 MHz band, and Narrowband TACS (NTACS) operated in the 860–870/915–925 MHz band (by using narrower channel spacing, it supported more channels for the same amount of spectrum).
- **NMT** Nordic Mobile Telephone, deployed in many European countries, was first launched in the Scandinavian region (as its name may suggest) in 1979, and it was the first analog cellular system operating in both the 450 MHz and 900 MHz bands. The operation in the 450 MHz band affords particularly good coverage due to the propagation properties of radio waves, so it has been kept alive for quite a long time in Scandinavia, often used by boat owners in the Baltic region, or rural area dwellers, where it was not economical to deploy systems in different bands. The "450" frequencies are therefore particularly appealing for these reasons, and digital systems offering the capability to cover these subscribers (GSM, CDMA, and also 3G) have been offered to refarm this system.

1G systems were deployed on a country-by-country basis and did not offer international roaming. This became an apparent issue, especially in Europe where there were two different analog systems operating in different frequencies and according to different rules. This clearly was creating a problem for the development of the cellular industry, and therefore even at the political level it was clearly understood that the development of competing digital systems in that region would have been a critical mistake.

Beyond forcing compatibility issues and hampering roaming capabilities for European citizens, this would have fragmented the market and made it more difficult for European vendors to compete globally. European operators would also be unable to benefit from effects of scale for both equipment and, most important, handsets. In summary, this was at the core of the reason why European regulatory bodies encouraged operators and vendors to come together and agree on the common digital system, which was later named GSM.

2G Cellular digital systems in the first wave to appear in the mobile communications industry are known as 2G systems. These were rolled out worldwide in the course of the 1990s. These systems are characterized by the digital transmission of all services, including voice, which is digitally encoded for transmission over the radio interface.

Initially they were conceived to deliver circuit services only, but then their evolution to deliver packet data services was devised (these systems' evolution to support packet data later became known as 2.5G).

Typical examples of 2G systems include:

- **GSM** The Global System for Mobile Communications initially is the European 2G system, specified by ETSI and currently maintained by 3GPP. It is now adopted in practically every country or region of the world, except Japan, Korea, and a few others. GSM was initially operating in the 900 MHz band only, but then operation at 1800 MHz, 1900 MHz, 450 MHz, and other frequencies was also defined. GSM uses a time division multiple access (TDMA) multiplexing over-the-air interface. Its 2.5G system evolution is known as General Packet Radio Service (GPRS), and its 2.5G air interface evolution is known as Enhanced Data Rates for GSM Evolution (EDGE). EDGE has also been accepted as an IMT-2000 technology, so technically it is also part of the "3G" mobile systems; albeit it is deeply linked to its 2G heritage.
- **TDMA** Time division multiple access, defined in TIA IS-136 [96], or D-AMPS (for Digital-AMPS), has been adopted in North and South America. It uses a time division multiple access technology (like GSM), over-the-radio interface, but unlike in GSM, this technology was not globally adopted, so it has been largely phased out in favor of GSM in every region where it was deployed (except some South American countries, where it may still be available for a while).
- **PDC** Personal Digital Cellular (PDC) is the Japanese standard for digital cellular telephony. In Japan, this is quickly being replaced by 3G systems, and it has received quite phenomenal competition from a Japanese cordless telephony standard (PHS—Personal Handy-phone System), which has been made available in major urban areas to the large population of pedestrians and users of public transportation systems. PDC is also a TDMA system, replacing the analog NTT and JTACS Japanese systems. It operates in the 800 and 1400 MHz frequency bands.
- **CDMA** Code Division Multiple Access, specified in standard TIA IS-95A [98], uses a technique to assign to all transmitters their respective, specific, bit vectors, which are mutually orthogonal so that a receiver can recover the signal transmitted even if multiple transmitters use the same carrier at the same time to modulate the RF signal. This standard is now maintained by 3GPP2 and has been adopted in many countries in Asia and South America, after its initial deployment in North America. The evolution of IS-95 to support packet services is known as IS-95B, and it supports data rates up to 64 Kbps.

3G Similarly to what happened in Europe during the migration from 1G to 2G, during the migration from 2G to 3G it appeared that having many flavors of 3G standards across the globe was not advantageous. So various standards organizations from different countries came together to form the Third-Generation Partnership Project (3GPP) to define a standard based on the evolution of the GSM core network and W-CDMA radio transmission technology (the most promising and efficient at the time).

In North America, this evolutionary path to 3G was not received too well, though, as major CDMA operators (and their main suppliers) perceived it not to be protecting their investment sufficiently. So a competing partnership was formed, called 3GPP2, developing a 3G standard based on the evolution of IS-95 CDMA radio transmission technology and the ANSI-41-based core network.

With the creation of 3GPP and 3GPP2, the intent of achieving a global cellular standard for 3G has failed. However, there was a considerable momentum toward harmonization for both competing standards as the number of different systems went down from four in 2G to two in 3G.

The 3G standardization activity took place under the supervision of the IMT-2000 in ITU-T, which was assigning frequencies and acknowledging technologies suitable for the 3G standards (also known hence as IMT-2000 technologies). 3G Systems, launched after the year 2000, promised to offer faster access to the Internet and other data services with typical speeds ranging in the hundreds of Kbps. They also offered circuit services like speech and real-time video. The systems resulting from the efforts of the 3GPPs were:

- **UMTS** The Universal Mobile Telecommunications System, which has been specified by 3GPP, is a multiradio interface system, which includes satellite communications, but its most widespread use for now is based on a W-CDMA radio interface, and it operates in different frequency bands, depending on the region of deployment. W-CDMA comes in FDD (frequency-division duplexing) and TDD (time-division duplexing) flavors. In FDD, uplink and downlink signals are allocated to different frequencies, while in TDD they share the same frequency on a time-division basis. UMTS offers both packet data and circuit services. In China, the TD-SCDMA (time division–synchronous code division multiple access) radio interface has been selected to constitute the homegrown UMTS radio interface. Japan launched 3G UMTS before any other country, due to the leadership of DoCoMo in 3G UMTS-based standards with its Freedom of Mobile Access (FOMA) system.
- **CDMA 2000** CDMA 2000 evolves IS-95 to include additional service capabilities based on packet data. It is a direct competitor of the other major 3G standard, UMTS, and operates at 450 MHz (used to refarm NMT, as mentioned earlier, along with GSM operating in the same band, and in developing countries to allow better coverage), 850 MHz, 900 MHz, 1800 MHz, 1900 MHz, and 2100 MHz. CDMA2000 1XRTT has been the first step in the evolution to 3G, which has been recognized as an IMT-2000 technology, and also the first 3G technology to be deployed worldwide.

Since the first releases of the 3G systems, they have evolved quite significantly. CDMA2000 EV-DO (Evolution–Data Only or –Data Optimized, also known as the High-Rate Packet Data air interface) and EV-DO revision A (DOrA), HSDPA (High-Speed Downlink Packet Data Access) are examples of the 3G high-speed data services–capable systems that grew out of the original UMTS and CDMA2000 standards.

If the industry continues to follow the trend established during the transition from 1G to 3G in the transition from 3G to 4G, we should expect to see only one global cellular system based on a common core and radio transmission technology. While this is not yet a certain fact, all evidence suggests that this is going to be the case, as major operators of 3GPP and 3GPP2 networks seem to be converging on a single evolutionary path to 4G.

We must mention, however, another trend developing in parallel with cellular standardization. It appears that systems such as WiMAX (and, to a certain extent and with some additional limitation, Wi-Fi) are being positioned as yet other candidates for deployment in many operators' networks as a complement to or even a complete replacement for 3GPP and 3GPP2 cellular systems.

So, at a time when major cellular families seem to be on an eventual path of convergence, there is a potential for competing technologies (if only on the radio interface side) to be adopted by both the cellular and wireline operators. As a consequence, this may result once again in a plurality of systems. On the other hand, due also to the potential existence of such a plurality of access technologies that need to provide access to the same set of services, it is also recognized that using a single access-independent core is indeed valuable. As such, the industry is experiencing more and more a drive toward using a common core for all mobile (and nonmobile) systems, providing access to the same set of services, maybe based on IMS, thus validating the overall direction toward convergence.

In the following sections we provide a more detailed review of the mobile systems, which are best positioned to participate in FMC solutions. In this discussion we are going to focus on the relevant aspects of these systems such as core network details and operation, and characteristics of the access network that need to be considered when being converged with the fixed network in the context of practical FMC solutions.

3GPP Systems

Both the GSM 2G mobile system and the UMTS 3G system are specified and maintained by 3GPP. The GSM system was originally specified by ETSI under the drive of the European countries[4] to share a common digital system to enable easier intraregion subscriber roaming, but when 3GPP started its work to define a 3G system evolved from the GSM core, it became clear that it would have made perfect sense to also maintain GSM specifications and define their evolution within 3GPP.

Today it is possible to roam using GSM in more than 210 countries. GSM operates in the 900 MHz and 1.8 GHz bands in Europe and the 1.9 GHz and 850 MHz bands in the U.S. The 850 MHz band is also used for GSM and 3GSM in Australia, Canada, and many South American countries. UMTS was originally defined to operate in the

[4] The European Conference of Postal and Telecommunications Administrations (CEPT) created the *Groupe Spécial Mobile (GSM)* in 1982 aiming at developing a standard for a mobile telephone system that could be used across Europe.

1885–2025 MHz band for uplink and 2110–2200 MHz for downlink, though, in addition to these spectrum ranges, today it is commonly run on 850 MHz and 1900 MHz in some countries, notably in the U.S. by AT&T.

3GPP subscribers are identified by means of an International Mobile Subscriber Identity (IMSI), and they are assigned one (or more) MSISDN (Mobile Station ISDN) number, that is, an E.164-compliant telephone number. These are stored on a Smart Card known as the Subscriber Identity Module (SIM) card for GSM, or Universal SIM (USIM) card for UMTS. The smart cards are given to subscribers when they sign up for service, and they can be installed on any 3GPP-compatible handset for its activation with the service. The SIMs are not commonly used in 3GPP2 systems, where subscriber identity is linked to a specific terminal; albeit in recent years the capability to use a smart card has been added to CDMA standards and is now being deployed (especially in China, among other countries) with the smart card–based Removable User Identity (RUID).

The GSM and the UMTS systems share a common core network for both the CS domain (also known as circuit core) and the PS domain (also known as GPRS core, or packet core).

The 3GPP CS core The 3GPP circuit core (shown in Figure 4.1) is based around the Mobile Switching Center (MSC), which acts as a switch for voice and circuit data calls and handles mobility management of "CS-attached" users. CS-attached users are authenticated and accepted by the circuit-switched mobile core and can therefore be handled by the 3GPP system. Authentication of 3GPP users is based on data and algorithms stored in the SIM. On the network side, the authentication function is based on data downloaded from the Home Location Register (HLR), specifically from the

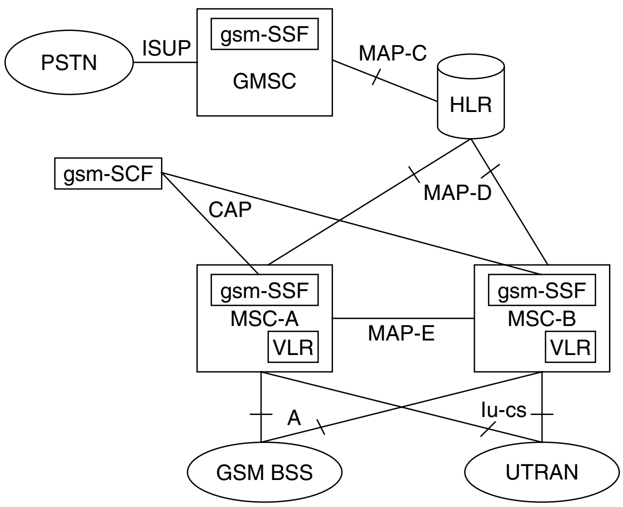

Figure 4.1 The 3GPP circuit core

authentication center (AUC) component of the HLR, into the serving MSC, and more precisely in the Visitor Location Register (VLR), also commonly a component of the MSC. The HLR and VLR are subscriber databases where the subscriptions to services, their parameters, and their activation status information are stored, along with the authentication information.

The HLR is always located in the home network, the network with which the subscriber has a customer-provider relationship. The VLR is located in the visited network. Since both the roamers' and home subscribers' data are stored in the VLR when a subscriber is registered with an MSC, the VLR effectively assumes a role as a cache of subscriber data, used to avoid continuous interrogations of the HLR, which would cause significant signaling load. Note that the VLR was defined to be potentially stand-alone, but in all practical cases today it is implemented within the MSC platform.

MSCs also host Customized Applications for Mobile Network Enhanced Logic (CAMEL) Intelligent Network triggers via the GSM Service Switching Function (gsm-SSF), which are armed to provide Intelligent Network–supported capabilities such as toll-free calling, caller ID, location determination, call forwarding, and so on, by interacting with the GSM Service Control Function (gsm-SCF).

In addition to these functions, the MSC often acts as a gateway to the PSTN, and as such it is identified as gateway MSC (GMSC). In this role the GMSC, as shown in Figure 4.2, would receive incoming ISUP call establishment signaling messages from the PSTN and query the HLR for the whereabouts of the user (more precisely, find out the MSC where the user is known to have last registered with the HLR).

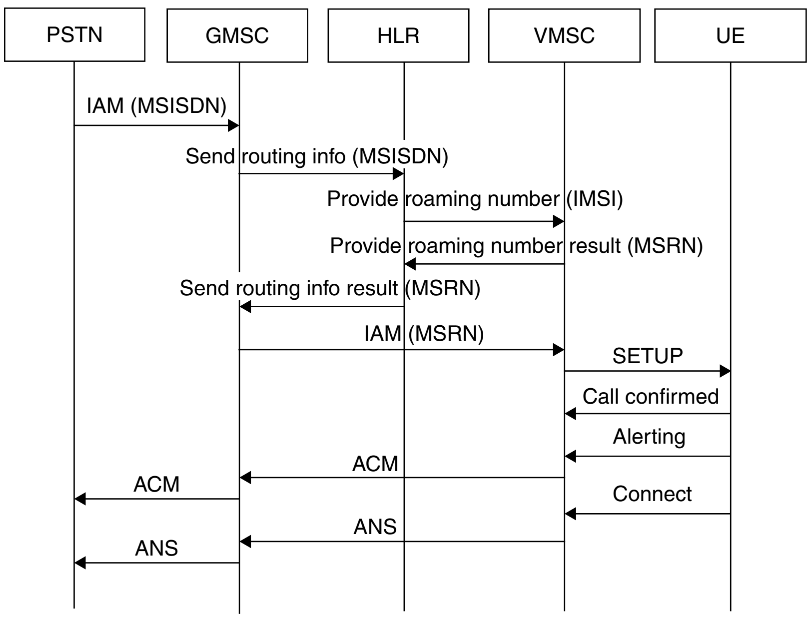

Figure 4.2 Mobile-terminated call setup

The HLR, as shown in Figure 4.2, then queries the visited MSC's VLR to obtain a Mobile Station Roaming Number (MSRN) for the subscriber; the VLR allocates one MSRN and returns it to the HLR, which passes it back to the GMSC. The GMSC would then use ISUP to establish a circuit using the MSRN as the destination number. When the call is set up, the MSRN can be released and used for another subscriber, thus limiting the number of E.164 addresses needed for mobile-terminated call routing at an MSC.

The approaches similar to the one used for such termination of calls have been used for a mechanism to route calls to the IMS or the CS domain in Voice Call Continuity (VCC—described in detail in the next chapter) for dual-mode terminals capable of receiving a voice call in the IMS-based PS or in the CS domain, depending on which network they are attached to. VCC enables the termination of calls in either domain and also enables continuing the call from one domain to another as the terminal changes the access technology it is camped on. VCC is therefore a potentially fundamental component in many FMC applications described in this book.

An MSC can act as a point of interconnection toward the PSTN for outgoing calls, so that they are optimally routed to the PSTN destination if necessary. MSCs interact with the HLR using the IS-41 [101] interface in CDMA and the Mobile Application Part (MAP [102]) interface in GSM. MAP interface variations include:

- MAP-D between VLR and HLR
- MAP-C between the GMSC and the HLR
- MAP-E between MSCs to prepare handover

The MSC also implements circuit-switched supplementary services based on settings and an activation status provided by the HLR (or retrieved from the VLR in the last visited MSC) when a subscriber is accepted by an MSC. This is in contrast to relying on a centralized execution of service logic as in the case of CAMEL-based services, which follow an Intelligent Network model of decoupling service execution from switching.

When integrating a CS network with a PS (for example, an IMS-based PS) network in a converged environment, the operator needs to make sure that services invoked and triggered in the CS network have their state updated or kept in sync in the PS network. Ideally, the services themselves should be evolved to be executed in a single centralized location (logical and/or physical). The example of such centralization is presented by IN and the use of IMS application servers, when dual-mode CS/PS terminals are being used.

Mobility Management MSCs are directly involved in *mobility management (MM)* of users in the idle and active states of both GSM and UMTS, by handling location update procedures and by being involved in handovers between MSCs or between different nodes in the radio access directly attached to the MSC. When the inter-MSC mobility events occur, the new MSC updates the location of the subscriber with the HLR, so that the HLR knows how to route mobile-terminated calls for the subscriber, or how to enforce some asynchronous actions (e.g., purge the subscriber identity and profile from the last known MSC).

Handling mobility management implies interaction with the terminal, which is also necessary for call control. The GSM and UMTS systems use an ISDN-access-signaling-like interaction with the terminal for call control, specified in 3G TS 24.008 [180].

The interfaces to the radio access network of GSM and UMTS, respectively, as shown in Figure 4.1 earlier in the chapter, are called the A interface and the $I_{u\text{-}cs}$ interface. The $I_{u\text{-}cs}$ interface is the interface between the UMTS access and the 3GPP CS core, and it also has an $I_{u\text{-}ps}$ component for the PS domain core. The A interface assumes an E1 (or T1) transport to be available, while the $I_{u\text{-}cs}$ interface assumes an ATM or IP-based transport.

Transcoding The transcoding between the PCM encoding used in the PSTN and the voice codecs used in GSM (AMR, or adaptive multirate voice coding) happens in the base station controller (BSC). Specifically, the *transcoding unit (TRAU)* is a function of the BSC dealing with transcoding. The *A* interface therefore carries the PCM-encoded voice-over-TDM multiplexed channel.

In UMTS, this model changes, with transcoding taking place in the core or preferably avoided altogether with the Transcoder-Free Operation (TrFO) option, where the same encoding of voice is used between terminals in mobile-to-mobile calls. In the TrFO model, the voice quality is therefore quite substantially improved because it avoids several transcodings necessary in the end-to-end data path. For communication with the PSTN, the transcoding between the AMR [63] (or wideband AMR [64]) codec used in UMTS and the PCM codec used in the PSTN takes place as close as possible to the point of interworking with the PSTN.

Bearer-Independent Circuit-Switched Network (BICSN) The UMTS TrFO feature has been defined in a server-based architecture introduced in 3GPP Release 4. By enabling packet-based transport of voice, it is possible to eliminate the need of transit switches in the core network and as such the need to convert AMR- or WB-AMR-encoded voice into PCM for switching in a classic TDM framing. This server-based architecture for the CS core, also known as a bearer-independent circuit-switched network (BICSN), is represented in Figure 4.3.

The attentive reader has already noticed that the difference between the classic architecture and the BICSN is that the MSC is split into a media gateway and MSC server components. MSC servers control the media gateway via the H.248-based M_c interface. The N_b interface supports the transport of the media components between gateways, and the N_c interface, based on BICC signaling, is used to let MSC servers interact with one another to establish calls or set up inter-MSC legs during handover. In addition, starting with Release 4 of the 3GPP specifications, the HLR has been replaced by the new functional element called the Home Subscriber Server (HSS) as a part of the IMS framework. The HSS extends the HLR functionality to support additional interfaces for the interaction with IMS entities, via DIAMETER-based interfaces.

The 3GPP PS Core The PS core of GSM and UMTS, shown in Figure 4.4, is in many aspects similar to the CS core, in that there is a gateway entity, called the gateway

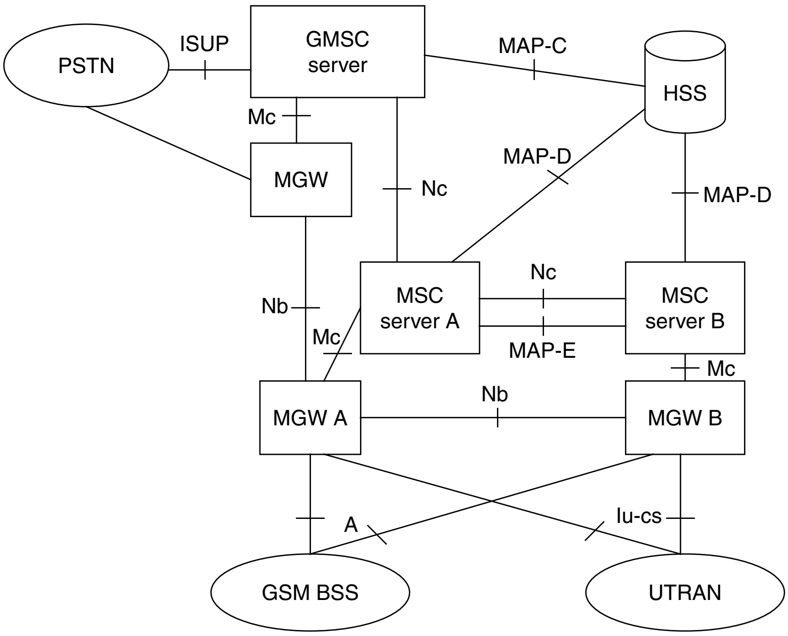

Figure 4.3 Bearer-independent CS network

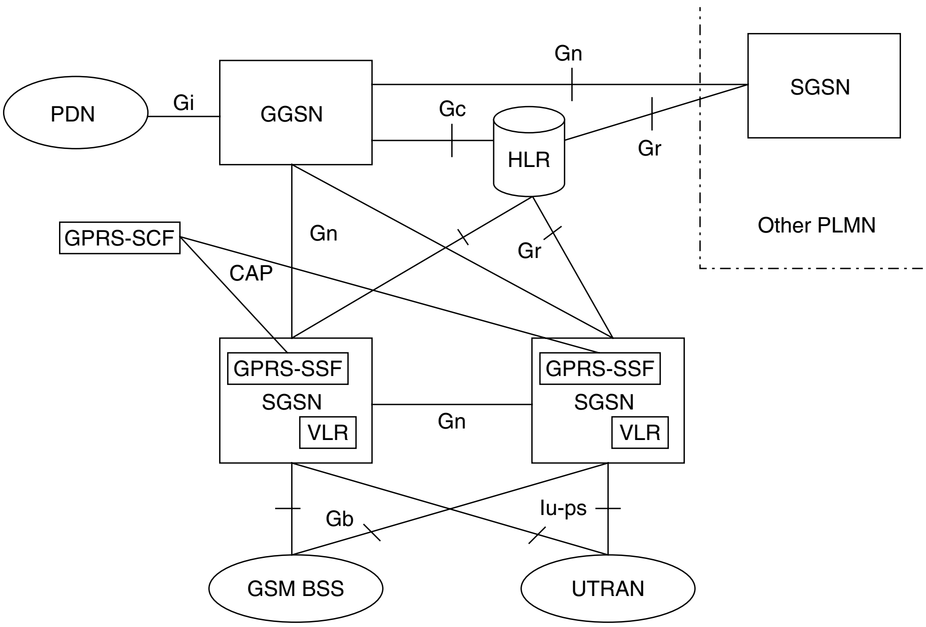

Figure 4.4 The GPRS core network

GPRS support node (GGSN), and a serving entity called the Serving GPRS support node (SGSN) supporting packet data mobility. GPRS itself stands for General Packet Radio Service, which is an extension of the GSM system designed to support packet data services. GPRS is optional to GSM but is an integral component of UMTS from the outset, so technically speaking, the support of GPRS core and services is "not an option," if we can say so, when deploying a UMTS system.

Similarly to the CS core, it is also possible to use CAMEL Intelligent Network services in GPRS, mainly to support prepaid charging models. This is based on the interaction of the SGSN-hosted gprs-SSF, where the CAMEL triggers are armed, with the gprs-SCF. Since the Intelligent Networking subsystem had its roots in the legacy circuit domain, it often does not provide optimal solutions for packet data applications. For example, since deep packet inspection and per-flow charging and QoS policies are better supported at the GGSN, the prepaid and other charging models and services traditionally associated with Intelligent Networking are now transitioning to being handled by the DIAMETER-based interfaces between the GGSN and servers specialized for these functions. This trend is also in alignment with other sectors of the industry (e.g., the RACS/RACF subsystems use DIAMETER-based interfaces for QoS policy control).

The interconnection between the elements of the GPRS core and the HLR (or HSS, in 3GPP Rel-4–based systems) happens via interfaces called G_r (between SGSN and HLR) and G_c (between GGSN and HLR). The G_r interface is used for user data download in the SGSN and location update, while the role of the G_c interface is linked to the support of the network-initiated data sessions feature. This feature works only for statically assigned IP addresses, and it has not proven to be very popular, as IPv4 addresses are a scarce resource and therefore are rarely statically assigned to mobiles. On the other hand, although IPv6 is supported by GPRS standards, and it does not suffer from the issue of scarcity of IP addresses like IPv4, this IP version has not been widely adopted in commercial deployments yet.

The interface between the SGSN and the UMTS access is called $I_{u\text{-}ps}$, and the interface toward the GSM access is called G_b. The $I_{u\text{-}ps}$ interface assumes that either IP transport or Asynchronous Transfer Mode (ATM) transports are available. The G_b interface assumes a Frame Relay transport. Other than these distinct Data Link–layer interfaces and some difference in QoS capabilities defined for GSM and UMTS, there is virtually no difference between the GPRS core for GSM and that for UMTS. The most notable functional allocation difference between GSM and UMTS is that the functions of header compression and ciphering of user data are in the core (and more precisely in the SGSN) for GPRS operating in G_b mode, and in the UTRAN for the I_u mode of operation. "G_b mode" is a way to identify the 3GPP PS core for GSM access only, and "I_u mode" is a way to identify the 3GPP PS core for UMTS access.

The GPRS Tunneling Protocol (GTP) is the protocol for the transfer of user-plane packets between the UMTS access and the UMTS core. GTP is also used over the G_n interfaces between SGSN and GGSN, and between SGSNs during handover. The G_n interface, unlike the I_u interface, uses GTP for both control and user planes (that is, both the GTP-C and GTP-U versions of GTP, specified in 3GPP TS 29.060 [181]). In the $I_{u\text{-}ps}$ interface, only GTP-U is used and the control is based on the RAN Application Part (RANAP) protocol.

In the course of 3GPP Release 7 development, an option to bypass the user plane of the SGSN under certain conditions (i.e., nonroaming user, no lawful interception activated, no CAMEL services enabled) has been introduced for the I_u mode of operation, thus enabling a direct tunnel between the access network and the GGSN. This feature seems to find its justification in higher data rates introduced in the UTRAN in 3GPP Rel-6 and Rel-7.

In the roaming case, the GGSN can be located in the home network or in the visited network, depending on the roaming agreements. This is different from the CS core, where the GMSC is always in the home network, regardless of the user location. When the GGSN is in the home network and the SGSN is in the visited network, the G_n interface connecting them becomes the G_p interface (which is only a difference in names, rather than a protocol-level difference).

Even though the capability to use a GGSN in the visited network is foreseen by the GPRS specifications, this option has not yet been used by operators as part of their roaming agreements. This is perhaps because of the practices linked to a legacy of operation of CS networks, but it is also because the operators want to have tight control of the user traffic at all times, so they wish to enforce policies or perform deep packet inspection in the home network when users are roaming.

The GGSN connects to external networks (also identified with the acronym PDN, or Packet Data Network) via the G_i interface, and the selection of an external network by the UE is done by submitting an access point name (APN) when the first Packet Data Protocol (PDP) context is created for a PDP session. A PDP context identifies a bearer used for a GPRS data session. For a single data session there can be one or multiple PDP contexts (up to 11 in UMTS), depending on the different levels of QoS used. Operator policies may determine the value of a default APN for the user when one is not specified at PDP context activation, and also the level of QoS allowed for a PDP context.

From 3GPP Release 7 onward, a framework to enforce QoS and charging policies on a per–IP flow basis has been introduced, so that the allowed QoS and the charging for each IP flow can be controlled based on the information derived from the applications associated with these flows. This framework is known as Policy Control and Charging (PCC), specified in 3GPP TS 23.203 [52]. As illustrated in Figure 4.5, PCC enables the

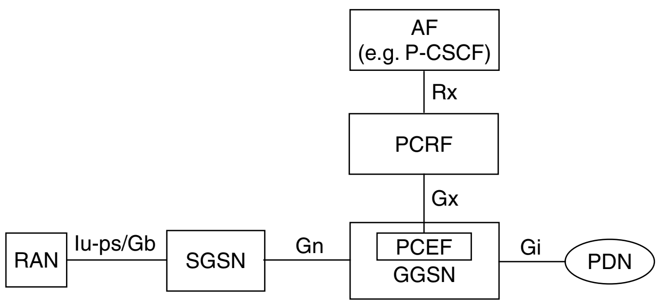

Figure 4.5 PCC framework

GGSN to act as the Policy and Charging Enforcement Function (PCEF) and interact with a Policy and Charging Rules Function (PCRF) via a DIAMETER-based G_x interface to enforce PCC decisions taken by the PCRF. The PCRF bases its decisions on the interactions with an Application Function (AF) via the DIAMETER-based R_x interface.

As VoIP becomes popular within wireline networks, it is likely that, given its acceptance, it will gain prominence in the cellular environment too. The IP Multimedia Subsystem has been defined to support VoIP service via the cellular PS domain in both 3GPP and 3GPP2. When VoIP is deployed in cellular, the PCC infrastructure is also introduced to support prioritization of voice flows (especially those related to emergency calls) and to provide fine-granularity QoS as well as gating of undesirable data that is not related to ongoing and accepted voice sessions. In the case of IMS, the Application Function is the Proxy CSCF (P-CSCF).

Radio Access Network and Terminal Aspects Since aside from minor differences, GSM and UMTS share a common core, the substantial distinction between GSM and UMTS mobile systems is confined to the radio access network. Besides Physical-layer differences, where multiple access to the radio resources is based on TDMA for GSM and W-CDMA for UMTS (at least in its terrestrial aspects), the radio access networks for GSM and UMTS differ in both the respective network elements and their capabilities.

The GSM Radio Access Network The GSM base station subsystem, depicted in Figure 4.6, includes a base station controller (BSC) connected via A-bis interfaces to a number of a base transceiver stations (BTSs). BTS supports radio frequency transmission to and reception from the mobile station (MS) via the U_m interface. The BSC, in addition to supporting inter-BTS mobility and encryption of voice communications, also performs transcoding between the voice-encoding format used over the radio interface and that used in the PSTN.

When the optional GPRS feature is added, the BSC supports the PCU (Packet Control Unit) used to add the packet data transmission capabilities without impact on the rest of the access network. When EDGE is deployed, theoretically raising the data rates to approximately 300 Kbps, then some modification to the BTS is needed.

Recently 3GPP has defined the I_u mode of operation for GSM, where the GSM BSS (depicted in Figure 4.6) is made compatible with the I_u interface used to access 3GPP core. However, since this would not change the overall GSM capabilities for the end user, which are limited by the BSS itself, and, especially, GSM terminal capabilities,

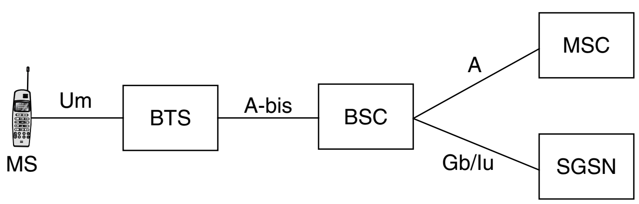

Figure 4.6 The GSM BSS (base station subsystem)