CHAPTER 6

CDMA Technology

Upon completion of this chapter, the student should be able to:

- Discuss the basic concepts and evolution of CDMA technology.
- Discuss the difference between the various access technologies; namely FDMA, TDMA, and CDMA.
- List the United States frequency bands used for CDMA technology.
- Discuss CDMA network and system architecture.
- Discuss network management.
- Discuss CDMA channel and frame concepts.
- Discuss the functions of the forward and reverse logical channels.
- Discuss CDMA system operations: initialization, call establishment, call handoff, and power control.
- Discuss the implementations of 3G cellular using CDMA technology.

This chapter introduces another cellular wireless air interface technology known as code division multiple access or CDMA. Because of the importance of CDMA as the air interface technology of the future and the amount of detail included in this chapter, it has been organized into three parts: CDMA system overview, CDMA basics, and 3G CDMA. First deployed commercially in 1995, CDMA is a relatively new technology. However, CDMA-based systems are overwhelmingly being counted on to provide the needed infrastructure to implement future 3G systems and beyond (4G). Part I of this chapter begins with an introduction to the first deployment of 2G CDMA systems and the subsequent evolution to 3G CDMA systems. Included in this introduction is an explanation of basic CDMA operation, the frequency allocations allowed for CDMA use in the United States, and CDMA frequency reuse issues. An overview of the present cdma2000 (the initial phase of 3G cellular) network and system architecture is presented next with short descriptions of the operation and functions of the network elements included in the overview. Since many of the common network elements have been previously discussed, the emphasis in this chapter is on new network elements and differences in the wireless network due to the use of CDMA technology. A detailed introduction to cellular network management techniques is included also.

In an effort to not overwhelm the reader, the second part of this chapter provides a detailed explanation of the IS-95B CDMA channel concept and the actual implementation details of the air interface signals for this 2G technology. Forward and reverse logical channels are described and their functionality within the system is explained. The CDMA frame format is also introduced and its significance within the system explained for both forward and reverse logical channels. With the basic technical details fairly well covered,

CDMA system operations are introduced. Initialization/registration procedures are covered and call establishment is introduced through the context of the four states of CDMA mobile station operation. Sophisticated handoff procedures and power control operations that are peculiar to CDMA technology are covered in detail to conclude this section.

Part III of this chapter concludes with an overview of the changes and modifications made to 2G CDMA (IS-95A) to provide 2.5G (IS-95B) services and the further changes needed to provide 3G functionality with cdma2000. Cdma2000 channel structure and operation is examined fairly extensively with additional information presented about the evolution of GSM cellular to 3G UMTS (a CDMA-based system). Finally, a short introduction to wideband CDMA and other emerging 3G technologies based on time division multiplexing versions of CDMA is presented.

PART I CDMA SYSTEM OVERVIEW

6.1 INTRODUCTION TO CDMA

As outlined earlier in Chapter 2, in a response to the 1988 Cellular Telecommunications Industry Association's (CTIA) User Performance Requirements (UPRs) for the next generation of wireless mobile service, a totally new digital technology known as code division multiple access or CDMA was starting to be developed by Qualcomm Corporation in 1989. This development of CDMA technology continued into the early 1990s at which time it was accepted for use as an air interface standard.

During the 1980s, AMPS was the cellular telephone system employed in the United States. In 1989, the Telecommunications Industry Association (TIA) adopted time division multiple access (TDMA) technology as the radio interface standard that would meet the requirements of the next generation of wireless systems. However, Qualcomm, with the support of various players in the mobile wireless industry, developed an alternative air interface technology that also met these requirements. In 1992, the TIA Board of Directors adopted a resolution that eventually led to the acceptance of IS-95 in July of 1993 as the CDMA air interface standard for the digital transmission technologies known as wideband spread spectrum. The first CDMA commercial network began operation in Hong Kong in 1995. Since that time, CDMA systems have been used in both the cellular and PCS bands extensively in the United States and throughout the rest of the world. CDMA has experienced very rapid growth (see the CDMA Development Group Web site at www.cdg.org) and is predicted to continue this growth as one of the primary technologies for the eventual deployment of 3G cellular in one CDMA form or another (time division CDMA [TD-CDMA], time division synchronous CDMA [TD-SCDMA], multicarrier CDMA [MC-CDMA], wideband CDMA [W-CDMA], etc.).

Evolution of 2G CDMA

The first form of CDMA to be implemented, IS-95, specified a dual mode of operation in the 800-MHz cellular band for both AMPS and CDMA. This first standard defined the mobile station and base station requirements that would ensure compatibility for both AMPS and CDMA operation. Additional features were added to the CDMA standard in 1995 when IS-95A was published. IS-95A is the basis for many of the commercial 2G CDMA systems installed around the world. The IS-95A standard describes the structure of wideband 1.25-MHz CDMA channels and the operations necessary to provide power control, call processing, handoffs, and registration procedures for proper system operation. Besides voice service, cellular operators were able to provide circuit-switched data service at 14.4 kbps over these first CDMA systems. ANSI J-STD-008 provided for CDMA operation in the PCS bands. Newer additional features and capabilities were added and the standard became TIA/EIA-95-B in 1999 (also known as TIA/EIA-95). This updated standard provided for the compatibility of 1.8- to 2.0-GHz CDMA PCS systems with IS-95A and

superceded ANSI J-STD-008. Since these systems allowed packet-switched data service at rates up to 64 kbps, they are known as 2.5G CDMA technology.

These early forms of CDMA are grouped together under the banner of **cdmaOne,** which is the trademark of the CDMA Development Group. Figure 6–1 shows a typical cdmaOne network and the standards associated with the various network components.

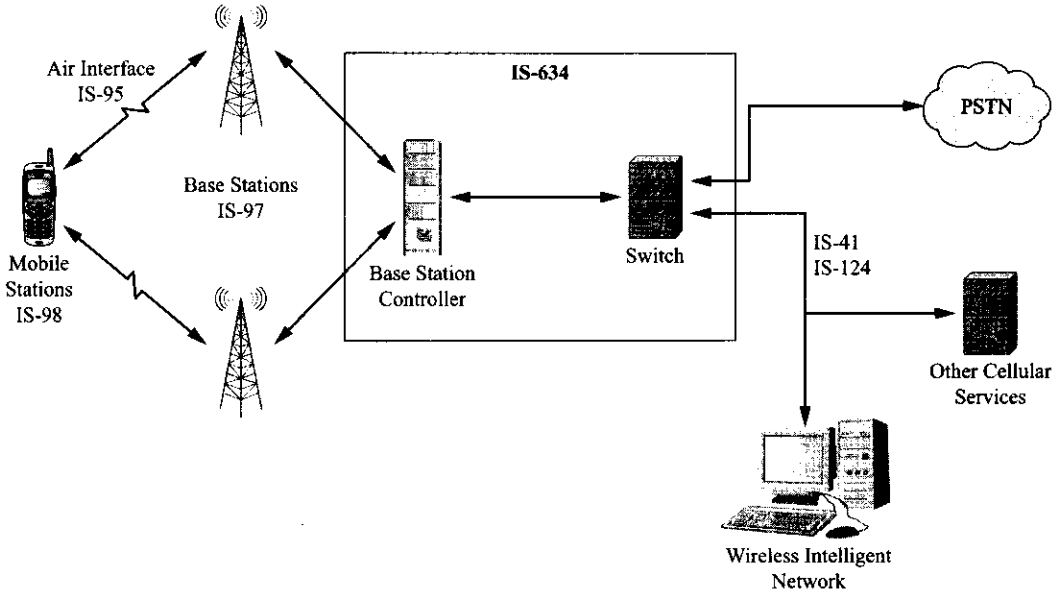


Figure 6–1 Typical components of a cdmaOne network.

Evolution of 3G CDMA

Cdma2000 is the term used for 3G CDMA systems. Cdma2000 was one of five proposals the ITU approved for IMT-2000 third-generation (3G) standards. As previously mentioned in Chapter 2, cdma2000 is the wideband enhanced version of CDMA. It is backward compatible with TIA/EIA-95-B and provides support for data services up to 2 mbps, multimedia services, and advanced radio technologies. The implementation of cdma2000 technology is to occur in planned phases with the first phase known as 1xRTT (1X radio transmission technology) happening over a standard 1.25-MHz CDMA channel. The next phase of implementation is known as cdma2000 1xEV (where EV stands for evolutionary). There are two versions of 1xEV: 1xEV-DO (data only) and 1xEV-DV (data and voice). 1xEV-DO can support asymmetrical peak data rates of 2.4 mbps in the downlink direction and 153 kbps in the uplink direction. 1xEV-DV can support integrated voice and data at speeds up to 3 mbps over an all-IP network architecture. The changeover from cdmaOne to cdma2000 1xRTT has been ongoing in the United States and the rest of North America since late in the year 2000. Currently, there are several cdma2000 1xEV-DO systems in operation worldwide with more in the planning stage. Again, see the CDMA Development Group's Web site for information about the worldwide deployment of 3G cdma2000 systems. Further information about cdma2000 and other 3G CDMA technologies will be presented later in this chapter.

CDMA Basics

CDMA is a multiple-access technology that is based on the use of wideband spread spectrum digital techniques that enable the separation of signals that are concurrent in both time and frequency. All signals in this system share the same frequency spectrum simultaneously. The signals transmitted by the mobile

stations and the base stations within a cell are spread over the entire bandwidth of a radio channel and encoded in such a way as to appear as broadband noise signals to every other mobile or base station receiver. The identification and subsequent demodulation of individual signals occur at a receiver through the use of a copy of the code used to originally spread the signal at the transmitter. This process has the net effect of demodulating the signal intended for the receiver while rejecting all other signals as broadband noise. Since a specific minimum level of signal-to-noise ratio is necessary to provide for a certain level of received signal quality, the level of background noise or interference from all system transmissions ultimately limits the number of users of the system and hence system capacity. Therefore, CDMA systems are carefully designed to limit the output power of each transmission to the least amount of power necessary for proper operation.

At this time, it will be helpful to compare the CDMA air interface scheme with the frequency division multiple access (FDMA) and time division multiple access (TDMA) air interfaces (see Figure 6–2). For FDMA, the available radio spectrum is divided into narrowband channels and each user is given a particular channel for his or her use. The user confines transmitted signal power within this channel, and selective filters are used at both ends of the radio link to distinguish transmissions that are occurring simultaneously on many different channels. The frequency allocations can only be reused at a distance far enough away that the resulting interference is negligible. The TDMA scheme goes one step further by dividing up the spectral allocation into timeslots. Now, each user must confine its transmitted spectral energy within the particular timeslot assigned to it. For this case, the mobile and the base station must employ some type of time synchronization. This technique increases spectral efficiency at the expense of each user's total data rate. In CDMA, each mobile has continuous use of the entire spectral allocation and spreads its transmitted energy out over the entire bandwidth of the allocation. Using a unique code for each transmitted signal, the mobiles and the base station are able to distinguish between signals transmitted simultaneously over the same frequency allocation. CDMA can also be combined with FDMA and TDMA technologies to increase system capacity.

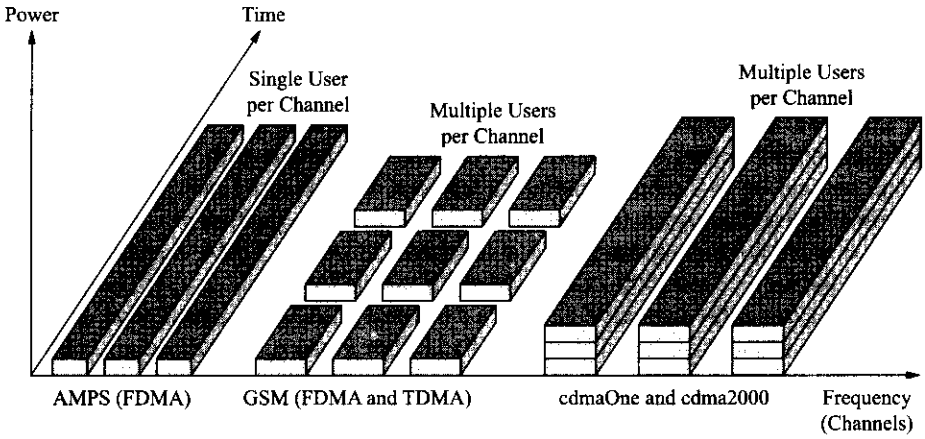


Figure 6–2 Comparison of FDMA, TDMA, and CDMA air interfaces.

For 2G CDMA systems, one might be inclined to state that the frequency separation between adjacent carriers or channels is 1.25 MHz. In CDMA standards, the terms *carrier* and *channel* are carefully distinguished from one another. A carrier frequency may be divided by means of codes into sixty-four different channels. Each of these channels may carry information related to a separate and distinct conversation or data connection in digital form. This distinction is also true of TDMA systems where each carrier is divided into timeslots and each timeslot serves as a channel. In older FDMA systems, the two terms are synonymous and hence a source of confusion when discussing these new technologies.

CDMA Frequency Bands

Presently, in the United States, CDMA systems can be deployed for use in the existing cellular frequency bands (Band Class 0) and the personal communications service (PCS) bands (Band Class 1). In the future, 3G CDMA systems will also be allowed in the newly released 1710–1755 MHz and 2110–2155 MHz advanced wireless services (AWS) bands (see the FCC Web site at www.fcc.gov for further details about the use of these bands). In other parts of the world there are various additional frequency bands (with band class designations given by the CDMA standards) available for CDMA use including a lower frequency band at 450 MHz. When used in the cellular bands, a frequency separation of 45 MHz between the forward and reverse channels is employed. The MS transmit frequency band is 824–849 MHz and the BS transmit frequency band is 869–894 MHz. In this band, not all of the frequencies are designated for use by CDMA cellular wireless networks. Recall that the FCC requires AMPS service to be supported until 2007, so some of the channels are reserved for this purpose. This dual use of the cellular frequency band gives rise to dual-mode CDMA phones.

The 1900-MHz PCS band may be used for either GSM, NA-TDMA, or CDMA technologies. Refer back to Figure 5–2 for details of the PCS bands and Table 5–3 for GSM carrier frequencies. Table 6–1 shows the corresponding CDMA and NA-TDMA PCS channel numbers and carrier frequencies. For CDMA, with a 50-kHz channel spacing, the chart indicates a total of 1200 CDMA channel numbers (carrier frequencies) over the 60 MHz of allocated frequency. The chart also indicates the NA-TDMA channel numbers. One can see that there is not a one-to-one correspondence between the CDMA and NA-TDMA channel numbering systems or between either of these systems and the GSM channel numbers shown in Table 5–3. Additionally, the CDMA spacing between transmit and receive frequencies is 80 MHz whereas for NA-TDMA it is 80.04 MHz and for GSM it is 90 MHz. All this means is that there are possible interference concerns between all of these systems on both the uplink and downlink frequencies where coexisting systems are located.

Table 6–1 CDMA and NA-TDMA channel numbers and frequency assignments for the PCS band (Band Class 1) (Courtesy of 3GPP2)

Transmitter	*CDMA PCS Channel Number (N)*	*Center Frequency for CDMA Channel (MHz)*	*TDMA PCS Channel Number (N)*	*TDMA PCS Channel Frequency (MHz)*
Mobile Station	$0 \le N \le 1199$	$1850.000 + 0.050\ N$	$1 \le N \le 1999$	$1849.980 + 0.030 \times N$
Base Station	$0 \le N \le 1199$	$1930 + 0.050\ N$	$1 \le N \le 1999$	$1930.020 + 0.030 \times N$

In an effort to reduce interference issues in the PCS band, the FCC has indicated the availability of a channel for CDMA use by designating the channels in the PCS band as valid, conditionally valid, or not valid for CDMA use as shown in Table 6–2. Table 6–3 shows a listing of preferred CDMA channels by PCS frequency block and spreading rate (to be discussed later). These preferred channels are the channel numbers a CDMA mobile will scan when looking for service. Note that the spacing between the preferred channels is 1.25 MHz or the minimum spacing allowed between adjacent CDMA carrier frequencies. Note also that conditionally valid channels 300, 400, 700, 800, and 900 can only be used if the service provider has a license for both the frequency block containing the channel and the immediately adjacent frequency block.

Frequency Planning Issues

Because of a frequency reuse factor of $N = 1$, CDMA frequency planning is relatively simple compared to analog cellular systems. For a system that only requires one carrier per base station, that carrier must be

Table 6–2 Useable CDMA channel numbers and assigned frequencies for Band Class 1 (Courtesy of 3GPP2)

Table 2.1.1.1.2-3. CDMA Channel Numbers and Corresponding Frequencies for Band Class 1 and Spreading Rate 1

Block Designator	*CDMA Channel Validity*	*CDMA Channel Number*	*Transmit Frequency Band (MHz)*	
			Mobile Station	*Base Station*
A (15 MHz)	Not Valid	0–24	1850.000–1851.200	1930.000–1931.200
	Valid	25–275	1851.250–1863.750	1931.250–1943.750
	Cond. Valid	276–299	1863.800–1864.950	1943.800–1944.950
D (5 MHz)	Cond. Valid	300–324	1865.000–1866.200	1945.000–1946.200
	Valid	325–375	1866.250–1868.750	1946.250–1948.750
	Cond. Valid	376–399	1868.800–1869.950	1948.800–1949.950
B (15 MHz)	Cond. Valid	400–424	1870.000–1871.200	1950.000–1951.200
	Valid	425–675	1871.250–1883.750	1951.250–1963.750
	Cond. Valid	676–699	1883.800–1884.950	1963.800–1964.950
E (5 MHz)	Cond. Valid	700–724	1885.000–1886.200	1965.000–1966.200
	Valid	725–775	1886.250–1888.750	1966.250–1968.750
	Cond. Valid	776–799	1888.800–1889.950	1968.800–1969.950
F (5 MHz)	Cond. Valid	800–824	1890.000–1891.200	1970.000–1971.200
	Valid	825–875	1891.250–1893.750	1971.250–1973.750
	Cond. Valid	876–899	1893.800–1894.950	1973.800–1974.950
C (15 MHz)	Cond. Valid	900–924	1895.000–1896.200	1975.000–1976.200
	Valid	925–1175	1896.250–1908.750	1976.250–1988.750
	Not Valid	1176–1199	1908.800–1909.950	1988.800–1989.950

chosen from the list of preferred CDMA channels. The same channel should be used by all the base stations throughout the system to take advantage of soft and softer handoff capabilities that are possible with CDMA technology. This topic will be covered in more detail later in this chapter. Additional system capacity can be added by the addition of new base stations or by increasing the number of base station carriers. The latter option is the most economical and therefore most commonly taken route. Due to typically nonuniform growth in the subscriber base across a system, it is very likely that not every base station will have the same number of carrier frequencies. This fact will degrade system operation, since there will be times that soft or softer handoff will not be available because the carrier in use is not available in the new cell. As a general rule, there should be no more than one different frequency carrier across coverage boundaries.

Frequency planning in the PCS bands becomes much more problematic if one considers intersystem issues. There are three possible cases to consider. If the two systems are both CDMA, then geographically neighboring systems should not affect one another. However, the pilot phase offset assignments (this topic will be considered later) must be coordinated between the systems. If the second system is either an NA-TDMA or a GSM system operating in an adjacent geographic area within the same frequency block, the service providers involved will have to coordinate the base station frequency utilization along the boundary between the systems. This process will also include the establishment of a frequency guard zone between the two systems. It should be pointed out that this is not a trivial problem and it will not be addressed at any

Table 6–3 Preferred set of CDMA frequency assignments for Band Class 1 (Courtesy of 3GPP2)

Frequency Block	*Spreading Rate*	*Preferred Channel Numbers*
A	1	25, 50, 75, 100, 125, 150, 175, 200, 225, 250, 275
	3	50, 75, 100, 125, 150, 175, 200, 225, 250
D	1	325, 350, 375
	3	350
B	1	425, 450, 475, 500, 525, 550, 575, 600, 625, 650, 675
	3	450, 475, 500, 525, 550, 575, 600, 625, 650
E	1	725, 750, 775
	3	750
F	1	825, 850, 875
	3	850
C	1	925, 950, 975, 1000, 1025, 1050, 1075, 1100, 1125, 1150, 1175
	3	950, 975, 1000, 1025, 1050, 1075, 1100, 1125, 1150

further length here. The last case to be considered is when some preexisting service is still using the PCS frequency spectrum. In this case, frequency coordination is again necessary in conjunction with the consideration of the type of preexisting service and the interference that it produces or can tolerate.

6.2 CDMA NETWORK AND SYSTEM ARCHITECTURE

The reference architecture for wireless mobile systems deployed in North America is based upon standards developed by the TIA. The TIA Committee TR-45 develops system performance, compatibility, interoperability, and service standards for the cellular band, and committee TR-46 coordinates the same activities for the PCS band. The TR-45.3 subcommittee deals with NA-TDMA and the TR-45.5 subcommittee with CDMA. Furthermore, the TR-45 committee works closely with the 3GPP2 organization to specify the standards for cdma2000. For more information about these activities visit the TIA Web site at www.tiaonline.org.

The initial reference architecture for IS-95 CDMA is very similar to the GSM reference architecture presented in Chapter 5. The adoption of TIA/EIA-95 provided for additional network interfaces that exist between the various system elements. This reference model developed by TR-45/46 is depicted by Figure 6–3.

The new cdma2000 reference architecture (see Figure 6–4) has been enhanced to include even more additional network access interfaces. These interfaces are mainly concerned with the evolving structure of cdma2000 toward an all-IP core network.

As was discussed with GSM cellular, messaging between CDMA system network elements is carried out through the use of protocols very similar to SS7. TIA/EIA-634-B is an open interface standard that deals with signaling between the MSC and the BSC (over the A interface), and TIA/EIA-41-D describes

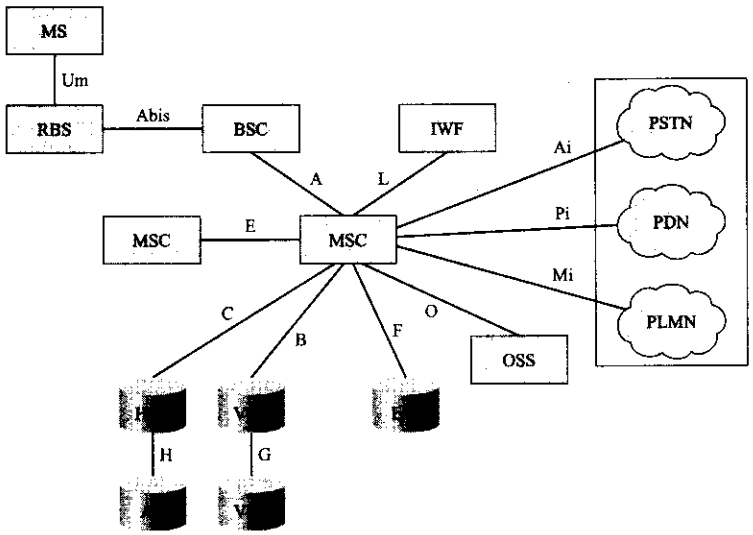


Figure 6–3 Initial CDMA (IS-95) reference architecture.

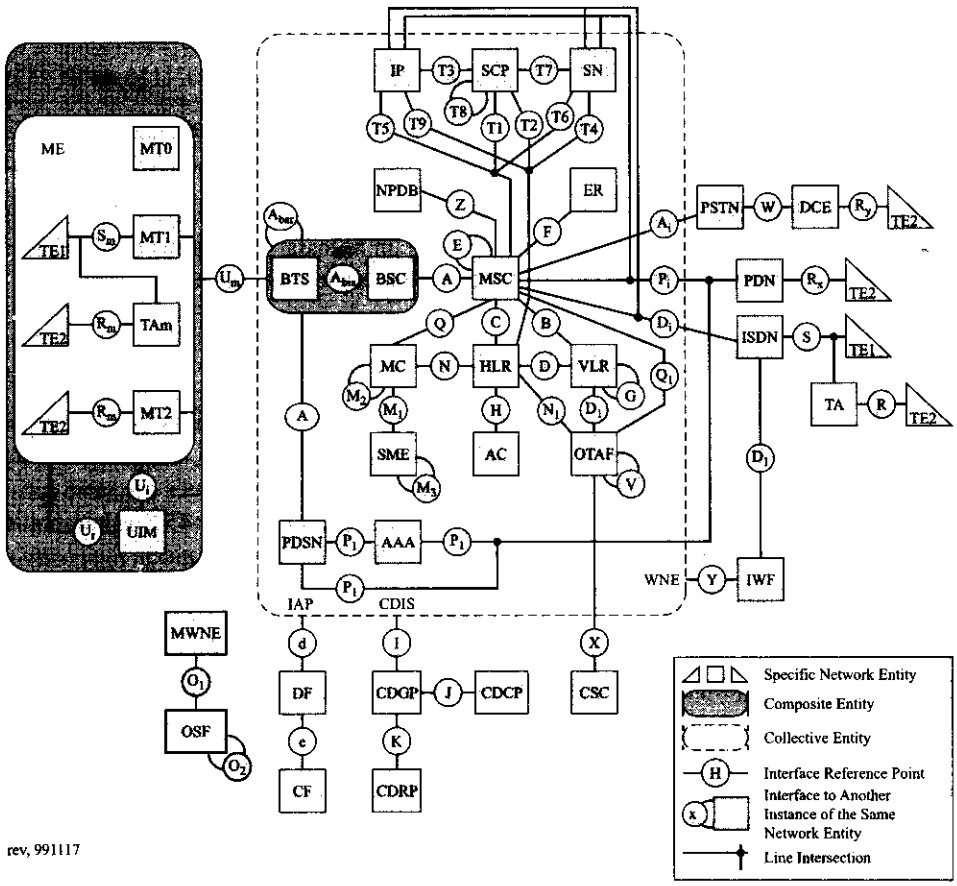


Figure 6–4 Cdma2000 reference architecture (Courtesy of 3GPP2).

the protocols used between the other core network elements (MSC, VLR, HLR, AC, etc.). For these other network elements, each vendor's equipment provides compatibility with this latter protocol suite and hence is capable of interoperability with other vendor's equipment.

In the case of the MSC-to-BSC interface, TIA/EIA-634-B provides for the messaging between these two system elements and now allows the equipment used for these functions to be provided by multiple different vendors. Figure 6–5 shows the layered architecture specified by TIA/EIA-634-B.

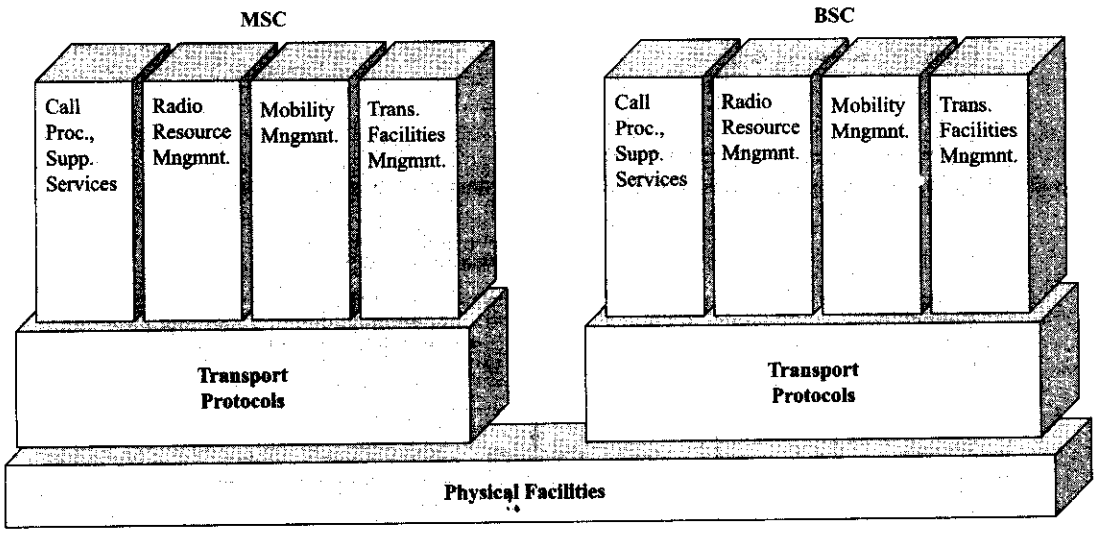


Figure 6–5 Cdma2000 MSC-BSC interface functional planes (Courtesy of 3GPP2).

The A interface between the MSC and the BSC, as shown by Figure 6–5, supports four functional planes. Call processing and mobility management functions occur between the mobile station and the MSC. The types of call processing and supplementary services supported over TIA/EIA-634-B include calls originated and terminated by the subscriber, call release, call waiting, and so forth. The mobility management functions support the typical operations of registration and deregistration, authentication, voice privacy, and so forth. The BSC passes these messages from the MSC through to the subscriber terminal over the air interface (via the RBS). The functions of radio resource management and transmission facilities management occur between the MSC and the base station. The transmission facilities management operations are concerned with the facilities that transport the voice, data, or signaling information between the MSC and the base station. The radio resource management operations are concerned with the maintenance of the radio link between the subscriber and the radio base station, the operations necessary to accomplish this, and the initiation of handoff operations. As CDMA evolves toward 3G, the 3GPP2 group will continue to update the standards involving the newer interfaces that have been defined for cdma2000 and at some point will supercede the original IS-95 standards.

Most of the CDMA system network elements have been discussed in other chapters of this book and have the same functionality as previously explained. In an effort to provide continuity within this chapter a brief overview of these elements will be presented again, with emphasis placed on network elements not previously discussed. The next sections refer to Figure 6–6 that shows the major network elements of a modern cdma2000 system and Figure 6–7 that shows additional detail of the typical network nodes found in cdma2000.

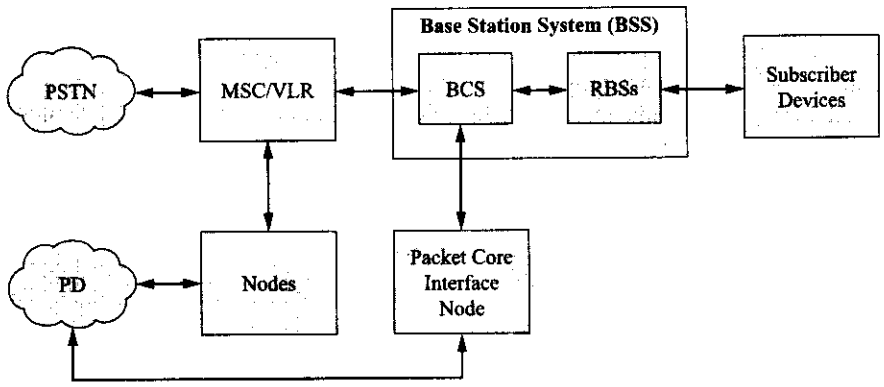


Figure 6–6 Major network components of a cdma2000 wireless system (Courtesy of Ericsson).

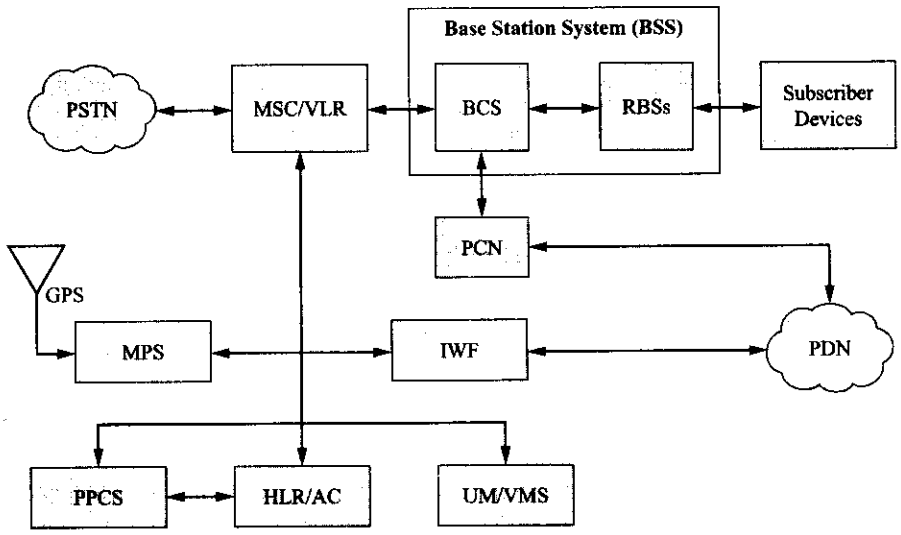


Figure 6–7 Details of the network nodes found in a cdma2000 wireless system (Courtesy of Ericsson).

Mobile-Services Switching Center and Visitor Location Register

The CDMA mobile-services switching center (MSC) serves as the interface between the public switched telephone network (PSTN) and the base station subsystem (BSS). The MSC performs the functions necessary for the establishment of calls to and from the system's mobile subscribers. Additionally, the MSC, in conjunction with other network system elements, provides the functionality needed to permit subscriber mobility and roaming. Some of these operations include subscriber registration and authentication, location updating functions, call handoffs, and call routing for roaming subscribers.

Typically the visitor location register (VLR) function is colocated with the MSC. Its function is to provide a database containing temporary information about registered subscribers that may be needed by the MSC in the performance of call control operations and the provisioning of subscriber services for the mobiles currently registered in the MSVC/VLR service area.

Interworking Function

In the early (IS-95) CDMA systems, the interworking function (IWF) node is the only gateway between the wireless network and the packet data network (PDN). As such, it provides a direct connection to the PDN

for packet data calls. Additionally, the IWF node supports circuit-switched data calls by providing internal modems for connections to dial-up Internet service providers (ISPs). These circuit-switched data calls are routed to the PSTN through the MSC. Today, the IWF typically uses Ethernet for the signaling between itself and the MSC and for the exchange of packet data between itself and the PDN. In cdma2000, the IWF's packet data transfer function is augmented by the packet core network (PCN) element.

Mobile Positioning System

In an ongoing program mandated by the FCC and designed to upgrade the United States' cellular systems, a location system is incorporated by the CDMA system that can determine the geographic position of a mobile subscriber. This **mobile positioning system** (MPS) is based on the Global Positioning System (GPS) and is to be used for emergency services. The ability to locate the caller is known as Enhanced 911 or E911. Other proposed uses of this system capability relate to what are known as "location-based services" or location-specific marketing tools.

For Phase 1 of the wireless E911 program, the cellular system must be able to tell a local public safety answering point (PSAP) the location of the cellular antenna that is handling the emergency call. In Phase 2 of the first implementations of this location determining system, the MPS uses a form of mobile-assisted GPS and triangulation to determine the latitude and longitude of the mobile within 50 to 100 meters. It is believed that later phases of this system will be able to lower the system uncertainty even further. The FCC has set a timetable for the rollout of this service with an expected implementation by cellular service providers by the end of 2005.

There has already been much discussion about the idea of "big brother" knowing one's location via one's cell phone and it remains to be seen where this technology will lead to over the coming years vis-à-vis the privacy issue. Additionally, unwanted spam over the Internet and unsolicited calls from telemarketers have recently become hot political topics and it remains to be seen whether location-based services will be accepted by the cellular subscriber or just become another form of telemarketing or wireless spam.

Unified Messaging/Voice Mail Service

Ericsson Corporation's new cdma2000 systems contain a unified messaging/voice mail service (UM/VMS) node that integrates e-mail and voice mail access. This node provides messaging waiting indication using short message service (SMS) and multiple message retrieval modes including the use of DTMF or either a Web or WAP browser. As shown in Figure 6–7, the UM/VMS node connects to the PDN and the MSC in Ericsson's system.

HLR/AC

The home location register (HLR) and authentication center (AC) are typically colocated in cdma2000 systems. The HLR holds subscriber information in a database format that is used by the system to manage the subscriber device (SD) activity. The type of information contained in the HLR includes the SD electronic serial number (ESN), details of the subscriber's service plan, any service restrictions (no overseas access, etc.), and the identification of the MSC where the mobile was last registered.

The AC provides a secure database for the authentication of mobile subscribers when they first register with the system and during call origination and call termination. The AC uses shared secret data (SSD) for authentication calculations. Both the AC and SD calculate SSD based on the authentication key or A-key, the ESN, and a random number provided by the AC and broadcast to the SD. The A-key is stored in the SD and also at the AC and never transmitted over the air. The AC or MSC/VLR compares the values calculated by the AC and the SD to determine the mobile's status with the system.

PPCS and Other Nodes

The prepaid calling service (PPCS) node provides a prepaid calling service using the subscriber's home location area MSC. This node provides the MSC with information about the subscriber's allocated minutes and provides the subscriber with account balance information. The PPCS node is usually associated with a prepaid administration computer system that provides the necessary database to store subscriber information and update it as needed. The prepaid administration system (PPAS) provides the subscriber account balance information to the PPCS system. The MSC sends information about subscriber time used to the PPAS for account updating. In the future, other additional nodes may be added to the system to provide increased system functionality like intersystem roaming.

Base Station Subsystem

A base station subsystem (BSS) consists of one base station controller (BSC) and all the radio base stations (RBSs) controlled by the BSC (refer back to Figure 6–6). The BSS provides the mobile subscriber with an interface to the circuit switched core network (PSTN) through the MSC and an interface to the public data network (PDN) through the packet core network (PCN). There can be more than one BSS in a cdma2000 system. Today, the combination of all the CDMA BSSs and the radio network management system that oversees their operation is known as the CDMA radio access network or C-RAN.

Base Station Controller

In a cdma2000 system, the base station controller (BSC) provides the following functionality. It is the interface between the MSC, the packet core network (PCN), other BSSs in the same system, and all of the radio base stations that it controls. As such, it provides routing of data packets between the PCN and the RBSs, radio resource allocation (the setting up and tearing down of both BSC and RBS call resources), system timing and synchronization, system power control, all handoff procedures, and the processing of both voice and data as needed.

Radio Base Station

The cdma2000 radio base station (RBS) provides the interface between the BSC and the subscriber devices via the common air interface. The functions provided by the RBS include CDMA encoding and decoding of the subscriber traffic and system overhead channels and the CDMA radio links to and from the subscribers. The typical RBS contains an integrated GPS antenna and receiver that is used to provide system timing and frequency references, a computer-based control system that monitors and manages the operations of the RBS and provides alarm indications as needed, communications links for the transmission of both system signals and subscriber traffic between itself and the BSC, and power supplies and environmental control units as needed.

PLMN Subnetwork

A cdma2000 public land mobile network (PLMN) (refer back to Figure 3–5) provides mobile wireless communication services to subscribers and typically consists of several functional subnetworks. These subnetworks are known as the circuit core network (CCN), the packet core network (PCN), the service node network (SNN), and the CDMA radio access network (C-RAN). The cdma2000 PLMN subscriber has access to the PSTN and the PDN through these subnetworks. The organization of the PLMN into subnetworks facilitates the management of the system.

Circuit Core Network

The circuit core network (CCN) provides the switching functions necessary to complete calls to and from the mobile subscriber to the PSTN. The major network element in the CCN is the MSC. This portion of the

system is primarily concerned with the completion of voice calls between the subscriber and the PSTN. The MSC is basically an extension of the PSTN that services the various cells and the associated radio base stations within the cells. The MSC provides circuit switching and provides features such as call charging, subscriber roaming support, and maintenance of subscriber databases.

CDMA Radio Access Network

In cdma2000, the CDMA radio access network or **C-RAN** provides the interface between the wireless cellular subscriber and what is known as the circuit core network (CCN). The CCN consists of the MSC and other system components involved with connections to the PSTN for all circuit-switched voice and data calls. The C-RAN can consist of multiple base station subsystems (BSSs) and some form of radio network manager (RNM) system. The RNM system provides operation and management (O&M) support for multiple BSSs.

Packet Core Network

In cdma2000, the **packet core network** (PCN) provides a standard interface for wireless packet-switched data service between the C-RAN and the public data network (PDN). The PCN provides the necessary links to various IP networks to and from the C-RAN. The PCN typically consists of three main hardware nodes: the authentication, authorization, and accounting (AAA) server, the home agent (HA), and the packet data serving node (PDSN). Figure 6–8 depicts the elements of the PCN and their interconnection to each other and the relationship of the PCN to the PDN and the C-RAN.

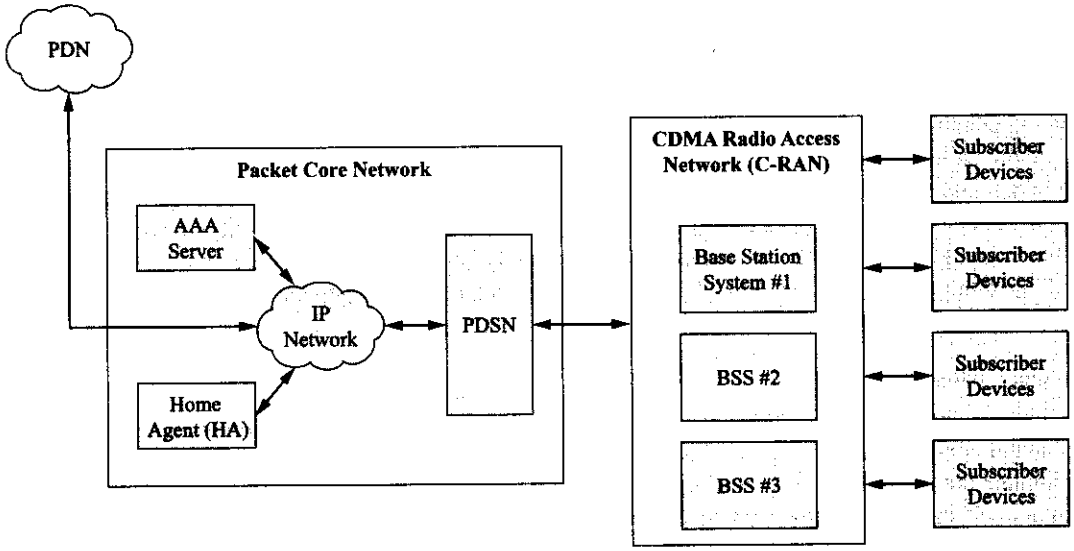


Figure 6–8 Elements of the cdma2000 packet core network (Courtesy of Ericsson).

In a cdma2000 cellular system, the packet data serving node (PDSN) provides the needed IP transport capability to connect the C-RAN and hence the subscriber to the public data network. The PDSN connects to the C-RAN through the A_{quater} interface (also known as the radio-packet (R-P) interface). The PDSN also interfaces the C-RAN with the home agent and the authentication, authorization, and accounting nodes. In such a capacity, it sets up, maintains, and terminates secure communications with the home agent and the authentication, authorization, and accounting nodes. It further serves as a point of connection to the radio network and the IP network and provides IP service management to offered IP traffic. Finally, to facilitate wireless mobile IP functionality, it also serves as a foreign agent to register network visitors (this topic will be discussed in more detail shortly).

The authentication, authorization, and accounting **(AAA) server** both authenticates and authorizes the subscriber device to employ the available network services and applications. To facilitate this operation, the AAA server manages a database that contains user profiles. The user profile information will also include information about quality of service (QoS) for the PDSN. The AAA server receives accounting information from the PDSN node that together with session information can be used for billing of the subscriber. An AAA server may be configured primarily for billing purposes. If that is the case, the PDSN may send accounting information to the billing AAA server and use a different AAA server for authentication and authorization.

In the cdma2000 system, the **home agent** (HA) has the task of forwarding all packets that are destined for the subscriber device (SD) to the PDSN over an IP network. The PDSN then sends the packets to the SD via the C-RAN and the common air interface. To be able to perform this operation the HA in conjunction with the PDSN authenticates mobile IP registrations from the mobile subscriber, performs SD registration, maintains current location information for the SD, and performs the necessary packet tunneling. Packet tunneling refers to the following operation: IP packets destined for a particular SD's permanent address are rerouted to the SD's temporary address. If the SD is registered in a foreign network (i.e., not its home network), then the SD has been assigned a temporary dynamic IP address by the **foreign agent** (this functionality is provided by the foreign network PDSN) and this temporary address is sent to the HA.

A relatively recent addition to the elements of the PCN is a wireless LAN serving node (WSN). This node provides IP transport capability and connectivity between the wireless network and wireless LAN-enabled subscriber devices through wireless LAN access points (APs). More will be said about this topic in a later chapter.

Network Management System

Modern wireless cellular systems employ sophisticated network management systems to oversee the operation of an entire network. Most service providers have one or several network operations centers or NOCs that serve as control points for nationwide cellular networks. AT&T has a NOC that oversees its entire U.S. wireless cellular network located in the Seattle, Washington, area. A typical network management system consists of several layers of management that deal with various levels of the network infrastructure. At the highest level is usually a network management system, then there is usually a subnetwork management system, and then at the lowest level a network element management system. A brief overview of each of these management systems will be given next.

Network Management

The highest level of network management gives an overarching view of the entire network including all of the subnetworks that it comprises. This computer-based system usually provides a platform that allows one to monitor the overall network. The system typically provides integrated graphical views of the complete network and modular software applications that may be used to support the operation and maintenance of the entire network, and it further provides the means by which operators are able to assess the quality of network service and to provide corrective action when network problems occur.

There are basically five functions that a wireless network management system will perform: network surveillance or fault management, performance management, trouble management, configuration management, and security management. Fault management is concerned with the detection, isolation, and repair of network problems to prevent network faults from causing unacceptable network degradation or downtime. Using the tools provided by the system, a human operator can attempt to repair the problem from the NOC. Performance management functions are concerned with the gathering and reporting of relevant network performance statistics that can be used to continuously analyze network operation. Trouble management functions allow for the display and subsequent description of occurrences that have affected the network and also provide the operator with the ability to communicate this information to other persons involved

with the maintenance of the network. If the operator at the NOC is unable to clear a trouble or a fault and depending upon the type of problem, it must be escalated and communicated to someone in the field who will now have the responsibility of dealing with it. Configuration management functions are used to support the administration and configuration of the network. These functions support the installation of new network elements as well as the interconnection of network nodes. Finally, security management functions manage user accounts and provide the ability to control and set user-based access levels.

Subnetwork Management and Element Management

Subnetwork management platforms provide management of the circuit, packet, and radio networks that compose the typical CDMA system. The circuit core network management system is mainly concerned with the CDMA mobile-services switching center. It provides fault, performance, configuration, software, and hardware management functions that support the operation of this particular network element at the subnetwork level. The computer system used for this function provides an operator with access to one or more MSCs for the performance of the various functions listed earlier. The packet core network management system is concerned with the PCN node of the CDMA system. Besides the standard functions of fault and performance management, the PCN management platform can perform statistics administration, online documentation, backup and restore functions, and maintain dynamic network topology maps and databases for the PCN nodes. The CDMA radio access network (C-RAN) management system is concerned with CDMA base station subsystems. It provides the ability to configure the radio and network parameters of the system BSSs, monitor C-RAN alarms and performance, and install or upgrade software to any network element in the C-RAN. Additionally, it provides the capability to manage user security and the ability to back up and restore the configuration of any C-RAN element.

Element management refers to the ability to interface directly with a network element through a "craft" data port. Using element specific software, a technician on-site with a laptop computer or off-site through a remote connection is able to interface directly with the specific network element. This type of software-driven element management is usually performed at a cell site during the initial deployment, installation, and testing of a radio base station and during any necessary diagnostic testing and troubleshooting if an escalated alarm or hardware trouble develops with the system.

System Communication Links

Today, equipment vendors are still using legacy channelized T1/E1/J1 copper pairs for connectivity from the MSC to the PSTN. Recently, however, CDMA equipment vendors have started to add fiber-optic interfaces to deliver SONET signals at data rates of 155.52 mbps as shown by Figure 6–9. Channelized T1/E1/J1 with control information is used over the A interface between the MSC and the BSC. Between the BSC and the RBSs unchannelized T1/E1/J1 is used. Between the MSC and the various network elements such as HLR, AC, and so on, signaling protocol TIA/EIA-41-D is used over T1/E1/J1 timeslots. T1/E1/J1 is used to transport data between the nodes and the MSC. Data between the service nodes and the PDN is typically carried by Ethernet at 10/100 mbps. Between the BSC to the PCN, fiber-optic signals at 155.52 mbps are converted to Ethernet at 10/100 mbps. Lastly, from PCN to PDN, data is carried by Ethernet at 10/100 mbps rates.

Recently, most wireless equipment vendors are offering integrated network solutions to service providers by providing microwave links capable of T1/E1/J1 transport or higher data rates for backhaul of aggregated signals to the PSTN. Several vendors offer high-capacity microwave radio systems that offer OC3/STM-1 data rates with the ability to transport asynchronous transfer mode (ATM) traffic. As service providers upgrade their systems to offer 3G CDMA services with high-data-rate access, the C-RAN will need to be interconnected and serviced by data transport technologies that offer higher data rates than T-carrier transport technology. At this point, it appears that ATM has been selected to be the data transport technology around which the next generation of radio access networks for 3G CDMA systems will be designed.

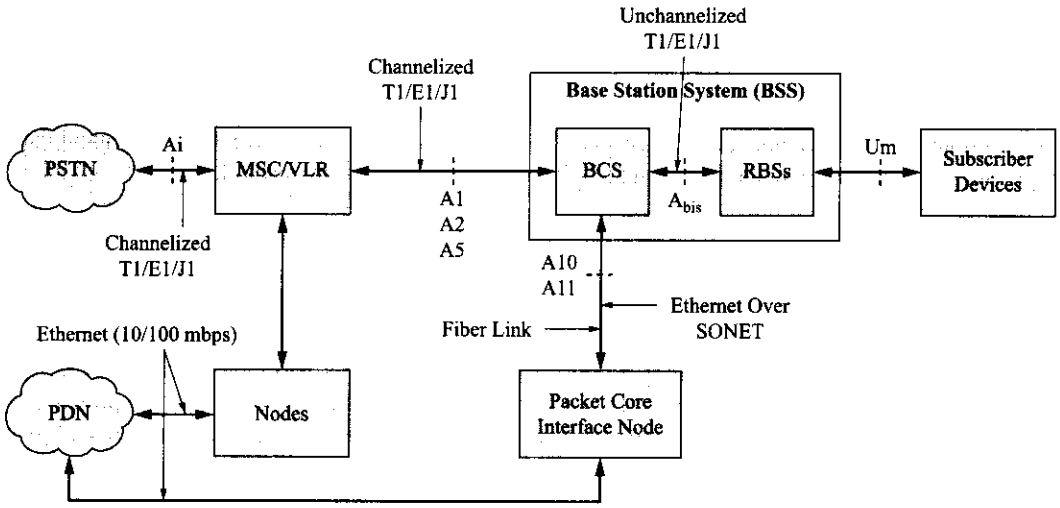


Figure 6–9 Network interfaces for CDMA systems (Courtesy of Ericsson).

Subscriber Devices

Subscriber device (SD) is a generic term used to describe several types of wireless phones and data devices that perform CDMA encoding/ decoding and vocoding operations for the transmission of voice or data in a wireless mobile environment. Each subscriber device has a band or set of radio bands over which it can operate and various modes of possible operation. Subscriber devices can be divided into two broad groups or categories depending upon their applications. Portable devices can operate in the cellular, PCS, or in both bands and can handle the transmission of voice, data, and other nonvoice applications. Typically, these types of SDs are used by people for mobile voice connectivity first, with the other data capabilities being of secondary importance. Wireless local loop (WLL) devices can handle the transmission of data over the CDMA system and typically are used with a laptop or personal digital assistant (PDA) type of device for high-speed Internet access. In the near future, the latter type of SD will probably be used to provide Voice over IP (VoIP) capabilities that will allow wireless video conferencing over either a laptop or tablet PC. In the coming years, the typical SD will include additional functionality for multimedia applications and the ability to use any additional frequency bands that might support CDMA services.

PART II CDMA BASICS

6.3 CDMA CHANNEL CONCEPT

As mentioned in previous chapters, cellular telephone networks use various control and traffic channels to carry out the operations necessary to allow for the setup of a subscriber radio link for the transmission of either data or a voice conversation and the subsequent system support for the subscriber's mobility. The cdmaOne and cdma2000 cellular systems are based on the use of code division multiple access (CDMA) technology to provide additional user capacity over a limited amount of radio frequency spectrum. This feat is accomplished by using a spread spectrum encoding technique that provides for numerous radio channels that all occupy the same frequency spectrum. To enable these distinct but same frequency channels, orthogonal Walsh spreading codes are used for channel encoding. Several of these encoded channels are used specifically within the CDMA system to provide precise system timing, control, and overhead information while other channels are used to carry user traffic.

This text will not attempt to derive the values or properties of these **Walsh codes** but only describe the basic structure of the 64-bit codes and their usage in IS-95 CDMA systems. To that end, each Walsh code consists of a binary combination of sixty-four 0s and 1s, and all the codes except one (the all-0s Walsh code—W_0^{64}) have an equal number of 0s and 1s. Suffice to say that the sixty-four Walsh codes used in the IS-95 CDMA systems have the unique quality of being orthogonal to one another. As stated earlier, this principle is exploited to create sixty-four distinct communications channels that can all exist in the same frequency spectrum. Also, as mentioned before, all other Walsh encoded signals will appear as broadband noise to the CDMA receiver except for the unique signal that was created with the same Walsh code as the one the receiver uses for demodulation. Figure 6–10 shows the basic principle behind the use of an 8-bit Walsh orthogonal spreading code to create a distinct signal. Note how the use of the spreading code increases the number of bits sent in the same time interval as the original digital signal and hence increases the overall signal bandwidth.

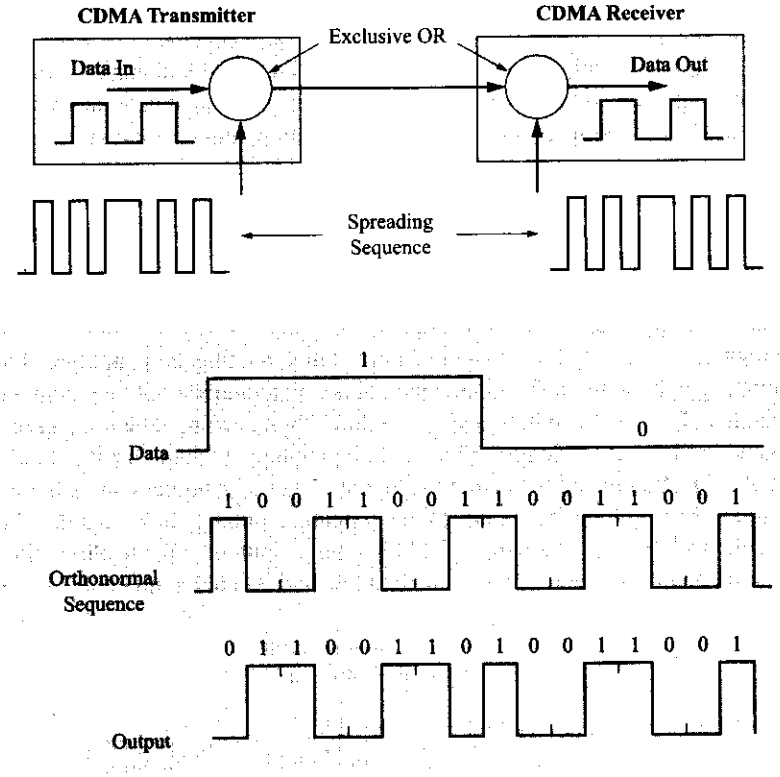


Figure 6–10 The basic spectrum spreading operation.

It should be pointed out right away that the forward channels in a CDMA system are encoded differently than the reverse channels. The different encoding schemes will be explained in more detail in the following sections about the forward and reverse CDMA logical channels.

Additionally, two types of pseudorandom noise (PN) codes are used by the IS-95 CDMA system. These two types of PN code sequences are known as short and long PN codes. The short PN code is time shifted both to identify the particular CDMA base station and to provide time synchronization signals to the subscriber device so that it can become time synchronized with the radio base station. The long PN code is used to provide data scrambling on the forward traffic channels and for providing a means by which reverse link channels may be distinguished. These concepts will be explored further in the next few sections.

In summary, for an IS-95 CDMA cellular system, a single radio base station may consist of up to sixty-four separate channel elements (CEs) that all use the same carrier frequency or portion of the radio frequency spectrum. Each of the base station's modulated signals effectively becomes a separate channel when the digital signal to be transmitted is encoded with a distinct Walsh code. Several of the Walsh codes are reserved for use with particular forward channels that serve various logical system functions as will be presented next. At this time, only the basic IS-95 CDMA system will be discussed. Later, the modifications and improvements incorporated into IS-95B and then into cdma2000 will be discussed. Chapter 8 will present more detail about the actual hardware used to implement a CDMA system.

Forward Logical Channels

The IS-95 CDMA forward channels exist between the CDMA base station and the subscriber devices. The first CDMA systems used the same frequency spectrum as the AMPS and NA-TDMA systems. However, the IS-95 signal occupies a bandwidth of approximately 1.25 MHz whereas the AMPS and NA-TDMA system standards each specify a signal bandwidth of 30 kHz. Therefore, an IS-95 signal will occupy approximately the same bandwidth as forty-two AMPS or NA-TDMA channels. Although the bandwidth required for a CDMA signal is substantial, a cellular service provider is able to overlay an IS-95 CDMA system with enhanced data capabilities onto an earlier-generation cellular system.

The basic spreading procedure used on the forward CDMA channels is illustrated by Figure 6–11. As shown in Figure 6–11, the digital signal to be transmitted over a particular forward channel is spread by first Exclusive-OR'ing it with a particular Walsh code (W_i^{64}). Then the signal is further scrambled in the in-phase (I) and quadrature phase (Q) lines by two different short PN spreading codes. These short PN spreading codes are not orthogonal codes; however, they have excellent cross-correlation and auto-correlation properties that make them useful for this application. Additionally, it seems that all Walsh codes are not created equal when it comes to the amount of spectrum spreading they produce. Therefore, the use of the short PN spreading code assures that each channel is spread sufficiently over the entire bandwidth of the 1.25-MHz channel. The short in-phase and quadrature PN spreading codes are generated by two linear feedback shift registers (LFSRs) of length 15 with a set polynomial value used to configure the feedback paths of each of the LFSRs (for additional information about this process see the present CDMA standards). The resulting short PN spreading codes are repeating binary sequences that have approximately equal numbers of 0s and 1s and a length of 32,768. The outputs of the in-phase and quadrature phase signals are passed through baseband filters and then applied to an RF quadrature modulator integrated

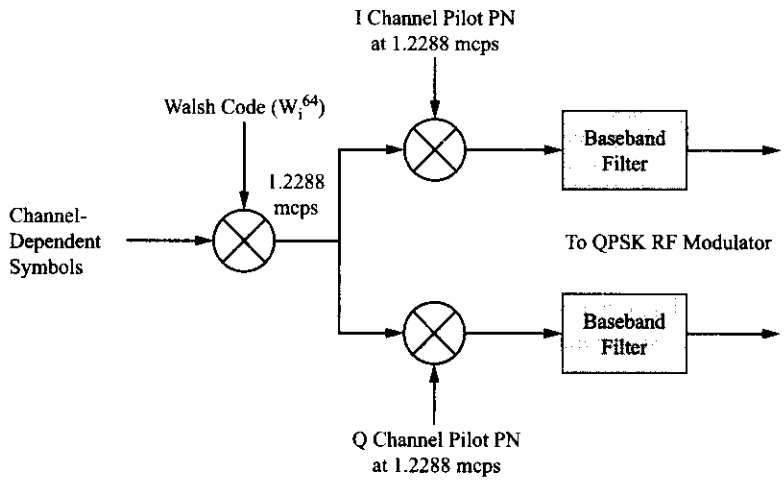


Figure 6–11 Basic spreading procedure used on CDMA forward channels.

circuit (IC) that upconverts the final output signal to the UHF frequency bands. This channel element signal is linearly combined with other forward channel element signals, amplified, and the composite passband signal is transmitted over the air interface.

The short PN spreading codes provide the CDMA system with the ability to differentiate between different base stations (or cells) transmitting on the same frequency. The same short PN code sequence is used by all CDMA base stations; however, for each base station the PN sequence is offset from the sequences used by other area base stations. The offset is in 64-bit increments, hence there are 512 possible offsets. In a scheme analogous to the frequency reuse plans described for other access techniques in Chapter 4, the same offset may be reused at a great enough distance away from its first use. Figure 6–12 shows but one example of this reuse method. The use of this offset scheme requires that the base stations used in a CDMA system must all be time synchronized on the downlink radio channels. This precise timing synchronization is achieved through the use of the Global Positioning System (GPS) to achieve a system time that has the required accuracy.

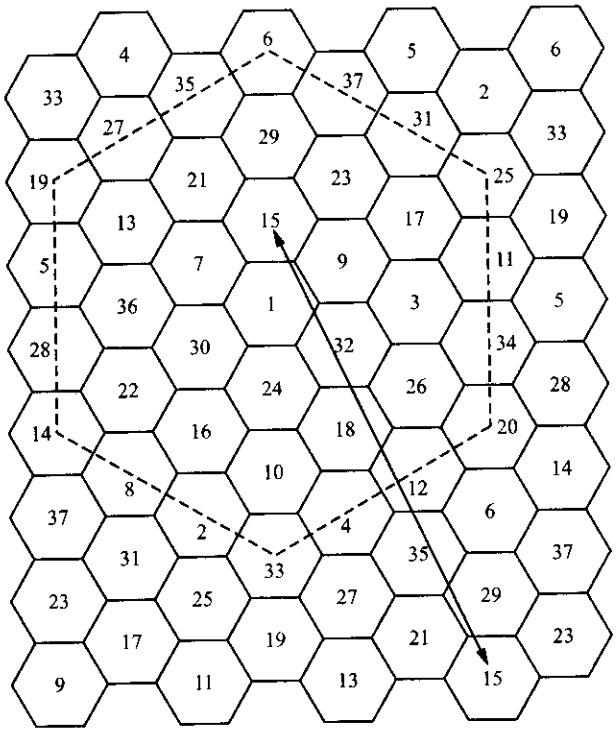


Figure 6–12 CDMA base station timing offset reuse pattern.

The initial IS-95 CDMA system implementation uses four different types of logical channels in the forward direction: the pilot channel, synchronization channel, paging channels, and traffic/power control channels. Each one of these types of forward channels will be discussed in more detail in the following sections.

Pilot Channel

The CDMA pilot channel is used to provide a reference signal for all the SDs within a cell. Figure 6–13 depicts the generation of the pilot channel signal. The all-0s Walsh code (W_0^{64}) is used for the initial signal spreading on a sequence of all 0s. This results in a sequence of all zeros that are further spread using the short PN spreading sequences resulting in a sequence of 0s and 1s. The I and Q signals drive a quadrature

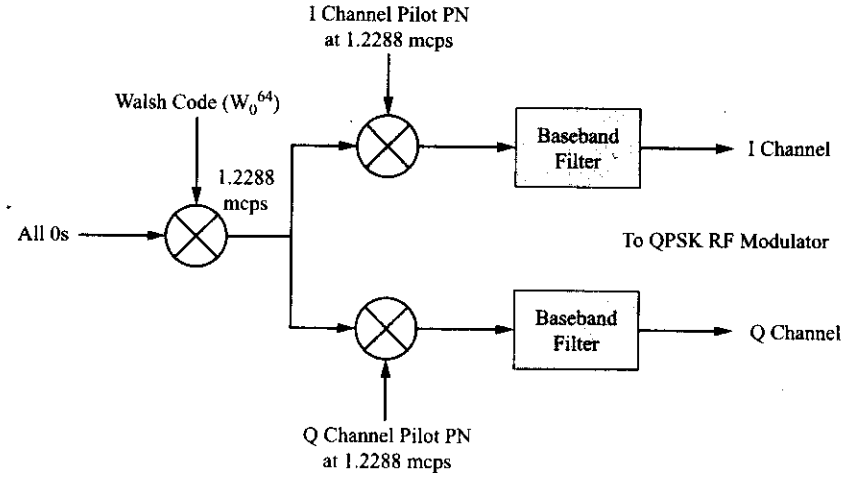


Figure 6–13 Generation of the CDMA pilot channel signal.

modulator. Therefore, the resulting pilot signal is an unmodulated spread spectrum signal. The short PN spreading code is used to identify the base station and the pilot signal is transmitted at a fixed output power usually 4–6 dB stronger than any other channel. The pilot channel, transmitted continuously, is used as a phase reference for the coherent demodulation of all other channels. It also serves as the reference for signal strength measurements and other signal power comparisons.

Synchronization Channel

The CDMA synchronization channel is used by the system to provide initial time synchronization. Figure 6–14 depicts the generation of the synchronization channel signal. In this case, Walsh code W_{32}^{64} (thirty-two 0s followed by thirty-two 1s) is used to spread the synchronization channel message. Again, the same short PN spreading code with the same offset is used to further spread the signal.

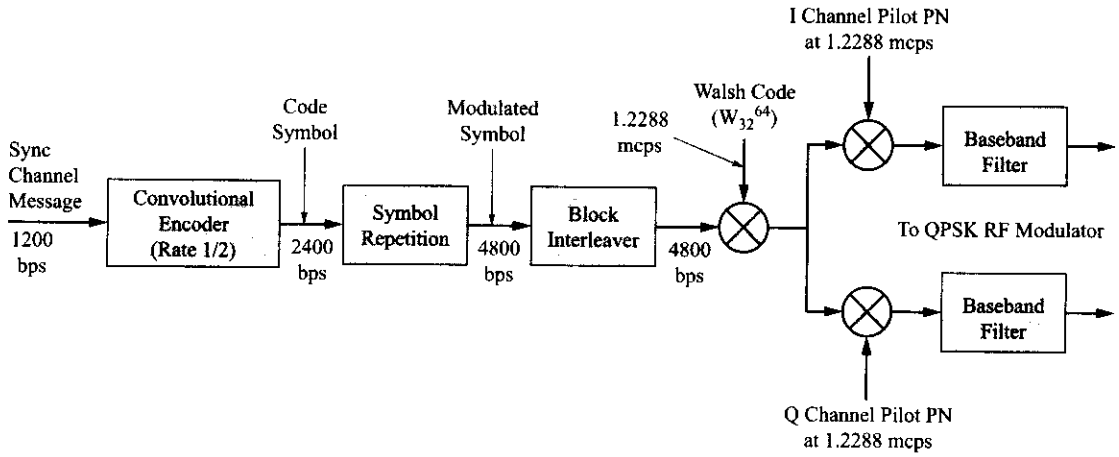


Figure 6–14 Generation of the CDMA synchronization channel signal.

As shown in Figure 6–15, the initial synchronization channel message has a data rate of 1200 bps. The sync messages undergo convolutional encoding, symbol repetition, and finally block interleaving (to be explained in Chapter 8). This process raises the final sync message data rate to 4.8 kbps. The information

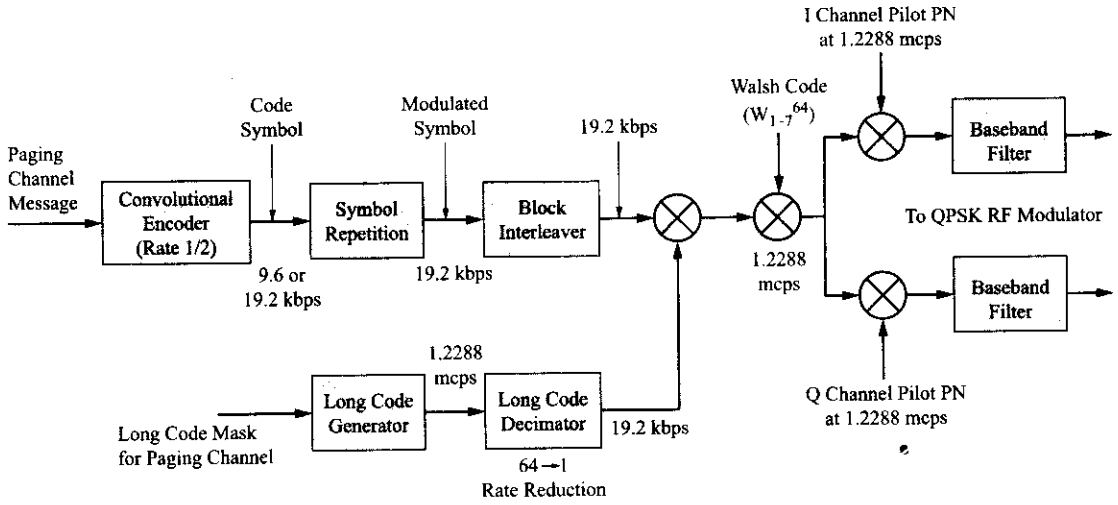


Figure 6–15 Generation of the CDMA paging channel signal.

contained in the sync message includes the system and network identification codes, identification of paging channel data rates, the offset value of the short PN spreading code, and the state of the long PN spreading code. Like the pilot channel, the synchronization channel has a fixed output power.

Paging Channels

The CDMA paging channels serve the same purpose as the paging channels in a GSM cellular system. These channels are used to page the SDs when there is a mobile-terminated call and to send control messages to the SDs when call setup is taking place. Figure 6–15 depicts the generation of a paging channel message.

For IS-95 CDMA there can be as many as seven paging channels in operation at any one time. Walsh codes W_1^{64} through W_7^{64} are used for this purpose. As seen in Figure 6–15, the paging channel undergoes an additional scrambling operation using the long PN spreading code sequence. The long PN code is generated by using a 42-bit linear feedback shift register that yields a repeating sequence of length 2^{42}. The paging channel message also goes through a convolutional encoding process, symbol repetition, and block interleaving before being scrambled by a slower version of the long PN code.

Traffic/Power Control Channels

The CDMA forward traffic channels carry the actual user information. This digitally encoded voice or data can be transmitted at several different data rates for IS-95 CDMA systems. Rate Set 1 (RS1) supports 9.6 kbps maximum and slower rates of 4.8, 2.4, and 1.2 kbps. Rate Set 2 (RS2) supports 14.4, 7.2, 3.6, and 1.8 kbps. Figure 6–16 and Figure 6–17 depict the generation of a forward traffic channel. As shown in Figure 6–17, for generation of Rate Set 2 traffic an additional operation is performed after the symbol repetition block. For a data rate of 14.4 kbps the output from the symbol repetition block will be 28.8 kbps. The "puncture" function block selects 4 bits out of every 6 offered and thus reduces the data rate to 19.2 kbps, which is what the block interleaver needs to see. More details about this operation will be presented in Chapter 8.

All of the CDMA system's unused Walsh codes may be used to generate forward traffic channels. The traffic channels are further scrambled with both the short PN sequence codes and the long PN sequence codes before transmission. As also shown in Figures 6–16 and 6–17, power control information is transmitted to the mobile stations within the cell over the traffic channels. This power control information is used to

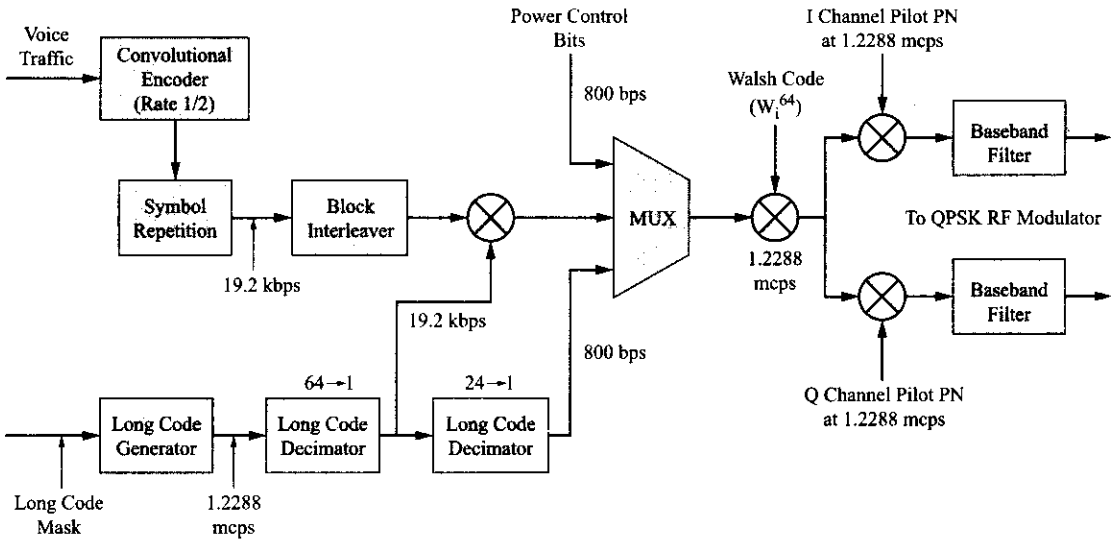


Figure 6–16 Generation of the CDMA forward traffic/power control channel for 9.6-kbps traffic.

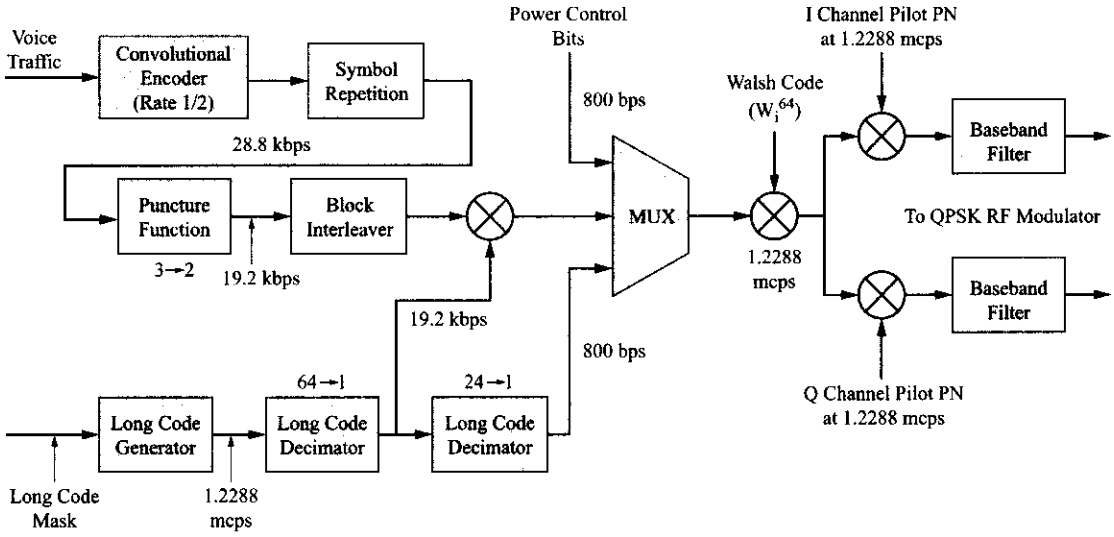


Figure 6–17 Generation of the CDMA forward traffic/power control channel for 14.4-kbps traffic.

set the output power of the mobile on the reverse link and is multiplexed with the scrambled voice bits at a rate of 800 bps or 1 bit every 1.25 msec.

Reverse Logical Channels

The IS-95 CDMA reverse logical channels exist between the subscriber devices and the CDMA base station. As mentioned previously, the encoding of digital information on the reverse channels is performed differently than on the forward channels. The data to be transmitted is not initially spread by a Walsh codes; instead, the data is mapped into Walsh codes that are then transmitted. Since there are sixty-four, 64-bit Walsh codes, every 6 bits of data to be transmitted may be mapped to a particular Walsh code. This technique yields an over tenfold increase in bandwidth since 64 bits are now transmitted for every 6 bits of

data; however, the system error rate is reduced in the process. The mapping of groups of 6 data bits to a Walsh code is very straightforward since there exists a one-to-one relationship between the two.

Each reverse channel is spread by a long PN sequence code and scrambled by the short PN sequence code. The long PN sequence code is derived from the subscriber device's 32-bit electronic serial number (ESN) and therefore provides the means by which the user is uniquely identified within the CDMA system. There are basically two types of reverse CDMA channels: access channels and reverse traffic/control channels. These logical channels will be further described in the next sections.

Access Channels

The CDMA access channels are used by the mobile to answer pages and to transmit control information for the purpose of call setup and tear down. Figure 6–18 shows the access channel processing for a IS-95 CDMA system. As shown in the figure, an access message at 4.8 kbps undergoes the familiar convolutional encoding, symbol repetition, and block interleaving that raises the data rate to 28.8 kbps. At this point, the orthogonal modulation subsystem processes the signal by encoding every 6 bits into a 64-bit Walsh code. This process raises the signal rate to 307.2 kcps. The reader should note the use at this time of chips per second (cps) instead of bits per second. This is standard notation within the CDMA industry when referring to the signal spreading process. Next, the long PN code spreads the signal by a factor of 4 that yields a chip rate of 1.2288 mcps. The signal is further scrambled by the short PN sequence codes. The long PN code is used by the system to differentiate the thirty-two possible access channels.

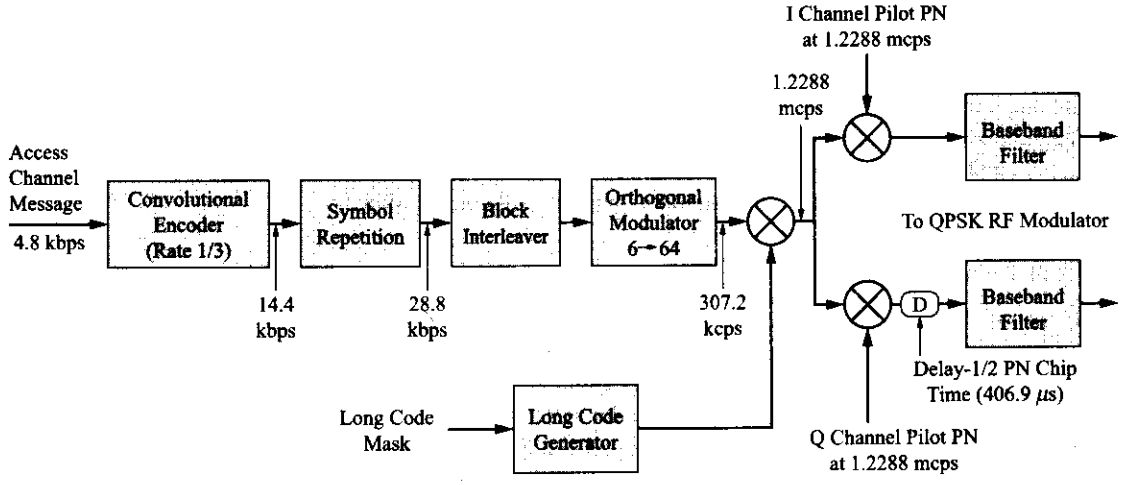


Figure 6–18 Generation of the CDMA reverse access channel.

At this point, the CDMA signal is applied to an RF quadrature modulator subsystem or IC. However, for the reverse channels, the form of modulation used to produce the final UHF passband signal is slightly different than for the forward channels. In this case, offset QPSK (OQPSK) is used instead of straight QPSK as in the case of the forward channels. Note the delay block of one-half of a PN chip (406.9 ns) used in the Q path to implement the OQPSK modulation. This form of modulation allows for a more power efficient and linear implementation by the subscriber device's RF electronics. As noted previously, any type of power savings technique that can lengthen battery life is usually employed when designing a mobile subscriber device.

Traffic/Power Control Channels

The IS-95 CDMA reverse traffic/power control channels support both voice and data at the two rate sets (RS1 and RS2) previously introduced. Figure 6–19 depicts the generation of a reverse traffic channel. In

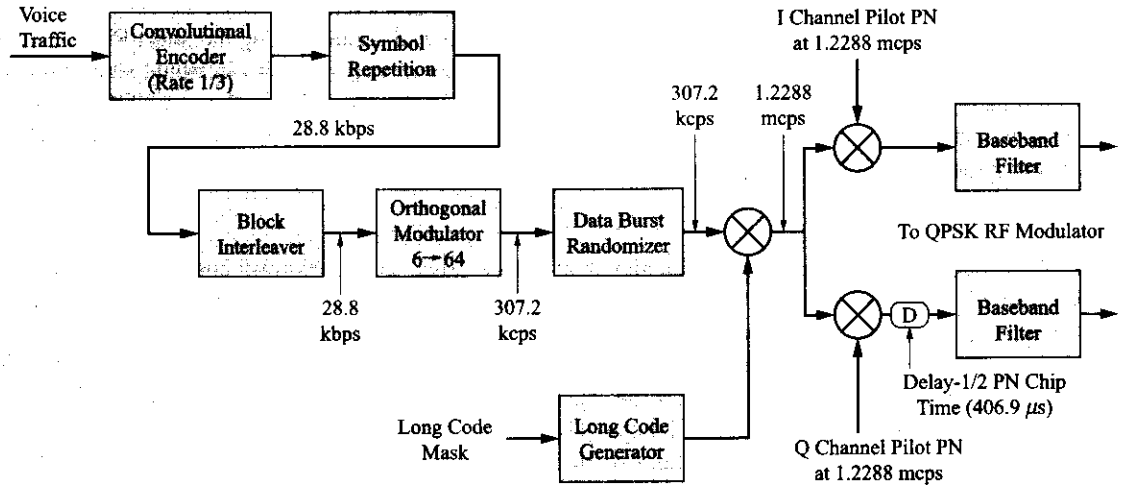


Figure 6–19 Generation of the CDMA reverse traffic channel.

either rate set case, the data rate at the input to the orthogonal modulator subsystem will be 28.8 kbps. At the output of this process the signal rate is 307.2 kcps. At this point the signal is processed by a data burst randomizer that in essence is used to eliminate redundant data. The signal is then spread by a long PN sequence code and further scrambled by the short PN sequence code. The final signal rate is the standard 1.2288 mcps with a signal bandwidth of approximately 1.25 MHz.

The reverse traffic channel is also used to send information to the base station controller about pilot channel signal strength, control information regarding handoff operations, and ongoing frame error rate (FER) statistics. More detail about these topics will be forthcoming shortly.

CDMA Frame Format

Now that the logical CDMA channels in the forward and reverse direction have been introduced, it is time to examine the format of a basic CDMA frame and its role in the operation of the system. Similar to GSM system operation, CDMA systems take 20-ms segments of digital samples of a voice signal and encode them through the use of a speech coder (vocoder) into variable rate frames. Thus the basic system frame size is 20 ms. The first IS-95 systems employed the 8-kbps Qualcomm-coded excited linear prediction (QCELP) speech coder that produced 20-ms frame outputs of either 9600, 4800, 2400, or 1200 bps (Rate Set 1), with the addition of overhead (error detection) bits. The actual net bit rates are 8.6, 4.0, 2.0, or 0.8 kbps. A second encoder, the 13-kbps QCELP13 encoder, was introduced in 1995 and produced outputs of 14.4, 7.2, 3.6, and 1.8 kbps (Rate Set 2), with a net maximum bit rate of 13.35 kbps. In each case, the speech encoder makes use of pauses and gaps in the user's speech to reduce its output from a nominal 9.6 or 14.4 kbps to lower bit rates and 1.2 or 1.8 kbps during periods of silence.

The basic 20-ms speech encoder frame size is used in various configurations by several of the logical channels to facilitate CDMA system operation, increase system capacity, and improve mobile battery life. The next several sections will detail these operations.

Forward Channel Frame Formats

Of the four forward logical channels, only the pilot channel does not employ a frame format. It consists of a continuous transmission of the system RF signal (refer back to Figure 6–14). The forward traffic channel frames are 20 ms in duration and contain a varying number of information bits, frame error control check

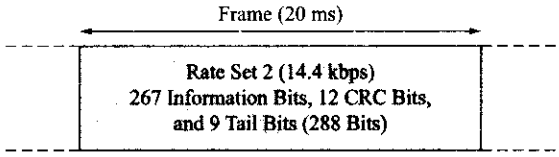


Figure 6–20 Rate Set 2 traffic channel structure.

bits, and tail bits depending upon the rate set and the data rate. Figure 6–20 depicts a forward traffic frame for Rate Set 2 at 14.4 kbps. The forward traffic channel frames are further logically subdivided into sixteen 1.25-ms power control groups. Power control bits transmitted over the forward traffic channels are randomly inserted into the data stream of each 1.25-ms power control group yielding a power control signal rate of 800 bps. More detail about the power control operation will be forthcoming later in this chapter.

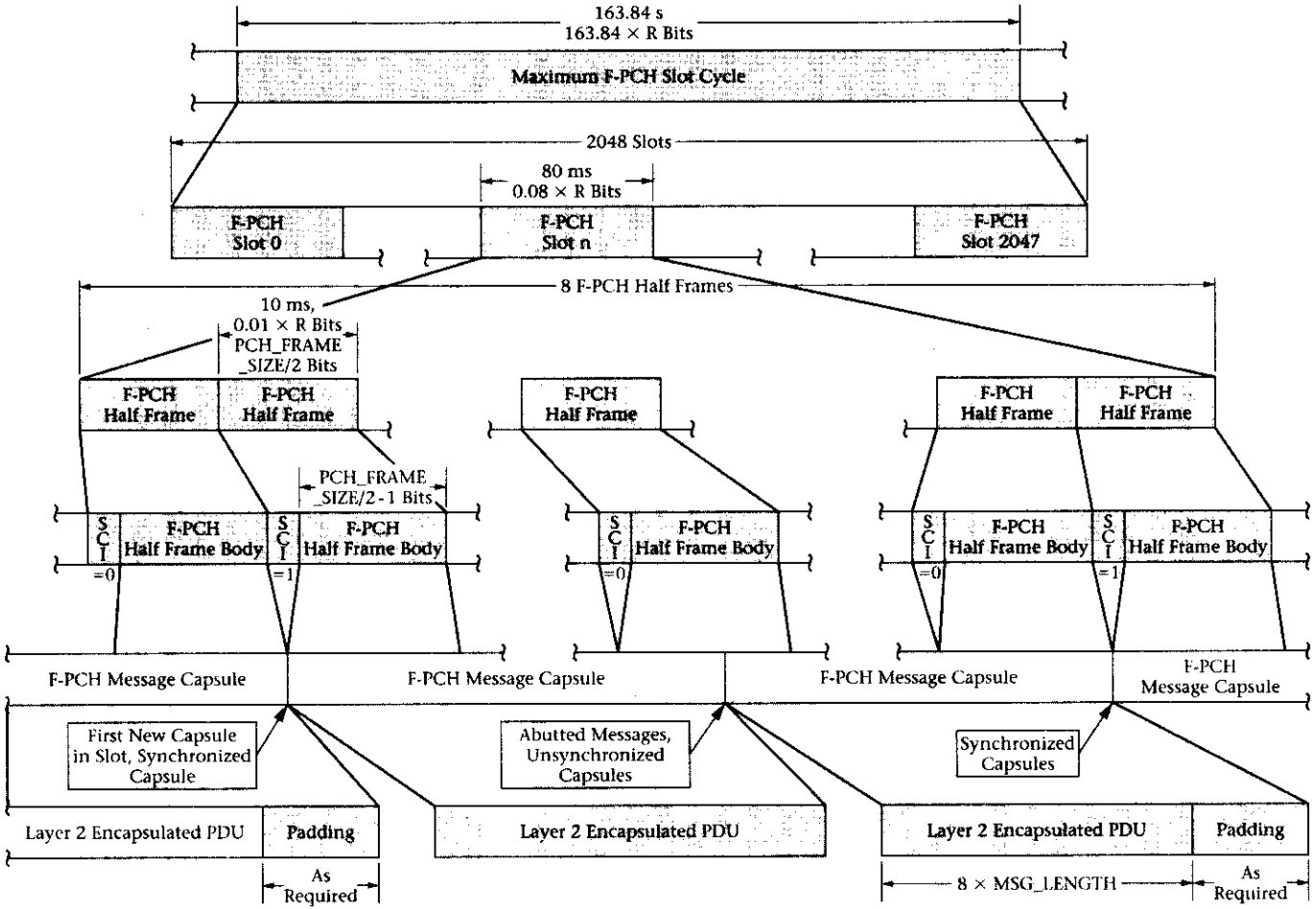
The CDMA forward synchronization (sync) channel provides the mobile or subscriber device with system configuration and timing information. A sync channel message can be long and therefore the message is typically broken up into sync channel frames of 32 bits each. The sync channel frame consists of a start of message (SOM) bit and 31 data bits. The start of a sync message is indicated by a SOM bit set to 1 in the first frame and 0 in subsequent frames of the same message. At a data rate of 1200 bps, a sync channel frame is $26.66\bar{6}$ ms in duration (the same repetition period employed by the short PN codes). Three sync channel frames of 96 bits form a sync channel superframe of 80-ms duration (equal to four basic 20-ms frames). The sync message itself consists of a field that indicates the message length in bits, the message data bits, error checking code bits, and additional padding bits (zeros) as needed.

The forward paging channels are used by the CDMA base station to transmit system overhead information and mobile station-specific messages. In IS-95A, the paging channel data rate can be either 4800 or 9600 bps. The paging channel is formatted into 80-ms paging slots of eight half frames of 10-ms duration. Each half frame starts with a synchronized capsule indicator (SCI) bit that is functionally similar to the SOM bit. A synchronized paging channel message capsule begins immediately after an SCI bit set to 1. To accommodate varying-length paging messages and to prevent inefficient operation of the paging channel, additional message capsules may be appended to the end of the first message capsule if space is available within the half frame or subsequent half frames. A paging message must be contained in at most two successive slots.

Furthermore, the paging channel structure is formatted into paging slot cycles to provide for increased mobile station battery life. A CDMA mobile may operate in either a slotted or unslotted mode. In the unslotted mode the mobile reads all the page slots while in the *mobile station idle state*. In the slotted mode, the mobile wakes up periodically to check for paging messages directed to it in specific preassigned slots (again, in the *mobile station idle state*). Therefore, slotted mode operation permits the mobile station to power down energy-consumptive RF electronic circuitry until its specific paging slot arrives. The mobile station will wake up for one or two paging slots (if required) of the paging slot cycle. The length of the paging cycle can vary from a minimum of sixteen slots (1.28 s) to a maximum of 2048 slots (163.84 s) (see Figure 6–21 for a diagram of the paging channel structure) as established by the system. Typically, minimal length cycles are employed; otherwise, significant delays in call termination could result. The CDMA system uses the mobile station's ESN to determine the correct slot to use for paging of the mobile. Further power savings are realized while in slotted mode by the transmission of a _DONE message by the base station after the end of the paging message scheduled for the particular mobile. In the case of a short message that uses only several half frames of a slot, the mobile can power down before the end of the slot to save even more battery power.

Reverse Channel Frame Formats

The reverse traffic channel, like the forward traffic channel, is also divided into 20-ms traffic channel frames. The reverse traffic channel frame is also further logically subdivided into sixteen 1.25-ms power



R = F-PCH Data Rate (9600 bps or 4800 bps)
PCH_FRAME_SIZE = Number of Information Bits in an F-PCH Frame

Note 1: See IS-2000-5 for Maximum Length Limitations.

Figure 6–21 CDMA Paging channel structure (from 3GPP2).

control groups. As was the case for the forward traffic channel, variable rate data are also sent on the reverse traffic channel. The coded bits from the convolutional encoder used in the reverse traffic channel are repeated before interleaving when the speech characteristics are such that the encoded data rate is less than the maximum. When the mobile transmit data rate is maximum, all sixteen power control groups are transmitted. If the transmitted data rate is one half of the maximum rate, then only eight power control groups are transmitted. Similarly, for a transmitted data rate of one-quarter or one-eighth, only four or two power control groups are transmitted per frame, respectively. As mentioned, this process, termed *burst transmission*, is made possible by the fact that reduced data rates have built-in redundancy that has been generated by the code repetition process. A data burst randomizer ensures that every repeated code symbol is only transmitted one time and that the transmitter is turned off at other times. This process reduces interference to other mobile stations operating on the same reverse CDMA channel by lowering the average transmitting power of the mobile and hence the overall background noise floor. The data burst randomizer generates a random masking pattern for the gating pattern that is tied to the mobile station's ESN. Figure 6–22 shows this process in more detail.

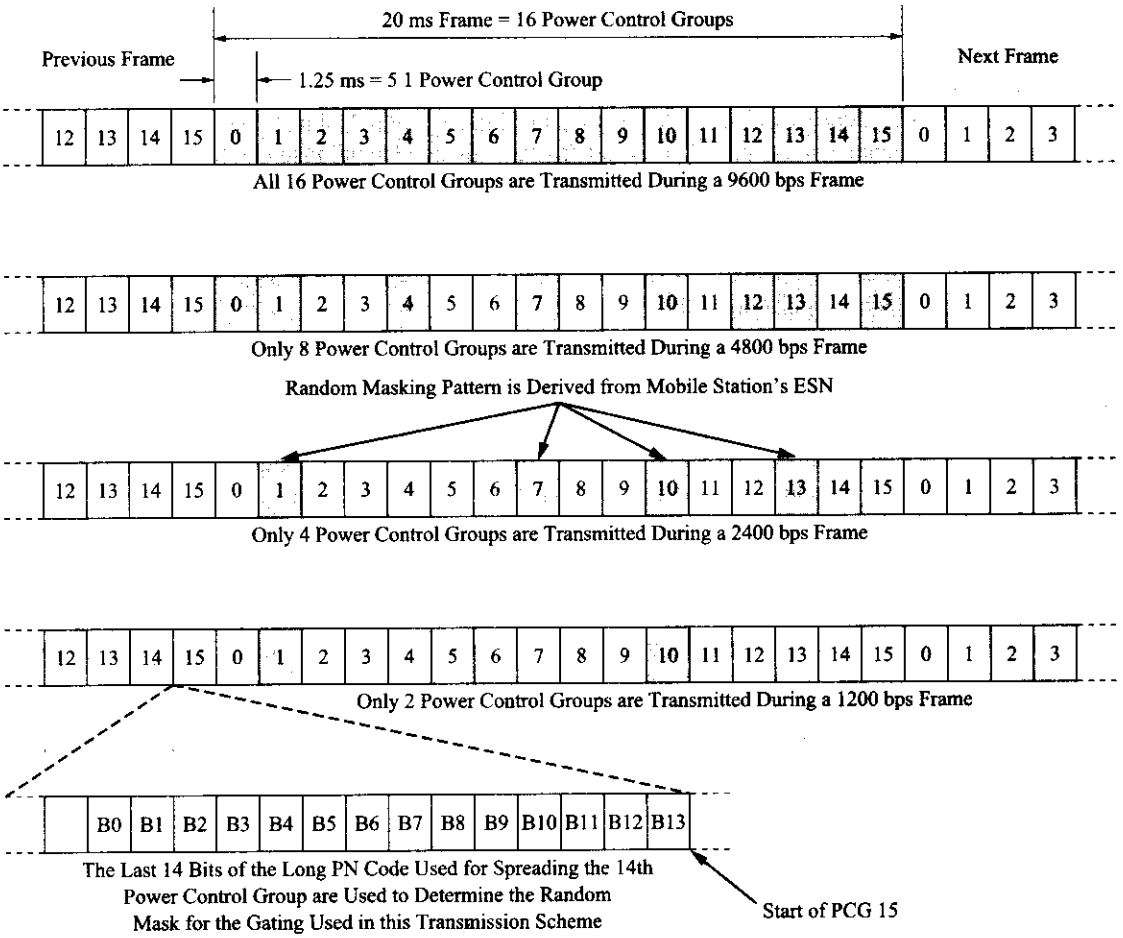


Figure 6–22 CDMA reverse channel variable data rate transmission.

The reverse access channel is used by the mobile station to communicate with the base station. The access channel is used for short message exchanges, such as responses to commands from the base station, for system registrations, and for call origination requests. The access channel data rate is 4.8 kbps using a

20-ms frame that contains 96 information bits. Each access channel message is typically composed of several access channel frames.

Since multiple mobile stations associated with the same paging channel may try to simultaneously access the same access channel, a random access protocol has been developed to avoid signal/data collisions. This topic will be discussed further in the next section about CDMA System Operations.

6.4 CDMA SYSTEM (LAYER 3) OPERATIONS

The reader has already been introduced to the typical generic wireless network operations of call setup, location updating, and handoff in Chapters 2–4 in the context of the common tasks and operations performed by the various elements of a wireless cellular network. Chapter 5 provided additional details of these traffic cases for the GSM cellular system. The purpose of this section is to present the reader further details about how these operations are handled within the CDMA system. Since there is substantial commonality between the GSM and CDMA systems for operations that support a subscriber's connectivity and mobility and since a great deal of detail was presented about GSM, the emphasis of this section will be on the differences between the two systems. It should be noted that the use of spread spectrum technology to implement CDMA cellular gives it certain advantages over the GSM TDMA system and thus the use of CDMA technology drives some of these differences. Some of these advantages are better immunity to interference and multipath propagation, a frequency reuse factor of $N = 1$, the ability to perform soft handoffs, and extremely precise power control. This last feature is important because it affords increased battery life since the mobile is always operated at the minimum output power needed for satisfactory system performance. Unfortunately, due to the extremely complex nature of the actual implementation details of today's CDMA technology-based cellular and PCS systems, these operations can not be covered in anything other than general terms in a textbook of this nature. As has been stated before, the modern cell phone is an extremely complex telecommunications device with an amazing amount of embedded processing power. In all cases, the details presented about CDMA system operations in this book will attempt to give the reader an accurate sense of how the operations are accomplished.

A word about the type of documentation used to describe cellular system's Layer 3 operations is appropriate at this time. Due to the inherent complexity of cellular system operations and the multitude of possible operational states and steps involved in the processes required to achieve certain system outcomes, most system states are documented in flowchart form within the particular standards pertaining to the technology used. These flowcharts indicate the possible steps involved in the performance of various system operations or traffic cases and are usually grouped by being performed by either the mobile or base station. An example of this concept would be the state of a mobile station. When the mobile is active it might be in the initialization, idle, access, or traffic state. These states will be illustrated and explained within the standard through the use of a flowchart that would show all the possible actions (states) that could result during the performance of a particular function.

As was the case for GSM, the reader should refer to the most up-to-date CDMA standards (see www.3gpp2.org) for information about all of the possible CDMA system operations and traffic cases. Again, more detail about CDMA data calls and the various message services will be provided in Chapter 7.

Initialization/Registration

As is the case with GSM cellular, CDMA system registration procedures are dependent upon the status of the mobile station. The mobile may be either in a detached condition (powered off or out of system range) or in an attached condition. When first turned on, the mobile goes through a power-up state (see Figure 6–23) during which it selects a CDMA system and then acquires the pilot and sync channels, which allows it to synchronize its timing to the CDMA system. When attached, the mobile may be in one of three states: the mobile station idle state, the system access state, or the mobile station control on the traffic channel state (see Figure 6–24).

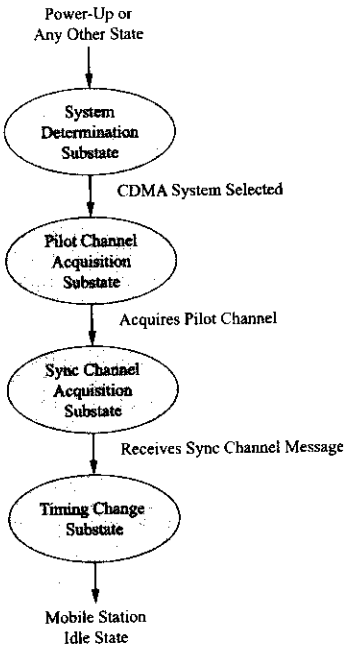


Figure 6–23 CDMA mobile station initialization state (Courtesy of 3GPP2).

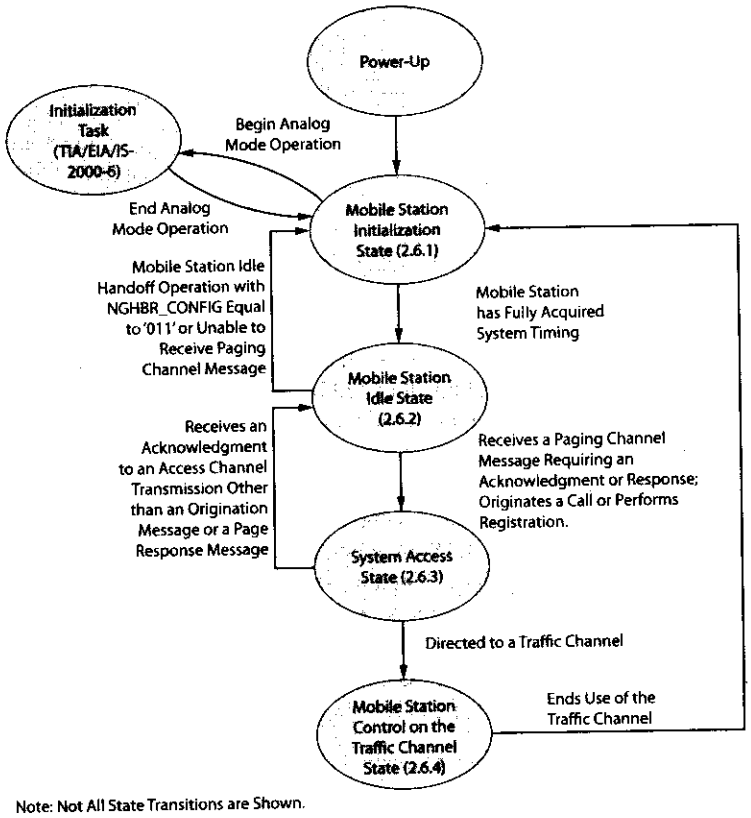


Figure 6–24 CDMA mobile station call processing states (Courtesy of 3GPP2).

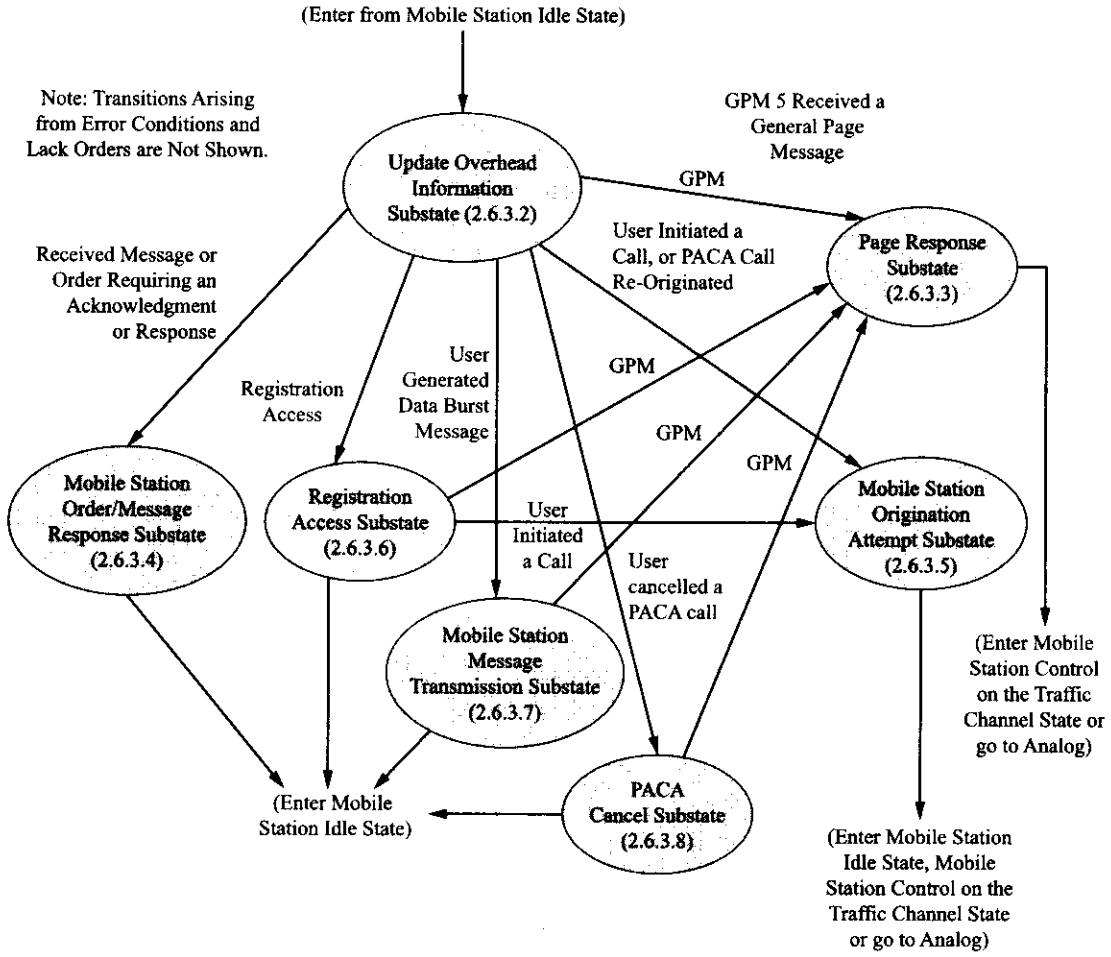


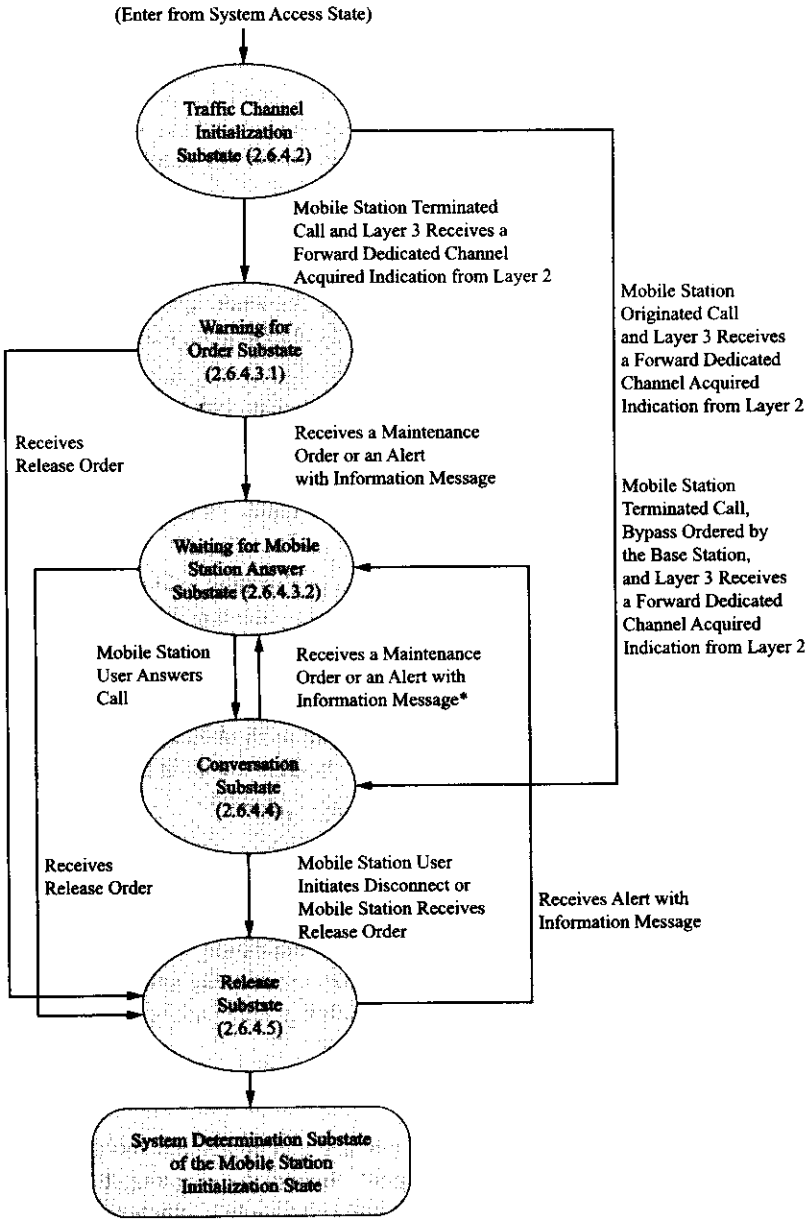
Figure 6–25 CDMA system access state flow chart (Courtesy of 3GPP2).

While in the idle state, the mobile monitors the paging channel (PgC). In the *system access state* the mobile station communicates with the CDMA base station, sending and receiving messages, as shown by Figure 6–25, while performing various operations dictated by the different system access substates.

In the *mobile station control on the traffic channel state* the mobile communicates with the base station using the forward and reverse traffic channels while in various traffic channel substates as shown by Figure 6–26. As indicated by Figure 6–24, the mobile may move back and forth between these three states depending upon the movement of the subscriber and the use of the mobile.

Registration is the process by which the CDMA mobile station, through messages to the base station, informs the cellular system of its identification, location, status, slot cycle, and other pertinent information necessary for proper and efficient system operation. For slotted mode operation the mobile provides the base station with the SLOT_CYCLE_INDEX value so that the base station may determine which slots the mobile is monitoring. Classmark values and protocol revision numbers allow the base station to know the capabilities of the mobile station. Presently, the CDMA system supports ten different forms of registration:

Power-up registration: The mobile station registers when it powers on or switches between different band classes or PCS frequency blocks, alternative operating modes, or analog and CDMA operation.



*If SIGNAL_TYPE is Equal to '01' or '10' or if the Signal Information Record is not Included

Note: Not all State Transitions are Shown.

Figure 6–26 CDMA mobile station control on the traffic channel flow chart (Courtesy of 3GPP).

Power-down registration: The mobile registers when it powers off if it has previously registered in the currently serving system.

Timer-based registration: The mobile registers whenever various timers expire. This process forces the mobile to register at regular intervals.

Distance-based registration: The mobile is forced to register whenever the distance between the current serving base station and the base station where it last registered exceeds a certain threshold. The

mobile station calculates this distance by using the latitude and longitude values for the base stations involved.

Zone-based registration: The mobile station registers when it enters a new zone. Registration zones are groups of base stations within a particular system and network. Zone registration causes the mobile to register whenever it enters a new zone that is not on its internally stored list of visited registration zones.

These first five modes of registration are known as autonomous registration and are enabled by roaming status. In each case, they are initiated by the occurrence of some event.

Parameter-change registration: The mobile station registers when specific parameters stored in its memory change or when it enters a new system. This form of registration is independent of roaming status.

Ordered registration: The mobile station registers when requested to by the base station through the issue of an order message.

Implicit registration: Whenever the mobile station successfully sends an origination message or a page response message, the base station is able to deduce the location of the mobile. These circumstances are considered to constitute an implicit registration.

Traffic channel registration: Whenever a base station has registration information for a mobile that has been assigned to a traffic channel, the base station may notify the mobile that it is registered.

User zone registration: Whenever the mobile selects an active user zone, it registers.

Any of the various forms of autonomous or parameter-change registration may be enabled or disabled by the CDMA system. Additionally, the mobile station may enable or disable autonomous registration for the two types of foreign roaming defined by the CDMA standards. The reader is reminded that authentication of the mobile station is typically performed during the registration process.

Call Establishment

Similar to the GSM cellular system, CDMA system call setup requires various system tasks including mobile initialization, idle, system access, traffic channel communication, and call termination. Additionally, CDMA systems use a sophisticated form of power control for both the mobile and the base station and a more complex form of handoff to provide subscriber mobility that can be more transparent than that employed by GSM cellular systems.

Initialization State

As explained previously, when the mobile is first powered on, it enters the mobile station initialization state. During this process the mobile searches for a pilot channel by aligning its short PN code with a received short PN code. Once a valid pilot channel is acquired the mobile synchronizes with it. The mobile has fifteen seconds to locate and acquire a pilot signal. If the mobile cannot perform this operation, it may decide to search for an AMPS control channel and enter an analog operational mode. When the mobile locates a CDMA pilot signal, it switches to Walsh code 32, W_{32}^{64}, and looks for the start of the sync channel message. The sync channel message contains information about system time and the PN codes needed to synchronize its PN codes. After decoding the sync channel, the mobile aligns its timing to that of the serving base station. Referring back to Figure 6–23, one can more easily visualize the sequence of the operations that occur during this initialization state.

Idle State

Once the mobile has achieved initialization it moves into the idle state. While in the idle state, the mobile is waiting to receive calls or data messages or is ready to originate a call or some form of data transfer. To

support subscriber connectivity and mobility, the mobile is constantly monitoring radio channel quality, decoding paging channel messages to obtain system parameters, access parameters, and a list of neighboring cell sites to monitor. After acquiring sufficient system information, the mobile may be allowed to enter a sleep mode to conserve mobile battery power. This will be facilitated through the use of slotted mode operation by the mobile when monitoring the paging channel as explained previously. Also, to ensure optimal system operation, the mobile will monitor several other neighboring cells to see if a stronger pilot channel is available for a possible idle state handoff. This feature will be explained in more detail when handoff is discussed.

Access State

The CDMA mobile will enter the access state when it receives a mobile-directed message requiring an acknowledgment, originates a call, or is required to perform registration. When in the access state, the mobile will randomly attempt to access the system. Access to the system is obtained when the mobile station receives a response from the base station on the paging channel. Since multiple mobiles may be associated with a particular paging channel, they may simultaneously attempt to use the same access channel. The resulting signal collisions at the base station will most likely result in few if any of the requesting mobiles being granted access to the system. Therefore, to alleviate this problem, some form of collision avoidance scheme is necessary to increase the probability of a successful system access by a mobile. For the CDMA system, this access protocol is implemented through the use of access class groups with assigned priorities, a gradual increase in access request power level, random time delays for access requests, and a maximum number of automatic access attempts. Figure 6–27 depicts what is known as access channel probing. The transmission of a series of access probe sequences is known as an access attempt.

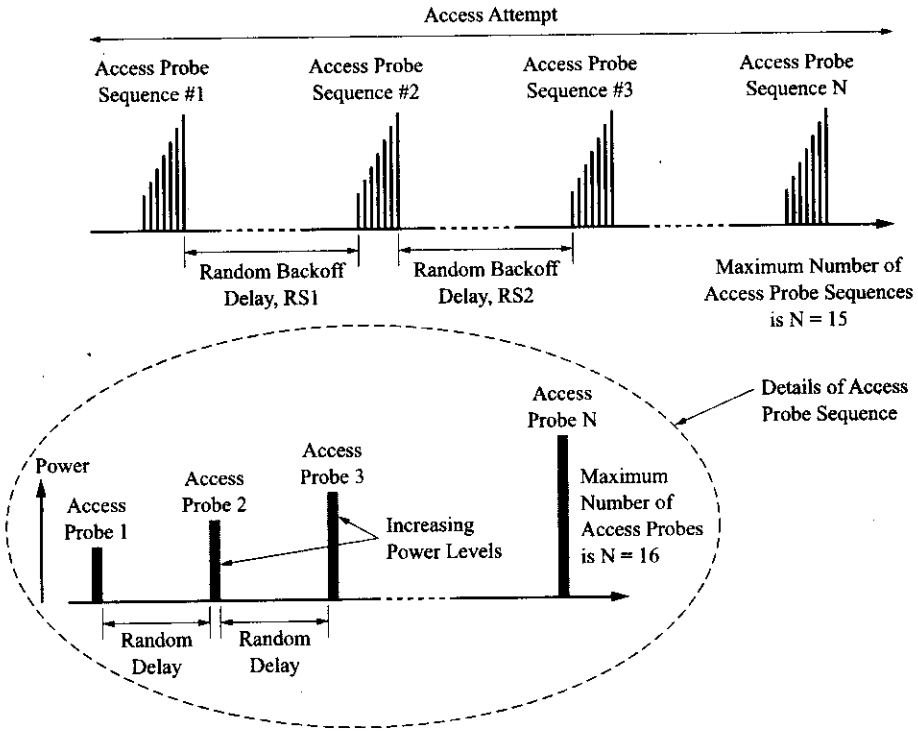


Figure 6–27 CDMA access channel probing (Courtesy of 3GPP2).

Each access probe consists of an access channel preamble (one to sixteen frames consisting of 0s) and an access channel message capsule of three to ten frames. This yields an access probe with a duration of four to twenty-six 20-ms frames. Two types of access messages may be transmitted by the mobile on the access channel: either a response message or a request message. Within an access probe sequence, the access channel message is the same for each access probe. Referring to Figure 6–27 again, one can see that the access channel probing process consists of the mobile station sending a series of sequences of access probes of increasing power levels. Furthermore, an access probe sequence is formed by the repeated transmission of additional access probes until either the mobile has received an acknowledgement over the paging channel or the mobile station's power limit has been reached. If the mobile station's first access probe sequence is unsuccessful, additional probe sequences are transmitted until a successful access occurs or the maximum number of allowed probe sequences has been exceeded.

The mobile station will randomly determine the start of each access probe transmission within a sequence and the backoff delay for the start of the next access probe sequence and the start of any additional access attempts if needed. Additionally, the access channel to be used during the access probe sequence is also randomly selected from the access channels associated with the current paging channel for each access probe sequence.

Traffic State

The mobile enters the traffic state when it begins to transfer user information between the mobile and the base station (refer back to Figure 6–26). As was the case for GSM cellular, this information can be voice or data that originates from the PSTN or PDN or another mobile in the same or another network. While in the traffic state, the mobile transmits voice and signaling information on the reverse traffic channel (RTC) and receives voice and signaling information on the forward traffic channel (FTC). Signaling over the traffic channel can be performed by either a blank-and-burst or dim-and-burst process. The blank-and-burst signaling method replaces 1.25 ms of speech data with signaling message bursts. The dim-and-burst method inserts signaling messages when speech activity is low. The 8-kbps QCELP vocoder combines lower-rate voice data and signaling data into a higher-rate frame (only done at the 9600-bps rate) whereas the 13-kbps vocoder can use any frame for both voice and signaling. Various mode and flag bits are used to alert the receiver to the signaling method (dim or blank) and structure of the mixed voice and signaling frames. Depending upon the message, the number of frames needed to send the signaling information will vary. Although the dim-and-burst method will not affect speech quality, it requires more time to transmit the signaling. In the interest of continuity, call setup operations will be discussed next.

Mobile-Originated Call To originate a call, the mobile sends a system access message on the access channel and then monitors the paging channel for a response from the system. If the access is successful, a forward traffic channel is assigned that corresponds to a particular Walsh code and a base station receiver is assigned for the reverse traffic channel long PN code. Additionally, the base station sends a paging channel message to the mobile with the Walsh code information and a reverse traffic channel assignment. The mobile configures itself and begins decoding null traffic that the base station has started to transmit over the forward traffic channel. The mobile starts to transmit a preamble over the reverse traffic channel. The base station uses the forward traffic channel to acknowledge the preamble and the mobile responds by starting to send traffic. Figure 6–28 shows these steps in timeline chart form. During the call, there are constant power control operations taking place and, if the mobile is moving about, handoffs may occur between different base stations. The reader is advised to consult the latest 3GPP2 standards for more detail if it is desired.

Mobile-Terminated Call For a mobile-terminated call, the base station sends a message to the mobile on the paging channel. If attached to the system, the mobile sends an acknowledgement response on the access channel. The base station receives the acknowledgement, configures a forward traffic channel, and assigns a receiver to the mobile's reverse traffic channel. The base station begins to send null traffic on the FTC

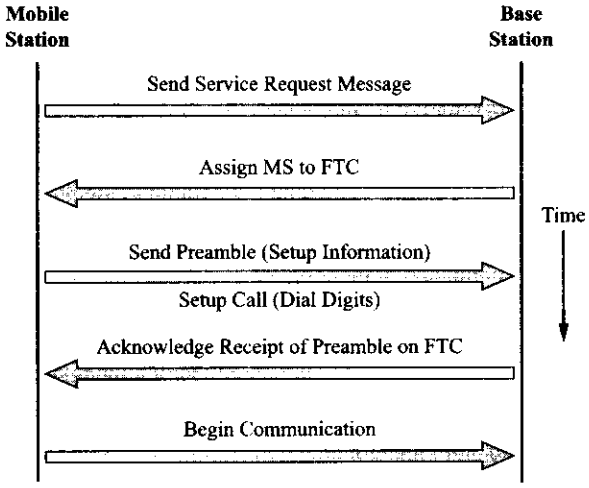


Figure 6–28 CDMA mobile-originated call timeline.

and sends a PgC message containing Walsh code and RTC information. The mobile configures itself and begins decoding the null traffic and transmitting a preamble on the RTC. The base station acknowledges the preamble sent on the RTC. The mobile receives the acknowledgement and begins transmitting null traffic on the RTC. The base station sends an alert message for a ring tone and the display of calling number information. The mobile acknowledges the message by ringing the handset and displaying the calling number information. When the subscriber answers the incoming call a connection message is sent on the RTC. The base station acknowledges the connection message and begins to send traffic. See Figure 6–29. Again, the current standards provide much more detail for the interested reader.

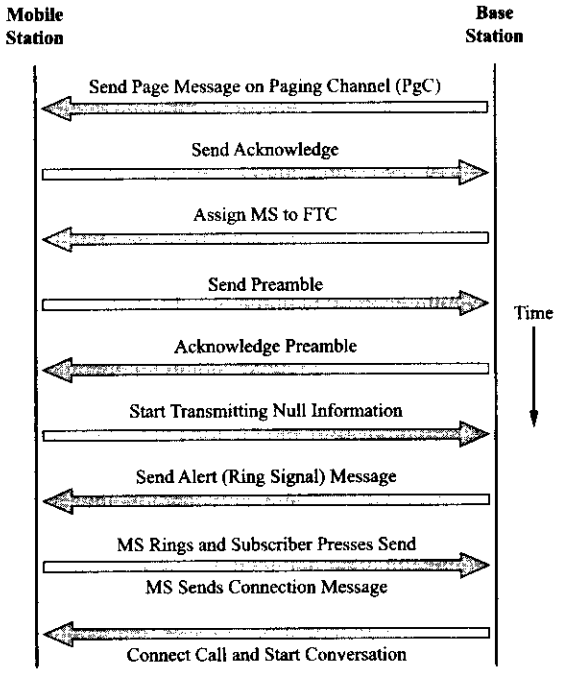


Figure 6–29 CDMA BS-originated call timeline.

Call Termination Call termination occurs at the end of a call and can be initiated by either the mobile or the base station. If the mobile initiates the call termination, it sends a call termination message to the base station, stops transmitting on the RTC, and returns to the mobile station initialization state. If the network initiates the call termination (the calling party hangs up), the base station sends a call termination message to the mobile. The mobile stops transmitting on the RTC and returns to the initialization state.

Call Handoff

The specifications for IS-95 CDMA delineate three mobile station states during which a handoff can occur. Referring back to Figure 6–24, these states are the idle state, access state, and traffic state. The procedures used and the type of handoff performed will depend upon the mobile's present state. In all cases, the handoffs are mobile assisted since the mobile station is tasked with reporting signal-strength measurements of various pilot channels to the network. As is typical with any wireless mobile system, handoff occurs when the serving sector/cell is no longer capable of supporting communications between the mobile and itself. CDMA is unique in that it supports soft/softer handoffs. There are several advantages to this type of handoff including improved system performance for the support of voice traffic calls and the support of high-speed data transfers. The details of these handoff operations will be presented next.

Idle/Access Handoff

If the mobile is in the idle state and moves from the coverage area of one sector/cell into another sector/cell, an idle handoff can occur. When the received signal strength of a different pilot channel (PC) is determined to be twice as strong (3 dB greater) than the current PC, the mobile will start listening to the paging channel (PgC) associated with the stronger PC. This type of handoff is considered a form of hard handoff since there is a brief interruption of the communication link. But it is certainly different from and less disrupting than a hard handoff that might occur when the mobile is in the traffic mode.

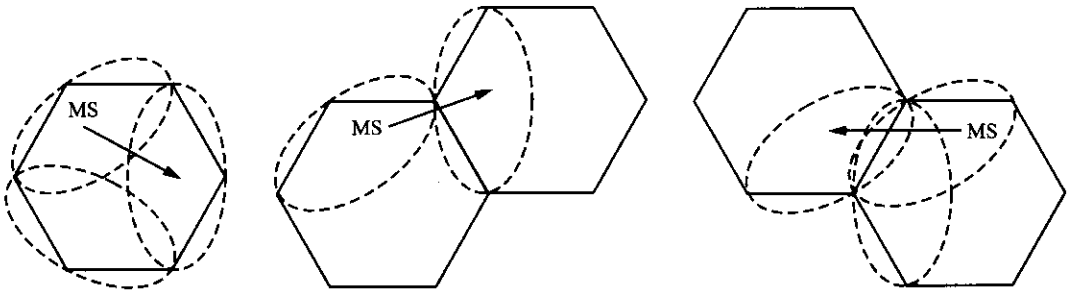
While the mobile is in the access state, it can also perform a handoff. The access handoff may occur before the mobile begins sending access probes, during access probes, and even after it receives an access probe acknowledgement. An access entry handoff allows the mobile to perform a hard idle handoff from one PgC to another in the best signal-strength sector/cell just after the mobile enters the access state. After the mobile has started to send access probes, it can perform an access probe handoff if it detects a stronger pilot signal that may provide it a better chance of receiving service. Even after the mobile has received an access probe acknowledgement, a handoff to a stronger pilot may be possible and necessary to prevent an access failure due to the rapid motion of the mobile away from the current pilot and its base station.

Soft Handoff

A distinct advantage of the CDMA system is that it can support soft handoffs. Basically, a **soft handoff** occurs when the mobile is able to communicate simultaneously with several new cells or a new sector of the current cell over a forward traffic channel (FTC) while still maintaining communications over the FTC of the current cell or sector. The mobile station can only perform a soft handoff while in the traffic state to a new cell or sector that has the same frequency carrier. The use of soft handoffs is associated with the near-far problem and the associated power control mechanism used in CDMA systems. If a mobile moves away from a base station and continually increases its output power to compensate for the signal attenuation encountered at the greater distance, it will cause a great deal of interference to mobiles in neighboring cells and raise the level of background noise in its own cell. To alleviate this problem and to make sure that the mobile is connected to the base station with the greatest RSS, a strategy employing soft handoffs has been designed into CDMA wireless mobile systems. In theory, the optimal CDMA system operation will occur when each mobile is connected to the nearest base station (the base station with the strongest signal) and is transmitting with the lowest output power necessary for proper operation. In fact, the use of soft handoff can actual improve system performance since the procedure used can actually lower reverse link

output power because the received signal from several base stations can be combined. A carefully implemented soft handover process can enhance system performance by increasing call quality, improving coverage, and increasing capacity.

Figure 6–30 depicts the three types of soft handoffs defined in the IS-95 CDMA standard. The first type of handoff is known as a *softer* handoff since the handoff is between two sectors of the same cell. A *soft* handoff occurs between two different cells and a *soft-softer* handoff can occur when the motion of the mobile gives it a handoff choice between two sectors of the same cell and a sector from an adjacent cell.



(a) Softer Handoff (b) Soft Handoff (c) Soft Softer Handoff

Figure 6–30 Three types of soft CDMA handoff.

In all CDMA handoff procedures a number of base stations and their pilot channels are involved. The procedures for soft and softer handoffs control the manner in which a call is maintained as a mobile crosses boundaries between cells or enters a new sector of the same cell. In a soft handoff, more than one cell simultaneously supports the mobile's call. In a softer handoff, more than one sector of a cell simultaneously supports the mobile's call. The CDMA mobile station will continuously scan for pilots and establish communication with any sector or cell (up to a maximum of three) that has a pilot RSS that exceeds a certain threshold value (T_ADD). In a similar fashion, the mobile will drop communications with a sector or cell that has a pilot RSS less than a certain threshold (T_DROP). Recall that each pilot has a different time offset for the same short PN sequence code. This fact is used to differentiate cells and sectors within the system. The mobile's identification of different pilot signals depends upon this property. Since the offsets are integral multiples of a known time delay, the mobile's search for the pilots is made easier. The mobile will categorize pilots that it receives as well as other pilots that the serving sector/cell specifies to it into the following groups: an active set that consists of the pilots that are currently supporting the mobile's call, a candidate set that consists of pilots that based upon their RSS could support the mobile's call, a neighbor set that consists of pilots not in the active or candidate set but that are geographically nearby, and a remaining set of pilots that consists of the rest of the pilots within the system.

The mobile's continuous assessment of pilot RSS and a set of adjustable threshold values will determine the movement of pilot signals within these sets. These measurements, in conjunction with information received from the serving sector/cell and mobile station timers, give rise to dynamically changing sets if the mobile moves about the system. Figure 6–31 depicts a simplified flowchart of this process.

To complete our coverage of this topic, let us compare soft/softer handoff to handoff in other systems. In most other access technologies a mobile station moving from one sector/cell to another must switch to an available channel in the new sector/cell. This process requires a brief interruption of the communications link. Since a CDMA system reuses the same frequency in every sector/cell within the system, soft/softer handoff does not cause an interruption in the communications link. This fact is extremely important when it comes to the ability of the system to transmit high-speed data since there is no potential loss of data due to a hard handover. Furthermore, the use of soft/softer handoff gives rise to improved system performance as previously mentioned. With soft/softer handoff reduced mobile transmit power is

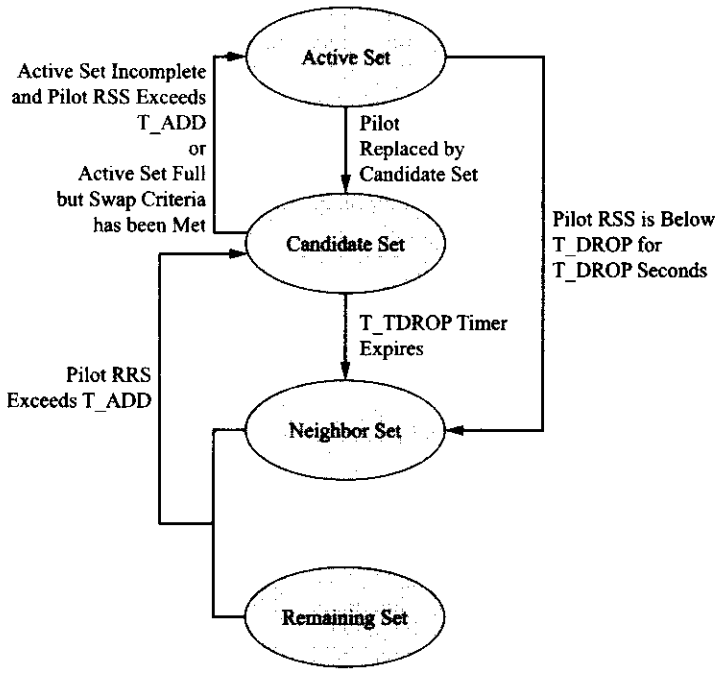


Figure 6–31 Flowchart of the generation of the active and candidate pilot set for CDMA handoff operations.

possible because of the inherent gain involved with the use of multiple receivers. With soft handoff, the MSC selects the best signal on a frame-by-frame basis of those received (this could be up to three different signals). This process tends to mitigate signal impairments that occur during transmission over the air interface. With softer handoff, the increase in performance is realized at the base station by a combining of the signals from multiple sectors.

Hard Handoff

A CDMA mobile in the traffic state can also experience a hard handoff. This will occur for the case of an intercarrier handoff. Intercarrier handoff causes the radio link to be abruptly interrupted for a short period while the base and mobile station switch from one carrier frequency to another. There are two basic types of intercarrier handoff: a **hand-down** is a hard handover between two different carriers within the same cell, and a handover is a hard handoff between two different carriers in two different cells. The circumstances necessary to cause a hard handoff can be due to the particular coverage area implementation of a service provider or the less frequent case of the existence of two service providers in adjacent areas.

In the first case, known as a pocketed implementation, a service provider might use a second CDMA carrier in individual or noncontiguous cells to provide additional capacity during system growth or for local high-traffic hot spots. Figure 6–32 depicts a possible scenario of this situation. A mobile that is using the second carrier and exiting the pocket of second-carrier cells must be handed off to the common carrier to continue the call. The best way to perform this handoff is to first hand down the call to the common carrier before the mobile leaves the pocketed area. Then a soft handoff can be performed as the mobile moves across the border from the pocketed area into the surrounding service area.

Typically, this process of hand-down occurs, if possible, at the border cells (sectors) of the pocketed area. In general, border cells (sectors) must be identified and configured to operate in a slightly different fashion than nonborder cells (sectors). In Figure 6–32 this can be more readily accomplished for the pocket in the middle of the system but is not as easily achieved for the pockets in the lower left and right corners

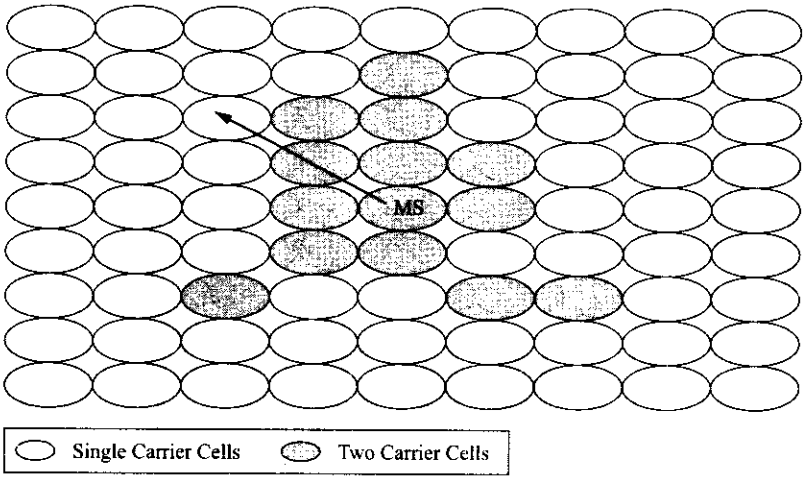


Figure 6–32 Hard CDMA handoffs due to intercarrier handoff.

of the diagram. Usually, careful examination of cell geometry and local traffic routes can aid in the selection of a border cell (sector).

When a mobile enters a border sector, it is instructed by the base station to issue frequent pilot-strength measurement messages. This process allows the sector to more closely monitor the mobile's status instead of waiting for reports triggered by other pilot events. If the pilot report indicates that the sector's pilot has dropped below a certain threshold level, the base station directs the mobile to hand down to the first carrier. The value of threshold used in this process forces this hand-down to occur before the mobile has reached the edge of the sector. This process allows sufficient time for the normal soft handoff to occur as the mobile exists at the border sector. This type of process will work well for a large pocket with well-defined border cells but does not work well where insufficient first-carrier capacity is available to accommodate the required hand-down as might be the case for an isolated cell with a second carrier. In the latter case, the solution is to expand the second-carrier pocket so that it has sufficient first-carrier capacity to handle normal first-carrier traffic and hand-downs. In the case where a second carrier is added to a cell to facilitate hand-downs instead of providing normal traffic relief, the term *transition cell* is used instead of border cell. The area around the original isolated cell is known as the transition zone and hand-down is only allowed in the transition zone providing relief for the heavily loaded original cell.

It is possible to have disjoint systems where distinct CDMA carriers exist in different regions due to issues such as the availability of appropriate spectrum. Figure 6–33 depicts this situation. The most common methods used to provide handoff between the two regions is to implement a border area that supports the use of both carrier frequencies and is configured to provide hand-down as previously described or to simply execute a hard handoff from one carrier to the other as the mobile crosses the border between the two regions.

The first scenario works well for a clearly defined border area with a predictable flow of traffic. However, if a mobile might be expected to turn around within the border area and return to the region it had previously left, a more complex border area must be created to prevent the possibility of thrashing (extremely undesirable) between the two carriers. The last situation requires the identification of border cells that facilitate the handover from one carrier to the other. These border cells are configured to make frequent pilot-strength measurements and use a threshold value that will cause a handover from the host (current) cell to the target (future) cell in the vicinity of the border between the two cells.

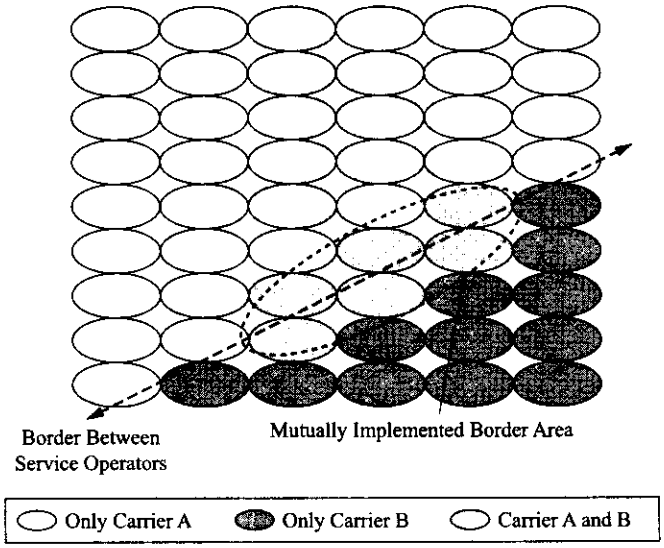


Figure 6–33 Hard CDMA handoffs due to disjointed regions.

Power Control

CDMA cellular is interference limited. However, for the CDMA case, it is not adjacent and cochannel interference that are the main cause of problems. Instead, it is interference from other mobiles using the same frequency spectrum at the same time. The use of spread spectrum technology gives rise to what is known as the near-far effect. What this expression refers to is the possibility that in a system using spread spectrum modulation a single nearby transmitter with the strongest signal may capture a receiver even though there are other users also transmitting. For this reason and to also combat typical UHF signal propagation effects such as fading and shadowing, it is imperative that a high-quality power control system be used. Therefore, the objective of CDMA power control is to limit the transmitting and receiving power of all users to the minimum levels required for proper system operation. To this end, the power control system precisely controls mobile transmit power in an attempt to have all the mobile signals arrive at the base station with the same minimum required signal-to-interference ratio.

Therefore, in IS-95, a sophisticated power control system is employed that maintains received signals within approximately 1 dB of their optimal level. On the reverse link, which uses noncoherent detection, two different types of power control are implemented. This scheme allows the mobile output power level to be continually adjusted. The forward link uses its own form of mobile-assisted power control. In both cases, the frame error rate (FER) is used to make power control decisions. Since the RSS may be good and frames may still contain errors, the use of FER is preferred for CDMA systems. The usual acceptable system FER is in the 2% range. The next several sections will give a more detailed accounting of these power control methods.

Forward Link Power Control

The power for each forward traffic channel (FTC) is dynamically controlled in response to information transmitted to the base station by the mobile. The base station starts transmitting on the FTC at a nominal power level and then continually reduces its output power level. The mobile periodically reports the FTC frame error rate (FER) statistics to the base station over the reverse traffic channel (RTC). This report could indicate when the FER increases or when it reaches a certain threshold. The base station then adjusts its output power for the particular FTC accordingly. Since this adjustment can be made only once per frame time (20 ms), this process is known as slow forward link power control. As the mobile moves about or

propagation or interference conditions change, the base station changes its output power level to compensate for the changes.

Reverse Open Loop

A fairly good first approximation is that the path loss between the base station and the mobile station is the same in either direction. Using this assumption, the mobile station makes an open loop estimate (no base station feedback) of its required output power level when attempting a system access. Using the pilot signal level as a reference, the mobile continually measures the RSS and transmits a low-level signal if the pilot is strong or a higher-level signal if the pilot is weak. As explained in the section about access attempts, if the access probe is not acknowledged, a stronger signal is sent on the next access probe and so on. As the mobile moves about and possibly changes its distance from the base station, it will adjust its output power for any new access probes in response to changes in the received pilot signal power.

Fast Closed Loop

Since the forward and reverse channels may fade differently (recall that they are at different frequencies), a fast closed loop power control scheme is employed during the mobile station control on the traffic channel state to help overcome fades over the reverse link that are not apparent to the mobile station. This is made possible by the transmission of a power control bit over the FTC every 1.25 ms. At the base station, the BS receiver determines the average received signal-to-interference ratio every 1.25 ms for the mobile RTC. If the value is above a preset target value, the base station transmits a power control bit set to 1. This instructs the mobile to reduce its output power level by 1 dB. The transmission of a 0 indicates an increase of 1 dB in output power level. The process continues until the mobile's output power level converges on the correct value. This process is known as the inner-loop power control. There is not a direct relationship between the FER and the signal-to-interference ratio so the target value is constantly updated to reflect the actual FER. If the FER increases the target value may be rapidly increased and the mobile's power will be quickly adjusted by the transmission of the appropriate power control bits. This process is known as the outer-loop power control.

PART III 3G CDMA

6.5 IS-95B, CDMA2000, AND W-CDMA

A high market demand and continuing advances in the field of microelectronics technology have motivated the cellular industry to develop numerous wireless standards over the past few years that have led to new service offerings particularly in the mobile data arena. Also, due to the global nature of the market, cellular standards have been the focus of several international committees such as the 3GPP and 3GPP2 collaborations. As pointed out earlier, in the effort to establish next-generation (3G) cellular standards, a number of proposals have been submitted to ITU-R for evaluation and adoption. The desired harmonization of proposals for W-CDMA, TD-CDMA, TD-SCDMA, and EDGE (a follow-on to GSM) systems are being dealt with by the 3GPP group (UMTS standard) while cdma2000 is under the purview of the 3GPP2 group. In all cases, the ultimate evolution to true 3G capabilities involves the use of CDMA technology for the air interface portion of the system. Although EDGE technology enables a number of 3G data services to be supported, it is still a form of GSM (further EDGE details will be provided in Chapters 7 and 8). Due to spectrum considerations, EDGE service (which can operate in noncontiguous 200-kHz blocks of spectrum) will offer a bridge solution to 3G capabilities until sufficient spectrum is available to implement the UMTS CDMA-based 3G solution.

IS-95B

Up until this point, this chapter has primarily focused on IS-95A CDMA technology that was designed mainly for voice communications. An evolutionary improvement to IS-95A, IS-95B, was adopted in October 1998 and added additional mobile data functionality to the earlier standard. IS-95B features the use of combinative channels. That is, a primary channel may be combined with up to seven supplementary data channels. So theoretically, IS-95B should be able to support packet data services with up to a maximum transfer throughput rate of 106.8 kbps. In practice, a much more realistic data rate that can be achieved by a mobile user is 64 kbps. The next section will outline the major differences between IS-95A and IS-95B.

IS-95B Forward and Reverse Channels

The most dramatic changes to IS-95A are found in the channel structure. To implement an increased packet data rate, IS-95B employs what are known as **supplementary code channels** (SCCHs) in both the forward and reverse direction. Also, the former forward and reverse traffic channels are now known as fundamental channels (FCHs). These channels are still used primarily for voice traffic. In IS-95B, the system may assign from one to seven idle CDMA channels to a user as supplementary code channels and therefore provide the extra bandwidth capacity needed to increase the packet data transfer rate for a subscriber. Since this technique will be discussed in more detail in Chapter 7, it will not be discussed any further at this time. Aside from several improvements made to handoff algorithms, the rest of the operations that are supported by IS-95B are similar to those of the original standard. Packet and frame formats are similar as are power control functions. As a consequence of the use of supplementary code channels in IS-95B, the function of radio resource management is naturally more complex and sophisticated.

Cdma2000

Cdma2000 is considered one of the primary air interface technologies for implementation of 3G cellular. Using CDMA to provide 3G functionality is an evolutionary approach based on the IS-95B standard that is designed to build on legacy IS-95 wireless networks. This approach allows a service provider to upgrade or overlay this technology on an existing 2G or 2.5G system. Cdma2000 consists of two phases of development. The first phase involves the enhancement of IS-95B to cdma2000 1xRTT (a single-carrier system) with enhanced packet data capacities. The first release (0) of cdma2000 1xRTT allows packet data speeds to 153.6 kbps and the second release (1) increases that speed to 307.2 kbps over a single 1.25-MHz carrier. Note that a data rate of 614.4 kbps is also included in the standard but is not slated to be implemented at present. In North America this upgrade process to 1xRTT technology is close to completion (see www.cdg.org). The changeover to cdma2000 or new deployment of cdma2000 systems continues on a worldwide basis, with only the traditional GSM strongholds (Europe, Africa, Greenland, and areas of the Middle East) still without any coverage or widespread coverage depending upon the region.

The second phase of the 3G evolution, known as cdma2000 1xEV (still only one carrier evolution), uses enhanced higher-level modulation schemes (8-QPSK and 16-QAM) that allow for more data bits per CDMA frame. This last evolutionary phase also consists of two steps. The generally accepted first step is to migrate to cdma2000 1xEV-DO (data only). 1xEV-DO employs a shared downlink transmission process for data that is presently incompatible with 1xRTT but promises a peak downlink data rate of up to 2.4 mbps for packet data. The uplink will still use 1xRTT technology. Therefore, dual-mode devices would be needed for voice (1xRTT) and data calls (1xEV-DO) in this overlay structure. The next step, 1xEV-DV, is an advanced technology that will integrate both voice and data on the same carrier and also retain backward compatibility with 1xRTT. 1xEV-DV promises a peak packet data rate of 3.09 mbps in the downlink direction. The system packet data rate asymmetry (downlink:uplink) for both 1xEV-DO and 1xEV-DV range from 1 : 1 to 4 : 1.

Cdma2000 Differences

The most important characteristics of cdma2000 are its backward compatibility with IS-95B, support for high-speed packet data and multimedia services (QoS), and advanced radio technologies such as smart antennas. To achieve enhanced packet data transfer rates cdma2000 has incorporated several improvements and additions to the IS-95B air interface and the coding schemes employed by the system. Specifically, the standard has added additional logical channels into its forward and reverse channel structures, specified two spreading rates (1X and 3X) and numerous radio configurations (depending upon vocoding rates, optional frame lengths, spreading rates, and modulation schemes), and has included enhancements to its radio transmission/reception technology through the use of a reverse channel pilot, enhanced power control, and additional forward pilots that permit the utilization of diversity techniques to improve signal reception. The use of additional pilot signals allows the system to further combat radio channel impairments, reducing the bit error rate and as a consequence reducing frame error rates.

A few comments about cdma2000 spreading rates and radio configurations are appropriate now since this will help readers in their understanding of some of the modifications to IS-95B that follow, in the context of these different rates and configurations. As just indicated, the cdma2000 standard specifies two spreading rates. Spreading Rate 1 (SR1) is commonly designated as 1X and indicates a standard single direct-sequence spread CDMA carrier with a chip rate of 1.2288 mcps. Spreading Rate 3 (SR3) is similarly designated by 3X. A forward 3X CDMA channel is implemented through the use of three direct-sequence spread carriers (this is known as multicarrier CDMA) each with a chip rate of 1.2288 mcps. A reverse uplink 3X CDMA channel is implemented with a single direct-sequence spread carrier with a chip rate of 3.6864 mcps (usually referred to as wideband CDMA). The use of either three carriers (downlink) or a higher chip rate with its larger spectrum (approximately 3.75 MHz) will provide the system with the ability to obtain higher-speed data transfer rates over the air interface. Radio configurations (labeled as RCNs) also need explanation at this time. Cdma2000 supports numerous different radio configurations in both the forward and reverse directions. For example, RC1 supports IS-95B backward compatibility for all services defined under Rate Set 1 whereas RC2 supports Rate Set 2 services. Other higher-index radio configurations support higher data transfer rates that depend upon the spreading rate, base data rate (9.6 or 14.4 kbps), channel type, encoding rate, and frame length. Presently, RC1 through RC5 and RC10 use Spreading Rate 1 while RC6 through RC9 use Spreading Rate 3. For example, in the forward direction, radio configuration 10 (RC10) allows a maximum data transfer rate of 3.0912 mbps over the forward packet data channel while employing Spreading Rate 1. It should further be pointed out that the cdma2000 standard allows for Walsh codes with lengths from 4 to 1024 bits to assist in implementing the various encoding schemes.

Additionally, cdma2000 has enhanced the IS-95 protocol stack to include advanced Layer 2 functionality. The new protocol stack contains both a media access control (MAC) sublayer and a signaling link access control (LAC) sublayer. Both of these sublayers have been designed to optimize circuit-switched and packet-switched data services. This optimization includes both enhanced control state functions and quality of service (QoS) control functions. Note that 1xRTT does not include these QoS enhancements. More details about this topic will be offered in Chapter 7.

Cdma2000 Forward and Reverse Channel Structures For cdma2000 various additional forward and reverse logical channels have been defined. In the forward direction, one can classify the logical channels into three broad categories: overhead, control, and traffic channels. In the overhead group there are four pilot channels (forward common pilot channel, forward common transmit diversity pilot channel, and an auxiliary pilot channel and auxiliary transmit diversity pilot channel) that are used for enhanced system timing, phase, radio link characteristic estimation, diversity reception, and power reference purposes by the mobile station. Additionally, there is a sync channel used to provide system synchronization information, paging channels to provide IS-95B compatibility, and a quick paging channel designed to provide slotted mode operation and save mobile station battery power. Figure 6–34 displays the forward channel structure for cdma2000. Note the references to spreading rate and radio configurations within the appropriate blocks.

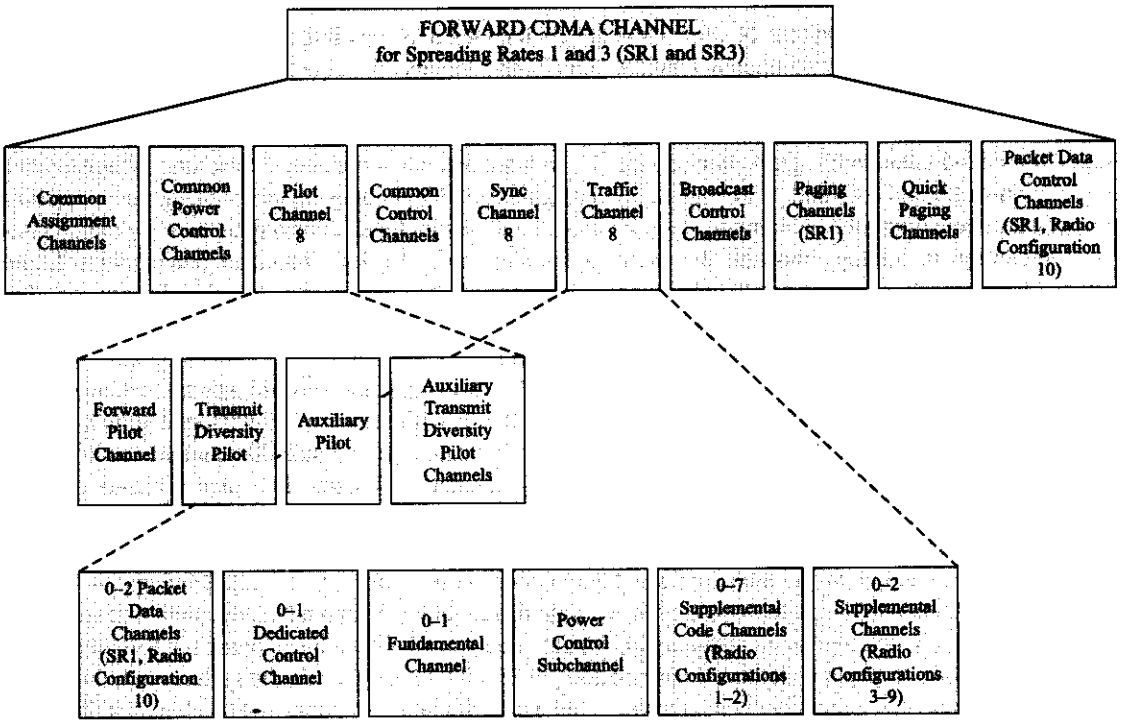


Figure 6–34 Forward channel structure of cdma2000 (Courtesy of 3GPP2).

The forward control channel group consists of common assignment channels, common power control channels, common control channels, broadcast control channels, and packet data control channels. The common assignment channel is used by the CDMA base station to acknowledge a mobile station accessing the reverse enhanced access channel and to supply information to the mobile about which reverse common control channel to use and information about the associated common power control subchannel. The common power control channels are used to transmit power control bits to multiple mobile stations when they are operating in modes (e.g., packet data transfers) that do not include a forward fundamental channel or a forward dedicated control channel . Without a F-FCH or F-DCCH communications link no power control subchannel information would be transmitted, hence the need for the common power control channels to provide this function. The common control channels are used by the base station to transmit mobile station-specific messages whereas the broadcast control channels are used to transmit system messages to all mobile stations within the range of the base station. The packet data control channel is used by the base station to send control information for the associated forward packet data channel.

As shown in Figure 6–34, the forward traffic group supports the forward fundamental channel (F-FCH) and up to seven supplemental code channels (SCCHs) for IS-95B compatibility. Additionally, two supplemental channels (SCHs) specifically designed for high-speed data services (RC3 through RC9) and two high-speed packet data channels for RC10 use have been added, along with a dedicated control channel (DCCH) that is used for signaling message support.

In cdma2000, the fundamental channel is equivalent to the IS-95B fundamental channel. Used primarily for voice service, it supports variable rate coding, can also support low rate data services, and may also carry signaling messages. The fundamental channel in cdma2000 supports 5-ms frames that can be used to carry MAC messages that are required for fast assignment of radio resources for packet data services. As in IS-95B, the F-FCH also carries power control information for fast closed loop power control. The supplemental

code channels (SCCHs) are similar to IS-95B supplemental code channels. They can be used to support data rates of 9.6 and 14.4 kbps. The forward supplemental channels (SCHs) can be used for RC3 through RC9 with data transfer rates of up to 1.0368 mbps. F-SCHs use two types of coding, convolutional or turbo, and may use frame lengths of 20, 40, and 80 ms. To implement 3G functionality, multiple SCHs may be used between a base station and mobile station to support multimedia services. There can be several SCHs operating simultaneously, each with its own data rate and QoS requirements. Any MAC signaling must be carried on either an associated F-FCH or DCCH since the SCHs do not support 5-ms frames nor do they carry power control information needed to maintain the radio link. The forward packet data channels are capable of data rates to 3.0912 mbps with frame lengths of 1.25, 2.5, and 5 ms. One can certainly say that the additional logical channels specified in cdma2000 are necessary to facilitate the additional functionality embodied in the 3G specifications.

The reverse link channel structure is shown by Figure 6–35 for SR1 and SR3. Figure 6–35 depicts two kinds of information. First, the various operational modes of the mobile are arranged into columns and then the types of reverse channels that can be transmitted by the mobile station within each operational group are shown. IS-95B operation is indicated by the two left-most columns with the reverse access, fundamental, and seven supplemental code channels whereas cdma2000 operation adds the three right-most columns in the figure.

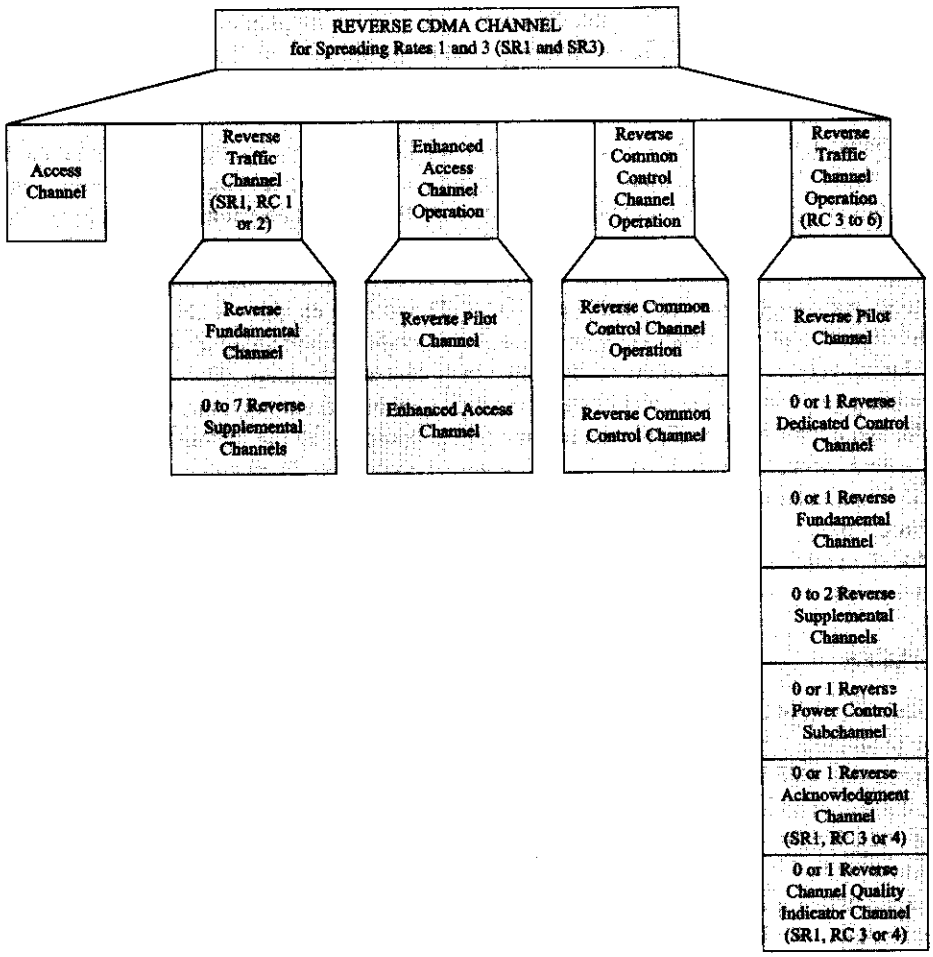


Figure 6–35 Reverse channel structure of cdma2000 (Courtesy of 3GPP2).

Added to the basic IS-95B channels in cdma2000 are a reverse pilot channel that includes within it a reverse power control subchannel, an enhanced access channel, a reverse common control channel, a reverse dedicated control channel, a reverse acknowledgement channel, a reverse channel quality indicator channel, and two supplemental channels.

The reverse pilot channel has been introduced to enhance reverse radio link performance. The reverse pilot allows the base station to coherently demodulate signals transmitted by the mobile station with fewer bit or frame errors. As can be seen from Figure 6–35, the reverse pilot is used during enhanced access channel operation, reverse common control channel operation, and reverse traffic channel operation. During the first two operational modes, the reverse pilot is multiplexed with the other information being sent by these channels. During calls (traffic operation) the pilot and its associated reverse power control subchannel are multiplexed with the traffic. The reverse acknowledgement and channel quality indicator channels are similar to the power control subchannel and are only operational for RC3 and RC4. As was the case for the forward logical channels, the reverse logical channels have frame lengths of 5, 10, 20, 40, and 80 ms.

The enhanced access channel allows three different modes of operation in cdma2000. The first mode is similar to the access probe used by IS-95A/B and described in Section 6.3, only it takes place on the enhanced access channel. The second mode of operation, known as reservation access mode, is used by the mobile to gain control of a common control channel so that the risk of an access collision is reduced. The last mode, known as power controlled access mode, is used in conjunction with a forward power control channel to provide power control on the reverse link channels. The reverse supplemental channels, like the forward supplemental channels, can have different data rates and there need not be a one-to-one correspondence between the number of forward and reverse supplemental channels in use during a session. For cdma2000 the maximum data rate for a supplemental channel is 1.0368 mbps.

During cdma2000 operation, as shown by Figure 6–35, there are five different configurations of physical channels that may exist on the reverse link at any time depending upon the mobile's mode of operation and the radio configuration (RC1 through RC6). A short description of these configurations is given here. The mobile may use the IS-95B access channel to gain system access. The mobile engages in standard IS-95B traffic operations using the reverse fundamental channel and up to seven additional reverse supplemental code channels to increase the data transfer rate (RC1 and RC2). The mobile engages in an enhanced access channel system access. The use of the enhanced access channel operation is designed to reduce the probability of a collision during access and to improve the efficiency of channel usage. The mobile has been successful in implementing the reservation access mode and uses a reverse common control channel to talk to the base station. The last operational profile is the reverse traffic operation mode. While in this mode, the reverse pilot and the reverse power control subchannel are always operational. Furthermore, the mobile station may support an R-FCH or an R-DCCH. Cdma2000 supports up to two supplemental channels for data services and, since user signaling cannot take place over the SCHs, either the R-FCH or the R-DCCH must be present continuously. This short introduction to cdma2000 will be enhanced in Chapters 7 and 8.

W-CDMA and UMTS

As discussed in Chapter 5, GSM wireless cellular systems have more subscribers worldwide then any other type of cellular technology. In its evolution toward 3G functionality, GSM technology has adopted general packet radio service (GPRS) to provide enhanced packet data transfer rates with a maximum potential rate of 171.2 kbps. In the next phase of its evolution, GSM makes use of advanced modulation techniques to achieve even higher packet data rates. This next system upgrade is known as enhanced data rates for global evolution or EDGE. Using the same GSM radio resources, EDGE, in theory, can provide a data rate of 473.6 kbps when all eight GSM timeslots are combined and used by a single subscriber; however, the data throughput rate is actually less. EDGE therefore enables a number of 3G data services but really requires numerous GSM carriers to satisfy the 3G functionality requirements. A new AMR

vocoder has further increased GSM system capacity, but the same basic GSM radio interface using TDMA technology remains.

In an effort to migrate GSM/TDMA standards to 3G, the Third Generation Partnership Program (3GPP) group has recently defined the Universal Mobile Telecommunications System (UMTS) (see www.umts-forum.org) that relies on some form of CDMA technology to implement the air interface. The form of CDMA used is heavily dependent upon the cellular service provider's spectrum holdings or potential holdings. Most service providers are licensed for both paired and unpaired spectrum. The UMTS standard provides different-flavor CDMA solutions for both cases.

The **UMTS** network architecture defines a core network and a terrestrial radio access network. Together the UMTS terrestrial radio network is known as UTRAN. The two networks (core and UTRAN) are interconnected in the UMTS specification by the Iu interface, and it is also possible to connect the UTRAN network to a GSM/EDGE radio access network (also known as GERAN) as provided in the standard. The integration of GSM and UMTS core network elements allowed by this interconnection will facilitate network development, provisioning of network components, and introduction of UMTS-based services. It is felt that multimode mobile stations for both GSM and UMTS will provide a smooth migration path from GSM to UMTS and 3G services.

The UTRAN system allows for several radio interface models: frequency division duplexing (FDD) or wideband CDMA (W-CDMA) for operation in paired frequency bands, or time division duplexing (TDD) for operation in unpaired bands. At higher layers of the radio network protocols both FDD and TDD are harmonized and the various nodes (either FDD or TDD) are hidden from the core network. The details of FDD or TDD operation are only important to the UTRAN and the end terminals (mobile stations). Therefore, where an operator has paired frequency bands, the operator will implement **W-CDMA** using higher chip rates than cdma2000 (3.84 mcps) over 5-MHz widebands. If a license holder has unpaired spectrum (typical of European and Asian countries), then time division duplex is the optimized solution for this case. With TDD, uplink and downlink traffic can be transmitted on the same carrier frequency but during different timeslots. One version of this radio interface is time division CDMA or **TD-CDMA.** The standard calls for a single carrier with a chip rate of 3.84 mcps in a 5-MHz bandwidth. Another version of TDD is time division synchronous CDMA or TD-SCDMA. This technology combines both TDMA and CDMA principles with other capacity-enhancing techniques. The radio signal is spread by a chip rate of 1.28 mcps and is contained in a 1.6-MHz bandwidth. This gives rise to the possible use of three TD-SCDMA carriers in the same 5-MHz bandwidth as used by TD-CDMA. See Figure 6–36 for a comparison TD-CDMA and TD-SCDMA spectrum usage. Unfortunately, the details of the W-CDMA (similar to cdma2000), TD-CDMA, and TD-SCDMA radio interfaces would fill another book and thus are not discussed any further here.

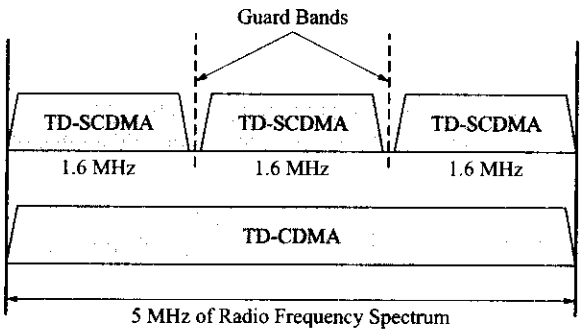


Figure 6–36 TD-CDMA and TD-SCDMA spectrum usage.

QUESTIONS AND PROBLEMS

1. What does the term *cdmaOne* stand for?
2. What is the unique aspect of CDMA technology?
3. What ultimately limits the number of users of a CDMA cellular wireless system?
4. If the basic CDMA signal bandwidth is 1.25 MHz, why are allocated CDMA channels only separated by 50-kHz spacing in Band Class 0?
5. How can additional CDMA system capacity be achieved?
6. What is the function of the interworking function node in a 2G CDMA system?
7. What is the function of the mobile positioning system?
8. In a cdma2000 system, what is the function of the packet core network? What are its main components?
9. What is the function of the home agent in a cdma2000 system?
10. What is the function of the packet data serving node in a cdma2000 system?
11. What are Walsh codes?
12. How does the use of spreading codes increase signal bandwidth?
13. What is the length of the CDMA short PN spreading codes?
14. Describe how different base stations in a CDMA system are able to be differentiated by mobile stations.
15. Describe the generation of the IS-95 CDMA pilot channel.
16. Describe how the CDMA traffic channel is also able to provide power control information to the subscriber's mobile device.
17. Describe how the Walsh codes are used for generating the CDMA reverse logical channel signals.
18. How does the CDMA system differentiate uplink signals transmitted by different mobiles?
19. Of what use is the CDMA frame format in the context of paging channel operation?
20. Describe the use of power control groups on the CDMA reverse traffic channels. What purpose do they serve?
21. Describe the three states that a CDMA mobile may be in while in the attached mode.
22. Describe the steps a CDMA mobile goes through in the initialization state.
23. Describe the three circumstances that put the CDMA mobile into the access state.
24. Describe the CDMA mobile operation known as access channel probing.
25. Describe the CDMA soft handoff.
26. What is the difference between the CDMA soft handoff and the CDMA softer handoff?
27. What measurement does the CDMA mobile use to implement soft/softer handoff?
28. How is the CDMA forward traffic channel power level controlled in a CDMA system?
29. What assumption is made when determining the initial CDMA mobile output power level when attempting a system access?
30. Describe the fast closed loop power control used over the CDMA reverse link.
31. What is the function of CDMA supplementary code channels in IS-95B and cdma2000?
32. What is meant by a CDMA 3X spreading rate?
33. How many additional supplemental code channels may be supported by IS-95B?
34. What is the function of the reverse pilot channel in cdma2000?
35. Describe the most probable conditions for the use of frequency division duplexing CDMA.

CHAPTER 7

Cellular Wireless Data Networks—2.5 and 3G Systems

Upon completion of this chapter, the student should be able to:

- Discuss the factors that have been driving the wireless cellular evolution.
- Discuss the basic principles behind the operation of CDPD.
- Explain the basics of GSM GPRS and EDGE operation.
- Explain the basic operation of CDMA data networks.
- Discuss the evolution of GSM to 3G UMTS.
- Discuss the evolution of CDMA to 3G cdma2000.
- Discuss the modern implementation of the radio access network.
- Explain the basic operation of the SMS family of services.

This chapter provides detailed information about the delivery of data over the two major cellular wireless systems, GSM and CDMA. After a brief overview of the motivating factors driving the evolution of cellular wireless toward 3G, a review of packet data networks is presented. The first form of wireless packet data delivery, introduced to work over 1G cellular and known as cellular digital packet data or CDPD, is examined. The required modifications and additions to the first wireless networks (intended primarily for voice service), necessary to interface with the public data network, are described. Attention is paid to the details of how these two services are able to coexist with one another over the same limited wireless resources.

The steps needed to enable 2G GSM systems for packet data services are outlined next. Details of the general packet radio service (GPRS) run over the GSM air interface are provided and the changes to the wireless network are chronicled. For the GSM case, additional GSM logical channels have been added that provide the GPRS functionality to the system. Finally, the GSM/GPRS/EDGE evolutionary path is completely covered as EDGE technology is introduced. Emphasis is placed on the advantages of the GSM/GPRS/EDGE evolutionary path and the rationale for its adoption by NA-TDMA operators as they migrate to 3G. With GSM packet data transfer technology covered, the focus turns to packet data services over 2G CDMA systems. Again, the necessary system modifications and network changes to provide basic packet data transfer are outlined as are the modifications put in place to increase packet data rates for 2.5G CDMA.

The last few sections of this chapter provide a look at packet data service over 3G wireless networks. Emphasis is placed on the changes occurring to the radio access networks and the types of service that will

be available from these systems. Both UMTS and cdma2000 are examined with an eye to the future when the core networks are predicted to become all IP. The last topic in the chapter deals with the increasingly popular SMS family of messaging systems that is driving the multimedia use of today's wireless cellular phones.

7.1 INTRODUCTION TO MOBILE WIRELESS DATA NETWORKS

The growth of the Internet and its daily use by the average person coupled with the public's desire for anytime, anywhere voice and data communications has been the driving force behind the growth and development of mobile wireless data networks. If one plots the number of Internet Web sites or Internet users versus time, the resulting upward curve is closely matched only by the growth in the number of worldwide wireless cellular subscribers. If desired, the reader may view any number of the previously listed Web sites (i.e., GSM, UMTS, CDMA forums or industry collaborations) that provide impressive, near real-time running totals of existing subscribers to a particular air interface technology and maps of worldwide deployment and coverage areas with detailed information about the service providers, frequency bands used, technology used, and so on. Most cellular industry predictions of future system expansion and total numbers of wireless subscribers are heavily optimistic, with double-digit growth predicted for at least this decade.

What is not so certain, however, are the predictions concerning the user take-up rate for mobile digital data services. Although the initial response for these services has been extremely encouraging in several applications areas (SMS, MMS, etc.), disruptive technologies like wireless local area networks (WLANs) and even newer initiatives like radio LANs (RLANs) and mobile wireless metropolitan area networks (WMANs) have started to cast some doubt as to the eventual shakeout that will occur in this industry. Another critical issue involves the subscriber's end device. The classic cellular telephone itself just does not provide the same experience when browsing the World Wide Web as does the traditional desktop PC or a notebook PC despite efforts to improve this situation through specialized software and mobile operating systems. It has been very difficult to get around the small display screen employed by most low-cost mobile phones. What this problem has spawned is the evolution of the end device. Personnel digital assistants (PDAs) have been around for a number of years and continue to evolve into what are now known as handhelds. Devices in this category are able to provide wireless connectivity either through WLAN hot spots or over nationwide wireless data networks and also provide acceptable-size, high-resolution color screens to improve the delivered data services experience to a more acceptable level. In some cases, PDA devices have incorporated cell phone functionality. At the same time, high-end cellular telephones have been morphing into multimedia infotainment/connectivity devices with the addition of larger, color, high-resolution displays; greater memory capacity and processing power; improved software and operating systems optimized for mobile operation; and one or more color cameras. This new generation of cellular phones is able to allow the user to play games, listen to music, watch MP3 movies, send and display color pictures, and connect to other user devices through both hardwired and wireless connections among other things. This morphing of the end user device is going to continue. One can only predict with certainty that today's end user devices will look like outdated relics by the year 2010. This also applies to today's desktop PC. Many futurists predict its rapid demise toward the end of this decade with a changeover to some morphed version of the notebook/tablet PC with anytime, anywhere wireless network connectivity.

As has been chronicled elsewhere in this text, the first-generation wireless cellular systems were designed for voice traffic. Support for data services over first-generation wireless networks was provided through the use of a modem similar to the classic PSTN modem. Modems that supported the AMPS wireless interface were typically used with a laptop computer by businesspeople on the road. The modem operated over a circuit-switched connection made available through the wireless network connection to the PSTN. This was not a cellular application that enjoyed widespread popularity due to its inherent high rate of cost per minute. Introduced during the early 1990s, **cellular digital packet data** (CDPD) evolved out of a perceived need for

wireless mobile data services. Basically, CDPD is a wireless packet data network that was able to be overlaid on an AMPS network. Supporting data rates up to 19.2 kbps, CDPD was designed for short, bursty type data transactions such as credit card verification, e-mail, and fleet dispatch type services. Later, limited support for short message service (SMS) was introduced into CDPD capabilities. Second-generation cellular systems were designed with data services in mind. Early 2G GSM systems and 2G CDMA systems supported packet data in rates from 9.6 to 19.2 kbps. During the late 1990s (most would say, driven by the Internet), modifications to installed cellular systems enabled so-called 2.5G data rates that included bit rates (not data throughput rates) approaching 115.2 kbps. The industry's push toward higher-rate mobile data services brought with it the ITU specification of universal 3G capabilities and the formulation of the evolutionary path that the industry is presently on to upgrade its systems to provide worldwide 3G service. This chapter will detail the delivery of 2.5 and 3G data services over the most important air interface technologies, GSM and CDMA, and outline the steps that will bring the cellular industry to the inevitable all-IP wireless network.

7.2 CDPD, GPRS, AND EDGE DATA NETWORKS

This section will begin with a short overview of the packet data network and then briefly trace the implementation of first-generation cellular packet data delivery through the use of CDPD technology. Next, second-generation packet data deliver schemes for GSM networks will be examined. This section concludes with a description of the evolution to higher-data-rate 2.5G GSM/GPRS systems and the EDGE standard, a bridge technology, used by GSM/GPRS service providers to afford some basic 3G data service functionality before the eventual system upgrade to a UMTS network.

Overview of the Packet Data Network

A short review of the packet data network is appropriate at this time. Essentially, the packet data network consists of an interconnection of numerous data networks, both public and private, that use packet switching to deliver data to a final destination. The network is set up to deliver data packets through the use of header information appended to the beginning of the data. The packet header typically includes such information as the destination address, the sender's address, and other overhead information necessary for the successful and perhaps necessary timely delivery of the data contained in the packet. Some of this overhead information might also be appended to the end of the packet (thus encapsulating the data). Within the packet data network there are nodes (routers) that connect to other routers and eventually to other packet networks and so on and so forth. The function of these routers is to inspect the packet header destination information and forward or switch individual packets on to the correct router output interconnection as they make their way toward their final destinations (hence the term *connectionless switching*). Numerous types of packet data networks exist, both public and private. As technology has evolved, various protocols (review Chapter 1 and its coverage of the OSI model) have been developed to facilitate the transmission of data over networks utilizing different types of physical media, providing different and ever increasing data rates, dealing with various quality of service (QoS) issues, using different error handling techniques, and interconnecting with other possibly different networks. Furthermore, depending upon the physical scope of the data network (i.e., LAN, MAN, or WAN) many sophisticated transport technologies (Ethernet, ATM, SONET, frame relay, X.25, T-carrier, xDSL, etc.) exist today.

Interestingly, the almost universal use of transport control protocol/ internet protocol (TCP/IP) makes the packet data network transparent to the user and basically hides the network hardware from view. At this point, most consider the packet data network and the Internet one in the same. The wireless packet data network is an extension of the Internet that provides the end user mobility with Internet connectivity in a WAN environment somewhat similar to the untethered environment offered by a wireless LAN.

CDPD

As mentioned before, CDPD was created to provide bursty packet data delivery over the AMPS system. It is able to perform this data service by defining a specific network architecture, a set of protocols, and having a radio interface that is compatible with the AMPS technology. CDPD works by sharing AMPS spectrum (and later on, NA-TDMA spectrum) for both data and voice services. It uses idle time on the AMPS channels to transmit data packets and dedicated spectrum from an NA-TDMA system. It should be pointed out that CDPD can also be overlaid on a CDMA network. The CDPD network architecture is depicted by Figure 7–1.

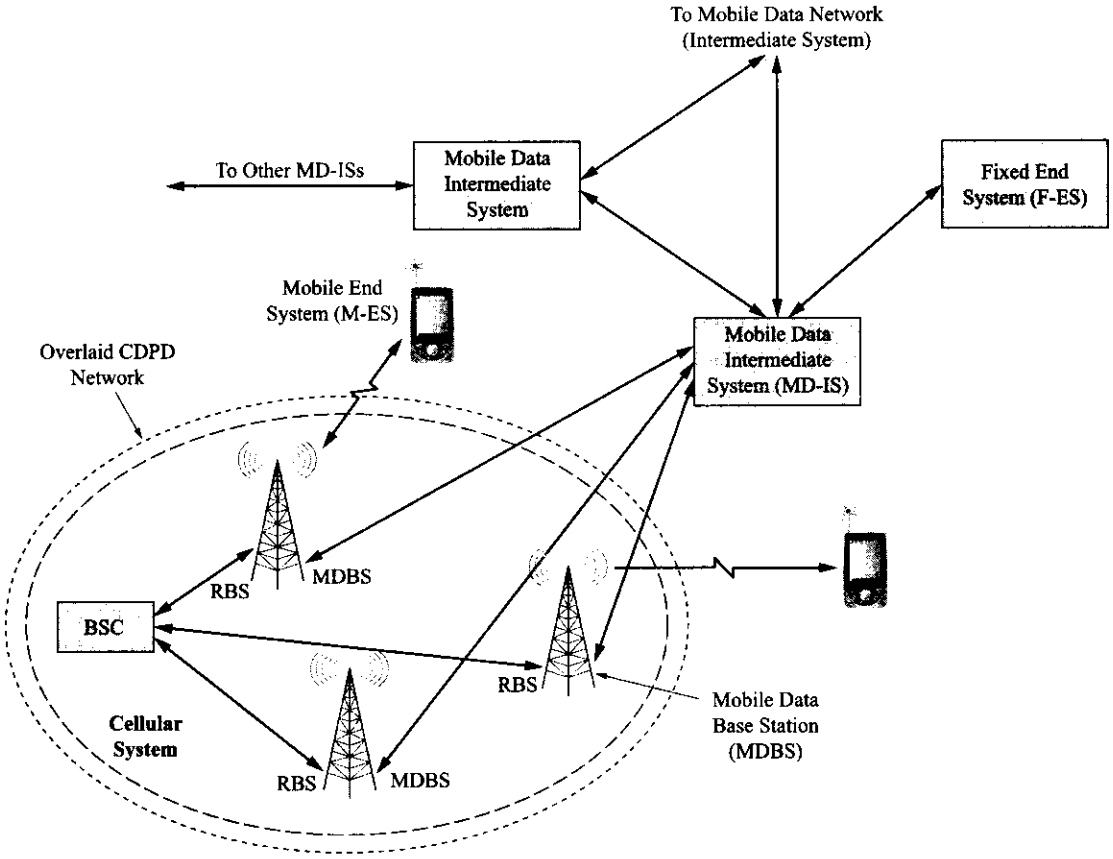


Figure 7–1 Typical CDPD network architecture.

As shown by Figure 7–1, the CDPD network consists of several network elements that provide the functionality necessary for system operation. The basic CDPD network elements are the intermediate systems, the mobile data intermediate system, and the mobile data base stations. The intermediate systems act as gateways between the CDPD network and other packet data networks. Essentially, they are routers that form the CDPD network backbone and provide the necessary connections to other external networks. The mobile data intermediate system provides the interface between the fixed CDPD network and the mobile user of the network. This network element provides the end user with mobility within the system and performs similar functions as the HLR and the VLR in a cellular network. The mobile data base stations provide the radio interface to the end users of the network. Every cell that supports CDPD delivery contains

a base station supporting CDPD operation. Lastly, the CDPD standard specifies two types of end terminal devices, the user mobile end system (M-ES) and a fixed end system (F-ES). The M-ES might be a credit card verification unit installed in a taxi cab, a wirelessly enabled PDA, or some other form of handheld. Since the CDPD system is able to be colocated with the host AMPS system (and other later cellular systems) and share both the antenna and the site, CDPD was viewed as a cost-effective solution to packet data service early on in the evolution of cellular technology.

For proper CDPD operation, the CDPD wireless network must overlay the host AMPS network. This is accomplished through one of several possible scenarios involving the two networks. The AMPS system can dedicate one or more of its available traffic channels for CDPD service. This will certainly provide superior-quality CDPD service; however, if there is not a great deal of CDPD traffic it might compromise the AMPS service. Another possible arrangement is to have shared channels for CDPD and voice traffic with voice calls having the highest priority. In this case, the CDPD network detects unused or idle voice channels and allocates them to packet data calls as needed. If the AMPS system needs the channel for a voice call, it will be relinquished by the CDPD network. The CDPD network will continue the data call if it can detect another idle voice channel within the system and transfer the call to it before the expiration of a system timer. In this case, the performance of the CDPD network depends upon the amount of voice traffic on the AMPS network. A third option is to dedicate a number of the AMPS channels as voice only and then share a number of channels for both voice and data traffic. This option guarantees a certain level of AMPS performance at the expense of the CDPD network. For colocated operation with host NA-TDMA or CDMA networks, the CDPD network usually requires a dedicated allocation of spectrum.

The operation of a CDPD wireless network is very similar to typical wireless cellular system operation. For an M-ES-originated packet data call, the mobile device must acquire a CDPD channel. Depending upon the system setup, either a dedicated CDPD channel will be specified and programmed into the M-ES's memory or the mobile device will need to perform what is known as channel sniffing to find a CDPD-enabled channel. Once a CDPD channel has been acquired by the M-ES it will perform a registration and authentication process with the CDPD network. The CDPD network's versions of the HLR and VLR (located in the mobile data intermediate system) will be updated with the mobile device's present location and required routing information. Once these operations are complete, the M-ES may commence sending and receiving packets over the radio link that has been setup. For an M-ES-terminated packet data call the process is somewhat different. Each MD-IS broadcasts identification information about itself over the forward CDPD radio link. If the M-ES moves from its home MD-IS serving area into a new MD-IS serving area, it will register with the system and hence provide its present location within the system to the network. Packet data destined for the M-ES will be routed to the new serving area and be broadcast over the forward link. All M-ESs within the radio coverage area will receive the data packets, but only M-ESs with valid network identifiers are able to decode them.

If the channel being used for the packet data call is reallocated to a voice call, the mobile again must perform channel sniffing. If successful, the mobile will hop to the newly acquired channel and continue the packet data call. CDPD networks provide mobility to end users. Through a process similar to handoff, the packet data session may be continued as the end user moves about the network's coverage area. This CDPD network operation is known as cell transfer. Finally, the M-ES device may end the data session, at which point the mobile deregisters with the CDPD network. CDPD service may continue to hang on in the near term but will most likely fade away as time passes and newer data services are rolled out (also recall the FCC's mandate for support of AMPS in the United States until 2007).

GPRS

When the second-generation GSM standards were developed, the digital-based GSM system was designed to be an integrated wireless voice-data service network that offered defined data services. Phase 1 of GSM deployment defined both teleservices and bearer services that included short message service, teletex, FAX,

both asynchronous and synchronous data, and synchronous packet data delivery albeit at low data rates by today's standards (9600 bps maximum). Phase 2 of the GSM specifications added enhanced circuit data throughput rates, and Phase 2+ of the standards have addressed the evolution to higher packet data transfer rates. Phase 2+ calls for GSM support for high-speed circuit-switched data (HSCSD), the ability to transfer small data packets over radio interface signaling channels, general packet radio service (GPRS), and enhanced data rate for global evolution (EDGE). This section will discuss GPRS in more detail and the next section will discuss EDGE technology.

GPRS Networks

Although GSM wireless networks have the vast majority of cellular subscribers worldwide, extensive GSM networks have only recently been introduced into the United States. Nationwide GSM/GPRS networks are being rapidly built out by several service providers in the PCS bands (1900 MHz) while other service providers have systems operating at 850 MHz. In a related development, NA-TDMA service providers have deployed GSM/GPRS systems to provide high-speed packet data services to complement their legacy voice service systems (requires a dual-mode handset). The overlay of these new GSM/GPRS systems will gradually reduce the spectrum available for NA-TDMA systems and eventually these service providers will migrate totally to GSM/GPRS/EDGE wireless networks. As always, economics will dictate the speed at which these events happen. However, the process has been set into motion and there appears to be a worldwide commitment by the wireless industry to deploy true 3G service-capable networks during the middle of this decade. The conversion to GSM by the NA-TDMA operators affords them a clearer migration path to 3G than they previously had.

Figure 7–2 shows a typical GSM/GPRS network. The GPRS network runs in concert with a GSM wireless network. A typical GPRS public land mobile network (PLMN) allows a mobile user to roam within the geographical coverage area of the GSM/GPRS system and provides continuous, moderate-speed, wireless packet data service. In the case of a mobile subscriber moving about the system, the GSM PLMN keeps track of the subscriber's location and aids the GPRS PLMN in routing the incoming data packets to the correct serving cell.

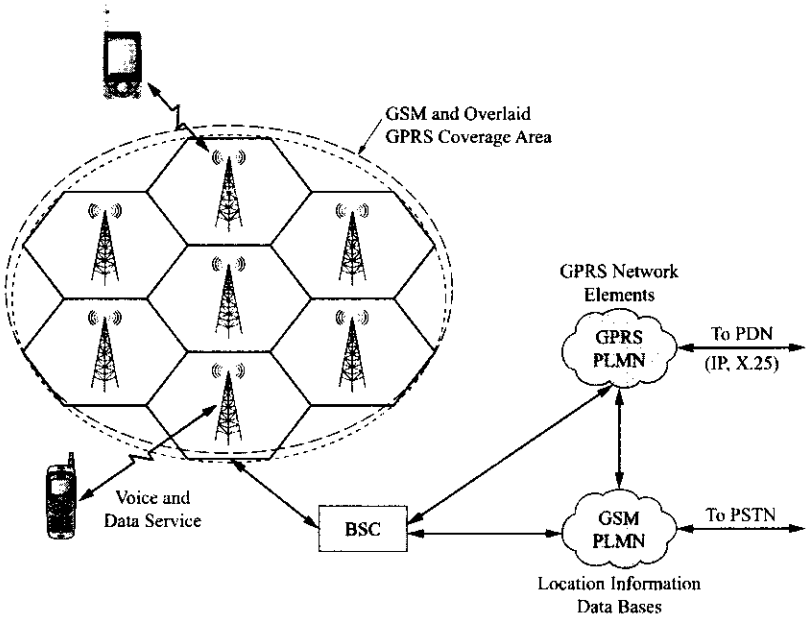


Figure 7–2 Typical GSM/GPRS network.

The GPRS PLMN uses the GSM air interface to provide packet data service to the subscriber and the fixed portion of the network interfaces with the public data network using standard packet data protocols. Network layer protocols like X.25 and IP (Internet protocol) are supported and therefore the end user is able to access Internet Web sites and private enterprise servers via the GPRS PLMN. The GPRS user can also receive voice services via the GSM PLMN. Depending upon the mobile's capabilities, these services may be accessed either one at a time or simultaneously.

The GPRS standard supports many different and useful features: roaming between different GPRS networks, several different connection topologies (point-to-point, point-to-multipoint, etc.), SMS service over packet data channels, different quality of service (QoS) levels, different modes of addressing (e.g., static, dynamic, multiple simultaneous), and security and confidentiality through a GSM-based system of authentication, sophisticated encryption, and a packet temporary mobile subscriber identity (P-TMSI).

GPRS Network Details

A GPRS PLMN is made up of several network elements and various communications links that interface these elements to one another. The GSM standards specify a GPRS network reference model with these network elements and signaling interfaces and their interconnection to the standard GSM network elements. Figure 7–3 depicts the components of a GPRS network and the GPRS logic architecture with some of the signaling interfaces labeled. The key new network elements in the GPRS PLMN are the **GPRS support nodes** (GSNs) of which there are two types. There is a gateway GPRS support node (GGSN) that serves as the gateway between the GPRS network and other packet data networks, and the serving GPRS support node (SGSN) that controls GPRS service in a coverage area. The GGSN is also responsible for routing data to the correct SGSN. All of the GSNs within a GPRS PLMN are interconnected by an IP backbone and perform routing functions specific to the GPRS PLMN.

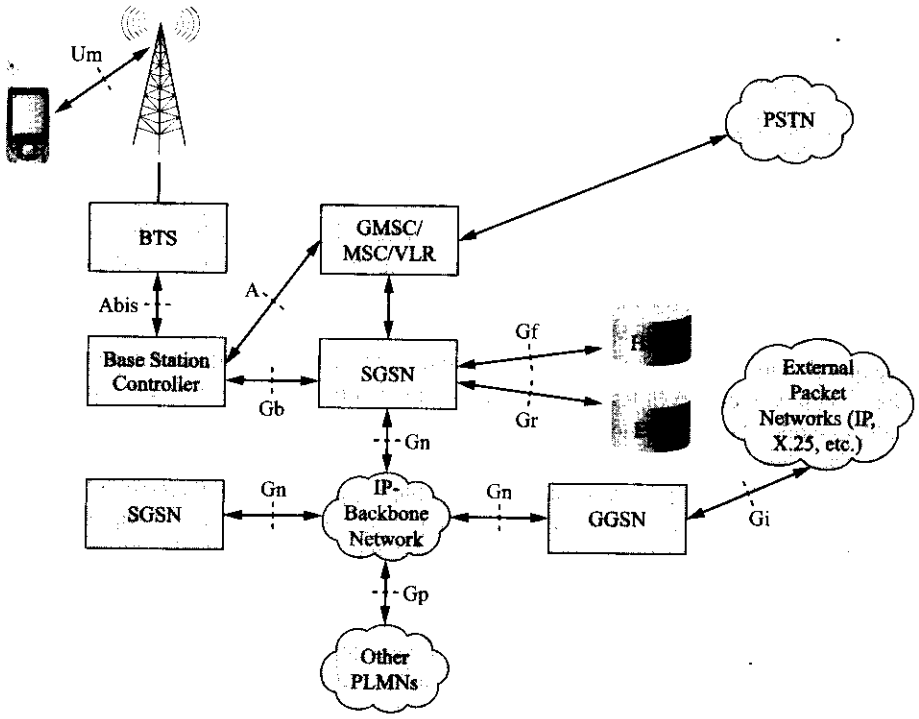


Figure 7–3 GPRS network components.

GPRS Network Elements The gateway GSN serves as the access point to the packet data networks supported by the GPRS PLMN. The primary function of the GGSN is to route packets from the packet data networks to the GSM mobile station. When a mobile station attaches to the GSM network and activates its packet data address, the mobile becomes registered with the GGSN. The GGSN's routing table is updated with the correct serving GSN (SGSN), indicating the mobile's point of attachment. The GGSN also is tasked with performing mobile station address management and activation functions. That is, if the mobile needs a packet data address, the GGSN will provide it and also activate the mobile's address in its routing table. The serving GSN node basically provides a point of attachment to the GPRS mobiles. The SGSN is responsible for the delivery of packets to and from the mobile. To perform this function correctly, the SGSN must be aware of the location of the mobiles attached to it (akin to the function of a VLR). Furthermore, the SGSN is tasked with performing GPRS system security functions (authentication, encryption, etc.), which are performed in conjunction with the HLR of the host GSM system. Both the GGSN and the SGSN are linked to the GSM PLMN and therefore have access to the network elements of the GSM system (MSC/VLR, SMS-GMSC, HLR, etc.), which facilities the performance of their operations. The SGSN is normally connected to the base station system by Frame Relay or some other high speed data transport technology. The SGSN may provide service to multiple base stations thus providing coverage to a group of cells. Lastly, the functionality of the SGSN and the GGSN may be physically combined into a single SGSN/GGSN unit by a wireless equipment vendor.

Within a GPRS PLMN, both the GSM base station subsystem and the mobile stations must be able to cope with GPRS data. The GSM HLR already has the responsibility of keeping track of the mobile subscriber's location within the GSM network and hence within the GPRS network. Therefore, in support of GPRS service, the HLR manages GPRS subscription data that includes mobile roaming privileges, details of QoS-level privileges, and the mobile's static IP or other packet data address information. Other network elements within the GPRS network include an intra-PLMN backbone (high-speed data network). This is a private network for GPRS users. It has the function of connecting multiple GGSNs and SGSNs within the same GPRS PLMN. Additionally, an inter-PLMN backbone is used to connect multiple intra-PLMN backbone networks together through what are known as border gateways.

GPRS Network Layout and Operation

The basic coverage area for the GPRS network is a cell, the same as the GSM network. Additionally, GPRS also defines a routing area somewhat akin to the GSM location area discussed in Chapter 5 (see Figure 7–4). When a GPRS-enabled mobile desires to send data, it searches for the strongest radio base station within its area and then proceeds to perform the necessary steps to set up the packet data call. This process is quite similar to what has been painstakingly laid out in Chapter 5 for a GSM voice call and therefore will not be detailed here. Once attached, the GSM network and hence the GPRS network know the details of its cell location. If the mobile moves around the system coverage area while in the idle mode, it may have to perform what is known as cell reselection (a form of location updating) by choosing a new strongest radio base station. While in idle mode, the GPRS mobile will listen to the base station it is attached to for announcements of any incoming data packets. The process used by the GPRS network to inform a mobile about incoming data packets is known as paging and is very similar to the paging process used by wireless GSM networks. As shown in Figure 7–4 a contiguous group of cells may be grouped together to form a routing area. As explained previously, when attempting to page a mobile that has not been recently active within the network, the use of a larger geographic coverage area during paging can help increase system efficiency by balancing network location updating and paging traffic.

When a GPRS mobile initiates attachment to the GSM system it must also attach itself to a serving GSN (SGSN). The SGSN must determine whether it should allow the mobile GPRS to attach (performs authentication, authorization, and encryption functions) and whether it can provide the QoS levels being requested by the mobile device. Once an SGSN accepts an attachment request, it will keep track of the mobile's location so that it may correctly route packet data to the mobile. If the mobile moves out of the

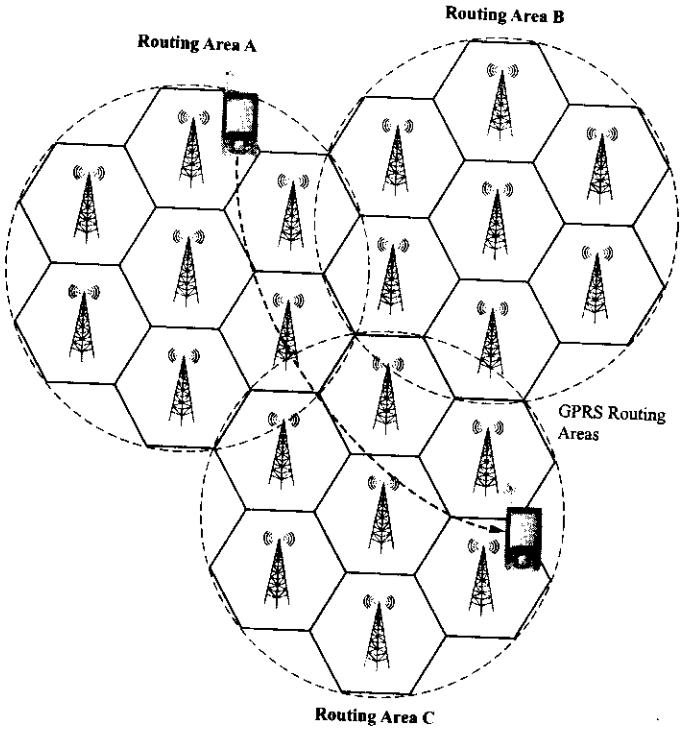


Figure 7–4 GPRS cells and routing areas.

current SGSN's serving area, the mobile must repeat the attachment procedure again with the SGSN serving its new location.

Once the mobile is attached to a SGSN it must activate a packet data protocol (PDP) address if it wishes to begin packet data transfers. Activation of a PDP address sets up the required link or association between the mobile's current SGSN and the GGSN that "anchors" the PDP address. The SGSN and GGSN keep track of this association, known as a PDP context. What this means is that all packet data transfers sent from the public packet data network for that address go to the GGSN. In essence, the GGSN conceals the fact that the subscriber possesses mobility from the packet data network. The subscriber's static IP address (or other PDP address) is normally anchored in the subscriber's home location area. Dynamically assigned IP addresses can be anchored either in the home location area or in a network that is being visited (roaming). It is important to note that a GPRS mobile may attach to only one SGSN but it may have multiple PDP address active at the same time and each of these PDP addresses may be anchored at different GGSNs. Therefore, if a data packet for a particular IP address arrives at a GGSN that does not have an active PDP context for that IP address, the packet is dropped. However, if the IP address belongs to a particular mobile and is anchored at the GGSN receiving the packet, the GGSN will attempt to activate a PDP context with the GPRS mobile.

GPRS Packet Data Transfers

Assuming that a GPRS-enabled mobile has attached to the GPRS network and activated an IP address, it is now ready to begin transferring packet data. Packet data transfers between the GGSN and the GPRS mobile take place using a technique known as "tunneling." In this context, tunneling is the process of encapsulating a data packet so that it may be routed through the GPRS PLMN IP backbone network eliminating the problem of protocol interworking. An example of this process should help the reader understand this technique. Data packets for a certain IP address arrive from the public data network at the GGSN that anchors the IP address. At the GGSN, the data packets are given new headers. Inside the GPRS PLMN IP network,

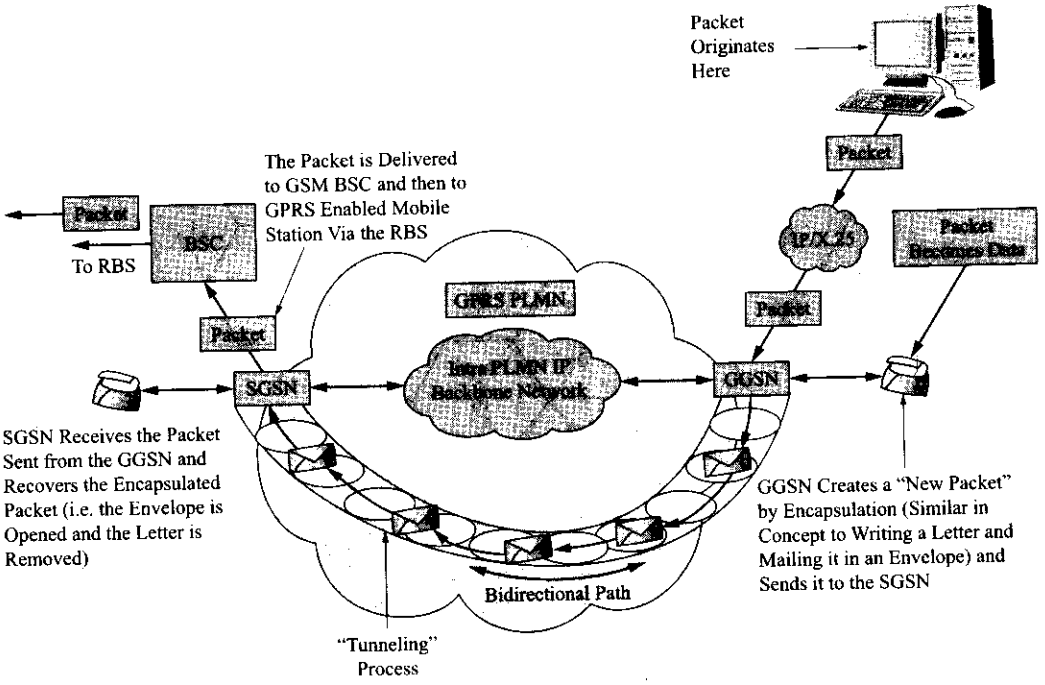


Figure 7–5 GPRS data transfer via tunneling.

these packets are routed based on the new header while the original packet is transported as the data. Once through the network, the new header is stripped of the packet and the data packet is now routed based on the original header. Likewise, packets sent from the GPRS mobile to the public data network must be sent from the SGSN to the GGSN in the same fashion. See Figure 7–5 for a depiction of this process. This use of tunneling within the GPRS network solves the mobility problem and hides the fact that the GPRS mobile is in fact a mobile station.

GPRS Protocol Reference Model

At this time, it should prove instructive to take a look at the various protocols used in the delivery of packet data over the GPRS network. Figure 7–6 shows the GPRS protocol reference model with the various protocol

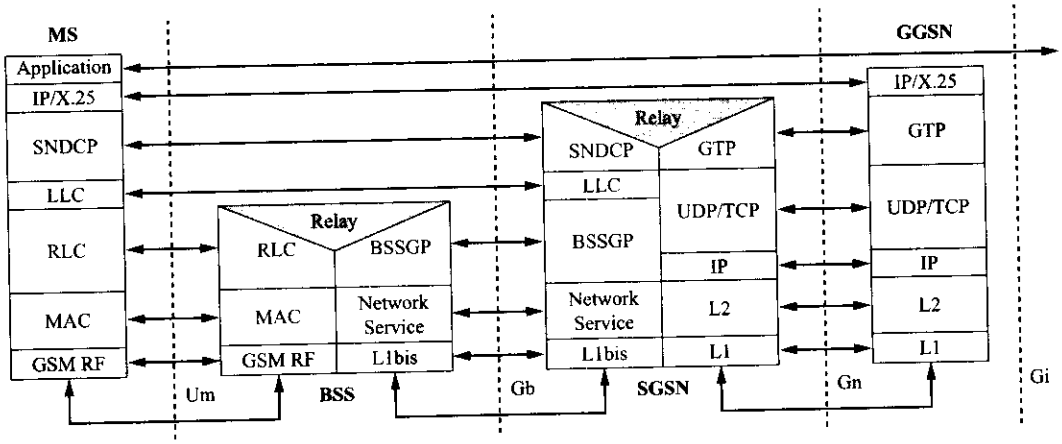


Figure 7–6 GPRS signaling model.

stacks for the different GPRS network elements. The reader might want to refer back to Figure 5–6 to compare it with the GSM signal model for system management signaling. Notice in Figure 7–6 the use of frame relay, a wireline protocol, to provide packet data communications between the base station subsystem (BSS) and the SGSN, the use of the GPRS tunneling protocol (GTP) between the GPRS support nodes (GSNs), the use of TCP/UDP to carry GTP packets between the GSNs, and the use of BSS GPRS protocol (BSSGP) that provides routing between the BSS and the SGSN and QoS management functions. Recall the OSI model and the way information flows between equivalent layers in the protocol stacks. As shown in Figure 7–6, the GPRS system supports IP and X.25 delivery from end to end. Also, both the BSS and the SGSN have two protocol stacks to deal with the distinctly different media and transport technologies used for the air interface, Um, between the mobile station and the BSS, the wireline interface, Gb, using frame relay between the BSS and the SGSN, and the Gn interface that consists of an IP backbone between the SGSN and the GGSN.

GPRS Logical Channels

All wireless cellular systems use a combination of control, signaling, and traffic channels to deliver user traffic and mobility to the subscribers of the system. In Chapter 5, a fairly detailed explanation of GSM logical channels was presented in the context of the TDMA-based GSM air interface. This TDMA-based system, uses eight equal timeslots to provide increased system capacity over a limited amount of radio frequency spectrum. To provide GPRS functionality the GSM system standard has added several additional logical channels to perform the functions necessary to deliver moderate-speed packet data (see Figure 7–7). These new logical channels are packet broadcast control channel (PBCCH), packet common control channel (PCCH), packet data traffic channels (PDTCHs), and packet dedicated control channels (PDCCHs). The function of these new channels will be briefly explained next.

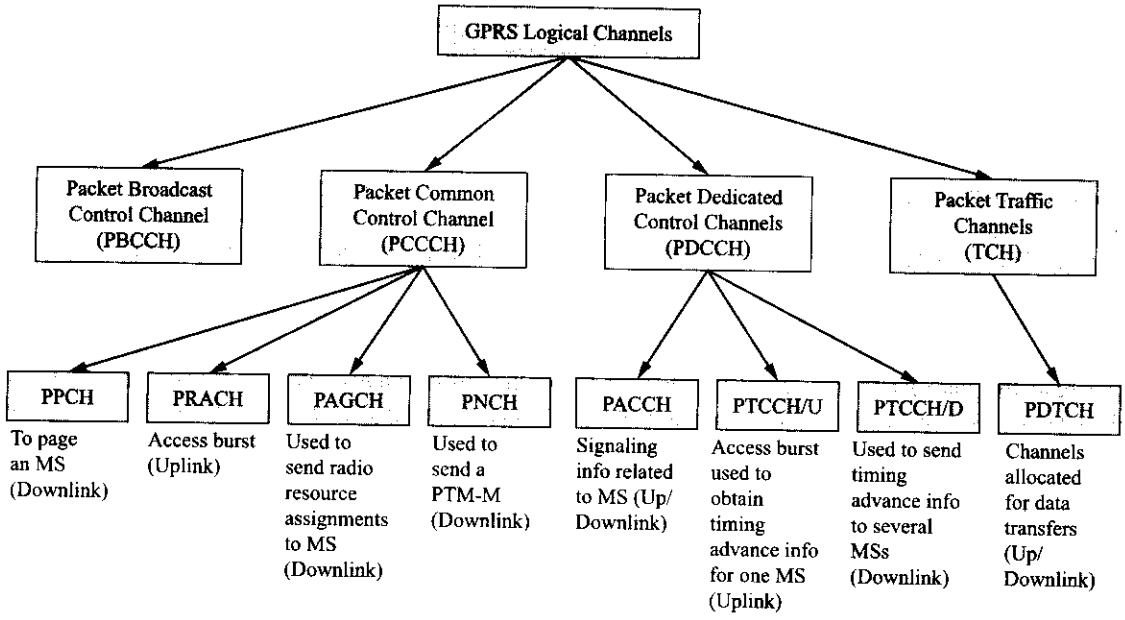


Figure 7–7 GPRS logical channels.

The packet broadcast control channel , used only on the downlink, broadcasts system information to all GPRS mobiles in the cell coverage area. If a PBCCH is not used in the cell, the standard BCCH may be used to broadcast packet data-specific information to the mobiles within the cell coverage range. There are four different types of packet common control channels: the packet access grant channel (PAGCH), the packet

notification channel (PNCH), the packet paging channel (PPCH), and the packet random access channel (PRACH). The PAGCH is used on the downlink to assign radio resources to the mobile during the GPRS call setup. The PNCH is used on the downlink to notify a group of mobiles of a pending multicast before the data is sent. This is known as point-to-multipoint operation. The PPCH is used on the downlink to page a mobile for a mobile-terminated packet data transfer. This channel may be shared for both packet and circuit data services paging operations. The PRACH is used on the uplink by the GPRS mobile to gain access to the GPRS system after receiving a paging message. The packet data traffic channels are used for subscriber packet data transfers in both the downlink and uplink direction. PDTCHs for downlink and uplink are unidirectional and they are assigned separately so as to allow for asymmetrical traffic (typical of the Internet). Lastly, there are three different types of packet dedicated control channels: the packet associated control channel (PACCH), the packet timing advance control channel—downlink (PTCCH/D), and the packet timing advance control channel—uplink (PTCCH/U). The PACCH (both downlink and uplink) is used to transmit signaling information both to and from the GPRS mobile. The PACCH and PDTCH share system resources. The PTCCH channels are used to estimate timing advances for the GPRS mobiles. PTCCH/D is used to transit timing advance information updates to several mobiles whereas PTCCH/U is used to transmit random access bursts to allow estimation of the timing advance for one mobile.

GPRS Physical Channels

The GPRS physical channel structure is identical to the GSM physical channel structure (see Figure 7–8). The timeslot structure used by GSM allows the system to assign a timeslot to either GSM service or GPRS service. A timeslot assigned to GPRS service is called a packet data channel (PDCH).

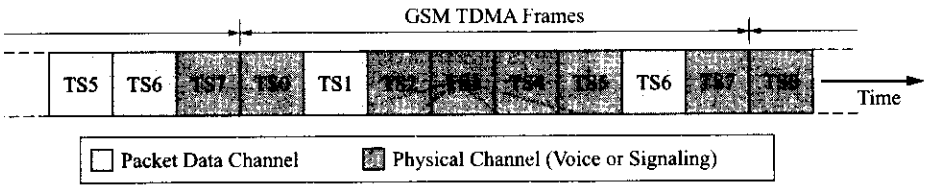


Figure 7–8 GPRS physical channels.

The GPRS standard allows for a flexible allocation of timeslots to GPRS service. In theory all eight timeslots could be assigned for use by the GPRS system. Also, since GPRS traffic tends to vary with time the GSM/GPRS network has the ability to dynamically alter the allocation of timeslots with demand. More detail will be provided about how the system performs this process in Chapter 8. Presently, the GPRS standard calls for four new coding sets (CS-1 through CS-4) that provide a net data rate of between 9.05 to 21.4 kbps per timeslot or a theoretical maximum of 171.2 kbps for all eight timeslots. In practice, the actual packet data transfer rates for operating systems are much less than the maximum since most operators are not yet ready to allocate all eight timeslots to GPRS operation.

As a final note about the GPRS logical and physical channels, it should be pointed out that multiple logical channels may be mapped on to the physical channels in a time-sharing fashion using a superframe structure. This system capability is carried over from the original superframe structure of GSM. Figure 7–9 depicts the multiplexing of the GPRS logical channels on to the GSM/GPRS physical channels.

GSM/GPRS/EDGE Technology

Until recently (the end of 2003) this section of this chapter would have consisted of much more detail about NA-TDMA EDGE technology and its planned two-stage implementation as the pathway to 3G for NA-TDMA service providers. However, at this time the planned migration path for NA-TDMA evolution has taken a radical change in direction. Originally, the United Wireless Communication Consortium's proposal

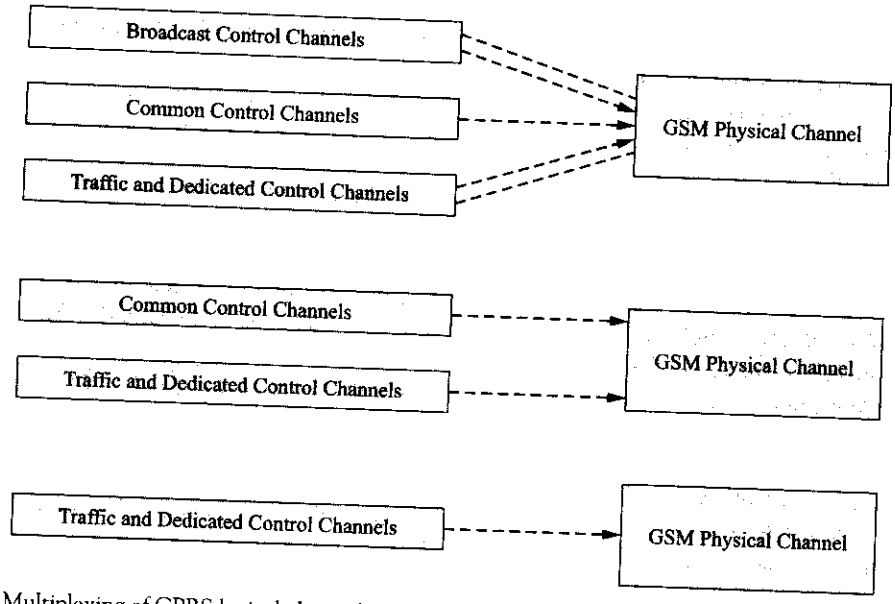


Figure 7–9 Multiplexing of GPRS logical channels.

for a 3G radio transmission technology (RTT), known as Universal Wireless Communication–136 or UWC-136, was seen as the migration path for NA-TDMA. This proposal was accepted by the ITU and would have had several implementation phases. NA-TDMA operators would have first added a reduced bandwidth form of GPRS and then upgraded to a modified version of EDGE known as Compact EDGE (as opposed to ETSI's EDGE standard for GSM) to fit the needs of the NA-TDMA operators. Instead, the major United States NA-TDMA operators have opted to either overlay their networks with GSM/GPRS networks and follow the migratory GSM/GPRS/EDGE path or build out totally new nationwide GSM/GPRS networks with EDGE as the next evolutionary phase. It is reported that AT&T Wireless has initially spent $2.5 billion to roll out its new GSM/GPRS/EDGE network. Effectively, UWC-136 is a non-issue at this time.

One might question why UWC-136 was not adopted by the NA-TDMA operators. A significant part of the answer lies with several recent improvements (AMR codec, frequency hopping, EDGE, etc.) put into operation by GSM systems. These enhancements have improved the spectral efficiency of GSM to such an extent that combined with the well-defined GSM path to 3G and the available 850-MHz spectrum in the United States, GSM/GPRS/EDGE has become an attractive path to follow. Some proponents of GSM would even argue that GSM is one of the most spectrally efficient technologies for wireless access and compares favorably with CDMA technology. These previously mentioned enhancements to the typical GSM wireless system will be addressed in more detail in Chapter 8 under a discussion of typical GSM hardware.

EDGE is the GSM/GPRS follow-on technology that will effectively allow GSM operators the ability to use their present equipment to provide near-3G services. EDGE is really only an enhancement to the radio transmission technology used by the GSM/GPRS system. The GPRS network components and interfaces are still needed for packet data transfers by the system. EDGE uses advance modulation schemes, octantal (eight symbol) phase shift keying (8-PSK), and GMSK to achieve higher data rates. The EDGE standard introduced a combination of new coding sets with adaptive coding and digital modulation techniques to enhance transmission quality by more effectively compensating for the typical radio channel's fluctuating quality (see Chapter 8 for details about the particular challenges presented by the radio channel) and encoding more bits per transmitted symbol. The fundamental GSM radio interface (200-kHz bandwidth and

TDMA and FDMA structure) remains unchanged by either GPRS or EDGE. Additionally, EDGE—like GPRS—may be implemented in existing spectrum allocations.

Table 7–1 shows the net user data rates for GPRS and EDGE per timeslot. The advanced modulation and coding schemes used by EDGE ensure that one timeslot can transport more data bits than can be transported through the use of GMSK modulation alone (CS-4 versus MCS-5). As indicated in Table 7–1, EDGE can employ nine different modulation and coding schemes (MCS-1 through MCS-9) that allow for net bit rates of 8.8 kbps to a maximum of 59.2 kbps per timeslot. Therefore, theoretically, if all eight timeslots are utilized for packet data using MCS-9 coding, a 473.6-kbps data rate per carrier frequency could be achieved with EDGE. In actual practice, the user data throughput would be determined by the number of allocated EDGE timeslots and the modulation scheme employed (MSC-1 to MSC-9). The level of MSC used is determined by the radio channel conditions and is automatically adjusted by the system in response to measured transmission bit error rates. Given the fact that interference levels are highest near cell boundaries, a user close to the cell boundary would tend to experience a higher rate of retransmission requests that would lower overall data throughput. Eventually, the EDGE system would fall back to a lower index MSC-n scheme that employed more robust coding and the overall data traffic throughput would be reduced accordingly. The net result is that a GSM/EDGE user close to the base station will experience the highest throughput rate and that rate will decrease as the user moves away from the base station. Lastly, one should not overlook the fact that the available data capacity per carrier is shared between multiple EDGE mobiles simultaneously contending for the allocated packet data traffic channels.

Table 7–1 GPRS and EDGE net user data rates.

Standard	*Coding Set*	*Modulation Scheme*	*Net Data Rate Per Timeslot in kbps*
GPRS	CS-1	**GMSK**	9.05
	CS-2		13.4
	CS-3		15.6
	CS-4		21.4
EDGE	MCS-1		8.8
	MCS-2		11.2
	MCS-3		14.8
	MCS-4		17.6
	MCS-5	**8-PSK**	22.4
	MCS-6		29.4
	MCS-7		44.8
	MCS-8		54.4
	MCS-9		59.2

Other Aspects of EDGE

One should recall that GSM uses both TDMA and frequency division multiple access (FDMA) and therefore needs to employ frequency reuse to provide the necessary system capacity. As discussed in Chapter 4, the carrier-to-interference ratio, C/I, dictates the minimum reuse number and hence the cluster size to be used. The combined use of frequency hopping, a new adaptive multirate (AMR) codec, and dynamic power control have been able to lower the required C/I ratio in such a manner as to allow GSM systems to employ a reuse number of $N = 3$ or, in some cases, even $N = 1$, for traffic channels. However, the reuse pattern required for GSM broadcast control channels (BCCHs) is not as easily reduced and common practice is to overlay a 4/12 reuse pattern for the BCCHs over the typical $N = 3$ traffic channel pattern. The net effect of the requirement of a 4/12 BCCH cluster is that the minimum spectrum needed to implement GSM EDGE is 2.4 MHz or 2.6 MHz with one guard band. Optimally, to fully reap the benefits of GSM frequency hopping, 3.6 MHz of spectrum is needed. The good news is that the required spectrum does not need to be contiguous and that spectrum at 850 MHz is available in North America on an overlay basis. Until UMTS spectrum is available, GSM EDGE presents a solution to service providers looking to offer more advanced packet data services. Lastly, the EGDE standard supports limited QoS (Classes 3 and 4) and it is really not much more than a software upgrade for the latest model GSM base station systems.

7.3 CDMA DATA NETWORKS

CDMA wireless cellular networks, like GSM networks, are based on 2G digital technology. The first CDMA networks (IS-95A) have the ability to provide both circuit-switched data and packet-switched data to the subscriber. The key network element that was added to the wireless network that supported these functions is known as the interworking function (IWF) (see Figure 7–10). For circuit-switched data transfers, the IWF provides a pool of modems that are allocated on an as-needed basis to the mobile station to enable a data session over the wireless interface. The mobile has the responsibility of configuring the modem and the IWF passes the analog traffic to the PSTN through the MSC. For packet data transfers, the IWF provides the interface between an external packet data network (IP, X.25, etc.) and the wireless system. The IWF transmits digital packet data to both the base station subsystem and the packet network through direct connections. Note that the MSC does not participate in this operation. The next several sections will present more detail about both CDMA circuit and packet data operations.

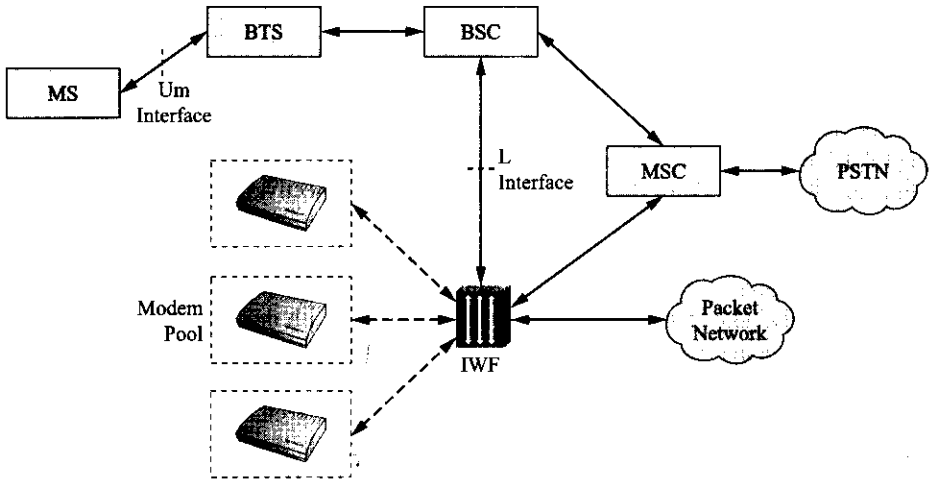


Figure 7–10 CDMA data network components.

CDMA Circuit-Switched Data

The first CDMA standards and successor system upgrades have supported a wide variety of basic circuit-switched data services. These services can be grouped in three broad categories: asynchronous data service, FAX service (both analog and digital), and short message service (SMS). Each service is associated with a service option number (SOn). Asynchronous data service provides the same service as a dial-up wireline modem connection except that it is provided over a wireless network. In this case, the wireless network acts like an extension of the PSTN. Two service options are specified for asynchronous data: Service Option 4 with speeds up to 9.6 kbps and Service Option 12 with speeds up to 14.4 kbps. Fax service can have one of two different flavors. Analog Fax service provides the capability for an office fax machine to connect to a mobile station to both transmit and receive faxes over the wireless interface. Digital fax service allows a laptop connected to a mobile station to send a fax. In both cases, service options provide speeds up to either 9.6 or 14.4 kbps. Short message service supports the transmission of short messages. Two SMS teleservices originally specified for CDMA include cellular messaging teleservice and cellular paging teleservice. Cellular messaging offers short message service to mobile stations. An extensive character set is available with mobile-originated, mobile-terminated, or broadcast (multicast) calls. Cellular paging offers paging-like service to mobile stations (only a limited character set is allowed). For short message service the data rate is 8 kbps for Service Option 6 and 13 kbps for Service Option 14.

For each data session over IS-95A, the CDMA wireless network assigns a single dedicated forward and reverse traffic channel for data transport. IS-95A specified two rate sets (RS1 and RS2). Rate Set 1 supports transmission rates of 1.2, 2.4, 4.8, and 9.6 kbps. Rate Set 2 supports transmission rates of 1.8, 3.6, 7.2, and 14.4 kbps. The maximum rates indicated for the circuit-switched services listed previously only occur for optimum conditions.

The transport of data over the CDMA air interface is supported by radio link protocol (RLP). RLP is designed to provide the reliable transmission of data over the air interface with low error rates. There are presently three versions of RLP. RLP1, used with IS-95A, supports one forward and reverse traffic channel. RLP2, used with IS-95B, supports one fundamental code traffic channel and up to seven supplemental code channels in both directions for high-speed data services. RLP3 is able to support both the IS-95B air interface and cdma2000 3G traffic rates. With RLP3, cdma2000 can support a fundamental channel and/or a control channel and up to two very high-speed (307.2 kbps) supplemental channels and/or up to two very high-speed (3.0912 mbps) packet data channels in the forward direction. In the reverse direction RLP3 supports a fundamental channel and/or a control channel and up to two very high-speed (1.0368 mbps) supplemental channels.

CDMA Packet Data Network

The first CDMA standards also supported enhanced packet data services. These various service options supported packet data over IP/CLNP (Internet protocol/connectionless network protocol) at data rates up to a maximum of either 9.6 or 14.4 kbps (Service Options 7 and 15, respectively). Additionally, the CDPD protocols were supported by Service Options 8 and 16 at the same maximum rates. Later on, the IS-95B upgrade to CDMA specified (what was then considered) high-speed packet data rates that were based on enhancements made to the CDMA air interface. IS-95B allowed the subscriber to be allocated up to eight traffic channels simultaneously. The service options (22–29) associated with this packet data service allowed from one to eight channels at a maximum of 9.6 or 14.4 kbps to be used at the same time by a single user for data transmission. The 14.4 kbps rate per channel yields a maximum possible packet data rate of 115.2 kbps for IS-95B.

The architecture for these enhanced data services is identical to that used for CDMA circuit-switched data services (refer back to Figure 7–10); however, the IWF does not interact with the MSC. Instead, the IWF acts like a gateway to the external packet network or networks as the case may be. The IWF is responsible for the proper protocol conversion between the CDMA wireless network (can be frame relay, T1-carrier,

or Ethernet) and the external packet data network (typically, ATM, Ethernet, or SONET). The CDMA network can support simultaneous voice and packet data traffic. As mentioned in the prior section, radio link protocol is used for packet data transport over the air interface once the radio link has been established. RLP3 is designed to support reliable packet data transmission over the air interface and supports both IS-95B and cdma2000 systems. RLP is a negative acknowledgement (NAK)-based protocol. As such, the receiving end of the link only requests retransmissions of lost frames (effectively increasing the data transfer rate). RLP frames are given sequence numbers and are assigned a priority level by RPL to increase the efficiency of the data transmission process. Also allowed by RLP is the transmission of data in either encrypted or nonencrypted format. The transformation of IS-95B to cdma2000 will be covered in Section 7.5.

7.4 EVOLUTION OF GSM AND NA-TDMA TO 3G

The evolutionary path for GSM/GPRS/EDGE operators to 3G is fairly well laid out at this point. The Third Generation Partnership Project (3GPP) industry collaboration has been working on harmonized standards since approximately 1999 and has specified many of the details of the third-generation universal mobile telecommunication system (UMTS). The first release of the UMTS specifications (Release '99) has been followed by numerous updates and several new "releases" that document improvements and enhancements to the many aspects and elements that make up the UMTS. It should be noted that the UMTS specification is considered a work in progress and will be constantly updated as time goes forward and technology evolves. During the same time period, the plans for UWC-136, the 3G upgrade path for NA-TDMA, were abandoned for the reasons laid out in the section of this chapter on GSM/GPRS/EDGE. At this time, the upgrade path for NA-TDMA is the same as that for GSM/GPRS/EDGE, once an operator overlays its legacy NA-TDMA system with GSM.

High-speed Internet access is driving the wireline, broadband cable, wireless, and, to a much lesser degree, satellite telecommunications industry today. The specifications for 3G wireless emphasize the delivery of high-speed data services and QoS levels that can deliver real-time data over the air interface. The Internet has been accepted as the network of the future. The legacy circuit-switched networks built and maintained by the Bell system and its successors will hang on for quite some time from now into the future; however, new high-speed applications will be delivered over IP-based networks. The delivery of applications with rich multimedia content, information, and entertainment will occur over high-speed IP delivery platforms and, as technology improves, Voice over IP (VoIP) will become commonplace. These changes are driving the wireless industry to eventually migrate to an all-IP wireless network. In an effort to provide a path for GSM operators to this future network, in as least a disruptive fashion as possible, several intermediate steps have been formulated.

The first step in this migration process is to define and implement a standard for a GSM/EDGE radio access network (GERAN). This step allows a GSM operator to interconnect to an UMTS core network and thus enable the GERAN network to become a UMTS RAN that can support 3G services. The next section will take a look at the GERAN, UTRAN, and UMTS network architectures in more detail.

GERAN, UTRAN, and UMTS

For comparison purposes, Figure 7–11 shows a simplified version of the GSM/GPRS/EDGE network architecture. It consists of both a base station subsystem and a core network that connects to the PSTN/ISDN and to various packet data networks. The UMTS architecture is shown in Figure 7–12. It consists of both GERAN and UTRAN air interface (radio access) networks and a core network. The UMTS network also connects to the PSTN/ISDN and various packet data networks through its core network. The motivation behind the 3GPP's standardization of GERAN is to align GSM/EDGE services and to be able to interface GERAN with the 3G UMTS core network. For the GSM operators this allows them to offer 3G services over present spectrum allocations. Note that UMTS is currently intended to be used in designated

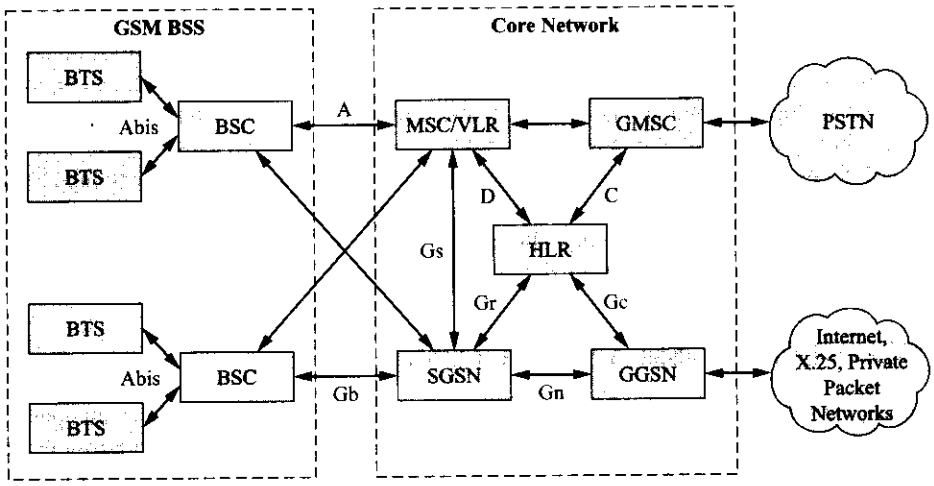


Figure 7–11 GSM/GPRS/EDGE network architecture (Courtesy of ETSI).

UMTS spectrum that may not yet be available in various locations around the world. The UMTS terrestrial radio access networks (UTRANs) have already embodied the changes necessary to interface properly with the UMTS core network.

GERAN System Architecture

The **GERAN** specification allows support for all QoS classes defined for UMTS, it provides support for the AMR codec, and it allows for seamless services to be provided across both UTRAN and GERAN for both circuit-switched and packet data services. Figure 7–13 depicts the GERAN reference architecture. As can be seen in Figure 7–12 and Figure 7–13, to connect to the third-generation UMTS core network or the UTRAN network the lu interface specified for UMTS must be used by the GERAN. Actually, there are several versions of the lu interface. The lu-cs interface is used to connect the GERAN to the circuit-switched portion of the core network and eventually to the PSTN. The lu-ps interface is used to connect to the packet-switched side of the core network and eventually to the packet data network or networks as the case may be. The lur-g interface interconnects the GERAN and UTRAN networks together. One can also

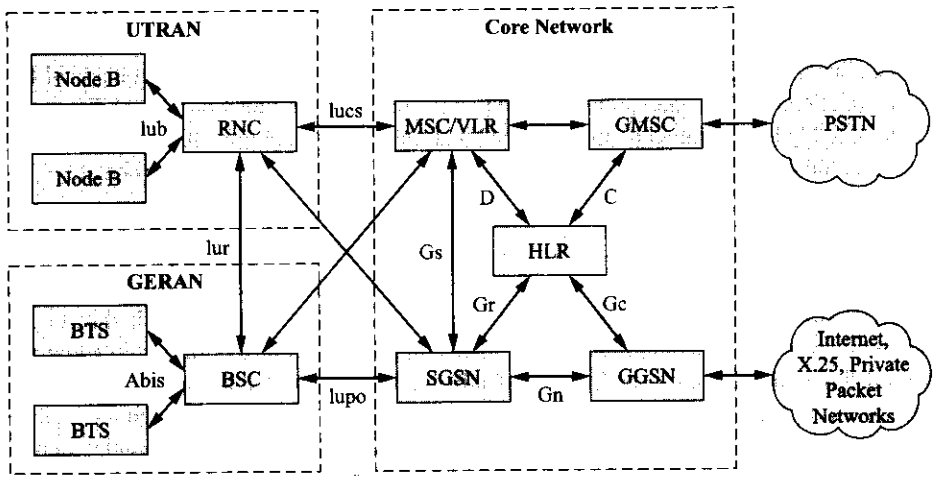


Figure 7–12 UMTS network architecture (Courtesy of 3GPP).

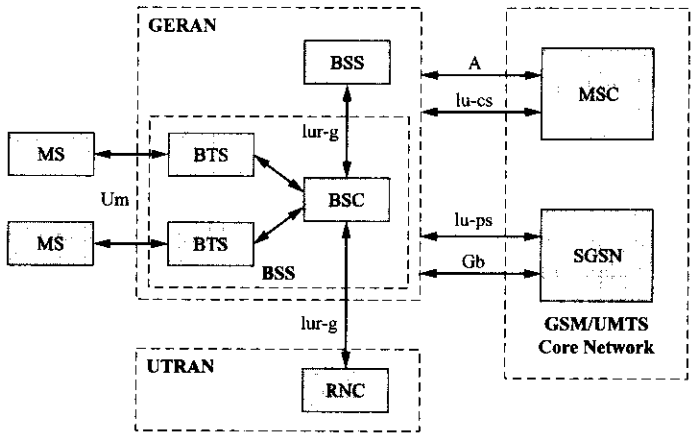


Figure 7–13 GERAN reference architecture (Courtesy of 3GPP).

see from Figure 7–13 that the GERAN specification allows for continued support for legacy 2G GSM/GPRS services over the preexisting A and Gb interfaces; however, only QoS Classes 3 and 4 are supported (more on this later). EDGE provides the increased 3G data rates for GERAN whereas several enhancements to radio link protocol layers will provide the needed QoS level support. Additionally, use of the AMR codec, enhanced power control, and new GSM frequency hopping algorithms will serve to enhance the operation of the GERAN physical layer. This planned migratory path to UMTS is likely to be followed by many service providers.

UTRAN and UMTS

The universal mobile telecommunications system (UMTS) network architecture depicted in Figure 7–12 shows a core network, a UMTS terrestrial radio access network (UTRAN), and a GSM/EDGE radio access network (GERAN). Figure 7–14 shows a more detailed view of the UTRAN connected to both

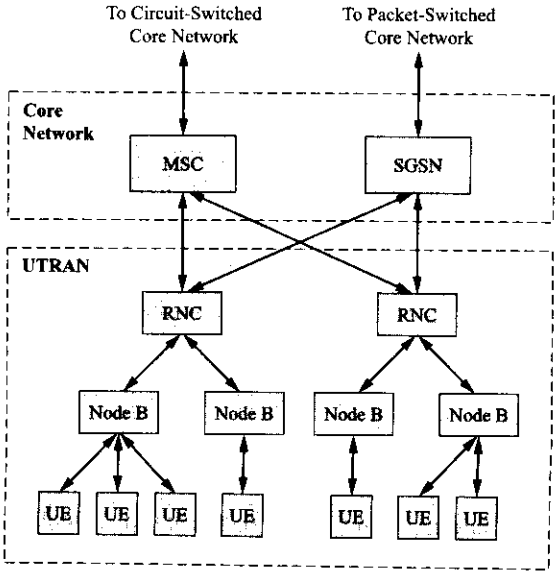


Figure 7–14 UTRAN network connected to circuit-switched and packet-switched networks (Courtesy of 3GPP).

circuit-switched and packet-switched networks within the UMTS core network. The use of wideband CDMA (W-CDMA) technology over the air interface will fully satisfy the present IMT-2000 3G data transfer rate standards and also provide service-independent operation. This last feature is important because it allows for a mixture of services and a flexible introduction of new future services. This service independence is enabled by the lu interface. The lu interface is designed to provide radio access bearers (RAB) that provide bearer services through the radio access network.

Each radio access bearer is associated with a set of attributes that allows it to match the service request and provide the requested QoS level. Presently, there are four UMTS basic QoS levels that correspond to classes of service: Class 1 represents real-time conversational traffic (VoIP) and requires low jitter and delay, Class 2 represents real-time multimedia streaming (MP3) and requires low jitter and modest delay, Class 3 represents interactive services (Web browsing, database retrieval, etc.) and requires modest delays, and Class 4 represents what are known as background services (e-mail, SMS, MMS, etc.) and has no delay guarantees. Note that the term *jitter* used in this context refers to the strict or proper ordering of data packets.

Referring back to Figure 7–14 one notes that the function of the GSM base station controller (BSC) has been replaced by the radio network controller (RNC) in the UTRAN, and GSM radio base stations (RBS) have become Node Bs. The UMTS standard calls for the RNCs to perform the following tasks: manage the radio access bearers for transporting end user data, manage and when possible optimize radio network resources, control end user mobility, and to maintain radio links. The RBSs or Node Bs provide the actual radio resources for the system. The interface between the RNC and the core network is the lu interface, between the RNC and Node B the lub interface, between RNCs the lur interface, and between the user equipment (UE) and Node B is the Uu interface.

The **UTRAN** system is designed to efficiently handle many different traffic forms over the same air interface simultaneously and in any mix of voice and data. A comprehensive channel structure has been defined for the radio interface consisting of dedicated channels that may be assigned to only one mobile at a time, shared channels that are used for packet data transfer and can be assigned to a subset of mobiles at any given time, and common channels that may be used by all mobiles within the cell coverage area. Furthermore, UTRAN can be implemented in several different radio interface modes. The frequency division duplexing (UTRAN FDD) mode employs W-CDMA for operation in paired frequency bands and the time division duplexing (UTRAN TDD) mode employs either time division CDMA (TD-CDMA) or time division synchronous CDMA (TD-SCDMA) for operation in unpaired frequency bands. Refer back to Section 5 of Chapter 6 for more detail about these forms of CDMA.

Further evolution of UMTS will occur for both the core network and the RAN. The evolution of the core network to an IP-based core network will gradually occur as other enabling technologies such as IP over wavelength division multiplexing mature and are deployed within the public packet data network. More details about the IP-based core network are provided in Chapter 12. In the most recent (as of this writing) 3GPP Release 5 update, high-speed downlink packet access (HSDPA) provides improved support for best-effort UMTS services. This enhancement to all wideband modes of UMTS CDMA enables user downlink speeds of from 8 to 10 mbps. These higher data rates are achieved by using a higher-level digital modulation scheme, sixteen (symbol) quadrature amplitude modulation (16-QAM), rapid adaptive modulation and coding, and fast scheduling of users over a new high-speed downlink shared channel (HS-DSCH). These are but only a few examples of the changes that are forthcoming in the world of UMTS 3G wireless that will eventually evolve to provide 4G functionality.

7.5 EVOLUTION OF CDMA TO 3G

CDMA wireless technology was introduced in Chapter 6 of this text. In that chapter, basic CDMA wireless system operation, the details of CDMA downlink and uplink logical channel functions, and basic CDMA frame structures were outlined. Additionally, enhancements to 2G CDMA (2.5G) were discussed and a great deal of detail about 3G CDMA (cdma2000) channel structure and cdma2000 system evolution was

presented. As was the case with 3G UMTS, the Third Generation Partnership Program 2 (3GPP2) industry collaboration has been actively developing the 3G standards for cdma2000. Their work is very similar in nature to that being done by the 3GPP group and will also continue on for some time to come. The evolutionary steps to 3G CDMA as laid out by the 3GPP2 group have been presented in Chapter 6 and elsewhere in this text. Therefore, at this time, the focus of this section will be on the constantly evolving structure of the cdma2000 radio access network (RAN) as it moves toward an all IP-core.

The cdma2000 RAN (C-RAN) as implemented by a major CDMA equipment vendor is shown in Figure 7–15. The radio access network is built around interoperability specifications (IOS) for cdma2000 access network interfaces as defined by the new cdma2000 standards. The cdma2000 RAN uses IOS/IS-2001 compliant interfaces to the MSC and the packet data service node (PDSN), an additional network element that complements the IS-95 CDMA interworking function (IWF) node. The C-RAN base station controller (BSC) is connected to the circuit-switched portion of the core network by an A1/A2/A5 interface, to the packet-switched portion of the core network by an A10/A11 interface, to the radio base stations (RBSs) within the C-RAN by the Abis interface, to other BSCs via the A3/A7 interface, and finally, the radio base station to subscriber device interface, or the air interface, is known as the Um interface. In cases where two or more interface designations are listed, this indicates both signaling and data interfaces coexist.

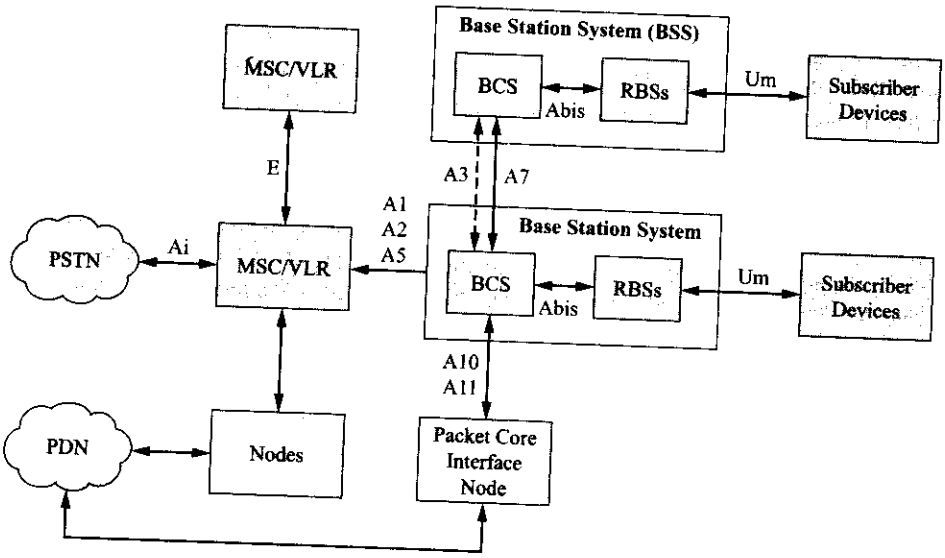


Figure 7–15 Cdma2000 radio access network (C-RAN) (Courtesy of Ericsson).

Cdma2000 RAN Components

The base station controller in cdma2000 performs the same complementary functions as the radio network controller in the UMTS network (i.e., manage the radio access for transporting end user data, manage and radio network resources, control end user mobility, and manage radio links). Additionally, in cdma2000 the BSC provides interfaces to the RBSs, the radio network management (RNM) element, and packet data nodes. An additional element, the packet control function (PCF), has been added to the cdma2000 RBS to provide the RAN-to-PDSN interface. The PCF is responsible for managing packet data service states, relaying packets between the subscriber device and the PDSN, PDSN selection, supporting handovers, and buffering packet data received from the PDSN for mobiles in the dormant state (more about this shortly). An additional interface, A8/A9, has been defined between the RBS and the PCF even though the RBS and the PCF may be housed in the same cabinet. As in UMTS, the cdma2000 RBSs provide the actual radio resources for the system and also play a role in maintaining radio links to subscribers. In cdma2000, the

combination of the BSC and the RBSs it serves are also known as a base station subsystem (BSS). Typically, the RBSs and the BSCs contain all the necessary functions for their own management. Another important element in the C-RAN is the RNM (discussed in Chapter 6) that supports cdma2000 operations at the radio access network level.

Cdma2000 Packet Data Service

This last section devoted to 3G CDMA will take a closer look at the steps and operations that are involved in a packet data session over cdma2000. Four system activities will be addressed: packet data call setup, session data rate allocation, session mobility management, and session activity states. In each case, the basic operations of the system will be chronicled and related to the functions performed by the C-RAN elements.

Cdma2000 Packet Data Call Setup

What happens when a cdma2000 mobile user initiates a packet data call? To the system, the steps are very similar to those required for a voice call. Basically, there are two tasks required to establish the packet data session. The system must first allocate radio resources to the user and then the system must establish a PDSN link and point-to-point protocol (PPP) session. Figure 7–16 illustrates the process. The user dials the appropriate number and presses send. The mobile station transmits an origination message that contains the packet data service option number (e.g., Service Option 33 for 144-kbps packet data service), which is relayed to the BSC (Step #1). The BSC sends a connection management service request message to the MSC (Step #2). If the request comes from an authorized user, the MSC response to the request with an assignment request message to the BSC (Step #3). The BSC allocates the required radio resources and once the radio link has been established, the BSC sends an assignment complete message to the MSC (Step #4). At this point, the BSC generates an A9-setup-A8 message to the PCF that begins the process of setting up a data session with the PDSN (Step #5). The PCF responds to the BSC with an A9-connect-A8 message (Step #6). To initiate the setup of an A10 connection to the PDSN, the BSC/PFC sends an A11 registration request message to the selected PDSN (Step #7). The PDSN validates the request and returns a registration reply message back to the BSC/PCF (Step #8). Finally, with the A10 connection operational, link layer and network layer frames are able to be passed in both directions. At this point, a PPP connection is in place between the originating subscriber device and the PDSN (Step #9). The user can now communicate over the Internet or another packet data network.

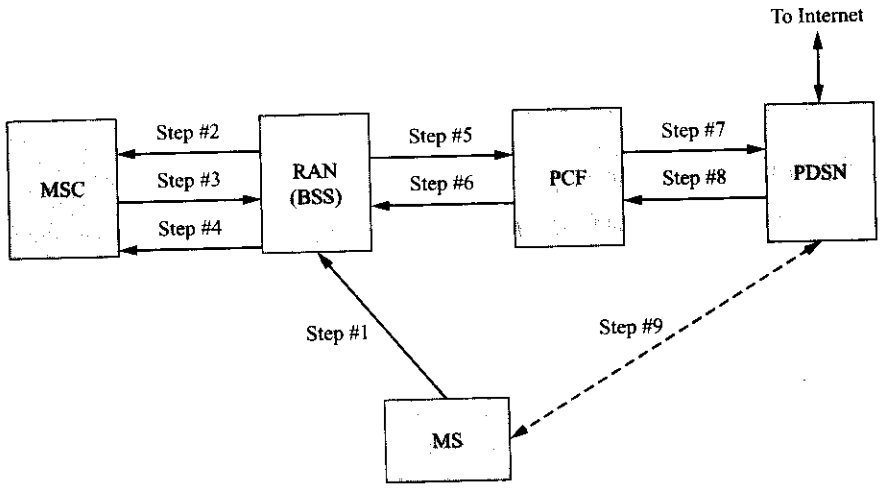


Figure 7–16 Cdma2000 call setup.

Session Data Rate Allocation

Once the user's PPP session has been setup, the C-RAN will setup the appropriate radio links for the packet data call. Fundamental and supplemental channels (if necessary), with the appropriate rates, will be selected by the system. This selection process involves several steps. The C-RAN checks the packet sizes and the packet buffer contents to determine the need for a supplemental channel for data transfer to the mobile. The C-RAN will not setup a supplemental channel unless a certain packet threshold is exceeded or the mobile has requested one. If the use of a supplemental channel is justified by the system, the BSC will setup the channel at the highest data rate allowed or the highest data rate for which resources are available. The setup of the forward supplement channel (F-SCH) and the determination of the maximum data rate to be used is determined by system measurement of the channel conditions for the user's radio link. A threshold level for satisfactory channel conditions is defined for each possible data rate. Note that presently only data rates of 2X, 4X, 8X, and 16X the base rate of 9.6 kbps are allowed over the supplemental channel in the 1xRTT specification. Transmission over the F-SCH continues as long as the channel quality is satisfactory and as long as enough packet data continues to be transmitted. Deallocation of the F-SCH occurs if the channel conditions deteriorate to such an extent that the frame error rate exceeds a threshold value. Furthermore, handover techniques for the F-SCH are also slightly modified to conserve radio resources and to ensure that the best F-SCH radio link is always used.

Session Mobility Management

If the user is moving about the system coverage area during a packet data session, the network is tasked with maintaining the radio link and the connection to the packet core network. This mobility management function must be performed regardless of the state of the mobile (i.e., active or dormant). All of the different types of handover scenarios supported for circuit-switched traffic are also supported for packet data sessions. However, there are some differences that will be addressed now. If the present F-SCH serving sector is no longer the best serving sector, then the BSC will redirect the mobile to the better serving sector. In the case of this intra-BSC sector selection, all other existing links remain unchanged while the original F-SCH channel is deallocated and the new F-SCH channel is allocated to the packet data call. If an intra-BSC hard handover is required, the fundamental channel is deallocated and a new fundamental channel is allocated on the new CDMA channel. The F-SCH and/or R-SCH will be deallocated and a new F-SCH and/or R-SCH will be reallocated once the handover has taken place. It is important to note that during this process the PPP session between the mobile and the PDSN remains intact. The last case to consider is the inter-BSC hard handover. For a hard handover between BSCs, the same PDSN may or may not serve both BSCs. For the case of different PDSNs, the mobile station may continue to use the same IP address if the system supports mobile IP (MIP). In this situation the packets will be either forwarded or tunneled to the serving PDSN by the packet core network. If the same PDSN serves both BSCs there is no problem. While the handover occurs, the system maintains the connection between the mobile and the PDSN until the new PCF attaches to the PDSN. To summarize, the mobile continues to use the same IP address, deallocation and reallocation of channels occur as in the intra-BSC hard handover, and the new BSC becomes the anchor for the call.

Session Activity States

If a long enough period of inactivity occurs during a packet data session, the mobile will change from an active state to a dormant state. This process can be initiated by either the mobile or the BSC through a release order message, which will cause the traffic channel radio link to be torn down. However, the PPP session between the mobile station and the PDSN is maintained. This always-on mode ensures a rapid reconnection when the mobile returns to the active state from the dormant state. Handovers, while the mobile is in the dormant state, are handled by the network the same as idle state handovers; however, the PPP session between the mobile and the PDSN is maintained as the mobile changes PCFs. To transition

from the dormant to the active state, either the mobile, via an origination message with the correct service option code, or the BSC, with a paging message, can reactivate the mobile. In each case, the PPP session does not need to be reestablished since it is already on.

7.6 SMS, EMS, MMS, AND MIM SERVICES

Short message service (SMS) was first introduced commercially in 1995 and by the early 2000s over a billion SMS messages per day were being sent. There are several theories as to why SMS and various related successor services have become so popular. Most of the explanations offered include references to popular youth culture and next-generation users that have even devised their own abbreviated text language. Suffice to say, SMS has heralded a suite of new applications for mobile phones that will continue to grow as 3G is deployed and mobile device technology matures. This section will outline the basic operation of SMS service and then introduce enhanced message service (EMS), multimedia message service (MMS), and other similar related store and forward messaging technologies.

Introduction to SMS

SMS service was created as part of the Phase 1 GSM standard. An excellent Web reference about its history and other M-services initiatives exists at www.gmsworld.com. The reader should refer back to Figure 5–4, which depicts the architecture of a GSM system. Shown in the figure is an SMS-gateway MSC (SMS-GMSC) and an SMS-interworking MSC (SMS-IWMSC) with associated communication links to the GSM wireless network HLR and the MSC/VLR. These are the components that are required by the GSM network to provide SMS service functionality. A short text message consisting of up to 160 alphanumeric characters may be sent or received by a short message entity (SME) via a service center (SC). An SME is a device capable of sending and receiving short messages. The SC acts as a storage/forward center for short messages. The SC can be located within an operator's cellular network; however, it is not included in the GSM specifications. The SMS support elements necessary for a CDMA system are similar.

Figure 7–17 shows the flow of a mobile-originated SMS message. The mobile station sends a service request message to the MSC/VLR with the service type indicating an SMS message (1). The message itself is carried via a control protocol (CP) data message from the mobile to the MSC/VLR. The MSC/VLR returns a CP acknowledgement message to the mobile (2). The VLR checks on the mobile's SMS permission/authorization status and then the MSC forwards the message to the SMS-IWMSC, (3) which in turn forwards the message to the SC (4). A delivery or failure report is sent back through the network to the MSC/VLR from the SMS-IWMSC depending upon the results of the operation (5 & 6). This report is eventually sent to the mobile and the mobile acknowledges it in turn (7).

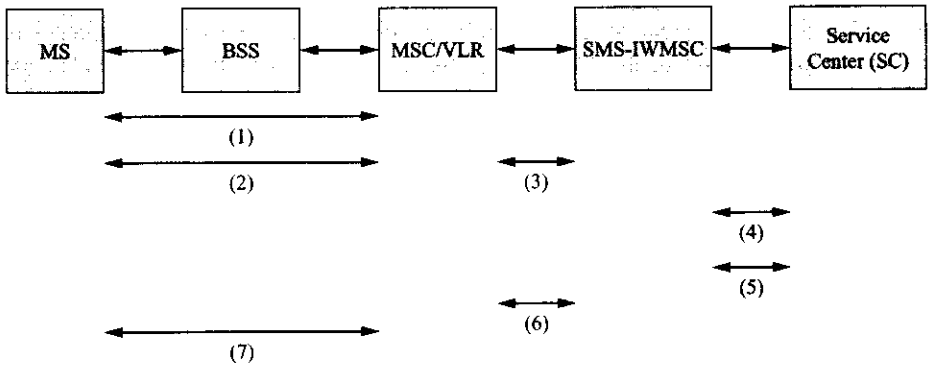


Figure 7–17 Operations involved in a mobile-originated SMS message transfer.

For a mobile-terminated SMS transfer the message is always routed from the SC to the SMS-GMSC (see Figure 7–18). The SMS-GMSC requests routing information from the HLR. If SMS service is permitted to the mobile, the HLR provides the SMS-GMSC with the correct address information for the serving MSC. The SMS-GMSC forwards the message to the serving MSC from which point it is delivered over the air interface to the mobile in standard fashion. Messages are returned to the SMS-GMSC and passed on to the SC indicating success or failure in the delivery of the message. If the target mobile is not active or out of range, a process is put into place to update a message waiting list in the HLR. If the mobile becomes active or performs a location updating function, the HLR sends a message back through the network that alerts the SC that it should attempt the message delivery again.

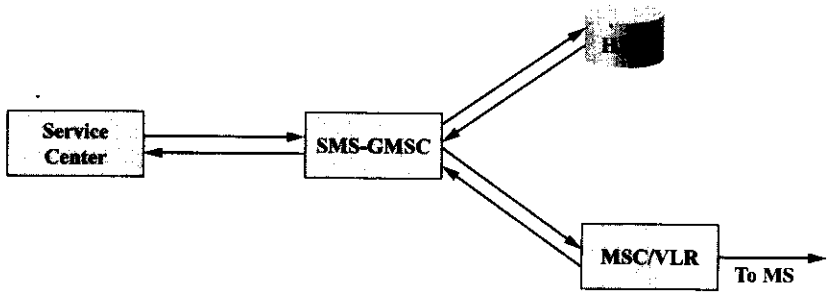


Figure 7–18 Operations involved in a mobile-terminated SMS message transfer.

Introduction to EMS, MMS, and MIM

Early on in the development of 3G specifications, both the 3GPP and the 3GPP2 industry groups embraced an enhanced version of SMS known as **enhanced message service** (EMS). EMS added rudimentary multimedia functionality to SMS in the form of ringtones, operator logos, picture messages, and both animated and static screen savers. In other words, images, melodies, and simple animations are supported by EMS. It was not long before the wireless industry (under 3GPP and 3GPP2) developed new specifications for the next evolutionary step in store-and-forward messaging. **Multimedia message service** (MMS) was soon adopted with the ability to send and receive content consisting of digital audio, video, color images, and sophisticated animations. Today, many mobile phones are MMS enabled with high-resolution color displays and one or more color cameras. Most observers familiar with world of cellular wireless believe MMS provides a service environment that will facilitate the development of new interactive applications and services suitable for use over 3G networks.

MMS, unlike SMS, has virtually no limit on the size or complexity of the message. Although the basic principles behind SMS and MMS are similar, the difference in content is extraordinary. Whereas SMS messages tend to average somewhere over 100 bytes, MMS messages are in the tens to hundreds of kilobytes range. Today standards exist for MMS, **wireless application protocol** (WAP) MMS message encapsulation, and WAP MMS network architecture. WAP provides significant support for MMS by serving as its air interface protocol. Using WAP as its bearer technology, MMS can be used over wireless high-speed packet data networks (GPRS/EDGE and cdma2000) and it supports a high degree of interoperability. The MMS architecture calls for several new network elements to provide the MMS functionality. An MMS server with its associated message store is used to store and handle incoming and outgoing messages. Additionally, the MMS proxy relay element is used to transfer messages between different messaging systems (2G, 3G, Internet, etc.). Together these MMS elements compose the MM service center (MMSC) and as such manage the flow of multimedia messages to and from MMS-enabled devices and between mobile terminals and Internet (or other data network) sources and destinations. Interoperability between different wireless networks and technologies is handled via border gateways and the forwarding of messages over the Internet or another suitable packet network.

A few additional thoughts are offered about WAP to close this topic. Another industry initiative known as M-Services promoted the development and adoption of WAP. In essence, WAP is a suite of specifications that defines a protocol for wireless communications specifically for a client/server network type environment. Figure 7–19 shows a simplified view of the use of WAP as a gateway to the Internet for a wireless network. Furthermore, WAP is an open standard not designed around any particular cellular technology and hence it will eventually become a global standard. I-mode is a fairly successful, but limited geographically, Japanese initiative that is very similar in nature to WAP. The reader is urged to go to the Open Mobile Alliance at www.wapforum.org for more information about WAP.

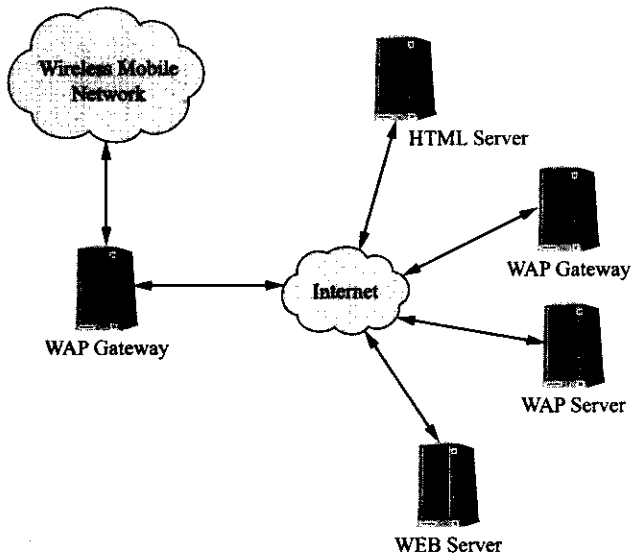


Figure 7–19 Simplified view of the use of WAP as a gateway to the Internet for a mobile wireless network.

The next evolution in these types of messaging services is known as **mobile instant messaging** or MIM. This type of service is akin to instant messaging (IM) over a fixed network using one of several popular instant messaging networks. With MIM, the users will be able to use aliases, buddy lists, and so on and also register with the system that they have available to enable more real-time messaging than is presently available with MMS.

QUESTIONS AND PROBLEMS

1. How did 1G cellular wireless systems support data services?
2. Why was CDPD developed?
3. Describe the basic difference between 1G and 2G wireless in terms of data services.
4. Contrast packet-switched data transmission to circuit-switched data transmission.
5. Give a short description of a CDPD system. How does it interface with the host AMPS system?
6. Describe the CDPD operation of cell transfer.
7. Describe the CDPD operation of channel sniffing.
8. Describe the basic operation of GSM GPRS.
9. What two new network nodes are needed to implement GPRS operation?
10. What is the purpose of a packet data protocol address in the context of GPRS operation?
11. Describe the "tunneling" process in the context of GPRS operation.
12. What is a GSM cellular system packet data channel?

13. Describe basic GSM EDGE operation.
14. For IS-95A, what is the function of the IWF?
15. Describe the functionality of the three versions of radio link protocol.
16. Describe the basic evolutionary path from GSM to UMTS.
17. What is a "Node B" in the UTRAN system?
18. Describe the basic operations involved in cdma2000 packet data call setup.
19. What happens to the user's PPP session during CDMA handover?
20. What system parameter determines the data rate over the cdma2000 forward supplemental channel during a packet data call?
21. What happens to the user's PPP session if the mobile goes into a dormant state?
22. What is the purpose of the delivery/failure report sent during a mobile originated SMS transfer?
23. What is the basic difference between EMS/MMS and SMS?
24. From a network viewpoint, what is the basic difference between SMS and MMS?
25. Describe the relationship between WAP and MMS.

CHAPTER 8

Wireless Modulation Techniques and Hardware

Upon completion of this chapter, the student should be able to:

- Discuss the general characteristics of wireline and fiber-optic transmission lines.
- Discuss the propagation conditions peculiar to the air interface for wireless mobile systems and wireless LANs.
- Discuss the coding techniques used by wireless mobile systems to combat transmission errors.
- Explain the basic fundamental concepts of digital modulation techniques and their advantages.
- Explain the basic operation and characteristics of spread spectrum modulation systems.
- Discuss the basic principles behind the operation of ultra-wideband radio technology.
- Explain the theory behind the use of diversity techniques for the improvement of wireless communications.
- Discuss the typical BSC and RBS hardware found at a modern cell site.
- Discuss the technical attributes of a subscriber device.

The first seven chapters of this text have introduced the reader to present-day wireless cellular telecommunications networks that can deliver both voice and rich multimedia messages via high-speed packet data over state-of-the-art, nationwide wireless networks. The focus of these first chapters has been on the network architectures and the various system operations necessary to provide the subscriber with radio link access, security, and mobility. When talking about the air interface for a particular type of technology, such topics as frequency reuse, frequency of operation, modulation techniques, logical channels, timing and synchronization, bit rates, and frame structure have received the most attention. The reasons why these systems were designed in the way they were has not been discussed at any great length.

This chapter is going to delve more deeply into the physical layer (air interface) of wireless mobile systems. It is hoped that some of the natural questions that might arise as the reader has gone through the early chapters of this text will be answered by the coverage provided in this chapter. Starting with a comparison of guided wave transmission and wireless transmission it is felt that the reader will develop an appreciation for the complex coding schemes employed by wireless systems. Emphasis shifts to an explanation of today's modern digital encoding techniques with their inherent spectral efficiencies and their ability to mitigate radio channel impairments. This section also sets the stage for the next several chapters that cover the technologies used to implement wireless LANs, PANs, and MANs. Another section that presents system enhancement techniques such as antenna diversity and rake receivers sheds some light on present and future system developments that are and will be used to improve wireless system quality and data transmission rates.