

APPENDIX B

Second-Generation (2G)

B.1 Overview

To better understand the issues with *Third-Generation* (3G) and the interim 2.5G radio and network access platforms, it is essential to know the fundamentals of *Second-Generation* (2G) systems. This Appendix will attempt to cover a vast array of topics with reasonable depth and breadth related to some of the more prevalent 2G wireless mobility systems that have been deployed.

Second-Generation (2G) is the generalization used to describe the advent of digital mobile communication for cellular mobile systems. When cellular systems were being upgraded to 2G capabilities, the description at that time was digital, and there was little, if any, indication of 2G because voice was the service to deliver, not data. Personal communication systems at the time of their entrance were considered the next generation of communication systems and boasted about new services that the subscriber would want and could be provided with readily by this new system or systems. However, *Personal Communication Services* (PCS) took on the same look and feel as those originating from the cellular bands.

2G mobility involves a variety of technology platforms as well as frequency bands. The issues regarding 2G deployment are as follows:

- Capacity
- Spectrum utilization
- Infrastructure changes
- Subscriber unit upgrades
- Subscriber upgrade penetration rates

The fundamental binding issue with 2G is the use of digital radio technology for transporting the information content.

It is important to note that while 2G systems used digital techniques to enhance their capacity over analog, their primary service was voice communication. At the time that 2G systems were being deployed, 9.6 kbps was more than sufficient for existing data services, usually mobile fax. A separate mobile data system was deployed in the United States, called *Cellular Data Packet Data* (CDPD), that was supposed to meet the mobile data requirements. In essence, 2G systems were deployed to improve the voice traffic throughput compared with an existing analog system.

Digital radio technology was deployed in cellular systems using different modulation formats with the attempt to increase the quality and capacity of existing cellular

B.2 Appendix B

	IS-136	IS-136*	IS-95	GSM	IDEN
Base Tx, MHz	869–894	851–866	869–894	925–960	851–866
Base Rx, MHz	824–849	806–821	869–894	880–915	806–821
Multiple access method	TDMA/FDMA	TDMA	CDMA/FDMA	TDMA/FDMA	TDMA
Modulation	$\Pi_t/4$ DPSK	$\Pi_t/4$ DPSK	QPSK	0.3 GMSK	16QAM
Radio channel spacing	30 kHz	30 kHz	1.25 MHz	200 kHz	25 kHz
Users/channel	3	3	64	8	3/6
Number of channels	832	600	9 (A), 10 (B)	124	600
CODEC	ACELP/VCELP	ACELP	CELP	REL P-LTP/ ACELP	
Spectrum allocation	50 MHz	30 MHz	50 MHz	50 MHz	30 MHz

*IS-136 deployed in the SMR band

TABLE B.1 Cellular and SMR Bands

systems. As a quick point of reference in an analog cellular system, the voice communication is digitized within the cell site itself for transport over the fixed facilities to the *Mobile Telephone System Office* (MTSO) or *Mobile Switching Center* (MSC). The voice representation and information transfer used in *Advanced Mobile Phone Service* (AMPS) cellular were analog, and it is this part in the communication link on which digital transition focuses.

The digital effort is meant to take advantage of many features and techniques that are not obtainable for analog cellular communication. Several competing digital techniques are being deployed in the cellular arena. The digital techniques for cellular communication fall into two primary categories: AMPS and the *Total Access Communication Services* (TACS) spectrum. For markets employing the TACS spectrum allocation, the *Global System for Mobile* (GSM) communications is the preferred digital modulation technique. However, for AMPS markets, the choice is between *Time Division Multiple Access* (TDMA) and *Code Division Multiple Access* (CDMA) radio access platforms. In addition to the AMPS/TACS spectrum decision, the *Integrated Dispatch Enhanced Network* (iDEN) radio access platform is available, and it operates in the *Specialized Mobile Radio* (SMR) band, which is neither cellular or PCS. With the introduction of PCS licenses, three fundamental competing technologies exist, which are CDMA, GSM, and TDMA. Which technology platform is best depends on the application desired, and at present, each platform has its pros and cons, including if it is a regulatory requirement to use one particular platform or not.

Table B.1 represents some of the different technology platforms in the cellular and SMR while Table B.2 represents technology platforms in the PCS bands.

PCS was described at the time the frequency bands were made available as the next generation of wireless communications. PCS by default has similarities and differences with its counterparts in the cellular band. The similarities between PCS and cellular lie

	IS-136	IS-95	DCS-1800 (GSM)	DCS-1900 (GSM)	IS-661
Base Tx, MHz	1930–1990	1930–1990	1805–1880	1930–1990	1930–1990
Base Rx, MHz	1850–1910	1850–1910	1710–1785	1850–1910	1850–1910
Multiple access method	TDMA/FDMA	CDMA/FDMA	TDMA/FDMA	TDMA/FDMA	TDD
Modulation	Π /4DPSK	QPSK	0.3 GMSK	0.3 GMSK	QPSK
Radio channel spacing	30 kHz	1.25 MHz	200 kHz	200 kHz	5 MHz
Users/channel	3	64	8	8	64
Number of channels	166/332/498	4–12	325	25/50/75	2–6
CODEC	ACELP/VCELP	CELP	RELTP-LTP/ACELP	RELTP-LTP/ACELP	CELP
Spectrum allocation	10/20/30 MHz	10/20/30 MHz	150 MHz	10/20/30 MHz	10/20/30 MHz

TABLE B.2 2G Technology

in the mobility of the user of the service. The differences between PCS and cellular fall into the applications and spectrum available for PCS operators to provide to their subscribers.

The PCS spectrum in the United States was made available through an action process set up by the *Federal Communications Commission* (FCC). The license breakdown is shown in Figure B.1.

The geographic boundaries for PCS licenses are different from those imposed on cellular operators in the United States. Specifically, PCS licenses are defined as *Metropolitan Trading Area* (MTA) and *Basic Trading Area* (BTA). The MTA has several BTAs within its geographic region. A total of 93 MTAs and 487 BTAs are defined in the United States. Therefore, a total of 186 MTA licenses were awarded for the construction of a PCS network, and each license has a total of 30 MHz of spectrum to use. In addition, a total of 1948 BTA licenses were awarded in the United States. Of the BTA licenses, the C band has 30 MHz of spectrum, whereas the D, E, and F blocks will have only 10 MHz available.

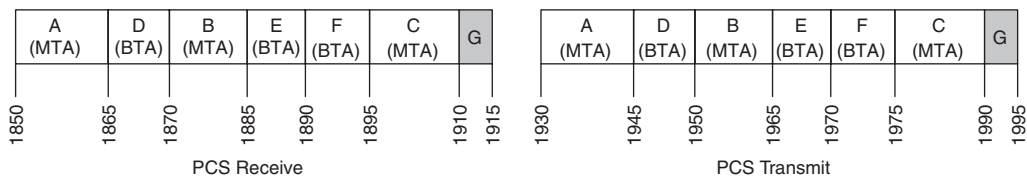


FIGURE B.1 U.S. PCS spectrum chart.

Recently, the G block was added to the spectrum offering as part of the 800-MHz rebanding process with public safety in the United States. The G block has 10 MHz, 5 MHz paired, as shown in Figure B.1.

Currently, PCS operators do not have a standard to use for picking a technology platform for their networks. The choice of PCS standards is daunting, and each has its advantages and disadvantages. The current philosophy in the United States is to let the market decide which standard or standards are the best. This is significantly different from the approach used for cellular, where every operator has one set interface for the analog system from which to operate.

Table B.2 represents various PCS systems that are used throughout the world, particularly in the United States. The major standards used so far for PCS are DCS-1900, IS-95, IS-661, and IS-136. DCS-1900 uses a GSM format and is an upbanded DCS-1800 system. IS-95 is the CDMA standard that is used by cellular operators, except that it is upbanded to the PCS spectrum. The IS-136 standard is an upbanded cellular TDMA system that is used by cellular operators. IS-661 is a *Time Division Duplex* (TDD) system offered by Omnipoint Communications with the one notable exception that it was supposed to be deployed in the New York market as part of the pioneer preference license issued by the FCC.

Digital, or digital modulation, is now prevalent throughout the entire wireless industry. Digital communication references any communication that uses a modulation format that relies on sending the information in any type of data format. More specifically, digital communication is where the sending location digitizes the voice communication and then modulates it. At the receiver, the exact opposite is done.

Data are digital, but they need to be converted into another medium to facilitate transport from point *A* to point *B* and, more specifically, between the base station and the host terminal. The data between the base station and the host terminal are converted from a digital signal into *Radiofrequency* (RF) energy. Its modulation is a representation of the digital information that enables the receiving device, base station, or host terminal to replicate the data properly.

Digital radio technology is deployed in a cellular/PCS/SMR system primarily to increase the quality and capacity of the wireless system over its analog counterpart. The use of digital modulation techniques enables the wireless system to transport more bits per hertz than would be possible with analog signaling using the same bandwidth. However, the service offering for 2G is mainly a voice offering.

Figure B.2 is a block-diagram representation of the differences between analog and digital radio. Reviewing the digital radio portion of the diagram, the initial information content, usually voice, is input into the microphone of the transmission section. The speech then is processed in a vocoder, which converts the audio information into a data stream using a coding scheme to minimize the number of data bits required to represent the audio. The digitized data then go to a channel coder that takes the vocoder data and encodes the information even more so that it will be possible for the receiver to reconstruct the desired message. The channel-coded information is then modulated onto an RF carrier using one of several modulation formats covered previously in this Appendix. The modulated RF carrier then is amplified, passes through a filter, and is transmitted out an antenna.

The receiver, at some distance away from the transmitter, receives the modulated RF carrier through use of an antenna, which then passes the information through a filter and into a preamp. The modulated RF carrier is then downconverted in the digital

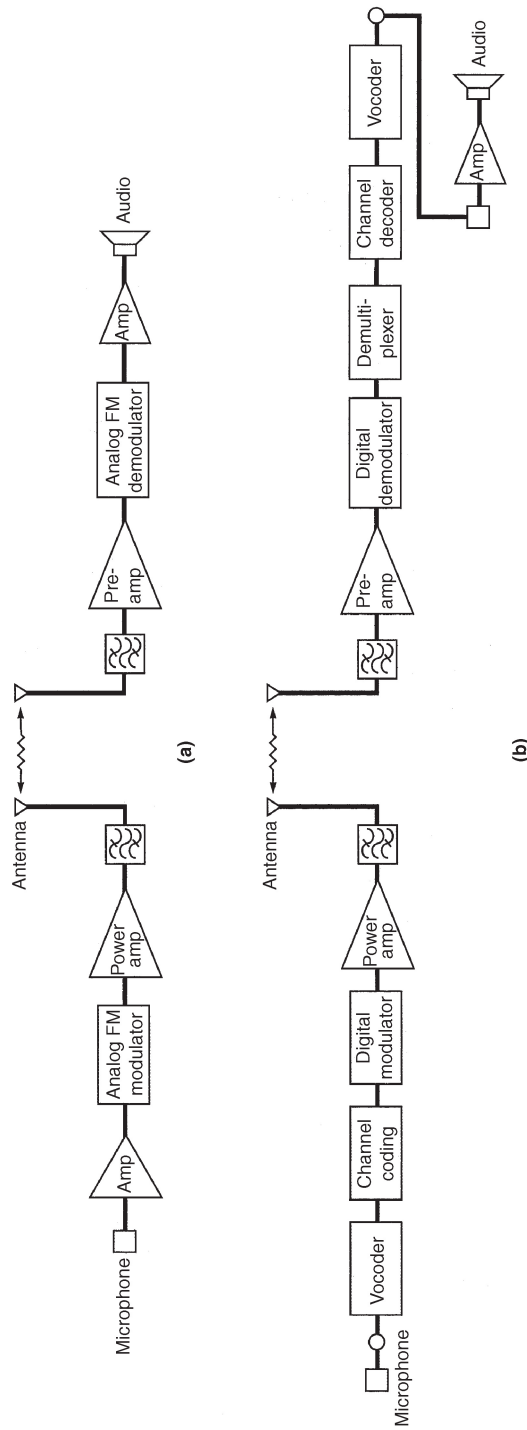


FIGURE B.2 Analog and digital radio.

demodulator section of the receiver to an appropriate intermediate frequency. The demodulated information then is sent to a channel decoder that performs the inverse of the channel coder in the transmitter. The digital information then is sent to a vocoder for voice information reconstruction. The vocoder converts the digital format into an analog format, which is passed to an audio amplifier connected to a speaker for the user at the other end of the communication path in order to listen to the message sent.

B.2 Enhancements over 1G Systems

The introduction of 2G mobility systems, while focused on voice transport, brought about numerous improvements or enhancements for mobile wireless operators and their customers. The major benefits associated with the introduction of 2G systems are

- Increased capacity over analog
- Reduced capital infrastructure costs
- Reduced capital-per-subscriber cost
- Reduced cellular fraud
- Improved features
- Encryption

The benefits, when looking at this list, were geared toward the operators of wireless systems. Implementation of 2G brought about a reduction in operating costs for the mobile operators through improved capital equipment and spectrum utilization and a reduction in cellular fraud. The improved features were centered around *Short Message Service* (SMS) features, which the subscriber benefited from. The onslaught of 2G systems, however, benefited the customer primarily in that the overall cost was reduced significantly.

B.3 Integration with Existing 1G Systems

The advent of 2G digital systems brought about several implementation issues that the existing operators and infrastructure vendors needed to solve. At the heart of the issue was how to implement 2G cost-effectively into an existing analog network. The problems involved the available spectrum, existing infrastructure, and subscriber equipment. Most of the staff that went through this period of time can remember the issues.

For the cellular operators, several decisions needed to be made (or options selected) about how to integrate the new system into the existing analog network. However, for PCS operators, integration with legacy systems did not present a problem because there was no legacy system. The PCS operators in the United States had one other obstacle to overcome, and that dealt with microwave clearance issues because the RF spectrum auctioned for use by PCS operators was currently being used by 2-GHz point-to-point microwave systems.

The integration with the existing 1G legacy systems therefore was an issue that affected only the analog systems operating in the 800- to 900-MHz bands. The 2G technologies that were applicable involved GSM, TDMA, and CDMA radio access systems. Several options were available for the 1G operators to follow, and they are listed in this

section relative to each access platform because the actual implementation also depends on the technology.

B.3.1 GSM

GSM is the European standard for digital cellular systems operating in the 900-MHz band. This technology was developed out of the need for increased service capacity owing to the analog systems' limited growth. This technology offers international roaming, high speech quality, increased security, and the ability to develop advanced systems features. The development of this technology was completed by a consortium of pan-European countries working together to provide integrated cellular systems across different borders and cultures.

GSM is a European standard that has achieved worldwide success. GSM has many unique features and attributes that make it an excellent digital radio standard to use. GSM has the unique advantage of being the most widely accepted radio communication standard at this time. GSM was developed as a communication standard that would be used throughout all of Europe in response to the problem of multiple and incompatible standards that still exist there today.

GSM consists of the following major building blocks: the *Switching System* (SS), the *Base-Station System* (BSS), and the *Operations and Support System* (OSS). The BSS consists of both the *Base-Station Controller* (BSC) and the *Base Transceiver Stations* (BTS). In an ordinary configuration, several BTSs are connected to a BSC, and then several BSCs are connected to the MSC.

The GSM radio channel is 200 kHz wide. GSM has been deployed in several frequency bands, namely, the 900-, 1800-, and 1900-MHz bands. Both the 1800- and 1900-MHz bands required some level of spectrum clearing before the GSM channel could be used. However, the 900-MHz spectrum was used by an analog system, the *Enhanced Total Access Communication System* (ETACS), that occupied 25-kHz channels. The introduction of GSM into this band required the reallocation of traffic, or rather channels, to accommodate GSM.

B.3.2 TDMA (IS-54/IS-136)

IS-136, an enhancement of IS-54, is the digital cellular standard developed in the United States using TDMA technology. Systems of this type operate in the same band as the AMPS systems and are used in the PCS spectrum as well. IS-136 therefore applies to both the cellular and PCS bands, as well as in some unique situations to downbanded IS-136, which operates in the SMR band.

TDMA technology enables multiple users to occupy the same channel by employing time division. The TDMA format used in the United States follows the IS-54 and IS-136 standards and is referred to as *North American Dual Mode Cellular* (NADC). IS-136 is an evolution to the IS-54 standard and enables a feature-rich technology platform to be used by current cellular operators.

TDMA, using the IS-136 standard, is currently deployed by several cellular operators in the United States. IS-136 uses the same channel bandwidth as analog cellular: 30 kHz per physical radio channel. However, IS-136 enables three and possibly six users to operate on the same physical radio channel at the same time. The IS-136 channel presents a total of six time slots in the forward and reverse directions. IS-136 at present uses two time slots per subscriber, with the potential to go to half-rate vocoders that require the use of only one time slot per subscriber.

IS-136 has many advantages in its deployment in a cellular system:

- Increased system capacity, up to three times over analog
- Improved protection for adjacent-channel interference
- Authentication
- Voice privacy
- Reduced infrastructure capital to deploy
- Short message services

Integrating IS-136 into an existing cellular system can be done more easily than for the deployment of CDMA. The use of IS-136 in a network requires the use of a guard band to protect the analog system from the IS-136 signal. However, the guard band required consists of only a single channel on either side of the spectrum block allocated for IS-136 use. Depending on the actual location of the IS-136 channels in the operator’s spectrum, it is possible to require only one or no guard-band channel.

The IS-136 has the unique advantage of affording the implementation of digital technology into a network without elaborate engineering requirements. The implementation advantages mentioned for IS-136 also facilitate the rapid deployment of this technology into an existing network.

The implementation of IS-136 is further augmented by requiring only one channel per frequency group as part of the initial system offering. The advantage to requiring only one channel per sector in the initial deployment is minimization of capacity reduction for the existing analog network. Another advantage with deploying one IS-136 channel per sector initially is elimination of the need to preload the subscriber base with dual-mode IS-136 handsets.

B.3.3 CDMA

The operators who chose to deploy CDMA systems had basically two methods to use in deploying CDMA IS-95 systems. The first method is to deploy CDMA in every cell site for the defined service areas on a 1:1 basis. The other method is to deploy CDMA on an N:1 basis. Both the 1:1 and the N:1 deployment strategies had their advantages and disadvantages. Of course, a third method involved a hybrid approach to both the 1:1 and N:1 methods (Table B.3).

Figures B.3 and B.4 illustrate at a high level both 1:1 and N:1 deployment scenarios for integrating a CDMA system into an existing 1G analog network.

Layout	Advantages	Disadvantages
1:1	Consistent coverage	Cost
	Facilitates gradual growth	Guard-band requirements
	Integrates into existing 1G system	Digital-to-analog boundary handoff
	Large initial capacity gain	Slower deployment than N:1
N:1	Lower capital cost over 1:1	Engineering complexity
	Faster to implement over 1:1	Lower capacity gain

TABLE B.3 CDMA Deployment Strategies

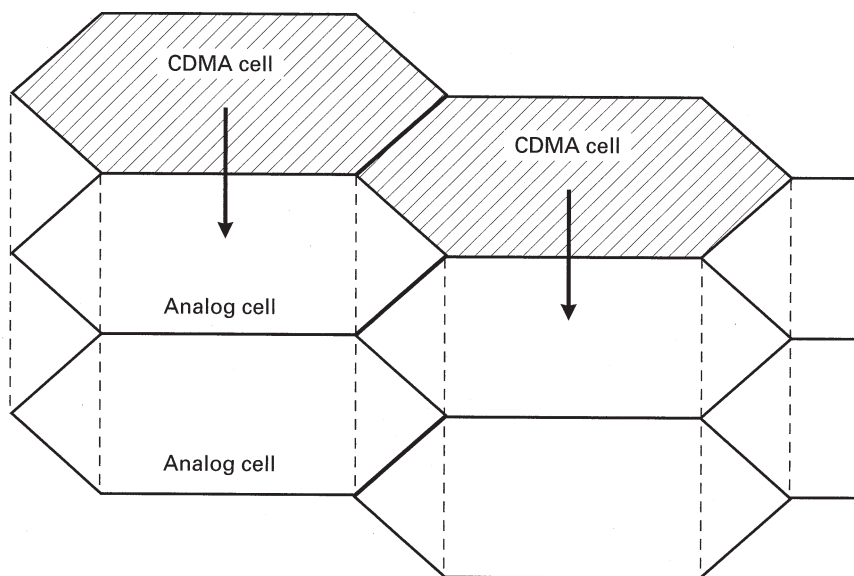


FIGURE B.3 1:1 CDMA deployment.

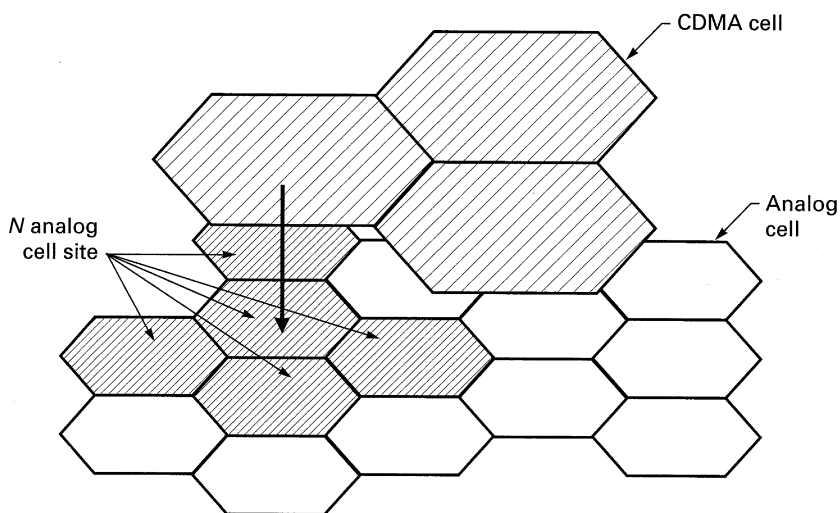


FIGURE B.4 N:1 CDMA deployment.

The introduction of CDMA into an existing AMPS system also required the establishment of a guard band and guard zone. The guard band and guard zone are required for CDMA to ensure that the interference received from the AMPS system does not have a negative impact on the ability of CDMA to perform well.

The specific location that the CDMA channel (or channels) occupies in a cellular system depends on a multitude of issues. The first issue is how much spectrum will be dedicated to the use of CDMA for the network. The spectrum issue ties into the fact that one CDMA channel occupies 1.77 MHz of spectrum, 1.23 MHz per CDMA channel, and 0.27 MHz of guard band on each side of the CDMA channel. With a total of 1.77 MHz per CDMA, the physical location in the operator's band that CDMA will operate in needs to be defined. For the B-band carrier, wireline operators, two predominant locations were used. The first location in the spectrum is the band next to the control channels, and the other section is in the lower portion of the extended AMPS band. The upper end of the AMPS band is not as viable owing to the potential of *Air to Ground Telephone* (AGT) interference because AGT transmit frequencies have no guard band between AMPS receiving and AGT transmitting. The lower portion of the AMPS band has the disadvantage of receiving A-band mobile-to-base interference, which will limit the size of the CDMA cell site.

The other issue with the guard band ties into the actual amount of spectrum that will be unavailable for use by AMPS subscribers in the cellular market. With the expansive growth of cellular, assigning 1.77 MHz of spectrum to CDMA reduces the spectrum available for AMPS usage by 15 percent, or to 59 radio channels from the channel-assignment chart. The reduction in available channels for regular AMPS requires the addition of more cell sites to compensate for the number of radio channels no longer available to the AMPS system. Using a linear evaluation, the reduction in usable spectrum by 15 percent involves a reduction in traffic-handling capacity by the AMPS system of a maximum of 21 percent at an Erlang B 2 percent *Grade of Service* (GOS) with a maximum of 16 channels per sector versus 19. The reduction of 21 percent in the initial AMPS traffic-handling capacity results in the need to build more analog cell sites to compensate for this reduction in traffic-handling capabilities. The only ways to offset the reduction in the traffic-handling capacity experienced by partitioning the spectrum are to preload the CDMA subscriber using dual-mode phones or to build more analog cell sites.

The guard zone is the physical area outside the CDMA coverage area that can no longer use the AMPS channels now occupied by the CDMA system. Figure B.5 presents an example of a guard zone versus a CDMA system coverage area. The establishment and size of the guard zone depend on the traffic load expected by the CDMA system. The guard zone usually is defined in terms of a signal-strength level from which analog cell sites operating with the CDMA channel sets cannot contribute to the overall interference level of the system. The interesting point about the guard zone is when the operator of one system wants to use CDMA and must require the adjacent system operator to reduce his or her channel utilization in the network to accommodate the introduction of this new technology platform.

However, regardless of the method chosen for the implementation of CDMA into an existing 1G analog system, part of the RF spectrum needed to be cleared of existing analog radio usage. The impact to this situation, as discussed, was the need to build more cell sites with lower traffic-carrying capacity owing to the spectrum reduction or to increase the blocking percentage at which the system would be allowed to operate. Obviously, the mix of both increased blocking and additional cell sites was the method followed by wireless operators.

In addition to the reduction in spectrum that is experienced by existing 1G subscribers for base stations that had CDMA installed, there are also numerous sites that did not

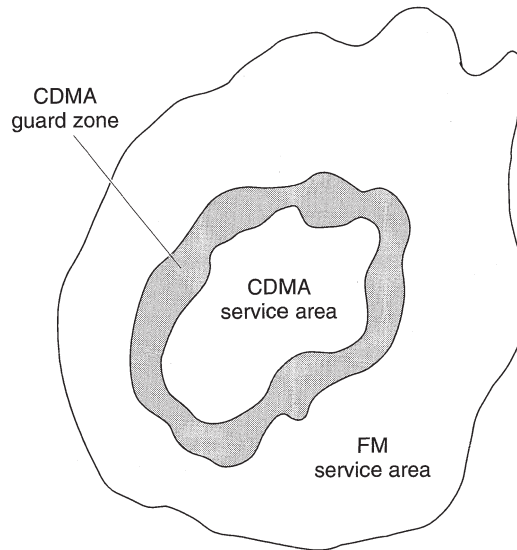


FIGURE B.5 Guard zone.

have CDMA installed but still had to surrender the use of spectrum to accommodate the introduction of CDMA into the system. Naturally, if the system was a complete 1:1 system, then there would be no need for implementation of a guard zone and only a guard band. But when the CDMA system butted up to another radio access system such as TDMA or even analog, where another operator decided not to implement 2G systems, both a guard zone and guard band were required.

B.3.4 DECT

Digital European Cordless Telephone (DECT) is one of the few IMT2000-compliant radio access technologies. The DECT standard is referred to as *ETS-300 175-2*. DECT was designed as a *Wireless Local Loop* (WLL) technology that typically is used as a WPBX. DECT is based on a TDD access method using a 1.728-MHz-wide channel. Each of the DECT channels is divided into 12 individual time slots using *Gaussian Frequency Shift Keying* (GFSK) modulation. DECT uses a variant of *Integrated Services Digital Network* (ISDN) for its signaling, *Link Access Protocol Control* (LAPC), and is designed to interface with *Universal Mobile Telecommunications Service* (UMTS) networks.

DECT has been deployed largely as a low-mobility cordless-phone product. However, several BTAs in the U.S. market have used DECT as their primary radio access network offering as a WLL. There also has been a dual-mode DECT/GSM mobile available in the marketplace. DECT, however, has not been deployed widely and has become isolated.

The most common spectrum allocation is 1880 to 1900 MHz, but outside of Europe, spectrum is also available in the 1900- to 1920-MHz and 1910- to 1930-MHz bands. In the United States, DECT has seen more deployment in the unlicensed 902- to 928-MHz and 2.400- to 2.4835-GHz *Industrial Scientific and Medical* (ISM) bands. In addition, 5.4-GHz *Unlicensed National Information Infrastructure* (UNII) bands have been defined.

Modulation	Half-Slot Rate (kbps)	Full-Slot Rate (kbps)	Double-Slot Rate (kbps)	Maximum Asymmetric Data Rate (11 Double Slots) (kbps)
2-level	8	32	80	880
4-level	16	64	160	1760
8-level	24	96	240	2640
16-level	32	128	320	3520
64-level	48	192	480	5280

TABLE B.4 DECT Slot and Data-Rate Relationship

DECT is based on a microcellular radio communication system that provides low-power radio (cordless) access between *Portable Parts* (PPs) and DECT *Fixed Parts* (FPs) at ranges of up to a few hundred meters (up to several kilometers for fixed access systems).

Table B.4 shows the relationship between modulation schemes and channel configurations. As discussed earlier, there are a total of 12 data slots with a DECT carrier. These data slots can be configured by the system, based on user demand, to be either half or full slots.

The simplest duplex service uses a single pair of time slots to provide a 32-kbps (2-level modulation) throughput for the channel. Higher data rates are achieved by using more time slots, and a lower data rate may be achieved by using half-slots. In addition, different uplink and downlink data rates are realized by using asymmetric connections, where a different number of time slots are used for the uplink and downlink.

DECT is a 3G defined wireless access system meeting IMT2000 specifications. However, the lack of deployment in the United States and elsewhere as a commercial mobile system makes its potential use for 3G services a nonstarter.

B.4 GSM

Unlike IS-136 or IS-95, GSM was designed from scratch as a complete system, including air interface, network architecture, interfaces, and services. In addition, the design of GSM included no compatibility with existing analog systems. The reasons for this included the fact that multiple analog systems were used in Europe, and it would have taken great effort to design a system that would provide backward-compatibility with each of them. The lack of compatibility also meant that carriers had a greater impetus to build GSM coverage as extensively and as quickly as possible.

In the following sections we spend some time describing the GSM architecture and functionality. The main reason is that GSM is the foundation of a number of more advanced technologies such as the *General Packet Radio Service* (GPRS) and the UMTS. An understanding of GSM is necessary to understand those technologies.

B.4.1 GSM Network Architecture

Figure B.6 shows the basic architecture of a GSM network. Working our way from the left, we see that the handset, known in GSM as the *Mobile Station* (MS), communicates over the air interface with a *Base Transceiver Station* (BTS). Strictly speaking, the MS has two parts—the handset itself, known as the *Mobile Equipment* (ME), and the *Subscriber Identity Module* (SIM), a small card containing an integrated circuit. The SIM contains

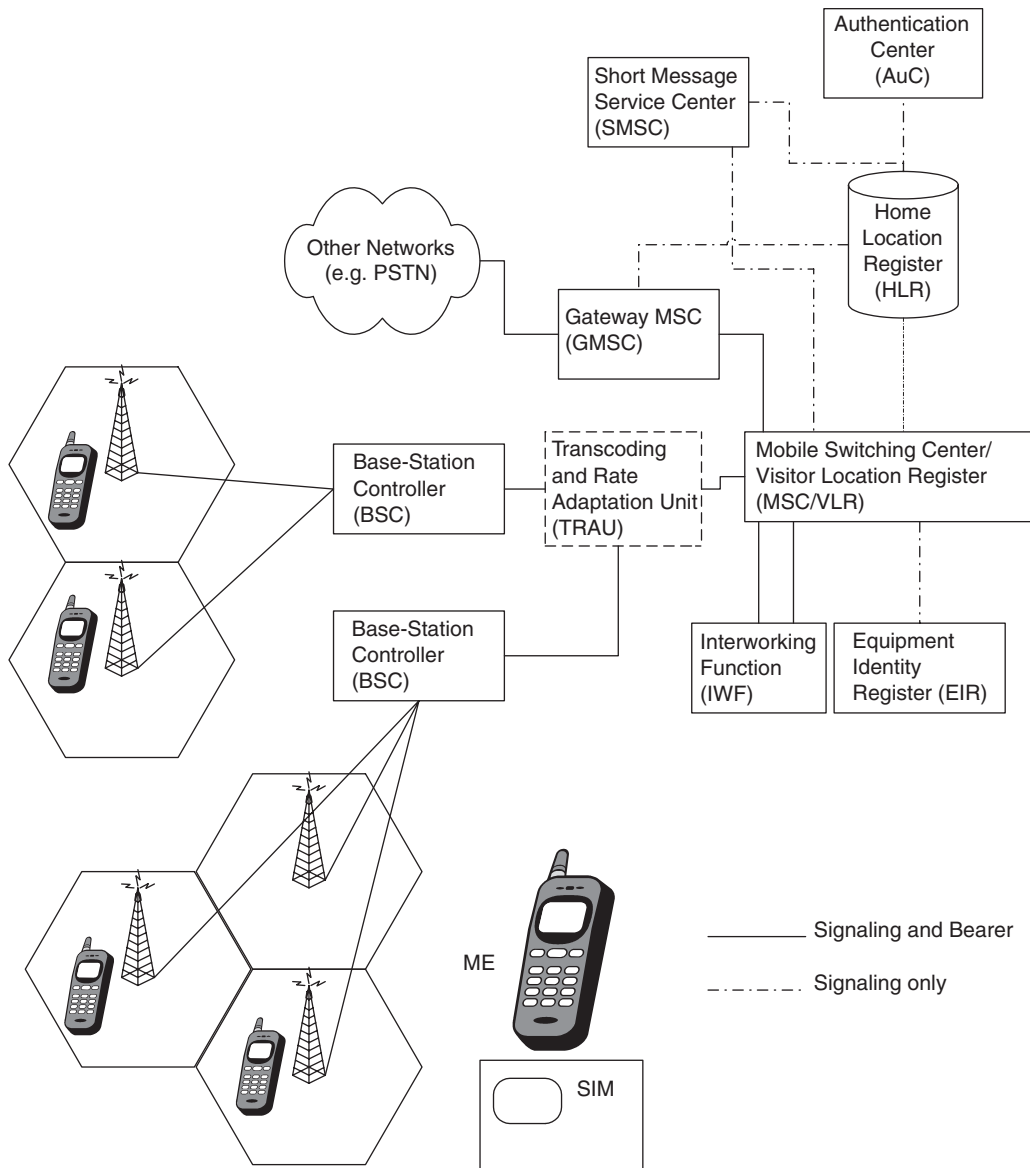


FIGURE B.6 GSM architecture.

user-specific information, including the identity of the subscriber, subscriber authentication information, and some subscriber service information. It is only when a given subscriber's SIM is inserted into a handset that the handset acts in accordance with the services to which the subscriber has subscribed. In other words, my handset acts as my handset only when my SIM is inserted.

The BTS contains the radio transceivers that provide the radio interface with mobile stations. One or more BTSs are connected to a *Base-Station Controller* (BSC). The BSC

provides a number of functions related to *Radio-Resource* (RR) management, some functions related to *Mobility Management* (MM) for subscribers in the coverage area of the BTSs, and a number of operation and maintenance functions for the overall radio network. Together, BTSs and BSCs are known as the *Base-Station Subsystem* (BSS).

The interface between the BTS and the BSC is known as the *Abis interface*. Many aspects of this interface are standardized. One aspect, however, is proprietary to the BTS and BSC vendor and is the part of the interface that deals with configuration, operation, and maintenance of the BTSs. This is known as the *Operation and Maintenance Link* (OML). Because the internal design of a BTS is proprietary to the BTS vendor, and because the OML needs to have functions that are specific to that internal design, the OML is also proprietary to the BTS vendor. The result is that a given BTS must be connected to a BSC of the same vendor.

One or more BSCs are connected to an MSC. The MSC is the switch—the node that controls call setup, call routing, and many of the functions provided by a standard telecommunications switch. The MSC is no ordinary *Public Switched Telephone Network* (PSTN) switch, however. Because of the fact that the subscribers are mobile, the MSC needs to provide a number of MM functions. It also needs to provide a number of interfaces that are unique to the GSM architecture.

When we speak of an MSC, a *Visitor-Location Register* (VLR) also usually is implied. The VLR is a database that contains subscriber-related information for the duration that a subscriber is in the coverage area of an MSC. A logical split exists between an MSC and a VLR, and the interface between them has been defined in standards. No equipment vendor, however, has ever developed a stand-alone MSC or VLR. The MSC and VLR are always contained on the same platform, and the interface between them is proprietary to the equipment vendor. Although early versions of GSM standards defined the MSC-VLR interface (known as the *B-interface*) in great detail, later versions of the standards recognized that no vendor complies with the standardized interface. Therefore, any “standardized” specification for the B-interface should be considered informational.

The interface between the BSC and the MSC is known as the *A-interface*. This is a *Signaling System 7* (SS7)-based interface using the *Signaling Connection Control Part* (SCCP), as depicted in Figure B.7. Above Layer 3 in the signaling stack, we find the *BSS Application Part* (BSSAP), which is the protocol used for communication between the

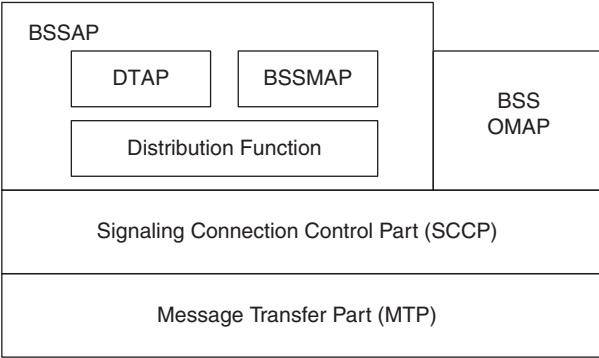


FIGURE B.7 BSSAP protocol layers.

MSC and the BSC, as well as between the MSC and the MS. Since the MSC communicates separately with both the BSC and the MS, the BSSAP is divided into two parts—the *BSS Management Application Part* (BSSMAP) and the *Direct Transfer Application Part* (DTAP). BSSMAP contains messages that are either originated by the BSS or need to be acted on by the BSS. DTAP contains messages that are passed transparently through the BSS from the MSC to the MS, or vice versa. Note that there is also a *BSS Operation and Maintenance Application Part* (BSSOMAP). Although this is defined in standards, it is normal for the BSC to be managed through a vendor-proprietary management protocol.

In Figure B.6 we find (in the dashed outline) the *Transcoding and Rate Adaptation Unit* (TRAU). In GSM, the speech from the subscriber usually is coded at either 13 kbps [*full rate* (FR)] or 12.2 kbps [*enhanced full rate* (EFR)]. In some cases, we also find half-rate coding at a rate of 5.6 kbps, but this is rare in commercial networks. In any case, it is clear that the speech to and from the MS is very different from the standard 64-kbps *Pulse Code Modulation* (PCM) used in switching networks.

Since the MSC interfaces with the PSTN, it needs to send and receive speech at 64 kbps. The function of the TRAU is to convert the coded speech to or from standard 64 kbps. Strictly speaking, the TRAU is a part of the BSS. As far as the MSC is concerned, voice to and from the BSS is passed at 64 kbps, and the BSS takes care of the transcoding. In practice, however, it is common for the TRAU to be physically separate from the BSC and placed near the MSC. This reduces the bandwidth required between the MSC and the BSC locations and can mean significant savings in transport cost, particularly if the BSC and MSC are separated by a significant distance. In cases where the BSC and TRAU are separated, the interface between them is known as the *Ater interface*. This interface is proprietary to the BSS equipment vendor. Hence, the BSC and TRAU must be from the same vendor.

In Figure B.6 we also find a *Home-Location Register* (HLR)—a node found in most, if not all, mobile networks. The HLR contains subscriber data, such as the details of the services to which a user has subscribed. Associated with the HLR, we find the *Authentication Center* (AuC). This is a network element that contains subscriber-specific authentication data, such as a secret authentication key called the *Ki*. The AuC also contains one or more sophisticated authentication algorithms. For a given subscriber, the algorithm in the AuC and the *Ki* are also found on the SIM card. Using a random number assigned by the AuC and passed down to the SIM via the HLR, MSC, and ME, the SIM performs a calculation using the *Ki* and authentication algorithm. If the result of the calculation on the SIM matches that in the AuC, then the subscriber has been authenticated. The interface between the HLR and AuC is not standardized. Although implementations can set up the HLR and AuC to be separate, it is more common to find the HLR and AuC integrated on the same platform.

Calls from another network, such as the PSTN, first arrive at a type of MSC known as a *Gateway MSC* (GMSC). The main purpose of the GMSC is to query the HLR to determine the location of the subscriber. The response from the HLR indicates to the MSC where the subscriber may be found. The call is then forwarded from the GMSC to the MSC serving the subscriber. A GMSC may be a full MSC/VLR such that it may have some BSCs connected to it. Alternatively, it may be a dedicated GMSC whose only function is to interface with the PSTN and query the HLR. The choice depends on the amount and types of traffic in the network and the relative cost of a full MSC/VLR versus a pure GMSC.

In Figure B.6 we also note the *Short Message Service Center* (SMSC). Strictly speaking, the correct term is *Short Message Service Service Center* (SMS-SC), but that is a bit of a mouthful and usually is shortened to SMSC. The SMSC is a node that supports the storing and forwarding of short messages to and from mobile stations. Typically, these short messages are text messages up to 160 characters in length.

Logically, an SMSC has three components. First is the *Service Center* (SC) itself, which stores messages and interfaces with other systems such as e-mail or voice-mail equipment. Second, there is the *SMS Gateway MSC* (SMS-GMSC), which is used for the delivery of short messages to a mobile subscriber. Much like a GMSC, the SMS-GMSC queries the HLR for the subscriber's location and then forwards the short message to the appropriate visited MSC, where it is relayed to the subscriber. Third is the *SMS Interworking MSC* (SMS-IWMSC), which receives a short message from the MSC serving the subscriber. It forwards the message to the SC, which then passes it on to the final destination. It is very common for the SC, SMS-GMSC, and SMS-IWMSC to be included within the same platform, although certain implementations enable a stand-alone SC. In such implementations, the SMS-GMSC function may be included within a GMSC, and the SMS-IWMSC function may be included with an MSC/VLR.

In a GSM network, we also may find a node known as the *Equipment Identity Register* (EIR). As mentioned, it is not the handset that identifies a subscriber; rather, it is the information on the SIM. Therefore, to some degree, the handset used by a particular subscriber is not relevant. On the other hand, it may be important for the network to verify that a particular handset (ME) or a model of ME is acceptable. For example, a network operator might want to restrict access from a handset that has not been fully type approved. Also, a network operator might want to restrict access from a handset that is known to be stolen.

Stored in each handset is an *International Mobile Equipment Identity* (IMEI) number (15 digits) or the *International Mobile Equipment Identity and Software Version* (IMEISV) number (16 digits). Both the IMEI and IMEISV numbers have a structure that includes the *Type Approval Code* (TAC) and the *Final Assembly Code* (FAC). The TAC and FAC combine to indicate the make and model of the handset and the place of manufacture. The IMEI and IMEISV numbers also include a specific serial number for the ME in question. The only difference between IMEI and IMEISV numbers is the software version number.

Within the EIR are three lists—black, gray, and white. These lists contain values of TAC, TAC and FAC, or complete IMEI or IMEISV number. If a given TAC, a TAC/FAC combination, or a complete IMEI number appears on the black list, then calls from the ME are barred. If it appears in the gray list, then calls may or may not be barred at the discretion of the network operator. If it appears in the white list, then calls are allowed. Typically, a given TAC included in the white list has the model of handset that has been approved by the handset manufacturer. The EIR is an optional network element, and some network operators have chosen not to deploy an EIR.

Finally, we find the *Interworking Function* (IWF). This is used for circuit-switched data and fax services and is basically a modem bank. Typical dial-up modems and fax machines are analog. For example, when one uses a computer with a 28.8-kbps modem on a regular telephone line, the modem modulates the digital data from the computer to an analog format that appears like analog speech. The same cannot be done directly for a digital system such as GSM because all transmissions are digital, and it is not possible to transmit data over the air in a manner that emulates analog voice. Furthermore, a

remote dial-up modem, such as an *Internet Service Provider* (ISP), expects to be called by another modem. Therefore, a circuit-switched data call from an MS is looped through the IWF before being routed onward by the IWF. Within the IWF, a modem is placed in the call path. The same applies for facsimile service, where a fax modem would be used rather than a data modem. GSM supports data and fax services up to 9.6 kbps.

B.4.2 The GSM Air Interface

GSM is a TDMA system with *Frequency-Division Duplex* (FDD). It uses *Gaussian Minimum Shift Keying* (GMSK) as the modulation scheme. TDMA means that multiple users share a given RF channel on a time-sharing basis. FDD means that different frequencies are used in the downlink (from network to MS) and uplink (from MS to network) directions.

GSM has been deployed in numerous frequency bands—including the 900-MHz band, the 1800-MHz band, and the 1900-MHz band (in North America). Table B.5 shows the frequency allocations for these three bands.

Of course, the amount of spectrum allocated in a given band in a given country is at the discretion of the appropriate regulatory authorities of that country. Moreover, even if the entire spectrum in a given band is made available in a given country, it is likely to be divided among several operators such that it is extremely rare for a single network operator to have access to a complete band.

In GSM, a given band is divided into 200-kHz carriers or RF channels in both the uplink and downlink directions. In addition, a guard band of 200 kHz is located at each end of each frequency band. For example, in standard GSM 900, the first uplink RF channel is at 890.2 MHz and the last uplink RF channel is at 914.8 MHz, allowing for a total of 124 carriers. Similarly, DCS-1800 has a maximum of 374 carriers, and PCS-1900 has a maximum of 299 carriers.

As mentioned, in GSM, a given band is divided into a number of RF channels or carriers, each 200 kHz in both the uplink and downlink. Thus, if a handset is transmitting on a given 200-kHz carrier in the uplink, then it is receiving on a corresponding 200-kHz carrier in the downlink. Because the uplink and downlink are rigidly associated, when one talks about a carrier or RF channel, both the uplink and downlink usually are implied. A given cell can have multiple RF carriers—typically one to three in a normally loaded system, although as many as six carriers might exist in a heavily loaded cell in an area of very high traffic demand. Note that when we talk about a cell in GSM terms, we mean a sector. Thus, a three-sector BTS implies three cells. This is a somewhat confusing distinction between GSM and some other technologies.

Each RF carrier is divided into eight time slots, numbered 0 to 7, and these are transmitted in a frame structure. Each frame lasts approximately 4.62 ms, such that each time

	GSM-900	Extended GSM (E-GSM)	DCS-1800	PCS-1900
Uplink (MS to network)	890–915 MHz	880–915 MHz	1710–1785 MHz	1850–1910 MHz
Downlink (network to MS)	935–960 MHz	925–960 MHz	1805–1880 MHz	1930–1990 MHz

TABLE B.5 GSM Frequency Bands

slot lasts approximately 576.9 ms. Depending on the number of RF carriers in a given cell, all eight time slots on a given carrier might be used to carry user traffic. In other words, the RF carrier might be allocated to eight *Traffic Channels* (TCHs). However, there must be at least one time slot in a cell allocated for control-channel purposes. Thus, if only one carrier is in a cell, then there is a maximum of seven TCHs, such that a maximum of seven simultaneous users can be accommodated.

B.4.3 Types of Air-Interface Channels

The foregoing description of the RF interface suggests that only traffic channels and control channels exist. This is only partly correct. In fact, there are traffic channels, numerous types of control channels, and a number of other channels. To begin with, a number of broadcast channels are available:

- *Frequency Correction Channel* (FCCH). This is broadcast by the BTS and used for frequency correction of the MS.
- *Synchronization Channel* (SCH). This is broadcast by the BTS and is used by a mobile station for frame synchronization. In addition to frame-synchronization information, it also contains the *Base-Station Identity Code* (BSIC).
- *Broadcast Control Channel* (BCCH). This is used to broadcast general information regarding the BTS and the network. It is also used to indicate the configuration of the *Common Control Channels* (CCCHs) described in the following section.

The CCCH is a bidirectional control channel used primarily for functions related to initial access by a mobile station. It has a number of components:

- *Paging Channel* (PCH). This is used for the paging of mobile stations.
- *Random-Access Channel* (RACH). This is used only in the uplink direction. It is used by an MS to request the allocation of a *Stand-alone Dedicated Control Channel* (SDCCH) described later.
- *Access Grant Channel* (AGCH). This is used in the downlink in response to an access request received on the RACH. It is used to allocate an MS to an SDCCH or directly to a *Traffic Channel* (TCH).
- *Notification Channel* (NCH). This is used with voice group-call and voice broadcast services to notify mobile stations regarding such calls.

A number of dedicated control channels exist. These are channels that are used by one MS at a time, typically either during call establishment or while a call is in progress. The dedicated control channels are as follows:

- *Stand-alone Dedicated Control Channel* (SDCCH). This is a bidirectional channel used for communication with an MS when the MS is not using a TCH. The SDCCH is used, for example, for SMS when the MS is not in a call. It is also used for call-establishment signaling prior to the allocation of a TCH for a call.
- *Slow Associated Control Channel* (SACCH). This is a unidirectional or bidirectional channel used when the MS is using a TCH or SDCCH. For example, when an MS is engaged in a call on a TCH, power-control messages from a BTS to an MS are sent on the SACCH. In the uplink, the MS sends measurement reports to the

BTS on the SACCH. These reports indicate how well the MS can receive transmissions from other BTSs, and the information is used in determining if or when a handover should occur. The SACCH is also used for short message transfers when the MS is in on a TCH.

- *Fast Associated Control Channel (FACCH)*. This is associated with a given TCH and thus is used when the ME is involved in a call. It is typically used to transmit nonvoice information to and from the MS. Such information would include, for example, handover instructions from the network, commands from the MS for generation of *Dual Tone Multi-Frequency (DTMF)* tones, supplementary service invocations, and so on.

B.4.4 Air-Interface Channel Structure

Clearly, it does not make sense for these different types of channels to each be allocated one of the eight time slots. First, there simply would not be enough time slots. Moreover, different data rates apply to the various types of channels. Instead, a sophisticated framing structure is used on the air interface to allocate the various channel types to the available time slots. The structure includes frames, multiframes, superframes, and hyperframes.

As mentioned previously, a single frame lasts approximately 4.62 ms and contains eight time slots. In standard GSM (as opposed to GPRS), two types of multiframes are used—a 26 multiframe (containing 26 frames and having a duration of 120 ms) and a 51 multiframe (containing 51 frames and having a duration of 235.4 ms). The 26 multiframe is used to carry TCHs and the associated SACCH and FACCH. The 51 multiframe is used to carry BCCH, CCCH (including PCH, RACH, and AGCH), and SDCCH (and its associated SACCH). A superframe lasts 6.12 s, corresponding to 51×26 multiframes or 26×51 multiframes. A hyperframe corresponds to 2048 superframes (a total of 2,715,648 frames, lasting just under 3 h, 28 min, and 54 s). When numbering frames over the air interface, each frame is a numbered modulo of its hyperframe. In other words, a frame can have a *Frame Number (FN)* from 0 to 2,715,467. The reason for the large hyperframe is to allow for a large value of FN, which is used as part of the encryption over the air interface.

Certain time slots on a given RF carrier may be allocated to control channels, whereas the remaining time slots are allocated for traffic channels. For example, time slot 0 on the first carrier in a cell is used to carry the BCCH and CCCH. It also may carry four SDCCH channels. It is also common to find that time slot 1 on the first RF carrier in a cell is used to carry eight SDCCHs (with the associated SACCHs), with the remaining time slots allocated as TCHs. Exactly how much SDCCH capacity is allocated depends on the number of carriers and the amount of traffic in the cell. Figure B.8 shows two typical arrangements.

As mentioned, the 26 multiframe is used for the TCH. The structure is depicted in Figure B.9, where only one time slot per frame is shown (only full-rate TCH is considered in the figure). A given time slot carries user traffic (voice) for 24 of 26 frames. One of the 26 frames is idle, and one of the 26 frames carries the SACCH. The FACCH is transmitted by preempting half or all of the user traffic in a TCH.

This overall structure enables a TCH to have a gross bit rate of 22.8 kbps. Of course, this rate is not allocated completely to user data (such as speech). Rather, a sophisticated coding and interleaving scheme is applied. This scheme adds a significant number of bits

BCCH/ CCCH/ SDCCH/4	TCH	TCH	TCH	TCH	TCH	TCH	TCH
---------------------------	-----	-----	-----	-----	-----	-----	-----

SDCCH sharing time slot zero with BCCH and CCCH, common when only one carrier per cell.

BCCH/ CCCH	SDCCH/8	TCH	TCH	TCH	TCH	TCH	TCH
TCH	TCH	TCH	TCH	TCH	TCH	TCH	TCH

SDCCH using time slot one on first carrier — common when more than one carrier per cell.
Second carrier dedicated to traffic channels.

FIGURE B.8 Example GSM air-interface time slot allocations.

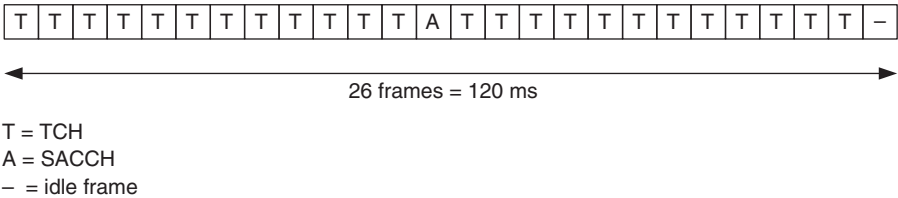


FIGURE B.9 TCH/SACCH framing structure.

for error detection and correction, which reduces the bandwidth available for raw user data. In fact, for standard GSM *Full-Rate* (FR) voice coding, the speech is carried at 13 kbps, and for *Enhanced-Full-Rate* (EFR) voice coding, the speech is carried at 12.2 kbps. Although it may seem that a great deal of the gross 22.8 kbps is consumed by coding overhead, it is worth remembering that an RF interface is unreliable at best, and error-correction overhead is necessary to overcome the limitations of the medium.

Since the control channels (with the exception of FACCH and SACCH) are carried on different time slots from the TCHs, it is possible to have a different framing structure. In fact, a 51-multiframe structure is used for transmitting the control channels, and this structure applies to any time slot that is allocated to control channels.

B.4.5 GSM Traffic Scenarios

The following sections provide some straightforward examples of GSM traffic. This allows for an understanding of the differences between the technologies, the evolution from one to the other, and how compatibility can be achieved.

B.4.6 Location Update

When an MS is first turned on, it must first “camp on” a suitable cell. This largely involves scanning the air interface to select a cell with a suitably strong received signal strength and then decoding the information broadcast by the BTS on the BCCH. Generally, the MS will camp on the cell with the strongest signal strength, provided that the cell belongs to the *Home Public Land Mobile Network* (HPLMN) and provided that the cell is not barred. The MS then registers with the network, which involves a process known as *location updating*, as shown in Figure B.10.

The sequence begins with a channel request issued by the MS on the RACH. This includes an establishment cause, such as location updating, voice-call establishment, and emergency-call establishment. In the example in Figure B.10, the cause is location updating.

The BSS allocates an SDCCH for the MS to use. It instructs the MS to move to the SDCCH by sending an immediate assignment message on the AGCH. The MS then moves to the SDCCH and sends the location updating request. This contains a set of information including the location area identity (as received by the MS on the BCCH) and the mobile identity. The mobile identity is usually either the *International Mobile Subscriber Identity* (IMSI) or the *Temporary Mobile Subscriber Identity* (TMSI). This is sent through the BSS to the MSC using a generic message known as *Complete Layer 3 Info*. This message is included as part of an SCCP Connection Request. Hence, it uses connection-oriented SCCP.

If the subscriber attempts to register with TMSI and the TMSI is unknown in the MSC/VLR, then the MSC/VLR may request the MS to send the IMSI (not shown in the figure). Equally, the MSC/VLR may request the MS to send the IMEI so that it can be checked (also not shown in the figure).

On receipt of the location updating request, the MSC/VLR may attempt to authenticate the subscriber. If the MSC/VLR does not already have authentication information for the subscriber, then it requests that information from the HLR, using the *Mobile Application Part* (MAP) operation *Send Authentication Info*. The HLR/AuC sends a *MAP Return Result* (RR) with up to five authentication vectors, known as *triplets*. Each triplet contains a *Random Number* (RAND) and a *Signed Response* (SRES).

The MSC sends an *Authentication Request* to the MS. This contains only the RAND. The MS performs the same calculations as were performed in the HLR/AuC and sends an *Authentication Response* containing an SRES parameter. The MSC/VLR checks to make sure that the SRES received from the MS matches that received from the HLR/AuC. If a match is made, then the MS is considered authenticated.

At this point, the MSC/VLR uses the MAP operation *Update Location* to inform the HLR of the subscriber's location. The message to the HLR includes the subscriber's IMSI and the *SS7 Global Title Address* (GTA) of the MSC and VLR. The HLR immediately sends a *MAP Cancel Location* message to the VLR (if any) where the subscriber had been registered previously. That VLR deletes any stored data related to the subscriber and issues a return result to the HLR.

The HLR uses the MAP operation *Insert Subscriber Data* to the VLR to inform the VLR about a range of data regarding the subscriber in question, including information regarding supplementary services. The VLR acknowledges receipt of the information. The HLR then issues a return result to the MAP *Update Location*.

On receipt of that return result, the MSC/VLR sends the DTAP message *Location Updating Accept* to the MS. It then clears the SCCP connection to the BSS. This causes the BSS to release the MS from the SDCCH by sending a *Channel Release* message to the MS.

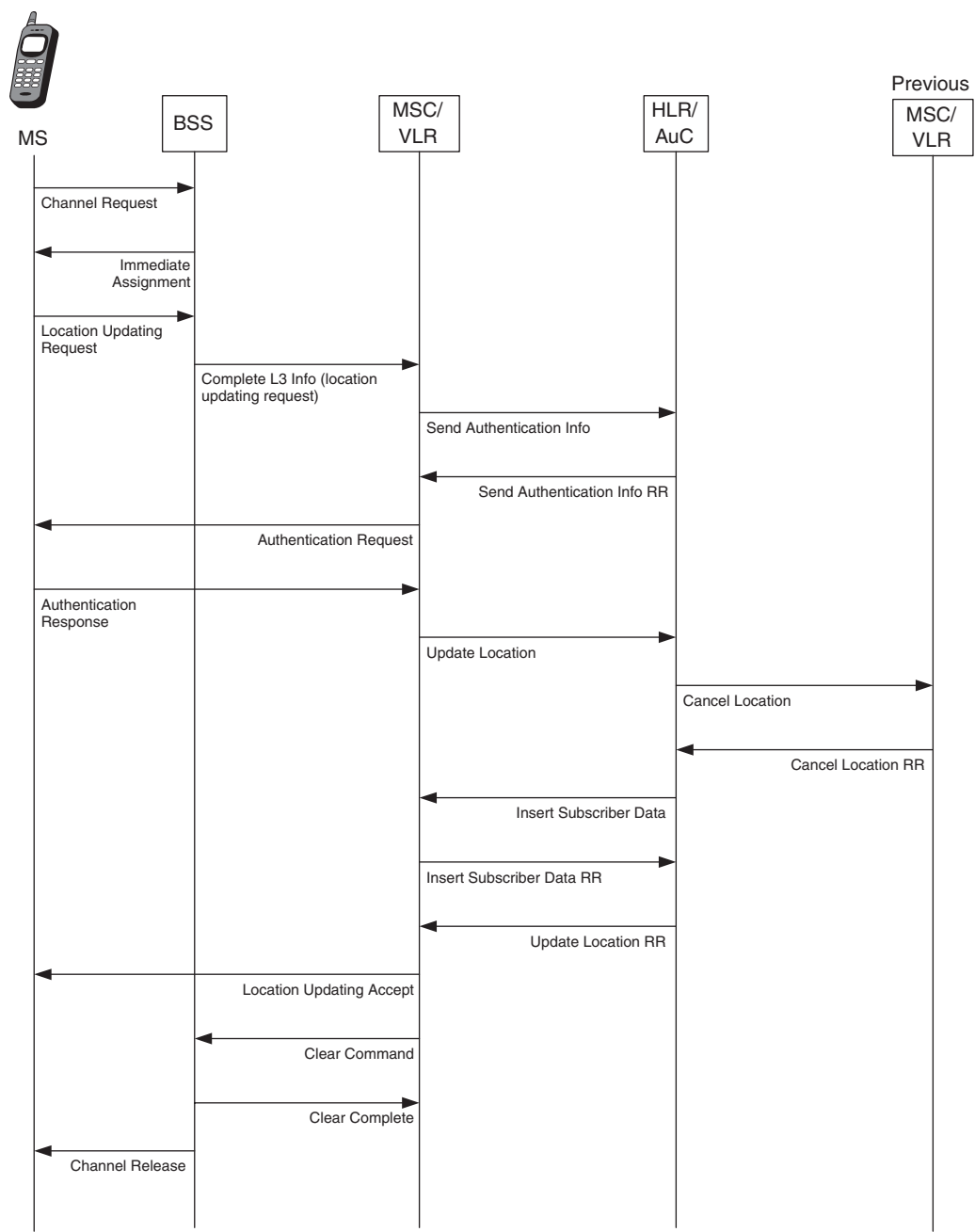


FIGURE B.10 GSM location update.

A number of optional messages have been excluded from Figure B.10. For a complete understanding of all the options, the reader is referred to GSM Specification 04.08. A number of messages shown in Figure B.10 (e.g., Channel Request, Immediate Assignment, and Channel Release) are common to many traffic scenarios. For the sake of brevity, they are not shown in the following call examples.

B.4.7 Mobile-Originated Voice Call

Figure B.11 shows a basic mobile-originated call to the PSTN. After the MS has been placed on an SDCCH by the BSS (not shown), the MS issues a CM Service Request to the MSC (CM 5 Connection Management). This includes information about the type of service that the MS wants to invoke (a mobile-originated call in this case, but it also could be another service such as SMS).

On receipt of the CM Service Request, the MSC optionally may invoke authentication of the mobile. Typically, an MSC is configured to authenticate a mobile whenever it performs an initial location update and every N transactions thereafter (every N calls). Next, the MSC initiates ciphering so that the voice and data sent over the air are encrypted. Since it is the BSS that performs the encryption and decryption, the MSC needs to pass the *Cypher Key* (Kc) to the BSS. The BSS then instructs the MS to start ciphering. The MS, of course, generates the Kc independently so that it is not passed over the air. Once the MS has started ciphering, it informs the BSS, which, in turn, informs the MSC.

Next, the MS sends a Setup message to the MSC. This includes further data about the call, including information such as the dialed number and the required bearer capability. Once the MSC has determined that it has received sufficient information to connect the call, it lets the MS know by sending a Call Proceeding message.

Next, using the Assignment Request message, the MSC requests the seizure of a circuit between the MSC and BSS. That circuit will be used to carry the voice to and from the MS. At this point, the BSS sends an Assignment Command message to the MS, instructing the MS to move from the SDCCH to a TCH. Further signaling between the MS and the network now will occur on the FACCH associated with the assigned TCH. The MS responds with an Assignment Complete message, indicating that it has moved to the assigned TCH. On receipt of this message, the BSS sends an Assignment Complete message to the MSC, which indicates that a voice path is now available from the MS through to the MSC.

On receipt of the Assignment Complete message from the BSS, the MSC initiates the call setup toward the PSTN. This starts with issuance of an *Initial Address Message* (IAM). A subsequent receipt of an *Address Complete Message* (ACM) from the destination end indicates that the destination phone is now ringing. The MSC informs the MS of this fact by sending an Alerting message. In addition, the ACM triggers a one-way path to be opened from the destination PSTN switch through to the MS, and the ring-back tone heard at the MS is actually being generated at the destination PSTN switch.

Upon answer at the called phone, an *Answer Message* (ANM) is returned. This leads the MSC to open a two-way path to the MS and also causes the MSC to send a Connect message to the MS. On receipt of the Connect message, the MS responds with a Connect Acknowledge message. The two parties are now in conversation, and from a billing perspective, the clock is now ticking.

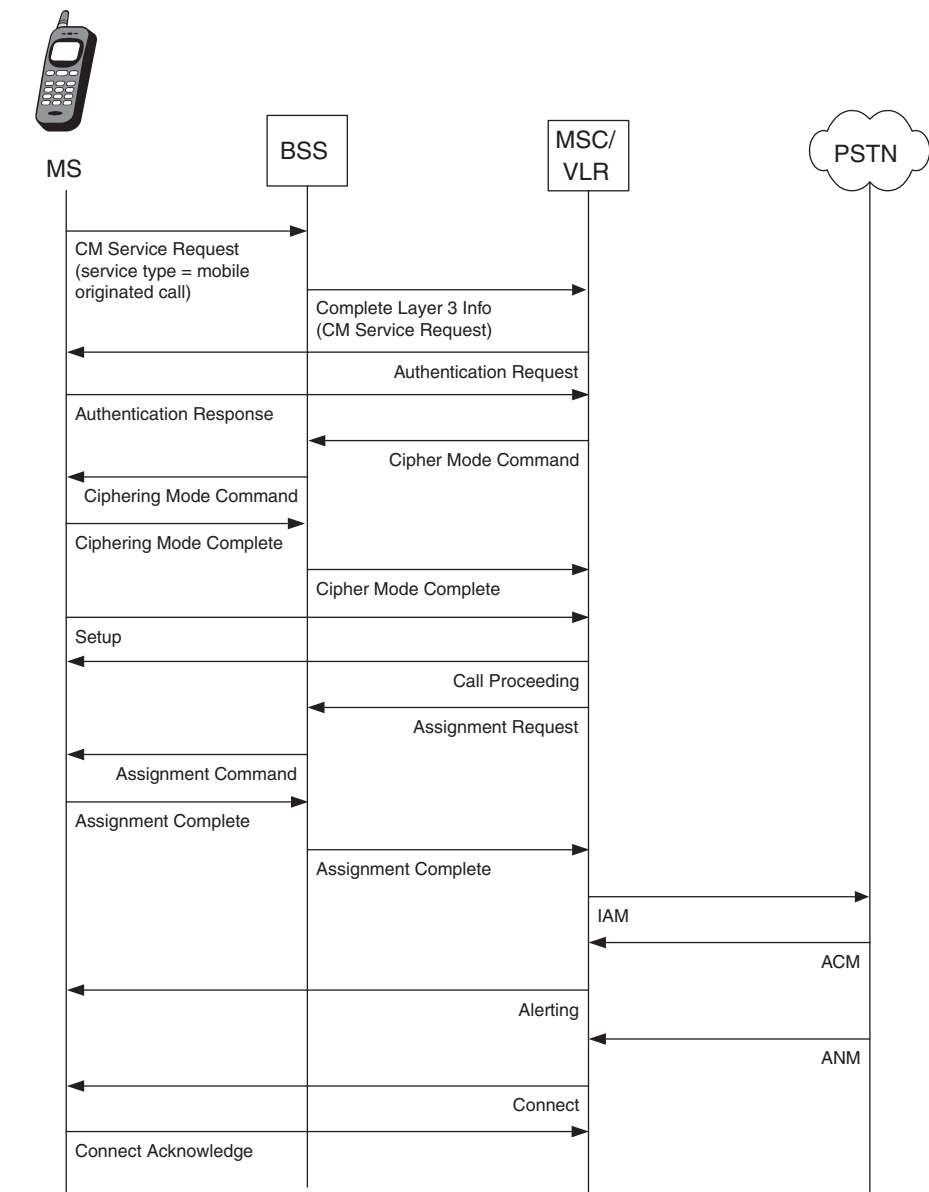


FIGURE B.11 Mobile-to-land call flow diagram.

B.4.8 Mobile-Terminated Voice Call

Figure B.12 shows a basic mobile-terminated call from the PSTN. It begins with the arrival of an IAM at the GMSC. The IAM contains the directory number of the called subscriber, known as the *Mobile Station ISDN Number (MSISDN)*. The GMSC uses this information to determine the applicable HLR for the subscriber and invokes the MAP

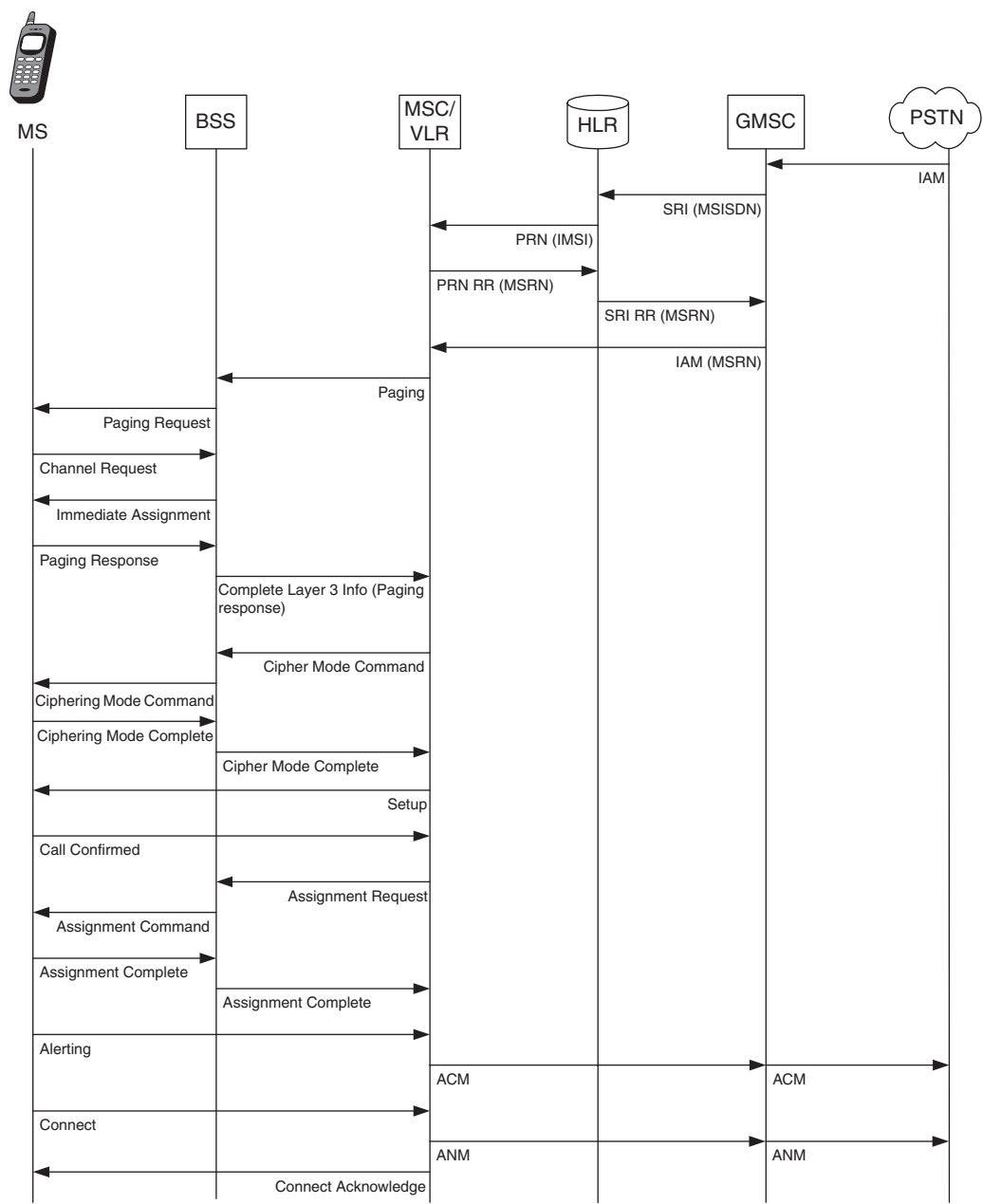


FIGURE B.12 Land-to-mobile call flow diagram.

operation *Send Routing Information* (SRI) toward the HLR. The SRI contains the subscriber's MSISDN.

The HLR uses the MSISDN to retrieve the subscriber's IMSI from its database. Through a previous location update, the HLR knows the MSC/VLR that serves the

subscriber, and it queries that MSC/VLR using the MAP operation *Provide Roaming Number* (PRN), which contains the subscriber's IMSI. From a pool, the MSC/VLR allocates a temporary number, known as a *Mobile Station Roaming Number* (MSRN), for the call and returns that number to the HLR. The HLR returns the MSRN to the GMSC.

The MSRN is a number that appears to the PSTN as a dialable number. Thus, it can be used to route a call through any intervening network between the GMSC and the visited MSC/VLR. In fact, this is exactly what the GMSC does. It routes the call to the MSC/VLR by sending an IAM, with the MSRN as the called-party number. On receipt of the IAM, the MSC/VLR recognizes the MSRN and knows the IMSI for which the MSRN was allocated. At this point, the MSRN can be returned to the pool for use with another call.

Next, the MSC requests the BSS to page the subscriber using the Paging Request message, which indicates the location area where the subscriber should be paged. The BSS uses the PCH to page the MS.

On receipt of the page, the MS attempts to access the network using a Channel Request message on the RACH. The BSS responds with an Immediate Assignment message, instructing the MS to move to an SDCCH. The MS moves to the SDCCH and, once there, indicates to the network that it is responding to the page. The BSS passes the response to the MSC.

At this point, the MSC optionally may authenticate the MS (not shown). It then will proceed to initiate ciphering, which is done in the same manner as was described previously for a mobile-originated call. Once ciphering is started, the MSC sends a Setup message to the MS. This is similar to the Setup message that is sent from an MS for a mobile-originated call, including information such as the calling-party number and the required bearer capability.

On receipt of the Setup message, the MS sends a Call Confirmed message to the MSC, indicating that it has the information it needs to establish the call. The Call Confirmed message acts as an instruction to the MSC to establish a path through to the MS. Therefore, the MSC begins the assignment procedure, which establishes a circuit between the MSC and the BSS and a TCH between the BSS and the MS (rather than an SDCCH). Further signaling between the MS and the network now will use the FACCH associated with the TCH to which the MS has been assigned.

Once established on the TCH, the MS starts ringing to alert the user and informs the network by sending the Alerting message to the MSC. This triggers the MSC to open a one-way path back to the original caller, generate a ring-back tone, and send an ACM back to the originating PSTN switch via the GMSC.

Once the called user answers, the MS sends a Connect message to the MSC. This triggers the MSC to send an ANM back to the originating switch and to open a two-way path. Finally, it sends Connect Acknowledge to the MS, and conversation begins.

B.4.9 Handover

A *handover* (also known as a *handoff*) is the process by which a call in progress is transferred from a radio channel in one cell to another radio channel either in the same cell or in a different cell. A handover can occur within a cell, between cells of the same BTS, between cells of different BTSs connected to the same BSC, between cells of different BSCs, or between cells of different MSCs. Not only can a handover occur between TCHs, but a handover is also possible from an SDCCH on one cell to an SDCCH on another cell. It is also possible from an SDCCH on one cell to a TCH on another cell. The most common, however, is a handover from TCH to TCH.

Depending on the source (the original cell) and the target (the destination cell) involved in the handover, the handover may be handled completely within a BSS or may require the involvement of an MSC. In the case where a handover occurs between cells of the same BSC, the BSC may execute the handover and simply inform the MSC after the handover has taken place. If, however, the handover occurs between BSCs, then the MSC must become involved because no direct interface exists between BSCs.

A handover in GSM is known as a *Mobile-Assisted Handover* (MAHO). This means that it is the network that decides if, when, and how a handover should take place. The MS, however, provides information to the network to enable the network to make the decision.

Recall that GSM is a TDMA system, with eight time slots per frame in the case of FR speech. This means that the MS is transmitting for one-eighth of the time and receiving for one-eighth of the time. In fact, at the BTS, a given time slot on the uplink is three time slots later than the corresponding downlink time slot, which means that the MS is not required to receive and transmit simultaneously. We note that this offset is specified at the BTS rather than at the MS because the distance of the MS from the BTS influences the exact instant at which the MS should transmit. For example, when an MS is close to the BTS, it should transmit slightly later than if it were farther from the BTS. This variation is known as *time alignment* and is controlled by the BSS. In other words, the BSS periodically instructs the MS to change its time alignment as necessary.

Nonetheless, it is clear that for most of the time the MS is neither transmitting nor receiving. During this time, the MS has the opportunity to tune to other carrier frequencies and determine how well it can receive those signals. It then can relay that information to the network to allow the network to make a determination as to whether the MS would be better served by a different cell. Because of frequency reuse, it is possible that a number of nearby cells might be using the same BCCH frequency. Therefore, it is not sufficient for the MS simply to report signal strength for specific frequencies. Rather, the MS must be able to synchronize to the BCCH of neighboring cells and decode the information being transmitted. Exactly which frequencies the MS should check for are specified in system information messages transmitted by the BTS on the BCCH and the SACCH. The MS sends measurement reports to the BSS on the SACCH as often as possible. These reports include information on how well the MS can “hear” the serving cell, as well as information about signal-strength measurements on up to six neighboring cells. Specifically, for the serving cell, the MS reports the RXLEV (an indication of received signal strength) and the RXQUAL (an indication of the bit error rate on the received signal). For neighboring cells, the MS reports the BSIC, the BCCH frequency, and the RXLEV.

In addition to the measurements reported by the MS, the BTS itself makes measurements regarding the RXLEV and RXQUAL received from the MS. These measurements and those from the MS are reported to the BSC. Based on its internal algorithms, the BSC makes the decision as to whether a handover should occur and, if so, to which cell.

Figure B.13 shows an inter-BSC handover. In this case, it is not sufficient for the BSC to handle the handover autonomously—it must involve the MSC. Therefore, once the serving BSC determines that a handover should take place, it immediately sends the message *Handover Required* to the MSC. This message contains information about the desired target cell (or the cells in the preferred order) plus information about the current channel that the MS is using. The MSC analyzes the information and identifies the target BSC associated with at least one of the target cells identified

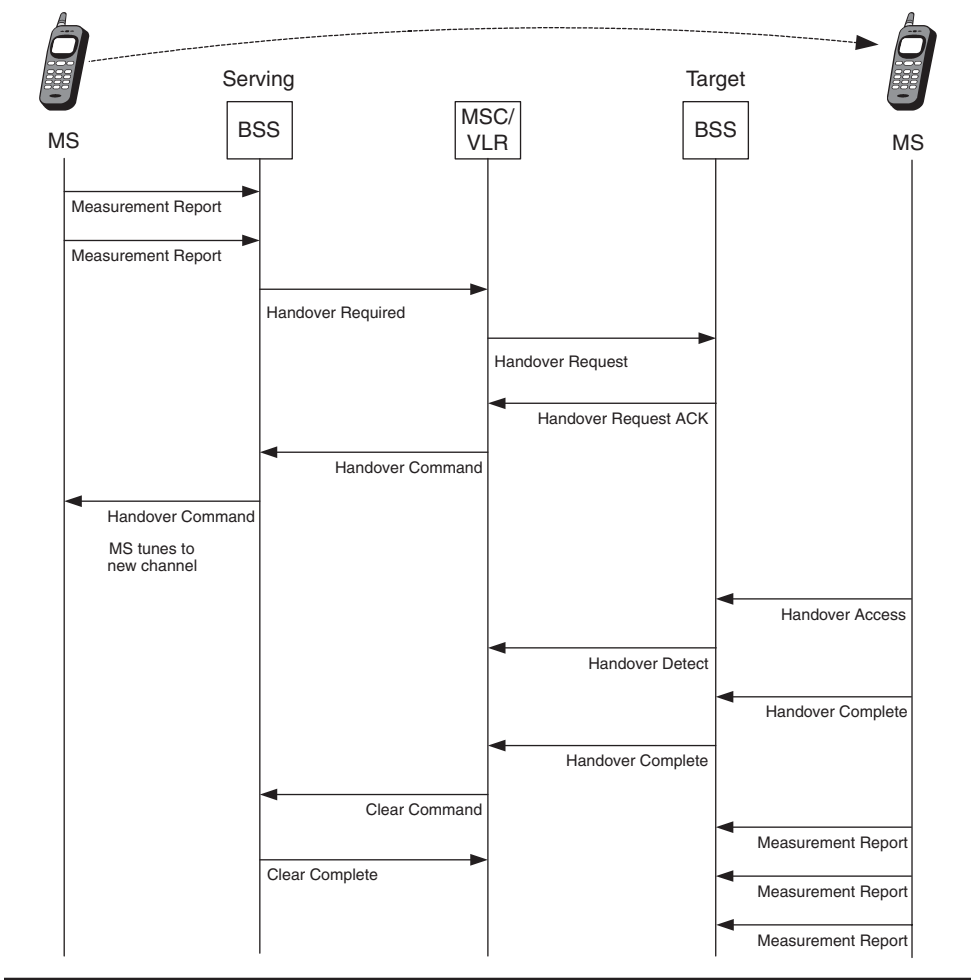


FIGURE B.13 Inter-BSC handover.

by the source BSC. It then sends a Handover Request message to the target BSC. This contains, among other items, information about the target cell, the type of channel required, and in the case of a speech or data call, the circuit to be used between the MSC and the target BSC.

If the target BSC can accommodate the handover (if resources are available), then it allocates the necessary resources and responds to the MSC with the Handover Request Acknowledge message. This message contains a great deal of information regarding the cell and channel to which the MS is to be transferred, such as the cell identity, the exact channel to be used (including the type of channel), synchronization information, the power level to be used by the MS when accessing the new channel, and a handover reference. The MSC then sends the Handover Command message to the serving BSC. This message is used to relay the information received from the target BSC. On receipt

of the Handover Command message from the MSC, the serving BSC passes the information to the MS in a Handover Command message over the air interface.

On receipt of the Handover Command message, the MS releases existing RF connections, tunes to the target channel, and attempts to access that channel. On access, it may send a Handover Access message to the target BSS. It will do so if it was commanded to do so in the Handover Command message. If the Handover Access message is received by the target BSS, then it sends a Handover Detect message to the MSC. When the MS has established all lower-layer connections on the target channel, it sends a Handover Complete message to the target BSC, which, in turn, sends a Handover Complete message to the MSC. At this point, the MS again starts taking measurements of neighboring cells. Meanwhile, the MSC instructs the old BSC to release all radio and terrestrial resources related to the MS.

B.4.10 Traffic Calculation Methods

As with any mobile communications technology, traffic calculation and system dimensioning for GSM begin with an estimation of how much traffic demand there will be and from where it will come. In other words, one must estimate the traffic demand in the coverage of each cell. This is rather an inexact science. One certainly can acquire demographic data such as population density, average household income, and so on. One also can acquire data related to vehicular traffic in order to estimate traffic demand for cells that cover roads. Based on these factors and others (such as how many competing operators exist), one makes an estimate of the peak traffic demand per cell. This estimate may well be incorrect. Fortunately, however, time is an ally. In a new network, traffic demand grows gradually, which provides the operator with sufficient time to monitor usage and more accurately predict traffic demand over time.

Because all GSM traffic is circuit-switched, network dimensioning is a relatively straightforward process once traffic demand per cell is specified. The process largely involves determining the amount of traffic to be carried in the busy hour and dimensioning the network according to Erlang tables.

The air interface, which represents the scarcest resource in the network, is dimensioned with the highest blocking probability. Typically, network designers dimension the air interface according to a 2 percent blocking probability (Erlang B). For a one-TRX cell with seven TCHs (BCCH, CCCH, and SDCCH/4 are sharing time slot 0), the cell can accommodate approximately 2.9 Erlangs. For a two-TRX cell with 14 TCHs (time slot 0 on one carrier is used for BCCH and CCCH and time slot 1 is used for SDCCH/8), the cell can accommodate approximately 8.2 Erlangs. For a three-TRX cell with 22 TCHs (one time slot is allocated for SDCCH/8), the cell can accommodate approximately 14.9 Erlangs. It is important to note that the traffic-carrying capacity of each cell must be calculated independently.

Other interfaces in the network usually are dimensioned at much lower blocking probabilities. For example, the A interface typically would be designed for a 0.1 percent blocking probability. Similar blocking would apply to other network-internal interfaces such as the interface between the MSC and IWF. Typically, interfaces to other networks, such as the PSTN, are dimensioned at slightly higher blocking probabilities—such as 0.5 percent. Of course, the choice of blocking probability for any interface is a balance between cost and quality. The lower the blocking probability, the higher is the quality, and the higher is the cost. The higher the lower blocking probability, the lower is the quality, and the lower is the cost.

B.5 IS-136 System Description

IS-54 and IS-136 represent the most direct evolution from 1G systems. In fact, IS-54 and IS-136 were designed to allow significant compatibility with analog AMPS so that dual-mode handsets could be developed at a reasonable cost. Since IS-54 and then IS-136 began initially as islands in a sea of AMPS coverage, it was important to have dual-mode phones so that subscribers still could obtain AMPS coverage when roaming outside of IS-54 or IS-136 coverage.

IS-54 represents the first step in moving from analog AMPS to digital technology and is often known as *Digital AMPS* (D-AMPS). IS-54 could be called a generation 2.5 technology because it is not completely digital. Only the voice channels are digital—the control channel is still analog. Introduction of the digital control channel came about with introduction of IS-136. Nevertheless, IS-54 was an important step forward because it provided a number of significant advantages over AMPS, including increased system capacity and security through support for authentication. Support for authentication within analog AMPS had been designed already, but since it involved changes to the air interface, it required support within the handsets. Unfortunately, millions of handsets were already in the field, and these did not support authentication. IS-54, however, required new handsets, and these new phones incorporated authentication from the start.

B.5.1 The IS-54 Digital Voice Channel

IS-54 takes the existing 30-kHz AMPS voice channel and, applying *Time-Division Multiplexing* (TDM), divides it into a number of time slots, as shown in Figure B.14. Rather than having a full 30-kHz channel for a conversation, each user is assigned a number of

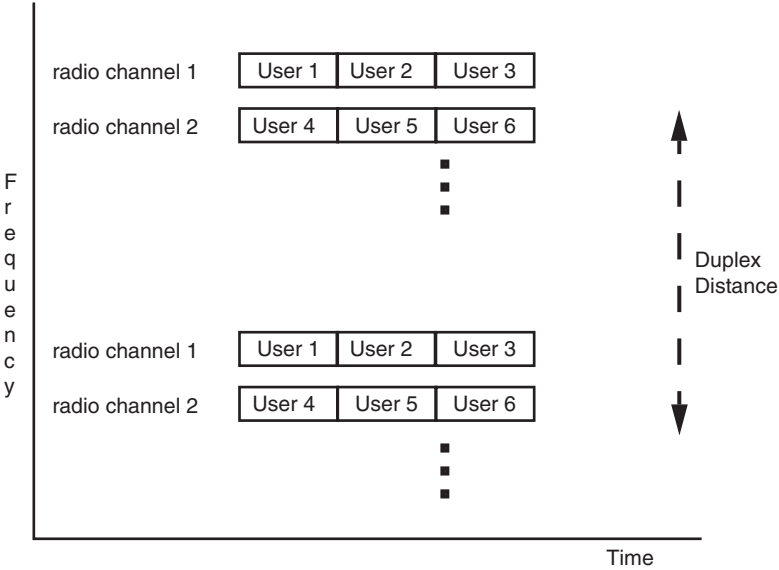


FIGURE B.14 Time-Division Multiplexing (TDM).

time slots, each known as a *Digital Traffic Channel* (DTC). In IS-54, typically three users are supported on a given RF channel. Having three users per RF channel implies an obvious increase in capacity over analog AMPS, which supports just a single user on an RF channel.

B.5.1.1 Voice Channel Structure

Associated with each DTC are two other channels—the *Fast Associated Control Channel* (FACCH) and the *Slow Associated Control Channel* (SACCH). The FACCH is a signaling channel used for the transmission of control and supervisory information between the mobile and the network. For example, if a mobile is to send DTMF tones, then these are indicated on the FACCH. The SACCH is also used for the transmission of control and supervisory information between the mobile and the network. Most notably, the SACCH is used by the mobile to transmit measurement information to the network describing the mobile’s experience of the RF conditions. This information is used by the network to determine when and how a handoff should occur.

Figure B.15 shows the structure of the DTC. It is notable that the figure does not show the FACCH. This is so because the DATA field, which is normally used to transmit voice, is also used to transmit FACCH information. In other words, if information is to

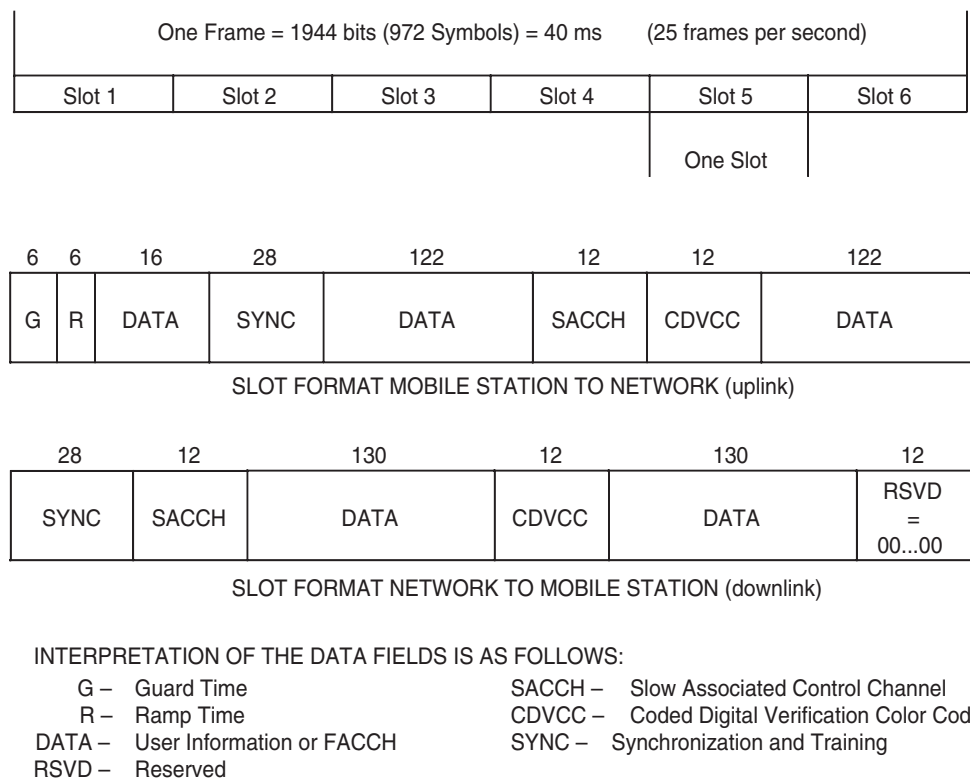


FIGURE B.15 Digital Traffic Channel (DTC).

be sent on the FACCH, then user data are suspended briefly while the FACCH information is being sent. Figure B.15 also shows six time slots within the frame structure. In fact, IS-54 enables two types of mobiles: full rate and half rate. A full-rate mobile uses two of the time slots in the frame (1 and 4, 2 and 5, or 3 and 6), whereas a half-rate mobile uses just a single time slot. A full-rate mobile transmits 260 bits of speech per time slot (520 bits per frame). Since there are 25 frames per second, this means that the gross bit rate for speech is 13 kbps. In practice, only full-rate handsets are used.

In addition to the user data and SACCH within the DTC, we see a number of other fields, as follows:

- *Guard Time*. This field is three symbols (6 bits) in duration. It is used as a buffer between adjacent time slots employed by different mobiles and enables compensation for variations in distance between the mobile and the base station.
- *Ramp Time*. This is three symbols in duration allowing for ramp-up of the RF power.
- *Sync*. This is a special synchronization pattern that is unique for a given time slot. It is used for correct time alignment.
- *Coded Digital Voice Color Code (CDVCC)*. This is analogous to the Supervisory Audio Tone used in analog AMPS. It is used to detect cochannel interference.

B.5.1.2 Offset Between Transmit and Receive

IS-54 is a frequency-duplex TDMA system. In other words, the mobile transmits on one frequency and receives on another frequency. In the uplink, the mobile transmits on a given pair of time slots, and on the downlink, it receives on the corresponding pair of time slots. If, for example, a given mobile transmits on time slots 1 and 4 on the uplink, then it receives on time slots 1 and 4 on the downlink. Time slots 1 and 4 on the downlink do not, however, correspond to the same instants in time as time slots 1 and 4 on the uplink. A time offset between the downlink and the uplink corresponds to one time slot plus 45 symbol periods (207 symbol periods total, or 8.5185 ms), with the downlink lagging the uplink. Therefore, the mobile does not transmit and receive simultaneously. Rather, during a conversation, it receives a time slot on the downlink shortly after sending a time slot on the uplink. Figure B.16 depicts this offset, showing the transmission and reception by a given mobile on time slots 1 and 4.

As can be seen from Figure B.16, times will occur when the mobile is neither transmitting on a given time slot nor listening to the base station on the corresponding downlink time slot. So what does it do during these times? Rather than do nothing, the mobile tunes briefly to other base stations to measure the signal from those base stations. As described later in this Appendix, these measurements can be provided to the network to assist the network in determining when a handoff should take place.

B.5.1.3 Speech Coding

Because the DTC is digital, it is necessary to convert the user speech from analog form to digital. In other words, the handset (and the network) must include a digital speech-coding scheme. In IS-54, the speech-coding technique uses *Vector Sum Excited Linear Prediction* (VSELP). This is a *Linear Predictive Coding* (LPC) technique that operates on

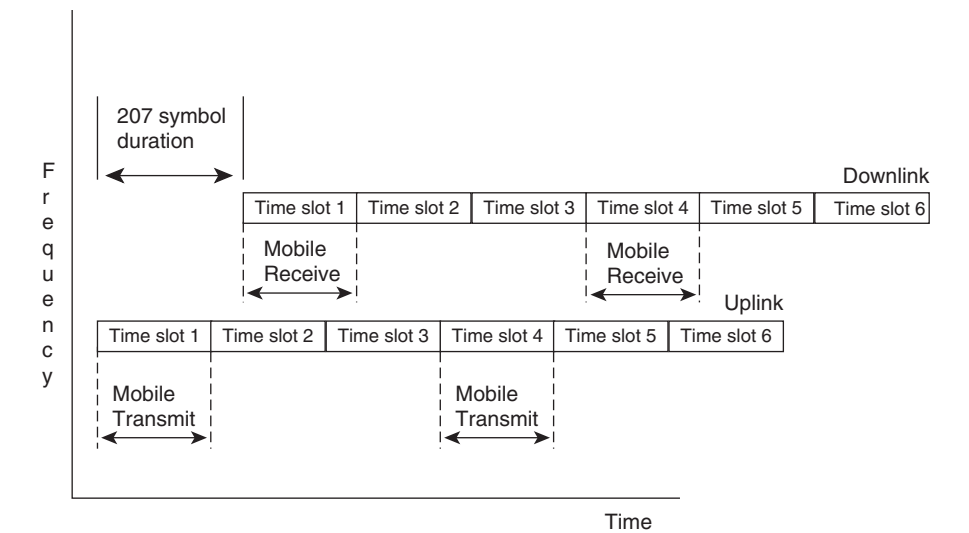


FIGURE B.16 Transmit and receive offset.

20-ms speech samples at a time. For each 20-ms sample, the coding scheme itself generates 159 bits. Thus, the coder provides an effective bit rate of 7.95 kbps.

The RF interface, however, is an error-prone medium. Therefore, to ensure high speech quality, it is necessary to include mechanisms that mitigate against errors caused in RF propagation. Consequently, the 159 bits are subject to a channel-coding scheme designed to minimize the effects of errors. Of the 159 bits, 77 are considered class 1 bits (of greater significance to speech perception), and 82 are considered class 2 bits. As shown in Figure B.17, the 77 class 1 bits are passed through a convolutional coder,

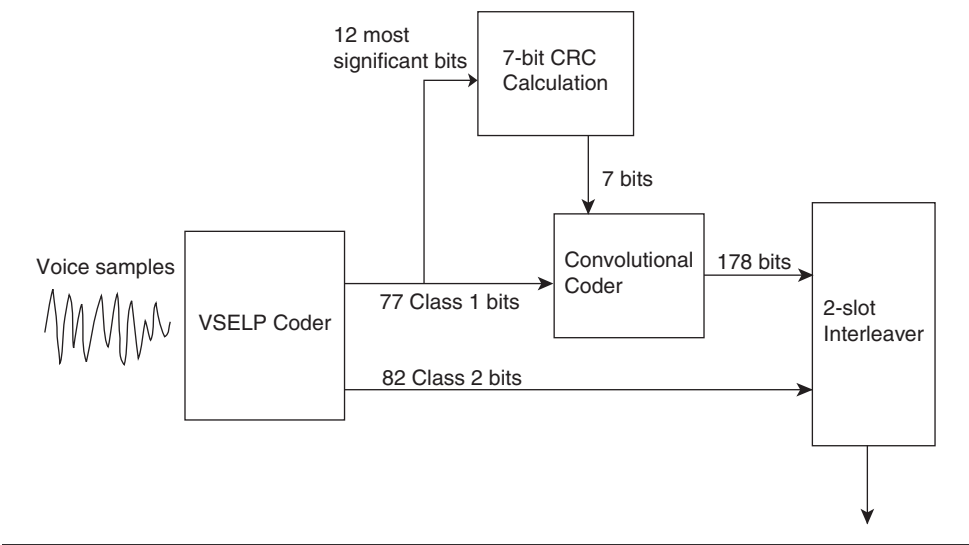


FIGURE B.17 IS-S4 speech coding.

which results in 178 bits. These 178 bits are combined with the 82 class 2 bits to give a total of 260 bits, and the 260 bits are allocated across the time slots used by the subscriber. Thus, each 20 ms of speech gives rise to a transmission of 260 bits, resulting in a gross rate of 13 kbps over the air interface.

B.5.1.4 Time Alignment

Since three mobiles use a given RF channel on a time-sharing basis, it is necessary that they each time their transmissions exactly. Otherwise, their signals would overlap and cause interference at the BSR. Furthermore, a given cell may be many miles in diameter, and the time for transmission from one mobile to the base station may be different from the time taken by the transmission from another mobile. Therefore, if one mobile begins transmission immediately after another mobile stops transmission, it is possible that the two signals could collide at the base station.

For example, consider a situation where mobile *A* is far away from the base station and mobile *B* is close to the base station. It takes longer for mobile *B*'s transmission to reach the base station than that of mobile *A*. Therefore, if mobile *A* starts transmitting immediately after mobile *B* stops transmitting, the transmission from mobile *B* still could be arriving at the base station when mobile *A*'s transmission starts to arrive. Consequently, it is necessary not just to ensure that no two mobiles transmit at the same time but also to time transmissions such that no two transmissions arrive at the base station at the same time. The methodology for this timing is called *time alignment*, which involves advancing or retarding the transmission from a given mobile so that the transmission arrives at the base station at the correct time relative to transmissions from other mobiles using the same RF channel.

When a mobile first accesses the system, the network assigns it a traffic channel, including a *Digital Voice Color Code* (DVCC). At this point, however, the network has not provided any time-alignment information. Given that the mobile could be close to the base station or far away, it needs the correct time-alignment information before transmitting real user data, which means that the base station must determine roughly how far away the mobile happens to be and must send time-alignment instructions. In order to help the base station determine what the time-alignment instructions should be, the mobile sends a special sequence of 324-bit duration called a *shortened burst*, as shown in Figure B.18. The structure of the shortened burst is such that if the base station detects



- G1: 3 symbol length guard time.
 - R: 3 symbol length Ramp time.
 - S: 14 symbol length Sync Word; the mobile station uses its assigned sync word.
 - D: 6 symbol length CDVCC; the mobile station uses its assigned DVCC.
 - G2: 22 Symbol length guard time.
- V = 0000
W = 00000000
X = 000000000000
Y = 0000000000000000

FIGURE B.18 Shortened burst structure.

two or more sync words of the burst, it can determine the mobile's distance from the base station. The base station then sends a Time Alignment Message instructing the mobile to adjust its transmission timing.

B.5.2 Control Channel

Even though the IS-54 control channel is analog, and even though IS-54 is designed to include a certain degree of compatibility with analog AMPS, the control channel contains a number of significant differences from the analog control channel. These changes were introduced to overcome known problems in AMPS and to provide control-channel support for digital voice channels. For example, when assigning a mobile to a given traffic channel, the downlink control channel must specify the time slots to be used by the mobile. Obviously, such capability does not exist in the standard AMPS control channel.

Access to the TDMA system is achieved through either the primary control channel, used for analog communication, or the secondary dedicated control channel. During the initial acquisition phase, the mobile reads the overhead control message from the primary control channel and determines if the system is digital-capable. If the system is digital-capable, a decision will be made whether to use the primary or secondary dedicated control channel. The secondary dedicated control channels are assigned as FCC channels 696 to 716 for the A-band system and channels 717 through 737 for the B-band system. Use of the secondary dedicated control channels enables a variety of enhanced features to be provided by the system operator to subscribers.

IS-136 brings to the table the *Digital Control Channel* (DCCH), and it enables the delivery of adjunct features that were not really possible in cellular. The DCCH occupies two of the six time slots, and therefore, if a physical radio also has a DCCH assigned to it, only two subscribers can use the physical radio for communication purposes.

The DCCHs can be located anywhere in the allocated frequency band; however, certain combinations of channels are preferred. The preference is based on the method that the subscriber unit uses to scan the available spectrum looking for the DCCH.

The preferred channel sets are broken down into 16 relative probability blocks for each frequency band of operation, both cellular and PCS. Relative probability block a_1 is the first group of channels the subscriber unit uses to find the DCCH for the system and cell. The subscriber unit then will scan through the entire frequency band, going through channel sets according to the relative probability blocks until it finds a DCCH. In the case of cellular, if no DCCH is found, it reverts to the control channel for a dual-mode phone and then either acquires the system through the control channel or is directed to a specific channel that has the DCCH.

B.5.3 MAHO

One of the unique features associated with TDMA is the capacity for a *Mobile-Assisted Handoff* (MAHO). The MAHO process enables the mobile to constantly report back to the cell site, indicating its present condition in the network. The cell site is also collecting data on the mobile through the reverse link measurements, but the forward link, base to mobile, is being evaluated by the mobile itself, therefore providing critical information about the status of the call.

For the MAHO process, the mobile measures the *Received Signal Strength Level* (RSSL) received from the cell site. The mobile also performs a *Bit-Error-Rate* (BER) test and a *Frame-Error-Rate* (FER) test as another performance metric.

The mobile also measures the signals from a maximum of six potential digital hand-off candidates using either a dedicated control channel or a beacon channel. The channels used by the mobile for the MAHO process are provided by the serving cell site for the call. The dedicated control channel is either the primary or secondary control channel, and the measurements are performed on the forward link. The mobile also can use a beacon channel for the performance measurement. The beacon channel is either a TDMA voice channel or an analog channel, both of which are transmitting continuously with no dynamic power control on the forward link. The beacon channel is used when the setup or control channel for the cell site has an omni configuration and not a dedicated setup channel per sector.

B.5.4 Frequency Reuse

The modulation scheme used by the NADC TDMA system is a $\pi/4$ DQPSK format. The *C/I* levels used for frequency management associated with IS-54 or IS-136 are the same for analog, 17 dB *C/I*. The *C/I* level desired is 17 dB and is the same for DCCH and the DTC. This is convenient because in all the cellular systems, most of the channels are analog, and they too require a minimum of 17 dB *C/I*. The fundamental issue here is that the same *D/R* ratios can be and are used when implementing the radio channel assignments for digital.

The additional parameters associated with IS-136/IS-54 involve SDCC, DCC, and DVCC. DCC is the *Digital Color Code*, SDCC is the *Supplementary Digital Color Code*, and DVCC is the *Digital Verification Color Code*.

DCC and SDCC must be assigned to each sector, cell, or control channel of the system that uses IS-136/IS-54. The DCC is used by analog and dual-mode phones for accessing the system. The SDCC is used by dual-mode phones only and should be assigned to each control channel along with the DCC.

Parameter	Values
DCC	0, 1, 2, 3
SDCC	0–15

The DVCC is assigned to each DTC. A total of 255 different DVCC values exist, ranging from 1 to 255, leaving much room for variations in assignments.

B.5.4.1 Call Flow

No discussion of a wireless technology would be complete without a flow diagram. Figure B.19 illustrates a mobile-originated call with IS-136. The call flowchart in Figure B.19 is effectively the same for 800 and 1900 MHz. For 800-MHz systems, it is assumed that there are DCCHs and the FCCH; analog has the associated DCCH locator word in the overhead message.

Some additional comments will help in reviewing Figure B.19. An 800-MHz *Subscriber Unit* (SU) keeps the last-seen DCCHs in temporary memory and will scan these DCCHs in addition to the standard 21 analog control channel (ACC), tuning to the strongest signal. If the SU “camps on” an ACC, it will look for the DCCH locator word and retune to the DCCH, if possible. The SU will camp on the DCCH, if available, and camp on the strongest DCCH signal. If the SU cannot find a DCCH, it will tune to the strongest ACC.

BER	BER%	Voice Quality	
		ACELP	VSELP
0	<0.01	Good	Good
1	0.01–0.1	Good	Good
2	0.1–0.5	Good	Good
3	0.5–1.0	Good	Good
4	1.0–2.0	Good	Marginal
5	2.0–4.0	Marginal	Bad
6	4.0–8.0	Bad	Bad
7	>8.0	Bad	Bad

TABLE B.6 BER and Voice Quality Relationship

Also, a 1900-MHz SU will scan the initial set of DCCH frequencies it has programmed in, which can follow a standard list or be operator-specific. The SU will camp on the strongest signal. If it is not allowed to camp on that channel, it will go to another channel on the list. If it exhausts the primary selection list, it then will scan all channels looking for the DCCH.

B.5.5 Call Quality

The call quality with IS-136 depends on the RF environment. The RF environment conditions are reflected in the BER that is imparted on the digital signal for IS-136. Table B.6 shows the relationship between BER and voice quality, which can and should be used to help define the design and performance guidelines for the wireless network.

B.6 IS-95 System Description

Code-Division Multiple Access (CDMA), also known as *IS-95* and *J-STD-008*, is a spread-spectrum technology platform that enables multiple users to occupy the same radio channel, or frequency spectrum, at the same time. CDMA has been and is being used for microwave point-to-point communication and satellite communication, as well as by the military. With CDMA, subscribers, or users, employ their own unique code to differentiate themselves from other users. CDMA offers many unique features, including the ability to thwart interference and improved immunity to multipath effects owing to its bandwidth. The IS-95 technology has been championed by many system operators in the United States and Asia.

CDMA in this Appendix refers strictly to IS-95/J-STD-008. Both CDMA2000 and IS-856 draw heavily on IS-95/J-STD-008, and therefore, to understand CDMA2000 and IS-856, it is necessary to have a firm understanding of IS-95/J-STD-008.

IS-95 has two distinct versions, IS-95A and IS-95B, besides the J-STD-008. J-STD-008 is compatible with both IS-95A and IS-95B, with the exception of the frequency band of operation. However, the difference between IS-95A and IS-95B is that IS-95B enables ISDN-like data rates to exist. Although this would seem to be an interim step between 2G and 3G, for the purpose of this text, IS-95A and IS-95B are considered 2G only.

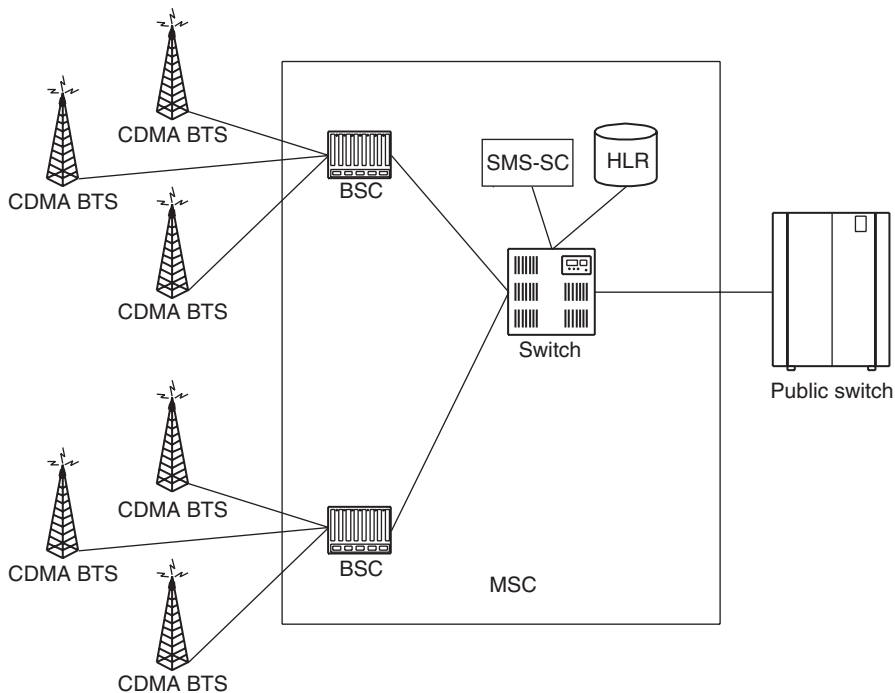


FIGURE B.20 IS-95A/B simplified system architecture.

CDMA is based on the principle of *Direct Sequence* (DS) and is a wideband spread-spectrum technology. The CDMA channel is reused in every cell of the system and is differentiated by the *Pseudorandom Number* (PN) code that it uses. Depending on whether the system will be deployed in an existing AMPS or new PCS-band system, the design concepts are fundamentally the same, with the exception of frequency-band particulars that are directly applicable to the channel assignments in an existing cellular band. Beyond the nuances, the design principles for CDMA are the same for both cellular and PCS systems.

The introduction of CDMA into an existing cellular network is not simple owing to the issue of immediate capacity reduction, but there is a long-term upside. Also, for PCS operators, a requirement specifies that they must relocate existing microwave links to clear the spectrum for their use. The degree of ease or difficulty in implementing CDMA into the PCS market will be affected directly by the ability to clear microwave spectrum. The diagram in Figure B.20 is a simplified version of the IS-95A/B architecture.

B.6.1 Standard CDMA Cell-Site Configurations

Several general types of cell sites are currently usable at this time. The configuration is slightly different for both cellular and PCS owing to colocation issues with the legacy systems. However, both cellular and PCS have the commonality of either being an omni- or three-sector cell site; it is just the number of antennas per sector that drives the difference.

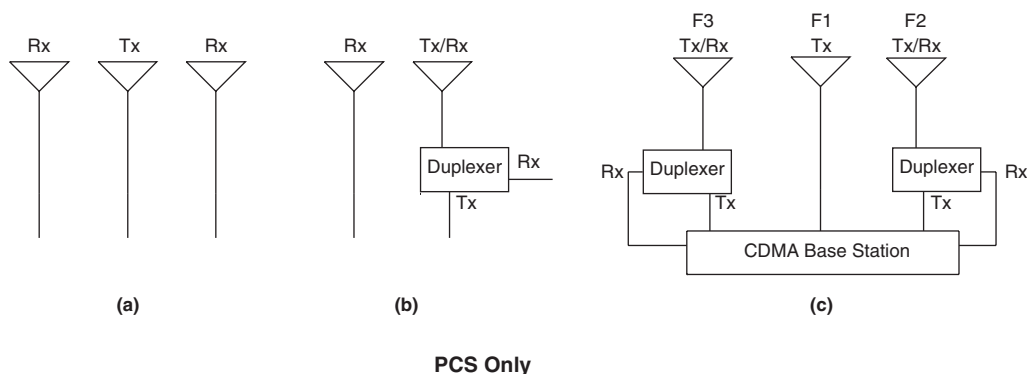


FIGURE B.21 PCS system. CDMA antenna configuration: (a) one carrier with three antennas, (b) single carrier with two antennas, and (c) multiple carriers with three antennas.

It is important to note that the radio equipment for both cellular and PCS is fundamentally the same. The difference between the two is that for PCS, the frequency for transmitting and receiving is upbanded; that is, an additional mix is taking place. Typically, each cell or sector will require a separate transmit antenna per CDMA carrier and two receive antennas. The reason for the separate transmit antennas per sector lies in the forward transmit power for the cell in that combing the channels either through use of a cavity or hybrid results in about a 3-dB loss.

The generic configurations that follow are meant for PCS and cellular CDMA-only cells, and only a single sector, or omni site, is represented. The first configuration involves a PCS system deploying CDMA-only in Figure B.21.

The figure illustrates several situations that do occur for PCS operators. The first configuration is one that involves only a single carrier, where three antennas can be installed on a per-sector or cell-site basis. The second configuration is where, owing to a multitude of reasons, only two antennas can be installed, thereby requiring the use of a duplexer. The third situation assumes that three antennas are used and shows how multiple carriers can be supported by three antennas.

Regarding cellular systems, initially, common use of the antennas at a cell site that had legacy 1G technology was promoted. However, after implementation, it was found that this might not have been the best choice. The reason for the error was that the AMPS system and the CDMA system have different design requirements, and having the common antenna system restricts the flexibility of either system for optimization and expansion purposes.

Therefore, where possible, the use of a separate set of antennas for CDMA and AMPS systems is preferred. However, as the reader would surmise, leasing, loading, roof space, and of course, local ordinances may preclude this method of deployment.

Figure B.22 illustrates a common situation when integrating 2G systems into a 1G environment. The first diagram represents the typical situation where only three antennas are available for use in a given sector, necessitating the use of duplexers. However, as discussed briefly earlier, the sharing of antennas can lead to optimization problems because both systems have different design criteria. The second diagram in Figure B.22 illustrates a configuration where the AMPS and CDMA systems share the same cell-site location, but the systems use different antenna systems.

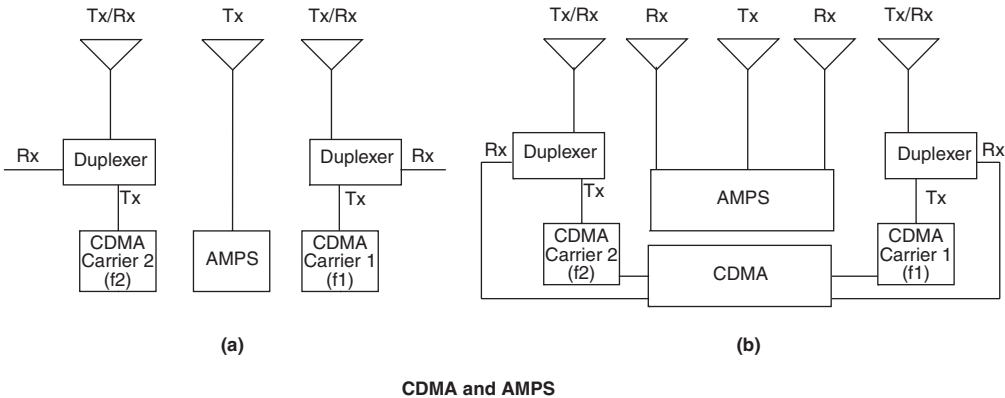


FIGURE B.22 CDMA and AMPS antenna configurations: (a) three antennas, (b) separate AMPS and CDMA systems.

B.6.2 Pilot Channel Allocation

The locations within the AMPS spectrum where the primary and secondary IS-95 pilot channels are supposed to operate are shown in Figure B.23 and are further clarified in Table B.7, the CDMA channel designation channel table.

The CDMA channel assignment for cellular is defined as requiring use of the primary or secondary CDMA channel defined in the table. The rationale behind this issue lies in the initialization algorithm that is used for CDMA. Simply put, if the subscriber unit, dual mode, does not find a pilot channel on either the primary or secondary channel, then it reverts to an analog mode.

Figure B.24 is a brief illustration of where a second CDMA carrier could be placed for, say, a B-band operator. Specifically, the fact that a preferred channel is used enables the deployment of a second CDMA carrier that is more congenial for the operator. In this case, the second channel is planted next to the primary preferred channel, and the guard band is now shifted up in frequency.

PCS, on the other hand, has a different set of preferred channels that are recommended. The initialization algorithm is simply that when the subscriber powers up, it will search in its preferred block for a pilot channel using the preferred channel set located in Figure B.25. The preferred channels are designated by the PCS operator from

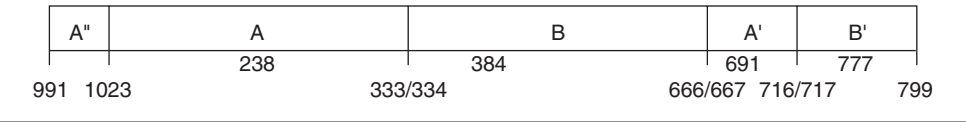


FIGURE B.23 IS-95 pilot channel locations.

CDMA Channel Designation	A-Band	B-Band
Primary	238	384
Secondary	691	777

TABLE B.7 CDMA-Preferred Channels

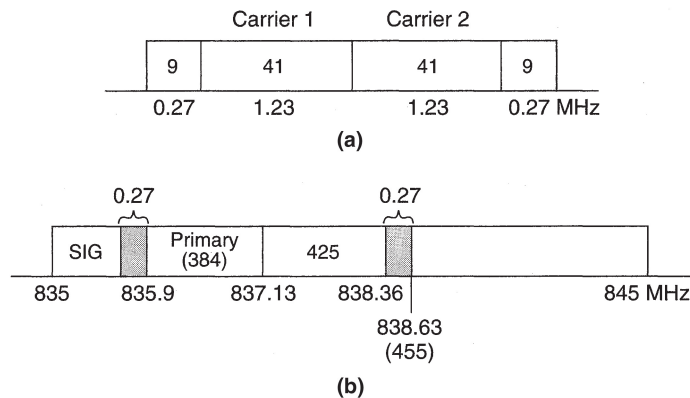


FIGURE B.24 Multiple CDMA carriers.

PCS block	CDMA channel no.	Valid CDMA assignment	Preferred set channel numbers
A (15 MHz)	0–24	NV	25, 50, 75, 100, 125, 150, 175, 200, 225, 250, 275
	25–275	V	
	276–299	CV	
D	300–324	CV	325, 350, 375
	325–375	V	
	376–399	CV	
B	400–424	CV	425, 450, 475, 500, 525, 550, 575, 600, 625, 650, 675
	425–675	V	
	676–699	CV	
E	700–724	CV	725, 750, 775
	725–775	V	
	776–799	CV	
F	800–824	CV	825, 850, 875
	825–875	V	
	876–899	CV	
C	900–924	CV	925, 950, 975, 1000, 1025, 1050, 1075, 1100, 1125, 1150, 1175
	925–1175	V	
	1176–1199	NV	

NV = not valid.
V = valid.
CV = conditionally valid.

FIGURE B.25 PCS-preferred pilot channels.

which the subscriber has contracted mobile service. The pilot channels, like cellular, also can exist in any of the valid ranges listed in the table.

Additionally, the comments listed as *Conditionally Valid* (cv) are based on the premise that the operator has control of the adjacent block of frequencies. The comments also could be based on the fact that both the adjacent blocks, such as C and F, use CDMA technology, therefore eliminating the need for a guard band on each side of the allotted spectrum.

B.6.3 Forward CDMA Channel

The forward CDMA channel, shown in Figure B.26, consists of the pilot channel, one sync channel, up to seven paging channels, and potentially 64 traffic channels. The cell site transmits the pilot and sync channels for the mobile to use when acquiring and synchronizing with the CDMA system. When this occurs, the mobile is in the mobile station initiation state. The paging channel also transmitted by the cell site is used by the subscriber unit to monitor and receive messages that might be sent to it during the mobile station idle state or system access state.

The pilot channel is transmitted continuously by the cell site. Each cell site uses a time offset for the pilot channel to uniquely identify the forward CDMA channel to the

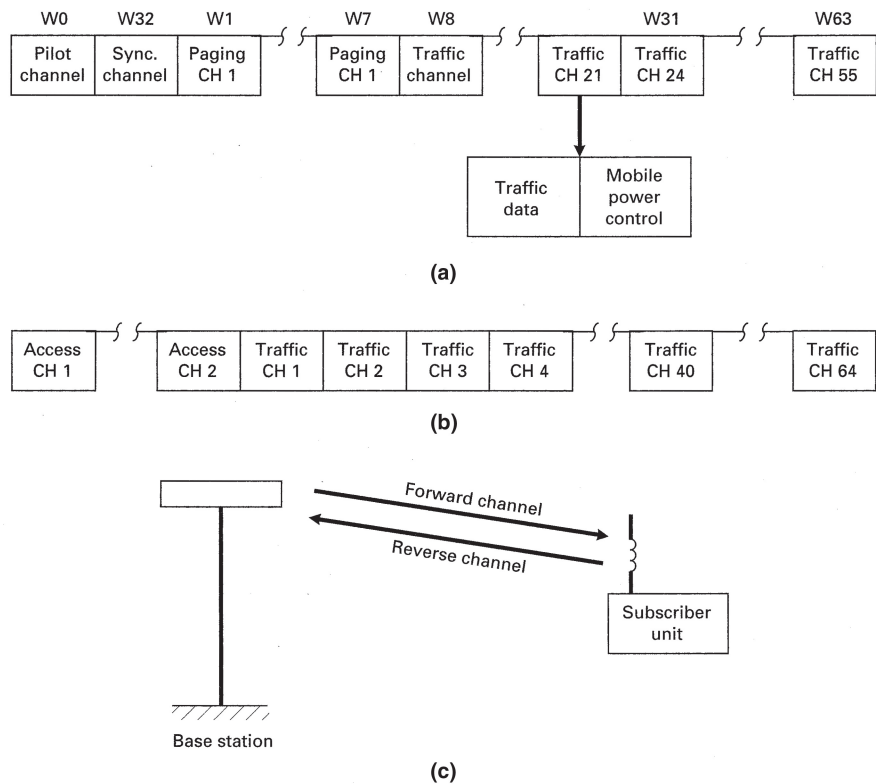


FIGURE B.26 CDMA forward channel.

mobile unit. The cell site can use a possible 512 different time-offset values. If multiple CDMA channels are assigned to a cell site, the cell still will use only one time-offset value, which is employed during the handoff process.

The sync channel is a forward channel that is used during the system acquisition phase. Once the mobile acquires the system, it will not normally reuse the sync channel until it powers on again. The sync channel provides the mobile with timing and system-configuration information. The sync channel uses the same spreading code and time offset as the pilot channel for the same cell site. The sync-channel frame is the same length as the pilot PN sequence. The information sent on the sync channel is the paging channel rate and the time of the base station's pilot PN sequence with respect to system time.

The cell site uses the paging channel to send overhead information and subscriber-specific information. The cell site will transmit at a minimum one paging channel for each supported CDMA channel that has a sync channel.

Once the mobile unit has obtained the paging information from the sync channel, it will adjust its timing and begin monitoring the paging channel; each mobile unit, however, monitors only a single paging channel. The paging channel conveys four basic types of information. The first set of information is the overhead information. The overhead information conveys the system's configuration by sending the system and access parameter messages, neighbor lists, and CDMA channel lists.

Paging is another message type sent when a mobile unit is paged by the cell site for a land-to-mobile or mobile-to-mobile call. The channel assignment messages allow the base stations to assign a mobile unit to the traffic channel, alter the paging channel assignment, or redirect the mobile unit to use the analog FM system.

The forward traffic channel is used for transmission of primary or signaling traffic to a specific subscriber unit during the duration of a call. The forward traffic channel also transmits the power control information on a subchannel continuously as part of the closed-loop system. The forward traffic channel also will support the transmission of information at 9600, 4800, or 1200 bps using a variable rate that is selected on a frame-by-frame basis, but the modulation symbol rate remains constant.

B.6.4 Reverse CDMA Channel

The cell site continuously monitors the reverse access channel to receive any message that the subscriber unit might send to the cell site during the system access state. The reverse CDMA channel consists of an access channel and the traffic channel. The access channel provides communication from the mobile unit to the cell site when the subscriber unit is not using a traffic channel. One access channel is paired with a paging channel, and each access channel has its own PN code. The mobile unit responds to the cell site's messages sent on the paging channel by using the access channel.

The forward and reverse control channels use a similar control structure that can vary from 9600 to 4800 to 2400 to 1200 bps, which enables the cell or mobile unit to alter the channel rate dynamically to adjust for the speaker. When a pause occurs in the speech, the channel rate decreases so as to reduce the amount of energy received by the CDMA system, thus increasing overall system capacity.

Four basic types of control messages are used on the traffic channel. The four messages involve control of the call itself, handoff messages, power control, security, and authentication. CDMA power control is fundamentally different from that used for AMPS or IS-54. The primary difference is that control of total power coming into the cell

Station Class	EIRP (max), dBm
I	3
II	0
III	3
IV	6
V	9

TABLE B.8 CDMA Subscriber Power Levels

site, if limited properly, will increase the traffic-handling capability of that cell site. As more energy is received by the cell site, its traffic-handling capabilities will be reduced unless it is able to reduce the power coming into it.

Forward traffic power control has two distinct parts. The first part is the cell site, which will estimate the forward link transmission loss using the mobile subscriber's received power during the access process. Based on the estimated forward link path loss, the cell site will adjust the initial digital gain for each of the traffic channels. The second part of power control involves the cell site making periodic adjustments to the digital gain, which is done in concert with the subscriber unit.

The reverse traffic channel signals arriving at the cell site vary significantly and require a different algorithm than that for forward traffic power control. The reverse channel also has two distinct elements for making power adjustments. The first is the open-loop estimate of the transmit power, which is performed solely by the subscriber unit without any feedback from the cell site itself. The second is the closed-loop correction for errors in the estimation of transmit power. The power control subchannel is transmitted continuously on the forward traffic channel every 1.25 ms, instructing the mobile unit either to power up or to power down, which affects the mean power output level. A total of 16 different power control positions are available. Table B.8 illustrates the CDMA subscriber power levels available by station class.

B.6.5 Call Processing

The call flows for 2G CDMA are shown next. It is important to note that 2G CDMA is primarily a voice system, not a data-oriented system. However, data are available to be sent via circuit-switched methods, but the call-processing flow is the same as voice because it still uses a traffic-channel setup for voice transport. The first call-processing flowchart is for a mobile-to-land call (origination), shown in Figure B.27, whereas Figure B.28 illustrates a land-to-mobile call (termination).

B.6.6 Handoffs

Several types of handoffs are available with CDMA. The types of handoffs involve soft, softer, and hard. The difference between the types depends on what one is trying to accomplish.

Several user-adjustable parameters help the handoff process take place. The parameters that need to be determined involve the values to add or remove a pilot channel from the active list and the search window sizes. Several values determine when to add or remove a pilot from consideration. In addition, the size of the search window cannot be too small, nor can it be too large.

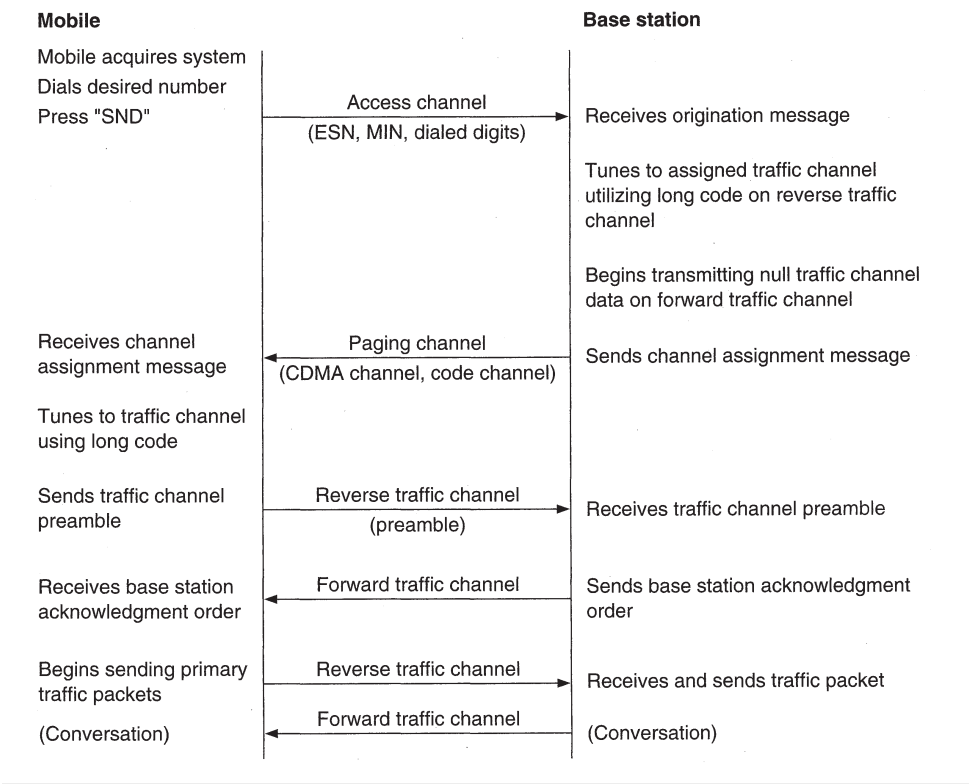


FIGURE B.27 CDMA mobile origination.

As mentioned previously, the handoff process for CDMA can take on several variants. Each of the handoff scenarios is a result of the particular system configuration and where the subscriber unit is in the network.

The handoff process begins when a mobile unit detects a pilot signal that is significantly stronger than any of the forward traffic channels assigned to it. When the mobile unit detects the stronger pilot channel, the following sequence should take place: The subscriber unit sends a pilot strength measurement message to the base station, instructing it to initiate the handoff process. The cell site then sends a handoff direction message to the mobile unit, directing it to perform the handoff. On the execution of the handoff direction message, the mobile unit sends a handoff completion message on the new reverse traffic channel.

In CDMA, a *soft handoff* involves an intercell handoff and is a make-before-break connection. The connection between the subscriber unit and the cell site is maintained by several cell sites during the process. A soft handoff can occur only when the old and new cell sites are operating on the same CDMA frequency channel.

The advantage of the soft handoff is path diversity for the forward and reverse traffic channels. Diversity on the reverse traffic channel results in less power being required by the mobile unit, reducing the overall interference, which increases traffic-handling capacity.

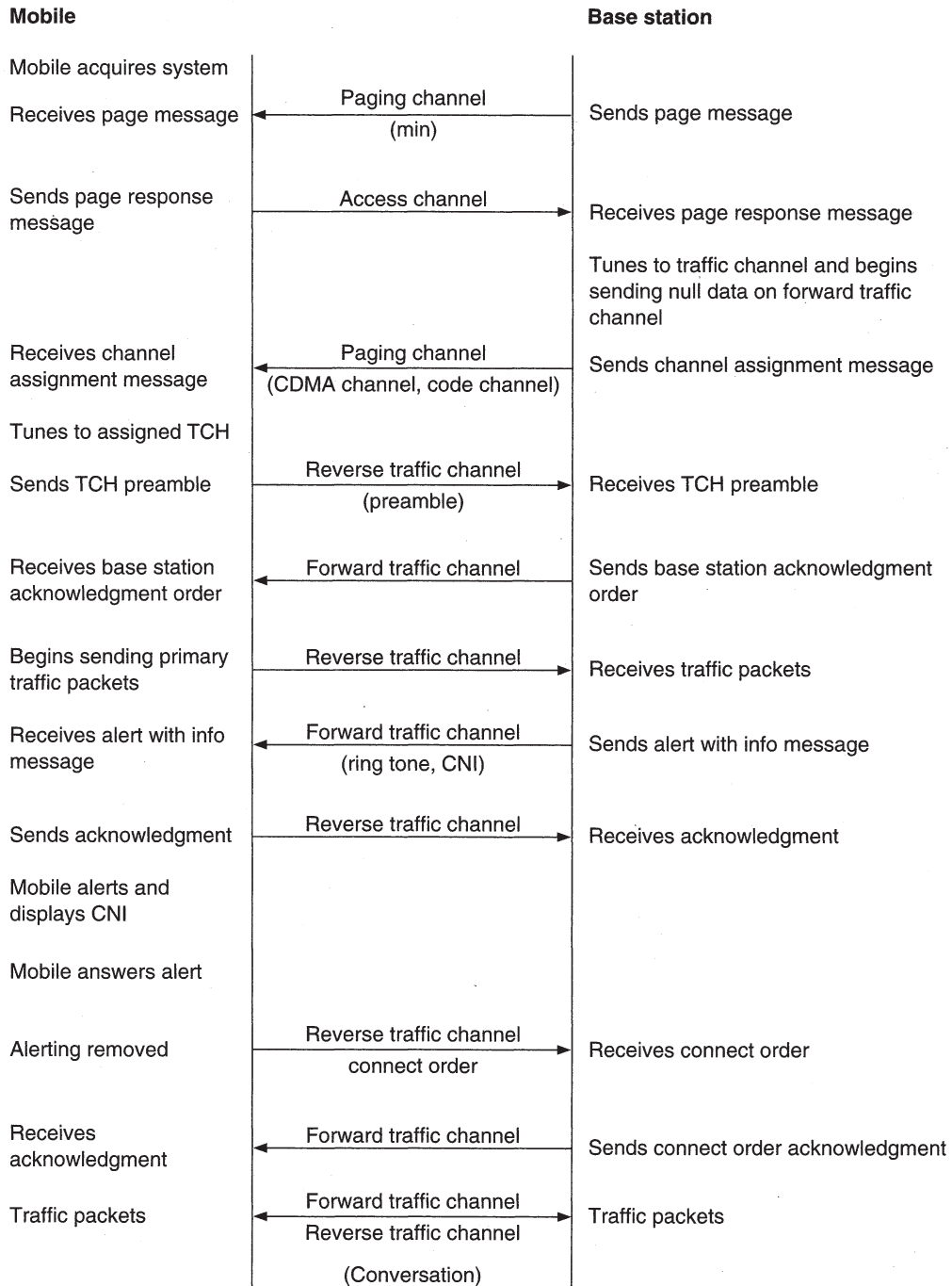


FIGURE B.28 CDMA mobile termination.

The CDMA *softer handoff* is an intracell handoff occurring between the sectors of a cell site and is a make-before-break type. The softer handoff occurs only at the serving cell site.

The *hard handoff* process is meant to enable a subscriber unit to hand off from a CDMA call to an analog call. The process is functionally a break-before-make type and is implemented in areas where CDMA service is no longer available for the subscriber to use while on a current call. The continuity of the radio link is not maintained during the hard handoff. A hard handoff also can occur between two distinct CDMA channels that are operating on different frequencies.

B.6.6.1 Search Window

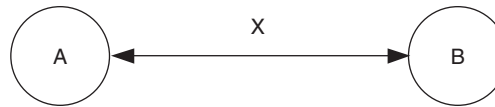
Several Search windows are used in CDMA. Each of the Search windows has its own role in the process, and it is not uncommon to have different Search window sizes for each of the windows of a particular cell site. Additionally, the Search window for each site needs to be set based on actual system conditions; however, several system startup values are shown that can be used to get you in the ballpark initially.

The Search windows needed to be determined for CDMA involve the Active, Neighbor, and Remaining windows. The Search window is defined as the amount of time, in terms of chips, that the CDMA subscriber’s receiver will hunt for a pilot channel. A slight difference exists in how the receiver hunts for pilots depending on its type.

If the pilot is an Active set, the receiver center for the Search window will track the pilot itself and adjust the center of the window to correspond to fading conditions. The other Search windows are set as defined sizes (Table B.9).

Search Window A, N, R	Window Size, PN Chips
0	2
1	4
2	6
3	8
4	10
5	14
6	20
7	28
8	40
9	56
10	80
11	114
12	160
13	226
14	320
15	452

TABLE B.9 Search Window Sizes



$$X = 10 \text{ Chips}$$

Therefore Search Window = ± 10 chips

$$\text{Search Window} = 6 \text{ (20 chips)}$$

FIGURE B.29 Search window.

The size of the Search window depends directly on the distance between the neighboring cell sites. How to determine what the correct Search window is for your situation can be extrapolated using the example shown in Figure B.29.

To determine the Search window size, the following simple procedure is used:

1. Determine the distance between the sites *A* and *B* in chips.
2. Determine the maximum delay spread in chips.
3. Search window 6 (cell spacing 1 maximum delay spread).

The Search window for the Neighbor and Remaining sets consists of parameters *SRCH_WIN_N* and *SRCH_WIN_R*, which represent the Search window sizes associated with the Neighbor set and Remaining set pilots. The subscriber unit centers its Search window around the pilots' PN offsets and compensates for time variants with its own time reference.

The *SRCH_WIN_N* should be set so that it encompasses the whole area in which a neighbor pilot can be added to the set. The largest the window should be set is $1.75D + 3$ chips, where *D* is the distance between the cells.

SRCH_WIN_A is the value that is used by the subscriber unit to determine the Search window size for both the Active and Candidate sets. The difference between the Search window for the active and candidate sets and the neighbor and remaining sets is that the Search window effectively floats with the Active and Candidate sets based on the first-arriving pilot it demodulates.

B.6.6.2 Soft Handoffs

Soft handoffs are an integral part of CDMA. The determination of which pilots will be used in the soft handoff process has a direct impact on the quality of the call and the capacity of the system. Therefore, setting the soft handoff parameters is a key element in the system design for CDMA.

The parameters associated with soft handoffs involve the determination of which pilots are in the Active, Candidate, Neighbor, and Remaining sets. The list of neighbor pilots is sent to the subscriber unit when it acquires the cell site or is assigned a traffic channel.

A brief description of each type of pilot set follows:

1. The *Active* set is the set of pilots associated with the forward traffic channels assigned to the subscriber unit. The Active set can contain more than one pilot

because a total of three carriers, each with its own pilot, could be involved in a soft handoff process.

2. The *Candidate* set is made up of the pilots that the subscriber unit has reported are of a sufficient signal strength to be used. The subscriber unit also promotes the Neighbor set and Remaining set pilots that meet the criteria to the candidate set.
3. The *Neighbor* set is a list of pilots that are not currently on the Active or Candidate pilot lists. The Neighbor set is identified by the base station via the Neighbor list and Neighbor list update messages.
4. The *Remaining* set consists of all pilots in the system that possibly can be used by the subscriber unit. However, the Remaining set pilots that the subscriber unit looks for must be a multiple of Pilot_Inc.

Figure B.30 shows an example of a soft handoff region, which is an area between cells A and B. Naturally, as the subscriber unit travels farther away from cell A, cell B

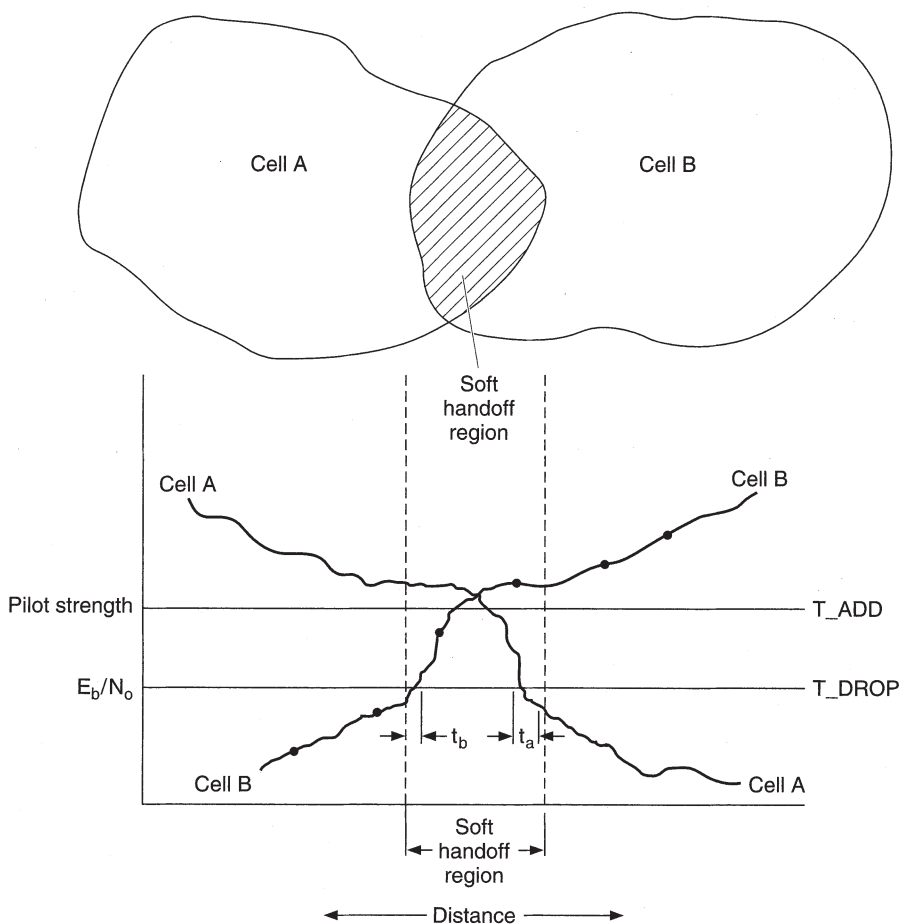


FIGURE B.30 Soft handoff.

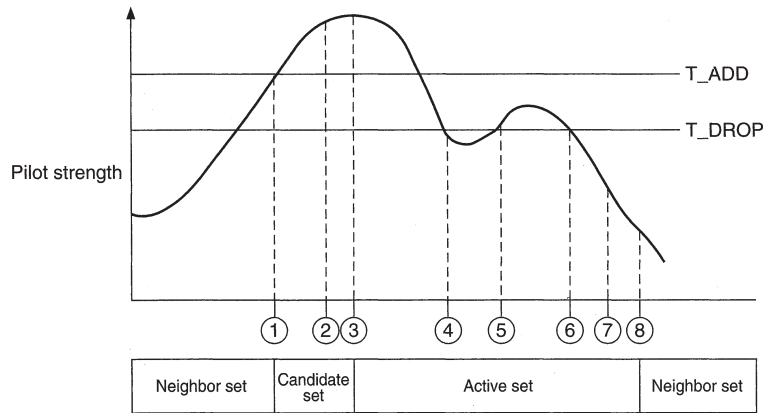


FIGURE B.31 The pilot elevation and demotion process.

increases in signal strength for the pilot. When the pilot from cell *B* reaches a certain threshold, it is added to the active pilot list.

The process of how a pilot channel moves from a neighbor to a candidate, to active, and then back to neighbor is depicted in Figure B.31.

Here are the steps that a pilot channel takes:

1. Pilot exceeds T_ADD , and the subscriber unit sends a *Pilot Strength Measurement Message* (PSMM) and a transfer pilot to the Candidate set.
2. The base station sends an extended handoff direction message.
3. The subscriber unit transfers the pilot to Active set and acknowledges this with a handoff completion message.
4. The pilot strength drops below T_DROP , and the subscriber unit begins the handoff drop time.
5. The pilot strength goes above T_DROP prior to the handoff drop time expiring and T_DROP sequences topping.
6. The pilot strength drops below T_DROP , and the subscriber unit begins the handoff drop timer.
7. The handoff drop timer expires, and the subscriber unit sends a PSMM.
8. The base station sends an extended handoff direction message.
9. The subscriber unit transfers the pilot from the Active set to the Neighbor set and acknowledges this with a handoff completion message.

To help augment this description, Figure B.32 highlights how T_COMP is factored into the decision matrix for adding and removing pilots from the Neighbor, Candidate, and Active sets.

B.6.7 Pilot Channel PN Assignment

The pilot channel carries no data, but it is used by the subscriber unit to acquire the system and assist in the process of soft handoffs, synchronization, and channel estimation.

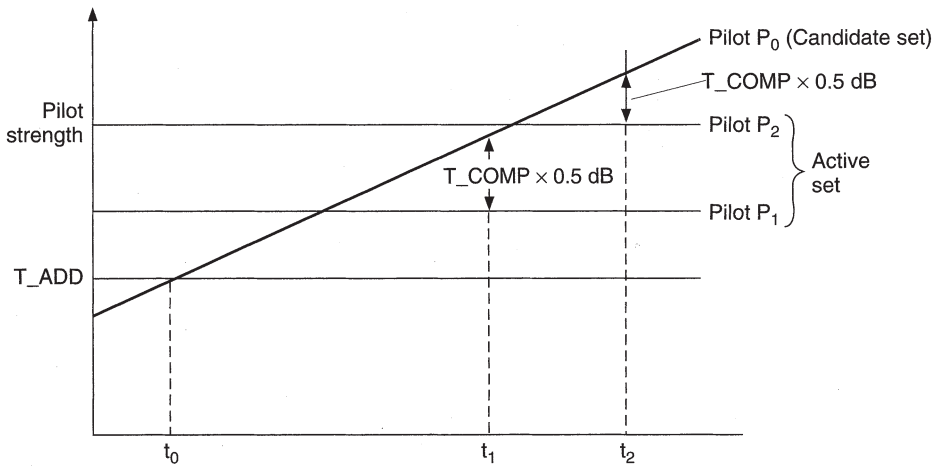


FIGURE B.32 Active set.

A separate pilot channel is transmitted for each sector of the cell site. The pilot channel is uniquely identified by its PN offset, or rather the PN short code that is used.

The PN sequence has some 32,768 chips that, when divided by 64, result in a total of 512 possible PN codes available for use. The fact that there are 512 potential PN short codes to pick from almost ensures that no problems will be associated with the assignment of these PN codes. However, some simple rules must be followed in order to ensure that no problems are encountered with the selection of the PN codes for the cell and its surrounding cell sites.

$$\begin{aligned}
 (32,768)/64 &= 512 \text{ possible PN offsets } f_{\text{chip}} \\
 &= 1.228 \times 10^6 \text{ chips/time (s)} \\
 &= 1/f_{\text{chip}} = 0.8144 \mu\text{s/chip} \\
 \text{Distance} &= 244 \text{ m/chip}
 \end{aligned}$$

Numerous perturbations exist for how to set the PN codes, but it is suggested that a reuse pattern be established for allocating the PN codes. The rationale behind the establishment of a reuse pattern lies in the fact that it will facilitate operation of the network for maintenance and growth. In addition, when adding a second carrier, the same PN code should be used for that sector.

Table B.10 can be used for establishing the PN codes for any cell site in the network. The method that should be used is to determine whether you want to have a 4, 7, 9, or 19 reuse patterns for the PN codes.

The suggested PN reuse pattern is an $N = 19$ pattern for a new PCS system, as shown in Figure B.33. If you are overlaying the CDMA system onto a cellular system, an $N = 14$ pattern should be used when the analog system uses an $N = 7$ voice channel reuse pattern.

Please note that not all the codes have been used in the $N = 19$ pattern. The remaining codes should be left in reserve for use when a PN code problem arises. In addition, a PN_INC value of 6 is also recommended for use.

	Sector	PN Code
Alpha	3	P N 2P
Beta	3	P N
Gamma	3	P N P
Omni	3	P N

Note: Where N = reuses of PN cell and P PN code increment.

TABLE B.10 PN Reuse Scheme

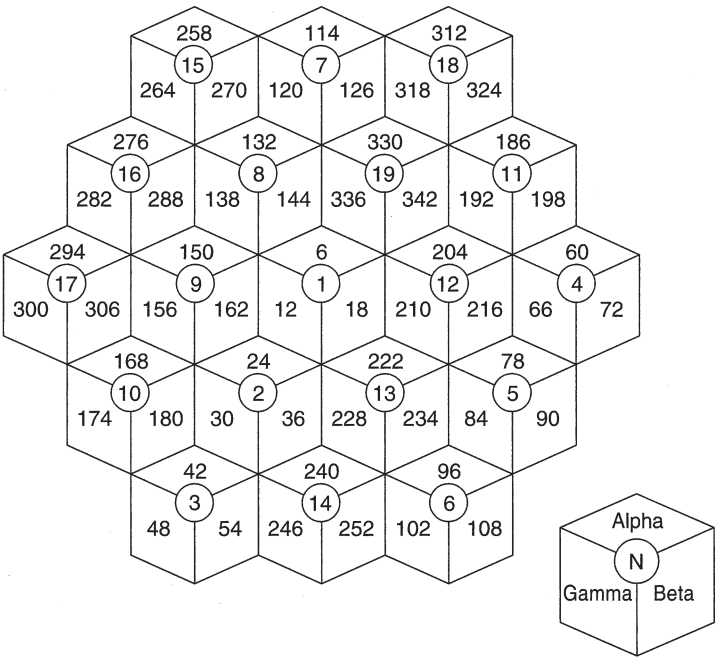


FIGURE B.33 PN reuse pattern.

The PN short code used by the pilot channel is an increment of 64 from the other PN codes, and an offset value is defined. The Pilot_INC is the value that is used to determine the number of chips, or rather the phase shift that one pilot has versus another pilot.

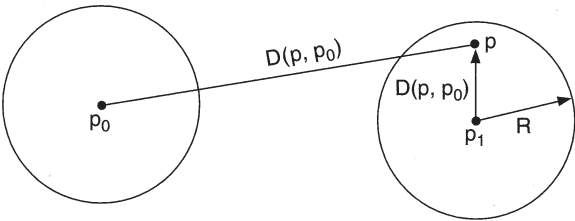
The method that is used for calculating the PN offset uses the equations in the following example shown in Figure B.34.

Pilot_INC is valid from the range of 0 to 15. Pilot_INC is the PN sequence offset index and is a multiple of 64 chips. The subscriber unit uses the Pilot_INC to determine which are the valid pilots to be scanned. Included in the example is a simple table that can be used to determine the Pilot_INC as a function of the distance between reusing sites.

$$C/I = 10 \log_{10} \left(\frac{D(P, P_0)}{D(P, P_1)} \right)^{-3} \geq \alpha$$

$$M \geq (R + S) \cdot (10^{\alpha/(\alpha)10} - 1)$$

where M = offset
 R = radius in chips
 $S = \frac{1}{2}$ Search window_A
 $\alpha = C/I$
 α = attenuation factor, propagation exponent



<i>R</i> , km	<i>R</i> (chips)	<i>S</i>	<i>C/I</i>	<i>m</i> (chips)	Pilot_INC	No. of offsets
25	103	14	24	622	10	50
20	82	12	24	499	8	64
15	61	12	24	390	6	85
12.5	51	10	24	325	5	102
10	41	10	24	271	4	128
7	29	10	24	207	4	128
5	21	10	24	165	3	170
3	12	10	24	117	2	256
2.5	10	10	24	106	2	256
2	8	10	24	96	2	256

FIGURE B.34 PN offset.

B.6.8 Link Budget

The link budget calculations directly influence the performance of the CDMA system because the link budget is used to determine power settings and capacity limits for the network. Proper selection of the variables that comprise the link budget is a very obvious issue.

Two links are used: forward and reverse. The forward and reverse links use different coding and modulation formats. The first step in the link budget process is to determine the forward and the reverse links' maximum path losses. The forward link's maximum path loss is determined using Table B.11a.

The data gathered show that the maximum path loss sustainable is about 2159.6 dB using the parameters selected. The reverse link calculations are shown in Table B.11b.

Forward Link Budget	14.4 kbps	Value (units)		Comment
Tx power distribution	Tx PA power	39.0 dBm		8 W
	Pilot channel power	30.8 dBm	15.0%	% of max power per channel
	Sync channel power	20.8 dBm	10.0%	% pilot power
	Paging channel power	26.2 dBm	35.1%	% pilot power
	Traffic channel power	38.0 dBm	78.2%	% of max power per channel
	Number of mobiles per carrier	13		
	Soft/softer handoff traffic	13		1.85 overhead factor
	Max no. of active traffic chs	26		
	Avg traffic channel power	23.8 dBm		26 total traffic channels
	Voice activity factor	0.479		Voice = 0.479, data =1.0
	Peak traffic channel power	27.0 dBm		Avg traffic ch power/ voice activity factor
Base station	Traffic channel Tx power	27.0 dBm		
	Duplexer loss	0.5 dB		
	Jumper and connector loss	0.25 dB		
	Lightening arrestor loss	0.25 dB		
	Feedline loss	1 dB		
	Jumper and connector loss	0.25 dB		
	Tower iop amp loss	0 dB		
	Antenna gain	15 dBd		
	Net base-station Tx power	39.8 dBm		10 W ERP per traffic channel (voice)
	Total base-station Tx power	51.8 dBm		151 W ERP per carrier
Environmental	Fade margin	5 dB		Log normal
	Penetration loss	10 dB		(Street/vehicle/building)
	Cell overlap	3 dB		
	External losses	18 dB		
Subscriber	Antenna gain	0 dBd		
	Cable loss	2 dB		
	Rx noise figure	10 dB		
	Receiver noise density	174 dBm/Hz		
	Information rate	60.90 dB		1230 kbps
	Rx sensitivity	101.1 dBm		
Subscriber traffic	Base Tx	39.8		
Channel RSSI	Environmental loss	18		
	Max path loss	139.77		Obtained from uplink path analysis
	RSSI at sub antenna	118.01		
Forward Link Budget	14.4 kbps	Value (units)		Comment

TABLE B.11a Forward Link Budget (Continued)

Forward Link Budget	14.4 kbps	Value (units)		Comment
Subscriber total RSSI	Base Tx	51.8		
	Environmental loss	18		
	Max path loss	139.77		Obtained from uplink path analysis
	Total RSSI at sub antenna	105.99		
Interference Internal interference Total interference	Orthogonality factor	8 dB		0.16 same-sector interference
	Total RSSI at sub antenna	105.99		
	Other user interference level (RSSI total)	113.99		Orthogonal factor
	Other sector interference	4 dB		
	Interference density	109.99		
	Internal interference	109.99		
	External interference	117 dBm		Depends on local environment
	Total interference on TCH	107.95		External interference + Rx sensitivity + other user interference
RSSI E_b/N_o	Mobile TCH RSSI	118.01		
	Information rate	41.58 dB		14.4
	Traffic channel E_b	159.59		
	Total RSSI	107.95		
	Information rate	60.90 dB		1230
	Traffic channel N_o	168.85		
	Traffic channel E_b	159.59		
	Traffic channel N_o	168.85		

TABLE B.11a Forward Link Budget

The maximum path loss that is sustainable in the reverse direction is 139.77 dB, which shows that the base station is reverse-link-limited for the parameters in the link budget.

B.6.9 Traffic Model

The capacity for a CDMA cell site is driven by several issues. The first and most obvious point for traffic modeling in a CDMA cell site involves how many channel cards the cell site is configured with. A total of 55 possible traffic channels are available for use at a CDMA cell site, but unless the channel cards are installed, the full potential is not realizable using IS-95/J-STD-008 specifications.

Additionally, the other factor that fits into the traffic calculations for the site involves system noise. A simple relationship exists between system noise and the capacity of the

Reverse Link Budget	14.4 kbps	Value (units)	Comment
Subscriber terminal	Tx power	23 dBm	Maximum power per traffic channel
	Cable loss	2 dB	
	Antenna gain	0 dBd	
	Tx power per traffic channel	21 dBm	
External factors	Fade margin	5 dB	Log normal (Street/vehicle/building)
	Penetration loss	10 dB	
	External losses	15 dB	
Base station	Rx antenna gain	15 dBd	(Approx 17.25 dBi)
	Tower top amp net gain	0	
	Jumper and connector loss	0.25 dB	
	Feedline loss	1 dB	
	Lightening arrestor loss	0.25	
	Jumper and connector loss	0.25	
	Duplexer loss	0.5	
	Receive configuration loss	0	
	Handoff gain	4 dB	
	Rx diversity gain	0 dB	
	Rx noise figure	5 dB	
	Receiver interference margin	3.4 dB	
	Receiver noise density	174 dBm/Hz	
	Information rate	41.58 dB	
	Rx sensitivity	124.0 dBm	
	E_b/N_o	7 dB	
	Total base station	140.77 dBm	
	E_b/N_o	7.00 dB	
	Maximum path loss	139.77 dB	

TABLE B.11b Reverse Link Budget

cell site. Typically, the load of the cell-site design is somewhere in the vicinity of 40 to 50 percent of the pole capacity, with a maximum of 75 percent.

The third major element determining the capacity of a CDMA cell is the soft handoff factor. Since CDMA relies on soft handoffs as part of the fundamental design of the network, this also must be factored into the usable capacity of the site. The reason for factoring soft handoffs into capacity is that if 33 percent of the calls are in a soft handoff mode, then this will require more channel elements to be installed at the neighboring cell sites to keep the capacity at the desired levels.

With CDMA, the capacity of the site is dynamic because as the system noise floor is raised, base-station loading decreases. The specific capacity for any CDMA base station is typically achieved through computer simulation owing to the dynamics of cell loading and interference levels, making a pure traffic calculation on a spreadsheet rather impractical. However, some rules of thumb should be followed for simple planning exercises that do not require a computer simulation.

As stated earlier, a total of 64 Walsh codes are available. Typically, the Walsh codes are allocated in the following manner:

Channel Type	Number of Walsh Codes
Pilot	1
Sync	1
Paging	1–7
Traffic channels	55

The pole capacity for CDMA is the theoretical maximum number of simultaneous users that can coexist on a single CDMA carrier. However, at the pole, the system will become unstable, and therefore, operating at less than 100 percent of the pole capacity is the desired method of operation.

The effective traffic channels for a CDMA carrier are the number of CDMA traffic channels needed to handle the expected traffic load. However, since soft handoffs are an integral part of CDMA, they also need to be included in the calculation for capacity. In addition to each traffic channel that is assigned for the site, a corresponding piece of hardware also is needed at the cell site.

The actual traffic channels for a cell site are determined using the following equation:

$$\text{Actual traffic channels} = (\text{effective traffic channels} + \text{soft handoff channels})$$

The maximum capacity for a CDMA cell site should be 75 percent of the pole, but typical loading in IS-95 systems has found that the pole point is really around 50 percent.

The physical limit for a CDMA system's capacity is dictated by the mutual interference driven by the forward channel. Therefore, the number of users that can be placed onto a CDMA system at any time is limited by mutual interference, which is directly related to power.

$$P (\text{pole point}) = g / [\alpha \times d \times (1 + \beta)] + 1$$

where α = voice activity factor

d = required E_b/N_o

g = processing gain

β = other cell/sector interference factor

Looking at the pole-point equation, it is obvious that it is unique for every site because it depends on the local situation at that site. Additionally, owing to the E_b/N_o factor, the cell can be allowed to degrade, allowing for the soft capacity factor, which, of course, affects the pole point, leading to more dynamics and the need for computer simulation.

However, assuming the 50 percent pole point, the Erlangs of offered traffic, using Erlang B, can be derived for an individual CDMA carrier and are shown in Table B.12.

The Channel Elements (CEs) are a pooled resource, and therefore, equipping a full complement of CEs for all sectors to be used simultaneously is not a practical approach. Instead, it is typically recommended that only 95 percent of the CE estimate be installed for the cell.

When more than one carrier is in a sector, the capacity can be estimated. In Table B.12 it is assumed that the sector has two carriers; if more carriers are in that sector, then it is a matter of multiplication to arrive at the new traffic levels because no trunking efficiency exists between CDMA carriers.

Blocking Rate	Offered Traffic	CEs Required/Sector	CEs Required/Cell (3 Sectors)
1%	7.35	14	40
2%	7.4	13	38
3%	7.48	12	35
5%	7.63	11	32
10%	8.06	10	29

Blocking Rate	No. of Carriers	Offered Traffic Erlangs	CEs Required/Sector	CEs Required/Cell (3 Sectors)
1%	2	14.7	28	80
2%	2	14.8	26	74
3%	2	14.96	24	69

TABLE B.12 Channel Elements

B.7 iDEN (Integrated Dispatch Enhanced Network)

iDEN stands for either the *Integrated Dispatch Enhanced Network* or the *Integrated Digital Enhanced Network*. The iDEN system is a unique wireless access platform because it involves integrating several mobile phone technologies together, based on a modified GSM platform. The services that are integrated into iDEN involve a dispatch system, full-duplex telephone interconnections, data transport, and short messaging services.

The iDEN system, because of the band it typically operates in, has been the center of the public safety 800-MHz rebanding process. As part of the rebanding process, another remapping of the 800-MHz SMR band is occurring in the United States right now, with the final objective of eliminating iDEN's interference in the public safety frequency band and harmonizing the 800- and 700-MHz public safety frequency bands.

The dispatch system with iDEN, also known as *Push to Talk* (PTT), involves a feature called *group call*, where multiple people can engage in a conference. The user list is pre-programmed, and the conference call can be set up just like it is done in two-way or *Specialized Mobile Radio* (SMR) with the exception that the connection can take place using any of the frequencies that are available from the pool of channels where the subscriber is physically located.

The telephone interconnect and data transport are meant to offer conventional mobile communications. The short messaging service enables the iDEN phones to receive up to 140 characters for an alphanumeric message. An example of a typical iDEN system is shown in Figure B.35.

The elements that make up the iDEN system, as shown in Figure B.35, are listed here:

- DAP—Dispatch application processor
- EBTS—Enhanced base transceiver
- HLR—Home-location register
- MPS—Metro packet switch

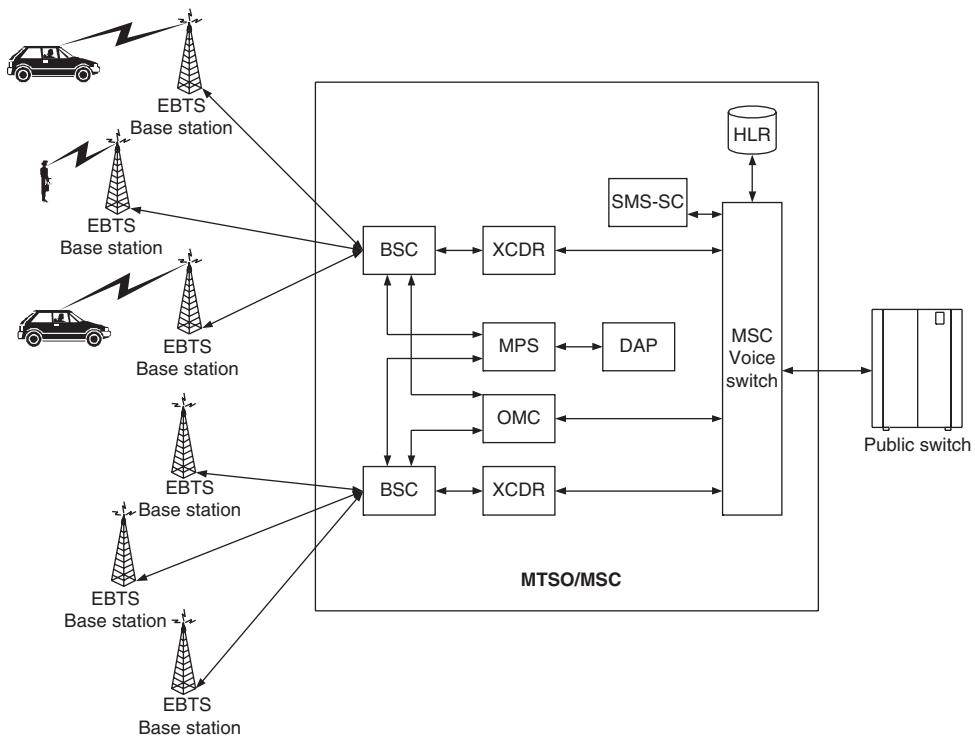


FIGURE B.35 iDEN system architecture.

- MSC—Mobile switching center
- OMC—Operations and maintenance center
- SMS-SC—Short Message Service service center
- XCDR—Transcoder

In review of Figure B.35, there are several differences between an iDEN system and a typical mobile wireless system. iDEN is unique in wireless mobility because it combines both interconnect and dispatch services in the same wireless system. The two distinct systems, interconnect and dispatch, are effectively overlaid on top of each other but are integrated and share some common elements such as the EBTS radio.

The BSC is responsible for traffic and control channel allocations in addition to hand-over data collection and controlling handovers between other BSCs. The MPS provides the connectivity for the dispatch calls. It also distributes the dispatch packets as well as the ISMI assignment. The DAP is the processing entity responsible for overall coordination and control of the dispatch services. The DAP enables the following types of dispatch calls to take place:

- Talk group
- Private call
- Call alert

The radio access system used by an iDEN system is TDMA. The channel bandwidth is 25 kHz, which consists of four independent side bands, each being a 16QAM base-band signal. The center frequencies of these side bands are 4.5 kHz from each other, and they are spaced symmetrically about a suppressed RF carrier frequency, resulting in a 16-point data symbol constellation that carries 4 data bits per symbol. The location where iDEN is used in the spectrum is shown in Figure B.36 which is pre-rebanding. The RF channel structure shown in Figure B.36 illustrates the relationship between the TCHs and the various control and signaling channels that make up an iDEN channel. Examining Figure B.37 reveals that the iDEN channel is made up of six time slots

What is interesting is that the iDEN channel is divided into multiple logical slots (i.e., 24). Each TCH therefore consists of four logical slots, and this is due to the modulation format, QAM, that is used. Interleaving is used to make 12:1, 6:1, or 3:1 channels.

iDEN was introduced using a 6:1 interleave for both dispatch and interconnect services. Later the system was upgraded, enabling a 3:1 interleave for interconnect-only service. Subsequently, iDEN was introduced with a 12:1 interleave using the same six time slots but half rate under good RF conditions.

Therefore, the wireless operator has the choice of offering 12:1, 6:1, or 3:1 voice service in addition to dispatch services. Capacity is affected by the selection of the interconnection method and the amount of dispatch traffic that is carried on the system. Looking at a simplistic example, a 3:1 voice call requires two TCHs, whereas a 6:1 or dispatch call requires only a single TCH, but for 12:1, there are two subchannels per TCH as compared with 4 for 6:1 and 8 for 3:1 . Of course, other issues related to signaling and call quality are factored into this.

iDEN uses several control channels similar in nature to GSM systems. The control channels used by iDEN are listed here for reference. In addition to the control channels, two other channels are used in iDEN: the TCH and PCH, which are also listed.

- *PCCH*. The primary control channel is a multiple-access channel used for the transmission of general system parameters. The outbound PCCH contains the

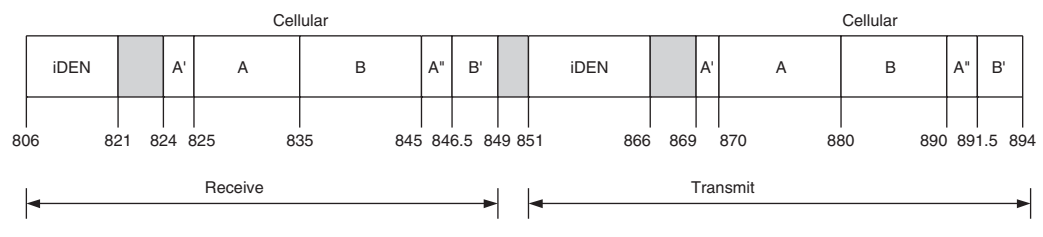


FIGURE B.36 iDEN spectrum location, pre-rebanding.

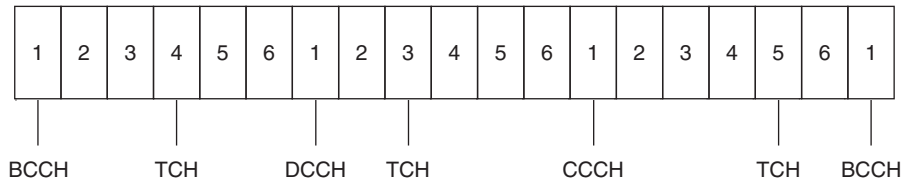


FIGURE B.37 iDEN RF channel structure.

Broadcast Control Channel (BCCH) and the *Common Control Channel (CCCH)*, whereas the inbound PCCH is referred to as the *Random Access Channel (RACH)*:

- Inbound service requests
- Outbound service grants
- *BCCH*
 - I. Neighbor cells
 - II. Control channels
 - III. Packet channels
 - IV. Location areas
 - V. Common control channel
 - VI. Paging subchannel
 - VII. Service grants
- *TCCH*. Temporary control channel.
 - Inbound dispatch reassignment requests
 - Outbound handover target
- *DCCH*. Dedicated control channel.
 - Inbound location updating
 - I. Authentication
 - II. SMS
 - III. Registration
 - IV. Outbound
 - V. Location updating
 - VI. Authentication
 - VII. SMS
 - VIII. Registration
- *ACCH*. Associated control channel.
- *TCH*. Traffic channel that provides circuit-mode transmission for voice and data.
 - Inbound dispatch reassignment requests
 - Outbound handover target
- *PCH*. Packet channel provides for multiaccess packet-mode transmission.

Many interesting issues are associated with the iDEN call processing for either dispatch or interconnection calls. From the time an iDEN mobile subscriber is powered up until it is powered down, a series of procedures is executed between the EBTS and the mobile unit to control the radio communications link. Before a call description flow-chart is shown, a few terms or processes used in iDEN systems associated with the mobile need to be covered briefly.

- *Cell selection*. At power up, the mobile unit scans a preprogrammed list of system frequencies called a *bandmap* looking for a PCCH. When the mobile unit “hears” a PCCH, outbound power and *Signal Quality Estimate (SQE)* measurements are taken, and the frequency is added to a list. The mobile unit continues scanning channels until either 32 PCCHs are found or the bandmap list is exhausted, which is market-specific. The PCCH list is sorted based on SQE and *Receive Signal Strength Indicator (RSSI)*, and the subscriber then attempts to “camp on” the first cell on the list. If it fails, it will attempt to camp on the next cell and so on until it either succeeds in camping or exhausts the list, requiring a new cell selection process to begin.

- *Cell reselection.* Each serving cell will transmit its neighbor-cell list to all the subscribers it serves, and the mobile unit will take SQE measurements of the received power of the serving cell and of each neighbor cell. It then will sort the neighbor-cell list according to received signal strength. When the mobile unit determines that the best neighbor cell is a better candidate for a serving cell than the current serving cell, a reselection occurs, making the formerly best neighbor cell the new serving cell.
- *Fast reconnect.* Throughout the duration of a dispatch call, the mobile unit continues to monitor the SQE and signal strength of the serving and neighbor cells. Under certain conditions, the mobile may decide to change its serving cell.
When the mobile unit is on the traffic channel (during the talk phase of a call), it initiates a reconnect if the serving cell's outbound SQE is less than desired or on failure or disconnect of the serving cell.
- *Power control.* The mobile unit periodically adjusts its transmit power based on the power received at the *Fixed Network Equipment* (FNE). The mobile unit periodically receives a power control constant and measures the serving cell's output power. The mobile unit then calculates the desired mobile transmit power by subtracting the serving-cell output power from the power control constant and adjusts its transmit power accordingly.
- *Handoff.* iDEN uses *Mobile-Assisted Handover* (MAHO) to assist in the handoff process. The handoff can be initiated by either the mobile unit or the base station depending on the parameter settings. Handoffs are possible only with interconnection calls. However, for a dispatch, the location information supplied in the response also includes the neighbor list from cells that are on the beacon channel list. Therefore, if the *Dispatch Location Area* (DLA) is set up incorrectly, it is possible that the subscriber will need to reacquire the system if it moves outside the coverage area of the sites in the list.

The MAHO process is as follows:

1. The mobile unit monitors information on BCCH as to which cells to monitor for inclusion in MAHO list.
2. The mobile unit continues to monitor SQE, the RSSI for the primary serving channel, and the channels in the MAHO list.
3. If the subscriber detects trouble in the primary service or a better neighbor cell, the mobile unit sends a sample of its measurements.
4. The subscriber signals in the ACCH with an SQE measurement.
5. MSC/BSC/EBTS finds a new server to hand over to and allocates a TCH for this process.
6. MSC/BSC/EBTS senses a handover command on ACCH with the initial power setting, channel, and TCH to tune to.
7. MS changes to an assigned channel.
8. MS uses the *Random Access Procedure* (RAP) to get its timing information from the target EBTS.
9. The channel changes to TCH, and conversation continues.

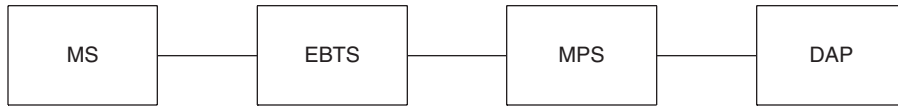


FIGURE B.38 Dispatch only.

Lastly, SQE is used extensively in various cell-site selection decisions and is based primarily on the outbound RSSI measurements of the serving cell as well as of neighboring cells that are potential handover candidates. SQE is very similar to $C/(I + N)$ in the range of 15 to 23 dB. The dispatch system involves the key components of the iDEN system (Figure B.38).

The dispatch system basically has three primary service offerings or functions:

- Private
- Talk group
- Call alert (twiddle)

Whereas private dispatch is where the originating call uses PTT between one subscriber unit and another (classic two-way), this is not *Talk-Around/Direct Mode Only* (DMO). Call alert is used to notify a subscriber that a voice communication is desired. However, talk groups involve a more extensive look.

Service Areas (SAs) define talk groups, as shown in Figure B.41. The SA is used for dispatch group calls. When a dispatch call takes place, a single voice-channel slot is used in any coverage area for a cell when one or more members of the call group are in that coverage area. Fleets are assigned to the same group, and a mobile unit can be included in several talk groups in order to communicate between specific groups that make up the entire fleet.

As stated briefly earlier, a mobile unit can be included in several talk groups used to communicate with a group of mobiles in the fleet at the same time or all the mobiles. For example, let's say that there is a fleet for all of New York City, but the subscriber wants to talk only with the Queens fleet. The mobile for the Queens fleet is assigned its own talk group, which is part of the overall fleet group. In doing so, a mobile can be part of numerous talk groups.

To help clarify or further confuse the situation, a call-flow diagram for dispatch calls is shown in Figure B.39. Looking at the flowchart in the figure, the following text better explains some of the sequences:

1. PTT dispatches a call request.
2. The call request packet is routed to the DAP.
3. The DAP recognizes subscriber units' group affiliation and tracks the group members' current location area.
4. The DAP sends a location request to each group member location area to obtain the various subscribers' cell/sector location information.
5. The subscriber units in the group respond with their current cell/sector location information.

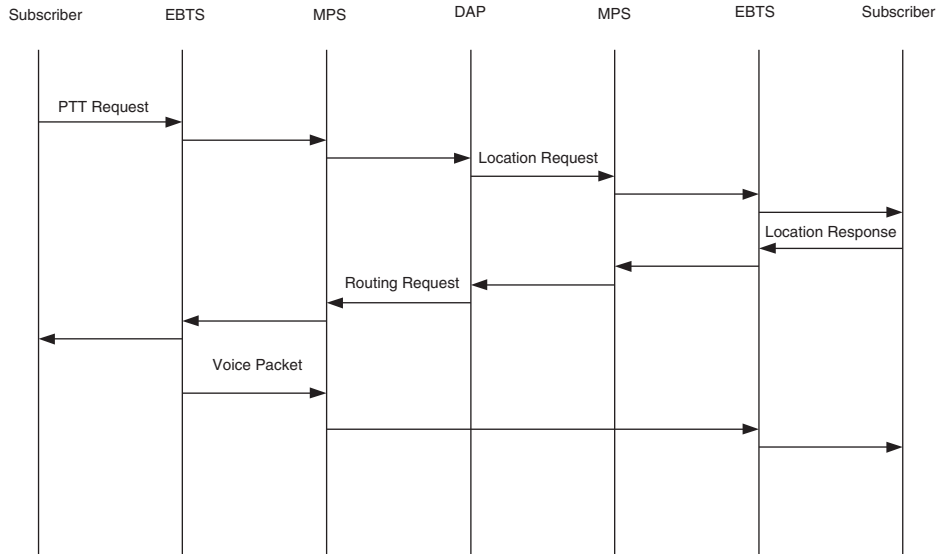


FIGURE B.39 Dispatch call sequence.

6. The DAP instructs the originating EBTS with packet routing information for all group members.
7. Call voice packets are received by the PD and then are replicated and distributed to the group's end node.

For interconnections, another portion of the iDEN system is used after the radio access. The general sequence of events for an interconnection call is the same, whether it is for a 3:1, 6:1, or 12:1 call, with the exception of the number of TCHs assigned.

Therefore, the interconnection sequence for a mobile-to-land call is listed here in brevity:

1. Call initiation
2. RAP on PCCH
3. DCCH assigned
4. Authentication
5. Call setup transaction
6. TCH assignment
7. Conversation
8. Call termination request via ACCH
9. Call is released

Figure B.40 is a call-flow diagram for a mobile-land interconnection call sequence that should help to bring the components together. It is interesting to note the differences between the interconnection-call diagram and that for the dispatch sequence.

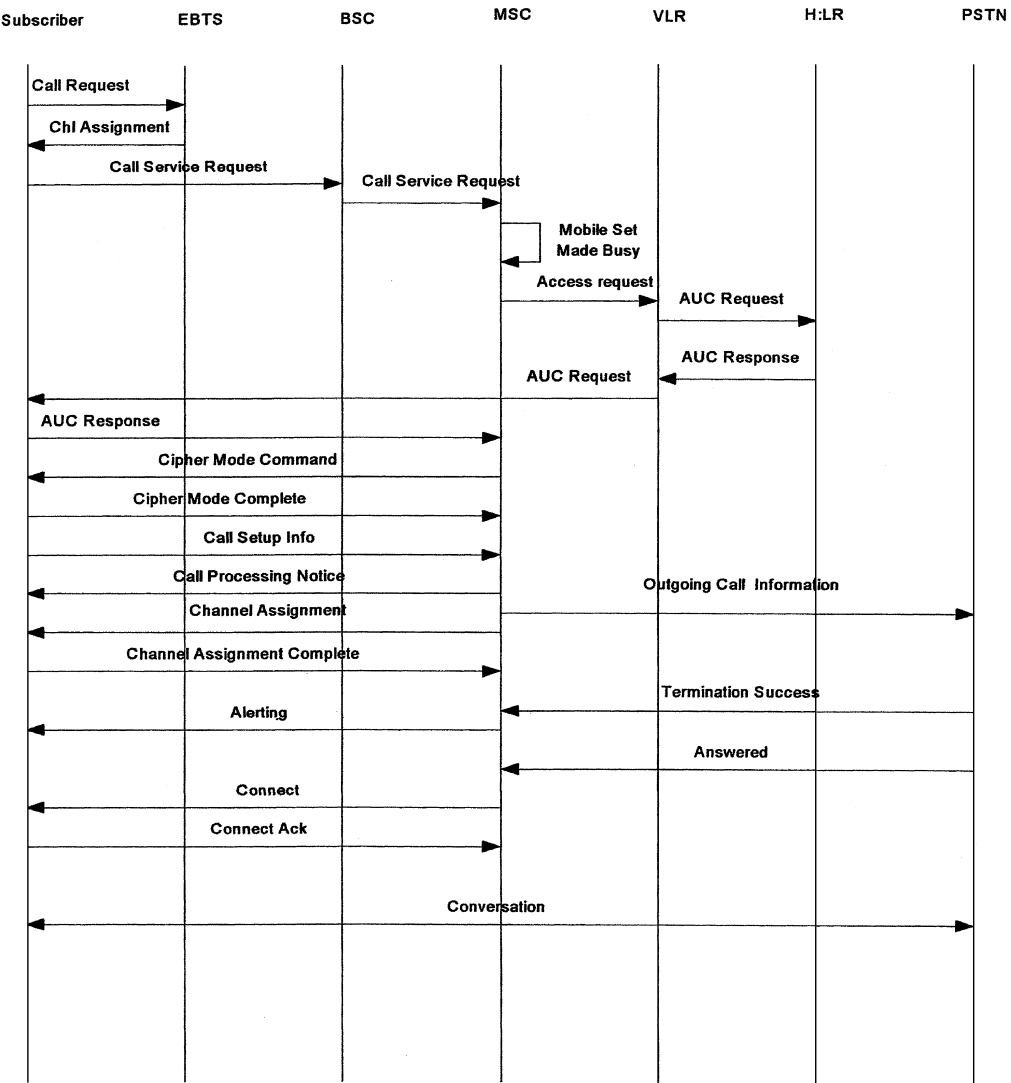


FIGURE B.40 Mobile-land interconnection call-flow diagram.

The interaction of sharing resources for radio access for both interconnections and dispatches involves the establishment of dispatch and interconnection location areas, referred to as *Dispatch Location Areas* (DLAs) and *Interconnection Location Areas* (ILAs). The DLAs and ILAs usually are designed independently but have interactions that require joint considerations to be made for the selection of both the DLA and ILA boundaries. The DLA and ILA boundaries are in addition to BSC boundaries; however, the ILA or DLA needs to be inclusive of the EBTSs, which are connected to a the BSC.

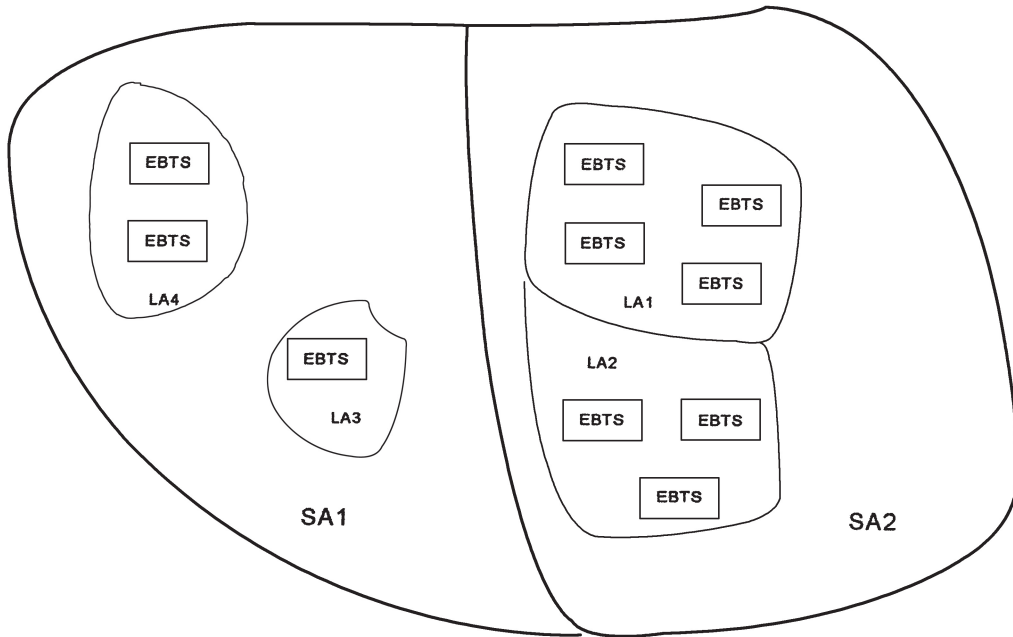


FIGURE B.41 Dispatch location areas (DLAs).

An example of a DLA boundary is shown in Figure B.41, which shows a total of four location areas associated with dispatch. Each location area then is folded into an SA. Keeping in mind the dispatch discussion regarding SAs, the design engineer must take care not only during the selection of location areas but also in what constitutes the service area. The location area is where the dispatch call is broadcast when the service area defines which location areas are possible for inclusion in the dispatch call.

Figure B.42 is the corollary to the DLA boundaries and shows the ILAs for the same sample system. The ILA is used for call delivery and paging for the subscriber unit. The ILA boundaries should not be set up such that the subscriber units regularly transition from one ILA to another, increasing the amount of overhead signaling required to keep track of the mobile.

In looking at Figures B.41 and B.42, the differences between the ILA and DLA boundaries become evident. Next, Figure B.43 shows the composite view of both ILA and DLA boundaries.

B.7.1 WIDEN

WiDEN, known as *Wide Band iDEN*, is the next generation of iDEN. WiDEN was introduced to provide packet-data services. There are several differences with WiDEN compared with iDEN.

WiDEN combines four iDEN carriers into one 100-kHz channel. The combining of the channels allows for data speeds approaching 96 kbps. WiDEN was introduced as a competing technology for CDMA2000-1xRTT and GSM/GPRS/EDGE.

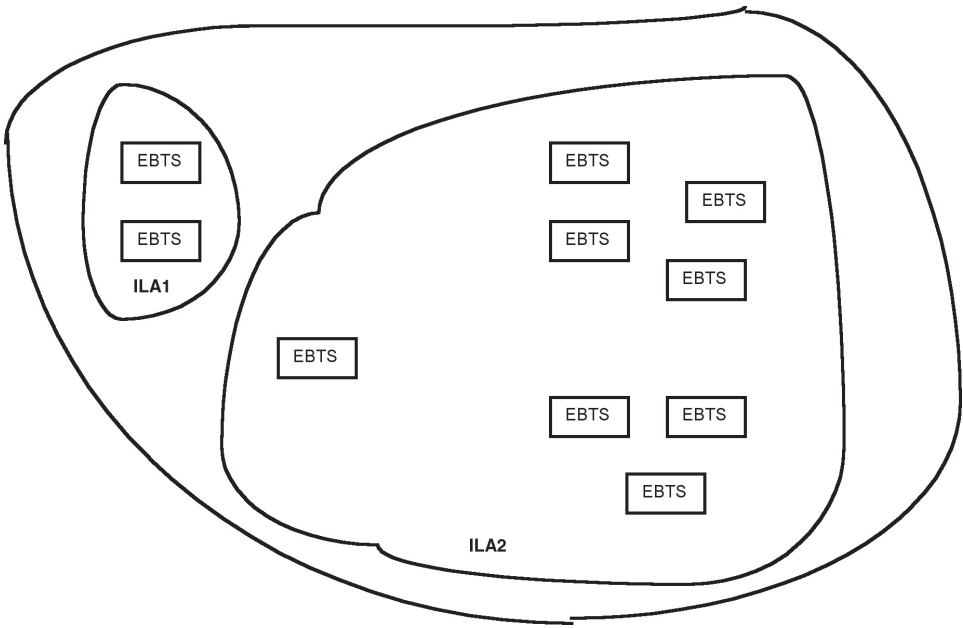


FIGURE B.42 Interconnection location areas (ILAs).

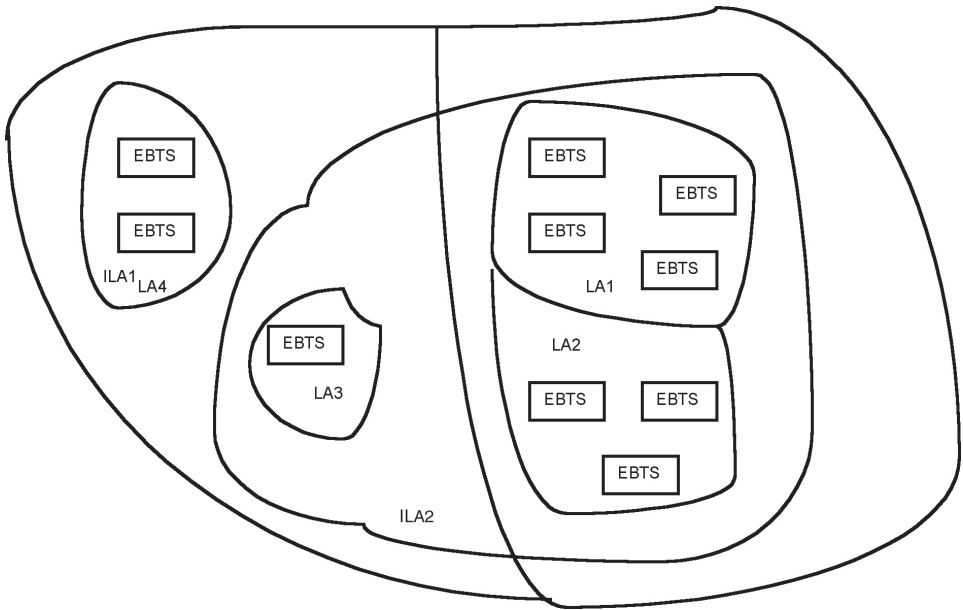


FIGURE B.43 The ILA and DLA composite view.

In addition, to take advantage of WiDEN, the subscriber unit needs to be able to support iDEN. In the event that legacy devices are used in a WiDEN network, the system will revert to standard iDEN. This allows for possible niche target areas to have WiDEN deployed.

B.8 CDPD

Cellular Data Packet Data (CDPD) is a packetized data service using its own air interface standard that is employed by the cellular operators. CDPD is a functionally separate data communication service that physically shares the cell site and cellular spectrum.

CDPD has many applications but is most applicable for short, bursty-type data applications and not large-file transfers. CDPD application of the short messages would consist of e-mail, telemetry applications, credit-card validations, and global positioning, to mention a few potentials. CDPD is a pure data service designed for mobility; however, it cannot, nor was it ever designed to, supply the data speeds needed for 3G services.

CDPD does not establish a direct connection between the host and server locations. Instead, it relies on the *Open Systems Interconnection* (OSI) model for packet-switching data communications, and the model routes the packet data throughout the network. The CDPD network has various layers that make up the system. Layer 1 is the physical layer, Layer 2 is the data link itself, and Layer 3 is the network portion of the architecture. CDPD uses an open architecture and has incorporated authentication and encryption technology into its airlink standard.

The CDPD system consists of several major components, and a block diagram of a CDPD system is shown in Figure B.44. The *Mobile End System* (MES) is a portable wireless computing device that moves around the CDPD network communicating with the MDBS. The MES is typically a laptop computer or other personal data device that has a cellular modem. The *Mobile Data Base Station* (MDBS) resides in the cell site itself and can use some of the same infrastructure that the cellular system does for transmitting and receiving packet data. The MDBS acts as the interface between the MES and the MDIS. One MDBS can control several physical radio channels depending on the site's configuration and loading requirements. The MDBS communicates to the MDIS via a 56-kbps data link. Often the data link between the MDBS and MDIS uses the same facilities as that for the cellular system, but it occupies a dedicated time slot.

The *Mobile Data Intermediate System* (MDIS) performs all the routing functions for CDPD. The MDIS performs the routing tasks using the knowledge of where the MES is physically located within the network itself. Several MDISs can be networked together to expand a CDPD network.

The MDIS also is connected to a router or gateway that connects the MDIS to a *Fixed End System* (FES). The FES is a communication system that handles Layer 4 transport functions and other higher layers.

The CDPD system uses a *Gaussian Minimum-Shift Keying* (GMSK) method of modulation and is able to transfer packetized data at a rate of 19.2 kbps over the 30-kHz-wide cellular channel. The frequency assignments for CDPD can take on two distinct forms. The first is a method of dedicating specific cellular radio channels to be used by the CDPD network for delivering the data service. The other method of frequency assignment for CDPD is to use channel hopping where the CDPD's MDBS employs unused

is assigned by the cellular system for a voice-communication call, the CDPD MDBS detects the channel's assignment and instructs the MES to retune to another channel before it interferes with the cellular channel. The MDBS uses a scanning receiver, or "sniffer," that scans all the channels it is programmed to scan to determine which channels are idle or in use.

The disadvantage of the channel-hopping method involves the potential interference problem with the cellular system. Coexisting on the same channels with the cellular system can create mobile-to-base-station interference. This kind of interference occurs because of the different handoff boundaries for CDPD and cellular for the same physical channel. The difference in handoff boundaries is due largely to the fact that CDPD uses a BER for handoff determination and the cellular system uses RSSI at either the cell site, analog, or MAHO for digital.

B.9 Summary

This Appendix covered numerous radio access platforms that were built to improve the efficiency of mobility systems offering voice services. The advent of the Internet during the time that these services were beginning to be deployed has resulted in a desire to have a wireless mobility system capable of handling high-speed data traffic. However, as with migrating from 1G to 2G, the path to 3G is not straightforward. It is hoped that inclusion of the 2G systems will facilitate introduction of 3G systems and the interim platforms that are currently being deployed, which are referred to as 2.5G.

References

- AT&T, *Engineering and Operations in the Bell System*, 2d ed., AT&T Bell Laboratories, Murray Hill, NJ, 1983.
- Barron, Tim, "Wireless Links for PCS and Cellular Networks," *Cellular Integration*, September 1995, pp. 20–23.
- DeRose, James E., *The Wireless Data Handbook*, Quantum Publishing, Mendocino, CA, 1994.
- Dixon, Robert, *Spread Spectrum Systems*, 2d ed., Wiley, New York, 1984.
- GSM 01.02: Digital cellular telecommunications system (Phase 21); General description of a GSM Public Land Mobile Network (PLMN).
- GSM 02.09: Digital cellular telecommunications system (Phase 21); Security aspects.
- GSM 02.17: Digital cellular telecommunications system (Phase 21); Subscriber identity modules functional characteristics.
- GSM 03.01: Digital cellular telecommunications system (Phase 21); Network functions.
- GSM 03.03: Digital cellular telecommunications system (Phase 21); Numbering, addressing, and identification.
- GSM 03.18: Digital cellular telecommunications system (Phase 21); Basic call handling; Technical realization.
- GSM 03.20: Digital cellular telecommunications system (Phase 21); Security-related network functions.
- GSM 04.02: Digital cellular telecommunications system (Phase 21); GSM Public Land Mobile Network (PLMN) access reference configuration.

- GSM 04.03: Digital cellular telecommunications system (Phase 21); Mobile Station-Base Station System (MS-BSS) interface channel structures and access capabilities.
- GSM 04.07: Digital cellular telecommunications system (Phase 21); Mobile radio interface signaling layer 3 general aspects.
- GSM 04.08: Digital cellular telecommunications system (Phase 21); Mobile radio interface layer 3 specification.
- GSM 05.02: Digital cellular telecommunications system (Phase 21); Multiplexing and multiple access on the radio path.
- GSM 05.03: Digital cellular telecommunications system (Phase 21); Channel coding.
- GSM 05.04: Digital cellular telecommunications system (Phase 21); Modulation.
- GSM 05.05: Digital cellular telecommunications system (Phase 21); Radio transmission and reception.
- GSM 05.08: Digital cellular telecommunications system (Phase 21); Radio subsystem link control.
- GSM 09.02: Digital cellular telecommunications system (Phase 21); Mobile Application Part (MAP) specification.
- Harte, Hoenig, and Kikta McLaughlin. *CDMA IS-95 for Cellular and PCS*, McGraw-Hill, New York, 1996.
- Jakes, W. C., *Microwave Mobile Communications*, IEEE Press, New York, 1974.
- Johnson, R. C., and H. Jasik, *Antenna Engineering Handbook*, 2d ed., McGraw-Hill, New York, 1984.
- Kaufman, M., and A. H. Seidman, *Handbook of Electronics Calculations*, 2d ed., McGraw-Hill, New York, 1988.
- Lee, W. C. Y., *Mobile Cellular Telecommunications Systems*, 2d ed., McGraw-Hill, New York, 1996.
- Lynch, Dick, "Developing a Cellular/PCS National Seamless Network," *Cellular Integration*, September 1995, pp. 24–26.
- MacDonald, V.H., "The Cellular Concept," *Bell Systems Technical Journal* 58(1), pg 15-42 1979.
- Newton, Harry, *Newton's Telcom Dictionary*, 14th ed., Flatiron Publishing, New York, 1998.
- Pautet, Mouly, *The GSM System for Mobile Communications*, Mouly Pautet, 1992.
- Qualcomm, "An Overview of the Application of Code Division Multiple Access (CDMA) to Digital Cellular Systems and Personal Cellular Networks," Qualcomm, San Diego, CA, May 21, 1992.
- Rappaport, Theodore, *Wireless Communications Principals and Practices*, IEEE Press, New York, 1996.
- Reference Data for Radio Engineers*, 6th ed., 1983.
- Smith, Clint, *Practical Cellular and PCS Design*, McGraw-Hill, New York, 1997.
- Smith, Clint, *Wireless Telecom FAQ*, McGraw-Hill, New York, 2000.
- Smith, Gervelis, *Cellular System Design and Optimization*, McGraw-Hill, New York, 1996.
- Steele, *Mobile Radio Communications*, IEEE Press, New York, 1992.