SIERRA WIRELESS
HEART OF THE WIRELESS MACHINE™

Sierra Wireless

CDPD Primer

2130006 Rev 1.0
April 2001

Copyright

The information in this manual is subject to change without notice and does not represent a commitment on the part of Sierra Wireless, Inc. Sierra Wireless, Inc. shall not be liable for incidental or consequential damages resulting from the furnishing, performance, or use of this manual.

Trademarks

AirCard® is a registered trademark of Sierra Wireless, Inc.

GroupWatcher™ is a trademark of Sierra Wireless, Inc.

Windows® and Microsoft® are registered trademarks of Microsoft Corporation.

All other brand or product names, logos, trademarks, etc. mentioned in this manual are owned by their respective companies.

Contact Information

Technical Support:	Canada/US:	1-877-231-1144
	Worldwide:	1-604-231-1128
	Hours:	6:00am to 5:00pm Pacific Time
	e-mail:	support@sierrawireless.com
Sales Desk:	Phone:	1-604-232-1488
	Hours:	8:00am to 5:00pm Pacific Time
	e-mail:	sales@sierrawireless.com
Post:	Sierra Wireless, Inc. 13811 Wireless Way, Richmond, BC Canada V6V 3A4	
Fax:	1-604-231-1109	
Web:	www.sierrawireless.com	

Consult our website for
up-to-date product descriptions, documentation,
application notes, firmware upgrades,
troubleshooting tips, and press releases:

www.sierrawireless.com

Contents

List of Figures

SIERRA WIRELESS
HEART OF THE WIRELESS MACHINE™

1. About this Guide

1.1. Introduction

The Sierra Wireless *CDPD Primer* is an overview of **Cellular Digital Packet Data** (**CDPD**), a standard for data transmission over wireless cellular telephone networks, such as those using the analog AMPS system, and widely available in North America. Many Sierra Wireless products support CDPD (see section 6). You can find more detailed information in the documents noted in section 7 at the end of this guide, and in the technical documents available for download from the Sierra Wireless Web site at www.sierrawireless.com.

1.2. Document Structure

1.2.1. Format

This document was prepared for distribution in Adobe Systems' Portable Document Format (PDF) from the Sierra Wireless Web site at www.sierrawireless.com. It includes bookmarks and hyperlinks to allow you to jump to sections, follow references, and access the Sierra Wireless Web site by clicking within the document. The PDF edition is designed for printing single-sided on standard letter-size paper. If your computer cannot read or print PDF files, Adobe provides a free reader at www.adobe.com/acrobat/readstep.html.

1.2.2. Organization

This guide consists of seven sections, of which this introduction is the first.

Section 2 covers the traditional and wireless **voice telephone systems**, including the plain old telephone system (POTS) and cellular telephones.

Section 3 discusses the **background of the CDPD standard:** its history, and its features in comparison with other wireless data standards.

Section 4 details the **architecture of a CDPD network:** its technology, hardware, and protocols. This section includes information about the physical components of the network, its protocol layers and how they interact, and the services it provides.

Section 5 goes into some detail about the **operation of a CDPD network**, including: how CDPD devices register with the network, how data moves through it, how radio resources are managed, how users share bandwidth, and how CDPD modems save power using sleep mode.

Section 6 discusses **Sierra Wireless products** that support CDPD, and **section 7** lists **resources** for further reading, study, and reference.

1.3. References

1.3.1. Terminology and Acronyms

This document makes wide use of acronyms that are in common use in data communications. For our *Glossary* of acronyms and terms used in Sierra Wireless documentation (document 2110032), please consult the document downloads on our Web site at www.sierrawireless.com, as well as section 7 of this document.

2. Telephones and Wireless Data Transmission

2.1. Telecommunications and the Telephone

Today's wireless data communications standards, including CDPD and more recent varieties, evolved from technologies in different industries, including radio and data communications. CDPD's most direct and well known ancestor is the traditional telephone system, which is where we begin our history.

2.1.1. Wireline Telephones

The wireline telephones with which we are all familiar evolved from the telegraph system, and are known within the industry as the **Plain Old Telephone System**, or **POTS**. They are connected to the **Public Switched Telephone Network** (**PSTN**). Wireline telephones operate on a **circuit-switched** system (see section 2.3.1), which means that in any phone call there is effectively a single, continuous, dedicated wire connecting one party to the other. In today's digital-switched telephone systems, the situation is slightly more complex, but the dedicated circuit remains.

Through the twentieth century, many other technologies piggybacked upon the PSTN, including telegrams, fax transmissions, credit card authorizations, newswires, various videophone techniques, corporate PBX telephone exchanges, e-mail, and Internet access. Each adapted itself to an underlying infrastructure designed purely for the human voice.

2.1.2. Wireless Telephones

Most radio transmissions are broadcasts, where a single powerful transmitter sends signals—such as music, speech, or television images—to anyone who can receive them in a given (often fairly large) area. Two-way radio communication has long been used by law enforcement, other public safety agencies, marine and aircraft navigation, the military, urban dispatchers, and CB and Ham radio enthusiasts.

Neither broadcast nor two-way radio was initially linked into the vast telephone network. Early attempts to connect them and create a wireless telephone system were unsuccessful, largely because they generally used a single large transceiver station for each city. Radio frequencies are limited, so only a few people could make wireless calls simultaneously, even in a large city. Conversations had to be patched through an operator who linked the radio transmission into the PSTN, and the calling phones (to be powerful enough to reach the single central antenna) were bulky. Also, only one person could speak at a time: the sets could either send or receive, but not both at once.

For wireless telephones to succeed, engineers and regulators needed to find ways to make the process simpler and more convenient, subdivide the radio bandwidth, and make smaller phones.

2.2. The Advanced Mobile Phone System (AMPS)

Although originally developed in the 1960s, it wasn't until 1983 that the **Advanced Mobile Phone System** (**AMPS**) was implemented in North America. AMPS was the first widespread wireless mobile telephone system, replacing the one or two large and powerful transmitters and receivers in a city with a constellation of dozens or hundreds of small transceivers, running at much lower power (originally about 100 W each, but with new technology about 50 W today).

The range of each transceiver—also known as a **base station** or **cell site**—is limited, and so it acts as the hub of a relatively small **cell**. In that cell, personal transceivers—cellular phones, also

called **handsets**—can both receive signals from, and send signals to, the base station. All the cell sites for one cellular service provider connect into an automated central management system, and from there into the wider PSTN; so AMPS users can seamlessly call both traditional wireline phones and other mobile phones (whether on their network or not), and vice versa.

AMPS has been remarkably successful. In the 1960s, its developers predicted perhaps a million users in North America by the year 2000. In reality, that number was in excess of 50 million. AMPS, an analog system, is the oldest of the North American cellular phone technologies. Newer digital systems may use different radio frequencies and encode voice information differently, but as a whole they operate fundamentally the same way.

2.2.1. Why Cellular?

A cellular system lets the same limited range of radio frequencies get used over and over again. Even though there are only 832 conversation channels available in the 50 MHz of radio bandwidth assigned to AMPS networks, tens of thousands of simultaneous conversations can take place. Many cellular telephones across a city may be using the same channels at one time, but because each cell base station has a limited range (and because of other limitations imposed on the system, see section 2.2.6 below), they do not interfere with one another.

Since cellular telephones must be relatively close to their base stations to operate, the phones can be quite small and use low-power transmitters. Early AMPS phones were suitcase-sized—similar to their non-cellular counterparts—but technological improvements mean that today's analog cellular phones, and especially their digital descendants, can be small enough to fit in a shirt pocket.

2.2.2. Analog FM Using Different Channels to Send and Receive

AMPS is an analog standard, which means that voice conversations are directly represented in the radio transmission as changes in the radio waveforms. Digital systems, by contrast, encode voices as binary digits which are *then* modulated into the radio waveform. AMPS uses **frequency modulation** (**FM**), the same technique implemented in FM radio broadcasts, but an AMPS cellular phone channel has a far smaller slice of bandwidth (30 kHz) than an FM radio station (200 kHz)—so a cellular phone call is obviously of lower quality than an FM radio broadcast. (To avoid interference and crosstalk, the frequency range of the voice transmissions themselves is only 3 kHz, slightly less than the 4 kHz of a wireline POTS phone call.)

Cellular networks use a portion of the radio frequency spectrum assigned by government regulators. For AMPS cellular phones, that range is between 824 and 894 MHz. A connection consists of two 30 kHz channels, widely separated in frequency: a receiving channel (also known as the **forward channel**) from the base station to the phone, and an independent sending channel (known as the **reverse channel**) from the phone to the base station. Since the channels are separated by frequency, the AMPS technology is also known as **Frequency Division Multiple Access** (**FDMA**). The frequency separation allows AMPS calls to be **full duplex**: both parties can speak, and be heard, at the same time.

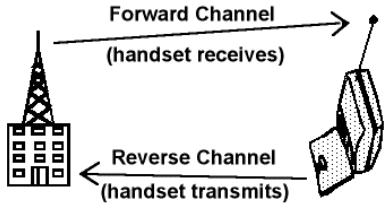

Figure 2-1: Forward and reverse channels

2.2.3. A-side and B-side Carriers

The 50 MHz of spectrum assigned to AMPS cellular phones has been further divided by regulatory bodies. In each region served by AMPS services, there can be two competing cellular phone providers, arbitrarily known as the **A-side** and **B-side carriers**. One carrier is usually the same company that provides local wireline telephone service, and the other is a separate firm, most often one that does not provide wireline phone service.

A-side carriers use **Band A** of the AMPS spectrum. Their cellular phones transmit in the frequency ranges 824-835 MHz and 845-846.5 MHz, and they receive in the 869-880 MHz and 890-891.5 MHz ranges. These correspond to cellular channels numbered 1-333, 667-716, and 991-1023. B-side carriers use **Band B**, which transmits at 835-845 MHz and 846.5-849 MHz, and receives at 880-890 MHz and 891.5-894 MHz, corresponding to cellular channels 334-666 and 717-799. Each carrier has 416 pairs of 30 kHz channels available, although the number for calls is smaller, since each cell requires one or two control channels to manage the operation of the network.

Each carrier has its own infrastructure, and sets up transceiver base stations at cell sites on towers, in buildings, or on hilltops. In any particular coverage area, each of the two carriers organizes its cells so that telephones can move from one to another without losing contact with the network.

2.2.4. Cell Sites Coordinated by the MTSO

The coverage areas of each base station—the cells that give the cellular network its name—are roughly hexagonal (see Figure 2-3), although in rural areas and those of rough terrain, cell shapes may differ. The interaction between sites is managed by the carrier's central **Mobile Telephone Switching Office** (**MTSO**). At the heart of the MTSO is the **cellular switch**, which also links into the voice circuits of the PSTN. For cellular phone users, the cellular switch makes the cellular network a nearly seamless part of the PSTN.

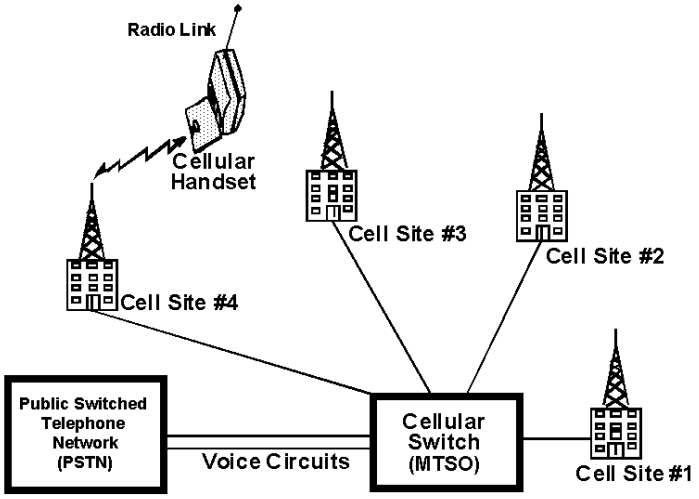

Figure 2-2: A cellular telephone system

The cellular switch is the central coordinating element for all of the cell sites for one carrier in one area, such as a city. It performs all call processing functions and supports certain aspects of network accounting and management.

Purchasers of cellular handsets generally activate them with their carrier, and with a particular local cellular switch for that carrier, providing that handset with a **home** cellular network. Arrangements within that carrier and between it and other carriers in other cities may allow the handset to operate outside the home region when the subscriber travels. When the handset communicates with a different carrier than normal, it is said to be **roaming**.

2.2.5. Assigning and De-Assigning Frequencies

When a cellular subscriber originates or receives a call, the MTSO assigns the subscriber an available radio channel from the group of channels assigned to that carrier. Once assigned this channel, the call progresses until:

- the subscriber terminates the call, when the MTSO de-assigns the radio channel from the cell site and makes it available for new calls.
  –or–

- the subscriber moves so that a different cell site provides better coverage, when the MTSO de-assigns the radio channel from the old cell site and assigns a new radio channel from the new cell site—one which provides better signal quality. This scenario is known as a **handoff** (see section 2.2.7). The user might notice a handoff as a very brief (about 1/10 second) gap in a voice call during the switch to a new channel.

The designers of AMPS chose a hexagonal shape for cells because hexagons can be tiled together indefinitely over any reasonably flat terrain (see Figure 2-3), and so can adapt to a city of any size. Since radio frequencies in the 824-894 MHz range travel line-of-sight, and because transmissions from 50 W antennas fall off rapidly, cell sites need to be evenly spaced. They can be more or less densely packed depending on the number of subscribers in the area, and on the number and type of obstacles nearby. Cells are likely to be more densely packed, and the hexagons smaller, in downtown cores than in outer suburbs, for instance.

2.2.6. Reusing Frequencies

Cellular radio engineers have improved system throughput and capacity by dividing each cell into three **sectors** (although some systems support up to six sectors per cell). The basic cell reuse pattern consists of seven cells in which only 21 individual radio channels are required to provide radio coverage over any desired geographic area.

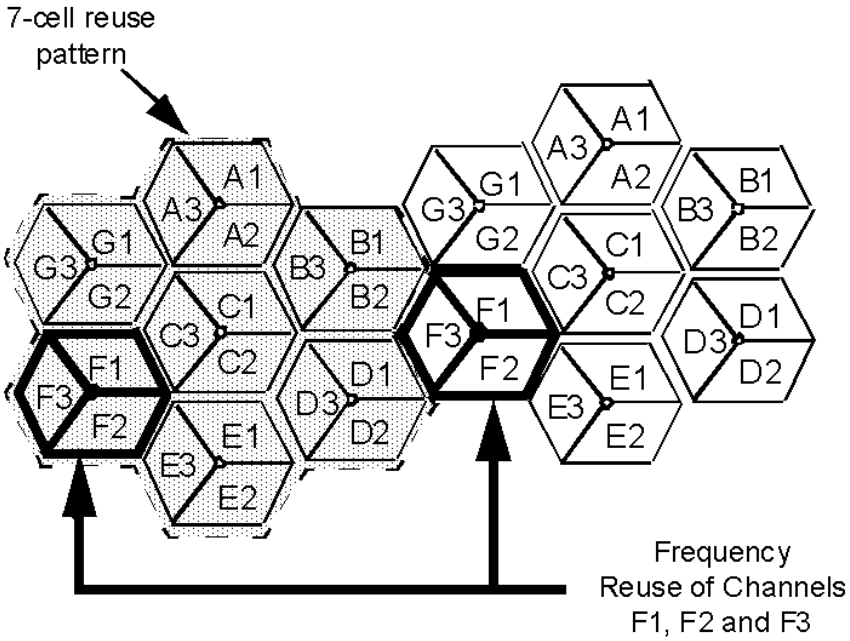

Figure 2-3: Cellular channel reuse using three sectors per cell

In this example, the seven cell sites are labeled A though G, and the three sectors per cell site are labeled 1, 2, and 3. Thus, the 21 sectors per reuse pattern are labeled A1, A2, A3, B1, B2, and so on through G1, G2, and G3. The cellular switch assigns a unique radio channel in each of these sectors for use in that sector only.

So, for instance, the three radio channels at cell site F are not reused until approximately four cell radii away. Such an arrangement avoids interference and crosstalk between separate cellular telephone calls. The seven-cell pattern can also be tiled like puzzle pieces, so no two cells sharing radio channels are close enough to cause interference problems.

2.2.7. Cell Handoff

Using a typical seven-cell, three-sector channel reuse pattern, call handoff is straightforward, allowing a cellular handset to move through and between cells while smoothly continuing a call.

In this example, the cellular subscriber makes (or receives) a call in sector A3. They move to sector A1 and experience a handoff at location 1 where they are handed off to a new radio channel in sector A1. From sector A1 they travel to sector A2 and are handed off at location 2. In the cases of the handoffs at locations 1 and 2, the cellular subscriber has been handed off to radio sectors within the same cell site.

As the cellular subscriber travels from sector A2 to C1, they are handed off to a new radio channel being served by a different cell site. This handoff procedure continues until the cellular subscriber eventually arrives in sector B2 after having been handed off at location 5.

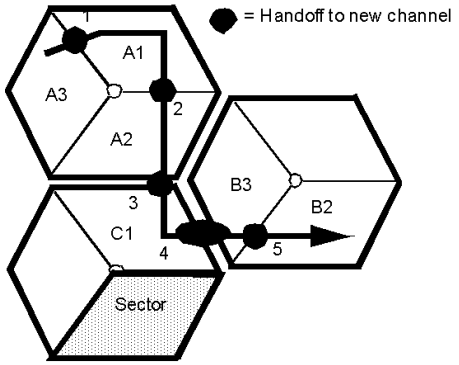

Figure 2-4: Cell handoff in three-sector cells

In all cases, the cellular subscriber is assigned a radio channel available within a certain sector and that radio channel is de-assigned from that subscriber once they have been handed off by the cellular switch to the new sector. The de-assigned radio channel is then made available for another user within that sector.

Although the cellular handset uses six different radio frequencies and communicates with three different base stations over the course of this portion of the call, the continuity of the call is not affected. Other than possible short delays during the five handoffs, the call continues transparently.

2.3. Cellular Data Transmission

The introduction of the AMPS cellular system in North America in 1983 coincided with the first public popularity of long-distance data transmissions between personal computers. Using **modems** (modulator-demodulators) and POTS wireline telephones, personal computer users could convert data streams into audible tones that could be transmitted through the phone system, initially at 110 or 300 **bits per second** (**bps**). Like fax before it, such data transmission took advantage of a system designed purely for voice to transmit something else.

It would not be long before users of notebook computers, once they were widely available, wanted to be able to connect modems wirelessly, perhaps to hook up to an online service, a corporate bulletin board system (BBS), or even a home computer. Once again, a system designed for voice—in this case, the AMPS cellular network—would be used for data.

2.3.1. Circuit-Switched vs. Packet-Switched Data

While public safety bodies and large corporations such as IBM and FedEx created their own proprietary wireless data networks in the 1970s and ’80s, individual users who really wanted to move data in a mobile environment developed methods of connecting their conventional wireline modems to their cellular phones, with mixed results. This groundswell of demand led engineers to develop modems specifically for connections through cellular telephones, yielding a fairly reliable service capable of offering data at 9600 bps (9.6 kbps).

The ad-hoc solution of connecting a modem to a cellular phone works, but the end user pays by the minute with long distance charges where applicable, because each call remains **circuit-**

switched—using up the entire bandwidth of a cellular channel for the audible tones used to modulate the data transmission.

With the growing popularity of the Internet in the 1990s, circuit-switched became even less appropriate for most data transmissions. Like many computer data transmissions, Internet connections are "bursty", with short flows of information interspersed with long idle periods.

The Internet's standard **Transmission Control Protocol** and **Internet Protocol** (**TCP/IP**) take advantage of this burstiness by being **packet-switched**. Data is broken into small **packets** that are wrapped with information describing their length and destination (specified in the **packet header**). Thousands or millions of these packets can share a transmission medium—whether a wire, a laser in a fiber-optic cable, a microwave beam, or a radio channel—because each one is targeted to a destination.

The Internet's technology infrastructure reads the packet headers and routes them to their destinations, where the receiving computer can reassemble the packets into a reconstituted version of the original information. An additional advantage is that packets can include error correction, such as the **Forward Error Correction** (**FEC**) used by CDPD (see section 5.5) to prevent data loss.

Creating a packet-switched data standard that could be widely used over the AMPS cellular network, using the emerging Internet standards of TCP/IP for packet encapsulation—and which could be billed by the packet instead of by the minute—was a reasonable goal for the telecommunications industry. It led to the birth of CDPD.

3. Background: Introduction to CDPD

3.1. Cellular Digital Packet Data (CDPD)

In 1991 the U.S. cellular operators began a process to offer packet data technology for services such as e-mail and telemetry. The result was **Cellular Digital Packet Data** (**CDPD**), which the carriers began to deploy in 1993. Today, regions of CDPD coverage include most of North America's population.

CDPD is an open specification. It is fully documented, with the complete specification available online from www.wirelessdata.org/develop/cdpdspec.

CDPD shares radio frequency channels with AMPS cellular voice calls, but it has its own infrastructure that piggybacks upon the AMPS technology. Cellular carriers who choose to support CDPD must install additional equipment to handle data separately from AMPS voice. CDPD also requires its own modems for end users, and operates quite separately from cellular voice handsets—even while sharing channels with them.

Cellular carriers derive the vast majority of their revenues from voice, and are expected to continue to do so for some time, although data use is growing. The need to optimize voice revenues therefore drives the development of new technology, so CDPD was developed with the primacy of voice in mind.

The overall **CDPD network** operates as a collection—an **internetwork**—of **CDPD service provider networks**, where the CDPD networks of each cellular carrier communicate with one another, routing data from one CDPD network to another, often through the wider Internet. CDPD carriers provide services such as:

- Data connection to other networks
- Application services
- Network management
- Network security
- Accounting and billing

Just as cellular carriers ensure that end users see the AMPS network as a nearly seamless part of the wireline PSTN, they work to ensure that CDPD users are transparently connected to the Internet, and to each other.

3.1.1. Packet-Switched Data Shared With Voice Calls

Although CDPD operates over the AMPS analog cellular telephone network, CDPD itself is fully digital, using **Gaussian Minimum Shift Keying** (**GMSK**) modulation to encode data on the same 824-894 MHz radio frequency channels as AMPS voice calls. In fact, CDPD is designed as a way for cellular carriers to capture additional revenue by using the short blank spaces between AMPS voice calls to transfer data.

There are long periods during which one or more of the radio channels within an AMPS cell sector are not in use. In other words, there is spare capacity available on the cellular system. Figure 3-1 shows a simplified sample with three channels in a sector allocated for cellular voice use.

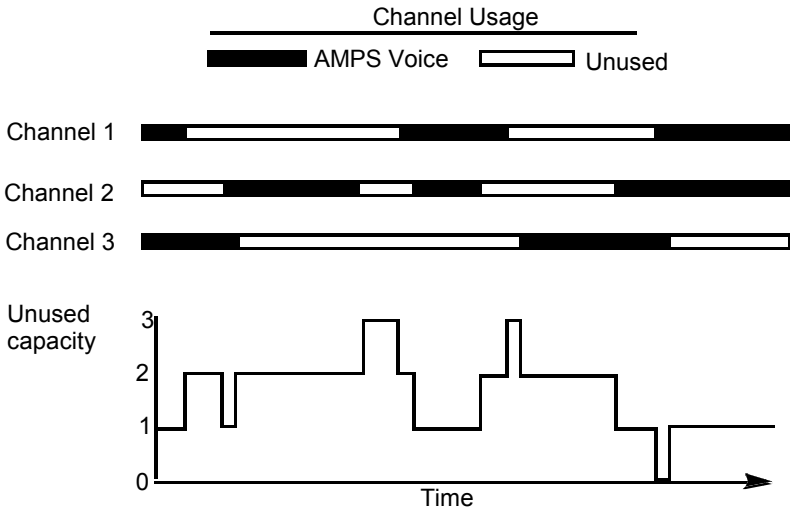

Figure 3-1: Cellular radio channel usage within a single cell sector

In this example, the unused channel capacity ranges between 0 and 3 radio channels. The CDPD concept is based on sending packet-switched data on radio channels within a sector when they are not used for cellular voice communications. It reuses these unused voice channels by hopping from one unused voice channel to another whenever that channel is required for cellular voice. In other words, CDPD reuses the unused channel capacity in a voice cellular network for packet switched data.

3.1.2. Channel Hopping

Figure 3-2 shows how short data packets can be interleaved between voice calls on the cellular network, using the idle capacity in the system—known as a **"sniff and hop"** configuration. is known as the **airlink**.

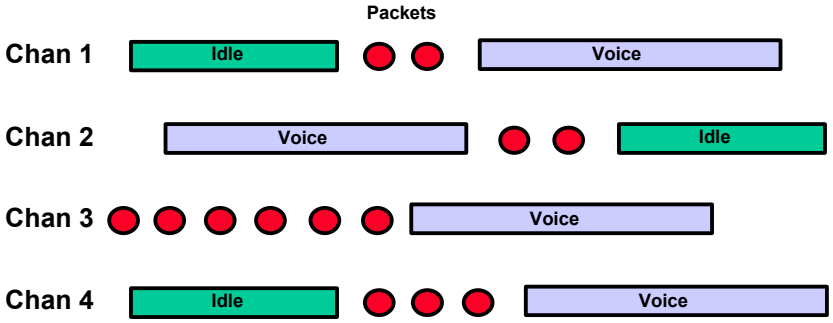

Figure 3-2: CDPD channel hopping

Channel hopping on the **airlink**—the wireless portion of a CDPD transmission—works well under typical voice usage, but as the network becomes congested, less room is available for data traffic. Many CDPD carriers have therefore agreed to guarantee to have channels dedicated to data transmission only (see section 3.1.3). Otherwise, in an emergency situation like a flood or hurricane, the cellular system could become completely clogged. Even in a dedicated system, there is no guarantee that the modem will stay on an acquired channel very long. If the modem is mobile, it will be forced to frequently change channels as it travels through the carrier's territory from cell to cell.

Two types of channel hops can occur in CDPD systems not using dedicated channels:

- Planned channel hops
- Forced channel hops

Planned channel hops occur at a time specified by the CDPD network. For example, the CDPD network management function may configure the CDPD base station to use only a specific channel for a fixed period of time and then hop in a round-robin fashion to another of the radio channels used within a specific sector. In this case, the CDPD base station (known as the **Mobile Data Base Station**, or **MDBS**) directs the modem (the **CDPD subscriber device**) to the new channel to be used for CDPD activity. If not within another sector, the same channel may be acquired.

Forced channel hops occur when cellular voice activity is detected on a channel currently carrying CDPD packet-switched data traffic. In this case, the CDPD base station initiates a change of frequency to a new channel available within that sector that does not have any cellular voice activity on it.

The base station in the CDPD system uses both planned and forced hops to switch CDPD subscribers between the unused cellular voice channels to avoid interference between CDPD and cellular voice traffic. While this channel-hopping activity is in progress, the CDPD network maintains the data link connection between the CDPD subscriber and the CDPD network even though the physical radio link between the CDPD subscriber and the CDPD network changes radio channels over time. This channel hopping activity is transparent to the CDPD subscriber.

Figure 3-3 shows an example of simultaneous cellular voice and CDPD data use on a sector supporting three radio channels.

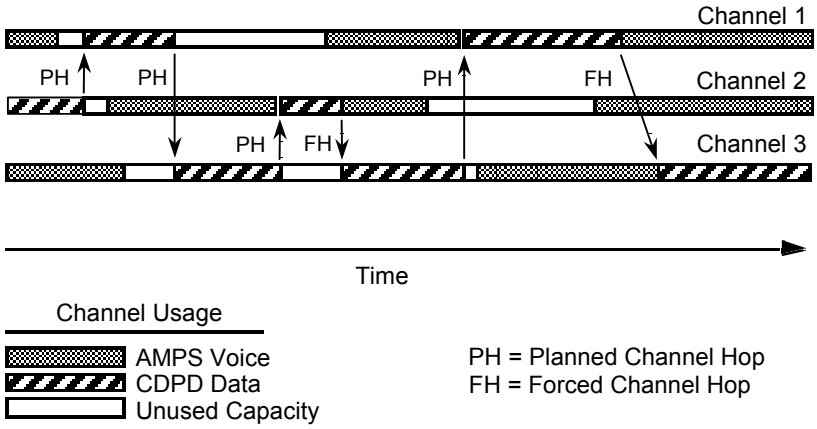

Figure 3-3: How cellular voice and CDPD coexist in a three-channel sector

In this example, a single CDPD data link is supported within the three-channel sector. Of the six channel hops shown in the example, four are planned and two are forced. The first forced channel hop is used to avoid the cellular voice activity that occurs on channel 2, and the CDPD data link is maintained by the CDPD base station, forcing the subscriber device to hop to channel 3.

3.1.3. Dedicated CDPD Channels

CDPD data traffic was originally expected to be infrequent short bursts of data typical of telemetry or credit-authorization applications. In the early days, most CDPD systems used shared channels only with voice having priority.

It quickly became apparent that during busy periods there were few if any channels available for CDPD to switch to—the CDPD system was "blocked." A number of applications, including public safety and credit card authorization, could not tolerate blockage of the system. The carriers solved the problem by reserving one or more channels on most CDPD cell sites for CDPD traffic only.

Although giving up a voice channel for CDPD meant less voice revenue, carriers did not want to hinder the growth of CDPD by forcing it to use only the available extra space on voice channels, although such service can still be found in some rural areas.

3.1.4. Base Station Broadcast Parameters

CDPD base stations regularly broadcast information (known as **cell configuration messages**) to all CDPD subscriber devices so that they know all channels available both within the cell and in neighboring cells. This information is then used by the CDPD subscriber device to find new CDPD channels in the event of a planned handoff or forced channel hop. Other information is also sent as broadcast messages, allowing CDPD subscriber devices to determine, for instance:

- When they have moved to different areas within the cellular geographic coverage area
- Parameters to control the subscribers' transmitter power levels

The operating parameters broadcast by the MDBS include:

- Thresholds and threshold time limits
- Available channel lists
- An evaluation (rescan) frequency
- A signal strength change (hysteresis) value

The modem continually monitors its radio environment and compares the current values to the thresholds and time limits; if any of the thresholds are exceeded for longer than their permissible time limit, the modem must find a better channel. To speed up this search, the modem makes use of the available channel lists picked up from the MDBS along with the operating parameters.

In addition, the modem periodically (typically every 90 seconds) evaluates the alternative channels to ensure that it is always operating on the best available channel. Also, if the **Received Signal Strength Indication** (**RSSI**—see section 3.2.6) changes by more than a predetermined amount (typically 8 dB) from its initial acquisition value (either up or down), the modem must re-evaluate the alternative channels to ensure that it is currently using the strongest one in the area. See section 5.6 for more information.

3.1.5. CDPD Services Provided Over the Airlink

CDPD includes a number of mechanisms to manage the airlink and provide data services over it. They include **Medium Access Control** (**MAC**), the **Mobile Data Link Protocol** (**MDLP**), and the **Subnetwork Dependent Convergence Protocol** (**SNDCP**)—discussed in section 5. Services they provide include:

- Compression of packet header and information fields transmitted over the wireless channel to reduce the amount of airlink time used.
- Support of many users on the same cellular radio channel at the same time.
- Error correction of data sent over the airlink.
- Encryption of data while transmitted over the airlink.
- Tracking movement of the user from one cell site to another.
- Delivery of properly-sequenced data between user applications over the airlink.
- Multicast service: a company can periodically broadcast company updates to sales and service people on the road; a news subscription service can transmit its issues as they are published.

Mobility management services within the CDPD network provide continuous communications to mobile subscribers while their location changes within the coverage area provided by CDPD.

The CDPD network provides a **Connectionless Network Service** (**CLNS**), one in which the network routes each packet individually within the network based on the destination address carried in the packet and knowledge of the current network topology. It is often referred to as a **datagram** service.

3.1.6. A Buffer Between the Internet and the Modem

A key difference between CDPD and more typical Internet data connections is that a CDPD modem has no fixed location. Pure Internet technologies using TCP/IP cannot handle such mobility, because they assume that a destination address does not change from minute to minute or second to second.

The CDPD infrastructure provides a buffer so that, to the wider Internet, packets destined for a CDPD device can be routed as normal, through a fixed series of addresses. The CDPD system captures these packets and then routes them to the CDPD device according to information the CDPD network maintains about the modem's current location. From the user's point of view, only the destination address is known, since the CDPD network manages the packet routing (see section 5.2.1).

3.2. Features of CDPD

CDPD is designed to be flexible, efficient, and open. It is packet-switched, based on standard data protocols used on the Internet, operates at full duplex, provides good data throughput, supports a large number of simultaneous users, is straightforward for carriers to implement, and provides effective data encryption and access control.

3.2.1. Packet-Switched

As mentioned previously, CDPD is a packet-switched system, which allows users to pay only for data they send and receive, not the time they are connected to the CDPD network. An additional benefit is that once registered with the network (see section 5.1), a CDPD modem can stay connected indefinitely at no cost if no data is sent or received—the equivalent of an "always on" wired Internet connection. Finally, a packet-switched system allows many more users to transfer data over a single radio channel (see section 3.2.5) than a circuit-switched system, which can support only one user per channel at a time.

3.2.2. Based on Internet Protocols

Some other wireless data standards (such as ARDIS and Mobitex/RAM) use their own proprietary protocols, or ones that differ from standard Internet TCP/IP implementations. Connecting them to the Internet requires protocol translation, adding an extra step to the data connection, and thus making it slower and potentially less reliable.

CDPD was originally built as an IP-based system, so once a CDPD network is properly set up and configured, CDPD devices can connect to them the same way as they would to a LAN or dial-up Internet connection. In many instances, notebook users can simply replace an Ethernet or modem PC Card with a CDPD modem PC Card and continue working. CDPD is therefore easy to develop for, and easy to integrate into existing systems and applications. A CDPD subscriber device can access anything accessible over the Internet. (CDPD can support protocols other than TCP/IP as well, as long as both ends of the connection do—see section 4.3.8.)

3.2.3. Full Duplex

Like early radio telephones, and like "walkie-talkie"–style two-way voice radio, some wireless data standards are half-duplex, allowing unidirectional transmission only. If a client device is sending data, no data can come in; and if data is being received, no data can be transmitted until the reception is complete.

CDPD takes advantage of the AMPS cellular system's two-channel setup. Like AMPS voice calls, As with the separate AMPS voice channels discussed in section 2.2.2, CDPD uses two widely-separated radio frequencies for any given transfer, one for receiving (forward) information, and one for transmitting (reverse) information. Sending and receiving can happen simultaneously—a **full-duplex** connection.

3.2.4. Transmission Rate and Peak Throughput

CDPD offers raw transmission rates of 19.2 kbps. Error control overhead means that actual throughput of useful data can be up to 12 kbps on a clean, lightly-loaded channel. Data transfer rates may be lower on congested networks with many voice or CDPD transmissions underway. Data compression can, of course, increase the effective throughput.

CDPD protocols have low overhead, especially since they require no protocol conversion to TCP/IP for Internet connectivity. CDPD also compresses the IP protocol overhead, increasing throughput and using less radio bandwidth.

3.2.5. Number of Users Supported

Like any data communications system, each CDPD data link has a maximum capacity it can support. In the case of CDPD, the airlink is the limiting resource of the network. The user data transmitted over the air is a **frame** (a data block that includes header and error detection information) with a maximum length. The maximum 19.2 kbps throughput of CDPD limits the number of frames that can be sent over the channel. On average, if a user has an application that requires 5% of this maximum channel capacity, then one radio channel data link can support 20 users. On average, if a user has an application that requires 1% of this maximum channel capacity (not unusual, especially for light Internet connectivity), then a single radio channel data link can support 100 users.

The nature of most user data applications is that the amount of data sent is small (a few frames) and the rate at which the data is sent is bursty (short periods of activity, followed by long periods of idle time). As a result, a CDPD radio channel data link can support a large number of users at one time. The maximum number of users that can be supported on a single radio channel data link depends on the nature of the data traffic that the users' applications send.

3.2.6. Coverage and Availability

CDPD operates as an overlay on top of the existing analog AMPS cellular infrastructure. Thus, to implement CDPD, carriers need only add **Mobile Data Base Stations** (**MDBSs**), **Mobile Data Intermediate Systems** (**MD-ISs**), and other **Intermediate Systems** (**ISs**) to quickly deploy CDPD (see section 4.1 for details on these components). Although no single nationwide CDPD service exists across the U.S., most major metropolitan areas are covered, and **roaming agreements** between most CDPD carriers—in which a CDPD device activated in one area can connect through base stations linked to MD-ISs in another region, similar to voice roaming arrangements—generally allow a single account to be used across the broad CDPD network.

Currently, CDPD coverage is available for the majority of the population of North America. However, even carriers that provide CDPD service may not make it available over their entire analog cell coverage area. Subscribers need to obtain coverage information for their region from their carriers.

The strength of the radio signal received by the modem indicates the airlink quality, and can be measured using the **Received Signal Strength Indication** (**RSSI**). RSSI is expressed on a logarithmic scale, in decibels relative to one milliwatt (dBm). A strong signal level has a less negative number; a weak signal level has a more negative number. For example, a signal level of -60 dBm is stronger than one of -100 dBm.

CDPD modems are designed to measure the RSSI and adjust their transmitted power output accordingly, within the limits permitted by telecommunications regulations and how the local carrier has set the serving MDBS (see section 5.6.2). However, connections are lost for signals below a certain strength level. For example, many devices lose their CDPD connections when the signal strength falls below the -105 to -110 dBm range.

A CDPD carrier attempts to ensure that the signal level is fairly strong (-80 dBm or stronger) throughout the coverage area. Shielding of the signal by artificial structures or natural obstacles may weaken the signal, sometimes cutting off the connection.

The signal could be weaker than desired in locations such as:

- Underground parking garages
- Tunnels
- Buildings with all metal construction
- Old concrete buildings with many steel reinforcing bars

In these cases, the CDPD subscriber may be able to get a stronger signal by locating the antenna near an opening or window.

One of the functions of the CDPD service provider is to manage their CDPD network in order to support a CDPD subscriber anywhere in their cellular geographic coverage area and deliver an acceptable level of service. The CDPD service provider should also make the necessary agreements with other providers so that roaming access is available outside of the original provider's coverage area.

3.2.7. Encryption and Security

Since CDPD is a public wireless data communications service that could be susceptible to eavesdropping, all data transferred between the CDPD modem and the MD-IS (except broadcast messages) is **encrypted** by CDPD's **Encryption Services**, using RSA algorithms (see section 4.2.7). Data beyond the MD-IS is generally not encrypted, much as general Internet traffic remains unencrypted unless the end user provides it.

3.2.8. Access Control and Congestion

Like wired Ethernet connections, CDPD is a **contention-based** system. It uses **DSMA-CD** (**digital sense, multiple access, collision detect**), while Ethernet uses **CSMA-CD** (**carrier sense, multiple access, collision detect**). In both systems, when a device has data to send it senses the transmit medium to determine if it is currently busy (see section 5.5.1). If not, it will send its data, and then wait to see if it is acknowledged by the receiver. If two devices did this at approximately the same time a data "collision" would occur. The receiver would be unable to decode the "smashed" data and would return a "decode failure" indicator. This indicator would be sensed by the sending devices, which would then enter a random back-off period before trying again (see section 5.5.2).

The CDPD-defined **MAC** (**Medium Access Control**) protocol is used to manage this function (see section 5.5). Since each CDPD channel actually consists of physically separate forward (network to modem) and reverse (modem to network) data paths, the system can operate in full duplex mode. The forward (receive) channel maintains a busy/idle flag for the reverse (send) channel, allowing the modem to monitor and determine when the channel is open.

The CDPD system allows a single user to access the radio channel data link while transmitting. This inhibits all other users from transmitting until the currently active user becomes idle. The maximum time a single user can access the radio channel on any single transmission is about 1 second. CDPD networks can allow a maximum of 64 blocks, of 385 bits each, in a single transmission, but the actual limit is set by a parameter controlled by the MDBS. Initial access to the channel is random, due to the contention-based nature of the access mechanism.

The impact of this mechanism to the CDPD user is that there may be small delays in accessing the radio channel data link. When the user traffic on the channel is light, these delays are minor (typically less than 0.1 seconds). When the traffic on the channel is heavy, the delays can become larger (typically less than 1 second). As a result, user applications may experience slightly lower apparent throughput when the CDPD radio channel data link becomes more heavily loaded. It is fairly typical for the channel loading to vary cyclically throughout the day. Typically, channel loading is light at midnight and heavier near daybreak, noon, and late afternoon.

3.2.9. CDPD Data Transmission Format

CDPD data is sent in **Reed-Solomon blocks** of 378 bits, each consisting of 63 six-bit symbols. Of the 63 symbols, 47 carry user data or protocol, while the remaining 16 symbols provide parity. Since the airlink is inherently vulnerable to interference and noise, the high number of parity bits enables the protocol to recover blocks in which up to 7 of the 63 symbols have been damaged. Full-duplex devices are permitted to chain multiple Reed-Solomon data blocks. The CDPD recommended default value for the maximum number of blocks is 64. Many carriers use a lower number—32 is common.

CDPD adds capacity to a sector in a cellular system by supporting several active CDPD data link channels at one time (these are also known as **channel streams**—see section 4.1.2). The CDPD network manages the control of these multiple data links such that users always maintain their end-to-end data connection. It prevents the subscriber's device from becoming confused about which data link it is operating on. This control is transparent to the user.

4. Infrastructure: CDPD Network Architecture

4.1. Physical: Components of the CDPD Network

As mentioned in section 3.2.6, a cellular carrier can construct a CDPD network with a few new components added to the existing AMPS cellular phone infrastructure. Such a process costs less than creating a completely separate wireless data infrastructure. However, it is far from inexpensive, since not only does it require new interface elements between the CDPD network and the Internet, but also additional equipment installed at each cell site. Users desiring CDPD connectivity also require CDPD-capable modems, such as those designed by Sierra Wireless (see section 6).

A CDPD service provider network can be constructed from four of the five basic building blocks described below (that is, the M-ES, MDBS, MD-IS, and IS). The F-ES is the destination system, which can be outside the CDPD network. This network construction takes into account such things as:

- Providing coverage over a large geographic area. This ranges from coverage within a city to nationwide and international coverage.
- Matching the airlink capacity available with the demand placed on it by users requiring service within the CDPD coverage areas.
- The need to provide access to private and commercial external networks.

Networks are often constructed by interconnecting several networks into an **internetwork** (see section 3.1). The networks that make up the internetwork often have their own administration and routing policies and are called **administrative domains**. The CDPD network is actually an internetwork composed of multiple administrative domains, with each administrative domain operated by a service provider. This administrative domain is referred to as the **CDPD service provider network**.

4.1.1. End Systems (M-ES and F-ES)

The purpose of the CDPD network is to allow data to be transmitted to and received from **End Systems** (**ESs**) that are attached to the network. An end system in the CDPD sense is a host running a user application and having a unique identity. This unique identity is provided in the end system through at least one globally unique **Network Entity Identifier** (**NEI**—see section 5.1.1). The CDPD subscriber obtains an NEI from the service provider when they activate their CDPD modem on the service provider network. This is equivalent to activating a cellular telephone with a cellular service provider when signing up for service on that voice network.

In the terminology of CDPD networks, the CDPD subscriber device—often, for instance, a PC Card CDPD modem inserted into a notebook computer—is known as the **Mobile End System**, or **M-ES**. It connects to the network via the airlink, and is always part of the CDPD network. By contrast, a host computer connected into the CDPD network with a traditional wired connection, such as through the Internet, is known as a **Fixed End System**, or **F-ES**. An F-ES can be anywhere, either inside the CDPD network or outside of it.

The CDPD network makes a distinction between Mobile End Systems and Fixed End Systems for the purposes of mobility management. M-ESs can change their **Subnetwork Point of Attachment** (**SNPA**) dynamically while receiving network services, whereas F-ESs do not. Also, M-ESs must support a wireless connection to the CDPD network, and F-ESs generally must support a wired connection to the CDPD network or some connected external network. Because of the need to manage the mobility of M-ESs throughout the CDPD network, the connection between the CDPD network and the M-ES requires two network elements that are unique to the CDPD network: the MDBS and the MD-IS.

4.1.2. Mobile Data Base Station (MDBS)

The **Mobile Data Base Station** (**MDBS**), together with the Mobile Data Intermediate System, connects the traditionally non-mobile protocols of the Internet to mobile CDPD subscriber M-ESs.

The MDBS provides a relay function between the MD-IS and the M-ESs. It is responsible for the detailed control of the airlink interface between the M-ES and the CDPD network, such as managing forward error correction, providing M-ES transmitter power control parameters, and controlling access of several M-ESs to a single radio channel. In some cases, the MDBS may support more than one radio channel to provide CDPD service if there is a large enough demand in the coverage area provided by the MDBS in question. The MDBS usually shares a location (and an antenna) with the base station of a cell site.

The logical medium that connects the MDBS to a set of M-ESs that are receiving on a particular radio channel at any given time, is called a **channel stream** (see section 3.2.9). This channel stream may be thought of as a pair of point to multipoint connections. Each channel stream within a cell is uniquely identified by a **Channel Stream Identifier** (**CSI**) in the messages sent by the MDBS to all M-ESs listening to that channel stream.

CDPD, as a full-duplex protocol, supports communication in two directions simultaneously. In the forward direction, the transmissions are sent from the MDBS to all of the M-ESs listening on that channel. In the reverse direction, the MDBS receives the transmissions from any transmitting M-ES. The MDBS may support one or more channel streams within a sector depending on the data traffic demands placed by the M-ESs within that sector.

In general, the "downstream" components of a CDPD network (the modem/subscriber device, and the MDBS at the cell site antenna) have a much greater involvement in the selection of channels for channel hopping and in network management than their AMPS voice counterparts (the cellular handset and the cell site base station).

4.1.3. Mobile Data Intermediate Station (MD-IS)

The **Mobile Data Intermediate System** (**MD-IS**) controls the mobile data link between the M-ESs and the CDPD network as well as the mobility management aspect of CDPD (see section 5.2.1). The MD-IS is the only element in the CDPD network that has any knowledge of M-ES mobility with the network—the MD-IS insulates the upstream elements of the CDPD network and the rest of the Internet from having to track the location of any M-ES, and it also prevents the MDBSs from needing to know anything about each other. The MD-IS is often in the same location as a cellular carrier's Mobile Telephone Switching Office (MTSO—see section 2.2.4).

4.1.4. Connections to Other Networks – Intermediate Systems (IS)

Since CDPD is an IP-based system, it can connect individual CDPD service provider networks to others, and to any other network connected to the Internet. Hardware and software systems such as routers, firewalls, and others that permit these connections fall under the general term of **Intermediate Systems** (**ISs**). In particular, ISs connected to a CDPD MD-IS permit M-ESs connected through the CDPD airlink to link seamlessly into other networks, potentially anywhere in the world, using any IP-compatible technology.

The network layer functions provided within the CDPD network allow any pair of end systems in the CDPD network to communicate with each other. These functions must determine a path through a series of interconnected elements called **Intermediate Systems** (**ISs**) until the desired destination end system is reached. ISs along the communication path must forward network layer packets (datagrams) between themselves to provide the required end-to-end connectivity. They must deal with route calculation, packet fragmentation, and congestion control within the interconnected ISs. The IS functionality is provided through commercially available **routers** within the service provider network. Their presence is not visible to the CDPD subscriber.

4.2. Services: CDPD Network Services

When a cellular carrier constructs a CDPD network, it provides a number of services to provide security, enable easy connection to the Internet, permit roaming, track usage, maintain accounting information, and prevent unauthorized access.

4.2.1. Domain Name Server

As on the Internet as a whole, the **Domain Name Server** (**DNS**) system translates human-readable host names into numerical IP addresses in the network. A CDPD network requires its own DNS both to simplify Internet access for clients using that system and to allow incoming packets to find their proper destinations.

4.2.2. Subscriber Location Service

Subscriber Location Service tracks the location of a CDPD subscriber and reports the location to the appropriate application. This is not as precise as a global positioning system (GPS) location, but only as specific as the cell sector of the device in question. Nevertheless, this service can be useful, for example, in tracking delivery vehicles for more efficient dispatching.

4.2.3. Mobility Management Service

Mobility Management Service manages network roaming and tracks the location of each CDPD subscriber, as well as keeping the serving MD-IS informed of that location down to the specific cell site. In a traditional data network, the endpoints of the data connections remain in the same physical location, and routing of data between these system endpoints is not a problem. However, in a wireless mobile data network, the endpoints of the data connections can be located anywhere in the network coverage area, and the location of these endpoints can change over time.

Like voice cellular networks, CDPD supports **roaming**. CDPD devices have a **home subdomain** (or, in some cases, more than one—see section 5.1.1), usually the home city of the subscriber. For example, you may live in Las Vegas and your CDPD modem may have been activated with a CDPD carrier there.

You may travel from a subdomain registered as your home area to a new serving area. The CDPD network's Mobility Management Service handles the routing of packets for all visiting M-ESs in its serving area. If you have pre-arranged with your service provider, you can obtain service in another area served by that carrier, or even in an area supported by another service provider—so your CDPD modem can roam outside its home subdomain anywhere that CDPD service is available.

The **home area** is that in which the CDPD subscriber has registered their device with a CDPD service provider. If the subscriber travels to another area, the mobility management services maintain information about their current serving area. If data is destined for that subscriber in their new location, the mobility management services at the home area forward the data to the subscriber in their new location.

Mobility management services in the new serving area regularly notify the subscriber's home-area CDPD network of the subscriber's new location. Therefore, a CDPD subscriber can travel throughout the country and still obtain CDPD network services. The subscriber in the CDPD network appears to have a seamless data connection as they change their location within the network coverage area. The mobility management services that provide this seamless coverage are transparent to the CDPD subscriber. See section 5.2.1 for more detail on mobility management.

4.2.4. Network Management Services

Network Management Services are administrative services for the network provider itself, and do not involve the subscriber. They include:

- Configuration Management of the various components of the CDPD network, which includes collecting data from and sending data to them, as well as controlling them remotely.
- Fault Management to detect, isolate, and correct, abnormal operations in any portion of the CDPD network.
- Performance Management to evaluate and report the behavior and effectiveness of the telecommunications equipment making up the CDPD network.
- Security Management to detect and prevent access to the network and the network management resources by unauthorized subscribers.

4.2.5. Accounting Services

Accounting Services provide information to the CDPD service providers about how the CDPD network resources are being used. They maintain statistics about the **Protocol Data Units** (**PDUs**) sent across the network—packets successfully transferred by users through the network. Accounting Services permit CDPD carriers to know how their systems are being used, and how much to charge their customers.

4.2.6. Authentication Services

Authentication Services verify that subscribers accessing a CDPD network are who they say they are. CDPD modems must be registered on the CDPD network before communication can begin (see section 5.1 for more detail). The registration process involves an exchange of identification, authentication, encryption key, and sleep characteristic information. Modems can be set to register manually (on command) or automatically when they start or reset, but they generally register automatically. Using the Diffie-Hellman Electronic Key Exchange mechanism, credentials maintained by the CDPD subscriber's modem are checked against authentication information maintained in a CDPD Authentication Center. These credentials are updated by the CDPD Network Operations Center on a regular basis to provide additional security.

4.2.7. Encryption Services

Encryption Services encrypt data transferred between the M-ES and the MD-IS—but not any other portion of the network—using RSA RC-4 encryption, and managed by the Subnetwork-Dependent Convergence Protocol (SNDCP), which is discussed in section 5.3. If necessary, the carrier or end user may encrypt data traveling over other portions of the network using other mechanisms.

4.3. Logical: CDPD Protocols

The basic structure of the CDPD network communications is based on the **International Standards Organization** (**ISO**) layered communications reference model. Using this layering technique, communication between application processes can be viewed as being logically partitioned into an ordered set of layers in a stack (known as a protocol stack).

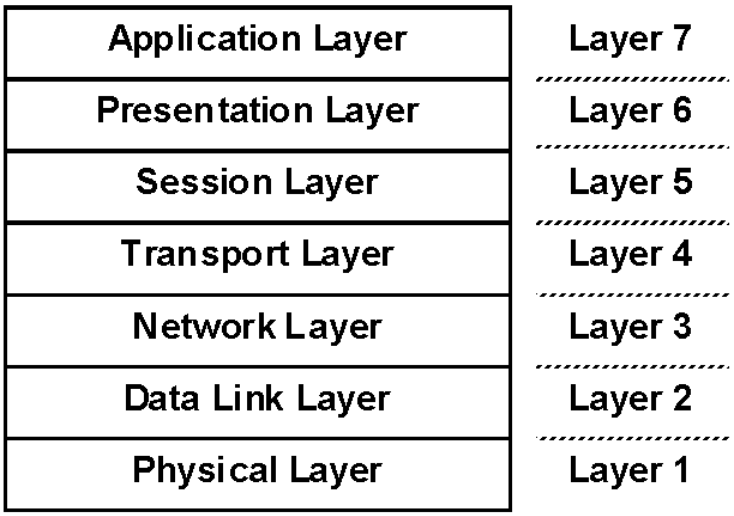

Figure 4-1: ISO layered communications architecture

4.3.1. The Application Layer (Layer 7)

The top layer of the stack includes interaction with the end user. It allows for protocols and services required by a particular user-designed or commercially written application. Particular user requirements and application services that can be used by more than one application are contained in this layer.

4.3.2. The Presentation Layer (Layer 6)

Layer 6 defines the method of representing information for exchange by applications. It is concerned only with the syntax of the transferred data and not with the meaning of the data itself. It provides the representation of:

- Data transferred between applications
- The data structures that the applications use
- Operations on the data structures

4.3.3. The Session Layer (Layer 5)

The session layer allows cooperating application processes to organize and synchronize the conversation between them and to manage the data conversation. During a session, these services are used by applications to regulate dialogue by ensuring an orderly message exchange on the session connection.

4.3.4. The Transport Layer (Layer 4)

This layer provides reliable, transparent transfers of data between cooperating session entities. It optimizes the available network services to provide the performance required by each session. Connection-oriented transport protocols regulate the flow of data, detect and correct errors, and multiplex data end to end.

4.3.5. The Network Layer (Layer 3)

The network layer provides packet routing and relaying between end systems on the same network or on interconnected networks, independent of the transport protocol used. It can also provide service enhancements, flow control, and load leveling.

4.3.6. The Data Link Layer (Layer 2)

The data link layer provides communication between two or more connected systems. It performs frame formatting, error checking, addressing, and other functions to provide accurate data transmission between systems. It also governs access of users to the communication medium, such as the radio channel.

4.3.7. The Physical Layer (Layer 1)

The bottom layer provides a physical connection for the transmission of data between data link layer entities. It performs electrical encoding and decoding of the data (or bits) for transmission over the medium in use (that is, the radio channel).

4.3.8. Where CDPD Fits Into the Protocol Stack

CDPD provides services and protocols to the Network Layer (Layer 3) and below. Protocols in layers 4 through 7 are external to the CDPD network.

The CDPD network is a **multi-protocol connectionless network**, providing network services in any of several different network protocols. CDPD networks support the **Internet Protocol** (**IP**) and ISO's **Connectionless Network Protocol** (**CLNP**). Other network layer protocols may be offered in the future. The only requirement is that both communicating end systems using the CDPD network use the same network layer protocol, since the CDPD network itself does not provide protocol translation.

Connection-oriented services may be provided by end-to-end protocols operating above the network layer (such as TCP/IP). Individual CDPD service providers do not directly provide or operate the Transport Layer or higher services—that is the responsibility of the communicating end systems.

4.3.9. CDPD Communications Subprofiles

The CDPD network specifications define a number of **subprofiles** as building blocks that may be selected and combined to define a particular CDPD network element. These subprofiles define specific multi-layer protocol requirements for a CDPD network element or CDPD network service. CDPD **application subprofiles** specify the Layer 5, 6, and 7 requirements for each application service.

The CDPD network achieves interoperability across all CDPD service providers by requiring the support of **lower layer subprofiles** to assure interoperable data transfer for Layer 4 and Layer 3. These include the mandatory support of lower layer services provided by Transmission Control Protocol (TCP) over Internet Protocol (IP).

The **subnetwork subprofiles** refer to the data link and physical layers, which are within the CDPD network and are therefore transparent to the CDPD subscriber. An example of a virtual terminal subprofile is represented in the following illustration. Some of the technologies used include X.25 and Frame Relay.

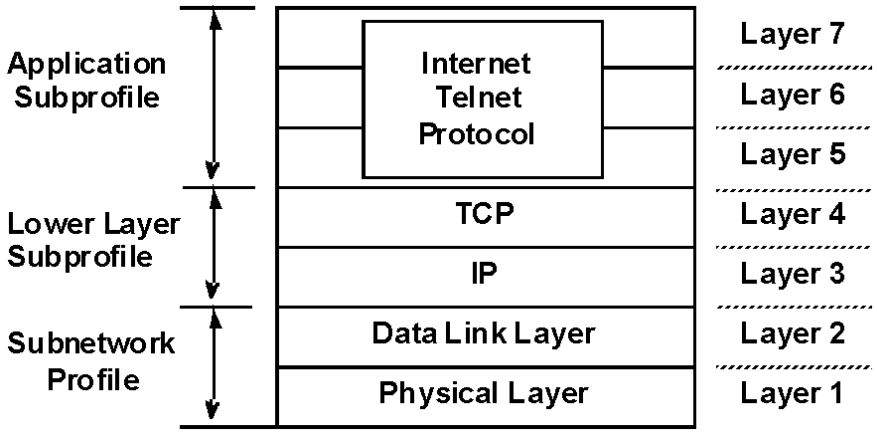

Figure 4-2: Example of a CDPD virtual terminal subprofile

5. Operations: Making a CDPD Connection

Understanding a CDPD network requires more than knowing how it is physically and logically configured. The actual process by which a mobile end system (M-ES), such as a CDPD modem plugged into a notebook, connects to the network and moves data through it is particularly important, and requires the M-ES to have a verified address on the system.

5.1. The Registration Process

After a CDPD subscriber purchases a CDPD modem or other M-ES, they must contact their preferred CDPD service provider and arrange to have it connected to the CDPD network. This process is similar to setting up a cellular phone with a carrier network. Without activation, the CDPD device or cellular handset is useless, because it has no network to connect to. Each time an M-ES is turned on or reset, it acquires a channel and **registers** with the CDPD network, then goes through an authentication and verification process to sign on.

5.1.1. Network Entity Identifier (NEI) and Home Subdomain

Whenever it is connected to a CDPD network, each M-ES is identified by a distinct **Network Entity Identifier** (**NEI**) assigned by the CDPD carrier, which gives a CDPD modem a unique address visible to the rest of the Internet. In fact, the NEI is an Internet Protocol (IP) address of the same form as that used by other machines connected to the Internet. The CDPD network uses the NEI (through its analog, the **Temporary Equipment Identifier**—see section 5.1.2) to send messages to the M-ES via the MD-IS that is serving the M-ES at any particular time.

The NEI is 32 bits long, and like other IP addresses it is generally represented as four 8-bit numbers, separated by periods, with each number being written in a decimal format (such as 64.114.87.11). Without the unique NEI, connecting to the CDPD network and the wider Internet would not work.

Each NEI has a single **home subdomain**—its normal location in the network—that is set by the subscriber's CDPD carrier. However, some CDPD modems may support more than one NEI, each of which has a home subdomain, which may or may not be the same.

For example, one CDPD modem may have three available NEIs, one each for Las Vegas, New York, and Dallas. When in New York, the owner would use the NEI with a New York home subdomain. Alternatively, two NEIs might belong to the same subdomain—perhaps to maintain separate billing for business and personal use of CDPD services. The subscriber can set the NEI from the available choices using software.

If an M-ES moves to a non-home subdomain (a **roaming subdomain**), the CDPD network's mobility management features (see section 5.2.1) handle the routing of packets appropriately, provided that the subscriber has made appropriate roaming arrangements with the home CDPD carrier, and that carrier has a roaming agreement with any new carrier in the roaming area. Neither the NEI nor the behavior of the network connection needs to change, although transmission costs may vary depending on the rate structures of the carriers involved.

5.1.2. Temporary Equipment Identifier (TEI)

Since the airlink portion of the CDPD network is encrypted (see sections 3.2.7 and 5.3), the CDPD network can actually use a masqueraded value of the NEI for improved security. Using the Mobile Data Link Protocol (see section 5.4), the CDPD network actually transmits a value known as the **Temporary Equipment Identifier** (**TEI**), which is a data link layer frame address that corresponds directly to the NEI for a particular M-ES.

5.1.3. Equipment Identifier (EID)

Each M-ES device has an **Equipment Identifier** (**EID**), which, unlike the changeable NEI, is a fixed number completely unique to that M-ES. The EID is a 48-bit number based on the **IEEE Organizationally Unique Identifier** (**OUI**). The EID represents a universal address that is unique to a subscriber unit such as a modem or cellular handset. The first 24-bits of this address are the OUI assigned to each CDPD equipment manufacturer by the IEEE, and the second 24-bits are assigned by the equipment manufacturer when the device is made. It represents a unique electronic serial number for the subscriber device. No two devices in CDPD can have the same EID.

When a user initially signs up for service with a CDPD service provider, they are required to give the EID to the service provider. This EID then becomes part of the CDPD **Subscriber Directory Profile** that the CDPD service provider maintains for each subscriber on that CDPD network.

So, for instance, a subscriber with a CDPD modem already functioning on the network might replace the modem with a newer one. That newer modem will have a different EID that must be reported to the CDPD carrier, which must then assign an NEI to the new unit. Until the new EID is mapped to an NEI, the new modem will not work on the CDPD network.

5.1.4. Authentication and Verification

In order to prevent piracy and "cloning" of CDPD devices, and thus fraudulent network use and billing, the CDPD standard provides sophisticated mechanisms for NEI authentication and verification. It can confirm that only the authorized possessor of the NEI (the modem assigned that NEI by the carrier) is using it.

The authentication process uses three numbers: the NEI, the **Authentication Sequence Number** (**ASN**), and the **Authentication Random Number** (**ARN**), which together form the **credentials** of that M-ES. Although a CDPD subscriber can determine their NEI, they cannot obtain the ASN or ARN. When a subscriber's M-ES performs the authentication procedure during network registration, the CDPD network's serving MD-IS forwards these credentials to the home MD-IS (if they differ), which is holding the current values of the ASN and ARN. If the stored values do not match those provided by the M-ES, the home MD-IS notifies the serving MD-IS of the failure, and the M-ES is not allowed to connect.

From time to time, the home MD-IS generates a new (random) value for the ARN, and it then increments the ASN by one. The home MD-IS delivers the new ARN to the M-ES via the serving MD-IS, as an option in the final step of the encrypted registration process. The M-ES stores this ARN internally and increments its local ASN by one.

Note that although the ARN is synchronized between the M-ES and the MD-IS, they maintain separate versions of the ASN, which are separately incremented by one with each change to the ARN. This process helps prevent other M-ESs from impersonating the real one, since there is no way for another M-ES to know the initial value of the ASN—it is never sent over the airlink or any other part of the network—and if the ARN and ASN do not correspond, authentication fails. In addition, the end user cannot read or alter the ASN or ARN values stored locally in the M-ES.

Once a user has registered an NEI and an M-ES, which establishes an ASN and ARN pair, they cannot simultaneously use that NEI with a different CDPD modem—although the modem, which *is* the M-ES as far as the network is concerned, could be used in a different notebook, for instance. If anyone attempted authentication with a different M-ES, then the ASN and ARN stored at the home MD-IS (which correspond to those stored in the original M-ES) and the ASN and ARN stored in the new M-ES (which would most likely be the initial values set when the unit was manufactured) would disagree. The authentication would fail, and the subscriber would be denied access to the CDPD network. Any subscriber attempting to use another subscriber's NEI on the CDPD network would also be denied access.

Therefore, if a user replaces or changes modems, they must contact their service provider to establish new credentials before they can use the new modem. The carrier can reset the NEI and

update the Subscriber Directory Profile (see section 5.1.3) so that the old NEI can be re-used with the new device.

5.1.5. Service Provider Network Identifier (SPNI)

Just as each M-ES has its unique numbers, including the NEI and EID, each CDPD carrier has a number identifying it to M-ESs connecting to its network equipment. That 16-bit number is known as the **Service Provider Network Identifier** (**SPNI**). This number enables M-ES units communicating over the airlink to identify equipment for their own network (as opposed to those used by another carrier), and also to determine when they are roaming in another carrier's CDPD network space.

Whenever an M-ES connects to an AMPS channel to make a CDPD connection, the SPNI is included in the information sent to that M-ES by the nearest MDBS. CDPD modems can be configured to register only on a network operated by a carrier whose SPNI is on a list set in the modem. If so configured, a modem will not lock onto a channel unless the SPNI matches one in the list. Some Sierra Wireless CDPD products also permit the user to specify an exclusion list of SPNIs to which they should *never* connect.

Businesses that provide CDPD devices for use only on one carrier's network, or in a limited range, can configure their M-ESs this way to simplify usage and billing. Others who want their devices to connect whenever possible, as permitted by the carrier, can configure their M-ESs to connect regardless of the SPNI provided by the network.

5.2. Moving Data Through the CDPD Network

Once registered and connected to a CDPD network, an M-ES can begin communicating. As mentioned in section 3.2.1, a packet-switched protocol can remain connected all day—as long as the M-ES is powered up and within radio range of an MDBS, and has performed the proper registration and authentication procedures. It incurs charges only when data is actually moved over the network. The M-ES may move from sector to sector and cell to cell while maintaining its network connection.

5.2.1. CDPD Mobility Management

As mentioned in section 3.1.6, traditional Internet protocols are not designed to handle nodes that travel, changing how they are connected to the network from moment to moment. CDPD gets around the problem with a system similar to that used by the roaming cellular phones using the same radio infrastructure. For CDPD, the system is known as **mobility management** (see section 4.2.3).

A CDPD modem (or M-ES) has a static IP address (the NEI) so, as far as the Internet is concerned, it sits behind its home MD-IS, which acts like a normal Internet router. However, if an M-ES changes location so that it now connects to a different MD-IS through a different set of MDBSs, its NEI does not change—yet the same IP address cannot logically be connected to a different router. CDPD therefore encapsulates and forwards Internet data packets so that the M-ES appears to the rest of the Internet as though it still resides behind its home MD-IS.

Figure 5-1 and Figure 5-2 illustrate the process for a sample situation. Notebook computers labeled M-ES A and B are the end systems communicating with each other. Notebook A's home is labeled MD-IS (A). Notebook B's home, MD-IS (B) is elsewhere; B is roaming. Both notebooks are currently being served from MD-IS (A) — the home MD-IS for Notebook A, but a roaming MD-IS for Notebook B.

In Figure 5-1, Notebook B sends a transmission to Notebook A. The packet takes these steps:

1. From ME-S (B) to the local MDBS.
2. MDBS to the controlling MD-IS (A) where the destination user is determined to be at home.
3. MD-IS (A) back to the local MDBS.
4. MDBS to ME-S (A); the destination.

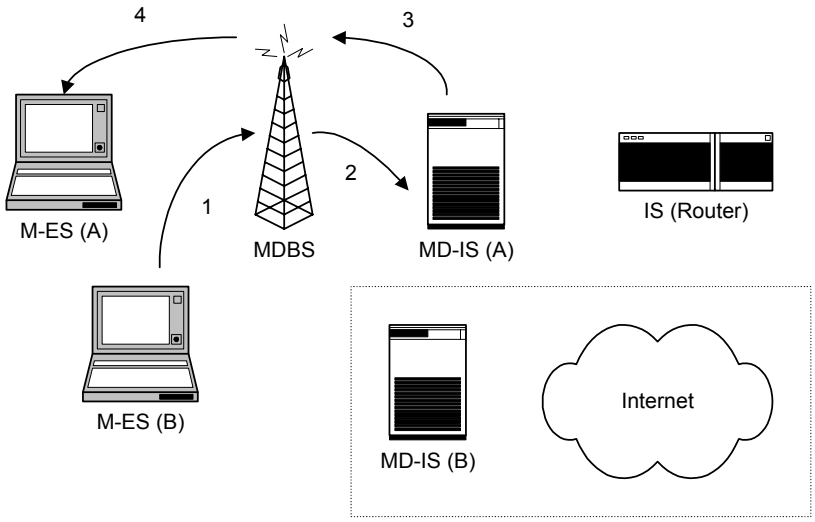

Figure 5-1: CDPD mobility management scenario 1

The packet travels a short path because both the sender and receiver are within the home subnetwork of the destination Notebook A. The path passes over the airlink (1) to MD-IS (A) (2) and directly back out to Notebook A, again over the airlink (3 and 4).

In scenario 2 (Figure 5-2 on the following page), Notebook A sends a reply transmission to Notebook B. In this case, the packet travels through a much longer path because Notebook B is roaming. The steps are:

1. From ME-S (A) to the local MDBS.
2. MDBS to the controlling MD-IS (A) where the destination user (NEI) is determined to be on the Internet.
3. MD-IS (A) routes through the gateway IS.
4. The IS sends the packet to the Internet (and any number of IS routers).
5. The Internet eventually delivers the packet to the home of the destination NEI, MD-IS (B).
6. MD-IS (B) knows that the user is roaming on MD-IS (A) and routes the packet back there using the TEI.
7. MD-IS (A) now knows the true destination (TEI) is on the local MDBS.
8. MDBS to the destination ME-S (B).

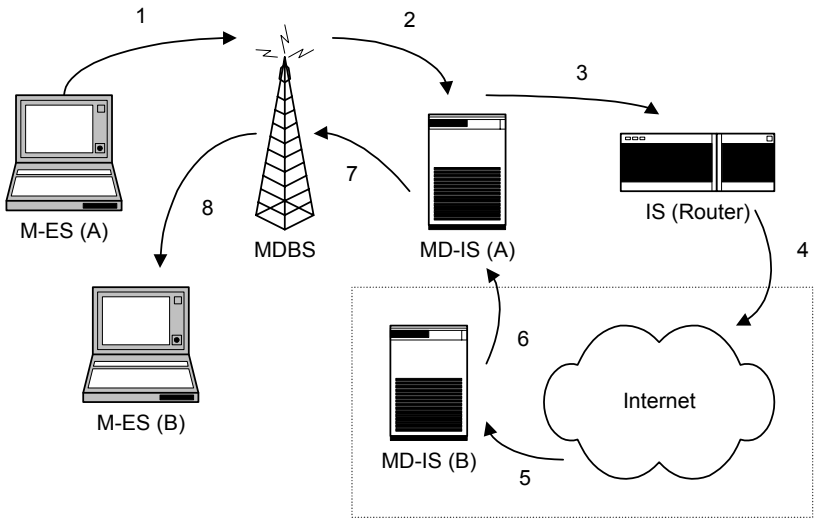

Figure 5-2: CDPD mobility management scenario 2

The difference between scenarios 1 and 2 is transparent to the notebook users, except for the delays introduced by the longer transmission in scenario 2.

If either notebook were communicating with a fixed system on the Internet, the paths would be similar. Traffic destined for Notebook B always has to travel first to MD-IS (B), the home of its NEI, where the traffic is re-directed via the serving MD-IS (A) to the roaming ME-S (B).

5.2.2. Functions of a Modem on a CDPD Network

The CDPD modem performs a number of specific functions. In order to connect, it must:

- Find an available CDPD channel by doing a wide-area scan
- Verify that the channel is usable; that the block error rate (BLER) is acceptable; and that the SPNI of the channel is authorized for use (if configured to check)
- Establish operation of the data link (channel)
- Establish encryption between the modem and the MD-IS
- Register by providing appropriate NEI and authentication credentials
- Choose a channel whenever required from the available list broadcast by the local MDBS:
  - Whenever the received signal strength indication (RSSI) or block error rate (BLER) parameters are exceeded
  - Whenever CDPD synchronization is lost
  - When the scan timer expires
- Detect voice signals and hop channels as appropriate
- If in a "sniff and hop" environment (see 3.1.2), change channels as directed by the MDBS, either as planned channel hops or by being forced off by an impending voice call on the current channel

When transmitting data on the reverse (transmit) channel to the MDBS, it must:

- Accept commands and digital data from the end-user application equipment (for instance, software running on a notebook computer, or a credit-card authorization system in a taxi)
- Encrypt the data
- Assemble the encrypted data into packets
- Add forward error correction (FEC)
- Adjust its transmission power according to received signal strength and parameters set by the CDPD carrier (see section 5.6.2)
- Check for reverse (transmit) channel availability—congestion or busy
- Transmit the encrypted data packets to the CDPD network
- Retransmit packets depending on error correction performance and packet collisions

When receiving data on the forward (receive) channel from the MDBS, it must:

- Receive packet data from the network
- Request retransmission of packets depending on error correction performance
- Decrypt the packets
- Disassemble the packets to extract the application data
- Pass the serial data to the end-user's application equipment

5.3. Subnetwork-Dependent Convergence Protocol (SNDCP)

In a CDPD network, the **Subnetwork Dependent Convergence Protocol** (**SNDCP**) provides compression, encryption, and segmenting for data transferred over the network. It operates between the Internet-standard IP and the next layer, the MDLP (section 5.4), and between the M-ES and its serving MD-IS. In other words, SNDCP takes standard Internet packets, compresses their header information, segments them for transfer over the CDPD network, and encrypts the segments.

5.4. Mobile Data Link Protocol (MDLP)

The **Mobile Data Link Protocol** (**MDLP**) is CDPD's link layer protocol, also operating between the M-ES and the MD-IS. It provides the interface between SNDCP and the MAC layer (see section 5.5), and enables framing, the data link connection, sequence control, and flow control. MDLP controls the throughput of a connection, and divides the segments provided by SNDCP into frames. It also manages CDPD sleep mode (see section 5.7).

MDLP establishes procedures for frame delivery, and detects and recovers from frame loss.

The CDPD network establishes and maintains a number of values using MDLP, including:

- Assigning the Temporary Equipment Identifier (TEI) for each connected M-ES (see section 5.1.2)
- Setting the maximum number of frames that can be transmitted or received in a single block, known as the **window size**
- Defining wait-for-acknowledgement periods and other administrative values
- Measuring information and statistics about the number and various types of data frames transferred

5.5. Medium Access Control (MAC)

The MDBS supports a **Medium Access Control** (**MAC**) mechanism to coordinate the transmissions from many M-ESs on a single radio channel. While one M-ES is transmitting, the MAC mechanism prevents other M-ESs from doing so simultaneously. MAC is the CDPD airlink protocol that provides **Forward Error Correction** (**FEC**) and controls the sharing of the airlink resource between multiple users. MAC helps manage and prevent congestion on the CDPD network.

MAC operates over the last leg of the CDPD connection: the airlink between the MDBS and the M-ES subscriber device. It controls and manages channel access, synchronizes data communications, provides error correction, manages the DSMA-CD collision detection and packet retry process (see sections 3.2.8 and 5.5.2), and divides frames into blocks for transfer over the airlink.

Using MAC, the CDPD carrier establishes a number of parameters, including:

- How many times to attempt retransmissions
- The maximum number of blocks to transmit in a single burst
- Values for the M-ES to use when generating a random back-off time when packet retransmission is necessary

MAC also measures and maintains statistics about:

- The number of frames, blocks, and bursts transmitted, and how many succeeded
- How many frames had to be rescheduled and why

5.5.1. Details of MAC Transmission Access Management

The MAC protocol enables the CDPD carrier to set a limit on how many times an M-ES can attempt to transmit the same data block, to prevent an overflow of stale data that a modem is unable to send. The transmit and receive channels of the CDPD connection are also interlinked using MAC to provide status information and permit many users to share them (see section 3.2.8).

The forward (receive) channel from the MDBS to the M-ES is always keyed with a signal carrier. This constant signal supplies a busy/idle flag that indicates to the M-ES whether the reverse (transmit) channel is ready for data. The busy/idle flag is set at the MDBS to indicate that the reverse channel is either busy or available.

So, when a CDPD modem has data to send through the network:

- The modem checks the busy/idle flag on the forward channel to determine if the reverse channel is idle—available for transmission.
- If the channel is available, the modem begins to send data.
- While sending on the reverse channel, the modem regularly checks the busy/idle and decode status on the forward channel to determine if the transmission is proceeding as expected. In a normal transmission the MDBS will see the incoming data from the modem and set the busy flag on the reverse channel to prevent other devices from attempting to access the channel while it is in use. In a transmission without unrecoverable errors, the MDBS also sets the decode flag as positive to indicate that the blocks arrived intact.
- If the modem senses that the incoming busy/idle flag is busy and that the decode status is positive for the data blocks sent so far, it will continue with its transmission. If either the flag is idle or there is a decode failure, the modem must stop transmission immediately and try again.
- When the last of the chained data blocks has been sent, the modem must wait until the final decode status is received before it can terminate this specific transmission.

If it has more data to send, the modem cannot immediately start on the next set of blocks. The MDBS uses the MAC protocol to specify a minimum waiting period to allow sharing of the channel between multiple devices.

5.5.2. The Exponential Back-Off Process

When the modem is unable to get access to the reverse channel due to a data collision or similar problem, it waits for a randomized period before retrying. The period is determined by a formula based on MAC parameters provided by the MDBS.

The CDPD carrier sets these parameters individually for each MDBS, typically using values recommended in the CDPD specification. After waiting a randomized time based on the formula, the modem must reacquire the channel (which may be busy) before it can try again. If the re-transmission is successful, the back-off counters are reset.

5.6. Radio Resource Management (RRM)

Radio Resource Management (**RRM**) refers to the process of managing CDPD channel acquisition, channel hopping, cell transfer, and signal strength. The RRM process for CDPD enables the limited available spectrum to serve many CDPD users.

5.6.1. The Radio Resource Management Entity (RRME)

The forward and reverse channels of a CDPD data conversation, like AMPS voice channels, are different radio frequencies, widely separated in the assigned spectrum. The M-ES selects these channels according to a list made regularly available by the local MDBS, but the overall selection process is managed by an entity in the CDPD network known as the **Radio Resource Management Entity** (**RRME**).

The RRME manages and provides many pieces of information about the radio frequency in each cell of a CDPD network, such as:

- The carrier's SPNI
- The number of the current cell
- The number of channels allocated to the call
- How many channels are currently in use and their channel numbers
- Data to enable M-ESs and MDBSs to handle handoffs smoothly
- A reference channel to enable M-ESs to evaluate received signal strength (RSSI)
- Information to enable M-ESs to set their transmission power
- The maximum transmission power allowed for M-ESs in the cell
- Channel management diagnostics
- Error control information

As an M-ES moves about the CDPD network coverage area, it may move from one sector to another within a cell, and between different cells in the CDPD network.

If in a new sector where the MDBS is connected to the same MD-IS as the MDBS in the previous sector, and the handoff is called an **Intra-Area Cell Transfer**. In such a transfer, the link between the virtual data connection and the physical radio connection to the M-ES changes. The serving MD-IS updates this link, and the data link resumes from the point of interruption on a new radio channel in the new sector. This procedure occurs very rapidly and is transparent to the user.

When moving to a new cell where the M-ES is served by an MDBS connected to a different MD-IS from the MDBS in the previous cell, the handoff is called an **Inter-Area Cell Transfer**. In this case, a new data link connection is established between the M-ES and the new MD-IS. Once the data link connection is re-established in the new serving area, the M-ES registers with the new MD-IS.

Based on the channel stream information (see section 4.1.2) and the Subscriber Location Service (see section 4.2.2), the M-ES is always aware of its location. When it moves to another cell, it notifies the CDPD network of the change. The network uses this location information, the modem's unique identifier (the TEI), and the CDPD's mobility management features (see section 5.2.1) to ensure that data continues to move smoothly.

5.6.2. Power Level Issues

The CDPD specification for controlling transmission power is complex, but in essence permits any M-ES to transmit at one of eight **power levels**. Devices known as **Class I** can transmit from Level 7 (lowest power, usually 6 mW) to Level 0 (highest power, usually 4000 mW). However, many modems are not capable of transmitting at the two highest power levels, 1 and 0. Such **Class III** devices, like most cellular handsets, have maximum transmission power of Level 2 (600 mW).

Unlike a cellular handset, which has its transmit power controlled by the cellular base station, the M-ES sets its own transmit power by applying a formula defined in the CDPD specification. That formula uses the power product parameters obtained from the MDBS and the current measured received signal strength (RSSI) measured by the modem. Using the algorithm, the modem computes the required transmit power, which is then checked against the maximum power level allowed, a parameter also obtained from the MDBS. If the computed power exceeds the allowable power, the modem lowers the transmit level to allowable limit before it begins transmitting.

In most urban areas, the maximum power level allowed is 2 (600 mW) because of the high density of cells. However, the carrier may set a lower value (a higher level number), believing that CDPD traffic can cause noise problems on the voice channels. There is little evidence that this actually happens, but voice-conscious carriers may arbitrarily set the maximum to a level from 3 to 5. This may cause serious problems for CDPD operation.

For voice systems, any adjustments made to the cell transmit power or receiver sensitivity, to improve voice system operation, are automatically compensated for by the cell site base station algorithms that control the voice system power level. This is not true for the CDPD system: the modem is responsible for determining its own transmit power level by using the parameters provided by the serving MDBS.

A site may have been set up properly for voice and CDPD, but over time adjustments made for voice issues may have caused the CDPD configuration to fall out of balance. This can happen if the cell site transmitter (forward channel) power or receiver (reverse channel) sensitivity have been adjusted without making compensating changes to the appropriate CDPD parameters. End users may need to contact their carrier if CDPD service is unreliable because the M-ESs are not being permitted to transmit at sufficient power for their local conditions.

5.7. Sleep Mode

CDPD provides a facility to allow modems to go into **sleep mode** when they do not have active traffic with the network, allowing the M-ES to shut down hardware to reduce power consumption.

When the modem is waiting for data from either the host or the network, it does not need to keep all hardware systems running. The modem can negotiate with the CDPD network during the registration process to have the network send a periodic message advising if there is pending traffic. Between these messages, the modem can be programmed to shut down the radio (go to sleep). The modem will wake up at the predetermined intervals to check the network for incoming traffic. If there is no pending traffic, then the device can go back to sleep until the next scheduled notification message.

Sleep mode is managed using the Mobile Data Link Protocol (MDLP, see section 5.4). During the registration process (see section 5.1), the CDPD network advises the modem of the time interval between periodic notification messages. This is typically 60 to 90 seconds, set by the carrier.

The CDPD modem goes to sleep after a specified period of inactivity, the modem wakes up after every interval to listen to the list of TEIs (see section 5.1.2) broadcast by the MD-IS. If one of the broadcast TEIs corresponds to the NEI for the sleeping device, it goes back online to make the connection. Otherwise, it returns to sleep for another interval.

The disadvantage to sleep mode is that traffic from the network will have to wait up to a full interval before the modem can receive it. This delay in responding can be too great for some time-critical applications.

Most CDPD networks support sleep mode, and many M-ES devices can go to sleep. Those that do, also let the end user disable sleep mode to keep the data connection as fast as possible, especially when the modem is plugged into a wall socket or other power source that does not require conservation of battery power.

6. Sierra Wireless Products and CDPD

Sierra Wireless produces a number of devices and applications that work with CDPD, as well as other wireless data technologies. For more information about any of the following items, visit the Sierra Wireless Web site at www.sierrawireless.com.

6.1. CDPD-Only and Multi-Mode Devices

An industry leader in wireless data connectivity, Sierra Wireless makes a wide range of devices that support both CDPD and other technologies, including circuit-switched data communications (CSC), wireline data connections, the Global Positioning System (GPS), telemetry, and legacy protocols.

Other Sierra Wireless devices support only CDPD; for those for whom the single standard is sufficient.

6.2. AirCard® PC Cards for Handhelds and Notebooks

Sierra Wireless AirCard 300 PC Card modems plug directly into industry-standard PC Card slots in notebook and handheld computers. They allow easy wireless access to the Internet for any supported portable computer in areas with CDPD coverage.

The **AirCard 300** is a CDPD-only modem, available as two models: one that supports **handheld computers** (such as Pocket PC devices with PC Card slots), and another that supports both **handhelds and notebooks**.

The **AirCard 350** extends the technology of the 300 with a more rugged antenna and support for the **AirBooster 350** 3-watt RF amplifier, for areas with poor coverage (the two together are known as the **AirCombo 350**). This modem is primarily intended for public safety and field service.

6.3. Wireless Telemetry Systems

The **Dart 300**, successor to the popular Dart 200, allows remote locations such as energy distribution sites, water and waste water plants, material storage and distribution areas, traffic signals, time clocks, and other fixed data systems to relay data through the CDPD network, and thus not have to be connected to landline wires.

6.4. Mobile In-Vehicle Dispatch/Database Access

The **MP200** series modems provide wireless access via CDPD, and also have an option for GPS telemetry. They have high-power transmitters, and are very rugged modems for the harshest environments.

Used by public safety and field service personnel, the MP200 series has also provided data for real-time graphical displays of the positions of boats in the 2000 Americas Cup yacht race.

The **MP210** is a multi-mode device, adding circuit-switched cellular (CSC) data capabilities to their CDPD support.

6.5. Original Equipment Manufacturer (OEM) CDPD Devices

The **SB300** Type III-size CDPD modem is a cost-effective wireless data modem that can be integrated into original equipment manufacturer (OEM) devices. The more fully-featured **SB320** also offers circuit-switched cellular (CSC) support and wireline connections for data and voice.

6.6. End-to-End and Legacy Systems

The Sierra Wireless **AirPac** system provides wireless connectivity and protocol conversion for transaction-based applications based around legacy systems. These include Automated Teller Machines (ATMs), Point-of-Sale (POS) devices, remote terminals for travel reservations, and lottery ticket dispensers. Such systems often run on legacy protocols, such as SDLC and X.25, for which AirPac provides data conversion to operate over the CDPD network.

6.7. Software

Sierra Wireless also creates software to support its hardware. That software includes:

- **Watcher**, which is a graphical, menu-driven application for operating and configuring Sierra Wireless modems.
- **WirelessExpert**, a wizard-driven setup utility that makes installing Watcher and configuring Sierra Wireless modems even simpler.
- **PortWatcher**, a tool to configure, monitor, and control the general-purpose I/O ports of the MP200 series of CDPD modems.
- **SkyWatcher II**, software to configure and monitor the GPS module installed in some Sierra Wireless products.
- **Toolkit**, a graphical, menu-driven application for configuring Sierra Wireless modems.
- **CDPD Software Development Kit (SDK)**, an aid to developing applications that use Sierra Wireless CDPD products. For more information visit www.sierrawireless.com/developers/

7. Additional Resources

7.1. Books

Cellular Digital Packet Data System Specification
Release 1.1, January 19, 1995
CDPD Forum Inc./Wireless Data Forum

Computer Networks
Andrew S. Tannenbaum
Prentice Hall Inc., 1981
ISBN 0-13-165183-8

Data and Computer Communications
William Stallings
MacMillan Publishing Inc., 1988
ISBN 0-02-415451-2

The Race for Bandwidth: Understanding Data Transmission
Cary Lu
Microsoft Press, 1998
ISBN 1-57231-513-X

Open Systems Interconnections: Computer Communication Standards and Gossip Explained
Gary Dickson and Alan Lloyd
Prentice Hall, 1992
ISBN 0-13-640111-2

Internetwork Mobility - The CDPD Approach
Mark S. Taylor, William Waung, Mohsen Banan
Prentice Hall PTR, 1997
ISBN 0-13-209693-5

7.2. Web Sites

Wireless Data Forum (originally the CDPD Forum).
www.wirelessdata.org

CDPD Specification online.
www.wirelessdata.org/develop/cdpdspec

WAP Forum—an organization working towards integrating IP access into wireless services.
www.wapforum.org

Weekly CDPD news: see the Wireless Alliance's News Access section.
http://www.wirelessready.org/news.asp

7.2.1. CDPD Coverage and Carriers

Wireless Data Forum's CDPD Coverage Maps.
www.wirelessdata.org/maps

CDPD details for major U.S. cellular carriers:

- AT&T Wireless Services – Wireless IP
  www.attws.com/general/explore/wireless_ip/downloads/wip_mail_whitepaper.pdf
- Cingular Wireless
  www.cingular.com/cingular/products_services/wireless_data
- Verizon Wireless – AirBridge.
  http://www.bam.com/wireless

Some key CDPD carriers in international markets:

- Canada:
  - Telus Mobility. www.telusmobility.com
  - SaskTel Mobility. www.sasktelmobility.com
- Venezuela: Movilnet. www.movilnet.com.ve
- Colombia: Comcel. www.comcel.com.co
- New Zealand: Telecom. www.telecom.co.nz
- Israel: Cellcom. www.cellcom.co.il

7.2.2. Related Technologies

Mobitex/RAM packet data service.
www.ericsson.se/wireless/products/mobsys/mobitex/mobitex.shtml

ARDIS (Advanced Radio Data Information Services) packet-switched system from Motient.
www.motient.com

GPRS (General Packet Radio Services), GSM data specification to deploy in 2001.
www.wirelessready.org/nettech_gsm.asp

7.3. Additional Sierra Wireless Documents

A number of technical documents are available for download from the Sierra Wireless Web site at www.sierrawireless.com. A Glossary of Terms and Acronyms (#2110032) is available from www.sierrawireless.com/pub/doc/2110032.pdf

SIERRA WIRELESS
HEART OF THE WIRELESS MACHINE™