CDMA2000 SYSTEM

Introduction

The nets CDMA2000 are compatible with the nets cdmaOne, that which protects the investments of the operators cdmaOne and it provides a simple and economic migration to the following generation. Also, the nets CDMA2000 offers improvements in the voice quality and support for data multimedia services.

Standardization

CDMA2000 was approved as terrestrial standard of IMT-2000, CDMA2000 1X and CDMA2000 1xEV (including 1xEVDO and 1xEV-DV) constitute part of that the UIT IMT-2000 has denominated CDMA Multi-Carrier (MC).

CDMA2000 is commercially for more than three years, the first technology of third generation that made reality IMT-2000 was. The first system 3G in the world starts in Korea at the end of the 2000.

Today, 97 millions of subscribers access to CDMA2000 nets in Asia, Europe and America. Other 35 CDMA2000 nets will be deployed in the whole world in a future not very distant.

Evolution de Cdma2000

CDMA2000:

- Common denomination for IMT-2000 CDMA Multi-Carrier.

CDMA2000 1X (October 2000)**:**

- 3G Technology that it duplicates the voice capacity.

- It provides data transmission speeds up to 307 kbps in a single carrier (1.25 MHz, or 1X).

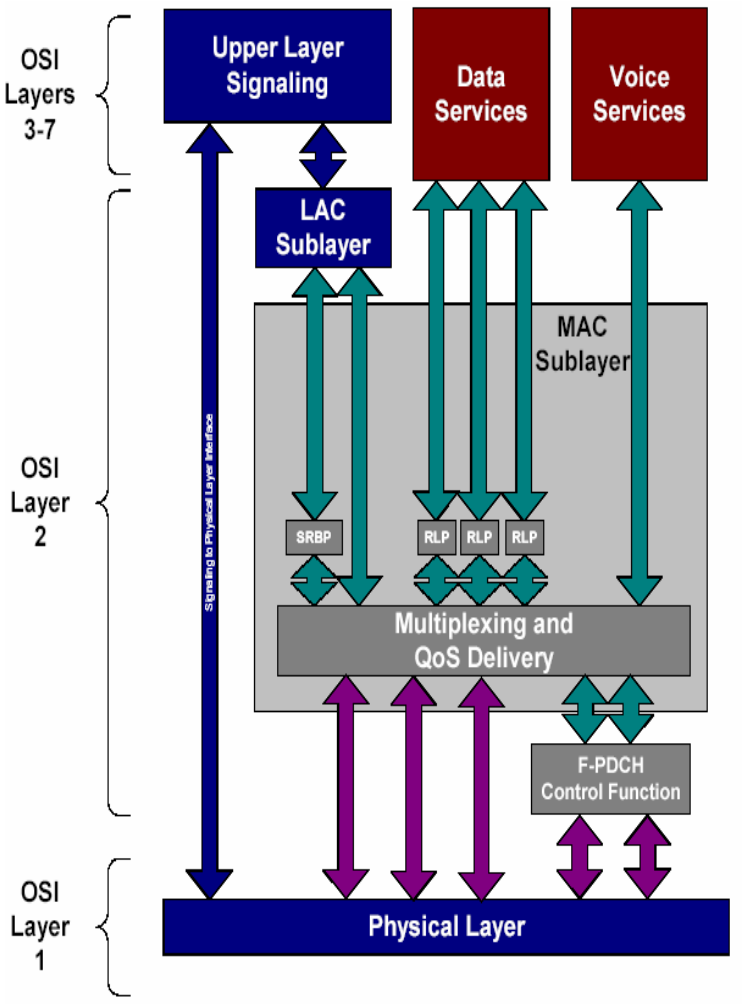
CDMA2000 1xEV :

- Evolution of CDMA2000 1X that it offers bigger data transmission speed can offer up to 2.4 Mbps in a single carrier the same as the previous one (1.25 Mhz).

CDMA2000 1xEV-DO (firsts of 2002)**:**

- 3G Technology that only uses a carrier of 1.25MHz for data.

- It reaches transmission speeds of up to 2.4 Mbps.



Architecture

Figure 3.8: Architecture Diagram CDMA 2000

[Source: Text book- Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

Logical channels Carry data over the air and are mapped directly to the physical channels(logical channels)

- Dedicated Traffic Channel (f/r-dtch): A point to point logical channel that carries data or voice traffic over a dedicated physical channel.
- Common Control channels (f/r-cmch control) : These are used to carry MAC messages with shared access for several terminals.

- Dedicated signalling Cannel (f/r-dsch): A point to point logical channel that carries upper layer signalling traffic over a dedicated physical channel, for a single terminal.
- Common Signalling Channel (f/r-csch): A point to multipoint logicalchannel that carries upper layer signalling traffic over a common physical channel, with shared access for several terminals.

Multi-Carrier Mode

Uplink Spreading and modulation

The uplink spreading is done with Walsh functions. The uplink code used for scrambling a period of 2^{42} -1 chips. And the access channels have a specific scrambling code with a period of 2^{15} chips.

Downlink Spreading and modulation

Multi carrier nature is the characterised of downlink, the downlink carries can be operated independently or in the same time. As each carries havea pilot channel, they can be sent from different antennas to allow additional diversity.

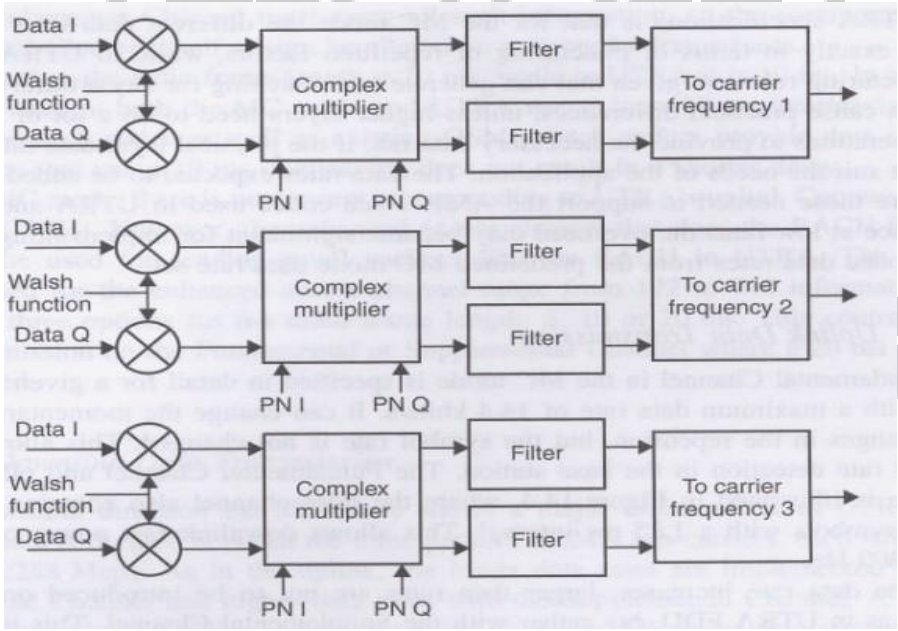


Figure 3.9: Multi-Carrier Mode

[Source: Text book- Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

The channel on each carrier is spread with Walsh functions using a constant spreading factor during the connection, it separate channels from the same source. The spreading factors for data transmission range from 256 down to 4.Downlink modulation consisting of three carriers. Downlink scrambling is characterised by the use of a single code. MC mode is a synchronised base station, a single code is used and the different base station uses the same code with different phase (512 different phases).

The single carrier bandwidth discussed has often been 1.25 MHz, the bandwidth that has been defined for a single carrier spectrum mask with 40 dB attenuation for the power level is 1,48 MHz for the base station transmission.

User Data transmission

Uplink Data Transmission

In MC mode the fundamental channel is specific to obtain a maximum data rate(14,4 bits/s),it can change but the symbol rate is not changed. The pilot symbols and the power control symbols have a interval like 1,25 ms, it allows in the downlink fast power control (rate 800Hz). The user data he radio frame length is 20 ms.

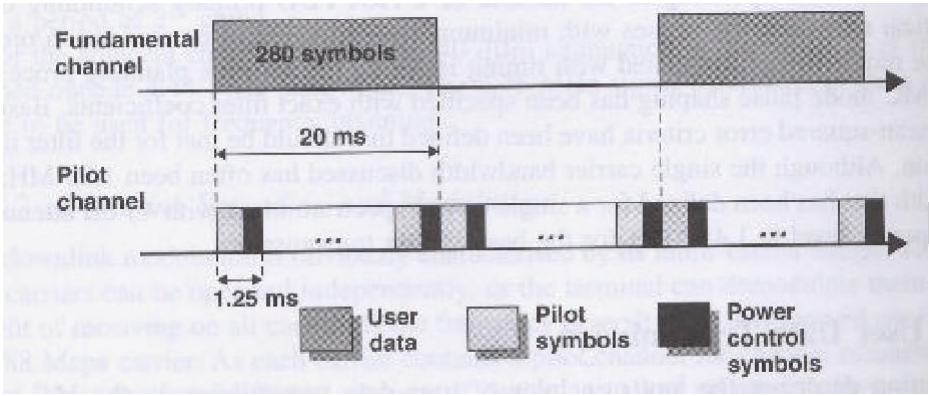


Figure 3.10: Uplink Data Transmission frame length is 20 ms

[Source: Text book- Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

Downlink Data Transmission

In the downlink direction the MC mode divided the user data in three parallel CDMA sub- carries, each with a rate of 1.2288 Mcps

The symbol rate for the traffic channels after channels coding and interval is multiplied by a factor of three.

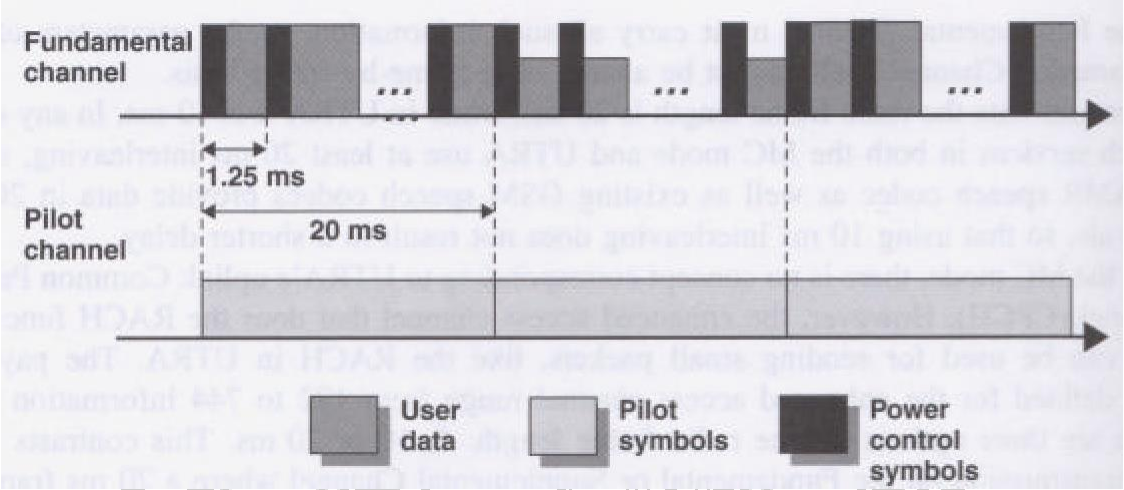


Figure 3.11: Downlink Data Transmission frame length is 20 ms

[Source: Text book- Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

Signalling

Pilot Channel:

The MC mode has a separate common pilot channel for each carrier.

Synch Channel:

It helps the terminal to acquire initial timing synchronization.

Broadcast Channel:

Typical information sent on the Broadcast channel is the availability of access channels or enhanced access channels for random access purposes.

Quick paging channel:

It indicates to mobile stations whether are accepted to receive the paging information or information in the Forward common control channel.

Common Power Control Channel:

It provides the power control information.

Common and dedicated control channels:

It is designed to carry higher layer control information for one or more terminals.

Random Access Channel:

RACH is the transport channel for the uplink, all the cell received this channel but is probably the collision. It carries control information from the terminal (suchas request to set up a connection.

Physical Layer

Power Control

The power control is the same that in WCDMA but it have open and fast close loops with 800Hz rate.

Spectrum

CDMA2000 is designed to operate in all the spectrum bands attributed for the wireless telecommunications services, including the analogical, cellular bands, PCS and those of IMT - 2000.

CDMA2000 facilitates the benefit of services 3G making use of a very small quantity of spectrum (1.25 MHz for carrier), protecting this way this resource important for the operators.

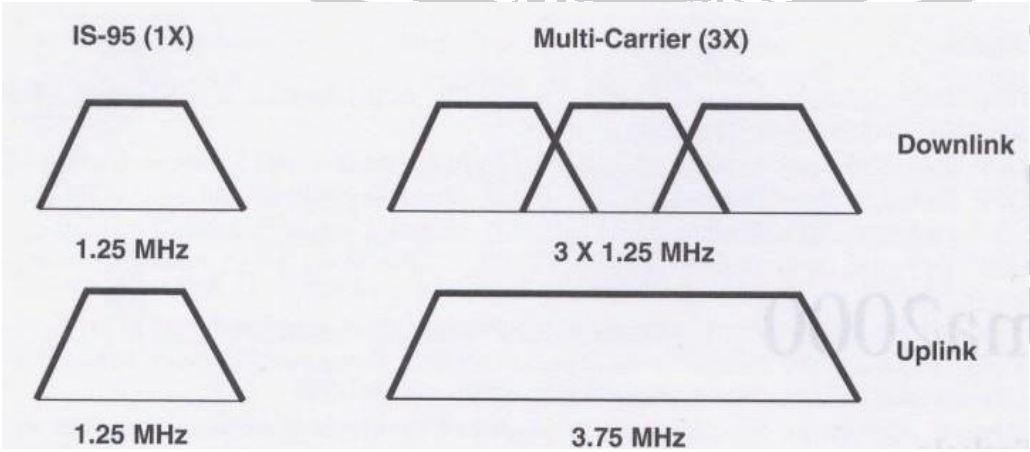


Figure 3.12: CDMA 2000 Spectrum

[Source: Text book- Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

Terminals

More than 578 terminals CDMA2000 1X and of 68 terminal CDMA2000 1xEV-DO are at the moment available, by manufacturing leaders like Audiovox, Axesstel, Ericsson, CURITEL, Handspring, Huawei, Kyocera, LG, Motorola, Nokia, Research in Motion, Samsung, Sanyo, SK TeleTech, Telular and ZTE.

Next to the telephones, they have also been thrown to the market wireless modems by AnyDATA, Sierra Wireless and others. There are plans of introducing, in a future next, many devices CDMA2000.

CDMA2000 Packet Data

In this section we describe the core packet data architecture associated with the CDMA2000 radio interface. This architecture is described in 3GPP2 recommendations and TIA standards such as [IS835] and [TS115]. It allows CDMA2000 cellular wireless service providers to offer bidirectional packet data services using the Internet Protocol. To provide this functionality, CDMA2000 utilizes two access methods: Simple IP and Mobile IP.

In *Simple IP*, the service provider must assign the user a dynamic IP address. This address stays constant while the user maintains connection with the same IP network within a wireless carrier's domain—that is, until the user does not exit the coverage area of the same Packet Data Serving Node (PDSN). Anew IP address must, however, be obtained when the user moves into a geographical area attached to a different IP network—that is, into the coverage area of another PDSN. Simple IP service does not include any tunneling scheme providing mobility on a network layer described in the beginning of this chapter and supports mobility only within certain geographical boundaries.

Note One of the significant advantages of Simple IP lies in the fact that unlike Mobile IP it does not require special software of any kind to be installed in the mobile station. All the MS needs is the CDMA2000 terminal capabilities and a standard PPP stack similar to that used to establish wireline dial-up session, usually bundled

with most modern operating systems such as PocketPC2002 and Windows XP.

The *Mobile IP* access method is mostly based on [RFC2002] now superseded by [RFC3220], described in Chapter 2. The mobile station is first attached to serving PDSN, supporting FA functionality, and assigned an IP address by its Home Agent (HA). Mobile IP enables a mobile station to maintain its IP address for the duration of a session while moving through CDMA2000 or other systems supporting Mobile IP.

For mobile stations compatible with a TIA/EIA [IS-2000] standard attached to a CDMA2000-1x network, available data rate can vary between the fundamental rate of 9.6 Kbps and any of the following burst rates: [3]

- 19.2 Kbps
- 38.4 Kbps
- 76.8 Kbps
- 153.6 Kbps

These higher-speed bursts are allocated by the infrastructure based on user need (data backlog in either direction), and resource availability (both airlink bandwidth and infrastructure elements). Bursts are typically allocated to a given mobile for a short duration of time of 1 to 2 seconds. The resource and mobile situation is then reevaluated.

CDMA2000 Packet Data Architecture

The architecture of CDMA2000 data system is based on the following components (as shown in Figure 4.3):

- A mobile station in a form of a handset, PDA, or PCMCIA card in handheld/portable computer supporting Simple IP or Mobile IP client or both
- CDMA2000-1x Radio Access Network (RAN)
- Packet Control Function (PCF)
- Packet Data Serving Node (PDSN) supporting FA functionality in case of Mobile IP

- Home and foreign AAA servers
- Home Agent (for the Mobile IP access method)

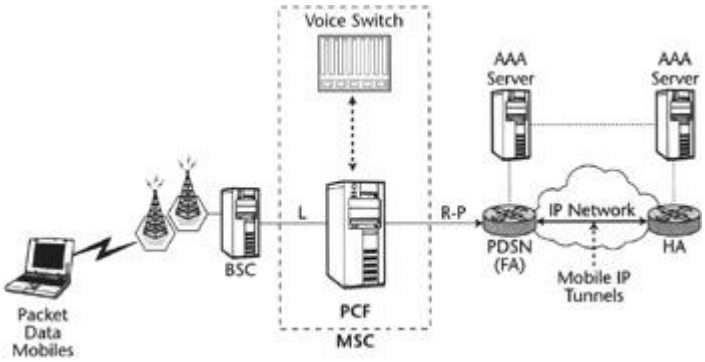


Figure 3.13: Example of CDMA2000 packet data architecture.

[Source: Text book- Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

When the mobile station connects to the CDMA2000 base station, it first establishes a connection to a PDSN. In the case of Mobile IP, the mobile station is then connected to its serving HA by a tunnel between PDSN/FA and the HA established using Mobile IP. The IP address of the mobile station is assigned from the address space of its *Home* network, either statically provisioned or dynamically allocated by the HA at the beginning of the session. On a high-level Mobile IP authentication and authorization is normally performed by both the PDSN and HA by querying the AAA infrastructure (more on this in Chapter 7). In the case of Simple IP, the address must be assigned to mobile station by the PDSN and cannot be statically provisioned in the MS. The authentication for this access method is based only on PDSN.

The connection between the mobile station and its serving PDSN requires a second layer of connectivity to be established for successful IP communication. This connectivity is provided by Point-to-Point Protocol (PPP) as defined by [RFC1661] and supporting IPCP, LCP, PAP, and Challenge Handshake Authentication Protocol (CHAP). [4] PPP is initiated by the mobile station during connection negotiation and is terminated by the PDSN. Between the CDMA2000 radio network and PDSN, PPP traffic is encapsulated into the Radio-Packet (R-P) interface. CDMA2000 protocol stack examples for both the Simple IP and Mobile IP cases are shown in Figure.

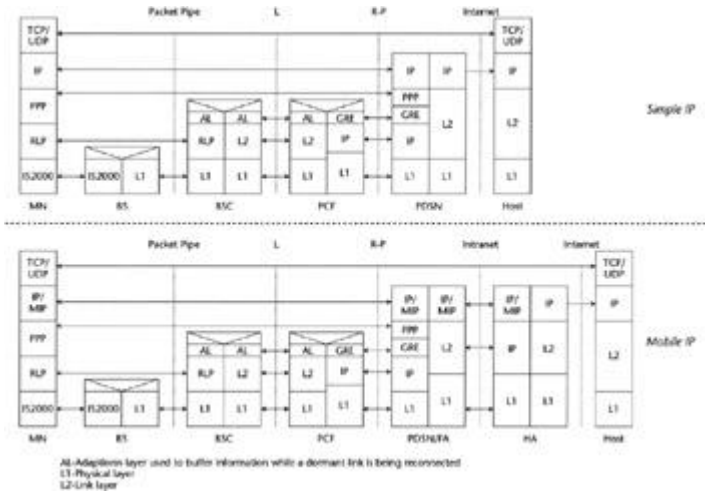


Figure 3.14: Examples of CDMA2000 data service protocol stacks.

[Source: Text book- Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

The PCF shown in this figure is the element of the CDMA2000 Radio Access Network responsible for R-P interface setup and processing. It is often implemented as a component of CDMA2000 MSC. One exception is CDMA2000-1xEV DO architecture, which does not rely on MSC. The PCF can be implemented there as a part of 1xEV Radio Network Controller (RNC—or BSC depending on the vendor). Stand-alone PCF implementation is also possible. Once link layer connections are established, the PCF simply relays PPP frames between the mobile device and the PDSN. Another important function of PCF is providing micro-mobility support, which is accomplished by allowing the MS to change the PCF while keeping the mobile anchored on the same PDSN and buffering the user data while a dormant radio link is being re-connected. The significance of the latter feature is explained later in the chapter.

The major role of *PDSN* in CDMA2000 architecture is to terminate PPP sessions originated from the mobile station and provide FA functionality, in case Mobile IP service is requested, or to deliver IP packets to the appropriate next hop when Simple IP is used. The PDSN is also charged with authenticating the users and authorizing them for requested services. Finally the PDSN is responsible for establishing, maintaining, and terminating the PPP-based link layer connection to the mobile station. Optionally, PDSN must support secure reverse tunneling to the Home Agent.

For basic Internet service using the Simple IP access method, the PDSN assigns a dynamic IP address to the mobile, terminates the user's PPP link, and forwards packets directly toward the Internet via the default gateway router on the service provider backbone IP network. The normal PPP timers are enforced, and the packets from the mobile may be checked to ensure the mobile is using the source IP address assigned by the PDSN. (Among other filtering rules and policies, the PDSN may implement in Simple IP mode.)

For Mobile IP access methods, the PDSN establishes the Mobile IP protocol connectivity to the mobile station's home network represented by the HA, which is responsible for IP address assignment. The PDSN must support an AAA client functionality to aid in partial authentication of the mobile by local AAA server. Per [IS835], the PDSN is also required to support Van Jacobson TCP/IP header compression and three PPP compression algorithms: Stac LZS [RFC1974], MPPC [RFC2118], and Deflate [RFC2394]—the latter mostly used by Linux- and UNIX-based mobile stations.

The R-P interface connecting PCF and PDSN—also defined by TIA/EIA as A10/A11—is an open interface based on the GRE Tunneling Protocol and is used to connect radio network and PDSN. The R-P interface protocol is actually similar to the Mobile IP where the PCF acts as the FA and the PDSN acts as the HA (the R-P interface uses GRE tunnels for the traffic plane and Mobile IP-like RRQ/RRP messages for signaling). There are a few reasons for the introduction of R-P interface or in other words "splitting" PCF and PDSN functionalities. By supporting the R-P interface, IP-based mobile devices can cross MSC boundaries without impacting the continuity of user sessions. In other words, if the user moves to another MSC coverage area, the user session is not disconnected and the user is not forced to reconnect via the new MSC and obtain a new IP address. This is accomplished by performing PCF *transfers* while keeping mobile devices anchored to the same PDSN. This does, however, require that all serving PCFs have network connections to the same pool of PDSNs. Another purpose of splitting PDSN from PCF is to allow service providers to select PDSNs from third-party vendors, other than those proving the bulk of their infrastructure including MSCs and PCFs. R-P therefore enables wireless carriers to introduce multivendor PDSN solutions into their network. Not

surprisingly, the carrier community was the most vocal during the R-P standardization process.

Mobile Station Perspective

The CDMA2000 mobile station can authenticate with the service provider's HLR for wireless access and authenticate with the PDSN and HA, using the Simple IP or Mobile IP access methods, for data network access. The mobile stations are required to support a standard PPP networking protocol and be capable of supporting CHAP-based authentication during PPP authentication phase for Simple IP service. For Mobile IP service, the mobile device must also support the Mobile IP client as described by the [IS-835]. In this mode, the mobile station communicates with its Home Agent via serving PDSN in the visited network. If the mobile supports one or more of the optional PPP compression algorithm options such as MPPC or Stac LZS, then PPP compression during the connection phase with the PDSN can be negotiated, thus optimizing radio network resources usage and enhancing the user experience via a higher effective data rate.

Dormancy

The mobile device is expected to support airlink "dormancy" (as defined by TIA [IS-707A1]), which allows either the mobile or the MSC to time out the active airlink connection after a period of inactivity and to release the air interface and serving base station resources. If either the mobile station or the associated PCF have packets to send while dormant, the connection is reactivated and the transmission continues. Dormant mobile stations are defined as stations that do not have an active link layer connection to the serving PCF. All mobile stations—active and dormant—registered using Mobile IP access method have an entry in the PDSN visitor list and a binding with the corresponding HA.

The PDSN serving the users on the foreign network serves as the default router for all registered mobile users, active and dormant, and maintains host routes to them. For Mobile IP mode the PDSN/FA keeps track of the time remaining of the *registration lifetime* for each mobile station in its routing tables and the MS is responsible for renewing its lifetime with the HA. If the mobile does not re-register before the expiry of

the registration lifetime, the PDSN will close the link with the PCF for this mobile and terminate the mobile's session (and the HA will do likewise if the mobile has not re-registered via some other PDSN). Once the mobile station's registration lifetime has expired, the PDSN/FA will stop routing packets to it. To receive and send packets, dormant stations must therefore transition to the active state. Given that any registered mobile stations at any moment can be in active or dormant sub-states, the PDSN generally does not require an indication of the state of PPP links to mobile stations except for the current dormancy timer value for that particular link. Traffic may arrive on the dormant link at any time, forcing the associated mobile station to transition to active state. For active, traffic-carrying PPP links, the PDSN terminates the PPP session with the mobile station and relays the encapsulated IP traffic to the mobile from the HA or from the mobile to the HA via reverse tunneling. A separate tunnel exists for each unique HA for all registered users.

Mobile Station Types

There are two basic types of mobile station configurations—relay model and network model. In *relay model* mobile stations, the CDMA2000 Mobile Terminal is connected to another portable data terminal device such as a laptop, handheld computing device, or some other embedded data terminal. The relay model phone does not terminate any of the protocol layers except for the CDMA2000 physical layer (radio interface) and RLP layers. The attached data terminal device must terminate all other higher-layer protocols (PPP, IP, TCP/UDP, etc.).

Network model mobile stations, in addition to the radio interface, terminate all necessary protocols and do not require any additional data terminal devices. The mobile phone itself provides all user input and display capabilities—as well as a user applications—to make use of the packet data network. Examples of this kind of phone include the "smart phone" or "micro-browser" phone. These devices normally include some embedded Web browsing or information service application, as well as a display screen for viewing the information retrieved from the Internet server. Such kind of terminals may also offer the ability to connect a laptop to a data network via a PPP connection terminated at the terminal itself.

CDMA2000 Mobility Levels

CDMA2000 packet data architecture defines as many as three levels of mobility for the mobile station, as depicted in Figure 4.5. One level is represented at the physical layer by BTS-to-BTS soft or semisoft handoff, while the mobile station is anchored at the same PCF. This is accomplished by the CDMA2000 radio access and is invisible to both PCF and PDSN.

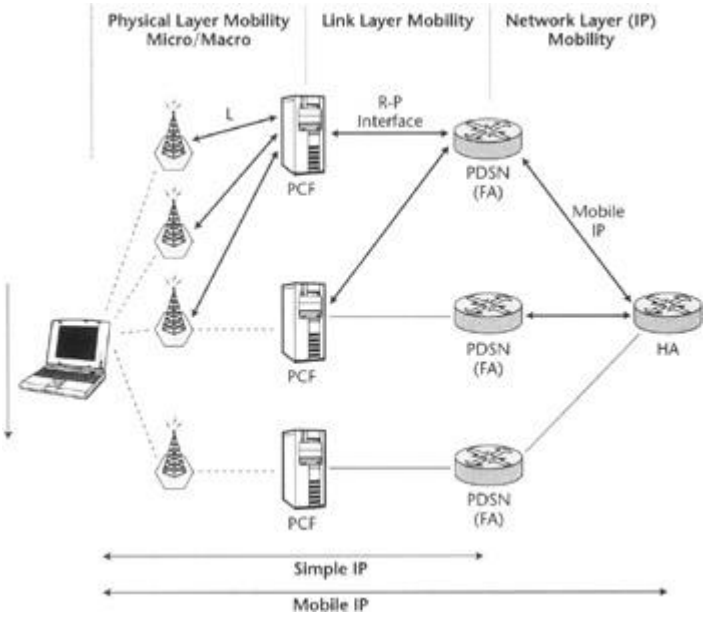


Figure 3.15: CDMA2000 mobility hierarchy.

[Source: Text book- Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

The second mobility level is represented by the R-P interface on the link layer, which allows for a transparent handoff from PCF to PCF while keeping the session at the same PDSN. In this case, two options described previously come into play: dormant and active. In active state, when the user crosses PCF boundary, the handoff is transparent for the mobile station. The MS participates in a semisoft handoff to the new BSC (or MSC, depending on the vendor), while the link layer data session remains anchored to the original PCF for the duration of the call and the mobile is in the active state.

When a mobile crosses a PCF coverage boundary while dormant, the mobile will trigger reactivation at a new BSC (MSC) to establish a new PCF connection. That results in a PCF but not necessarily a PDSN change if both the current and previous PCFs were

attached to the same PDSN. The new PCF attempts to assign the mobile to its current serving PDSN. If the new PCF has connectivity to that PDSN, the PPP session previously established between the mobile station and the PDSN will be totally unaffected.

The third level of mobility, the network layer, is the inter-PDSN handoff, based on the use of Mobile IP protocol. Let's assume that the mobile station has registered with the HA and PDSN (the MS has been authenticated by each of them) to establish the Mobile IP tunnel over which traffic is delivered. Whenever the mobile roams to a location that is served by a PCF connected to a different PDSN, the mobile receives an indication that it must reregister with this new PDSN. This reregistration updates the mobility binding tables at the HA, so that all subsequent traffic is routed to the new PDSN for this mobile. In this case the mobile's PPP link is impacted by this change while the IP layer stays intact, and the mobility remains invisible to the mobile station's correspondents.

Note that the last type of handoff is not available in Simple IP mode; Simple IP provides only partial mobility, via the other two levels, to the mobile station. One of the functions of the R-P interface is to bring Simple IP service closer in functionality to Mobile IP service, along with addressing other problems. For example, it addresses the situations where the mobile station changes its point of attachment to the network so frequently that basic Mobile IP tunnel establishment introduces significant network overhead in terms of the increased signaling messages. Another often-cited problem is the latency of establishing each new tunnel, which introduces delays or gaps during which user data is unavailable. This delay is inherent in the round-trip incurred by Mobile IP as the registration request is sent to the HA and the response is sent back to the PDSN.

CDMA2000 Mobile AAA

CDMA2000, just like the majority of other cellular systems, supports the concept of home and visited networks. A CDMA2000 subscriber has an account established with one wireless carrier, which provides the user with wireless voice and data services. This same wireless carrier may provide a *home network* for the mobile subscriber. The home network holds user profile and authentication information. When the user roams into the territory of a different wireless carrier—that is, a visited network—that carrier must

obtain the authentication information and the *service profile* for this particular user from its home network. The service profile indicates what radio resources the user is authorized to use, such as a maximum bandwidth or access priority. In CDMA2000 the user profiles are stored in a Home Location Register (HLR) located in the home network and are temporarily retrieved into a Visitor Location Register (VLR) located in the serving network. The HLR and VLR are databases housed on fault-tolerant computing platforms. Similar procedures take place to authenticate the user access to data networks.

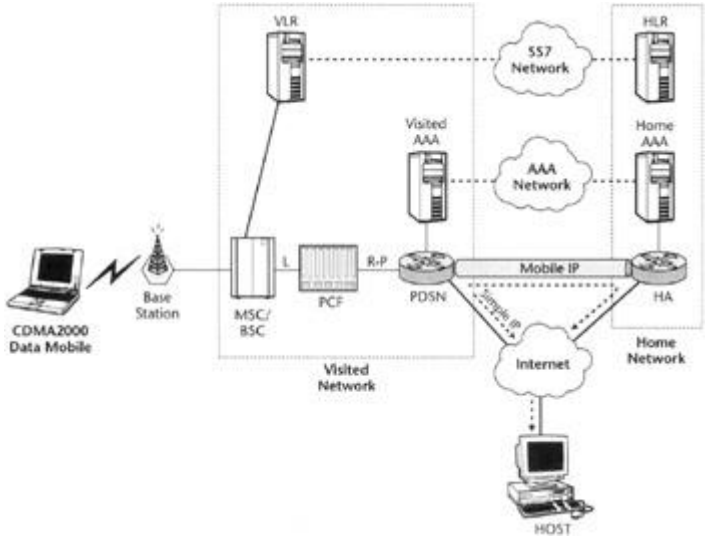


Figure 3.16: Typical CDMA2000 core network with AAA subsystems.

[Source: Text book- Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

Mobile stations requesting data service in CDMA2000 systems will have to be authenticated twice: on the physical layer and on the link layer (or, using other terminology frequently used in the industry, both wireless access and network access authentication will take place). Physical layer (or wireless access and user terminal equipment) authentication is performed by the cellular wireless system's HLR and VLR infrastructure. It is based on an International Mobile Station (IMSI) and is defined in [IS-2000] (the details of this authentication method are outside the scope of this book). CDMA2000 link layer, or packet data network access, authentication of the mobile station is conducted by the infrastructure of AAA servers and clients, the latter being hosted by PDSNs and HAs. It is based on a Network Access Identifier [6] (NAI, defined by IETF [RFC2486])—that is, a user identifier of the form user@homedomain, which allows the visited network to identify the home network AAA server by mapping the

"home-domain" label to the home AAA IP address. A challenge from the PDSN also allows for protection from replay-based attacks.

Among other services, NAI allows for distribution of specific Mobile IP security association information to support PDSN/HA authentication during mobile registration, HA assignment, and inter-PDSN handoff. Note that data network AAA authenticates the user, as opposed to physical layer authentication, which only authenticates the mobile. Therefore, users wishing to gain access to public or private data networks are presented with a login and password sequence, familiar to wireline remote data access users, in addition to mobile device authentication taking place at registration stage, which results in the momentary hesitation at phone startup familiar to most mobile phone users.

The CDMA2000 data subsystem provides two user authentication mechanisms when simple IP or Mobile IP access methods are requested, as defined in [IS835] and [RFC3141]. As mentioned, for the Simple IP access mode, authentication is based on CHAP, which is a part of PPP negotiation. In CHAP, the PDSN challenges the mobile station with a random value to which it must respond with a signature based on MD-5 digest of the challenge, a username, and a password. The PDSN passes the challenge/response pair to the home AAA server for user authentication.

For Mobile IP, the PDSN sends a similar challenge within the agent advertisement message to the mobile station. Again, the MS must respond to the challenge with a signature and NAI that is verified by the home network, but this time the response is sent along with the Mobile IP registration request rather than during PPP session establishment. Both of these mechanisms rely on shared secrets associated with the NAI, which are stored in the home network, and both will be supported by the same AAA infrastructure. In both cases the accounting data is collected in the PDSN and transferred to the AAA server. The PDSN collects data usage statistics for each user, combines these with the radio access accounting records sent by the PCF, and forwards them to the local AAA server. Note that accounting information is collected by both the PCF and the PDSN. For roaming users, the AAA server may be configured to forward a copy of all RADIUS accounting records to the home AAA server in addition to keeping a copy at the visited AAA server.

When a handoff between two PDSNs occurs, an *Accounting Stop* message is sent to the AAA server from the releasing PDSN, and an *Accounting Start* is sent to the AAA server from the connecting PDSN (more details on this and other accounting mechanisms is provided in Appendix B). The Accounting Stop from the releasing PDSN may arrive some time after the Accounting Start from the new PDSN (the releasing PDSN may not be aware that mobile has moved, but it must wait for a Registration Lifetime or PPP Inactivity timeout to end the session). This means the billing server must accept multiple stop/start sequences from different PDSNs that contain overlap and treat these as a single session, per [IS 835]. When a PPP inactivity timer or an MIP lifetime expires, or the mobile terminates the session, the R-P link is released and an Accounting Stop is sent to the AAA server.