3GPP

The 3rd Generation Partnership Project (3GPP) unites [Seven] Tele communications standard development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), known as "Organizational Partners" and provides their members with a stable environment to produce the Reports and Specifications that define 3GPP technologies.

The project covers cellular telecommunications technologies, including radio access, core network and service capabilities, which provide a complete system description for mobile telecommunications.

The 3GPP specifications also provide hooks for non-radio access to the core network ,and for interworking with non-3GPP networks. 3GPP specifications and studies are contribution-driven, by member companies, in Working Groups and at the Technical Specification Group level.

The three Technical Specification Groups (TSG) in 3GPP are;

- Radio Access Networks (RAN),
- Services & Systems Aspects (SA),
- Core Network & Terminals (CT)

The Working Groups, within the TSGs, meet regularly and come together for their quarterly TSG Plenary meeting, where their work is presented for information, discussion and approval.

The last meeting of the week of TSG Plenary meetings (see example below) is TSG SA, which also has responsibility for the overall coordination of the technical work and for the monitoring of its progress. The 3GPP technologies from these groups are constantly evolving through Generations of commercial cellular / mobile systems (see table below). With LTE, LTE-Advanced, LTE Advanced Pro and 5G work - 3GPP has become the focal point for the vast majority of mobile systems beyond 3G.

Although these Generations have become an adequate descriptor for the type of network under discussion, real progress on 3GPP standards is measured by the milestones achieved in particular Releases. New features are 'functionality frozen' and are ready for implementation when a Release is completed. 3GPP works on a number of Releases in parallel, starting future work well in advance of the completion of the current Release. Although this adds some complexity to the work of the groups, such a way of working ensures that progress is continuous & stable.

Backward Compatibility

The major focus for all 3GPP Releases is to make the system backwards and forwards compatible where possible, to ensure that the operation of user equipment is uninterrupted. A good example of this principle was the priority placed on backward compatibility between LTE and LTE-Advanced, so that an LTE-A terminal can work in an LTE cell and an LTE terminal works in the LTE-A cell.

For 5G, many operators are starting with dual connectivity between LTE and 5G NR equipment - using the 'Non-Standalone' work completed early in Release 15. In the process of completing the early drop of 5G NR care has been taken to build 'forward compatibility' in to Non-Standalone NR equipment, to ensure that it will be fit for use on Standalone 5G NR systems.

Generations of Mobile Systems

Generation	Major Systems Milestones
1G	Analogue technology, from the 1980s onwards. Various technologies were deployed, Nationally or Regionally, including: NMT (Nordic Mobile Telephone), AMPS (Advanced Mobile Phone System), TACS (Total Access Communications System), A-Netz to E-

Generation	Major Systems Milestones
	Netz, Radiocom 2000, RTMI (Radio Telefono Mobile Integrato), JTACS (Japan Total Access Communications System) and TZ-80n (Source:wikipedia)
2G	First digital systems, deployed in the 1990s introducing voice, SMS and data services. The Primary 2G technologies are: GSM/GPRS & EDGE, CDMAOne, PDC, iDEN, IS-136 or D-AMPS.
3G	The 3G system from 3GPP is based on evolved Global System for Mobile communication (GSM) core networks and the radio access technologies that they support. This has allowed for the maintenance and development of GSM, with the evolution of General Packet Radio Service (GPRS) and Enhanced Data rates for GSM Evolution (EDGE), as well as further developments with the Universal Mobile Telecommunications System (UMTS) and High Speed Packet data Access (HSPA). 3G brought a global vision to the evolution of mobile networks, with the creation of the ITU's family of IMT-2000 systems which included EDGE, CDMA2000 1X/EVDO and UMTS-HSPA+ radio access technologies.

3G/4G	LTE and LTE-Advanced have crossed the “generational boundary” offering the next generation(s) of capabilities. With their capacity for high speed data, significant spectral efficiencies and adoption of advanced radio techniques, their emergence has been the basis for all

Generation	Major Systems Milestones
	new mobile systems from Release 8 onwards. It should be noted that LTE-Advanced (From Release 10) is 3GPP's ITU-R IMT-Advanced radio interface. LTE-Advanced is the first true 4G technology to be specified by 3GPP. LTE-Advanced Pro is the name that helps the industry describe what has been achieved with the completion of Release 13. LTE Pro is set to be used by other sectors, beyond telecoms, including Critical Communications (blue light services & other Mission Critical systems), the machine-to-machine or Internet of Things (IoT) sector, Transport (Rail, ITS, etc), Education and many other areas. LTE- Advanced Pro is 3GPP's stepping stone to 5G systems
5G	5G brings another major technology step, with the creation of a 'New Radio' (NR). Unlike with 4G, where 3GPP hesitated to join the generational march onwards beyond 3G, we have embraced the alignment of the industry on NR and on LTE-Advanced Pro to provide 5G – from 3GPP Release 15 onwards.

Radio Access Milestones

3GPP Technical Specification Group RAN, like other TSGs, ensures that systems based on 3GPP specifications are capable of rapid development and deployment with the provision of global roaming of equipment.

Each progressive 3GPP radio access technology aims to reduce complexity and avoid fragmentation of technologies on offer.

Core Network Evolution

GSM networks used circuit-switch telephony initially, with packet-switching added with GPRS. In the UMTS architecture, this dual-domain concept was kept on the core network side. Some network elements were evolved, but the concept remained very similar.

When considering the evolution of the 3G system towards LTE, the 3GPP community decided to use IP (Internet Protocol) as the key protocol to transport all services. It was therefore agreed that the Evolved Packet Core (EPC) would not have a circuit-switched domain but that the EPC should be an evolution of the packet-switched architecture used in GPRS/UMTS.

INTRODUCTION

The Third Generation (3G) wireless systems offer services and thereby reduce the distinction between the range of services of wire line and wireless. It is an advanced technology and it enhances the features of second generation and adds its own advanced features. Updating cellular telecommunications network around the world are using 3G technologies.

The main reason for the evolution of 3G was due to the limited capacity of the 2G networks.

2G networks were built for voice calls and slow data transmission. But these services were unable to satisfy the requirements of present wireless revolution.

International Telecommunication Union (ITU) has defined the demand for 3G in the International Mobile Telecommunication (IMT)-2000 standards to facilitate growth, increase bandwidth, support diverse applications.

The development like 2.5G or GPRS (General Packet Radio Service) and 2.75G or EDGE (Enhanced Data rates for GSM Evolution) technologies resulted in the transition to 3G. These technologies act like bridge between 2G and 3G.

Features of 3G

It provides cost efficient high quality, wireless multimedia applications and enhanced wireless communications.

It supports greater voice and data capacity and high data transmission at low cost.3G mobiles can operate on 2G and 3G technologies.

It offers greater security features than 2G. It supports network access security, network domain security, user domain security, application security.

It supports video calls and video conferences. It provides support from localized service like accessing traffic and high end services like weather updates. We can listen to music, watch videos online and can download huge files with in less time.

Advantages of 3G

All the functions in a normal 2G mobile devices can be performed in 3G at a higher speed.

It provides faster connectivity, faster internet access and music with improved quality.

Applications of 3G

- The 3G mobile can be used as a modem for computer which can access internet and can download games and songs at high speed.
- It provides high quality voice calls and video calls.
- It provides weather updates, news headlines and TV broadcasting in mobile phone.
- It provides high speed internet facility for many applications. It can provide data transmission speed up to 2Mbits /sec.
- It provides multimedia services such as sharing of digital photos and movies. It provides location based services and real time multi-player gaming.
- It supports virtual banking and online selling.
- It supports teleconferencing.

Drawbacks

There are few drawbacks:

Upgrading the base station and cellular infrastructure to 3G in cur's very high costs.

- Service provider has to pay high amount for 3G licensing and agreements.
- Problem with the availability of handsets and few regions and their

Costs.

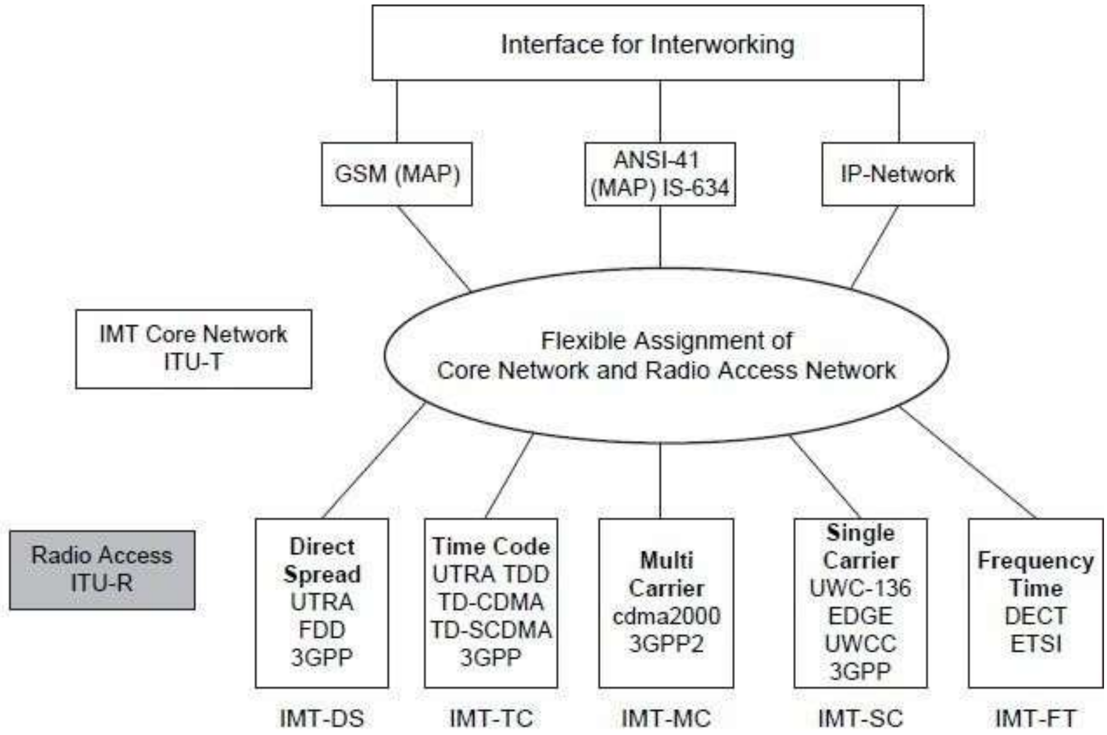
- High power consumption.

IMT Family

The International Telecommunication Union (ITU) identified the long-term spectrum requirements for the future third-generation (3G) mobile wireless telecommunications systems. In 1992, the ITU identified 230 MHz of spectrum in the 2 GHz band to implement the IMT (International Mobile Telecommunications)-2000 system on a worldwide basis for satellite and terrestrial components. The aim of IMT-2000 is to provide universal coverage enabling terminals to have seamless roaming across multiple networks. The ITU accepted the overall standardization responsibility of IMT-2000 to define radio interfaces that are applicable in different radio environments including indoor, outdoor, terrestrial, and satellite.

The above figure provides an overview of the IMT family. IMT-DS is the direct spread (DS) technology and includes WCDMA systems. This technology is intended for UMTS terrestrial radio access (UTRA)-FDD and is used in Europe and Japan.

IMT-TC family members are the UTRA-TDD system that uses time division (TD) CDMA, and the Chinese TD-synchronous CDMA (TD-SCDMA).Both standards are combined and the third-generation partnership project (3GPP)is responsible for the development of the technology. IMT-MC includes multiple carrier (MC) cdma2000 technology, an evolution of the c dma one family.


Interface for Interworking
GSM (MAP)
ANSI-41 (MAP) IS-634
IP-Network
IMT Core Network ITU-T
Flexible Assignment of Core Network and Radio Access Network
Radio Access ITU-R
Direct Spread UTRA FDD 3GPP
Time Code UTRA TDD TD-CDMA TD-SCDMA 3GPP
Multi Carrier cdma2000 3GPP2
Single Carrier UWC-136 EDGE UWCC 3GPP
Frequency Time DECT ETSI
IMT-DS
IMT-TC
IMT-MC
IMT-SC
IMT-FT

ITU: International Telecommunication Union
MAP: Mobile Application Part
FDD: Frequency Division Duplex
3GPP: Third-Generation Partnership Project

Fig. 3.1 IMT Family

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

3GPP2is responsible for standardization. IMT-SC is the enhancement of the US TDMA systems. UWC-136 is a single carrier (SC) technology. This technology Applies EDGE to enhance the 2 G IS-136 standards. It is now integrated into the 3GPPefforts. IMT-FT is a frequency time (FT) technology. An enhanced version of the cordless telephone standard digital European cordless technology (DECT) has been selected for low mobility applications. The ETSI has the responsibility for standardization of DECT.

In Europe, 3G systems are intended to support a substantially wider and enhanced range of services compared to the 2G (GSM) system. These enhancements include multimedia services, access to the Internet, high rate data, and soon. The enhanced services impose additional requirements on the

Fixed network functions to support mobility. These requirements are achieved through an evolution path to capitalize on the investments for the 2G system in Europe, Japan, and North America.

In North America, the 3G wireless telecommunication system, cdma2000was proposed to ITU to meet most of the IMT requirements in the indoor office, indoor to outdoor pedestrian, and vehicular environment. In addition, thecdma2000 satisfies the requirements for 3G evolution of 2G TIA/EIA 95 family of standards (cyma One).

In Japan, evolution of the GSM platform is planned for the IMT (3G) core network due to its flexibility and widespread use around the world. Smooth migration from GSM to IMT-2000 is possible. The service area of the 3G system overlays with the existing 2G (PDC) system. The 3G system connects and interworks with 2G systems through an interworking function (IWF). An IMT- 2000-PDC dual mode terminal as well as the IMT-2000 single mode terminal is deployed.

UMTS as discussed today and introduced in many countries is based on the initial release of UMTS standards referred to as release 99 or R99. This (release) is aimed at a cost-effective migration from GSM to UMTS. After R99 the Release of 2000 or R00 followed. 3GPP decided to split R00 into two standards and call them release 4 (Rel-4) and release 5 (Rel-5). The version of all standards finalized for R99 is now referred to as Rel-3 by 3GPP. Rel-4 introduces Qi's in the fixed network plus several execution environments (e.g., Mixed, mobile execution environment) and new service architectures. Rel-4 was suspended in March 2001.

Rel-5 specifies a new core network. The GSM/GPRS-based core network will be replaced by an almost all-IP core network. The content of Rel-5 was suspended

CDMA2000 SYSTEM

Introduction

The nets CDMA2000 are compatible with the nets cdmaOne, that which protects the investments of the operator's 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, European America. Other 35 CDMA2000 nets will be deployed in the whole world in a future not very distant.

Evolution de 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:

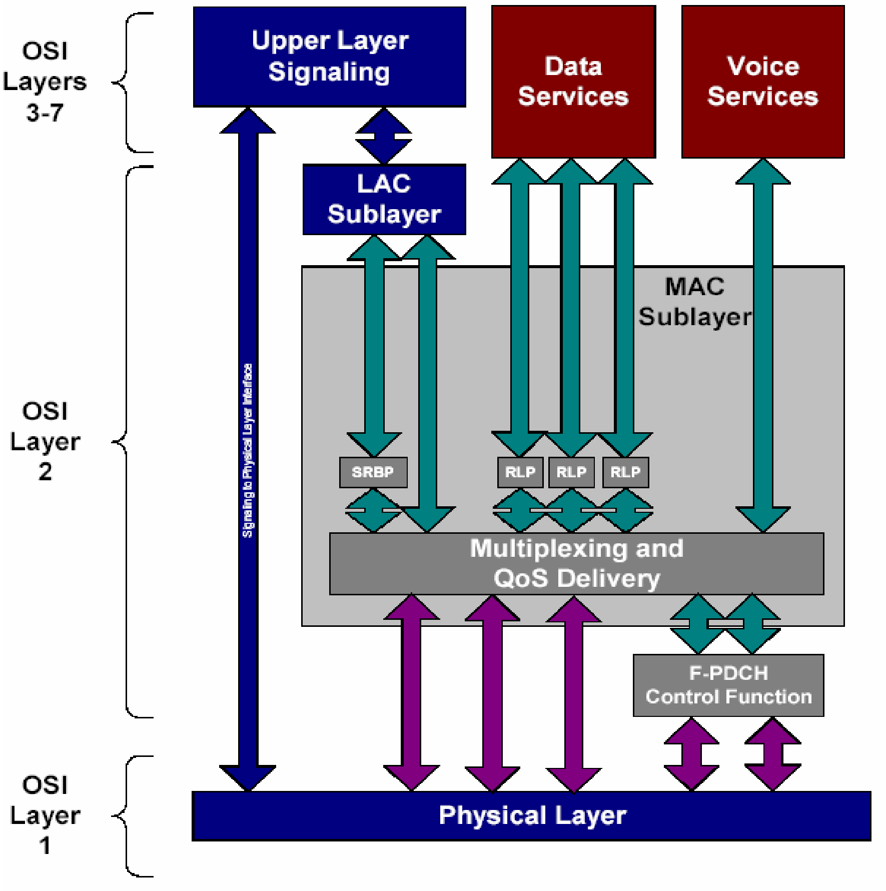
- Evolution of CDMA2000 1X that it offers bigger data transmission speed can offer up to 2.4 Mbps in a single carrier the same as the previous one (1.25 MHz).

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 Johan Schiller]

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

Dedicated Traffic Channel (f/r-ditch): A point to point logical channel that carries data or voice traffic over a dedicated physical channel.

- Common Control channels (f/r-cache control): These are used to carry MAC messages with shared access for several terminals.

- Dedicated signaling Cannel (f/r-disc): A point to point logical channel that carries upper layer signaling traffic over a dedicated physical channel, for a single terminal.
- Common Signaling Channel (f/r-cash): A point to multipoint logical channel that carries upper layer signaling 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 characterized 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.

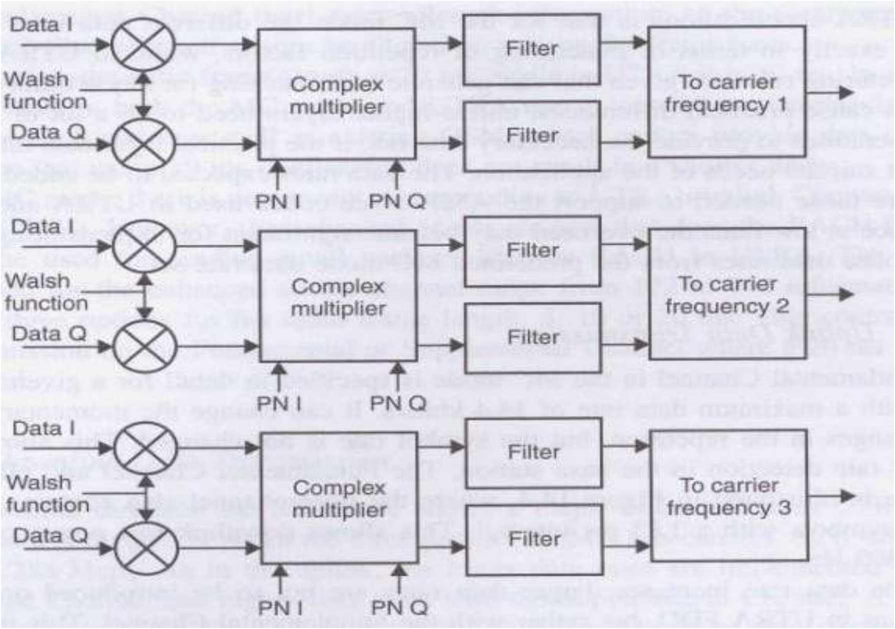


Figure 3.9: Multi-Carrier Mode [Source: Text book- Mobile Communications, Second Edition, Pearson Education Johan Schiller]

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 characterized by the use of a single code. MC mode is a synchronized 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 an interval like 1, 25 mms, it allows in the downlink fast power control (rate 800Hz). The user data he radio frame length is 20 Ms.

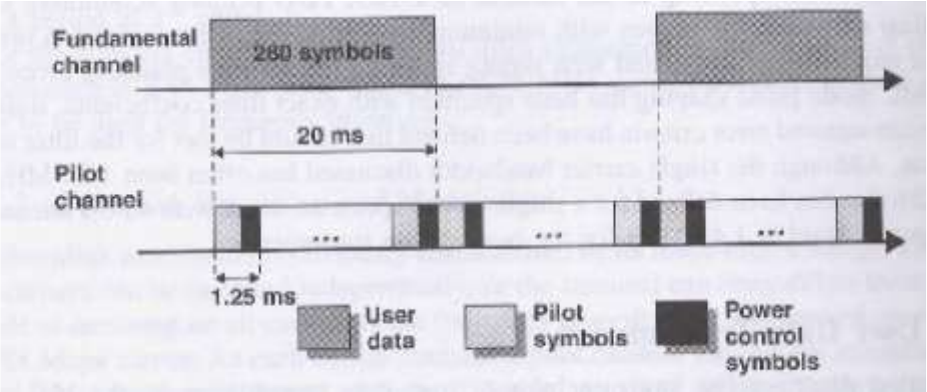


Figure 3.10: Uplink Data Transmission frame lenth is 20 ms

[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 MPs

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

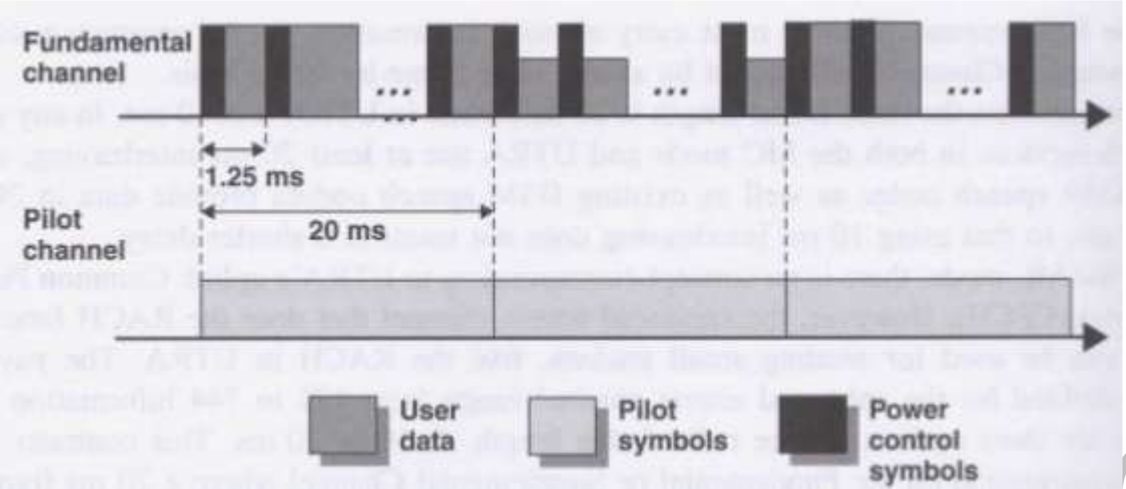


Figure 3.11: Downlink Data Transmission frame length is 20 ms

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

Signaling

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 (such as 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.

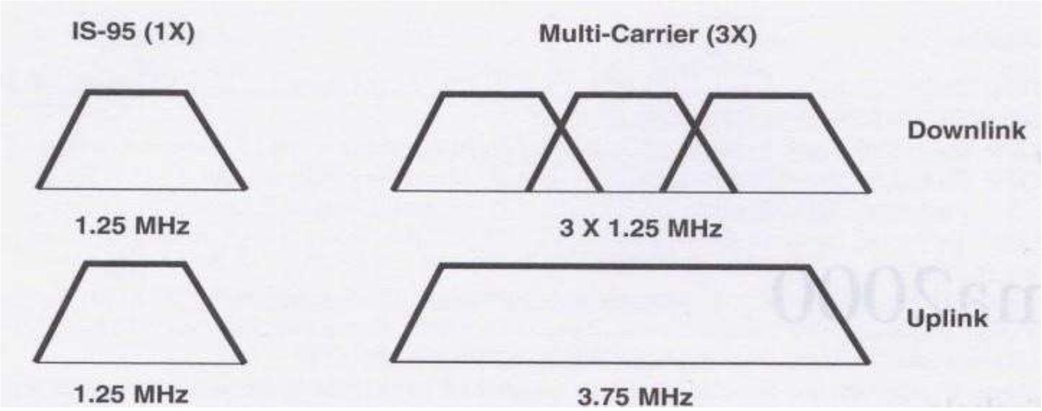


Figure 3.12: CDMA 2000 Spectrum

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

Johan Schiller]

Terminals

More than 578 terminals CDMA2000 1X and of 68 terminal CDMA2000 1xEV-DO are at the moment available, by manufacturing leaders like Audio ox, Axesstel, Ericsson, CURITEL, Handspring, Huawei, Kyocera, LG, Motorola, Nokia, Research in Motion, Samsung, Sanyo, SK TeleTech, Titular 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 wire line 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 air link 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 atthe 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.

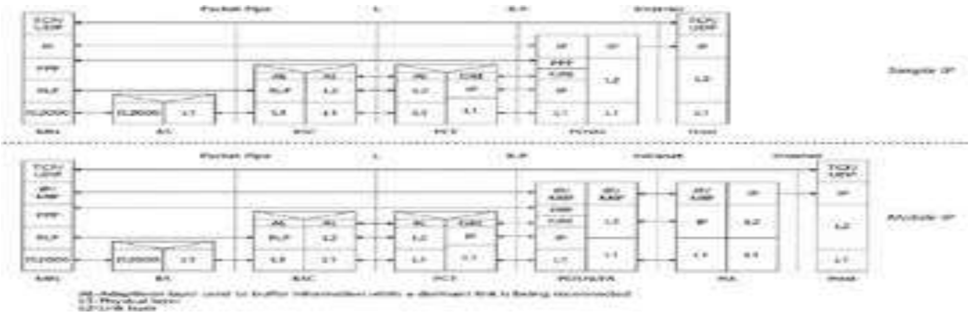


Figure 3.14: Examples of CDMA2000 data service protocol stacks.

[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 DOarchitecture, 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,must support secure reverse tunneling to the Home

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 Stack 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.

Dormer another mobile device is expected to support air link "dormancy" (as defined by TIA [IS- 707A1]), which allows either the mobile or the MSC to time out the active air link 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/Fees 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.). 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.

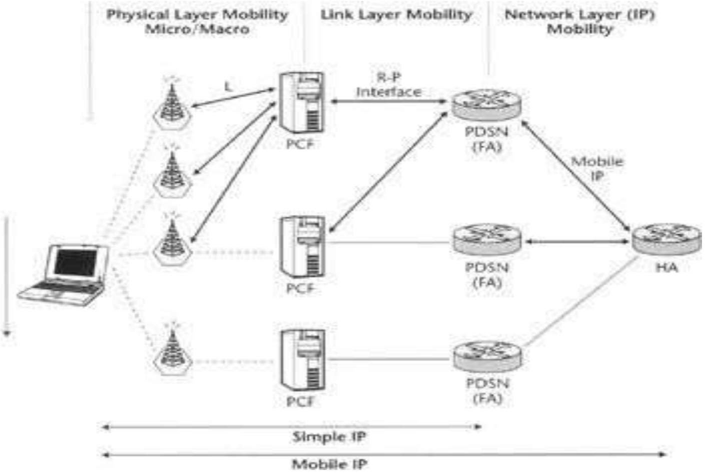


Figure 3.15: CDMA2000 mobility hierarchy.

[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

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 face, terminate all necessary protocols and do not require any additional terminal itself. at the *Network model* mobile stations, in addition to the radio in 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

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

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.

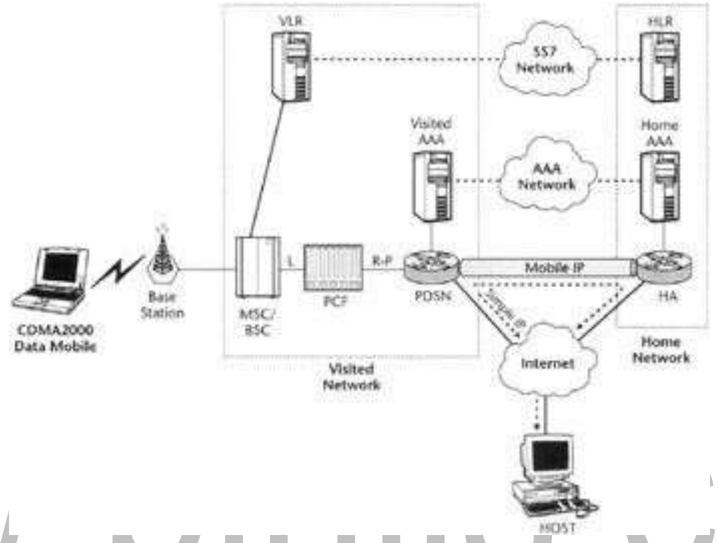


Figure 3.16: Typical CDMA2000 core network with AAA subsystems.

[Source: Text book- Mobile Communications, Second Edition, Pearson Education by Jochen SchillerMobile 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 wire line 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 territory of a different wireless carrier—that is, a visited network—that carrier must

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 the 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 time out to end the session).The means the billing sever must accept multiple stop\start sequences from different PDSN that contain overlap and treat these as a single session. (IS835). 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 sever.

TD-CDMA, TD – SCDMA

-CDMA (WCDMA; Wideband Code-Division Multiple Access), along with UMTS-FDD, UTRA-FDD, or IMT-2000 CDMA Direct Spread is an air interface standard found in 3G mobile telecommunications networks. It supports conventional cellular voice, text and MMS services, but can also carry data at high speeds, allowing mobile operators to deliver higher bandwidth applications including streaming and broadband Internet access

W-CDMA uses the DS-CDMA channel access method with a pair of 5 MHz wide channels. In contrast, the competing CDMA2000 system uses one or more available 1.25 MHz channels for each direction of communication. W-CDMA systems are widely criticized for their large spectrum usage, which delayed deployment in countries that acted relatively slowly in allocating new frequencies specifically for 3G services (such as the United States).

The specific frequency bands originally defined by the UMTS standard are 1885–2025 MHz for the mobile-to-base (uplink) and 2110–2200 MHz for the base-to-mobile (downlink). In the US, 1710–1755 MHz and 2110–2155 MHz are used instead, as the 1900 MHz band was already used While UMTS2100 is the most widely deployed UMTS band, some countries' UMTS operators use the 850 MHz (900 MHz in Europe) and/or 1900 MHz bands (independently, meaning uplink and downlink are within the same band), notably in the US by AT&T Mobility, New Zealand by Telecom New Zealand on the XT Mobile Network and in Australia by Telstra on the Next G network. Some carriers such as T-Mobile use band numbers to identify the UMTS frequencies. For example, Band I (2100 MHz), Band IV (1700/2100 MHz), and Band V (850 MHz).

UMTS-FDD is an acronym for Universal Mobile Telecommunications System (UMTS) – Frequency-division duplexing (FDD) and a 3GPP standardized version of UMTS networks that makes use of frequency-division duplexing for duplexing over an UMTS Terrestrial Radio Access (UTRA) air interface

W-CDMA is the basis of Japan's NTT DoCoMo's FOMA service and the most-commonly used member of the Universal Mobile Telecommunications System (UMTS) family and sometimes used as a synonym for UMTS It uses the DS-CDMA channel access method and the FDD duplexing method to achieve higher speeds and support more users compared to most previously used time-division multiple access (TDMA) and time-division duplex (TDD) schemes.

TD-CDMA (UTRA-TDD 3.84 MPs High Chip Rate (HCR))

TD-CDMA, an acronym for Time-Division-Code-Division Multiple Access, is a channel-access method based on using spread-spectrum multiple-access (CDMA) across multiple time slots (TDMA). TD-CDMA is the channel access method for UTRA-TDD HCR, which is an acronym for UMTS Terrestrial Radio Access-Time Division Duplex High Chip Rate

UMTS-TDD's air interfaces that use the TD-CDMA channel access technique are standardized as UTRA-TDD HCR, which uses increments of 5 MHz of spectrum, each slice divided into 10 ms frames containing fifteen time slots (1500 per second). The time slots (TS) are allocated in fixed percentage for downlink and uplink. TD-CDMA is used to multiplex streams from or to multiple transceivers. Unlike W-CDMA, it does not need separate frequency bands for up- and downstream, allowing deployment in tight frequency bands

TD-CDMA is a part of IMT-2000, defined as IMT-TD Time-Division (IMT CDMA TDD), and is one of the three UMTS air interfaces (UTRAs), as standardized by the 3GPP in UTRA-TDD HCR. UTRA-TDD HCR is closely related to W-CDMA, and provides the same types of channels where possible. UMTS's HSDPA/HSUPA enhancements are also implemented under TD-CDMA

TD-SCDMA is a time division duplex, TDD version of UMTS that was developed in China and offered some key advantages as a TDD version. TD-SCDMA standards for Time Division - Synchronous CDMA.

Although different to the more standard TDD version of UMTS, TD-SCDMA was adopted by 3GPP and was included in the 3GPP standards as an accepted version of UMTS.

Much of the work to develop TD-SCDMA was undertaken by China Academy of Telecommunications Technology (CATT).

TD-SCDMA offers the advantages of the of any TDD system, but also was designed to incorporate many new technologies including joint detection, adaptive antennas, and dynamic channel allocation.

Although TD-SCDMA was never deployed outside China, it promoted the advantages of TDD systems and enabled 4G LTE push forwards the TDD versions of 4G LTE.

TD-SCDMA basics

One of the key elements of TD-SCDMA is the fact that it uses a TDD, Time Division Duplex approach. As seen with UMTS TDD this has advantages in a number of areas, enabling the balance to be changed between uplink and downlink to accommodate the different levels of data transfer. It also has advantages in terms of using unpaired spectrum, spectrum efficiency for certain loads and it does not require expensive diplexers in the handsets to enable simultaneous transmission on the uplink and downlink, although transmit / receive switching times must be accommodated and can reduce the efficiency of the system.

As a further advantage, TD-SCDMA uses the same RAN as that used for UMTS. In this way it is possible to run TD-SCDMA alongside UMTS, and thereby simplifying multi-system designs.

Although UMTS (W-CDMA) and cdma2000 are widely recognized as 3G cellular standards, TD-SCDMA is equally valid. In fact it has been adopted as the low chip rate (LCR) version of the 3GPP TDD standard.

TD-SDCMA specification overview

The TD-SCDMA standard provides many advantages. As already mentioned it has many similarities to W-CDMA, although a summary of the basic features and specification is given below:

TD-SCDMA SPECIFICATION SUMMARY

TD-SCDMA CHARACTERISTIC	FIGURE
Bandwidth	1.6 MHz
Chip rate per carrier	1.28 MPs
Frame Rate	10ms
Spectrum spreading mode	DS SF=1/2/4/8/16
Modulation	QPSK / 8PSK / 16QAM
Channel coding	■ Convolutional codes: R=1/2,1/3 Turbo implemented
Interleaving	10/20/40/80 MS Frame structure Super frame 720ms, Radio frame 10ms Sub frame 5 mms
Uplink synchronization	1/2 chip
Number of voice channels per carrier	48
Spectrum Efficiency	25Erl./MHz
Total transmission rate provided by each carrier	1.971Mbps

TD-SCDMA operation

The UMTS TD-SCDMA system has adopted a number of advanced techniques and technologies to optimize the operation. These are often above and beyond those that have been catered for in the more widely used standard forms of FDD and TDD UMTS. Some

Of these result from the fact that TD-SCDMA uses the same frequency for both uplink and downlink, and as a result of the higher processing levels now available.

These include:

- ***art antennas:*** Smart antenna technology is incorporated into the base station. This enables beams to be formed and this is able to reduce interference between terminals and concentrate transmitted power at active terminals. This technique is implemented using smart antenna arrays that incorporate advanced DSP algorithms. The base station is able to locate the mobile terminals and to steer transmit beams to specific terminals. In this way spatial beam forming is able to reduce interference within a given channel with a resulting improvement in the downlink capacity.
- ***Joint detection technology:*** Within CDMA, multiple users all occupy the same frequency band, accessing he base station using different codes. In this way, multiple-access interference results and this is a major problem in CDMA-based systems. A technique referred to as joint detection technology treats signals from all users as useful and processes them in parallel. As the maximum number of users in any time slot is 16, the processing complexity to separate users is kept within manageable limits.
- ***User terminals and base station synchronization:*** The synchronization of the network enables precise adjustment of the timing advances for transmission from terminals so that signals from different users arrive at the base station together, and not overlapping in time into the transmit time frames making detection much simpler. This synchronization enables faster search for neighboring cells during handover and it also removes the need for soft handover

UMTS CORE NETWORK ARCHITECTURE

The UMTS network architecture can be divided into three main elements:

1. **User Equipment (UE):** The User Equipment or UE is the name given to what was previous termed the mobile, or cellphone. The new name was chosen because the considerably greater functionality that the UE could have. It could also be anything between a mobile phone used for talking to a data terminal attached to a computer with no voice capability.
2. **Radio Network Subsystem (RNS):** The RNS also known as the UMTS Radio Access Network, UTRAN, is the equivalent of the previous Base Station Subsystem or BSS in GSM. It provides and manages the air interface for the overall network.
3. **Core Network:** The core network provides all the central processing and management for the system. It is the equivalent of the GSM Network Switching Subsystem or NSS.

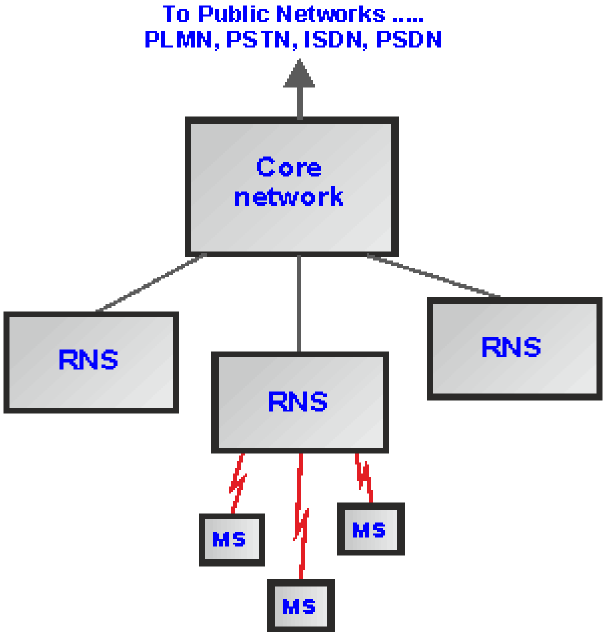


Fig.3.5 UMTS Network Architecture Overview

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

User Equipment, UE

The USER Equipment or UE is a major element of the overall 3G UMTS network architecture. It forms the final interface with the user. In view of the far greater number of applications and facilities that it can perform, the decision was made to call it user equipment rather than a mobile. However it is essentially the handset (inthe broadest terminology), although having access to much higher speed data communications, it can be much more versatile, containing many more applications. It consists of a variety of different elements including RF circuitry, processing, antenna, battery, etc.

There are a number of elements within the UE that can be described separately:

- UE RF circuitry: The RF areas handle all elements of the signal, both forth receiver and for the transmitter. One of the major challenges for the RF power amplifier was to reduce the power consumption. The form of modulation used for W-CDMA requires the use of a linear amplifier. These inherently take more current than nonlinear amplifiers which can be used for the form of modulation used on GSM. Accordingly to maintain battery life, measures were introduced into many of the designs to ensure the optimum efficiency.
- Baseband processing: The base-band signal processing consists mainly of digital circuitry. This is considerably more complicated than that used in phones for previous generations. Again this has been optimized to reduce the current consumption as far as possible.
- Battery: While current consumption has been minimized as far as possible within the circuitry of the phone, there has been an increase in current drain on the battery. With users expecting the same lifetime between charging batteries as experienced on the previous generation phones, this has necessitated the use of new and improved battery technology. Now Lithium Ion (Li-ion) batteries are used. These phones to remain small and relatively light while still retaining or even improving the overall life between charges.

- Universal Subscriber Identity Module, USIM: The UE also contains a SIM card, although in the case of UMTS it is termed a USIM (Universal Subscriber Identity Module). This is a more advanced version of the SIM card used in GSM and other systems, but embodies the same types of information. It contains the International Mobile Subscriber Identity number (IMSI) as well as the Mobile Station International ISDN Number (MSISDN). Other information that the USIM holds includes the preferred language to enable the correct language information tobe displayed, especially when roaming, and a list of preferred and prohibited Public Land Mobile Networks (PLMN).

3G UMTS Radio Network Subsystem

This is the section of the 3G UMTS / WCDMA network that interfaces to both the UE and the core network. The overall radio access network, i.e. collectively all the Radio Network Subsystem is known as the UTRAN UMTS Radio Access Network.

The radio network subsystem is also known as the UMTS Radio Access Network or UTRAN.

3G UMTS Core Network

The 3G UMTS core network architecture is a migration of that used for GSM with further elements overlaid to enable the additional functionality demanded by UMTS. In view of the different ways in which data may be carried, the UMTS core network may be split into two different areas:

- **Circuit switched elements:** These elements are primarily based on the GSM network entities and carry data in a circuit switched manner, i.e. a permanent channel for the duration of the call.
    - It is used to provide voice and CS data services.
    - It contains Mobile Switching Center (MSC) and Gateway MSC(GMSC) as functional entities.
- **Packet switched elements:** These network entities are designed to carry packet

data. This enables much higher network usage as the capacity can be shared and data is carried as packets which are routed according to their destination.

- It is used to provide packet based services.

It contains Serving GPRS support node (SGSN),

Gateway GPRS support node (GGSN),

Domain Name Server (DNS),

Dynamic Host Configuration Protocol (DHCP) server,

packet charging gateway,

and firewalls.

The core network can be split into the following different functional areas:

Functional entities needed to support PS services (e.g.3G-SGSN, 3G- GGSN)

Functional entities needed to support CS services (e.g. 3G-MSC/VLR)

Functional entities common to both types of services (e.g. 3G-HLR)

Other areas that can be considered part of the core network include:

Network management systems (billing and provisioning, service management, element management, etc.)

IN system (service control point (SCP), service signaling point (SSP), etc.)

ATM/SDH/IP switch/transport infrastructure.

Some network elements, particularly those that are associated with registration are shared by both domains and operate in the same way that they did with GSM.

The below figure shows all the entities that connect to the core network — UTRAN, PSTN, the Internet and the logical connections between terminal equipment (MS, UE), and the PSTN/Internet.

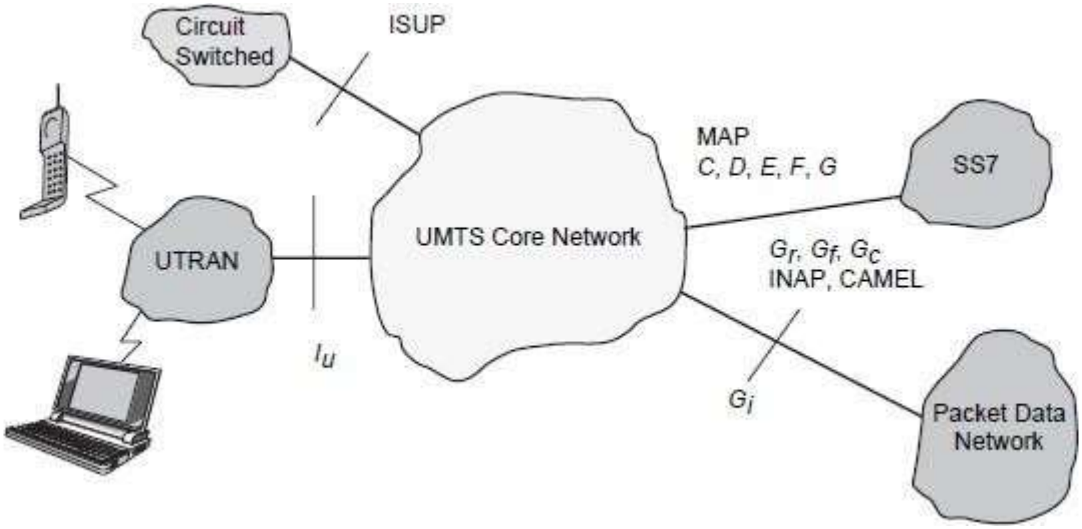


Fig.3.6 UMTS Core network architecture

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

Circuit switched elements

The circuit switched elements of the UMTS core network architecture include the following network entities:

Mobile switching Centre (MSC): This is essentially the same as that within GSM, and it manages the circuit switched calls under way.

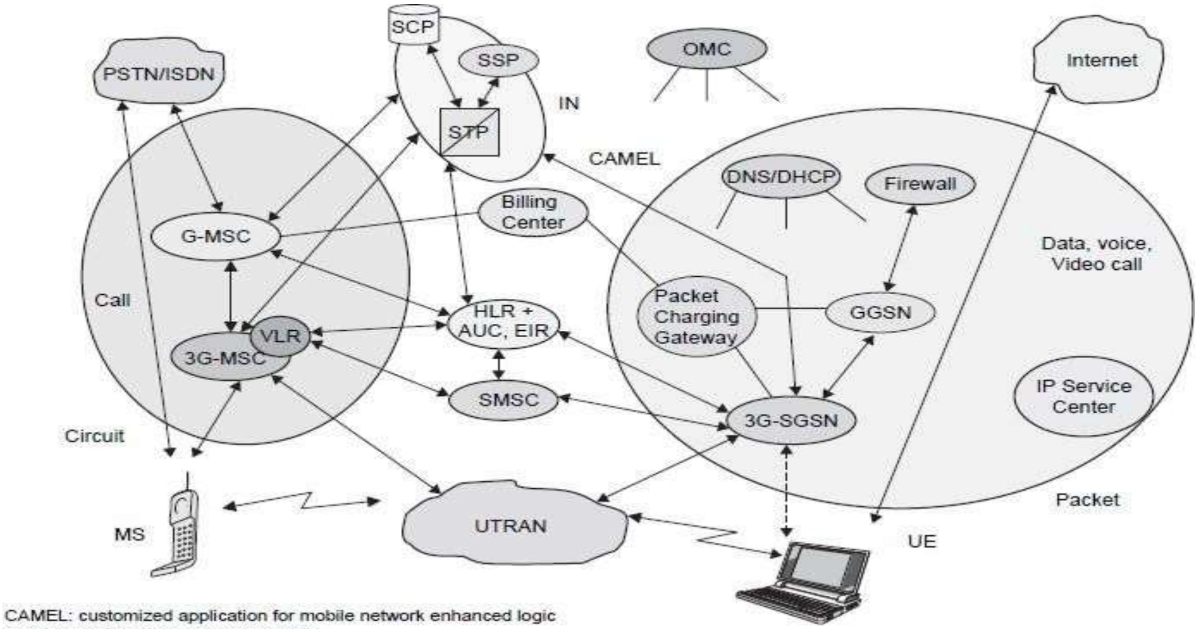
Gateway MSC (GMSC): This is effectively the interface to the external networks.

Packet switched elements

The packet switched elements of the 3G UMTS core network architecture include the following network entities:

Serving GPRS Support Node (SGSN):

Gateway GPRS Support Node (GGSN):



CAMEL: customized application for mobile network enhanced logic
SMSC: short message service center
DNS: domain name server
DHCP: dynamic host configuration protocol

Fig.3.7 Logical architecture of the UMTS core network.

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

3G-MSC

The MSC is the control Centre for the cellular system, coordinating the actions of the BSCs, providing overall control, and acting as the switch and connection into the public telephone network. As such it has a variety of communication links into it which will include fiber optic links as well as some microwave links and some copper wire cables. These enable it to communicate with the BSCs, routing calls to them and controlling them as required. It also contains the Home and Visitor Location Registers, the databases detailing the last known locations of the mobiles. It also contains the facilities for the Authentication Centre, allowing mobiles onto the network. In addition to this it will also contain the facilities to generate the billing information for the individual accounts.

In view of the importance of the MSC, it contains many backup and duplicate circuits to

Ensure that it does not fail. Obviously backup power systems are an essential element of this to guard against the possibility of a major power failure, because if the MSC became inoperative then the whole network would collapse.

While the cellular network is not seen by the outside world and its operation is a mystery to many, the cellular network is at the very center of the overall cellular

System and the success of the whole end to end system is dependent largely on its performance.

This is essentially the same as that within GSM, and it manages the circuit switched calls under way.

It is the main CN element. It provides CS services.

It provides the necessary control and corresponding signaling interfaces includingSS7, MAP, ISUP (ISDN user part), etc.

It is used to provide the interconnection to external networks like PSTN and ISDN.

The following functionality is provided by the 3G-MSC.

Mobility management:

Handles attach, authentication, updates to the HLR,SRNS relocation, anointer systems handover.

Call management:

Handles call set-up messages from/to the UE.

Supplementary services:

Handles call-related supplementary services such as call waiting, etc.

CS data services:

The IWF provides rate adaptation and message translation for circuit mode data services, such as fax.

Coding

SS7, MAP and RANAP interfaces:

The 3G-MSC is able to complete originating or terminating calls in the network in interaction with other entities of a mobile network, e.g., HLR, AUC (Authentication center). It also controls/communicates with RNC using RANAP which may use the services of SS7.

ATM/AAL2

Connection to UTRAN for transportation of user plane traffic across the Iu interface. Higher rate CS data rates may be supported using a different adaptation layer.

Short message services (SMS):

This functionality allows the user to send and receive SMS data to and from the SMS-GMSC/SMS-IWMSC (Interworking MSC).

VLR functionality:

The VLR is a database that may be located within the3G-MSC and can serveas intermediate storage for subscriber data in order to support subscriber mobility.

IN and CAMEL.

OAM

(Operation, administration, and maintenance) agent functionality.

3G-SGSN-Serving GPRS Support Node

The 3G-SGSN is the main CN element for PS services. The 3G-SGSN provides the necessary control functionality both toward the UE and the 3G-GGSN. It also provides the appropriate signaling and data interfaces including connection to an IP-based network toward the 3G-GGSN, SS7 toward the HLR/EIR/AUC and TCP/IP or SS7 toward the UTRAN.

The 3G-SGSN provides the following functions:

Session management:

Handles session set-up messages from/to the UE and the GGSN and operates Admission Control and QoS mechanisms.

I_u and G_n MAP interface:

The 3G-SGSN is able to complete originating or terminating sessions in the network by interaction with other entities of a mobile network, e.g., GGSN, HLR, and AUC. It also controls/communicates with UTRAN using RANAP.

ATM/AAL5

Physical connection to the UTRAN for transportation of user data plane traffic across the I_u interface using GPRS tunneling protocol (GTP).

Connection across the G_n interface toward the GGSN for transportation of user plane traffic using GTP. Note that no physical transport layer is defined for this interface.

SMS:

This functionality allows the user to send and receive SMS data to and from the SMS-GMSC /SMS-IWMSC.

Mobility management:

Handles attach, authentication, updates to the HLR and SRNS relocation, and intersystem handover.

Subscriber database functionality:

This database (similar to the VLR) is located within the 3G-SGSN andserves as intermediate storage for subscriber data to support subscriber mobility.

Charging:

The SGSN collects charging information related to radio network usage bythe user.

3G-GGSN

The GGSN provides interworking with the external PS network. It is connected with SGSN via an IP-based network. The GGSN may optionally support an SS7interface with the HLR to handle mobile terminated packet sessions.

The 3G-GGSN provides the following functions:

It Maintain information locations at SGSN level (macro-mobility) Gateway between UMTS packet network and external data networks(e.g. IP, X.25)

Gateway-specific access methods to intranet (e.g. PPP termination)Initiate mobile terminate Route Mobile Terminated packets User data screening/security can include subscription based, user controlled, or network controlled screening.

User level address allocation: The GGSN may have to allocate (depending on subscription) a dynamic address to the UE upon PDP context activation.

This functionality may be carried out by use of the DHCP function. Charging: The GGSN collects charging information related to external data network usage by the user.

SMS-GMSC/SMS-IWMSC

The overall requirement for these two nodes is to handle the SMS from pointto point. The functionality required can be split into two parts.

The SMS-GMSC is an MSC capable of receiving a terminated short messagefrom a service center, interrogating an HLR for routing information and SMSinformation, and delivering the short message to the SGSN of the recipient UE.

The SMS-GMSC provides the following functions: Reception of short message packet data unit (PDU)Interrogation of HLR for routing information Forwarding of the short message PDU to the MSC or SGSN using the routing information The SMS-IWMSC is an MSC capable of receiving an originatingshort message from within the PLMN and submitting it to the recipient service center.

The SMS-IWMSC provides the following functions:

Reception of the short message PDU from either the 3G-SGSN or3G-MSC

Establishing a link with the addressed service center

Transferring the short message PDU to the service center

Note: The service center is a function that is responsible for relaying, storing, and forwarding a short message. The service center is not part of UCN, although the MSC and the service center may be integrated.

Firewall

A firewall is a network security system, either hardware- or software-based, that controls incoming and outgoing network traffic based on a set of rules.
This entity is used to protect the service providers' backbone data networks from attack from external packet data networks. The security of the backbone data network can be ensured by applying packet filtering mechanisms based on access control lists or any other methods deemed suitable.

Introduction

Firewalls are computer security systems that protect your office/home PCsor your network from intruders, hackers & malicious code. Firewalls protect you from offensive software that may come to reside on your systems or from prying hackers. In a day and age when online security concerns are the top priority of the computer users, Firewalls provide you with the necessary safety and protection.

Firewalls are software programs or hardware devices that filter the traffic that flows into you PC or your network through a internet connection. They sift through the data flow & block that which they deem (based on how & for what youhave tuned the firewall) harmful to your network or computer system.

When connected to the internet, even a standalone PC or a network of interconnected computers make easy targets for malicious software & unscrupulous hackers. A firewall can offer the security that makes you less vulnerable and also protect your data from being compromised or your computers being taken hostage.

Firewalls are setup at every connection to the Internet, therefore subjecting all data flow to careful monitoring. Firewalls can also be tuned to follow "rules". These Rules are simply security rules that can be set up by the network administrators to allow traffic to their web servers, FTP servers, Telnet servers, thereby giving the computer owners/administrators immense control over the traffic that flows in & out of their systems or networks.

Rules will decide who can connect to the internet, what kind of connections can be made, which or what kind of files can be transmitted in out. Basically all traffic in & out can be watched and controlled thus giving the firewall installer a high level of security & protection.

Firewall logic

Firewalls use 3 types of filtering mechanisms:

Packet filtering or packet purity

Data flow consists of packets of information and firewalls analyze these packets to sniff out offensive or unwanted packets depending on what you have defined as unwanted packets.

Proxy

Firewall in this case assumes the role of a recipient & in turn sends it to the node that has requested the information & vice versa. **Inspection**

In this case Firewalls instead of sifting through all of the information in the packets, mark key features in all outgoing requests & check for the same matching characteristics in the inflow to decide if it relevant information that is coming through.

Firewall Rules

Firewalls rules can be customized as per our needs, requirements & securitythreat levels.

We can create or disable firewall filter rules based on such conditions as:

IP Addresses

Blocking off a certain IP address or a range of IP addresses, which you think are predatory.

Domain names

Only certain specific domain names are allowed to access our systems/servers or allow access to only some specified types of domain names or domain name extension like .edu or.mil.

Protocols

A firewall can decide which of the systems can allow or have access to common protocols like IP, SMTP, FTP, UDP, ICMP, Telnet or SNMP.

Ports

Blocking or disabling ports of servers that are connected to the internet will help maintain the kind of data flow you want to see it used for & also close down possible entry points for hackers or malignant software.

Keywords

Firewalls also can sift through the data flow for a match of the keywords or phrases to block out offensive or unwanted data from flowing in. **Types of Firewall**

Software firewalls

New generation Operating systems come with built in firewalls or you can buy a firewall software for the computer that accesses the internet or acts as the gateway to your home network.

Hardware firewalls

Hardware firewalls are usually routers with a built in Ethernet card and hub. Your computer or computers on your network connect to this router & access the web.

Packet firewalls

The earliest firewalls functioned as packet filters, inspecting the packets that are transferred between computers on the Internet. When a packet passes through a packet-filter firewall, its source and destination address, protocol, and destination port number are checked against the firewall's rule set. Any packets that aren’t specifically to their destination). For example, if a firewall is configured with a rule to block Telnet access, then the firewall will drop packets destined for TCP port number 23.

Packet-filter firewalls work mainly on the first three layers of the OSI reference model (physical, data-link and network), although the transport layer is used to obtain the source and destination port numbers. While generally fast and efficient, they have no ability to tell whether a packet is part of an existing stream of traffic. Because they treat each packet in isolation, this makes them vulnerable to spoofing attacks and also limits their ability to make more complex decisions based on what stage communications between hosts are at.

Stateful firewalls

In order to recognize a packet's connection state, a firewall needs to record all connections passing through it to ensure it has enough information to assess whether a packet is the tart of a new connection, a part of an existing connection,or not part of any connection. This is what's called "stateful packet inspection." Stateful inspection was first introduced in 1994 by Check Point Software in its FireWall-1 software firewall, and by the late 1990s, it was a common firewall product feature.

This additional information can be used to grant or reject access based on the packet's history in the state table, and to speed up packet processing; that way, packets that are part of an existing connection based on the firewall's state table can be allowed through without further analysis. If a packet does not match an existing connection, it's evaluated according to the rule set for new connections.

Application-layer firewalls

As attacks against Web servers became more common, so too did the need for a firewall that could protect servers and the applications running on them, not merelythe network resources behind them. Application-layer firewall technology first emerged in 1999, enabling firewalls to inspect and filter packets on any OSI layer up to the application layer.

The key benefit of application-layer filtering is the ability to block specific content, such as known malware or certain websites, and recognize when certain applications and protocols -- such as HTTP, FTP and DNS -- are being misused.

Firewall technology is now incorporated into a variety of devices; many routers that pass data between networks contain firewall components and most home computer operating systems include software-based firewalls. Many hardware- based firewalls also provide additional functionality like basic routing to the internal network they protect.

Proxy firewalls

Firewall proxy servers also operate at the firewall's application layer, acting as an intermediary for requests from one network to another for a specific network application. A proxy firewall prevents direct connections between either sides of the firewall; both sides are forced to conduct the session through the proxy, which can block or allow traffic based on its rule set.

Firewalls in the perimeter less age

The role of a firewall is to prevent malicious traffic reaching the resources that it is protecting. Some security experts feel this is an outdated approach to keeping information and the resources it resides on safe. Some of the firewall products that you may want to check out are:

McAfee Internet Security

Microsoft Windows Firewall

Norton Personal Firewall

Trend Micro PC-cillin

ZoneAlarm Security

UMTS TERRESTRIAL RADIO ACCESS NETWORK OVERVIEW

The UTRAN (Universal Mobile Telecommunications System**)** consists of a set of radio network subsystems (RNSs). There are two logical elements in RNS. One is node B and another is RNC.

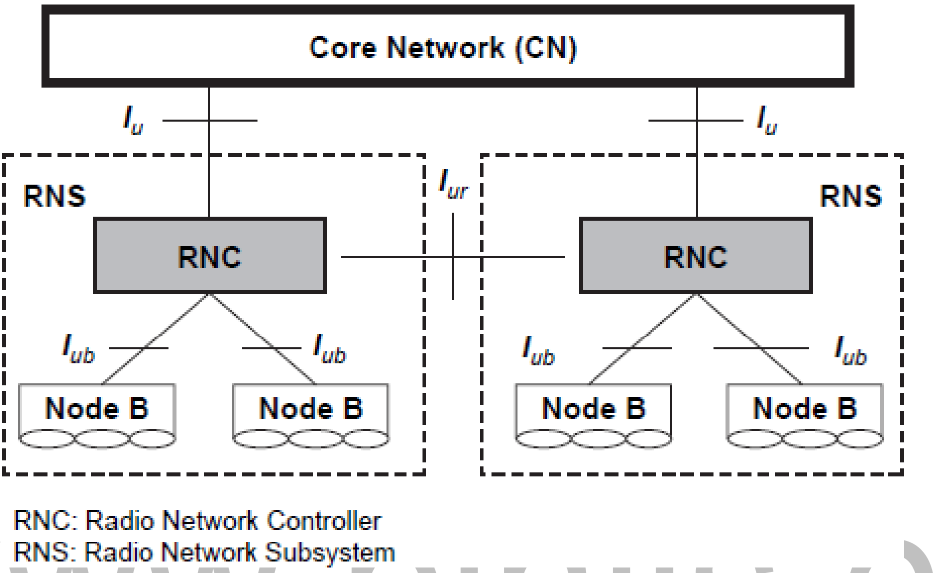


Fig.3.2 UTRAN Logical Architecture

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

Each cell consists of one group of nodes and one RNC (Radio Network Controller). The RNC is responsible for the use and allocation of all the radio resources of the RNS.

The responsibilities of RNC

This element of the UTRAN / radio network subsystem controls the Node Bs whichis connected to it, i.e. the radio resources of the domain. The RNC is responsible for the radio resource management and some of the mobility management functions. It is responsible for data encryption / decryption.

a. Intra UTRAN handover

b. Macro diversity combining/splitting of I_{ub} data streams

c. Frame synchronization

d. Radio resource management

e. Outer loop power control

f. I_u interface user plane setup

g. Serving RNS (SRNS) relocation

h. Radio resource allocation (allocation of codes, etc.)

i. Frame selection/distribution function necessary for soft handover

j. UMTS radio link control (RLC) sub layers function execution.

k. Termination of MAC, RLC, and RRC protocols for transport channels, i.e., DCH, DSCH, RACH, Fuchou's user plane protocols termination.

The Node B architecture and responsibilities:

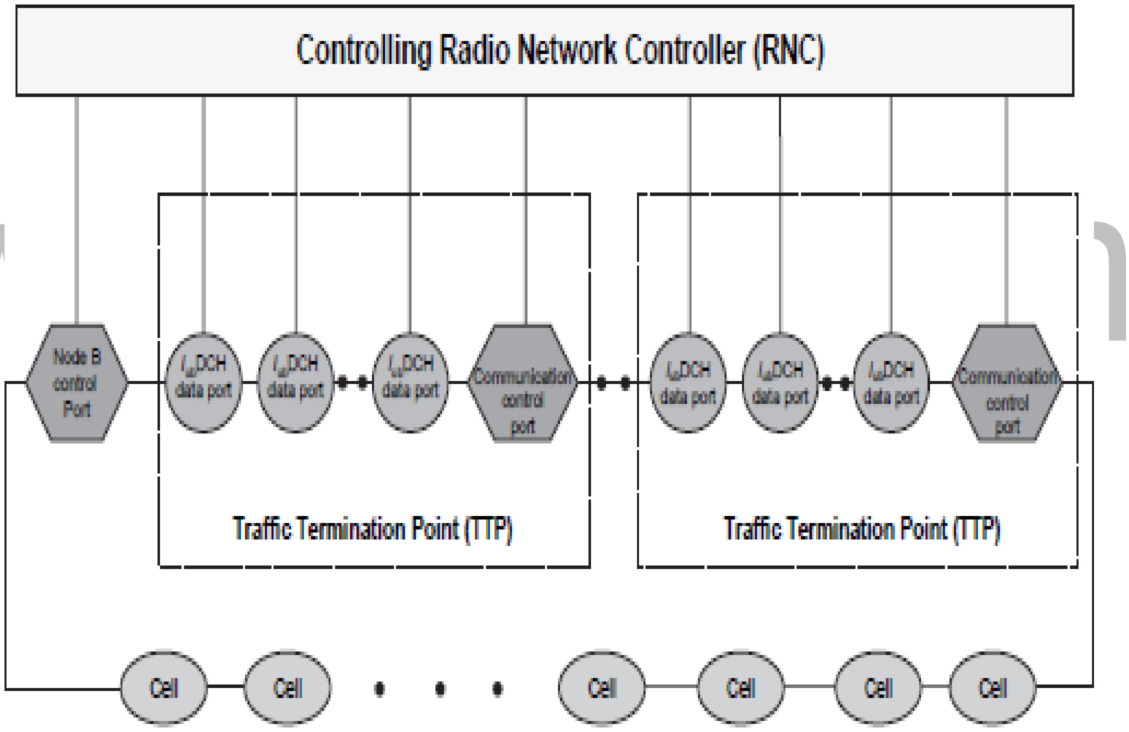


Fig.3.3 Node B logical Architecture

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

A Node B is responsible for radio transmission and reception in one or more cells to/from the user equipment (UE).

Node B denotes the base station transceiver within UMTS. It contains the transmitter and receiver to communicate with the UEs within the cell. It participates with the RNC in the resource management. Node B is the 3GPP term for base station, and often the terms are used interchangeably.

The following are the responsibilities of the Node B:
PCH Termination of I_{ub} interface from RNC

Termination of MAC protocol for transport channels RACH, FACH Termination of MAC, RLC, and RRC protocols for transport channels: BCH,

Radio environment survey (BER estimate, receiving signal strength, etc.)

Inner loop power control

Open loop power control

Radio channel coding/decoding

Macro diversity combining/splitting of data streams from its cells (sectors)

Termination of U_u interface from UE

Error detection on transport channels and indication to higher layers

FEC encoding/decoding and interleaving/deinter leaving of transport channels

Multiplexing of transport channels and de- multiplexing of coded composite transport channels

Power weighting and combining of physical channels

Modulation and spreading/demodulation and dispreading of physical channels

Frequency and time (chip, bit, slot, frame) synchronization RF processing.

UTRAN Logical Interfaces

The UTRAN protocol structure contains two main layers

The radio network layer(RNL) The

transport network layer (TNL)

Control Plane: It is used for all UMTS- specific signaling. It includes the application protocol (i.e., radio access network application part (RANAP) in I_u, radio network subsystem application part (RNSAP) in I_ur and node B application part (NBAP) in I_{ub}).

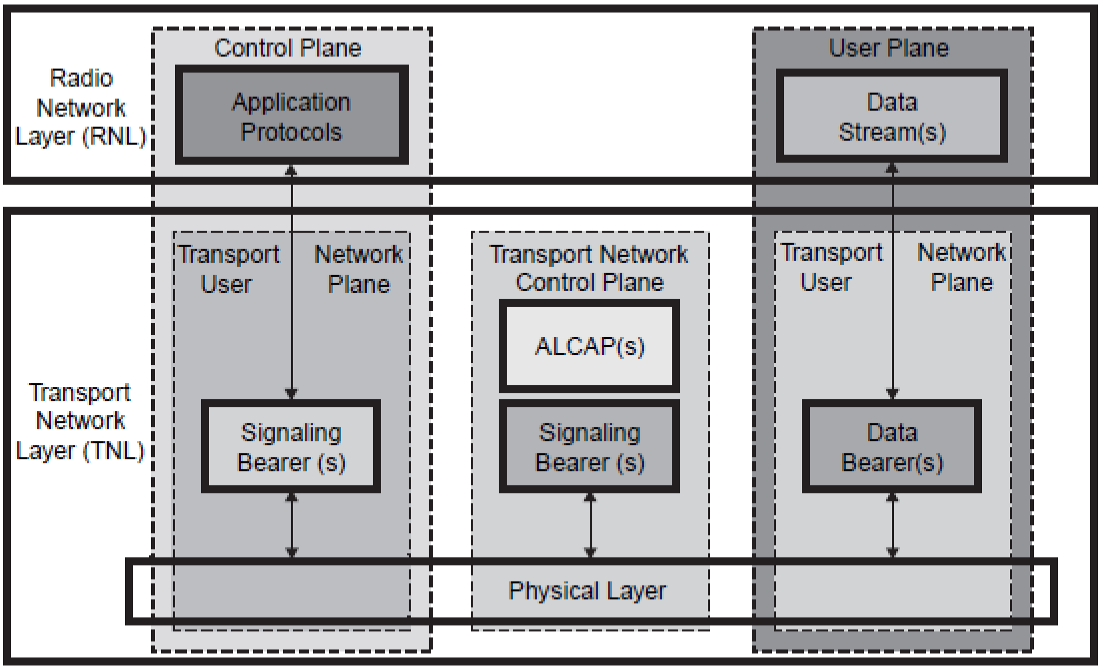


Fig.3.4 General Protocol model for UTRAN interfaces

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

User Plane:

The user plane carries the user information. It includes data streams and data bearers for data streams.

Transport network control plane:

It carries all control signaling. It contains access link control application part (ALCAP) required to set up the transport bearers (data bearers) for the user plane It also includes the signaling bearer needed for the ALCAP. The transport plane lies between the control plane and the user plane. The addition of the transport plane in UTRAN allows the application protocol in the radio network control plane to be totally independent of the technology selected for the data bearer in the user plane.lu Interface

The UMTS Iu interface connects the UTRAN to the UMTS core network (UCN). It consists of three planes.

1. Radio network control plane:

It carries information for the general control of UTRAN radio network operations.

It carries information for control of UTRAN in the context of each specific Call.

It carries user call control (CC) and mobility management (MM) signaling Messages.

2. The transport network control plane (TNCP):

It carries information for the control of transport network used within UCN.

3. User plane (UP):

It carries user voice and packet data information.

AAL2 is used for the following services: narrowband speech (e.g., EFR, AMR); unrestricted digital information service (up to 64 kbps, i.e., ISDN B channel); any low to average bit rate CS service (e.g., modem service to/from PSTN/ISDN). AAL5 is used for the following services: non-real-time PS data service (i.e., best effort packet access) and real-time PS data.

I_{ur} Interface

The I_{ur} interface allows communication between different RNCs within the UTRAN. The open I_{ur} interface enables capabilities like soft handover to occur as well as helping to stimulate competition between equipment manufacturers. **Two different protocol planes are defined for it:** Radio network control plane (RNCP) Transport network control plane (TNCP)

User plane (UP)

The I_{ur} interface is used to carry:

Information to control the radio resources in the context of specific service request of one mobile on RNCP

Information to control the transport network used within UTRAN on TNCPUser voice and packet data information on UP

The protocols used on this interface are:

Radio access network application part (RANAP)

RANAP signaling protocol resides in the control plane of Radio network layer of I interface in the UMTS (Universal Mobile Telecommunication System) protocol stack. I interface is the interface between RNC (Radio Network Controller) and CN (Core Network).

DCH frame protocol (DCHFP)

The data transfer takes place using a frame protocol. The procedures belonging to this set include establishment, modification and release of dedicated channel in the DRNC due to hard and soft handover, set-up/release of dedicated transport connections over Our interface and data transfer for dedicated channels.

RACH frame protocol (RACHFP)

A random-access channel (RACH) is a shared channel used by wireless terminals to access the mobile network (TDMA/FDMA, and CDMA based network) for call set-up and burst data transmission. Whenever mobile wants to make a MO call it schedules the RACH. RACH is transport-layer channel.

FACH frame protocol (FACHFP)

Forward Access Channel

Access link control application part (ALCAP)

Control plane protocol for the transport layer. It is used for multiplexing of different users onto one AAL2 transmission path using channel IDs (CIDs).

Signaling connection control part (SCCP)

A network layer protocol that provides extended routing, flow control, segmentation, connection-orientation, and error correction facilities in Signaling System & telecommunications networks.

Message transfer part 3-B (MTP3-B)

Signaling ATM adaptation layer for network-to-network interface (SAALNNI) (SAAL-NNI is further divided into service specific coordination function for network to network interface (SSCF-NNI), service specific connection oriented protocol (SSCOP), and ATM adaptation layer 5 (AAL5))

Basic inter-RNC mobility support

Support of SRNC relocation

Support of inter-RNC cell and UTRAN registration area update Support of inter-RNC packet paging

Reporting of protocol errors

Dedicated channel traffic support

Establishment, modification, and release of a dedicated channel in the DRNC due to hard and soft handoff in the dedicated channel state

Setup and release of dedicated transport connections across the interface Transfer of DCH transport blocks between SRNC and DRNC Management of radio links in the DRNS via dedicated measurement report procedures and power setting procedures

Common channel traffic support

Setup and release of the transport connection across the Our for common channel data streams

Splitting of the MAC layer between the SRNC (MAC-d) and DRNC (MAC-c and MAC-sh); the scheduling for downlink data transmission is performed in the DRNC

Flow control between the MAC-d and MAC-c/MAC-sh

Global resource management support

Transfer of cell measurements between two RNCs Transfer of Node B timing between two RNCs

I_{ub} Interface

The I_{ub} connects the Node B and the RNC within the UTRAN. Although when it was launched, a standardization of the interface between the controller and base station in the UTRAN was revolutionary, the aim was to stimulate competition between suppliers, allowing opportunities like some manufacturers who might concentrate just on base stations rather than the controller and other network entities.

Three different protocol planes are defined for it.

Radio network control plane (RNCP)

Transport network control plane (TNCP)

User plane (UP)

The interface is used to carry the information for the general control of Node B for radio network operation on RNCP Information for the control of radio resources in the context of specific service request of one mobile on RNCP Information for the control of a transport network used within UTRAN on TCNP User CC and MM signaling message on RNCP.

UTRA uplink & downlink

At the radio air interface and its associated properties, it is necessary to define the directions in which the transmissions are occurring. Being a full duplex system, i.e. transmitting simultaneously in both directions, it is necessary to be able to define which direction is which.

- Uplink; This may also sometimes be known as the reverse link, and it is the link from the User Equipment (UE) to the Node B or base station.
- Downlink; This may also sometimes be known as the forward link, and it is the link from the Node B or base station to the User Equipment (UE).

UTRA FDD & TDD

In view of the fact that transmissions have to be made in both directions, i.e. in both uplink and downlink. It is necessary to organize the way these transmissions are made. Two techniques are used to ensure concurrent or near concurrent transmissions in both directions: frequency division duplex and time division duplex.

UTRA-FDD: The frequency division duplex version of UTRA uses a scheme whereby transmissions in the uplink and downlink occur on different frequencies. Although this requires double the bandwidth to accommodate the two transmissions, And filters to prevent the transmitted signal from interfering with their cover. Even though there is a defined split between uplink and downlink, effective filters are required.

UTRA-TDD: The time division version of the UTRA uses uplink and downlink transmissions that use the same frequency but are timed to occur at different intervals.

Distribution of UTRAN Functions

Located in the RNC

Radio resource control (L3 Function)

Radio link control (RLC)

Macro diversity combining

Active cell set modification

Assign transport format combination set (centralized data base function)

Multiplexing/de-multiplexing of higher layer PDUs into/from transport block delivered to/from the physical layer on shared dedicated transport channels (used for soft handover)

L1 function: macro diversity distribution/combining (centralized multipoint termination)

Selection of the appropriate transport format for each transport channel depending upon the instantaneous source rate — collocate with RRCP riority handling between data flows of one user.

Located in Node B

Scheduling of broadcast, paging, and notification messages; location in Node B — to reduce data repetition over I_{ub} and reduce RNC CPU load and memory space Collision resolution on RACH (in Node B — to reduce non constructive Traffic over I_{ub} interface and reduce round trip delay) Multiplexing/de-multiplexing of higher layer PDUs to/from transport blocks delivered to/from the physical layer on common transport channels