1

UMTS Basics

UMTS is real. In a continuously growing number of countries we can walk in the stores of mobile network operators or resellers and take UMTS PC cards or even third-generation (3G) phones home and use them instantly. Every day the number of equipments and their feature sets gets broader. The "dream" of multimedia on mobile connections, online gaming, video conferencing, real-time video or even mobile TV becomes reality.

With rapid technical innovation the mobile telecommunication sector has continued to grow and evolve strongly.

The technologies used to provide wireless voice and data services to subscribers, such as Time Division Multiple Access (TDMA), Universal Mobile Telecommunications System (UMTS), and Code Division Multiple Access (CDMA), continue to grow in their complexity. This complexity imparts a time-consuming hurdle to overcome when moving from 2G to 2.5G and then to 3G networks.

GSM (Global System for Mobile Communication) is the most widely installed wireless technology in the world. Some estimates put GSM market share above 80 %. Long dominant in Europe, GSM has a foothold in Latin America and is expanding its penetration in the North American market.

One reason for this trend is the emergence of reliable, profitable 2.5G General Packet Radio Service GPRS elements and services. Adding a 2.5G layer to the existing GSM foundation has been a cost-effective solution to current barriers while still bringing desired data services to market. The enhancement to EGPRS (Enhanced GPRS) allows a maximum speed of 384 kbps. However, now EDGE (EDGE; Enhanced Data Rates for GSM Evolution) is under pressure, because High Speed Downlink Packet Access (HSDPA; see Section 1.2.3) and its speed of 2 Mbps will take huge parts of the market share once it becomes more widely available.

So, the EGPRS operators will sooner or later switch to 3G UMTS services (Figure 1.1), the latest of which is UMTS Release 7 (Rel. 7). This transition brings new opportunities and testing challenges, in terms of both revenue potential and addressing interoperability issues to ensure QoS (Quality of Service).

With 3G mobile networks, the revolution of mobile communication has begun. 4G and 5G networks will make the network transparent to the user's applications. In addition to horizontal handovers (for example between Node Bs), handovers will occur vertically between

UMTS Signaling Second Edition Ralf Kreher and Torsten Rüdebusch

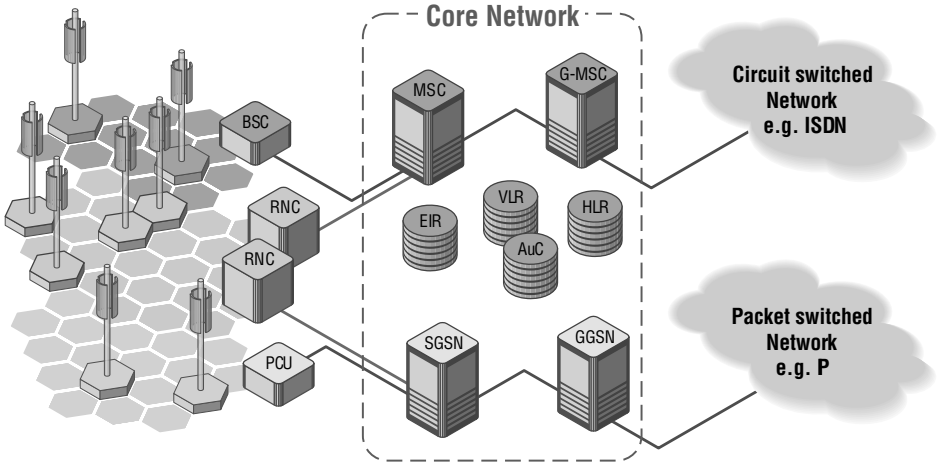


Figure 1.1 Component overview of a UMTS network.

applications, and the UTRAN (UMTS Terrestrial Radio Access Network) will be extended by a satellite-based RAN (Radio Access Network), ensuring global coverage.

Every day the number of commercial networks in different parts of the world increases. Therefore, network operators and equipment suppliers are desperate to understand how to handle and analyze UMTS signaling procedures in order to get the network into operation, detect errors, and troubleshoot faults.

Those experienced with GSM will recognize many similarities with UMTS, especially in Non-Access Stratum (NAS) messaging. However, in the lower layers within the UTRAN and Core Network (CN), UMTS introduces a set of new protocols, which deserve close understanding and attention.

The philosophy of UMTS is to separate the user plane from the control plane, the radio network from the transport network, the access network from the CN, and the Access Stratum from the Non-Access Stratum.

The first part of this book is a refresher on UMTS basics, and the second part continues with in-depth message flow scenarios.

1.1 Standards

The ITU (the International Telecommunication Union) solicited several international organizations for descriptions of their ideas for a 3G mobile network:

CWTS	China Wireless Telecommunication Standard group
ARIB	Association of Radio Industries and Businesses, Japan
T1	Standards Committee T1 Telecommunications, United States
TTA	Telecommunications Technology Association, Korea
TTC	Telecommunication Technology Committee, Japan
ETSI	European Telecommunications Standards Institute

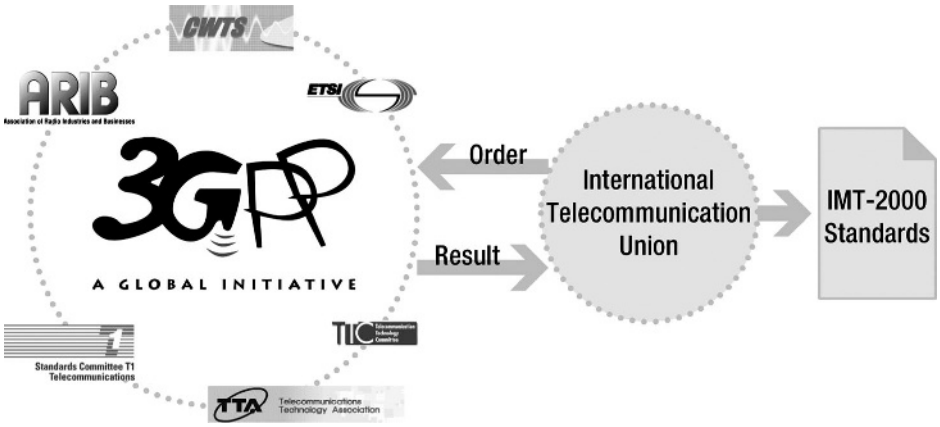


Figure 1.2 IMT-2000.

The ITU decided which standards would be used for "International Mobile Telecommunications at 2000 MHz." Many different technologies were combined in IMT-2000 standards (Figure 1.2).

The main advantage of IMT-2000 is that it specifies international standards and also the interworking with existing PLMN (Public Land Mobile Network) standards, such as GSM.

In general, the quality of transmission will be improved. The data transfer rate will increase dramatically. Transfer rates of 384 kbps are already available; 2 Mbps (with HSDPA technology) is under test and almost ready to go live in certain parts of Asia. New service offerings will help UMTS to become financially successful for operators and attractive to users.

The improvement for the users will be the worldwide access available with a cell phone, and the look and feel of services will be the same wherever the user may be (Figure 1.3).

There is a migration path from 2G to 3G systems that may include an intermediate step, the so-called 2.5G network. Packet switches –Gateway GPRS Support Node (GGSN) or Serving GPRS Support Node (SGSN) in the case of a GSM network – are implemented in the existing CN while the RAN is not changed significantly (Figure 1.4).

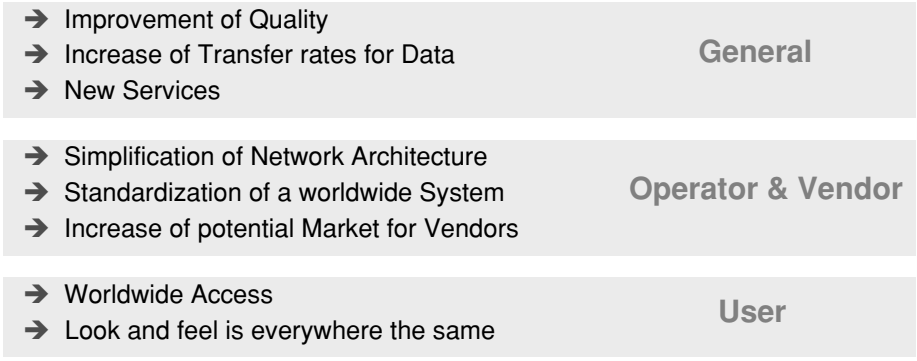


Figure 1.3 IMT-2000 standards benefit users, operators, and vendors.

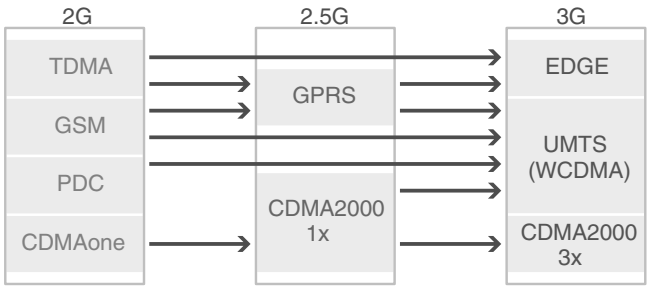


Figure 1.4 Possible migration paths from 2G to 3G.

In the case of a migration from GSM to UMTS a new Radio Access Technology (RAT; W-CDMA instead of TDMA) is introduced. This means the networks will be equipped with completely new RANs, which replace the 2G network elements in the RAN. However, EDGE opens a different way to offer high-speed IP services to GSM subscribers without introducing W-CDMA.

The existing CDMA cellular networks, which are especially popular in the Americas, will undergo an evolution to become CDMA2000 networks with larger bandwidth and higher data transmission rates.

1.2 Network Architecture

UMTS maintains a strict separation between the radio subsystem and the network subsystem, allowing the network subsystem to be used with other RATs. The CN is adopted from GSM and consists of two user traffic-dependent domains and several commonly used entities. Traffic-dependent domains correspond to the GSM or GPRS CNs and handle:

- circuit-switched-type traffic in the CS domain;
- packet-switched-type traffic in the PS domain.

Both traffic-dependent domains use the functions of the remaining entities – the Home Location Register (HLR) together with the Authentication Center (AuC), or the Equipment Identity Register (EIR) – for subscriber management, mobile station roaming and identification, and handling different services. Thus the HLR contains GSM, GPRS, and UMTS subscriber information.

Two domains handle their traffic types at the same time for both the GSM and the UMTS access networks. The CS domain handles all circuit-switched traffic for the GSM as well as for the UMTS access network; similarly, the PS domain takes care of all packet-switched traffic for both the access networks.

1.2.1 GSM

The second generation of PLMN is represented as a Subsystem by a GSM network consisting of a Network Switching Subsystem (NSS) and a Base Station Subsystem (BSS) (Figure 1.5).

The first evolution step (2.5G) is a GPRS PLMN connected to a GSM PLMN for packet-oriented transmission.

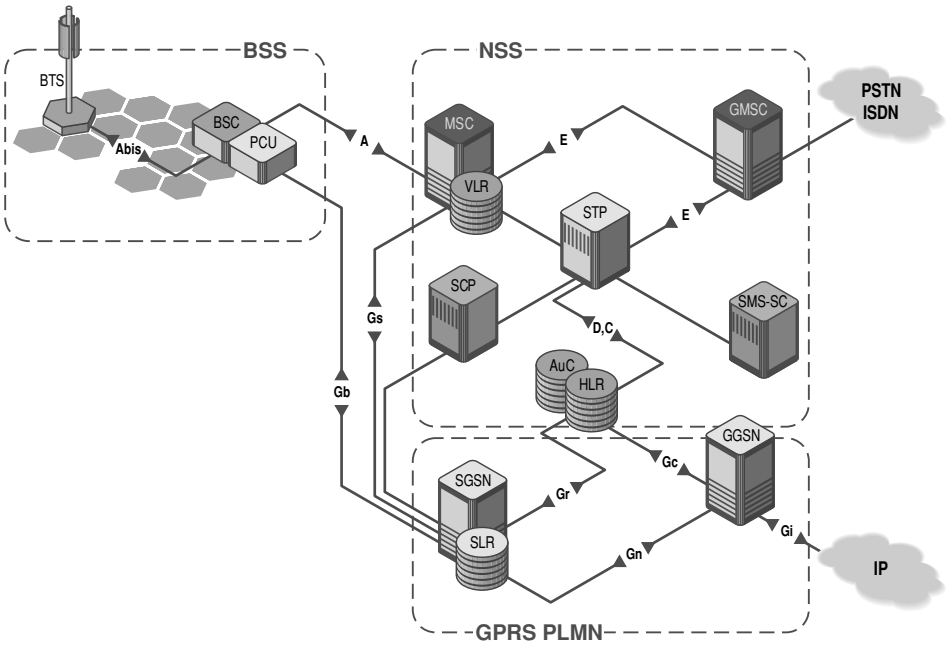


Figure 1.5 GSM network architecture. HLR: Home Location Register; SGSN: Serving GPRS Support Node with Location Register Function; GGSN: Gateway GPRS Support Node; AuC: Authentication Center; SCP: Service Control Point; SMSC: Short Message Service Center; CSE: CAMEL Service Entity (Customized Application for Mobile network Enhanced Logic).

The main element in the NSS is the Mobile Switching Center (MSC), which contains the Visitor Location Register (VLR). The MSC represents the edge toward the BSS and on the other side as the Gateway MSC (GMSC), the connection point to all external networks, such as the Public Switched Telephone Network (PSTN) or Integrated Services Digital Network (ISDN). GSM is a circuit-switched network, which means that there are two different types of physical links to transport control information (signaling) and traffic data (circuit). The signaling links are connected to Signaling Transfer Points (STP) for centralized routing whereas circuits are connected to special switching equipment.

The most important entity in the BSS is the Base Station Controller (BSC), which, along with the Packet Control Unit (PCU), serves as the interface with the GPRS PLMN. Several Base Transceiver Stations (BTS) can be connected to the BSC.

1.2.2 UMTS Release 99

Figure 1.6 shows the basic structure of a UMTS Release 99 network. It consists of two different radio access parts (BSS and UTRAN) and the CN parts for circuit-switched (e.g. voice) and packet-switched (e.g. email download) applications.

To implement UMTS means to set up a UTRAN, which is connected to a circuit-switched CN (GSM with MSC/VLR) and to a packet-switched CN (GPRS with SGSN). The interfaces are named Iu, where IuCS goes to the MSC and IuPS goes to the SGSN. Alternatively, the

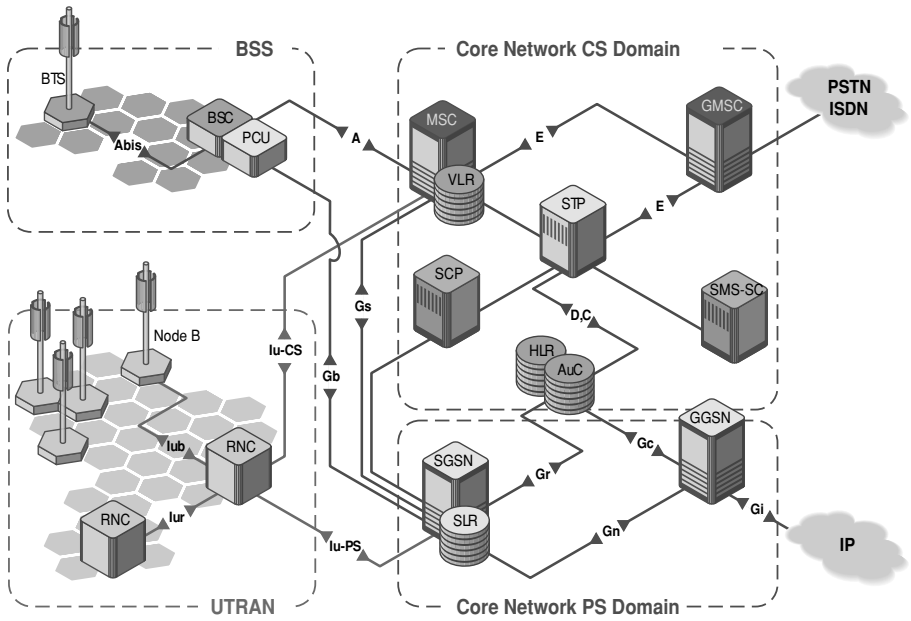


Figure 1.6 UMTS Rel. 99 network architecture.

circuit and packet network connections could also be realized with a UMSC (UMTS MSC), which combines MSC and SGSN functionalities in one network element.

The corresponding edge within UTRAN is the Radio Network Controller (RNC). Other than in the BSS the RNCs of one UTRAN are connected with each other via the Iur interface.

The base stations in UMTS are called *Node B*, which is just its working name and has no other meaning. The interface between Node B and RNC is the Iub interface.

Release 99 (sometimes also named Release 3) specifies the basic requirements to roll out a 3G UMTS RAN. All following releases introduce a number of features that allow operators to optimize their networks and offer new services. A real network environment in the future will never be designed strictly following any defined release standard. Rather it must be seen as a kind of patchwork that is structured following the requirements of network operators and service providers. So it is possible to introduce, e.g., HSDPA, which is a feature clearly defined in Rel. 5 in combination with a Rel. 99 RAN.

In addition, it must be kept in mind that owing to changing needs of operators and growing experience of equipment manufacturers, every three months (four times per year!) all standard documents of all releases are revised and published with a new version. So development of Rel. 99 standards is not even finished yet.

It might also be possible that in later standard versions the introduction of features promised in earlier versions is delayed. This happened, for instance, in the definition of the Home Subscriber Server (HSS), which was originally introduced in early Rel. 4 standards, but then delayed to be defined in detail in Rel. 5.

The feature descriptions for higher releases in the following sections are based on documents not older than the 2004–06 revision.

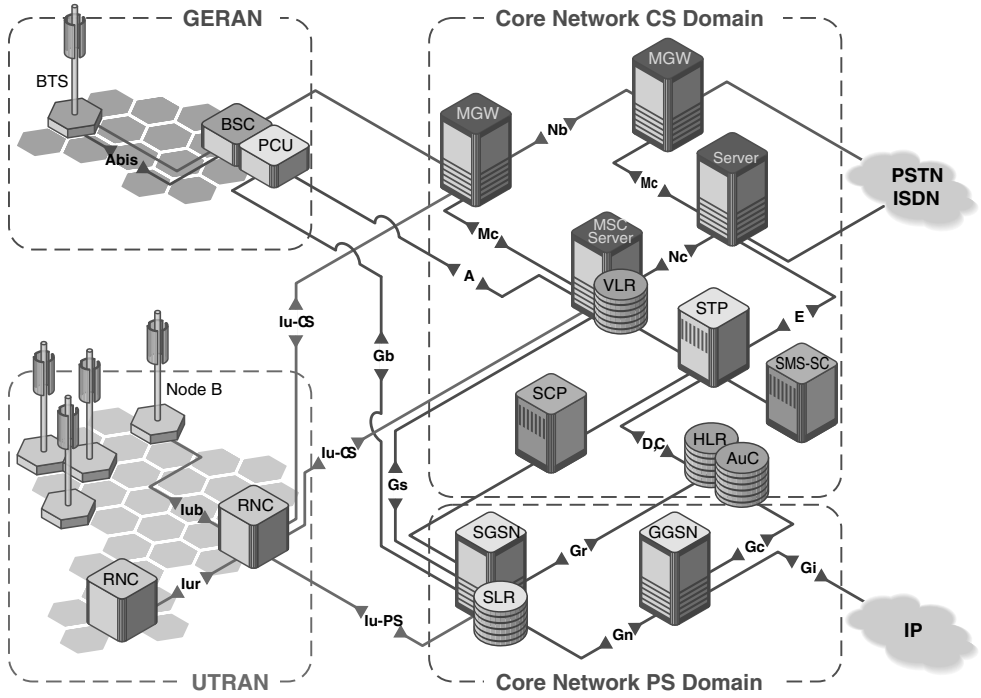


Figure 1.7 UMTS Rel. 4 network architecture.

1.2.3 UMTS Release 4

3GPP Release 4 introduces some major changes and new features in the CN domains and the GERAN (GPRS/EDGE Radio Access Network), which replaces GSM BSS (Figure 1.7). Some of the major changes are:

- Separation of transport bearer and bearer control in the CS CN.
- Introduction of new interfaces in the CS CN.
- ATM (Asynchronous Transfer Mode; AAL2, ATM Adaptation Layer Type 2) or IP (Internet Protocol) can now be used as the data transport bearer in the CS domain
- Introduction of low chiprate (also called narrowband) TDD (Time Division Duplex) describes the RAT behind the Chinese TD-SCDMA standard while UMTS TDD (wideband TDD, TD-CDMA) is seen as the dominating TDD technology in European and Asian standards outside China. It is expected that interference in low chiprate TDD has less impact on cell capacity compared to the same effect in wideband TDD. In addition, low chiprate TDD equipment will support advanced radio transmission technologies such as "smart antennas" and beamforming, which allows pointing a single antenna or a set of antennas at the signal source to reduce interference and improve communication quality.
- IP-based Gb interface.
- IPv6 support (optional).

The new features and services are (in no specific order):

- Multimedia services in the CS domain.
- Handover of real-time applications in the PS domain.
- UTRAN transport evolutions:
  - AAL2 connection QoS optimization over Iub and Iur interfaces;
  - Transport bearer modification procedure on Iub, Iur, and Iu interfaces.
- IP transport of CN protocols.
- Radio interface improvements:
  - UTRA repeater specification;
  - DSCH power control improvement.
- Radio Access Bearer (RAB) QoS negotiation over Iu interface during relocation.
- RAN improvements:
  - Node B synchronization for TDD;
  - RAB support enhancement.
- Transparent end-to-end PS mobile streaming applications.
- Emergency call enhancements for CS-based calls.
- Bearer independent CS architecture.
- Real-time facsimile.
- Tandem free operation.
- Transcoder free operation.
- ODB (Operator Determined Barring) for packet-oriented services.
- Multimedia Messaging Service.
- UICC/(U)SIM enhancements and interworking.
- (U)SIM toolkit enhancements:
  - USAT local link;
  - UICC Application Programming Interface (API) testing.
  - Protocol standardization of a SIM Toolkit Interpreter.
- Advanced Speech Call Items enhancements.
- Reliable QoS for PS domain.

The main trend in Rel. 4 is the separation of control and services of CS connections and at the same time the conversation of the network to be completely IP-based. In CS CN the user data flow will go through the Media Gateway (MGW), which are elements maintaining the connection and performing switching functions when required (bearer switching functions of the MSC are provided by the MGW). The process is controlled by a separate element evolved from MSC/VLR called the MSC Server (control functions of the MSC are provided by the MSC Server and also contains the VLR functionality), which, in terms of voice over IP networks, is a signaling gateway. One MSC Server controls numerous MGWs. To increment control capacities, a new MSC Server will be added. To increase the switching capacity, MGWs have to be added.

1.2.4 UMTS Release 5

In 3GPP Release 5, the UMTS evolution continues. The shift to an all IP environment will be realized: all traffic coming from UTRAN is supposed to be IP-based (Figure 1.8). By changing GERAN, the BSC will be able to generate IP-based application packets. That is why the

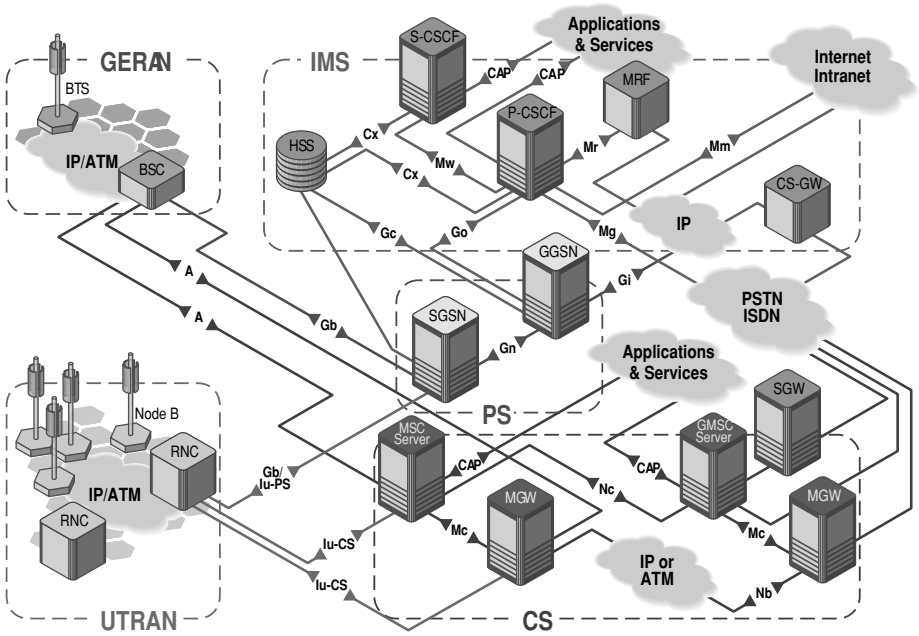


Figure 1.8 UMTS Rel. 5 basic architecture.

circuit-switched CN will no longer be part of UMTS Rel. 5. All interfaces will be IP-based rather than ATM-based.

The databases known from GSM/GPRS will be centralized in an HSS. Together with value-added services and CAMEL, it represents the Home Environment (HE). CAMEL could perform the communication with the HE completely. When the network has moved toward IP, the relationship between circuit- and packet-switched traffic will change. The majority of traffic will be packet-oriented because some traditionally circuit-switched services, including speech, will become packet-switched (VoIP). To offer uniform methods of IP application transport, Rel. 5 will contain an IP Multimedia Subsystem (IMS), which efficiently supports multiple media components, e.g. video, audio, shared whiteboards, etc.

HSDPA will provide data rates of up to 10 Mbps in downlink direction and lower rates in uplink (e.g. Internet browsing or video on demand) through the new High Speed Downlink Shared Channel (HS-DSCH) (for details see *3GPP 25.855*).

New in Release 5

- All network node interfaces connected to IP network.
- HSS replaces HLR/AuC/EIR.
- IMS:
  - Optional IPv6 implementation;
  - Session Initiation Protocol (SIP) for CS signaling and management of IP multimedia sessions;
  - SIP supports addressing formats for voice and packet calls and number translation requirements for SIP **<->** E.164.

- HSDPA integration:
  - Data rates of up to 10 Mbps in downlink direction; lower rates in uplink (e.g. Internet browsing or video on demand);
  - New HS-DSCH.
- All voice traffic is voice over packet.
- MGW required at Point of Interconnection (POI).
- SGW (Signaling Gateway; MSC Server) translates signaling to "legacy" (SS7) networks.
- AMR-WB, an enhanced Adaptive Multirate (Wideband) codec for voice services.
- New network element MRF (Media Resource Function):
  - Part of the Virtual Home Environment (VHE) for portability across network boundaries and between terminals. Users experience the same personalized features and services in whatever network and whatever terminal;
  - Very similar in function to an MGCF (Media Gateway Control Function) and MGW using H.248/MEGACO to establish suitable IP or SS7 bearers to support different kinds of media streams.
- New network element CSCF (Call Session Control Function):
  - Provides session control mechanisms for subscribers accessing services within the IM (IP Multimedia) CN;
  - CSCF is a SIP Server to interact with network databases (e.g. HSS for mobility and AAA (Authorization, Authentication, and Accounting) for security).
- New network element SGW:
  - In CS domain the user signaling will go through the SGW, which is the gateway for signaling information to/from the PSTN.
- New network element CS-GW (Circuit-Switched Gateway):
  - The CS-GW is the gateway from the IMS to/from the PSTN (e.g. for VoIP calls).
- Location services for PS/GPRS.
- IuFlex:
  - Breaking hierarchical mapping of RNCs to SGSNs (MSCs).
- Wideband AMR (new 16-kHz codec).
- End-to-end QoS in the PS domain.
- GTT: Global Text Telephony (service for handicapped users).
- Messaging and security enhancements.
- CAMEL Phase 4:
  - New functions such as mid call procedures, interaction with optimal routing, etc.
- Load sharing:
  - UTRAN (Radio Network for W-CDMA);
  - GERAN (radio network for GSM/EDGE);
  - W-CDMA in 1800/1900-MHz frequency spectrums;
  - Mobile Execution Environment (MExE) support for Java and WAP applications.

IP Multimedia Subsystem (IMS)

The IMS is a standardized architecture for fixed and mobile multimedia services. It is completely IP based and uses a 3GPP version of Voice over IP (VoIP) together with SIP. Additionally it supports all existing phone systems.

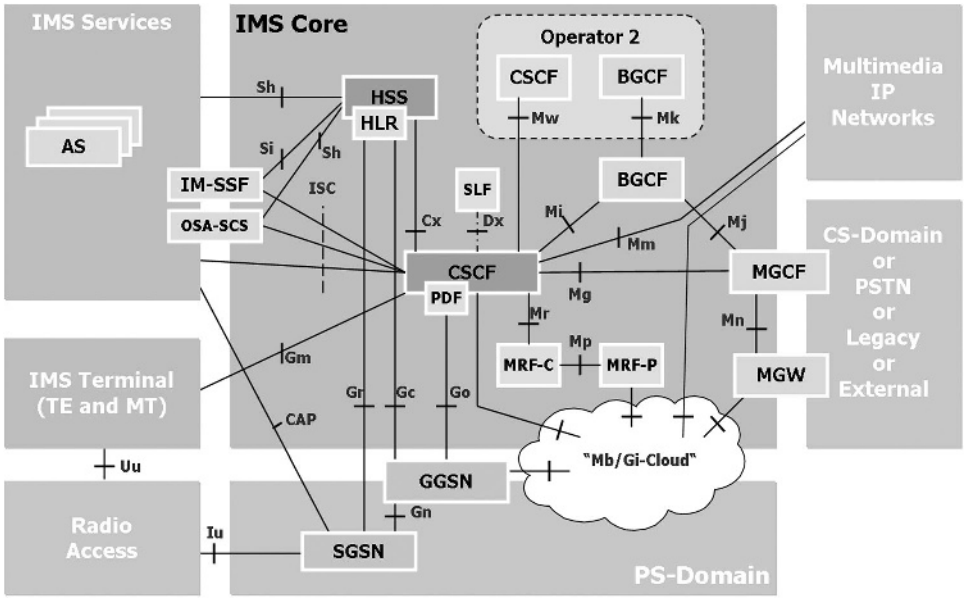


Figure 1.9 Overview of IMS architecture.

The IMS will support all current and future services communication networks. All services can easily be controlled and charged with this approach. Users can access their services in their home networks and when roaming.

As the complete IMS is based on IP it really merges cellular networks with all kinds of internet and multimedia services.

The Proxy-Call State Control Function (P-CSCF) is located together with the GGSN in the same network. Its main task is to select the I-CSCF in the user's home network and do some basic local analysis, e.g. QoS surveillance or number translation.

The Interrogating-CSCF (I-CSCF) provides access to the user's home network and selects the S-CSCF (in the home network, too).

The Serving-CSCF (S-CSCF) is responsible for the Session Control, handles SIP requests, and takes care of all necessary procedures, such as bearer establishment between home and visited network.

The HSS is the former HLR. It was renamed to emphasize that the database not only contains location-related, but also subscription-related data (subscribed services and their parameters, etc.) too (Figure 1.9).

IMS Protocols

- **SIP** (Session Initiation Protocol) is a text-based protocol that provides call signaling, registration, status, control, and security.
- **SDP** (Session Description Protocol) is embedded in order to share endpoint media capabilities.

- **Diameter** is an evolution of RADIUS for Authentication, Authorization, and Accounting. A peer-to-peer protocol specified as a base protocol and a series of applications.
- **H.248** is a device control protocol that grew out of MGCP. Available as a binary or text implementation. It instructs MGWs to setup and teardown voice calls and manages media resources (available circuits and IP ports) and signals endpoint events to the MG (e.g. off-hook, on-hook).
- **COPS** is a protocol used to transmit media-level access control and QoS policy information. (It is used on the Go interface between the GGSN and the Packet Data Function (PDF).)
- **RTP** (Real-time Transport Protocol) and **RTCP** (Real-Time Control Protocol) provide transport of media streams.

1.2.5 HSPA

A few years ago, UMTS technology was at the early deployment. Now, UMTS is a mainstream technology, with suitable handsets available in the mid- and low-price range. 3G network operators are searching for ways to satisfy an increasing number of 3G subscribers and especially to improve the user's experience. They have to improve the capacity of 3G networks and support higher data rates than 384 kbps supported by Rel. 99 UMTS. The solution for these needs were the enhancements included in 3GPP Rel. 5 known as HSDPA (High Speed Downlink Packet Access). However, the higher download speed was not enough. With an increasing number of interactive services the need for improved uplink capacity grew. 3GPP Rel. 6 addressed that with the standardization HSUPA (High Speed Uplink Packet Access). Both HSDPA and HSUPA introduce new functions to the radio access network (UTRAN). Node Bs and RNCs have to be upgraded (Figure 1.11).

HSDPA

A packet-based data service with data speed of up to 1.2–14.4 Mbps (and 20 Mbps for MIMO systems) over a 5-MHz bandwidth in downlink. Major enhancements are the new transport channel (HS-DSCH) and two control channels for the uplink and downlink (High-Speed Dedicated Physical Control Channel, HS-DPCCH; High-Speed Shared Control Channel, HS-SCCH – see Figure 1.10/Table 1.1 and Figure 1.13 for the protocol architecture):

- HS-SCCH is a downlink channel, which is used to provide control information associated with the High Speed Physical Downlink Shared Channel (HS-PDSCH). It includes information such as the identity of the mobile terminal for which the next HSDPA subframe is intended, channel code set information, and modulation scheme to be used for decoding the HS-DSCH subframes.
- HS-DPCCH is an uplink control channel, which is used to convey channel quality information (carried by CQI – Channel Quality Indicator – bits) as well as ACK/NACK messages related to the HARQ operation in the Node B.
- HS-DSCH is a shared channel that can be used by several users simultaneously, especially useful for applications with a bursty traffic profile. This new transport channel impacts the protocol layers; most significantly the physical and the MAC layer.

The enhanced throughput capabilities of HSDPA are mainly achieved by:

- Adaptive Modulation and Coding (AMC) scheme: Modulation method and coding rates are selected based on channel conditions (provided by the terminal and Node B).

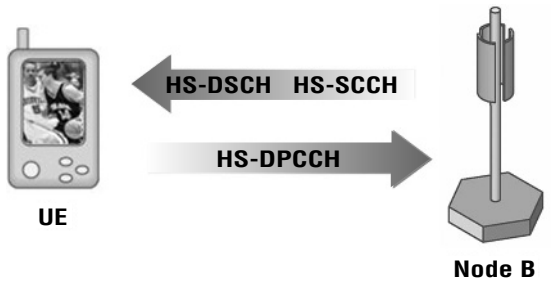


Figure 1.10 HSDPA – New transport and physical channels.

- 16ary Quadrature Amplitude Modulation (16QAM) for downlink is a higher order modulation method for data transmission under good channel conditions (QPSK was already specified for use in WCDMA).
- Hybrid Automatic Repeat reQuest (HARQ): Handles re-transmissions and guarantees error-free data transmission. HARQ is a key element of the new MAC entity (MAChs). It is located both in the Node B and in the User Equipment (UE).
- Fast packet scheduling algorithm: A Node B functionality that allocates HS-DSCH resources to different users.

Former RLC protocol and SRNC functions have been moved into the MAC protocol layer and the Node B. A proximity of time-critical functions (HARQ processing; packet scheduling) to the air interface is crucial. The Transmission Time Interval (TTI) is specified at only 2 ms, so that re-transmissions, modulation changes, and coding rate adaptations take place in that interval. This needs high performance Node Bs for a fast reaction to varying channel conditions.

MAC Layer

Different MAC entities exist for different transport channel classes. 3GPP Rel. 99 defines dedicated and common transport channels, which reflects in MAC-d and MAC-c entities. In

Table 1.1 HSDPA transport and physical channels

	Abbreviation	Name	Function
Downlink	HS-DSCH	High-Speed Downlink Shared Channel	Common transport channel for U-plane traffic
	HS-SCCH	High-Speed Shared Control Channel	Common control channel including information such as user equipment identity
Uplink	HS-DPCCH	High-Speed Dedicated Physical Control Channel	Feedback channel for HARQ, ACK/NACK messages as well as for channel quality information

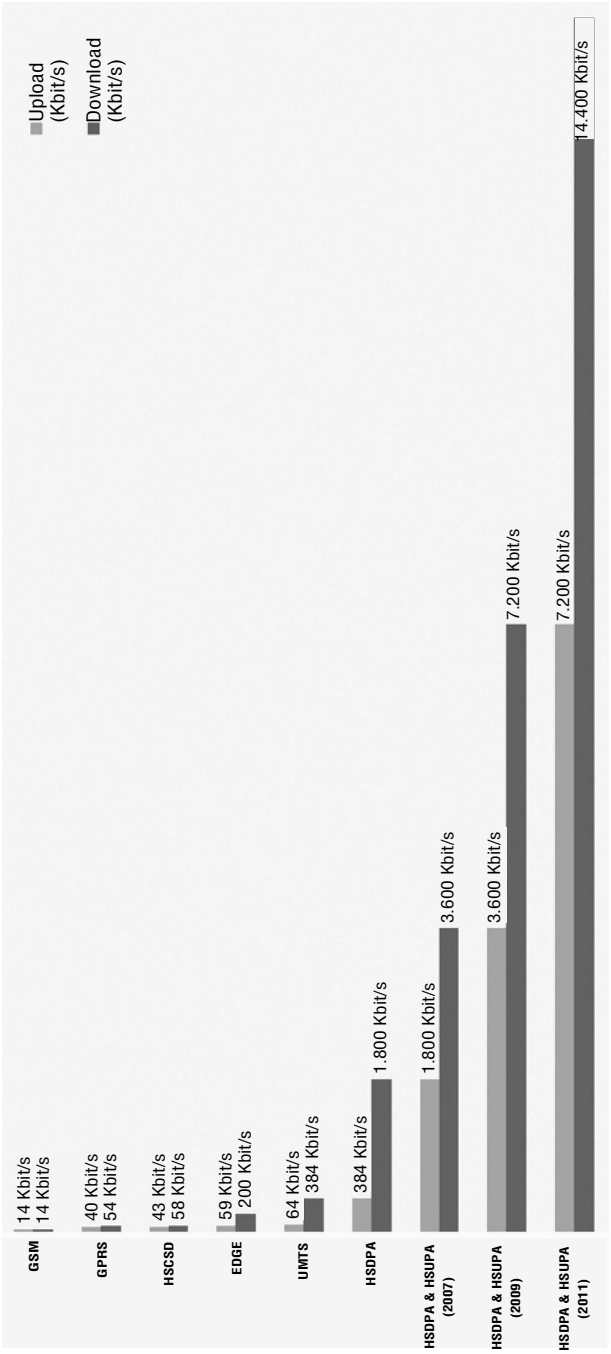


Figure 1.11 Technology datarate comparison in up- and downlink.

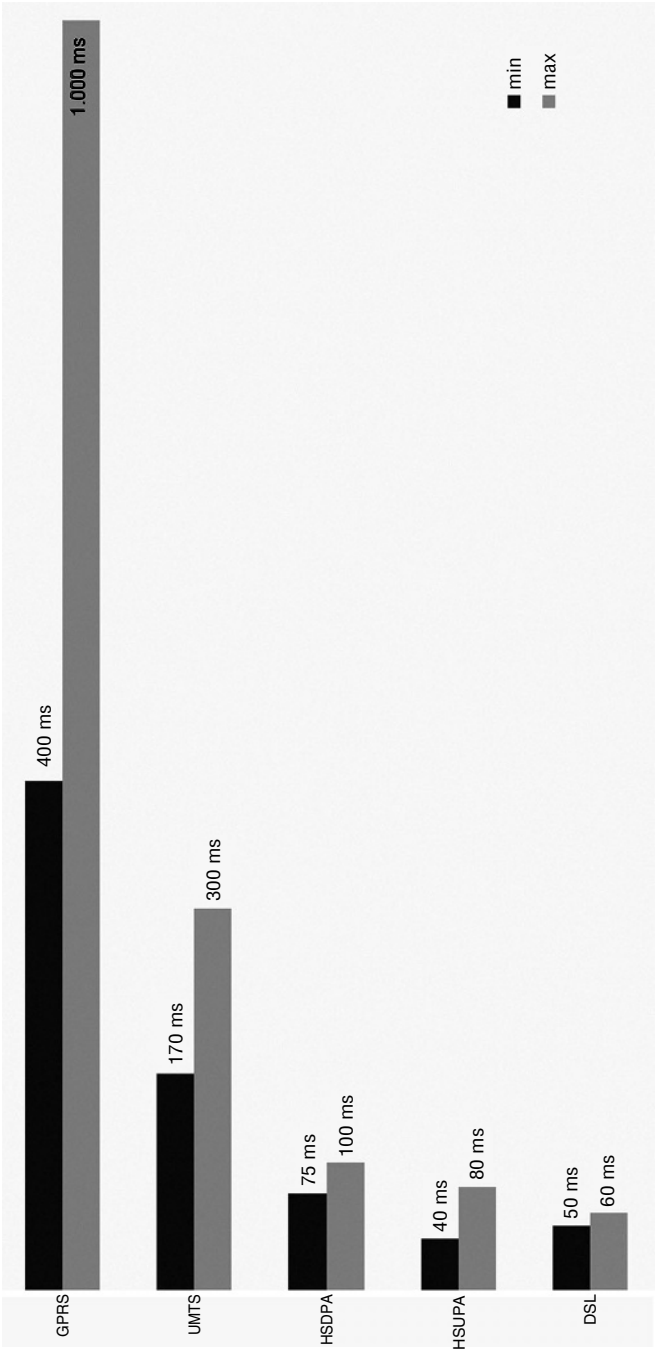


Figure 1.12 Reduced latency (TTI) in the different mobile technologies.

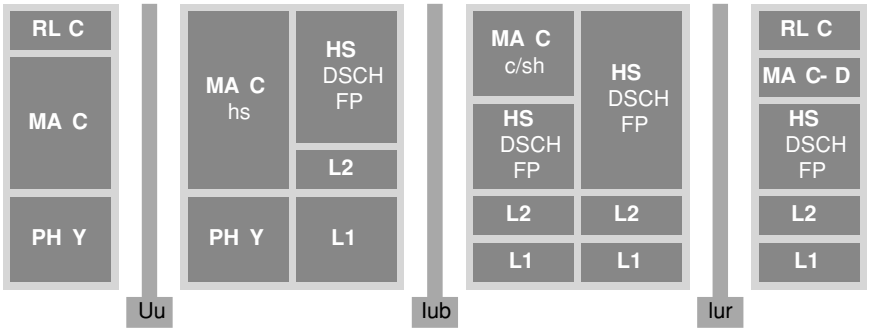


Figure 1.13 HSDPA protocol architecture.

HSDPA there is a new entity, the MAC-hs. It is used in the Node B to ensure a high performance. MAC-hs handles layer-2 functions of the HS-DSCH and includes:

- HARQ protocol handling, including generation of ACK and NACK messages.
- Re-ordering of out-of-sequence subframes. (Normally a function of the RLC protocol, but not implemented for HS-DSCH. MAC-hs handles the critical RLC tasks; subframes may arrive out of sequence as a result of the re-transmission activity of the HARQ processes.)
- Multiplexing and de-multiplexing of multiple MAC-d flows onto/from one MAC-hs stream
- Downlink packet scheduling.

Control Plane

HSDPA requires modifications of the UTRAN. Some examples are:

- Radio Resource Control (RRC) protocol, responsible for different UTRAN specific functions (e.g. radio bearer management).
- Node-B Application Part (NBAP) enables the RNC to manage resources in the Node-B; the HS-DSCH is an additional Node-B resource, which is managed by the NBAP protocol, too.
- Radio Network Subsystem Application Part (RNSAP), on the Iur interface between two RNCs is adopted, as in HSDPA resources in the Node B, is managed by a Serving RNC which is different from the Node B's Controlling RNC.

User Plane

Relevant in the user plane for the HS-DSCH transport blocks is the HS-DSCH Frame Protocol (HS-DSCH FP). It controls the 'packaging' of Transport Blocks (basic data unit from MAC to physical layer) into a transmission format for the UTRAN network (ATM-based in 3GPP Rel. 99). Additionally Node B and transport channel synchronization is supported. The flow control of MAC-d Packet Data Units (PDUs) in the HS-DSCH between RNC and Node B is achieved by dedicated HS-DSCH FP messages (Figure 1.14).

A Capacity-Request goes from RNC to Node B. It indicates "data ready for transmission". The Node B answers with a Capacity-Allocation message. It contains a number (if any) of

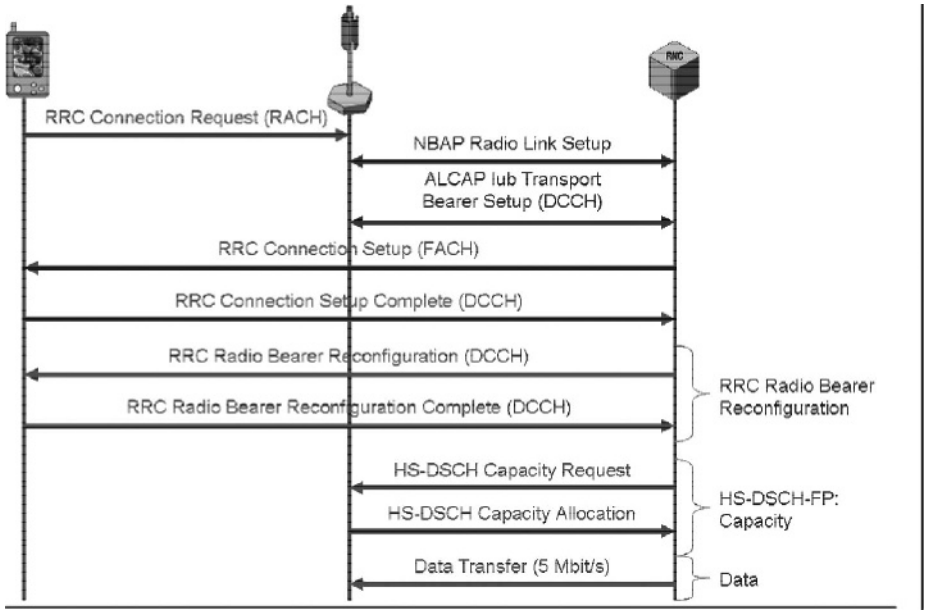


Figure 1.14 Signaling over HS-DSCH.

allowed MAC-d PDUs to be sent to the RNC in a given time period, depending on the current buffer status.

HSUPA

Improves the uplink data rates and reduce the delays (TTI/latency) in dedicated channels in the uplink (Figure 1.12). (This is a vital feature for all online gamers.) A new transport channel, the Enhanced Dedicated Channel (E-DCH) introduces five new physical layer channels. It achieves a theoretical maximum uplink data rate of 5.6 Mbps. The E-DCH relies on improvements implemented both in the PHY and the MAC layer. However, HSUPA does not introduce a new modulation scheme but relies on the use of Quadrature Phase Shift Keying (QPSK), an existing modulation scheme specified for Wideband Code Division Multiple Access (WCDMA).

The Enhanced HARQ Acknowledgment Indicator Channel (E-HICH) is similar to the HS-DPCCH in HSDPA. It provides HARQ feedback information (ACK/NACK), but does not contain CQI information, as HSUPA does not support Adaptive Modulation and Coding. The Node B contains an uplink scheduler for HSUPA in the same way as in HSDPA, even though the goal of the scheduling is different. In HSDPA the HS-DSCH allocates resources (time slots and codes) to multiple users. The uplink scheduler allocates only the capacity (transmit power) to each E-DCH user, which avoids a "power-overload".

The Enhanced Dedicated Physical Data Channel (E-DPDCH) is the physical channel of the E-DCH for transmission of user data. In uplink the Enhanced Dedicated Physical Control

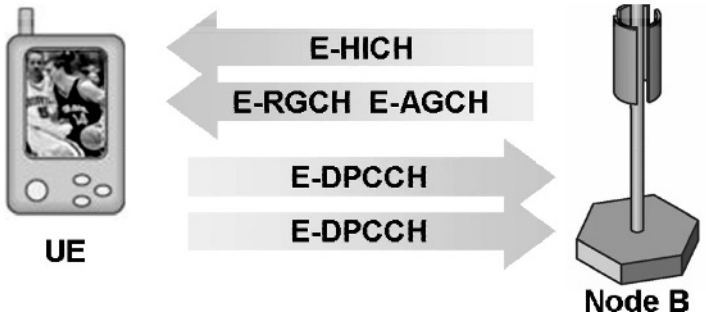


Figure 1.15 HSUPA new transport and physical channels.

Channel Control channel (E-DPCCH) associates with the E-DPDCH and provides information to the Node B on how to decode the E-DPDCH (Figure 1.15/Table 1.2).

The transmit power of a UE is directly related to the information transmission data rate as a result of the spreading operation inherent with WCDMA.

Many UEs transmitting at the same time cause interference for each other. The Node B tolerates a maximum amount of interference before it is no longer able to decode the transmissions of individual UEs.

The E-DCH is a dedicated channel, so multiple UEs might be transmitting at the same time, causing interference at the Node B. Therefore it regulates the power level of the individual UEs. This transmit power regulation controls the uplink capacity for each UE, so it is basically a very fast power control mechanism. The scheduling channels E-RGCH (Enhanced Relative Grant Channel) and E-AGCH (Enhanced Absolute Grant Channel) control how a UE regulates

Table 1.2 E-DCH transport and physical channel definition

	Abbreviation	Name	Function
Uplink	E-DPDCH	Enhanced Dedicated Physical Data Channel	Physical channel used by the E-DCH for the transmission of user data
	E-DPCCH	Enhanced Dedicated Physical Control Channel	Control channel associated with the E-DPDCH providing information to the Node B on how to decode the E-DPDCH
Downlink	E-AGCH	Enhanced Absolute Grant Channel	Provides an absolute power level above the level for the DPDCH (associated with a DCH) that the UE should adopt
	E-RGCH	Enhanced Relative Grant Channel	Indicates to the UE whether to increase, decrease, or keep unchanged the transmit power level of the E-DCH
	E-HICH	Enhanced HARQ Acknowledgement Indicator Channel	Used by Node B to send HARQ ACK/NACK messages back to the UE

its transmit power level. On the one hand the E-RGCH can "instruct" the UE either to increase or decrease the transmit power level by one step, or to keep the current transmit power level. On the other hand the E-AGCH demands an absolute value for the power level of the E-DCH at which the UE is allowed to transmit.

MAC Layer

In addition to the new physical channels, the E-DCH includes new MAC entities for the UE, Node B and SRNC (MAC-e and MAC-es; mapped onto network elements):

- MAC-e is included in the UE and in Node B with the main function involving the handling of HARQ retransmissions and scheduling. This low-level MAC layer is very close to the physical layer.
- MAC-es is implemented in the UE and SRNC. In the UE, it is partially responsible for multiplexing multiple MAC-d flows onto the same MAC-es stream. In the SRNC, it takes care of:
  – in-sequence delivery of MAC-es PDUs;
  – de-multiplexing of the MAC-d flows;
  – distribution of these flows into individual queues according to their QoS characteristics.

MAC-d flows correspond to individual Packet Data Protocol (PDP) contexts at the Iu-PS interface with different QoS profiles (e.g. streaming vs. background). The MAC layer for E-DCH is split between the Node B and the SRNC, because it supports soft handover. Additionally the E-DCH supports a TTI of 2 ms and/or 10 ms (HS-DSCH mandates a TTI of 2 ms). While the Node B takes care of time-critical functions (HARQ processing, scheduling), MAC-es takes care of in-sequence delivery of MAC-es frames, coming from different Node Bs currently serving the UE.

Table 1.3 Feature comparison between HSDPA and HSUPA

Feature	HSDPA	HSUPA
Peak data rate	14.4 Mbps	5.6 Mbps
Modulation scheme(s)	QPSK, 16QAM	QPSK
TTI	2 ms	2 ms (optional)/10 ms
Transport channel type	Shared	Dedicated
Adaptive Modulation and Coding (AMC)	Yes	No
HARQ	HARQ with incremental redundancy; Feedback in HS-DPCCH	HARQ with incremental redundancy; Feedback in dedicated physical channel (E-HICH)
Packet scheduling	Downlink scheduling (for capacity allocation)	Uplink scheduling (for power control)
Soft handover support (U-Plane)	No (in the downlink)	Yes

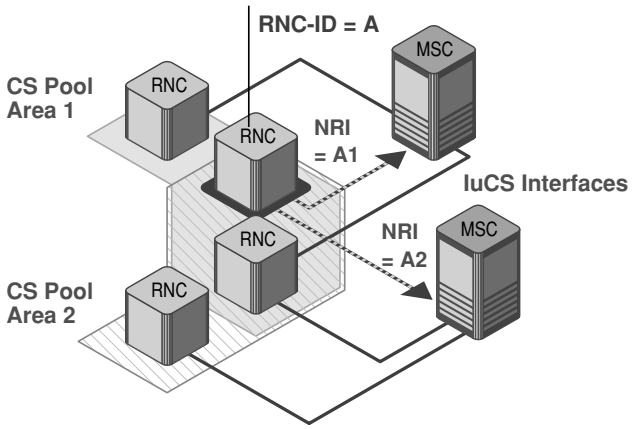


Figure 1.16 IuFlex basic description.

IuFlex

Before UMTS Rel. 5 the RNC <-> SGSN relation was hierarchical: Each RNC was assigned to exactly one SGSN; each SGSN served one or more RNCs (Figure 1.16).

With Rel. 5, IuFlex allows "many-to-many" relations of RNCs, SGSNs, or MSCs, where RNCs and SGSNs belong to "Pool Areas" (can be served by one or more SGSNs/MSCs in parallel). All cells controlled by an RNC belong to one or more Pool Areas so that a UE may roam in Pool Areas without changing the SGSN/MSC (Figure 1.17).

The integration of IuFlex now offers load balancing between SGSNs/MSCs in one Pool Area, reduction of SGSN relocations, and reduced signaling and access to HLR/HSS. An overlap of Pool Areas might allow mapping mobility patterns onto Pool Areas (e.g. cover certain residential zones plus city center).

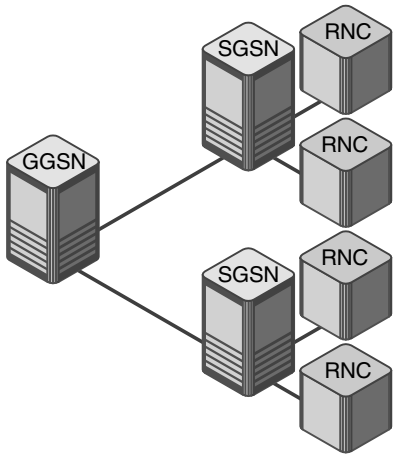


Figure 1.17 Hierarchical RNC <-> SGSN relation.

When the UE performs a GPRS Attach, the RNC selects a suitable SGSN and establishes the connection. The SGSN encodes its NRI (Network Resource Identification) into the Packet-Temporary Mobile Subscriber Identity (P-TMSI). Now the UE, RNC, and Serving SGSN know the mapping International Mobile Subscriber Identity (IMSI) **<->** NRI, and RNC and SGSN are able to route the packets accordingly.

As long as the UE is in (Packet Mobility Management) PMM-Connected Mode the RNC retains the mapping IMSI **<->** NRI. If the status changes to PMM-Idle Mode the RNC deletes UE data (no packets from/to UE need to be routed). If the UE reenters PMM-Connected Mode, it again provides the NRI of its Serving SGSN to the RNC.

1.2.6 UMTS Release 6

UMTS Release 6 is still under development; however, major improvements have already been made: a clear path toward UMTS/WLAN interworking, IMS "Phase 2," Push-to-Talk service, Packet-Switched Streaming Service (PSS), Multimedia Broadcast and Multicast Service (MBMS), Network Sharing, Presence Service, and the definition of various other new multimedia services. Figure 1.18 describes the basic Rel. 6 architecture. The following paragraphs give a more detailed description of the new features and services that Rel. 6 will have to offer.

The P-CSCF is the first contact point for the GGSN to the IMS after PDP Context Activation. The S-CSCF is responsible for the Session Control for the UE and maintains and stores session states to support the services.

The Breakout-CSCF (B-CSCF) selects the IMS CN (if within the same IMS CN) or forwards the request (if breakout is within another IMS CN) for the PSTN breakout and the MGCF for PSTN interworking. Protocol mapping functionality is provided by the MGCF (e.g. handling of SIP and ISUP) while bearer channel mapping is being handled by the MGW. Signaling between MGW and MGCF follows H.248 protocol standard and handles signaling and session management. The MRF provides specific functions (e.g. conferencing or multiparty calls), including bearer and service validation.

New in Release 6

UMTS/WLAN Interworking (Figure 1.19)

- WLAN could be used at hotspots as the access network for IMS instead of the UMTS PS domain (saves expensive 3G spectrum and cell space).
- Access through (more expensive) PS domain allows broadest coverage outside hotspots.
- Handovers between 3G (even GPRS) and WLAN will be supported (roaming).
- WLANs might be operated either by mobile operators or by third party.
- Architecture definition for supporting authentication, authorization, and charging (standard IETF AAA Server) included:
  – AAA Server receives data from HSS/HLR.

Push-to-Talk over Cellular (PoC) Service

- Push-to-Talk is a real-time one-to-one or one-to-many voice communication (like with a walkie-talkie, half duplex only) over data networks.
- Instead of dialing a number a subscriber might be selected, e.g. from a buddy list.

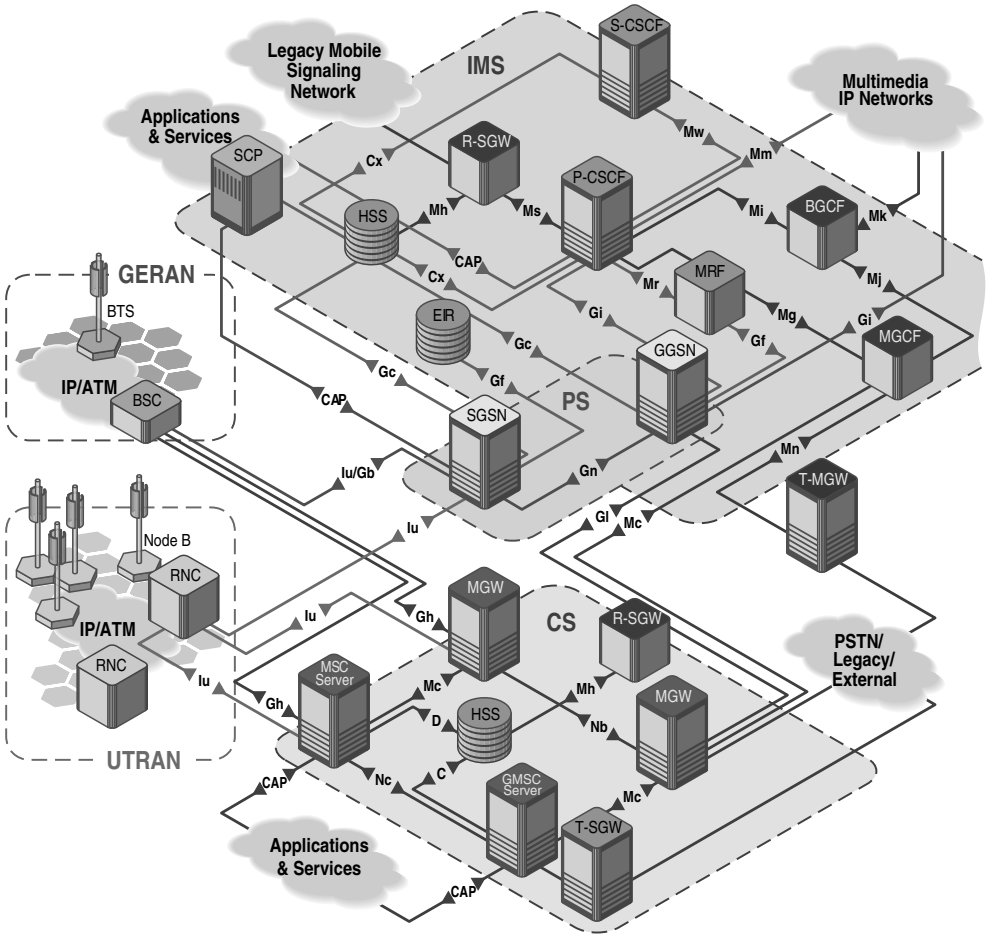


Figure 1.18 3GPP UMTS Rel. 6 network model.

Packet-Switched Streaming Services (PSS)

- PSS is used to transmit streaming content (subscriber can start to view, listen in real time, even though the entire content has not been downloaded).
- Support of End-to-End-Bitrate-Adaptation to meet the different conditions in mobile networks (offers QoS from "best effort" to "guaranteed").
- Digital Rights Management (DRM) is supported.
- Different codecs will be supported (e.g. MPEG-4 or Windows Media Video 9).

Network Sharing

- Allows cost-efficient sharing of network resources such as Network Equipment (Node B, RNC, etc.) or Spectrum (Antenna Sites), reduces time to market and deployment, and finally enables earlier profit generation for operators.

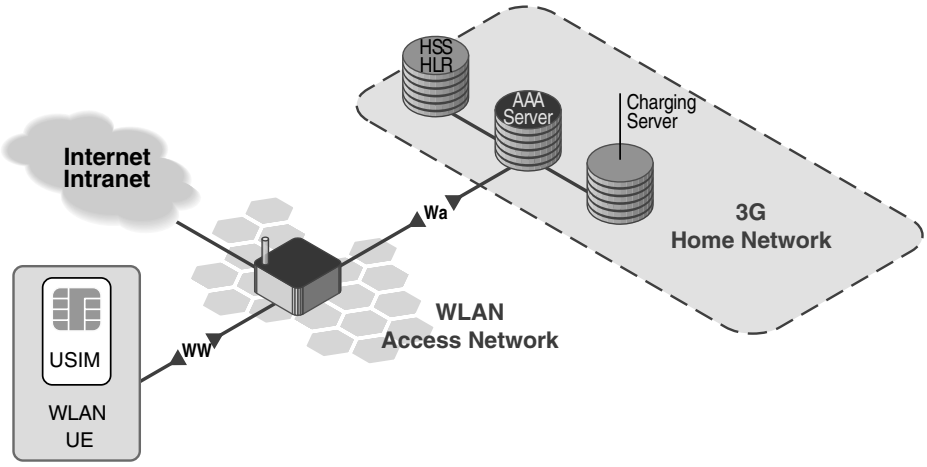


Figure 1.19 WLAN/UMTS support architecture.

- Sharing can be realized with different models:
  - Multiple CNs share common RANs (each operator maintains individual cells with separate frequencies and separate MNC (Mobile Network Code); BTSs and RNCs are shared, but the MSCs and HLRs are still separated);
  - Sharing of a common CN with separated RANs (as above);
  - Operators agree on a geographical split of networks in defined territories with roaming contracts so that all the mobile users have full coverage over the territory.

Presence Service

- Users will have the option to make themselves "visible" or "invisible" to other parties and allow or decline services to be offered.
- Users can create "buddy lists" and be informed about state changes.
- Subscribers own "user profiles" that make service delivery independent of the type of UE or access to the network.

Multimedia Broadcast and Multicast Service (MBMS)

- MBMS is a unidirectional point-to-multipoint bearer service (push service).
- Data is transmitted from a single source to multiple subscribers over a common radio channel.
- Service could transmit, e.g., text, audio, picture, video.
- Users will be able to enable/disable the service.
- Broadcast mode sends to every user within reach (typically not charged, e.g. advertisement).
- Multicast mode selectively transmits only to subscribed users (typically charged service).
- Application examples:
  - multicast of, e.g., sport events
  - multiparty conferencing
  - broadcast of emergency information
  - software download
  - Push-to-Talk.

IMS "Phase 2"

- The IMS architecture of Rel. 5 was improved and enhanced for Rel. 6.
- The main purpose is to integrate all the CNs to provide IP multimedia sessions on the basis of IP multimedia sessions, support real-time interactive services, to provide flexibility to the user, and to reduce cost.
- QoS needed for voice and multimedia services is integrated.
- Examples of supported services:
  - voice telephony (VoIP)
  - -call conferencing
  - -group management
    - setting up and maintaining user groups
    - supporting service for other services (multiparty conferencing, Push-to-Talk)
  - messaging;
    - SIP-based messaging
    - instant messaging
    - "chat room"
    - deferred messaging (equivalent to MMS)
    - interworks with Presence Service to determine whether addressee is available
  - location-based services
    - UE indicates local service request
    - S-CSCF routes request back to visited network
    - mechanism for UE to retrieve/receive information about locally available services
  - IP <-> IMS interworking functions
  - IMS <-> CS interworking functions
  - lawful interception integration.

1.2.7 UMTS Release 7 and Beyond

UMTS is quite "blurry" beyond Release 6. New services demand higher data rates and more capacity (radio resources are physically limited), so that the radio interface capabilities are permanently enhanced. Larger bandwidth and especially higher resource efficiency have been the target of this evolution. While in 3G "Rural/Suburban Areas" (macro cells, maximum speed 120 km/h) 384 kbps was enough, 2 Mbps has been defined for 4G (2 Mbps large area coverage; 200 Mbps Stationary/Indoor).

For "Indoor and Hot Spot" coverage (small cells, maximum pedestrian speed) there are 3G defined data rates up to 2048 kbps. For 4G this level rises to 200 Mbps or beyond. Of course future 4G systems will cover central areas first and may take years for a nation-wide coverage. A smooth evolution will minimize the cost, protect investments, and limit risks on the path towards the successor standard. The following are some examples of other drivers:

- Capacity:
  - capacities of normal macro cells for large area coverage will be reached soon
  - downlink throughput and handling of asymmetric traffic (e.g. Internet, email) is very limited
  - average downlink/uplink (DL/UL) throughput of macro cells will not exceed some 900/1000 kbps.

- Coverage:
  - frequency range is significantly higher than in GSM
  - UMTS cells are much smaller than GSM cells.
  - limited UE Tx power (21 dBm).
- Higher data rates than 384 kbps:
  - type of needed applications changed; symmetric services (e.g. speech and video telephony) are more and more displaced by asymmetric services (e.g. email download, Internet surfing)
  - service volume is continuously demanding more downlink and uplink capacities.
- Smooth evolution towards 4G:
  - evolution is necessary rather than a cut in technology
  - protect investments
  - reduce costs
  - reduce risks.

As this book has a stronger focus on real signaling and on message flow examples, the following is a collection of possible solutions, which are partially already under development:

- Lower frequency ranges, UMTS 800/850/900 (500?):
  - less attenuation $\Rightarrow$ larger cells.
- Extension bands:
  - more carriers (e.g. UMTS2600) $\Rightarrow$ higher capacity.
- Support of complementary technologies:
  - WLAN (mainly indoor high-data rate coverage)
  - WiMAX (macro cells in urban, suburban, and rural areas)
  - MBWA (high-speed applications up to 1 Mbps; supports speeds of max. 250 km/h (e.g. high-speed trains, telematic services); macro cells for large area coverage)
  - higher capacities
  - very high data rates (WLAN)
  - large cells/high mobility (MBWA).
- Multiple Input Multiple Output (MIMO):
  - spatial multiplexing with multiple input and multiple output
  - improves HSDPA capacity and peak rates
  - peak rates up to 30 Mbps and beyond.

Milestones of the Mobile Network Evolution (Figure 1.20)

1990/91	GSM Phase 1 (GSM900/1800) Tele, bearer, and some supplementary services, CS data up to 9.6 kbps.
1994	GSM Phase 2 Full set of supplementary services, half rate speech, CS data up to 57.6 (115.2) kbps, GPRS (PS data up to 171.2 kbps) and EDGE (E-GPRS: PS data up to 473.6 kbps.
1996	UMTS-GSM compatibility; evolution of GSM towards UMTS.
1997–99	GSM Phase 2+ PS core network (GPRS), VHE, CAMEL, MExE, STK, OSA, higher data rates (HSCSD, GPRS and EDGE), enhanced speech codecs (EFR and AMR), MMS.

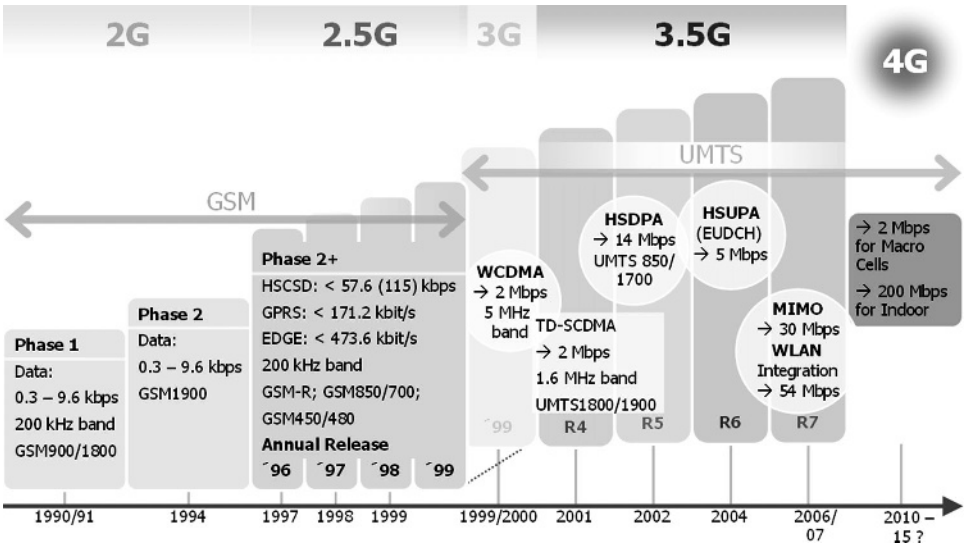


Figure 1.20 3GPP Release timeline.

1999/2000 UMTS Rel. 99
UMTS on GSM CN, UTRAN and WCDMA air interface (FDD and TDD mode).

2002 UMTS Rel. 4
ATM-CN, LCR-TDD mode (up to 2 Mbps).

2002/03 UMTS Rel. 5

IP Multimedia Subsystem IMS, HSDPA for enhanced data rates (up to 14 Mbps)

2005 UMTS Rel. 6
Enhanced IMS support, new services (MBMS, PoC), enhanced data rates, HSUPA (up to 5.7 Mbps), WLAN integration (up to 54 Mbps).

2006/07 UMTS Rel. 7
Enhanced WLAN integration, HSDPA (up to 30 Mbps), MIMO (enhanced antenna concepts and data rates, 7.68 Mbps TDD).

2010–15 4G
Pure IP core network and RAN for data rates up to 2 Mbps for large area coverage and high mobility, 200 Mpbs and higher for indoor coverage.

Just getting under way in mid-2005, and currently expected to focus on leftovers from Release 6, as well as defining fixed broadband access via IMS, are: policy issues, voice call handover between CS, WLAN/IMS and end-to-end QOS. It is likely that this list will expand.

1.2.8 TD-SCDMA

Time Division-Synchronous Code Division Multiple Access (TD-SCDMA) is China's approach to 3G, standardized by the Chinese Academy of Telecommunications Technology (CATT), Datang and Siemens. This approach was taken to avoid a dependency on "western technologies" and the payment of any license fees. TD-SCDMA allows combined operation

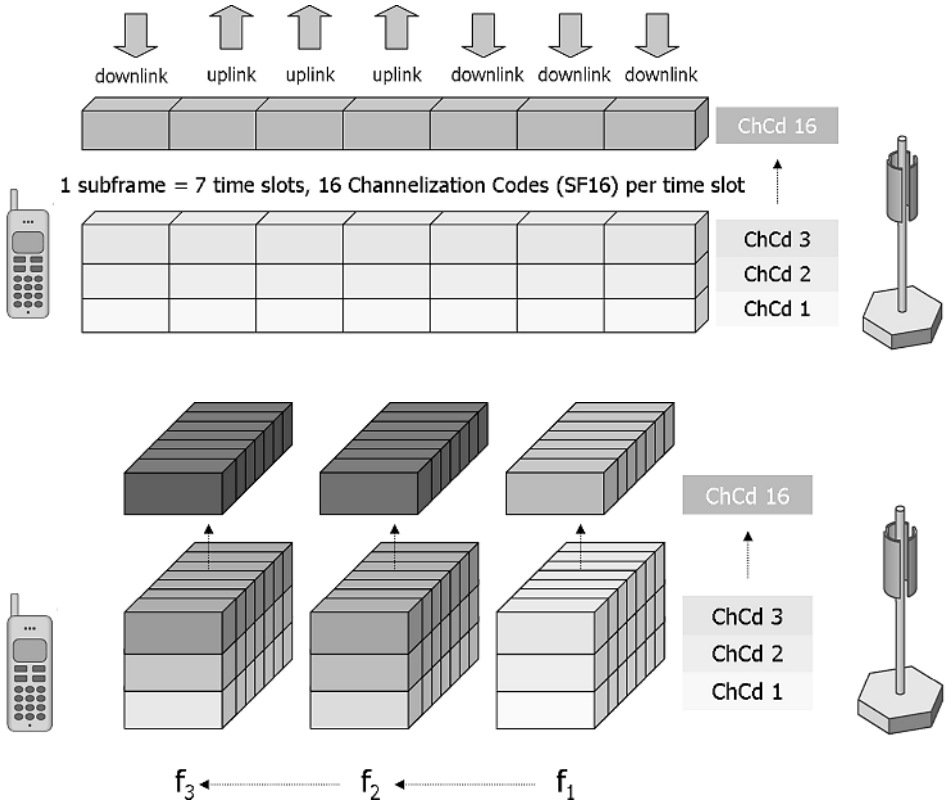


Figure 1.21 Timeslots, subslots, and channelization codes in single- and multi-frequency cells.

with W-CDMA/UMTS. Both systems share the same core network and UTRAN, which allows a flexible use of resources, e.g. in dense urban areas. With these possibilities TD-SCDMA has been integrated by 3GPP since Rel. 4 as "UTRA TDD 1.28Mcps Option"; it is based on CDMA spread spectrum technology. The launch is underway while this book is being published.

TD-SCDMA uses Time Division Duplex (TDD), in contrast to the Frequency Division Duplex (FDD) scheme used by W-CDMA/UMTS (Figure 1.21).

TDD applies TDMA into separate uplink and downlink signals. TDD takes advantage of asymmetric traffic, where different uplink and downlink data speeds are beneficial. The bandwith assignment is variable so that uplink capacity can be increased if needed and taken away again if the capacity need is shrinking. Additionally uplink and downlink radio paths are very similar for slow moving systems, so that e.g. beamforming will work well with TDD systems.

FDD applies Frequency Division Multiple Access (FDMA) into separate uplink and downlink signals. Uplink and downlink channels/bands are separated by a "frequency offset". FDD is very efficient for symmetric traffic. TDD "wastes" bandwidth for the switch from transmit to receive, has greater latency, and requires a complex, typically more power-consuming circuitry.

With the dynamic timeslot adjustment, TD-SCDMA easily accommodates data rate requirements on downlink and uplink of asymmetric traffic (data rate ranging from 4.75 kbps to 2 Mbps). The spectrum allocation is rather flexible as TD-SCDMA does not require a paired

spectrum for downlink and uplink. The use of the same carrier frequencies for up- and downlink means that there are always the same channel conditions in both directions. A base station deduces e.g. the downlink from uplink channel information. This supports the in-built antenna beamforming techniques.

The TD-SCDMA implementation also includes TDMA, which results in a reduced number of users in each timeslot. This again reduces the implementation complexity for multiuser detection and beamforming schemes. On the negative side are the non-continuous transmission that reduces coverage (higher peak power needed), the reduced mobility (lower power control frequencies), and more complicated radio resource management algorithms.

The "synchronous" in TD-SCDMA means that uplink signals are synchronized at the base station by continuous timing adjustments. This happens to achieve reduced interference between users in the same timeslot but with different codes. With this approach the orthogonality between the codes is improved. At the same time the system capacity increases. To achieve the necessary uplink synchronization a more complex hardware is needed.

1.3 UMTS Interfaces

Figure 1.22 shows a basic overview of the different interfaces in a UMTS Rel. 99 network. A detailed description of objectives and functions follows.

1.3.1 Iu Interface

The Iu interface is located between the RNC and MSC for circuit-switched traffic and between the RNC and SGSN for packet-switched traffic. Iu provides the connection to "classic" voice services and at the same time as the connection for all kinds of packet services. It plays a vital role for the handover procedures in the UMTS network.

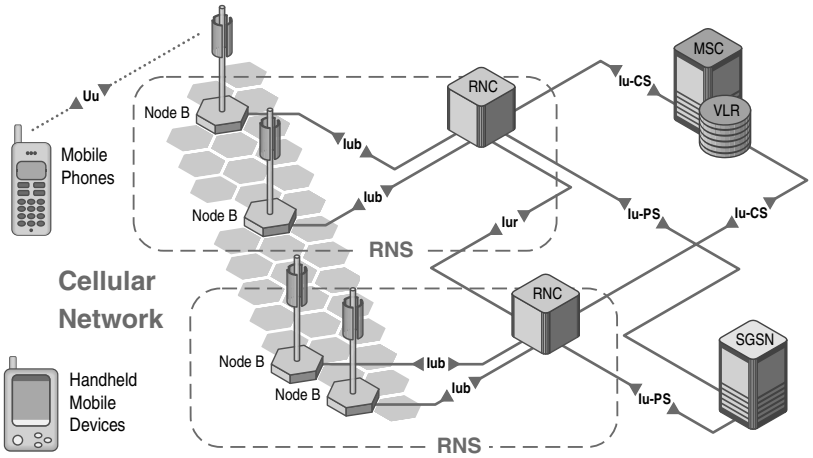


Figure 1.22 UMTS interface overview.

Objectives and Functions of the Iu Interface

The Iu interface will take care of the interconnection of RNCs with the CN Access Points within a single PLMN and the interconnection of RNCs with the CN Access Points irrespective of the manufacturer of any of the elements. Other tasks are the interworking toward GSM, the support of all UMTS services, the support of independent evolution of Core, Radio Access, and Transport Networks, and finally the migration of services from CS to PS.

The Iu interface is split into two types of interfaces:

- IuPS (packet switched), corresponding interface toward the PS domain.
- IuCS (circuit switched), corresponding interface toward the CS domain.

The Iu interface supports the following functions:

- Establishing, maintaining, and releasing RABs.
- Performing intra- and intersystem handover and SRNS relocation.
- A set of general procedures, not related to a specific UE.
- Separation of each UE on the protocol level for user-specific signaling management.
- Transfer of NAS signaling messages between UE and CN.
- Location services by transferring requests from the CN to UTRAN, and location information from UTRAN to CN.
- Simultaneous access to multiple CN domains for a single UE.
- Mechanisms for resource reservation for packet data streams.

1.3.2 Iub Interface

The Iub interface is located between an RNC and a Node B. Via the Iub interface, the RNC controls the Node B. For example, the RNC allows the negotiating of radio resources, the adding and deleting of cells controlled by the individual Node B, or the supporting of the different communication and control links. One Node B can serve one or multiple cells.

Objectives and Functions of the Iub Interface

The Iub interface enables continuous transmission sharing between the GSM/GPRS Abis interface and the Iub interface and minimizes the number of options available in the functional division between RNC and Node B. It controls – through Node B – a number of cells and adds or removes radio links in those cells. Another task is the logical Operation and Maintenance (O&M) support of the Node B and to avoid complex functionality as far as possible over the Iub. Finally, it accommodates the probability of frequent switching between different channel types.

The Iub interface supports the functions described in Table 1.4.

1.3.3 Iur Interface

The Iur interface connects RNCs inside one UTRAN.

Table 1.4 Iub function overview.

Function	Description
Relocating SRNC	Changes the SRNC functionality as well as the related Iu resources (RAB(s) and signaling connection) from one RNC to another
Overall RAB management	Sets up, modifies, and releases RAB
Queuing the setup of RAB	Allows placing some requested RABs into a queue and indicates the peer entity about the queuing
Requesting RAB release	Requests the release of RAB (overall RAB management is a function of the CN)
Release of all Iu connection resources	Explicitly releases all resources related to one Iu connection
Requesting the release of all Iu connection resources	Requests release of all Iu connection resources from the corresponding Iu connection (Iu release is managed from the CN)
Management of Iub transport resources	
Logical O&M of Node B	Iub link management Cell configuration management Radio network performance measurements Resource event management Common transport channel management Radio resource management Radio network configuration alignment
Implementation-specific O&M transport	
System information management	
Traffic management of common channels	Admission control Power management Data transfer
Traffic management of dedicated channels	Radio link management, radio link supervision Channel allocation/deallocation Power management Measurement reporting Dedicated transport channel management Data transfer
Traffic management of shared channels	Channel allocation/deallocation Power management Transport channel management Data transfer
Timing and synchronization management	Transport channel synchronization (frame synchronization) Node B-RNC node synchronization Inter-Node B node synchronization

Objectives and Functions of the Iur Interface

The Iur interface provides an open interface architecture and supports signaling and data streams between RNCs, allows point-to-point connection, and the addition or deletion of radio links supported by cells belonging to any RNS (Radio Network Subsystem) within the UTRAN.

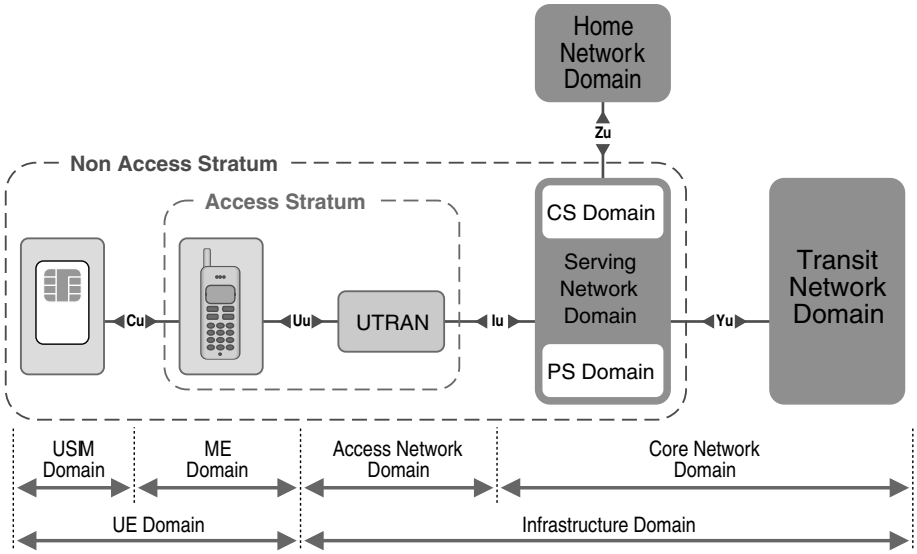


Figure 1.23 UMTS domain architecture.

Additionally, it allows an RNC to address any other RNC within the UTRAN so as to establish signaling bearer or user data bearers for Iur data streams.

The Iur interface supports the following functions:

- Transport network management.
- Traffic management of common transport channels.
- Preparation of common transport channel resources:
  – paging.
- Traffic management of dedicated transport channels:
  – radio link setup/addition/deletion;
  – measurement reporting.
- Measurement reporting for common and dedicated measurement objects.

1.4 UMTS Domain Architecture

From the beginning it was decided that UMTS would be very modular in its structure. This is the basis of becoming an international standard even though certain modules will be national specific.

The two important modules are the Access Stratum (Mobile and UTRAN) and the Non-Access Stratum (containing serving CN, Access Stratum, and USIM (Universal Subscriber Identity Module)) (Figure 1.23).

1.5 UTRAN

Two new network elements are introduced in UTRAN: RNC and Node B. UTRAN is subdivided into individual RNS, where an RNC controls each RNS.

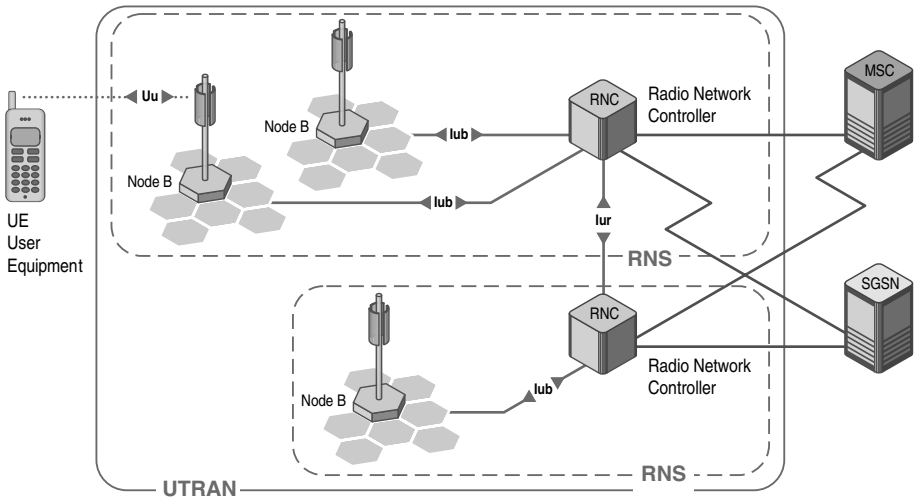


Figure 1.24 UTRAN.

The RNC is connected to a set of Node B elements, each of which can serve one or several cells.

Existing network elements, such as MSC, SGSN, and HLR, can be extended to adopt the UMTS requirements, but RNC and Node B require completely new designs. RNC will become the replacement for BSC, and Node B fulfills nearly the same functionality as BTS. GSM and GPRS networks will be extended and new services will be integrated into an overall network that contains both existing interfaces, such as A, Gb, and Abis, and new interfaces that include Iu, Iub, and Iur (Figure 1.24).

The main UTRAN tasks are:

- *Admission Control (AC):* Admits or denies new users, new radio access bearers, or new radio links. The AC should try to avoid overload situations and will not deteriorate the quality of the existing radio links. Decisions are based on interference and resource measurements (power or on the throughput measurements). Together with the Packet Scheduler it allocates the bitrate sets (transmission powers) for non-realtime connections. The AC is employed at, for example, the initial UE access, the RAB assignment/reconfiguration, and at handover. The functionality is located in the RNC.

  Power-based AC needs the reliable Received Total Wideband Power measurements from the Node B and assures the coverage stability. In the power-based case, the upper boundary for the AC operation is defined by the maximum allowed deterioration of the quality for the existing links (= the maximum allowed deterioration of the path loss). This limit is usually defined as P_{RX} Target [dB] (Figure 1.25).

  Throughput-based AC assures the constant maximum cell throughput in every moment of the operation, but allows excessive cell breathing. On the linear scale the received power changes [dB] can be expressed as the cell loading [%]. Via a simple equation the cell loading [%] is bounded with the cell throughput [kbps] and call quality [E_b/N_0].

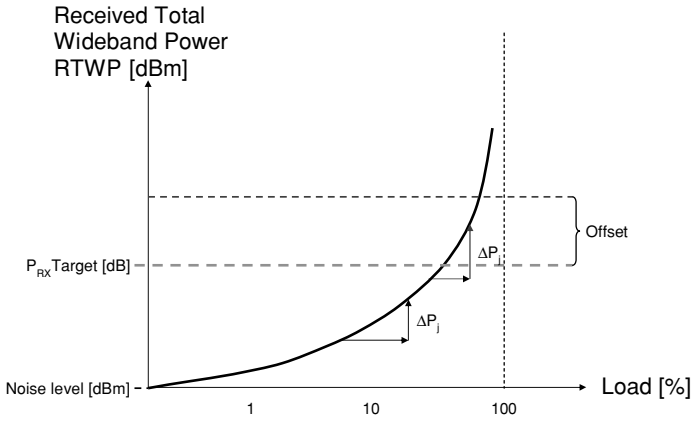


Figure 1.25 Throughput-based admission control.

- *Congestion Control:* Monitors, detects, and handles situations when the system is reaching a near overload or an overload situation with the already connected users.
- *System Information Broadcasting:* Provides the UE with the Access Stratum and Non-Access Stratum information, which are needed by the UE for its operation within the network.
- *Ciphering:* Encrypts information exchange and is located between UE and RNC.
- *Handover (HO):* Manages the mobility of the radio interface. It is based on radio measurements and for Soft/Softer HO it is used to maintain the QoS requested by the CN. An Intersystem HO (IS-HO) is necessary to avoid losing the UE's network connection. In this case an even lower QoS might be accepted. Handover may be directed to/from another system (for example, UMTS to GSM HO).

Further functions of UTRAN are configuration and maintenance of the radio interface, power control, paging, and macrodiversity.

1.5.1 RNC

The RNC is the main element in the RNS and controls usage and reliability of radio resources. There are three types of RNCs: SRNC (Serving RNC), DRNC (Drift RNC), and CRNC (Controlling RNC). Tasks of the RNC are:

- *Call Admission Control:* Provides resource check procedures before new users access the network, as required by the CDMA air interface technology.
- *Radio Bearer Management:* Sets up and disconnects radio bearers and manages their QoS.
- *Code Allocation:* Manages the code planning that the CDMA technology requires.
- *Power Control:* Performs the outer loop power control 10–100 times per second and defines the SIR (Signal-to-Interference Ratio) for a given QoS.
- *Congestion Control:* Schedules packets for PS CN data transmission.
- *O&M Tasks:* Performs general management functions and connection to Operation & Maintenance Center (OMC).

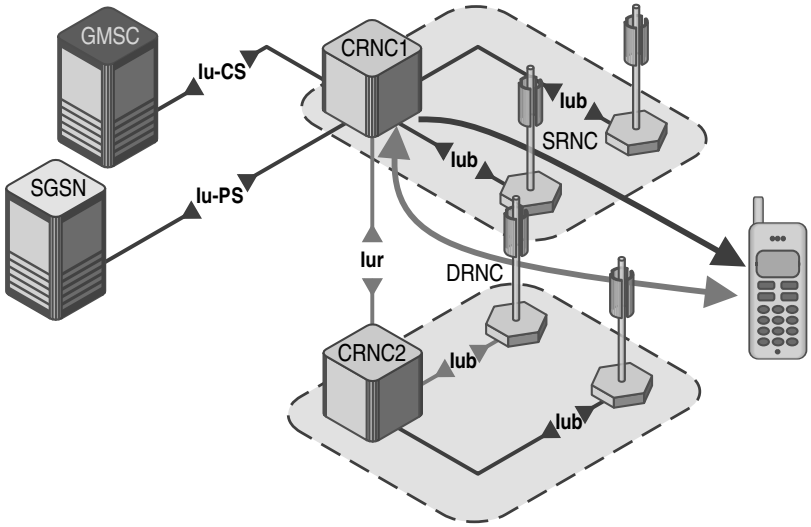


Figure 1.26 Different RNC types.

Additionally, the RNC can act as a macrodiversity point, for example a collection of data from one UE that is received via several Node Bs.

Different RNC Types

Controlling RNC (CRNC)
The CRNC controls, configures, and manages an RNS and communicates with NBAP (Node B Application Part) with the physical resources of all Node Bs connected via the Iub interfaces. Access requests of UEs will be forwarded from the related Node B to the CRNC (Figure 1.26).

Drift RNC (DRNC)
The DRNC receives connected UEs that are handed over (drifted) from an SRNC cell connected to a different RNS because, e.g., the received level of that cell became critical (mobility). The RRC, however, still terminates with the SRNC. The DRNC then exchanges routing information between SRNC and UE.

DRNC in Inter-RNC Soft HO situation is the only DRNC from the SRNC point of view. It lends radio resources to SRNC to allow Soft HO. However, radio resources are controlled by the CRNC function of the same physical RNC machine. Functions can be distinguished by the protocol used: DRNC "speaks" RNSAP with SRNC via Iur, CRNC "speaks" NBAP with cells via Iub.

Serving RNC (SRNC)
The SRNC controls a user's mobility within a UTRAN and is also the connection point to the CN toward MSC or SGSN. The RNC, which has an RRC connection with a UE, is its SRNC. The SRNC "speaks" RRC with UE via Iub, Uu and – if necessary – via Iur and "foreign" Iub (controlled by DRNC).

1.5.2 Node B

The Node B provides the physical radio link between the UE and the network. It organizes transmission and reception of data across the radio interface and also applies codes that are necessary to describe channels in CDMA systems. The tasks of a Node B are similar to those of a BTS. The Node B is responsible for:

- *Power Control:* Performs the inner loop power control, which measures the actual SIR, compares it with the specific defined value, and may trigger changes in the TX power of a UE.
- *Measurement Report:* Gives the measured values to the RNC.
- *Microdiversity:* Combines signals (from the multiple sectors of the antenna that a UE is connected to) into one data stream before transmitting the sum-signal to the RNC. (The UE is connected to more than one sector of an antenna to allow for a Softer HO.)

The Node B is the physical unit used to carry one or more cells (1 cell = 1 antenna). There are three types of Node Bs:

- UTRA-FDD Node B.
- UTRA-TDD Node B.
- Dual Mode Node B (UTRA-TDD and UTRA-FDD).

Note: It is not expected to have 3.84 TDD and 1.28 TDD cells in the same network, but operators in the same areas are expected to work with different TDD versions. So, three-band Node Bs are not necessary.

1.5.3 Area Concept

The areas of 2G will be continuously used in UMTS.

UMTS will add a new group of locations specifying the UTRAN Registration Areas (URAs). These areas will be smaller Routing or Location Areas and will be maintained by UTRAN itself, covered by a number of cells. The URA is configured in the UTRAN, and broadcast in relevant cells (Figure 1.27).

The different areas are used for Mobility Management, e.g. Location Update and Paging procedures.

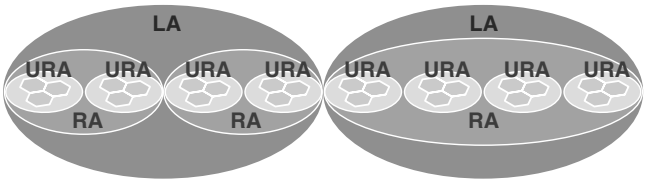


Figure 1.27 UMTS areas.

Location Area (LA)

The LA is a set of cells (defined by the mobile operator) throughout which a mobile will be paged. The LA is identified by the LAI (Location Area Identity) within a PLMN and consists of MCC (Mobile Country Code), MNC (Mobile Network Code), and LAC (Location Area Code).

$$\text{LAI} = \text{MCC} + \text{MNC} + \text{LAC}$$

Routing Area (RA)

One or more RA is controlled by the SGSN. Each UE informs the SGSN about the current RA. RAs can consist of one or more cells. Each RA is identified by an RAI (Routing Area Identity). The RAI is used for paging and registration purposes and consists of LAC and RAC (Routing Area Code). The RAC (length: 1 octet fixed) identifies an RA within an LA and is part of the RAI.

$$\text{RAI} = \text{LAI} + \text{RAC}$$

Service Area (SA)

The SA identifies an area of one or more cells of the same LA, and is used to indicate the location of a UE to the CN.

The combination of SAC (Service Area Code), PLMN-ID (Public Land Mobile Network Identifier), and LAC is the Service Area Identifier (SAI).

$$\text{SAI} = \text{PLMN-ID} + \text{LAC} + \text{SAC}$$

UTRAN Registration Area (URA)

The URA is configured in the UTRAN, is broadcast in relevant cells, and covers an area of a number of cells.

1.5.4 UMTS User Equipment and USIM

In UMTS the Mobile Station (MS) is called *User Equipment* (UE) and is constructed in a very modular way (Figure 1.28). It consists of the following parts.

Mobile Termination (MT)

Represents the termination of the radio interface and, by that, the termination of an IMT-2000 family-specific unit. There are different MT messages for UMTS in Europe as opposed to in the United States.

Terminal Adapter

Represents the termination of the application-specific service protocols, for example, AMR for speech. This function will perform all necessary modifications to the data.

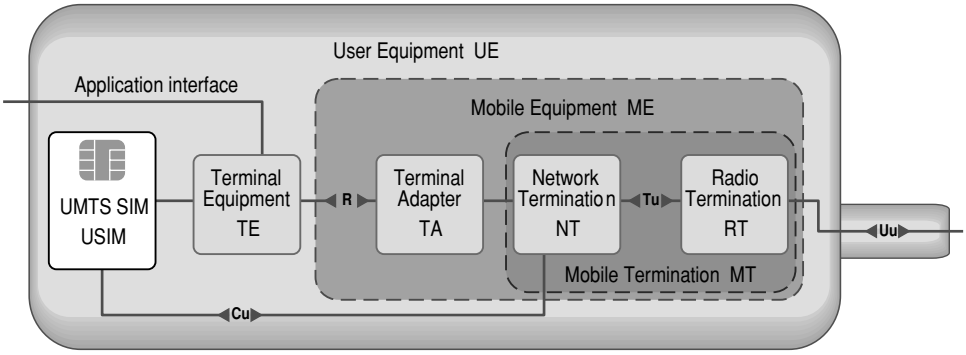


Figure 1.28 UMTS User Equipment.

Terminal Equipment

Represents the termination of the service.

USIM

USIM is a user subscription to the UMTS mobile network and contains all relevant data that enables access onto the subscribed network (Figure 1.29). Every UE may contain one or more USIM simultaneously (100 % flexibility). Higher layer standards like MM/CC/SM address 1 UE + 1 (of the several) USIM when they mention an MS.

The main differences between a USIM and a GSM SIM is that the USIM is downloadable (by default), can be accessed via the air interface, and can be modified by the network.

The USIM is a Universal Integrated Circuit Card (UICC), which has much more capacity than a GSM SIM. It can store Java applications. It can also store profiles containing user management and rights information and descriptions of the way applications can be used.

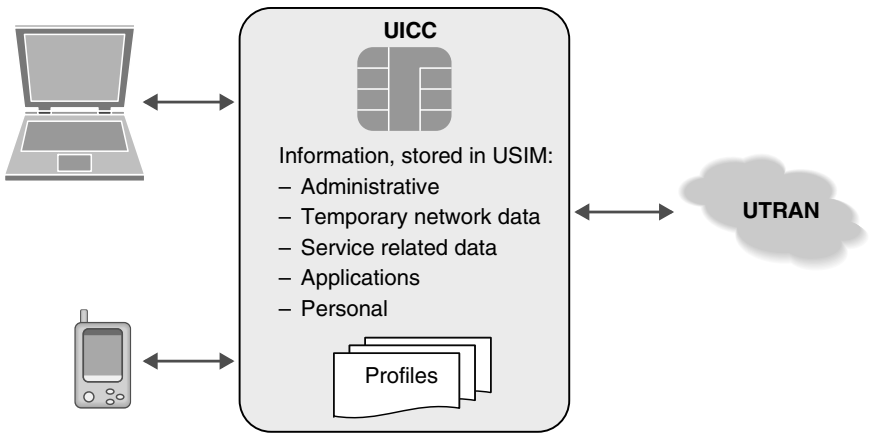


Figure 1.29 UMTS Service Identity Module (USIM).

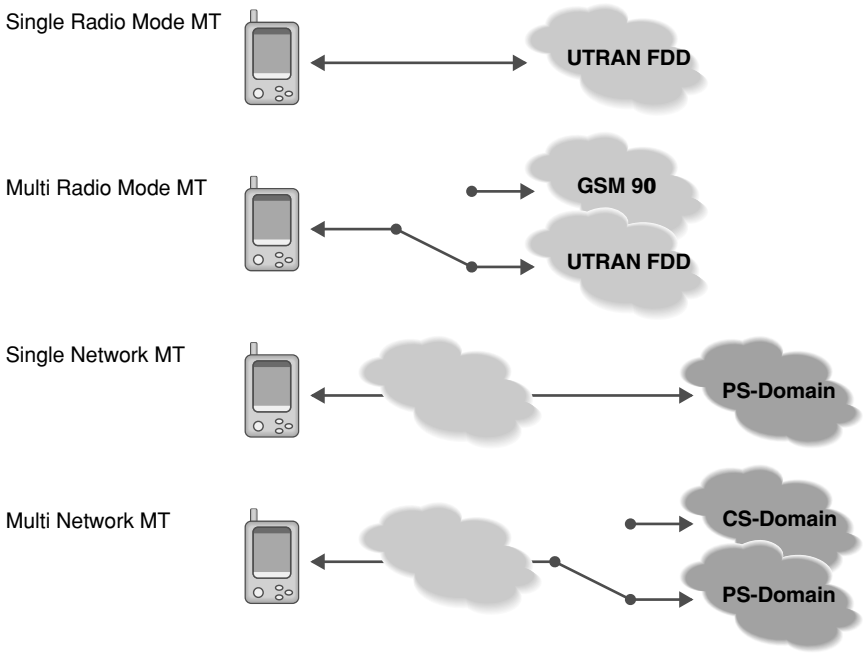


Figure 1.30 Types of Mobile Terminations.

1.5.5 Mobiles

Mobile Terminations

The Mobile Terminations are divided into different groups (Figure 1.30).

Single Radio Mode MT
The UE can work with only one type of network because only one RAT is implemented.

Multiradio Mode MT
More than one RAT is supported. 3GPP specifies handover between different RATs in great detail.

Single Network MT
Independent of the Radio Mode, the Single Network MT is capable of using only one type of CN; for example only the packet-switched CN (PC Card).

Multinetwork MT
Independent of the Radio Mode, the Multinetwork MT can work with different types of CNs. At the beginning of UMTS, the multinetwork operations will have to be performed sequentially, but, at a later stage, parallel operations could also be possible. This ability will depend heavily on the overall performance of the UE and the network capacity.

The first UMTS mobiles should be Multiradio-Multinetwork mobiles.

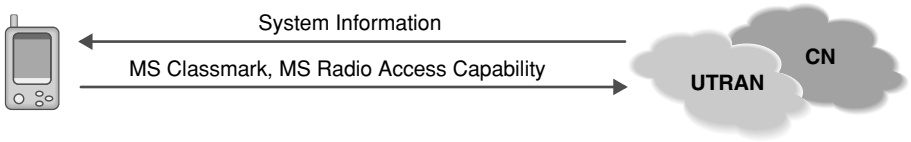


Figure 1.31 Mobile capabilities.

Mobile Capabilities

The possible features of UTRAN and CN will be transmitted via System Information on the radio interface via broadcast channels. A UE can, by listening on these channels, configure its own settings to work with the actual network (Figure 1.31).

On the other hand, the UE will also indicate its own capabilities to the network by sending MS Classmark and MS Radio Access Capability information to the network. Below is an extract of possible capabilities:

- Available W-CDMA modes, FDD or/and TDD.
- Dual-mode capabilities, support of different GSM frequencies.
- Support of GSM PS features, GPRS or/and HSCSD.
- Available encryption algorithms.
- Properties of measurement functions, timing.
- Ability of positioning methods.
- Ability to use universal character set 2 (16-bit characters).

In GSM, MS Classmark 1 and 2 were used. In UMTS, MS Classmark 2 and the new MS Classmark 3 are used. The difference is the number of parameters for different features that can be transmitted.

1.5.6 QoS Architecture

There is one-to-one relation between Bearer Services and QoS in UMTS networks.

Other than in 2G systems where a bearer was a traffic channel in 3G the bearer represents a selected QoS for a specific service. Only from the point of view of the physical layer is a bearer a type of channel.

A Bearer Service is a service that guarantees a QoS between two endpoints of communication. Several parameters will have to be defined from operators. A Bearer Service is classified by a set of values for these parameters:

- Traffic class.
- Maximum bitrate.
- Guaranteed bitrate.
- Delivery order.
- Maximum SDU (Service Data Unit) size.
- SDU format information.
- SDU error ratio.

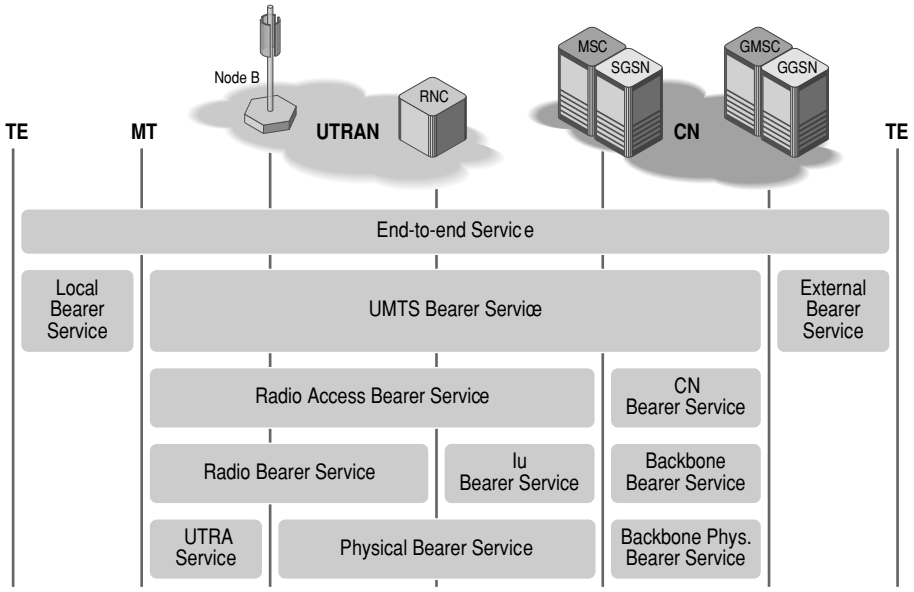


Figure 1.32 UMTS Bearer/QoS architecture.

- Residual bit error ratio.
- Delivery of erroneous SDUs.
- Transfer delay.
- Traffic handling priority.
- Allocation/retention priority.

The End-to-End Service will define the constraints for the QoS. These constraints will be given to the lower Bearer Services, translated into their configuration parameters, and again passed to the lower layer. By this, UMTS sets up a connection through its own layer architecture fulfilling the requested QoS (Figure 1.32).

Problems are foreseen in the External Bearer Services because they are outside of UMTS and the responsibility of the UMTS network operator.

QoS classes with QoS attributes have been specified to meet the needs of different End-to-End Services (Figure 1.33).

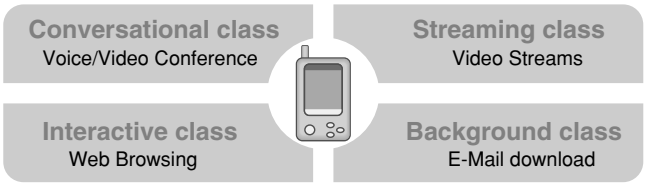


Figure 1.33 UMTS Bearer/QoS classes.

Conversational Class

Real-time applications with short predictable response time. Symmetric transmission without buffering of data and with a guaranteed data rate.

Streaming Class

Real-time applications with short predictable response time. Asymmetric transmission with possible buffering of data and with a guaranteed data rate.

Interactive Class

Non-real-time applications with acceptable variable response time. Asymmetric transmission with possible buffering of data but without guaranteed data rate.

Background Class

Non-real-time applications with long response times. Asymmetric transmission with possible buffering of data but without a guaranteed data rate.

1.6 UMTS Security

After experiencing GSM, the 3GPP creators wanted to improve the security aspects for UMTS. For example, UMTS addresses the "Man-in-the-Middle" Fake BTS problem by introducing a signaling integrity function.

The most important security features in the access security of UMTS are:

- Use of *temporary identities* (TMSI, P-TMSI).
- Mutual *authentication* of the user and the network.
- Radio access network *encryption.*
- Protection of *signaling integrity* inside UTRAN.

1.6.1 Historic Development

Although ciphering and cryptanalysis are now a hot topic accelerated by the current geopolitic environment, information security is not a new issue. Four hundred years B.C. the Ancient Greeks used the so-called *skytals* (Gr. *Sky tale*) for encryption. A skytal is a wooden stick of fixed diameter with a long paper strip winded around the stick. The sender wrote a message on the paper in longitudinal direction. The unwinded paper strip gave no meaningful information to the courier or other unauthorized person. Only a receiver who owns a stick with the same diameter was able to decipher the message (Figure 1.34).

Caesar ciphered secret information simply by replacing every character with one that was in the alphabet three places ahead of it. The word "cryptology" would be ciphered as "fubswrorjb". Code books were widely used in the twelfth century. Certain key words of a text were replaced by other predefined words with completely different meaning. A receiver who owns an identical code book was able to derive the original message.

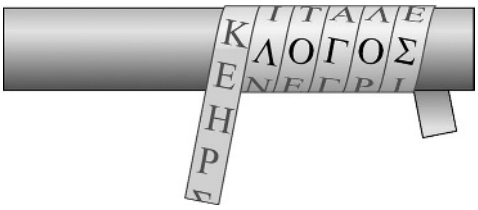


Figure 1.34 Ciphering in Ancient Greece.

Kasiski's and Friedman's fundamental research about statistical methods in the nineteenth century is the foundation of modern methods for ciphering and cryptanalysis. The Second World War gave another boost to ciphering technologies. The Enigma was an example of advanced ciphering machines used by the German military. Alan Turing, from Great Britain, using his "bomb" was able to crack Enigma (Figure 1.35).

Another milestone was Claude E. Shannon's article "Communication Theory of Secret Systems" published in 1949. It gives the information-theoretic basis for cryptology and proves Vernam's "One-Time Pad" as a secure cryptosystem.

In the last century several ciphering technologies have been developed, which can be divided into symmetric and asymmetric methods. Symmetric methods are less secure because the same key is used for ciphering and deciphering. Examples are the Data Encryption Standard (DES) developed by IBM and the International Data Encrypted Algorithm (IDEA) proposed by Lai and Massey.

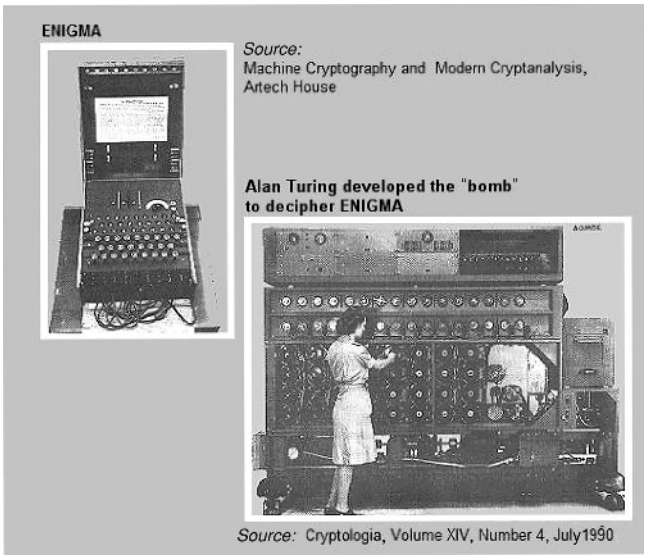


Figure 1.35 Enigma and Bomb as examples for decryption and encryption.

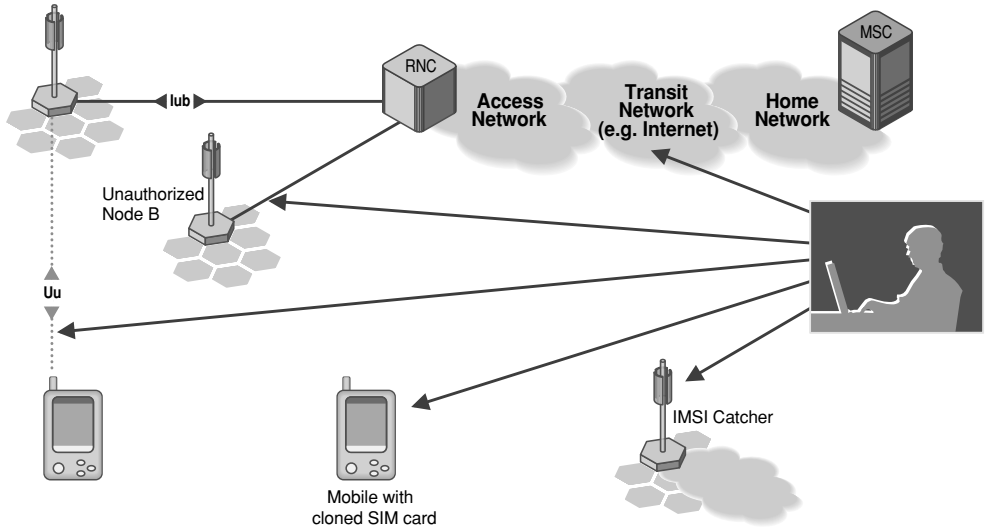


Figure 1.36 Potential attack points of intruders.

Asymmetric technologies use one encryption key (public key) and another decryption key (private key). It is not possible to calculate the decryption key by knowing only the encryption key. The most common asymmetric ciphering method is RSA, developed by *R*ivest, *S*hamir, and *A*dleman in 1978. The method is based on the principle of big prime numbers: It is relatively easy to detect two prime numbers x and y with 1000 and more digits. However, even today it is not possible to calculate the factors of the product "$x * y$" in reasonable time. Kasumi from Mitsubishi developed an algorithm for ciphering and integrity protection used in UMTS networks. The 3GPP standard is open to other ciphering methods, but Kasumi is the first and only ciphering algorithm used in UMTS at the moment.

Security Threats and Protection in Mobile Networks

In a digital mobile network the subscriber is exposed to several basic attacks as described below (Figure 1.36):

- Eavesdropping (theft of voice and data information).
- Unauthorized identification.
- Unauthorized usage of services.
- Offending the data integrity (data falsification by an intruder).
- Observation:
  – detection of the current location;
  – observation of communication relations (who is communicating with whom?);
  – generation of behavior profiles.

```
000001--  Actual Timing Advance                          1
L3 Information
00001011  IE Name                                       L3 Information
00000000  Spare                                         0
00010010  LLSDU Length                                  18
**B18***  DTAP LLSDU                                    06 15 2a 2a 01 25 06 a7 97 63 85...
E-GSM 04.08 (DTAP) 5.3.0) (DTAP)  MEASREP (= Measurement report)
Measurement report
----0110  Protocol Discriminator                        radio resources management msg
0000----  Skip Indicator                                0
-0010101  Message Type                                  21
0-------  Extension bit                                 0
Measurement Results
0-------  BA-USED                                       0
-0------  DTX-USED                                      not used
--101010  RXLEV-FULL-SERVING-CELL                       -69 dBm to -68 dBm
0-------  Spare                                         0
-0------  Measurement results valid                     Valid
--101010  RXLEV-SUB-SERVING-CELL                        -69 dBm to -68 dBm
0-------  Spare                                         0
-000----  RXQUAL-FULL-SERVING-CELL                      BER less than 0.2%
----000-  RXQUAL-SUB-SERVING-CELL                       BER less than 0.2%
***b3***  NO-NCELL-M                                    4 NCELL measurement result
--100101  RXLEV-NCELL 1                                -74 dBm to -73 dBm
00000---  BCCH-FREQ-NCELL 1                             0
-----110  BSIC-NCC-NCELL 1                              6
101-----  BSIC-BCC-NCELL 1                              5
```

Figure 1.37 Measurement Report Message sent unciphered via GSM radio channels.

As an example for unlawful observation, Figure 1.37 shows a part of a Measurement Report Message captured on the GSM Abis interface. An active mobile permanently measures the power level and the bit error rate of its serving cell and up to six neighbor cells. This information is transmitted from the mobile over the BTS to the BSC. In addition, the BTS sends the Timing Advance Information to the mobile. The Timing Advance is a value in the range of 0–63. The Timing Advance is an indicator of the distance between BTS and mobile. Assuming that the maximum cell size in GSM is 30 km, the Timing Advance value allows estimating the distance with 500 m precision. In urban places, however, the cell size is much smaller. Combining that information, a potential intruder can determine the location of the mobile subscriber. GSM was originally designed as a circuit-switched voice network. Contrary to the voice data, controlling information is never ciphered in GSM. In addition, the ciphering is limited to the air interface. It is needless to say that short messages are transferred over the signaling network and therefore are never ciphered.

GPRS as extension to GSM already offers significant security improvements. User and controlling information are ciphered not only over the air interface but also over the Gb interface between BSC and SGSN. GEA1 (GPRS Encryption Algorithm) and GEA2 are commonly used in commercial networks, and GEA3 is under development. The most secure mobile network is the UMTS network.

UMTS actively combats prior mentioned threats by offering the following security procedures:

- Ciphering of control information and user data.
- Authentication of the user toward the network.
- Authentication of the network toward the user.
- Integrity protection.
- Anonymity.

The UMTS security procedures are described in the following sections. Security mechanisms over transport networks (Tunneling, IPsec) are not covered in this book.

Principles of GSM Security and the Evolution to UMTS Security

As UMTS can be seen as an evolution of the 2G (GSM) communication mobile systems, the security features for UMTS are based on the GSM security features and are enhanced. When UMTS was defined from the Third Generation Partnership Project, better known as 3GPP, there was the basic requirement to adopt the security features from GSM that have proved to be needed and robust and to be as compatible with the 2G security architecture as possible. UMTS should correct the problems with GSM by addressing its real and perceived security weaknesses and to add new security features to secure the new services offered by 3G.

The limitations and weaknesses of the GSM security architecture stem largely from design limitations rather than from defects in the security mechanisms themselves. GSM has the following specific weaknesses that are corrected within UMTS.

- Active attacks using a false base station:
  - used as "IMSI catcher" (collect "real" IMSIs of MSs that try to connect with the base stations) $-> $ cloning risk;
  - used to intercept mobile originated calls – encryption is controlled by network, so user is unaware if it is not on.
- Cipher keys and authentication data are transmitted in clear between and within networks:
  - signaling system vulnerable to interception and impersonation.
- Encryption of the user and signaling data does not carry far enough through the network to prevent being sent over microwave links (BTS to BSC) – encryption terminated too soon.
- Possibility of channel hijack in networks that do not offer confidentiality.
- Data integrity is not provided, except traditional noncryptographic link-layer checksums.
- IMEI (International Mobile Equipment Identity – unique) is an unsecured identity and should be treated as such – as the terminal is an unsecured environment, trust in the terminal identity is misplaced.
- Fraud and lawful interception were not considered in the design phase of 2G.
- There is no HE knowledge or control of how an SN (Serving Network) uses authentication parameters for HE subscribers roaming in that SN.
- Systems do not have the flexibility to upgrade and improve security functionality over time.
- Confidence in strength of algorithms:
  - failure to choose best authentication algorithm
  - improvements in cryptanalysis of A5/1
    - key length too short
    - lack of openness in design and publication.

Furthermore, there are challenges that security services will have to cope within 3G systems, and these will probably be:

- Totally new services are likely to be introduced.
- There will be new and different providers of services.

- Mobile systems will be positioned as preferable to fixed-line systems for users.
- Users will typically have more control over their service profile.
- Data services will be more important than voice services.
- The terminal will be used as a platform for e-commerce and other sensitive applications.

The following features of GSM security are reused for UMTS:

- User authentication and radio interface encryption.
- Subscriber identity confidentiality on the radio interface.
- SIM as a removable, hardware security module in UMTS, called USIM:
  – terminal independent;
  – management of all customer parameter.

1. Operation without user assistance.
2. Minimized trust of the SN by the HE.

1.6.2 UMTS Security Architecture

Based on Figure 1.38, which shows the order of all transactions of a connection, the next section will cover Authentication and Security Control and explain the overall security functions for the connection.

The 3G security architecture (Figures 1.39 and 1.40) is a set of security features and enhancements that are fully described in *3GPP 33.102* and is based on the three security principles.

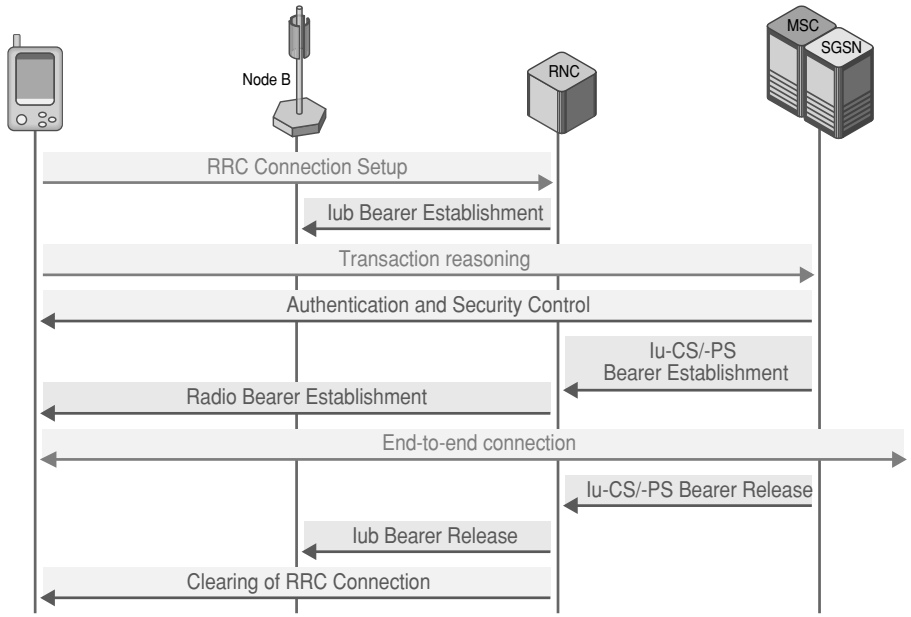


Figure 1.38 Network transitions.

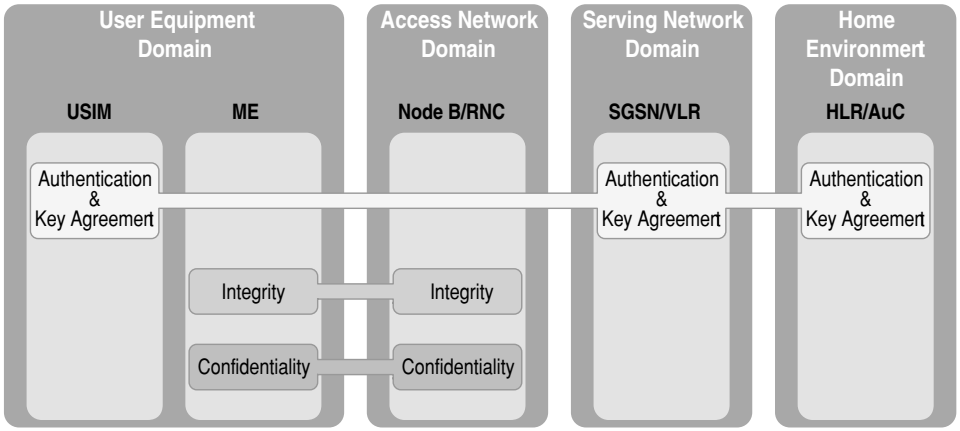


Figure 1.39 UMTS security architecture.

Authentication and Key Agreement (AKA)

Authentication is provided to assure the claimed identity between the user and the network. It is divided into two parts:

- Authentication of the user toward the network.
- Authentication of the network toward the user (new in UMTS).

This is done in so-called one-pass authentication, reducing messages sent back and forth. After these procedures the user will be sure that he is connected to his served/trusted network and the network is sure that the claimed identity of the user is true. Authentication is needed for other security mechanisms such as confidentiality and integrity.

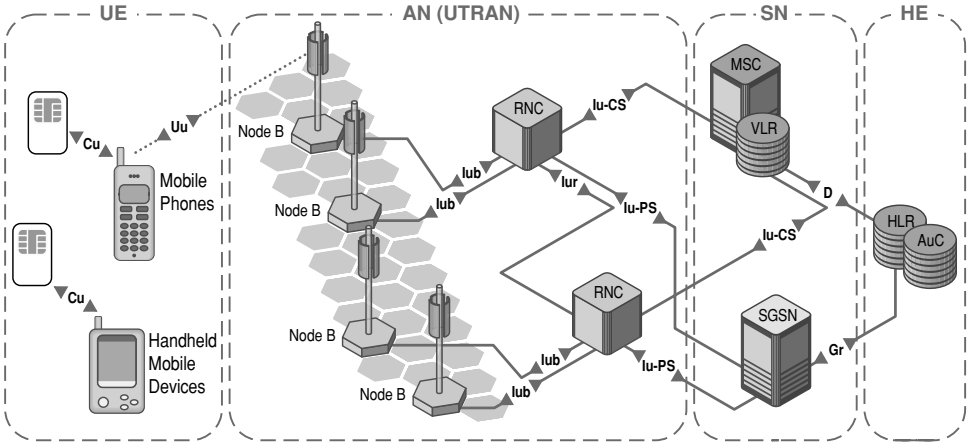


Figure 1.40 UMTS interface and domain architecture overview.

Integrity

Integrity protection is used to secure that the content of a signaling message between the user and the network has not been manipulated, even if the message might not be confidential. This is done by generating "stamps" individually from the user and the network that are added to the transferred signaling messages. The stamps are generated based on a pre-shared secret key K, which is stored in the USIM and the AuC. At transport level, the integrity is checked by CRC checksum, but these measures are only to achieve bit-error-free communication and are not equivalent to transport level integrity.

Confidentiality

Confidentiality is used to keep information secured from unwanted parties. This is achieved by ciphering the user/signaling data between the subscriber and the network and by referring to the subscriber by temporary identities (TMSI/P-TMSI) instead of using the global identity, IMSI. Ciphering is carried out between the user's terminal (USIM) and the RNC. User confidentiality is between the subscriber and the VLR/SGSN. If the network does not provide user data confidentiality, the subscriber is informed and has the opportunity to refuse connections.

Parts that are confidential are:

- Subscriber identity.
- Subscriber's current location.
- User data (voice and data).
- Signaling data.

1.6.3 Authentication and Key Agreement (AKA)

UMTS security starts with the AKA, the most important feature in the UMTS system. All other services depend on it since no higher level services can be used without authentication of the user.

Mutual Authentication

- Identifying the user to the network.
- Identifying the network to the user.

Key Agreement

- Generating the cipher key.
- Generating the Integrity key.

After Authentication and Key Agreement

- Integrity protection of messages.
- Confidentiality protection of signaling data.
- Confidentiality protection of user data.

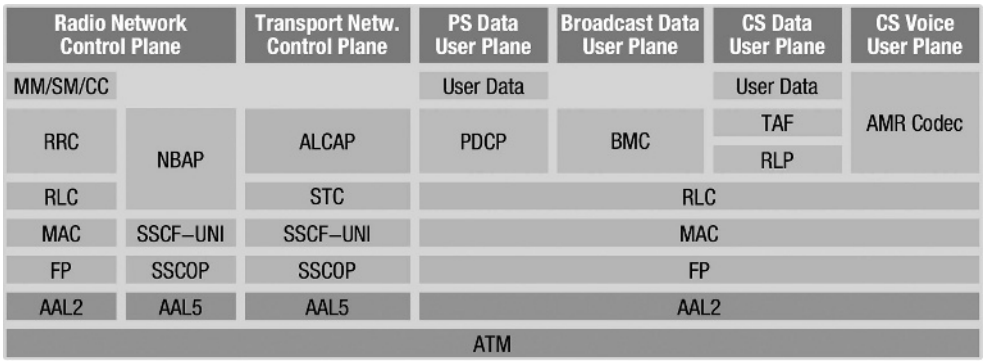


Figure 1.41 Example of AV sending from HE to SN in authentication data response.

The mechanism of mutual authentication is achieved by the user and the network showing knowledge of a secret key (K) which is shared between and available only to the USIM and the AuC in the user's HE. The method was chosen in such a way as to achieve maximum compatibility with the current GSM security architecture and facilitate migration from GSM to UMTS. The method is composed of a challenge/response protocol identical to the GSM subscriber authentication and key establishment protocol combined with a sequence number-based one-pass protocol for network authentication.

The authenticating parties are the AuC of the user's HE (HLR/AuC) and the USIM in the user's MS. The mechanism consists of the distribution of authentication data from the HLR/AuC to the VLR/SGSN and a procedure to authenticate and establish new cipher and integrity keys between the VLR/SGSN and the MS.

AKA Procedure

Once the HE/AuC has received a request from the VLR/SGSN, it sends an ordered array of *n* Authentication Vectors (AVs) to the VLR/SGSN. (Figure 1.41). Each AV consists of the following components: a Random Number (RAND), an Expected Response (XRES), a Cipher Key (CK), an Integrity Key (IK), and an Authentication Token (AUTN). Each AV is valid only for one AKA between the VLR/SGSN and the USIM and is ordered based on sequence number. The VLR/SGSN initiates an AKA by selecting the next AV from the ordered array and sending the parameters RAND and AUTN to the user. If the AUTN is accepted by the USIM, it produces a Response (RES) that is sent back to the VLR/SGSN. AVs in a particular node are used on a first-in/first-out basis. The USIM also computes CK and IK. The VLR/SGSN compares the received RES with XRES. If they match, the VLR/SGSN considers the AKA exchange to be successfully completed. The established keys CK and IK will then be transferred by the USIM and the VLR/SGSN to the entities that perform ciphering and integrity functions. VLR/SGSNs can offer secure service even when HE/AuC links are unavailable by allowing them to use previously derived cipher and integrity keys for a user so that a secure connection can still be set up without the need for an AKA. Authentication is in that case based on a shared integrity key, by means of data integrity protection of signaling messages (Figure 1.42).

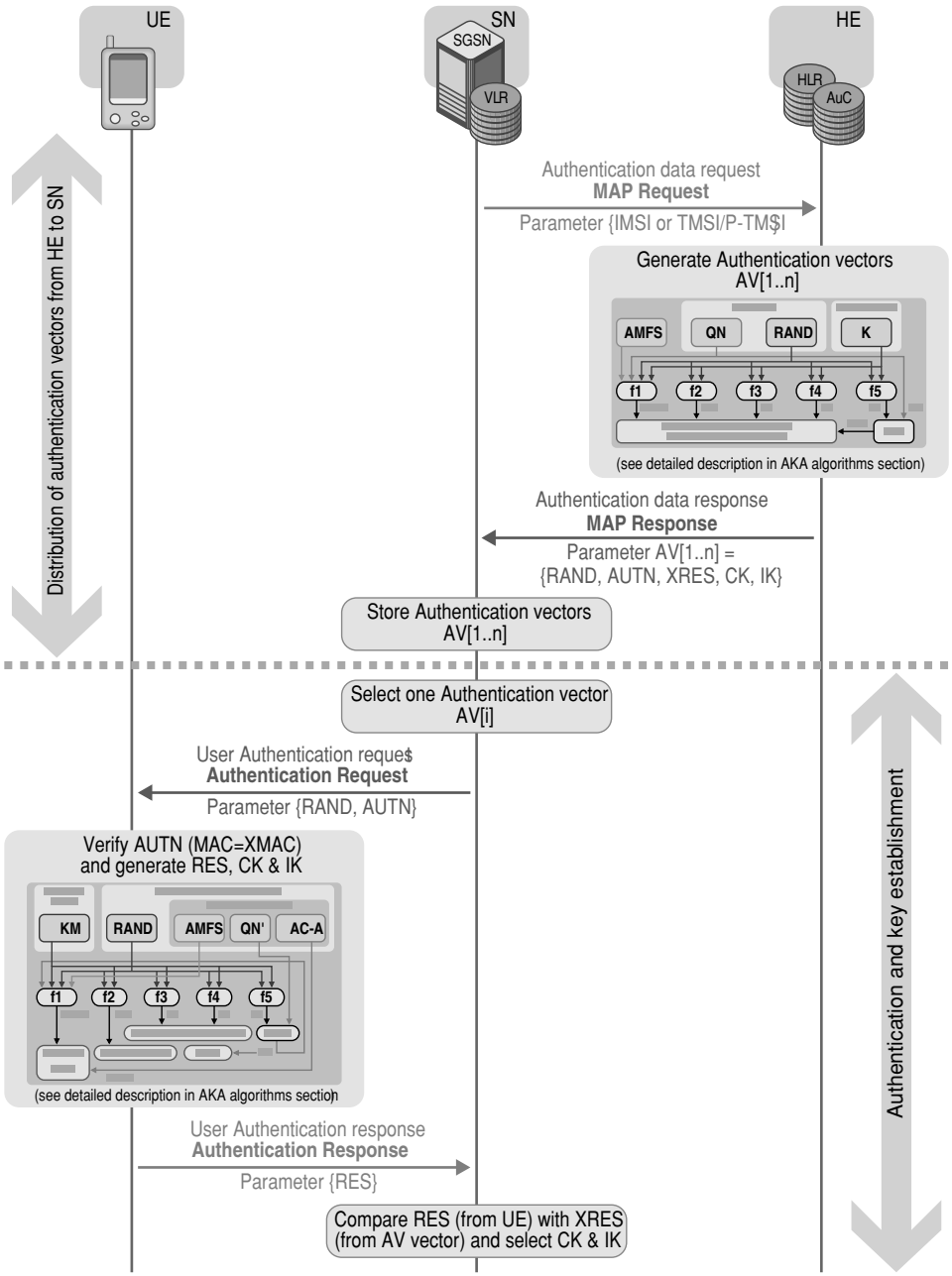


Figure 1.42 AKA procedure – sequence diagram.

AKA is performed when the following events happen:

- Registration of a user in an SN.
- After a Service Request.
- Location Update Request.
- Attach Request.
- Detach Request.
- Connection reestablishment request.

Registration of a subscriber in an SN typically occurs when the user goes to another country. The coverage area of an operator is nationwide, and roaming between national operators will therefore be limited. The first time the subscriber connects to the SN, he gets registered in the SN.

Service Request is the possibility for higher level protocols/applications to ask for AKA to be performed, e.g. performing AKA to increase security before an online banking transaction. The terminal updates the HLR regularly with its position in Location Update Requests.

Attach request and detach request are procedures to connect and disconnect the subscriber to/from the network.

Connection re-establishment request is performed when the maximum number of local authentications has been conducted.

A weakness of the AKA is that the HLR/AuC does not check whether the information sent from the VLR/SGSN (authentication information) is correct or not.

Algorithms Used for AKA (Tables 1.5 and 1.6)

The security features of UMTS are fulfilled with a set of cryptographic functions and algorithms. A total of 10 functions are needed to perform all the necessary features, f0–f5, f8, and f9.

f0 is the random challenge generating function, the next seven are key generating functions, and so they are all operator-specific. The keys used for authentication are generated only in the USIM and the AuC, the two domains that the same operator is always in charge of.

Functions f8 and f9 are used in USIM and RNC, and since these two domains may be of different operators, they cannot be operator-specific. The functions use the pre-shared secret key (K) indirectly. This prevents distributing K in the network, and keeps it safe in the USIM and AuC.

The functions fl–f5 are called key-generating functions and are used in the initial AKA procedure. The lifetime of Key depends on how long the keys have been used. The maximum limits for use of same keys are defined by the operator, and whenever the USIM finds the keys being used for as long as allowed, it will trigger the VLR/SGSN to use a new AV.

The functions fl–f5 will be designed so that they can be implemented with an 8-bit microprocessor running at 3.25 MHz with 8-kbyte ROM and 300-kbytes RAM and produce AK, XMAC-A, RES, CK, and IK in less than 500-ms execution time.

When generating a new AV the AuC reads the stored value of the sequence number SQN and then generates a new SQN′ and a random challenge RAND. Together with the stored AV and Authentication Management Field (AMF) and the pre-shared secret key (K), these four input parameters are ready to be used. The functions fl–f5 use these inputs and generate the values for the Message Authentication Code, MAC-A, the expected result, XRES, the CK, the IK, and the AK. With the SQN XOR'ed AK, AMF and MAC, the AUTN is made. The AV is sent

Table 1.5 AKA function overview

Function	Description	Input parameter	Output parameter
f0	Random challenge generating function	RAND	RAND
fl	Network authentication function	AMF, K, RAND	MAC-A (AuC side)/XMAC-A (UE side)
f2	User authentication function	K, RAND	RES (UE side)/XRES (AuC side)
f3	Cipher key derivation function	K, RAND	CK
f4	Integrity key derivation function	K, RAND	IK
f5	Anonymity key derivation function	K, RAND	AK
f8	Confidentiality key stream generating function	COUNT-C, BEARER, DIRECTION, LENGTH, CK	< Key stream block>
f9	Integrity stamp generating function	IK, FRESH, DIRECTION, COUNT-I, MESSAGE	MAC-I (UE side)/XMAC-I (RNC side)

Table 1.6 AKA parameter overview

Parameter	Definition	Bit size
K	Pre-shared secret key stored in the USIM and AuC	128
RAND	Random challenge to be sent to the USIM	128
SQN	Sequence Number	48
AK	Anonymity Key	48
AMF	Authentication Management Field	16
MAC	Message Authentication Code	64
MAC-A/XMAC-A	MAC used for AKA	64
MAC-I/XMAC-I	Message authentication code for data integrity	64
CK	Cipher key for confidentiality	128
IK	Integrity key for integrity checking	128
RES	Response	32-128
XRES	Expected result from the USIM	32-128
AUTN	Authentication token that authenticates the AuC toward the USIM (AMF, MAC-A, SQN')	128 (16 + 64 + 48)
COUNT-I	Integrity sequence number	32
FRESH	Network-side random value	32
DIRECTION	Either 0 (UE $\rightarrow$ RNC $\rightarrow$ uplink) or 1 (RNC->UE=downlink)	1
MESSAGE	Message itself	Variant

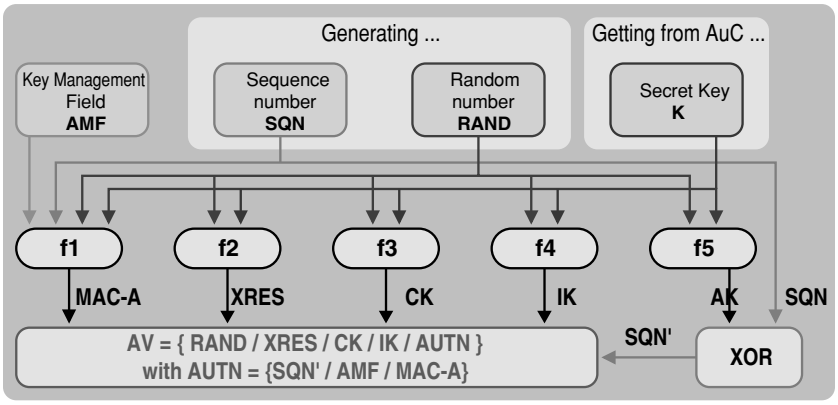


Figure 1.43 Authentication Vector generation on the AuC side (HE).

to the SGSN/VLR and stored there, while the parameter pair AUTN and RAND are then sent from the SGSN/VLR to the user. The CK and IK are used, after a successful authentication, for confidentiality (ciphering) and integrity (Figure 1.43).

Only one of the four parameters of the Auc, the pre-shared secret key (K), is stored in the USIM. The rest of the parameters it has to receive from the network (RAND and AUTN). The secret key K is then used with the received AMF, SQN′, and RAND to generate the Expected Message Authentication Code (XMAC-A). This is then compared with the MAC-A. If the XMAC and MAC matches, the USIM has authenticated that the message is originated in its HE and thereby connected to an SN that is trusted by the HE. With a successful network authentication, the USIM verifies if the sequence number received is within the correct range. With a sequence number within the correct range, the USIM continues to generate the RES, which is send back to the network to verify a successful user authentication (Figure 1.44).

1.6.4 Kasumi/Misty

The Kasumi algorithm is the core algorithm used in functions f8 (Confidentiality) and f9 (Integrity). Kasumi is based on the block cipher "Misty" proposed by Mitsuru Matsui (Mitsubishi) and first published in 1996. Misty translated from English to Japanese means Kasumi.

Misty was designed to fulfill the following design criteria:

High security

- Provable security against differential and linear cryptanalysis.

Multiplatform

- High speed in both software and hardware implementations:
  - Pentium III (800MHz) (Assembly Language Program)
    - encryption speed 230 Mbps
  - ASIC H/W (Mitsubishi 0.35 micron CMOS Design Library)
    - encryption speed 800 Mbps
    - gate size 50 kgates

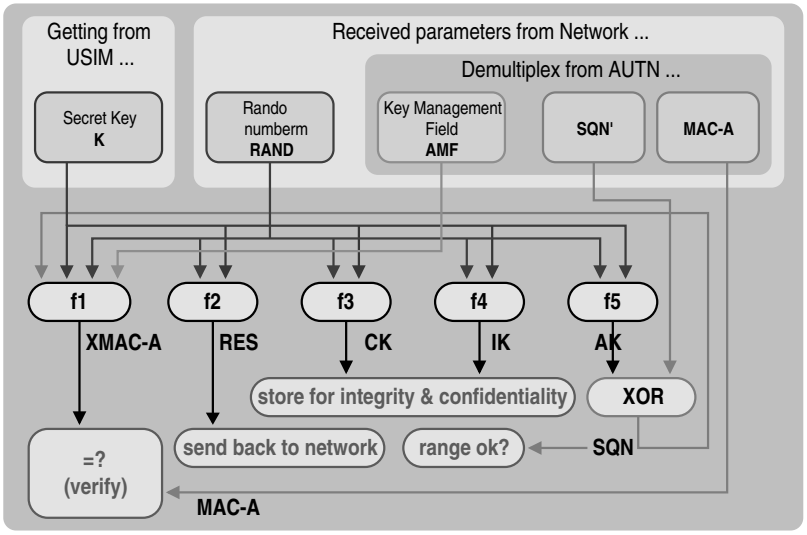


Figure 1.44 User Authentication Response on the user side.

Compact

- Low gate count and low power consumption in hardware:
  - ASIC (Mitsubishi 0.35 micron CMOS Design Library)
    - encryption speed 72Mbps
    - gate size 7.6 kgates
- A requirement for W-CDMA encryption algorithm: "gate size must be smaller than 10 kgates".

Kasumi is a variant of Misty 1 designed for W-CDMA systems and has been adopted as a mandatory algorithm for data confidentiality and data integrity in W-CDMA by 3GPP in 1999. Here are some examples of improvement:

- Simpler key schedule.
- Additional functions to complicate encryption analysis without affecting proven security aspects.
- Changes to improve statistical properties.
- Minor changes to speed up.
- Stream ciphering f8 uses Kasumi in a from of output feedback, but with:
  - BLKCNT added to prevent cycling
  - initial extra encryption added to protect against chosen plaintext attack and collision
- Integrity f9 uses Kasumi to form CBC MAC with:
  - nonstandard addition of second feedforward.

Mitsubishi Electric Corporation, Japan, holds the rights on essential patents on the algorithms. Therefore, the Beneficiary must get a separate royalty-free IPR License Agreement from Mitsubishi.

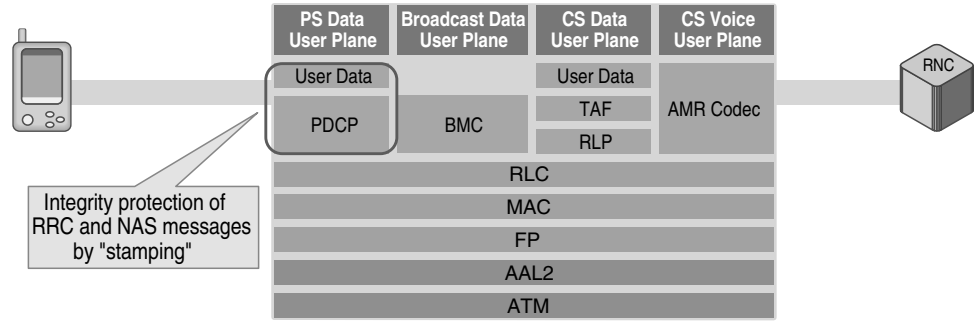


Figure 1.45 Integrity protection on Iub control plane.

Basically Kasumi is a block cipher that produces a 64-bit output from a 64-bit input under the control of a 128-bit key. A detailed description can be found in the *3GPP Specification TS 35.202*. Misty/Kasumi has been widely studied since its publication, but no serious flaws have been found.

1.6.5 Integrity – Air Interface Integrity Mechanism

Most control signaling information elements that are sent between the UE and the network are considered sensitive and must be integrity protected. Integrity protection will apply at the RRC layer. A message integrity function (f9) will be applied on the signaling information transmitted between the UE and the RNC. User data are, on the other hand, not integrity protected and it is up to higher level protocols to add this if needed. Integrity protection is required, not optional, in UMTS for signaling messages.

After the RRC connection has been established and the security mode set up procedure has been performed, all dedicated control signaling messages between UE and the network will be integrity protected (Figure 1.45).

Threats Against Integrity

Manipulation of messages is the one generic threat against integrity. This includes deliberate or accidental modification, insertion, replaying, or deletion by an intruder.

Both user data and signaling/control data are vunerable to manipulation, and the attacks may be conducted on the radio interface, in the fixed network, or on the terminal and the USIM/UICC.

The threats against integrity can be summarized as:

- *Manipulation of transmitted data:* Intruders may manipulate data transmitted over all reachable interfaces.
- *Manipulation of stored data:* Intruders may manipulate data stored on system entities, in the terminal, or stored by the USIM. These data include the IMEI stored on the terminal, and data and applications downloaded to the terminal or USIM. Only the risks associated with the threats to data stored on the terminal or USIM are regarded to be significant, and only the risk for manipulation of the IMEI is regarded as being of major importance.

- *Manipulation by masquerading:* Intruders may masquerade as a communication participant and thereby manipulate data on any interface. It is also possible to manipulate the USIM behavior by masquerading as the originator of malicious applications or data downloaded to the terminal or USIM.

  On the radio interface this is considered to be a major threat, whereas manipulation of the terminal or USIM behavior by masquerading as the originator of applications and/or data is considered to be of medium significance. Masquerading could be done both to fake a legal user and to fake an SN.

Distribution of Keys

The integrity protection in UMTS is implemented between the RNC and the UE. Therefore, IK must be distributed from the AuC to the RNC. The IK is part of an AV which is sent to the SN (VLR/SGSN) from the AuC following an authentication data request. To facilitate subsequent authentications, up to five AVs are sent for each request. The IK is sent from the VLR/SGSN to the RNC as part of an RANAP message called security mode command.

Integrity Function f9

The function f9 is used in a similar way as the AUTN. It adds a "stamp" to messages to ensure that the message is generated at the claimed identity, either the USIM or the SN, on behalf of the HE. It also makes sure that the message has not been tampered with.

The input parameters to the algorithm are the Integrity Key (IK), the integrity sequence number (COUNT-I), a random value generated by the network side (FRESH), the direction bit (DIRECTION), and the signaling data (MESSAGE). On the basis of these input parameters the user computes MAC for data integrity (MAC-I) using the integrity algorithm f9. The MAC-I is then appended to the message when sent over the radio access link. The receiver computes XMAC-I on the message received in the same way as the sender computed MAC-I on the message sent and verifies the data integrity of the message by comparing it to the received MAC-I (Figure 1.46).

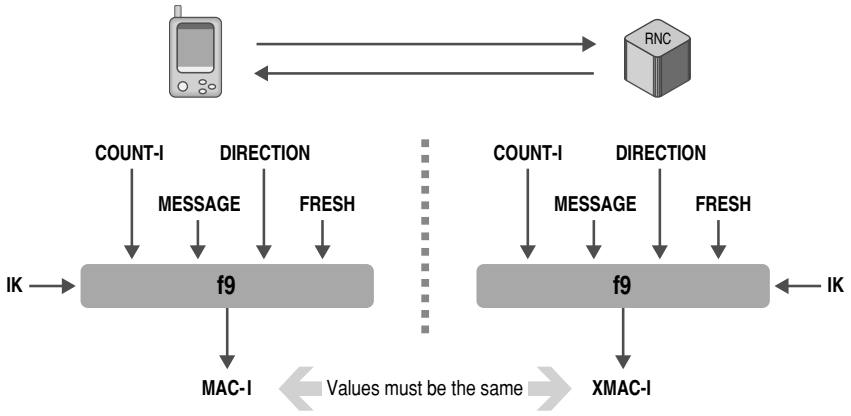


Figure 1.46 Integrity check procedure.

Protection against replay is important and guaranteed with:

- The value of COUNT-I is incremented for each message, while the generation of a new FRESH value and initialization of COUNT-I take place at connection setup.
- The COUNT-I value is initialized in the UE and therefore primarily protects the user side from replay attacks. Likewise the FRESH value primarily provides replay protection for the network side.

Integrity Initiation – Security Mode Setup Procedure

The VLR/SGSN initiates integrity protection (and encryption) by sending the RANAP message security mode control to the SRNC. This message contains a list of allowed integrity algorithms and the IK to be used. Since the UE can have two ciphering and integrity key sets (for the PS and CS domains, respectively), the network includes a CN type indicator in the security mode command message.

The security mode command to UE starts the downlink integrity protection; i.e., all subsequent downlink messages sent to the UE are integrity protected. The security mode complete from UE starts the uplink integrity protection; i.e., all subsequent messages sent from the UE are integrity protected. The network must have the "UE security capability" information before the integrity protection can start; i.e., the "UE security capability" must be sent to the network in a UMTS security-integrity protection unprotected message. Returning the "UE security capability" to the UE in a protected message later will allow UE to verify that it was the correct "UE security capability" that reached the network.

Some messages does not include integrity protection (Figure 1.47); these messages are:

- HANDOVER TO UTRAN COMPLETE
- PAGING TYPE 1
- PUSCH CAPACITY REQUEST
- PHYSICAL SHARED CHANNEL ALLOCATION
- RRC CONNECTION REQUEST
- RRC CONNECTION SETUP
- RRC CONNECTION SETUP COMPLETE
- RRC CONNECTION REJECT
- RRC CONNECTION RELEASE (Common Control Channel (CCCH) only)
- SYSTEM INFORMATION (BROADCAST INFORMATION)
- SYSTEM INFORMATION CHANGE INDICATION
- TRANSPORT FORMAT COMBINATION CONTROL (TM DCCH only)

Key Lifetime

To avoid attacks using compromised keys, a mechanism is needed to ensure that a particular integrity key set is not used for an unlimited period of time. Each time an RRC connection is released, the values $START_{CS}$ and $START_{PS}$ of the bearers that were protected in that RRC connection are stored in the USIM. When the next RRC connection is established these values are read from the USIM.

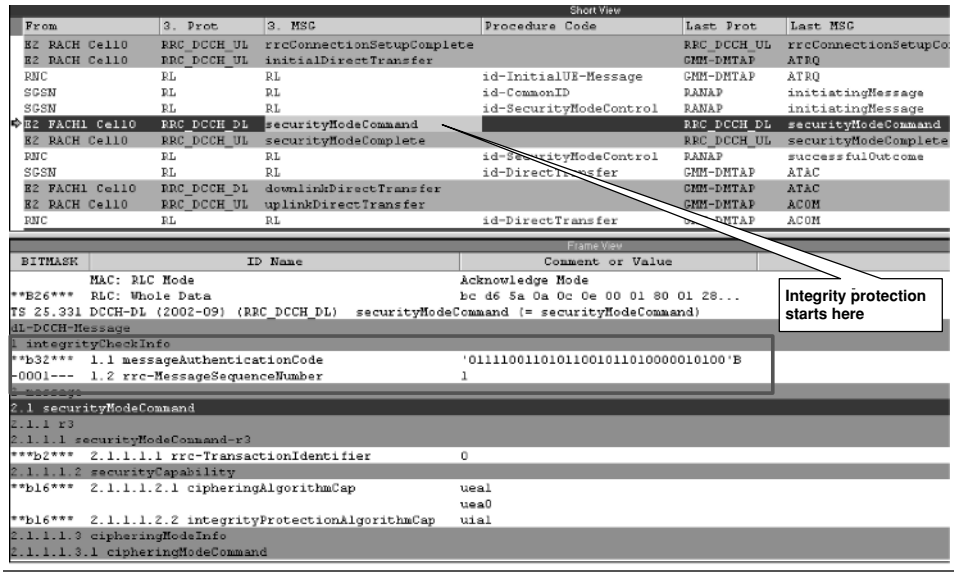


Figure 1.47 Example of "stamped" message for integrity check.

The operator will decide on a maximum value for $START_{CS}$ and $START_{PS}$. This value is stored in the USIM. When the maximum value has been reached, the cipher key and integrity key stored on USIM will be deleted, and the ME triggers the generation of a new access link key set (a cipher key and integrity key) at the next RRC connection request message.

Weaknesses

The main weaknesses in UMTS integrity protection mechanisms are:

- Integrity keys used between UE and RNC generated in VLR/SGSN are transmitted unencrypted to the RNC (and sometimes between RNCs).
- Integrity of user data is not offered.
- For a short time during signaling procedures, signaling data are unprotected and hence exposed to tampering.

1.6.6 Confidentiality – Encryption (Ciphering) on Uu and Iub

Threats Against Confidentiality

There are several different threats against confidentiality-protected data in UMTS. The most important threats are:

- *Eavesdropping* on user traffic, signaling, or control data on the radio interface.
- *Passive traffic analysis:* Intruders may observe the time, rate, length, sources, or destinations of messages on the radio interface to obtain access to information.
- *Confidentiality of authentication data in the UICC/USIM:* Intruders may obtain access to authentication data stored by the service provider in the UICC/USIM.

The radio interface is the easiest interface to eavesdrop, and should therefore always be encrypted. If there is a penetration of the cryptographic mechanism, the confidential data would be accessible on any interface between the UE and the RNC. Passive traffic analysis is considered as a major threat. Initiating a call and observing the response, active traffic analysis, is not considered as a major threat. Disclosure of important authentication data in the USIM, i.e. the long-term secret K, is considered a major threat. The risk of eavesdropping on the links between RNCs and the UICC-terminal interface is not considered a major threat, since these links are less accessible for intruders than the radio access link. Eavesdropping of signaling or control data, however, may be used to access security management data or other information, which may be useful in conducting active attacks on the system.

Ciphering Procedure

Ciphering in UMTS is performed between UE and RNC over air and Iub interfaces. Figure 1.48 shows the protocol stack of the Iub interface for Rel. 99.

The Iub protocol stack contains a Radio Network Control Plane, a Transport Network Control Plane, and a User Plane for AMR-coded voice, IP packages, video streaming, etc. The Radio Network Control Plane is split into two parts, the NAS and the NBAP. The NAS contains Mobility Management (MM), Session Management (SM), and Call Control Management (CC) for communication between UE and CN.

Before UE and RNC are able to exchange NAS messages and user data, one or more transport channels are required. All information related to the establishment, modification, and release of transport channels is exchanged between RNC and Node B over NBAP and the Access Link Control Application Part (ALCAP). Transport channels are based on AAL2 connections. The concept of those transport channels is very important for the understanding of ciphering and integrity protection.

The task of the transport channel is an optimal propagation of signaling information and user data over the air interface. In order to do so, a transport channel is composed of several RBs. The characteristic of every RB is defined during establishment by the NBAP and RRC layer. This is done by a list of attributes, the so-called Transport Format Set (TFS). The TFS describes the way of data transmission using different parameters, like block size, transmission time interval (TTI), and channel coding type.

The UTRAN selects these RABs for the communication between mobile and network, which use the radio resources in the most efficient way. Every RAB has its own identifier and

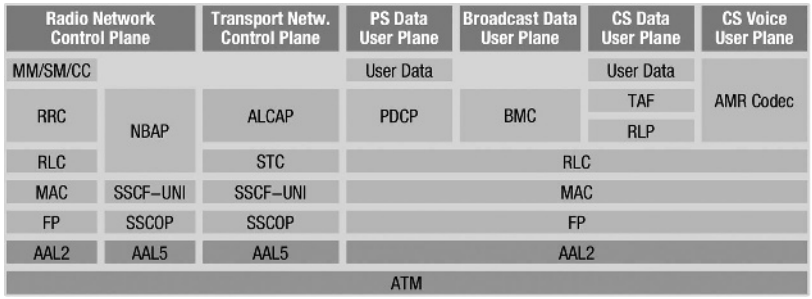


Figure 1.48 Iub protocol stack.

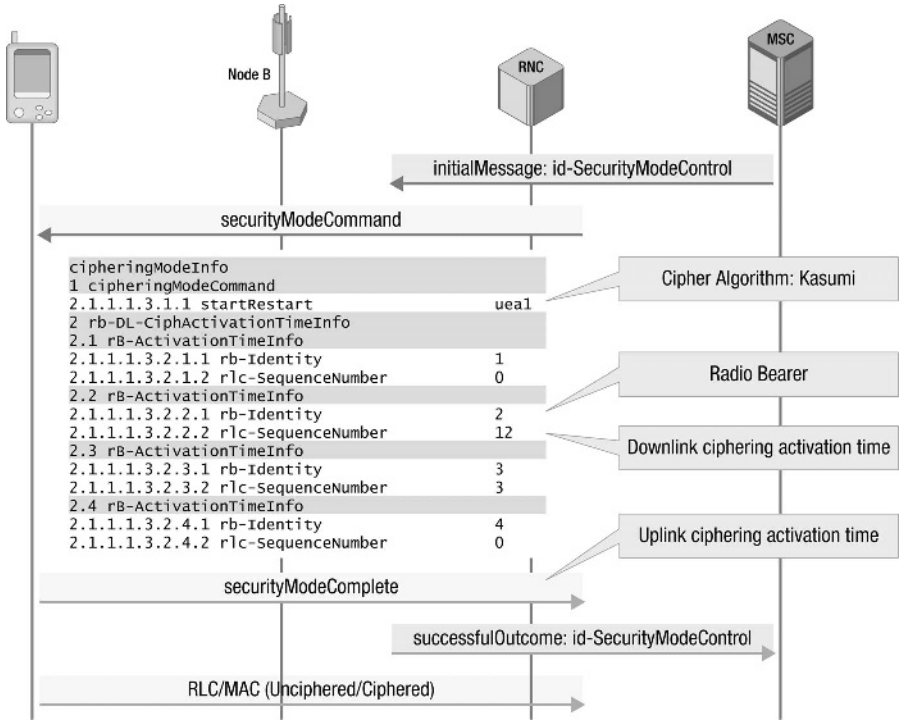


Figure 1.49 Ciphering activation procedure.

every transport block has its own sequence number. This technique allows from one side a fast switchover between RBs and from the other one a parallel communication over several RABs. This technique requires a bearer-independent ciphering mechanism.

Ciphering will be activated with the messages flow shown in Figure 1.49. Ciphering is always related to a certain transport channel. Therefore, ciphering will be activated independently for control and user planes and independently for packet-switched and circuit-switched planes. In other words, if a mobile subscriber has two independent sessions (voice calls and IP packet transfer) activated, UE and RNC need to exchange the ciphering activation procedure twice. It is important to note that NAS messages exchanged prior to ciphering activation (typically the Authentication procedure) are not ciphered.

The message **securityModeCommand** establishes the Activation Time for the RABs in downlink direction and the message **securityModeComplete** determines the Activation Time in uplink direction. Ciphering for a certain RAB starts for that RLC (Radio Link Control) block where Sequence Number is equal to Activation Time.

The ciphering depth depends on the RLC mode. The RLC protocol contains Control PDUs (never ciphered) and Data PDUs. For Data PDUs, the RLC protocol works in three different modes:

- Unacknowledged Mode (UM).
- Acknowledged Mode (AM).
- Transparent Mode (TM).

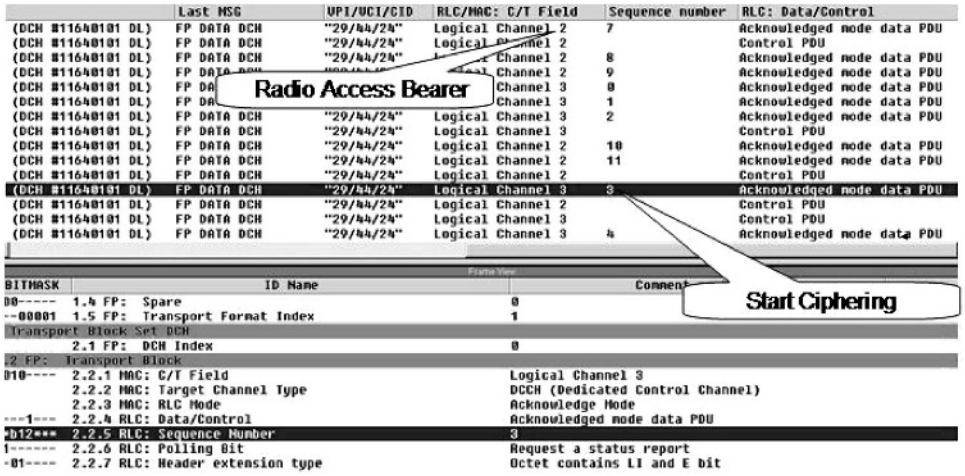


Figure 1.50 RLC: Ciphering Activation Time.

UM and AM messages (e.g. data) are secured against bit errors with a check sequence, while TM information (e.g. AMR voice) is not. Therefore, RLC UM and RLC AM are ciphered beginning with the RLC layer and above, while ciphering for RLC TM already starts with the MAC layer (Figure 1.50).

The Kasumi algorithm requires the following parameters (Figure 1.51):

- Cipher Sequence Number (COUNT).
- Direction (uplink or downlink).
- KB Identifier.
- Block Length.
- Ciphering Key (CK).

CK is never sent over the Uu and Iub interfaces. The RNC receives this value from MSC or SGSN and the USIM calculates CK as described before (Figure 1.51).

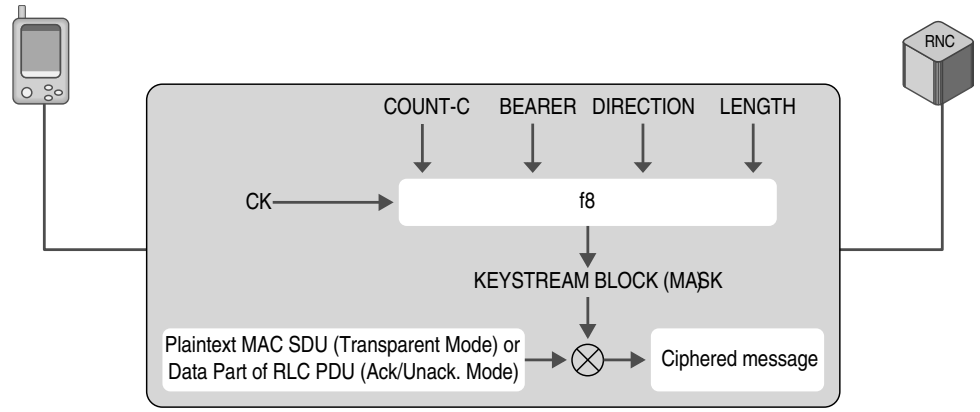


Figure 1.51 UTRAN encryption.

COUNT is initially derived from the START value of the **rrcConnectionSetup Complete** message. The START value is not constant during a ciphering session. It can be modified by different procedures, such as Cell Reselection or Channel Type Switching. The following messages can trigger an update of the COUNT value:

- RRC_rrcConnectionSetupComplete
- RRC_physicalChannelReconfigurationComplete
- RRC_transportChannelReconfigurationComplete
- RRC_radioBearerSetupComplete
- RRC_radioBearerReconfigurationComplete
- RRC_radioBearerReleaseComplete
- RRC_utranMobilityInformationComplete
- RRCInitialDirectTransfer

If the message **securityModeFailure** is received the ciphering information will be removed from USIM and RNC.

Advantages of this method:

1. The key can be generated even before the message is available to the algorithm.
2. To decipher, the receiving side generates the same Keystream Block (Mask) and adds it, bit by bit, to the received encrypted message. This second addition of the mask cancels out the mask that was previously added and thereby decrypts the message.

A second bit-by-bit addition negates the first addition = successful deciphering!

Testing UMTS Networks when Ciphering is Active

As described earlier, ciphering in UMTS networks is also performed between the UE and RNC over the Uu (air) and the Iub interface. Ciphering causes the RRC and NAS messages to be encrypted (Figure 1.52).

RRC and NAS messages contain key information to perform network optimization and troubleshooting, which results in the fact that when ciphering is active, traditional protocol analyzer and network monitoring systems cannot be used to carry out these two very important tasks.

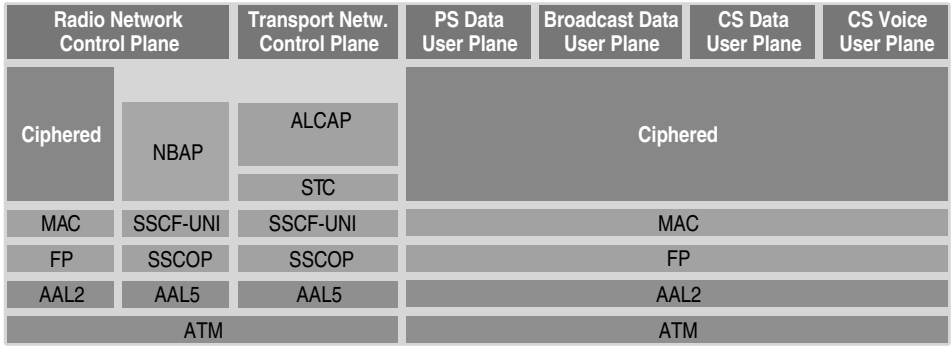


Figure 1.52 Ciphered Iub protocol stack.

In UMTS networks, in order to perform network optimization and troubleshooting, protocol test equipment would need the ability to decipher the messages. As shown here for the Iub interface, connected to the Iu and Iub, protocol analyzers collect the ciphering parameters, feed them to the deciphering algorithm, and allow full access to the content of the protocol messages. In addition to network optimization and troubleshooting, the equipment also enables the testing of the impact of Iub ciphering/deciphering on network element/network behavior and performance.

Please see Chapter 2 for a short introduction to network monitoring, troubleshooting, and network optimization.

1.6.7 UMTS Network Transactions

Figure 1.53 shows the order of the necessary transactions of a connection. It further indicates the interworking of pure signaling exchange and RB procedures.

The procedures running between UE, Node B, and RNC will exchange Access Stratum messages whereas procedures going through to the CN, MSC and SGSN, will exchange NAS messages.

1.7 Radio Interface Basics

To understand the relation between UTRAN signaling messages and the UE, it is also necessary to discuss some procedures and methods used on the UMTS air interface.

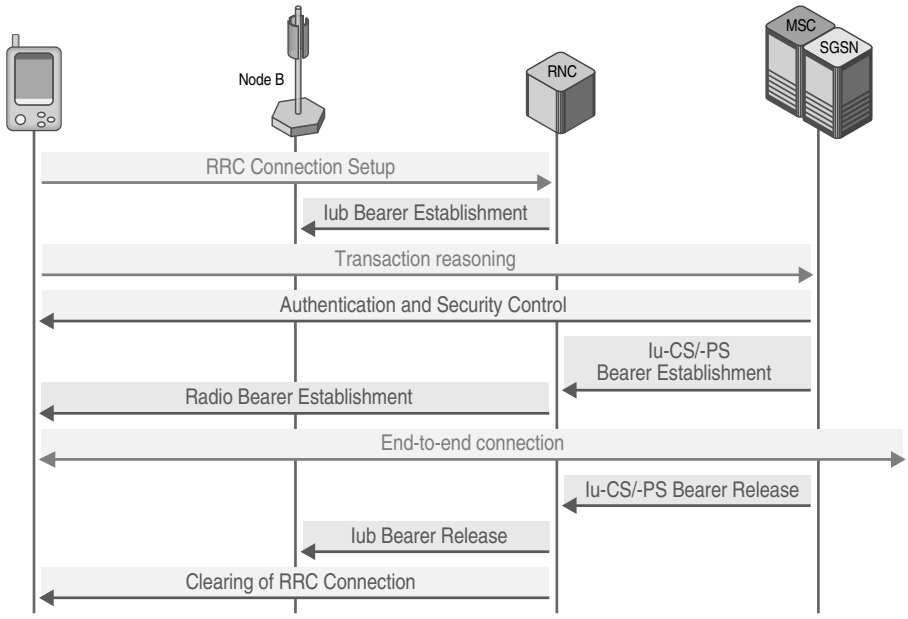


Figure 1.53 UMTS network transactions.

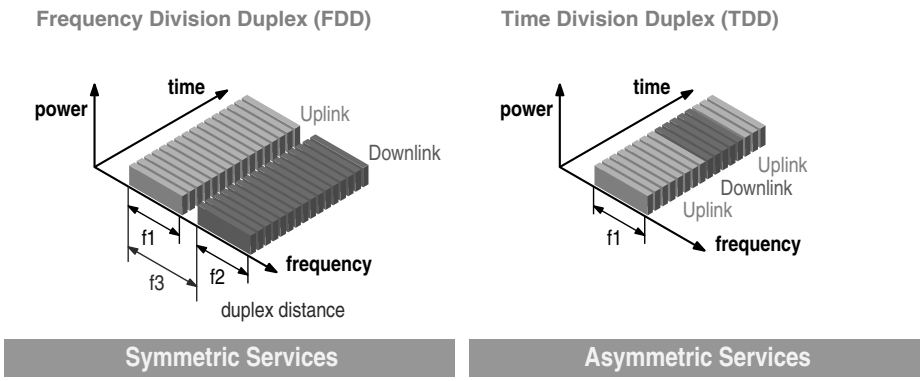


Figure 1.54 Duplex methods.

1.7.1 Duplex Methods

Duplex methods are used to separate transmit and receive signals, for example, speak and listen signals. Two different methods of duplex control are used on the radio interface. By these methods it is guaranteed that TX and RX data can be separated from each other. These methods have no limits for parallel usage of the radio interface (Figure 1.54).

One method is Frequency Division Duplex (FDD). It provides an uplink and downlink radio channel between network and user, and frequencies are separated by a duplex spacing. Users tune in between uplink and downlink frequencies to transmit and receive signals, respectively. FDD is also used in GSM, where the unidirectional frequency is 200 kHz.

The other method is Time Division Duplex (TDD). A common carrier is shared between uplink and downlink and resources are switched in time. Users are allocated to one or more time slots for uplink and downlink transmission. The main advantage of TDD operation is that it allows an asymmetric flow, which is more suitable for data transmission.

In UMTS, these methods will be used as UTRA-FDD and later as UTRA-TDD. The bandwidth of f1 and f2 will be 5 MHz, and the duplex distance will be 190 MHz.

1.7.2 Multiple Access Methods

Multiple access methods specify how user signals can be separated from each other. Again, there is no overall capacity of a cell or a radio access system that could be derived from this method (Figure 1.55).

Multiplex methods are used to divide the limited resources of a cell between the different MSs in a cell.

- FDMA: Uses different frequencies to separate the users. This technique is used in analog systems.
- TDMA: Uses different time slots over the whole frequency to separate the users. In this case, different users use the air interface resources at different times. This technique is used in GSM.
- CDMA: Uses the whole frequency bandwidth over the whole time. Using different codes applied to their data separates different users. This will be used in UMTS.

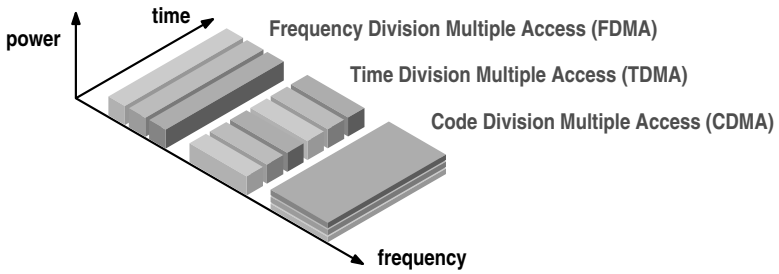


Figure 1.55 Multiple access methods.

For network operators, the difference in planning is that for FDMA and TDMA, frequency planning is the major task, whereas for CDMA, code planning is the major task.

1.7.3 UMTS CDMA

The tasks that result from the CDMA technique are mainly implemented in Node B and in the UE (Figure 1.56).

The following work steps must be performed before the signal can be transmitted via the antenna:

- Spreading of the data with Orthogonal Codes with Variable Spreading Factor (OVSF) codes.
- Scrambling of the spread stream with scrambling codes.
- Modulation of the digital signal onto the air interface.

The receiver will have to perform these steps in reverse order.

Since spreading codes and scrambling codes are important to identify UTRAN signaling messages belonging to a defined user, a short introduction to these techniques is given, while modulation is outside the scope of this book. However, the following section will demonstrate the process for CDMA-FDD only, because TDD is close to implementation, but typically not introduced into the networks yet.

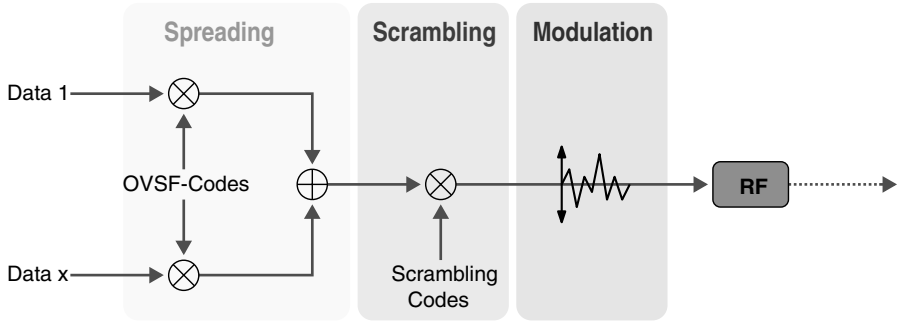


Figure 1.56 UMTS CDMA.

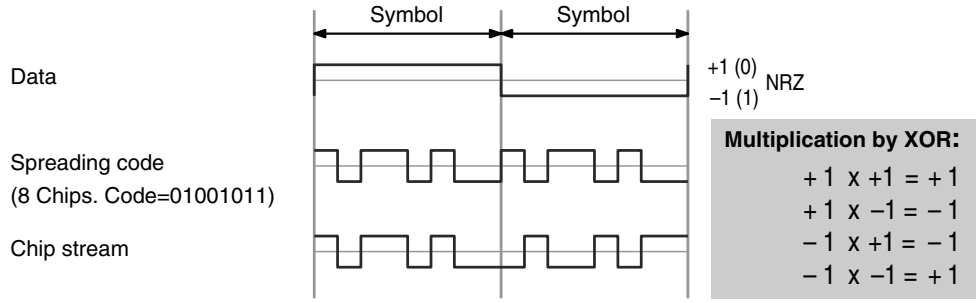


Figure 1.57 Spreading using Direct Sequence CDMA.

1.7.4 CDMA Spreading/Channelization

CDMA can use different methods of spreading channelization:

- Direct Sequence CDMA (DS-CDMA).
- Frequency Hopping CDMA (FH-CDMA).
- Time Hopping CDMA (TH-CDMA).
- Hybrid Modulation CDMA (HM-CDMA).
- Multi-Carrier CDMA (MC-CDMA).

UMTS will use, in the first stage, the DS-CDMA technique (Figure 1.57).

Every bit of the data (symbol) stream will be spread (coded) by a number of code bits (chips). By this, the data stream becomes a chip stream with the length:

data bits × code chips

The input data rate is also called symbol rate.

For the spreading, the data bit values have to be turned to nonreturn to zero (NRZ) codes: for example, +1 or –1. Binary zero is presented as +1 and binary one is presented as –1.

Multiplying the code to the bit using the XOR function performs the spreading. As can be seen, the chip stream is a picture of the code; i.e., if a binary zero has to be spread, the chip stream is the code. If a binary one has to be spread, the chip stream is the inverted code.

One of the main reasons for spreading is to convert a narrowband signal to a wideband signal, nearly as wide as the radio interface frequency band.

In UMTS, the chip stream always has the size of 3,840,000 chips/s, for example 3.84 Mcps, equal to a frequency of 3.84 MHz.

Depending on the data stream variable, spreading codes have to be used. First of all, the value of the code is not important, but its length is. Secondly, the used codes should be orthogonal; they differ completely from each other. In the uplink direction, the UE separates different data channels from each other by using different codes for each data channel.

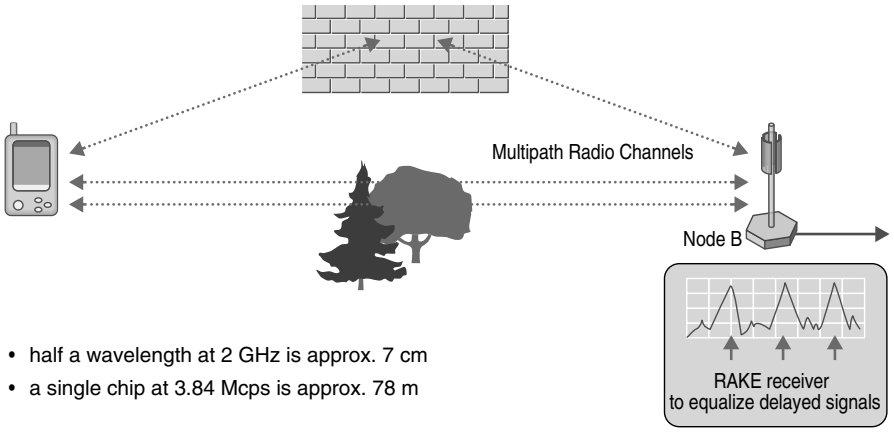


Figure 1.58 Multipath.

1.7.5 Microdiversity – Multipath (FDD and TDD)

The transmission of a radio wave is not straight. Because of reflection, diffraction, and scattering of the radio wave, the received signal appears as a multiple of the sent signal, different in time. This phenomenon is called *multipath* (Figure 1.58).

In UMTS, it means that the UE and the Node B receive multiple signals from each other. A special *RAKE receiver* is implemented in both units to overcome this problem. It receives each of the parallel signals in a finger and combines them to one strong output signal, which will be given to the higher layer.

Microdiversity stands for the small diversity the receiver has to deal with.

1.7.6 Microdiversity – Softer Handover (FDD)

A special case where microdiversity is used is the *Softer Handover.* In this situation the UE is connected to more than one sector of a Node B (Figure 1.59). The advantage is a stronger RX signal. The disadvantage is that more radio resources are in use than necessary. It is up to the network planning if and when this feature is used.

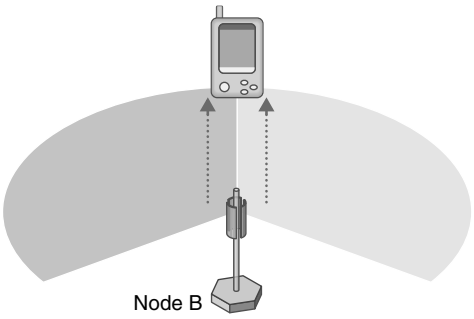


Figure 1.59 Softer Handover.

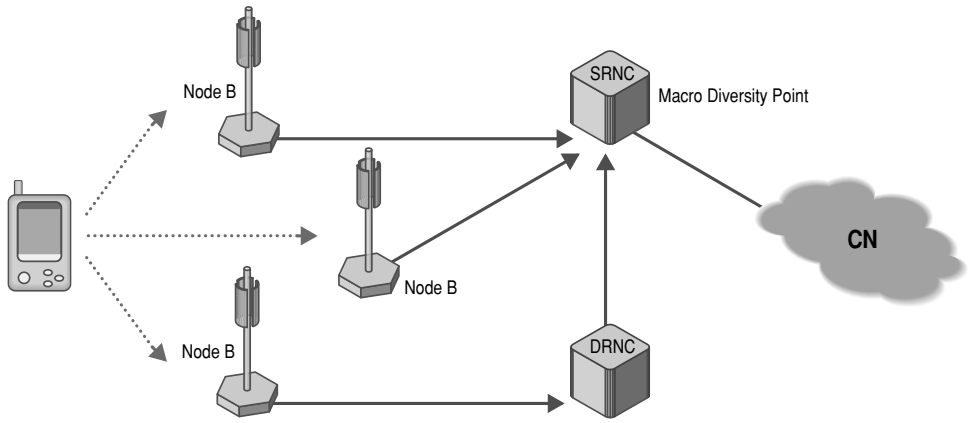


Figure 1.60 Soft Handover.

1.7.7 Macrodiversity – Soft Handover (FDD)

The function of *macrodiversity* is to collect data from one UE coming into the network via different Node Bs. Macrodiversity is implemented in the SRNC. The maximum number of parallel serving Node Bs in Rel. 99 is three, but may be increased in further releases of UMTS standards.

The described situation is called *Soft Handover* (Figure 1.60). It will again use more resources than necessary for a single connection not only on the radio interface, but also in the UTRAN on the different Iub and Iur interfaces. The advantage is that in the case of transmission errors on one radio link there is a high chance of gettin the same frame error-free on a different link. The SRNC compares the incoming messages from all links and selects the error-free frames. That method prevents Node Bs to change their transmission power multiple times to maintain contact with UEs that are close to the cell border. A change of transmission power could cause interference of the neighborhood cells or cell breathing effects.

In the downlink direction, several Node Bs may send data to the UE, but the UE will only receive the data of the sender with the strongest RX signal.

1.7.8 UMTS Spreading (FDD and TDD)

Figure 1.61 lists possible Spreading Factor (SF) values both for CDMA forms and for the uplink and downlink directions. The table within this figure also shows the SFs that should apply for certain data rates to reach 3.84 Mcps.

Possible SF:

- FDD UL: 4 – 8 – 16 – 32 – 64 – 128 – 256
- FDD DL: 4 – 8 – 16 – 32 – 64 – 128 – 256 – 512
- TDD: 1 – 2 – 4 – 8 – 16

Transmission of pure signaling information should always use SF = 256.

Data rate (After channel coding)	SF	Chip rate
960 kbit/s	4	3.84 Mcps
480 kbit/s	8	3.84 Mcps
240 kbit/s	16	3.84 Mcps
120 kbit/s	32	3.84 Mcps
60 kbit/s	64	3.84 Mcps
30 kbit/s	128	3.84 Mcps
15 kbit/s	256	3.84 Mcps
7 .5 kbit/s	512	3.84 Mcps

FDD Example:

A Call requires a 12.2 kbit/s voice channel. With special channel coding it will increase up to 30 kbit/s.

Looking into the table will indicate to use SF=128 (C_{128}).

Figure 1.61 UMTS spreading.

1.7.9 Scrambling

Scrambling describes the multiplication of another code to the chip stream without changing its length and is done to remove the quasi-orthogonal signals from different users and to identify different sources.

Scrambling in Uplink

- Short scrambling codes (256 bits) are used in Node B if there is advanced multiuser detection or an interference cancellation receiver.
- Long scrambling codes (38,400 bits) are used if the RAKE receiver is implemented in the Node B.

Scrambling in Downlink

- Long scrambling codes (38,400 bits) are used.

Note: Scrambling does not spread the chip stream.

A *scrambling code* is a random code called *Gold code*, and because of their random appearance, they are also called *pseudo-Noise (PN) codes.*

Scrambled signals of different users are orthogonal to each other again. Scrambling codes are of length 38,400 bits (*long scrambling code*). With evolved Node Bs *short scrambling codes,* 256 bits will be used.

1.7.10 Coding Summary (FDD)

Table 1.7 and Figure 1.62 give an overview of channelization and scrambling. In uplink and downlink, these codes have different meanings as described in the figure.

1.7.11 Signal to Interference (FDD)

Every user is an interference source to all other users in one cell (also in neighboring cells). To guarantee the success of the request QoS, a special ratio has to be calculated: Eb/N_0. This

Table 1.7 Channelization and scrambling

	Channelization	Scrambling
Usage	Uplink: Separation of physical data (DPDCH) and control channels (DPCCH) from same terminal	Uplink: Separation of terminals
	Downlink: Separation of connections to different users within one cell	Downlink: Separation of sectors (cells)
Length	4–256 chips (1.0–66.7 μs) Downlink also 512 chips	38.400 chips (10 ms) Uplink also 256 chips (66.7 μs)
Number of codes	Spreading factor dependent	Uplink: several millions Downlink: 512
Code family	Orthogonal Variable Spreading Factor	Long 10 ms code: Gold code Short code: Extended S(2) code family
Spreading	Yes, increase transmission bandwidth	No

value represents the ratio between the *energy of one signal* (bit) compared to the interference at the receiver.

The value is the SIR multiplied by the Processing Gain, which is more or less the SF (Figure 1.63).

If for any reason E_b/N_0 gets too low, one way of increasing the ratio is to increase the SF. With a fixed chip stream rate of 3.84 Mcps, the SF cannot just be increased. So the data rate also has to be changed; the data rate must be decreased and then the SF can be increased.

1.7.12 Cell Breathing (FDD)

Cell breathing describes a constant change of the range of a geographical area covered by a Node B cell based on the amount of traffic currently using that transmitter. When a cell becomes

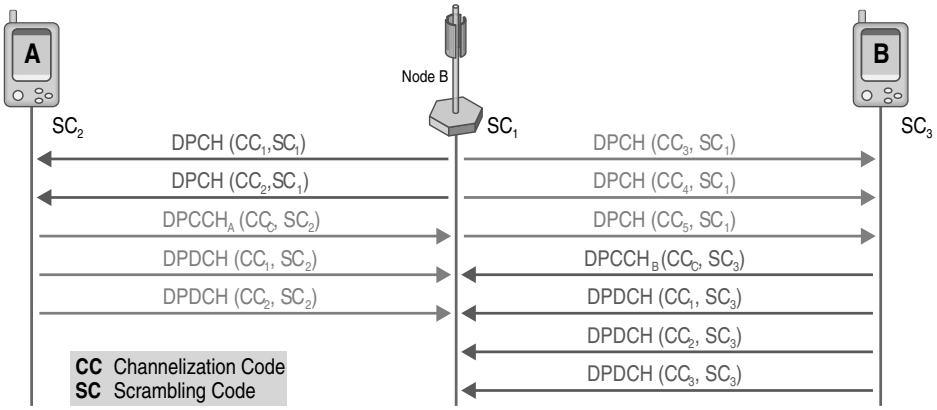


Figure 1.62 Channelization and scrambling.

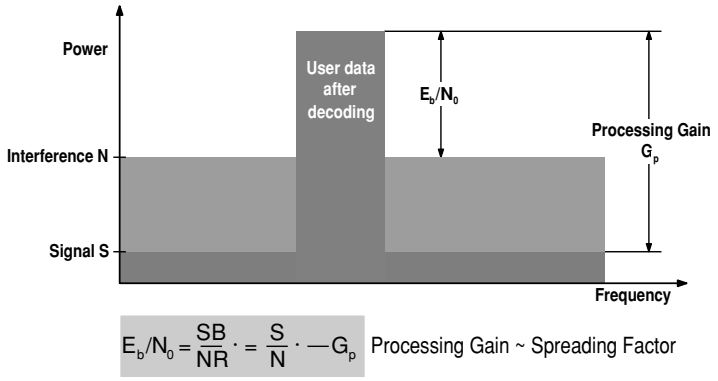


Figure 1.63 Signal to interference. B: Bandwidth of radio interface; R: User data rate.

heavily loaded, it shrinks. Subscriber traffic is then redirected to a neighboring cell that is more lightly loaded, which is called load balancing. Cell breathing is a common phenomenon of 2G and 3G wireless systems including CDMA (Figure 1.64).

The cause of cell breathing is the given QoS. The QoS then defines/causes E_b/N_0, limited bandwidth, and limited TX power.

Part of the cell breathing is also the *Near-Far-Effect,* where users who are closer to a Node B use less TX power than users who are further away from the Node B. The reason for this cell breathing effect is the fact that the RX power should, ideally, be the same for all users; for example, the SIR should be the same for all users.

Summary

- Every service requires a certain E_b/N_0 ratio (QoS).
- Received SIR should be the same for all users in a cell.
- Users with longer distance to Node B than others must use higher transmit power.
- Users with higher data rates (smaller SF) must use higher transmit power.
- If interference increases, the signal power must be increased.
- Signal power can only be increased to a maximum (∼0.5 W).
- Result: the "usable" area of a cell shrinks!

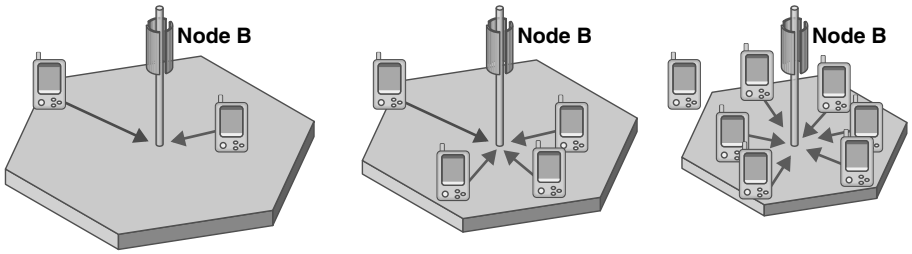


Figure 1.64 Cell breathing.

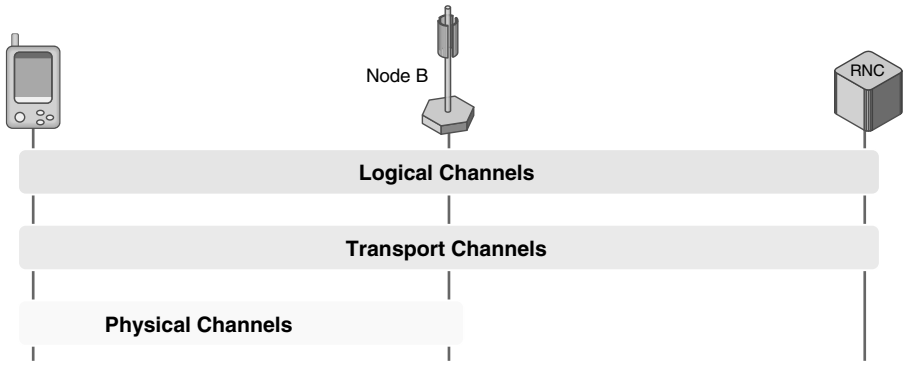


Figure 1.65 UMTS channels.

1.7.13 UMTS Channels (FDD and TDD)

Three types of UMTS channel levels (Figure 1.65) are defined (3GPP 25.301; 3GPP 25.302; 3GPP 25.211).

Physical Channels

Each Physical Channel is identified by its frequency, spreading code, scrambling code, and phase of the signal. Physical Channels provide the bearers for the different transport channels (see overviews below).

Dedicated Physical Channels identify a destination UE by SF and scrambling code. One or more Dedicated Physical Data Channels (DPDCHs) can be configured in uplink or downlink direction. The Dedicated Physical Control Channel (DPCCH) is used for radio interface related control information only. One DPCCH always belongs to the set of DPDCHs and is used for RRC messages and other signaling between UE and network.

Transport Channels

Transport Channels are unidirectional virtual channels, mapped onto physical channels. They provide bearers for information exchange between the MAC protocol and physical layer. Only Transport Channels of one type (e.g. Dedicated Channels – DCHs) are mapped.

Logical Channels

Logical Channels are uni- or bidirectional and provide bearers for information exchange between the MAC protocol and RLC protocol. There are two types of Logical Channels:

- Control Channels for signaling information of the control planes.
- Traffic Channels for user data of the user planes.

Table 1.8 gives all physical channels available in a UMTS network.

Table 1.8 Physical channels in UMTS

Channel	Abbreviation	Direction	Duplex mode
Dedicated Physical Data Channel	DPDCH	Uplink	FDD
Dedicated Physical Control Channel	DPCCH	Uplink	FDD
Dedicated Physical Channel	DPCH	Downlink	FDD, TDD
		Uplink	TDD
Synchronization Channel	SCH	Downlink	FDD
Primary Synchronization Channel	P-SCH	Downlink	FDD
Secondary Synchronization Channel	S-SCH	Downlink	FDD
Common Control Physical Channel	CCPCH	Downlink	FDD, TDD
Primary Common Control Physical Channel	P-CCPCH	Downlink	FDD
Secondary Common Control Physical Channel	S-CCPCH	Downlink	FDD
Common Pilot Channel	CPICH	Downlink	FDD
Physical Random Access Channel	PRACH	Uplink	FDD, TDD
Physical Common Packet Channel	PCPCH	Uplink	FDD
Paging Indicator Channel	PICH	Downlink	FDD
Acquisition Indicator Channel	AICH	Downlink	FDD
Physical Downlink Shared Channel	PDSCH	Downlink	FDD, TDD
Physical Uplink Shared Channel	PUSCH	Uplink	TDD

Different Types of Physical Channels in UTRA-FDD

- *Dedicated Physical Data Channel (DPDCH)*: Transmission of user data and higher layer signaling (RRC, NAS) in uplink direction coming from higher layers.
- *Dedicated Physical Control Channel (DPCCH)*: Transmission of radio control information in uplink direction. This channel exists only once per radio connection.
- *Dedicated Physical Channel (DPCH)*: Transmission of user data and control information in downlink direction. Both types of information will be mapped onto the DPCH.
- *Synchronization Channel (SCH)*: Cell search and synchronization of the UE to the Node B signal. Subdivided into Primary Synchronization Channel (P-SCH) and Secondary Synchronization Channel (S-SCH).
- *Common Control Physical Channel (CCPCH)*: Transmission of common information and is divided into Primary Common Control Physical Channel (P-CCPCH) and Secondary Common Control Physical Channel (S-CCPCH). P-CCPCH transmits the broadcast channel (BCH) and S-CCPCH transports the Forward Access Channel (FACH) and the Paging Channel (PCH). FACHs and PCH can be mapped to the same or to separate S-CCPCHs.
- *Common Pilot Channel (CPICH)*: Supports channel estimation and allows estimations in terms of power control. It is subdivided into Primary Common Pilot Channel (P-CPICH) and Secondary Common Pilot Channel (S-CPICH), which differ in scrambling code and availability within a cell.
- *Physical Random Access Channel (PRACH)*: Transmission of the Random Access Channel (RACH), which is used for the random access of a UE and for transmission of a small amount of data in the uplink direction.
- *Physical Common Packet Channel (PCPCH)*: Common data transmission using the collision detection CSMA/CD method.

- *Paging Indicator Channel (PICH)*: Transmission of the Page Indicator (PI) to realize the paging in the downlink direction. One PICH is always related to an S-CCPCH, which transports the PCH.
- *Acquisition Indicator Channel (AICH)*: Transmits the positive acknowledgment of a random access of a UE via PRACH or PCPCH.
- *Physical Downlink Shared Channel (PDSCH)*: Common transmission of data in downlink direction. Parallel UEs will have different codes assigned.

Different Types of Physical Channels in UTRA-TDD

- *Dedicated Physical Channel (DPCH):* Bidirectional transmission channel for user data and control information.
- *Common Control Physical Channel (CCPCH)*: Same as in FDD mode.
- *Physical Random Access Channel (PRACH)*: Same as in FDD mode.
- *Physical Uplink Shared Channel (PUSCH):* Common transmission of data and control information in the uplink direction. Parallel UEs will have different codes assigned.
- *Physical Downlink Shared Channel (PDSCH)*: Common transmission of data in downlink direction.
- *Paging Indicator Channel (PICH)*: Same as in FDD mode.

1.7.14 Transport Channels (FDD and TDD)

W-CDMA (*3GPP 25.302, 3GPP 25.211-25.215*) interworks with the higher layer MAC protocol. It offers the transport channels to the MAC. To be flexible in data rates, etc., all information on the transport channel is described by transport formats and certain attributes.

1.7.15 Common Transport Channels (FDD and TDD)

Common Transport Channels can be used by all UEs located in the same cell. A special identifier, the so-called RNTI (Radio Network Temporary Identity), is used to mark messages coming from or sent to a single UE on RACH, FACH or shared channels.

To the Common Transport Channels belong (Figure 1.66):

- *Broadcast Channel (BCH)*: Transmits system information (mandatory).
- *Paging Channel (PCH)*: Calls a UE, which has no RRC connection (mandatory).
- *Forward Access Channel (FACH)*: Transmits a small amount of data in the downlink direction. There can be multiple FACHs in one cell with different bandwidths (mandatory).
- *Random Access Channel (RACH)*: Transmits the acknowledgment to a Paging Request and transmits a small amount of data in the uplink direction (mandatory).
- *Uplink Common Packet Channel (CPCH)*: Transmits a small number of data packets in the uplink direction. The differences from RACH are fast power control, collision detection, and a status monitoring function (optional).

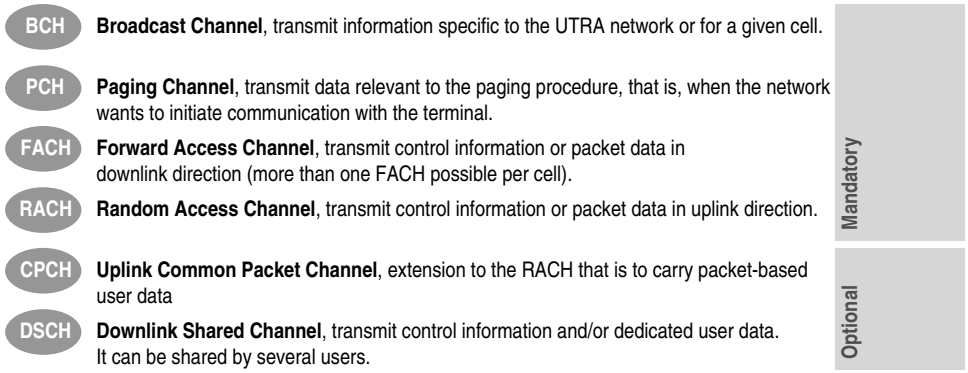


Figure 1.66 Common Transport Channels.

- *Downlink Shared Channel (DSCH)*: Transmits a small number of user data packets or control information in the downlink direction. It is shared between different users. The differences from FACH are fast power control and a variable bit rate on a frame-by-frame base. DSCH is not mandatory in every cell, but, if it exists, it is related to a Dedicated Transport Channel (similar to GSM Associated Control Channel (ACCH)).
- *Shared Channels* require a parameter to identify a UE, the RNTI. The DSCH is always related to DCHs: several DCHs can be mapped into one DSCH (optional).

1.7.16 Dedicated Transport Channels (FDD and TDD)

Dedicated Transport Channel (DCH)

DCHs are used for the transport of user data and control information for a particular UE coming from layers above the physical layer, including service data, such as speech frames, as well as higher layer control information, such as handover commands or measurement reports.

There is no need for a UE identifying parameter. One UE can have several DCHs for data transmission but only one for control information transmission.

Coded Composite Transport Channel (CCTrCH)

The CCTrCH encodes and multiplexes all transport channels of the same type on the physical layer.

Mapping of Transport Channels onto Physical Channels

The Common Transport Channels as well as the Dedicated Transport Channels are mapped onto physical channels. Figure 1.67 shows an example of the relationship between different transport channels and physical channels. Figure 1.68 shows a UE example for QoS handling and distribution of Logical, Transport and Physical Channels.

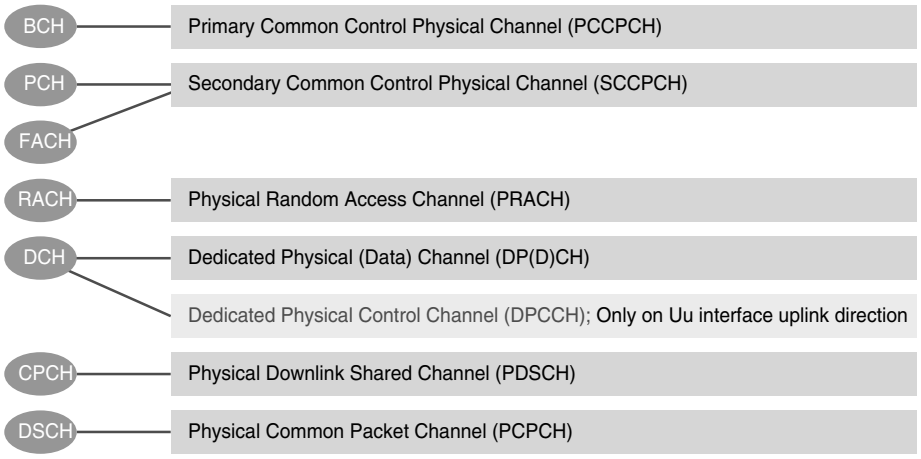


Figure 1.67 Mapping of transport channels.

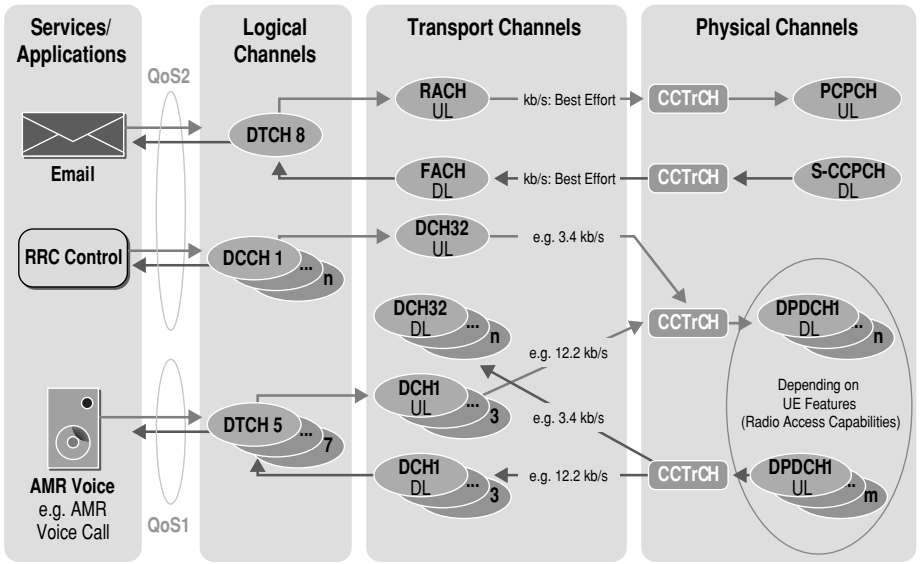


Figure 1.68 Channel mapping example.

1.7.17 Initial UE Radio Access (FDD)

When a UE is switched on for the first time in a cell of the UMTS network it starts to perform the following Initial UE Radio Access procedure that can be described in four steps (Figure 1.69):

1. UE reads the Primary Synchronization Channel, which is not scrambled and spread by a predefined spreading code (SF = 256). By reading this, the UE become time synchronic with the Node B.

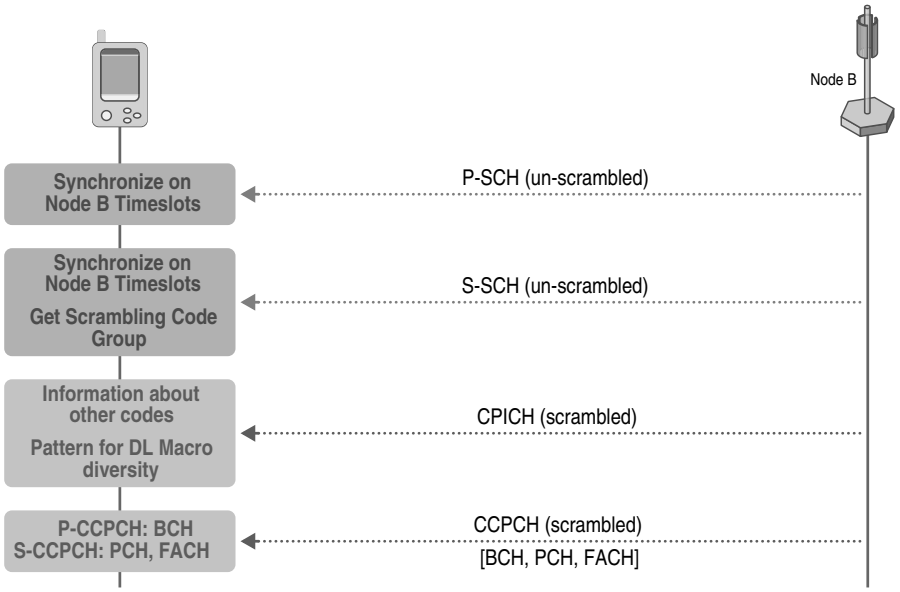


Figure 1.69 Initial UE radio access.

2. UE reads the S-SCH, which is also not scrambled. The S-SCH will transmit five hex values, which come out of a table. By reading these values the UE will become frame synchronic with the Node B and will get the scrambling group the actual Node B is using (see Figure 1.61).
3. UE can now read the Common Pilot Channel, which is scrambled with one of eight primary scrambling codes of the scrambling group. It is a matter of trial and error to find the correct code. The Pilot Channel will contain further information about other necessary codes and about the DL macrodiversity synchronization pattern.
4. UE will read the Common Control Physical Channel, which uses the same scrambling code as the CPICH, to get detailed information about UTRAN and the CN, to allow the P-CCPCH to transport the BCH, and to be able to get paged, and to allow the S-CCPCH to transport PCH. The system information in the BCH will also indicate the secondary scrambling code of the actual Node B for further data transmission on the DCHs.

1.7.18 Power Control (FDD and TDD)

Because of the fact that the SIR should be the same for all users in a cell, the demand for power control in UMTS is very high. Two forms of power control exist in UMTS (Figure 1.70).

Open Loop Power Control is a kind of one-way power control used before the UE is connected to the RRC and describes the ability of the UE transmitter to set the output power to a specific value for initial *uplink* and *downlink* transmission powers. The power control tolerance is ± 9 dB (normal conditions) or ± 12 dB (extreme conditions).

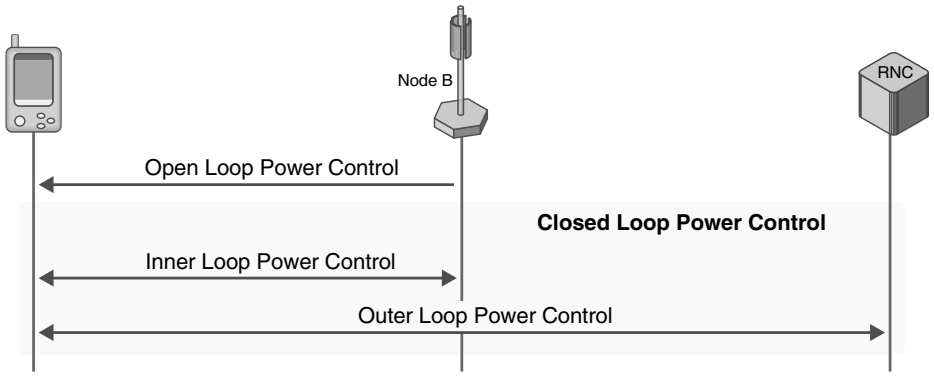


Figure 1.70 Power control.

- SIR should be the same for all users in a cell.
- Each user produces a signal, which, to other users, is just noise.
- Received signal = S (User 1) + $\sum$N (User n − 1)
- The goal must be to keep signal S at a minimum so that the noise will be low.

Closed Loop Power Control is performed when the UE has an RRC connection. It contains an *Inner and Outer Loop Power Control* mechanism.

Inner Loop Power Control (1500 Hz) runs in the uplink and describes the ability of a UE transmitter to adjust output power in accordance with one or more Transmit Power Control (TPC) commands of the downlink. The received uplink SIR will be kept at a given SIR target. UE transmitters might change the output power (step size of 1, 2, and 3 dB) in the slot after TPC_cmd was derived. Serving cells estimate SIR of received uplink DPCH, generate TPC commands (TPC_cmd), and transmit the commands once per slot according to:

$$\text{If } SIR_{est} > SIR_{target} \rightarrow \text{TPC command is “0”}$$

$$\text{If } SIR_{est} < SIR_{target} \rightarrow \text{TPC command “1”}$$

After reception of the TPC command, the UE derives a TPC command for each slot. The UE-specific higher layer parameter **PowerControlAlgorithm** determines which of the two algorithms is used for the evaluation.

Outer Loop Power Control maintains the quality of communication for bearer service quality requirements, using power as low as possible. Uplink outer loop power control takes care of setting a target SIR in Node Bs for individual uplink inner loop power control. This target SIR is updated for each UE according to the estimated uplink quality (BLock Error Ratio, Bit Error Ratio) for each RRC connection. Downlink outer loop power control describes the ability of the UE receiver to converge to required link quality (BLER) defined by the network (RNC) in downlink.

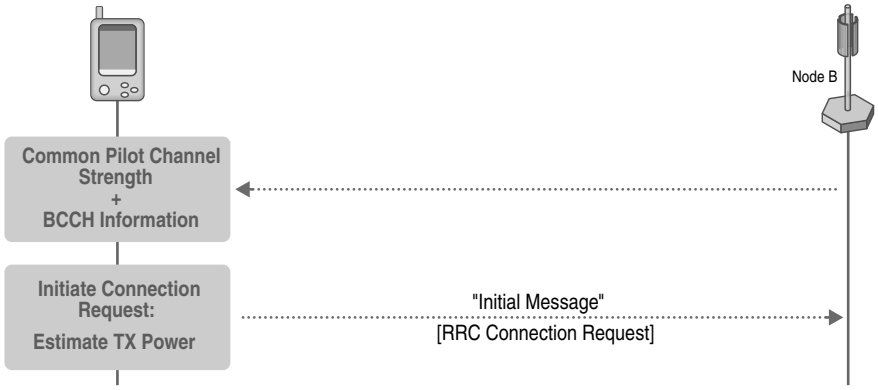


Figure 1.71 Open Loop Power Control.

Open Loop Power Control

By receiving the CPICH and the Broadcast Control Channel (BCCH) information parameters on the BCH, the UE can estimate a TX power. The stronger the RX signal, the less the TX power will be (Figure 1.71).

Closed Loop Power Control

After finding out what type of service the UE wants, the SRNC will define a QoS target for the Radio Bearer (SIR). Node B will store the target SIR and will compare it with the actual measurements of that UE. The result of the comparison will be given to the SRNC, which in turn will send a new target. The communication between Node B and SRNC is called the Outer Loop Power Control and will be performed between 10 and 100 times per second. This is why this method is called *Slow Power Control*!

On the other side, the Node B must control the UE TX power to reach the given SIR. Node B sends TPC commands to the UE to indicate either to increase or to decrease the TX power. UE will have to modify its TX power immediately. This method is called the Inner Loop Power Control and is performed up to 1500 times per second, and thus is called *Fast Power Control* (Figure 1.72).

Power control mechanisms will become a very important part of network optimization in the future, but in the current state of deployment there is still only little experience in this field for network operators.

1.7.19 UE Random Access (FDD)

After estimating the TX power (Open Loop Power Control) the UE will send an Initial Access frame on the Physical Random Access Channel. It will then wait for an acknowledgment. If there is no acknowledgment, then the UE will increase TX power and send the frame again. It will perform this until it receives an Access Detected message via the AICH or until it reaches the maximum value for TX power.

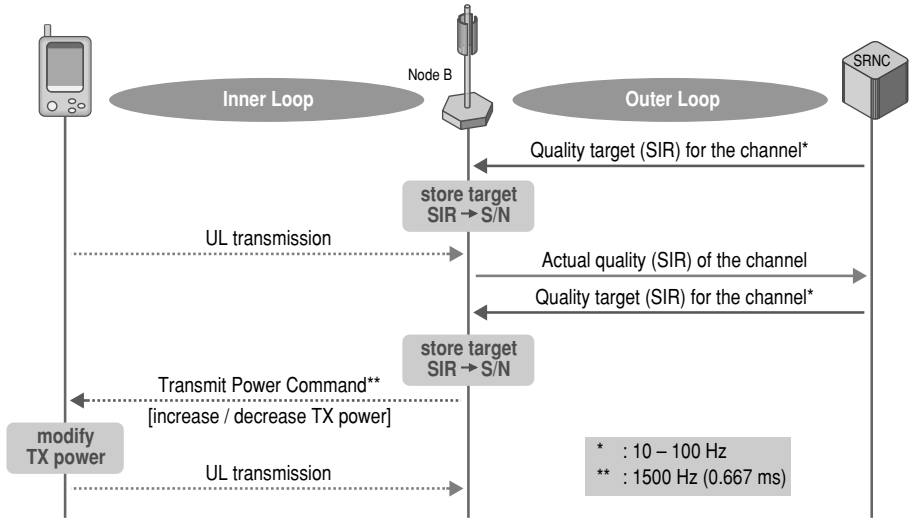


Figure 1.72 Closed Loop Power Control.

Now the UE knows about good TX power strength and will send the real Random Access Information containing the RRC Connection Request (Figure 1.73).

1.7.20 Power Control in Soft Handover (FDD)

In Soft Handover, the UE is connected to more than one Node B. All Node Bs will by default transmit **Transmit Power Command** messages. The rule is that the less the TX power the better! In the example, one Node B indicates to decrease the TX power. This forces the UE to decrease TX power even if it loses the contact to the other Node Bs. With this rule the Near-Far Effect cannot become an endless problem.

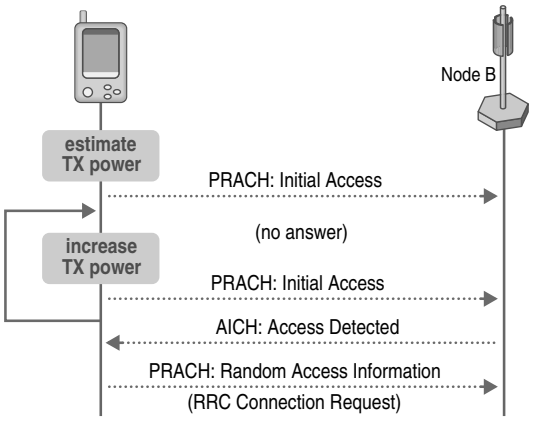


Figure 1.73 UE random access.

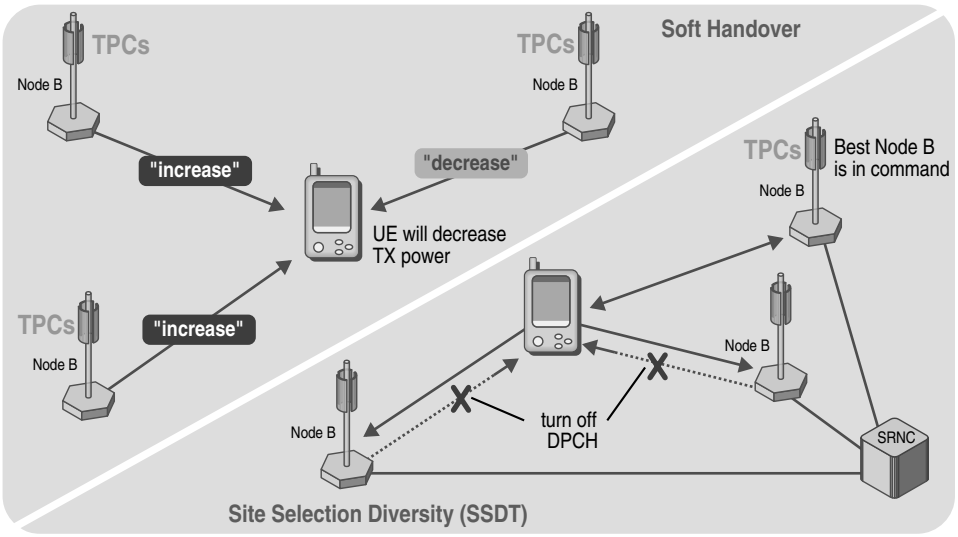


Figure 1.74 Power control in Soft Handover.

A special alternative is the *Site Selection Diversity Transmission (SSDT).* Using this UTRAN option the RNC will get the measurements of the actual radio interface connection toward one UE by several Node Bs and decide that some of the Node Bs should stop transmitting DCHs and also stop transmitting TPC commands to the UE. Only the Node B with the best radio contact will be the UE "server" in downlink (Figure 1.74).

1.8 UMTS Network Protocol Architecture

The protocol architecture of UTRAN (Figure 1.75) is subdivided into three layers:

1. *Transport Network Layer.* Physical and transport protocols and functions to provide AAL2 resources and allow communication within UTRAN and CN. The protocols are not UMTS specific.
2. *Radio Network Layer.* Protocols and functions to allow management of radio interface and communication between UTRAN components and between UTRAN and UE.
3. *System Network Layer.* NAS protocols to allow communication between CN and UE.

Each of the layers is divided into a control and a user plane.

- *Control plane:* Transmission of control signaling information.
- *User plane:* Transmission of user data traffic.

The following sections give an overview about protocol stacks on the different interfaces in UTRAN and the CN. The description of functions of protocol layers, their messages and procedures follows in Chapter 2.

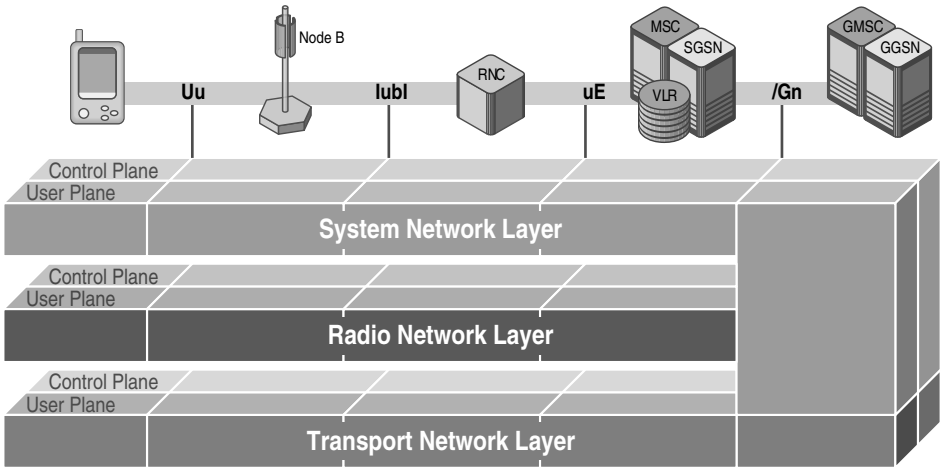


Figure 1.75 UMTS network protocol architecture.

1.8.1 Iub – Control Plane

The protocol stacks of Uu and Iub interfaces – control plane – contain (Figure 1.76):

ATM Asynchronous Transfer Mode is used in UMTS as the transmission form on all Iu interfaces. The physical layer is SDH over fiber. The smallest unit in ATM is the ATM cell. It will be transmitted in the *Virtual Channel.* Many virtual channels are running within a *Virtual Path.*

AAL ATM Adaptation Layer – To transmit higher protocols via ATM, it is required to have adaptation sublayers. These sublayers contain a common adaptation and a service-specific adaptation part.

UPFP User Plane Framing Protocol – Used on Iur and Iub interfaces to frame channels supported between SRNC and Node Bs.

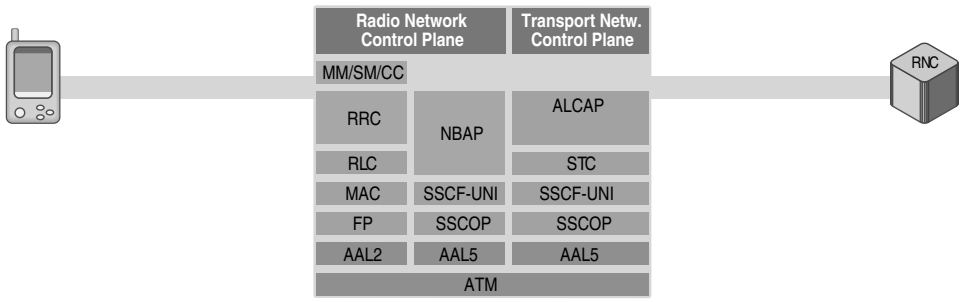


Figure 1.76 Iub – control plane.

SSCOP Service Specific Connection Oriented Protocol Provides mechanisms for establishment and release of connections and reliable exchange of signaling information between signaling entities.

MAC Medium Access Control Protocol – Coordinates access to physical layer. Logical channels of higher layers are mapped onto transport channels of lower layers. MAC also selects appropriate TFSs depending on necessary transmission rate and organizes the priority handling between different data flows of one single UE.

RLC Radio Link Control Protocol – Offers transport services to the higher layers called Radio Bearer Services; the three work modes are transparent, acknowledged, and unacknowledged mode.

SSCF Service Specific Coordination Function (User-Network-I/F, Network-Network-1/F) – Not a protocol but an internal coordination function, which does internal adaptation of the information coming or going to higher layers, for example, MTP3-B routing information.

STC Signaling Transport Converter – An internal function, which has no own messages; it converts primitives from lower and higher layers (either MTP3 or MTP3-B primitives) and their parameters fitting the requirements of the other.

RRC Radio Resource Control Protocol – A sublayer of Layer 3 on UMTS radio interface and exists in the control plane only. It provides information transfer service to the NAS and is responsible for controlling the configuration of UMTS radio interface layers 1 and 2.

AAL2L3 AAL2 Layer 3 Protocol – Generic name for transport signaling protocol to set up and release transport bearers. In UMTS the main ALCAP protocol is the AAL2 signaling protocol.

NBAP Node B Application Part – Protocol used between RNC and Node B to configure and manage the Node B and set up channels on Iub and Uu interfaces.

MM Mobility Management – A generic term for the specific mobility functions provided by a PLMN including, e.g., tracking a mobile as it moves around a network and ensuring that communication is maintained.

SM Session Management – Protocol used between UE and SGSN and creates, modifies, monitors, and terminates sessions with one or more participants, including multimedia and Internet telephone calls.

CC Call Control – includes some basic procedures for mobile call control (no transport control!): Call Establishment, Call Clearing, Call Information Phase, and other miscellaneous procedures.

1.8.2 Iub – User Plane

The user plane protocol stacks of Uu and Iub interfaces introduce some new layers (Figure 1.77):

PDCP Packet Data Convergence Protocol – Used to format data into a suitable structure prior to transfer over the air interface and provides its services to the NAS at the UE or the relay at the RNC.

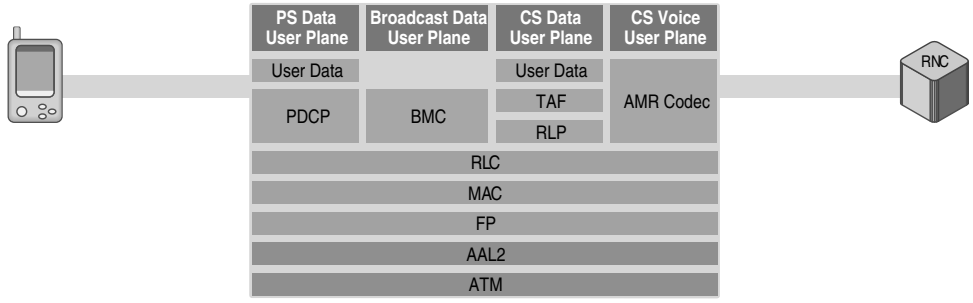


Figure 1.77 Iub – user plane.

BMC Broadcast/Multicast Protocol – Adapts broadcast and multicast services on the radio interface and is a sublayer of L2 that exists in the user plane only.

Application Data IP-based packet protocols

Speech (AMR) will be transported transparently on AAL2.

1.8.3 Iur – User/Control Plane

The Iur interface between RNCs shows two alternative solutions on the transport network layer: Either SCCP and RNSAP messages can be transported using MTP3-B running on top of SSCOP, or it is possible to run SCCP on top of M3UA if the lower transport layer is IP-based (Figure 1.78).

IP Internet Protocol – Provides connectionless services between networks and includes features for addressing, type-of-service specification, fragmentation and reassembly, and security.

SCTP Stream Control Transmission Protocol – Transport protocol that provides acknowledged error-free nonduplicated transfer of data. Data corruption, loss of

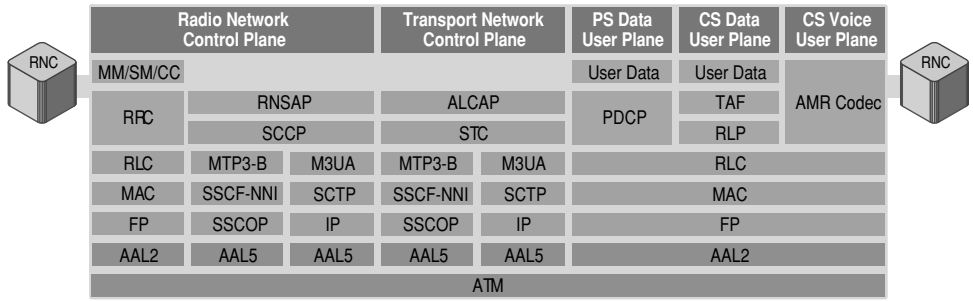


Figure 1.78 Iur – user/control plane.

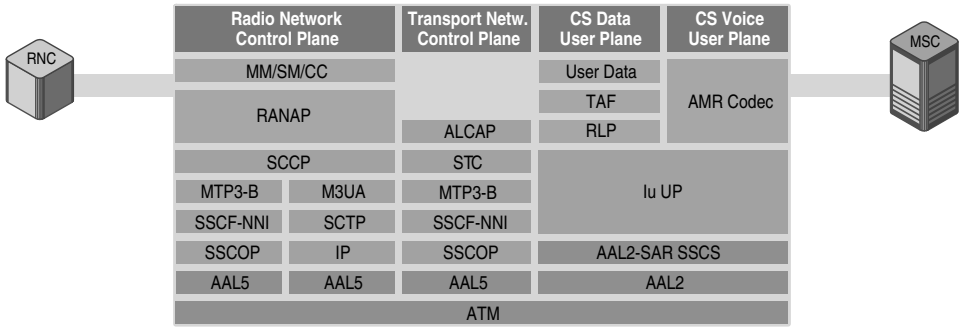


Figure 1.79 IuCS – user/control plane.

data, and duplication of data are detected by checksums and sequence numbers. Retransmission mechanisms are applied to correct loss or corruption of data.

MTP3-B Message Transfer Part Level 3 Broadband – Fulfills the same sort of work as the standard narrowband MTP; it provides identification and transport of higher layer messages (PDUs), routing, and load sharing.

M3UA MTP Level 3 User Adaptation Layer – Provides equivalent primitives to MTP3 users as provided by MTP3. ISUP and/or SCCP are unaware that expected MTP3 services are offered remotely and not by local MTP3 layer. M3UA extends access to MTP3 layer services to a remote IP-based application.

SCCP Signaling Connection Control Part – Provides a service for transfer of messages between any two signaling points in the same or different network.

RNSAP Radio Network Subsystem Application Part – Communication protocol used on the Iur interface between RNCs and specified using ASN.1 Packed Encoding Rules (PER).

Speech (AMR) will be transported transparently on AAL2.

1.8.4 luCS – User/Control Plane

The protocol stack of luCS interface – control/user plane – contains (Figure 1.79):

AMR Adaptive Multirate Codec (speech) – Offers a wide range of data rates and is used to lower codec rates as interference increases on the air interface.

TAF Terminal Adaptation Function (V. and X. series terminals) – A converter protocol to support the connection of various kinds of TE to the MT.

RLP Radio Link Protocol – Controls circuit-switched data transmission within the GSM and UMTS PLMN.

The CS domain refers to the set of all entities handling the circuit-switched type of user traffic as well as entities supporting the related signaling. These are the MSC, the GMSC, the VLR, and the IWF (InterWorking Function(s)) towards the PSTN/ISDN networks.

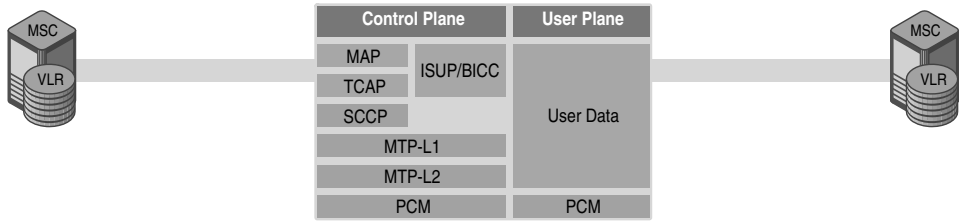


Figure 1.80 IuPS – user/control plane.

1.8.5 IuPS – User/Control Plane

The PS domain includes the related entities for packet transmission, the SGSN, GGSN, and BG (Border Gateway) (Figure 1.80).

Note: The user plane payload (IP-traffic) is transported using AAL5. So there is no ALCAP layer necessary in the control plane to set up and delete switched virtual AAL2 ATM connections.

1.8.6 E – User/Control Plane

The E interface protocol stack is a well known form of GSM environment with both control and user planes (Figure 1.81).

PCM Pulse Code Modulation – An analog signal is encoded into a digital bit stream by first sampling, then quantizing, and finally encoding into a bit stream. The most common version of PCM converts a voice circuit into a 64 kbps stream.

TCAP Transaction Capability Application Part – Enables deployment of advanced intelligence in networks by supporting noncircuit-related information exchange between signaling points using SCCP connectionless service.

MAP Mobile Application Part – Enables real-time communication between nodes in mobile networks. Example: transfer of location information from VLR to the HLR.

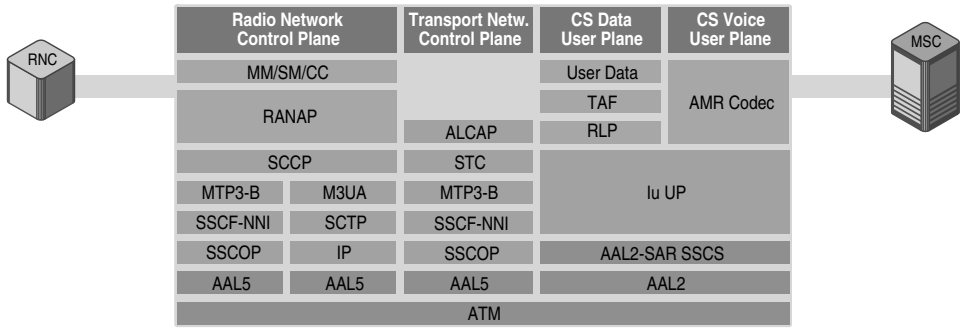


Figure 1.81 E – user/control plane.

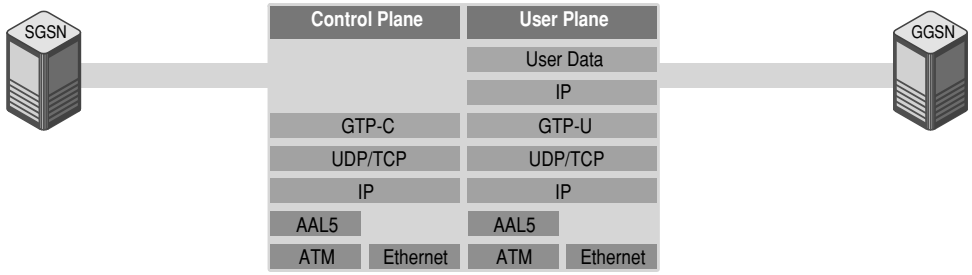


Figure 1.82 Gn – user/control plane.

ISUP ISDN User Part – Part of SS7 protocol layer, used for setting up, management, and release of voice calls and data between calling and called parties.

MTP2 Message Transfer Part Level 2 – Takes care of reliable transmission through retransmission techniques of signaling units over signaling links.

MTP3 Message Transfer Part Level 3 – Represents the highest level of MTP and takes care of the general MTP management and the discrimination, distribution, and routing of signaling messages.

Note: The MAP is also able to carry containers with, for example, RANAP and Base Station Subsystem Application Part (BSSAP) messages to exchange these messages between different MSCs in the case of inter-MSC or intersystem handover procedures.

1.8.7 Gn – User/Control Plane

The protocol stack on GPRS Gn interface has not changed significantly in comparison with 2.5G networks (Figure 1.82).

GTP-C GPRS Tunneling Protocol – Control – GTP-C messages are exchanged between GSNs to create, update, and delete GTP tunnels, for path management and to transfer GSN capability information between GSN pairs. GTP-C is also used for communication between GSNs and the Charging Gateways.

GTP-U GPRS Tunneling Protocol – User – Messages are exchanged between GSN pairs or GSN/RNC pairs for path management and error indication, to carry user data packets and signaling messages.

UDP User Datagram Protocol – UDP is a connectionless, host-to-host protocol that is used on PS networks for real-time applications.

TCP Transmission Control Protocol – Provides reliable connection-oriented, full-duplex point-to-point services.

1.9 SIGTRAN

Signaling Transport (SIGTRAN) is a set of IETF protocol standards. It has been defined to provide a model for signaling transport for SS#7 and ISDN over IP networks. Most significant

is the Stream Control Transmission Protocol (SCTP), which defines the transport of PSTN signaling over IP. A major driver was the intent to adapt Voice-over-IP (VoIP) and Media-over-IP (MoIP) networks to the PSTN.

The major problems of this approach were:

- Voice quality:
  – no pre-allocated bandwidth and variable packet delay
  – jittered conversations
  – chunks of speech missing.
- No standards for packetized voice and connection establishment and management:
  – parties needed the same VoIP package to establish a communication.
- Only point-to-point connections:
  – no defined interfaces between Internet and PSTN.
- Only simple call services:
  – almost only conversations
  – no additional service (e.g. call forwarding) supported.

These limitations made it impossible to deploy VoIP service on a large scale.

The SIGTRAN architecture is now the approach used to support the integration between the PSTN and IP networks. It provides signaling capabilities for call management and defined media paths through IP networks with reserved bandwidth.

SIGTRAN includes the following protocols (Figure 1.83):

- M2UA provides client-server services of MTP2.
- M2PA provides peer-to-peer services of MTP2.
- M3UA provides client-server (SG to MGC) and peer-to-peer services of MTP3.
- SUA provides peer-to-peer services of SCCP.
- IUA provides services of the ISDN Data Link Layer (LAPD).
- V5UA provides V.5.2 protocol services.

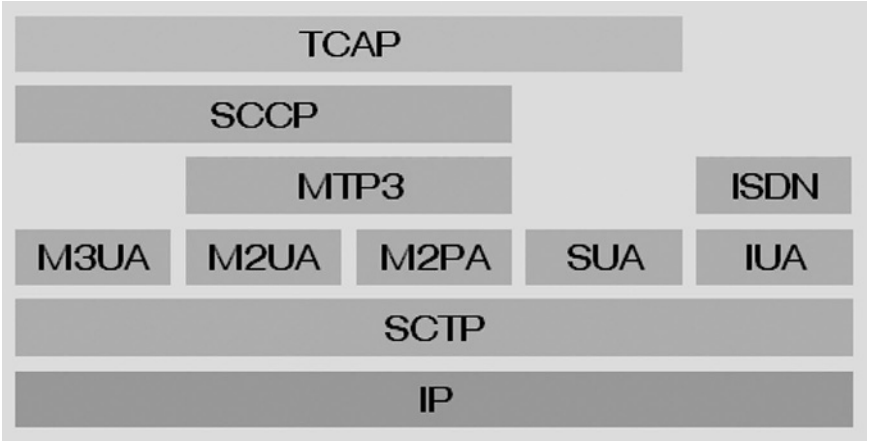


Figure 1.83 SIGTRAN protocols.

The SCTP is a replacement of the classic TCP and removes its shortcomings when it comes to VoIP (as this book will not cover IP issues in-depth, this problem is not discussed here). SCTP is a general-purpose protocol with the following set of features:

- Reliable transport of user data:
  – detects corrupt or out-of-sequence data
  – performs repair.
- Defines data exchange between two known endpoints.
- Provides shorter timers than TCP.
- Rate-adaptive:
  – considers network congestion and reduces transmission speed.
- Multi-homing:
  – each SCTP endpoint may be known by multiple IP addresses
  – routing to one address is independent of all others
  – if a route becomes unavailable, another is used.
- Uses an initialization procedure, based on cookies, to prevent denial of service attacks.
- Bundling and segmentation:
  – a single SCTP message may contain multiple "chunks" of data; each may contain a whole signaling message
  – a single message may be split into multiple SCTP messages to fit into the underlying PDU.
- Multi-streaming capability:
  – data is split into multiple streams, with independent sequenced delivery.

The SIGTRAN approach is typically also integrated on Iu interfaces that are based on pure IP technology.

1.10 ATM

Asynchronous Transfer Mode (ATM) is used in UMTS as the transmission form on all Iu interfaces. The physical layer is SDH over fiber.

The smallest unit in ATM is the *ATM cell.* It will be transmitted in a *Virtual Channel.* Many virtual channels are running within a *Virtual Path* (Figure 1.84).

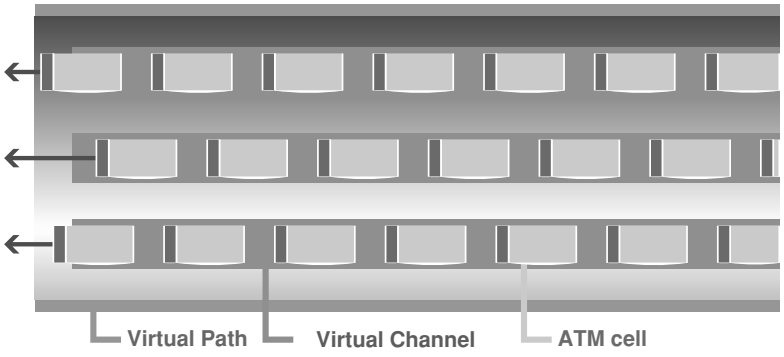


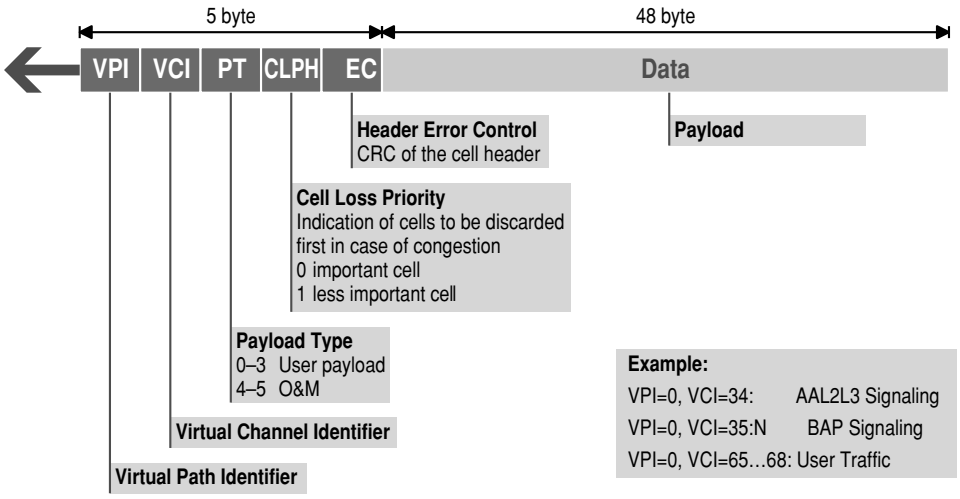
Figure 1.84 Asynchronous Transfer Mode.

A Virtual Path is, for example, the Permanent Virtual Connections (PVCs) for exchanging NBAP and ALCAP messages between RNC and Node B. This connection will be set up once and will run until it is changed or deleted by O&M operation. Over this PVC many user connections are running, which represent virtual channels.

1.10.1 ATM Cell

An ATM cell contains two address parameters: Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI); an identification of the type of payload; a cell loss priority; and a header Cyclic Redundancy Check (CRC). This means that the transmission of the payload contents is not secured by a checksum. For transmission error detection and correction, the higher layers must have certain functions. The header is 5 bytes and the payload is 48 bytes long.

The example in Figure 1.85 shows a possible configuration of the UMTS Iur interface. Certain signaling protocols are running over different VCIs as well as the user data traffic. The VCIs for traffic are *switched virtual connections (SVCs);* that is, they will be set up only on request.



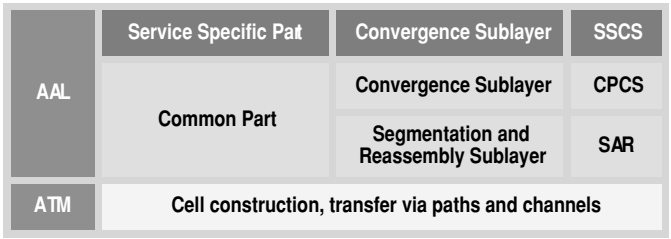


Figure 1.85 (a) ATM cell and (b) layer architecture.

1.10.2 ATM Layer Architecture

To transmit higher protocols via ATM, it is required to have adaptation sublayers. These sublayers contain a common adaptation and a service-specific adaptation part (Figure 1.85).

The *Convergence Sublayer* is responsible for getting the PDUs of the higher layer and for modifying its size so that each of the PDUs fits into an SSCS and a CPCS message, respectively. Additionally, extra parameters will be inserted to guarantee that a receiver can allocate each message to a specific stream of information.

The *Segmentation Sublayer* is responsible for segmenting the SSCS or CPCS message so that each part of the original will fit into the ATM cell payload. Reassembly is the counterpart to segmentation and is performed at the receiver side.

1.10.3 ATM Adaption Layer (AAL)

The AAL is specified by four classes (A–D) that differ from each other in bit rate, synchronization method, and connection type (Figure 1.86):

A Constant Bit Rate Service (CBR)
B Unspecified Bit Rate Service (UBR)
C Available Bit Rate Service (ABR)
D Variable Bit Rate Service (VBR)

For each class a specific adaptation layer has been developed to support the specific use of it. These are ATM Adaptation Layers 1, 2, 3/4, and 5.

Each of the AALs contains a different frame structure which contains all necessary parameters to support the need. Part of every AAL frame is a data field in which the AAL-SDU message, or segment of a message of a higher protocol, will be placed and transmitted.

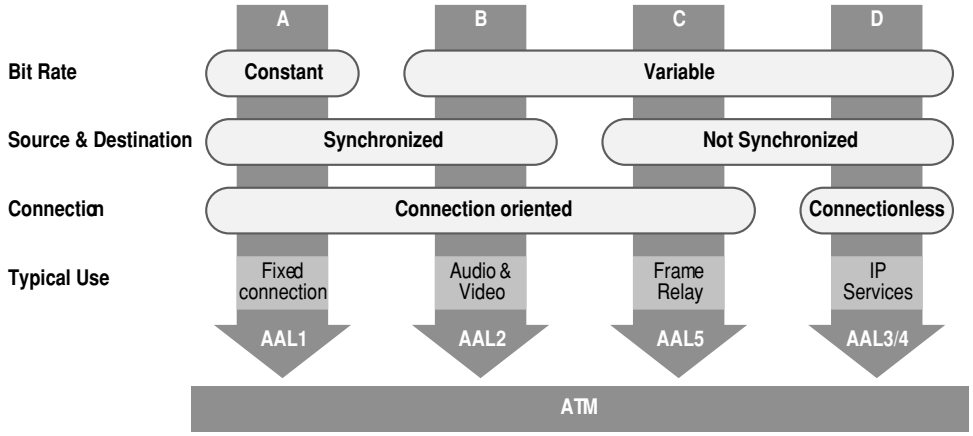


Figure 1.86 ATM Adaptation Layer.

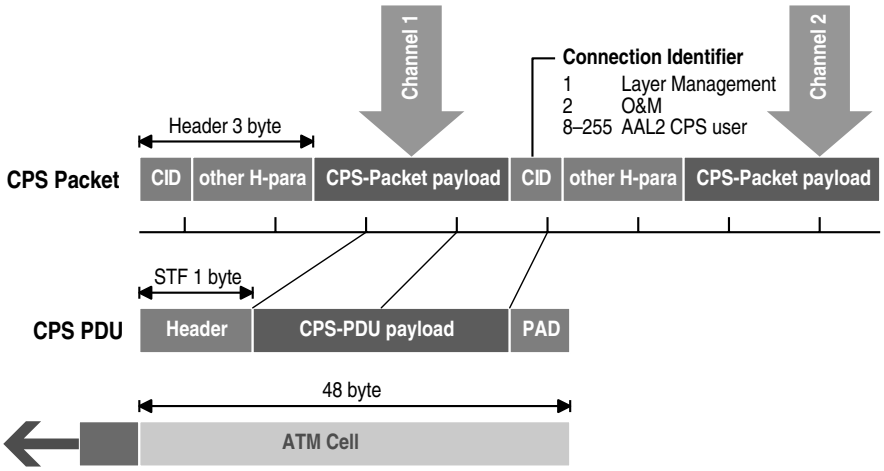


Figure 1.87 AAL2 format.

1.10.4 AAL2

The AAL2 (*ITU-T1.363.2*) provides for the bandwidth-efficient transmission of low-rate, short, and variable length packets in delay-sensitive applications (Figure 1.87). More than one AAL2 user information stream can be supported on a single ATM connection.

The AAL2 is subdivided into the Common Part Sublayer (CPS) and the Service Specific Convergence Sublayer (SSCS). Different SSCS protocols may be defined to support specific AAL2 user services, or groups of services. The SSCS may also be null, merely providing for the mapping of the equivalent AAL primitives to the AAL2 CPS primitives and vice versa.

AAL2 has been developed to transport multiple data streams. The *Connection Identifier* (*CID*) identifies every stream. The CID value can be found in the Layer 3 signaling as a reference (AAL2L3/ALCAP signaling protocol).

The *Start Field* (*STF*) is used to point to the payload or *Padding* (*PAD*) as well as for transmission error detection.

1.10.5 AAL5

The AAL5 (*ITU-TI.363*.5) enhances the service provided by the ATM layer to support functions required by the next higher layer (Figure 1.88). This AAL performs functions required by the user, control, and management planes, and supports the mapping between the ATM layer and the next higher layer.

The AAL5 supports the nonassured transfer of user data frames. The data sequence integrity is maintained and transmission errors are detected. The AAL5 is characterized by transmitting in every ATM cell (but the last) of a PDU, 48 octets of user data. In most of the cells, there is no overhead encountered.

The AAL5 does not support input data streams; it supports frames. Maximum size of a frame is 64 kbytes. The higher layer message will be put in the CPCS-PDU payload field. One

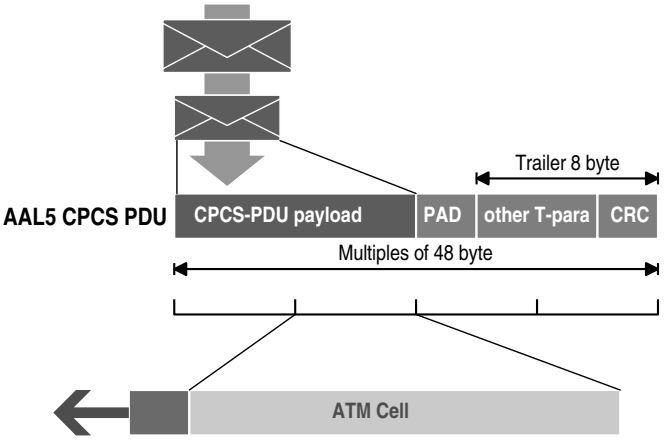


Figure 1.88 AAL5 format.

of the tail parameters will indicate the length of the payload. The CRC field will also protect the payload. In this way, the transmission is protected and is mainly used for transmission of control information, for example signaling.

1.11 User Plane Framing Protocol

The user plane Framing Protocol (FP, defined in *3GPP 25.427*) transports Transport Block Sets (TBSs) across the Iub and Iur interfaces. It is also responsible for transmission of outer loop power control information between Node B and SRNC and for transfer of radio interface parameters from SRNC to Node B. A set of FP signaling messages supports mechanisms for transport channel synchronization and node synchronization. In addition, FP also provides transport services for DSCH TFIs (Transport Format Indicators) from SRNC to Node B.

Transport channels on the Iur that lead from SRNC to DRNC must have the same configuration parameters as the same transport channels on Iub between DRNC and Node B.

The SRNC is responsible for the complete configuration of the transport channels. Appropriate signaling messages are exchanged between SRNC and Node B(s) via Iub and – if necessary – via Iur control plane. Transport channels in downlink direction are multiplexed by the Node B onto radio physical channels, and de-multiplexed in uplink direction from the radio physical channels.

1.11.1 Frame Architecture

There are two different FP frame formats for data and control frames (Figure 1.89). For the FP data frame the frame type field in the header is set to "0".

Figure 1.89 UP FP frame architecture.

Header

- Frame Type (FT): 0 = data.
- Connection Frame Number (CFN): Reference to radio frame.
- Transport Format Indicator (TFI): Information about data block.

Payload

- CFN: Indicator as to which radio frame the first data was received on uplink or will be transmitted on downlink.
- TFI: The local number of the transport format used for the transmission time interval.
- Transport Block (TB): A block of data of DCH to be transmitted or received over the air interface. The transport format indicated by the TFI describes the transport block length and transport block set size.

1.11.2 FP Control Frame Architecture

In the case of a FP control frame, the frame type field is set to "1" and control frame type indicates the name of the FP signaling message (Figure 1.90).

Header

Frame Type (FT):	0=data, l=control
Control Frame Type:	OUTER LOOP POWER CONTROL
	TIMING ADJUSTMENT
	DL SYNCHRONIZATION
	UL SYNCHRONIZATION
	DSCH TFCI SIGNALING
	DL NODE SYNCHRONIZATION
	UL NODE SYNCHRONIZATION
	RX TIMING DEVIATION
	RADIO INTERFACE PARAMETER
	UPDATE TIMING ADVANCE

Payload

Contains only parameters (CFN, Time of Arrival, UP SIR Target, other Timing Information, etc.).

Figure 1.90 UP FP control frame architecture.

1.12 Medium Access Protocol (MAC)

The MAC protocol (*3GPP 25.321*) coordinates the access of the physical layer. The logical channels of higher layers are mapped onto transport channels of lower layers. MAC also selects the appropriate TFSs, depending on necessary transmission rate, and organizes the priority handling between different data flows of one single UE.

If the UE uses Common Transport Channels, MAC provides a unique RNTI for each single UE, which is also known by the RRC.

In the case of random access to the network via RACH, MAC defines a priority by assigning an Access Service Class (ASC). The values of ASC can be 0–7, where 0 is the highest priority. An emergency call would, for example, get the ASC = 0. During Radio Bearer connection setup, MAC will receive a MAC Logical Link Priority (MLP). This corresponds with the ASC.

1.12.1 MAC Architecture

The diagrams that describe the MAC architecture show the different MAC entities (Figure 1.91), which are:

MAC-b is the MAC entity that handles the following transport channel:

- Broadcast Channel (BCH).

MAC-c/sh is the MAC entity that handles the following transport channels:

- Paging Channel (PCH).
- Forward Access Channel (FACH).

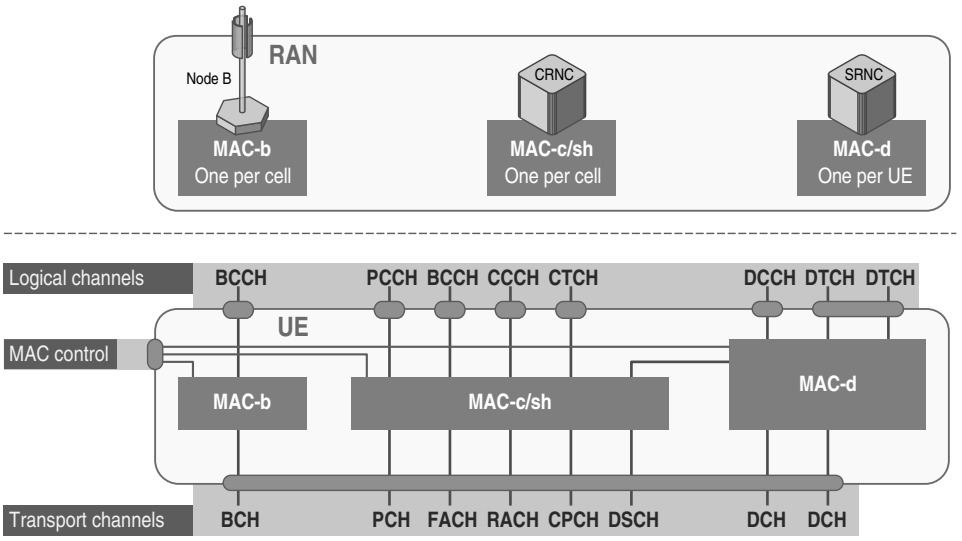


Figure 1.91 MAC architecture.

- Random Access Channel (RACH).
- Common Packet Channel (CPCH). The CPCH exists only in FDD mode.
- Downlink Shared Channel (DSCH).
- Uplink Shared Channel (USCH). The USCH exists only in TDD mode.

MAC-d is the MAC entity that handles the following transport channel:

- Dedicated Transport Channel (DCH).

All entities are controlled via the MAC Control SAP, which is connected to the RRC unit.

1.12.2 MAC Data PDU

The MAC Data PDU contains the following information elements (definitions following *3GPP 25.321*; Figure 1.92).

Target Channel Type Field (TCTF)

The TCTF field is a flag that provides identification of the logical channel class on FACH and RACH transport channels. The flag tells whether the channel carries BCCH, CCCH, Common Traffic Channel (CTCH), SHCCH, or dedicated logical channel information.

UE-Id (Different RNTIs)

The UE-Id field provides an identifier of the UE on Common Transport Channels. The following types of UE-Id used on MAC are defined:

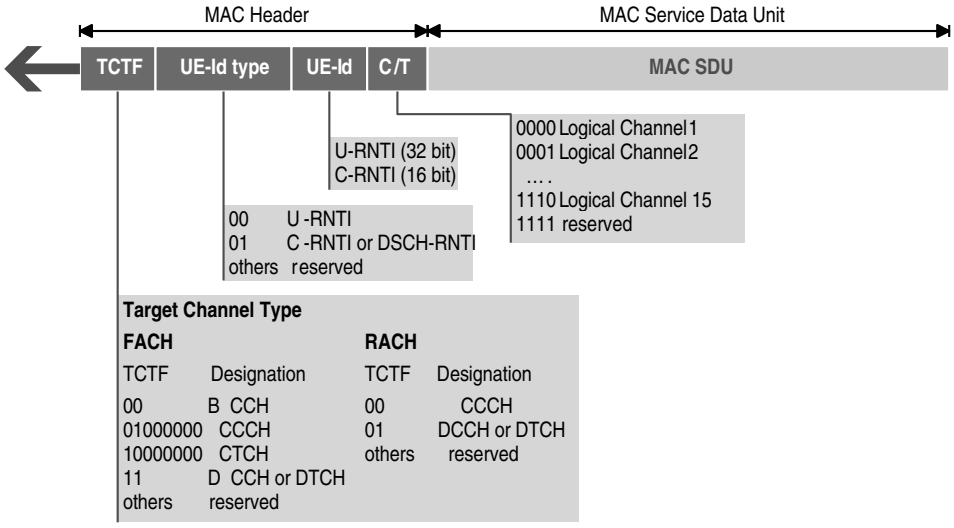
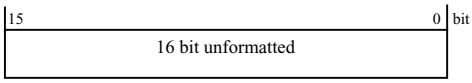
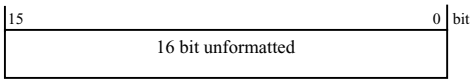


Figure 1.92 MAC data PDU.

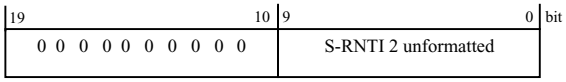
- The **Cell Radio Network Temporary Identity (C-RNTI)** uniquely identifies a UE within one cell and is assigned by the SRNC (=CRNC). It is used on DTCH and DCCH in uplink, may be used on DCCH in downlink, and is used on DTCH in downlink when mapped onto Common Transport Channels except when mapped onto the DSCH transport channel.



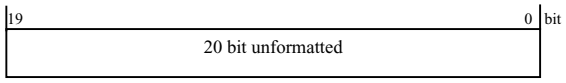
- The **DSCH Radio Network Temporary Identity (DSCH-RNTI)** uniquely identifies a UE within one cell, when DSCH-TrCHs are used as bearers for DCCH/DTCH. The DSCH-RNTI is assigned by the CRNC. In FDD, the DSCH-RNTI is used on DTCH and DCCH in downlink when mapped onto the DSCH transport channel.



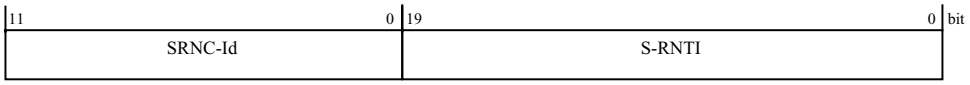
- The **SRNC Radio Network Temporary Identity** (S-RNTI) uniquely identifies a UE in the SRNS (e.g. in RNSAP messages) and is assigned by SRNC for an RRC-connection establishment. An S-RNTI is discarded, if the RRC connection is released or when the SRNC changes (e.g. during an SRNC relocation).



- The **DRNC Radio Network Temporary Identity (D-RNTI)** uniquely identifies a UE in RNSAP messages from SRNC to DRNC and is assigned by DRNC.



- The **UTRAN Radio Network Temporary Identity (U-RNTI)** uniquely identifies the UE within the UTRAN, because the SRNC-Id is included. It consists of S-RNTI and SRNC-Id and is assigned/released upon an RRC-connection establishment/release.



C/T Field

The C/T field provides identification of the logical channel instance when multiple logical channels are carried on the same transport channel (for example it indicates which radio signaling bearer is used in RRC message transport). The C/T field is also used to provide identification of the logical channel type on Dedicated Transport Channels and on FACH and RACH when used for user data transmission.

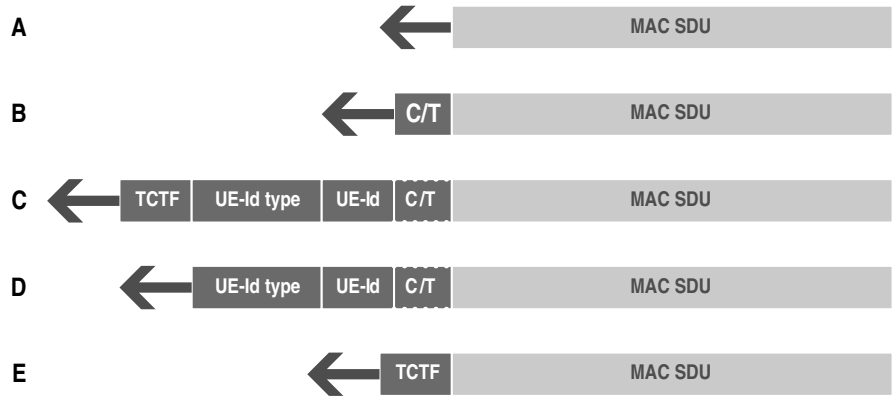


Figure 1.93 MAC header alternatives.

1.12.3 MAC Header Alternatives

Depending on the channel used, the MAC header can contain a different parameter (Figure 1.93):

A DTCH or DCCH will be mapped on DCH; there is no multiplexing of dedicated channels in MAC. No header information is required.

B DTCH or DCCH will be mapped on DCH. MAC performs multiplexing of dedicated channels. C/T is required.

C DTCH or DCCH will be mapped on RACH/FACH. If multiplexing of dedicated channels is necessary, C/T is included.

D DTCH or DCCH will be mapped on DSCH/USCH as long as DTCH or DCCH are the only logical channels. If multiplexing of dedicated channels is necessary, C/T is included.

E Could be used if BCCH is mapped on FACH and must be used if CCCH is mapped on RACH/FACH and CTCH messages are used.

1.13 Radio Link Control (RLC)

The RLC protocol offers transport services to the higher layers called *Radio Bearer Services* and is specified in *3GPP 25.322.* RLC supports segmentation and the transport of user and signaling information.

The RLC sublayer consists of RLC entities for the UE-UTRAN interface, of which there are three modes of operation:

- Transparent Mode (TM).
- Unacknowledged Mode (UM).
- Acknowledged Mode (AM).

1.13.1 RLC Services

Connection Establishment/Release

The RLC Connection Establishment/Release organizes the setup or ending of RLC connections.

Transparent Data Transfer

Transparent Data Transfer transmits higher layer PDUs without adding any protocol information, possibly including segmentation and reassembly functionality.

Unacknowledged Data Transfer

Unacknowledged Data Transfer transmits higher layer PDUs without guaranteeing delivery to peer entity. The unacknowledged data transfer mode has the following characteristics:

- Detects erroneous data by using a sequence-number check function. The RLC sublayer delivers to the receiving higher layer only the SDUs that are free of transmission errors.

Unique Delivery

Using duplication detection, the RLC sublayer delivers each SDU to the receiving higher layer only once.

Immediate Delivery

The receiving RLC sublayer entity delivers an SDU to the higher layer receiving entity as soon as the SDU arrives at the receiver.

Acknowledged Data Transfer

Acknowledged Data Transfer transmits higher layer PDUs and guarantees delivery to peer entity. If RLC is unable to deliver data correctly, the user of RLC at the transmitting side is notified. In-sequence delivery and out-of-sequence delivery are supported.

Acknowledged Data Transfer mode has the following characteristics:

- *Error-free delivery:* Ensured by means of retransmission; the receiving entity delivers only error-free SDUs to the higher layer.
- *Unique delivery:* Using duplication detection, the RLC sublayer delivers each SDU to the receiving higher layer only once.
- *In-sequence delivery:* RLC sublayer provides support for a sequential delivery of SDUs. The RLC sublayer delivers SDUs to the receiving higher layer entity in the same order as the transmitting higher layer entity submits to RLC sublayer.
- *Out-of-sequence delivery:* As an alternative to in-sequence delivery, the receiving RLC entity delivers SDUs to the higher layer in a different order than they were submitted to the RLC sublayer at the transmitting side.

1.13.2 RLC Functions

Segmentation and Reassembly

Used for variable length of higher layer PDUs into or from smaller RLC Payload Units (PUs). The PDU size depends on the actual set of transport formats.

Concatenation

Concatenates the contents of RLC SDU with the first segment of the next RLC if they do not fill an integer number of RLC PUs. The SDU may be put into RLC PU in concatenation with the last segment of the previous RLC SDU.

Padding

When concatenation is not applicable and the remaining data to be transmitted does not fill the entire RLC PDU of a given size, then the remainder of the data field is filled with padding bits.

Transfer of User Data

RLC conveys data between users of RLC services and supports acknowledged, unacknowledged, and transparent data transfer. The QoS setting controls the transfer of user data.

Error Correction

Errors are corrected by retransmitting the data while in the acknowledged data transfer mode. Data can be retransmitted using commands such as Selective Repeat, Go Back N, or a Stop-and-Wait ARQ (Automatic Repeat Request).

In-Sequence Delivery of Higher Layer PDUs

Ensures transfer of higher layer PDUs (submitted for transfer by RLC) in the correct order, using acknowledged data transfer. If the function is not used, out-of-sequence delivery is provided.

Duplicate Detection

The RLC detects duplicated PDUs that it receives and ensures that the resultant higher layer PDU is delivered only once to the higher layer.

Flow Control

The RLC receiver controls the rate at which a peer RLC transmitting entity may send information.

Sequence Number Check (Unacknowledged Data Transfer Mode)

The RLC guarantees integrity of reassembled PDUs and provides a mechanism for detection of corrupted RLC SDUs through checking the sequence number in RLC PDUs when the PDUs are reassembled into an RLC SDU. All corrupted RLC SDUs will be discarded.

Protocol Error Detection and Recovery

The RLC detects and recovers from errors in the operation of its protocol.

Ciphering

Ciphering prevents unauthorized acquisition of data and is performed in the RLC layer for nontransparent RLC mode.

Suspend/Resume Function

Suspend/Resume function of data transfer works in the same way as in LAPDm (Ref. GSM 04.05).

Transparent Mode

No RLC information will be added to the message. Erroneous messages will be detected, registered, and discarded. There is no sequence control function available.

This mode is used for streaming application data where the data does not have to be segmented. Applications using transparent mode are video and audio data applications.

Unacknowledged Mode

By using the sequence number, the uniqueness of a data package can be checked, but there is no error correction method specified in this mode. Certain RLC information will be added to the message, and segmentation and ciphering will be performed.

Applications using unacknowledged mode are certain RRC procedures, where the RRC layer is responsible for the receive acknowledgment, the Cell Broadcast Service (CBS), and the VoIP.

Acknowledged Mode

Supports ARQ with all the necessary parameters, and performs segmentation and ciphering. Applications using acknowledged mode are secure transmission and packet-oriented data transfer.

Table 1.9 explains the functions in combination with the different modes.

Note: Ciphering is not part of RLC in the transparent entity.

Table 1.9 RLC function overview table

Transparent entity	Unacknowledged entity	Acknowledged entity
Segmentation/reassembly	Segmentation/reassembly	Segmentation/reassembly
Transfer of application data	Concatenation	Concatenation
	Padding	Padding
	Transfer of application data	Transfer of application data
	Ciphering	Ciphering
	Sequence number check	Error correction
		In-sequence delivery
		Flow control
		Duplicate detection
		Protocol error detection and recovery
		Suspend/resume functionality

1.13.3 RLC Architecture

A UM and a Tr RLC entity can be configured to be a transmitting RLC entity or a receiving RLC entity. The transmitting RLC entity transmits RLC PDUs; the receiving RLC entity receives RLC PDUs (Figure 1.94).

An AM RLC entity consists of a transmitting side and a receiving side, where the transmitting side of the AM RLC entity transmits RLC PDUs and the receiving side of the AM RLC entity receives RLC PDUs.

Elementary procedures are defined between a "Sender" and a "Receiver." In UM and Tr, the transmitting RLC entity acts as a Sender and the peer RLC entity acts as a Receiver. An AM RLC entity acts either as a Sender or as a Receiver depending on the elementary procedure. The Sender is the transmitter of AMD PDUs and the Receiver is the receiver of AMD PDUs. A Sender or a Receiver can reside either at the UE or at the UTRAN.

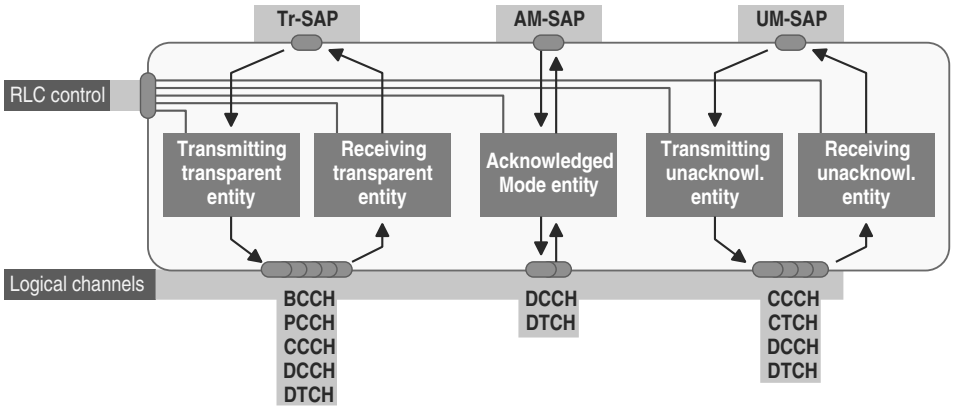


Figure 1.94 RLC architecture.

There is one transmitting and one receiving RLC entity for each TM and UM service. There is one combined, transmitting and receiving entity for the AM service.

Each RLC UM and TM entity uses one logical channel to send or receive data PDUs. An AM RLC entity can be configured to use one or two logical channels to send or receive data and control PDUs. If two logical channels are configured, they are of the same type – DCCH or DTCH.

1.13.4 RLC Data PDUs

Figure 1.95 shows the three different types of RLC Data PDUs.

TMD PDU (Transparent Mode Data PDU)

The TMD PDU is used to convey RLC SDU data without adding any RLC overhead. RLC uses the TMD PDU when RLC is in transparent mode.

UMD PDU (Unacknowledged Mode Data PDU)

The UMD PDU is used to convey sequentially numbered PDUs containing RLC SDU data. RLC uses UMD PDUs when RLC is configured for unacknowledged data transfer.

AMD PDU (Acknowledged Mode Data PDU)

The AMD PDU is used to convey sequentially numbered PDUs containing RLC SDU data. RLC uses AMD PDUs when RLC is configured for acknowledged data transfer.

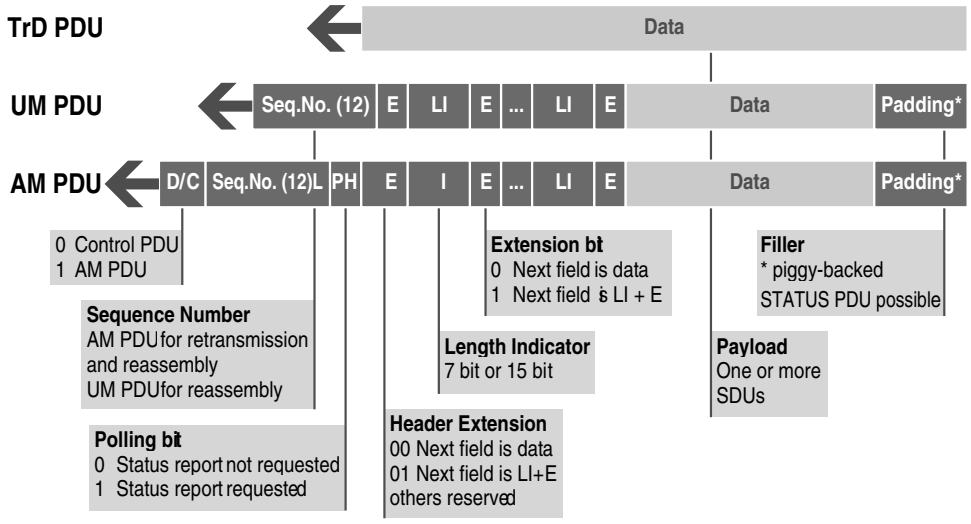


Figure 1.95 RLC data PDUs.

1.13.5 Other RLC PDUs

Other RLC PDUs are:

- RESET PDU – to reset RLC protocol entities and all their system variables.
- RESET ACK PDU – acknowledgment to RESET PDU.

Control PDUs are used only in acknowledged mode. **STATUS PDU** and **Piggybacked STATUS PDU** are used:

- By the Receiver to inform the Sender about missing and received AMD PDUs in the Receiver; selective and group acknowledgment is possible.
- By the Receiver to inform the Sender about the size of the allowed transmission window.
- By the Sender to request that the Receiver move the reception window.
- By the Receiver to acknowledge to the Sender the receipt of the request to move the reception window.

RESET PDU is used:

- To reset all protocol states, protocol variables, and protocol timers of the peer RLC entity in order to synchronize the two peer entities (sent from Sender to Receiver).
- To increment the Hyper Frame Number (Ciphering).

RESET ACK PDU is an acknowledgment of the **RESET PDU** (sent from Receiver to Sender).

1.14 Service Specific Connection Oriented Protocol (SSCOP)

The SSCOP (*ITU-T Q.2110*) has been defined to provide functions required in the Signaling AAL (SAAL). The SAAL is a combination of two sublayers: a common part and a service-specific part. The service-specific part is also known as the SSCS. In the SAAL, the SSCS itself is functionally divided into the SSCOP and an SSCF which maps the services provided by the SSCOP to the needs of the user of the SAAL. This structure allows a common connection-oriented protocol with error recovery (the SSCOP) to provide a generic reliable data transfer service for different AAL interfaces defined by the SSCF. Two such SSCFs. one for signaling at the User-Network Interface (UNI) and one for signaling at the Network-to-Network Interface (NNI), have been defined. It is also possible to define additional SSCFs over the common SSCOP to provide different AAL services.

Sequence Integrity

Preserves the order of SSCOP SDUs that were submitted for transfer by SSCOP.

Error Correction by Selective Retransmission

Through a sequencing mechanism, the receiving SSCOP entity can detect missing SSCOP SDUs. This function corrects sequence errors through retransmission.

Flow Control

Allows an SSCOP receiver to control the rate at which the peer SSCOP transmitter entity may send information.

Error Reporting to Layer Management

Indicates to the layer which management errors have occurred.

Keep Alive

Verifies that the two peer SSCOP entities participating in a connection are remaining in a link-connection-established state even in the case of a prolonged absence of data transfer.

Local Data Retrieval

Allows the local SSCOP user to retrieve in-sequence SDUs that have not yet been released by the SSCOP entity.

Connection Control

Performs the establishment, release, and resynchronization of an SSCOP connection. It also allows the transmission of variable length user-to-user information without a guarantee of delivery.

Transfer of User Data

Conveys user data between users of the SSCOP. SSCOP supports both assured and unassured data transfer.

Protocol Error Detection and Recovery

Detects and recovers from errors in the operation of the protocol.

Status Reporting

Allows the transmitter and receiver peer entities to exchange status information.

1.14.1 Example SSCOP

The example in Figure 1.96 shows the setup, connection, and release phase of an SSCOP connection on the IuPS. *BGN* (Begin) and *BGAK* (Begin Ack) represent the connection setup.

During connection, data of higher layers will be transmitted with Sequenced Data PDUs, *SD*. Every SD contains a sequence number, N(S). After the internal time-out of Timer-POLL, an acknowledgment will be requested, *POLL-PDU*. The acknowledgment is then the *STAT* message containing a receive sequence number, N(R). If there are no SD messages on the link

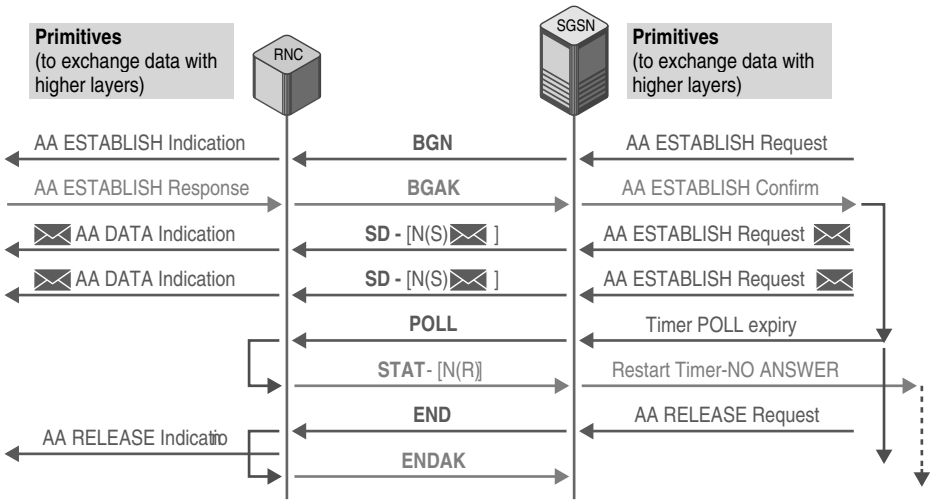


Figure 1.96 SSCOP (message flow).

in the meantime, then the POLL-STAT procedure will also run. The POLL-STAT procedure confirms that the SSCOP connection (link integrity) is established. *END* and *ENDAK* represent the disconnect procedure.

Note: An SSCOP connection is a permanent connection; it is not user-dependent. The connection is set up for each signaling link, for example VPI/VCI for signaling information. All user signaling will be transferred via an SSCOP connection.

1.15 Service Specific Coordination Function (SSCF)

SSCF (*ITU-T Q.2140*) is not a protocol but an internal coordination function, which does internal adaptation of the information coming or going to higher layers, for example MTP3-B routing information. SSCF provides the following mapping functions:

- Mapping of primitives from Layer 3 to signals of the SSCOP.
- Mapping of destination address (Signaling Point Code, SPC) to SSCOP connection.

Because of this modular concept, SSCOP can work with many different higher layer protocols.

1.16 Message Transfer Part Level 3 – Broadband (MTP3-B)

MTP3-B (*ITU.T Q.2210*) fulfills the same sort of work as the standard narrowband MTP; it provides identification and transport of higher layer messages (PDUs), routing, and load sharing (Figure 1.97).

The main address parameters are Originating and Destination Point Codes (ODC and DPC). Their unique value represents the SPC of a network component.

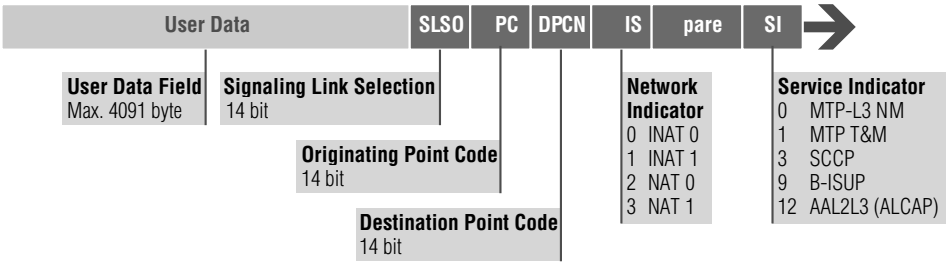


Figure 1.97 MTP3-B.

Network Indicator

Used on Points of Interconnection (POI) to build virtual interconnection networks on or between national and international network level.

Service Indicator

Identifies the contents of the user data field (for example the higher layer protocol).

1.17 Internet Protocol (IP)

The Internet Protocol (*RFC 791*) version 4, IPv4, provides connectionless services between networks and includes features for addressing, type-of-service specification, fragmentation and reassembly, and security. IP transmits data without a connection and without protection of the data, such as ciphering, authentication, flow control, or any other error correction mechanism.

The addressing is symmetrical; the source and destination addresses are always in the header. The data contained in an IP message can be 64 kbytes maximum, where every IP node must be able to handle packet sizes of 576 bytes minimum.

The next generation is IP version 6. The goal was to improve these negative features of IPv4. The address range has been enhanced to 128 bits. This version now includes protection mechanisms, including ciphering and integrity check of data and address. It also now supports real QoS.

- IP version 4:
  - no error control or correction
  - no sequence or flow control
  - fragmentation and reassembly of data; header minimum of 20 bytes
  - address size: 32 bits, source and destination included.
- IP version 6:
  - Qos parameter included and used
  - remote configuration of IP users
  - authentication and ciphering mechanism included
  - signature of address and contents
  - fragmentation and reassembly of data; header minimum of 40 bytes
  - address size: 128 bits, source and destination included.

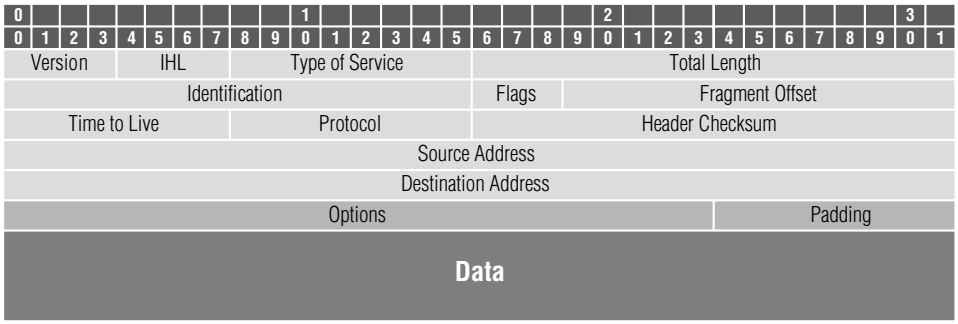


Figure 1.98 IPv4 frame architecture.

1.17.1 IPv4 Frame Architecture

Flags and *Fragment Offset* will indicate if the data part contains a full message or just a segment of one. The offset value will indicate a multiple of 8 bytes (Figure 1.98).

Time to Live is not a timer but a hop counter which has to be decremented by every IP node. If it reaches zero, the packet will be deleted.

Protocol identifies the next higher layer protocol. Table 1.10 gives some examples.

Source and Destination Address contains the 32-bit node address, for example 192.168.1.17.

Options are optional and usually not included.

1.18 Signaling Transport Converter (STC)

STC (*ITU-T Q.2150.1*) is an internal function, which has none of its own messages. It converts primitives from lower and higher layers (either MTP-3 or MTP3-B primitives) and their parameters fitting the requirements of the other. Other functions are:

- Provision of OPC, DPC and SIO value.
- UMTS: Service Indicator (part of SIO) = 12 (AAL2-L3).

Table 1.10 Protocol parameter meaning

Value	Meaning
1	ICMP, Internet Control Message Protocol
2	IGMP, Internet Group Management Protocol
6	TCP, Transmission Control Protocol
17	UDP, User Datagram Protocol
41	IPv6, IP version 6
132	SCTP, Stream Control Transmission Protocol

In UMTS the (AAL2L3) Signaling protocol could be on STC. To allow AAL2L3 to set up user connections in the network, it has to send certain messages to the partner instances. The routing and selection of SPCs is the responsibility of STC.

1.19 Signaling Connection Control Part (SCCP)

SCCP (*ITU-T Q.711-716*) provides a service for transfer of messages between any two signaling points in the same or different network and is used in the same way as it is known from SS7 and GSM. It can act as connectionless or connection-oriented transport protocol and provides the following connection types:

- Connectionless (Class 0 & l) and connection oriented (Class 2 & 3).
- Class 0:
  – addressing purposes, DPC or Global Title (GT)
- Class 2:
  – used on IuCS, IuPS, and Iur interfaces to organize connections (Class 3)
  – planned to be used on Iur interface by some switch manufacturers
  – SCCP user is called Subsystem and identified by a subsystem number (SSN)
- Class 3:
  – flow control connection-oriented class
  – (probably) not used on Iur.

The SCCP (Signaling Connection Control Part) user is called Subsystem and identified by an SSN that has the same function as the protocol field previously described in the IP protocol part (1.16). For instance on Iu interface RANAP is an SCCP subsystem. However, a subsystem can be both a higher layer protocol or a network element/function. Table 1.11 gives an overview of SSN used in live network environments.

Table 1.11 SSN overview

Value	Meaning
6	HLR
7	VLR
8	MSC
12	INAP/MAP operator defined
142	RANAP
143	RNSAP
146	CAP
147	gsmSCF
149	SGSN
150	GGSN
192	BSSAP+ on Gs interface
254	BSSAP

The differences between connectionless and connection-oriented data exchange are as follows.

Connectionless

SCCP is responsible for the end-to-end addressing. SCCP creates addresses by either giving the DPC or a GT of the endpoint. A GT has to be translated (GTT – Global Title Translation) on the way to the destination. On the last link to the destination point, the GT will be replaced with a DPC.

Connection Oriented

SCCP is responsible for the user connection running on one interface. It is not controlling an end-to-end connection. The connection is identified by a Source and a Destination Local Reference Number (SLR, DLR).

To identify the transported higher protocol, SCCP uses an SSN.

1.19.1 Example SCCP

Connection-Oriented Example

Connection Request (CR) and Connection Confirm (CC) represent the setup phase. In the setup phase, the two sides exchange the local reference numbers. A negative response would be the Connection Refused (CREF) message, which would contain a cause explaining the problem (Figure 1.99).

Some procedures use the CREF message as a fast method to release the procedure, for example, if all necessary information has been already send in the CC. During the connection Data Form 1 (**DT1**) message will transport higher layer messages. To release the SCCP connection, a Released (**RLSD**) and a Release Complete (**RLC**) message will be exchanged. Every main user procedure has its own SCCP connection on the Iu interfaces.

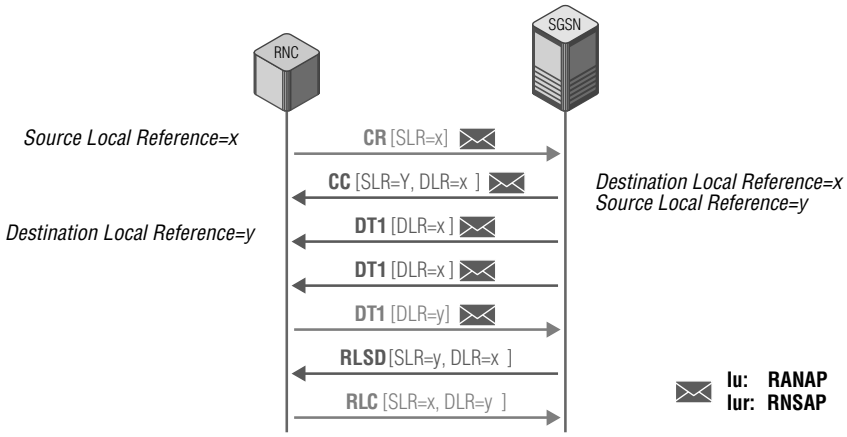


Figure 1.99 SCCP CO (message flow).

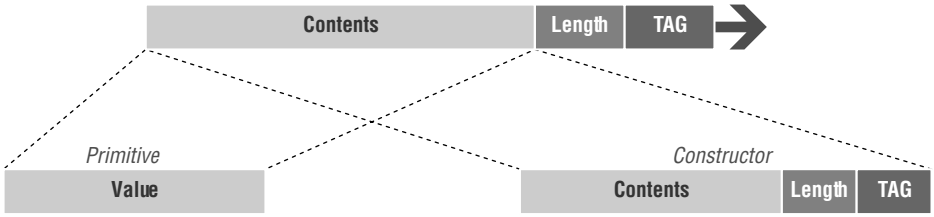
1.20 Abstract Syntax Notation One (ASN.1) in UMTS

The protocols RANAP, RNSAP, NBAP, RRC (Basic-PER, octet aligned), MAP, and CAP (BER) are specified by using ASN.l (ISO/IEC 8824-1), a protocol description language. ASN.l provides the following functions:

- Automatic generation of network component protocol software.
- Fast access of information by receiving entity.
- Compact form of information transmission by using special encoding rules:
  - Basic Encoding Rules (BER; ISO/IEC 8825 and 8825-1): used for MAP and CAP, easy-to-read raw data contents, messages are quite large, data clearly structured, big messages
  - Packed Encoding Rules (PER; ISO/IEC 8825-2): used for the other named protocols (running within UTRAN), very compact raw data contents, and small messages
    - data structure is known by sender and receiver – > omits extra data-specific information, compact and smaller messages.

1.20.1 ASN.1 BER

Every protocol element is represented by an identifying TAG, a length field, and a contents field. In the case of primitive contents forms, the contents field consists of one value. In the case of constructor contents forms, the contents field consists of one or more other TAG-Length-Contents constructions. In this case, the first byte of the contents field is a TAG. ASN.l BER is used by MAP and CAP in the CN (Figure 1.100).




```
invoke            [1] Invoke
Invoke: := SEQUENCE {
        invoke_id         INTEGER (size(1))
        … }
```

```
2.1 Invoke
10100001 Tag                        (CONT (C) [1])
00100100 Length                     36
2.1.1 Invoke ID
00000010 Tag                        (UNIV (P) Integer)
00000001 Length                     1
00000001 Invoke ID value            1
```

Figure 1.100 ASN.1 BER.


```
number ::= INTEGER (1..2)
name ::= OCTETSTRING (size(0..4))
number
1xxxxxxx  Contents                1
name
100xxxxx  Length                  4
***B4*** Contents                 LOLA

x = octet alignment bits
```

Figure 1.101 ASN.1 PER.

1.20.2 ASN.1 PER

The packed encoding rules aim to transmit as little data as possible. That is why a preamble (similar to a tag field) and the length field can be missing. Sender and Receiver have to use the same protocol versions; otherwise the Receiver will not understand the contents of a received message.

There are two alternative PER: octet aligned and octet unaligned. In UMTS the octet aligned version will be used, with the exception of the RRC, which uses unaligned. This means that even if a field requires just 1 bit (see the number in Figure 1.101), the field would be of size 1 byte, 7 bits filled with zeros (x). ASN.l PER is used by NBAP, RNSAP, RRC, and RANAP in the UTRAN.

1.21 Radio Resource Control (RRC)

The RRC (*3GPP 25.331*) protocol is the most complex one in UMTS. It reflects the tasks of the RNC.

RRC is a sublayer of Layer 3 on UMTS radio interface and exists in the control plane only. It provides an information transfer service to the NAS and is responsible for controlling the configuration of UMTS radio interface Layers 1 and 2 (Figure 1.102). Because RNC is a network node between UE and CN, RRC must be able to transport NAS message across the UTRAN.

The Radio Bearer control function is also implemented in RRC. This function is performed by a special RRC signaling procedure but also internally by controlling both the lower layers and the user plane protocols via the RRC Control SAP. The management of a UE during an RRC connection is controlled by RNC using the RRC protocol as well.

The main functions and services of RRC are:

- Routing of higher layer messages to different Mobility Management/Call Management (MM/CM) entities on UE side or to different CN domains.
- Creation and management of Radio Bearers.
- Broadcasting of system information.

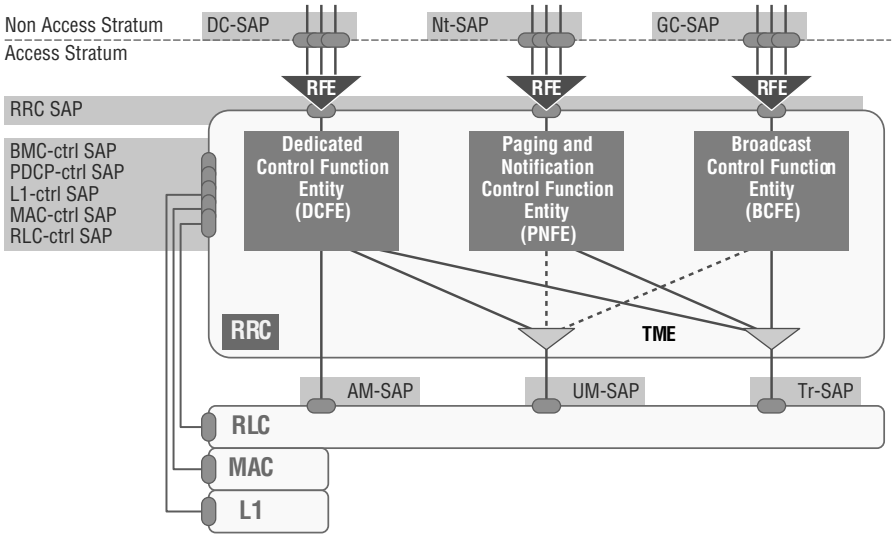


Figure 1.102 RRC architecture.

- Paging of Ues.
- Dedicated Control handles all functions specific to one UE:
  – Location Management
  – Handover.
- SMS Routing.
- Power Management (outer loop power control).
- Configuration of lower layer protocols.
- Setup of RRC measurement settings.
- Management of measurement report.

1.21.1 RRC States (3GPP 25.331)

To understand some of the signaling procedures described later in this book, for example cases of physical channel reconfiguration (channel-type switching), it is necessary to have a closer look at the RRC state machine (Figure 1.103). Figure 1.104 provides further details.

After power is on, the UE stays in Idle Mode (RRC Idle) until it transmits a request to establish an RRC connection. In Idle Mode the connection of the UE is closed on all layers of the access stratum. In Idle Mode the UE is identified by NAS identities such as IMSI, TMSI, and P-TMSI. In addition, the UTRAN has no information about the individual Idle Mode UEs, and it can only address all UEs in a cell or all UEs monitoring a paging occasion. The UTRAN Connected Mode is entered when the RRC connection is established. The UE is assigned an RNTI to be used as UE identity on Common Transport Channels (Figure 1.97).

The RRC states within the UTRAN Connected Mode reflect the level of the UE connection and which transport channels can be used by the UE.

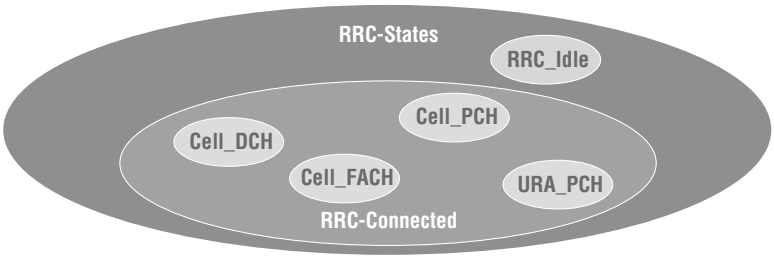


Figure 1.103 Overview of different RRC states.

For inactive stationary data users, the UE may fall back to PCH on both the Cell and URA levels. Upon the need for paging, the UTRAN will check the current level of connection of the given UE, and will decide whether the paging message should be sent within the URA or via a specific cell.

The *RRC_Idle* state is characterized by the following:

- UE is unknown in UTRAN, and no RNTIs have been assigned; TMSI or P-TMSI might be allocated if UE was registered into the network previously.
- UE monitors downlink PICH/PCH (paging must be detected to change into RRC Connected Mode).
- If UE is moving, it will perform Routing and Location Area Update procedures.

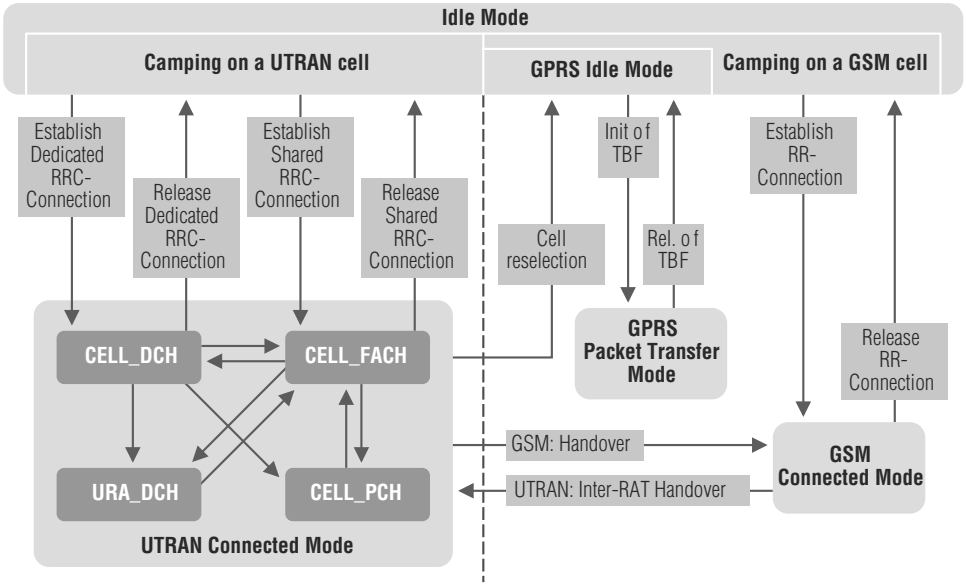


Figure 1.104 Detailed RRC state overview.

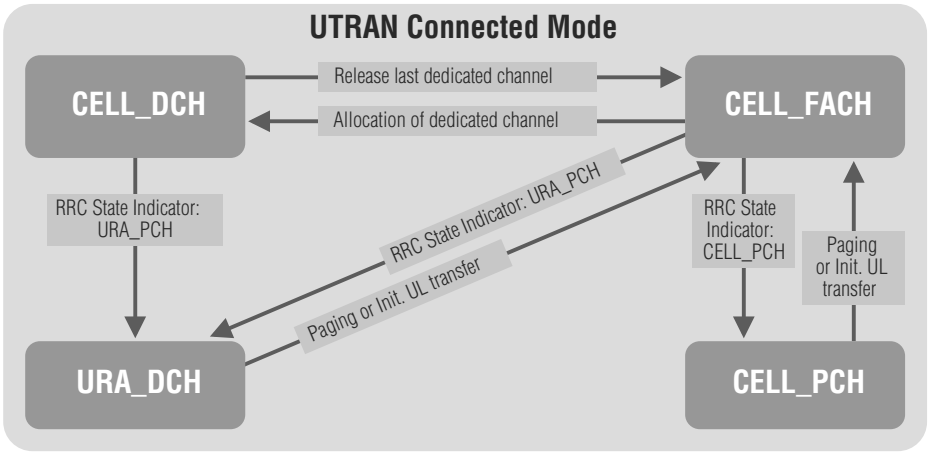


Figure 1.105 UTRAN – Connected Mode States.

- Cell Reselection will be performed depending on the radio conditions but no Cell Updates or URA Updates will happen.
- DCCHs or DPCHs do not exist.
- UE sends RRC_CONN_REQ on RACH to change into RRC Connected Mode.

Note: Not all states may be applicable for all UE connections. For a given QoS requirement on the UE connection, only a subset of the states may be relevant.

The transition to the UTRAN Connected Mode from the Idle Mode can only be initiated by the UE by transmitting a request for an RRC connection. The event is triggered either by a paging request from the network or by a request from higher layers in the UE. When the UE receives a message from the network that confirms the RRC connection establishment, the UE enters the CELL_FACH or CELL_DCH state of UTRAN Connected Mode.

In the case of a failure, to establish the RRC Connection, the UE goes back to Idle Mode. The possible causes are radio link failure, a received reject response from the network, or lack of response from the network (time-out).

Connected Mode States (Figure 1.105)

The *CELL_DCH* state is characterized by the following:

- A dedicated physical channel is allocated to the UE in uplink and downlink.
- Common/shared channels might be configured.
- The UE is known on cell level according to its current active set.
- Soft and Hard HO might be initiated.
- No Cell Update or URA Update is initiated by the UE.
- The UE sends Measurement Reports to RNC according to the RNC setup.
- The UE can use Dedicated Transport Channels (DCH), downlink and uplink (TDD) shared transport channels (TCH), and a combination of these transport channels.

The CELL_DCH state is entered from the Idle Mode through the setup of an RRC connection, or by establishing a dedicated physical channel from the CELL_FACH state.

A PDSCH may be assigned to the UE in this state, to be used for a DSCH. In TDD a PUSCH may also be assigned to the UE in this state, to be used for a USCH. If PDSCH or PUSCH are used for TDD, a FACH transport channel may be assigned to the UE for reception of physical shared channel allocation messages.

The *CELL-FACH* state is characterized by the following:

- No dedicated physical channel is allocated to the UE.
- The UE continuously monitors a FACH in downlink.
- The UE is assigned a default common or shared transport channel in the uplink (e.g. RACH or CPCH) that it can use anytime according to the access procedure for that transport channel.
- No Soft or Hard HO might be initiated.
- UTRAN knows the position of the UE on the cell level according to the cell where the UE last made a cell update.
- The UE performs Cell Updates, but no URA updates.
- In TDD mode, one or several USCH or DSCH transport channels may have been established.

In the *CELL.FACH* substate, the UE performs the following actions:

- Listens to all FACHs in the cell.
- Listens to the BCH transport channel of the serving cell for the decoding of system information messages.
- Initiates a cell update procedure on cell change of another UTRA cell.
- Uses C-RNTI assigned in the current cell as the UE identity on Common Transport Channels except for when a new cell is selected.
- Transmits uplink control signals and small data packets on the RACH.
- In FDD mode, transmits uplink control signals and larger data packets on CPCH when resources are allocated to the cell and UE is assigned use of those CPCH resources.
- In TDD mode, transmits signaling messages or user data in the uplink and/or the downlink using USCH and/or DSCH when resources are allocated to the cell and the UE is assigned use of those USCH/DSCH resources.
- In TDD mode, transmits measurement reports in the uplink using USCH when resources are allocated to it in order to trigger a handover procedure in the UTRAN.

The *CELL_PCH* state is characterized by the following:

- No dedicated physical channel is allocated to the UE.
- UE selects a PCH with an algorithm and uses DRX for monitoring the selected PCH via an associated PICH.
- DCCHs/DTCHs are configured but cannot be used.
- No Soft or Hard HO might be initiated.
- No uplink activity is possible (state change to Cell_FACH is needed).
- The UE performs Cell Updates, but no URA updates.
- Position of the UE is known by UTRAN on the cell level according to the cell where the UE last made a cell update in the CELL_FACH state.
- The UE sends Measurement Reports to RNC according to the RNC setup.

In the *CELL_PCH* state the UE performs the following actions:

- Monitors the paging occasions according to the DRX cycle and receives paging information on the PCH.
- Listens to the BCH transport channel of the serving cell for the decoding of system information messages.
- Initiates a cell update procedure on cell change.
- The DCCH logical channel cannot be used in this state. If the network wants to initiate any activity, it needs to make a paging request on the PCCH logical channel in the known cell to initiate any downlink activity.

The *URA_PCH* state is characterized by the following:

- No dedicated channel is allocated to the UE.
- UE selects a PCH with an algorithm and uses DRX for monitoring the selected PCH via an associated PICH.
- UE monitors downlink PICH/PCH (paging must be detected to change into RRC connected mode).
- No uplink activity is possible.
- DCCHs/DTCHs are configured but cannot be used.
- No uplink activity is possible (state change to CELL_FACH is needed).
- Location of the UE is known on the URA level according to the URA assigned to the UE during the last URA update in CELL_FACH state.

In the *URA_PCH* state the UE performs the following actions:

- Monitors the paging occasions according to the DRX cycle and receive paging information on the PCH.
- Listens to the BCH transport channel of the serving cell for the decoding of system information messages.
- Initiates a URA updating procedure on URA change.

The DCCH logical channel cannot be used in this state. If the network wants to initiate any activity, it needs to make a paging request on the PCCH logical channel within the URA where the location of the UE is known. If the UE needs to transmit anything to the network, it goes to the CELL_FACH state. The transition to URA_PCH state can be controlled with an inactivity timer, and, optionally, with a counter, which counts the number of cell updates. When the number of cell updates has exceeded certain limits (a network parameter), the UE changes to the URA_PCH state.

URA updating is initiated by the UE, which, upon the detection of the Registration area, sends the network the Registration area update information on the RACH of the new cell.

Note: A UE supporting CBS should be capable of receiving BMC messages in the CELL_PCH or URA_PCH state. If PCH and the FACH carrying CTCHs are not mapped onto the same S-CCPCH, UEs with basic service capabilities may not be able to monitor Cell Broadcast messages continuously in CELL_PCH state. In this case, UEs with basic service capabilities are capable of changing from the S-CCPCH that carries the PCH selected for paging to another S-CCPCH that carries Cell Broadcast messages (for example the CTCH mapped

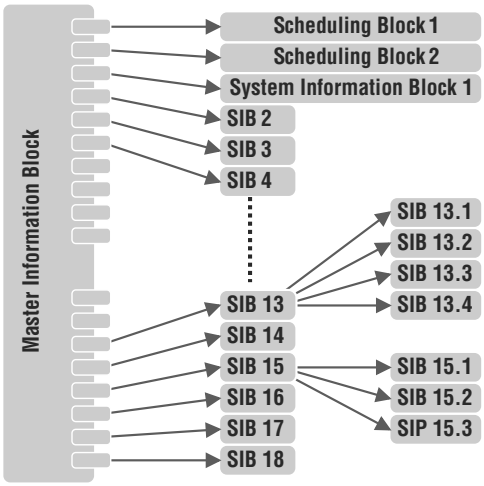


Figure 1.106 SIB overview.

to a FACH) and receives BMC messages during time intervals which do not conflict with the UE-specific paging occasions.

1.21.2 System Information Blocks (SIBs)

The system information elements are broadcast in System Information Blocks (SIBs) that can be monitored, for example in System Information Update messages during Node B setup/restart. A SIB groups together system information elements of the same nature. Different SIBs may have different characteristics, for example, regarding their repetition rate and the requirements on UEs to re-read the SIBs (Figure 1.106).

The system information is organized as a tree. A Master Information Block (MIB) gives references to a number of SIBs in a cell, including scheduling information for those SIBs. The SIBs contain the actual system information and optionally references to other SIBs having scheduling information for those SIBs. The referenced SIBs must have the same area scope and use the same update mechanism as the parent SIB.

Some SIBs may occur more than once with different content. In this case, scheduling information is provided for each occurrence of the SIB. This option is allowed only for SIB type 16.

All SIBs, except SIB 15.2, 15.3, and 16, use a random ID called a *value tag.* As long as the value tag contains the same value, the contents of the SIBs are unchanged. This means that a UE receives SIB and stores the value tag. The next occurrence of that SIB and UE will compare value tags. If the value is equal to the stored value, then the contents of the SIB can be discarded. If the value is different, then UE will read the SIB contents and store the new value tag.

SIB 15.2, 15.3, and 16 contain a value tag, too, but their contents must always be read. Depending on SIB, the contents and the value tag are valid within a cell or within UTRAN (Table 1.12).

Table 1.12 SIB content

Value	Meaning
SIB 1	NAS System Information, UE timer, and counter for RRC Idle and Connected Mode
SIB 2	URA Identity
SIB 3	Parameter for Cell Selection and Reselection
SIB 4	Parameter for Cell Selection and Reselection in RRC Connected Mode
SIB 5	Parameter for configuration of CPCH of actual cell
SIB 6	Parameter for configuration of Common and Shared Physical Channel of actual cell
SIB 7	Fast changing parameter for uplink Interference and Dynamic Persistence Level
SIB 8	Static CPCH Information of actual cell (FDD only)
SIB 9	CPCH Information of actual cell (FDD only)
SIB 10	Information for UE, which DCH is controlled by Dynamic Resource Allocation Control Procedure
SIB 11	Measurement Control Information of actual cell
SIB 12	Measurement Control Information of actual cell in RRC Connected Mode
IB 13	ANSI-41 System Information
SIB 13.1	ANSI-41 RAND Information
SIB 13.2	ANSI-41 User Zone Identification
SIB 13.3	ANSI-41 Private Neighbor List
SIB 13.4	ANSI-41 Global Service Redirection
SIB 14	UL outer loop power control information for common and dedicated physical channels in RRC Idle or Connected Mode
SIB 15	Information for UE positioning method
SIB 15.1	Information for UE GPS positioning method with Differential Global Positioning System (DGPS) correction
SIB 15.2	Information for GPS Navigation Model
SIB 15.3	Information for GPS Almanac, ionospheric, and UTC Model
SIB 15.4	UE-assisted information for OTDOA UE Positioning method
SIB 15.5	UE-based information for OTDOA UE positioning method
SIB 16	Information of Radio Bearer, transport, and physical channels for UE in RRC Idle or Connected Mode in case of HO to UTRAN
SIB 17	Fast changing parameter for the configuration of Shared Physical Channels in RRC Connected Mode (FDD only)
SIB 18	PLMN Identities of neighbor cells

SIB Content

Note: As SIBs are defined in RRC, but transmitted in NBAP, special decoders are needed to monitor SIBs with a protocol tester, which has to cope with the fact that one protocol is octet-aligned encoded, and the other protocol is not.

Example – Broadcast System Information

The *system information* is continuously repeated on a regular basis in accordance with the scheduling defined for each system information block (Figure 1.107).

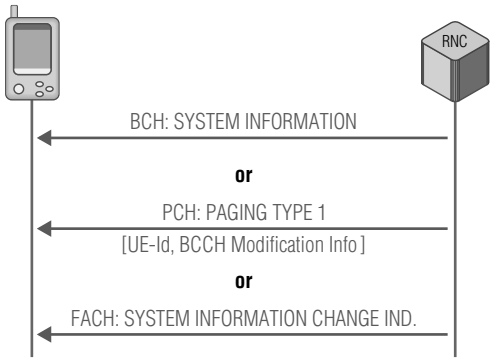


Figure 1.107 Broadcast System Information (message flow).

The UE reads **SYSTEM INFORMATION** messages broadcast on a BCH transport channel in Idle Mode as well as in states CELL_FACH, CELL_PCH, URA_PCH, and CELL_DCH (TDD only). Further, the UE reads SYSTEM INFORMATION messages broadcast on a FACH transport channel when in the CELL_FACH state. In addition, UEs that support simultaneous reception of one SCCPCH and one DPCH read system information on a FACH transport channel when in the CELL_DCH state.

Idle mode and connected mode UEs may acquire different combinations of SIBs. Before each acquisition, the UE should identify which SIBs are needed. The UE may store SIBs (including their value tag) for different cells and different PLMNs, to be used if the UE returns to these cells. The UE considers the SIBs valid for a period of 6 hours from reception. Moreover, the UE considers all stored SIBs as invalid after the UE has been switched off.

When selecting a new cell within the currently used PLMN, the UE considers all current SIBs with area scope cell to be invalid. If the UE has stored valid SIBs for the newly selected cell, the UE may set those as current SIBs.

After selecting a new PLMN, the UE considers all current SIBs to be invalid. If the UE has previously stored valid SIBs for the selected cell of the new PLMN, the UE may set those as current SIBs. Upon selection of a new PLMN, the UE stores all information elements specified in the variable SELECTED PLMN for the new PLMN.

For *modification of some system information* elements (for example, reconfiguration of the channels), it is important for the UE to know exactly when a change occurs. In such cases, the UTRAN should perform the following actions to indicate the change to the UEs.

Send the **PAGING TYPE 1** message on the PCCH in order to reach Idle Mode UEs as well as Connected Mode UEs in state CELL_PCH and URA_PCH. In the IE "BCCH Modification Information," UTRAN indicates the SFN when the change will occur and the new value tag that will apply for the MIB after the change has occurred. The PAGING TYPE 1 message is sent in all paging occasions.

Send the message **SYSTEM INFORMATION CHANGE INDICATION** on the BCCH mapped on FACH on all FACHs in order to reach all UEs in state CELL_FACH. In the IE "BCCH Modification Information," UTRAN indicates the SEN when the change will occur and the new value tag that will apply for the MIB after the change has occurred. UTRAN may repeat the SYSTEM INFORMATION CHANGE INDICATION on all FACHs to increase the probability of proper reception in all UEs needing the information.

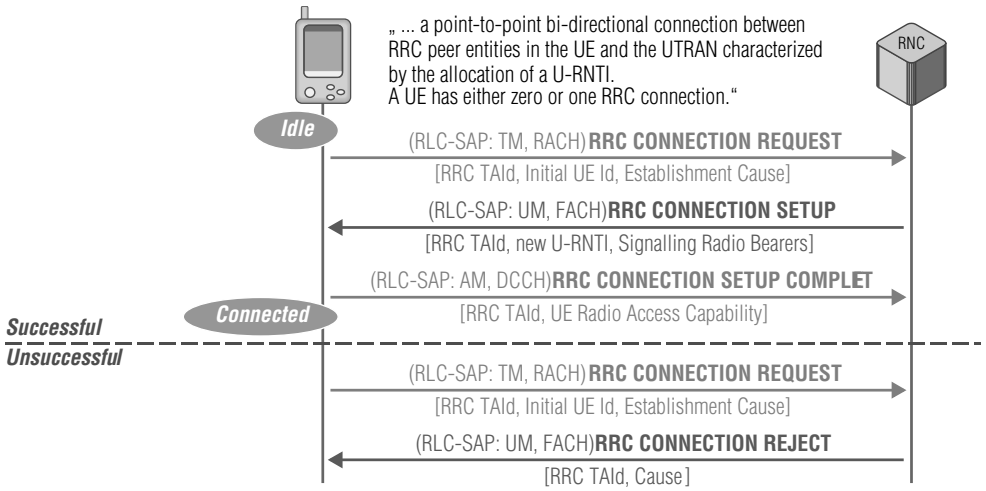


Figure 1.108 RRC Connection Establishment (message flow).

Example – RRC Connection Establishment

The NAS in the UE may request the establishment of only one RRC connection (Figure 1.108). Upon initiation of the procedure, the UE will:

- Set Connection Frame Number (CFN) in relation to System Frame Number (SFN) of current cell according to 8.5.17.
- Transmit an **RRC CONNECTION REQUEST** message on the uplink CCCH, reset counter V300, and start timer T300.
- Perform the mapping of the Access Class to an Access Service Class and apply the given Access Service Class when accessing the RACH.
- Set the IE "Establishment cause" reflecting the cause of establishment in the higher layers.
- Set the IE "Initial UE identity" to IMSI or TMSI.
- Include a measurement report, as specified in the IE "Intrafrequency reporting quantity for RACH reporting" and the IE "Maximum number of reported cells on RACH" in SIB type 11.

Upon receiving an RRC CONNECTION REQUEST message, UTRAN will do one of the following:

- Transmit an **RRC CONNECTION SETUP** message on the downlink CCCH.
- Transmit an **RRC CONNECTION REJECT** message on the downlink CCCH. In the RRC CONNECTION REJECT message, the UTRAN may direct the UE to another UTRA carrier or to another system. After the RRC CONNECTION REJECT message has been sent, all context information for the UE may be deleted in UTRAN.

Upon receiving an RRC CONNECTION SETUP message, the UE compares the value of the IE "Initial UE identity" in the received RRC CONNECTION SETUP message with the value

of the IE "Initial UE identity" in the most recent RRC CONNECTION REQUEST message sent by the UE. If the values are different, the UE will:

- Ignore the rest of the message.

If the values are identical, the UE will:

- Stop timer T300, and act upon all received information elements.
- Store the value of the IE "New U-RNTI".
- Initiate the signaling link parameters according to the IE "RB mapping info".
- If neither the IE "PRACH info (for RACH)" nor the IE "Uplink DPCH info" is included, let the physical channel of type PRACH that is given in the system information be the default in uplink to which the RACH is mapped.
- If neither the IE "Secondary CCPCH info" nor the IE "Downlink DPCH info" is included, start to receive the physical channel of type S-CCPCH that is given in system information to be used as the default by FACH.
- Transmit an **RRC CONNECTION SETUP COMPLETE** message on the uplink DCCH after successful state transition, with the contents set as specified below:
  - include START (*3GPP 33.102*) values to be used in ciphering and integrity protection for each CN domain
  - if requested in the IE "Capability update requirement" sent in the RRC CONNECTION SETUP message, include its UTRAN-specific capabilities in the IE "UE radio access capability"
  - if requested in the IE "Capability update requirement" sent in the RRC CONNECTION SETUP message, include its intersystem capabilities in the IE "UE system specific capability".

Example – RRC Connection Release

The purpose of the example in this procedure is to release the RRC connection including the signaling link and all radio bearers between the UE and the UTRAN. By doing so, all established signaling flows and signaling connections will be released (Figure 1.109).

When the UE is in the state CELL_DCH or CELL_FACH, the UTRAN may at any time initiate an RRC connection release by transmitting an **RRC CONNECTION RELEASE** message using UM RLC. When UTRAN transmits an RRC CONNECTION RELEASE message as response to a received **RRC CONNECTION RE-ESTABLISHMENT REQUEST**, **CELL UPDATE**, or **URA UPDATE** message from the UE, UTRAN will use the downlink CCCH to transmit the message. In all other cases, the downlink DCCH will be used, although the downlink CCCH may be used as well.

UTRAN may transmit several RRC CONNECTION RELEASE messages to increase the probability of proper reception of the message by the UE. The number of repeated messages and the interval between the messages is a network option.

The UE will receive and act on an RRC CONNECTION RELEASE message in states CELL_DCH and CELL_FACH.

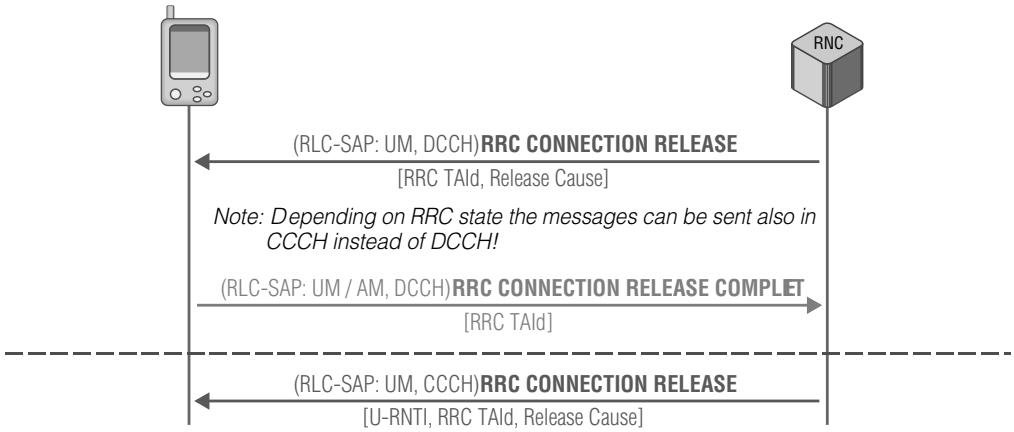


Figure 1.109 RRC Connection Release (message flow).

Furthermore, this procedure can interrupt any ongoing procedures with the UE in the above listed states.

When the UE receives the first RRC CONNECTION RELEASE message, it will:

- In state CELL_DCH:
  - initialize the counter T308 with the value of the IE "Number of RRC Message Transmissions," which indicates the number of times the RRC CONNECTION RELEASE COMPLETE message is sent
  - transmit an RRC CONNECTION RELEASE COMPLETE message using UM RLC on the DCCH to the UTRAN
  - start timer T308.
- In state CELL_FACH and if the RRC CONNECTION RELEASE message was received on the DCCH:
  - transmit an RRC CONNECTION RELEASE COMPLETE message using AM RLC on the DCCH to the UTRAN.

When in state CELL_FACH and if the RRC CONNECTION RELEASE message was received on the CCCH, the UE will not transmit an RRC CONNECTION RELEASE COMPLETE message.

The UE will ignore any succeeding RRC CONNECTION RELEASE messages that it receives. The UE will indicate release of all current signaling flows and radio access bearers to the NAS and pass the value of the IE "Release cause" received in the RRC CONNECTION RELEASE message to the NAS.

From the time of the indication of release to the NAS until the UE has entered idle mode, any NAS request to establish a new RRC connection will be queued. This new request may be processed only after the UE has entered idle mode. When in state CELL_FACH and if the RRC CONNECTION RELEASE message was received on the CCCH, the UE will release all its radio resources, enter idle mode, and end the procedure on the UE side.

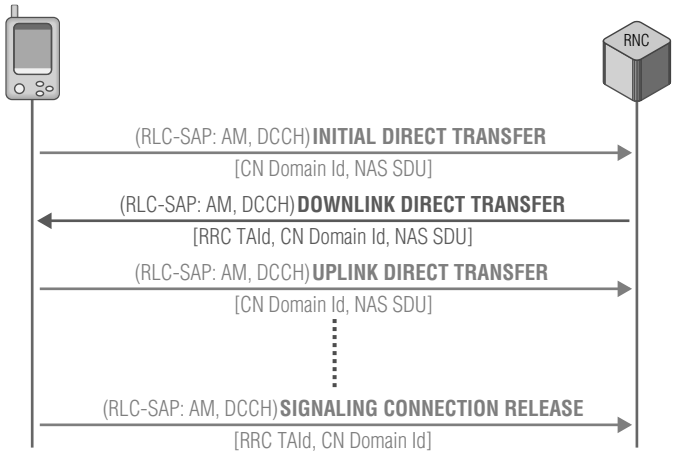


Figure 1.110 RRC Signaling Connection (message flow).

Example – RRC Signaling Connection

The INITIAL DIRECT TRANSFER procedure is used in the uplink to establish signaling connections and signaling flows. It is also used to carry the initial higher layer (NAS) messages over the radio interface.

A signaling connection comprises one or several signaling flows. This procedure requests the establishment of a new flow, and triggers, depending on the routing and if no signaling connection exists for the chosen route for the flow, the establishment of a signaling connection (Figure 1.110).

The DOWNLINK DIRECT TRANSFER procedure is used in the downlink direction to carry higher layer (NAS) messages over the radio interface.

The UPLINK DIRECT TRANSFER procedure is used in the uplink direction to carry all subsequent higher layer (NAS) messages over the radio interface belonging to a signaling flow.

The SIGNALING CONNECTION RELEASE request procedure is used by the UE to request from the UTRAN that one of its signaling connections should be released. The procedure may, in turn, initiate the signaling flow release or RRC connection release procedure.

1.22 Node B Application Part (NBAP)

NBAP (*3GPP 25.433*) is the communication protocol used on the Iub interface, between RNC and Node B, and is specified using ASN.l PER.

1.22.1 NBAP Functions

NBAP covers a large range of different functions as described in Table 1.13.

Table 1.13 NBAP function overview

Function	Description
Cell Configuration Management	Manages the cell configuration information in a Node B
Common Transport Channel Management	Manages the configuration of Common Transport Channels in a Node B
System Information Management	Manages the scheduling of system information to be broadcast in a cell
Resource Event Management	Informs the CRNC about the status of Node B resource
Configuration Alignment	Verifies and enforces that both nodes have the same information on the configuration of the radio resources
Measurements on Common Resources	Initiate measurements in the Node B Report the result of the measurements
Radio Link Management	Manages radio links using dedicated resources in a Node B
Radio Link Supervision	Reports failures and restorations of a radio link
Compressed Mode Control [FDD]	Control the usage of compressed mode in a Node B
Measurements on Dedicated Resources	Initiate measurements in the Node B and report the result of the measurements
DL Power Drifting Correction [FDD]	Adjusts the DL power level of one or more radio links in order to avoid DL power drifting between the radio links
Reporting of General Error Situations	Reports general error situations for which function-specific error messages have not been defined
Physical Shared Channel Management [TDD]	Manages physical resources in the Node B belonging to shared channels (USCH/DSCH)
DL Power Time Slot Correction [TDD]	Enables the Node B to apply an individual offset to the transmission power in each time slot according to the downlink interference level at the UE

1.22.2 NBAP Elementary Procedures (EPs)

The NBAP protocol is used between RNC and Node B to configure and manage the Node B and setup channels on Iub and Uu interfaces. It consists of EPs. An EP is a unit of interaction between the CRNC and the Node B; the NBAP INITIATING MESSAGE is transporting the procedure request. The EP is identified by the parameter **Procedure Identification Code.** The CRNC Communication Context contains all information for the CRNC to communicate with a specific UE.

The Context is identified by the parameter **CRNC Communication Context Identifier**.

An EP consists of an initiating message and possibly a response message. Two kinds of EPs are used:

- *Class 1:* EPs with response (success or failure).
- *Class 2:* EPs without response.

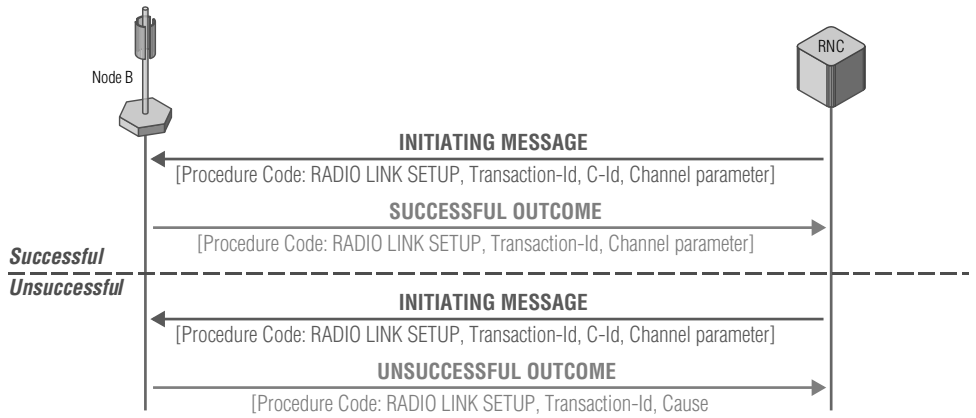


Figure 1.111 NBAP (message flow).

For *Class 1* EPs, the types of responses can be as follows:
Successful (**SUCCESSFUL OUTCOME** Message)

- A signaling message explicitly indicates that the elementary procedure has been successfully completed with the receipt of the response.

Unsuccessful (UNSUCCESSFUL OUTCOME Message)

- A signaling message explicitly indicates that the EP failed.

Class 2 EPs are considered always successful.

1.22.3 Example – NBAP

The example in Figure 1.111 shows the Radio Link Setup procedure, Class 1, both successful and unsuccessful.

1.23 Radio Network Subsystem Application Part (RNSAP)

RNSAP (*3GPP 25.423*) is the communication protocol used on the Iur interface between RNCs and is specified using ASN.l PER.

1.23.1 RNSAP Functions

The RNSAP protocol covers different functions as described in Table 1.14. RNSAP contains two classes of elementary procedures. The handling is the same as with NBAP.

The Iur interface RNSAP procedures are divided into four modules:

1. *RNSAP Basic Mobility procedures* – Contain procedures used to handle the mobility within UTRAN.

Table 1.14 RNSAP function overview

Function	Description
Radio Link Management	Manages radio links using dedicated resources in a DRNS
Physical Channel Reconfiguration	Reallocates the physical channel resources for a radio link
Radio Link Supervision	Reports failures and restorations of a radio link
Compressed Mode Control [FDD]	Controls the usage of compressed mode within a DRNS
Measurements on Dedicated Resources	Initiates measurements on dedicated resources in the DRNS. The function also allows the DRNC to report the result of the measurements
DL Power Drifting Correction [FDD]	Adjusts the DL power level of one or more radio links in order to avoid DL power drifting between the radio links
CCCH Signaling Transfer	Passes information between the UE and the SRNC on a CCCH controlled by the DRNS
Paging	Pages a UE in a URA or a cell in the DRNS
Common Transport Channel	Utilizes Common Transport Channel
Resources Management	Resources within the DRNS (excluding DSCH resources for FDD)
Relocation Execution	Finalizes a relocation previously prepared via other interfaces
Reporting of General Error Situations	Reports on the general error situations, for which function-specific error messages have not been defined
DL Power Time Slot Correction [TDD]	Applies an individual offset to the transmission power in each time slot according to the downlink interference level at the UE

2. *RNSAP DCH procedures* – Contain procedures that are used to handle DCHs, DSCHs, and USCHs between two RNSs. If procedures from this module are not used in a specific Iur, then the usage of DCH, DSCH, and USCH traffic between corresponding RNSs is not possible.
3. *RNSAP Common Transport Channel procedures* – Contain procedures that are used to control Common Transport Channel data streams (excluding the DSCH and USCH) over Iur interface.
4. *RNSAP Global procedures* – Contain procedures that are not related to a specific UE. The procedures in this module are in contrast to the above modules involving two peer CRNCs.

1.23.2 Example – RNSAP Procedures

Figure 1.112 shows the transport of Layer 3 information on the Iur interface, using Class 2 elementary procedures.

Figure 1.113 shows the Paging procedure, Class 2 (Example 2); and a successful Radio Link Setup procedure, using Class 1 (Example 3).

Figure 1.112 RNSAP Procedure example 1.

1.24 Radio Access Network Application Part (RANAP)

RANAP (*3GPP 25.413*) provides the signaling service between UTRAN and CN which is required to fulfill the RANAP functions. RANAP services are divided into three groups on the basis of Service Access Points (SAPs):

1. *General control services:* They are related to the whole Iu interface instance between the RNC and the logical CN domain, and are accessed in CN through the General Control SAP. They utilize connectionless signaling transport provided by the Iu signaling bearer.
2. *Notification services:* They are related to specified UEs or all UEs in a specified area, and are accessed in CN through the Notification SAP. They utilize connectionless signaling transport provided by the Iu signaling bearer.

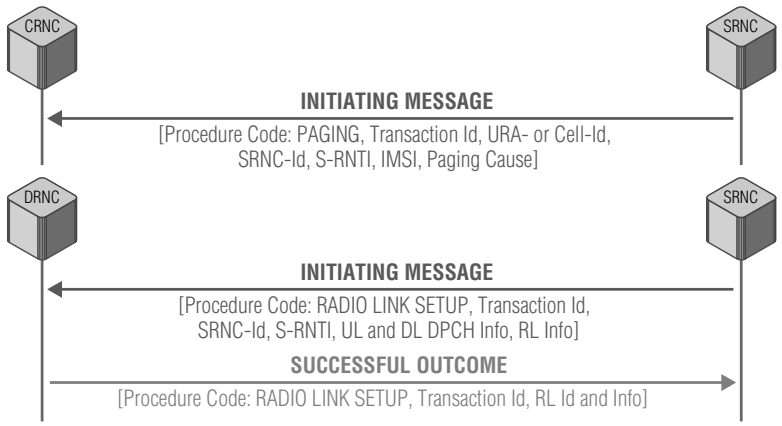


Figure 1.113 RNSAP Procedure examples 2 and 3.

3. *Dedicated control services:* They are related to one UE, and are accessed in CN through the Dedicated Control SAP. RANAP functions that provide these services are associated with Iu signaling connection that is maintained for the UE in question. The Iu signaling bearer provides connection-oriented signaling transport to realize the Iu signaling connection.

The RANAP protocol covers different functions as described in Table 1.15.

1.24.1 RANAP Elementary Procedures (EPs)

The RANAP protocol consists of EPs. An EP is a unit of interaction between the RNS and the CN; an RANAP **INITIATING MESSAGE** is transports the procedure request.

The EPs are defined separately and are intended to be used to build up complete sequences in a flexible manner. If the independence between some EPs is restricted, it is described under the relevant EP description.

Unless otherwise stated by the restrictions, the EPs may be invoked independently of each other as stand-alone procedures, which can be active in parallel.

An EP consists of an initiating message and possibly a response message. Three kinds of EPs are used:

- *Class 1:* EPs with response (success and/or failure).
- *Class 2:* EPs without response.
- *Class 3:* EPs with possibility of multiple responses.

For *Class 1* EPs, the types of responses can be as follows:
Successful (**SUCCESSFUL OUTCOME** Message)

- A signaling message explicitly indicates that the elementary procedure successfully completed with the receipt of the response.

Unsuccessful (**UNSUCCESSFUL OUTCOME** Message)

- A signaling message explicitly indicates that the EP failed.
- On time supervision expiry (for example absence of expected response).

Successful and Unsuccessful

- One signaling message reports both a successful and an unsuccessful outcome for the different included requests. The response message used is the one defined for a successful outcome.

Class 2 EPs are always considered successful. *Class 3* EPs have one or several response messages reporting both successful and unsuccessful outcomes of the requests, and temporary status information about the requests. This type of EP terminates only through response(s) or the EP timer expiry; the response is transmitted as **OUTCOME** message.

Table 1.15 RANAP function overview

Function	Description
Relocating SRNC	Changes the SRNC functionality as well as the related Iu resources (RAB(s) and Signaling connection) from one RNC to another.
Overall RAB Management	Sets up, modifies, and releases RAB
Queuing the setup of RAB	Allows placing some requested RABs into a queue and indicates the peer entity about the queuing
Requesting RAB release	Requests the release of RAB (overall RAB management is a function of the CN)
Release of all Iu connection resources	Explicitly releases all resources related to one Iu connection
Requesting the release of all Iu connection resources	Requests release of all Iu connection resources from the corresponding Iu connection (lu release is managed from the CN)
SRNS context forwarding function	Transfers SRNS context from the RNC to the CN for intersystem change in case of packet forwarding
Controlling overload in the Iu interface	Allows adjusting of the load in the Iu interface
Resetting the Iu	Resets an Iu interface
Sending the UE Common ID (permanent NAS UE identity) to the RNC	Makes the RNC aware of the UE's Common ID
Paging the user	Provides the CN for capability to page the UE
Controlling the tracing of the UE activity	Sets the trace mode for a given UE and deactivates a previously established trace
Transport of NAS information between UE and CN with two subclasses	Transport of the initial NAS signaling message from the UE to CN. This function transparently transfers the NAS information. As a consequence, the Iu signaling connection is also set up.
Transport of NAS signaling messages between UE and CN.	This function transparently transfers the NAS signaling messages on the existing Iu signaling connection. It also includes a specific service to handle signaling messages differently
Controlling the security mode in the UTRAN	Sends the security keys (ciphering and integrity protection) to the UTRAN, and sets the operation mode for security functions
Controlling location reporting	Operates the mode in which the UTRAN reports the location of the UE
Location reporting	Transfers the actual location information from RNC to the CN
Data volume reporting function	Reports unsuccessfully transmitted DL data volume over UTRAN for specific RABs
Reporting general error situations	Reports general error situations, for which function-specific error messages have not been defined

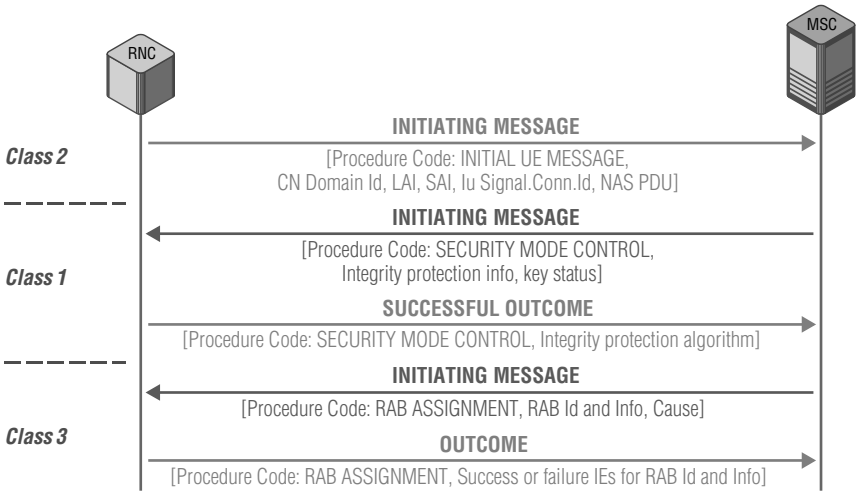


Figure 1.114 RANAP Procedure (message flow).

1.24.2 Example – RANAP Procedure

Figure 1.114 shows all types of EP classes of RANAP signaling.

1. EP: INITIAL UE MESSAGE, Class 2.
2. EP: SECURITY MODE CONTROL, Class 1, successful.
3. EP: RAB ASSIGNMENT, Class 3, with response.

1.25 ATM Adaptation Layer Type 2 – Layer 3 (AAL2L3/ALCAP)

On UMTS Iu interfaces, AAL2L3 (*ITU-T Q.2630*) represents the ALCAP function. ALCAP is a generic name for the transport signaling protocol used to set up and tear down transport bearers.

The AAL2 signaling protocol provides the signaling capability to establish, release, and maintain AAL2 point-to-point connections across a series of ATM VCCs that carry AAL2 links. The AAL2 signaling protocol also provides maintenance functions associated with the AAL2 signaling.

In the UTRAN the RNC always starts set up and release of AAL2 SVCs using AAL2L3 signaling procedures.

1.25.1 AAL2L3 Message Format

An AAL2L3 connection is identified by a pair of Destination and Originating Signaling Association IDs (Figure 1.115).

The Binding ID provided by the radio network layer is copied into the Served User Generated Reference (SUGR) parameter of ESTABLISH.request primitive. User Plane Transport bearers

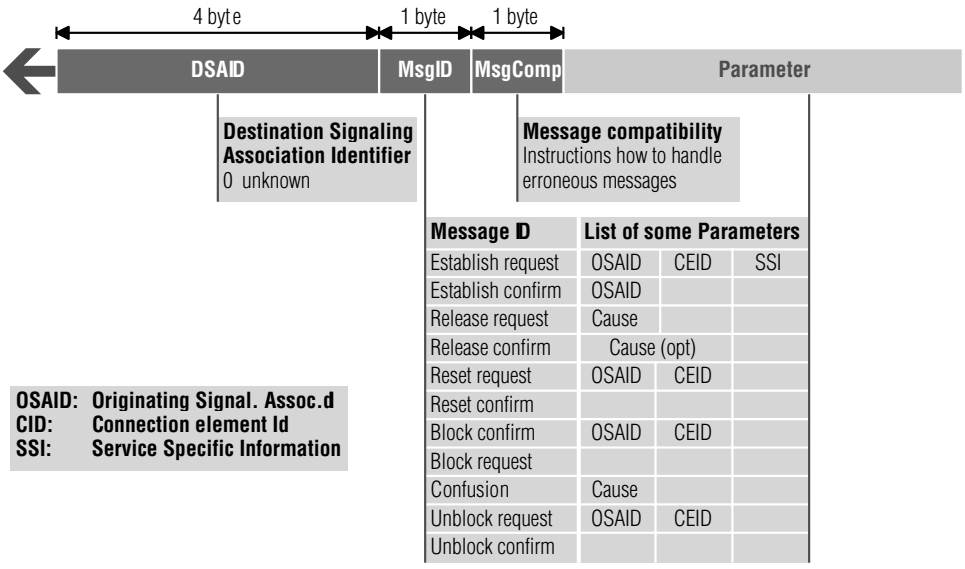


Figure 1.115 AAL2L3 message format.

for Iur interface are established and released by the AAL2L3 in the SRNC. The binding identity will already have been assigned and tied to a radio application procedure when the first AAL2L3 message was received over the Iur interface in the DRNC.

User Plane Transport bearers for Iub interface are established and released by the AAL2L3 in the CRNC. AAL2 transport layer addressing is based on embedded E.I64 or ATM End System Address (AESA) variants of the NSAP addressing format (E.191). Native E.164 addressing will not be used.

1.25.2 Example – AAL2L3 Procedure

Signaling Association Identifiers (SAIDs) are treated in the following way (Figure 1.116):

1. Whenever a new signaling association is created, a new protocol entity instance is created and an OSAID is allocated to it; this ID is then transported in the first message in the OSAID parameter. The DSAID in this message contains the value "unknown," meaning that all octets are set to "0." (In the figures, this is indicated by "DSAID = 0.")
2. Upon receipt of a message that has a DSAID field set to "unknown," a new protocol entity instance is created and an OSAID is allocated to it.
3. In the first message returned to the originator of the association, the OSAID of the sending protocol entity instance is transported in the OSAID parameter. The DSAID field carries the previously received OSAID of the originator of the association.
4. In all subsequent messages, the DSAID field carries the previously received OSAID of the destination entity.

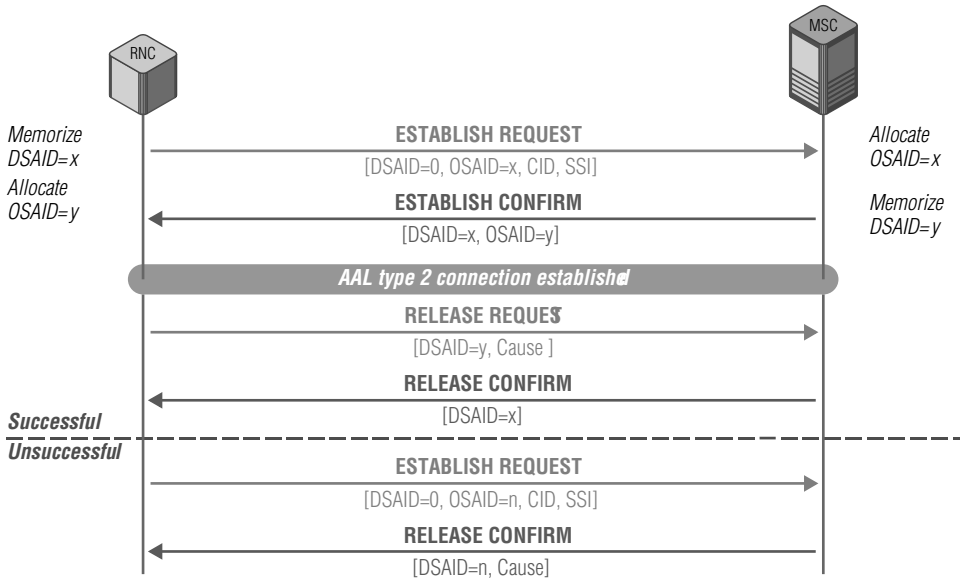


Figure 1.116 AAL2L3 establish and release example.

5. The first message returned to the originator of the association is also the last one for this signaling association (Release Confirm); no OSAID parameter is carried in the message. The SAID field carries the previously received OSAID of the originator of the association.

In order to minimize the likelihood of CID collision, the following CID allocation mechanism is used:

- If the AAL2 node owns the AAL2 path that carries the new connection, it allocates CID values from CID value 8 upwards.
- If the AAL2 node does not own the AAL2 path that carries the new connection, it allocates CID values from CID value 255 downwards.

Each AAL2 connection request (regardless of whether it comes directly from an AAL2 served user or from an adjacent AAL2 node) will contain an AAL2 service endpoint address, which indicates the destination of the intended AAL2 connection instance. This information is used to route the AAL2 connections via the AAL2 network to its destination endpoint. In capability set 1, the supported address formats are NSAP and E.I64.

It is up to the application area or the operator of a particular network to decide what addressing plan is used in the AAL2 network. The addressing plan in the AAL2 network can be a reuse of the addressing plan in the underlying ATM network, but it can also be an independent addressing plan defined exclusively for the AAL2 network.

1.26 IU User Plane Protocol

The Iu UP protocol (*3GPP 25.415*) is located in the user plane of the radio network layer over the Iu interface, the Iu UP protocol layer. It is used to convey user data associated to RABs to meet the needs of CS and PS domain user data traffic.

One Iu UP protocol instance is associated to one and only one RAB. If several RABs are established towards one given UE, then these RABs make use of several Iu UP protocol instances. These Iu UP protocol instances are established, relocated, and released together with the associated RAB.

The Iu UP protocol operates in modes. Modes of operation of the protocol are defined as:

1. *Transparent mode (TM)* – The transparent mode is intended for those RABs that do not require any particular feature from the Iu UP protocol other than transfer of user data.
   - null protocol
   - non-real-time data in plain GTP-U format
2. *Support mode for predefined SDU size (SMpSDU)* – The support modes are intended for those RABs that do require particular features from the Iu UP protocol in addition to transfer of user data.
   - rate control, time alignment
   - procedure control function, such as AMR speech data.

When operating in a support mode, the peer Iu UP protocol instances exchange Iu UP frames, whereas in transparent mode, no Iu UP frames are generated.

Determination of the Iu UP protocol instance mode of operation is a CN decision taken at RAB establishment based on, for example, the RAB characteristics. It is signaled in the radio network layer control plane at RAB assignment and at relocation for each RAB. It is internally indicated to the Iu UP protocol layer at user plane establishment. The choice of a mode is bound to the nature of the associated RAB and cannot be changed unless the RAB is changed.

1.26.1 Iu UP Transparent Mode

In this mode, the Iu UP protocol instance does not perform any Iu UP protocol information exchange with its peer over the Iu interface: no Iu frame is sent (Null protocol). The Iu UP protocol layer is crossed through by PDUs being exchanged between higher layers and the transport network layer (Figure 1.117). For instance, the transfer of GTP-U PDUs could utilize the transparent mode of the Iu UP protocol.

Note that the data is transmitted on user plane channels, which have to be established earlier on by the RANAP RAB Assignment procedure. At the end of the connection, RANAP needs to release the user plane channel again.

1.26.2 Iu UP Support Mode Data Frames

Support Mode data frames represent the Iu UP NAS Data Streams specific function (Figure 1.118). These functions are responsible for a limited manipulation of the payload and the consistency check of the frame number. If a frame loss is detected because of a gap in the sequence of the received frame numbers (for a RAB where frame numbers do not relate to time),

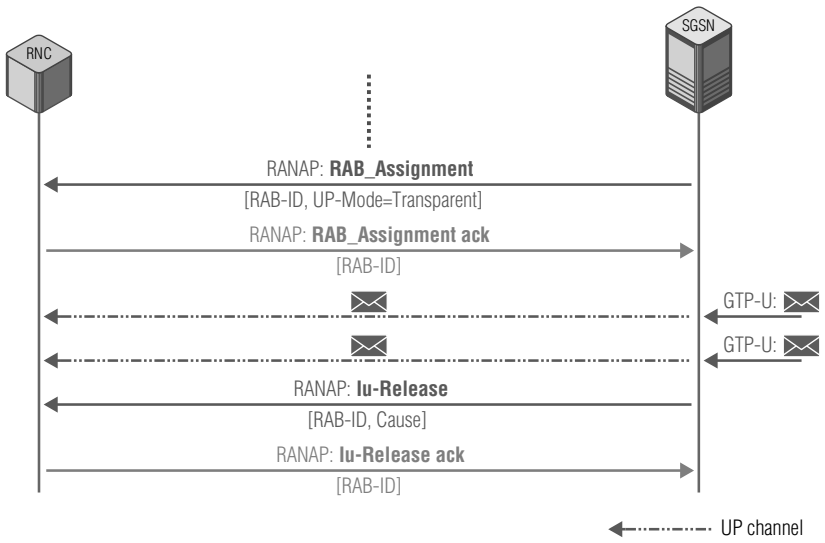


Figure 1.117 Iu UP transparent mode.

then this gap is reported to the Procedure Control function. These functions are responsible for the CRC check and calculation of the Iu UP frame payload part. These functions are also responsible for the Frame Quality Classification handling as described below.

- *PDU-Type 0* is defined to transfer user data over the Iu UP in support mode for predefined SDU sizes. An error detection scheme is provided over the Iu UP for the payload part.
- *PDU-Type 1* is defined to transfer user data over the Iu UP in support mode for predefined SDU sizes when no payload error detection scheme is necessary over the Iu UP, meaning there is no payload CRC.

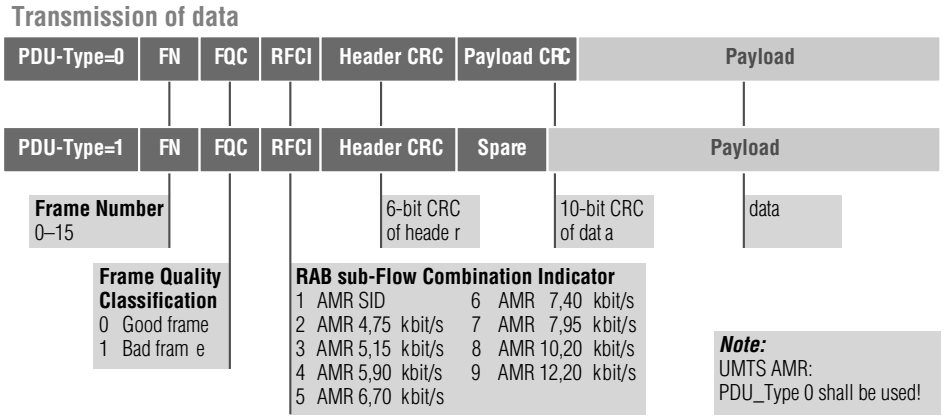


Figure 1.118 Iu UP support mode data frames.

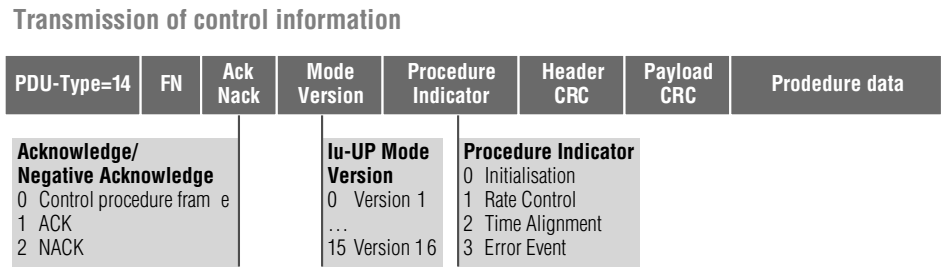


Figure 1.119 Iu UP support mode control frames.

1.26.3 Iu UP Support Mode Control Frames

A *Frame Number* handles the Iu UP frame numbering. The frame numbering can be based on either time or sent Iu UP PDU (Figure 1.119).

Frame Quality Classification is used to classify the Iu UP frames depending on whether errors have occurred in the frame or not. Frame Quality Classification is dependent on the RAB attribute *Delivery of Erroneous SDU* IE.

RAB Subflow Combination Indicator identifies the structure of the payload. This can be used to specify the sizes of the subflows. Subflows are AMR classes, meaning the maximum number of subflows is three and they correspond with AMR Class A, Class B, and Class C bits.

1.26.4 Example – Iu UP Support Mode Message Flow

The **Initialization** procedure is mandatory for RABs using the support mode for predefined SDU size. The purpose of the procedure is to configure both termination points of the Iu UP with RAB Subflow Combination Indicators (RFCIs) and associated RAB Subflows SDU sizes necessary to be supported during the transfer of user data phase. Additional parameters may also be passed, such as the Inter PDU Timing Interval (IPTI) information. The Initialization procedure is always controlled by the entity in charge of establishing the radio network layer user plane, meaning SRNC.

The Initialization procedure is invoked whenever indicated by the Iu UP Procedure Control function, for example, as a result of a relocation of SRNS or at RAB establishment over lu. The Initialization procedure will not be re-invoked for the RAB without a RAB modification requested via RANAP.

The Iu user plane data could be speech, using AMR. The data packets will be transmitted with Iu UP PDU type 0 frames.

There is no Iu UP release control frame. Instead the RANAP will release the resource (Figure 1.120).

1.27 Adaptive Multirate (AMR) Codec

The AMR codec (*3GPP 26.101*) offers a wide range of data rates and is used to lower codec rates as interference increases on the air interface. It is also used to harmonize codec standards among

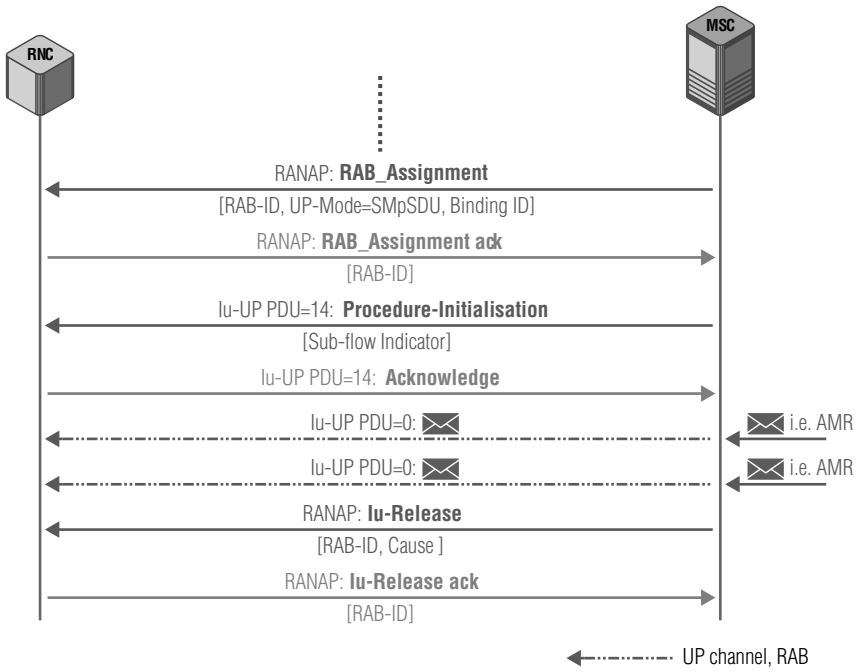


Figure 1.120 Iu UP support mode simple message flow.

different cellular systems. AMR consists of the multirate speech coder, a source-controlled rate scheme including a voice activity detector, a comfort noise generation system, and an error concealment mechanism to combat the effects of transmission errors and lost packets.

The multirate speech coder is a single integrated speech codec with eight source rates from 4.75 to 12.2 kbps, and a low rate background noise-encoding mode. The speech coder is capable of switching its bit rate every 20-ms speech frame upon command.

There are two formats of AMR frames. AMR Interface Format 1 (AMR IF1) is the generic frame format for both the speech and comfort noise frames of the AMR speech codec. AMR Interface Format 2 (AMR IF2) is useful, for example, when the AMR codec is used in connection with applicable ITU-T H-series of recommendations.

The mapping of the AMR speech codec parameters to the Iu interface specifies the frame structure of the speech data exchanged between the RNC and the Transcoder (TC) during normal operation. This mapping is independent from the radio interface in the sense that it has the same structure for both FDD and TDD modes of the UTRAN.

The RAB parameters are defined during the RANAP **RAB Assignment** procedure initiated by the CN to establish the RAB for AMR. The AMR RAB is established with one or more RAB coordinated subflows with predefined sizes and QoS parameters. In this way, each RAB subflow combination corresponds to one AMR frame type. On the Iu interface, these RAB parameters define the corresponding parameters regarding the transport of AMR frames. Some of the QoS parameters in the RAB assignment procedure are determined from the Bearer Capability Information Element used at call setup.

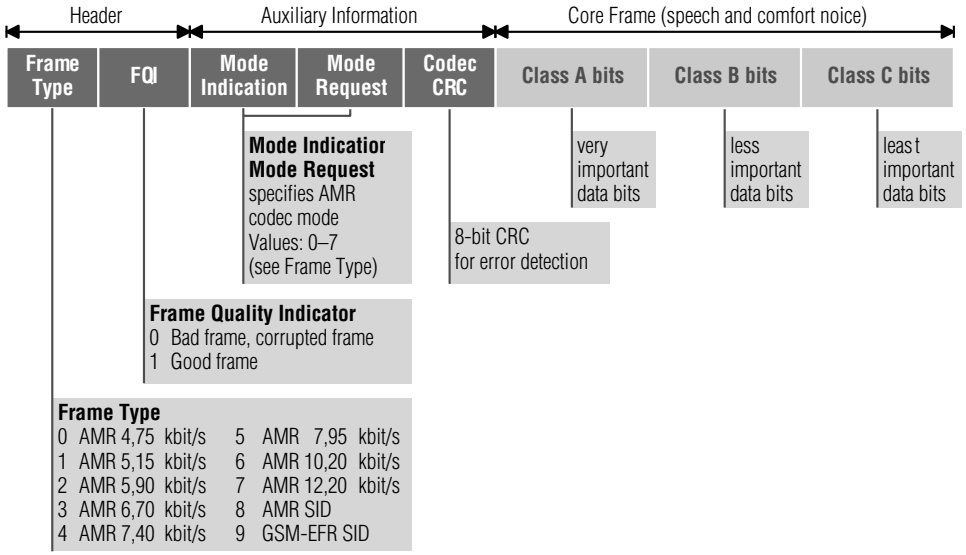


Figure 1.121 AMR IF1 frame architecture.

1.27.1 AMR IF1 Frame Architecture

The AMR IF1 frame is used in UMTS for transmission of speech information (Figure 1.121).

Frame Type will indicate the type and size of the core frame contents. Mode Indication and Mode Type are also used to specify the AMR codec mode. The Frame Quality Indicator indicates whether the data in the frame contains errors. Note that the parameter is also used in the Iu UP protocol with inverted value meaning.

The mapping of the bits between the generic AMR frames and the PDU is the same for both uplink and downlink frames.

The number of RAB subflows, their corresponding sizes, and their attributes, such as "Delivery of erroneous SDUs," are defined at the RAB establishment and are signaled in the RANAP RAB establishment request. The number of RAB subflows corresponds to the desired bit protection classes. The total number of bits in all subflows for one RFC has to correspond to the total number of a generic AMR frame format IF1, for the corresponding codec mode and frame type.

The RFCI definition is given in sequence of increasing SDU sizes. The definition describes codec type UMTS_AMR, with all eight codec modes, the Active Codec Set (ACS), and provision for Source Controlled Rate (SCR) operation.

1.28 Terminal Adaptation Function (TAF)

TAF (*3GPP 27.001,3GPP 27.002,3GPP 27.003*) is based on the principles of terminal adaptor functions presented in the ITU-T I-series of recommendations (I.460 to I.463).

The PLMN supports a wide range of voice and nonvoice services in the same network. To enable nonvoice traffic in the PLMN, there is a need to connect various kinds of terminal equipment to the MT. The main functions of the MT to support data services are:

- Ensures conformity of terminal service requests to network capability.
- Physically connects the reference points R and S.
- Controls flow of signaling and mapping of user signaling to/from GSM PLMN access signaling.
- Adapts rate of user data (see GSM 04.21) and data formatting for the transmission SAP.
- Controls flow of nontransparent user data and mapping of flow control for asynchronous data services.
- Supports data integrity between the MS and the IWF in the GSM PLMN.
- Provides end-to-end synchronization between terminals.
- Filters status information.
- Supports nontransparent bearer services, for example, termination of the RLP and the Layer 2 Relay (L2R) function including optional data compression function (where applicable).
- Checks terminal compatibility.
- Optionally supports local test loops.

1.29 Radio Link Protocol (RLP)

The RLP (*3GPP 24.022*) utilizes reliability mechanisms of the underlying protocols in order to deliver data and terminates at the MS and IWF (typically at the MSC). It has been specified for circuit-switched data transmission within the GSM and UMTS PLMN. RLP covers the Layer 2 functionality of the ISO/OSI Reference Model. RLP has been tailored to the special needs of digital radio transmission. RLP is intended for use with nontransparent data transfer. Protocol conversion may be provided for a variety of protocol configurations. Some more features of RLP:

- Nearly identical to LAPD (Link Access Procedures on the D-Channel).
- Intended for use with nontransparent data transfer.
- Foreseen data applications:
  - character-mode protocols using start-stop transmission (IA5)
  - X.25 LAP-B (Link Access Procedures on the Bearer Channel)
- Located in MT and IWF of the PLMN.
- In UMTS RLP supports the 576-bit frame length, in GSM 240-bit.
- Two modes of operation:
  - ADM (Asynchronous Disconnected Mode)
  - ABM (Asynchronous Balanced Mode).
- Three RLP versions:
  - Version 0: single-link basic version
  - Version 1: single-link extended (data compression) version
  - Version 2: multilink version (1—4 physical links).

In UMTS, the RLP frame has a fixed length of 576 bits.

A frame consists of a header, an information field, and an FCS (frame check sequence) field. The size of the components depends on the radio channel type, on the RLP version, and on the RLP frame. As a benefit of using strict alignment with underlying radio transmission, there is no need for frame delimiters (such as flags) in RLP. In consequence, there is no "bit stuffing" necessary in order to achieve code transparency.

1.30 Packet Data Convergence Protocol (PDCP)

PDCP (*3GPP 25.323*) is used to format data into a suitable structure prior to transfer over the air interface and provides its services to the NAS at the UE or the relay at the RNC. PDCP uses the services provided by the RLC sublayer. PDCP performs the following functions:

- Header compression and decompression of IP data streams (for example, TCP/IP and RTP/UDP/IP headers) at the transmitting and receiving entity, respectively. The header compression method is specific to the particular network layer, transport layer, or higher layer protocol combinations (for example, TCP/IP and RTP/UDP/IP).
- Transfer of user data (transmission of user data means that PDCP receives PDCP SDU from the NAS and forwards it to the RLC layer and vice versa).
- Maintenance of PDCP sequence numbers for radio bearers that are configured to support lossless SRNS relocation.
- Multiplexing of different RBs onto the same RLC entity.

1.30.1 PDCP PDU Format

Data using the Transparent SAP (Tr-SAP) will use the *PDCP-No-Header-PDU.* Data using the UM-SAP will use the *PDCP-Data-PDU* (Figure 1.122). Data using the AM-SAP will use the *PDCP-SeqNum-PDU.* The sequence number will allow the detection of frame loss. The *Packet Identifier* (*PID*) identifies the type of compression.

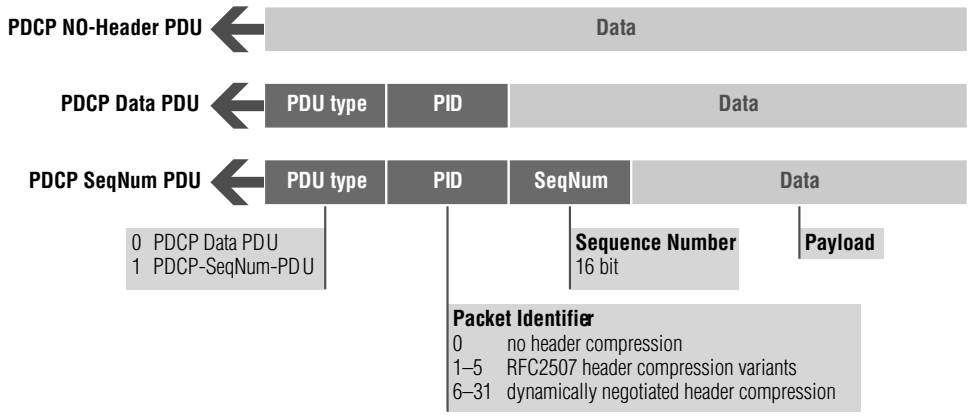


Figure 1.122 PDCP PDU format.

1.31 Broadcast/Multicast Control (BMC)

BMC (*3GPP 25.324*) adapts broadcast and multicast services on the radio interface and is a sublayer of Layer 2 that exists in the UP only. It is located above RLC. The L2/BMC sublayer is assumed to be transparent for all services except broadcast/multicast.

BMC Functions

- Storage of Cell Broadcast Messages (CBMs).
- Traffic volume monitoring and radio resource request for CBS.
- Scheduling of BMC messages.
- Transmission of BMC messages to UE.
- Delivery of CBMs to higher layer (NAS).
- Only one procedure: BMC Message Broadcast.

At the UTRAN side, the BMC sublayer consists of one BMC protocol entity per cell. Each BMC entity requires a single CTCH, which is provided by the MAC sublayer, through the RLC sublayer. The BMC requests the Unacknowledged Mode service of the RLC.

The BMC entity on the network side predicts periodically the expected amount of CBS traffic volume (CTCH transmission rate in kbps), which is needed for the transmission of CBMs and indicated to the RRC. The algorithms used for traffic volume prediction are implementation-dependent and thus do not need to be specified. Some parameters may be set by the O&M system.

The algorithms depend on the chosen algorithms for CBM scheduling. This procedure calculates the CBS schedule periods and assigns BMC messages (for example CBS Messages and Schedule Messages) to the CBS schedule periods. The procedure then gives an indication of which of the CTCH Block Sets containing part of or the complete BMC messages has the status "new."

1.31.1 BMC Architecture

It is assumed that there is a function in the RNC above BMC that resolves the geographical area information of the CB message (or, if applicable, performs evaluation of a cell list) received from the Cell Broadcast Center (CBC). A BMC protocol entity serves only those messages at BMC-SAP that are to be broadcast into a specified cell (Figure 1.123).

1.32 Circuit-Switched Mobility Management (MM)

Mobility Management is a generic term for the specific mobility functions provided by a PLMN. Such functions include, e.g., tracking a mobile as it moves around a network and ensuring that communication is maintained.

The CS-specific MM part is well known from GSM and is used quite unchanged for UMTS Rel.99 (*3GPP 24.008*).

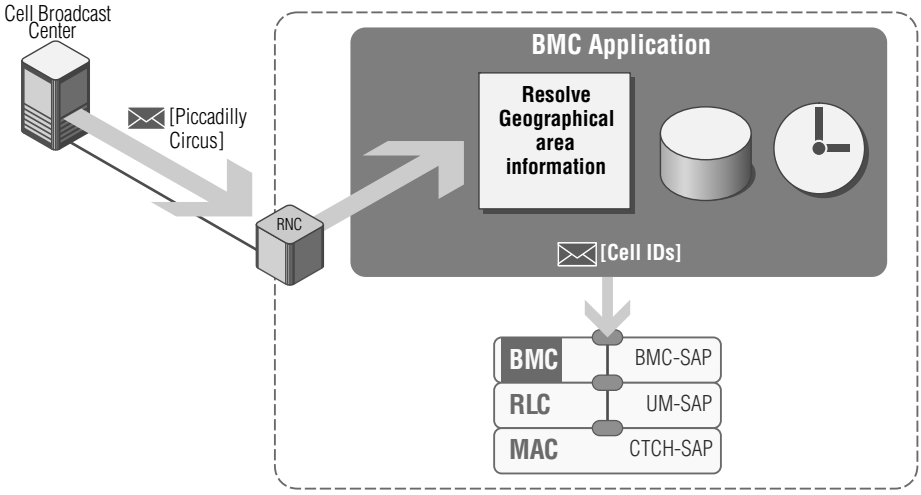


Figure 1.123 BMC architecture.

MM Functions

- MM procedures to establish and release connections.
- Transfer of CM sublayer messages.
- MM common procedures for security functions, for example, the Authentication procedure.
- MM-specific procedures for location functions such as periodic location updating or IMSI attach procedure.
- UE identified by IMSI or TMSI.

MM procedures are used to set up the connection between UE and the CS CN. Procedures like Authentication and Location Update are also part of CS MM. A CS CN will recognize a UE by the IMSI or by a previously assigned TMSI.

1.33 Circuit-Switched Call Control (CC)

The Circuit-Switched Call Control (CC) protocol includes some basic procedures for mobile CC (no transport control!):

- Call establishment procedures.
- Call clearing procedures.
- Call information phase procedures.
- Miscellaneous procedures.

CC entities are described as communicating finite state machines that exchange messages across radio interfaces and communicate internally with other protocol (sub)layers.

The Circuit-Switched Call Control protocol part has only slightly changed from GSM to UMTS Rel.99 (*3GPP 24.008*). Parameters for QoS (for example, the RAB specification) have been added to the signaling protocol.

CC Functions

- Procedures similar to GSM.
- CC establishes and releases CC connections between UE and CN.
- Activation of voice/multimedia codec:
  – based on 3G-324M, variant of H.324 (see *3GPP 26.111*).
- Interworking with RANAP for establishment of a RAB:
  – CC Setup QoS will be mapped onto RANAP RAB assignment.

1.34 Example – Mobile Originated Call (Circuit Switched)

As shown in Figure 1.124, the procedure is identical to GSM from the MM and CC point of view. However, the ciphering is not performed by the CN in the same way as known from GSM. Instead, the other main protocol of the IuCS interface, the RANAP, is in charge of all types of RAB signaling.

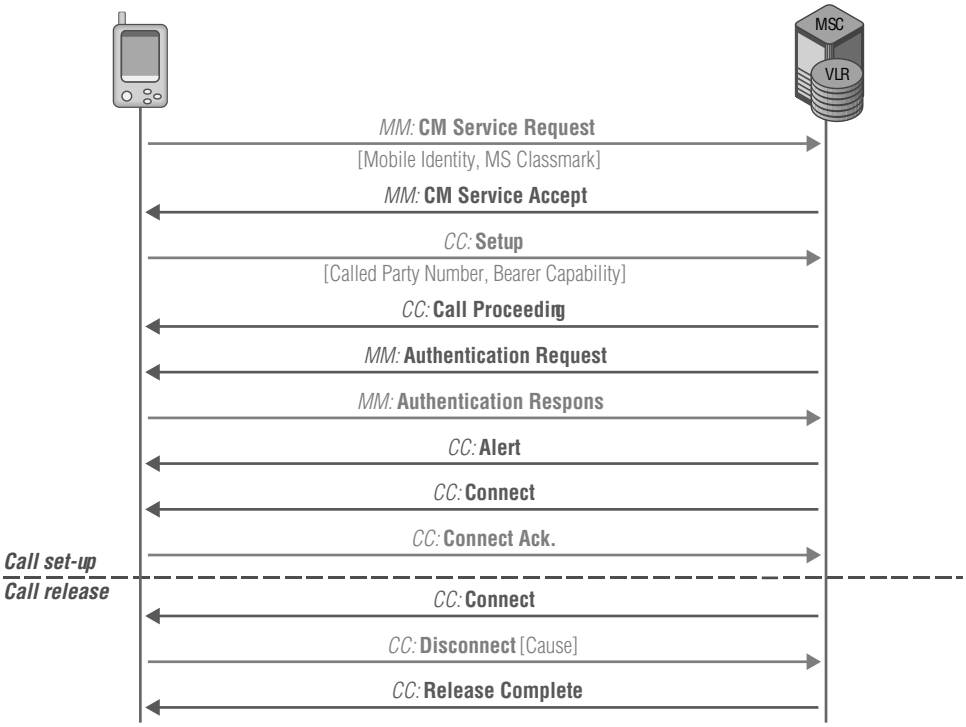


Figure 1.124 Mobile Originated Call (message flow).

The initial UE message, in this example the **CM Service Request**, will transport the UE Identity, whereas the CC **Setup** message will contain the dialed telephone number. All given messages will run on top of RANAP, which will run on top of SCCP protocol. The SCCP is responsible for defining the UE procedure connection.

1.35 Packet-Switched Mobility Management (GMM)

The **GPRS Mobility Management** protocol (*3GPP 24.008*) is used to make a UE known to the packet-switched CN and to follow its mobility. The procedures have changed only by a message, which is used as the initial UE message when connecting UE with the packet network, Session Management Activate PDP Context. This new message is the Service Request message and is used to set up a secure connection with the ability to define a QoS for the signaling information between UE and SGSN.

GMM Functions

- Procedures similar to GPRS (GMM).
- GMM protocol makes use of a signaling connection between UE and SGSN.
- GMM establishes and releases GMM contexts, for example, GPRS Attach.
- GMM-specific procedures for location functions like periodic RA updating.
- New message implemented to provide service to CM sublayer on top of GMM:
  - Service Request message
  - initiated by UE, used to establish a secure connection to the network and to request the bearer establishment for sending data
- UE identified by IMSI or P-TMSI.

1.36 Packet-Switched Session Management (SM)

The GPRS Session Management protocol (*3GPP 24.008*) is similar to the CS CC and is used to define the connection of a UE to a packet network. SM exists in the UE and in the SGSN and handles PDP Context Activation, Modification, Deactivation, and Preservation Functions. The GPRS SM protocol is used between UE and SGSN whereas the SGSN acts as relay function toward the GGSN.

SM Functions

- Procedures similar to GPRS (SM).
- Counterpart to CS CC protocol, meaning SM protocol is used to establish and release packet data sessions.
- SM procedures to set up and release one or more PDP Contexts.
- PDP Contexts are handled in UE and GGSN.
- SGSN represents IWF.

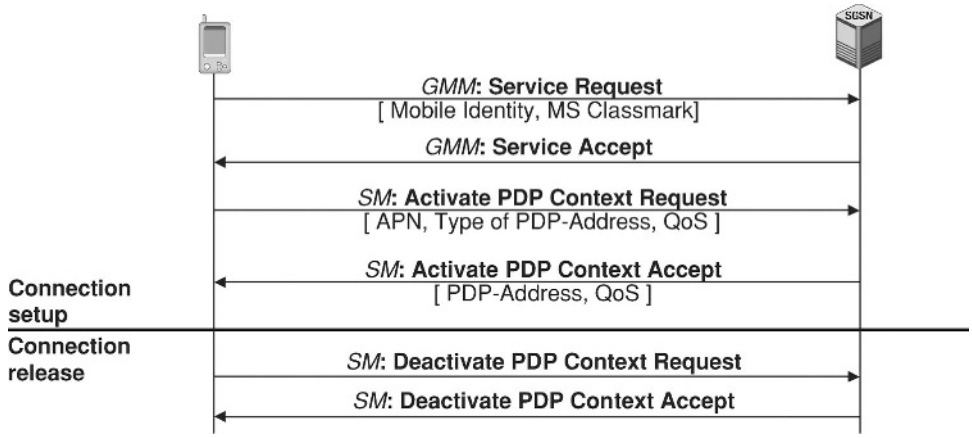


Figure 1.125 Activate PD Context (message flow).

1.37 Example – Activate PDP Context (Packet Switched)

Figure 1.125 shows the "new" signaling flow for activating and deactivating the PDP Context on the IuPS interface.

As mentioned earlier, the **GMM Service Request** and **Service Accept** are new to PS CN. The Service Request will contain the UE identity and the MS Classmark to define a QoS and an RB for the signaling. The Activate PDP Context message will contain the QoS parameter for the UP RB.