UMTS Networks

Nach Folien von Dr. Christian Gayda, Dr. Cornelia Kappler
Siemens AG
Vortrag: Sebastian Fudickar, Uni Potsdam
Netzwerktechnologien Basistechnologien

1

Course Overview

- Motivation
- Standardization issues
- UMTS architecture basics
- UE, UTRA, UTRAN, PS Domain
- Basic functionalities:
  - Accessing the network
  - Transferring data
  - Detaching from the network
  - Information storage
- Mobility
- QoS
- Security and charging
- IMS
- Example signaling flows
- Business considerations
- UMTS - what comes next?

Course UMTS Networks 2

Functionality overview

- Accessing the network
  - Finding the access point
  - Localizing UE
  - Establishing connectivity for signaling
  - Registration
    - Authentication and authorization *(-> security)*
  - Establishing connectivity for data transfer
    - Admission control *(-> QoS)*
  - Paging *(-> Mobility)*
- Transferring data
  - Routing
  - Encapsulating and tunneling
  - Address translation
  - Ciphering and encryption *(-> security)*
  - Compression
  - *Charging*
  - Resource management *(-> QoS)*
- *Mobility Handling*
- Detaching from the network

Course UMTS Networks 3

Accessing the network - Finding the access point I

Upon being switched on the UE…

- …scans all possible frequencies (time slots), in order to find elegible cells
  - elegible = UMTS technologie, e.g. UTRA FDD
- …synchronizes, and finds scrambling code
  - As described in lecture on UTRA
  - Now it is able to receive cell-specific broadcast information
    - Sent by RNC on BCCH

Accessing the network - Finding the access point II

- …prioritizes PLMNs (if more than one is available)
  - PLMN „Public Land Mobile Network“ mobile telecommunication network under the control of a single operator
  - PLMN identified by MCC-MNC Mobile Country Code - Mobile Network Code
  - UE prioritizes PLMNs according to a preference list stored on the USIM
    - Always prefer „home PLMN“
    - Availability of better PLMN is checked on a regular basis
  - PLMN identity broadcasted on special channel (P-CCPCH)
    - in regular intervals

Accessing the network - Finding the access point III

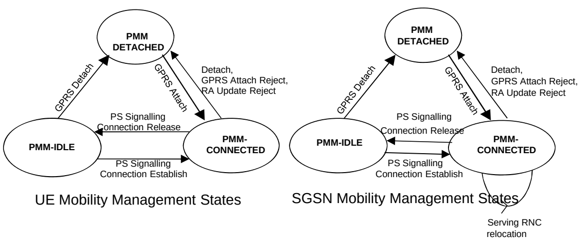
- …looks for suitable cells
  - Suitable = acceptable radio conditions
    - Signal to noise ratio is above threshold both uplink and downlink
- …finally picks cell
  - Listens on the BCCH for general cell configuration information, e.g. *localization*

Accessing the network - Localization of the UE II

- Identification of Localization
  - LAI - Location Area Identity = MCC + MNC + LA Code
  - RAI - Routing Area Identity = LAI + RA Code
  - URA Identity
  - CGI - Cell Global Identity = LAI + cell identity
- Globally unique identifiers

Accessing the network – Registration I

- Registration in PS Domain is called *UMTS GPRS Attach*
- Registration changes the *Mobilty Management State* (MM State) of UE at UE and SGSN
  - From PMM-Detached to PMM-Connected
- Mobility Management State Model:



Accessing the network – Registration II

- UE registers with SGSN, using
  - GMM / RANAP protocol between UE and SGSN
  - MAP protocol between SGSN and HLR
- Sequence of events
  - UE sends SGSN identity and location information (IMSI, IMEI, RAI)
  - SGSN checks identity with information obtained from HLR (-> *authentication*)
  - UE and SGSN activate *encryption*
  - SGSN ensures that equipment is not stolen with EIR
  - SGSN informs HLR is handling this UE and in return receives information on what services this user is allowed to use (-> *authorization*)
  - SGSN informs user if request has been granted and assigns temporary ID: P-TMSI (Packet Temporary subscriber identity)
    - For security reasons TMSI is only used for registration

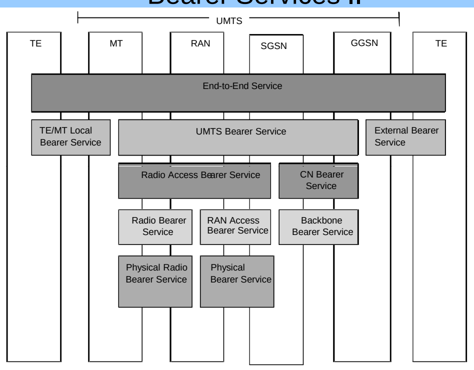
Accessing the network – Registration III

- GPRS attach is denied by SGSN when
  - Identity of user could not be confirmed
  - Equipment or USIM are listed as stolen
    - This USIM is henceforth listed as forbidden in TE,
      - No other GPRS attach will be initiated with this USIM
  - No roaming agreement between this PLMN and home PLMN, or user not allowed to switch PLMNs
    - This PLMN is henceforth listed as „forbidden“ in USIM
  - ...

Establishing connectivity for data transfer Bearer Services I

- In order to send or receive data, a so-called *Bearer Service* needs to be set-up
- A Bearer Service
  - is offered by one service layer to the upper layer
  - extends across a well-defined domain
    - E.g. UMTS Bearer Service from UE to GGSN
  - offers data transport, mobility and QoS
  - to do so may use services of lower-layer Bearers

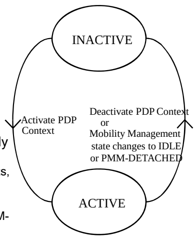
Establishing connectivity for data transfer Bearer Services II



Establishing connectivity for data transfer
PDP context activation I

- I.e. for the UE to use a service (send or receive data), it needs to signal for UMTS Bearer Service establishment
  - The UMTS Bearer is specific to the service used
  - This is called *PDP context activation*
    - PDP - Packet Data Protocol
  - A PDP context is characterized by
    - Beginning: PDP address of UE
    - End: Terminating GGSN
    - QoS specific to service
  - UE is assigned a dynamic PDP address, unless static PDP address exists
    - This is an IPv4 or IPv6 address
  - Terminating GGSN depends on end-point of session; UE must name APN (Access Point Name)
    - Is it a session internal to this PLMN?
    - Is an external network addressed? Which one?
  - UE can establish more than one PDP context simultaneously („*secondary PDP context*")
    - When UE uses two applications with different QoS requirements, it would establish two PDP contexts
  - Changes PDP state from Inactive to Active
    - Only possible if mobility management state is PMM-idle or PMM-Connected
      - PMM-IDLE then must change to PMM-CONNECTED

PDP State Model:



Course UMTS Networks 13

Information Storage

- UE maintains
  - Mobility Management State
  - PDP State
- SGSN maintains for each UE attached
  - Mobility Management State
  - PDP State
- GGSN maintains for each PDP context
  - PDP State
- HLR maintains
  - Static user subscription data

Cf. 23.060 Sec. 13

Course UMTS Networks 14

Summary – Basic Functionalities

- Accessing the network
  - Finding the access point
  - Localizing UE
    - Hierarchical organization of localization information
      - LA, RA, URA; cell
  - Establishing connectivity for signaling: RRC Connection Set-up
  - Registration: GPRS attach
  - Establishing connectivity for data transfer: PDP context activation
    - PDP context characterized by PDP address, APN and QoS
- Transferring Data
  - Each packet assigned to a PDP context
- Detaching from network
  - PDP context deactivation, GPRS detach, RRC Connection release
- UMTS end-to-end services are organized into layered Bearer services
- UE is always in one of three Mobility Management States
  - PMM-detached - PMM-idle - PMM connected
- UE is always in one of two PDP states
  - Active or inactive

Course UMTS Networks 15

Course Overview

- Motivation
- Standardization issues
- UMTS architecture basics
- UE, UTRA, UTRAN, PS Domain
- Basic functionalities:
  - Accessing the network
  - Transferring data
  - Detaching from the network
  - Information storage
- Mobility
- QoS
- Security and charging
- IMS
- Example signaling flows
- Business considerations
- UMTS - what comes next?

Role of QoS in UMTS I

- UMTS shall deliver multimedia services via the PS-domain
  - video conferencing,
  - voice
  - "rich voice"
  - web browsing
  - ...
- Each service has different requirements regarding
  - bandwidth
  - delay
  - delay variance (jitter)
  - ...
- Typically,
  real-time services have stringent requirements,
  non-realtime services have lax requirements
- In other words, each service requires different Quality of Service (QoS)

Role of QoS in UMTS II

- On UTRA, adequate QoS can be guaranteed by assigning common or shared channels
- In parts of UTRAN and in PS domain use IP protocol
- IP networks originally were not designed to deliver QoS
  - all packets are treated equal
  - no resources are reserved for particular applications / users

  => can deliver satisfactory real-time services only in low-load conditions

  => IP QoS technology needs to be applied to guarantee QoS in UMTS

IP QoS technology – How to?

- In order to support QoS, the following is needed:
  - QoS requirements of a session must be made known to all network elements delivering QoS, end-to-end:

    Protocol for QoS Signaling
  - QoS must be realized.
    e.g. by reserving resources in all network elements:

    Resource Provisioning Technique

  Both standardized by IETF
  - QoS needs to be managed and controlled

  Framework for UMTS QoS specified by 3GPP

IP QoS technology – Resource Provisioning I

- Overprovisioning
  - Provide sufficient resources to handle any traffic
  - Can be combined with admission control at the ingress
  - Probabilistic QoS guarantee
  - No signaling needed (except may be to ingress routers)
- DiffServ
  RFC 2475 "An Architecture for Differentiated Service"
  - prioritization of particular flows via Code Points (DSCP) in IP header
    - e.g. real-time packets are always handled first
  - should be used together with admission control
  - because packet paths are unknown, results in probabilistic QoS guarantees
  - resource requirements should be signaled to nodes performing admission control (ingress routers)

IP QoS technology – Resource Provisioning II

- IntServ
  RFC 1633 "Integrated Services in the Internet Architecture: an Overview"
- reservation of resources in each node along data path
    - results in guaranteed QoS
    - not scalable
  - resource requirements (QoS) must be signaled to each node
- MPLS
  RFC 3031 "Multiprotocol Label Switching Architecture"
  - reservation of paths (LSPs) with guaranteed resources possible
    - as in IntServ, results in guaranteed QoS
    - uses extension of RSVP for setting up paths
  - as in DiffServ, resource requirements should be signaled to ingress routers

IP QoS technology – QoS Signaling protocols

Today, no generally accepted solution exists:

- RSVP and its extensions
  RFC 2205 "Resource ReSerVation Protocol (RSVP)"
  - only QoS signaling protocol supported to any extent in commercial routers
  - powerful all-purpose QoS signaling protocol
    - for IntServ, extension for MPLS
    - for Admission Control
  - RSVP can do almost everything, but this implies overhead for most (simple) uses
  - travels hop-by-hop on transport layer
  - interpreted by each router on the data-path
- Signaling of DiffServ packet priority with DSCPs in IP Header
- can also use SIP (RFC 2543 "SIP: Session Initiation Protocol")
  - for negotiating sessions (codec, ports,...) between end-hosts on application layer
  - extended to exchange QoS parameters between end-hosts
  - may be picked up by dedicated intermediate nodes ("SIP proxies")
- In the NSIS Working Group, the IETF is currently working on a new transport-layer QoS signaling protocol
  http://www.ietf.org/html.charters/nsis-charter.html

QoS in UMTS

- Detailed Requirements on QoS
  - QoS Classes, Parameters, Values
- End-to-End QoS scenarios
  - signaling and resource provisioning
- QoS management functions defined for UMTS

Detailed QoS requirements: QoS Classes, Parameters, Values I

- UMTS QoS is offered by the UMTS Bearer Service
- 4 QoS classes are defined:
  - conversational class (e.g. voice, video conferencing)
  - streaming class (e.g. video streaming)
  - interactive class (e.g. Web browsing, gaming)
  - background class (e.g. Background email download)
- These classes are characterized by e.g.:
  - Guaranteed / max. Bit rate
  - max packet size
  - transfer delay
  - traffic handling priority

End-to-End QoS Scenarios I: Basics

- End-to-End QoS needs QoS signaling:
  - all network elements need be informed about the QoS that is to be provided
  - QoS signaling e.g. via
    - SIP
    - RSVP
    - DSCPs (DiffServ Code Points; limited information)
    - PDP context
- End-to-End QoS needs QoS provisioning via e.g.
    - Overprovisioning
    - DiffServ
    - IntServ
    - MPLS
- Signaling and provisioning mechanisms don't need be the same in all network segments
  - interworking possible

End-to-End QoS Scenarios II: Basics

- 5 end-to-end QoS signaling scenarios are described in Release 5
  - all scenarios with PDP context / DiffServ interworking
  - 2 scenarios with additional RSVP signaling
  - App. layer signaling via SIP
    - this is a UMTS specific SIP dialect with additional functionality compared to IETF SIP
- Not much in standard about QoS provisioning (because no interworking necessary)

What is necessary beyond the standard presented so far? I

- Not everything is standardized by 3GPP.
  - Only standardize what is necessary for interworking
  - In order to allow differentiation between equipment providers and operators
  - Because time did not permit
    - may be done in later Releases
  - Because IP does not provide a solution yet
- issues left open by the standard must be solved by equipment providers and operators

What is necessary beyond the standard presented so far? II

- Equipment providers deduce UMTS product specification from
  - 3GPP Standard
  - own work on open issues
- Factors influencing product specification
  - who are the customers?
    - „incumbent" or „greenfield"? (incumbent operator already owns network)
      - „incumbents" likely to be more conservative
      - already own equipment that needs to be integrated
    - what kind of networks do they operate?
  - continuous product „evolution" important
    - as opposed to completely new design for each release
      - too expensive for all parties involved

Course UMTS Networks 28

Summary – QoS in UMTS

- In order for UMTS to deliver multimedia services via the PS domain, QoS, particulary IP QoS, needs to be supported
- 4 QoS classes are offered by the UMTS Bearer Service
  - conversational, streaming, interactive, background
- QoS support includes
  - QoS signaling
    - RSVP, DSCPs, SIP, (nsis), PDP context
    - 5 scenarios for end-to-end QoS signaling are described by 3GPP
      - however they are not guaranteed to work
  - resource provisioning technique
    - overprovisioning, DiffServ, IntServ, MPLS
    - not prescribed by 3GPP
  - QoS management and control
    - 3GPP specifies
      - user plane: classification, conditioning, scheduling, queuing
      - control plane: admission control, subscription control, translation
    - 3GPP does not specify
      - resource management

Course UMTS Networks 29

Course Overview

- Motivation
- Standardization issues
- UMTS architecture basics
- UE, UTRA, UTRAN, PS Domain
- Basic functionalities:
  - Accessing the network
  - Transferring data
  - Detaching from the network
  - Information storage
- **Mobility**
- QoS
- Security and charging
- IMS
- Example signaling flows
- Business considerations
- UMTS - what comes next?

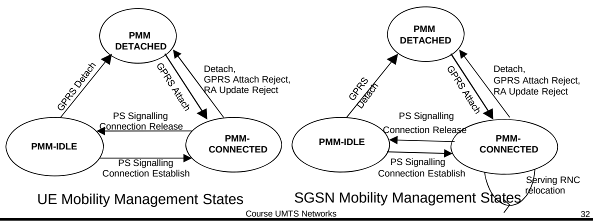
Course UMTS Networks 30

Mobility consequences

- In any network (IP, UMTS, GSM,...), mobility of the terminal requires extra functionality
  - terminal location needs to be registered
  - when moving from one cell to a neighboring cell, a handover needs to be performed
    - detect necessity
    - detect new access point
    - transfer user context?
      - incl. authentication and authorization credentials, QoS information
    - remove /loose connectivity on old path
    - establish connectivity on new path
      - update routing
      - establish QoS
  - paging support
- *Seamless handover* (= user doesn't notice) as desired in UMTS needs even more functionality
  - *fast* and *without loss of data*
  - "make before break" is desireable
    - establish connectivity along new path before handover takes place

Reminder: Mobility Management States

- In PMM Detached state, UE location is unknown
- In PMM Connected state, UE informs SRNC and SGSN about location with cell or URA granularity. The Serving RNC controls handover. SGSN knows Serving RNC
  - UE can be paged
- In PMM Idle state, UE location known at SGSN with Routing Area granularity.UE keeps network informed.
  - UE can be paged

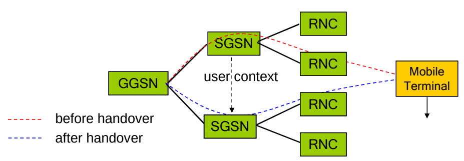


UE Mobility Management States SGSN Mobility Management States

Mobility in PMM-Idle Mode I

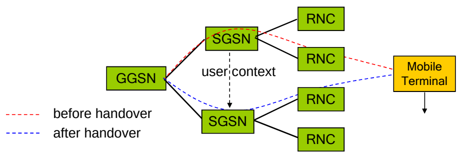
UE must perform location update with SGSN:

- in regular intervals to prevent time-out
  - when timed out, UE is moved to PMM-detached
    - guards against "lost UEs"
- when Routing Area changes
  - UE detects Routing Area change by listening to RAI broadcast
  - UE sends a Routing Area Update Request to SGSN serving new Routing Area using GMM protocol



Mobility in PMM-Idle Mode II

- if Routing Area change entails an SGSN change, new SGSN obtains user context from old SGSN
  - identify old SGSN from old RAI
  - SRNC is changed such that new SRNC is connected to SGSN
    - » User context is transferred between SGSNs, such as IMSI, P-TMSI, Charging Information

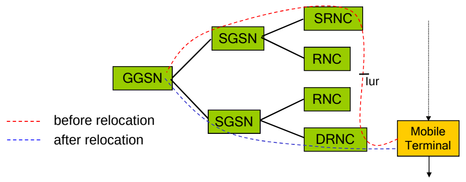


Mobility in PMM-Connected Mode

- Location control by UE
  - UE tracks cells / URAs and updates them with SRNC
  - UE tracks Routing Area and updates them with SGSN
    - when SGSN changes, same steps as in PMM-Idle mode, plus
      - PDP context information is transferred between SGSNs
      - PDP context is torn down on old path and set up on new path
  - updating in regular intervals or upon cell / URA /Routing Area change
- Handover controlled by SRNC
  - Soft handover
  - Softer handover
  - Hard handover

SRNC relocation

- Because of Soft Handover, the SRNC can in principle be maintained for the duration of the connection
- Sometimes it is desireable to change the SRNC in order to optimize routing
- (Old) SRNC instructs a DRNC to become (new) SRNC
  - may entail change of SGSN
- Algorithm for triggering (old) SRNC to perform relocation not specified in standard
- SRNC relocation timing independent of (soft) handover timing



Paging

- For a mobile-terminated session, the UE is paged, i.e. searched
  - when in PMM-idle mode UE is searched in the Routing Area
  - when in PMM-connected mode, paging request is directly sent to UE using existing signaling conection
  - by paging, the UE is requested to set up an additonal PDP context for the incoming session

Summary – UMTS Mobility

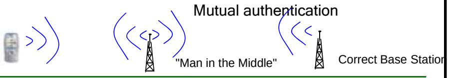
- mobility of the terminal requires extra functionality
  - terminal location needs to be tracked
  - when moving from one cell to a neighboring cell, a handover needs to be performed
  - seamless handover implies fast handover without packet loss
  - paging support
- The IETF is in the process of specifying support for seamless IP mobility
  - not clear yet how it will collaborate
- UMTS is specified to offer seamless mobility
  - in PMM-idle mode, Routing Area is tracked
  - in PMM-connected mode, cell or URA is tracked
  - Macrodiversity allows Soft Handover

Course Overview

- Motivation
- Standardization issues
- UMTS architecture basics
- UE, UTRA, UTRAN, PS Domain
- Basic functionalities:
  - Accessing the network
  - Transferring data
  - Detaching from the network
  - Information storage
- Mobility
- QoS
- Security
- Charging
- IMS
- Example signaling flows
- Business considerations
- UMTS - what comes next?

Security Threats and Counter Measures

Threat	Attack (how to realize a threat)	Counter Measures
Theft of service	Identity spoofing Session hijacking Repudiation Replay of messages	Temporary identities Integrity Protection Authentication and authorization Time-variant parameterization of messages
Denial of service	Unlimited state-setup Flooding with messages that need to be processed (Injection, replay and modification of messages)	Soft state Mutual authentication Integrity protection Authorization Low computational overhead
Eavesdropping of - User identity - Location - Data packet content	"Man-in-the-middle attack"	Encryption Mutual authentication



What is...

- ...*Authentication* of entity A to entity B:
  - B is assured the entity it is talking to is indeed A
- ...*Authorization* of entity A to use a service S
  - A is allowed to use S
  - usually A is authenticated first
- ...*Integrity protection* of a message between A and B
  - B can ascertain the message sent by A was not changed
- ...*Encryption* of a message between A and B
  - nobody except A and B can decipher the message
- ...(symmetric) *Security key*
  - a secret shared between two entities A and B
  - Authentication, Authorization, Integrity, Encryption etc all build on the security keys.

Basics of secure communication I

- For establishing a secure communication channel between entities A and B:
  - they need to share a secret (private keys)
    - manual configuration
    - obtain from trusted third party
  - A and B (mutually) authenticate e.g.
    - (password - unsecure and not mutual)
    - challenge-response calculated based on shared secret
  - messages exchanged between A and B are encrypted
    - calculated based on shared secret
  - messages exchanged between A and B are integrity protected
    - checksum calculated based on shared secret and appended to message

Basics of secure communication II

- An alternative to secret keys are public keys, however they are more expensive to use
- Authentication Challenge, Encrypted message and Integrity Checksum are calculated with *Cryptographic functions*
  - always takes as input secret key
  - easy to calculate, but difficult to back-engineer (invert)
  - cannot determine secret key even from a large number of input-output pairs
- Secure communication between whom?
  - End-hosts?
  - Hop-by-hop?

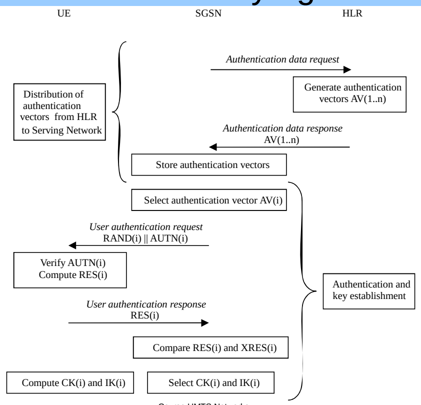
UMTS security overview

- UMTS security evolved from GSM security
  - GSM security satisfied its design goal
  - however more threats are accounted for
- additional features:
  - longer secret key
  - protection against Theft of Service, Denial of Service and Eavesdropping due to malicious nodes / Man-in-the-middle:
    - mutual authentication between user and network
    - Mutual key freshness assurance / replay protection by sequence numbers
  - encryption extended up to RNC
    - accounting for e.g. microwave links between Node Bs and RNC
  - mandatory integrity protection of signaling messages
    - between UE and RNC
    - integrity protection of all messages is too expensive
  - integrity protection and encryption in PS-domain
    - based on IPSEC (IETF specification)

Authentication and key agreement I

- Shared secret between USIM and AuC is Master Key (128 bits)
  - Master Key never transferred elsewhere
    - User doesn't know Master Key
  - usage of Master Key minimized
    - derive temporary keys from master key to protect bulk of data
- Serving Network authenticates user by challenge-response
  - however Serving Network receives all authentication information from Home Network
    - Trust in Serving Network minimized
- User checks implicitly whether Serving Network is authorized by Home Network

Authentication and key agreement IV



Course UMTS Networks 46

Lawful interception

- In many countries, authorities must be able to monitor and eavesdrop user traffic
  - IMSI, IMEI, PDP address, location, SMS content, packet content
- limits security level offered by network

Course UMTS Networks 47

Summary – Security in UMTS

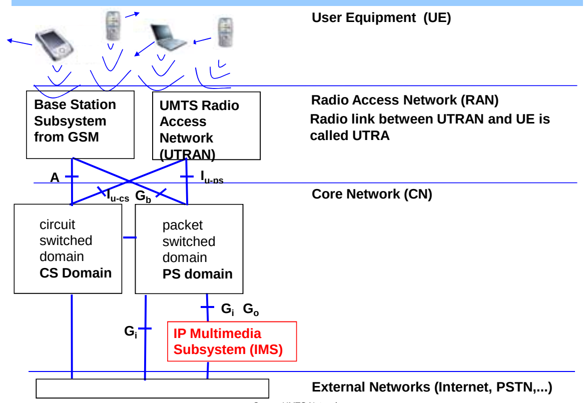
- Security threats:
  - Theft of Service, Denial of Service, Eavesdropping
- Threats are countered by
  - Authentication, authorization, integrity protection, encryption
  - counter measures based on security keys
- UMTS extends GSM security by
  - Mutual authentication
  - Encryption up to RNC
  - Integrity protection of signaling messages

Course UMTS Networks 48

Course Overview

- Motivation
- Standardization issues
- UMTS architecture basics
- UE, UTRA, UTRAN, PS Domain
- Basic functionalities:
  - Accessing the network
  - Transferring data
  - Detaching from the network
  - Information storage
- Mobility
- QoS
- Security
- Charging
- IMS
- Example signaling flows
- Business considerations
- UMTS - what comes next?

What is the IMS – where is it?

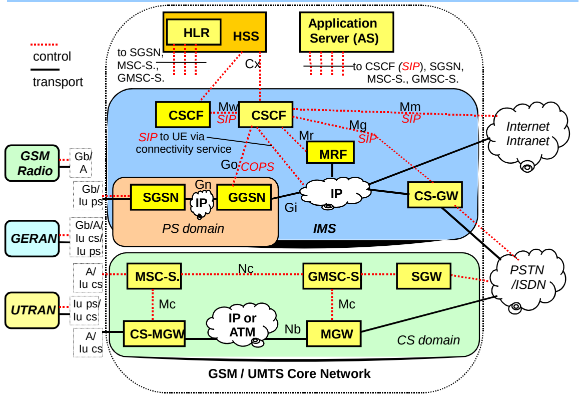


What is the IMS?

- The IMS enables the provisioning of
  - Multimedia services
  - Location based services
    - Details not standardized yet
- Such services can also be offered without IMS, however…
  - The IMS provides a standardized, convenient and commercially viable way for offering them
    - IMS does not define or standardize the services themselves
- The IMS can (in principle) be operated by a "third party", i.e. operator of PS-domain and IMS can be different
- The IMS was introduced in Release 5 (i.e. 2002)
  - R4 and R99 do not offer UMTS-intrinsic services
- Interfaces and protocols conform as far as possible with IETF Specifications
  - In order to achieve smooth interoperation with IP-based terminals across the Internet
- The IMS uses the RAN & PS-domain (called "IP connectivity access network (IPCAN))
  - for transport of user and signaling traffic
  - for taking care of mobility

=>IMS can be deployed without a CS-domain

IMS Architecture I



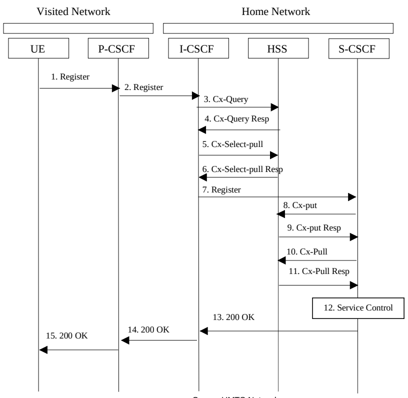
IMS Architecture II

- CSCF - Call State Control Functions
  - Controls and polices IMS services
  - first contact point of a mobile node setting up a *multimedia* session
    - Note this „session“ goes beyond a PS-domain session (PDP-context)
    - Using a „dialect“ of SIP (Session Initiation Protocol, RFC 3261)
  - Can act in three different roles
    - Proxy CSCF (P-CSCF)
    - Interogating CSCF (I-CSCF)
    - Serving CSCF (S-CSCF)
- MRF - Multimedia Resource Function
  - Consisting of two logical nodes
    - Controller on signaling path
    - Processor on data path
  - Provides e.g. multimedia conferencing, transcoding,...

IMS Architecture III

- CS-GW - Gateway to Circuit Switched Networks
  - consisting of several separate entities not shown in detail
  - supports a direct connection to PSTN / ISDN from packet domain
    - allows connecting IP-based voice calls to „normal“ phones
    - Involves transcoding of data and protocol conversion
- HSS - Home Subscriber Server
  - = HLR plus IMS functionality
- AS - Application Server
  - Offers IM services
  - Resides either in home network or 3rd party location
    - Other' operators IMS
    - Stand-alone location

Session Control – Registration of UE II



Unless otherwise indicated (e.g. Cx), these are SIP messages

When the user is in the Home Network, the same signaling flow applies. The P-CSCF is then located in the Home Network

Summary – UMTS IMS

- IMS offers Session Control for multimedia services and (in principle) for location-based services
  - IMS does not define services
- Network elements handling Session Control are CSCFs
  - P-CSCF, I-CSCF, S-CSCF
- User data is kept in the HSS (IMS extension of HLR)
- Services are offered by Application Servers (AS)
- Session Control involves
  - UE (de)registration
  - session set-up, modification, tear-down
    - Locating other users (independent of device they are using)
    - During session set-up end-points agree on session characteristics
      - Media types, codecs, ports
- Session Control is signaled with SIP
- The QoS signaled at IMS session set-up and resources reserved for the actual session are checked to be in agreement using Service Based Local Policy (SBLP)

Course Overview

- Motivation
- Standardization issues
- UMTS architecture basics
- UE, UTRA, UTRAN, PS Domain
- Basic functionalities
- Mobility
- QoS
- Security and charging
- IMS
- Example signaling flows
- Business considerations
- UMTS - what comes next?

Why standardization?

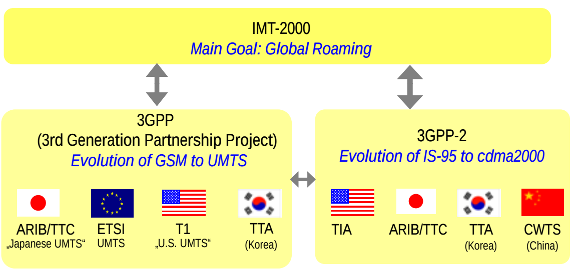
- standardization important because interworking is necessary:
  - Applications across the network
  - Equipment produced by different companies
  - Networks of different operators
- ☑ hence it is not a good idea for everybody to develop their own protocols / architectures
- ☑ Network Experts sit together
  - ☑ develop and standardize the technology simultaneously

Why standardization?

- What needs to be standardized? the "Essential What":
  - basic architecture
  - functionality of essential network elements
  - protocols and protocol stacks
  - interfaces
  - information storage
  - Everything else related to interworking
- What needs not be standardized? the "How" and everything not essential:
  - internal operation of network elements
  - intradomain solutions not related to core functionality
    - e.g. intra-domain resource management
  - ...
- Equipment vendors / operators have to come up with own solution for things not standardized

Standardization bodies

- ITU defined concept for IMT-2000
  - IMT-2000 is a *family* of compatible systems
  - for standardization of terrestial networks, two groups were formed



UMTS Standardization in 3GPP

- www.3gpp.org
- each company nominates delegates to represent them (nobody else may participate)
- standardization process:
  - standardized is what all delegates agree upon
  - delegates pursue company interests
- standardization proceeds via mailing lists and meetings at least 6 times a year
- standardization topics are pursued with timely termination as a guiding principle
  - lots of money is involved
- (almost) each year, a new Release of the UMTS standard is published
  - UTMS is evolving
  - First UMTS Release is "R99", subsequently numbered Rel4, Rel5,...
  - Rel5 is about to be closed
- Specifications publicly available (GSM Specs weren't)

Course UMTS Networks 61

3GPP organisation of technical bodies

TSG -
Technical Study Group

Course UMTS Networks 62

Standardization Bodies: IETF

- IP Technology is being standardized by IETF

  IETF - Internet Engineering Task Force
  - loose organization of „independent“ engineers and researchers
  - e.g. IP, TCP, SIP, IntServ, MPLS etc. are all by IETF
- Philosophies of 3GPP and IETF are very different

Course UMTS Networks 63

IP Technology Standardization in the IETF

- www.ietf.org
- everybody may participate in IETF standardization
  - influence on standard based on technical knowledge, reputation and availability.
    Employer - in principle - unimportant.
- Standardization according to the IETF motto:
  "We believe in running code and rough consensus"
  - only what has been implemented can be standardized
- standardization proceeds via mailing lists and meetings 3 times a year
- standardization topics pursued depend on the interest of the people involved
- Each topic is assigned to a dedicated Working Group (WG)
- All documents publicly available

3GPP - IETF interworking

- 3GPP and IETF are based on very different principles
  - 3GPP defines an entire system (-> cathedral)
  - IETF works one-protocol-at-a-time (-> bazaar)
- However, as Telecommunications and Internet converge, they need to collaborate
  - currently 3GPP needs collaboration from IETF more than vice-versa
    - e.g. SIP standardization
  - but IETF doesn't produce standards „on request"
  - 3GPP can't wait for standards that are produced „if people are interested and find a solution they are happy with"
- increasingly the same persons are active in both organizations
  - collaboration can be expected to improve

How to find a 3GPP specification

- standardization ideas are presented to a TSG in writing as "Technical Documents" (Tdocs)
- Tdocs agreed upon are published as "Technical Specification" (TS)
- Numbering Scheme:
  - TS topic.xxx, release.b.c
    e.g. 23.060-6.1.0
    "General Packet Radio Service (GPRS) Service description; Stage 2" version 1.0 for Release 6
- can be retrieved from http://www.3gpp.org/specs/specs.htm
- you need to know what you are looking for...

Topic	TS number
Requirements	21.xxx
Service Aspects ("stage 1")	22.xxx
Technical Realization (Stage 2")	23.xxx
Signaling ("stage 3") (user equipment to network)	24.xxx
Radio Aspects	25.xxx
CODECs	26.xxx
Data	27.xxx
Signaling ("stage 3") (Radio Access to Core network)	28.xxx
Signaling ("stage 3") (to fixed networks)	29.xxx
Programme Management	30.xxx
User Identity Management	31.xxx
Operation & Maintainance	32.xxx
Security Aspects	33.xxx
Test Specifications	34.xxx
Security Algorithms	35.xxx

How to read a 3GPP Specification

- TSs are a collaboration of very many (unnamed) authors.
  - Often, some content is not finalized, unless the Release is closed
  - Tdocs sometimes concern new ideas, sometimes only wording
    - per meeting, 100s of Tdocs may be discussed, whether they should be included in the corresponding TS
  - Many TSs assume terminology knowledge, or implicitly build on other TSs
    - sometimes poorly referenced
- TS aim at defining the entire system "top -down"
- TS Structure
  - Spec number and version, Date, Title
  - Keywords, Table of Contents
  - Scope, References, Abbreviations
  - Actual Content

How to find a IETF specification

- standardization ideas are presented to the community in writing as “Internet Drafts”
- Internet Drafts agreed upon by the community pass a "board review", then are published as “Request for Comment” (RFC)
- RFCs are numbered chronologically
  - most recent is RFC 3645
- retrieve from
  - http://www.ietf.org/rfc.html (RFCs)
  - http://search.ietf.org/ (Internet Drafts)
- Find out RFC number from RFC Index http://www.ietf.org/iesg/1rfc_index.txt
- Find Internet Drafts via keyword search (above address)

How to read a IETF specification

- RFCs have a small number of authors
  - others may contribute, by arranging with the authors
  - Internet Drafts are mainly discussed on mailing lists
- RFCs are written by engineers for engineers
  - pragmatic approach "bottom-up"
- RFCs, once published, are never changed
  - may be superseded (obsoleted) by new RFCs
- RFC Structure (slight variations possible depending on authors)
  - RFC Number, Date, Authors, Title
  - Abstract, Table of Contents (sometimes)
  - actual content
  - References

Summary - Standardization

- Standardization is important for all aspects requiring interworking
  - other aspects are not standardized
- ITU defined a concept for 3G systems, IMT-2000
  - standardization for terrestial networks was handed to
    - 3GPP (UMTS)
    - 3GPP2 (cdma2000)
- 3GPP standardization often draws upon work by IETF
- Both, 3GPP and IETF specifications are publicly available

Course Overview

- Motivation
- Standardization issues
- UMTS architecture basics
- UE, UTRA, UTRAN, PS Domain
- Basic functionalities:
  - Accessing the network
  - Transferring data
  - Detaching from the network
  - Information storage
- Mobility
- QoS
- Security
- Charging
- IMS
- Example signaling flows
- UMTS Evolution: from R99 to Rel6
- Beyond UMTS

UMTS Releases Overview

- (almost) each year, a new Release of the UMTS standard is published
  - UTMS is evolving
  - first UMTS Release is "R99“, finalized in 2000 (not 1999)
  - subsequently numbered Rel4, Rel5,...
  - Rel6 is about to be closed

GSM -> GPRS -> UMTS R99 -> UMTS Rel4 I

- GSM
  - CS domain
  - GSM RAN
    - initially < 10kb/s, evolved to today (EDGE) 384 kb/s
- GPRS
  - adds PS Domain, in parallel to CS Domain
  - Initially higher transmission rates than GSM (max 115 kb/s)
    - can also be used with EDGE
  - Shared radio channel (DSCH)
    => more efficient usage of radio resources,
    because bandwidth demands of e.g. web traffic are highly fluctuating
    (user needs time to read page) and bursty
  - allows a direct connection to e.g. the Internet
  - charging per data volume possible
    - in GSM always charging per time unit

GSM -> GPRS -> UMTS R99 -> UMTS Rel4 II

- UMTS R99
  - GSM RAN replaced by UTRAN
    - W-CDMA
    - Higher bandwidth
      - Up to 2Mb/s
    - Functionality differently distributed compared to GSM RAN
  - Support for QoS classes
- UMTS Rel4
  - Separation of Transport and Control in CS domain
  - CS Domain may also be IP-based

Rel5 Features

- IMS
- Layer 2 between RNC and GGSN not necessarily ATM-based
- Flexible RANs
  - May attach GSM RAN and GERAN to PS domain (see next slide)
    - GERAN = GSM EDGE Radio Access Network
  - The proper term to refer to a system including GERAN and GSM RAN is „3GPP network“ rather than „UMTS network“
    - UMTS network implies UTRAN
- Iu Flex
  - Breaking hierarchical mapping of RNCs to SGSNs (MSCs)
- HDSPA (High Speed Downlink Packet Access)
  - New Shared Channel on downlink
  - Up to 16 Mb/s

Rel6 Features – Overview I

- Network Sharing
  - Allow cost efficient sharing of network resources
    - Scenario 1: Multiple core networks sharing common radio access network (already in R99)
    - Scenario 2: Geographically split networks sharing
    - Scenario 3: Common Network Sharing
    - Scenario 4: Common spectrum network sharing
    - Scenario 5: Multiple radio access networks sharing common core network
- WLAN interworking
  - use WLAN as access network for IMS instead of PS Domain
- MIMO
  - Multiple antennas in UE and Node B / spacial multiplexing
- and many more…

Rel6 Features – Overview II

- Services
  - MBMS
    - Multimedia Broadcast and Multicast Service
      - Downstream broadcasting and multicasting support
      - Shares resources when transmitting data
  - Push Service
    - Pushing of information from network to UE
    - Support via
      - Push information using SMS
      - Network-initiated PDP context activation
        - » Need to change 23.060
        - » Need mapping of „user ID" onto IMSI
      - IMS / SIP
        - » Query CSCF to find users IP address
        - » Contact user with SIP INVITE
  - IMS Group Management
    - Setting up and maintaining user groups
    - Supporting service for other services
      - Multiparty conferencing
      - Push-to-talk
      - Etc.
  - IMS Presence Service
    - User defined visibility to others
    - User can find out presence of others

Rel6 Features – Overview III

- Services cont'.
  - IMS Messaging
    - SIP-based messaging
    - Instant messaging, „Chat room", and deferred messaging (equivalent to MMS)
    - Interworks with Presence Service to determine whether addressee available
  - Multiparty-multimedia conferencing service in IMS
    - utilizing MRF
  - Push-to-talk
    - Multicast of speech to predetermined list of parties („CB Funk")
    - „Half duplex": only one person can speak at a time
      - Whoever pushes the button first
    - No dialing necessary, just „push"
      - Uses „always-on" functionality
    - Already possible with GPRS (in 2004)
    - With IMS support presumably more efficient
      - Relying on other IMS services, e.g. group management, multiparty conferencing
  - Location-based services in IMS
    - UE indicates it wishes to use local service. S-CSCF routes request back to visited network
    - Mechanism for UE to retrieve / receive information about locally available services

Summary – UMTS Evolution

- UMTS R99 (compared to GPRS)
  - GSM RAN replaced by UTRAN
  - Support for QoS classes
- UMTS Rel4
  - No major changes to packet-based part
- UMTS Rel5
  - IMS
  - HDSPA
  - Iu Flex
- UMTS Rel6
  - WLAN Interworking
  - Numerous services are being defined

Course Overview

- Motivation
- Standardization issues
- UMTS architecture basics
- UE, UTRA, UTRAN, PS Domain
- Basic functionalities:
  - Accessing the network
  - Transferring data
  - Detaching from the network
  - Information storage
- Mobility
- QoS
- Security
- Charging
- IMS
- Example signaling flows
- UMTS Evolution: from R99 to Rel6
- Beyond UMTS

Current Definition of 4G I
Generations of mobile communication systems

	1st Generation (1G)	2nd Generation (2G)	3rd Generation (3G)	Beyond 3G (4G)
Timeframe	50s - mid 90s	90s - 2020?	2001 - ...?	in 10 to 15 years?
Technology	NMT, AMPS,...	GSM (worldwide), IS-95 (Americas, Asia), PDC (Japan),...	IMT 2000 , e.g. UMTS, CDMA2000	?
Standards	proprietary, domestic	A number of international standards	one accessible standard	One accessible standard ?
Bandwidth		Initially < 10kbps, evolves to 384 kbps	up to 2 Mbps	Yet more
A/D	Analogue radio, digital network	Digital	Digital	Digital
CS/PS	Circuit switched	Circuit switched	Circuit and packet switched	All-IP
Cell radius	Up to 150 km	kilometers	Meters to kms	Meters to kms?
Mobility	Basic (national scope)	Advanced (continental scope)	Global (within same technology)	Global, intertechnology
Services	Speech	Speech, some data (MMS, SMS, WAP)	Speech, data, multimedia	Speech, data, multimedia, all Internet services

Current Definition of 4G II

- There is not yet a universally agreed-upon definition of 4G
  - for some 3G + WLAN access is already 4G
  - for some bandwidth > 2Mb/s is already 4G
  - ...
- When will 4G be available?
  - (depending on definition)
    may be 2010 or earlier...or later…

Current Definition of 4G III

- Often cited features of 4G include
  - Lower cost/bit (than 3G)
  - Bandwidth on air interface up to 1 Gb/s (aggregated peak cell rate)
    - "translate desktop experience to mobile world"
  - “All-IP”
  - Transparent seamless integration of heterogeneous access technologies
    - Any fixed access and RAN technology (UTRAN, WLAN, Bluetooth,...)
      - integrated by means of IP-layer
    - IP-based core network
  - reconfigurable multi-mode multiband terminals
    - terminals can be adapted to local RAN technology by downloading appropriate software (SDR - Software Defined Radio)
  - smooth evolution path from 3G / integration of 3G

Current Definition of 4G IV

- Often cited features of 4G include cont'.
  - empowerment of user to act as service provider
    - movement away from provider-centric paradigm towards a decentralized
      peer-to-peer paradigm
    - intelligence moves towards the center of the network
  - "Ambient Intelligence"
    - multitude of embedded, networked devices in the environment ("ubiquitous computing")
      - sensors, controls, "natural" user interfaces
    - they interact with the person and personalize the surroundings
      - learning and adaptive environment
      - location-aware, context-aware, person-aware
      - raises interesting security issues
        - » what information is spread and stored where
        - » user needs to stay in control ("off-button" must exist)
      - e.g. "milk-ordering fridge", "perfect toast", "always the same favorite meal"...
  - Service integration

Current Definition of 4G V

- Often cited features of 4G include cont'.
  - integration of a multitude of interacting devices
    - moving networks
      - a network moves as a whole, thereby changing its point of attachment
      - e.g. passengers using train networks as access network
    - Ad-hoc networks
      - wireless devices communicating without infrastructure
      - all nodes can act as routers
      - e.g.
        - » PANs (Personal Area Networks)
        - » BANs (Body Area Networks)
        - » WSNs (Wireless Sensor Networks)
        - » vehicular networks
  - ad-hoc autoconfiguring networks
    - ad-hoc network formation for specific, possibly short-lived tasks with involving variable network elements and devices
    - interwoven networks
      - devices may belong to several (logical) networks at once
      - e.g. a laptop belongs to a PAN and to a moving network

Current Definition of 4G VI

- Technology issues
  - what spectrum?
    - is there any left?
    - Spectrum sharing
  - new radio technologies
  - seamless mobility
  - autoconfiguration
  - distributed management
  - security
  - Intelligent Agent technology
  - speech / gesture recognition
  - Artificial Intelligence
  - ...

Current 4G Activities

- "Ambient Intelligence" Scenarios defined by EU ISTAG (IST Advisory Group)
  - http://www.cordis.lu/ist/istag.htm
- Vision of the future wireless world ("Book of Visions") by WWRF (Wireless World Research Forum)
  - www.wireless-world-research.org/
  - founded in 2001
  - over 150 members from industry and academia
- EU 6th Framework IST Programme funds large-scale 4G research project
  - WWRF initiated a group of research projects funded in this programme (e.g. "Ambient Networks", "Winner",..)
- Several industry-funded 4G research institutes
- many more activities...

Summary – Beyond UMTS

- The definition of what is 4G is not stable yet
- A number of 4G features are being discussed
- Worldwide research on 4G has started

Accumulated Abbreviations I

1G, 2G, 3G	1st Generation,...3rd Generation
3GPP	3rd Generation Partnership Project, produces UMTS standard
3GPP2	3rd Generation Partnership Project 2, produces cdma2000 standard
APN	Access Point Name, address of network to which a PDP context is to be established
AS	Application Server, in IMS
AuC	Authentication Center
AV	Authentication Vector
B3G	Beyond 3rd Generation
BCCH	Broadcast Control Channel, one of the logical radio channels
BCH	Broadcast Channel, one of the transport radio channels
BMC	Broadcast and Multicast Control, Layer 2 protocol on Uu
BSC	Base Station Controller, controlling node in GSM RAN
BTS	Base Station Transceiver, network element, incl antenna in GSM RAN
CCCH	Common Control Channel, one of the logical radio channels
CDMA	Code Division Multiple Access; each user (application) uses different "code" on the radio interface
cdmaOne	One of the 2nd Generation Systems, mainly used in Americas and Korea, uses CDMA
cdma2000	member of the IMT-2000 family for 3G, successor of cdmaOne
CGI	Cell Global Identifier, unique identifier of cell
CK	Cipher Key used for encryption between UE and RNC
CN	Core Network; in UMTS consisting of CS Domain, PS Domain and IMS
CTCH	Common Transport Channels, one of the logical radio channels
CPICH	Common Pilot Channel, one of the physical radio channels
CSCF	Call State Control Function, network element in IMS
CS Domain	Circuit-switched Domain, one of the UMTS functional groups
DCCH	Dedicated Control Channel, one of the logical radio channels
DCH	Dedicated Channel, one of the transport radio channels
DPICH	Dedicated Pilot Channel, one of the physical radio channels
DRNC	Drift RNC, used in Macrodiversity
DSCH	Downlink Shared Channel, one of the transport radio channels
DSCP	DiffServ Code Point (IETF), priority marking of packet carried in IP header
DTCH	Dedicated Transport Channels, one of the logical radio channels

Accumulated Abbreviations II

EDGE	Enhanced Data Rates for GSM Evolution, high bandwidth radio interface for GSM
EIR	Equipment Identity Register
FDD	Frequency Divsion Duplex; uplink and downlink use different frequencies on the radio interface
FDMA	Frequency Division Multiple Access; each user (application) uses different frequency on the radio
GERAN	GSM EDGE Radio Network
GGSN	Gateway GPRS Support Node, network element in the PS domain
GMM	GPRS Mobility Management
GMSC	Gateway MSC, network element in CS Domain, gateway to external networks
GPRS	General Packet Radio Service, 2.5 Generation system
GSM	Global System for Mobile Communications, European 2G System
GSN	Term to refer to both GGSN and/or SGSN
GTP-C	GPRS Tunneling Protocol for the cotnrol plane between RNC and GGSN
GTP-U	GPRS Tunneling Protocol for the user plane. Realizes PDP context between RNC and GGSN
Go	Reference Point between P-CSCF and GGSN
HLR	Home Location Register, main subscriber database in GSM and GPRS
HDSPA	High Speed Downlink Packet Access, higher data rate downlink channel for UMTS
HSCSD	High Speed Circuit Switched Data, higher data rate for GSM
HSS	Home Subscriber Server = HLR plus IMS functionality
I-CSCF	Interrogating CSCF, one role of the Call State Control Function in the IMS
ID	Internet Draft, working document of the IETF, becomes RFC when generally accepted
IETF	Internet Engineering Task Force, responsible for Internet Standardization
IK	Integrity Key, for integrity protection of signaling messages.
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem, one of the UMTS functional groups
IMSI	International Mobile Station Identity
IMT-2000	International Mobile Telecommunications at 2000 MHz, 3G concept by ITU

Accumulated Abbreviations III

IPCAN	IP Connectivity Access Network for IMS, e.g. RAN & PS-domain
IS-95	= cdmaOne, one of the 2nd Generation Systems
ISIM	IMS SIM
ITU	International Telecommunication Union,
Iu	Reference Point between CN and RNC
Iub	Reference Point between RNC and Node B
Iur	Reference Point between RNCs
L1, L2,..	OSI Layer 1, Layer 2...
LA	Location Area, for localizing UE in CS domain
LAI	Location Area Identity, unique ID for identifying a location area
MBMS	Multimedia Broadcast and Multicast Service
MCC	Mobile Country Code, one constituent of PLMN identity and IMSI
MGW	Media Gateway Function
MGFC	Media Gateway Control Function
MM	Mobility Management
MNC	Mobile Network Code, one constituent of PLMN identity and IMSI
MPLS	Multiprotocol Label Switching (IETF), IP Traffic Engineering and QoS technology
MRF	Multimedia Resource Function
MS	Mobile Station (term used in GSM and GPRS)
MSC	Mobile Switching Center, network element in CS Domain
MSIN	Mobile Station Identification Number, part of IMSI
MT	Mobile Termination, part of UE
NSAPI	Network Service Access Point Name, PDP context identifier at UE

Accumulated Abbreviations IV

PCCH	Paging Control Channel, one of the logical radio channels
P-CCPCH	Primary Common Control Physical Channel, one of the physical radio channels
P-CSCF	Proxy CSCF, one role of the Call State Control Function in the IMS
PDCP	Packet Data Control Protocol, L2 protocol on Uu
PDP	Packet Data Protocol (e.g. IP)
PLMN	Public Land Mobile Network - mobile telecommunication network under the control of a single operator
P-SCH	Primary Synchronization Channel, one of the physical radio channels
PS Domain	Packet-switched Domain, one of the UMTS functional groups
PSTN	Public Switched Telephone Network
P-TMSI	Temporary Mobile Station Identity, used in PS Domain
QoS	Quality of Service
QPSK	Quaternary Phase Shift Keying, Modulation Technique used in UMTS
R99	UMTS Release 1999
RA	Routing Area, for localizing UE in PS domain
RAB	Radio Access Bearer, Bearer extending from
RAI	Routing Area Identity, unique ID for identifying a routing area
RAN	Radio Access Network, Bearer extending from MT to SGSN
RANAP	RAN Application Protocol
Rel4, Rel5..	UMTS Release 4,..
RFC	"Request For Comment", Specification by IETF
RLC	Radio Link Control Layer, L2 Protocol on Uu
RNC	Radio Network Controller
RNS	Radio Network Subsystem
RSVP	Resource Reservation Protocol, transport-layer QoS signaling protocol (IETF)
RRC	Radio Resource Control, protocol on L3 for control plane of Uu interface

Accumulated Abbreviations V

SBLC	Service Based Local Policy, procedure for coordinating QoS authorization in IMS and PS domain
S-CSCF	Serving CSCF, one role of the Call State Control Function in the IMS
SDMA	Space Division Multiple Access
SDP	Session Description Protocol, carried in SIP, encodes the actual session description
SIM	Subscriber Identity Module, part of mobile terminal in GSM
SIP	Session Initiation Protocol (IETF)
SGSN	Serving GPRS Support Node, in PS domain
SGW	Signaling Gateway Function, Node in IMS
SM	Session Management
SRNC	Serving RNC
TDD	Time Division Duplex; uplink and downlink use different time slots on the radio interface
TDMA	Time Division Multiple Access; each user (application) uses different time slot on the radio
TE	Terminal Equipment, part of UE
TEID	Tunnel Endpoint Identifier, identifies PDP context in network
TFT	Traffic Flow Template, describes how packets belonging to a given PDP context can be identified
TMSI	Temporary Mobile Station Identity, used in CS Domain
TRAU	Transcoding and Rate Adaptation Unit
TS	Technical Specification, Standard by 3GPP
Uu	Reference Point between UE and UTRAN
UE	User Equipment (term used in UMTS)
UMTS	Universal Mobile Terrestial System, member of the IMT-2000 family for 3G, successor of GSM
URA	UTRAN Registration Area, for localizing UE in PS domain
USIM	Universal Subscriber Identity Module, part of UE
UTRA	UMTS Radio Access; Radio link between UTRAN and UE
UTRAN	UMTS Radio Access Network
VLR	Visited Location Register, network element in GSM and GPRS, stores user data in visited network