Cellular Protocols for Mobile Internet

GPRS, EDGE, UMTS, HSPA demystified

Harald Welte <laforge@gnumonks.org>

gnumonks.org
OpenBSC
OsmocomBB
hmw-consulting.de
sysmocom GmbH

28C3, December 2011, Berlin/Germany

Outline

1. Evolution of cellular networks
2. GSM / GPRS / EDGE
3. UMTS / HSDPA / HSUPA

About the speaker

- Using + playing with Linux since 1994
- Kernel / bootloader / driver / firmware development since 1999
- IT security expert, focus on network protocol security
- Former core developer of Linux packet filter netfilter/iptables
- Board-level Electrical Engineering
- Always looking for interesting protocols (RFID, DECT, GSM)
- OpenEXZ, OpenPCD, Openmoko, OpenBSC, OsmocomBB, OsmoSGSN

GSM / CSD

- GSM is the first digital cellular system, developed in 1980ies, first deployment 1990
- GSM is a pure circuit-switched technology, like POTS/ISDN in the land-line world
- GSM offers CSD (circuit switched data) to provide similar service as analog modems in land-line telephone network
- CSD offers data rates 2400 / 4800 / 9600 / 14400 bps
- CSD still supported by a number of operators today

GSM / HSCSD

- HSCSD is High-Speed CSD
- HSCSD bundles up to four GSM time-slots to achieve 38.4/57.6kbps data speeds
- very expensive in terms of network load (1 data session occupies 4 to 8 times the bandwidth of a phone call)
- was popular for a very short time only, dead by now

GPRS

- GPRS (General Packet Radio Servie) specified in 1990ies, first deployed 1999
- A separate, independent network to GSM, using same modulation/channeling and time-slot structure
- Introduces lots of GPRS-specific equipment (CCU, PCU, SGSN, GGSN) to the network
- packet-switched, not circuit switched
- net band-width for IP around 56 to 114 kbits/sec
- available virtually anywhere on the world except Japan/Korea

EDGE

- Enhanced Data-rates for GSM evolution, EGPRS and ECSD
- Actually, most people mean only EGPRS when they say EDGE
- uses same channel/bandwidth/TDMA as GPRS
- physical layer uses 8PSK modulation instead of GMSK
- no real changes to any higher protocol layers
- most phones support EGPRS up to 236 kbits/sec
- available virtually anywhere on the world except Japan/Korea

UMTS

- UMTS (Universal Mobile Telephony Syststem) developed in 1996-1999
- First commercial deployments 2002
- 384 kbits/sec downlink, 128 kbits/sec uplink
- entirely new system, not an evolution/extensions of GSM/GPRS/EDGE
- Wideband CDMA (WCDMA) used as modulation technique
- Supports CS (ciruit switched) and PS (packet switched) services
- fixed part of the network heavily uses ATM over SONET/SDH

HSDPA

- introduces new transport channel: HS-DSCH (High Speed Downlink Shared Channel)
- added in UMTS Release >= 5
- uses new physical channels: HS-SCCH, HS-DPCCH, HS-PDSCH
- adaptive modulation (QPSK, 16-QAM, 64-QAM)
- 3.6 Mbits/sec downlink
- Rel-5 also introduces 384 kbits/sec uplink

HSDPA

- HSUPA (High Speed Uplink Packet Access) == EUL (Enhanced Uplink)
- added in UMTS Releae >= 6
- similar techniques as for HSUPA but uplink
- new physical channels: E-AGCH, E-RGCH, E-DPCH, E-HICH, E-DPCCH, E-DPDCH
- Hybrid-ARQ to improve performance of re-transmissions
- common use up to 5.76 Mbits/sec

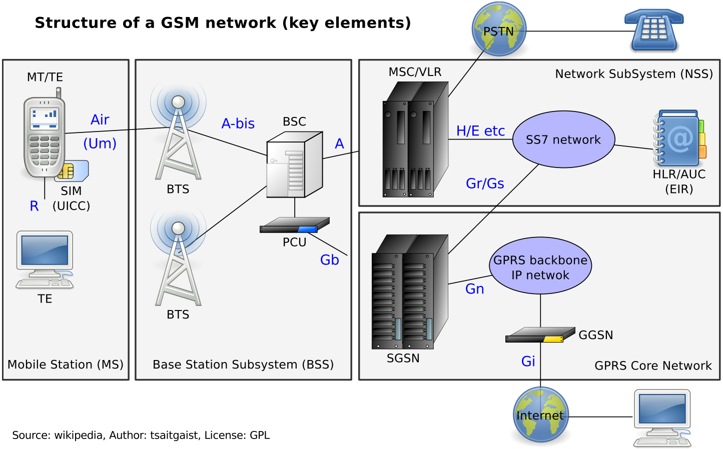
HSPA+

- HSPA+ == ESPA (Evolved High Speed Packet Access)
- added in UMTS Release >= 7
- up to 84 Mbits/sec DL, up to 22Mbits/s UL
- MIMO, QAM-64, combining two cells (dual-cell)
- theoretical maximum at 186 Mbit/s
- first deployments in 2008

Circuit Switched Data

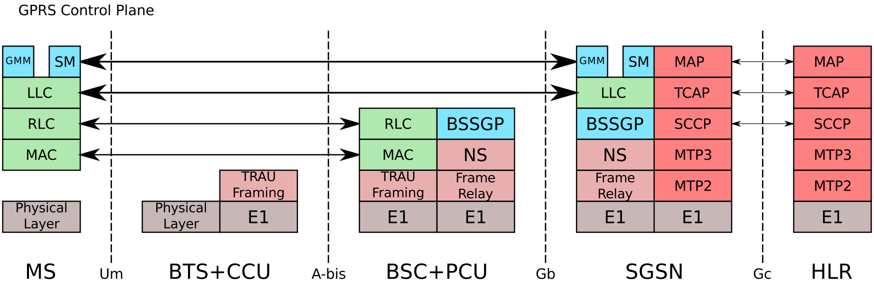
- Not covered here, only historic relevance...

GSM / GPRS Network Structure

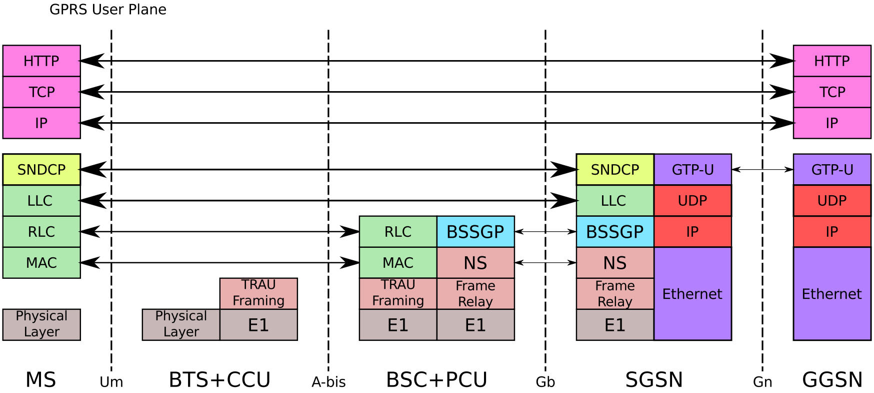


Source: wikipedia, Author: tsaitgaist, License: GPL

GPRS Control Plane Stacking



GPRS User Plane Stacking



GPRS Lower Layers

- MAC (Medium Access Control), TS 44.060
- MAC layer immediately on top of PDTCH physical channel
- RLC (Radio Lonk Control), also TS 44.060
- RLC layer on top of MAC layer
- resource allocation always controlled by network
- message encoding specified in CSN.1 (Concrete Syntax Notation)

GPRS Gb Layers

- NS (Network Service) layer, TS 08.16
  - maintains (redundant) physical links on top of frame relay
  - fail-over and load-sharing over various links
  - NS originally used over FR (Frame Relay)
  - sometimes NS in FR in IP
  - later also NS-over-IP (NSIP) using UDP
- BSSGP (Base Station Subsystem Gateway Protocol), TS 08.18
  - BVCI (BSSGP Virtual Connection Identifier)
  - maintains one BVC for each BTS in a BSS
  - maintains one additional BVC for eac
  - implements flow control (BSS, MS, PFC)
  - very inefficient due to large headers for every msg

GPRS LLC Layer

- SNDCP (Sub-Network Dependent Convergence Protocol), TS 04.64
- LLC (Logical Link Control) established between SGSN and MS
- supports acknowledged and unacknowledged mode
- one SAPI for signalling (GMM, SM)
- additional SAPIs available for user traffic in SNDCP
- GEA encryption happens on LLC layer
- Checksumming

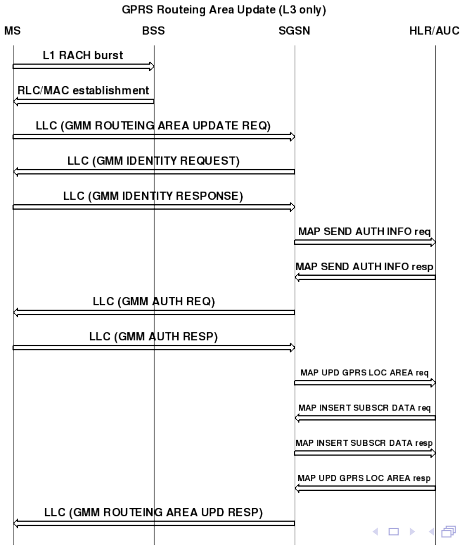
GPRS SNDCP Layer

- SNDCP (Sub-Network Dependent Convergence Protocol), TS 04.65
- general-purpose encapsulation for user packte data
- intiially intended for X.25 and OSI protocols, also IP
- today only used with IP payload
- IP header compression, v.42bis payload compression
- multiple streams (NSAPI) can exist over a LLC SAPI

GPRS Mobility Management

- GMM (GPRS Mobility Management) corresponds to GSM MM
- signalling directly on top of LLC, no SNDCP is used
  - Routeing Area Update
  - GPRS Attach/Detach
  - Authentication (same as GSM A3/A8)
  - P-TMSI reallocation
  - Identification Procedure
  - SMS delivery via GPRS

Example GRPS MM Procedure



GPRS Routeing Area Update (L3 only)

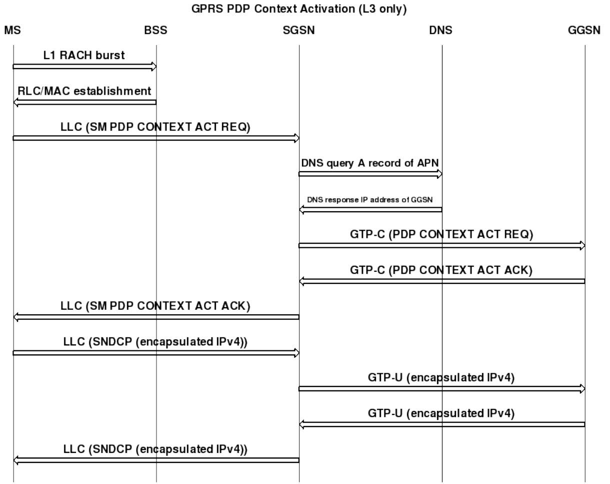
MS
BSS
SGSN
HLR/AUC

L1 RACH burst
RLC/MAC establishment
LLC (GMM ROUTEING AREA UPDATE REQ)
LLC (GMM IDENTITY REQUEST)
LLC (GMM IDENTITY RESPONSE)
MAP SEND AUTH INFO req
MAP SEND AUTH INFO resp
LLC (GMM AUTH REQ)
LLC (GMM AUTH RESP)
MAP UPD GPRS LOC AREA req
MAP INSERT SUBSCR DATA req
MAP INSERT SUBSCR DATA resp
MAP UPD GPRS LOC AREA resp
LLC (GMM ROUTEING AREA UPD RESP)

GPRS Session Management

- SM (Session Management) maintains tunnels to external packet data networks
- each session is called a PDP Context
- multiple PDP contexts can be active at any point in time
- Address of tunnel broker (GGSN) called APN (access point name)
- SSGN uses (private) DNS zones for resolving GGSN IP based on APN
- SGSN maintains state, but actual establishment is handled via GTP-C by the GGSN
- each PDP context has its APN, QoS, IPv4/IPv6 address, etc.

Example GRPS SM Procedure


GPRS PDP Context Activation (L3 only)
MS
BSS
SGSN
DNS
GGSN
L1 RACH burst
RLC/MAC establishment
LLC (SM PDP CONTEXT ACT REQ)
DNS query A record of APN
DNS response IP address of GGSN
GTP-C (PDP CONTEXT ACT REQ)
GTP-C (PDP CONTEXT ACT ACK)
LLC (SM PDP CONTEXT ACT ACK)
LLC (SNDCP (encapsulated IPv4))
GTP-U (encapsulated IPv4)
GTP-U (encapsulated IPv4)
LLC (SNDCP (encapsulated IPv4))

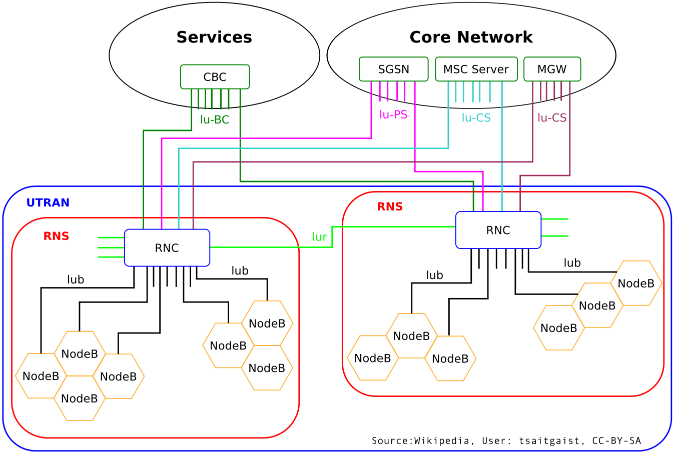
GTP Protocol between SGSN and GGSN

- GTP (GPRS Tunnelling Protocol), TS 29.060
- the only protocol specified over IP right from the beginning
- GGSN can be an IP-only device, no SS7/SIGTRAN/E1/FR required
- GTP-C for tunnel setup/teardown (SM procedures)
- GTP-U for encapsulating actual user data
- no authentication/encryption, intended to be used in private intra or inter-operator links only

UMTS PS Intro

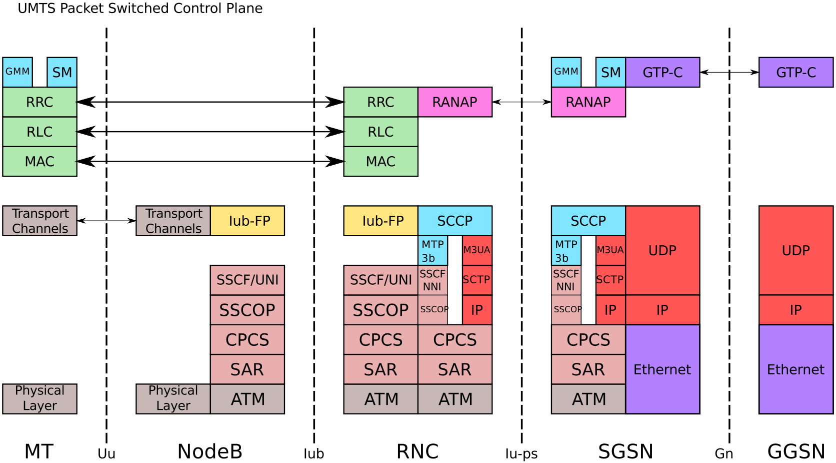
- Higher layers (GMM, SM) re-used from GPRS
- SGSN and GGSN functional entities remain almost unchanged
- Large differences in SGSN-RAN communication (RANAP instead of BSSGP/NS)
- Anything below RANAP again quite different from GPRS

UMTS Network Architecture

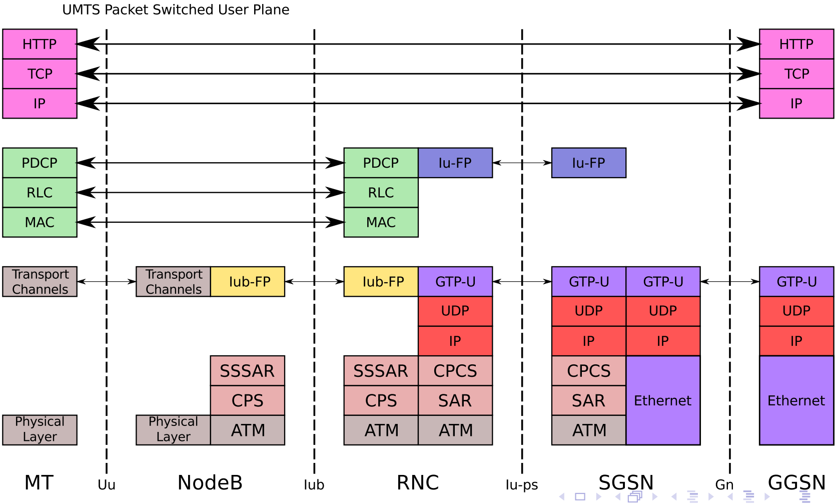


Source:Wikipedia, User: tsaitgaist, CC-BY-SA

UMTS Control Plane Stacking



UMTS User Plane Stacking



UMTS RLC/MAC Layer

- MAC specified in TS 25.321
- RLC specified in TS 25.322
- not in any formal syntax (uncommon in UMTS!)
- RLC level implements encryption, segmentation, retransmission

UMTS RRC Layer

- RRC specified in TS 25.331
- completely new protocol, unlike GSM/GRPS RR
- formally specified in ASN.1, uses PER
    - measurement control
    - ciphering control
    - paging
    - radio bearer management
    - SYS_INFO broadcast
    - integrity check

UMTS PDCP Layer

- PDCP specified in TS 25.323
- corresponds to functionality of SNDCP in GPRS
- handles user data payload and header compression
- utilizes RFC 3095 (ROHC) and RFC 2507 (IP Hdr Comp)
- between User IP and RLC

UMTS RANAP Layer

- RANAP (Radio Access Network Application Part), TS 25.413
- signalling between SGSN and RAN (RNC)
- formally specified in ASN.1, uses PER encoding
- never visible to the user, only in back-haul network
- Vodafone UK / Alcatel-Lucent Femtocells use RANAP!

UMTS NBAP Layer

- NBAP (NodeB Application Part), TS 25.443
- signalling between RNC and NodeB inside RAN
- formally specified in ASN.1
- never visible to the user, only in back-haul network
- is what you need to implment first to drive UMTS NodeBs from eBay ;)

UMTS GTP Layer between SGSN and GGSN

- exactly the same as for GPRS
- some new/extended information elements for e.g. 3G QoS
- GGSN doesn't need to change between 2G and 3G networks

HSPA+ related changes

- SGSNs have become a bottleneck in modern data-driven cellular networks
- SGSNs can be bought up to 40Gbps throughput, but most are smaller
- think of 20,000 cells, each 3 sectors with 20Mbps+ each...
- HSPA+ eNodeB contains small SGSN internally, user data directly passed to GGSN
- this means segmentation, compression and encryption is no longer on a centralized node but done on the edge of the network

Thanks

Thanks for your attention. I hope we have time for Q&A.