Cellular Networks
2G Technologies: GSM and GPRS

Vahid Shah-Mansouri, Fall 1397
Faculty of ECE, University of Tehran

References

- M. Sauter, "From GSM to LTE", John Wiled and Sons, 2011, chpaters 1 and 2.
- Jeffrey Bannister, Paul Mather and Sebastian Coope "Convergence Technologies for 3G Networks," John Wiley & Sons, Ltd, chapters 3 and 4.
- G. Stuber, "Principles of Mobile Communication, " Springer, 3rd edition, 2011. Chapter 1.
- Pahlavan and Krishnamurthy, "Principles of Wireless Networks," Prentice Hall, 2003. Chapters 7 and 9.
- 8101638

Wireless Comes of Age

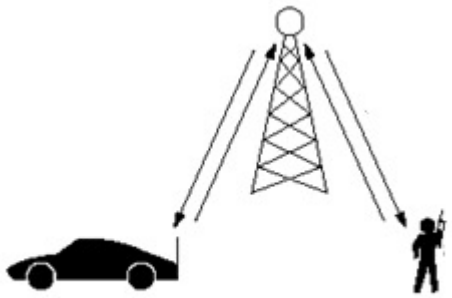
- Wireless communications began in 1895 when inventors including Guglielmo Marconi, Alexander Popov and Nicola Tesla independently demonstrated radio transmission/reception
- Marconi patented wireless telegraph in England in 1896
- First voice transmission over radio made by Fessenden in 1900 (over a distance of 1.6 km)
- Dec. 1901 Marconi made historic trans-Atlantic transmission from St. John, Nfd. to Cornwall, UK. (about 3200 km)
- Two-way FM mobile police radio first used in 1940
- First geosynchronous communications satellite launched in 1963 (NASA's Syncom)
- ALOHANET launched at University of Hawaii in 1971
- AMPS (1G cellular) tested in 1978 and deployed in 1984
- GSM (2G cellular) launched in 1994
- IEEE 802.11 first released in 1997
- UMTS (3G cellular) launched in 2001
- More recent: WiMAX, UWB, …

Cellular Technologies

	1G	2G	2.5G	3G	3.5G	4G
Starting time	Early 1980s	Early 1990s	Mid 1995	Early 2000s	2008	2011
Driven Technology	Analogue SP	Digital SP F/TDMA	Packet switching	Intelligent SP CDMA	Multiple antennas	OFDMA
Rep. Standard	AMPS, TACS, NTT	GSM, IS-95	GPRS, EDGE	UMTS, CDMA200	HSPA	LTE
Data rate (bps)			171 ~ 384 K	2M ~ 5M	80M ~ 300M	~ 1G
Core Network	Telecom	Telecom	Telecom, IP	Telecom, IP	Telecom, IP	IP
Service	Voice	+ SMS	+MMS, data	+ Internet access	+ multimedia	+ everything

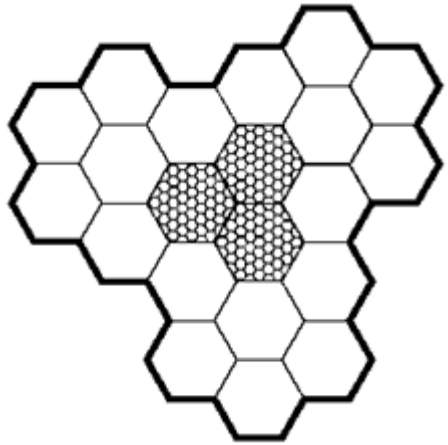
Zero Generation

- Started from push to talk one to many systems.
- In 1960, Improved Mobile Telephone System (IMTS) was installed with separate US and DS channels.
  - Single base station
  - Had a high power transmitter with 23 channels from 150 MHz to 450MHz
  - Problems with channel capacity



Cellular Idea Comes around

- Cellular radio is a technique to increase the capacity and save power.
- Each cell has a dedicated base station.
- Cellular system
  - Task: provide voice/data service
  - Pre-requisites: register and track mobile devices, assign them to the best base station.

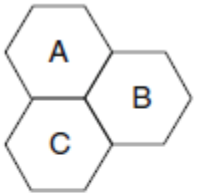


Frequency reuse

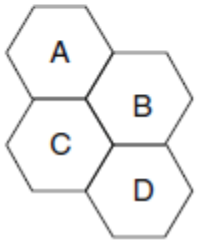
- A given frequency is reused at the closest possible distance that the radio link will allow.
- Smaller cells have a shorter distance between reused frequencies, and this results in an increased system spectral efficiency and traffic-carrying capacity.
- Tessellating frequency reuse clusters are those that will fit together without leaving any gaps. A tessellating reuse cluster of size *N* can be constructed if

$$N = i^2 + ij + j^2, i \geq j.$$

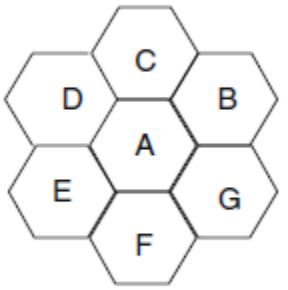
- Allowable hexagonal cluster sizes are *N* = 3, 4, 7, 9, 12.
- The co-channel reuse factor $D/R=\sqrt{3N}$
  - D=Distance between two cells with the same freq.
  - R=cell radius



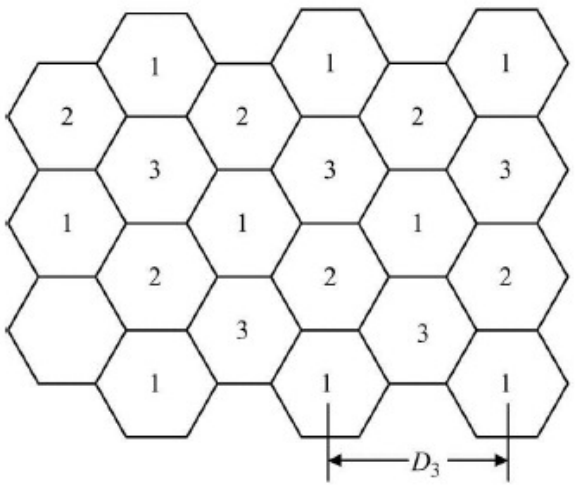
3-Cell



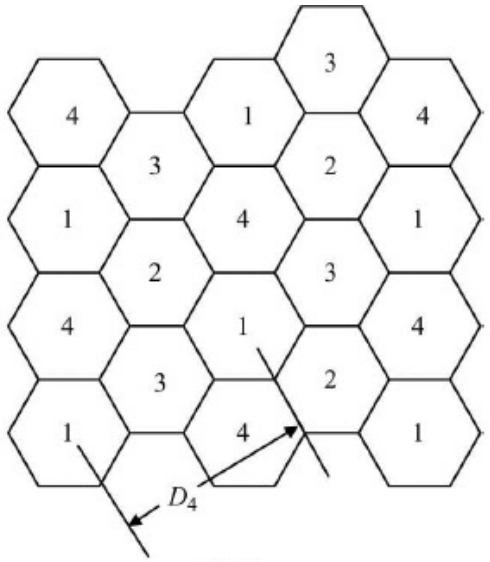
4-Cell



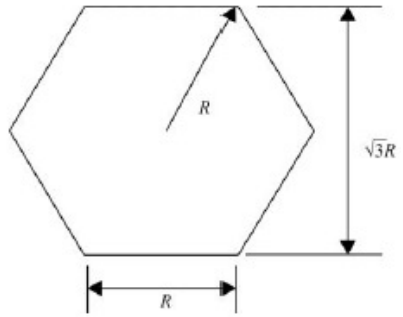
7-Cell



(a) 3-reuse



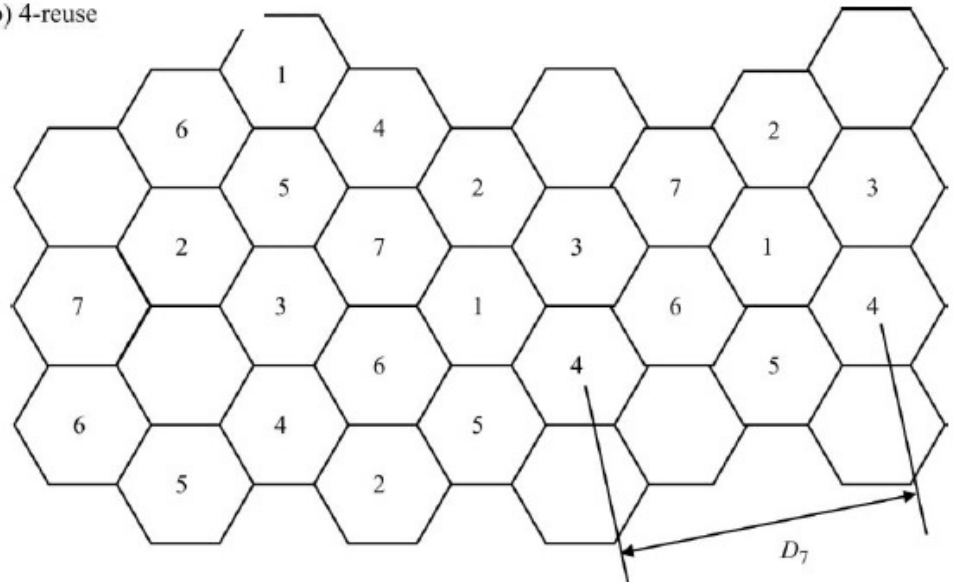
(b) 4-reuse



$$D_3 = 3R$$

$$D_4 = 2\sqrt{3}R$$

$$D_7 = \sqrt{21}R$$

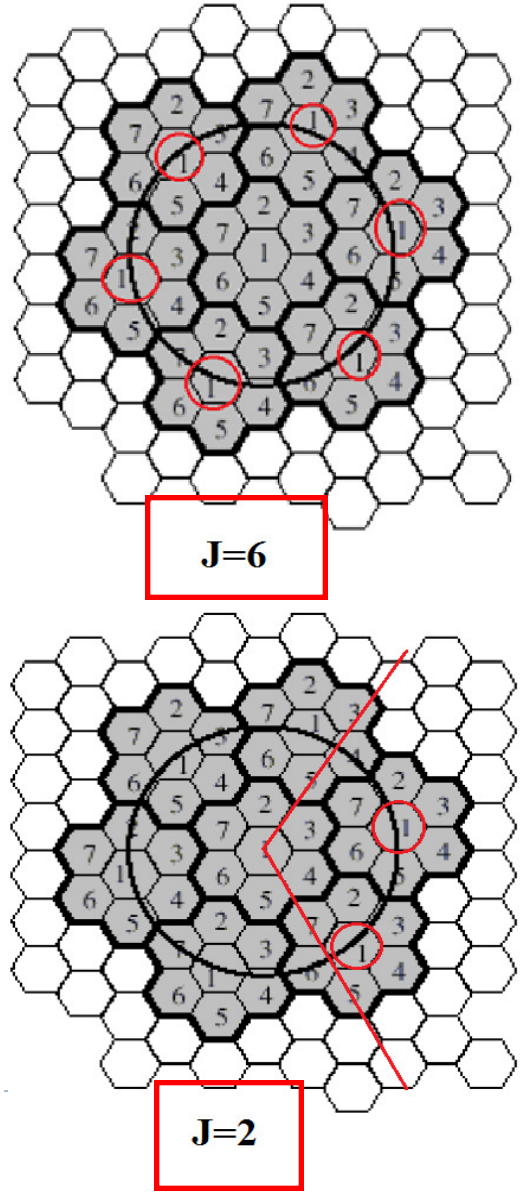


Signal to Interference and Sectoring

- Signal to Interference Ratio:
  - All the BSs have the same transmit power
  - Path loss component α
  - Consider the first tire co-channel cells (*J*)
  - Worst case downlonk Signal to interference ratio at a cell

$$\frac{S}{I} = \frac{1}{J}\left(\frac{R}{D}\right)^{-\propto}$$

- **Sectoring**
  - Instead of omni-directional, use directive antennas.
  - S/I can be increased significantly.



1st Generation

- 1979: first analog cellular system, the Nippon Telephone and Telegraph (NTT) system, became operational.
- 1981: Ericsson fielded the Nordic Mobile Telephone (NMT) 900 system,
- 1983: AT&T fielded the Advanced Mobile Phone Service (AMPS) in Chicago.

Feature	NTT	NMT	AMPS
Frequency band RL/FL[a] (MHz)	925–940/870–885 915–918.5/860–863.5 922–925/867–870	890–915/917–950	824–849/869–894
Carrier spacing (kHz)	25/6.25 6.25 6.25	12.5[b]	30
Number of channels	600/2400 560 280	1999	832
Modulation	Analog FM	Analog FM	Analog FM

[a] *RL* reverse link, *FL* forward link

[b] Frequency interleaving using overlapping channels, where the channel spacing is half the nominal channel bandwidth

2nd Generation Comes Around

Feature	GSM/DCS1800/PCS1900	IS-54/136	PDC	IS-95
Frequency band	GSM: 890–915/	824–829/	810–826/	824–829/
RL/FL[a]	935–960	869/894	940–956	869–894
(MHz)	DCS1800: 1710–1785/	1930–1990/	1429–1453/	1930–1990/
	1805–1880	1850–1910	1477–1501	1850–1910
	PCS1900: 1930–1990/			
	1850–1910			
Multiple access	F/TDMA	F/TDMA	F/TDMA	F/CDMA
Carrier spacing (kHz)	200	30	25	1250
Modulation	GMSK	$\pi/4$-DQPSK	$\pi/4$-DQPSK	QPSK
Baud rate (kb/s)	270.833	48.6	42	1228.8 Mchips/s
Frame size (ms)	4.615	40	20	20
Slots/frame	8/16	3/6	3/6	1
Voice coding (kb/s)	VSELP(HR 6.5)	VSELP (FR 7.95)	PSI-CELP (HR 3.45)	QCELP (8,4,2,1)
	RPE-LTP (FR 13)	ACELP (EFR 7.4)	VSELP (FR 6.7)	RCELP (EVRC)
	ACELP (EFR 12.2)	ACELP (12.2)	Rate-1/2 BCH	FL: rate-1/2 CC
Channel coding	Rate-1/2 CC	Rate-1/2 CC		RL: rate-1/3 CC
Frequency hopping	Yes	No	no	N/A
Handoff	Hard	Hard	Hard	Soft

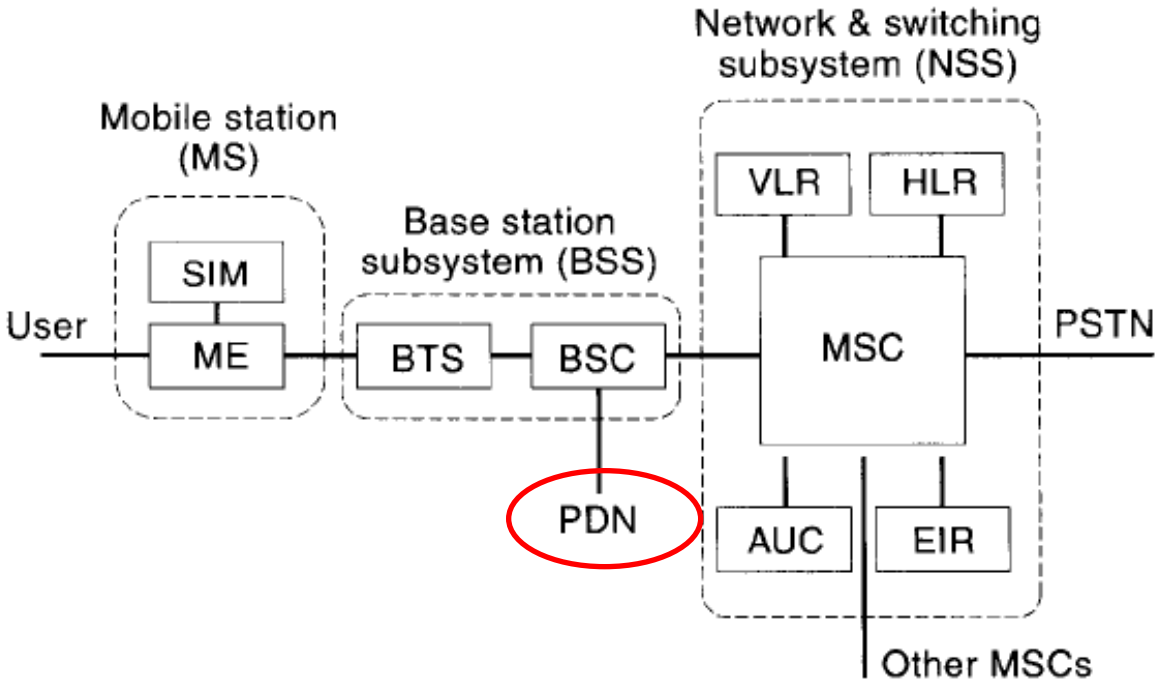
Global System for Mobile (GSM)

Global System for Mobile (GSM)

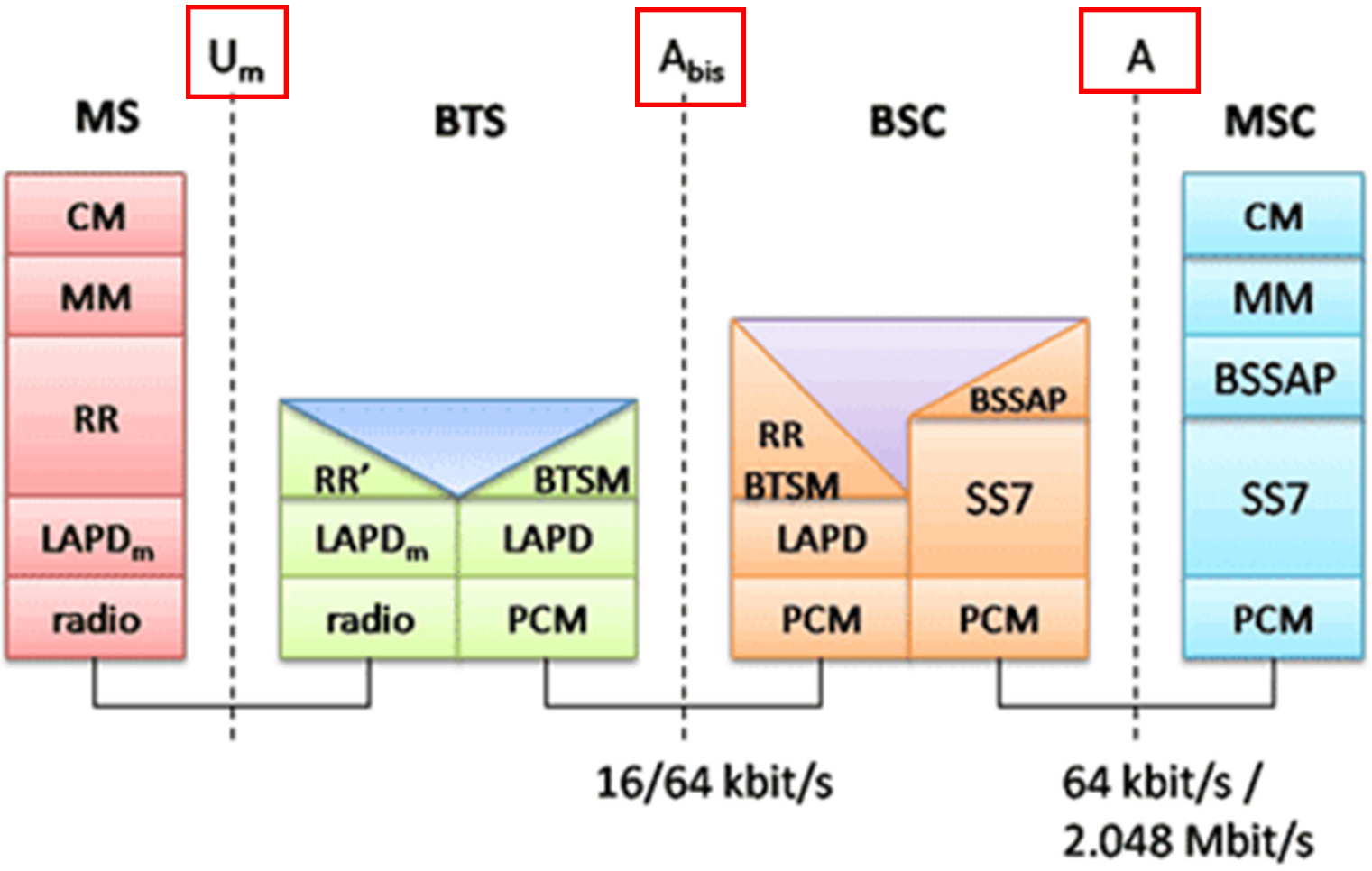
- An ETSI pan-European standard for public land mobile network (PLMN).
- The standard was released at 1991 and by 1994, 32 operators adopted the standard.
- GSM services:
  - Telephone services
    - Telephony
    - SMS,
    - FAX
  - Bearer services:
  - Sync, async data
- Supplementary:
  - Call fwd,

GSM System Architecture

- Three categories:
  - Mobile station (user equipment)
  - Base station subsystem (access and backhaul)
  - Network and switching subsystem (core network)



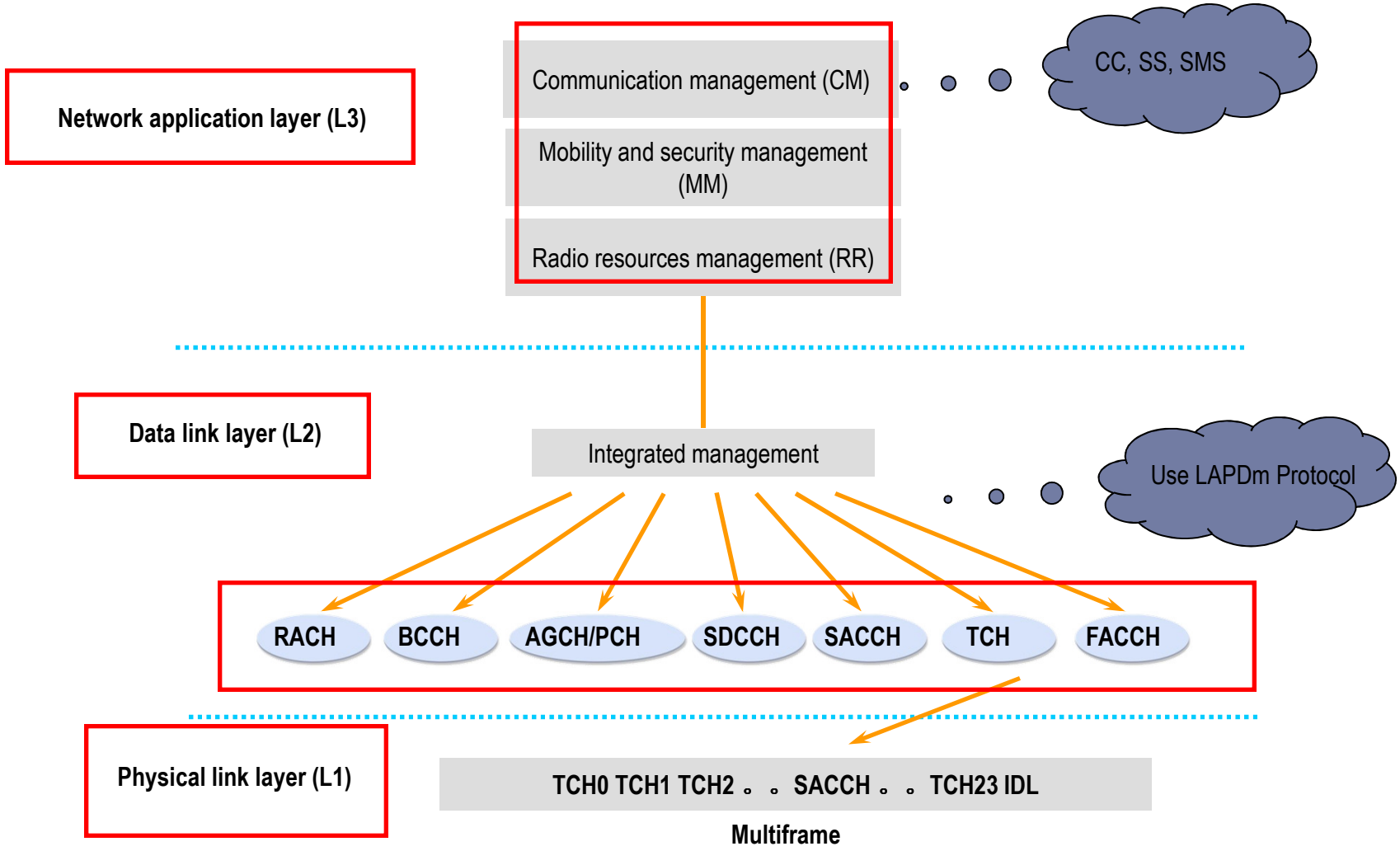
GSM Interfaces and Protocol Stacks



GSM Air Interface

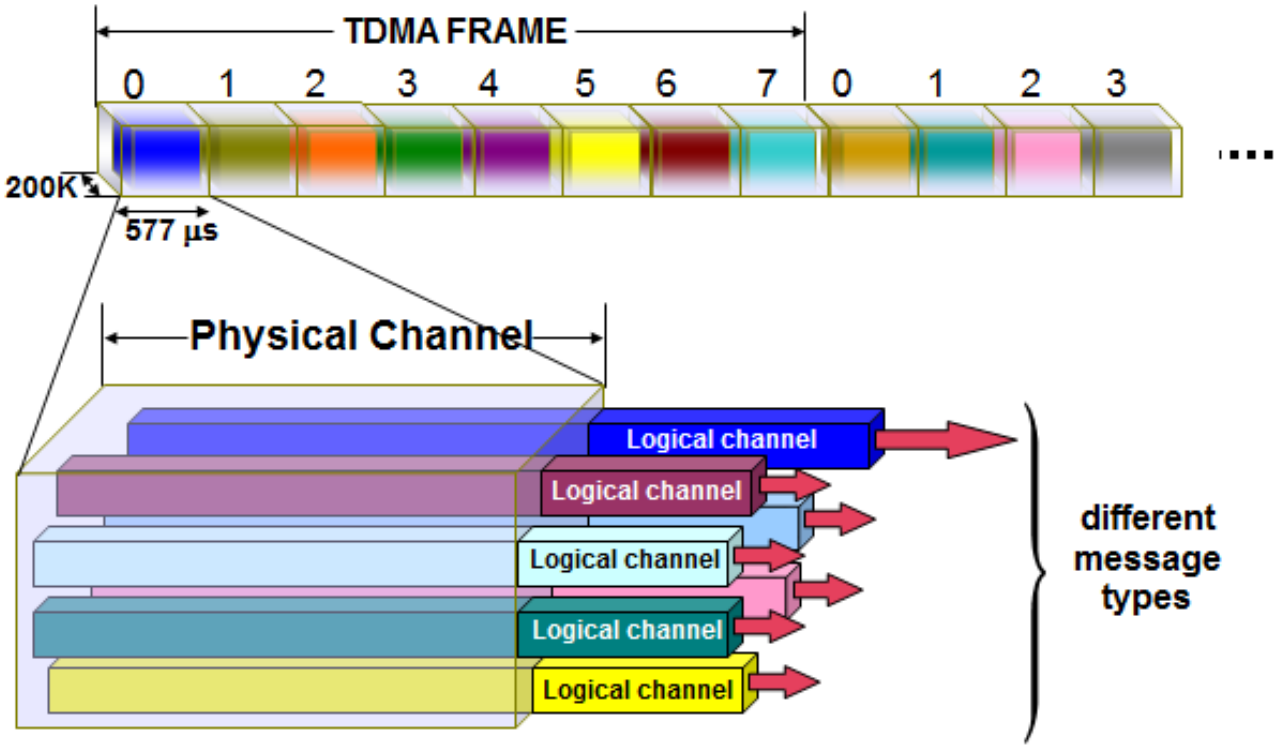
- Interface is called Um.
- Uplink/reverse: 890-915 Mhz
- Downlink/forward: 935-960 Mhz
- 25 Mhz bands are divided into 124 channels each 200 Khz.
- System is time slotted. Each GSM slot (burst) lasts for 0.577 mS.
- 8 burst comprises a frame.
- One time slot can support transmission of 156.25 bits.

Hierarchical Structure of Um Interface

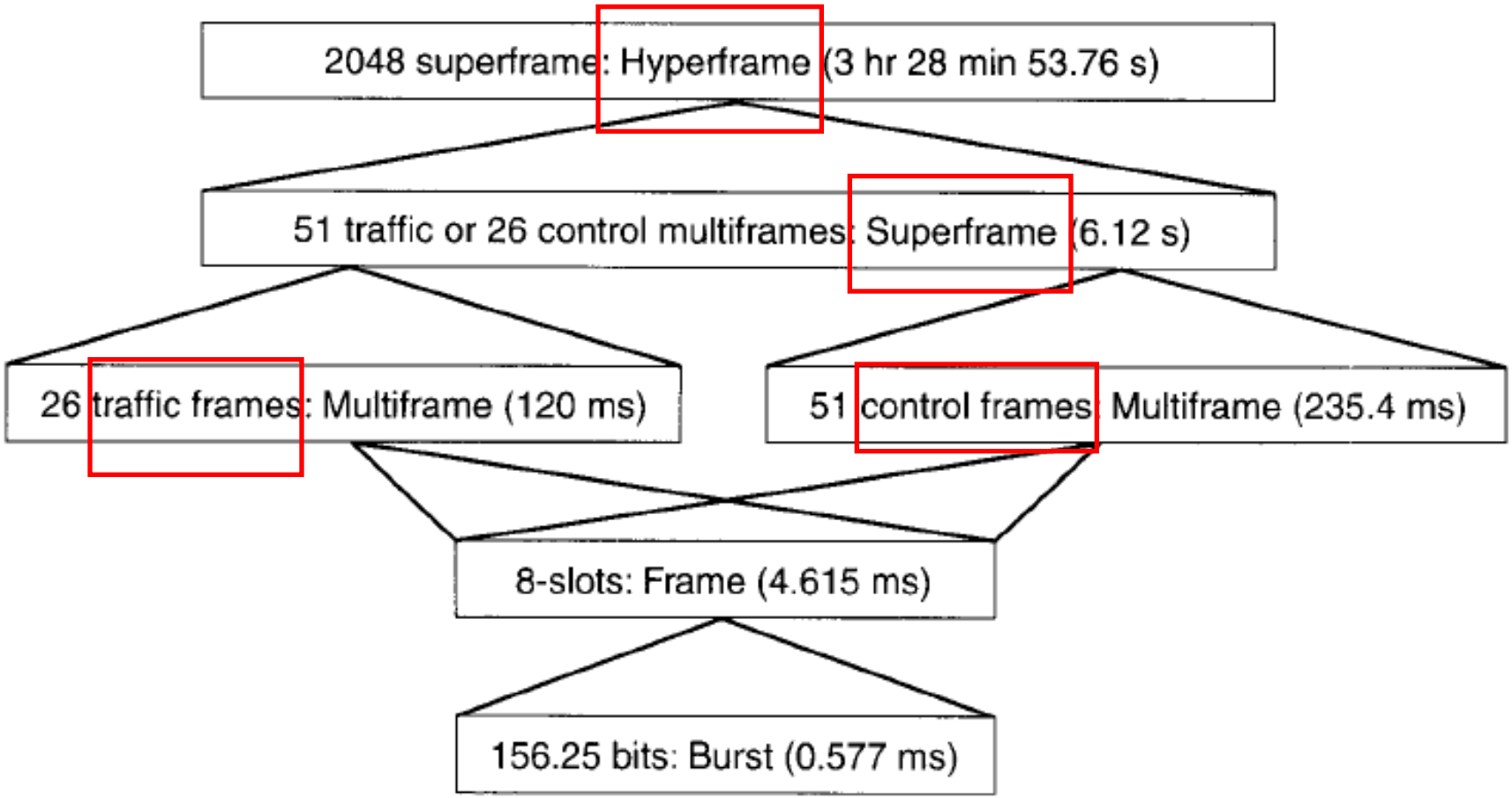


GSM Channels

- Physical channels
- Logical channels



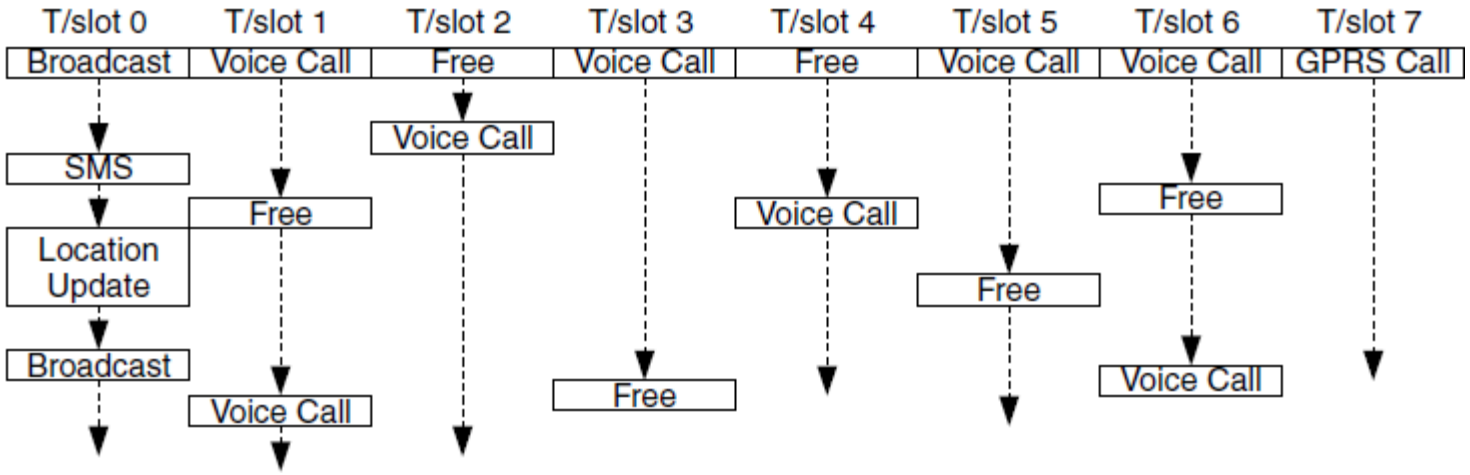
TDMA Frame Hierarchy



Logical Channel Types

- Common/Shared
  - forward common channels:
    - paging to inform a mobile of an incoming call, responding to channel requests, and broadcasting bulletin board information.
  - Return common channel
    - random access channel used by the mobile to request channel resources before timing information is conveyed by the BSS.
- Dedicated
  - Signalling/Control
    - maintenance of the call and for enabling call set up, providing facilities such as handover when the call is in progress, and finally terminating the call
  - Traffic
    - Actual voice

Example of Burst Assignments



Traffic Channels

- Traffic channels: two way channels carrying voice or data
  - **TCH/F** - Full rate traffic channel.
    - 13kbps speech coding, 9600 bps and 4800 bps data.
    - Adding signaling overhead, the rate would top up to 22.8 kbps.
  - **TCH/h** - Half rate traffic channel.
    - Support half rate
    - For applications which need half rate.

Control Channels

- Include three types:
  - Broadcast channels
  - Common Control channel
  - Dedicated control channel
- Broadcast Channels: one way
  - Frequency control/correction channel (FCCH)
    - MS uses it to synchronize its carrier frequency.
  - Synchronization Channel (SCH)
    - Used to broadcast frame synchronization signals to all MSs.
  - Broadcast Control Channel (BCCH)
    - General BTS information.
    - Usually burst 0 in one of the channels.
    - Repeats every three frame.

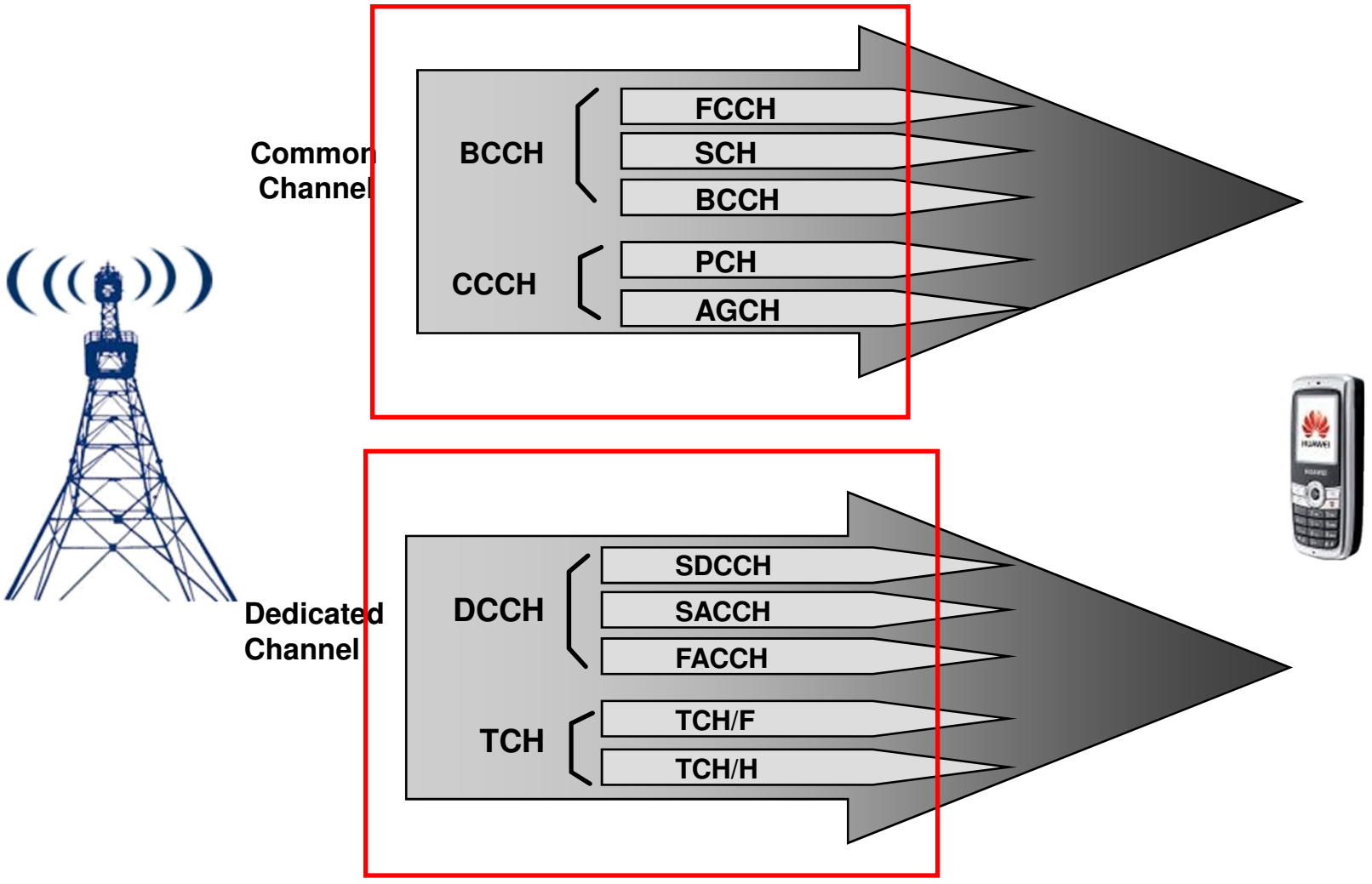
Control Channels

- Common/Shared Control channel: one way
  - Paging channel (PCH)
    - BTS inform MSs of an upcoming connection.
  - Random access channel (RCH)
    - MS request for a connection
  - Access Grant Channel (AGCH)
    - Acknowledge after a random access.

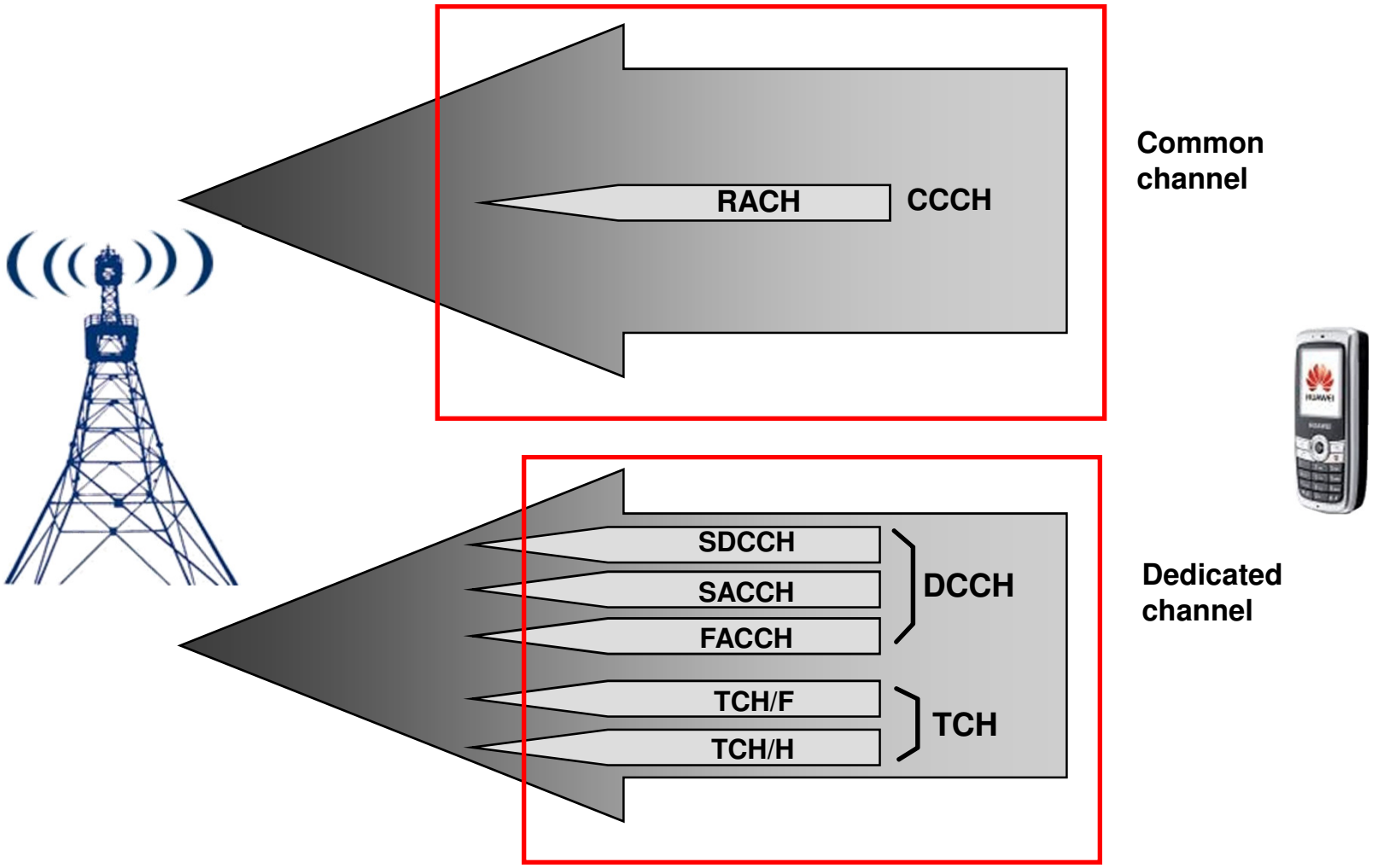
Control Channels

- Dedicated Control Channel: two way
  - Stand-alone dedicated control channel (SDCCH)
    - For call related control information
    - After RCH before TCH assignment.
    - Used to improve efficiency.
    - 4 slots in every 51 control frame (2kbps)
  - Slow associated control channel (SACCH)
    - Used for link parameters, half rate of SDCCH.
    - One slot in every 26 traffic channel allocated to SACCH.
    - Repeats every 480 msec.
  - Fast associated control channel (FACCH)
    - Stolen from TCH, indicated by three bits in the burst, immediate unscheduled control info

Downlink Logical Channel



Uplink Logical Channel



FN	TS-0	TS-1
0	FCCH	SDCCH/0
1	SCH	SDCCH/0
2	BCCH	SDCCH/0
3	BCCH	SDCCH/0
4	BCCH	SDCCH/1
5	BCCH	SDCCH/1
6	AGCH/PCH	SDCCH/1
7	AGCH/PCH	SDCCH/1
8	AGCH/PCH	SDCCH/2
9	AGCH/PCH	SDCCH/2
10	FCCH	SDCCH/2
11	SCH	SDCCH/2
12	AGCH/PCH	SDCCH/3
13	AGCH/PCH	SDCCH/3
14	AGCH/PCH	SDCCH/3
15	AGCH/PCH	SDCCH/3
16	AGCH/PCH	SDCCH/4
17	AGCH/PCH	SDCCH/4
18	AGCH/PCH	SDCCH/4
19	AGCH/PCH	SDCCH/4
20	FCCH	SDCCH/5
21	SCH	SDCCH/5
22	SDCCH/0	SDCCH/5
23	SDCCH/0	SDCCH/5
24	SDCCH/0	SDCCH/6
25	SDCCH/0	SDCCH/6
26	SDCCH/1	SDCCH/6
27	SDCCH/1	SDCCH/6
28	SDCCH/1	SDCCH/7
29	SDCCH/1	SDCCH/7
30	FCCH	SDCCH/7
31	SCH	SDCCH/7
32	SDCCH/2	SACCH/0
33	SDCCH/2	SACCH/0
34	SDCCH/2	SACCH/0
35	SDCCH/2	SACCH/0
36	SDCCH/3	SACCH/1
37	SDCCH/3	SACCH/1
38	SDCCH/3	SACCH/1
39	SDCCH/3	SACCH/1
40	FCCH	SACCH/2
41	SCH	SACCH/2
42	SACCH/0	SACCH/2
43	SACCH/0	SACCH/2
44	SACCH/0	SACCH/3
45	SACCH/0	SACCH/3
46	SACCH/1	SACCH/3
47	SACCH/1	SACCH/3
48	SACCH/1	Free
49	SACCH/1	Free
50	Free	Free

FN	TS-2	TS-7
0	TCH	TCH
1	TCH	TCH
2	TCH	TCH
3	TCH	TCH
4	TCH	TCH
5	TCH	TCH
6	TCH	TCH
7	TCH	TCH
8	TCH	TCH
9	TCH	TCH
10	TCH	TCH
11	TCH	TCH
12	SACCH	SACCH
13	TCH	TCH
14	TCH	TCH
15	TCH	TCH
16	TCH	TCH
17	TCH	TCH
18	TCH	TCH
19	TCH	TCH
20	TCH	TCH
21	TCH	TCH
22	TCH	TCH
23	TCH	TCH
24	TCH	TCH
25	Free	Free
0	TCH	TCH
1	TCH	TCH
2	TCH	TCH
3	TCH	TCH
4	TCH	TCH
5	TCH	TCH
6	TCH	TCH
7	TCH	TCH
8	TCH	TCH
9	TCH	TCH
10	TCH	TCH
11	TCH	TCH
12	SACCH	SACCH
13	TCH	TCH
14	TCH	TCH
15	TCH	TCH
16	TCH	TCH
17	TCH	TCH
18	TCH	TCH
19	TCH	TCH
20	TCH	TCH
21	TCH	TCH
22	TCH	TCH
23	TCH	TCH
24	TCH	TCH
25	Free	Free

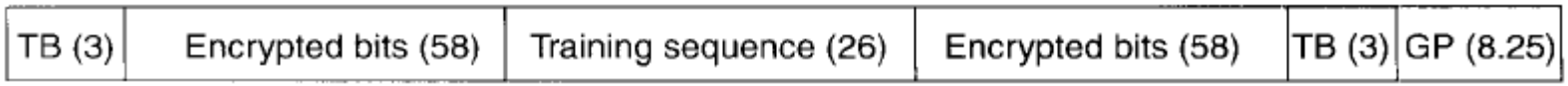
- Frequency control channel (FCCH)
- Synchronization Channel (SCH)
- Broadcast Control Channel (BCCH)
- Paging channel (PCH)
- Random access channel (RCH)
- Access Grant Channel (AGCH)
- Stand-alone dedicated control channel (SDCCH)
- Slow associated control channel (SACCH)
- Fast associated control channel (FACCH)

Call Establishment Procedure

Steps	MS	BTS	BSC	MSC
1. Channel request (RACH)	→	→		
2. Channel assigned (AGCH)	←	←		
3. Call establishment request (SDCCH)	→	→	→	
4. Authentication request (SDCCH)	←	←	←	
5. Authentication response (SDCCH)	→	→	→	
6. Ciphering command (SDCCH)	←	←	←	
7. Ciphering ready (SDCCH)	→	→	→	
8. Send destination address (SDCCH)	→	→	→	
9. Routing response (SDCCH)	←	←	←	
10. Assign traffic channel (SDCCH)	→	→		
11. Traffic channel established (FACCH)	←	←		
12. Available/busy signal (FACCH)	←			
13. Call accepted (FACCH)	←	←	←	
14. Connection established (FACCH)	→	→	→	
15. Information exchange (TCH)	←			→

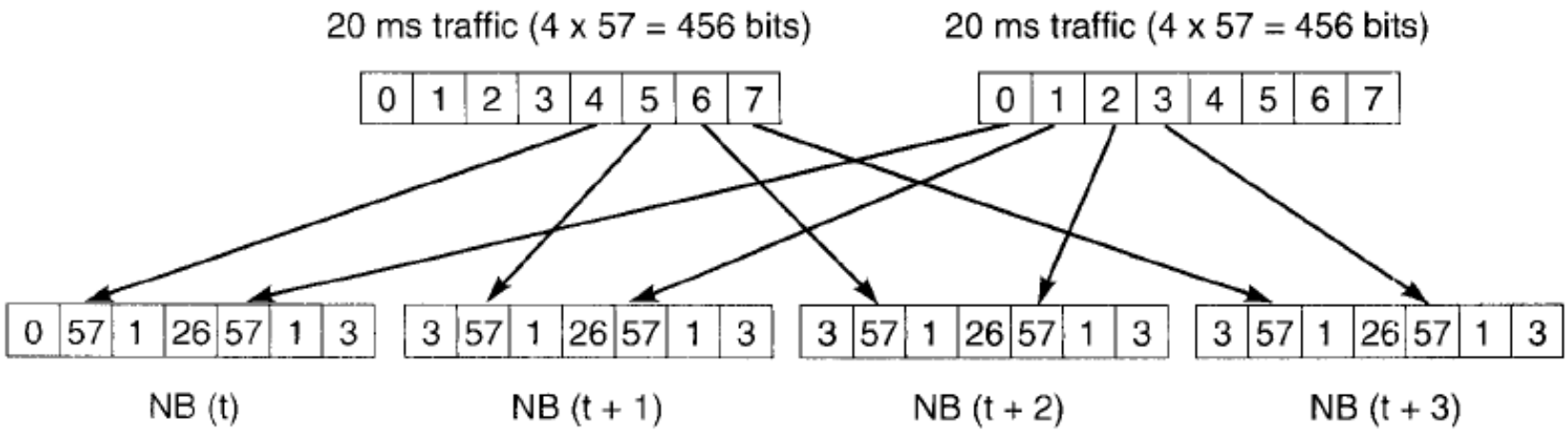
Burst (Packet) Format

- Normal Burst: for data transmission
  - Three tail bits: indicate beginning and end of a frame
  - 2 x 57 bits of data
  - 2 x 1 bits indicating the purpose of the packet (user/control)
  - Guard bits: 8.25 bits for guard band
  - Training sequence: used for timing reference and equalisation.



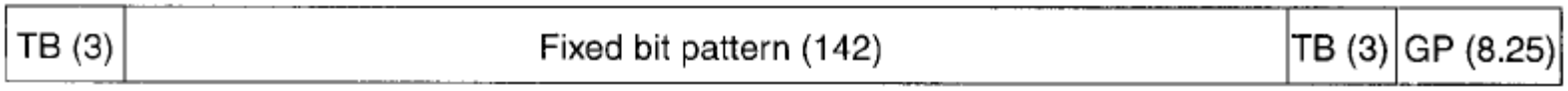
Burst (Packet) Format

- 456 bits of user data (260 raw speech bits) every 20 ms.

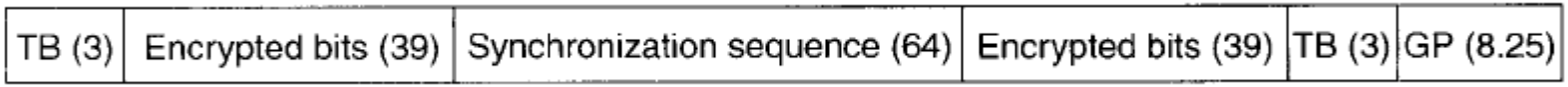


Burst (Packet) Format

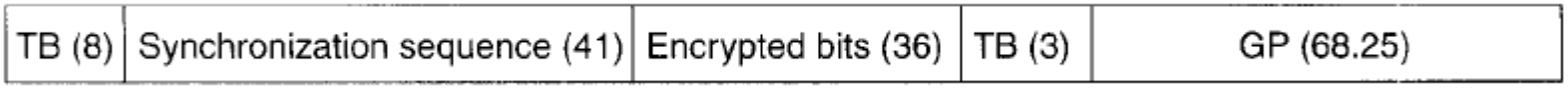
- Frequency Correction Bursts
  - Three tail bits
  - The rest are all zero → carrier frequency transmission



- Synchronization Burst
  - Slot synchronization



- Random Access Bursts (RAB)



Traffic Rates

- GSM has standardized voice codec for the air interface
  - Full-rate (FR) codec reduces the 64 kbit/s voice stream to about 13 kbit/s.
  - Enhance FR (EFR) is proposed with better quality at the same rate.
  - Half-rate (HR) codec
    - has been defined for GSM that only requires a bandwidth of 7 kbit/s.
    - While there is almost no audible difference between the EFR codec and a PCM-coded speech signal, the voice quality of the HR codec is noticeably inferior.

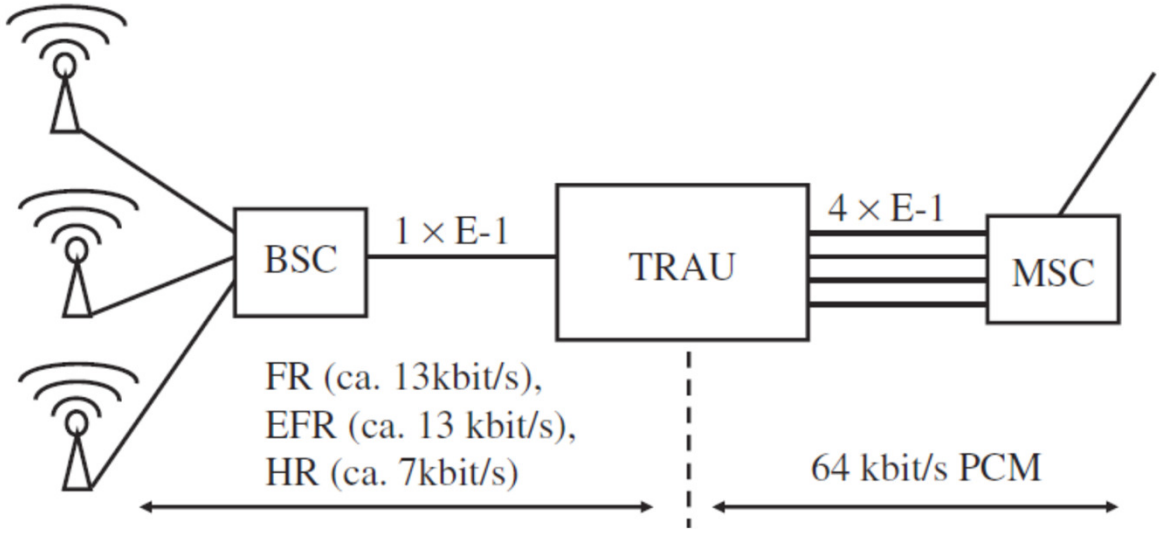
Traffic Rates

- 260 bits of voice data is generated every 20 ms (13 kbps).
- By adding forward error correction (FEC), the data is converted to 456 bits.
- The bits are interleaved to reduce effect of burst error.
- 26 frames composes a voice multi-frame.
- One burst of 24 frames is assigned for a TCH channel.
- One burst is left for SAACH and one burst is used to listen to the BCCH of the neighboring cell for hand off.
- Transmission rate: 24 x 114/(120 ms) = 22.8kbps

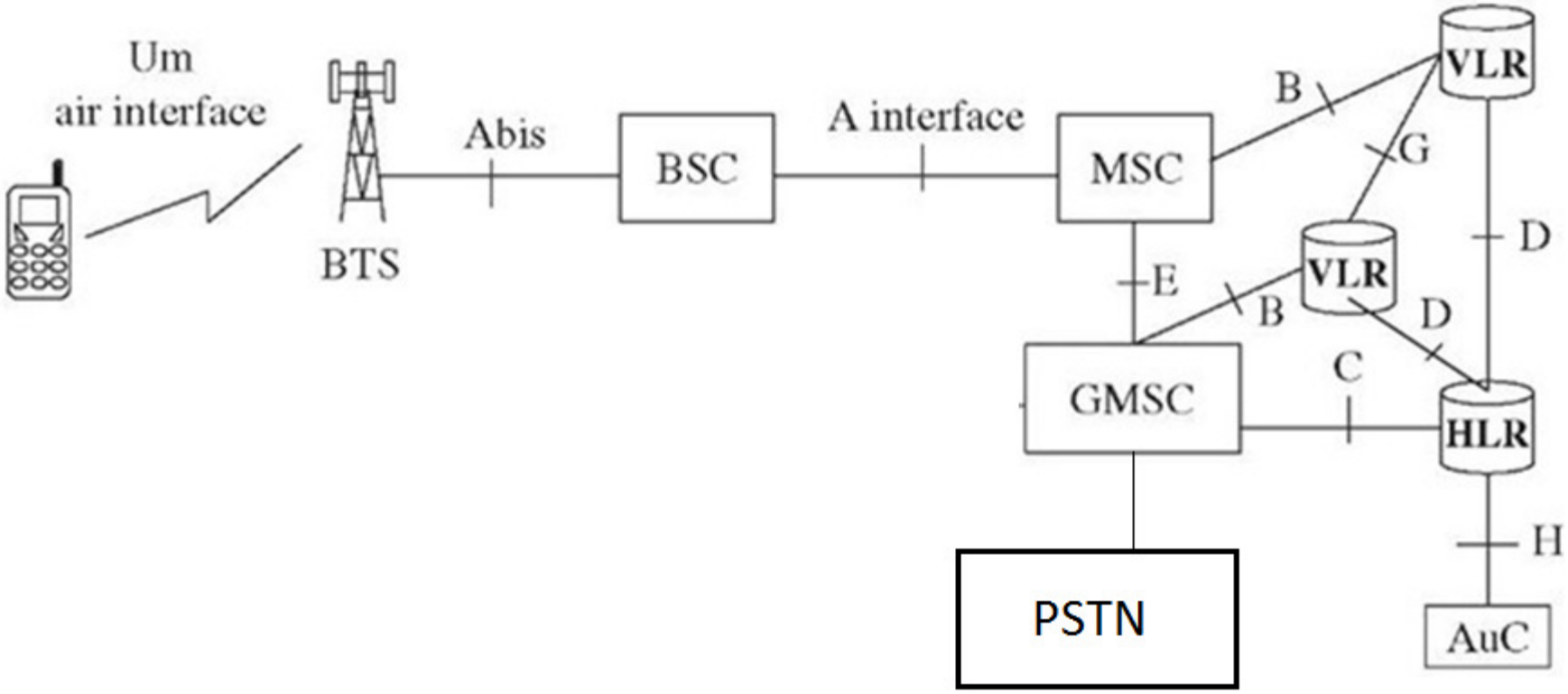
Transcoding and Rate Adaptation Unit (TRAU)

- In the mobile network, the compression and decompression of the voice data stream is performed in the Transcoding and Rate Adaptation Unit (TRAU),
- TRAU is responsible for trans-coding the user data from 12.2~16Kb/sec to standard ISDN rates of 64Kb/sec.
- It can physically reside on either BSC side or MSC side.

- If it resides on the MSC side, it provides substantial changes in the backhaul – 4 users over a single E-1 TDMA channel.



GSM Core Structure



The Base Station Controller (BSC)

- Designed to offload most of the radio link related processes from the BTS and MSC (establishment, release and maintenance of all connections of cells connected to).
- Although the main task of BSC falls in the control planed, it also switch calls from MSC to correct BTS.
- The BSC is responsible for **radio resource managements**
  - Activate, monitor, assign, and release all signaling and voice channels in the connected BTSs.
  - Make the decisions for the handover between BTSs.
  - It is in charge of controlling the transmission power for every air interface connection.

The Base Station Controller (BSC)

- Control channel assignment is based on BSC decision.
- Traffic channel is requested by the MSC for both mobile-originated and mobile-terminated calls.
  - Once the mobile device and the MSC have exchanged all necessary information for the establishment of a voice call via an SDCCH, the MSC sends an assignment request for a voice channel to the BSC.
- The interface between the BTS and BSC is called A-bis. Generally carried by a DS-1, ES-1, or E1 TDM circuit.
- Uses TDM subchannels for traffic (TCH), LAPD protocol for BTS supervision and telecom signaling, and carries synchronization from the BSC to the BTS and MS.

The Base Station Controller (BSC)

- It can happen that the subscriber roams out of the coverage area of the cell in which the call was initially established.
- In this case, the BSC has to redirect the call to the appropriate cell. This procedure is called handover (handoff).
- Handover decision is made by BSC using channel measurements:
  - The downlink signal quality measurements are reported to the BSC by the mobile device via SACCH.
  - The uplink signal quality is constantly measured by the BTS and reported to the BSC.

Mobile Switching Center (MSC)

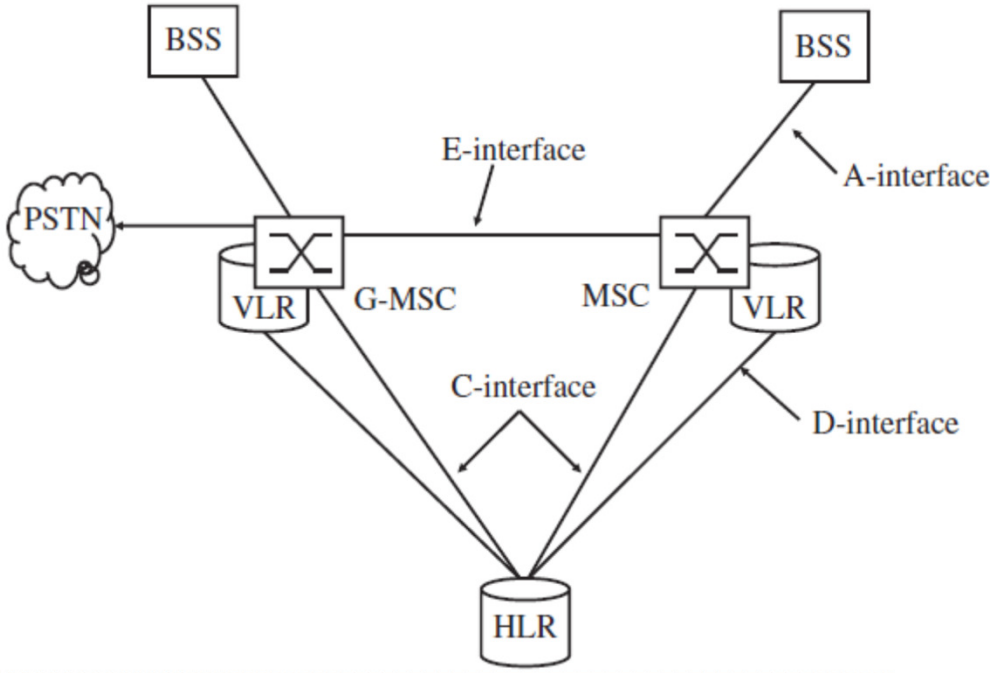
- The MSC is the central element of a mobile telecomm network.
- It is a regular PSTN switch center with some functionality to support mobility.
- All connections between subscribers are managed by the MSC and are always routed over the switching matrix even if two subscribers that have established a connection communicate over the same radio cell.

Mobile Switching Center (MSC)

- The management activities to establish and maintain a connection are part of the Call Control (CC) protocol
  - Registration of mobile subscribers as MS is switched on.
  - Call establishment and switching.
  - Forwarding of SMS messages.
- As subscribers can roam freely in the network, the MSC is also responsible for the Mobility Management (MM)
  - Authentication of subscribers at connection establishment.
  - If no active connection exists between the network and the mobile device, the MSC has to report a change of location.
  - If the subscriber changes its location while a connection is established with the network, the MSC is part of the process that ensures that the connection is not interrupted and is rerouted to the next cell.

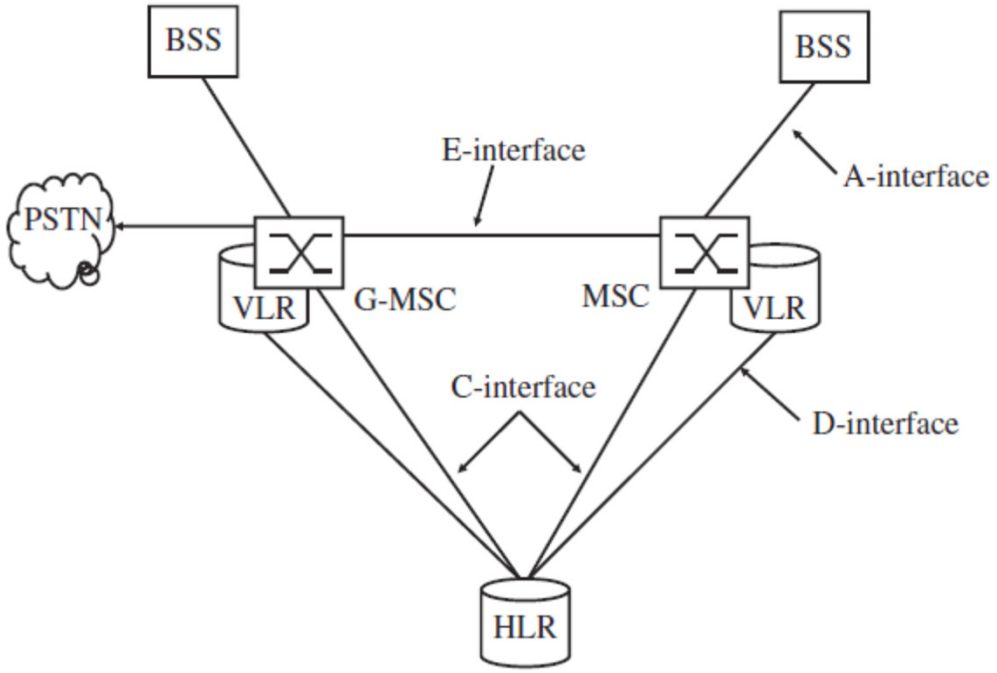
Mobile Switching Center (MSC)

- The MSC is connected to each BSC via a number of 2-Mbit/s E-1 (31 users) connections.
- This interface is called the A-interface and usually is carried over SDH.
- As an MSC only has a limited switching capacity and processing power, a PLMN is usually composed of dozens of independent MSCs. Each MSC thus covers only a certain area of the network.



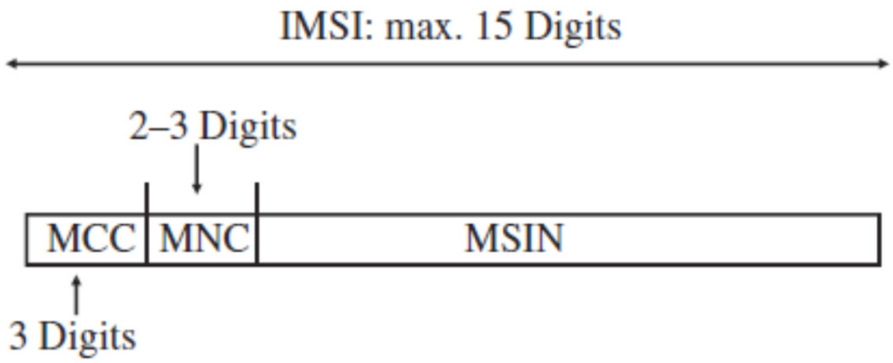
Mobile Switching Center (MSC)

- To enable the MSC to communicate with other nodes of the network, it is connected to them via standardized interfaces.
- MSCs are connected together via E-interface.
- One of the MSC has an added functionality for communication with public network – Gateway MSC (GMSC).



The Home Location Register (HLR)

- The HLR is the subscriber database of a GSM network.
- The International Mobile Subscriber Identity (IMSI) is an internationally unique number that identifies a subscriber in the HLR and the whole network.
- User phone number is Mobile Subscriber Integrated Services Digital Network Number (MSISDN) in the GSM standards which is different from IMSI.



The Home Location Register (HLR)

- IMSI is the information stored in the SIM not MSISDN.
- The Basic Parameters stored in the HLR are listed below:
  - Subscriber ID (IMSI)
  - Subscriber number (MSISDN)
  - Current Subscriber VLR (Current Location)
  - Supplementary Services Subscriber to
  - Subscriber Status (Registered or Deregistered)
  - Authentication Key and AUC Functionality
- The network may contain more than one HLR, but there is only one database record per subscriber

The Visitor Location Register (VLR)

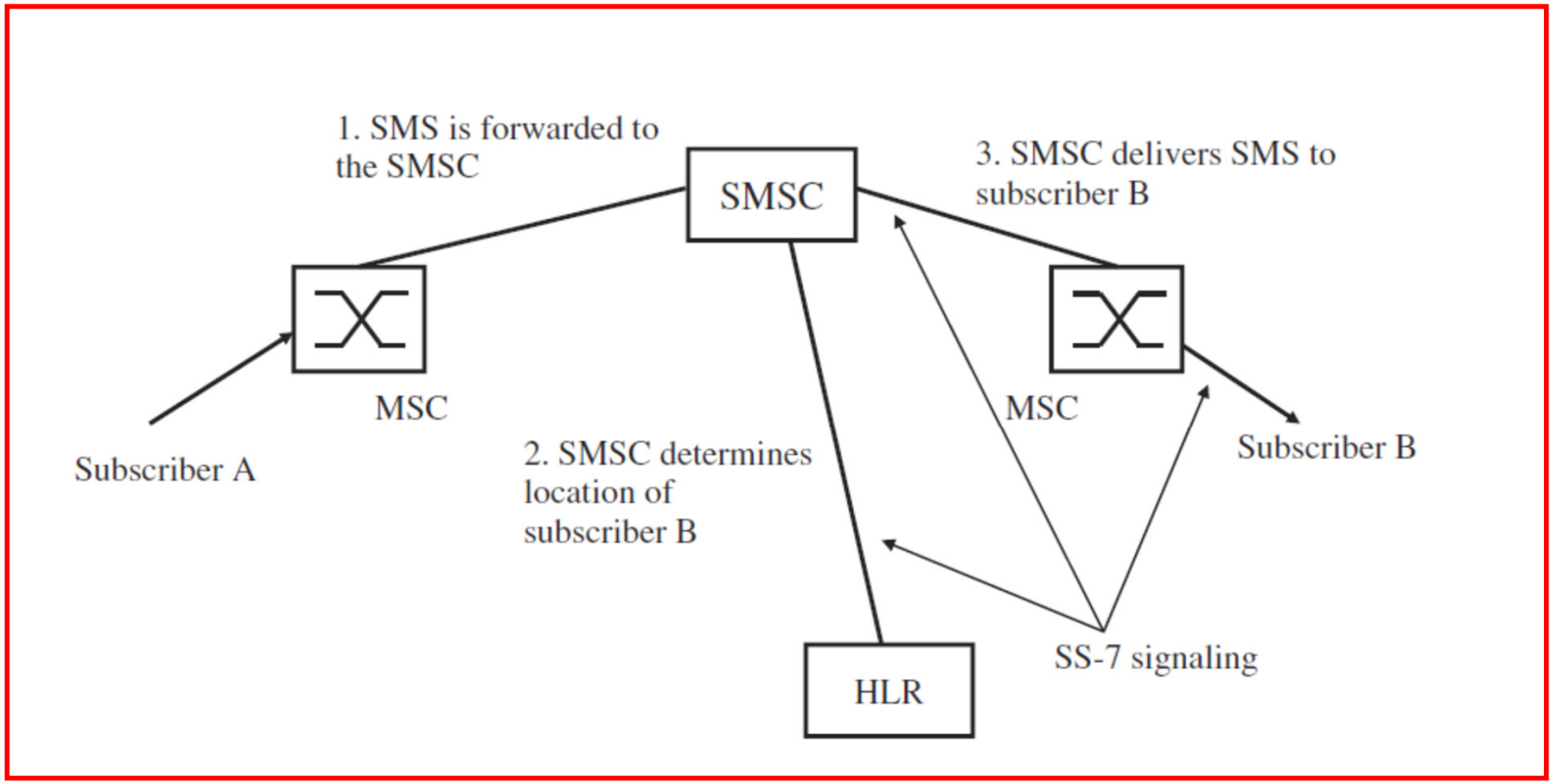
- The verification of the subscriber's record at every connection establishment is necessary, as the record contains information about the services that are active and the services from which the subscriber is barred.
- Since it is costly to get such information on every call from HLR, Each MSC has an associated Visitor Location Register (VLR).
- It holds the record of each subscriber that is currently served by the MSC.
- These records are only a copy of the original records, which are stored in the HLR.
- VLR is simply implemented as a software component in the MSC.

The Visitor Location Register (VLR)

- Data stored include:
  - IMSI.
  - Authentication data.
  - MSISDN.
  - GSM services that the subscriber is allowed to access.
  - Access point (GPRS) subscribed.
  - The HLR address of the subscriber.
  - …

The Short Messaging Service Center (SMSC)

- SMSC is used to store and forward short messages.

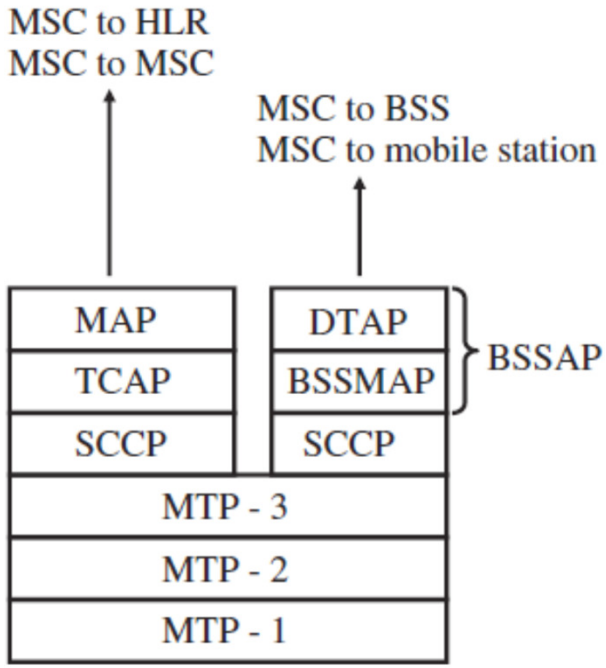


Other Components

- Operation Maintenance Center (OMC)
  - In charge of monitoring all the components of the network, error and failure detection, SLA provisioning.
- Authentication center (AUC)
  - Usually part of HLR.
  - The AUC contains an individual key per subscriber (Ki), which is a copy of the Ki on the SIM card of the subscriber.
- Equipment Identity Register (EIR)
  - Each built cell phone has a unique number called International Mobile Equipment Identity (IMEI).
  - EIR is a database that contains a list of all valid mobile equipment on the network, where IMEI identifies each MS.
  - An IMEI is marked as invalid if it has been reported stolen or is not type approved.

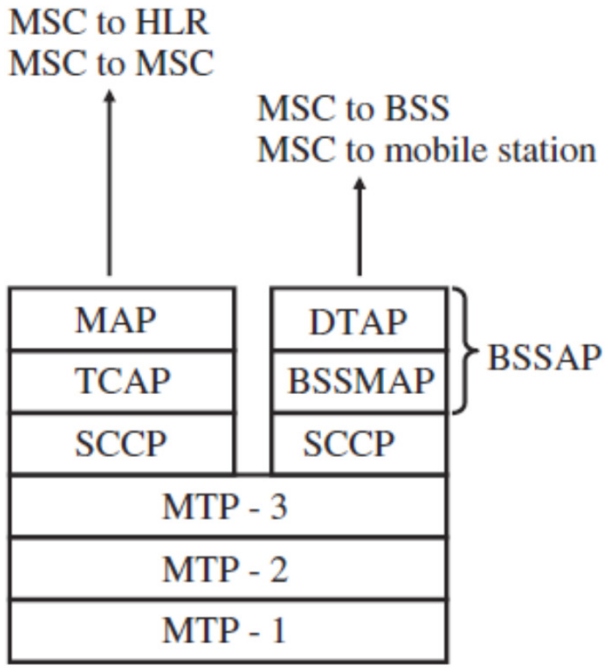
SS-7 Protocols for GSM

- Apart from the fixed-line network SS-7 protocols, the following additional protocols were defined to address the special needs of a GSM network.
  - **The Mobile Application Part (MAP)**: This protocol has been standardized in 3GPP TS 29.002 and is used for the communication between an MSC and the HLR.
  - MAP is also used between two MSCs if the subscriber moves into the coverage area of a different MSC while a call is ongoing.
  - MAP protocol uses the TCAP, SCCP and MTP protocols on lower layers.



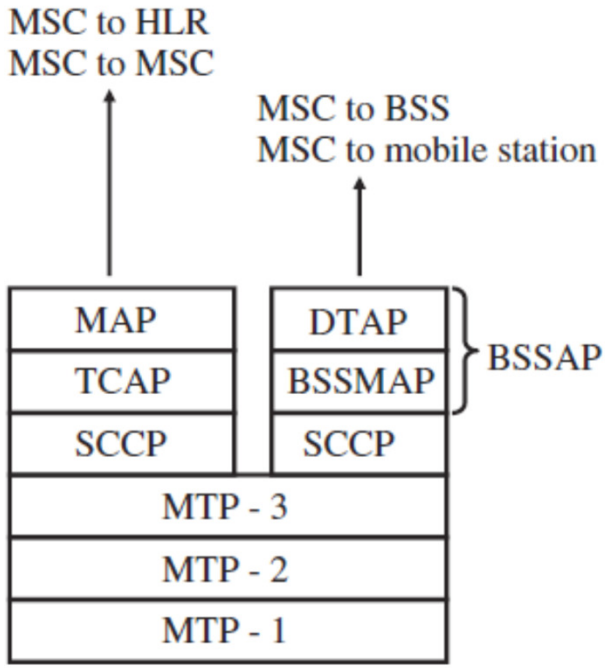
SS-7 Protocols for GSM

- Apart from the fixed-line network SS-7 protocols, the following additional protocols were defined to address the special needs of a GSM network.
  - **The Base Station Subsystem Mobile Application Part (BSSMAP):** This protocol is used for communication between the MSC and the radio network. (for example to establish a dedicated radio channel for a new connection to a mobile subscriber.)
  - As BSSMAP is not a database query language like the MAP protocol, it is based on SCCP directly instead of using TCAP in between.



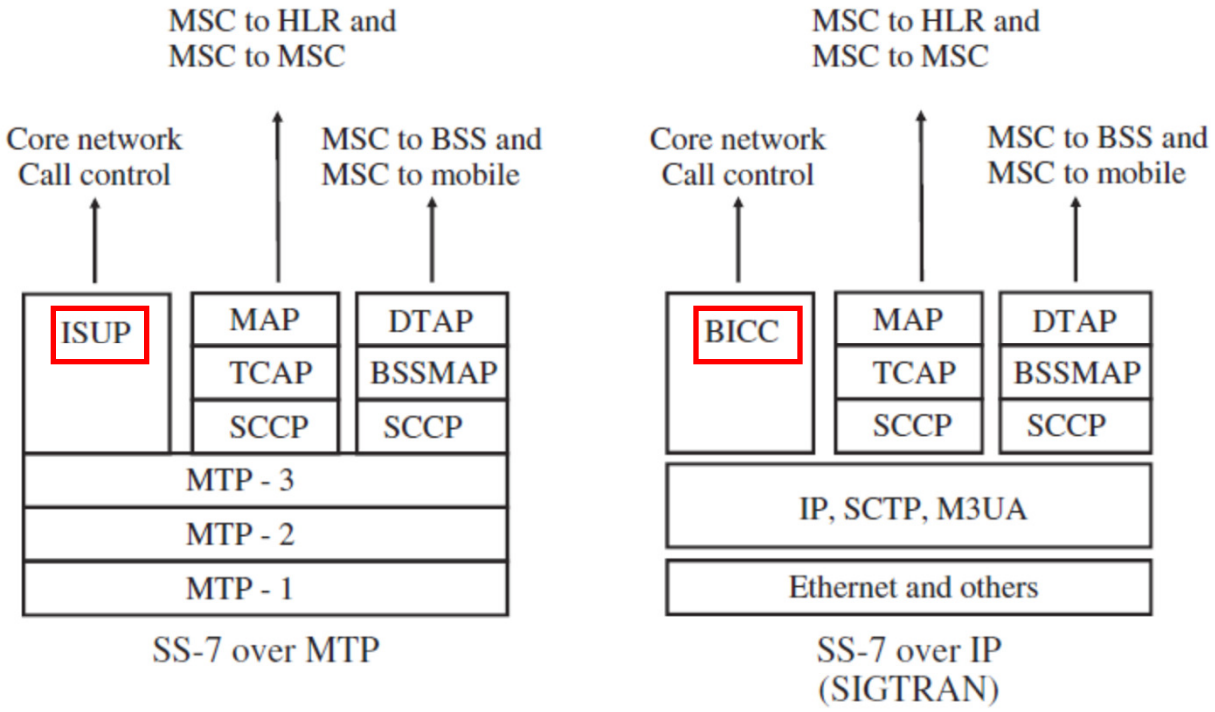
SS-7 Protocols for GSM

- Apart from the fixed-line network SS-7 protocols, the following additional protocols were defined to address the special needs of a GSM network.
  - **The Direct Transfer Application Part (DTAP):** This protocol is used between the user's mobile device and the MSC to communicate transparently such as
    - Call management
    - Mobility management (MM)



IP-Based SS-7 Protocol Stack (sigtran)

- When using an IP network for the transmission of SS-7 signaling messages, the MTP-1 and MTP-2 protocols are replaced by the IP and lower layer protocols.



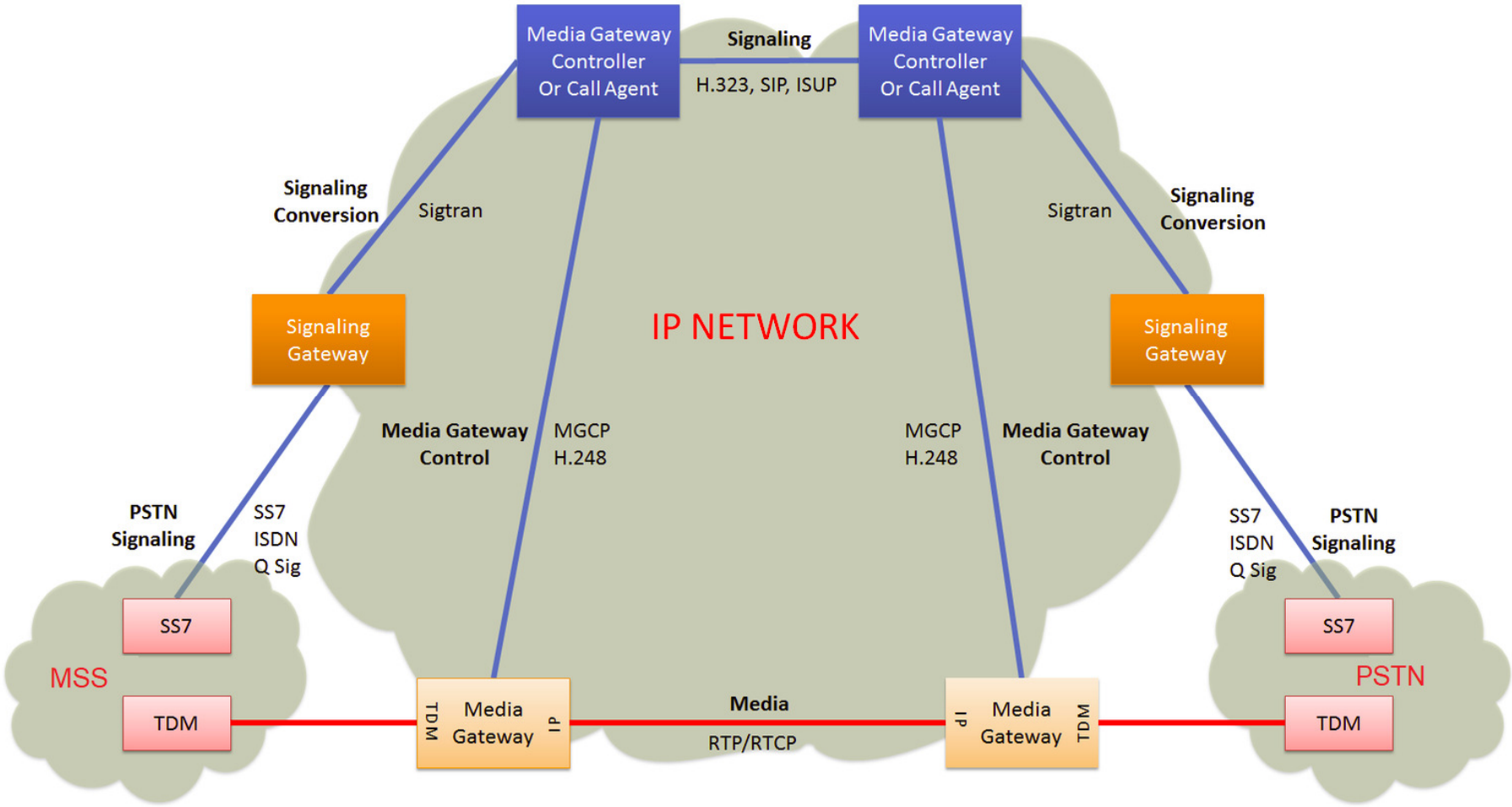
IP-Based SS-7 Protocol Stack (sigtran)

- Signaling Gateways (SGs) have been defined to bridge E-1 based and IP-based SS-7 communication in the signaling domain.
- The SGs adapt the lower layers of the protocol stack and thus make the differences transparent for both sides.
- This is necessary, for example, if the subscriber database has already been converted for IP interfaces while other components such as the switching centers are still using traditional signaling links.
- To bridge voice calls between E-1 based and IP-based networks, Media Gateways (MGs) are used.

IP-Based SS-7 Protocol Stack (sigtran)

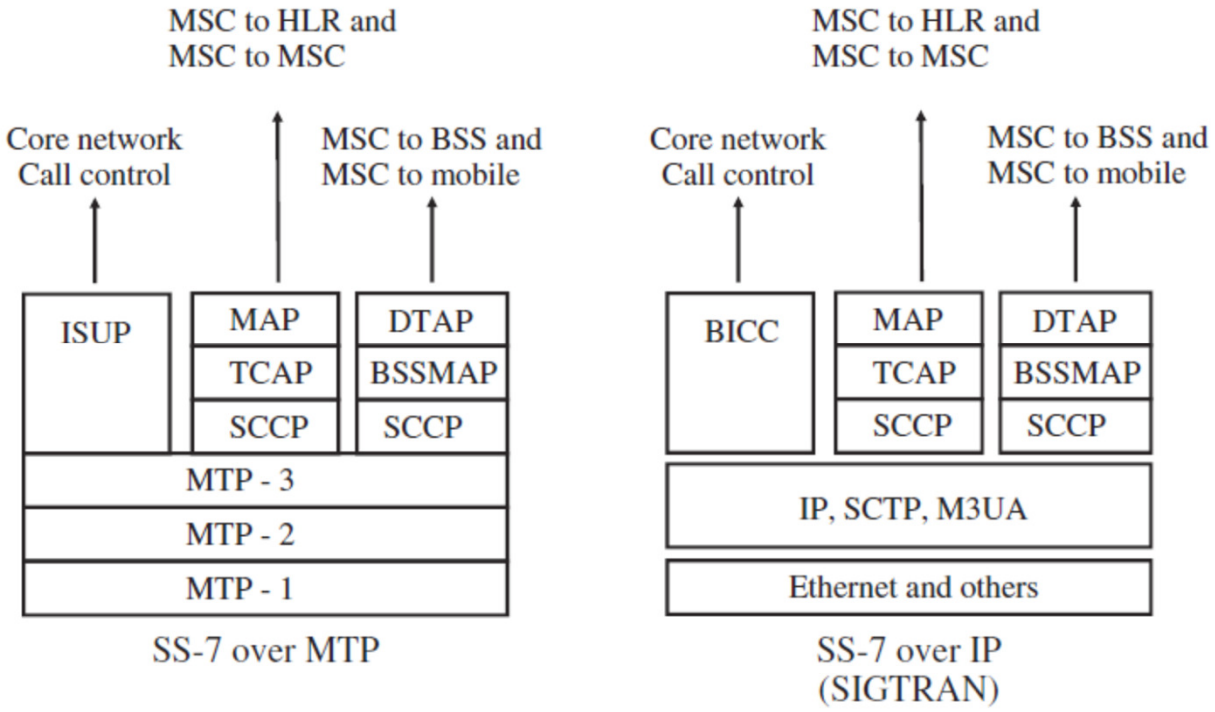
- In a virtual circuit-switched network (softswitch), the MSC is split into two parts: the MSC Server (MSC-S) and the media gateway (MG).
- The IP-based MG replaces the switching matrix while the MSC-S contains the same logic for subscriber management and call control as the central processing as a software.
- MG can handle both IP-based and E-1-based voice calls transparently as it implements both the classic and IP-based signaling protocol stacks.

MSS and MG


Media Gateway Controller Or Call Agent
Signaling
H.323, SIP, ISUP
Media Gateway Controller Or Call Agent
Signaling Conversion
Sigtran
Sigtran
Signaling Conversion
Signaling Gateway
IP NETWORK
Signaling Gateway
Media Gateway Control
MGCP H.248
MGCP H.248
Media Gateway Control
PSTN Signaling
SS7 ISDN Q Sig
SS7 ISDN Q Sig
PSTN Signaling
SS7
SS7
MSS
PSTN
TDM
TDM
Media Gateway
IP
Media
RTP/RTCP
IP
Media Gateway
TDM

IP-Based SS-7 Protocol Stack

- Bearer-Independent Call Control (BICC) protocol, which largely resembles ISUP, replaces ISUP to initiate the calls.
- SIP can be used instead but could not work perfectly!



IP-Based SS-7 Protocol Stack

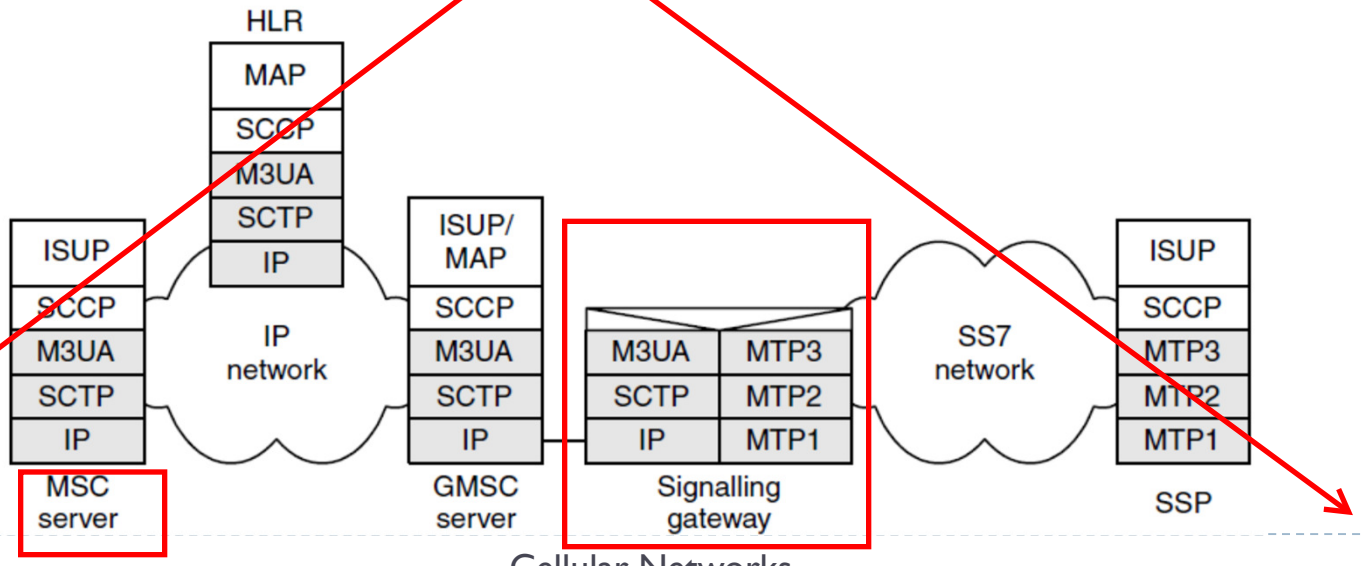
- Bearer-Independent Call Control (BICC) protocol, which largely resembles ISUP, replaces ISUP to initiate the calls.
- SIP can be used instead but could not work perfectly!

Table 8.9 BICC messages

Message	Acronym	Meaning/purpose
Initial address	IAM	Initiates call setup
Application transport	APM	Carries non-BICC information
Address complete	ACM	Indicates all addressing information has been received
Answer	ANM	Called party has answered phone
Release	REL	Request release of bearer
Release confirm	RLC	Confirm release of bearer

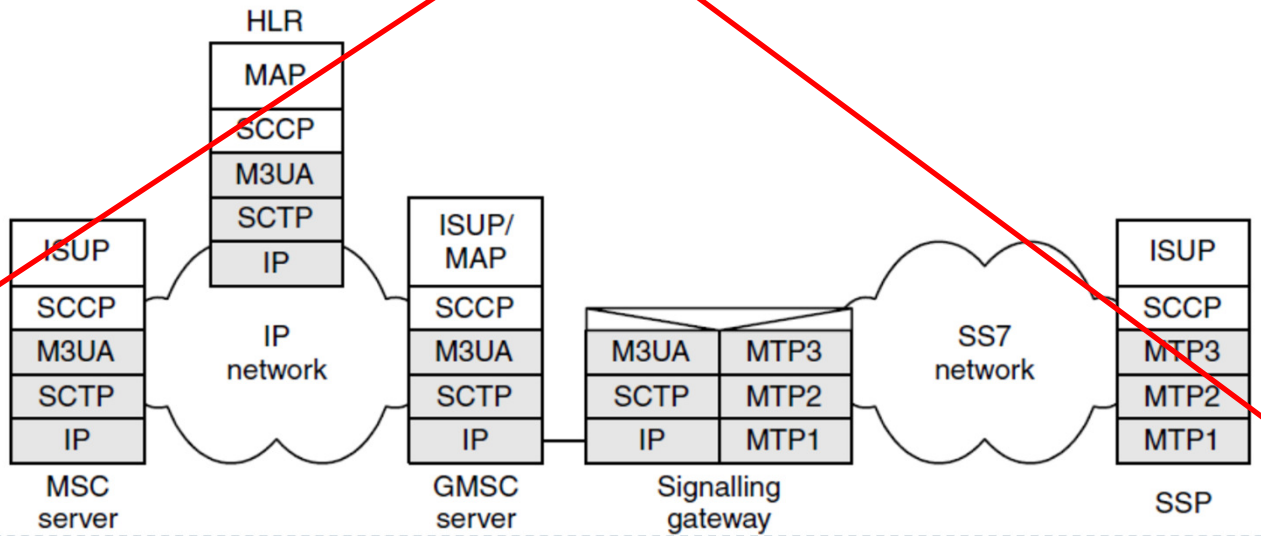
MTP3 user adaptation layer (M3UA)

- This protocol (RFC 3332) allows an SS7 application server residing on an IP network (e.g. MSC server, HLR, etc.) to communicate with entities residing on an SS7 network.
- M3UA also allows SS7 messages to be passed point-to-point between SS7 servers on the IP network.



MTP3 user adaptation layer (M3UA)

- Messages generated at signalling end points on the SS7 network are forwarded via the signalling gateway using the M3UA service to SS7 application servers residing on the IP network.
- The M3UA layer also allows the IP servers to send SS7 messages directly to each other.



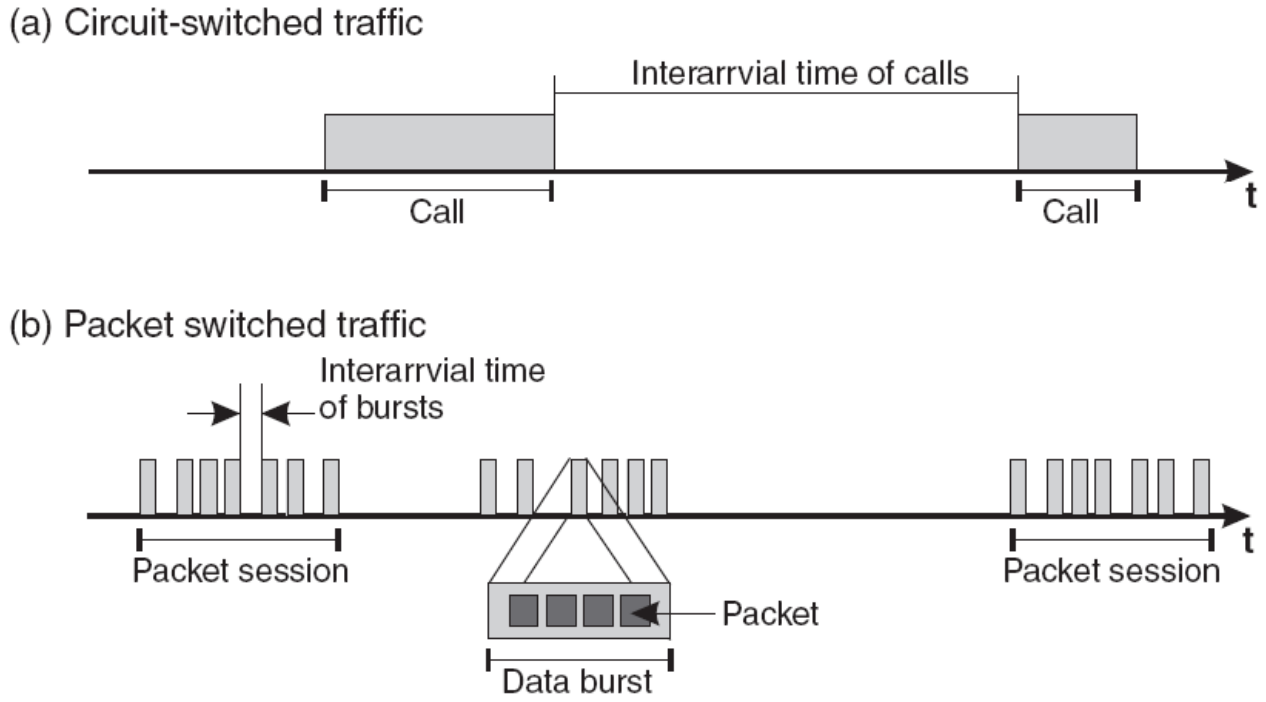
The Intelligent Network Subsystem (IN)

- IN comprises SCP databases that add optional functionality to the network including
  - prepaid service
  - Various call plans
  - Number portability
  - Call queueing
  - Call transfer
- It is a cheaper replacement of IMS.

General Packet Radio Service (GRPS)

Data over GSM Network

- "Packet overlay" network on top of the existing GSM (Digital) circuit switched voice-based network.



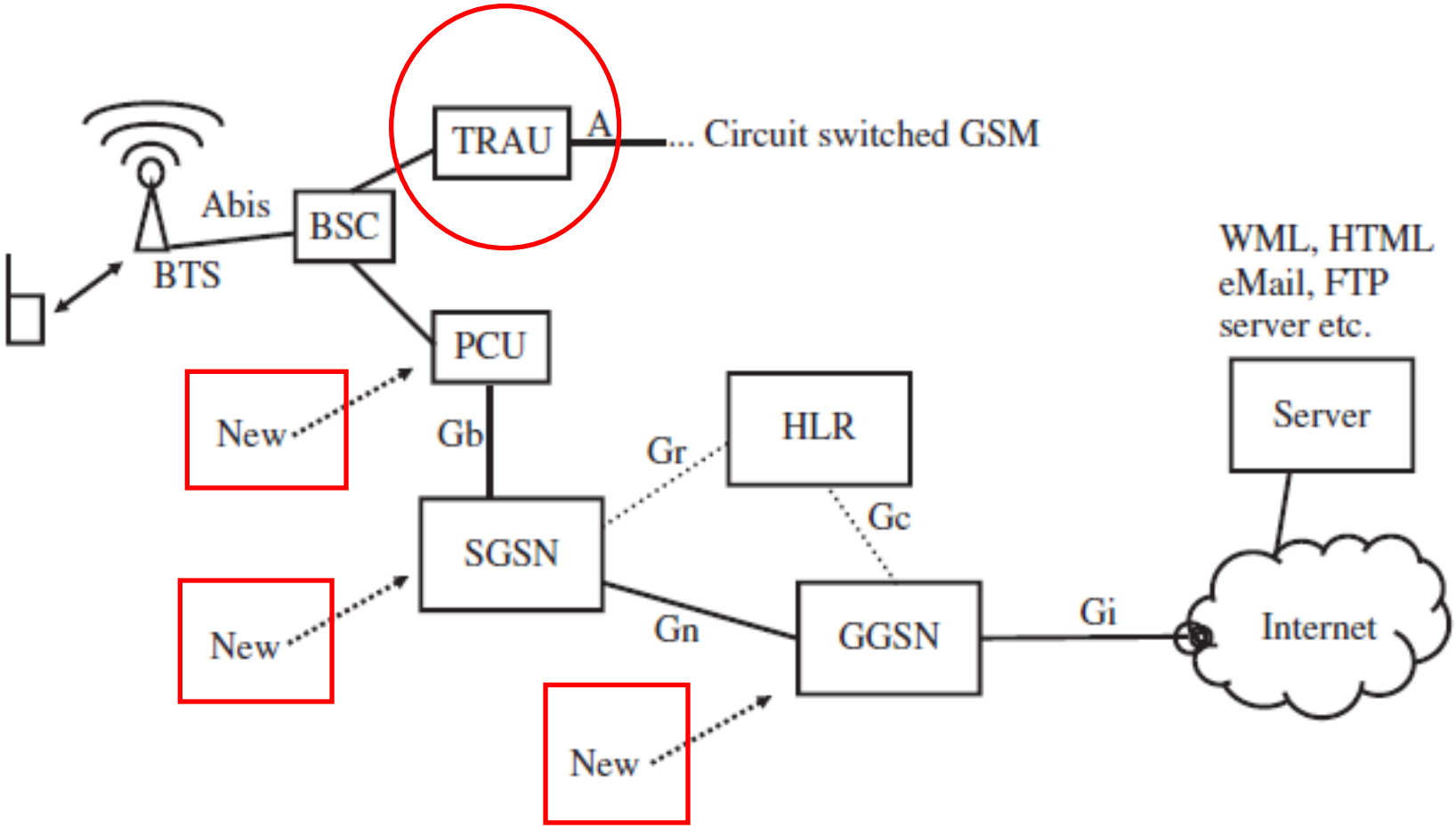
Data over GSM Network

- TCH channels can be allocated for data as well as seen in GSM. End-to-end circuit switching (Dial-up service).
- Benefits of using voice channel for data:
  - No need to new protocol
  - may not need headers
  - Constant delay
  - Fixed bandwidth
- Drawback: slow rates (13 or 9.6 kbps)

Revised GSM

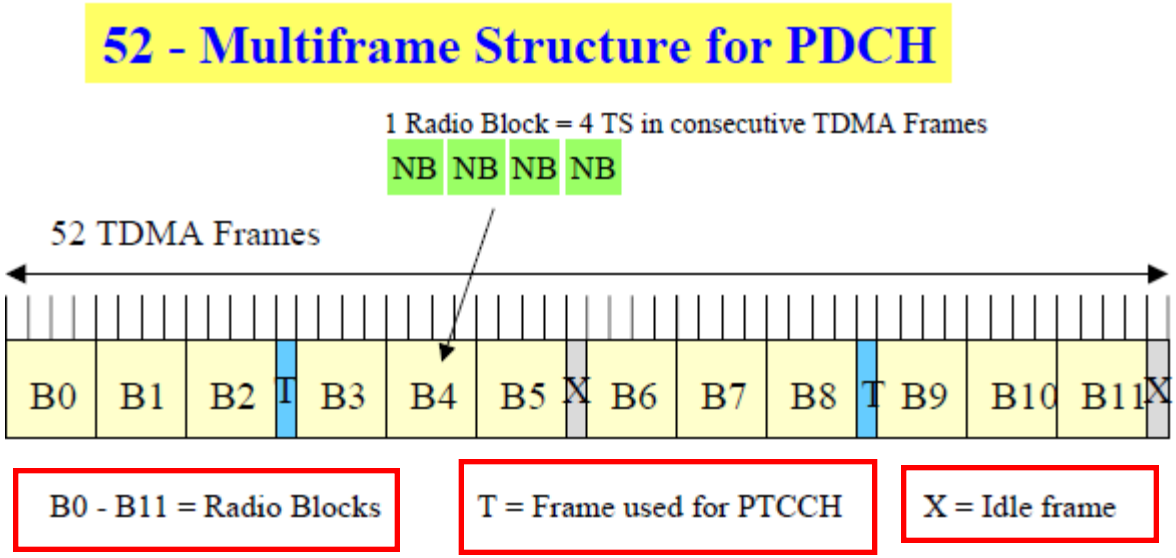
- To achieve higher rates, revision to core and access is made.
- What remains the same:
  - All the existing interfaces and devices
  - All the protocols used for voice traffic
- What is new
  - New logical channels are added to support data traffic.
  - Dynamic resource allocation is provided for data logical channels.
  - New core devices are added to control and switch the data traffic.
- General Packet Radio Service (GPRS) is a packet oriented mobile data service on the 2G and 3G cellular communication system's global system for mobile communications (GSM).
- Proposed by ETSI and now maintained by 3GPP.

Add-on Network Components to GSM

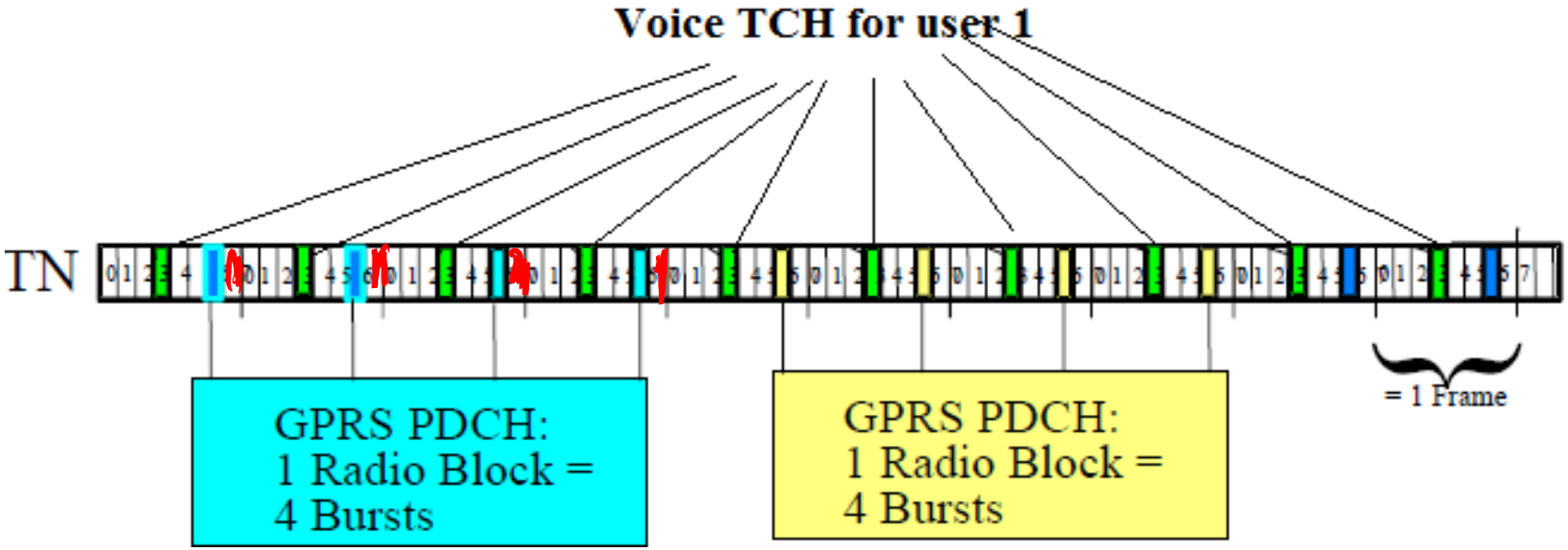


GPRS Air Interface

- GPRS uses a 52-multiframe structure.
  - Frames 24 and 51 used to allow the mobile device to perform signal strength measurements on neighboring cells.
  - Frames 12 and 38 are used for timing advance calculations
- The smallest unit that can be assigned is a block that consists of four bursts of a packet data traffic channel (PDTCH).



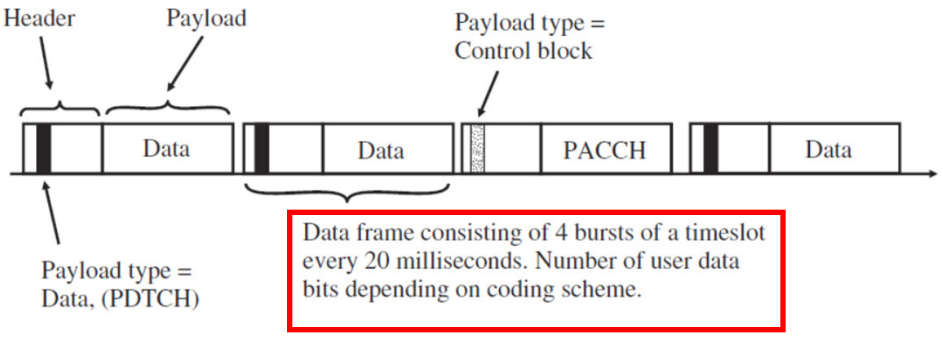
Voice vs. Data Logical Channel



- **Timeslot Aggregation**
  - To increase the transmission speed, a subscriber is no longer bound to a single TCH as in circuit-switched GSM.
  - If more than one timeslot is available when a subscriber wants to transmit or receive data, the network can allocate several timeslots (multislot) to a single subscriber.
  - Depending on the multislot class of the mobile device, three, four or even five timeslots can be aggregated for a subscriber at the same time.

New Logical Channels

- Packet Associated
  - The Packet Data Traffic Channel (PDTCH):
    - bidirectional data channel
    - Assigned by the radio resource manager in blocks of 4 bursts.
  - The Packet-Associated Control Channel (PACCH)
    - Bidirectional control channel
    - Convey acknowledgement or resource management signaling.
    - Share the same physical resources with PDTCH.
    - To distinguish between PACCH and PDTCH, a bit in the header determines the type of the packet.



New Logical Channels

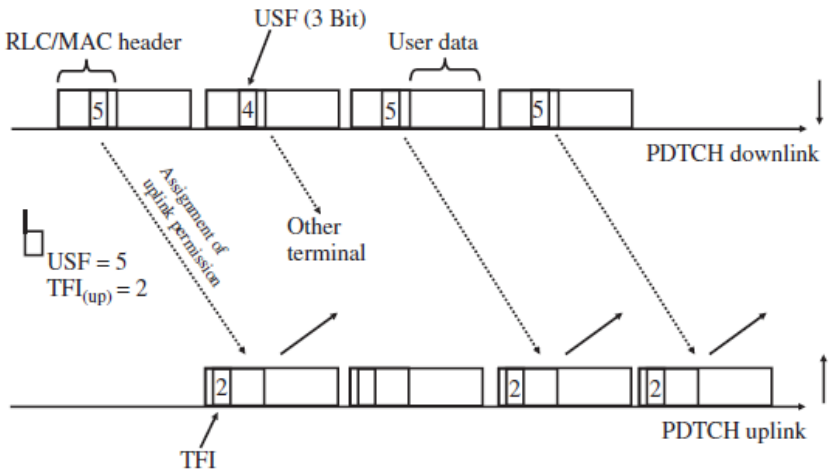
- Packet Associated
  - Packet Timing Advance Control Channel (PTCCH)
    - Used for timing advance estimation in both directions.
    - Frames 12 and 38 of the packet multiframe.
- Packet Common Control Channel (PCCCH)
  - The packet random access channel (PRACH),
  - Packet Paging Channel (PPCH)
  - Packet Access Grant Channel (PAGCH).
- PCCCH channels can be physically shared by PDTCH or they can be separated.
- A PDTCH that contains PCCCH is indicated on BCCH.
- On the downlink of this PDCH, the first block (B0) in the ordered list of blocks is used as PBCCH which indicates the location of PCCCH channels.
- On a PDCH that does not contain PCCCH, all blocks can be used as PDTCH or PACCH. The actual usage is indicated by the message type.

Dynamic Radio Resource Managements on PDTCH

- Temporary Block Flows (TBF) in the Uplink Direction
  - The smallest transmission unit that is assigned to a user is one block consisting of four bursts.
  - After paging, BTS announces the blocks a user can use.
  - Such time slots are shared however ! Up to eight mobiles can have potential access to a slot, but obviously only one can transmit at any given time.
  - To know when it can use the uplink timeslots, the mobile device has to listen to all the timeslots it has been assigned in the downlink direction.
  - Each device has two IDs associated:
    - Uplink state flag (USF): ID the device is known for.
    - Temporary flow identity (TFI): ID the device makes itself known to BTS

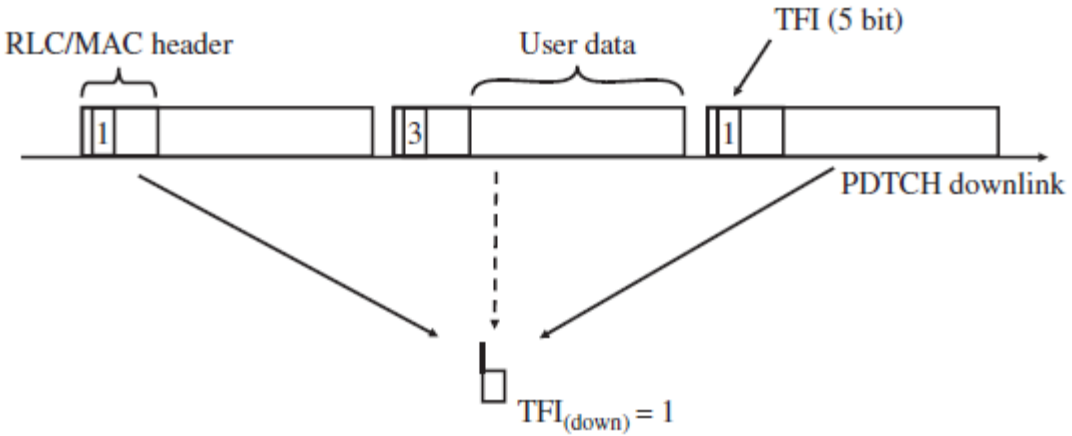
Dynamic Radio Resource Managements on PDTCH

- Every block sent in the downlink to a subscriber contains an uplink state flag (USF) in its header.
- It indicates who is allowed to send in the next uplink block.
- Note that the USF information in the header and data portion of a downlink block is usually not intended for the same user.
- The device informs the resource manager if it does not need any more uplink channels by setting a parameter in its header (count -down).
- It makes a connection too slow. Solution, keep uplink channels open till standby timer expires.



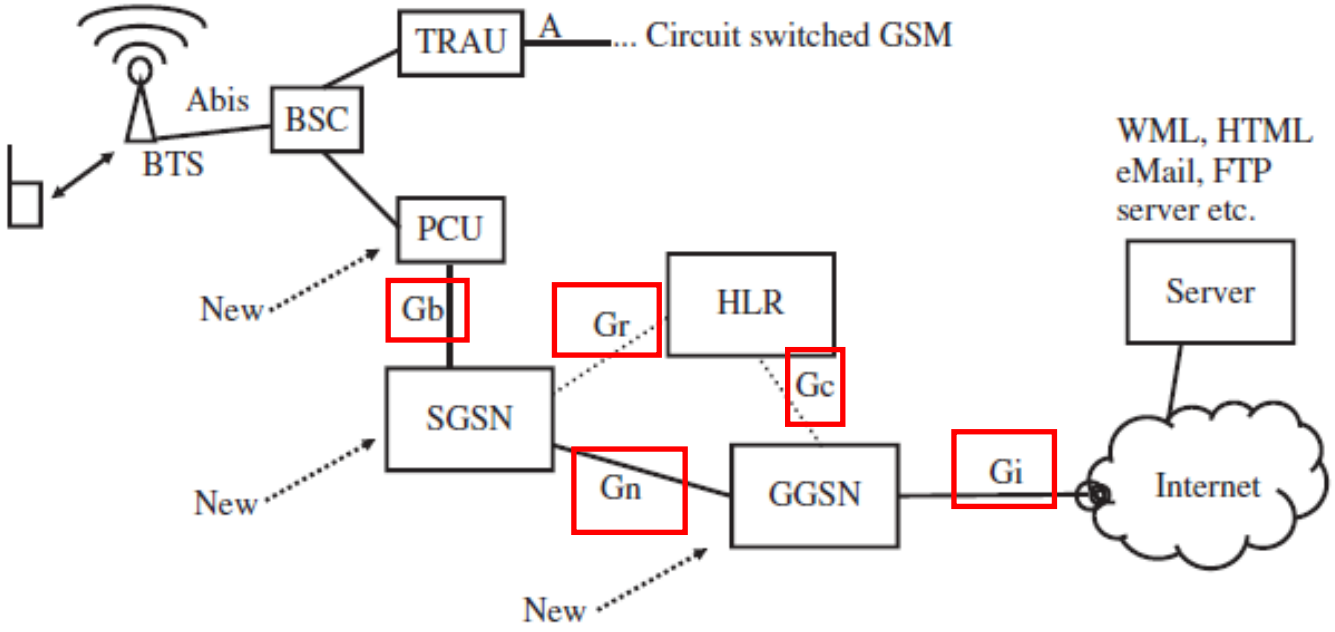
Dynamic Radio Resource Managements on PDTCH

- Temporary Block Flows in the Downlink Direction
  - If the PCU receives data for a subscriber from the SGSN, it will send a packet downlink assignment message to the mobile device in the Packet Paging Channel.
  - The message contains a TFI and the timeslots the mobile device has to monitor.
  - As the downlink is down, the PCU will set the 'final block indicator' bit in the last block it sends to the mobile device.
  - To acknowledge blocks, the device send control information via PACCH.
  - The network informs in the header of the downlink blocks the PACCH channel.



GPRS New Core Components

- Packet Control Unit
- Serving GSN (SGSN)
- Gateway GSN (GGSN)



The Packet Control Unit (PCU)

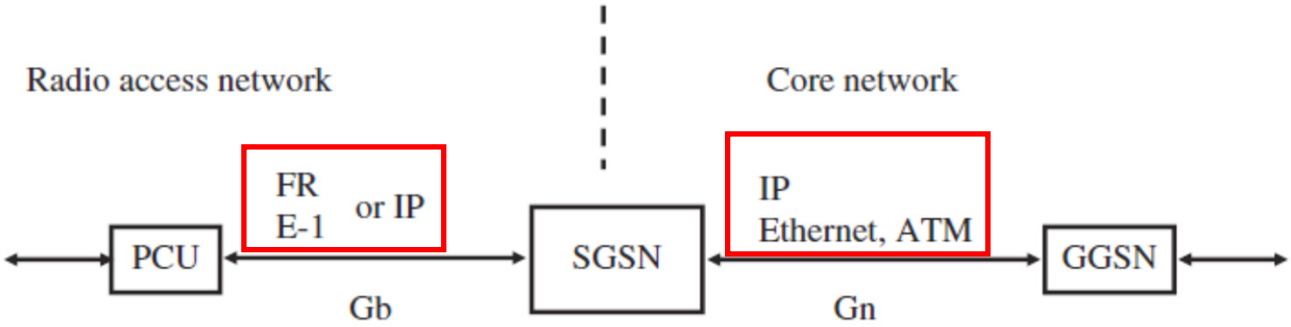
- The PCU is the packet-switched counterpart of the BSC and fulfills the following tasks:
  - Assignment of timeslots to subscribers in the uplink direction when requested for by the mobile device via the RACH or the PRACH;
  - Assignment of timeslots to subscribers in the downlink direction for data arriving from the core network;
  - Flow control of data in the uplink and downlink directions and prioritization of traffic;
  - Error checking and retransmission of lost or faulty frames;
  - Subscriber paging;
  - Supervising entity for subscriber timing advance during data transmission.

The Packet Control Unit (PCU)

- The BSC turns over control for some of the timeslots to the PCU.
- This is done by redirecting timeslots in the BSC switching matrix away from the MSC and TRAU toward the PCU.
- The BSC then simply forwards all data contained in these timeslots to and from the PCU without any processing.
- When the mobile device requests for GPRS resources, the BSC receives a channel request message for packet access.
- The BSC forwards such packet access request messages straight to the PCU without further processing.
- It is then the PCU's task to assign uplink blocks on a PDTCH and return an immediate packet assignment command, which contains a packet uplink assignment for the subscriber.

Serving GPRS Support Node (SGSN)

- The packet-switched counterpart to the MSC in the circuit-switched core network.
- It has two planes:
  - User plane management
  - Signaling plane management
- IP is used as the transport protocol in the GPRS core network between the SGSN and GGSN.



Serving GPRS Support Node (SGSN)

- To connect the SGSN with the PCU, the frame relay protocol was selected not IP which is not known today.
- ATM and IP are replaced frame relay in 3G.
- To be able to exchange data with the Internet, it is necessary to establish a data session with the GPRS network.
- This procedure is called Packet Data Protocol (PDP) context activation and is part of the session management (SM) tasks of the SGSN.
- SGSN provide mobility of IP done by GPRS mobility management (GMM) sublayer.

Serving GPRS Support Node (SGSN)

- Although ciphering for circuit-switched traffic is terminated in the BTS, ciphering for packet-switched traffic is terminated in the SGSN.
- To charge the subscriber for usage of the GPRS network, the SGSN and the GGSN, collect billing information in so-called call detail records (CDRs) forwarded to the billing server.

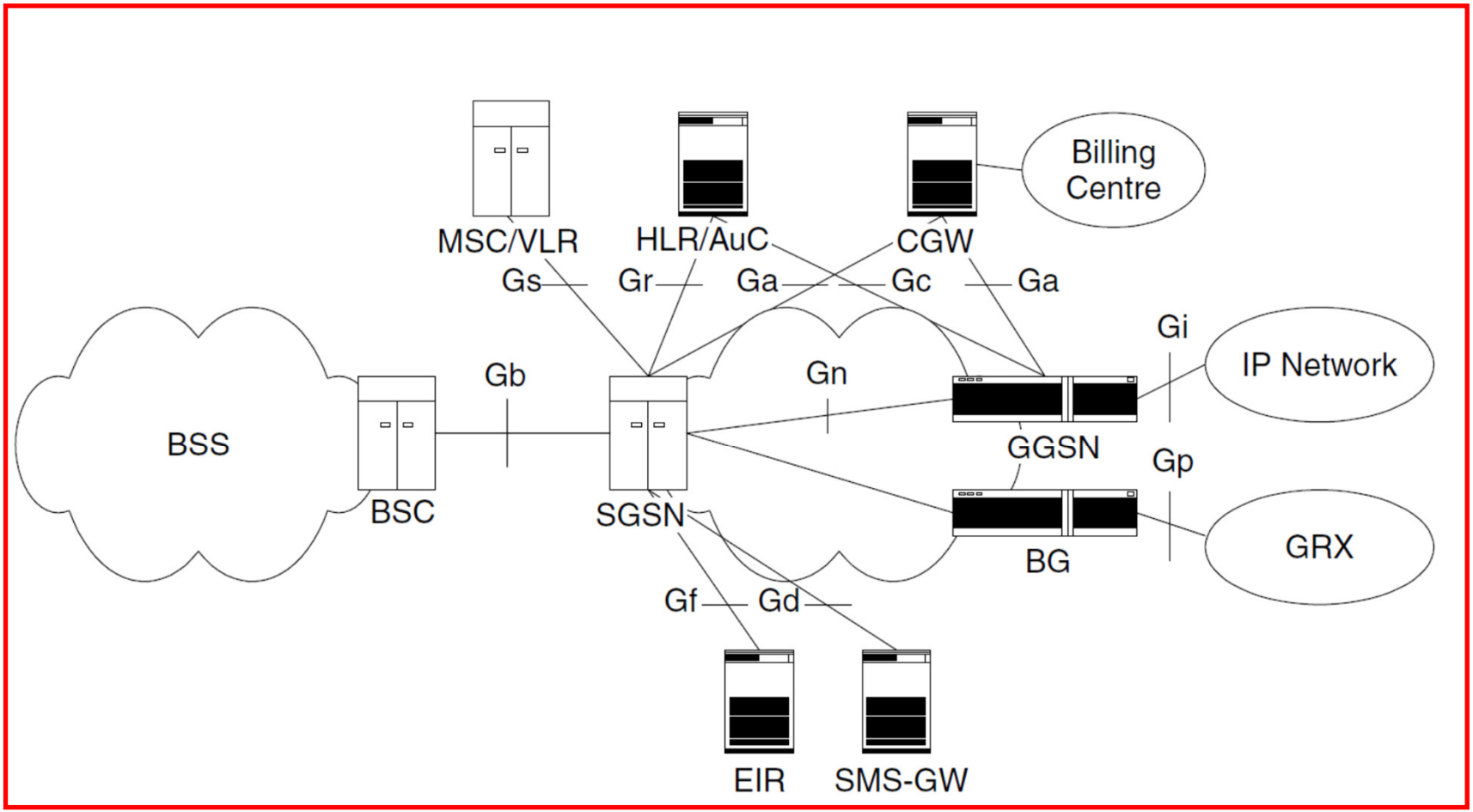
Gateway GPRS Support Node (GGSN)

- GGSN connects the GPRS network to the external data network.
- GGSN is responsible for assigning a dynamic or static IP address to the user.
- It also provides feature for mobile IP.
- GGSN supports mobility using tunnels.

Other components

- Charging gateway (CG):
  - CG is not required in the specifications but is generally implemented since it takes processing load off the SGSN and GGSN. It also introduces a single logical link to the operator's billing system and reduces the number of physical links and connections for billing system.
- Lawful interception gateway (LIG):
  - It is a requirement in many countries for the law enforcement agencies (LEA) to be able to monitor traffic.
- Border gateway (BG)
  - A border gateway (BG) is used as the gateway to a backbone connecting different network operators together. This backbone is referred to as an inter-PLMN backbone, or global roaming exchange (GRX).
  - The BG is essentially an IP router and is generally implemented as the same hardware platform as the GGSN.

Core Interfaces



Enhanced Data rates for GSM Evolution (EDGE)

- To further increase data transmission speeds, a new modulation and coding scheme, which uses 8 PSK (8 Phase Shift Keying), has been introduced into the standards.
- Together with the highest of the nine new coding schemes introduced with EDGE, it is possible to transfer up to 60 kbit/s per timeslot.

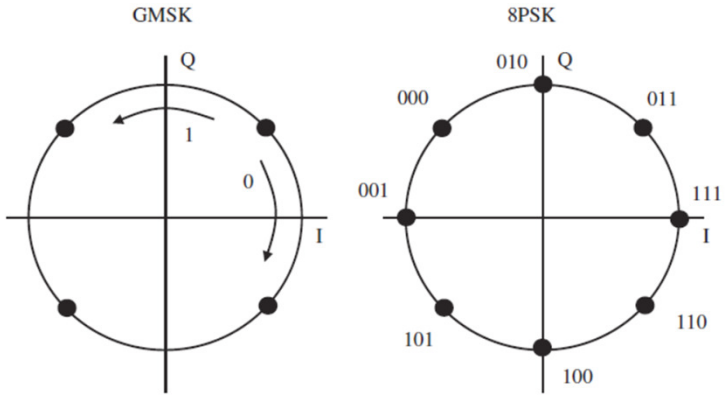


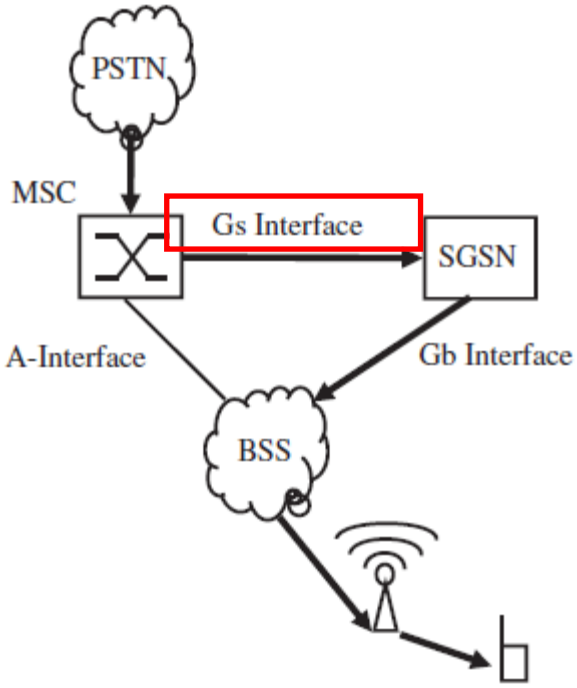
Figure 2.8 GMSK (GPRS) and 8PSK (EDGE) modulation.

Mobile Device Classes

- Class C:
  - Can only be attached to GPRS or GSM at a time.
- Class B
  - They can be attached to both GPRS and GSM at the same time but GPRS and GSM cannot be active at the same time.
- Class A:
  - Can be active on both networks.

Network Operation Mode (NOM)

- NOM 1:
  - Signaling for packet- and circuit-switched data is done either via the GSM PCH or the GPRS Packet Paging Channel (PPCH).
  - Incoming voice calls may be missed by the class B devices during an active data transfer.
  - To avoid that, an interface between the circuit-switched part (MSC) and the packet-switched part (SGSN) of the network is used.
  - This interface is called the Gs interface.

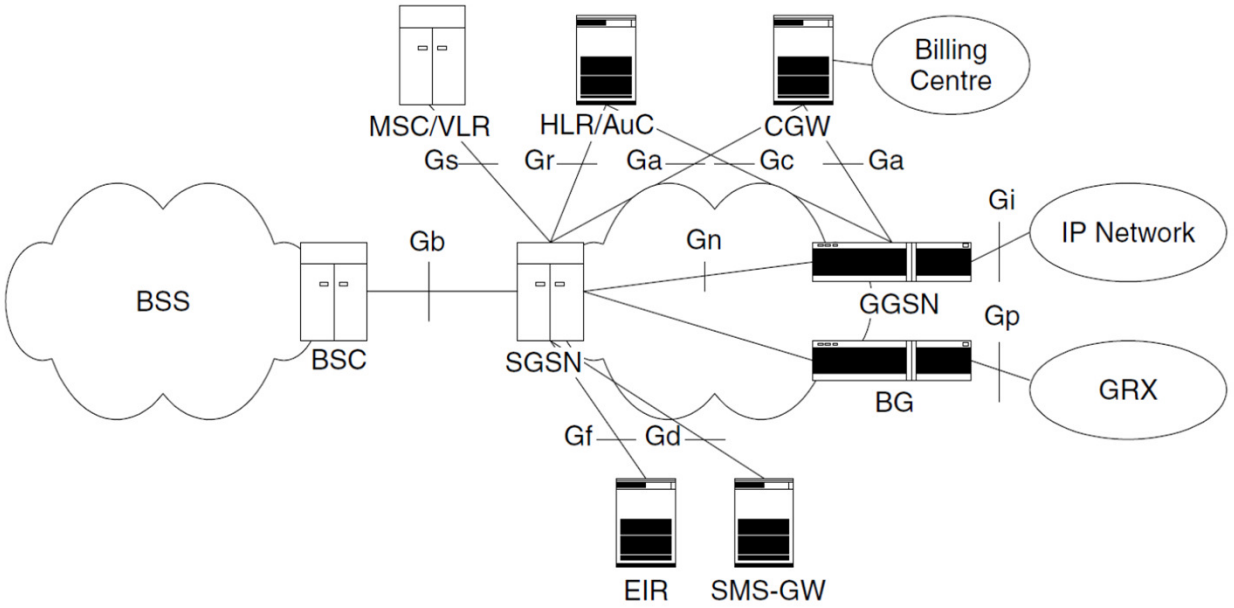


Network Operation Mode (NOM)

- NOM II:
  - The simplest of the network mode.
  - No interface between switched-packet parts.
  - You simply miss your call while surfing !
  - GPRS network informs its mode using BCCH.
- NOM III:
  - In this mode, the Gs interface is not available and the circuit-switched paging has to be done over the PCH.
  - In this mode, the GPRS common control channel with its subchannels PPCH, PRACH and PAGCH is available and the packet-switched side performs its signaling via its own channels.

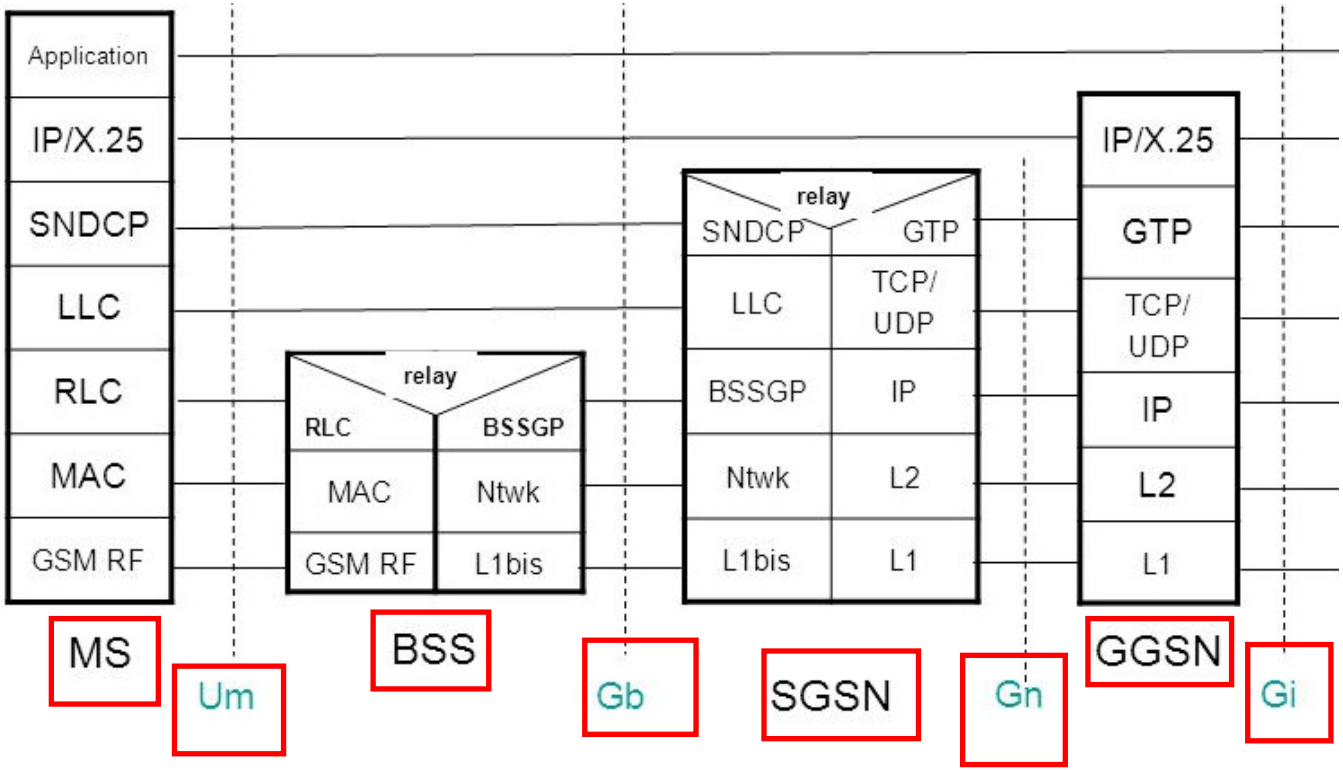
GPRS Interfaces

- The GPRS standards define a number of interfaces between components.
- Apart from the PCU, which has to be from the same manufacturer as the BSC, all other components can be selected freely.



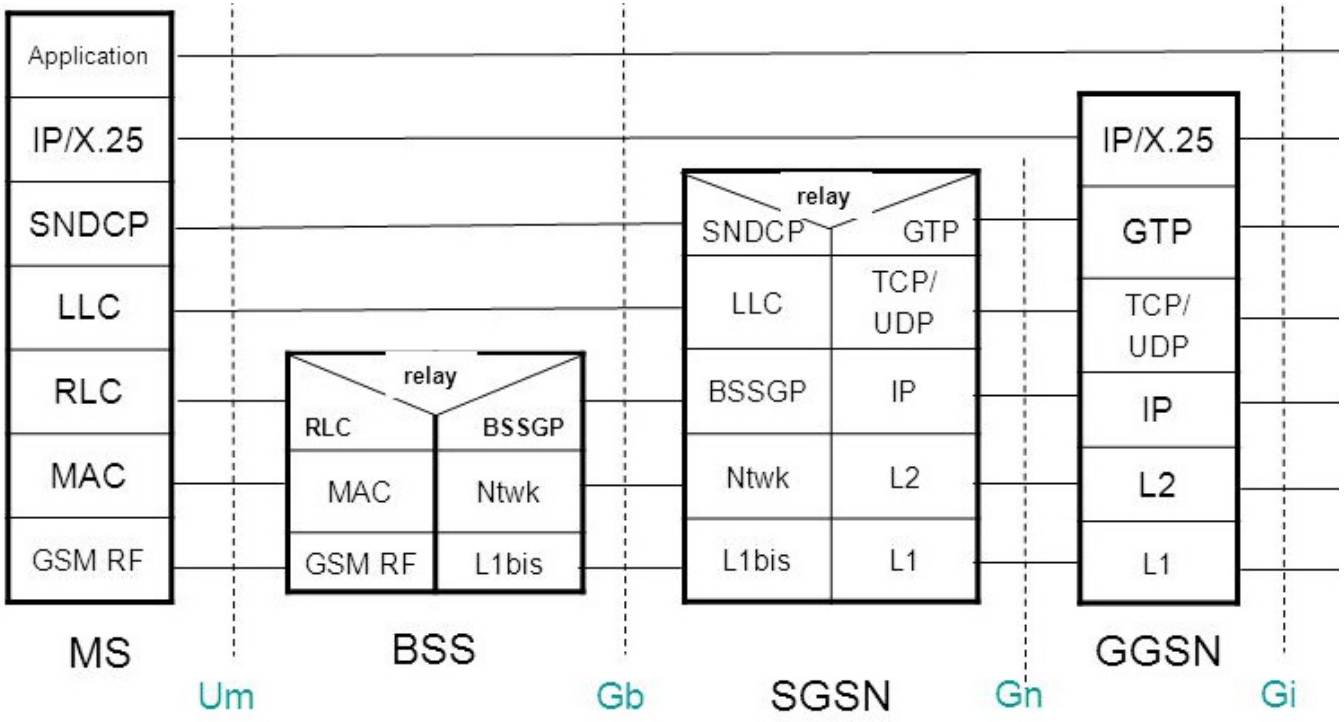
GPRS Interfaces

- Various protocols are involved in the interaction of GPRS components.
- The Logical Link Control (LLC) protocol is responsible for the framing of the user data packets and signaling messages of the mobility management and session management subsystems of the SGSN.



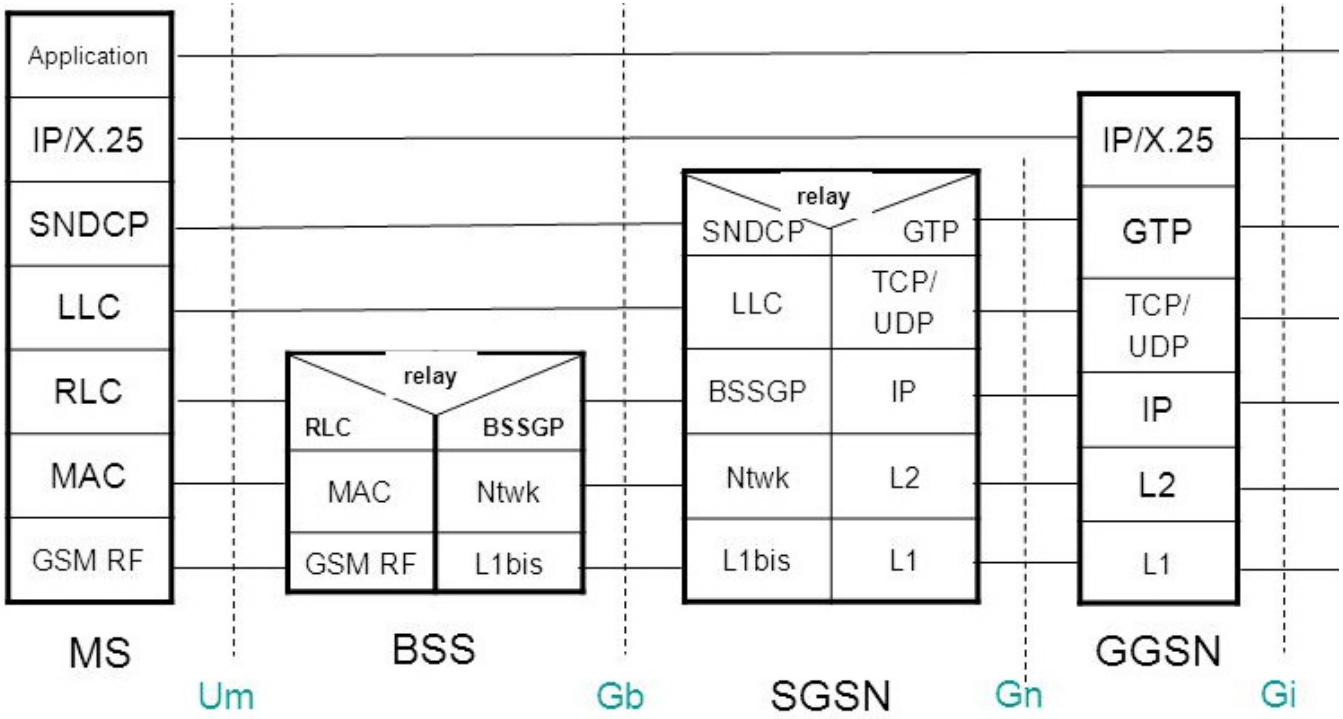
GPRS Interface

- Optionally, the LLC protocol can also ensure a reliable connection between the mobile device and the SGSN by using an acknowledgment mechanism for the correctly received blocks (acknowledged mode).



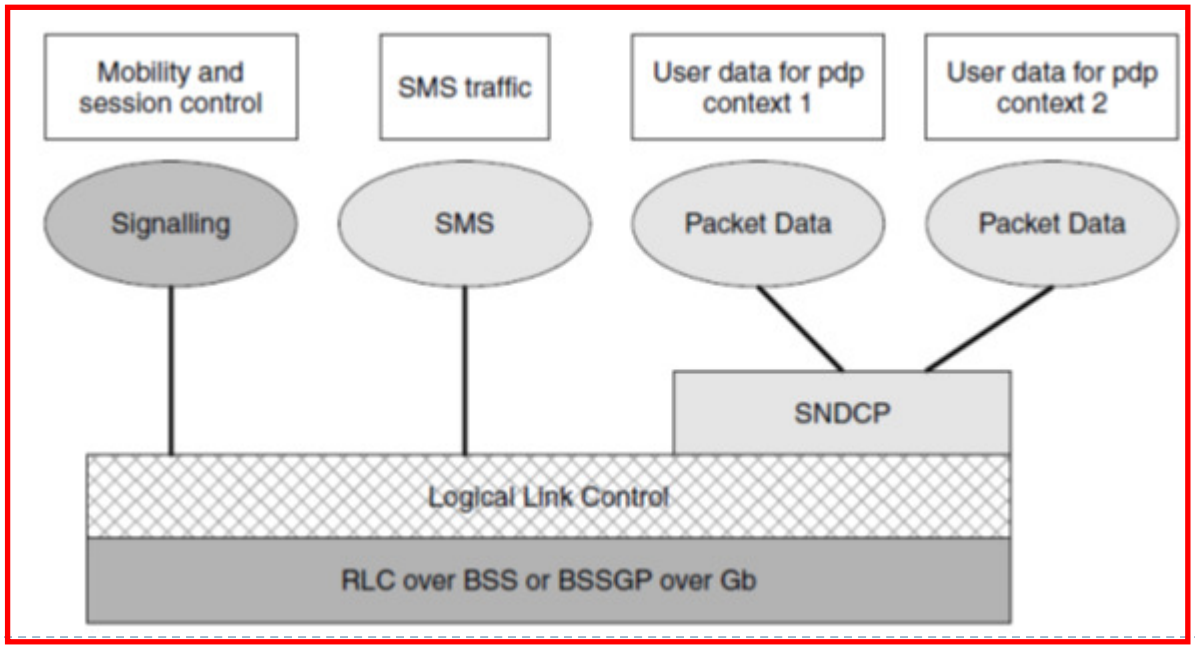
Subnetwork-Dependent Convergence Protocol (SNDCP)

- The Subnetwork-Dependent Convergence Protocol (SNDCP) is responsible for framing IP user data to send it over the radio network.
- The LLC layer and all layers above are transparent for the PCU, BSC and BTS as they are terminated in the SGSN and the mobile device, respectively.



Subnetwork-Dependent Convergence Protocol (SNDCP)

- The SNDCP is only used in the user plane to indicate a specific PDP context and not used by the mobility and session management.
- A subscriber may have a number of PDP contexts open
- The main functions of the SNDCP layer are to provide:
  - multiplexing of PDPs;
  - compression of user data (including IP header compression);
  - segmentation of data packets to be passed to the LLC layer.



BSSGP

- Base Station System GPRS Protocol (BSSGP) transfers information between SGSN and BSS over a BSSGP Virtual Connection (BVC).
- Each BVC has a unique Id which shows the connection between SGSN and a cell supporting GPRS.
- BSSGP is used to transport both control and user data over the Gb interface.

BSSGP

- The primary function of this layer is to introduce and provide the required QoS for the user as well as routing information between the BSS and the SGSN.
- Fragmentation and flow control (leaky bucket) are other tasks of BSSGP.
- The BVCI is used within the SGSN for routing and QoS support purposes.
- SGSN is responsible for processing incoming GTP packets from the GGSN and converting them into a BSSGP frame for transmission to the correct PCU and vice versa.

Gc and Gr Interface

Gc Interface

- This interface connects the GGSN with the HLR.
- It is optional and is thus not widely used in networks today.
- There is one scenario, for which this interface is used:
  - A mobile device, such as a wireless measurement device, offers services to clients on the Internet

Gr Interface

- This interface connects the SGSN with the HLR.
  - GPRS service admission on a per user (international mobile subscriber identity, IMSI) basis
  - GPRS services that a user is allowed to use (APN).
  - GPRS international roaming permissions and restrictions.