

Mobile Communications

Data Services and General Packet Radio System

3. Data Services and General Packet Radio System

3.1 Data services: new requirements and features

3.2 GPRS services

3.3 Radio transmission and Radio Resource Management

 **3.4 Core Network and IP**

3.5 WLAN – technology and service configurations

3 Data services and General Packet Radio System

3.4 Core Network and IP

architecture and mobility management
security
protocols and session management
integration with IP

extensions:



LLC and SNDCP protocols

2

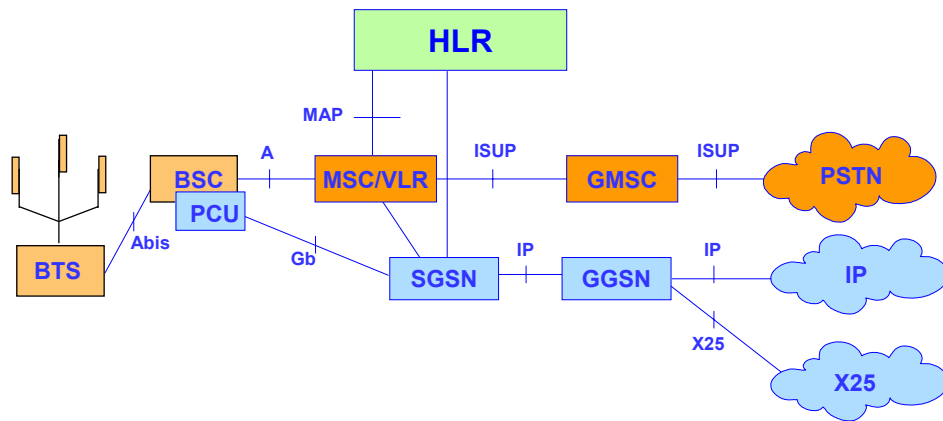
 TELECOM LAB
ITALIA

The section agenda. First, the GPRS architecture is described. Then, the tree basic (layer 3) functional aspects are described:

- mobility management
- security
- data session management.

The level of integration with IP are then discussed.

Network architecture GSM and GPRS



3

TELECOM LAB
ITALIA

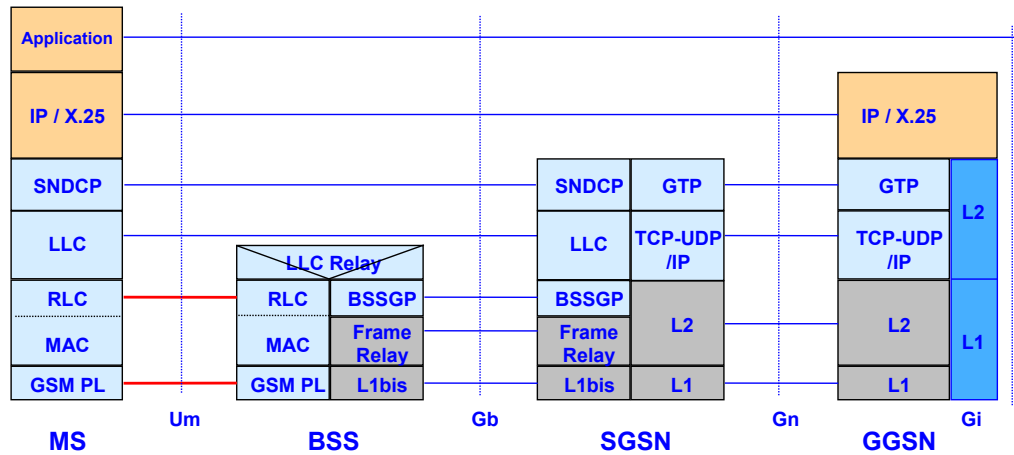
As seen in the service session, the GPRS behaves as a transparent channel between the terminal and the network. In this communication, the GPRS acts as a *default gateway*: the same role played by an *Intranet* or a *Local Area Network* towards the external networks.

The GPRS introduces in the neytwork three new entities:

- The *Packet Control Unit* in charge of:
 - managing the radio channels and making the relevant flows compatible with the core network formats
 - form the system information, including those related to the power control and the congestion control
- The *Service GPRS Support Node* playing a role similar to that of the MSC in a packet-switching context:
 - mobility and routine management
 - security control (ciphering and authentication)
 - counting for charging.
- The *Gateway GPRS Support Node* active in the phases:
 - routing and data transfer between mobile and data networks
 - *session management*
 - *security (firewall)*.

Within the *Core Network* il GPRS the IP protocol is extensively used.

Basic GPRS protocols



4

TELECOM LAB
ITALIA

The GPRS protocol stack denotes the extensive use of the IP protocol in the upper hierarchical levels. In the access segment packet routing towards the Gb interface (BSS) is done through the *BSSGPRS protocol* (BSSGP).

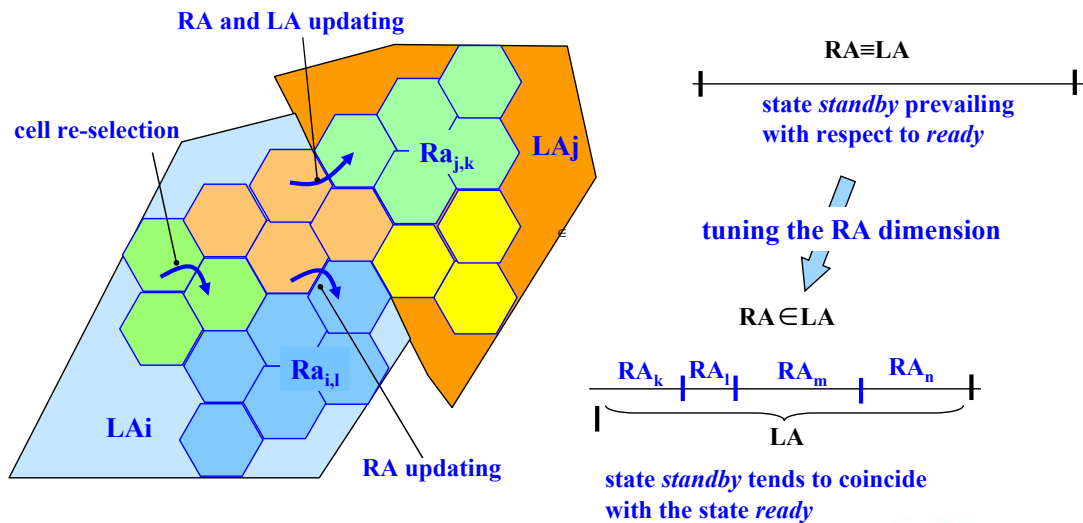
Within the radio access interface Um:

- the physical layer GSM PL supplies the physical channels between MS and the network
- the Medium Access Control (MAC) controls the adaptation and multiplexing functions
- the Radio Link Control (RLC) realises the protection and retransmission mechanisms.

Between the SGSN and the GGSN, the lower IP protocol multiplexes and transports the IP and X25 flows.

The *GPRS Tunnelling Protocol* (GTP) manages the mobility between the SGSNs through *tunnelling* schemes.

Location Area and Routing Area



5

TELECOM LAB
ITALIA

The GPRS introduces the *Routing Area* concept which is equivalent to the GSM *Location Area*. Each *Routing Area* is a set of cells belonging to a single LA. Also RAs are then covering the entire service area, just according to a different granularity.

The system, at the level of the SGSN, traces the terminal movements in function of its states. The tracing takes place:

- at a cell level when the terminal is in the *Ready State*
- at the level of the RA when the terminal is in the state of *Standby*.

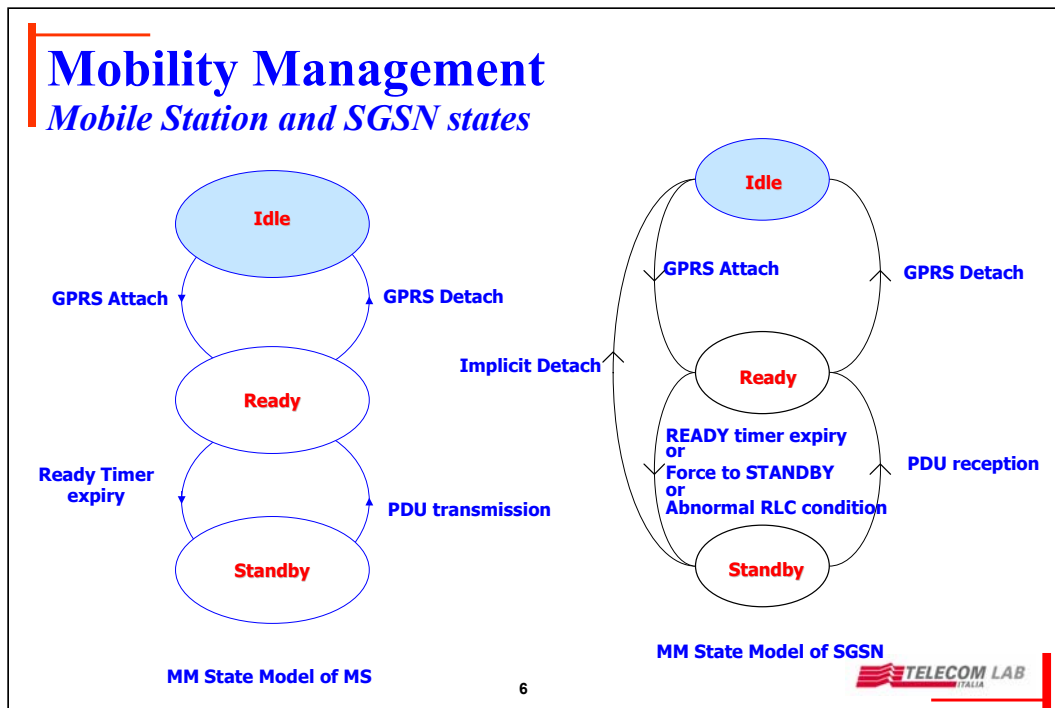
The RA dimension is typically less than the dimension of a LA. The reasons will be clear after having analysed the GPRS states tied to the mobility and data transmission.

Remind that the GSM states are:

Detach – the terminal is not localised by the network. The *Detach* status is registered by the network in the HLR to block useless paging transmissions for the incoming calls.

Idle – the terminal reaches this state through an *Attach* procedure. In this state MS is followed by the station with an LA granularity.

Active – the terminal communicates with the network and controlled cell by cell (the handover process is active)..



The GPRS states are depicted in the figure.

The *Idle* state corresponds to the *Detach* state seen for the GSM.

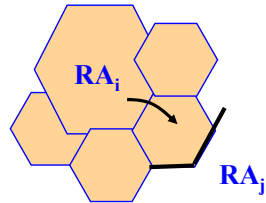
When in the *Standby* the terminal has been authenticated and registered by the network, which keeps track of it through the scheme of *Routing Areas*. The terminal and the network update the RA where MS is hosted in conjunction with any RA crossing (or according to a given time out).

In the *Standby* state, the terminal selects the cell in the *cell selection*; *cell re-selection* procedures.

The *Ready* state is entered when the terminal exchanges information with the network (this happens also in the passage between the *Idle* and the *Standby* states). The *Ready* state requires that the terminal is followed cell by cell.

The reduced dimensions of the RAs (with respect to the LAs) derive from the assumption that the user is in general reducing his mobility level when a data session is started. Hence, limited dimensions of the RA are adopted whenever the Standby status is often interrupted to give rise to data sessions. When dual conditions occur, the RA dimensions should approach the LA dimensions.

Cell update procedure

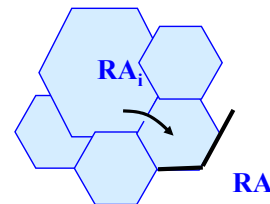


Standby States:

- tuning on the broadcast channel
- perform RA update if RA border is crossed

Ready State:

- cell update
- RA update if RA border is crossed
- new cell identity sent to SGSN through a BSS GP frame
- MM context updated by SGSN
- traffic re-directed towards the new cell



7

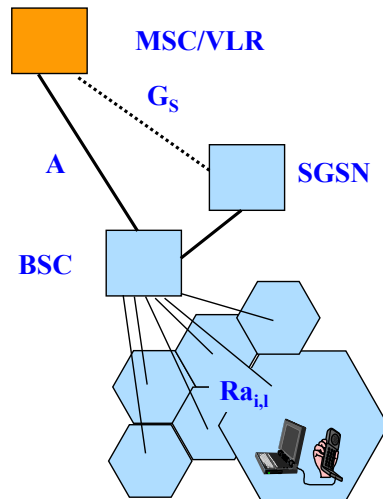
TELECOM LAB
ITALIA

The cell update is done as for the GSM. In the *stand-by* state the cell update triggers a RA update if the RA border is crossed.

In the *Ready* state the cell update must be notified to the network. This is done by sending to the SGSN any LLC frame with the MS identifier associated to the new cell identity (Cell Global Identity). In this way, SGSN updates the MM *context* and start sending (and receiving) the stream data towards (from) the new cell.

This procedure is similar to an handover. The MS has a central role in the cell re-selection: the procedure can be started on the basis of the MS measurements of the BCCHs. A completely decentralised procedure can however generate service degradation along the PDP *context*: if the chosen cell is overloaded, (in terms of traffic) the packet context undergoes a *throughput* decrease. To avoid this situation, the Standard includes the possibility that the re-selection of the cell is driver by the network, similarly to the GSM case.

Paging an MS within a Routing Area



Mode 1

GPRS paging channel used to page user for CS services (GPRS terminal attached)

Mode 2

Circuit packet channel used to page in both CS and PS domains

Mode 3

CS and PS users are paged independently

- in Mode 3 the terminal has to listen to two paging channels
- Mode specified for any RA through PBCCH (or BCCH)

8

TELECOM LAB
ITALIA

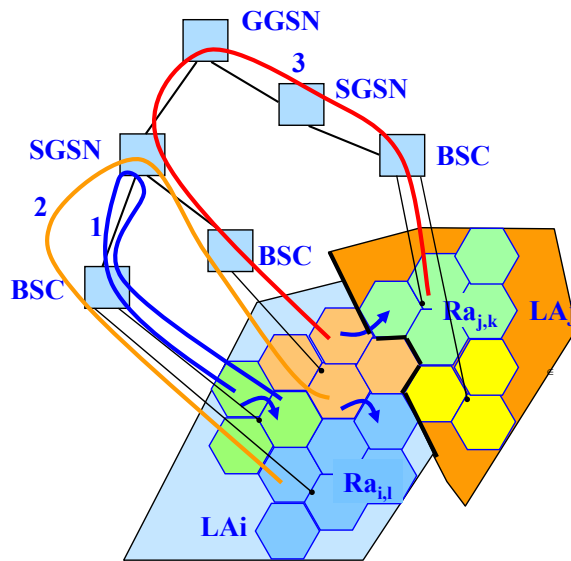
Each RA is fully included in a LA to guarantee that the LA change is always done in conjunction with a RA change. This correspondence is useful when mobility procedures are to be performed for both the circuit and the packet sessions:

- LA/RA updating, both periodic and mobility-tied (SGSN updates the RA and the MSC/VLR/HLR are updating the MS location for circuit services)
- *Attach/detach* procedures.

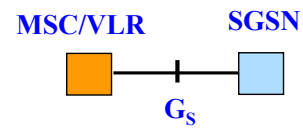
The *Routing Area Identifier* is broadcast (as for the GSM) through the *broadcast* channel

The *paging* can take place according to the three procedures depicted in the figure.

Location update cases (topology dependent)



Case 3 may imply combined operations with the circuit switched domain



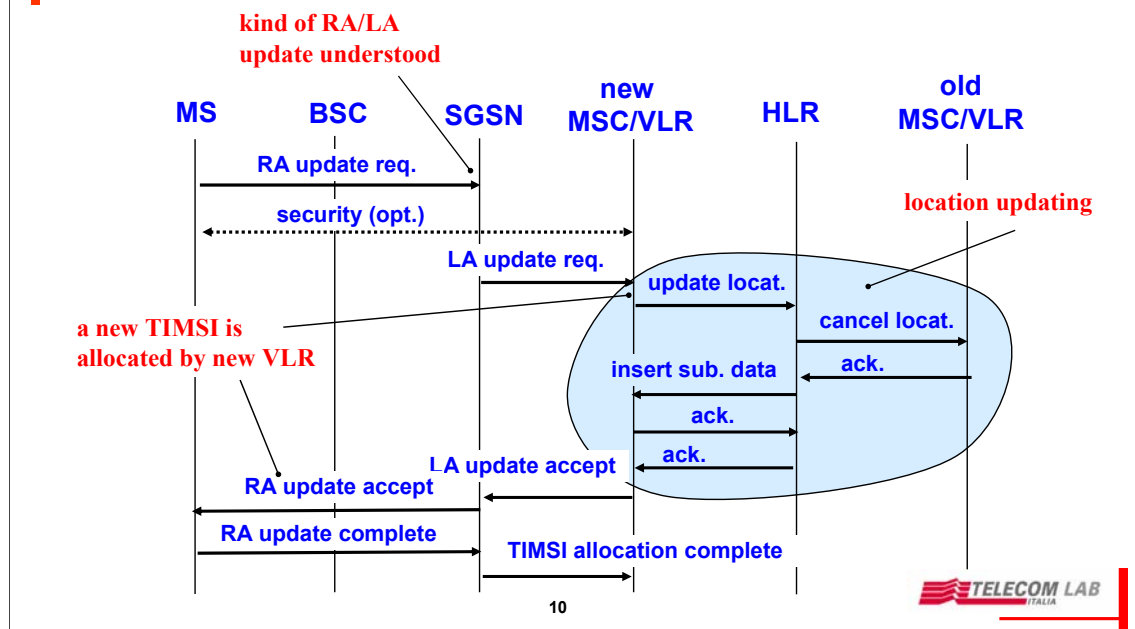
TELECOM LAB
ITALIA

9

The *routing area* procedure involves a number of devices dependent on the network topology. Case 3 triggers also a Location Updating procedure which may be directly managed through the Gs interface, controlling the GPRS-GSM interactions.

Remember that the *Routing/Location Area* update is one of the procedures to be managed (in general) jointly between the two CS and PS domains.

RA/LA updating procedure (intra SGSN)



As example, the case of joint updating of RA and LA has been chosen. The procedure is controlled by the same SGSN.

The SGSN is able to deduce from the MS data what kind of updating it must execute (the *Routing Area Indicator* defining the RA the MS is entering).

Since the change of MSC/VLR is involved, typically the *Temporary Mobile Station Identifier* (TMSI) is also updated. This TMSI will be used by the MS until an equivalent event take place.

In the *RA update request*, the MS sends to the SGSN the preceding RA identifier and the preceding P-TMSI. The SGSN can then understand if the updating must happen within the RAs under its control (figure) or if, conversely, the intervention of the GGSN has to be requested.

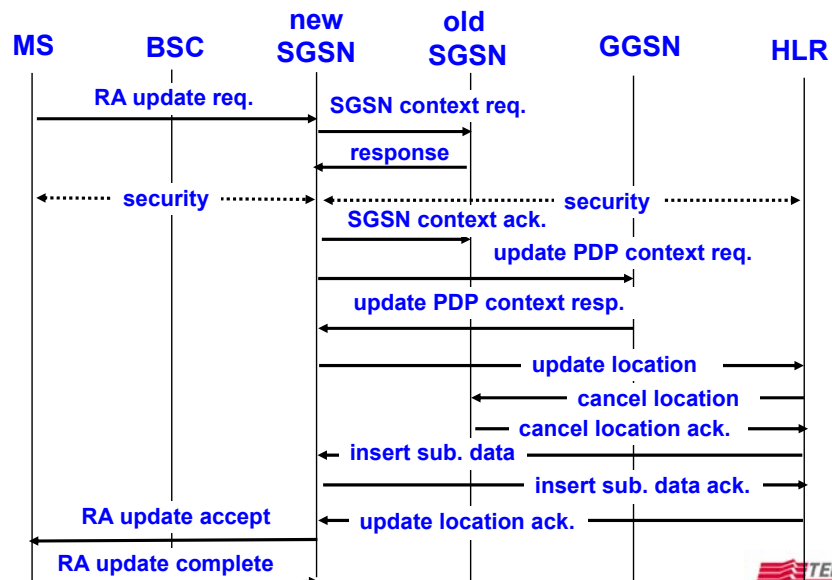
MS is also indicating if the update is joint with a *LA update*, if it is a periodic one or if, in conjunction with the RA/LA update, the MS needs to perform an *Attach*.

The SGSN knows the association *RA identifier-LA identifier*, hence the eventual *LA update request* is properly addressed. In the figure this event triggers an HLR updating because the new LA belongs to another VLR.

The SGSN may update the P-TMSI: in this case MS give a confirmation to the network.

The other location updates follow analogous procedures.

RA/LA updating procedure (inter SGSN)



11

TELECOM LAB
ITALIA

If the new RA is controlled by a new SGSN, the SGSN location has to be updated in the HLR. The MM context is recovered by the new SGSN. The figure represents the case where the user had one (or more) sessions in progress: the SGSN must also recover the PDP *context*.

The data flow must be re-addressed towards the new SGSN. The new address is resolved at the level of GTP protocol.

With an active flow, whenever an acknowledged LLC protocol is used, the change of SGSN forces the new one to recover data from the old SGSN:

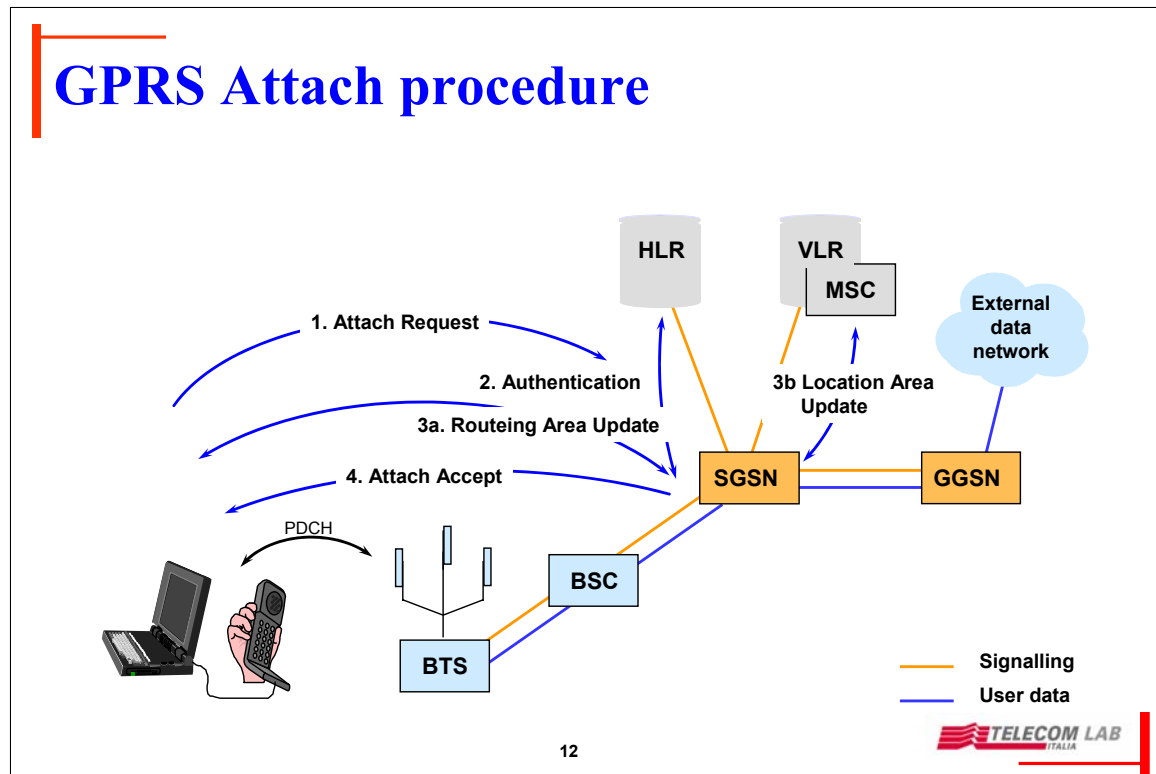
- the LLC frames already sent on the *down link* not yet acknowledged

- the sequence number of the acks related to the LLC frames already received in *up link* and not yet acknowledged towards the MS.

A similar procedure has to take place between the two SGSN for the GTP protocol packets: until the GGSN has not updated the flow re-routing, the data are received by the old SGSN.

The sequence number of the data packets sent in the up and in the down link are known in the PDP *context*. The system realises also periodical routing area updates, based on time outs that are reset and started in correspondence to specific states reached by the MS.

GPRS Attach procedure



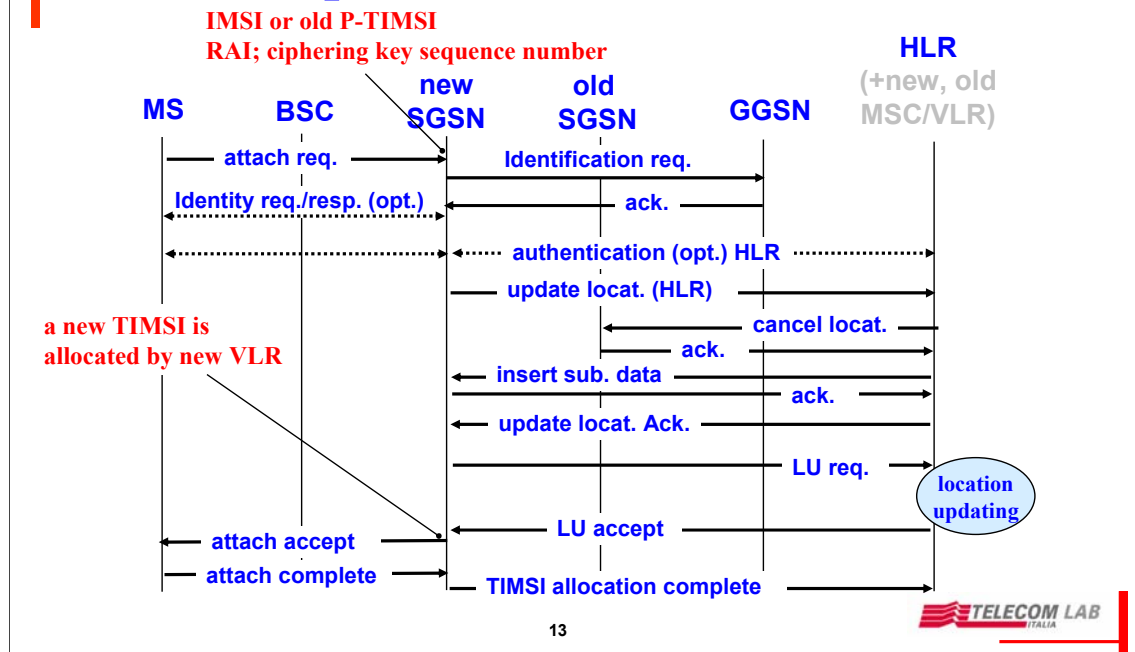
The *Attach* procedure leads the terminal (and the network) in the *Ready* state. The figure represents the main passages of the procedure in relation to the involved entities.

Also the *Attach* procedure induces, in general, the execution of combined procedures between the CS and PS domains. They concern two aspects of the process control:

- the mobility
- the authentication and the numbering assignment.

Both aspects are considered in the following.

The attach procedure (PS, CS combined)



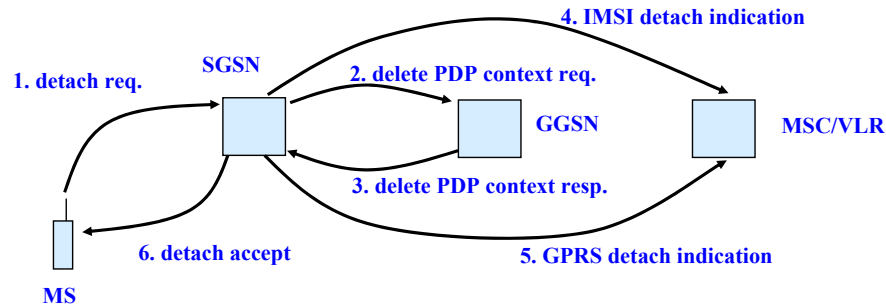
The *Attach* procedure brings the MS from the *idle* to the *ready* status and this implies that the terminal is followed with a cell granularity. In conjunction with the event, a *MM context* is created. The *Attach* can be requested:

- for the only GPRS domain (in this case the procedure concerns only the MS and the *Mobility Management* of the SGSN)
- for both CS and PS domains (in this case a combined procedure is needed: that reported in the figure)
- for the GPRS domain being the terminal already registered for the CS domain (the *Mobility Management* of the GSM is active).

In the example, it is assumed that the SGSN has changed since the last detach of the mobile terminal. In conjunction with the *Attach* request, the new SGSN requires to GGSN (by sending the P-TMSI and the preceding RAI) the data for identifying the terminal. If the temporary identity is not known, MS is asked to send the IMSI (the procedure is hence optional) and an authentication procedure is started.

Being the SGSN changed, a location updating procedure has to be launched (and the user data has to be assigned to the new SGSN and erased in the old SGSN). It is then necessary to start a location updating procedure for the circuit domain (the latter part would be useless in case of an *Attach* requested for the GPRS domain only). In the figure the interaction between the new MSC/VLR; HLR and the old MSC/VLR.

The detach procedure (MS initiated)



Explicit detach and
Implicit detach procedures

14

TELECOM LAB
ITALIA

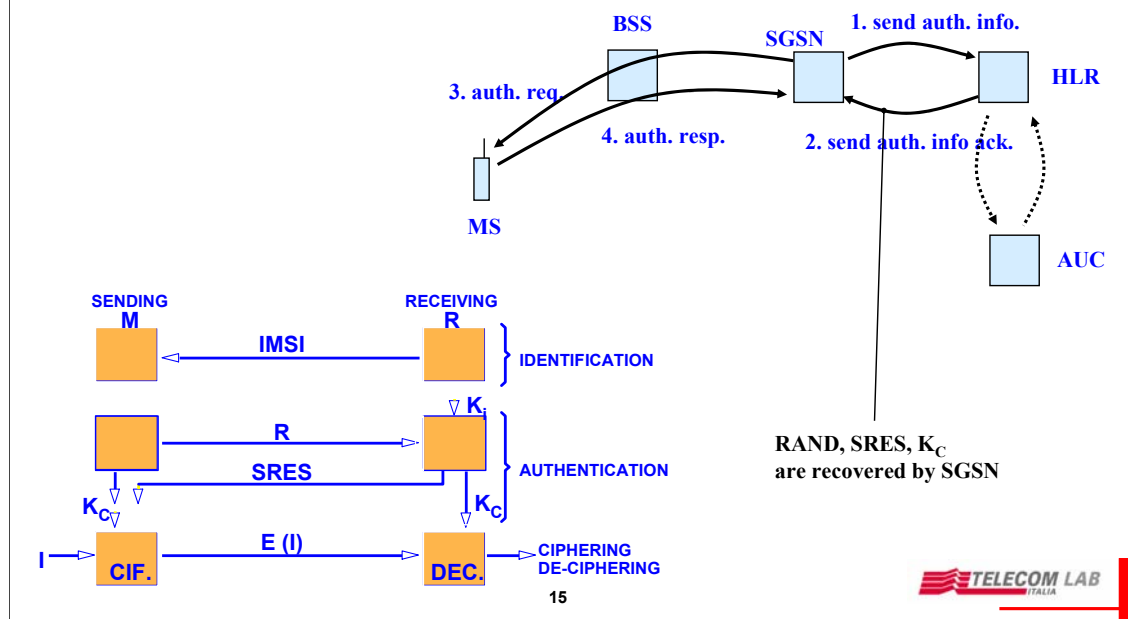
The *detach* procedure brings the MS to the *idle* state, hence it drops the mobility procedure in the network.

The procedure may be:

- explicit in case the MS (as in the figure) or the network require explicitly the *detach*
- implicit when the network decides to de-activate the PDP *context* since it has lost the logical connection with the MS (for example the latter has not performed the periodic RA *update* procedure).

If the GPRS detach procedure is activated towards the MSC/VLR (figure) then, from that moment on, the *paging* and the LA *updating* procedures are fully managed by the circuit domain.

GPRS security procedure

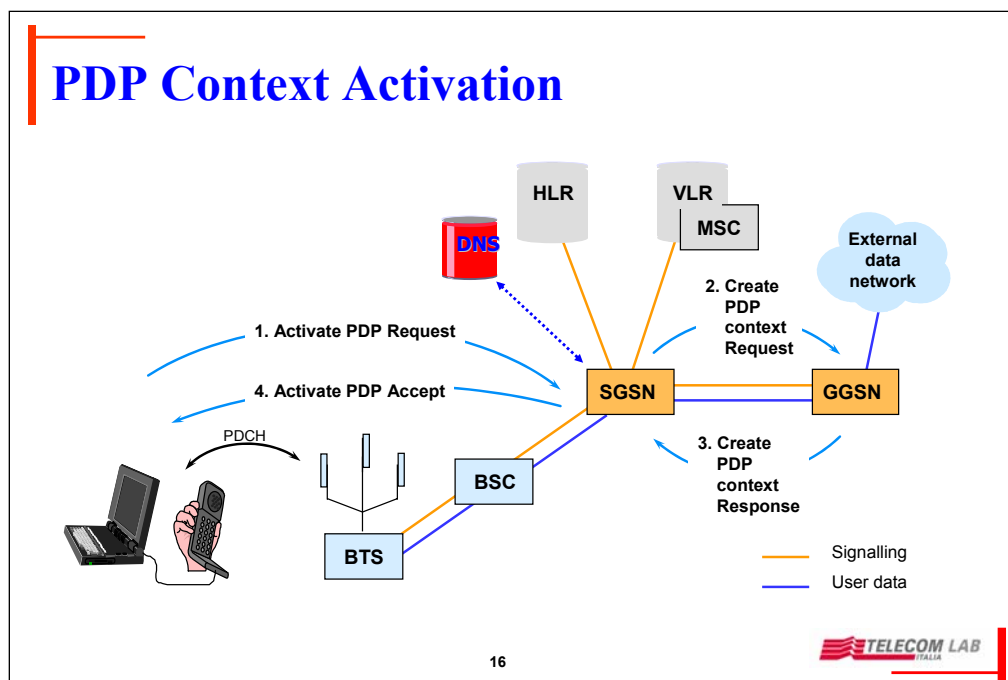


The security procedures are the same as those adopted for the GSM. The only difference is that it is involving the SGSN instead the MSC/VLR.

The user authentication is requested along the mobility procedures. The typical sequence is:

- SGSN sends the IMSI to the HLR
- the HLR interacts with the *Authentication Centre* which gives back to the SGSN the values RAND, SRES and K_c through which SGSN can manage the authentication process with the MS, until the ciphering key is obtained.

The GPRS specification allows to extend the protection up to the SGSN (the GSM *closes* the security flow at the BTS). In case of extension, the ciphering is managed at the *link* layer and not only at the physical layer as for the GSM.



The PDP *context activation* procedure can be started just after the *attach* procedure. The data sent by the MS through the message *activate PDP context request* are:

- *Access Point Name* (APN)
- the QoS parameters.

The same data can be deduced by the network on the basis of the service profile (the network can refuse the activation request whenever the MS data and the profile do not coincide). The SGSN sends the APN to the *Domain Name Server* which chooses the IP address of the GGSN. The SGSN sends then the APN and the QoS parameters to the GGSN.

The latter assigns an IP address to the mobile. The address is transferred to the MS by SGSN together with the negotiation outcome (*activate PDP context accept* message).

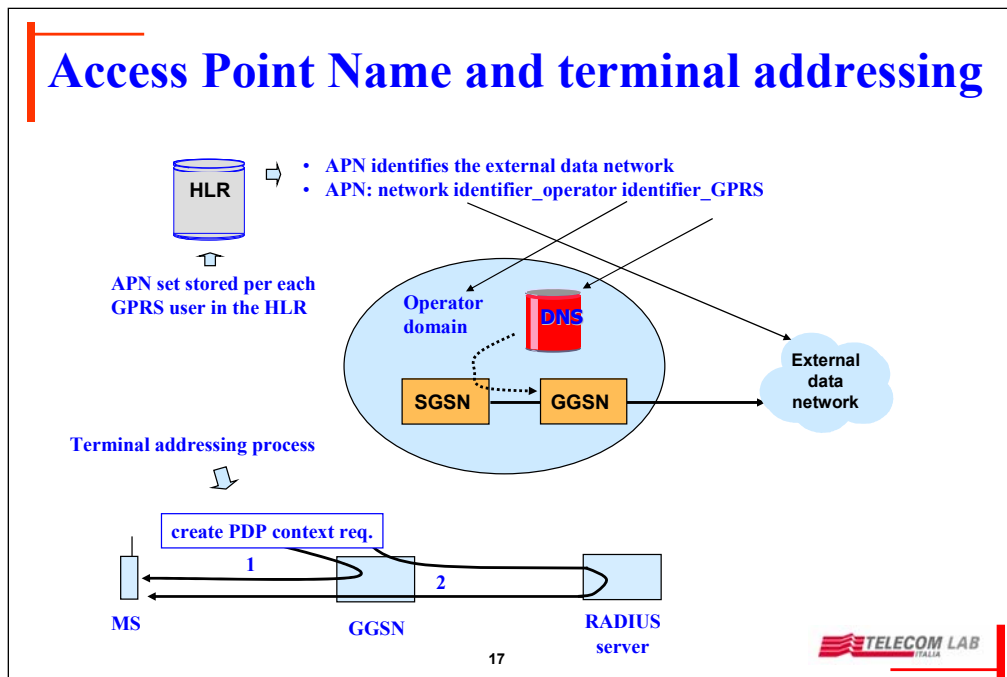
The three entities (MS, SGSN, GGSN) activate from this instant a PDP *context* (contains all the data necessary to manage traffic and mobility along the session). The PDP context will be referred to by any action concerning that specific data session. From that moment on, the PDP *context* is considered an attribute of the MM *context* managed between MS and SGSN.

APN and QoS profile are often included in the *terminal equipment* and supplied to the MS.

The mobile terminal can activate more than one PDP *context* at the same time. For each of them the rules explained hold independently. Each has specific attributes in MS, SGSN e GGSN.

The IP address assignment procedure is a transparent one. Extension e3.2, clarifies that a non transparent procedure can be adopted (an external server is assigning the address to the MS).

Access Point Name and terminal addressing



The set of *Access Point Names* that can be used by the MS is contained in the user profile of the HLR. The operator identifier identifies the PLMN and its *country code*. The external network to be used for the data session (*network identifier*) is normally defined by the operator. The “GPRS” range must be utilised only when the address identification is resolved by a public DNS. In the actual schemes, that is done by the DNS of the PLMN: the related range is not used.

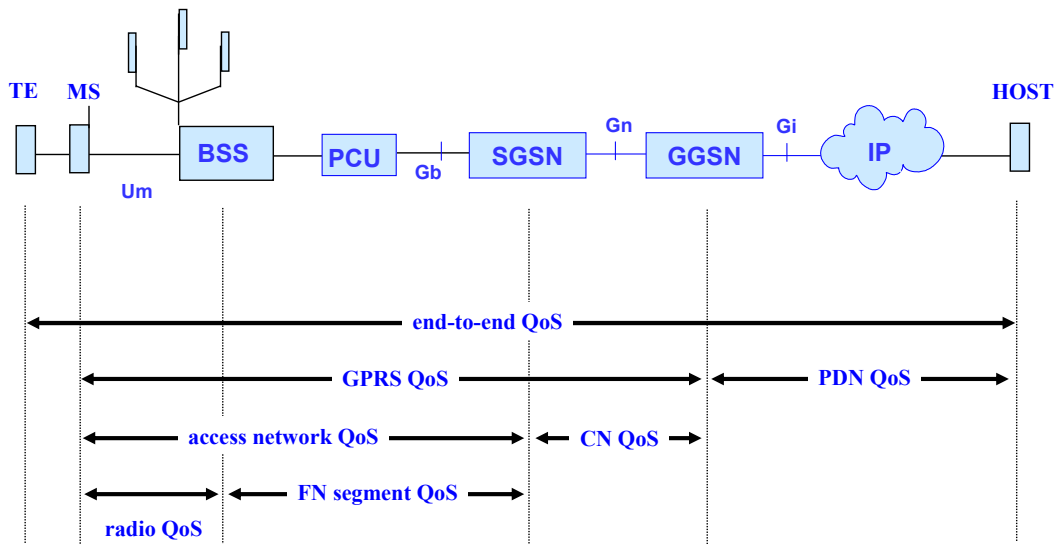
The APN can be unknown to the MS: it is then the network (SGSN) that assigns it consistently with the indications contained in the HLR.

The IP address assigned to the MS can be static (it is reported in the user profile). In this case it is recognized by the GGSN in the context construction phase (*create PDP context request* message) and assigned to the mobile (case 1 in figure).

If the address is not assigned permanently, the network assigns a dynamic address, typically extracted from a RADIUS server selected on the basis of the APN. The server belongs either to the operator network or to an external network (ISP, Intranet).

When a public entity assigns the address, it has no relation with the IP addresses assigned to the GGSN. The situation reflects the case of a *co-located care-of-address* (see extension 3.2). If instead the address is assigned within the PLMN domain, it belongs to the addresses assigned to the GGSN. In the first case a tunnelling scheme must be adopted between the external network and the GGSN; in the second case this is not necessary.

QoS management an overall view



18

TELECOM LAB
ITALIA

The QoS level of a session is established at the activation of any PDP *context*. It is in general re-defined by the SGSN and the GGSN on the basis of the available resources in that particular cell. The outcome of the negotiation is sent to the terminal through the *activate PDP context accept* message. The MS accepts (or not) in function of the minimal requirements characterizing its service profile.

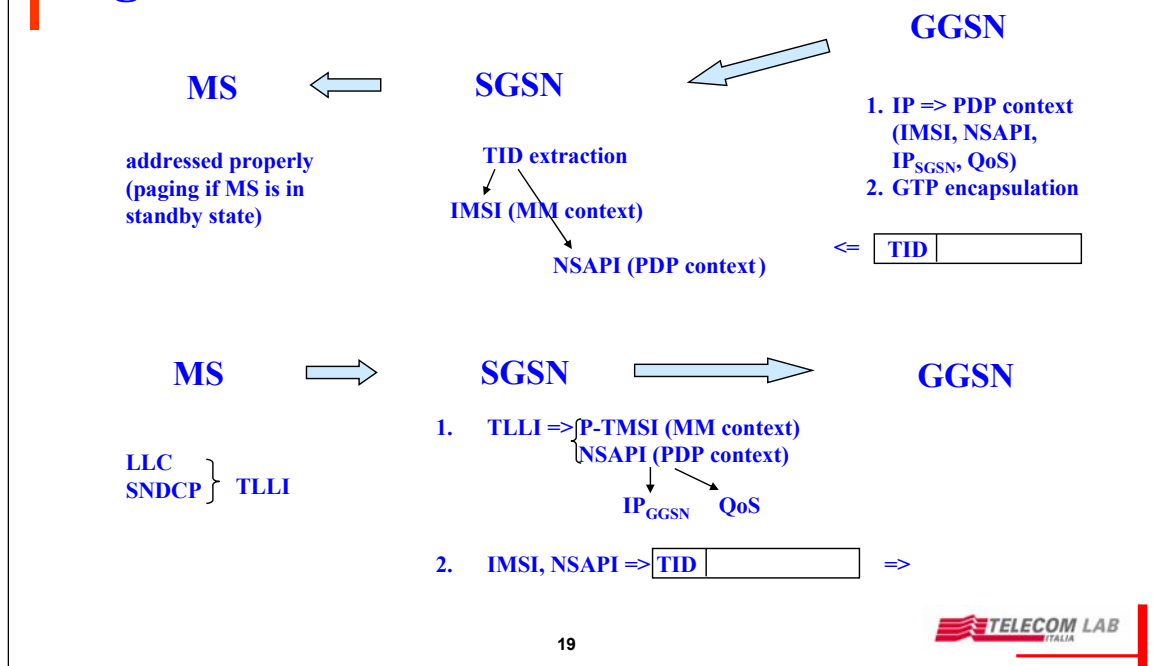
The QoS classes define for the GPRS are:

- *Service Precedence (high, medium, low)*: specifies the priority assigned to any single user
- *Reliability*: specifies the reliability class assigned to the service (robustness against the transmission errors). This is the protocol levels at which the reliability is guaranteed:
 - GTP ack/nack
 - LLC ack/nack
 - LLC protected/unprotected
 - RLC ack/nack.
- *Delay*: the *end to end* delay; three classes are defined, together with a *best effort* class
- *Throughput*: two parameters can be negotiated: the maximum *bit rate* and the average bit rate.

These classes concern mainly the radio access and the fixed segment in the access part of the system.

Obviously the point-to-point quality depends on a series of other factors that cannot be not directly ascribed to the GPRS control and resources.

Logical connections in GPRS



The PDP *context* is registered in all the network elements to guarantee the entire packet transmission in both directions:

- the GGSN maintains the IP address of the terminal, its IMSI, its NSAPI, the negotiated QoS, the APN and the IP address of the involved SGSN
- the SGSN maintains the IP address of the terminal, the NSAPI, the QoS accepted, the APN, the IP address of the involved GGSN
- the MS maintains its IP address, the negotiated QoS, and the NSAPI.

The figure describes how the data flow is managed in both directions MS=>GGSN e GGSN=>MS.

Based on the contexts set-up during the session activation, the network entities are deducing all the information needed to route properly the user data.

In the two directions:

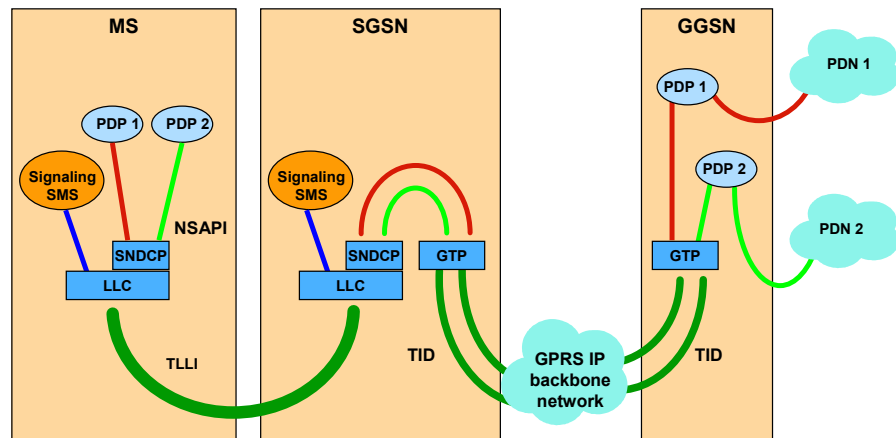
- the IMSI (or TMSI) identify the MM context
- the *Network Service Access Point Identifier* (NSAPI) identifies the PDP *context*.

For incoming packets (in GGSN) from the external networks, their *header* (IP address) identifies univocally the PDP *context* (IMSI, NSAPI, IP_{SGSN}, QoS). The first two parameters are inserted in the *header* of the IP packet carried towards the SGSN with the GPRS *Tunnelling Protocol* (GTP). The SGSN is able to identify MM and PDP *contexts*.

NSAPI and IMSI are sent to the MS; the two are forming the *Temporary Logical Link Identifier* (TLLI) which identifies the MS within the *routing area*.

In the opposite direction, a similar mechanism holds.

Logical connections in GPRS (II)



20

TELECOM LAB
ITALIA

The PDP *contexts* open between the MS and the network are managed transparently with respect the network. The different flows are controlled through specific *Tunnelling Identifiers* by the GTP protocol.

At the access side, the different flows are encapsulated in a single connection which is managed by the LLC layer (single *Temporary Logical Link Identifier*). The *Sub Network Dependent Convergence Protocol* is in charge of performing such encapsulation.

The transport mechanism of the IP (o X25) PDU is realised *above* the inter working functions implemented in BSS, SGSN and GGSN.

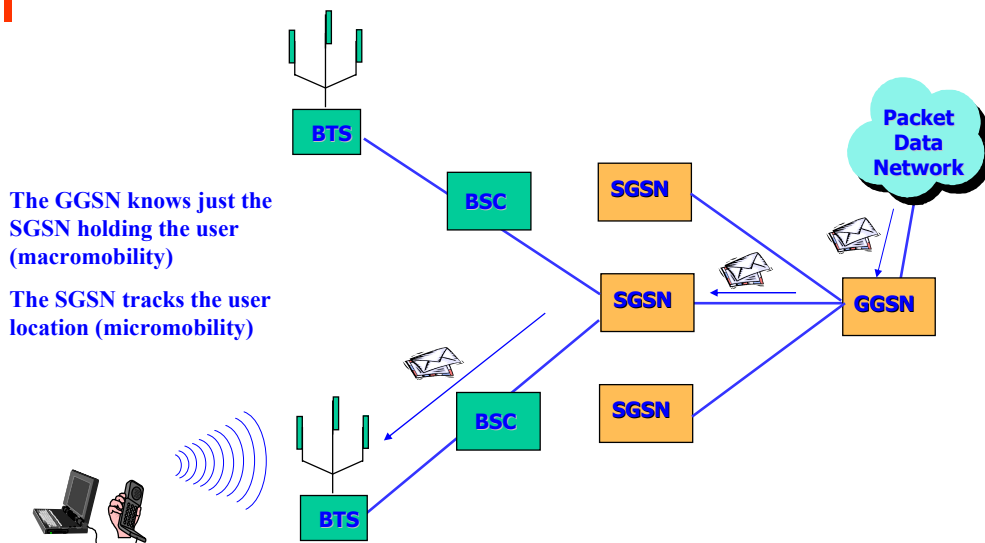
The PDU routing functions are executed:

- through a tunnelling mechanism (TID) in the *core network* segment
- through a single *Transport Link Layer Identifier* in the radio access segment.

These functions are repeated for all the packets belonging to the same data flow.

The *Link Layer Control* (LLC) can multiplex also other flows (e.g. SMS messages).

Macro and micro mobility



21

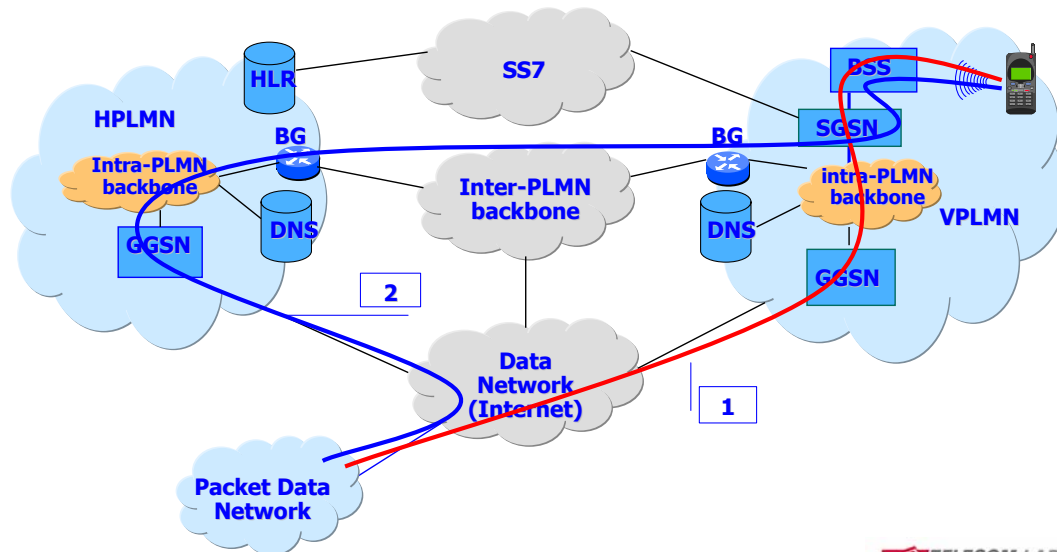
TELECOM LAB
ITALIA

The GPRS realises a joint control of the mobility:

- by adopting a *mobile IP* scheme in the upper segment of the network: *tunnelling* of IP packets in Ip packets; the latter address the flow towards the SGSN that controls the MS in that particular instant; the addressing is changed whenever the MS changes the SGSN
- by adopting a *continuous mobility* scheme, cell by cell through the mechanisms implemented in the access segment (cell re-selection and consequent packet re-routing).

The PDP *context* can be started by either the network or the MS. In the second case the GGSN receives a packet with the IP address of the terminal. The GGSN associates this address to the PDP *context* (not yet active). The IMSI is associated to the PDP *context*. GGSN requires routing info to the HLR (exactly as for an incoming call of the GSM). In this way it can address the SGSN under whose control the MS is attached. A *PDU notification* is sent to the SGSN. The SGSN generates a *Request PDP context activation* towards the MS. The latter starts the procedure as previously seen.

GPRS Roaming functions



22

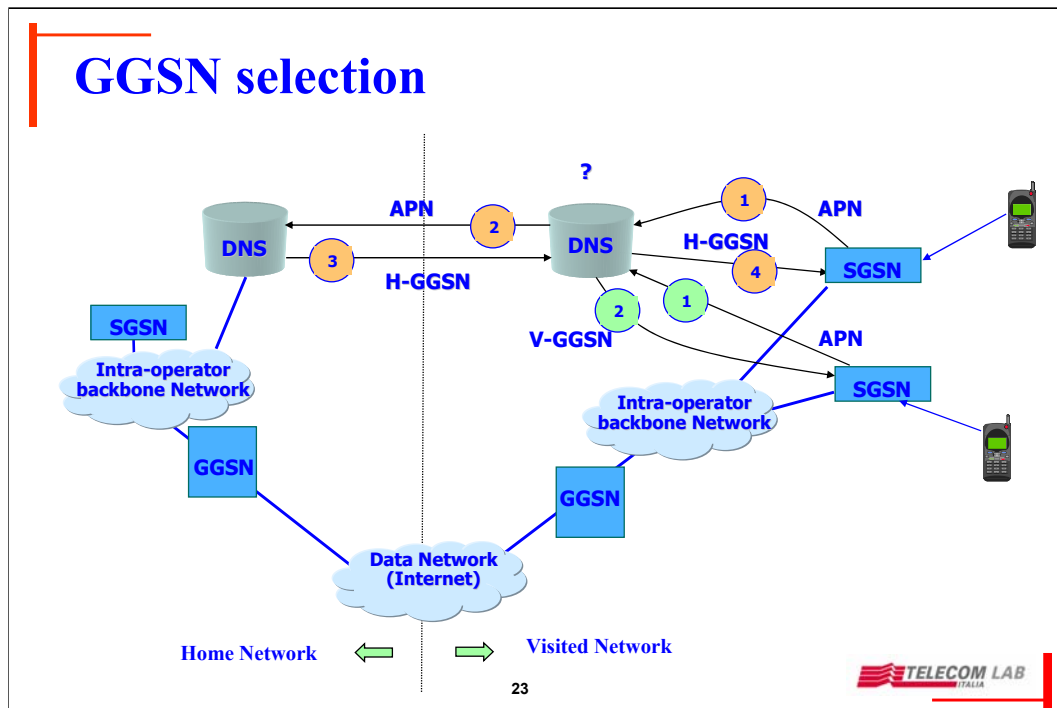
TELECOM LAB
ITALIA

The GPRS system accepts two *roaming* modes. For an MS *attached* to a *Visited Public Land Mobile Network* (PLMN) the traffic can be routed:

- through the GGSN of the VPLMN (case 1)
- through the GGSN of the *Home* PLMN (case 2).

The connection with the HLR is necessary owing to the need for the VSGSN of receiving the visiting user profile at the beginning of the *attach* procedure.

The inter-PLMN IP network is used through specific *Border Gateways* whenever the H-PLMN is used for the transport connection.



The two routing cases are determined by the user profile and the structure of the APN.

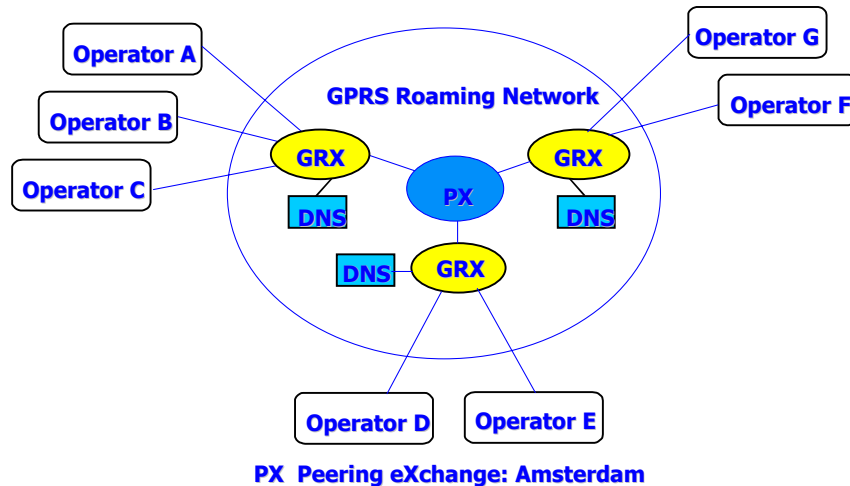
When the MS sends the V-SGSN the complete APN (*network identifier* and *operator identifier*) the DNS of the visited network sends the APN to the DNS home and the latter supplies the IP address of a H-GGSN. The same happens whenever the MS is sending the *network identifier* alone and it is possible at the same time to extend such identifier to the *operator identifier*: the SGSN is performing the extension and everything takes place as described for the complete APN address.

In the other case, the APN contains just the *network identifier* and the user profile allows to use the *network identifier* of the visited network: the V-DNS supplies the IP address of a GGSN of the visited network. This means that the two networks have agreed on common APNs in advance.

The table reports advantages and disadvantages of the two solutions.

	VGGSN	HGGSN
QoS	Not possible	Possible
Operator control on roamer behavior	As (bad) as GSM	Possible
Routing efficiency	Direct routing	Routing through IPBB
Ease of implementation	SS7 connection required	SS7 and IP connection required
Billing	Information from VPLMN required	Information not nec. required
Services	Best Effort Web browsing	Customized services

GRX - GPRS Roaming eXchange



24

TELECOM LAB
ITALIA

The problem of interconnecting different networks, belonging to different operators (Inter-PLMN *backbone*) may be resolved in two ways:

- the direct interconnection between all the operators having *roaming* agreements (in this case dedicated connections can be utilised through the public Internet)
- the interconnection performed through a GPRS Roaming eXchange (GRX) which establishes a mediation and interconnection stage recognised by all the operators that can take advantage from the solution by avoiding an expensive and complete interconnection. The GPRS supplies interconnection services and in the perspective it will supply *root DNS* services to directly assign IP addresses, bypassing the routing issues previously seen.