

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

3.2 GPRS services

services and terminals
Quality of Service
general architecture
integration with IP

extensions:

e3.2 IP mobility and numbering

2

TELECOM LAB
ITALIA

Section 3.2 analyses GPRS services and their allocation in the general context of data services. In its strong interaction with IP, the GPRS anticipates some solutions that have been successively designed for the UMTS:

- the radio resource optimisation in function of the statistical characteristics of data traffic
- the *always-on* features offering a permanent connection in line with the Internet paradigm
- service models based on *volumes* rather than on *times of connection*.

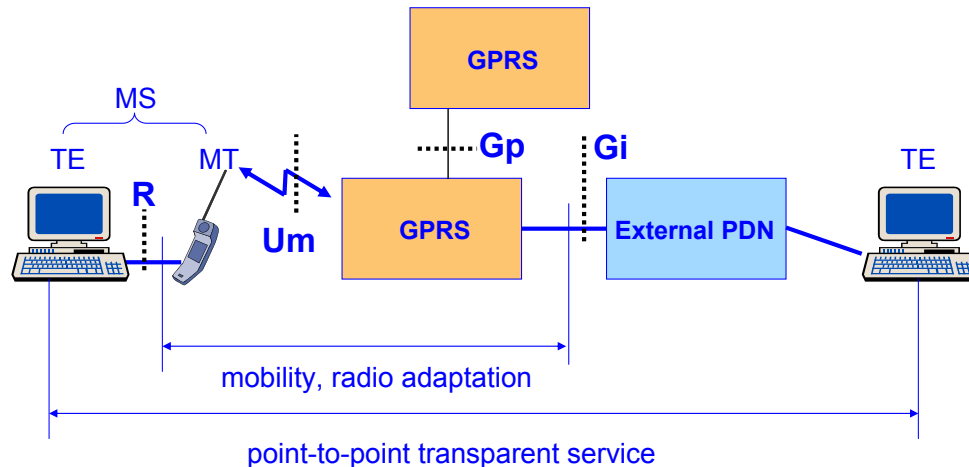
GPRS is particularly suited for:

- WAP; MMS services
- *web browsing*
- *e-mail*

Conversely, the GPRS solution is not suited at all for those services showing requirements on the delay al related dynamics (delay variance), in particular for voice, video communication and real time video streaming.

Extension 3.2 focuses on some elements tied to numbering and mobility in IP.

GPRS the transparency concept



3

TELECOM LAB
ITALIA

GPRS introduces an access mode to Internet much more advanced compared to the previous solutions (CSD, HSCSD). A key characteristic is the *end-to-end* data transport based on the packet switching model.

In the circuit-base service, the circuit connection is active for the entire transaction time and a *Remote Access Server* takes care of translating the data flow in a packet stream towards the data networks. In the GPRS the packet modality is realised starting from MS. Hence, the nature of data services is respected:

- *burst* transmission with long inter arrival times compared to the overall transmission delay of the burst data
- interactivity behaviour of the source, often accompanied to non symmetric volumes in the two transmission directions
- high degree of resource sharing and high delay values, suited for low delay requirements
- asymmetry between the two transmission directions

The GPRS network realises a transparent transport, enabling the TE to use directly and transparently its protocols (towards the external network) without any modification.

GPRS uses in a flexible way the radio resources (one or many slots; different multiplexing levels of the data streams).

Types of terminal

- ◆ **Class A:** the MS is allowed to generate and/or receive calls on both circuit and packet switched services simultaneously
- ◆ **Class B:** the MS can make and/or receive calls on either of the two services sequentially but not simultaneously
- ◆ **Class C:** the MS can make and/or receive calls on either of the two manually selected services

4



IP and X25 are the supported protocols. 4 coding schemes can be used on the radio interface, in function of traffic type and the needed protection degree. The transmission speeds can vary from 9.05 to 171.2 kbit/s.

The MT configurations with respect to the TE are the same already seen for the HSCSD solution.

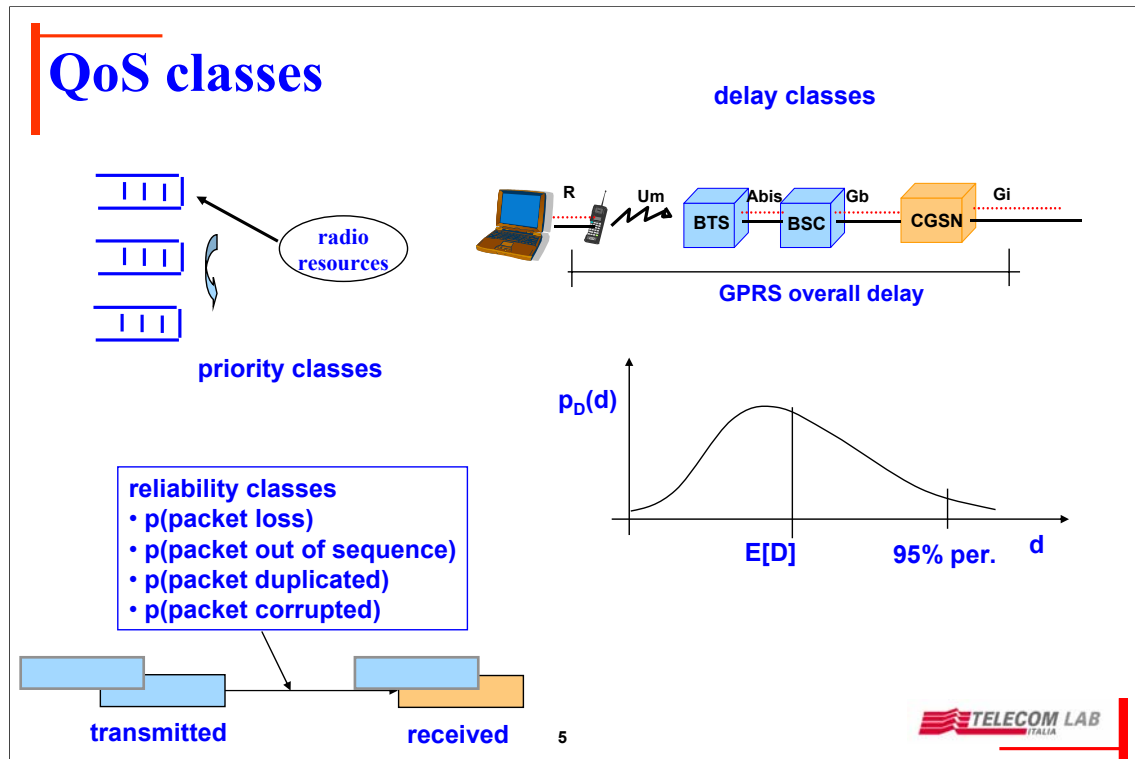
Point-to point or *point-to-multipoint* transmission schemes can be adopted. The latter can support content diffusion or application requiring the control of a multiplicity of dispersed devices.

GPRS co-exists with the circuit mode of the GSM. In this sense, three terminal classes are specified (figure).

The class A terminal can activate all the packet and circuit processes simultaneously

Class B terminal switches automatically between the two modalities (for instance, if a data session has to be started while a voice communication is in progress, the former is put in waiting list). This implies that the terminal is registered simultaneously in both domains.

Class C terminal allows to use of a single port at a time.



The GPRS system offers the QoS levels through a series of parameters sketched in the figure. The QoS level is associated to any packet session (*Packet Data Protocol Context*).

The classes of priority are defined over three levels. They reflect the ability of the system to maintain for level i the QoS constraints (which is higher than for services of class j if $j > i$).

Each delay class is defined through two parameters: the maximum value of the mean delay and the accumulated delay at the percentile of 95%. The delay is that accumulated between the interfaces R and Gi (the one that can be really associated to the GPRS segment).

There are three delay classes, respecting three reference levels and a *best effort* class, whose values are not specified. Reference values depend on the packet length. The extreme values are:

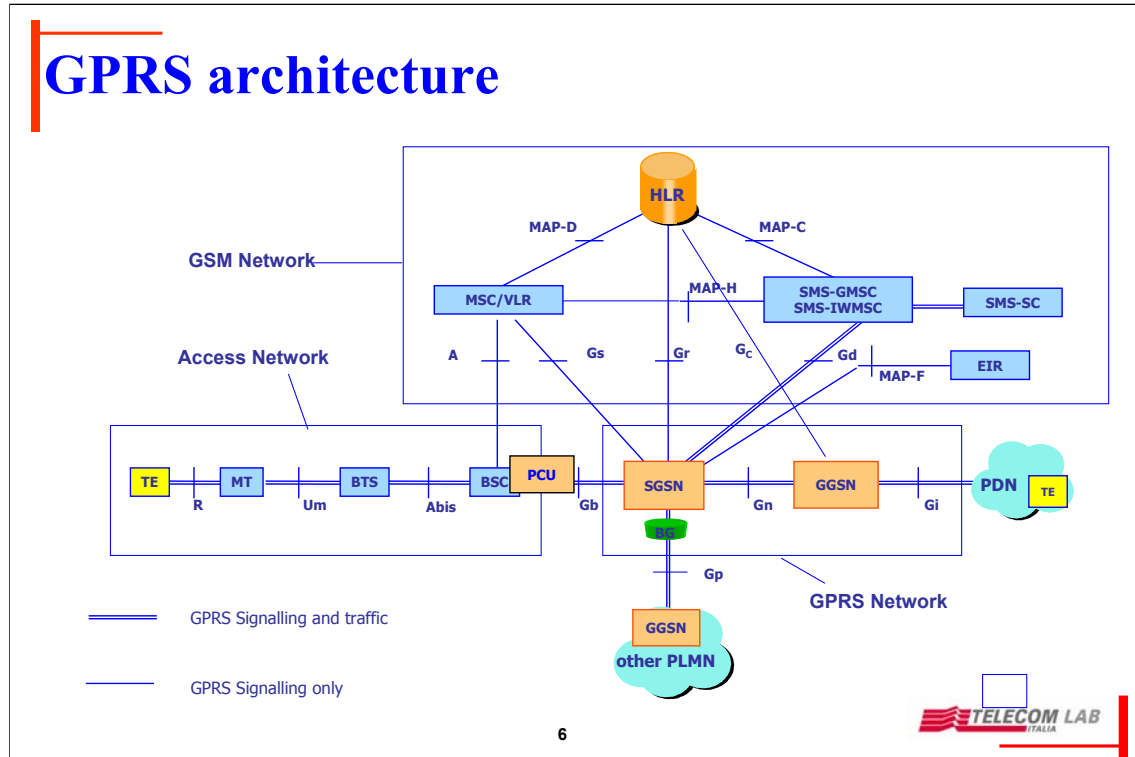
- average value $< 0.5s$; 95% percentile $< 1.5s$
- average value $< 75s$; 95% percentile $< 375s$.

There are in addition reliability classes. They apply to the layer 2 protocols (see subsequent paragraph).

The reliability classes are characterised by the probability of: packet loss, packet sequence error, packet error.

Finally, the *throughput*, can be characterised as QoS parameter, in terms of average and peak values.

GPRS architecture



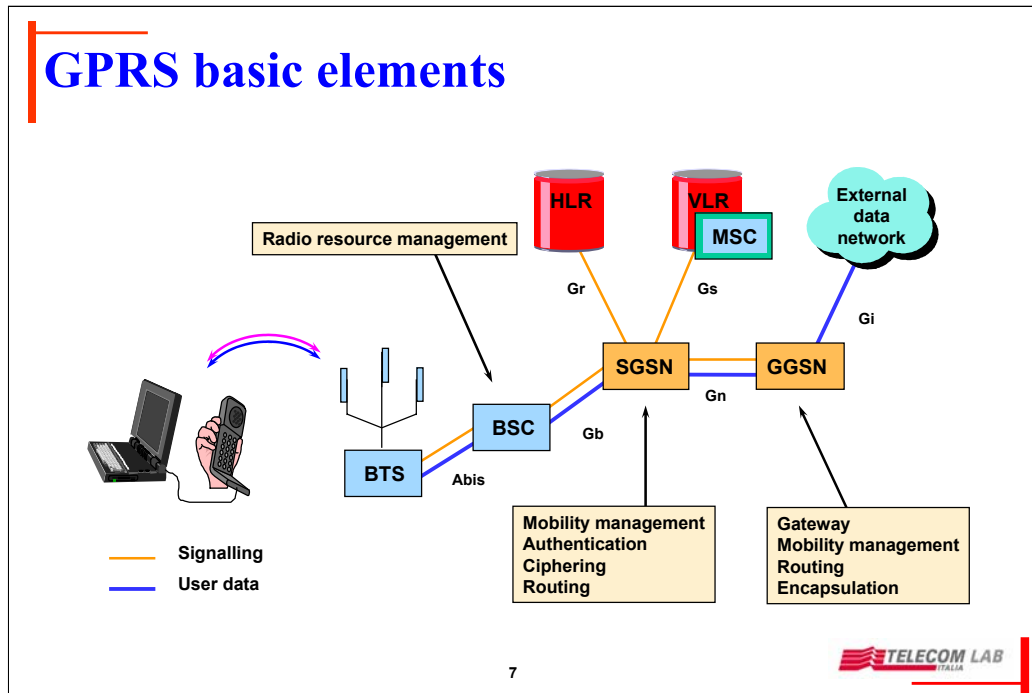
The GPRS shares the access segment with the GSM. To manage the packet section is however necessary to introduce new entities.

The bifurcation towards the upper hierarchy (and the multiplexing towards the access segment in the opposite direction) of the circuit and packet streams is realized by the *Packet Control Unit* (PCU) which manages the Gb interface by translating the packet/circuit flows in both directions.

The *Serving GPRS Support Node* (SGSN) controls (as the MSC for circuit traffic) the mobility functions and the session set-up phase. SGSN is connected through suitable interfaces with all the entities already introduced for the GSM (it is often necessary that packet and circuit sessions are synchronised)

The *Gateway GPRS Support Node* (GGSN) implements all the interfaces with the external *Packet Data Network*. It controls also the *tunneling* functions, the security (*firewall*) towards the external networks. Thanks to the GGSN, the GPRS network is perceived by the external data network as a sub-network.

It has to be stressed that control functions can be assigned to GGSN and SGSN with a certain degree of freedom.



The GPRS represents the first real integration between the mobile network and IP.

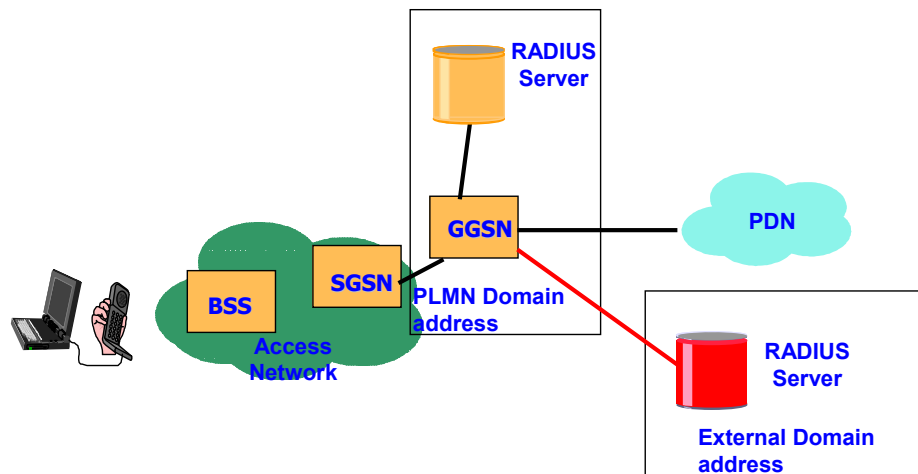
The A-bis interface (BTS-BSC) is maintained as a common interface for packet and circuit switched connections; this is appropriate for a unique Time Slot-based identification maintained up to the BSC level (as it is in the GSM).

The above identification scheme is not so interesting in case of CDMA access, where variable bit rate connections are possible. So, the above choice is re-considered in the 3rd generation perspective, where more innovative solutions will be adopted also in the Radio Access Network.

The Gn interface is an IP interface and SGSN and GGSN implement a good portion of the typical functions of a router.

Interconnection with Internet Services

transparent and non-transparent modes



8

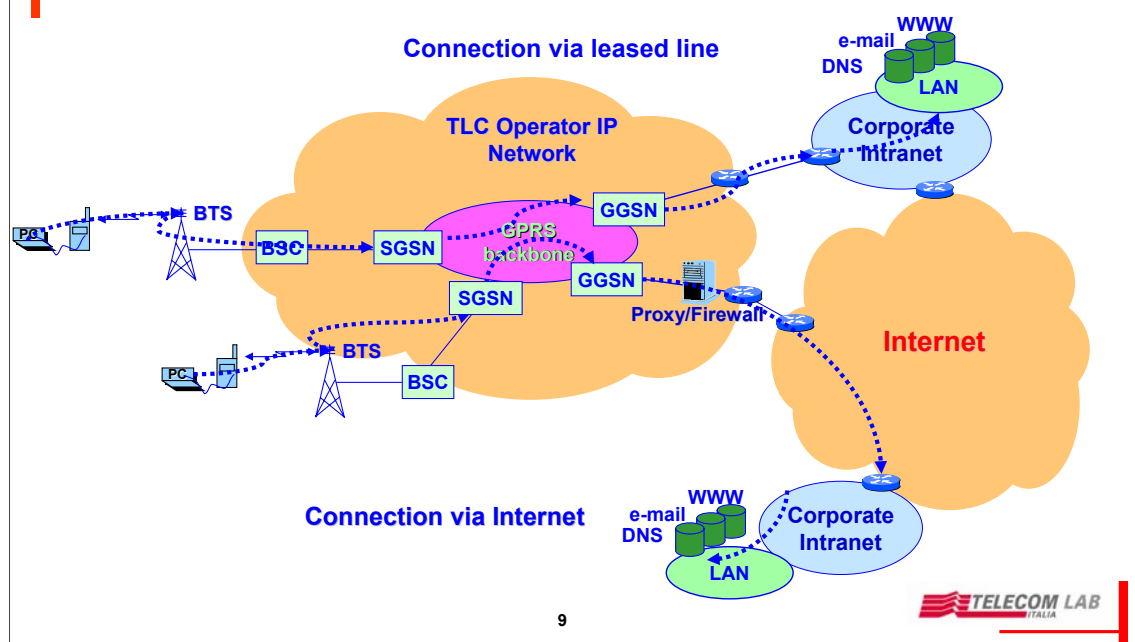
TELECOM LAB
ITALIA

A GPRS terminal can access an external network through two modalities: transparent and non-transparent mode. They differ for the assignment of the address to the mobile terminal: assigned by the PLMN in the first case, by an external address domain in the second.

If the terminal supports a dynamic addressing feature, it receives the address from the GGSN in conjunction with the request of the set-up of the *Packet Data Protocol Context*. This phase may be preceded by an authentication phase, still performed within the PLMN.

With the acquisition of the IP address, the terminal may access to any server, both in the PLMN domain (for instance a WAP server of the mobile Operator) and belonging to the public Internet. In the transparent access, both public and private addresses can be used. Public addresses are normally used when the terminal has to use security mechanisms like IPsec to access external servers.

GPRS access to Corporate networks

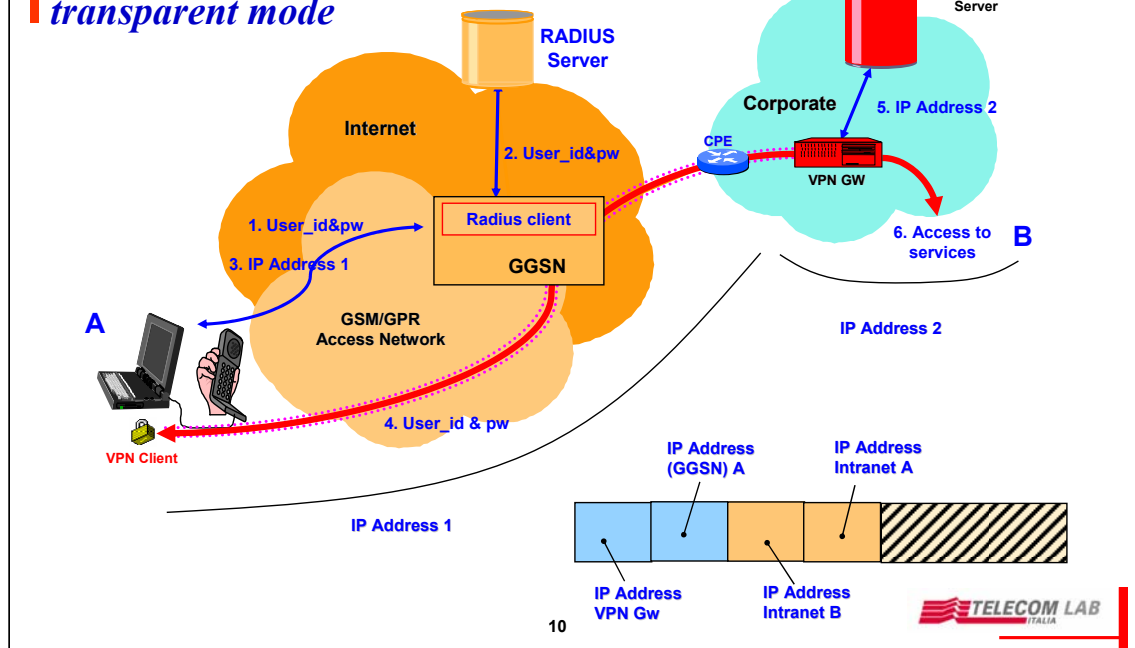


9

Often, the security of a connection with the Intranet is guaranteed by means of located connection capabilities.

Much more flexible and efficient may be the access through the public Internet, which is by turn posing some problems at security and addressing level. Some of them will be focused in the subsequent figures.

Remote access to Intranet *transparent mode*



The transparent connection with the Intranet is performed in the following way:

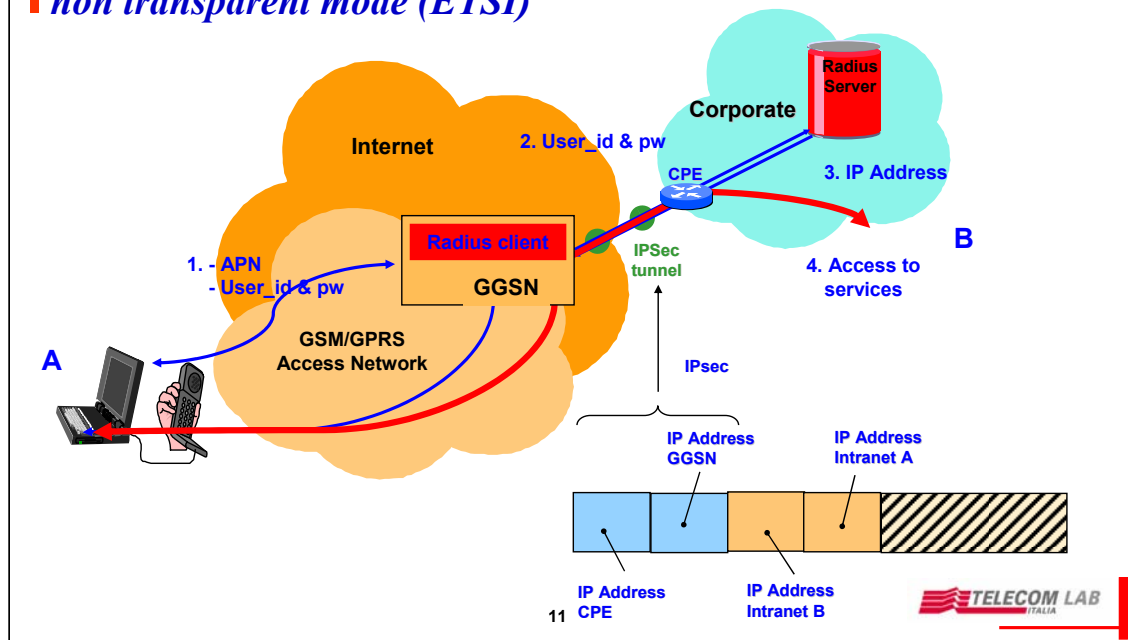
- as a consequence of a connection request, the GGSN (acting as an *Access Server* of the Internet Service Provider) assigns to MT a public IP address
- MT has a client VPN which allows it to access to the *VPN Gateway*
- the *VPN Gateway* and the *VPN Client* establish a secure connection Ipsec; Through this connection the *Gateway* assigns the MT an IP address belonging to the address pool of the Intranet.

The mailing of the IP packets to the Intranet adopts the nesting mechanism depicted in the figure.

This kind of access is named *Client Initiated* in fact it is completely managed by the *VPN Client*. The GGSN (ISP) just assigns to the MT the IP address enabling it to start the connection to the *VPN Gateway* through Internet.

Alternatively, a *Network Initiated* access can be used.

Remote access to Intranet *non transparent mode (ETSI)*



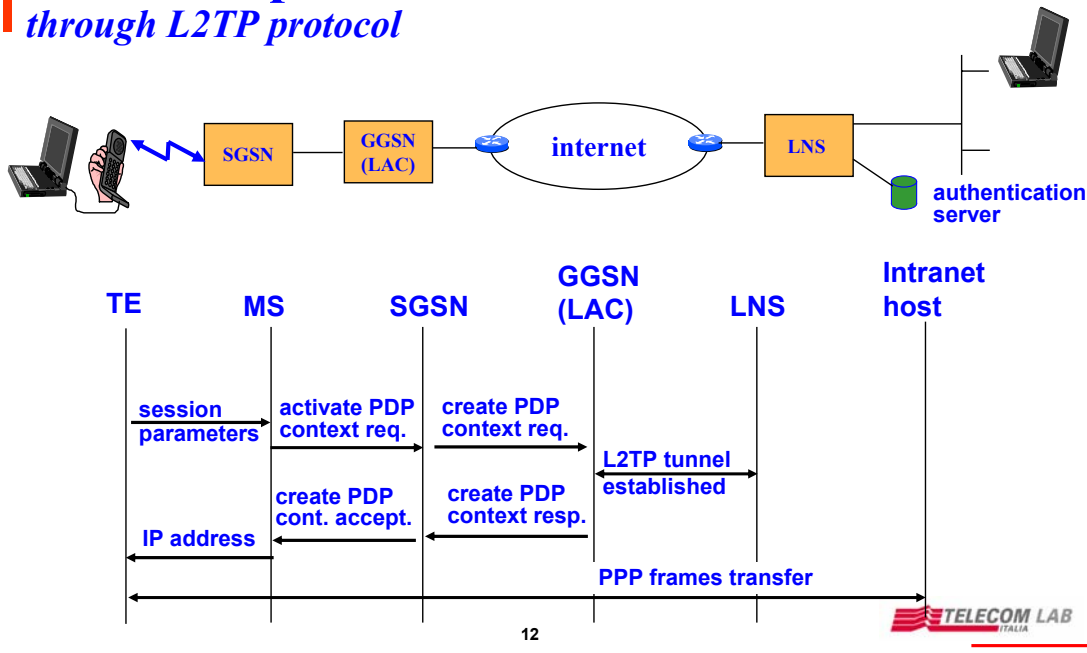
The non transparent mode specified by ETSI is based on the following sequence:

- MT activates a PDP *context* by sending to the GGSN *user name and password* as well as an *Access Point Name*
- the GGSN exchanges the needed authentication and addressing actions with the corporate server (the server is chosen through the *Access Point Name*); the latter authenticates the terminal and assigns it an Intranet address
- the IP Intranet address is passed to the terminal by the GGSN together with the *Activate PDP Context Accept* message
- the GGSN establishes a secure connection with the board router of the *Intranet* (typically an IPsec connection).

The encapsulation mechanisms adopted between MT and the *Intranet* end point are represented in the figure.

The solution requires that an agreement exist between the GPRS Operator and the administrative domain of the Intranet. Relevant *client/server* processes must be aligned as well.

Non-transparent access to Intranet through L2TP protocol



An alternative is to use the *Point-to Point Protocol* (PPP) protocol between MT and the destination end point. In this case security is ensured by the Layer 2 protocol named *Layer 2 Tunnelling Protocol* (L2TP) instead by the IPsec, (a layer 3 protocol).

TE requires a PDP *context* activation by sending to the GGSN *user name*, *password* and the *Access Point Name* as in the previous case.

The GGSN sets-up an L2TP tunnel with the *L2TP Network Server* (LNS) identified thanks to the *Access Point Name*. Authentication and address choice are performed within the Intranet, without involving GGSN. Through the L2TP connection, LNS supplies the GGSN with the MT address. The GGSN passes the address to TE (again in conjunction with the message for the activation of the PDP *context*).

TE can now transmit its data to the GGSN through the frames of the *Point to Point Protocol* (PPP). For this transmission the internal GPRS protocol are used (*GPRS Tunnelling Protocol e Sub Network Dependent Convergence Protocol*) as for the previous case. These frames are open by the GGSN and embedded in the *L2TP tunnelling* towards LNS.

Naturally both TE and GGSN/LNS must implement the PPP protocol.