Meeting the Challenges of a Successful GPRS Network Operation

Managing Quality of Service, Security, Roaming Scenarios and Charging Functions in the New GPRS Packet-Switched Domain

Mobile network operators face many new challenges with the introduction of the General Packet Radio Service (GPRS) as an overlay to the existing GSM circuit switched environment. GPRS networks incorporate new capabilities, services and concepts, and the new packet switched domain dramatically changes how we manage the overall network. A suite of integrated monitoring and analysis tools can help you meet the challenges and optimize the return from the upgraded resources.

This application note describes four key components of GPRS network operation – quality of service, security, roaming scenarios and charging functions – and demonstrates how the new NET-GPRS suite of network analysis applications provides the insight needed to improve network performance and customer satisfaction.

New Concepts for Quality of Service, Roaming and Charging in GPRS Networks

Packet switched services expand the definitions of Quality of Service, roaming and charging to include many new concepts that reflect the special characteristics of data transfers through a mobile wireless network.

Quality of Service Profiles

A GPRS network includes five classes of performance attributes that determine the allocation of network resources. Various levels of these attributes are combined to create a variety of Quality of Service (QoS) Profiles. Network operators are able to offer their subscribers a wide choice of QoS profiles and rates that reflect the specified levels of service they provide.

Tektronix
Enabling Innovation

The mobile station requests the desired QoS profile during a PDP context activation procedure. If this profile is beyond the capabilities of the network at that moment, the network negotiates a QoS profile that is as close as possible to the one that was requested. At this point the mobile station either accepts the negotiated QoS profile or does not activate the PDP context.

ETSI has standardized the definition of QoS Profile to include:

- Service Precedence Class
- Delay Class
- Reliability Class
- Peak Throughput Class
- Mean Throughput Class

GPRS – Packet-Switched Communications in GSM Wireless Mobile Systems

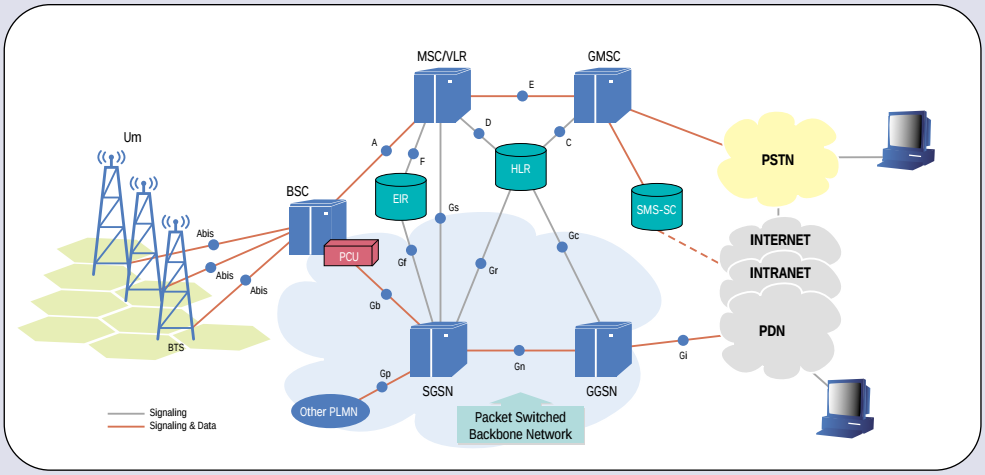
ETSI developed the GPRS standard to create a sound foundation for packet switching in existing GSM networks. The standard defines central requirements such as point-to-point data transfer, point-to-multipoint support, identities, coding schemes, billing schemes based on data volume, security features and TCP/IP and X.25 bearer capabilities. The strict separation of the Base Station Network Subsystem and the Network Switching Subsystem via an open interface enables multi-vendor environments and supports the evolution to UMTS where a new radio access network is attached to the NSS.

Packet switched methods are applied to the efficient transfer of both data and signaling information. Using encapsulation and tunneling techniques, data is transparently transferred between the mobile station and the external packet data network. GPRS supports the most common data protocols (IP and X.25) and is open for the addition of other interoperability protocols in the future. Direct access to external data packet networks helps to increase data transmission rate and reduces call establishment time. Security features such as ciphering and authentication are identical to those in existing GSM networks.

One of the most significant differences that GPRS introduces to existing GSM networks is the method of managing the air interface. Dynamic channel allocation, channel bundling and new coding schemes allow us to make more efficient use of the air interface and offer a variety of cost/performance choices to subscribers.

A cell's physical channels can be dynamically allocated for circuit switched and packet switched use. For example, in a cell with two transceivers, there are 14 physical channels available to transmit traffic. The operator can ensure a call completion probability of 98% for circuit switched calls by using less than 9 physical channels, on average, leaving 5 channels as spares for peak traffic situations. With GPRS, those spare resources can be used to carry packet switched traffic. As circuit switched traffic increases, more physical channels can be allocated for circuit switched use on demand and some packet switched users may have to wait to continue downloading their data.

Increased data transmission rates are achieved using channel bundling and new coding schemes. Up to 8 timeslots per TDMA frame can be combined. Depending on the codec speed, this allows for theoretical transmission speeds of up to 171.2 kbit/s (8 timeslots @ 21.4 kbit/s). Uplink and downlink resources are allocated separately and asymmetrically – each may differ in size,capacity and rate.



▶ ***Figure 1:*** *GPRS overall network architecture*

- Service Precedence Class

Under normal circumstances all users accessing GPRS services are treated equally, but there are times when network congestion or overloaded resources make it impossible to maintain full service for all. The Service Precedence Class assigns the relative importance of handling user transactions during abnormal periods according to Table 1.

- Delay Class

The Delay Class groups into categories the end-to-end transfer delay incurred in the transmission of packets through the GPRS network.

In the **uplink** path it includes:

- Radio channel access delay
- Radio channel transit delay
- GPRS network links transit delay

In the **downlink** path it includes:

- GPRS network links transit delay
- Radio channel scheduling delay
- Radio channel transit delay

The delay is measured between the R interface and the Gi interface (Figure 1); it does not account for transit delays due to non-GPRS external networks. The delay class categories are shown in Table 2.

Table 1 – Service Precedence Class Transaction Priorities

Service Precedence	Service Precedence Class	Description Name
1	High priority	Service commitments shall be maintained ahead of precedence classes 2 and 3
2	Normal priority	Service commitments shall be maintained ahead of precedence class 3
3	Low priority	Service commitments shall be maintained after precedence classes 1 and 2

Table 2 – Delay Class Categories

	Delay (maximum values)			
	SDU size: 128 octets		SDU size: 1024 octets	
	Mean Transfer Delay (sec)	95 percentile Delay (sec)	Mean Transfer Delay (sec)	95 percentile Delay (sec)
1. (Predictive)	< 0.5	< 1.5	< 2	< 7
2. (Predictive)	< 5	< 25	< 15	< 75
3. (Predictive)	< 50	< 250	< 75	< 375
4. (Predictive)	Unspecified			

Table 3 – Reliability Class Categories

Reliability Class	GTP Mode	LLC Frame Mode	LLC Data Protection	RLC Block Mode	Traffic Type
1	Acknowledged	Acknowledged	Protected	Acknowledged	Non real-time traffic, error-sensitive application that cannot cope with data loss
2	Unacknowledged	Acknowledged	Protected	Acknowledged	Non real-time traffic, error-sensitive application that can cope with infrequent data loss
3	Unacknowledged	Unacknowledged	Protected	Acknowledged	Non real-time traffic, error-sensitive application that can cope with data loss, GMM/SM and SMS
4	Unacknowledged	Unacknowledged	Protected	Unacknowledged	Real-time traffic, error-sensitive application that can cope with data loss
5	Unacknowledged	Unacknowledged	Unprotected	Unacknowledged	Real-time traffic, error non-sensitive application that can cope with data loss

- Reliability Class

When packets are traveling through the GPRS network from the R interface to the Gi interface they are transported by different interfaces that use different protocol stack layers and a variety of transport mechanisms. The reliability class specifies the characteristics of network protocol layers to ensure that predefined residual error rate limits are met for the following parameters:

- Probability of data loss
- Probability of data delivered out of sequence
- Probability of duplicate data delivery
- Probability of corrupted data

The reliability class categories are listed in Table 3.

- Peak Throughput Class and Mean Throughput Class

The peak throughput and the mean throughput rates are measured on the R and Gi interface respectively in units of octets per second and octets per hour. They specify the maximum rate and the average rate at which packets within a PDP context are to be transferred across the GPRS network.

The peak throughput class categories are shown Table 4. The mean throughput class categories are shown in Table 5.

Table 4 – Peak Throughput Class Categories

Peak Throughput Class	Peak Throughput in octets per second
1	Up to 1000 (8 kbit/s)
2	Up to 2000 (16 kbit/s)
3	Up to 4000 (32 kbit/s)
4	Up to 8000 (64 kbit/s)

Table 5 – Mean Throughput Class Categories	
Mean Throughput Class	Mean Throughput in octets per hour
1	100 (~0.22 bit/s)
2	200 (~0.44 bit/s)
3	500 (~1.11 bit/s)
4	1000 (~2.2 bit/s)
5	2000 (~4.4 bit/s)
6	5000 (~11.1 bit/s)
7	10000 (~ 22 bit/s)
8	20000 (~44 bit/s)
9	50000 (~111 bit/s)
10	100000 (~0.22 kbit/s)
11	200000 (~0.44 kbit/s)
12	500000 (~1.11 kbit/s)
13	1000000 (~2.2 kbit/s)
14	2000000 (~4.4 kbit/s)
15	5000000 (~11.1 kbit/s)
16	10000000 (~22 kbit/s)
17	20000000 (~44 kbit/s)
31	Best effort

Examples of Degraded Quality of Service

Inadequate Network Capacity Planning Limits Availability of QoS Profiles

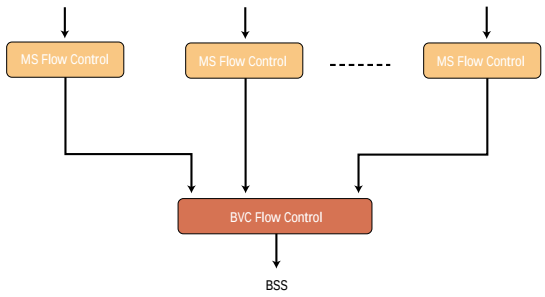
A discrepancy between the requested QoS profile and the negotiated QoS profile may be caused by shortcomings in:

- Radio resource allocation (not enough timeslots reserved for GPRS, signaling channels not properly dimensioned)
- Provisioning of core network resources (GSNs are not able to sustain a high number of attached users, GSNs are not able to provide a high number of concurrent tunnels)
- Interconnections to external ISP or PDN (packet delays introduced by external connected networks that do not respect SLAs)

Forwarding Rates and Latency Cause Bottlenecks in Data Flow

One of the main functions of the BSSGP protocol on the Gb interface is to provide control of the flow of data between the SGSN and the BSS in the downlink direction. The flow control mechanism is used by the BSS to adjust the amount of buffered packets in order to efficiently use the available radio resources. When queued packets in the BSS buffers are not transferred over the radio interface within a defined time interval, they are deleted and need to be retransmitted by upper protocol layers – reducing the overall throughput and increasing transit delay. (Note: uplink flow is not controlled, so uplink buffers and link capacity must be properly dimensioned in order to avoid loss of uplink data.)

In the BSS there is one downlink buffer for each BVC that in most cases contains downlink traffic for a single specific cell. The BSS controls the flow of data to its BVC buffers by indicating to the SGSN the maximum allowed total throughput for each BVC and for an MS within that BVC. Flow control is performed on each LLC-PDU – first by the MS flow control mechanism and then by the BVC flow control mechanism (Figure 2). If an LLC-PDU is passed by both flow control mechanisms, the entire LLC-PDU is delivered to the NS for transmission to be BSS.



▶ ***Figure 2:*** *MS and BVC flow control mechanism*

Mobility Management Procedures Slow Down Data Rate

When an SGSN detects a cell change from a moving MS, it has to reorganize the LLC-PDUs that have been stored in the buffers of the BSS (queued for that specific MS) to a cell update or a routing area update. The LLC-PDUs can be either deleted or transferred to a new buffer. Deleted LLC-PDUs would need to be retransmitted, reducing the overall throughput, while transferred LLC-PDUs would experience an increased latency.

Delays in External Network Increase GPRS Signaling Overhead

When an MS requests access to a web page on the Internet, the GPRS network must send a specific URL to the WWW and wait for a response from the web server. When the MS sends the request, the Mobility Management Context in the MS is in the READY state and the SGSN knows the cell location of the MS. If the response from the web server is received within a determined time interval, the SGSN immediately sends the PDP PDUs to the MS. However, if WWW congestion delays the response past that time interval, the Mobility Management Context in the MS switches to STANDBY state and the SGSN retains only the Routing Area for the MS. Before it can send the PDP PDUs the SGSN must execute the paging procedure to locate the mobile station cell, introducing signaling overhead in the network and increasing transmission delays.

User Data and Signaling Security

Security and privacy are critical concerns when data transmission is performed over the air in a cellular environment, especially for those GPRS services involving transactions that require sensitive data, such as bank account numbers, passwords, PIN codes or credit card numbers to be exchanged. In order to protect such information both signaling and data can be ciphered on the air interface. Due to GPRS network architecture, such ciphering interests also signaling and data traveling on the Gb interface.

If ciphering is applied on the Gb interface, some critical GPRS procedures (PDP Context Activation, for example) and usual subscriber activity (HTTP retrieval of a specific URL, for example) may be ciphered and consequently will not be visible using normal instrumentation.

The first protocol layer to guarantee a reliable logical link for peer to peer communication between the MS and the SGSN is the LLC. Among other functionality, the LLC may provide data confidentiality by performing ciphering/de-ciphering of data and signaling frames.

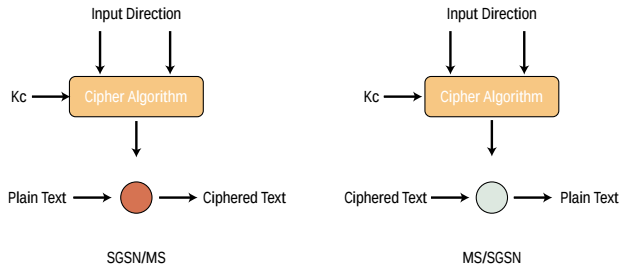
In GPRS networks, where uplink (from MS to SGSN) and downlink (from SGSN to MS) data and signaling transfer are independent from each other, ciphering for uplink and downlink is also independent from one another.

The LLC ciphering/de-ciphering algorithm is installed in the SGSN and in the MS.

The inputs for the ciphering/de-ciphering algorithm are:

- CIPHERING KEY Kc which is generated in the GPRS authentication and key management procedure
- INPUT which depends on the LLC frame type to be ciphered
- DIRECTION which identifies uplink or downlink transmission

The most important parameter is the Kc which is exchanged between the MS and the SGSN.



▶ ***Figure 3:*** *ciphering/de-ciphering algorithm*

In the uplink direction, when data and signaling must be transferred from the MS to the SGSN, the LLC in the MS may cipher all the frames coming from upper protocol layers. These frames travel ciphered first over the Um air interface, then over the Abis interface, and finally over the Gb interface. As soon as these frames get to the SGSN, they are de-ciphered again by the LLC and are then available for further use.

In the downlink direction, when data and signaling have to be transferred from the SGSN to the MS, the LLC may cipher all the frames coming from upper protocol layers. These frames travel ciphered first over the Gb interface, then over the Abis interface, and finally over the Um air interface. As soon as these frames get to the MS, they are de-ciphered again by the LLC and are available for further use.

The frames coming from upper protocol layers belong to three categories: SNDCP, SMS, GMM/SM.

- The SNDCP encapsulates user data typically coming from TCP/IP applications used by the GPRS subscriber; e.g. web browser, mail client, etc.
- The SMS encapsulates short messages to be sent over GPRS.
- The GMM/SM encapsulates signaling information for GPRS Mobility Management and for GPRS Session Management; e.g., Cell Update, PDP Context Activation, etc.

All these frames may be ciphered by the LLC. Therefore, unlike in GSM where only user data (voice) may be ciphered, in GPRS signaling data may also be ciphered.

Roaming – Home and Visited Networks

The packet-switched domain brings a new level of complexity to the concept of roaming. Home and Visited Public Land Mobile Networks (PLMNs) are used to verify status and direct visitor traffic for both in-roaming and out-roaming activities.

When a user subscribes with a GPRS mobile network operator, the network infrastructure owned by that operator is referred to as the HPLMN (Home Public Land Mobile Network). When a user accesses GPRS services on a network other than his HPLMN, the infrastructure is referred to as a VPLMN (Visited Public Land Mobile Network).

When accessing a VPLMN, an MS must first perform the GPRS attach procedure to the SGSN in the VPLMN (VSGSN). If this is the initial attachment, the SGSN communicates with the HLR in the HPLMN in order to verify that the user is allowed to roam before it accepts the MS within the VPLMN.

The VPLMN decides which of two roaming scenarios to activate based on information provided by the subscriber during GPRS PDP context activation and user profile information supplied by the HPLMN operator in the HLR.

- Scenario 1 - the MS connects to the VSGSN and creates GTP tunnels with the HGGSN
- Scenario 2 - the MS connects to the VSGSN and creates GTP tunnels with the VGGSN

Static and Dynamic IP Addresses

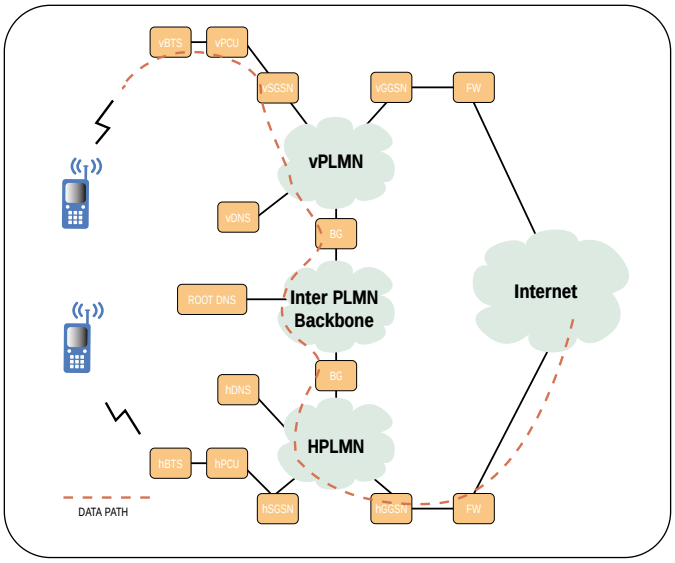
Each GPRS network element that interfaces with the Inter PLMN IP Backbone is identified by a unique IP address that is then managed and distributed by a single entity. The VSGSN then uses that IP address to create the GTP tunnel.

The VSGSN interrogates a DNS server which resolves the APN into the IP address of the GGSN to be used. In the first roaming scenario, the VPLMN DNS cannot directly resolve the APN locally and queries the DNS in the HPLMN that in turn provides the HGGSN IP address. In the second roaming scenario, the VPLMN DNS is able to resolve the APN into a GGSN IP address within the VPLMN.

During the PDP context activation procedure the user is assigned an IP address which can be either Static or Dynamic. Static IP Addresses are mapped to specific users. The mapping between static IP address and user IMSI is found in the user's subscription record in the HLR. During the GPRS Attach to the VPLMN, a copy of the user's subscription details is sent to the VSGSN by the HLR. At PDP Context Activation Accept, this address is passed to the MS. A Static IP address limits the user to establishing GTP tunnels only with the HGGSN in the HPLMN using specific APNs (Scenario 1, above).

The establishment of GTP tunnels in the VPLMN via VGGSNs (Scenario 2) requires Dynamic Allocation of IP addresses to the user. A Dynamic IP Address is mapped to the user only at context activation and may change every time a new PDP context activation takes place for the same user. The VGGSN assigns the dynamic IP address to the user and then forwards the result to the MS during the PDP Context Activation Accept procedure.

Scenario 1 – The MS Registers on the VPLMN Using the VSGSN and the HGGSN



▶ ***Figure 4:*** *VSGSN and HGGSN roaming scenario*

VSGSN and HGGSN-PLMN Roaming

Scenario 1 uses the Inter-PLMN backbone to exchange data and signaling in order to establish the context. See figure 4. The Inter PLMN backbone can be based on either direct connections between PLMNs using leased lines, tunneling via public IP networks or tunneling via a dedicated GPRS roaming network owned by a GRX. (A GRX is an independent company that provides interconnect services for the transportation of IP traffic between two or more GPRS network operators.)

Scenario 1 requires:

- VSGSN–HLR communication via the Gr interface, using SS7 MAP procedures on inter network links
- Either inter network DNS interactions or GPRS root DNS information exchange
- Inter PLMN backbone connectivity for GTP tunnels and IP address management
- Border gateway involvement and firewall configuration

The GPRS **root DNS** is a Domain Name Server that is either contained within the GPRS PLMN or located outside the network and controlled by an external party.

Border Gateways are similar to routers and firewalls – their primary function is to protect the GPRS PLMN from external intrusion. They provide message screening capabilities, filtering of unwanted signaling and traffic coming from other GPRS PLMNs, Inter Network Secure Tunneling and encryption that can be determined on a per-roaming agreement basis to guarantee the security of the data being transferred between PLMNs.

Scenario 2 – The MS Registers on the VPLMN Using the VSGSN and the VGGSN

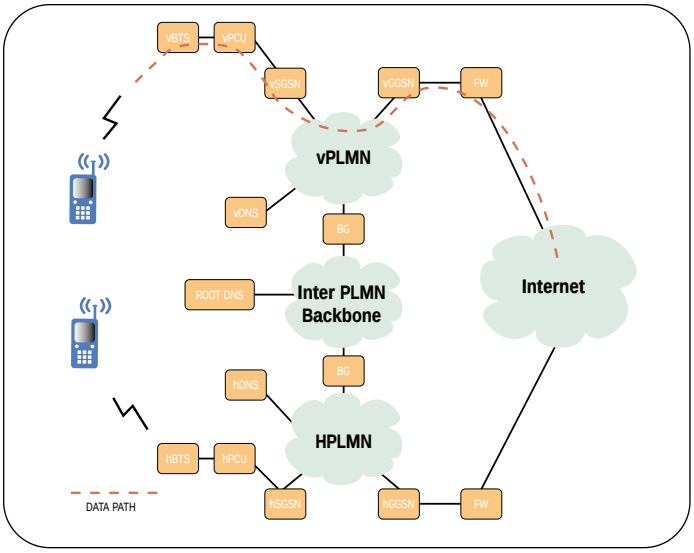


Figure 5: *VSGSN and VGGSN roaming scenario*

VSGSN and VGGSN-ISP Roaming

In Scenario 2, all data and signaling exchanges are made within the VPLMN using the Intra PLMN Backbone to establish the context, see figure 5. This scenario requires only VSGSN–HLR communication via the Gr interface, using SS7 MAP procedures on inter network links and Dynamic IP address allocation for the mobile user.

Charging – Collecting Transaction Information from All Network Nodes

GPRS networks derive charging information for each user transaction into Call Detail Records (CDRs) from SGSNs and GGSNs. Billing is typically based on the amount of data transferred – a more appropriate pricing scheme for bursts of data, since rates are based on actual usage rather than the overall connection time (as used for circuit-switched calls).

The Charging Gateway Functionality (CGF) provides the mechanism to transfer charging information from the GPRS Support Nodes (GSNs) to the Billing System (BS). The CGF can be a separate centralized element or it can be distributed among GPRS Support Nodes. The main functions of the CGF are:

- GPRS CDRs collection from GSNs
- Intermediate CDRs processing and buffering
- CDRs transfer to the BS

The CGF can be implemented:

- In the Charging Gateway (CG) with a separate centralized architecture
- In the GPRS Support Nodes (GSNs) with a distributed architecture
- In both the CG and the GSNs with a combination of centralized and distributed architecture

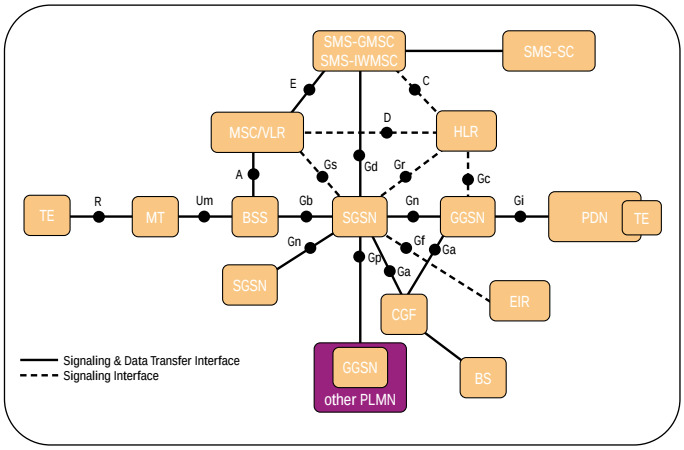


Figure 6: *GPRS network logical architecture*

When the CGF is implemented with a separate centralized architecture, a new interface named “Ga” and a new protocol named “GTP’” have been developed to transfer CDRs from the GSNs to the CGF, as shown in Figure 6. The GTP’ protocol provides:

- Either a best effort or a reliable way to send CDRs from the GSNs to the CGF
- Detection of communication failure among the GSNs handling CDRs
- Redirection of CDR transfer to other CGFs in case of network failure
- Prevention of sending duplicate CDRs

Charging information is collected for each MS by the SGSNs and GGSNs which are serving that MS. The SGSN collects charging information related to the radio network usage, while the GGSN collects charging information related to the external data network usage. Both GSNs also collect charging information on usage of the GPRS network resources. The Charging ID is used to correlate CDRs coming from different GSNs (S-CDRs and G-CDRs), but related to the same user transaction.

There are five different types of CDRs:

- S-CDR
- G-CDR
- M-CDR
- S-SMO-CDR
- S-SMT-CDR

S-CDRs are produced by the SGSNs and are available for each PDP context, as shown in Table 6.

G-CDRs are produced by GGSNs and are available for each PDP context, as shown in Table 7.

M-CDRs are produced by the SGSNs and are available for each attached MS, as shown in Table 8.

Table 6: S-CDRs

Mandatory Parameters	Record Type, Served IMSI, SGSN address, Charging ID, GGSN address used, Access Point Name Network Identifier, PDP type, Served PDP address, List of traffic data volumes, Record opening time, Duration, Cause for record closing, Access Point Name Operator Identifier
Conditional Parameters	Network Initiated PDP context, Anonymous Access Indicator, Served IMEI, Record Sequence Number
Optional Parameters	MS Network Capability, Routing Area, Location Area Code, Cell Identity, APN Selection Mode, Diagnostics, Node ID, Record Extensions, Local Record Sequence Number

Table 7: G-CDRs

Mandatory Parameters	Record Type, Served IMSI, GGSN Address, Charging ID, SGSN Address, Access Point Name Network Identifier, PDP Type, Served PDP Address, List of Traffic Data Volume, Record Opening Time, Duration, Cause for Record Closing
Conditional Parameters	Network Initiated PDP Context, Anonymous Access Indicator, Dynamic Address Flag, Record Sequence Number
Optional Parameters	APN Selection Mode, Remote PDP Address, Diagnostics, Node ID, Record Extensions, Local Record Sequence Number

Table 8: M-CDRs

Mandatory Parameters	Record Type, Served IMSI, SGSN Address, Record Opening Time, Cause for Record Closing
Conditional Parameters	Served IMEI, SGSN Change, Record Sequence Number
Optional Parameters	MS Network Capability, Routing Area, Location Area, Cell Identity, Change of Location, Duration, Diagnostics, Node ID, Record Extensions, Local Record Sequence Number

The S-SMO-CDRs and the S-SMT-CDRs are produced by the SGSNs and are available respectively for each short message sent and received by a mobile subscriber via SGSN, as shown in Table 9.

Table 9: S-SMO and S-SMT CDRs

Mandatory Parameters	Record Type, Served IMSI, MS Network Capability, Service Centre, Recording Entity, Event Time Stamp, Message Reference
Conditional Parameters	SMS Result
Optional Parameters	Served IMEI, Served MSISDN, Location Area Code, Routing Area Code, Cell Identity, Record Extensions, Node ID, Local Record Sequence Number

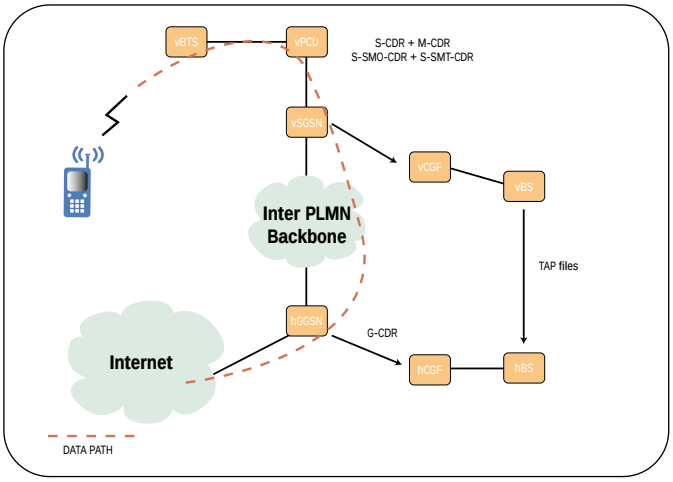


Figure 8: *External PDN while roaming using VSGSN and HGGSN charging scenario*

The following diagrams illustrate two typical charging scenarios:

- Data transfer from a GPRS MS to an external PDN, as shown in Figure 7.
- Data transfer from a GPRS MS to an external PDN while roaming using the HGGSN, as shown in Figure 8.

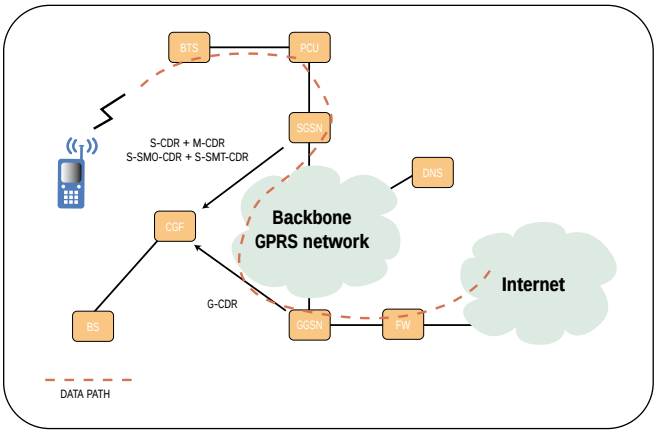


Figure 7: *MS – External PDN charging scenario*

How Network Monitoring and Optimization Tools Can Help Manage GPRS Networks

The sheer volume of new functions and information present a formidable challenge to GPRS network operators. Information must be gathered simultaneously from virtually every point in the system in order to trouble shoot problems and adequately describe QoS parameters. Real time and statistical data from actual user transactions are needed to plan resource allocations and improve customer satisfaction. Charging functions must be monitored to ensure accurate billing and protect revenues. NET-GPRS offers an integrated suite of powerful tools for network management and supervision. This section describes the NET-GPRS and shows how to use some of the tools to troubleshoot and optimize network performance, improve customer satisfaction and lower operating costs.

The NET-GPRS Network Monitoring System

The NET-GPRS from Tektronix is a non-intrusive monitoring system specifically designed to be connected to a GPRS network to collect all the activities related to the messages exchanged by different nodes. NET-GPRS uses monitoring probes connected to the network under observation, and collects and analyzes data from the probes in a central unit. The central unit displays network information to one or more users, who can be located at different user sites. No user intervention is required for normal operation of the system. Once a monitoring probe has been configured, it becomes completely autonomous – analyzing and storing data that are then collected by the central unit.

Signaling information is decoded at different protocol layers to provide on-line real-time information to the operator and off-line analysis from recorded data. Statistical measurements and counters are provided at different intervals based on specific protocol messages to evaluate the performance of the signaling network. Call or transaction related information is provided by the system to allow call detail records for every call or call attempt in the network. Configuration information about the network structure is stored in the system – allowing NET-GPRS to determine, for instance, the origin and destination of each call.

NET-GPRS Applications for Troubleshooting and Optimizing Network Performance and QoS

Network Status Monitoring

NET-GPRS offers an intuitive view of links to be monitored based on graphical representation of the GPRS network. Real-time alarms are available both on the monitored streams and on the monitoring equipment. For example, excessive Frame Relay errors on the Gb interface, degraded PCM signal quality on the Gr interface, or 10/100 Mbit/s Fast Ethernet loss of signal on the Gn interface are visualized in real time with both textual and graphical coloured warnings. Self-diagnostic alarms are also available to give a clear indication on the status of monitoring equipment.

Automatic De-ciphering of Gb Interface Signaling

If ciphering is applied on the Gb interface, some critical GPRS procedures, such as PDP Context Activation, and usual subscriber activity, such as HTTP get of a specific URL, may be ciphered and consequently not be visible using normal instrumentation. Thanks to the NET-GPRS capability of automatically decipher signaling and data flowing through the Gb interface, NET-GPRS Protocol Analysis and Procedure Trace have full access to the content of all protocol messages, just as if ciphering was not applied.

If ciphering is applied on the Gb interface, the SGSN has to cipher frames for downlink transfer going towards the MS and de-cipher frames in the uplink direction coming from the MS. This ciphering/de-ciphering operation puts additional burden on top of the usual switching operations carried out by the SGSN. Under these circumstances, it is crucial to verify and test whether the SGSN is behaving properly. Looking at the protocol messages traveling on the Gb interface, it is possible to find out information on the behavior of the SGSN. Since ciphering is applied on the Gb interface, normal instrumentation other than the NET-GPRS system is blind with respect to ciphered protocol messages. Using normal instrumentation other than the NET-GPRS system, the only chance to have full access to the content of all ciphered protocol messages traveling on the Gb interface is to switch ciphering off in the SGSN. Obviously, by switching off ciphering, the behavior of the SGSN changes, and therefore troubleshooting is carried out in an unreal situation.

The NET-GPRS system, eliminates the requirement to switch off ciphering in order to carry out troubleshooting campaigns. While ciphering on the Gb interface is switched on and guarantees security and privacy to subscribers, the NET-GPRS deciphering engine enables NET-GPRS applications to fully investigate data and signaling exchanged over the Gb interface.

Protocol Analysis

The NET-GPRS system captures all protocol messages flowing through new Frame Relay and IP based interfaces, as well as traditional and enhanced standard GSM and SS7 interfaces. Detailed analysis and filtering on protocol messages can be performed from a single central location in real time and on data previously stored to identify and solve problems.

Procedure Trace

GPRS Procedure Trace allows tracing of subscribers' packet switched data "calls" within the GPRS network by correlating information coming from different interfaces, contained in different protocol stacks and related to transactions taking place in different geographical areas of the network. By triggering on a specific user and selecting a specific time interval, GPRS Procedure Trace shows all the transaction carried out by that subscriber both in textual format with detailed protocol information and in graphical format with an intuitive arrow diagram representation.

More than one subscriber can be traced at the same time in the same "GPRS Procedure Trace" session.

The GPRS procedure tracing can be performed either on real time traffic or on off-line traffic previously recorded.

Should circuit switched GSM calls interrupt packet switched GPRS transactions, such GSM calls are also traced in the same "GPRS Procedure Trace" session, thus providing an integrated GSM and GPRS tracing of the subscribers' activity.

For more detailed information on NET-GPRS features and benefits see Tektronix' brochure, *NET-7 Network Monitoring System,* (Literature Number 2FW-14822-0).

Conclusion

GPRS networks introduce a number of new services and challenges to GSM network operators. The NET-GPRS suite of comprehensive integrated monitoring and analysis tools can help you meet the new challenges and optimize the return from the upgraded resources.

Tektronix is committed to the most advanced test solutions for mobile networks. As mobile networks continue to evolve through GPRS, UMTS and cdma2000, we will keep you in the forefront with the latest testing products and methods.

We welcome your comments and suggestions for improving these documents and your ideas for developing other tools to help you meet the measurement challenges of new wireless systems.

References

GSM 01.61 “Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements”, ETSI

GSM 02.60 “Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service Description; Stage 1”, ETSI

GSM 03.60 “Digital cellular telecommunications system (Phase 2+); GPRS Service Description; Stage 2”, ETSI

GSM 03.03 “Digital cellular telecommunications system (Phase 2+); Numbering, addressing and identification”, ETSI

GSM 04.08 “Digital cellular telecommunications system (Phase 2+); Mobile radio interface layer 3 specification”, ETSI

GSM 04.64 “Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Mobile Station – Serving GPRS Support Node (MS-SGSN) Logical Link Control (LLC) layer specification”, ETSI

GSM 08.16 “Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Base Station System (BSS) – Serving GPRS Support Node (SGSN) interface; Network Service”, ETSI

GSM 08.18 “Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Base Station System (BSS) – Serving GPRS Support Node (SGSN); BSS GPRS Protocol”, ETSI

GSM 09.02 “Digital cellular telecommunications system (Phase 2+); Mobile Application Part (MAP) specification”, ETSI

GSM 09.60 “Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); GPRS Tunneling Protocol (GTP) across the Gn and Gp Interface”, ETSI

GSM 12.15 “Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); GPRS Charging”, ETSI

IETF RFC 1034 “Domain Names – Concepts and Facilities”

IETF RFC 1035 “Domain Names – Implementation and Specification”

IETF RFC 1918 “Address Allocation for Private Intranets”

PRD IR.34: “Inter-PLMN Backbone Guidelines”

PRD IR.35: “End to End Functional Capability specification for Inter-PLMN GPRS Roaming”

PRD SE.20 “GPRS and WAP Service Guidelines”

Acronyms

APN	Access Point Name
BG	Boarder Gateway
BS	Billing System
BSS	Base Station Subsystem
BSSGP	Base Station Subsystem GPRS Protocol
BVCI	BSSGP Virtual Connection Identifier
CDR	Call Detail Record
C-ID	Charging ID
CGF	Charging Gateway Functionality
DNS	Domain Name Server
G-CDR	Gateway GPRS Support Node – Call Detail Record
GGSN	Gateway GPRS Support Node
GMM/SM	GPRS Mobility Management and Session Management
GMSC	Gateway MSC
GPRS	General Packet Radio Service
GSN	GPRS Support Node
GTP	GPRS Tunneling Protocol
HLR	Home Location Register
HTTP	Hyper Text Transfer Protocol
IETF	Internet Engineering Task Force
IMSI	International Mobile Subscriber Identity
IWMSC	Inter Working MSC
IP	Internet Protocol
ISP	Internet Service Provider
LLC	Logical Link Control
M-CDR	Mobility Management – Call Detail Record
MS	Mobile Station
MSC	Mobile Switching Center
MT	Mobile Terminal
NSS	Network Switching Subsystem
NE	Network Element
PCM	Pulse Code Modulation
PDN	Packet Data Network
PDP	Packet Data Protocol
PDU	Protocol Data Unit
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
SC	SMS Center
S-CDR	Serving GPRS Support Node – Call Detail Record
S-SMO-CDR	SGSN delivered Short message Mobile Originated – Call Detail Record
S-SMT-CDR	SGSN delivered Short message Mobile Terminated – Call Detail Record
SS7	Signaling System number 7
SGSN	Serving GPRS Support Node
SLA	Service Level Agreement
SMS	Short Message Service
SNDCP	Sub Network Dependent Convergence Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TDMA	Time Division Multiple Access
TE	Terminal Equipment
UMTS	Universal Mobile Telecommunication Service
URL	Universal Resource Locator
VLR	Visitor Location Register
WWW	World Wide Web

Contact Tektronix:

ASEAN Countries (65) 356-3900

Austria +43 2236 8092 262

Central Europe & Greece +43 2236 8092 301

Belgium +32 (2) 715 89 70

Brazil & South America 55 (11) 3741-8360

Canada 1 (800) 661-5625

Denmark +45 44 850 700

Finland +358 (9) 4783 400

France & North Africa +33 (0) 1 69 86 80 34

Germany +49 (221) 94 77 400

Hong Kong (852) 2585-6688

India (91) 80-2275577

Italy +39 (02) 25086 1

Japan (Sony/Tektronix Corporation) 81 (3) 3448-3111

Mexico, Central America & Caribbean 52 (5) 666-6333

The Netherlands +31 (0) 23 569 5555

Norway +47 22 07 07 00

People's Republic of China 86 (10) 6235 1230

Poland +48 (0) 22 521 53 40

Republic of Korea 82 (2) 528-5299

Russia, CIS & The Baltics +358 (9) 4783 400

South Africa +27 11 254 8360

Spain +34 (91) 372 6055

Sweden +46 8 477 6503/4

Taiwan 886 (2) 2722-9622

United Kingdom & Eire +44 (0) 1344 392400

USA 1 (800) 426-2200

For other areas contact Tektronix, Inc. at: 1 (503) 627-7111

Updated October 30, 2001

For Further Information
Tektronix maintains a comprehensive, constantly expanding collection of application notes, technical briefs and other resources to help engineers working on the cutting edge of technology. Please visit **www.tektronix.com**

02/02 BC/BT 2FW 14877-0

Tektronix
Enabling Innovation