



GSMA PRD IR.33 - "GPRS Roaming Guidelines"

3.4

21 July 2009

This is a non-binding permanent reference document of the GSM Association.

Security Classification – NON-CONFIDENTIAL GSMA Material

Copyright Notice

Copyright © 2009 GSM Association

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Security Classification: Unrestricted

This document is subject to copyright protection. The GSM Association (“Association”) makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice. Access to and distribution of this document by the Association is made pursuant to the Regulations of the Association.

Copyright Notice

Copyright © 2009 GSM Association

GSM™ and the GSM Logo™ are registered and the property of the GSM Association.

Document History

Version	Date	Brief Description
0.0.1	22 June 1999	Table of Contents presented at IREG GPRS #4 meeting and commented upon
0.0.2	20 August 1999	First draft of document for IREG GPRS group discussion (5 th Meeting)
1.0	21 September 1999	Issued First Version for approval
1.0.1	22 September 1999	Modified Section 8.2 for approval
2.0	23 September 1999	Approved by IREG#37
3.0	1 October 1999	PL Doc 162/99. Approved at Plenary 42
3.1	27 April 2000	CR#01, PL Doc 032/00 approved at Plenary 43
3.2	3 April 2003	SCR 02
3.3	15 October 2004	SCR 03: New section for descriptions of new GTP features and associated configuration.
3.4	21 July 2009	CR 04: Remove duplicate and redundant information, and general tidy-up.
Changes Since Last Version: See above		

Other Information

Type	Description
Document Owner	GSMA IREG Packet
Revision Control	As Required
Document editor/company	Massimo Chiavacci, Telecom Italia Sparkle

Feedback

This document is intended for use by the members of GSMA. It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at <mailto:prd@gsm.org>. Your comments or suggestions are always welcome.

Table of Contents

1	Introduction	4
2	Overview	4
2.1	Architecture and Interfaces	4
2.2	Roaming Scenarios.....	5
2.2.1	<i>Introduction</i>	5
2.2.2	<i>Scenario 1 - HGGSN Roaming</i>	5
2.2.3	<i>Scenario 2 - VGGSN Roaming</i>	6
3	Technical Requirements & Recommendations	7
3.1	Fundamental GPRS Functionality	7
3.1.1	<i>Introduction</i>	7
3.1.2	<i>Inter-PLMN IP backbone network requirements</i>	7
3.1.2.1	IP address & routing.....	7
3.1.2.2	DNS.....	7
3.1.3	<i>Access Point Name (APN)</i>	8
3.1.3.1	General	8
3.1.3.2	APN Components.....	8
3.1.3.3	Types of APN.....	11
3.1.4	<i>User IP Address Allocation</i>	12
3.1.4.1	Introduction	12
3.1.4.2	Static User IP Address Allocation.....	12
3.1.4.3	Dynamic User IP Address Allocation	13
3.2	Additional GPRS Functionality	13
3.2.1	<i>Introduction</i>	13
3.2.2	<i>Control of multiple, concurrent PDP Contexts</i>	13
3.2.2.1	Definition	13
3.2.2.2	Recommendations	14
3.2.3	<i>Flow Based Charging</i>	14
3.2.3.1	Definition	14
3.2.3.2	Recommendations	15
3.2.4	<i>Automatic Device Detection</i>	15
3.2.4.1	Definition	15
3.2.4.2	Recommendations	15
3.2.5	<i>Direct Tunnel Functionality</i>	15
3.2.5.1	Definition	15
3.2.5.2	Recommendations	16
4	References	16
5	Annex A: Known Issues and Solutions	16
5.1	GTP version 0 and version 1 Interworking Problem.....	16
5.1.1	<i>Introduction</i>	16
5.1.2	<i>VPLMN solution</i>	17
5.1.3	<i>HPLMN solution</i>	17
5.2	IP source address of GTPv1 response messages.....	17
5.3	GPRS QoS Classes.....	18

1 INTRODUCTION

This document aims to provide a standardised view on how GPRS networks can interwork in order to provide GPRS capabilities when users roam onto a network different from their HPLMN.

It makes references to current 3GPP specifications for GPRS, and also other GSMA PRDs where necessary, in particular GSMA PRD IR.34 [8] and GSMA PRD IR.35 [9].

Throughout this PRD, the term "GPRS" is used to denote both 2G GPRS and 3G Packet Switched ("PS") service.

2 OVERVIEW

2.1 Architecture and Interfaces

GPRS roaming is achieved using the standardised interfaces detailed in 3GPP TS 23.060 [1]. The GPRS architecture is shown below in Figure 1.

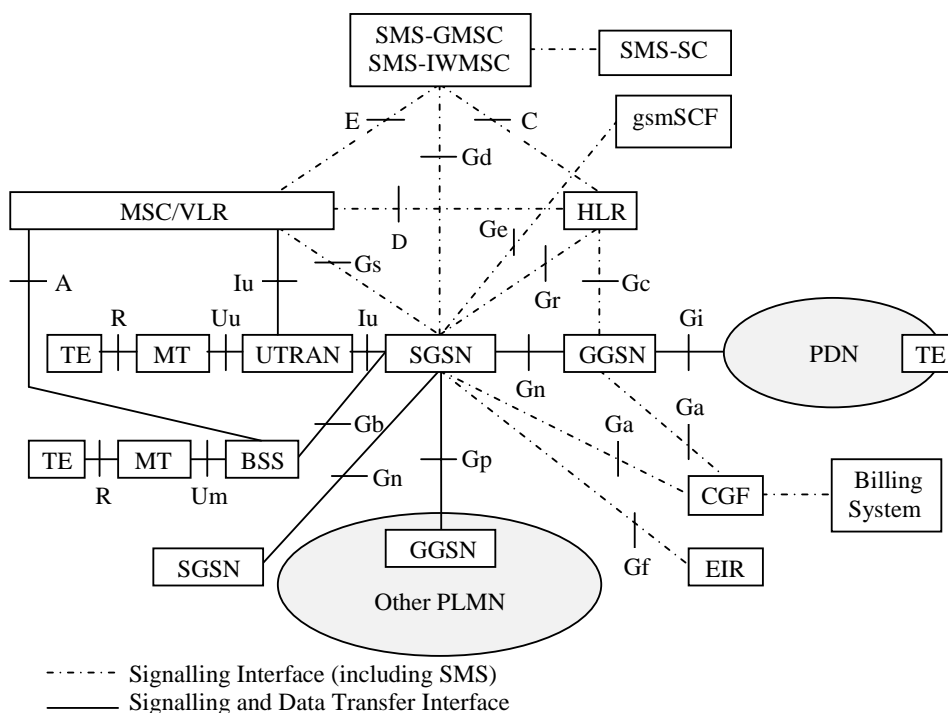


Figure 1: Overview of the GPRS Logical Architecture

See 3GPP TS 23.060 [1] for more information on the specification of each interface. Note that the "TE" and "MT" entities above are functions of the User Equipment (UE).

The following interfaces are relevant for GPRS roaming and are detailed as follows:

Nodes	Interface ID	Protocol
VERSION 3.4		
Page 4 of 18		

Nodes	Interface ID	Protocol
SGSN – HLR	Gr	MAP (3GPP TS 29.002 [3])
SGSN – SMS-IWMSC/GMSC	Gd	
SGSN – GGSN	Gn/Gp	GTP (3GPP TS 29.060 [4])
SGSN – SGSN	Gn	

Notes:

- The procedures and message flows for all the above interfaces are described in 3GPP TS 23.060 [1].
- The SGSN – SGSN interface is used in roaming only when inter-PLMN Hand Over is supported.
- The SGSN – GGSN interface when used within a single PLMN is known as the Gn interface. When used between PLMNs it is known as the Gp interface.
- The inter-PLMN DNS communications interface (used by the SGSN to find a GGSN) uses standard DNS procedures and protocol, as specified in IETF RFC 1034 [5] and IETF RFC 1035 [6].

The services that networks may support are detailed in GSMA PRD SE.20 [10].

The charging requirements for GPRS in a roaming environment are detailed in GSMA PRD BA.27 [11].

2.2 Roaming Scenarios

2.2.1 Introduction

There are two types of GPRS roaming scenarios:

- Subscribers PDP Contexts are terminated at a GGSN in the HPLMN
- Subscribers PDP Contexts are terminated at a GGSN in the VPLMN

In both scenarios, the subscriber always registers on an SGSN in the VPLMN

2.2.2 Scenario 1 - HGGSN Roaming

In this scenario, the user roams on to a VPLMN, registers on an SGSN and then activates a PDP Context to a GGSN in their home network (HGGSN). There are signalling exchanges across the Gp interface (provided by an Inter PLMN IP Backbone network e.g. GRX/IPX network) in order to establish the PDP Context, and if successful, user data is tunnelled between the two nodes.

This scenario is shown below in Figure 2, and requires:

- SGSN – HLR interactions via the Gr interface, using Inter PLMN SS7 links
- Static or Dynamic address allocation for the subscriber
- Non-Transparent (i.e. authenticated) network access-point access
- Inter PLMN DNS exchanges and possible GRX/IPX Root DNS server interactions (see GMS PRD IR.67 [13]).
- Inter PLMN Backbone connectivity and address management
- Border Gateway involvement, which may provide firewall and additional security functionality.

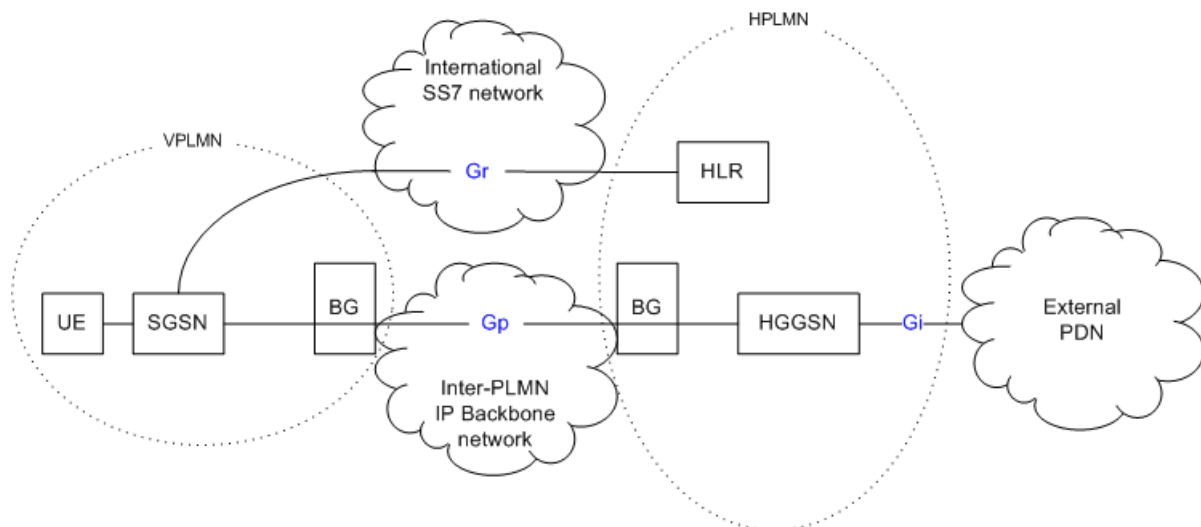


Figure 2: Scenario 1 - SGSN and HGGSN using the International Inter PLMN Backbone

2.2.3 Scenario 2 - VGGSN Roaming

In this scenario, the user roams on to a VPLMN and registers on an SGSN and then activates a PDP Context to a GGSN in the visited network (VGGSN).

There are signalling exchanges across the Gn interface (provided by an Intra-PLMN IP Backbone network) in order to establish the PDP Context, and if successful, user data is tunnelled between the two nodes.

This scenario is shown in Figure 3, and requires:

- SGSN – HLR interactions via the Gr interface, using Inter PLMN SS7 links
- Dynamic address allocation only for the subscriber
- Transparent (i.e. non-authenticated) network access-point access (see Note)
- NO inter PLMN DNS exchanges.
- NO Inter PLMN IP Backbone connectivity or address management
- NO Border Gateways involvement or firewall configuration

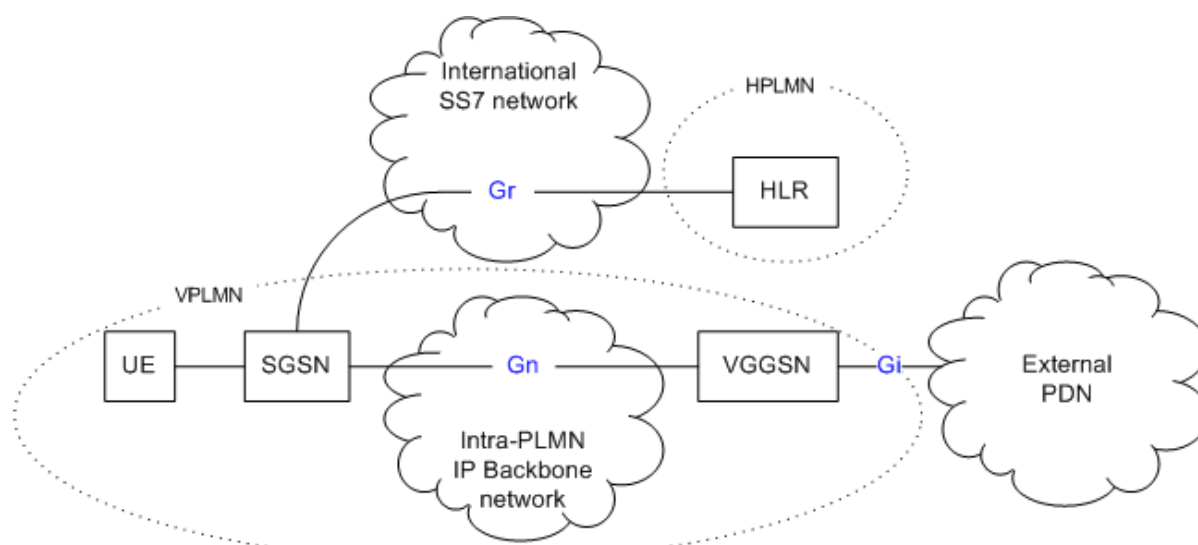


Figure 3: Scenario 2 - SGSN and VGGSN using VPLMN Intra GPRS Backbone

Note – Non-transparent network access-point access is possible, but it requires AAA (e.g. RADIUS or Diameter) servers at the VGGSN and the HGGSN sharing the same AAA data. For example: It is the responsibility of the external PDN to allow the PDP Context.

3 TECHNICAL REQUIREMENTS & RECOMMENDATIONS

3.1 Fundamental GPRS Functionality

3.1.1 Introduction

This section describes, and provides recommendations where appropriate, the fundamental GPRS and GPRS Tunnelling Protocol (GTP) functionality that is required at a minimum to enable GPRS roaming between PLMNs.

3.1.2 Inter-PLMN IP backbone network requirements

3.1.2.1 IP address & routing

The requirements in GSMA PRD IR.34 [8] and GSMA PRD IR.40 [13] shall apply for the routing and addressing within and between PLMNs for the Gn and Gp interfaces respectively. This includes the requirements on Border Gateways.

3.1.2.2 DNS

In GPRS, the SGSN utilises a DNS in order to resolve an Access Point Name (APN) (this procedure is detailed in section 3.1.3) and to resolve the FQDN of another SGSN (as used in inter-SGSN hand-overs). The DNS system used for these procedures will be hosted in accordance with the general requirements for Inter-PLMN IP backbone networks as specified in GSMA PRD IR.34 [8], and general requirements for DNS as specified in GSMA PRD IR.67 [13].

Since user data is encapsulated in GTP packets, the user cannot "see" the GRX/IPX network. As such, any FQDNs in URLs or any other addressing should be resolved by the

Internet DNS. Care should be taken by the PLMN in order to prevent DNS requests from end users being sent to the DNS used by the SGSN e.g. GRX/IPX network's DNS.

3.1.3 Access Point Name (APN)

3.1.3.1 General

The Access Point Name (APN) is an 8-bit ASCII character string that contains the user and network's desired IP access preference and is used to create the logical connection between UE and External PDN. It's maximum overall length is 100 characters.

3.1.3.2 APN Components

3.1.3.2.1 Overview

The APN consists of the following parts:

- Network ID – points to the access point within a GPRS PLMN
- Operator ID – points to a GPRS PLMN

The complete APN is a fully qualified domain name (FQDN) of the format:

<Network Identifier>.<Operator Identifier>.gprs

This is further detailed in 3GPP TS 23.003 [2], with further recommendations below.

3.1.3.2.2 Network Identifier

The Network Identifier is defined in 3GPP TS 23.003 [2] to be a string of a maximum of 63 characters, and it is recommended that its value be either a standardised value or an Internet reserved domain name (some values are prohibited, as defined in section 9.1.1 of 3GPP TS 23.003 [2]). It is used to identify the users chosen PDN to which to connect the UE and can be used to point to a GGSN in the HPLMN or in the VPLMN, depending on the presence of the "vplmnAddressAllowed" flag in the subscriber profile (enabled on a per APN, per subscriber basis, and downloaded from the HLR to the SGSN), and also the Operator Identifier appended to it either by the SGSN or by the subscriber himself.

The Network Identifier is provided by the subscriber when establishing a PDP Context. If the subscriber provides the whole APN (as depicted in 3.1.3.2.1 above), rather than just the Network Identifier, then the SGSN skips appending an Operator Identifier followed by the label ".gprs", and instead attempts to resolve the given full APN. In conjunction with the "vplmnAddressAllowed" flag in the subscriber profile, this can be used to enable the subscriber to control whether or not a HGGSN or VGGSN is used. This is depicted in Figure 9, below, where the subscriber opts to use the HGGSN.

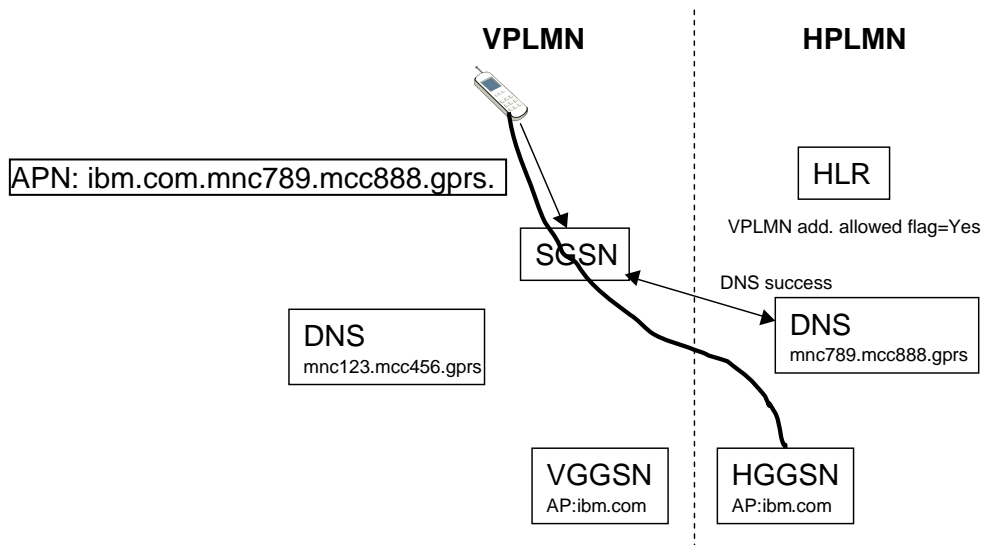


Figure 9: Subscriber enters whole APN.

In order for the subscriber to select a VGGSN, he would use the MNC and MCC of the VPLMN in the Operator Identifier part of the APN. And of course, the "vplmnAddressAllowed" flag would again have to be set by his HPLMN.

To make provisioning simpler for the subscriber, just the Network Identifier should be used (perhaps by pre-provisioning in UE or PC connection software), and control over if/when to use a VGGSN controlled by the subscriber's HPLMN.

The HPLMN can prohibit a VGGSN to be used by a subscriber for a given APN (and thus force that subscribers to always use the HGGSN for that APN), by simply disabling the vplmnAddressAllowed flag. . In this case the SGSN will append an Operator Identifier of the HPLMN to the Network Identifier, and the subscriber will then use the HGGSN, as depicted in Figure 10, below.

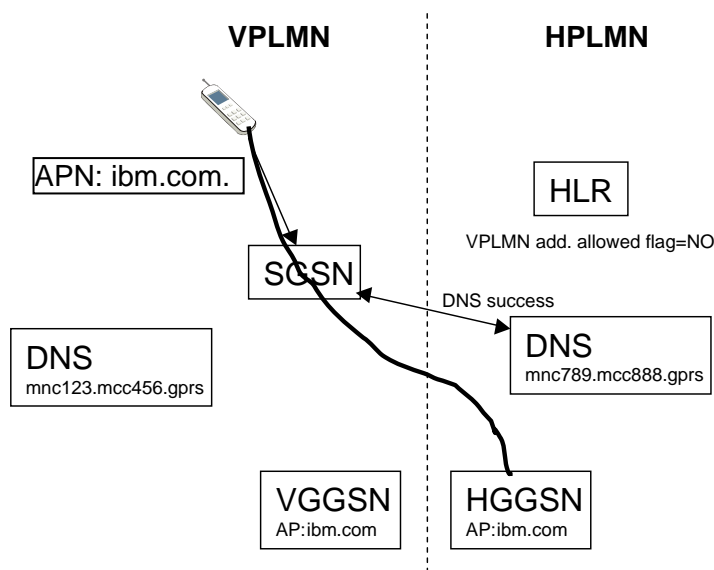


Figure 10: Subscriber has APN of ibm.com set with VPLMN allowed flag set to No.

In order to enable the subscriber to use a VGGSN for a given APN, the HPLMN simply enables the "vplmnAddressAllowed" flag, which then instructs the SGSN to append an Operator Identifier of the VPLMN to the Network Identifier.

In the subscriber supplying only a Network Identifier in the PDP Context activation and the HPLMN enabling VGGSN use by enabling the "vplmnAddressAllowed" flag, problems can arise with the PDN to which the Network Identifier points to. In particular, problems are likely to occur if a customer specific Network Identifier is shared between different parts of the company in different countries or regions. These customers may request the same value be used in the Network Identifier (e.g. the same .com or .org domain name) in different GPRS networks for the countries in which they have resident staff. This is depicted in Figure 11.

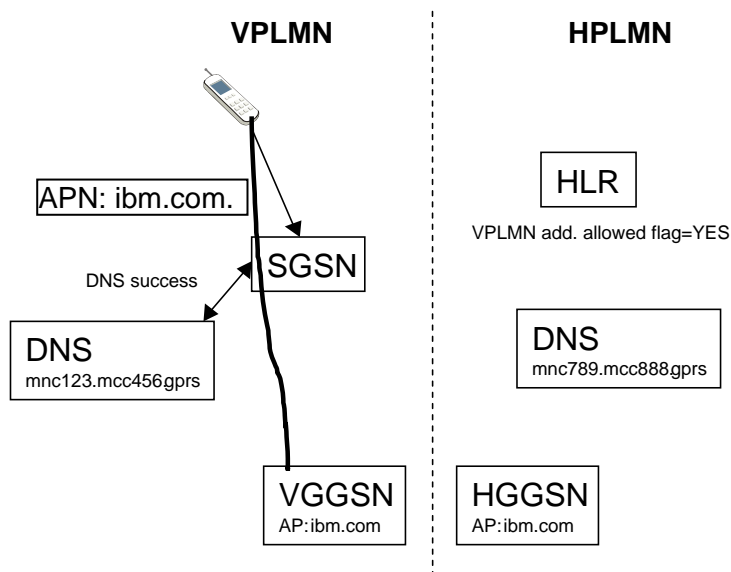


Figure 11: Visited and Home network have IBM.com as a registered Network Id

Although 3GPP TS 23.003 [2] recommends to use domain names reserved on the Internet for uniquely identifying customer specific PDNs, this solution has the disadvantage that the customer is responsible for the uniqueness of the APN Network Identifier between *all* PLMNs to which they have a subscription/commercial agreement with. The correct operation of the GPRS service thus depends on the careful behaviour of customers, which may or may not be manageable.

In order to guarantee uniqueness of APN Network Identifiers between PLMNs, the following is recommended:

- Provide only HGGSN roaming for the customer.
- If VGGSN roaming is required for the customer, then:
 - Inform the customer to not provide their chosen Internet domain name to any other PLMN with whom they will use GPRS roaming (perhaps formalised as part of a commercial agreement); or
 - Use the customer's chosen Internet domain name in conjunction with an HPLMN owned Internet reserved domain name e.g. a Network Identifier of "ibm.com.vodafone.co.uk".

3.1.3.2.3 Operator Identifier

The Operator Identifier is defined in 3GPP TS 23.003 [2]. It consists of the label "mnc" followed by the MNC and also the label "mcc" followed by the MCC, e.g. "mnc015.mcc234". Use of the HPLMN's or VPLMN's MNC/MCC is dependent on whether a HGGSN or VGGSN (respectively) is used.

GSMA PRD IR.67 [13] allows also for "human readable" Operator Identifiers. However, their usage is not widespread and cannot be guaranteed to be resolvable by SGSNs in all VPLMNs. Therefore, its usage should be limited e.g. to non-roaming scenarios only.

3.1.3.3 Types of APN

3.1.3.3.1 General

There are two types of APNs:

- Service APN
- Wildcard APN

These are both explained in the following sections.

3.1.3.3.2 Service APN

The Service APN is recognised by the APN Network Id consisting of just one label i.e. a network ID without any separating dots. This enables a Service APN to be differentiated from a normal Network Identifier. i.e. a Network Identifier that contains at least one dot.

The services to be supported and their *Service APN names* is described in GSMA PRD SE.20 [10].

If the service is not supported in the visited network, a GGSN in the home network will be used instead. In this case the resolved GGSN can vary dependent on the SGSN that makes the request (location based) or dependent on the workload of the GGSN.

The GGSN that the Service APN has resolved to must provide the service agreed upon as specified by GSMA PRD SE.20 [10].

The Service APN may provide a subscriber with transparent access to the service requested, thus removing the requirement for authentication, policing, packet filtering or NAT.

No guaranteed quality of service can be associated with a Service APN.

3.1.3.3 Wildcard APN

A Wildcard APN is an APN that contains a wildcard identifier (defined in 3GPP TS 23.003 [2] to be an asterisk - '*') stored in the subscriber's profile in the HLR and downloaded to the SGSN at attachment. This enables the following when the subscriber activates a PDP Context: .

- A "default" APN has to be chosen by the SGSN, if no APN is requested
- Any PDP Context with dynamic PDP address may be activated towards any requested APN

GGSNs have the ability to recognise if a subscriber is using the wildcard functionality, and may deny the attempted PDP Context activation. It is recommended that this functionality be enabled, in order to block subscribers attempting to fraudulently access PDNs that are not allowed access to i.e. APNs not in the subscriber profile.

3.1.4 User IP Address Allocation

3.1.4.1 Introduction

The user's IP address is allocated at PDP Context activation. The user can have either a **Static** or **Dynamic** address allocated, the former of which is valid for the whole time the user has the context activated, and the latter for the duration specified at allocation.

Note that user's IP address is **not** associated with the Inter- or Intra-PLMN IP backbone network, and strict separation of ranges used is recommended in GSMA PRD IR.40 [13].

3.1.4.2 Static User IP Address Allocation

A static user IP Address is allocated to a user by the HPLMN, and held in the user's subscription record within the HLR (a copy of which is sent down to the SGSN at GPRS attachment).

A static user IP address restricts the user to only use PDP Contexts in their HPLMN (HGGSN) with specified APNs. The user will have to have an IP address dynamically allocated by the VPLMN in order to enable use of PDP Contexts established to a VGGSN. Thus, this may restrict a user whilst roaming.

Also, the IP address issued to the user cannot be reused by any other user, so this has the disadvantage of exhausting IP address ranges as well as increasing burden upon O&M.

Therefore, static user IP address allocation is strongly discouraged.

3.1.4.3 *Dynamic User IP Address Allocation*

- A dynamic user IP address is allocated to a user at each PDP Context activation and is liable to change with each new PDP Context activation.

The GGSN may itself assign an IP address to a user (it can retrieve such data during AAA (i.e. RADIUS or Diameter) procedures with a AAA server), or, it may leave it to some other mechanism e.g. DHCP, stateless address auto-configuration.

For PDP Contexts of type "PPP" (Point-to-Point Protocol), dynamic IP address allocation is always performed.

Dynamic IP address allocation is recommended to be used over static address configuration.

3.2 Additional GPRS Functionality

3.2.1 Introduction

This section describes, and provides recommendations where appropriate, some of the additional enhancements to GPRS and the GPRS Tunnelling Protocol (GTP). These features are not required in order for GPRS roaming to work, however, they provide additional capabilities for VPLMNs and/or HPLMNs.

3.2.2 Control of multiple, concurrent PDP Contexts

3.2.2.1 Definition

In more modern GPRS equipment (both network and terminal equipment) it is possible for a subscriber to set-up a connection to the one PDN, e.g., the Internet, and then later setup another connection to another PDN e.g. corporate LAN. There is a security issue in doing this in that packets from the Internet could possibly get forwarded on to the subscriber's corporate LAN and vice versa (using the subscriber's terminal equipment as a router). The only available methods of stopping this right are solutions at the IP layer (layer 3) such as firewall software on the terminal equipment, which for large corporate organisations may not be very viable to maintain. Also, the user could (knowingly or unknowingly) easily disable such software.

In recognition of this potential security issue, 3GPP standardised in Rel-6 a method of controlling this at the layer 2 of the protocol stack i.e. GTP. The solution enables policing of PDP Context creations at the GGSN and also, in some cases where signalling can be saved, at the SGSN.

For each APN a new "APN Restriction" field is added to the APN information in the GGSN. The "APN Restriction" field takes the values of 1 to 4 inclusive (see the last four rows of the table below for the definition of each value).

Maximum APN Restriction Value	Type of APN	Application Example	APN Restriction Value of PDP contexts allowed to be established
0	No Existing Contexts or Restriction		All
1	Public-1	WAP or MMS	1, 2, 3
2	Public-2	Internet or PSPDN	1, 2
3	Private-1	Corporate (e.g. who use MMS)	1
4	Private-2	Corporate (e.g. who do not use MMS)	None

Upon PDP Context creation, the SGSN determines the maximum APN Restriction value based on all (if any) currently active primary PDP Contexts and includes this in the Create PDP Context Request message it sends to the GGSN. If there is currently only one primary PDP Context established and the type of the APN Restriction is Private-2, the SGSN may optionally (as an enhancement) deny any further primary PDP Contexts being established, rather than leaving it to the GGSN to determine this. This is beneficial as it saves on (sometimes inter-PLMN) signalling between SGSN and GGSN.

It is noted that the solution works only for networks who differentiate services by use of different APNs. If the non-standardised "single APN" solution is used, this method may not work (or at least, need some tweaking!).

3.2.2.2 Recommendations

It is recommended that operators configure APNs for access to WAP and MMS as APN restriction type Public-1 (value 1). It is also recommended that APNs for access to the public Internet (i.e. the "internet" APN) have the APN restriction type set to Public-2.

For APNs that give corporate customers access to their corporate LANs/Intranets, it should be agreed between mobile network operators and their respective corporate customers which restriction type best suites the corporate customer (commonly private-1 or private-2 restriction types).

3.2.3 Flow Based Charging

3.2.3.1 Definition

Flow Based Charging is a feature added in 3GPP Rel-6 that enables a finer granularity of charging to be performed at the GGSN than just duration or number of bytes sent/received in a PDP Context. This mainly consists of "deep packet inspection" in order to provide a more user understandable bill e.g. bill on number of web pages viewed. In addition, such information as location of the subscriber (geographically and also local time zone), what radio access technology is being used (e.g. 2G, 3G) and even what content is being downloaded/uploaded can be taken into account, however, this is subject to the SGSN implementing extra functionality to provide this information in real-time to the GGSN.

Flow Based Charging can be applied to both pre-pay and post-pay charging (also known as "on-line" and "off-line" charging, respectively). More details on this feature for both charging models can be found in section 15.1.1a of 3GPP TS 23.060 [1].

3.2.3.2 Recommendations

In the HGGSN roaming scenario (as described in section 2.2.2), Flow Based Charging can be used with or without additional billing agreements between the HPLMN and VPLMN (since the Flow Based Charging is performed on the GGSN). However, in order to realise the full benefits of FBC, the SGSN needs to provide additional information at PDP Context creation and update (it also needs to provide more frequent updates e.g. when intra-SGSN 2G/3G handovers occur). It should also be noted that the SGSN may continue to send its charging data as per standard inter-PLMN accounting; therefore the HPLMN should still expect to receive it.

In the VGGSN roaming scenario (as described in section 2.2.3), Flow Based Charging should only be used in agreement with the HPLMN. Where such agreements exist, charging in the SGSN can be disabled for subscribers from the Flow Based Charging enabled HPLMNs to save on inter-PLMN traffic.

3.2.4 Automatic Device Detection

3.2.4.1 Definition

Automatic Device Detection (ADD) is a feature added in 3GPP Rel-6 that enables the HPLMN to "know" the current IMEI being used by the subscriber, even when that subscriber is roaming. This in turn, enables the HPLMN to perform device specific rendering of media e.g. WAP/web pages, video size and codecs for streaming, as well as other functionality such as EIR interrogations by the HPLMN.

More details can be found in section 15.5 of 3GPP TS 23.060 [1].

3.2.4.2 Recommendations

EIR checks by the HPLMN may not be necessary if both the HPLMN and VPLMN connect to the GSMA's CEIR.

3.2.5 Direct Tunnel Functionality

3.2.5.1 Definition

The Direct Tunnel Functionality is a feature added in 3GPP Rel-7 that enables the routing of GTP User plane (GTP-U) packets directly between an RNC and GGSN (so removes the SGSN from the routing), whilst retaining the GTP Control plane (GTP-C) routing via the SGSN. This has the benefit of reducing the user plane capacity required on SGSNs. However, this functionality can only be used in the VGGSN roaming scenario, and of course, when the subscriber is in their HPLMN.

It should be noted that this functionality is defined only for subscribers on 3G, as direct routing between the BSS and GGSN is not possible. This is because, unlike the RNC, the BSS does not support GTP-U.

More information can be found in section 15.6 of 3GPP TS 23.060 [1].

	VERSION 3.4	Page 15 of 18
--	--------------------	----------------------

3.2.5.2 Recommendations

Since the SGSN is removed from the GTP-U path, any Legal Intercept (LI) requirements on the GTP-U will have to be realised at the GGSN. Therefore, LI support on the GGSN is required in such cases.

4 REFERENCES

- [1] 3GPP TS 23.060: "GPRS Service Description; Stage 2"
- [2] 3GPP TS 23.003: "Numbering, addressing and identification"
- [3] 3GPP TS 29.002: "Mobile Application Part (MAP) specification"
- [4] 3GPP TS 29.060: "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface"
- [5] IETF RFC 1034: "Domain Names – Concepts and Facilities"
- [6] IETF RFC 1035: "Domain Names – Implementation and Specification"
- [7] Void
- [8] GSMA PRD IR.34: "Inter-PLMN Backbone Guidelines"
- [9] GSMA PRD IR.35: "End to End Functional Capability specification for Inter-PLMN GPRS Roaming"
- [10] GSMA PRD SE.20: "GPRS and WAP Service Guidelines"
- [11] GSMA PRD BA.27: "Charging and Accounting Principles"
- [12] Void
- [13] GSMA PRD IR.67: "DNS/ENUM Guidelines for Service Providers & GRX/IPX Providers"

5 ANNEX A: KNOWN ISSUES AND SOLUTIONS

5.1 GTP version 0 and version 1 Interworking Problem

5.1.1 Introduction

When an Operator upgrades its GPRS nodes to GTPv1 it must still provide support for nodes which support only GTPv0. As such, an Operator will want to try to contact another Operator using GTPv1 first, but if that fails, it should fall back and try GTPv0. The problem comes when trying to establish when to fall back to using GTPv0. This is because GTPv1 runs on different UDP/IP ports than GTPv0 and in the 3GPP standards (specifically 3GPP TS 23.060 [1] and 3GPP TS 29.060 [4]) it is not clearly defined how an SGSN or GGSN discovers whether or not another the other supports GTPv1 i.e. there is certainly nothing at the application layer (GTP) to negotiate which version of GTP to use! Therefore, an SGSN and GGSN needs to first try contacting the other using GTPv1 and wait for an error at the IP layer to occur before trying to contact it again using GTPv0.

This error at the IP layer is defined in 3GPP TS 29.060 [4] as a time out (T3 RESPONSE multiplied by N3 REQUESTS). However, if an SGSN or GGSN has to wait for a time out to occur before trying GTPv0, then this reduces the amount of time given to the rest of the chain of nodes in a GPRS activation and hence increases the possibility of the UE (or indeed the actual user) giving up on the current PDP Context activation.

To overcome this, it is recommended that Operators should support GTPv1. However, until all PLMNs support GTPv1 it is strongly recommended that the following configuration be made in the network; both from an HPLMN point of view and from a VPLMN point of view.

5.1.2 VPLMN solution

Many SGSN vendors provide a local cache table within each SGSN that can store GTP versions associated with IP addresses. This means that for a configurable time period, the SGSN "knows" which version of GTP the destination GSN supports and so when setting up a GTP connection it does not have to attempt using GTPv1 if it already knows that the destination does not support it.

It is therefore recommended that Operators make full use of such tables within SGSNs. Doing this will reduce the number of re attempts that have to be made to establish a GTP connection.

5.1.3 HPLMN solution

Many firewalls are configured to simply "drop" packets (i.e. do not send back any error to the sender) destined for ports which do not have a service running on them. This means that a GTPv1 capable SGSN in a foreign network trying to contact a GTPv0 only GGSN in a subscriber's home network will have to wait for a specific period of time before re attempting the connection using GTPv0. The same applies for Inter-MNO Operator IP handover when the SGSN in the old network supports GTPv1 and the SGSN in the new network supports only GTPv0.

It is therefore recommended that Operators who do not yet support GTPv1 configure their firewalls on their GGSNs (and/or any border gateways at the edge of the network) to "deny" packets destined for the GTPv1 signalling/control plane port (UDP/IP port 2123) by sending back ICMP message 3 "destination unreachable" with error code 3, "Port unreachable". Doing this will greatly reduce the time taken for an SGSN to realise that the destination does not support GTPv1.

5.2 IP source address of GTPv1 response messages

Unlike GTP version 0, in GTP version 1 the GGSN is allowed to send GTP response messages back to an SGSN with the source IP address set to an IP address different to that which was in the destination address of the associated GTP request message. The change was made in 3GPP to optimize internal processing of GGSNs.

Unfortunately many firewalls (i.e. GTP-aware stateful firewalls) expect the source IP address of a GTP response message to always be the same as the destination IP address of the respective GTP request message and hence, if the response is received from a different IP address, the firewall will drop the response message and not pass it on for

further processing. Note that this behaviour by the firewall is perfectly valid for GTP version 0 where such IP address usage is specifically prohibited.

This can also have adverse effects for PLMNs who implement "traffic engineering" to control and balance their IP traffic.

It is therefore strongly recommended that Operators configure their GGSNs to always respond to GTP request messages using the source IP address that the GTP request message was sent to. If this is not possible, then a range of IP addresses that a GGSN is able to respond from shall be communicated and agreed between the HPLMN and VPLMN.

5.3 GPRS QoS Classes

GPRS Release 97 defines QoS parameters at the HLR level. However, it does not define QoS functionalities (e.g. scheduling in SGSN or GGSN). Furthermore, the GSM radio access network is not aware of subscription details. These facts are noted in 3GPP and a new definition of QoS classes and functions were introduced to GPRS Release 99 (GTPv1).

Mapping of the GPRS Release 97 and Release 99 QoS classes into IP service QoS parameters will be necessary later. Forthcoming GPRS release specific QoS issues should remain open for further study.

For data roaming taking place between two networks of different generations, i.e. 3G (GPRS R99/UMTS) and 2.5G (GPRS R97/98), Service Providers should comply with the IP QoS definitions for GPRS R97/98.