3GPP TSG SA WG3 Security — S3#15bis **S3z000005**

Ad-Hoc meeting 08-09 November, 2000

Munich, Germany

Source: **Telenor (origin GSMA)**

Title: **Inter-PLMN Backbone Guidelines**

Document for: **Information**

Agenda Item:

The attached document is provided by Telenor on behalf of GPRSWP chairman Anders Roos, PRD IR.34 "Inter-PLMN Backbone Guidelines".

GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

PRD IR.34

Title Inter-PLMN Backbone Guidelines

Version **3.0.1**
Date **5th September 2000**

GSM Association Classifications

Non-Binding

Security Classification Category:	
Unrestricted – Industry	√

Information Category	Roaming - Technical

Unrestricted

This document is subject to copyright protection. The GSM MoU 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 of the GSM MoU Association 2000

TABLE OF CONTENTS

Document History

Version	Date	Brief Description
0.0.1	22.06.1999	IREG Doc GPRS 14/99
0.0.2	30.11.1999	First draft of the document, presented in GPRSWP #6
0.1	1.1.2000	2nd draft
0.1.1	28.1.2000	Modifications according to comments
1.0	22.2.2000	Modifications after GPRSWP#7.
1.0.1	14.3.2000	Modifications after GPRSWP#8. Submitted to IREG#38 for approval.
2.0.0	15.3.2000	IREG 38 approval
3.0.0	28th April 2000	Approved at Plenary 43. PL Doc 35/00
3.0.1	5.9.2000	CR from GPRS Doc 51/00 incorporated GPRS DNS Usage Guidelines incorporated as annex A

1 Scope of the Document

This document introduces guidelines for GPRS inter-PLMN connections and requirements for inter-PLMN backbone network. This document should be used in conjunction with PRD IR.33 [1] and PRD IR.35 [2].

The reason for Inter-PLMN backbone network is the need to create GTP-tunnelled PDP contexts via Gp interface between GSNs in different PLMNs. Gp interface is needed in order to make services of the home network available for roaming users also in the visited network.

IP addressing issues introduced in this document apply to inter- and intra-PLMN nodes only. IP addressing of GPRS user plane (i.e. mobile stations) and service elements (e.g. WAP-GW) located beyond Gi reference point is not within the scope of this document.

The signalling network for MSC/VLR, HLR and other register access and Short Message Service are not within the scope of this document.

Mobile IP is not within the scope of this document.

2 Definitions, Abbreviations and Symbols

2.1 Definitions and Abbreviations

For the purposes of the present document, the following terms and definitions apply. Other definitions and abbreviations can be found in [3] and [4].

AS	In the Internet model, an Autonomous System (AS) is a connected segment of a network topology that consists of a collection of subnetworks (with hosts attached) interconnected by a set of routes. [5]
BG	Border Gateway, router between intra-PLMN and inter-PLMN backbone networks. (For additional information see IR.33 [1].)
BGP	Border Gateway Protocol (BGP) is an inter-Autonomous System routing protocol [6]. The current version of BGP is BGP-4.
Central Exchange Point	Service that provides for one-to-one peering for regional PLMN operators. Implementation can be combined with a GRX.
DNS	Domain Name System. For additional information, refer to IR.33 [1].
Gateway/Router	In the Internet model, constituent networks are connected together by IP datagram forwarders which are called routers or IP routers [5]. In this document, every use of the term router is equivalent to IP router. Some Internet documents refer to routers as gateways. See also Border Gateway (BG).
GPRS Roaming Network	Inter-PLMN backbone network that consist of interconnected GRX nodes and connections between PLMNs and GRXs. In this document used as a special case of Inter-PLMN Backbone.
GRX	GPRS Roaming eXchange, serving point of GPRS Roaming Network. Provides for routing, interconnecting and some additional services, such as DNS.
GRX Service Provider	PLMN operator, International Data Carrier or other service provider that provides GRX services within the GPRS Roaming Network.

GTP	GPRS Tunnelling Protocol [7].
IDC	International Data Carrier, a global datacom operator or a joint venture of operators offering world-wide data communication services.
Inter-PLMN Backbone	The IP network interconnecting GSNs and intra-PLMN backbone networks in different PLMNs [3]. In this document used as a general term.
Intra-PLMN Backbone	The IP network interconnecting GSNs within the same PLMN [3].
Transiting Traffic	GPRS roaming traffic that is routed via third party, such as a Transit Operator.
Transit Operator	PLMN (or GRX) Operator that has connections to two or more other PLMNs and is transiting GPRS roaming traffic between other operators.

2.2 Symbols

For the purposes of the present document, the following symbols apply [3]:

Gi	Reference point between GPRS and an external packet data network.
Gn	Interface between two GSNs within the same PLMN.
Gp	Interface between two GSNs in different PLMNs. The Gp interface allows support of GPRS network services across areas served by the co-operating GPRS PLMNs.

3 General Requirements of the Inter-PLMN Backbone

3.1 IP Routing via Gp Interface

In order to establish transport of roaming traffic between GPRS backbone networks, operators need to create IP packet routing connections between their Border Gateways. Intra-PLMN backbone networks are connected via the Gp interface using Border Gateways and an inter-PLMN backbone network [3].

3.2 IP Addressing

Public addressing should be applied in all GPRS backbone networks. Using public addressing means that each operator has a unique address space that is officially reserved from Internet addressing authority. However, public addressing does not mean that these addresses should be visible to Internet. GPRS intra- and inter-PLMN backbone networks shall remain invisible and inaccessible to public Internet.

It is imperative to use unique public addressing in *all* visible network elements of the intra and Inter-PLMN networks. With current Network Address Translation (NAT) implementations it is impossible to use NAT because NAT can not change IP addressed, such as SGSN address in PDP context activation request, that are carried inside GTP tunnel.

IP version 4 address space is a limited resource. IPv6 will eventually resolve addressing limitations but the introduction of GPRS services cannot be tied to the schedule of IPv6. Regardless of IPv4 address space limitations, the usage of public addresses is a feasible solution. Schedule and terms of IPv6 deployment in the Inter-PLMN backbone will be subject to bilateral agreements and/or Inter-PLMN backbone operators to PLMN operator agreements.

3.3 Security and Screening

In order to maintain the proper level of security within the Inter-PLMN backbone, there are some requirements for GPRS operators and Inter-PLMN backbone providers.

It is strongly recommended that operators should implement firewalls adjacent to Border Gateways. Firewall may be integrated to the Border Gateway or it can be a separate device.

Operator should be responsible for screening the traffic towards its BG. Generally operators should allow only routing information, such as BGP, GTP traffic and signalling and DNS traffic in addition to some diagnostic tools, such as ping. Description and usage policy of diagnostic tools should be included in the service agreement with Inter-PLMN backbone service provider and bilaterally agreed between PLMN operators.

The backbone network operator or service provider together with PLMN operator should be responsible for prevention of IP address spoofing (if applicable).

3.3.1 IPSec

GPRS operators may use IPSec [8, 9, 10] as an encryption and tunnelling method on the Inter-PLMN backbone, especially if the Inter-PLMN backbone medium itself does not guarantee security and data integrity.

Inter-PLMN backbone, if implemented on unsecured public networks, should support the use of IPSec, including Public Key Infrastructure (PKI) implementations such as Internet Key Exchange (IKE)[11].

3.4 Quality of Service (QoS)

Quality of Service provided by the Inter-PLMN backbone can be defined by physical characteristics of leased lines (Layer 1 and Layer 2) and by IP (Layer 3) parameters described in appropriate sections of this document.

Integration of Inter-PLMN QoS and GPRS QoS classes and parameters that define the quality of service in terms of radio resources etc. should remain for further study and may be implemented in forthcoming GPRS releases.

4 Services of the Inter-PLMN Backbone

Generally, Inter-PLMN backbone is a medium for GPRS roaming traffic exchange. All information over this medium is carried with TCP/IP suite of protocols.

4.1 IP Routing and Packet Forwarding

4.1.1 Dynamic IP Routing

In order to route TCP/IP PDUs between PLMNs, the Inter-PLMN Backbone network shall provide IP routing. Dynamic exchange of routing information between different networks may be accomplished by using BGP-4 routing protocol. In some simple cases, such as connection based on direct leased line, static routing is feasible.

4.1.2 GTP Tunnelling

Inter-PLMN backbone shall support GTP tunnelling on both TCP and UDP.

Explanation: All GPRS roaming traffic is carried on GPRS Tunnelling Protocol (GTP) defined in GSM 09.60 [7]. This protocol tunnels user data and signalling between GPRS Support Nodes in the GPRS backbone network. TCP carries GTP PDUs in the GPRS backbone network for protocols that need a reliable data link (e.g., X.25), and UDP carries GTP PDUs for protocols that do not need a reliable data link (e.g., IP) [3]. Only SGSNs and GGSNs implement the GTP protocol. No other systems need to be aware of GTP. [7]

4.2 Domain Name Service

As a minimum requirement, Inter-PLMN backbone shall provide a transport of DNS queries between PLMNs. In addition, Inter-PLMN backbone may provide root DNS services.

4.3 Other Services

The Inter-PLMN connection can also be used for different purposes than for GPRS roaming (access to common databases and service platforms, signalling exchange etc.). These additional services and commonly agreed policies are still open for discussion and further study.

5 Inter-PLMN Interconnection Possibilities

Fundamentally, there are two possibilities for interconnection between operators:

- Direct connections between two GPRS operators.
- Establishment of a GPRS Roaming Network.

Direct connections can be considered as a short-term solution to implement the IP-connectivity between the operators. As a long-term objective, a GPRS roaming network as described in section 5.2 should be established. GPRS roaming network can be complemented with local peering implementations (Central Exchange Points) for regional traffic as described in section 5.3.

5.1 Direct Connectivity between two GPRS operators

There are three alternatives to implement direct connectivity:

- Tunnelling via Public IP network (IPSec strongly recommended)
- Direct leased lines (FR, ATM or IP/PPP based)
- Virtual Private Data Network (VPN) as a supplementary service based on leased lines

All three solutions are more or less straightforward, but have disadvantages. Tunnelling via Internet can’t provide guaranteed QoS and may weaken security. That will be a threat for the GPRS network system itself and may not be acceptable by customers. Leased lines and VPNs have higher costs and may be economically unacceptable solution for roaming with a large number of roaming partners.

Alternative methods are described more thoroughly below.

5.1.1 Tunnelling via Public Data Network (Internet)

It is possible to use Internet as a basis for Inter-PLMN backbone. Due to unprotected nature of the Internet, operators should use IPSec or other security and layer-3 tunnelling protocols to ensure security, data confidentiality and integrity.

Internet is usually the quickest and cheapest way to implement direct connectivity, but operators should keep in mind that implementation of security requires additional work. Quality of service on the Internet may be compromised by factors that can not be influenced by GPRS operator.

All security and QoS issues of Internet-based Inter-PLMN backbone are subject to agreements between roaming partners and Internet service providers.

5.1.1.1 Security

IPSec [8] implementation between GPRS roaming partners is quite straightforward if certain rules are accepted between roaming partners. Proposed rules and guidelines are:

- Encryption algorithm used by default is DES. It is recommended to use 3DES, which is stronger than DES.

- The packet format used with IPSec connections is encapsulation security payload [10] (ESP) in tunnel mode. Implementation can be done with any equipment and software that is compliant with IPSec and IKE (if applicable) related RFCs and IETF drafts. IPSec can be implemented within BG but that is not required.
- Operators should agree bilaterally how to exchange encryption keys either manually or by an automated key management scheme that implements Public Key Infrastructure (PKI). PKI requires that trusted third parties, Certificate Authorities (CA), are used. Protocol that is used for negotiating parameters regarding to IPSec tunnels is Internet Key Exchange (IKE) [11].
- Use of firewalls adjacent to BG and IPSec nodes is strongly recommended.

5.1.1.2 Quality of Service

In the Internet it is usually difficult to ensure other quality than 'Best Effort'. Operators willing to use public Internet as a medium for direct connections are encouraged to negotiate terms described in section 6 with their ISP.

5.1.2 Direct Leased Lines

Point-to-point direct leased lines are the most secure and usually the most expensive solution. International carrier providing the leased line should guarantee QoS and security.

Operators using direct leased lines as an Inter-PLMN backbone should have bilateral agreements describing how to share the costs and to determine the service parameters (capacity, QoS, etc.) of the leased line.

5.1.2.1 Security

General security requirements apply.

5.1.2.2 QoS

Link-level QoS requirements apply.

5.1.3 Frame relay

Frame Relay connection requires a leased line to PLMN provided by an International Data Carrier. It can be provided as a separate physical interface into BG or as additional FR Virtual Circuit (VC) into existing physical connection. Frame Relay can be a basis of a VPN solution offered by data carriers.

Operators using Frame Relay as an Inter-PLMN backbone should have bilateral agreements describing how to share the costs and to determine the service parameters (capacity, CIR, QoS, etc.) of the Frame Relay VC.

5.1.3.1 Security

General security requirements apply.

5.1.3.2 QoS

Link-level and Frame Relay specific QoS requirements apply. Parameters are subject to agreements between PLMN operators and international carrier.

5.1.4 ATM

ATM based connection requires a leased line or fibre to PLMN provided by International carrier. It can be provided as a separate physical interface into BG or as additional ATM VC into existing physical connection. ATM can be a basis of a VPN solution offered by data carriers.

Operators using ATM as an Inter-PLMN backbone should have bilateral agreements describing how to share the costs and to determine the service parameters (capacity, service category, QoS, etc.) of the ATM VC.

5.1.4.1 Security

General security requirements apply.

5.1.4.2 QoS

Link-level and ATM specific QoS requirements apply. Parameters are subject to agreements between PLMN operators and international carrier.

5.2 GPRS Roaming Network

5.2.1 Overview of the GPRS Roaming Network Structure

As a long-term solution roaming traffic should be carried over GPRS Roaming Network, where commonly agreed policies are followed.

GPRS roaming network consists of GPRS Roaming Exchange (GRX) nodes. As a minimum, GRX consists of a router, the means to connect to PLMN networks and the means to connect to other GRX nodes. GRX nodes should be connected to each other either directly or via other GRXs so that transiting traffic can be forwarded to any part of the network. Defined Service Level Agreement (SLA) should apply along all paths between GRXs.

In this hierarchical backbone model GPRS operator needs only one logical connection to GRX. If redundancy is required, two or more connections to one or more GRX may be used. GPRS operators obtain connections to GRX nodes locally from GRX Service Provider or from other telcos (e.g. leased lines).

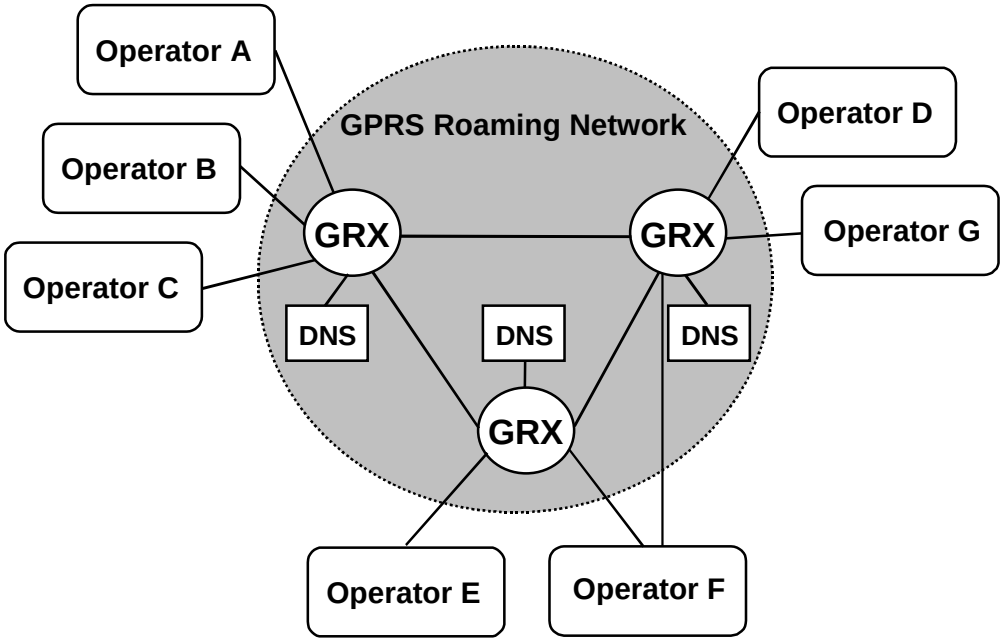

Figure 2. Topology of an Inter-PLMN backbone implemented as a GPRS Roaming Network

5.2.2 GRX Service Providers

GRX can be operated by a PLMN operator or by an International Data Carrier. It is very likely that due to joint ventures, close relationships between PLMN operators and carrier operators as well as geographical reasons, there will be a number of different GRX Service Providers.

Requirements for GRX Service Providers and operations are described in following sections.

5.2.3 Connections between PLMN and GRX

Every Roaming operator should have a dedicated connection to a GRX with either

- Layer 1 connection (e.g. leased line or fibre) *or*
- Layer 2 logical connection (e. g. ATM, LAN, Frame Relay) *or*

- Layer 3 IP VPN connection over public IP network (IPSec is recommended)

It is recommended that all GRX providers should offer all types of connection described above. It is up to GRX and GPRS operators to determine exact details of each connection. Direct connectivity basics described in section 5.1 apply to PLMN-to-GRX connections. Main benefits of the GRX structure for GPRS operators are:

- GPRS operator does not have to create dedicated connections to every roaming partner. Instead of tens or hundreds of separate connections, the o*perator can start offering the GPRS roaming service with number of roaming partners with only one connection to GRX*.
- GPRS operator may choose to start with low quality and low capacity connection to GRX and upgrade the level of connectivity when it is economically feasible and there are traffic volumes and type of traffic that require more bandwidth and better quality.

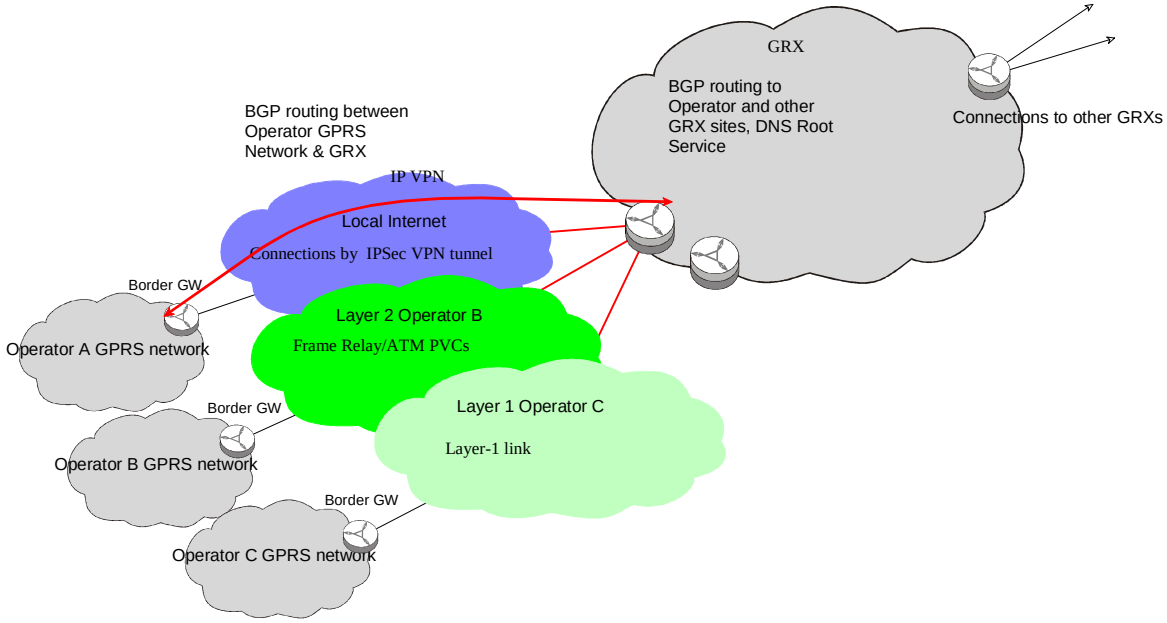

Figure 3. Connections between PLMN and GRX

5.2.4 Connections Between GRXs

Connections between GRXs are implemented and managed by GRX Service Providers. GRX Service Providers should guarantee that the network is reliable and its quality is not compromised by any traffic originated from connected GPRS networks or from any other source. GRX Service Providers should conform to Service Level Agreements (SLA) which are based on QoS requirements described in section 6.

GRX Service Providers are required to constantly improve their service due to increased traffic volumes or new standards.

GRX service providers should arrange peering with other GRXs either directly or indirectly via other GRXs so that every GRX and its connected PLMN networks have connectivity to other GRXs and their connected PLMN networks.

5.2.5 Dynamic Routing between PLMN and GRX

In addition to roaming data traffic, the GPRS roaming network should carry routing information. It is recommended that the address space used at operator's PLMN network will be advertised to GRX with BGP-4 [6] routing protocol. Similarly, GRX will advertise all

addresses of connected GPRS operators. Each operator using BGP-4 routing protocol should have an AS (Autonomous System) [6] number acquired from Internet addressing authority.

PLMN operator may screen unwanted routes by selecting address ranges of its roaming partners based on AS numbers carried on BGP-4 routing messages.

Dynamic routing between operators minimises the amount of management work when operators IP address space will change (i.e. new address ranges are applied). In addition, dynamic routing makes it possible to have redundant connection to GRXs.

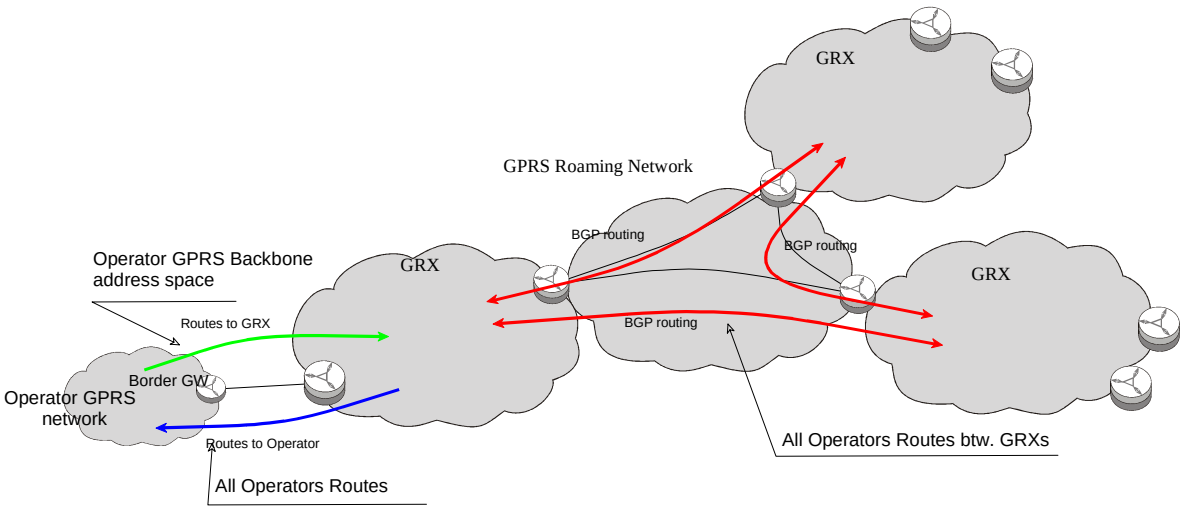

Figure 4. Dynamic routing within GPRS Roaming Network

5.2.6 Dynamic Routing between GRXs

GRX Service Providers are required to exchange routing information and traffic between all GRX nodes. GRX is responsible of distributing all Inter-PLMN BGP-4 information to all its peers.

5.2.7 IP Addressing

GRX Service Provider and its contracted PLMN operators should comply with IP addressing guidelines presented in ‘General Requirements of the Inter-PLMN Backbone‘ section of this document.

Operators, that is GRX or PLMN operators, who wish to employ IPv6 in their network are fully responsible for all network adjustments necessary for maintaining connectivity through the inter-PLMN network to other GRX operators or PLMN’s that deploy IPv4.

5.2.8 Domain Name Service (DNS)

GRX Service Providers should take the responsibility for arranging the management of .gprs top level domain name services and hosting of the root servers. Root DNS hosting requires that DNS information should be exchanged between all GRXs. GSM Association should authorise one GRX operator to be a master root DNS provider.

GRX Service Providers should arrange root DNS service for contracted PLMN operators within the GRX. GRX should distribute all required DNS information between PLMN operators.

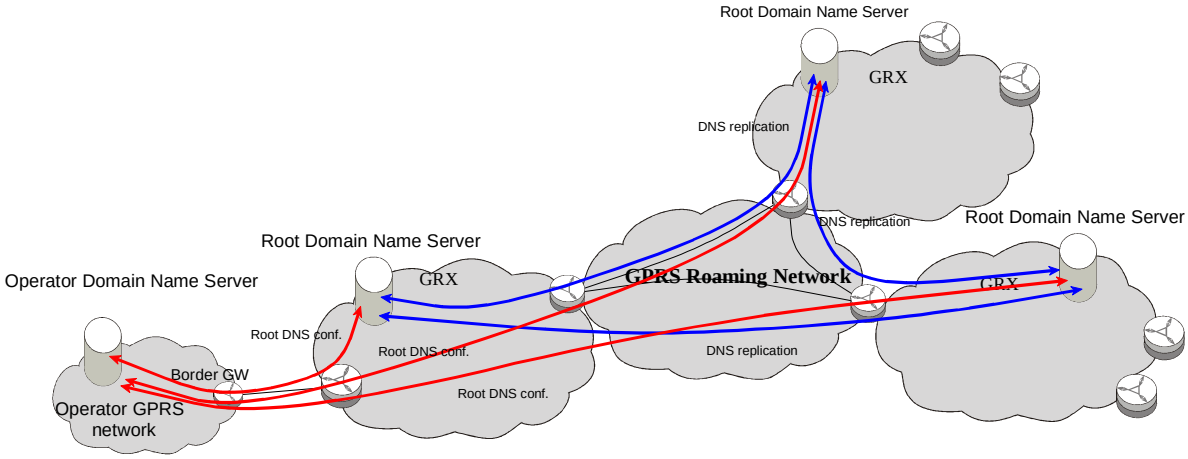

Figure 5. Root DNS service provided by GRX nodes

5.2.9 Security

General security requirements apply. For details of IPSec tunnelled connections between PLMN and GRX, refer to section 5.1.1.1.

5.2.10 Summary

Following sub-sections describe the minimum requirements that are needed for successful GPRS Roaming Network operations for both PLMN operators and GRX service providers.

5.2.10.1 Requirements for PLMN Operator

In order to connect to GRX-based Inter-PLMN Backbone, i.e. GPRS Roaming Network, PLMN operator should have:

- Compliance with IP addressing guidelines for intra-PLMN backbone
- DNS service within intra-PLMN
- Border Gateway and preferably a Firewall
- BGP-4 routing capability and an AS number (recommendation)
- Control which routes to accept from GRX
- Established or planned GPRS roaming agreement with one or more PLMN operators
- Contract with one or more GRX Service Providers

5.2.10.2 Requirements for GRX Service Provider

In order to offer services as a GRX Service Provider, service provider should have:

- Capability to provide connection from PLMNs in various ways (Layers 1,2 and 3)
- Compliance with IP addressing guidelines for inter-PLMN backbone
- DNS root service for contracted PLMNs
- BGP-4 routing capability
- Distribution of all known routes to PLMN operators
- Control which routes a PLMN operator can advertise to the GPRS roaming network
- Interconnectivity to other GRXs (either directly or via other GRXs)
- Conformance to Service Level Agreements (as described in section 6)

- Conformance to security requirements: IPSec (if applicable), anti-spoofing, non-visibility to public Internet etc.

5.3 Central Exchange Point

5.3.1 Overview of Central Exchange Point

In some cases roaming operators have two different types of roaming partners: One with whom there is more roaming traffic (such as an adjacent regional operator) and one with whom the roaming traffic is not very high (e.g. an international roaming partner). For connections with regional roaming partners, operators may have direct connections. Instead of having multiple layer 2 connections to regional roaming partners and to the GRX for international roaming, it is possible to bring all roaming traffic centrally to one point and then exchange traffic with multiple partners according to separate bilateral agreements. The 'Central exchange point' will provide for both direct (operator to operator) as well as GRX connections from one single location, thereby reducing the need for multiple layer 2 connections. The central exchange point will consist of an exchange switch (or a series of switches) in conjunction with one or multiple GRX(s) housed in one location. Switch functionality and GRX functionality may be combined.

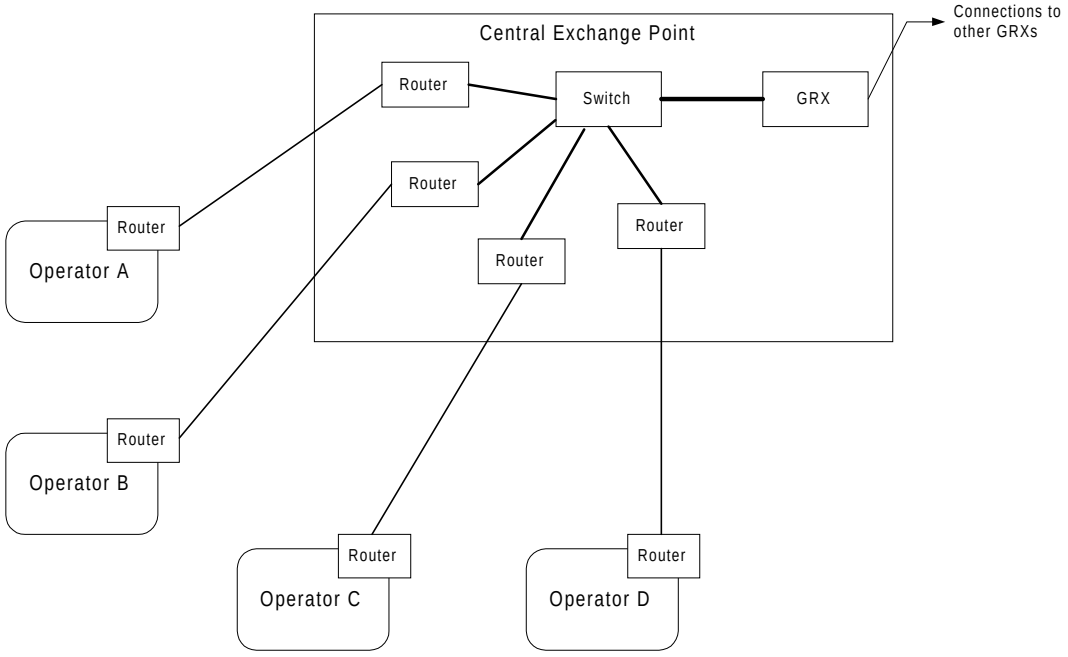

Figure 6. Interconnection via a Central Exchange Point

5.3.2 Backbone Architecture of Central Exchange Point

As shown in Figure 6, all the operators connect to a central exchange point. This point is akin to the NSFNet Network Access Point (NAP) implementations that are used for the ISP interconnections. Each operator may have a router in the exchange point and terminate roaming traffic from his network to this router in the exchange. Each operator also executes his own peering agreements with other operators, with whom they expect a lot of roaming traffic, on a one-to-one basis. When more than one operator advertises routes to the same destination, the individual operator makes a decision on which route should be loaded in its own forwarding tables. The exchange switch is used strictly to provide connectivity between the operators and will not have control over any routing decisions. The connectivity to the other operators, with whom there is not a need to have peer-to-peer connectivity, can be achieved by a connection between the operator's router and the router that belongs to the GRX. This GRX can be then be connected to the other GRXs such that it becomes a part of the GRX roaming backbone. SLA

agreements will be executed with one or more GRX operator(s) and the switch/location provider as well as multiple operators with whom the operator has direct connectivity.

The advantages of the proposed architecture are as follows:

It provides one point for termination of all roaming traffic from each operator regardless of where the traffic is intended, i.e., to the GRX or to a peer. This saves on the direct connection cost which will increase as the number of peering operators increases. The control on the routing decisions also rest on the operator solely and do not depend on the exchange switch/GRX provider.

5.3.3 Security

General security considerations apply. Additional security procedures have to be agreed bilaterally.

5.3.4 QoS

The SLA between two operators having direct connectivity is agreed bilaterally. It is outside the scope of this document. The central exchange point falls into the general category of direct connectivity and thus its SLA matters are not extensively discussed in this document.

However, the central exchange switch/location provider should advertise an SLA for its facilities. This SLA will be equally applicable on a non-discriminatory basis to all operators and GRX providers that have equipment in this facility. The switch/location provider SLA should include items about the operational characteristics of the facilities such as, equipment description, configuration, availability, time to repair, etc.

The SLA between an operator and a GRX provider should follow the guidelines provided in section 6.

5.3.5 IP Addressing

Central Exchange Point and the GRX operators should comply with IP addressing guidelines presented in ‘General Requirements of the Inter-PLMN Backbone‘ section of this document.

6 Service Level of the GPRS Roaming Network

6.1 Service Level Agreement (SLA)

A single GRX Service Provider is considered as responsible for aspects of the service delivery as seen from a PLMN operator’s point of view (”one-stop-responsibility”). That is, a given PLMN operator should not need to go beyond the nearest GRX Service Provider for the given aspects of the service. In the other words, agreed Service Level on interface between GSM operator and Inter-PLMN backbone operator should be supported through the whole network path towards other PLMN operators. It is noteworthy that PLMN operator should also be responsible for certain SLA components, such as forecasts of increase in traffic volume

An SLA defines end-to-end (PLMN-to-PLMN) service specifications where IP QoS definitions described in section 6.2 apply. Agreed IP QoS profile should be supported throughout the whole Inter-PLMN backbone network between Border Gateways of PLMN operators.

The Service Level Agreement should consist at least of following parts (adapted quotations from [12]:

6.1.1 Services Offered

The agreement describes offered service and its parameters, such as DNS services, protocols, interface type and capacity. An interface is a boundary between GSM operator and Inter-PLMN

Backbone service provider. Detailed description of the connection (Layer 1,2,3 protocols) should be part of the agreement.

6.1.2 Service Guarantees

Service guarantees should be defined for each IP QoS parameters defined in section 6.3. Additionally, there should be a defined reporting procedure, i.e. the provider takes responsibility to provide measurements and lets PLMN operators obtain the results.

6.1.3 Responsibilities

- Terms and conditions of each SLA component and the amount of charges PLMN operator's account should be credited for the service when SLA has not been met.
- Help Desk support and customer services

6.1.4 Reaction patterns

A set of reaction patterns must be described. The actions are to be applied in case when service degradation/failure is detected. A number of possible (re)actions may be taken, like:

- No action.
- Monitoring the achieved QoS, possibly storing an observed value for future reference (e.g. for enquiry purposes).
- Reserving or reallocating resources.
- Information flow controlling mechanisms such as traffic shaping, admission policy control as an attempt to keep information flow within limits.
- Warnings and error signals to the customer or service provider.
- Suspending or aborting the service.

Other aspects, like legal and regulatory, business, technical protocol-specific, etc. should be also considered.

6.2 GPRS QoS classes

GPRS Release 97 does define QoS parameters at HLR level. However, it does not define QoS functionalities (e.g. scheduling in SGSN or GGSN). Furthermore, GSM radio access network is not aware of subscription details. These facts are noted in 3GPP and new definition of QoS classes and functions will be introduced to GPRS Release 99 and UMTS[13].

Therefore at this time, the service level of the Inter-PLMN backbone will be defined by IP service QoS parameters described below. PLMN operators and GRX service providers are encouraged to monitor the development of improved IP QoS technologies, such as 'Differentiated Services (diffserv)' model that is currently in IETF's standardisation process [14].

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.

6.3 IP QoS Definitions

The QoS parameters, which characterise QoS, should be defined in the SLA. The QoS parameter set must be consistent and uniquely understood by both parties at the interface.

A number of QoS parameters' values can be stated in the agreement, such as:

- An operating target value,
- An upper and lower threshold,

- An acceptable limit.

If parameter measurements indicate a violation of SLA, GRX Service Provider should act to improve service. For instance, if the mean utilisation rate of one inter-GRX backbone link exceeds threshold value, GRX Service Provider should order more capacity for that particular link immediately.

6.3.1 Availability

GSM Association and GPRS operators should demand from GRX Service Providers guaranteed reliability of the GRX and backbone connections to other GRXs.

Required value of GRX service availability: > 99,95%

6.3.2 Latency

Packet transfer delay is dependent on many factors, e.g. distance, number of intermediate hops and available bandwidth. The following values are upper limits expected on any operator to operator connection between their Border Gateways

IP packet transfer delay (latency): **400 ms mean**

IP packet transfer delay variation (jitter): **20 ms (standard deviation)**

6.3.3 Packet Loss Rate

Backbone network between GRXs should be dimensioned so that packet drops do not occur (or do occur relatively rarely).

The maximum rate at which packets may be discarded: 0,3 %

7 References

[1] PRD IR.33: "GPRS Guidelines"

[2] PRD IR.35: "End to End Functional Capability specification for Inter-PLMN GPRS Roaming"

[3] GSM 03.60: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service Description; Stage 2"

[4] GSM 01.04: "Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms"

[5] RFC 1812: "Requirements for IP Version 4 Routers"

[6] RFC 1771: "A Border Gateway Protocol 4 (BGP-4)"

[7] GSM 09.60: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface"

[8] RFC 2401: "Security Architecture for the Internet Protocol"

[9] RFC 2402: "IP Authentication Header"

[10] RFC 2406: "IP Encapsulating Security Payload (ESP)"

[11] RFC 2409: "The Internet Key Exchange (IKE)"

[12] The EQoS Framework – Version 2; A Common Framework for QoS/Network Performance in a multi-Provider Environment, EURESCOM project P806 Deliverable 1; http://www.eurescom.de/Public/Projects/P800-series/P806/P806.htm

[13] 3G TS 23.107: “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; QoS Concept and Architecture”

[14] http://www.ietf.org/html.charters/diffserv-charter.html

8 Annex A: GPRS DNS Usage Guidelines

This annex describes usage of Domain Name Service (DNS) to resolve Access Point Names (APN) in GPRS networks and recommends a naming convention for inter-PLMN network nodes. User plane naming is out of scope of this document.

This annex is published for GSM Association IREG GPRS Working Party for discussion purposes in order to help definition of Inter-PLMN Domain Name Service between roaming partners.

All sample configurations of this annex are in valid format and syntax. However, the samples are not from actual DNS configuration and they may contain example information, such as IP addresses, that is not valid. GSM Association does not take responsibility of the usage of similar configurations in operators' DNS servers.

9 Domain Name Service Overview

9.1 Components

9.1.1 Hierarchical Database

9.1.1.1 Domains

Internet uses naming convention called domain names. Domain name consists of two or more parts separated with a '.'-character. It starts from the least significant domain and ends up to most significant domain or top-level domain. This naming convention naturally defines a hierarchy.

9.1.1.2 Zones

Domain Name Service (DNS) is a huge distributed database that contains information of each domain name. Each server maintains a part of the database called zone. Usually a zone contains information of one domain. However, one zone may contain information about many (sub)domains.

Each information element is stored in a record that contains at least a domain name and type and type specific information

9.1.1.3 Delegation

When a part of a zone is maintained separately, it is delegated to a new nameserver that will have authority of that part of domain namespace. Original zone will have nameserver (NS) record for the delegated domain and the new subzone will have a new Source Of Authority (SOA) record.

9.1.2 Client

DNS client is implemented as resolver library. Application programs use function calls like 'gethostbyname' to find IP address representing a domain name. The name may be specified only partially and in that case resolver library appends configured local domain name(s) at the end of the name. For instance user may give command:

ping hobbes

The resolver library will append domain search list and will query the nameserver with

'***hobbes.sonera.com hobbes.sonera.fi hobbes***'

Domain names ending with a dot are called fully qualified domain names. Search list components are not appended on these names.

9.1.3 Server

DNS server takes care of name service queries sent by clients. The query is answered by using either locally stored information or by asking the information from other name servers. Sending queries to other name servers is potentially time and network resources consuming task. Storing previously queried information in a local cache optimises the process. Each nameserver record has a time-to-live that specifies the time they may be cached. When time-to-live expires the record is discarded and a new query is performed.

Servers build a hierarchy. At the top of the hierarchy are root nameservers. They have information about all top-level domain nameservers like *.net* or *.fi* nameservers. These nameservers in turn know about all nameservers immediately under their domain. And so on.

One nameserver can serve several domains. There may also be several nameservers serving one domain. In fact, at least two nameservers for each domain are strongly recommended. This ensures service for the domain in case one of the nameservers is temporary out of order. One of the nameservers serving a domain contains the master or primary copy of the zone information. All changes are made to this copy. Other nameservers are slave or secondary nameservers for this domain.

10 DNS usage in GPRS

10.1 Access Point Names

Access Point Names are defined in GSM 03.03 Section 9. Access Point Names are not case sensitive. The name consists of two parts

Network id	Operator id
<= 63 Octets	18 Octets (or optionally <= 27 Octets)
<= 100 Octets	

Table1 Access Point Name Structure

Operator id consists of MNC and MCC codes derived from IMSI and ends with .gprs. Coding of MNC and MCC codes changed between SMG#29 and SMG#30 at A033r1. In addition PLMN may provide more human readable operator id format with DNS.

For instance the following are valid names:

Network id: ***ibm.com***

Operator id (prior SMG#30): ***mnc91.mcc244.gprs*** optionally also s***onera.fi.gprs***

Operator id (SMG#30 or later): ***mnc091.mcc244.gprs***

Operator id (optional human readable form):
sonera.fi.gprs

Network id + Operator id (prior SMG#30):
ibm.com.mnc91.mcc244.gprs

Network id + Operator id (SMG#30 or later):
ibm.com.mnc091.mcc244.gprs

Network id + Operator id (optional human readable form):
ibm.com.sonera.fi.grps

GSM 03.03-650 states:

'The APN Operator Identifier is composed of three labels. The last label shall be "gprs".'

In some countries like Great Britain, New Zealand and Japan there are always at least three labels on valid Internet registered domain names. In these countries national registered Internet domains may not be used for operators. Some GPRS implementations are known to always strip off three labels, when APN ends with .gprs.

User of MS may not give APN at all or give only Network id part or give the whole APN. The rules how to handle each case are described in GSM 03.60. The following SDL diagrams are from Annex A.2.

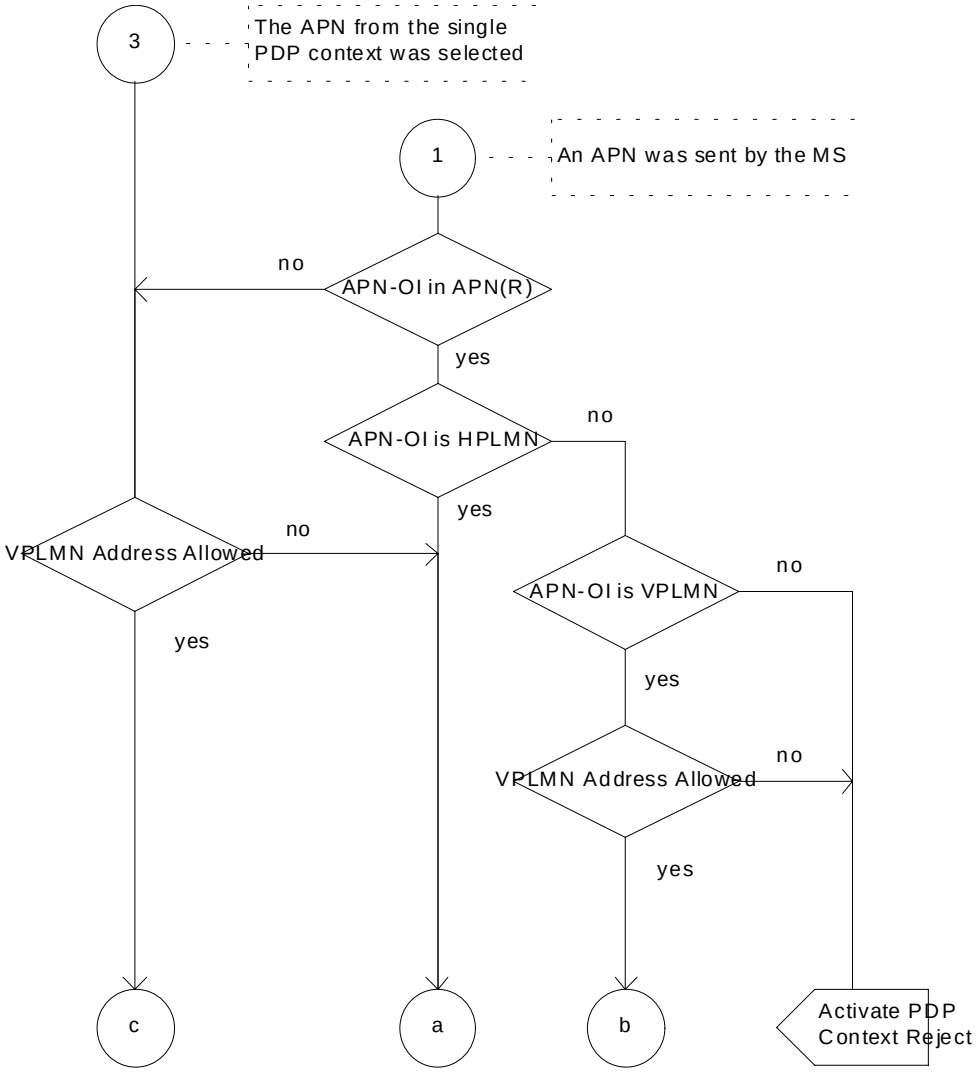

Figure 1 (GSM 03.60-650 A.2 SDL Diagram 4)

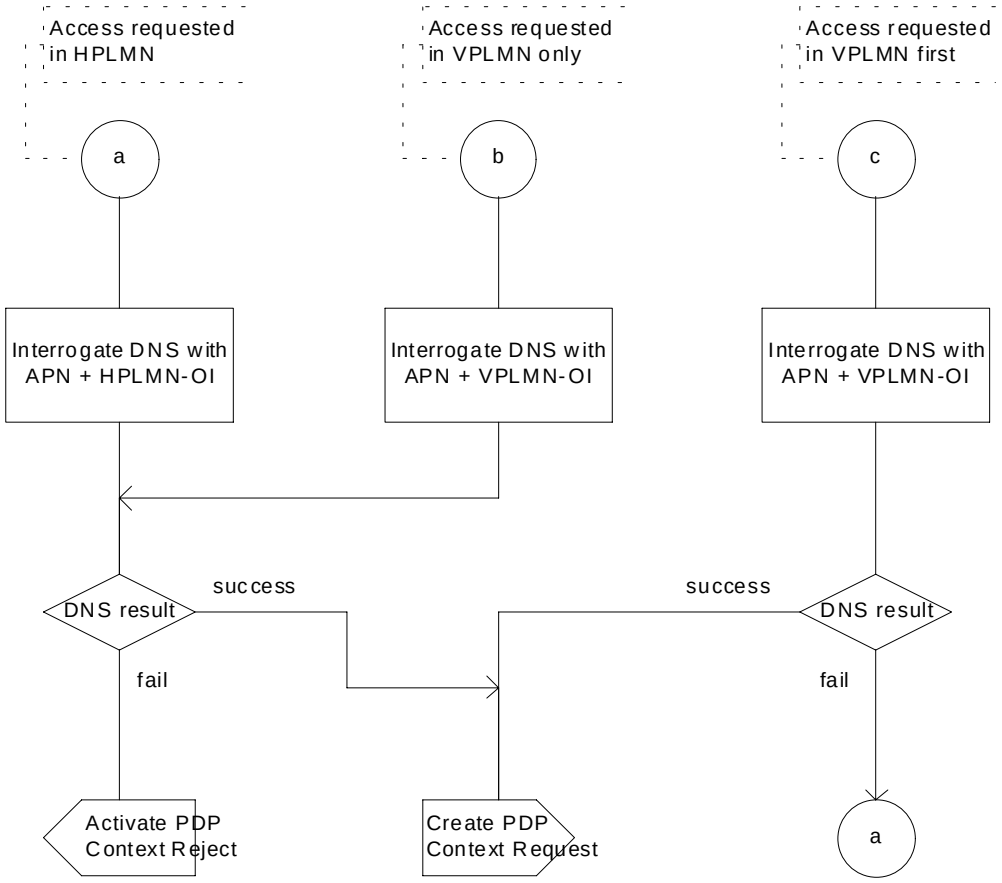

Figure 2 (GSM 03.60-650 A.2 SDL Diagram 6)

10.2 Routing Area Identities

GSM 09.60 Annex A.1 states:

"When an MS roams between two SGSNs within the same PLMN, the new SGSN finds the address to the old SGSN by the association old RA - old SGSN. Thus, each SGSN knows the address to every other SGSN in the PLMN.

When an MS roams from an SGSN to an SGSN in another PLMN, the new SGSN may not itself have access to the address to the old SGSN. Instead, the SGSN transforms the old RA information to a logical name of the form:

RACxxxx.LACyyyy.MNCzzzz.MCCwwww.GPRS; x,y,z and w shall be Hex coded digits.

The SGSN may then acquire the IP address of the old SGSN from a DNS server, using the logical address. Every PLMN should include one DNS server each. Note that these DNS servers are GPRS internal entities, unknown outside the GPRS system."

Note: The coding of DNS-name is subject of on-going change request because of in-consistency with GSM 03.03.

And later:

"Introducing the DNS concept in GPRS gives a general possibility to use logical names instead of IP addresses when referring to e.g. GSNs, thus providing flexibility in addressing of PLMN nodes.

Another way to support seamless inter-PLMN roaming is to store the SGSN IP addresses in HLR and request them when necessary."

In other words if DNS is used RAI should have a mapping to SGSN IP address with a name of format:

racF1.lac12EF.mnc091.mcc244.gprs

10.3 GPRS Support Node Names

GSM 09.60-650 Annex A.2 states:

"It shall be possible to refer to a GSN by a logical name that shall then be translated into a physical IP address. Here a GSN naming convention is proposed which would make it possible for an internal GPRS DNS server to make the translation.

An example of how a logical name of a SGSN could look like is:

SGSNxxxx.MNCyyyy.MCCzzzz.GPRS;	*x,y and z shall be digits."*	*Hex coded*

Note: The coding of DNS-name is subject of on-going change request because of in-consistency with GSM 03.03.

However this name format does not seem to have any functional use in standards.

10.4 Reverse Mapping

Reverse mapping i.e. translation of IP addresses to domain names is not needed for GPRS functionality. However, this feature has proven very useful for debugging purposes. Therefore it is highly recommended that each operator will provide reverse mapping.

By convention reverse mapping uses special domain in-addr.arpa and IP addresses are added starting from the most significant byte as subdomains. For instance reverse information for a host with IP address 192.168.21.5 may be found from domain 21.168.192.in-addr.arpa.

Because available tools use this hierarchy it would not be feasible to add .gprs at the end. GPRS specific name servers should use the same convention.

11 DNS and Inter-PLMN Network

Each PLMN operator should have at least two DNS servers. That makes it possible to for instance upgrade one of the servers without service interruption. The servers should keep cache of recently queried DNS records. Caching both shortens query response time and decreases network traffic.

There are two possibilities to arrange necessary DNS hierarchy. The first is to configure the nameserver of each domain at Inter-PLMN network individually at each PLMN operator. Every time a new domain is added to Inter-PLMN backbone network name service or any authoritative nameserver address is changed every operator must update DNS servers. Pretty soon this will come tedious at best, but most likely a frequent source for operational roaming problems.

Another alternative is to have common GPRS root nameserver. Every change in domain or DNS information is updated at the master GPRS root nameserver and the changed information is immediately active. Since the GPRS root nameserver is critical for operation, it should be replicated at several locations in Inter-PLMN backbone network.

GPRS root nameservers should contain necessary information to reach operator DNS servers. Root server security is crucial. For instance they may only allow zone transfer to other GPRS root nameservers.

GSM Association may have contract with one of the GRX operators to maintain the master replica. GRX operators may provide slave GPRS root nameservers at some or all GRX nodes.

12 Recommended Naming Convention

Having a consistent naming convention makes it easier to maintain DNS and also easier to use DNS information. The following convention is one possibility to achieve this goal. The usage of this naming methodology is recommended, but it doesn't exclude other conventions.

All GPRS backbone components that are relevant for roaming should be included in DNS. Such elements are Access Points, GGSNs, Border Gateways (and other routers), DNS-servers and SGSNs.

12.1 APNs

Access Points should have registered organisation domain names or Service Access Point Names e.g. *ibm.com* or *Internet*.

12.2 DNS Servers

Nameservers should have name

dns<nbr>

where <nbr> is 0 for the master nameserver and subsequent slave nameservers will have increasing numbers.

12.3 Other Equipment

GGSNs, Border Gateways (and other routers), firewalls and SGSNs should have names for each interface with format

<city>-<nbr>-<interface-type>-<interface-code>-<type>

where

- <nbr> is a running number of similar devices at the same city
- <interface-type> has a couple of characters describing the interface type
  - e - ethernet
  - fe - fast ethernet
  - ge - gigabit ethernet

- t - token ring
- s - serial
- h - HSSI
- a - ATM

- <interface-code> identifies interface slot/card/port etc.
- <type> describes device type
  - ggsn
  - sgsn
  - rtr - router
  - fw - firewall

e.g.

helsinki-4-fe-0-1-ggsn

13 Sample DNS Configuration

The following configuration examples are for bind version 8. A thorough discussion about nameserver operation and maintenance is available at: DNS and BIND, 3rd Edition by Paul Albitz and Cricket Liu.

13.1 named.conf

Named.conf file has configuration information for bind software. Following is only the necessary configuration to get DNS running. There are many more options that would be useful.

13.1.1 Sample PLMN Master Nameserver

```
options {
        directory "/var/named";
};      // where the files reside

zone "." in {
        type hint;
        file "gprs.hint";
};      // gprs root servers

zone "0.0.127.in-addr.arpa" in {
        type master;
        notify no;
        file "master/0.0.127.in-addr.arpa";
};      // only contains information about localhost.

/*
*       PLMN domain information
*/

zone "mnc91.mcc244.gprs" in {
        type master;
        file "master/mnc91.mcc244.gprs";
};      // prior SMG#30

zone "mnc091.mcc244.gprs" in {
        type master;
```

```
        file "master/mnc091.mcc244.gprs";
};      // SMG#30 and later

zone "sonera.fi.gprs" in {
        type master;
        file "master/sonera.fi.gprs";
};      // human readable operator id

zone "168.192.in-addr.arpa" in {
        type master;
        file "master/168.192.in-addr.arpa";
};
```

13.1.2 Sample PLMN slave nameserver

```
options {
        directory "/var/named";
};      // where the files reside

zone "." in {
        type hint;
        file "gprs.hint";
};      // gprs root servers

zone "0.0.127.in-addr.arpa" in {
        type master;
        notify no;
        file "master/0.0.127.in-addr.arpa";

};      // only contains information about localhost.

/*
*       PLMN domain information
*/

zone "mnc91.mcc244.gprs" in {
        type slave;
        file "slave/mnc91.mcc244.gprs";
        masters {192.168.1.2;}  // address of master nameserver
};      // prior SMG#30

zone "mnc091.mcc244.gprs" in {
        type slave;
        file "slave/mnc091.mcc244.gprs";
        masters {192.168.1.2;}  // address of master nameserver
};      // SMG#30 and later

zone "sonera.fi.gprs" in {
        type master;
        file "slave/sonera.fi.gprs";
        masters {192.168.1.2;}  // address of master nameserver
};      // human readable operator id;
```

```
zone "168.192.in-addr.arpa" in {
        type slave;
        file "slave/168.192.in-addr.arpa";
        masters {192.168.1.2;}  // address of master nameserver
};
```

13.2 Zone Configuration Files

Recommended values for SOA records are as specified in ripe-203.

13.2.1 gprs.hint

This file contains gprs root nameservers needed to initialise cache of gprs nameservers. Note that "."-characters are significant.

```
.       518400          IN      NS      dns0.root.gprs.
        dns0.root.gprs. IN      A       172.22.1.5

.       518400          IN      NS      dns1.root.gprs.
        dns1.root.gprs. IN      A       10.254.243.7

.       518400          IN      NS      dns2.root.gprs.
        dns2.root.gprs. IN      A       192.168.17.232
```

13.2.2 0.0.127.in-addr.arpa

This file contains only information about localhost i.e. 127.0.0.1

```
$TTL 172800

@       IN      SOA             localhost.. hostmaster.localhost. (
                2000030701      ; serial (YYYYMMDDvv)
                86400           ; refresh (24 hours)
                7200            ; retry (2 hours)
                3600000         ; expire (1000 hours)
                172800 )        ; minimum time to live (2 days)

1       IN      PTR     localhost.
```

13.2.3 PLMN zone files

PLMN may configure both mnc.mcc.gprs and operaror.cc.gprs type domains that will share exactly the same host information. In addition prior SMG#30 mnc didn't have leading zeroes to make mnc code always 3 digits long. In order to minimise both configuration work and possible errors zone files may include a common hosts configuration.

13.2.3.1 mnc91.mcc244.gprs

```
$TTL 172800

@       IN      SOA     mnc91.mcc244.gprs. hostmaster.mnc91.mcc244.gprs. (
                2000030701      ; serial (YYYYMMDDvv)
                86400           ; refresh (24 hours)
                7200            ; retry (2 hours)
                3600000         ; expire (1000 hours)
                172800 )        ; minimum time to live (2 days)

        IN      NS      dns0
        IN      NS      dns1

$INCLUDE master/hosts
```

13.2.3.2 mnc091.mcc244.gprs

```
$TTL 172800

@   IN   SOA   mnc091.mcc244.gprs. hostmaster.mnc091.mcc244.gprs. (
    2000030701   ; serial (YYYYMMDDvv)
          86000        ; refresh (24 hours)
          7200         ; retry (2 hours)
          3600000      ; expire (1000 hours)
          172800 )     ; minimum time to live (2 days)

    IN   NS   dns0
    IN   NS   dns1

$INCLUDE master/hosts
```

13.2.3.3 sonera.fi.gprs

```
$TTL 172800

@   IN   SOA   sonera.fi.gprs. hostmaster.sonera.fi.gprs. (
          2000030701   ; serial (YYYYMMDDvv)
          86400        ; refresh (24 hours)
          7200         ; retry (2 hours)
          3600000      ; expire (1000 hours)
          172800 )     ; minimum time to live (2 days)

    IN   NS   dns0
    IN   NS   dns1

$INCLUDE master/hosts
```

13.2.4 hosts

This file contains IP address records for all hosts at PLMN. The origin changes depending on which file includes the contents i.e. after the names not ending at dot the current domain name is appended automatically.

Load balancing may be performed configuring same access point with several IP addresses that actually are on different GGSNs. In this case addresses are used in round-robin fashion. However, DNS information is cached and a new query is performed only when time-to-live has expired. Therefore TTL of 0 seconds is configured for load balanced access points.

```
dns0                    IN   A    192.168.1.2
dns1                    IN   A    192.168.2.2

;
;       router
helsinki-1-fe-0-0-rtr   IN   A    192.168.1.254
helsinki-1-fe-0-1-rtr   IN   A    192.168.2.254
helsinki-1-fe-0-2-rtr   IN   A    192.168.3.254
helsinki-1-s-1-0-rtr    IN   A    172.22.5.6
```

```
;
;       access point
ibm.com                 IN      A       192.168.1.5

;
;       load balanced access point
compaq.com  0           IN      A       192.168.1.5
            0           IN      A       192.168.2.5

;
;       service access point
internet                IN      A       192.168.2.2

;
;       GGSN
helsinki-15-e-0-ggsn    IN      A       192.168.1.5
helsinki-25-e-0-ggsn    IN      A       192.168.2.5
helsinki-22-e-0-ggsn    IN      A       192.168.2.2

;
;       SGSN
helsinki-1-fe-0-1-3-sgsn        IN      A       192.168.3.3
;       SGSN with RAI
racF1.lac12EF                   IN      A       192.168.3.3
```

13.2.5 168.192.in-addr.arpa

There may be several PTR records so that each name associated with and address may have reverse mapping also. Note that IP address is reversed in in-addr.arpa domain i.e. 192.168.1.254 will be 254.1.168.192.in-addr.arpa.

```
$TTL 172800

@       IN      SOA     dns0.sonera.fi.gprs. hostmaster.sonera.fi.gprs. (
                        2000030701      ; serial (YYYYMMDDvv)
                        86400           ; refresh (24 hours)
                        7200            ; retry (2 hours)
                        3600000         ; expire (1000 hours)
                        172800 )        ; minimum time to live (2 days)

        IN      NS      dns0.sonera.fi.gprs.
        IN      NS      dns1.sonera.fi.gprs.

5.1             IN      PTR     ibm.com.sonera.fi.gprs.
                        PTR     ibm.com.mnc91.mcc244.gprs.
                        PTR     ibm.com.mnc091.mcc244.gprs.
                        PTR     compaq.com.sonera.fi.gprs.
                        PTR     compaq.com.mnc91.mcc244.gprs.
                        PTR     compaq.com.mnc091.mcc244.gprs.
                        PTR     helsinki-15-e-0-ggsn.sonera.fi.gprs.
                        PTR     helsinki-15-e-0-ggsn.mnc91.mcc244.gprs.
                        PTR     helsinki-15-e-0-ggsn.mnc091.mcc244.gprs.

254.1           IN      PTR     helsinki-1-fe-0-0-rtr.sonera.fi.gprs.
                        PTR     helsinki-1-fe-0-0-rtr.mnc91.mcc244.gprs.
                        PTR     helsinki-1-fe-0-0-rtr.mnc091.mcc244.gprs.
```

2.2	*IN*	*PTR*	*internet.sonera.fi.gprs.*
		PTR	*internet.mnc91.mcc244.gprs.*
		PTR	*internet.mnc091.mcc244.gprs.*
		PTR	*helsinki-2-e-0-ggsn.sonera.fi.gprs.*
		PTR	*helsinki-2-e-0-ggsn.mnc91.mcc244.gprs.*
		PTR	*helsinki-2-e-0-ggsn.mnc091.mcc244.gprs.*
5.2	*IN*	*PTR*	*compaq.com.sonera.fi.gprs.*
		PTR	*compaq.com.mnc91.mcc244.gprs.*
		PTR	*compaq.com.mnc091.mcc244.gprs.*
		PTR	*helsinki-25-e-0-ggsn.sonera.fi.gprs.*
		PTR	*helsinki-25-e-0-ggsn.mnc91.mcc244.gprs.*
		PTR	*helsinki-25-e-0-ggsn.mnc091.mcc244.gprs.*
254.2	*IN*	*PTR*	*helsinki-1-fe-0-1-rtr.sonera.fi.gprs.*
		PTR	*helsinki-1-fe-0-1-rtr.mnc91.mcc244.gprs.*
		PTR	*helsinki-1-fe-0-1-rtr.mnc091.mcc244.gprs.*
3.3	*IN*	*PTR*	*helsinki-1-fe-0-1-3-sgsn.sonera.fi.gprs.*
		PTR	*helsinki-1-fe-0-1-3-sgsn.mnc91.mcc244.gprs.*
		PTR	*helsinki-1-fe-0-1-3-sgsn.mnc091.mcc244.gprs.*
		PTR	*racF1.lac12EF.sonera.fi.gprs.*
		PTR	*racF1.lac12EF.mnc91.mcc244.gprs.*
		PTR	*racF1.lac12EF.mnc091.mcc244.gprs.*
254.3	*IN*	*PTR*	*helsinki-1-fe-0-2-rtr.sonera.fi.gprs.*
		PTR	*helsinki-1-fe-0-2-rtr.mnc91.mcc244.gprs.*
		PTR	*helsinki-1-fe-0-2-rtr.mnc091.mcc244.gprs.*