Inter-Service Provider IP Backbone Guidelines

PRD IR.34
Version 4.9

4 March 2010

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

Security Classification – NON-CONFIDENTIAL GSMA Material		

Table of Contents

1 GENERAL

1.1 Purpose

The purpose of this document is to provide guidelines and technical information on how Inter-Service Provider IP Backbone networks are set-up and how Service Providers will connect to the Inter-Service Provider IP Backbone.

This document provides a clear distinction between GRX and IPX (evolved GRX) networks where applicable.

This document also defines high level security requirements for the Inter-Service Provider IP network. Detailed complementary requirements can be found in the "Inter-Operator IP backbone Security Requirements For Service Providers and Inter-operator IP Backbone Providers" IR.77 [19].

1.2 Background

The Inter-Service Provider IP Backbone network was originally created to carry GTP-tunnels (GPRS Tunneling Protocol) via the Gp interface between the GPRS Support Nodes (GSNs) in different GSM Operators ie data roaming. The Gp interface allowed mobile end-users to make use of the GPRS/3G services of their home network while roaming in a visited network. Later, MMS interworking and WLAN (authentication) data roaming has been added to the services supported in Inter-Service Provider IP Backbone. This Inter-Service Provider IP Backbone is in fact an Inter-PLMN IP Backbone and is termed the GRX. The GRX model is used to interconnect in excess of 300 networks and has proven highly successful.

With the development of IP-based services, interworking of such services has become an industry wide challenge. The GRX model is applicable as an IP interworking solution; however the GRX specification does not meet all the requirements. It has been recognised that by adding interworking specific functionality to the GRX model and offering it to the industry, a common interconnect platform could be established for IP interworking. The enhanced GRX is called an IPX and is designed to support a variety of types of Service Providers in a secure and business sustainable way.

The core enhancements to the GRX are end-to-end Quality of Service and the introduction of the IPX Proxy which facilitates interconnect cascade billing and multi-lateral interconnect agreements.

1.3 About this Document

The document provides a brief introduction to the requirement for IP interworking and the IPX. It covers the background to the forerunner of the IPX, the GRX.

The technical architectures of both the GRX and IPX are described followed by the technical implementation guidelines for IPX and GRX Providers and connecting Service Providers. Technical guidelines for Security, Quality of Service and Traffic applications are also given.

Appendices provide details on known issues in the Inter-Service Provider IP Backbone and on the requirements for IPX proxies.

Note: In this document all references to the IP Inter-Service Provider IP Backbone Network (or abbreviated to IP Backbone Network) shall include both IPX and GRX where generic requirements exist. However specific requirements to IPX and GRX shall use each term independently. In addition, the term "evolution to an IPX network" shall not in any way suggest or mandate the GRX is either invalid or that it shall be replaced by an IPX.

2 DOCUMENT SCOPE

2.1 In scope

An Inter-Service Provider IP Backbone network architecture which connects Mobile Network Operators (MNOs), Fixed Network Operators (FNOs) Internet Service Providers (ISPs) and Application Service Providers (ASPs), from here on in referred to collectively as "Service Providers". Where there is specific reference to an Service Provider type they shall be directly referred to in each case.

Technical guidance to Service Providers for connecting their IP based networks and services together to achieve roaming and/or inter-working services between them.

Recommendations for IP addressing. (Applies to inter- and intra-Service Provider nodes only.)

Host name recommendations remain within the scope of the present document.

2.2 Out of Scope

IP addressing and host names of GPRS user plane (i.e. mobile stations) and service elements (e.g. WAP-GW) located beyond the Gi reference point. (IR 40)

Both hostname and domain name usage and recommendations are also outside the scope of this document, and are specified in GSMA PRD IR.67 [17].

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

Direct Connectivity among Service Providers by Leased line, VPN or Internet.

Aspects of the management of the Inter-Service Provider IP Backbone known as governance are not covered in this document.

Aspects of commercial agreements relating to the Inter-Service Provider IP Backbone are not covered by this document.

3 DEFINITIONS, ABBREVIATIONS AND SYMBOLS

3.1 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 sub-networks (with hosts attached) interconnected by a set of routes. [5]
BG	Border Gateway, a node located between intra-Service Provider and Inter-Service Provider IP Backbone networks, including network layer security functionality such as traffic filtering as well as routing functionality. For additional information see IR.33 [1]. Note: BG as defined here does not map directly into the TISPAN architecture (i.e. BGF)
BGP	Border Gateway Protocol (BGP) is an inter-Autonomous System routing protocol [6]. The current version of BGP is BGP-4
Blacklist	A list supplied by a Service Provider of interworking or roaming partners with whom connection is not allowed

DNS	Domain Name System. For additional information, refer to IR.67 [17].
End-to-End	Throughout this document end-to-end means from Service Provider premises to Service Provider premises, if not described otherwise. Thus, Service Provider core and access networks are excluded
EPS	Evolved Packet System (Core)
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)
GRX	GPRS Roaming eXchange. Provides for routing, interconnecting and some additional services, such as DNS. Generally used for GPRS/UMTS/LTE roaming, MMS interworking and WLAN roaming
GRX Provider	A Provider that offers GRX service only
GTP	GPRS Tunneling Protocol[7]
Interconnection	The connection of Service Providers in order to exchange traffic between them
Inter-Service Provider IP Backbone	The collection of interconnected GRX and IPX Providers' networks
IP Backbone Provider	A business entity that provides Inter-Service Provider IP Backbone Service. Either a GRX or an IPX/GRX Provider
Interworking	The ability for a service offered to subscribers of one network to communicate with a similar service offered to subscribers of a different network
IPX	IP Packet eXchange. The entity providing the IPX functions. In the interconnection context, IPX is used to mean an interconnection at the service level. Also refers to the collection of all the interconnected IPX Provider's networks
IPX Provider	A Provider that offers IPX services and may also offer GRX services
LTE	Long Term Evolution (Radio)
MMS	Multimedia Messaging Service
MNO-G	A GPRS/UMTS/LTE Mobile Network Operator that connects only to a GRX Network. The services they offer over the GRX network are on a bilateral basis with no guarantees of QoS end-to-end
MNO-I	This Service Provider is a GPRS/UMTS/LTE Mobile Network Operator who connects to either a GRX and IPX network or an IPX network only.
NGNO	This Service Provider connects only to the IPX network and can be any type of organization except a GPRS/UMTS/LTE mobile operator.
NGN Services	New generation IP-based fixed-line services offered using SIP/IMS technologies. There will be other services offered in the future
PCC	Policy and Charging Control
PGW	PDN (Packet Data Network) Gateway
PMIP	Proxy Mobile IP

Proxy	Proxy is used to describe an Inter-Service Provider IP Backbone element that supports service interworking. Proxies facilitate a multi-lateral model for each service
Roaming	The ability for a user to function in a serving network different from the home network
Single-root ENUM	An ENUM model with a unique global root database at the top of the hierarchy
SCTP	Stream Control Transmission Protocol
Service Provider	Mobile, fixed operator or other type of Operator connecting to Inter-Service Provider IP Backbone for roaming and/or interworking purposes
SGW	Serving Gateway
Whitelist	A list supplied by a Service Provider of interworking or roaming partners with whom connection is allowed
Hot Potato	A term typically used for routing decision where a party is handing over its traffic to a peering partner as quick as possible or at the nearest in terms of delay peering point. I.E. when two SPs are on different continents and behind two different IPXs, Hot Potato means that IPX1 hands over SP1's traffic to IPX2 at the Peering point nearest to the SP1's location. More information is given in IETF RFC documentation [24]
Cold Potato	A term typically used for routing decision where a party keeps its traffic on its network for as long as possible and handing over its traffic to a peering partner at the farthest in terms of delay peering point. I.E. when two SPs are on different continents and behind two different IPXs, Cold Potato means that IPX1 hands over SP1's traffic to IPX2 at the Peering place farthest to the SP1's location. More information is given in IETF RFC documentation [24]

3.2 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 Mobile Network Operator.
Gp	Interface between two GSNs in different Mobile Network Operators. The Gp interface allows support of GPRS network services across areas served by the co-operating GPRS Operators.
Mw	Reference point between CSCF elements of IMS
Mb	Reference point to IPv6 Network Services

4 INTRODUCTION

4.1 The need for IP Interconnect

Following the widespread deployment of packet infrastructures using the GSM and UMTS air interfaces, Mobile Network Operators (MNOs) are expected to launch a wide range of new data services. IP interconnect between MNOs is required to support IP interworking of these mobile data services.

At the same time, Fixed Network Operators (FNOs) are deploying Next-Generation Networks (NGNs) and ISPs are offering an ever-increasing number of services. Whilst competing, Service Providers (MNOs, FNOs, ISPs and ASPs) have the common objective of delivering traffic to each other in a profitable and cost effective way. The common protocol of these networks and services is the Internet Protocol (IP).

For their subscribers to appreciate the full value of these services, Service Providers need to maximise their connectedness through interworking and roaming arrangements for IP traffic.

Two possibilities exist for interconnection between Service Providers:

- Establishment of an inter-Service Provider IP Backbone connection via either GRX or IPX Providers , or
- Direct connection between two Service Providers using Leased lines, Internet using IPSec, VPN connectivity.

Direct Connectivity between Service Providers maybe a requirement and is out of scope for this document.

It is a commercial decision which method Service Providers choose. The benefits of connectivity via a GRX or IPX are substantial and include the ability to reach many different roaming and interworking partners across the globe via one connection.

To ensure interoperability, all Service Providers connected to the Inter-Service Provider IP Backbone network will need to adhere to common rules. These include rules regarding IP addressing, security (described in PRD IR.77 [19]), end-to-end QoS, and other guidelines that are described in this document.

The Inter-Service Provider IP Backbone does not offer “services” as such, to end users, but the Inter-Service Provider IP Backbone offers connectivity and interconnection services to Service Providers, and functions required to allow or enhance that interconnection, for example DNS or transcoding.

4.2 GRX

The GRX Network was first established in 2000 for the purpose of Mobile GPRS roaming and only MNOs were allowed to connect to it. Since then, other services have been added such as UMTS roaming, MMS interworking and WLAN (authentication) data roaming.

The GRX provides connectivity based upon best-effort between GSM and 3G Mobile Network Operators (end-to-end) whenever bilaterally agreed between those Operators. It includes the agreement of the IP Backbone Provider to carry diagnostic protocols, for example ICMP (Ping).

4.3 IPX

Building on the features of the GRX, the IPX also is able to support the following:

- Connectivity between any type of Service Provider
- End-to-end QoS for roaming and interworking
- Any IP services on a bilateral basis with end-to-end QoS and interconnect charging

An IPX may also use the service-aware functionality of the IPX Proxies to support:

- Further interconnect charging models such as Service-Based Charging in addition to the volume-based model of GRX
- Inter-operable interworking for specified IP services
- Multilateral interworking support for these specified services over a single Service Provider to IPX connection

5 INTER-SERVICE PROVIDER IP BACKBONE ARCHITECTURE

The purpose of the Inter-Service Provider IP Backbone is to facilitate interconnection between Service Providers according to agreed inter-operable service definitions and commercial agreements.

The model used for the Inter-Service Provider IP Backbone is that of a private IP backbone network. All information is carried over these networks using the IP suite of protocols.

In this hierarchical model, Service Providers require only one connection and one agreement with the Inter-Service Provider IP Backbone to be able to interconnect with selected Service Provider partners. If redundancy is required, two or more physical connections to one or more Inter-Service Provider IP Backbone networks may be used. (See Annex A for problems and solutions to this approach). Service Providers obtain connections to Inter-Service Provider IP Backbone nodes locally from an IP Backbone Provider or from other Providers (e.g. leased lines).

5.1 Service Provider to Inter-Service Provider IP Backbone connection

Service Providers are connected to their selected IP Backbone Provider(s) using a local tail. Service Providers may be connected to more than one Provider. Firewalls or Border Gateways (BGs) including firewall functionality may be used to protect the internal networks of the Service Providers. Service Providers may choose to implement redundant local tails and Firewalls/BGs to improve resilience.

5.2 GRX Architecture

A simplified high-level architecture of the GRX covering both roaming and interworking interconnection cases is illustrated in the figure below.

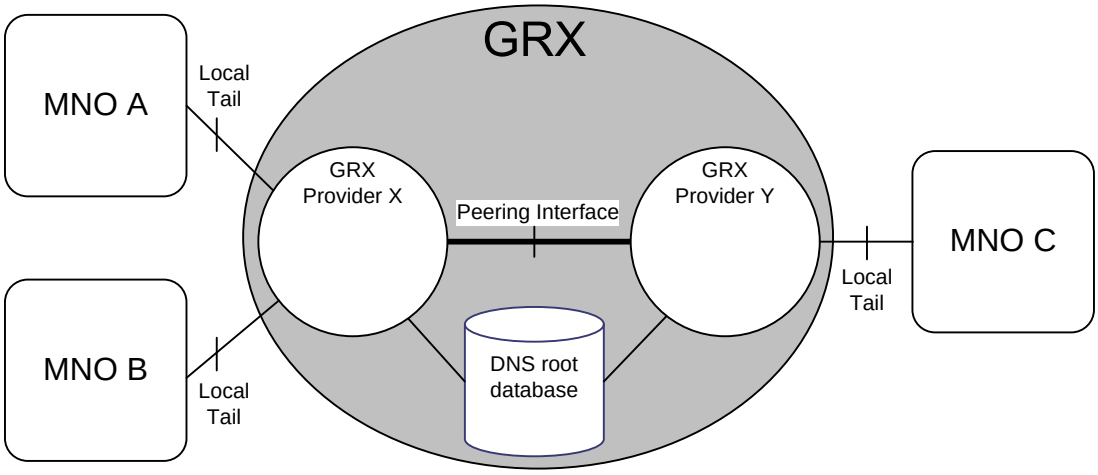

Figure 1 - GRX Model

The GRX consists of separate and competing GRX Providers (or GRX Carriers). A GRX network can be operated by any qualified party. Requirements for GRX Providers are described in section 6.1.

GRX Providers connect to each other via peering interfaces. These peering interfaces may be direct connections or may pass through a common peering point. GRX Providers should enter into Service Level Agreements (SLAs) with other GRX Providers.

A common DNS root database supports domain name resolution. This root database may be used by all GRX parties.

The GRX is isolated from the public Internet and security rules are defined to prevent unintended access from it.

Dynamic routing may be used on the GRX using the BGP-4 routing protocol. When using the GRX, interworking and/or roaming services can be established without specific configuration requirements and additional processing of protocols.

It is possible to connect a Service Provider to the GRX using IPSec. This possibility is described in the end-to-end QoS SLA. Other uses of IPSec are dependent on service requirements and will be described in the service specific documentation, e.g. IR.61 for WLAN roaming.

The GRX offers a transport-only interconnection service between mobile operators on a bilateral basis with no guarantees of QoS end-to-end. This transport-only function may be used to transport any protocol on a bilateral basis. In particular, the GRX is used to support traffic applications including: GPRS and 3G data roaming (using GTP), LTE data roaming as described in GSMA PRD IR.88 [25], WLAN roaming authentication, MMS Interworking and IMS Interworking. See section 9 for more information on traffic applications.

5.3 IPX Architecture

The IPX builds upon and extends the architecture of the GRX by introducing a number of other stakeholders – Fixed Network Operators, Internet Service Providers and Application Service Providers (which together with Mobile Network Operators are hereafter termed Service Providers). The IPX is formed from separate and competing IPX Providers. An IPX network can be operated by any qualified party.

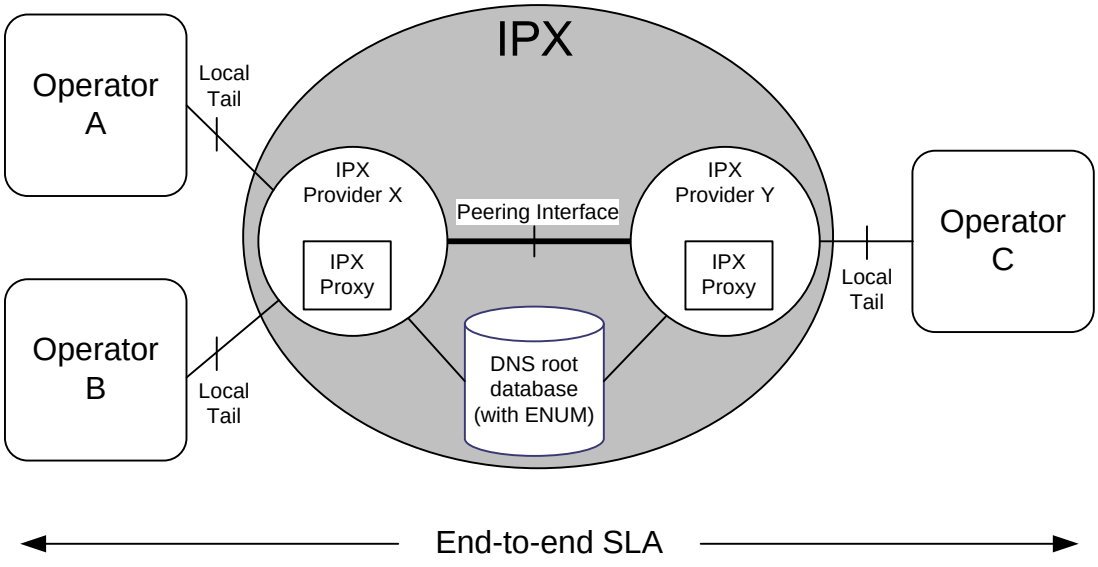

Figure 2 - IPX Model

The IPX introduces the requirement to support Quality of Service features end-to-end. That is, the parties involved in the transport of a service (up to the terminating Service Provider BG/firewall) are bound by end-to-end Service Level Agreements.

The IPX uses the same root DNS as the GRX.

The IPX also introduces IPX Proxy elements. These Proxies may support interworking of specified IP services and make it possible to use cascading interconnect billing and a multilateral interconnect model.

To assist with the translation of Telephone Numbers to URI the common DNS root database of the IPX will support ENUM capability.

In the IPX, all user traffic, (that is, UE-to-UE and UE-to-Server), is separated from Server-to-Server traffic. This is to fulfil the requirement of end users not being able to reach or "explore" the IPX network.

5.4 Interconnect Functions of the IPX

This section should be read in conjunction with PRD AA.80. The IPX has three connectivity options.

5.4.1 Transport-Only Connectivity Option

A bilateral agreement between two Service Providers using the IPX transport layer with guaranteed QoS end-to-end. As with the GRX, this model is not service aware and it can be used to transport any protocol between the two Service Providers (provided compliance with security requirements is maintained).

5.4.2 Bilateral Service Transit Connectivity Option

A bilateral agreement between two Service Providers using the IPX Proxy functions and the IPX transport layer with guaranteed QoS end-to-end. This model provides the opportunity to include service-based interconnect charging in addition to the transport charging of the transport-only model.

5.4.3 Multilateral Service Hub Connectivity Option

A model providing multilateral interconnect with guaranteed end-to-end QoS and including service-based interconnect charging. Hubbing/multilateral connectivity is where traffic is routed from one Service Provider to many destinations or interworking partners via a single agreement with the IPX Provider. The hub functionality is provided by IPX Proxies.

5.5 IPX Proxy Services

Interworking between Service Providers can be established without proxy services when using the Transport-Only Connectivity Option. However proxy services are required to support the hub and transit connectivity models described above, where they facilitate a Service Provider’s configuration and agreement management and the cascading of charging.

The different types of traffic may require processing by separate proxies functions available within the Inter-Service Provider IP Backbone. It is an implementation issue whether these functional entities will be separate or combined into one network node.

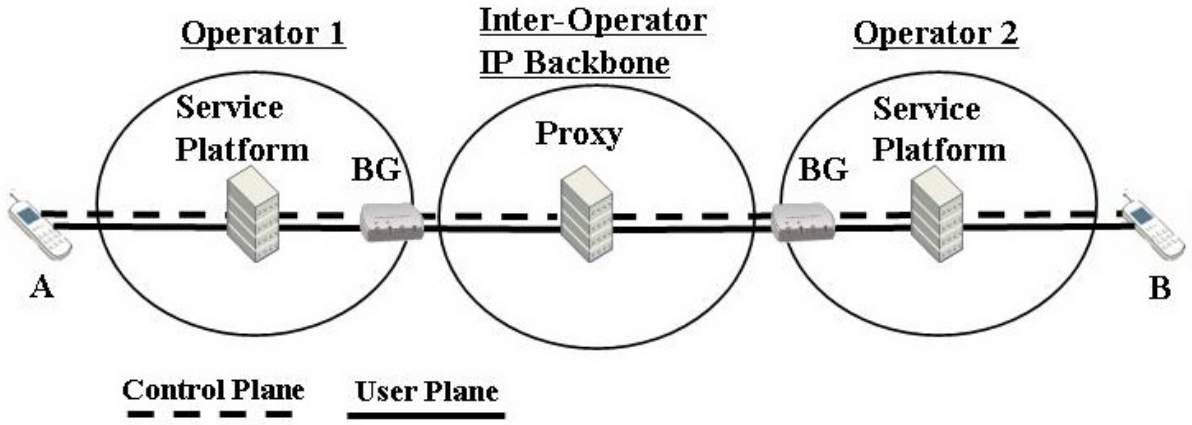

Figure 3 - Proxy in Inter-Service Provider IP Backbone

Figure 3 above shows the high-level architecture of bilateral Service Provider traffic traversing the Proxy element within Inter-Service Provider IP Backbone using any type of IP based traffic. The user plane may or may not go through the proxy depending on each service requirement.

5.6 Types of Service Provider and Interconnectivity Allowed

There are three different types of Service Provider. They are classified according to the type(s) of IP Backbone Provider(s) they connect to. This section describes each type and the connectivity allowed between the different types.

5.6.1 MNO-G

This Service Provider is a GPRS/UMTS/LTE Mobile Network Operator who connects only to a GRX network. The services they offer over the GRX network are on a bilateral basis with no guarantees of QoS end-to-end. In this document they are called type MNO-G.

5.6.2 MNO-I

This Service Provider is a GPRS/UMTS/LTE Mobile Network Operator who connects to both a GRX and an IPX network. They must be a GPRS/UMTS/LTE MNO because only these types of Service Provider are allowed to connect to the GRX. In this document they are called type MNO-I.

5.6.3 NGNO

This Service Provider connects only to the IPX network and can be any type of organisation. In practice they are unlikely to be a GPRS/UMTS/LTE Mobile Network Operator because GPRS/UMTS/LTE roaming requires connection to a GRX Network in order to reach existing GPRS/UMTS/LTE Mobile Network Operators. In this document they are called type NGNO.

5.6.4 Permitted Interconnectivity

Table 1 below describes the different types of Service Provider and the end-to-end interconnectivity allowed between them via a GRX or IPX network (or both).

Service Provider Type	MNO-G	MNO-I	NGNO
MNO-G	✓	✓(GRX Services Only)	×
MNO-I	✓(GRX services Only)	✓	✓ (IPX Services Only)
NGNO	×	✓ (IPX Services Only)	✓

Table 1 – Interconnectivity Options

5.7 Types of IP Backbone Provider

5.7.1 GRX Provider

A GRX Provider will only be able to:

- provide connections to Service Providers that are GPRS/UMTS/LTE network operators(MNO-G and MNO-I types of Service Providers)
- carry GRX services

The GRX offers a transport-only interconnection service between Service Providers that are GPRS/UMTS/LTE network operators on a bilateral basis with no guarantees of QoS end-to-end. This transport-only function may be used to transport any protocol on a bilateral basis as well as MMS hubbing and WLAN proxy services.
.

5.7.2 IPX Provider

An IPX Provider will be able to provide connections to any type of Service Provider – whether GPRS/UMTS/LTE operator or not – and can carry both GRX and IPX services.

6 REQUIREMENTS OF THE INTER-SERVICE PROVIDER IP BACKBONE

6.1 GRX Provider Requirement

GRX Providers should:

- Support connections from Service Providers in various ways (Layers 1,2 and 3)
- Comply with IP addressing guidelines for Inter-Service Provider IP Backbone in IR.40
- Comply with DNS guidelines as specified in GSMA PRD IR.67 [17]
- Offer DNS root service for contracted Service Providers
- Have BGP-4 routing capability
- Distribute all (valid) known routes to Service Providers
- Control which routes a Service Provider can advertise to the network
- Offer interconnectivity to other GRXs (GRX peering)
- Comply with Service Level Agreements
- Conform with security requirements laid out in PRD IR.77 [19]

Connection to the GRX is restricted to GSM and 3GSM MNOs. In this section, the term Service Provider above applies only to these parties.

GRX Providers should not act as a transit GRX. That is, GRX Providers should not pass traffic over their network from one connected GRX network to another connected GRX network. A packet should not pass through more than two GRX Providers' networks.

6.2 IPX Provider Requirements

All the requirements above relating to GRX Providers shall be supported by an IPX Provider. (In this case, the term Service Provider in section 6.1 applies to MNOs, FNOs, ISPs and ASPs). In addition, an IPX Provider shall:

- Support end-to-end QoS requirements, described in the end-to-end quality SLA and in this document
- Create the agreements required with other IPX Providers to fulfill the end-to-end SLA
- Maintain user traffic separation as described in 6.5.6

IPX Providers shall not act as a transit IPX. That is, IPX Providers shall not pass traffic over their network from one connected IPX network to another connected IPX network. A packet shall not pass through more than two IPX Providers' networks.

6.3 Connections between IP Backbone Provider and Service Provider

This section summarises the connections allowed between the different types of IP Backbone Provider and Service Provider.

The interconnection allowed between IP Backbone Providers and Service Providers is shown in the table below. Each connection must follow the rules shown. Note that a Service Provider may connect to multiple IP Backbone Providers provided that each connection complies with the rules in the table.

Types of IP Backbone Provider	**Types of Service Provider**		
	MNO-G	**MNO-I**	**NGNO**
GRX	✓	✓	✗
IPX	✓ (GRX Services Only)	✓	✓ (IPX Services Only)

Table 2 - Interconnections between IP Backbone Provider and Service Provider

6.4 Peering Interface

Connections between Inter-Service Provider IP Backbones are implemented and managed by the IP Backbone Providers. When operating an IPX, an IP Backbone Provider shall enter Service Level Agreements (SLAs) with other IP Backbone Providers. The end-to-end QoS SLA (QoSi SLA 15) sets out a minimum set of QoS requirements which shall be followed by the IP Backbone Providers when operating an IPX.

The Inter-Service Provider IP Backbone connectivity options are either:

- Private bilateral connection or

- Common Inter-Service Provider IP Backbone peering point (such as AMS-IX and Equinix)
- Figure 4 below shows the Inter-Service Provider IP Backbone connectivity.

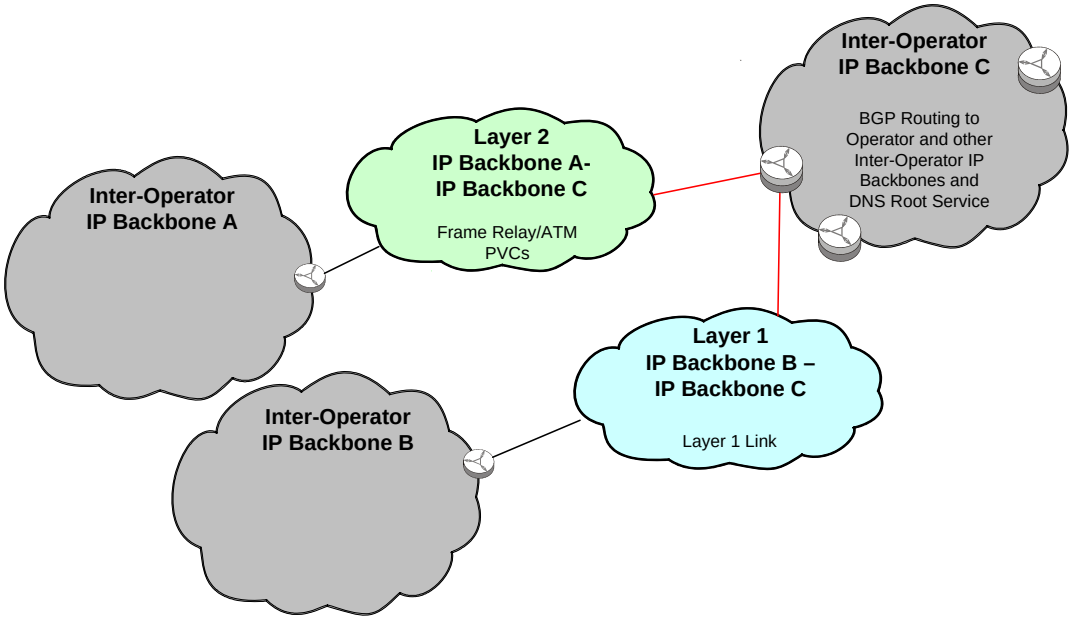

Figure 4 - Direct connections between Inter-Service Provider IP Backbone

Due to the scaleable nature of the Inter-Service Provider IP Backbone, Providers are frequently required to improve their service due to increased traffic volumes or new standards and services.

Every IPX Provider shall peer with every other IPX Provider in the areas in which they operate, through direct connection or peering points, which may be enforced by the governance rules. Where an IPX Provider has a Service Provider customer who requires a connection to a Service Provider customer of a GRX Provider that IPX Provider should peer with that GRX Provider.

It is highly recommended that a GRX Provider arrange peering with every other GRX Provider, if practicable. This facilitates and provides advantages to both GRX Providers and Service Providers in both geographical reach and service offering.

IPX Providers shall ensure that all traffic classes meet their agreed QoS values described in section 8 and shall meet their other SLA, cascade payment and IPX requirements. In particular they shall ensure that the low end-to-end delays for the transport of conversational and streaming class services are met. To meet these requirements IPX Providers will need to ensure that suitable direct connections and peering points are established. Real-time services may be used across continental boundaries and over very long distances. Peering-points must be established which minimize the geographical distance a packet must traverse, as well as the number of IP hops in the path. The equipment at the IPX peering point requires the functionality to support media traffic classes between IPXs in an unbroken stream, in such a way that peering point will not become a bottleneck for the overall IPX environment.

6.5 Technical Specification of the Inter-Service Provider IP Backbone

6.5.1 IP Routing

The Inter-Service Provider IP Backbone shall carry routing information to all parties within the connectivity agreements. Dynamic exchange of routing information between different networks should be accomplished by using BGP-4 routing protocol. When operating an IPX network, the BGP-4 routing protocol shall be used.

Dynamic routing reduces the amount of management work in the event of a change IP address requirements (i.e. new address ranges are applied). In addition, dynamic routing supports redundant connections to IP Backbones/Service Providers.

IP Backbone Providers should exchange routing information and traffic between all other Inter-Service Provider IP Backbone nodes. An IP Backbone Provider should be responsible for distributing all Inter-Service Provider BGP-4 information to all its peers. An IP Backbone Provider should advertise its customer networks to peering partners after a Service Provider has fulfilled the security requirements laid down in PRD IR.77 [19]. When operating an IPX network, the above requirements are mandatory.

The Service Provider and the IP Backbone Provider are both responsible for checking that all connected Service Provider and IP Backbone Provider networks are invisible to and inaccessible from the public Internet**.**

In an Inter-Service IP Backbone Provider environment with multiple peering points, it is recommended that “Hot potato”[24] routing (where traffic is exchanged with the next IP Backbone Provider at the *nearest peering point* in terms of delay) should be used. However “Cold potato” routing (where traffic is exchanged with the next IP Backbone Provider at the *furthest* peering point in terms of delay) may be agreed bilaterally between GRX/IPX Providers.

IP Backbone Providers shall not restrict protocols carried between Service Providers unless those protocols are non-compliant with the requirements set out in the PRD IR.77 [19].

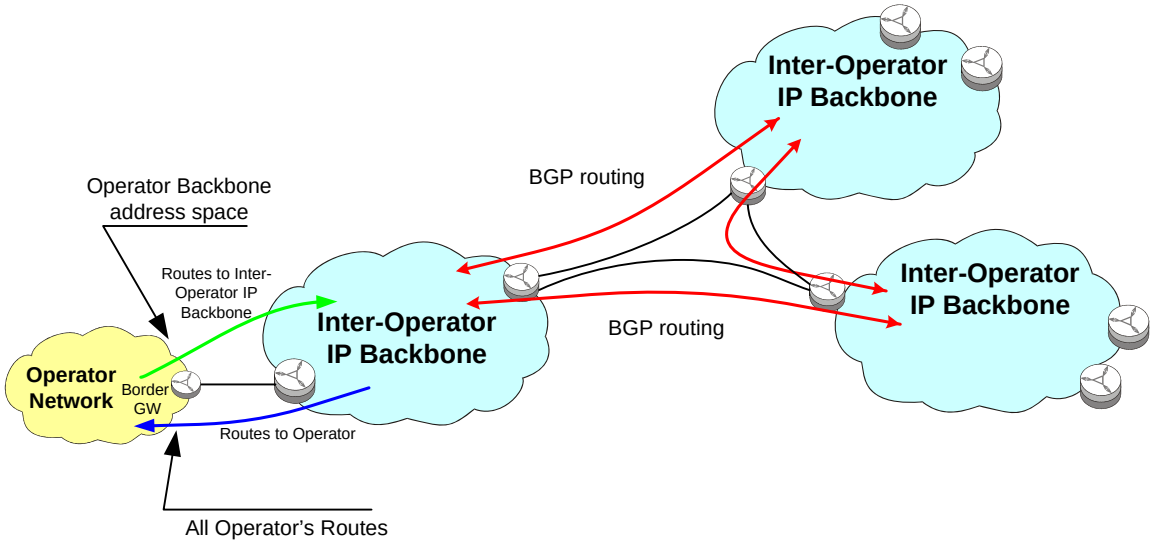

Figure 5 -Dynamic routing within Inter-Service Provider IP Backbone

6.5.2 BGP-4 Advertisement Rules

GRX Providers should not act as a transit GRX. Therefore, network routes received either over private peering or over a GRX peering point should not be re-advertised to other GRX peering partners. This requirement is mandatory for an IPX network.

IPX Providers shall also mark the IP routes they receive using the BGP community scheme presented in section 6.5.3 below.

6.5.3 BGP Extended Community Attributes

The GRX is an environment which is exclusively for GSM MNOs whereas the IPX also involves other kinds of Service Providers. Therefore there is a need to interwork these two environments in a manner which avoids unnecessary complexity for GSM MNOs. As a result of this interworking, there is a need to separate different types of Service Providers and to build a scheme that ensures that pure NGNO operators cannot have connectivity to MNO-G Service Providers and vice versa.

BGP Extended community attributes are introduced as a tool to build this separation. This section gives more precise descriptions of communities and how and where marking and filtering is done in IPX networks. By giving each type of Service Provider its own dedicated BGP extended community value we can ensure that, for example, a MNO-G Service Provider can route traffic to another MNO-G Service Provider but not to an NGNO Service Provider. By using extended community values coupled with a simple set of rules we can ensure that the IP addresses of an MNO-G Service Provider are never advertised to an NGNO Service Provider and vice versa. With other security rules like “no route of last resort” (see PRD IR.77[19]), this also ensures that traffic from an NGNO Service Provider does not route via a GRX Provider. This provides enhanced security for Service Providers and IP Backbone Providers.

6.5.3.1 Differentiating between Service Providers

IPX Providers shall separate different kinds of Service Providers, service types and geographical locations using BGP Extended Communities. IPX Providers shall mark each route it receives with one of the extended community values defined below to achieve this. This section describes how these extended community values are used.

Compliance with these rules is mandatory for IPX Providers. There is no mandatory requirement for a GRX Provider to mark or check communities; these tasks are performed by IPX Providers. GRX Providers may decide if they want to follow the guidance or not. GRX Providers may also decide whether or not to keep these BGP communities untouched through their network.

Marking is always performed by the originating IP Backbone Provider, except in the case where the originating IP backbone Provider is a GRX, when the marking in done by the first (and only) IPX Provider in the path.

The following table lists the rules for marking of extended community values inside BGP4 routing between different types of Providers. It shows:

- the possible settings for the BGP4 extended community value marking
- whether marking the routing information is optional or mandatory

	Advertisement coming from:				
		MNO-G Service Provider	**MNO-I Service Provider**	**NGNO Service Provider**	**GRX Provider**
Action By:	**GRX**	Marking: MNO-G Optional	None	None	Marking MNO-G Optional (Marking done in peering point)
	IPX	Marking: MNO-G Mandatory	Marking: MNO-I Mandatory	Marking: NGNO Mandatory	Marking: MNO-G Mandatory (Marking done in peering point)

Table 3 - BGP Extended Community Values in BGP4 Routing Information

6.5.3.2 BGP4 Community Definitions

BGP extended Communities are described in RFC 4360 [23].
Community values are often defined using the notation aaaaa:nnnnn which will be used in this document.
The values for aaaaa will always be the AS number of the originating IP Backbone Provider who is doing the marking. By using the AS number in the first part of the community it identifies the party which eases the troubleshooting.

Since multiple communities will be used, it is recommended to identify each community by a serial number as follows:

Community 1 identifies the regional info (:1nnnn)
Community 2 identifies the type of operator (:2nnnn)
Community 3 identifies (future use) (:3nnnn)

The regional info where the corresponding service providers are located and corresponding values of nnnn are defined as follows:

Area	**Used community1**
Europe	1000
North-Europe	1100
Middle-Europe	1200
East-Europe	1300
South-Europe	1400
Asia	2000
East Asia	2100
South-east Asia	2200
Oceania	2300
America	3000
North America (East Coast)	3100
North America (West Coast)	3200
Central America	3300
South America	3400
Africa	4000

Table 4 - BGP-4 Regional Community Values

The types of Service Provider and corresponding values of nnnn are defined as follows:

Service Provider Type	BGP Community Value nnnn
MNO-G	0100
MNO-I	0200
NGNO	0300

Table 5- BGP-4 Type of Operators Community Values

6.5.3.3 Filtering based on BGP communities

Among other security and routing definitions such as the prevention of transit Inter-Service Provider IP backbone traffic, IPX Providers shall base their BGP-4 outbound advertisements for BGP communities presented in section 6.5.3.

.

The following diagram demonstrates the full range of options for interconnection of Service Providers and IP Backbone Providers. It does not demonstrate all possibilities for peering between IP Backbone Providers.

6.5.3.4 BGP communities tagging

In the GPRS roaming environment other communities can be in use and should be left unhandled over the entire transport path. IP Backbone Provider should transparently transport all communities, bilateral agreed between Service Provider and IP Backbone Provider, and might add additional communities, but starting with their own AS number as described in section 6.5.3.2.

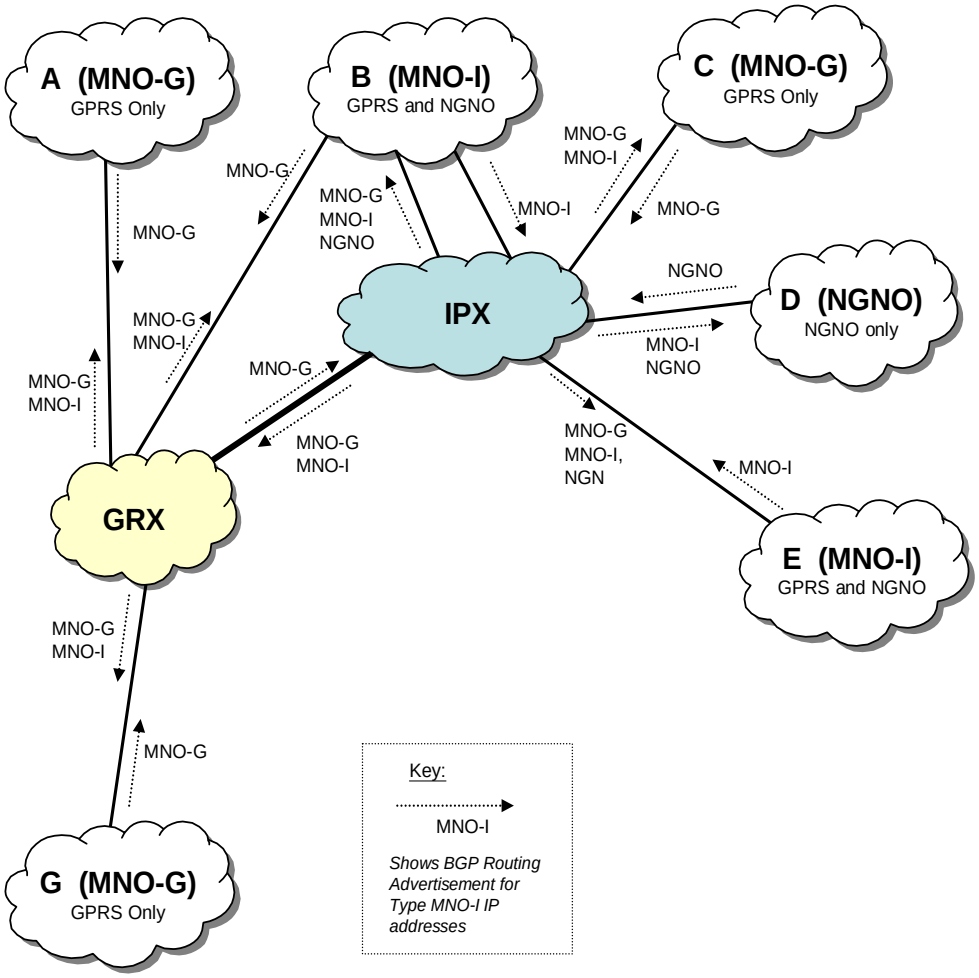

Figure 6 – Provider BGP-4 Route Advertisements

The following table (table 5) summarises the rules shown in the figure above. The table maps destinations to communities, indicating which communities may be advertised by IPX Providers to which destinations. Communities which are not permitted to be forwarded to a destination shall be filtered out by the IPX Provider on that route.

Destination of Advertisement	Communities forwarded
MNO-G	MNO-G, MNO-I
GRX	MNO-G, MNO-I
MNO-I	MNO-G, MNO-I, NGNO
NGNO	MNO-I, NGNO

Table 5 - Rules summary

6.5.3.5 Security Benefits

The use of BGP Extended Communities to enforce routing policy provides security and performance benefits to Service Providers

- Performance critical “NGN”-type services cannot be routed via GRX networks where QoS policies are not enforced
- MNO-G type Mobile Networks are protected from malicious attacks originating from NGNO networks and vice versa.
- MNO-I type Mobile Networks can optionally be protected from malicious attacks originating from NGNO networks.

6.5.4 IP Addressing

Internet routers should not be able to route to the IP addresses advertised to the Inter-Service Provider IP Backbone. The IP Backbone Providers and Service Provider networks shall be totally separated from public Internet, from an IP routing perspective.

Currently, Inter-Service Provider IP Backbone networks use IPv4 addressing and there is no plan to introduce native IPv6 addressing in the foreseeable future. It is intended that IPv6 is supported by tunnelling the IPv6 traffic over IPv4 between Service Providers where required.

Both IP Backbone Providers and Service Providers who employ IPv6 in their network should assume full responsibility for all network adjustments necessary for maintaining connectivity to all other IP Backbone Providers and/or Service Providers that deploy IPv4.

An IP Backbone Provider is responsible for the denial of IP spoofing attacks originated by its Service Provider customers, i.e. only traffic from valid IP address ranges is allowed to flow to other customers or other IP Backbone Providers.

6.5.5 DNS

As a minimum requirement, GRX Providers should support the transport of queries between MNOs to allow for correct resolution of FQDNs for all service requirements, for example APNs and MMSC hostnames (for MMS inter-working). IPX Providers shall support the transport of such DNS queries. IPX Providers shall also provide for transport of ENUM queries to support identified services.

The main specification for DNS of the Inter-Service Provider IP Backbone network, including hostname recommendations, is GSMA PRD IR.67 [17].

6.5.6 Security and Screening

The Inter-Service Provider IP Backbone should meet the requirements laid out in PRD IR.77 [19]. The requirements are mandatory for IPX Providers.

Service Providers and IPX Providers shall also ensure that all UE IP datagrams are encapsulated in tunnels to prevent the underlying IPX network from being reachable by end-users.

UE-to-UE and UE-to-Server SIP/IMS IP traffic shall be encapsulated using GRE when traversing the IPX. The encapsulation used for other types of UE IP datagrams shall be GTP for GRPS roaming and IPSec for WLAN interworking. The encapsulation methods for other types of UE IP datagrams are for further study.

Tunnels may terminate directly to other Service Providers, or may terminate at an IPX Proxy (with a corresponding tunnel being used between the IPX Proxy and the terminating Service Provider).

6.5.7 QoS

The GRX network may support Class of Service (CoS) parameters presented in section 8 of this document.

The QoS requirements for the IPX are outlined in section 8 and also in the end-to-end QoS SLA (IPX Agreement PRD AA.80 [22]). End-to-end QoS as described in [15] is a mandatory requirement for IP Backbone Providers in the case of IPX.

Section 8 of this document concentrates on providing a traffic class specification and the parameters for different classes of service.

6.5.8 Generic Proxy Requirements

The IPX will include a number of proxies that support specified IP service interworking. IPX Proxies are not mandatory but will be needed to support Service Transit and Hubbing Connectivity options. Note that the use of an IPX Proxy does not necessarily imply the adoption of a multilateral connectivity model; Proxies may also be used to support services on a bilateral basis. Specific requirements for each service will be captured elsewhere. The following is a non-exhaustive list of generic features required from all IPX Proxies.

- Session-based accounting including CDR generation
- Facility to implement Black list/White list requirements in Multilateral mode
- Capability of transporting both control plane & user plane packets between different IP multimedia networks
- Security functions (such as access control)
- IPv4 / IPv6 transition/translation – if not handled by other network elements
- Media protocol conversion / transcoding - if required.
- Signaling protocol conversion – if not handled by other network elements
- Destination address look-up (including MNP) – if not solved by originating Service Provider.
- Transparency - the proxy shall not in anyway manipulate service related aspects of protocol information except where required by an IPX service schedule or other GSMA PRD or agreed by the interconnecting parties in a bilateral agreement
- Support the ability to trace the originator of a service and the proxies used in its delivery wherever possible.

There are a number of practical advantages to using a Proxy. These include, but are not limited to:

- Proxy Services minimize configuration changes in Service Provider networks caused by modifications performed in interworking partner networks.
- Proxy Services can handle IP version and protocol conversions, as well as other functions required by Service Providers (such as address resolution/number portability handling).
- Proxies can handle overlapping IP addresses typically used by Service Providers.
- Proxies can be utilised in the generation of charging data between Service Providers, in either a bilateral or multilateral arrangement.

7 TECHNICAL REQUIREMENTS FOR SERVICE PROVIDERS

7.1 General Service Provider Requirements

It is recommended that Service Providers frequently review the services provided by IP Backbone Providers as these services may be affected by increased traffic volumes or new standards.

7.1.1 Service Provider IP Routing

The Service Provider is responsible for checking that all connected Service Provider and IP Backbone Provider networks are invisible to and inaccessible from the public Internet**.**

Service Providers may screen unwanted routes e.g. by selecting address ranges of their interconnect partners.

7.1.2 Service Provider IP Addressing

Public addressing shall be applied in all Service Provider IP Backbone network elements, which are advertised or visible to other Service Providers. Using public addressing means that each Service Provider has a unique address space that is officially reserved from the Internet addressing authority. However, public addressing does not mean that these addresses should be visible to Internet. For security reasons, Service Provider and inter-Service Provider backbone networks shall remain invisible and inaccessible to the public Internet.

Internet routers should not be able to route to the IP addresses advertised to the Inter-Service Provider IP Backbone. In other words the IP Backbone Providers' and Service Providers' networks shall be totally separated from public Internet, from an IP routing perspective.

Currently, the Inter-Service Provider IP Backbone networks use IPv4 addressing and there is no plan to introduce native IPv6 addressing in the foreseeable future. It is intended that IPv6 is supported by tunnelling the IPv6 traffic over IPv4 between Service Providers where required.

Both IP Backbone Providers and Service Providers who employ IPv6 in their network should assume full responsibility for all network adjustments necessary for maintaining connectivity to all other IP Backbone Providers and/or Service Providers that deploy IPv4.

7.1.3 Service Provider DNS

The recommendations in GSMA PRD IR.67 [17] shall apply.

7.1.4 Service Provider Security and Screening

Service Providers shall meet the requirements for security laid out in PRD IR.77.

It is strongly recommended that Service Providers implement firewalls at the ingress points of their networks; for mobile operators, that is adjacent to Border Gateways. It is further recommended that Service Providers using the IPX implement a firewall function to prevent packets with incorrect/invalid IP addresses from being passed onto the IPX.

Each Service Provider shall be responsible for screening traffic inbound to its own BG/ Firewall. Generally, Service Providers should allow only those protocols that are needed for established services, troubleshooting and network monitoring. Note that 'ping' and 'traceroute' are mainly used for testing, troubleshooting and QoS measurement purposes. The end-to-end QoS SLA (QoSi SLA 15) describes different options for measurements over an IPX backbone, including local tails used by both Service Providers. A description and a usage policy for diagnostic tools should be included in the interconnect agreement.

Service Providers shall ensure that for all IPX connections, all user traffic, (UE-to-UE and UE-to-Server), is separated from Server-to-Server traffic. This is to fulfil the requirement of end users not being able to reach or "explore" the IPX network.

Service Providers shall also ensure that all UE IP datagrams sent to the IPX are encapsulated in tunnels to prevent the underlying IPX network from being reachable by end-users. Tunnels may terminate directly to other Service Providers, or may terminate at an IPX Proxy (with a corresponding tunnel being used between the IPX Proxy and the terminating Service Provider).

UE-to-UE and UE-to-Server IP traffic shall be encapsulated using GRE when traversing the IPX except for GPRS/UMTS Roaming (where GTP is used)), LTE roaming (where PMIP and GTP is used) and WLAN interworking (where IPSec is used).

7.2 BGP Advertisement Rules

7.2.1 General Rules

Service Provider's core network addresses may be advertised to the Inter-Service Provider IP Backbone with the BGP-4 [6] routing protocol and shall have an AS (Autonomous System) [6] number acquired from the Internet addressing authority or the GSMA as appropriate. The acquired AS number should be used as an originating AS when a Service Provider advertises its own IP addresses to the Inter-Service Provider IP Backbone. When connecting to an IPX, the BGP-4 protocol shall be used for advertising a Service Provider's network addresses.

Service Providers using the GRX should follow the BGP advertisement style rules listed below.

- No host specific route or small block advertisements shall be advertised to the Inter-Service Provider IP Backbone. No mask/29 advertisements shall be made unless a smaller block was allocated to that Service Provider by the internet registry
- Advertised routes from each Service Provider shall be summarized whenever possible. Summarizing smaller subnets into bigger blocks will minimize size of the routing tables and reduce router processing load. This summary may be carried out by the Service Provider or the IP Backbone Provider
- Service Providers shall only advertise their own core public IP address ranges into the Inter-Service Provider IP Backbone
- Networks advertised by Service Providers shall originate from the AS number assigned to them. (AS path shall start Service Provider AS number)
- Service Providers must only notify to their IP Backbone Providers(s) IP address ranges used by their network infrastructure. This allows their Providers to build their routing filters
- Service Providers shall use BGPv4 communities presented in chapter 6.5.3, to tag all it's own network advertisements towards Inter-Service Provider IP Backbone
-
- IP address ranges used by User Terminals must not be advertised to or routed on the Inter-Service Provider IP Backbone

Service Providers using the IPX shall follow the rules above.

The BGP advertisements of Services Providers will be marked by IPX Providers according to the rules described in section 6.5.3. No action is required from the Service Provider.

7.3 Service Provider and Inter-Service Provider IP Backbone Connectivity

The end-to-end SLA [22, Annex] describes the different options for establishing physical connections from a Service Provider to the IPX. Different connection options can be divided into three categories:

- 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)

The use by a Service Provider of an Internet IPSec VPN for the local tail is strongly discouraged unless there is no viable alternative.

It is up to IP Backbone Provider and Service Provider to determine the exact details of each connection bilaterally, however details in the end-to-end SLA shall be followed in the case of IPX. The main benefits of the Inter-Service Provider IP Backbone structure to Service Providers are:

- The Service Providers do not have to create dedicated connections to every roaming partner. One connection to one Inter Service Provider IP Backbone Provider is required as a minimum.
- Service Providers may choose to start with low quality and low capacity connection to the Inter-Service Provider IP Backbone 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 i.e. the IP Backbone is scalable and able to meet Service Provider Requirements.
- Inter-Service Provider IP Backbone has QoS implemented and shall be measurable on a Service Provider by Service Provider basis.
- Inter-Service Provider IP Backbone introduces a Hub Connectivity Option to simplify different interworking scenarios

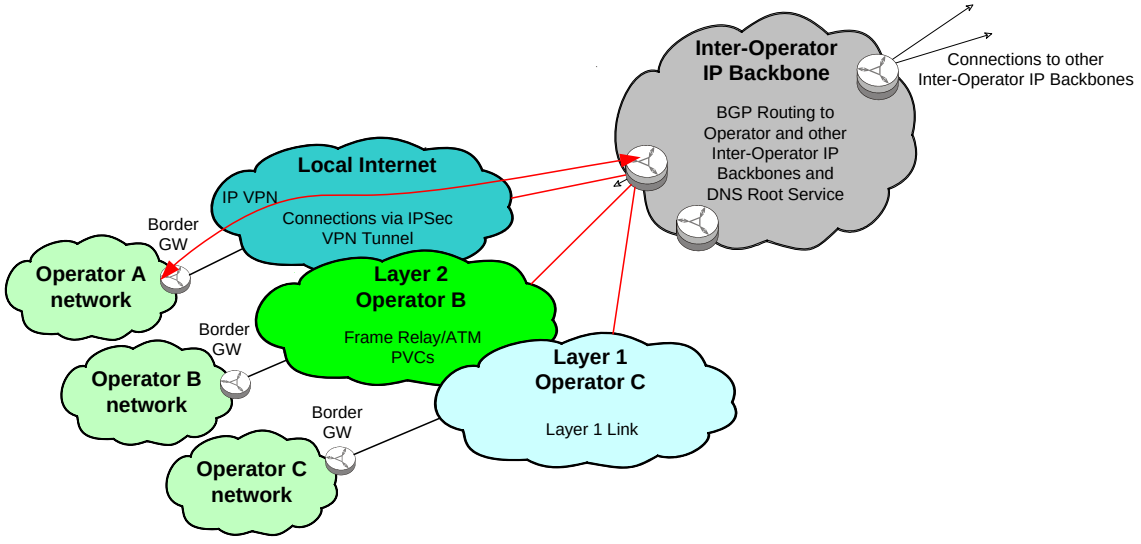

Figure 7 -Connections between Service Provider and Inter-Service Provider IP Backbone

8 QOS

8.1 SLA for Inter-Service Provider IP Backbone

The end-to-end QoS SLA [22] describes different kind of connection models and how QoS will be achieved in those cases. Actual values for different CoS class parameters can be found in this chapter.

An SLA defines a service specification between a Service Provider and an IP Backbone Provider (e.g. access availability). An SLA can also define IP Backbone Provider to IP Backbone Provider service specifications depending on bilateral agreements between IP Backbone Providers where IP QoS definitions described in the following sections might apply. The parties to the SLA may agree an IP QoS profile. This should be supported over the connection between an individual Service Provider and their IP Backbone Provider. The profile extends to the whole Inter-Service Provider IP Backbone network comprising IP Backbone Providers' maintained networks and routers.

The following aspects should be considered for inclusion in the agreement between Service Provider and Inter-Service IP Backbone provider

8.1.1 Service Guarantees

Service guarantees should be defined for each IP QoS parameters defined in sections 8.3 and 8.4. Additionally, there should be a defined reporting and escalation procedure, i.e. the Backbone Provider takes responsibility to provide measurements and permits the Service Provider to analyse the results.

8.1.2 Responsibilities

Terms and conditions of each SLA component should be examined and whether Service Provider's account should be credited and if so to extent where the SLA has not been met. Note penalties shall be in scope for any future governance.

Help desk support and customer services should be considered.

8.2 Traffic classification

It is recommended that following traffic classes are available and marked as presented in the table 7. Traffic classes are distinguished by Differential Service bits. These bits are seen in IP ToS field and used for prioritizing traffic if needed.

QoS Information		Diffserv PHB	DSCP
Traffic Class	**THP**		
Conversational	N/A	EF	101110
Streaming	N/A	AF41	100010
Interactive	1	AF31	011010
	2	AF21	010010

	3	AF11	001010
Background	N/A	BE	000000

Table 6. Traffic classes and their mapping to DSCP values

8.2.1 Traffic Handling Priority

The Traffic Handling Priority (THP) specifies the relative importance of applications that belong to the Interactive traffic class. [13].

8.2.2 Diffserv Per Hop Behaviour

The Per Hop Behaviour (PHB) is the packet forwarding function carried out by the Diffserv-capable routers on the path of a given packet flow. PHBs can be seen as the Diffserv classes of service.

Different types of PHB are defined for Diffserv:

- Expedited Forwarding (EF) [15],
- Assured Forwarding (AF) [16], and
- Best Effort or Default (BE) [16].

8.2.3 Differentiated Services Code Point

The 6-bit DSCP indicates the PHB that a packet belongs to. The DSCP values shown in Table 7 are recommended values in IETF [15][16].

8.2.4 Traffic classes

- Conversational – Typically in this class are placed services that needs tight delay and jitter values
- Streaming – Normally expectations are not as tight as in conversational class as UE normally buffering
- Interactive – Corporate sensitive traffic which needs reserved bandwidth to guarantee service requirements
- Background – Typically packet size in background class is pretty big, and traffic is not that much reliable to delay and jitter, as long as packets are not dropped in network to avoid retransmissions and extra load to network

Service providers are responsible for marking packets to correct traffic classes. They may outsource this functionality to Inter-Service IP Backbone provider when suitable. Inter-Service IP Backbone providers may change DSCP values in their own network as long as they return values set by operators before traffic is given to an other inter-Service IP Backbone provider or Service Provider and they fulfill given values for parameters per class.

An IPX provider can change the DSCP value, unless otherwise agreed bilaterally between two Service providers, to be in line with pre-agreed levels (Table 8) within an IPX environment. A GRX network is not QoS aware and therefore will not look into the DSCP value set by sending operators. Both providers, GRX and IPX will co-exist and will exchange GPRS Roaming traffic in the defined GRX peering points and therefore an IPX provider might change the DSCP value received from a GRX provider. The DSCP value shall not be altered in the transport mode only in an IPX environment.

Application	protocol	PHB	Potential QoS class name
VideoShare	N/A	EF	Conversational
VoIP	RTP	EF	Conversational
Push to talk	N/A	AF4	Streaming
Video streaming	N/A	AF4	Streaming
Unrecognized GTP traffic	N/A	AF3	Interactive
DNS	DNS	AF3	Interactive
Online gaming	N/A	AF3	Interactive
WAP browsing	GTP_C, GTP_U	AF2	Interactive
WEB browsing	N/A	AF2	Interactive
Instant messaging	N/A	AF1	Interactive
Remote conn.	SSH, telnet	AF1	Interactive
Email sync	N/A	BE	Background
MMS	SMTP	BE	Background

Table 7. Application mapping into DSCP

- GTP protocol port(s): UDP2123 (GTP_C), UDP2152 (GTP_U), UDP3386 (GTP_Prime)
  SMTP protocol port(s): 25

8.3 IP QoS Definitions for Inter-Service Provider IP Backbone

The QoS parameters, which characterize QoS, should be defined in the SLA (QoSi SLA15). The QoS parameter set should be consistent and uniquely understood by all parties involved in the IP connection.

Following QoS parameters are covered

- Service availability
- Jitter
- Packet Loss
- Delay

If parameter measurements indicate a violation of an SLA, the parties may wish to include the measures to be taken to rectify the violation.

To achieve QOS parameter values presented in following chapters, these requirements shall be followed:

- stated values will be maximum RTD over 1 or 2 Inter-Service IP Backbone Providers and Service Providers premises
- RTD performance assumes a Local Loop connection of no more than 20 km from Service Providers to the Inter-Service IP backbone Providers PoP (Point-of-Presence).
- Local Loop size is 2 Mbit/s as minimum

Following chapters uses SOURCE AND DESTINATION definitions for defining demarcation/measurement point between originating and terminating service provider premises. SOURCE and DESTINATION term shall follow above mentioned requirements.

8.3.1 Availability

Service availability is a proportion of the time that IP Backbone Providers service is considered available to service providers on a monthly average basis.

Service Providers should discuss with IP Backbone Providers the extent to which the latter can guarantee the reliability of their network. It is advisable to consider the availability of the following network elements or components in SLA agreement:

- Inter-Service Provider Backbone core, including peering/interworking functionality and possible DNS functionalities
- Service Provider to Inter-Service Provider IP Backbone connection,
- Monitoring/measurement equipment (if supported).

Values for availability are following

- Availability of the IP Backbone Service Provider Core: 99,995%
- Service Providers connection to IP Backbone Service Provider core with single connection: 99,7%
- Service Providers connection to IP Backbone Service Provider core with dual connection: 99,9%

8.3.2 Delay

Roundtrip delay is the total time that it takes to transmit an IP packet from the SOURCE to the Destination and receive the reply packet from the destination at the SOURCE. (Measured over a given period of time, in milliseconds)

Table 9 and Table 10 presents Roundtrip delay values between originating and terminating Service Provider premises.

It should be noted that actual performance of Inter Service provider IP backbone network could be better than given reference values in the Table 9 and Table 10.

approx round trip time in (ms)

EF & AF4	West Europe	North-Europe	East Europe	South Europe	East Asia	South Cental Asia	South-East Asia	Western Asia	Oceania	N America (East Coast)	N America (West Coast)	Central America (inc Caribbean)	S America	Africa
West Europe	55	45	80	72	340	171	360	129	380	120	200	225	330	242
North-Europe	45	40	35	75	350	145	360	119	400	130	215	249	335	269
East Europe	80	35	40	102	360	113	370	93	420	165	215	281	350	262
South Europe	72	75	102	72	345	154	355	104	380	145	220	247	335	218
East Asia	340	350	360	345	150	152	165	216	275	340	285	353	460	383
South Central Asia	171	145	113	154	152	80	108	68	271	306	334	394	411	242
South-East Asia	360	360	370	355	165	108	145	162	255	360	310	489	480	251
Western Asia	129	119	93	104	216	68	162	80	323	280	347	350	346	194
Oceania	380	400	420	380	275	271	255	323	90	360	310	369	470	287
N America (East Coast)	120	130	165	145	340	306	360	280	360	40	90	92	280	326
N America (West Coast)	200	215	215	220	285	334	310	347	310	90	40	126	300	418
Central America (inc Caribbean)	225	249	281	247	353	394	489	350	369	92	126	40	137	294
S America	330	335	350	335	460	411	480	346	470	280	300	137	120	180
Africa	242	269	262	218	383	242	251	194	287	326	418	294	180	180

Table 8. Delay values for conversational and streaming traffic classes

AF1-3 & BE	West Europe	North-Europe	East Europe	South Europe	East Asia	South Cental Asia	South-East Asia	Western Asia	Oceania	N America (East Coast)	N America (West Coast)	Central America (inc Caribbean)	S America	Africa
West Europe	66	54	96	86	408	206	432	154	456	144	240	270	396	290
North-Europe	59	48	42	90	420	174	432	143	480	156	258	298	402	322
East Europe	104	42	48	122	432	136	444	111	504	198	258	337	420	315
South Europe	94	90	122	86	414	185	426	124	456	174	264	297	402	262
East Asia	442	420	432	414	180	182	198	259	330	408	342	424	552	459
South Central Asia	223	174	136	185	182	96	130	81	326	367	401	473	493	291
South-East Asia	468	432	444	426	198	130	174	195	306	432	372	587	576	301
Western Asia	167	143	111	124	259	81	195	96	388	335	416	420	415	232
Oceania	494	480	504	456	330	326	306	388	108	432	372	442	564	345
N America (East Coast)	156	156	198	174	408	367	432	335	432	48	108	111	336	391
N America (West Coast)	260	258	258	264	342	401	372	416	372	108	48	151	360	501
Central America	292	298	337	297	424	473	587	420	442	111	151	48	165	352
S America	429	402	420	402	552	493	576	415	564	336	360	165	144	216
Africa	314	322	315	262	459	291	301	232	345	391	501	352	216	216

Table 9**. **Delay values for interactive and background traffic

"To determine which countries reside in each of the Regions specified in the RTD tables above, please refer to the following United Nations web site for this information http://www.un.org/depts/dhl/maplib/worldregions.htm

8.3.3 Jitter

Jitter (or the IP Packet Delay Variation as it may be known) is the delay variation among the different packets sent from the SOURCE to the DESTINATION (Measured over a given period of time, in milliseconds.) and measured as follows.

Definition
Standards-based definition: IETF RFC 3393, IP Packet Delay Variation Metric (IPPM);

RFC 3393 states, “A definition of the IP Packet Delay Variation (ipdv) can be given for packets inside a stream of packets.
The ipdv of a pair of packets within a stream of packets is defined for a selected pair of packets in the stream going from one measurement point MP1 to another Measurement point MP2. In this case the measurement points are the same as those that have been defined for Delay, as outlined in section 8.3.2.
The ipdv is the difference between the one-way-delay of the selected packets.”

RFC 3393 states that measuring jitter from a source to a destination host is useful for the following reasons:-

- One important use of delay variation is the sizing of play-out buffers for applications requiring the regular delivery of packets (for example, voice or video play-out). What is normally important in this case is the maximum delay variation, which is used to size play-out buffers for such applications;
- Other uses of a delay variation metric are, for example, to determine the dynamics of queues within a network (or router) where the changes in delay variation can be linked to changes in the queue length process at a given link or a combination of links;
- In addition, this type of metric is particularly robust with respect to differences and variations of the clocks of the two hosts. This allows the use of the metric even if the two hosts that support the measurement points are not synchronized.

Jitter Target Values

The following Jitter values shall only apply to conversational and streaming traffic classes (i.e. EF and AF4 traffic classes).

Intra-continent Jitter Value - **5mS** per GRX/IPX Provider (maximum of 2 involved in the service delivery chain)

Inter-continent Jitter Value - **10mS** per GRX/IPX Provider (maximum of 2 involved in the service delivery chain)

Intra-Continent Traffic

In the case where traffic is exchanged over one GRX/IPX Provider between Service Providers in the same Continent, the total end to end Jitter value would be 5mS. This would increase to 10mS (5mS x 2) where 2 GRX/IPX's are involved in the service delivery chain in that Continent).

Inter-Continent Traffic

In the case where traffic exchanged between Service Providers in different continents, and GRX/IPX1 is exchanging traffic with GRX/IPX2 in the same continent as the originating Service Provider, GRX/IPX 1 would have a 5mS Jitter target and GRX/IPX2 would have a 10mS target to recognise that IPX/GRX2 traffic is inter-continental.

8.3.4 Packet Loss Rate

Packet Loss is the ratio of dropped packets to all packets sent from the SOURCE to DESTINATION in percents (Measured over a given period of time)

Following table shows packet loss rate for traffic classes

Class of Service	Average Monthly Packet Loss
AF1	<0.1%
AF3	0.05 to 0.08%
EF + AF4	0.1%

Table 10. Packet loss requirements

The backbone network between Inter-Service Provider IP Backbones should be dimensioned so that packet drops do not occur (or occur relatively rarely).

9 TRAFFIC APPLICATIONS

The following sections describe some of the traffic applications for the Inter-Service Provider IP Backbone network.

9.1 GPRS/3G Data Roaming

All GPRS roaming traffic is carried on GPRS Tunnelling Protocol (GTP) defined in 3GPP TS 29.060 [7]. This protocol tunnels user data and signalling between GPRS Support Nodes in the GPRS IP Backbone network. TCP carries GTP PDUs in the GPRS IP Backbone network for protocols when a reliable data link is needed and UDP carries GTP PDUs otherwise (see 3GPP TS 23.060 [3] for more information). Only SGSNs and GGSNs implement the GTP protocol (see 3GPP TS 29.060 [3]). No other systems need to be aware of GTP.

In order to connect to an Inter-Service Provider IP Backbone, i.e. GPRS Roaming Network, it is recommended that the Service Provider have an established or planned GPRS or 3G data roaming agreement with one or more Service Providers.

9.2 Service Provider Bilateral Services

The Inter-Service Provider IP Backbone network may be used to transport any IP traffic on a bilateral basis as part of the transport only model, provided it does not have a negative impact on other services. The interworking services presented in the previous sections may be run with a bilateral agreement.

When using an IPX, the traffic may be transported with a guaranteed Quality of Service.

9.3 WLAN Roaming

The Inter-Service Provider IP Backbone can be used for WLAN roaming between Service Providers. At the first phase, Inter-Service Provider IP Backbone is used only for transporting RADIUS messages that are used for authentication, accounting and authorization of the WLAN services. For further information see PRD IR.61 WLAN Roaming Guidelines.

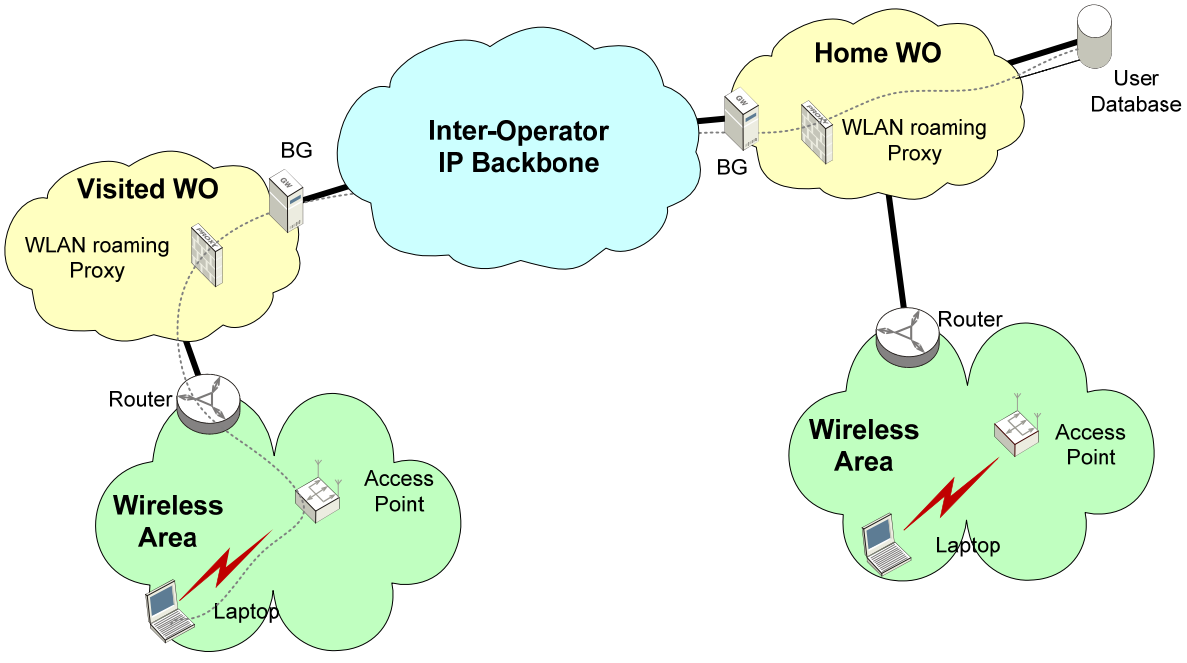

Figure 8 - Inter-Service Provider IP Backbone used for the WLAN roaming

9.4 MMS Interworking

The Inter-Service Provider IP Backbone can be used to exchange MMS traffic between Service Providers utilizing SMTP protocols. For further information see PRD IR.52 MMS Interworking Guidelines.

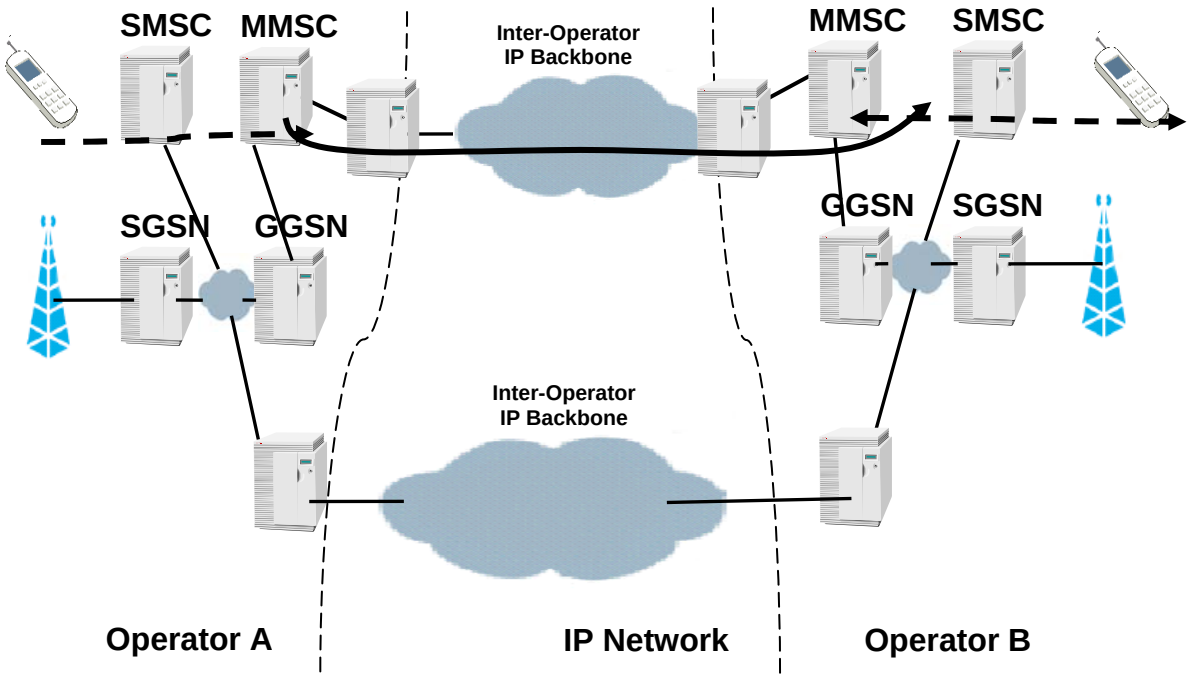

Figure 9 - Inter-Service Provider IP Backbone used for MM4

9.5 IMS

The Inter-Service Provider IP Backbone can be used for IMS interworking [20] between IMS networks [21] as depicted in Figure 10 below. Note that User Plane traffic may or may not be sent through the IPX Proxy.

IMS interworking will introduce new protocols (e.g used by peer-to-peer applications in the user plane) which the IP Backbone Provider shall not restrict. User-to-User or User-to-Server traffic shall be carried inside GRE tunnel over the Inter-Service Provider IP Backbone. At least the User Plane shall be encapsulated, and it is optional whether or not the Control Plane is encapsulated. For further information on IMS see PRD IR.65 IMS Roaming & Interworking Guidelines.

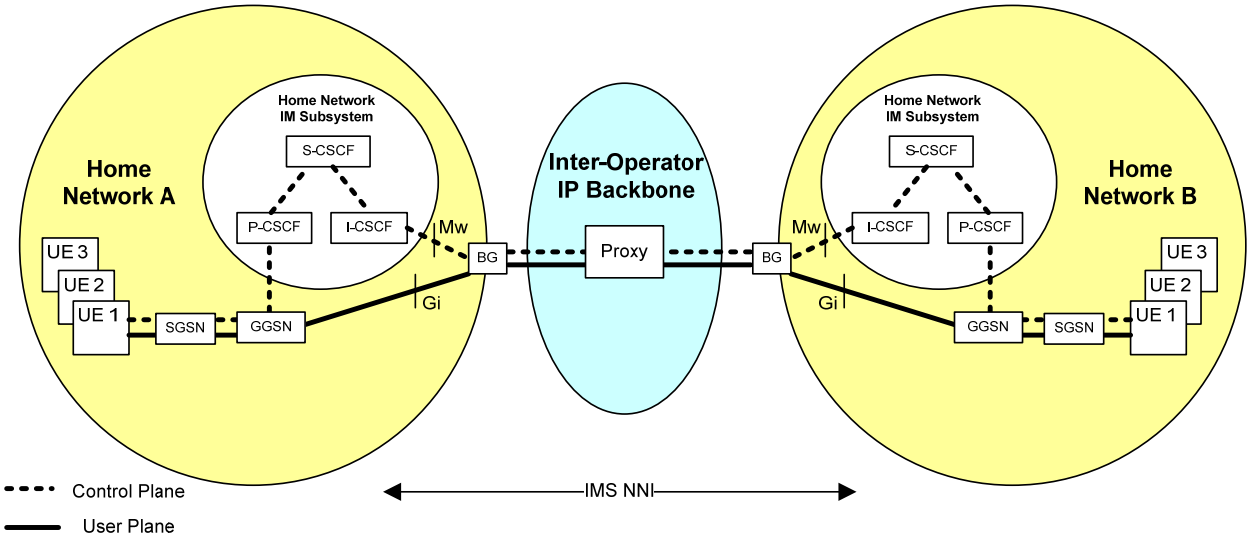

Figure 10 - Inter-Service Provider IP Backbone used for the IMS Interworking

More detailed requirements for an IPX Proxy for SIP-based traffic can be found in Annex B: Proxy requirements.

10 REFERENCES

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

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

[3] 3GPP TS 23.060: " General Packet Radio Service (GPRS); Service Description; Stage 2"

[4] 3GPP TS 21.905: "3G Vocabulary"

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

[6] IETF RFC 4271: "A Border Gateway Protocol 4 (BGP-4)"

[7] 3GPP TS 29.060: " General Packet Radio Service (GPRS); GPRS Tunneling Protocol (GTP) across the Gn and Gp Interface"

[8] IETF RFC 4301: "Security Architecture for the Internet Protocol"

[9] IETF RFC 4302: "IP Authentication Header"

[10] IETF RFC 4305: Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)

[11] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)":

[12] IETF RFC 4306: "The Internet Key Exchange (IKE)"

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

[14] Void

[15] IETF RFC 3246: "An Expedited Forwarding PHP"

[16] IETF RFC 2597: "Assured Forwarding PHB Group"

[17] GSMA PRD IR.67: "DNS/ENUM Guidelines for Service Providers & GRX/IPX Providers"

[18] 3GPP TS 23.003: "Numbering, addressing and identification"

[19] GSMA PRD IR.77 “Inter-Operator IP Backbone Security requirements For Service Providers and Inter-Operator IP Backbone Providers”

[20] GSMA PRD IR.65 “IMS Roaming & Interworking Guidelines”

[21] 3GPP TS 23.228: “IP Multimedia Subsystem (IMS); Stage 2”

[22] GSMA PRD AA.80 “General Terms & Conditions For Agreement for IP Packet eXchange (IPX) Services”

[23] IETF RFC 4360: “BGP Extended Communities Attribute”

[24] IETF RFC 4277: “MEDs and Potatoes”

[25] GSMA PRD IR.88: “LTE Roaming Guidelines”

11 DOCUMENT MANAGEMENT

Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
0.01 - 1.0	22.2.2000	Initial drafts & first issue		
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	28.4.2000	Approved at Plenary 43. PL Doc 35/00		
3.1.0	5.9.2000	CR from GPRS Doc 51/00 incorporated GPRS DNS Usage Guidelines incorporated as annex A Approved at Plenary 44		
3.2.0	19.10.2001	SCR 003 to IR.34 Incorporated - Changes related to Quality of Service - SCR IR.34(v3.2.0)		
3.3.0	20.05.2002	CRs from IREG Doc 035/02Rev1, 036/02Rev1, 039/02 and 040/02 to IR.34 Incorporated		
3.4.0	28.01.2003	IREG#44 Docs 041/03, 016/03Rev1, 050/03 and 033/03 incorporated		
3.5.0	20.10.2003	IREG#45 Docs 013/03, 015/03, 016/03 and 017/03 incorporated		
3.5.1	07.01.2004	IREG Doc 46_011 incorporated		
3.5.2	August 2004	IREG Docs 047_012_rev2 and 047_018 incorporated		
3.6	February 2006	Packet Doc 025_006 incorporated		
3.7	April 2006	Removal of DNS specific information (which can now all be found in GSMA PRD IR.67). The references have also been updated.		
4.0	November 2006	Major Revision to include IPX information		
4.1	January 2007	Restructuring to improve readability for non-GSMA parties. New Architectural Description section. New GRX-IPX connectivity section and community attribute rules		
4.2	October 2007	Major Revision to QoS information and minor modifications to IPX proxy information.		
4.3	April 2008	Packet Doc 033_004 incorporated (Jitter requirements).		
4.4	June 2008	Packet Doc 035_013r1 incorporated (Extended BGP communities and Hot potato routing).		
4.5	December 2008	Packet Doc 037_005 and Packet Doc 037_025r1		

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
		incorporated (redefinition of delay table and IPX proxy requirements)		
4.6	March 2009	Packet Doc 038_005r1 incorporated (added more detailed information into IPX proxy requirements)		
4.7	May 2009	Packet Doc 039_017rev1 incorporated (change of that an IPX provider can adapt Traffic classes if agreed with SP) Packet Doc 039_014rev2 incorporated (clarifying terminology of BG)		
4.8	September 2009	Packet Doc 040_009 incorporated. Move out hostname and GPRS related test into IR.33	IREG Packet	
4.9	March 2010	Packet Doc 042_010rev5 incorporated. Introduce of PMIP based LTE roaming	IREG Packet	Itsuma Tanaka / NTT DOCOMO

Other Information

Type	Description
Document Owner	IREG
Editor / Company	Marko Onikki / TeliaSonera

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.

ANNEX A: KNOWN ISSUES AND SOLUTIONS

A.1 Double IP Backbone Provider problem

Service Providers using more than one IP Backbone Provider should carefully design their network advertisement strategy to avoid unwanted routing behaviors. When Service Providers having more than one IP Backbone Provider it is important that The Service Provider makes a decision how IP Backbone Provider networks are used to reach interworking partners and vice versa. If the originating network is using more than one Inter-Service Provider IP Backbone, participating Service Providers have two different routes to the originating network and unwanted routes could be selected to the destination network

Figure 11 shows example about asymmetric routing. In following case return packets could be blocked by Service Provider B FW if the FWs are not synchronized together.

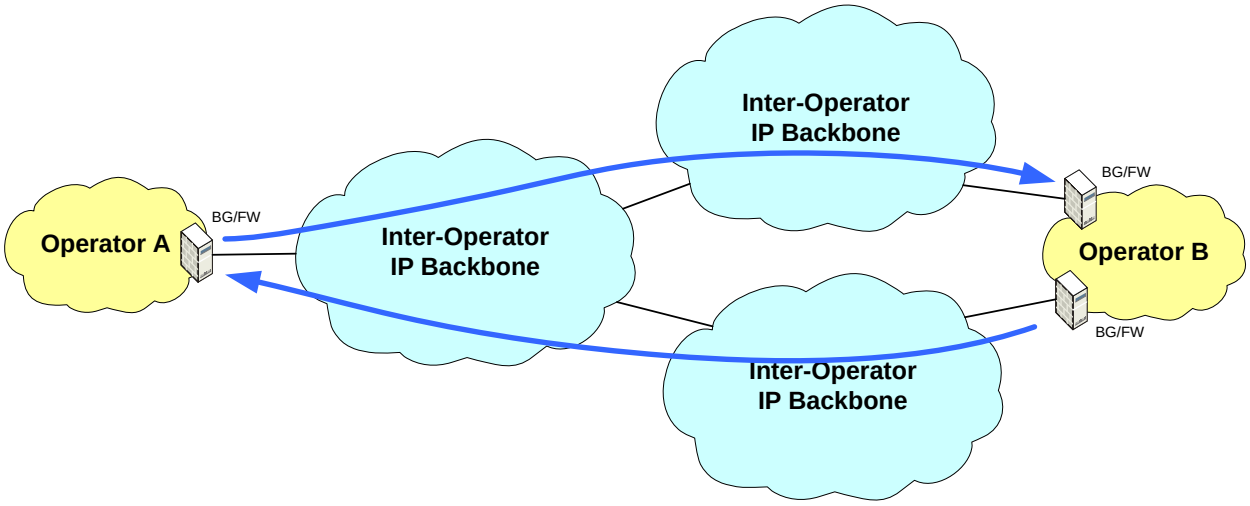

Figure 11 - Asymmetric routing

It is recommended that Service Providers agree with their own Inter-Service Provider IP Backbone Providers how backbone addresses are advertised to the IP Backbone Provider(s) of the participating Service Provider.

As shown in the figure asymmetrical routing causes FW (IP security device) problem on the Service Provider side since firewall state information of BG1 is typically not available on BG2. The packets will be dropped. Thus, the network design of the Service Provider is the source of the problem.Therefore, the Service Provider itself should implement such a network design within its network, which can avoid the "double Inter-Service Provider IP Backbone problem".

If the "double Inter-Service Provider IP Backbone problem" applies, Service Providers have two options:

A.1.1 Short term solution: Network configuration

The Service Provider can avoid asymmetrical routing by manipulation of the BGP protocol between Service Provider and Inter-Service Provider IP Backbone.

- Use of "local preference" to send all roaming traffic via one Inter-Service Provider IP Backbone.
- Use of "AS prepending" to qualify the different paths.

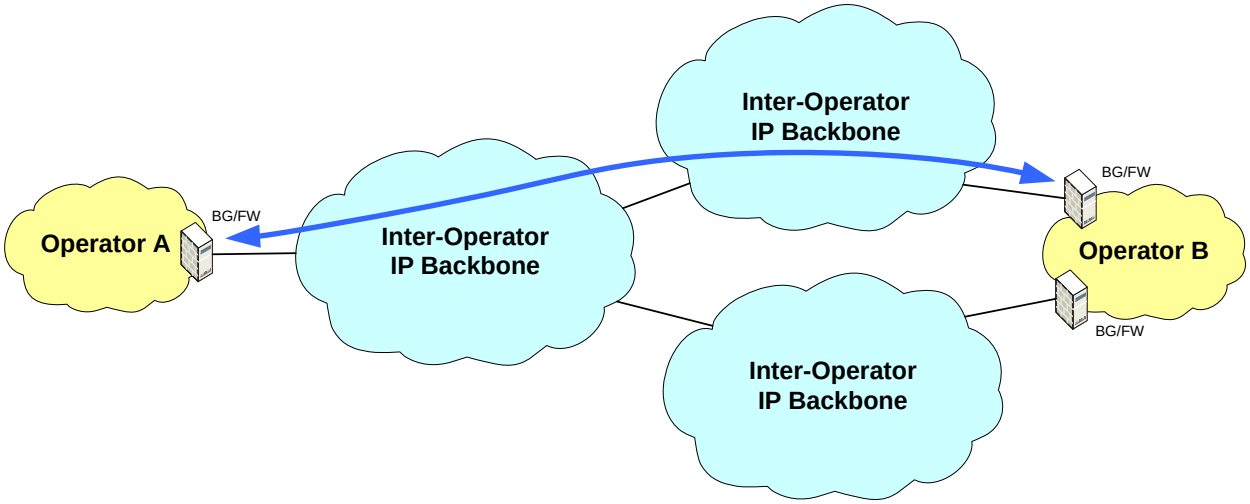

Figure 12 - Avoiding of asymmetric routing using network configuration

A.1.2Short-term solution disadvantages

- It is a "hot standby" solution. The IP traffic goes via the primary Inter-Service Provider IP Backbone only. Only in the case of failure of the primary Inter-Service Provider IP Backbone the traffic is routed via the other Inter-Service Provider IP Backbone.
- Avoids optimum path routing. That means, due to the BGP manipulation the selected path might not be the shortest one.
- Inter-Service Provider IP Backbone commercial problem. The not preferred Inter-Service Provider IP Backbone losses valuable traffic on the interface to the Service Provider. The traffic must be routed via the peering to another Inter-Service Provider IP Backbone.
- No scalability for the future. If the network of the Service Provider expands to more sites all the traffic must be routed towards the active BG.

A.1.3Long-term solution: Network design in Service Provider network

A more effective long-term solution allows asymmetrical routing without any FW problems.

- Separate security functionality (FW) from routing (BG) on the network border.

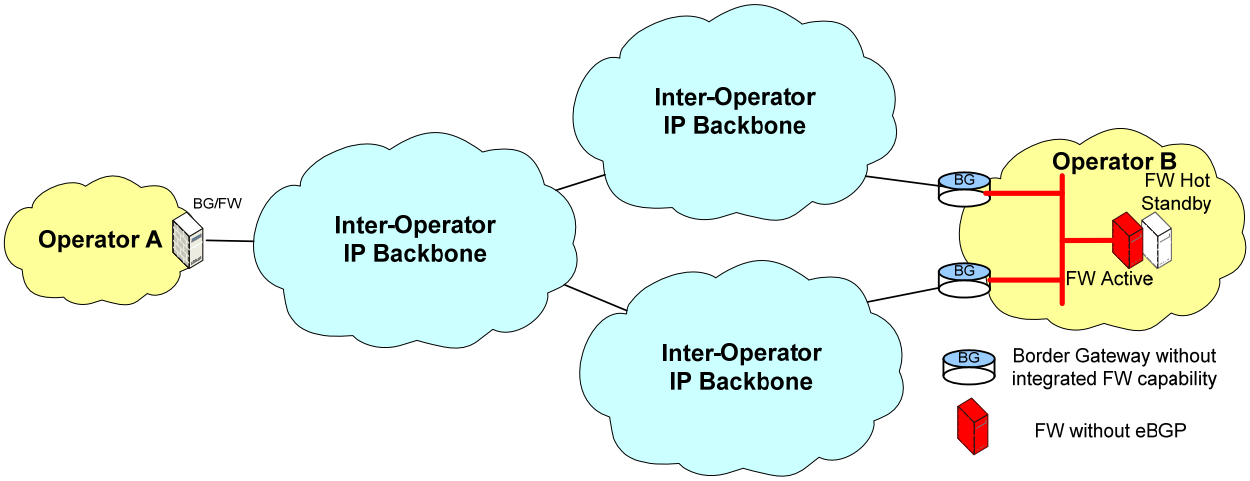

Figure 13 - Proposal for network design to overcome the "double Inter-Service Provider IP Backbone problem"

Since the FWs are located behind the both BGs the "double Inter-Service Provider IP Backbone problem" is solved. This network design allows unlimited future scalability if the network grows. The following figure shows a possible future network design. It shows an Service Provider network with different sites. Every site has its own IP range, which is routed in the backbone.

The Inter-Service Provider IP Backbone has QoS, the Service Providers need to define precise routing policy between Service Provider networks to account for this requirement

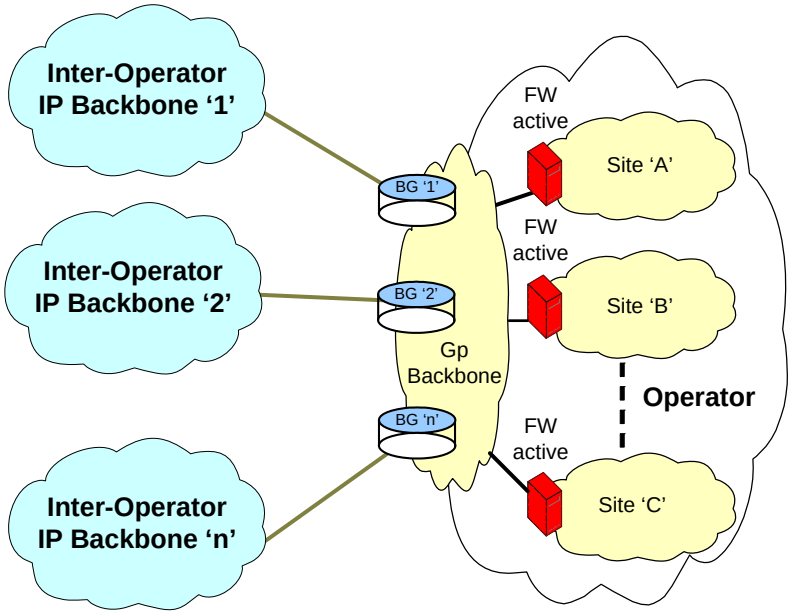

Figure 14 - Future network growth

To overcome the "double Inter-Service Provider IP Backbone problem", as an option, the following network design can be also considered. In this solution the security (FW) and the routing (BG) functionality is still integrated in one device or located nearby. This solution requires full-meshed Inter-Service Provider IP Backbone interconnection, which can be not cost efficient especially in the early stages. The Service Provider network IP ranges must be divided in two halves, e.g. "north" and "south".

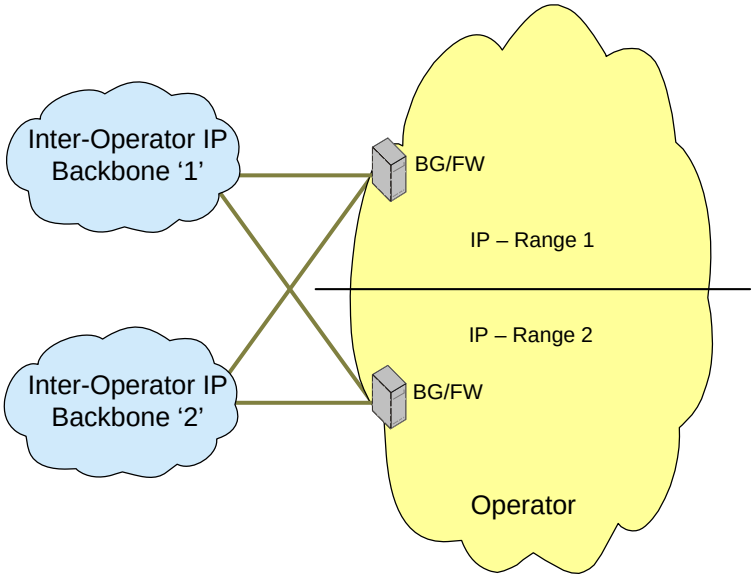

Figure 15 - Full-meshed Inter-Service Provider IP Backbone interconnection

The traffic routing must be based on the destination IP range for inbound traffic.

ANNEX B: IPX PROXY REQUIREMENTS

B1 INTRODUCTION

In implementing an IPX network, a number of functional requirements are placed upon an IPX Provider to support the correct operation of the IPX as a whole. As part of the commercial and technical agreement with a Service Provider, an IPX Provider may also be able to provide additional functions that relate to the operation of specific services, such as protocol interworking and transcoding. The term 'IPX Proxy' has been used throughout this document and in other documents to identify this complete set of functionality.
In this Annex, it is intended to identify requirements on the IPX Proxy and classify them in to one of two groups:

IPX Provider Requirements (identified as '**RI**' in the requirements sections below), which are those that IPX Providers are required to support for the correct operation of the whole IPX; and

Operational Requirements (identified as '**RO**' in the requirements sections below), which are those that may be implemented for specific applications and relate to support of specific Service Providers.

B2 REQUIREMENTS FOR IPX PROXY

B2.1 General

IPX Proxy Operational Requirements only apply for Bilateral and Multilateral interconnect models. Operational Requirements do not apply for the Transport interconnect model.

B.2.2.1IPX Provider Requirements

The set of IPX Provider Requirements described in this section provide functions for the overall support of the IPX. All IPX Provider Requirements shall be supported by all IPX Providers.

RI1. IPX Proxy shall be able to add, modify or remove fields/headers in the protocol in layer 5 and above. All additions, modifications or removals shall be agreed with the directly connected SP and IPX providers who are affected. No modifications to standard interworking/interconnection interfaces need to be done because of IPX Proxy.

RI2. IPX Proxy shall be able to handle inter-Service Provider traffic in a secured and controlled manner. More detailed requirements for the IPX Provider to achieve this are provided in section 6.5 of this document and in IR.77.

RI3. IPX Proxy shall support interconnection of interfaces required for the support of applications and services traversing the IPX.

RI4. It shall be possible to have an IPX Proxy-to-IPX Proxy connection.

RI5. IPX Proxy shall not require any major modification to enable a Service Provider to use a new service across the IPX network, where that service uses standard protocols that are already supported by the IPX Proxy.

RI6. The Control Plane shall always be routed via the IPX Proxy.

RI7. The User Plane may be routed via the IPX Proxy. Routing of the User Plane via the IPX Proxy shall be for the support of Operational Requirements (e.g. Transcoder insertion) as defined in section B.2.2.2 below.

RI8. IPX Proxy shall be able to relay traffic between terminals and servers that are using different addressing schemes. Therefore, IPX Proxy shall support functionality to allow this, such as NAT and PAT functionality, ALG or some other mechanism.

RI9. IPX Proxy shall verify that the source address of packets received from the Service Providers directly connected to it are associated with and registered to those Service Providers.

RI10. IPX Proxy shall have knowledge of the service specific capabilities of the Service Provider that it is serving for a specific session, and ensure media is appropriately handled for that session.

RI11. IPX Proxy shall be able to be used by a Service Provider as the point of connectivity for multiple destination Service Providers, without the need for the Service Provider to modify traffic based on destination Service Provider capabilities and connection options.

RI12. IPX Proxy should be able to verify that the next application level hop is reachable.

RI13. IPX Proxy shall have dedicated interface(s) towards an external management system for O&M purposes.

RI14. IPX Proxy shall have reporting capabilities, regarding IPX Proxy performance, and shall be able to provide reports to the Network Management system.

RI15. IPX Proxy shall support the requirements for availability of services as specified in AA.80 service schedules.

RI16. IPX Proxy shall be able to support single-ended loopback testing, in order to enable a Service Provider to test the IPX Proxy without involving another Service Provider.

RI17. IPX Proxy shall support QoS functions as described in Chapter 8 of this document.

RI18. IPX Proxy shall be able to support legal interception requirements, in compliance with national laws as well as international rules and obligations.

RI19. IPX Proxy shall be able to support dedicated interface(s) towards the billing system.

RI20. IPX Proxy shall support SIP error codes as specified by IETF & 3GPP.

RI21. IPX Proxy shall forward unknown SIP methods, headers, and parameters towards the recipient without modification.

This is to allow support of new SIP extensions. However, IPX Proxy should log and report when such unknown elements are detected, in case this is used for malicious purposes.

RI22. Addresses used in the underlying IPX network layer for IPX Proxy shall comply with requirements in IR.40 and IR.77. Such addresses include those for tunnel endpoints.

RI23. Where two interconnecting Service Providers are using the same IP version, the IPX Proxy shall not alter the IP version used.

RI24. Where two interconnecting Service Providers are using different IP versions, the IPX Proxy to IPX Proxy interface should be IPv6.

RI25. IPX Proxy shall not modify IPv6-based IP addresses in the user plane (if no IPv4 related conversion is needed).

RI26. IPX Proxy shall accept from Service Providers and other IPX Proxies traffic that originates from and terminates to servers (server-to-server traffic) either within a tunnel or un-tunneled.

RI27. IPX Proxy shall accept from Service Providers and other IPX Proxies traffic that originates from and terminates to end users (user-to-user traffic) and traffic that originates from end users and terminates to servers or vice versa (user-to-server and server-to-user traffic) only if it is transported within a tunnel.

RI28. IPX Proxy shall not adversely affect QoS KPI parameters to end-to-end connections compared to when there is no IPX Proxy.

RI29. IPX Proxy shall be able to relay the ToS (Type of Service) field of the IP header from source to destination unmodified. If the IPX Proxy inserts an Interworking function that requires the ToS field of the IP header to be modified, then the IPX Proxy shall modify the ToS field accordingly.

RI30. IPX Proxy shall block user plane traffic not related to ongoing control plane sessions.

RI31. IPX Proxy shall be able to apply session admission control based on session capacity and rate, on a per Service Provider basis. IPX Proxy shall generate alarms when the capacity or rate limit for a specific Service Provider is exceeded.

RI32. The IPX proxy shall be capable to interact with a Service Provider's black/white lists, so that the IPX Proxy is able to implement admission control of sessions from those Service Providers.

> Note: the black/white lists are provided by the Service Provider to the IPX Provider. How this is done is out of scope of the current PRD.

R33. IPX Proxy shall be able to support DiffServ packet queuing on interfaces where contention of multiple input interfaces to a single outgoing interface occurs.

RI34. IPX Proxy shall be able to generate Inter-Service Provider charging data based on the GSM Association charging principles as defined in GSMA PRD BA.27.

RI35. IPX Proxy shall be able to produce Inter-Service Provider charging data based on events detected in the User Plane and Control Plane.

RI36. IPX Proxy shall be able to produce application specific charging data reflecting the occurrence of Chargeable Events identified in Service Schedules for that application.

RI37. IPX Proxy shall support required CDR formats to report Chargeable events to external billing systems.

B.2.2.2 Operational Requirements

The set of Operational Requirements described in this section provide functions that could be hosted either by the Service Provider within their own networked implementation, or could be effectively 'outsourced' to the IPX Provider, for the IPX Provider to operate on behalf of the Service Provider. The decision on whether these functions are kept within the Service Provider's network or are operated on their behalf by the IPX Provider will be made bilaterally between an individual Service Provider and their IPX Provider, on a service by service basis.

Where such requirements and functions are operated by the IPX Provider, the IPX Provider shall implement these functions in a way that is 'transparent' to other Service Providers. In this case, transparent implies that a Service Provider B that is connecting to Service Provider A must be unaware at Layer 3, of whether the functions described in this section are implemented within Service Provider A's network or within their IPX Provider's network, as identified by requirements defined in IR.40 and IR.77.

All requirements described in the remainder of this section shall maintain this concept of transparency in their implementation.

RO1. IPX Proxy shall have DNS and ENUM resolver capability.

RO2. IPX Proxy shall be able to provide transcoding, when needed.

RO3. IPX Providers can offer support of interworking functionality between different control plane protocols to Service Providers. If Service Providers require the support of this functionality, it shall be provided transparently as an IPX Proxy function.

RO4. IPX Providers can offer support of interworking functionality between different user plane protocols to Service Providers. If Service Providers require the support of this functionality, it shall be provided transparently as an IPX Proxy function.

RO5. IPX Proxy shall be able to support 3GPP standards compliant interfaces relevant to interconnect functions for IMS-based services connectivity

RO6. IPX Proxy shall be able to relay traffic between terminals that are located in different networks and use overlapping private IPv4 addresses.

RO7. IPX Proxy shall be able to store routing information, regarding the IP address/port pair used for a particular media stream between two Service Providers. This information is required to allow the IPX Proxy to open and close pinholes for the media streams associated with a signaling exchange.

RO8. IPX Proxy shall support all transport protocols required for the services to be interconnected using that IPX Proxy.

RO9. IPX Proxy shall support ENUM resolution.

RO10. IPX Proxy shall support opening pinholes for user plane traffic traversal based on control plane protocol information.

RO11. IPX Proxy shall support closing pinholes used by user plane traffic based on control plane protocol information.

RO12. IPX Proxy may support the ability to provide maximum admission control limits on a per domain basis.

RO13. IPX Proxy shall be able to apply policy-based functionality on a per application and service provider basis.

RO14. IPX Proxy shall be able to support user plane policing based on the data rate.