Guidelines for IPX Provider networks (Previously Inter-Service Provider IP Backbone Guidelines)

Version 19.0

11 June 2024

Security Classification: Non-Confidential

Copyright Notice

Disclaimer

Compliance Notice

The information contain herein is in full compliance with the GSMA Antitrust Compliance Policy.

This Permanent Reference Document is classified by GSMA as an Industry Specification, as such it has been developed and is maintained by GSMA in accordance with the provisions set out GSMA AA.35 - Procedures for Industry Specifications.

Table of Contents

1 Introduction

1.1 Overview

1.1.1 Purpose

The internet Protocol (IP) Packet eXchange (IPX) Network is an inter-Service Provider IP backbone which comprises the interconnected networks of IPX Providers and General Packet Radio Service (GPRS) Roaming eXchange (GRX) Providers.

The IPX network supports multiple IPX services. The purpose of this document is to provide guidelines and technical information on how these networks are set-up and interconnect, and how Service Providers will connect to the IPX Provider networks. The services supported on IPX are out of scope for this document and are currently listed in GSMA Permanent Reference Document (PRD) AA.51. An IPX service is a service that requires the IPX network for either isolation from the Internet and/or for quality of service and experience. See GSMA PRD AA.51 [27] for a list of IPX Services.

Contrary to previous versions of IR.34, GRX is now considered an IPX service which is offered on an IPX Network. The term GRX network is no longer used; however, an entity which only offers the GRX service may refer to itself as a GRX Provider.

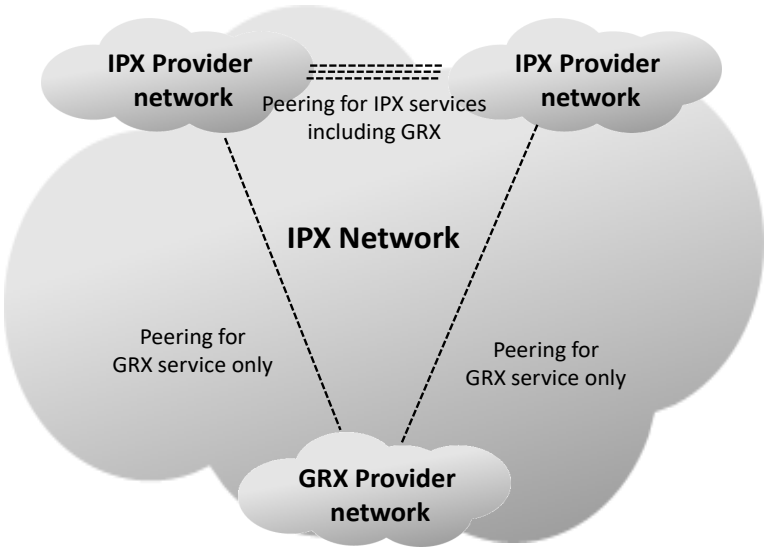

Figure 1: IPX Network comprising interconnected networks of GRX and IPX providers

The IP Packet eXchange (IPX) is thus a model which encompasses commercial, technical and operational requirements. The implementation of this model consists of a number of interconnected IP networks operated and managed by International Carriers and domestic Providers (IPX Providers) which compete for interconnecting Service Providers according to mutually beneficial business models.

From a network perspective IPX is a global, private, multiservice, secure IP network, open to any Service Provider under a contractual agreement which supports end-to-end quality of

service. From a commercial perspective, it supports the principle of cascading interconnect payments (when it applies),

In order to provide these features, the IPX can be service aware, unlike the Internet and the GPRS Roaming eXchange (GRX) network.

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

1.1.2 Background

The IPX Network was originally conceived as an inter-Service Provider IP backbone created to carry GTP-tunnels (GPRS Tunnelling Protocol) via the Gp interface between the GPRS Support Nodes (GSNs) in different GSM Operators that is, 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, Multimedia Messaging Service (MMS) interworking and Wireless Local Area Network (WLAN) authentication data roaming were added as supported services. This original inter-Service Provider IP backbone is in fact an Inter-PLMN (Public Land Mobile Network) IP Backbone and was termed the GRX. The GRX model is used to interconnect hundreds of networks and has proven highly successful.

With the subsequent development of IP-based services assisted by the spread of mobile and fixed broadband technologies, 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 network is called the IPX network 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 service awareness facilitates interconnect, cascaded billing and multi-lateral interconnect agreements.

1.1.3 About this Document

The document provides a brief introduction to the requirements for IP interworking and the IPX network.

The technical architectures of the IPX network 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 IPX Network and on the requirements for IPX proxies.

1.2 Scope

1.2.1 In Scope

- IPX Network: an inter-Service Provider IP backbone network architecture which connects Mobile Network Operators (MNOs), Fixed Network Operators (FNOs) Internet Service Providers (ISPs), Application Service Providers (ASPs), On-Line Service Providers (OSPs) etc., from here on in referred to collectively as "Service Providers". Where there is specific reference to a 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 but are further defined in GSMA PRD IR.67 [17].

1.2.2 Out of Scope

- IP addressing and host names of GPRS user plane (that is, mobile stations) and service elements (for example, Wireless Application Protocol (WAP) Gateway) located beyond the Gi reference point. See IR.40 [26] for further information.
- Both host name and domain name usage and recommendations are also outside the scope of this document, and are specified in GSMA PRD IR.67 [17].
- The Signalling System Number 7 (SS7) signalling network for Mobile Switching Centre / Visitor Location Register (MSC/VLR), Home Location Register (HLR) and other register access and Short Message Service (SMS) are not within the scope of this document, though SIGnaling TRANsport (SIGTRAN) can be within scope.
- Direct connectivity among Service Providers by leased line, Virtual Private Network (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.

1.2 Definition of Terms

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

Term	Description
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 (that is, BGF).

BGP	Border Gateway Protocol (BGP) is an inter-Autonomous System routing protocol [6]. The current version of BGP is BGP-4.
Black-list	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 the ingress point of the IPX Network to the egress point of the IPX Network. Thus, Service Provider core and access networks are excluded.
EPS	Evolved Packet System (Core) = Evolved-UTRAN +plus Evolved Packet 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 Service. An IPX service which provides for routing, interconnecting and some additional services, such as Domain Name System (DNS). Generally used for GPRS/UMTS/LTE roaming, MMS interworking and WLAN roaming.
GRX Provider	An IPX Provider that offers GRX service only.
GTP	GPRS Tunnelling Protocol [7].
Interconnection	The connection of Service Providers in order to exchange traffic between them.
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 is a telecommunications interconnection model for the exchange of IP based services between customers of separate mobile and fixed operators as well as other types of service provider (such as ISP), via IP based network-to-network interface, the IPX network. In the interconnection context, IPX is used to mean an interconnection at the service level (not at the network level). Also refers to all the IPX services and the network supporting those services.
IPX Network	Inter-Service Provider IP backbone which comprises the interconnected networks of various IPX Providers.
IPX Provider	A Provider that offers IPX services.
LTE	Long Term Evolution (Radio)
MMS	Multimedia Messaging Service
MNO-G	This Service Provider is a GPRS/UMTS/LTE Mobile Network Operator that connects to the IPX network ONLY for the GRX Service. The services that these Service Providers offer 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 that connects to the IPX network for any type of IPX Service.
NGNO	This Service Provider connects the IPX network for any service except the GRX Service. It 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

Proxy(ies)	Proxy is used to describe an IPX element that supports service awareness and interworking. Proxies facilitate a multi-lateral model for each service.
QCI	The QoS Class Identifier is scalar that is used as a reference to node specific parameters that control packet forwarding treatment (for example scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, and so on.) and that have been pre-configured by the operator owning the node (for example eNodeB)
Roaming	The ability for a user to function in a serving network different from the home network.
SEPP	Security Edge Protection Proxy
Single-root ENUM	An ENUM model with a unique global root database at the top of the hierarchy.
SCTP	Stream Control Transmission Protocol
Service Community	A group of Service Providers connected to the same service, and isolated (physically or logically) from other Service Communities. The GRX can be thought of as a Service Community, as can each service enabled by the IPX (for example. Packet Voice).
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
UPF	User Plane Function
White-list	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. That is, 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. That is, 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].

1.3 Document Cross-References

Ref	Document Number	Title
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 Tunnelling 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	3GPP TS 29.165	“Inter-IMS Network to Network Interface (NNI)”
15	IETF RFC 3246	"An Expedited Forwarding PHP"
16	IETF RFC 2597	"Assured Forwarding PHB Group"
17	GSMA PRD IR.67	"DNS Guidelines for Service Providers and GRX and 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 and 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”
26	GSMA PRD IR.40	"Guidelines for IP Addressing and AS Numbering for GRX/IPX Network Infrastructure and User Terminals"
27	GSMA PRD AA.51	“IPX Definition and Releases”
28	3GPP TS 23.203	"Policy and charging control architecture"
30	GSMA PRD	“Interworking Charging Principles”
31	GSMA PRD NG.105	“ENUM Guidelines for Service Providers and IPX Providers”
32	GSMA PRD IR.61	“Wi-Fi Roaming Guidelines”

33	IETF RFC 3393	IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)
34	3GPP TS 29.162	“Interworking between the IM CN subsystem and IP networks”
35	GSMA PRD IR.95	SIP-SDP Inter-IMS NNI Profile
36	GSMA PRD IR.90	RCS Interworking Guidelines
37	3GPP TS23.501	“System architecture for the 5G System (5GS); Stage 2”
38	3GPP TS23.503	Policy and charging control framework for the 5G System (5GS)

2 The Need for IP Interconnect

2.1 General

Following the widespread deployment of packet infrastructures using the GSM, UMTS and LTE air interfaces and other access networks, Mobile Network Operators 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 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.

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 IPX connection via IPX Providers (or GRX Providers if only for the GRX Service), or
- Direct connection between two Service Providers using leased lines, Internet using Internet Protocol Security (IPSec), or VPN connectivity.

Direct Connectivity between Service Providers is out of scope for this document.

It is a commercial decision which method Service Providers choose. The benefits of connectivity via 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 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.

2.2 IPX

IPX is able to support the following:

- Legacy GRX Service (connectivity between MNO-G and MNO-I Service Providers but without end-to-end Service Level Agreement (SLA)), including MMS interworking and WLAN (authentication) data roaming, as well as diagnostic protocols, for example ICMP (Ping).
- 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 functionalities to support:

- Further interconnect charging models such as service-based charging (including support of cascaded billing) 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.

For clarity:

- An IPX provider is under no obligation to offer all conceivable IPX services. IPX Providers offering only GRX may call themselves GRX Provider.
- In order to guarantee security, interconnection between Service Providers (other than bilateral) is established per IPX Service Community rather than across all IPX services; see sections 3.5 and 4.4.
- The list of “IPX services” is maintained through a release management cycle described in GSMA PRD AA.51.

3 IPX Network Architecture

The purpose of the IPX Network is to facilitate interconnection between Service Providers according to agreed inter-operable service definitions and commercial agreements.

The model used for the IPX Network 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 an IPX Provider to be able to interconnect with selected Service Provider partners. If redundancy is required, two or more physical connections to one or more IPX Providers may be used. (See Annex A for problems and solutions to this approach). Service Providers obtain connections to IPX Network nodes locally from an IPX Provider or from other Providers (for example, leased lines).

In this document, the physical connection between the IPX Provider and a Service Provider is termed a “local tail”.

3.1 IPX Network Connection

Service Providers are connected to their selected IPX 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.

3.2 IPX Architecture

The IPX is formed from separate and competing IPX Providers. An IPX network can be operated by any qualified party.

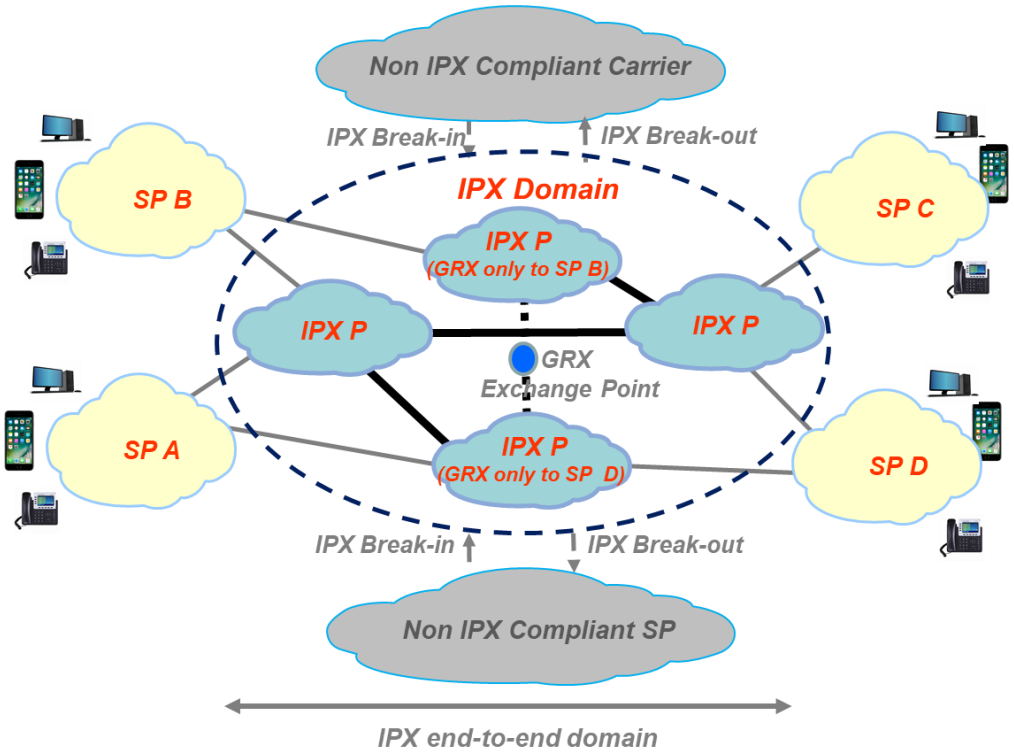

Figure 2: IPX Model

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 GRX service is an exception as this service is offered on IPX on best-effort basis.

The IPX also introduces service awareness and 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 E.164 NUmber Mapping (ENUM, NG.105 [31]) capability.

In the IPX, all user traffic, (that is, User Equipment (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.

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

3.3 IPX Connectivity Options

This section should be read in conjunction with GSMA PRD AA.80 [22]. The IPX is defined to have three connectivity options, detailed in the following sub-sections.

3.3.1 IPX Transport

A bilateral agreement between two Service Providers using the IPX transport layer with guaranteed QoS end-to-end. As with the GRX, this Connectivity Option 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).

3.3.2 IPX Service Transit

A bilateral agreement between two Service Providers using an IPX Proxy functions and the IPX transport layer with guaranteed QoS end-to-end.

Note: This Connectivity Option provides the opportunity to include service-based interconnect charging instead of, or in addition to, the transport charging. For more information on charging, see [28] and [38].

The details of this Connectivity Option are described in other PRDs. The list of those PRDs can be found in GSMA PRD AA.51.

3.3.3 IP Service Hub

A Connectivity Option 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 an IPX Proxy.

3.4 IPX Proxy Services

Interworking between Service Providers can be established without IPX Proxy services when using the IPX Transport Connectivity Option. However IPX Proxy services are required to support the IPX Service Transit and IPX Service Hub Connectivity Options (as defined in sections 3.3.2 and 3.3.3, respectively), where they facilitate a Service Provider’s configuration and agreement management and the cascading of charging.

NOTE: It is an implementation issue as to how the different services offered by an IPX Proxy are implemented, including whether they are implemented in separate physical entities or combined into one.

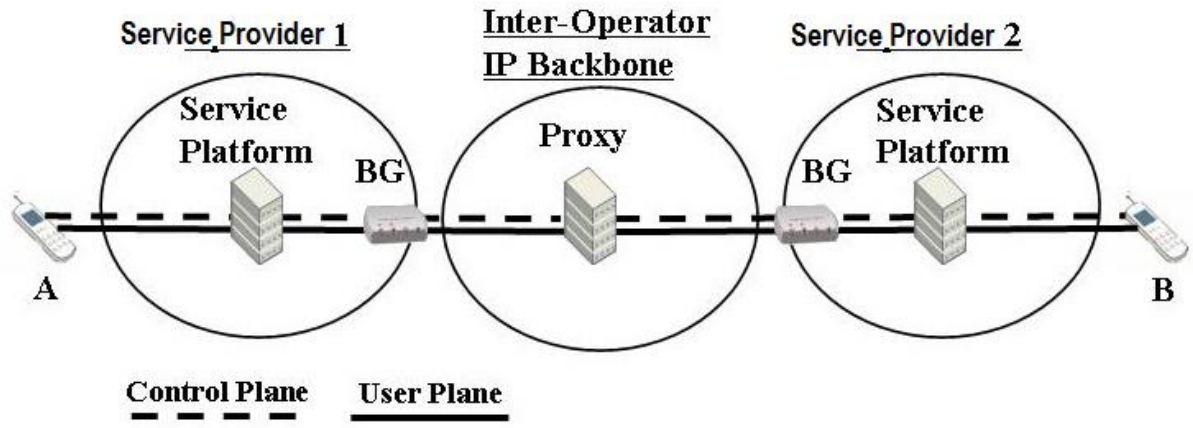

Figure 3: IPX Proxy in Inter-Service Provider IP Backbone

Error! Reference source not found. above shows the high-level architecture of bilateral Service Provider traffic traversing the IPX Proxy element within the Inter-Service Provider IP Backbone network using any type of IP based traffic. The user plane may or may not go through the IPX Proxy depending on each service requirement.

3.5 Types of Service Provider and Interconnectivity Allowed

The IPX Network supports various Service Communities currently listed in GSMA PRD AA.51 [27].

When connected to the IPX Network, a Service Provider is only connected to the Service Communities of its choice and thus only to Service Providers connected to the same Service Communities.

Isolation between Service Communities on an IPX Network can be logical (for example by VPNs on an IPX Network) or physical (that is, when the Service Provider connects to separate IPX Networks, for example for GRX and an IPX Service).

Implicitly, this ensures that only Service Providers that are GPRS/UMTS/LTE network operators connect to the GRX, since this Service Community does not offer any services that are of interest to other types of Service Providers.

4 Requirements of the IPX Networks

4.1 General

IPX Providers shall:

- Support connections from Service Providers as described in section 5.3.
- Comply with IP addressing guidelines for Inter-Service Provider IP Backbone in GSMA PRD IR.40 [26].
- Comply with DNS guidelines as specified in GSMA PRD IR.67 [17].
- Comply with ENUM guidelines as specified in GSMA PRD NG.105 [31]
- Offer DNS root service for contracted Service Providers.
- Have BGP-4 routing capability.

- Per Service Community: distribute all (valid) known routes to Service Providers.
- Control which routes a Service Provider can advertise to a Service Community.
- Offer interconnectivity to other IPXs (IPX peering).
- Comply with Service Level Agreements.
- Conform with security requirements laid out in GSMA PRD IR.77 [19]
- Maintain user traffic separation as described in 4.6.6.
- For session based services, comply with the IPX Proxy requirements in annex B.2.

Furthermore, with the exception of the GRX service, 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 fulfil the end-to-end SLA.

4.2 Separation of IPX Services on IPX Networks

IPX Providers shall maintain isolation between different IPX Services on their IPX Networks. This isolation can be logical or physical.

For example, logical separation could be achieved by the use of VPNs on an IPX Network).

Physical separation could be based on the use of separate underlying L1/L2/L3 network infrastructure for different IPX services; e.g. one physical network for IPX Transport (Data Roaming/GRX) service and another physical network for another IPX service.

Additionally, a Service Provider may connect to separate physical IPX Networks for different IPX services. For example, IPX Provider A for an IPX transport service (Data Roaming/GRX) and IPX Provider B for another IPX Service).

4.3 Number of IPX Providers used to Transit Packets between Service Providers

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

An exception is allowed in the IPX Service Hub connectivity option (as defined in section 3.3.3) when using the following "Packet Voice Interconnect" (PVI – as defined in AA.80 [22]) related protocols:

- Session Initiation Protocol (3GPP TS 29.165 [14])
- Session Initiation Protocol (3GPP TS 29.162 [34])
- Session Initiation Protocol with encapsulated ISUP (SIP-I)
- Real-time Transport Protocol (RTP)/ RTP Control Protocol (RTCP) (that is associated with the SIP-I signalling)

It is IPX Proxy implementation dependent as to how the above is achieved, whilst still maintaining the basic requirement for other IP data flows. However, this could be achieved by implementing specific physical equipment for the PVI service, and/or by inspection of IP packets related to the above stated protocols.

However, an IPX Provider should minimise, as far as practically possible, the number of other IPX Providers needed to transit a voice service related protocol packet to/from their Service

Providers to/from another Service Provider. It is recommended that such packet ideally pass through no more than two IPX Providers (as this minimises efforts in tracing problems).

Regardless of the number of IPX Providers used to transit a packet, all of the requirements in section 4.1 must be maintained for all packets.

4.4 Connections between IPX Provider and Service Provider

When connected to the IPX Network, a Service Provider is only connected to the Service Communities of its choice and thus only to Service Providers connected to the same Service Communities.

4.5 IPX Provider Peering Interface

Connections between IPX Providers are implemented and managed by the IPX Providers themselves based on bi-lateral Service Level Agreements (SLAs). The end-to-end QoS SLA (QoS SLA 15) sets out a minimum set of QoS requirements which shall be followed by the IPX Providers within the IPX Network.

The connectivity options between IPX Service Providers are either:

- Private bilateral connection, or
- Common IPX Network peering point (such as AMS-IX and Equinix).

For PVI/multimedia and signalling, IPX providers should use either private bilateral connections or, if a common peering VLAN is used (more than two providers), then IPsec tunnels are mandated.

In order to maintain isolation between IPX Services, where Inter Service Provider backbone networks are interconnected, separate VLANs and separate routing tables must be used for each service.

Every IPX Provider can peer with one or more other IPX Providers in the areas in which they operate, through direct connection or peering points. 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.

Error! Reference source not found. below shows the IPX Network peering arrangement for a mixture of IPX Providers and Service Providers.

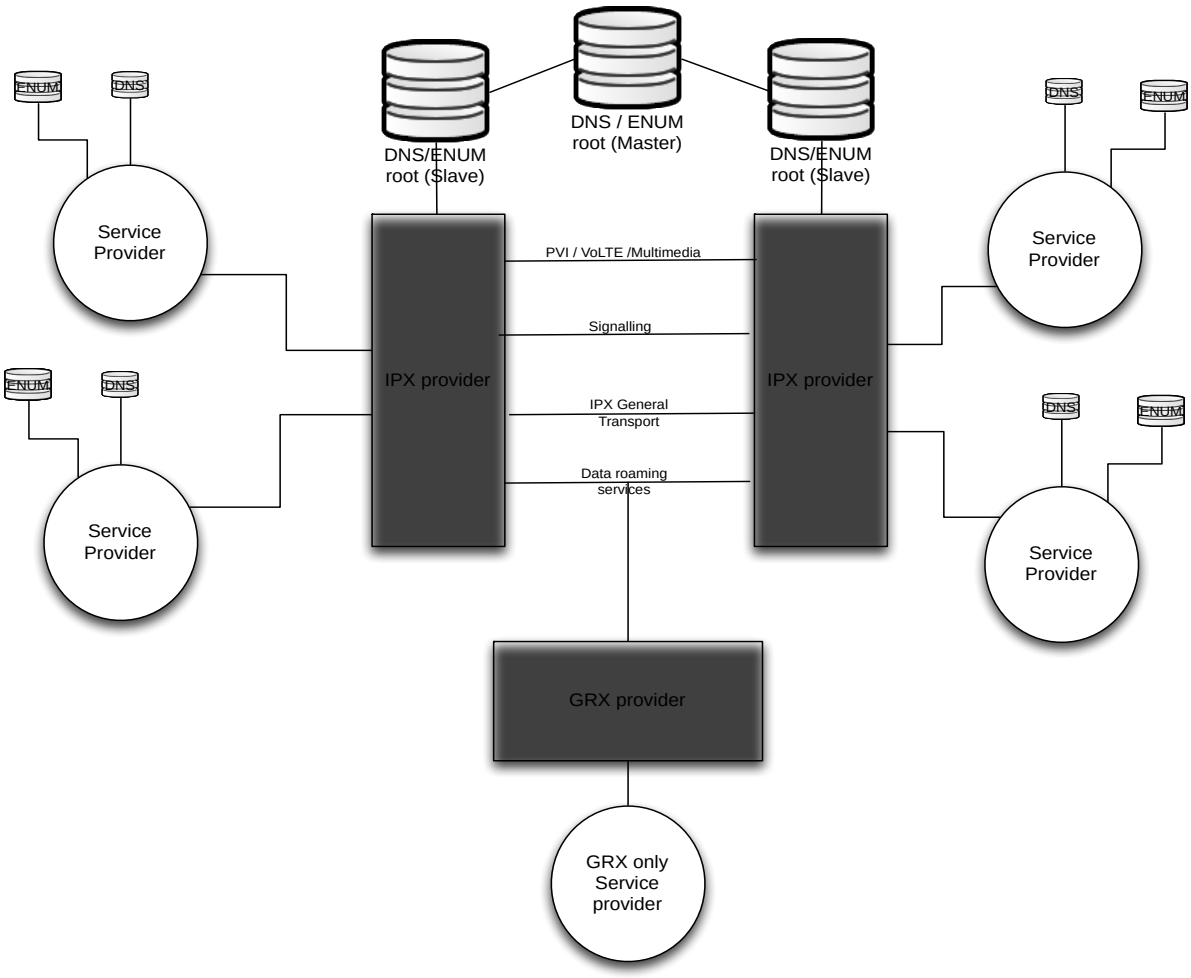

Figure 4: Peering between IPX Provider Networks

IPX Providers shall ensure that all traffic classes meet their agreed QoS values described in section 6 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 Provider peering point requires the functionality to support media traffic classes between IPX Providers in an unbroken stream, in such a way that peering point will not become a bottleneck for the overall IPX Network.

In addition, as indicated in figure 2, it is recommended that IPX Providers allow traffic break-in/break-out of the IPX Network via legacy networks, e.g. TDM, other IP Networks etc. It is recognised that though the IP migration process is in progress throughout the industry, many destinations will remain reachable for some considerable time only via TDM and/or non IPX compliant IP connections. Not allowing TDM and IP break-in / break-out traffic would exclude many destinations from a direct communication via the IPX domain. Therefore, Service Providers would have to keep costly TDM interconnects operational in parallel to IPX-based interconnects in order to have access to and to receive calls from those Service Providers. The

support of legacy NNIs enables a faster deployment of IPX services as it breaks the dependency on all Service Provider networks migrating to IP at the same time.

4.6 Technical Specification of the IPX Network

4.6.1 IP Routing

The IPX Networks shall carry routing information to all parties within the connectivity agreements. Dynamic exchange of routing information between different networks shall be accomplished using BGP-4 routing protocol.

Dynamic routing reduces the amount of management work in the event of a change of IP address (that is, new address ranges are applied). In addition, dynamic routing supports redundant connections to IPX Providers.

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

The Service Provider and the IPX Provider are both responsible for checking that all connected Service Provider and IPX Networks are invisible to and inaccessible from the public Internet.

In an IPX Provider environment with multiple peering points, it is recommended that “Hot Potato” [24] routing (where traffic is exchanged with the next IPX Provider at the nearest peering point in terms of delay) should be used. However, “Cold Potato” routing (where traffic is exchanged with the next IPX Provider at the furthest peering point in terms of delay) may be agreed bilaterally between IPX Providers. It is recognised that for session based services, other factors could also be considered when selecting the peering point, e.g. Least Cost Routing, price considerations etc.).

IPX Providers shall not restrict protocols carried between Service Providers unless those protocols are non-compliant with the requirements set out in the IR.77 [19] or the protocols are not appropriate on the current service VLAN; example: GTP traffic on the Diameter service VLAN.

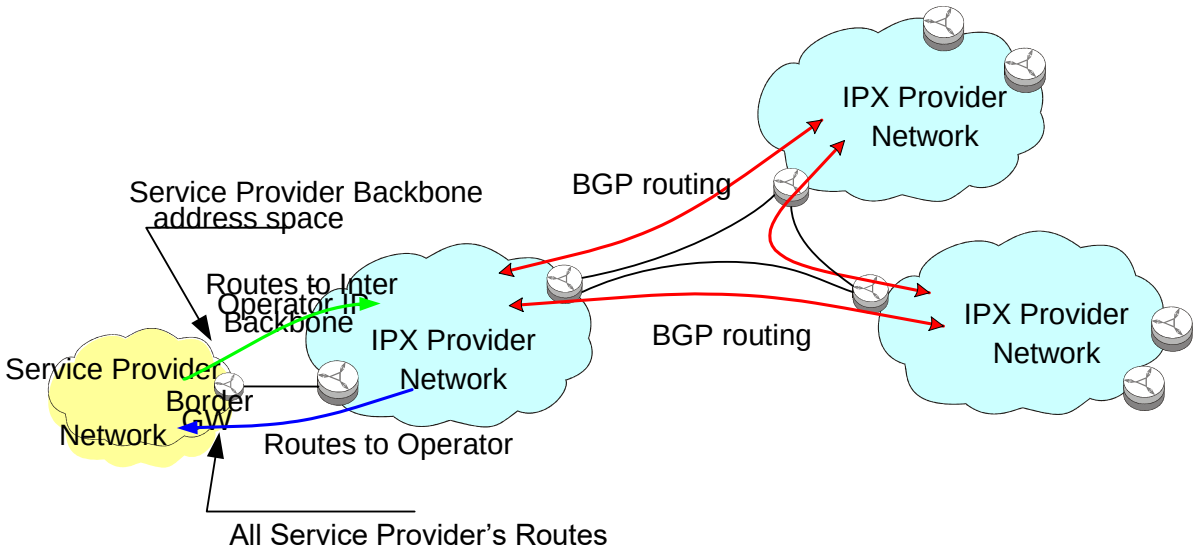

Figure 5: Dynamic routing IPX Network

4.6.2 BGP-4 Advertisement Rules

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

4.6.3 IPX Service to VLAN/VPN Mapping and Advertisement

The GRX is an environment which is exclusively for MNO use for the purpose of 2G/3G/4G/5G Data Roaming, whereas the IPX also involves other kinds of Service Providers and services. Therefore, there is a need to interwork these two environments in a manner which avoids unnecessary complexity.

As a result of this interworking requirement, while also maintaining good architectural & security practices, there is a need to segregate different types of IPX services (including GRX) so that different types of operators only have reachability and access to IPX services and associated service platforms to which they subscribe.

The simplest and most secure approach to achieve this is to separate the different IPX services and associated components into different connectivity domains which do not have IP reachability between them.

As such, this segregation of different IPX services is maintained through the use of multiple different VLANs at IPX Interconnection points (either IPX peering points or private bilateral IPX peering) and Virtual Private Networks (of some form) within IPX providers. Service platforms and endpoints associated with one IPX service must not be routed via the VLANs or VPNs of a different IPX service.

The use of separate IP address range assignments and advertisements for each IPX service & service platforms is mandatory except in cases where a service is common to more than one VLAN or VPN. This applies both to IPX providers and to Mobile and Fixed Operators using the IPX services.

As a result, IPX services must be clearly defined and grouped into a small set of VLANs/VPNs to ensure segregation is maintained and that the model is easily understood.

The mapping of IPX services to IPX VLANs/VPNs is shown in the table below.

IPX VLAN/VPN	IPX Service (s)	Notes
Data Roaming	2G/3G/4G/5G Mobile Data Roaming (Gp, S8, N9) and DNS) VoLTE Roaming (S8HR) Wi-Fi Roaming (see GSMA PRD IR.61 [32]) MMS	An IPX Transport service, not 'service aware'
Signalling	SIGTRAN & Diameter	May contain messaging hubbing platforms Includes legacy SMS
5G Control Roaming	5G SA control plane (N32)	
Packet Voice & Video (multimedia) services RCS Messaging Services	SIP/IMS VoLTE/ViLTE Interconnect SMSoIP Legacy SIP VoIP RCS Messaging	SIP/IMS Signalling & RTP Media traffic, ENUM Non IMS SIP Signalling & Media SIP/IMS Signalling & MSRP Media Traffic, ENUM
IPX General Transport	Non-service-aware general purpose connectivity for bilateral requirements	General purpose connectivity for transporting traffic of bi-lateral agreements between Operators

Table 1: Mapping of IPX services to IPX VLANs/VPNs

See GSMA PRD AA.51 [27] for the definitions of IPX services

The table below details which platforms from Operators and IPX providers are reachable within each IPX VLAN/VPN. Platforms should not be reachable through the incorrect VLAN/VPN. IP address ranges associated with the platforms should not be advertised into or through the incorrect VLAN/VPN.

IPX VLAN/VPN	Operators service platforms	IPX provider service platforms
Data Roaming	SGSNs, GGSNs, S-GW, P-GW, Data Roaming (GRX) DNS secondary, UPF	Connectivity to root Data Roaming (GRX) DNS, Roaming GW (e.g. Wi-Fi to Mobile Data)
Signalling	STPs/SGWs, DEAs	STPs/SGWs, DRAs, VAS platforms
5G Control Roaming	SEPPs	SEPPs (Note 1)
Packet Voice & Video (multimedia) Services RCS Messaging Services	IMS Signalling Gateways (IBCF, ATCF), Media Gateway (TrGW), ENUM Tier2	IMS Proxies, ENUM VAS platform (hosted tier 1 or tier 2), connectivity to Root ENUM (tier 0)
IPX General Transport	Anything which is not part of one of the other services above	None

Table 2: Platforms reachable within each IPX VLAN/VPN

Note1: SEPP could be Hosted or Hubbing solution

4.6.3.1 Differentiating between Service Providers

IPX Providers shall separate different kind of Service Providers, service types and geographical locations using VLANs.

Compliance with these rules is mandatory for IPX Providers but is not mandatory for a GRX Provider. GRX Providers may decide if they want to follow the guidance or not.

Marking is recommended to be performed by the originating IPX Provider, except where the originating IPX Provider is a GRX Provider, in which case the marking in done by the first (and only) IPX Provider in the path. Subject to the SLA, Service Providers can outsource the responsibility for packet marking to the IPX Provider.

4.6.4 IP Addressing and Routing

The IPX Providers and Service Provider networks must be totally separated from public Internet, from an IP routing perspective. That is, Internet routers must be prohibited from being able to route IP datagrams to IP addresses advertised to the IPX network and vice versa.

The IPX Provider's and Service Provider's networks must support IPv4 addressing and routing. IPv6 addressing and routing is recommended.

NOTE: IPv6 is currently supported on IPX Provider's networks between Service Providers where required by tunnelling the IPv6 traffic over IPv4.

Both IPX Providers and Service Providers that uses IPv6 in their networks must assume full responsibility for all network adjustments necessary for maintaining connectivity to all other IPX Providers and/or Service Providers that deploy IPv4.

Service providers and IPX providers may not yet be ready to change to IPv6 on the bgp peers, and such a change will not work right away for everybody. Therefore, a gradual introduction with Dual-Stack (i.e. both IPv4 and IPv6) is recommended.

The following migration steps from IPv4 to IPv6 are recommended on the IPX network:

- Start with one IPv4 and one IPv6-bgp-session on the NNI interface (service provider to IPX provider or IPX provider to IPX provider or between other network elements)
- In a mixed environment with v4/v6 addresses in a single and multi-VPN scenario, only the v6 information is advertised to v6-capable interfaces, which makes it easier for the migration to IPv6. There will be no direct communication between IPv4 and IPv6 addresses.

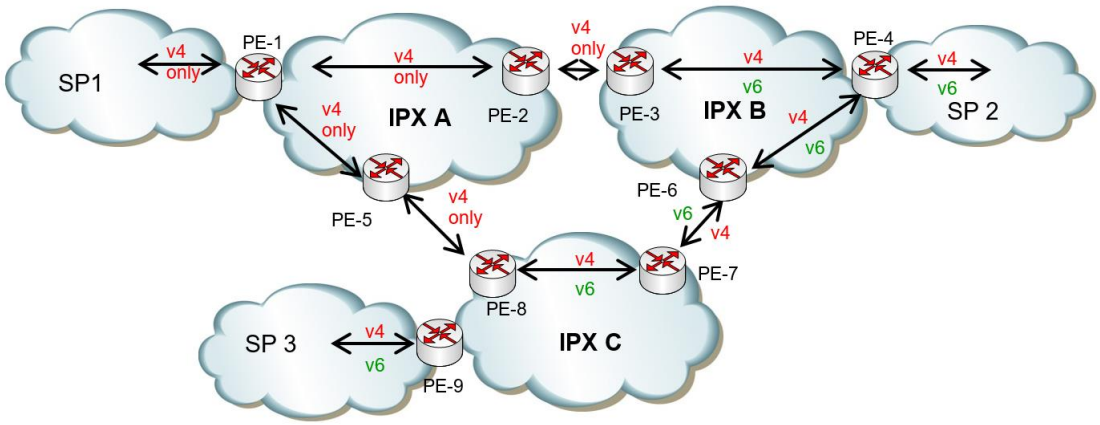

Figure 6: Dynamic routing IPX Network

- The connectivity in the IPX environment has to stay on IPv4 addressing despite the use of dual-stack, until a significant proportion of operators have implemented dual-stack. The more dual-stack ports are realized, the better IPv6-only ports would work; because many will support v6 in dual-stack.
- Gradually switch all interfaces to dual-stack until IPv4-only is mostly gone. If the risk can be taken, switch interfaces to IPv6 only.
- Protocol translators like SIIT, SOCKS, NAT-PT may be supported by some IPX providers but such support is not mandatory.
- Service providers who use IPv6 only inside their networks with dual-stack configuration, should use their own protocol translators
- For security reasons, route advertisement in multi-cast that are sent in regular intervals should be de-activated.

Note: Service providers can use IPv6 tunneling over IPv4, which is a good solution for service providers to migrate to IPv6 for GTP Tunneling, but it does not solve the shortage of IPv4 addresses in the case that an IPX provider in the transport chain, could run out of v4 addresses.

IPX Providers and Service Providers must use only valid IP address ranges, as defined in GSMA PRD IR.40 [26]. The IPX Provider must deny IP spoofing attacks originated by its Service Provider customers, that is, only traffic from valid IP address ranges (as defined in GSMA PRD IR.40 [26]) is allowed to flow to other customers or other IPX Providers.

As considered by Annex C of 3GPP TS 23.060 [3], IP MTU baseline over S8 and Gp interfaces is 1500 octets, assuming that GTP packets are exchanged between IPv4 addressed equipment.

IPX providers shall then engineer their internal networks in order to ensure that an IPv4 packet of 1500 octets, including IP, UDP and GTP headers, will be transmitted to the remote party with no fragmentation. In particular, IPX providers that provide IPSec access to their IPX network need to ensure that IPSec tunnel can transport 1500 octets based packet

4.6.4.1 BGPv4 Community Definitions

For improved routing control, and more flexibility for IPX providers to steer traffic with BGP attributes, regional communities may be used. This will support better quality and fulfilment of service provider requirements, especially for delay sensitive services like critical IoT or for 5G access technology.

In certain business situations, IPX providers cannot rely completely on the service provider traffic steering or when the IPX is expected to steer, the traffic on behalf of the service provider for best quality:

- To classify the source-IP prefix, to optimize the routing in the network
- A source could be identified by geographical location with the community values below. In the future maybe also the type of application and connection
- To propagate prefixes with BGP attributes for best path selection to achieve better RTT values
- Beneficial if BGP attributes need to be preferred over IP Backbone and IGP metrics for best path selection if the IPX is an overlay over an MPLS network
- Helpful if the same set of prefixes are received from the service providers or other IPX providers and the traffic needs to be kept local for business reasons, regional government policy like map data or delay sensitive traffic
- For capacity optimizations and QoS control in overload situations or re-routing becomes necessary

BGP extended Communities are described in RFC 4360. [23] and RFC 4384.

Communities can be added to the BGP announcements as attributes. A route can have multiple attributes attached. BGP communities can help to classify the source IP-prefix and optimize routing and QoS management in the IPX and service provider networks.

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 IPX Provider who is doing the marking. It identifies the party which eases the troubleshooting by using the AS number in the first part of the community.

Two cases have been identified as possible use cases so far: regions and type of traffic.

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

- Community 1 - 4 for internal/private use: (aaaaa:1nnnn) - (aaaaa:4nnnn)
- Community 5 identifies the regional info: (aaaaa:5nnnn)
- Community 6 identifies the type of traffic: (aaaaa:6nnnn)
- Community 7 - 9 for future GSMA/industry use: (aaaaa:7nnnn) - (aaaaa:9nnnn)

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

Area	Community
Europe	51000
Europe-North	51100
Europe-South	51200
Europe-East	51300
Europe-West	51400
Asia	52000
Asia-North	52100
Asia-South	52200
Asia-East	52300
Asia-West	52400
Oceania	53000
North America	54000
North America-North	54100
North America-South	54200
North America- East	54300
North America-West	54400
Central America	55000
South America	56000
South America- North	56100
South America- South	56200
South America- East	56300
South America- West	56400
Africa	57000
Africa – North	57100
Africa – South	57200
Africa – East	57300
Africa – West	57400

Table 3 – BGPv4 Regional Community values

If IoT traffic needs to be identified and handled differently from other traffic for low latency or other QoS adjustments, the types of traffic and corresponding values of nnnnn could be defined as follows:

Type	Community
Regular GTP traffic	61000
IoT traffic	62000
Other traffic	63000

Table 4 – Type of Traffic Community values

4.6.4.2 BGPv4 Community Definitions

In the LTE roaming environment other communities can be in use and should be left unhandled over the entire transport path. IPX providers should transparently transport all communities, bilaterally agreed between the Service Provider and the IPX Provider or between the IPX Providers and might add additional communities, but starting with their own AS number as described in section 4.6.4.1.

4.6.5 DNS/ENUM

As a minimum requirement, IPX Providers should support the transport of queries between MNOs to allow for correct resolution of FQDNs for all service requirements, for example Access Point Names (APNs) and Multimedia Messaging Service Centre (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, including hostname recommendations, is GSMA PRD IR.67 [17]. Specification for ENUM is GSMA PRD NG.105 [31].

4.6.6 Security and Screening

The IPX Network should meet the requirements laid out in GSMA 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/ IP Multimedia Subsystem (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).

4.6.7 QoS

Section 6 of this document concentrates on providing a traffic class specification and the parameters for different classes of service.

The QoS requirements for the IPX are outlined in section 6 and also in the end-to-end QoS SLA (IPX Agreement, GSMA PRD AA.80 [22]). End-to-end QoS as described in IETF RFC 3246 [15] is a mandatory requirement for IP Backbone Providers in the case of IPX.

The IPX network may support Class of Service (CoS) parameters presented in section 6 of this document.

4.6.8 Generic IPX 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 the IPX Service Transit and IPX Service Hub 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.

The following is a non-exhaustive list of generic features required from all IPX Proxies. Specific requirements for each service that an IPX Proxy can support will be captured as part of that service's definition/specification.

- 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.
- Signalling protocol conversion – if not handled by other network elements.
- Destination address look-up (including Mobile Number portability (MNP)) – if not solved by originating Service Provider.
- Transparency - the proxy shall not in any way 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.

5 Technical Requirements for Service Providers

5.1 General Service Provider Requirements

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

5.1.1 Service Provider IP Routing

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

Service Providers may screen unwanted routes for example, by selecting address ranges of their interconnect partners.

5.1.2 Service Provider IP Addressing

Public addressing shall be applied to all IPX 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, the use of IP public addressing does not mean that these addresses should be visible to Internet. For security reasons, Service Providers and IPX Networks must remain invisible and inaccessible to the public Internet. As such, Service Providers must ensure that the IP address ranges used by any network infrastructure connected to the IPX Network are totally separated from the IP ranges used by the UEs, and the routing for those IP address ranges by the UEs are not configured into any IPX Provider routers.

By keeping Infrastructure and UE IP ranges separated, UE traffic can be carried on the IPX Network while also ensuring that even if there is a misconfiguration somewhere, traffic from a UE will not be routed. This dramatically reduces the potential for an attack on the infrastructure in the IPX Network that has been initiated from end users/subscribers.

Where a Service Provider uses Network Address Translation (NAT) for traffic from the UEs, the same rule applies. That is, IP address ranges used for NAT of UE traffic must be kept separate from IP address ranges used by the remainder of their network infrastructure.

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

Currently, the IPX Provider networks use IPv4 addressing but in order for Service Providers to use IPv6 addressing for transport IPX functionality, enhancement is necessary. It is not feasible for the service providers to tunnel IPv6 transport traffic over IPv4 due to unknown, end-to-end, IPv6 to IPv4 mapping.

Both IPX 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 IPX Providers and/or Service Providers that also deploy IPv6. This shall be facilitated through announcing IPv6 backbone ranges on IR.21 and establishing BGP advertisements of those IPv6 ranges to a directly connected IPX.

However, it is recommended to start using IPv6 wherever possible to avoid v4 address shortage in the IPX Provider community. See section 4.6.4 for more information about usage of IPv4/IPv6 Dual-Stack.

5.1.3 Service Provider DNS

The recommendations in GSMA PRD IR.67 [17] and GSMA PRD NG.105 [31] shall apply.

5.1.4 Service Provider Security and Screening

Service Providers shall meet the requirements for security laid out in GSMA PRD IR.77 [19].

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/3G PS Roaming (where GTP is used), WLAN interworking (where IPSec is used), and LTE roaming (where GTP is used).

5.2 BGP Advertisement Rules

5.2.1 General Rules

Service Provider's core network addresses may be advertised to the IPX Network 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 IPX Network. When connecting to an IPX, the BGP-4 protocol shall be used for advertising a Service Provider's network addresses.

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

- 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 IPX Provider.
- Service Providers shall only advertise their own core public IP address ranges into the IPX Network.
- 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 IPX Providers 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 **Error! Reference source not found.**, to tag all its 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.

The BGP advertisements of Services Providers will be marked by IPX Providers according to the rules described in section **Error! Reference source not found.**. No action is required from the Service Provider.

5.3 Service Provider and IPX Network Connectivity

The end-to-end SLA in GSMA PRD AA.80 [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 (for example, leased line or fibre), or
- Layer 2 logical connection (for example 1G Ethernet, 10G Ethernet etc.),
- 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. This is because End to End IPX QoS and SLA enforcement cannot be achieved due to a non-IPX Public network being used for connectivity.

It is up to IPX Provider and Service Provider to determine the exact details of each connection bilaterally and to agree the SLA. The main benefits of the IPX Network structure to Service Providers are:

- The Service Providers do not have to create dedicated connections to every roaming partner. One connection to one IPX Provider is required as a minimum.
- Service Providers may choose to start with low cost connection to the IPX Network 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 that is, the IP backbone is scalable and able to meet Service Provider Requirements.
- IPX Network can have QoS implemented as long as the Internet IPSec VPN option is not used. The QoS that could be implemented shall be measurable on a Service Provider by Service Provider basis.
- IPX Network introduces a Hub Connectivity Option to simplify different interworking scenarios.

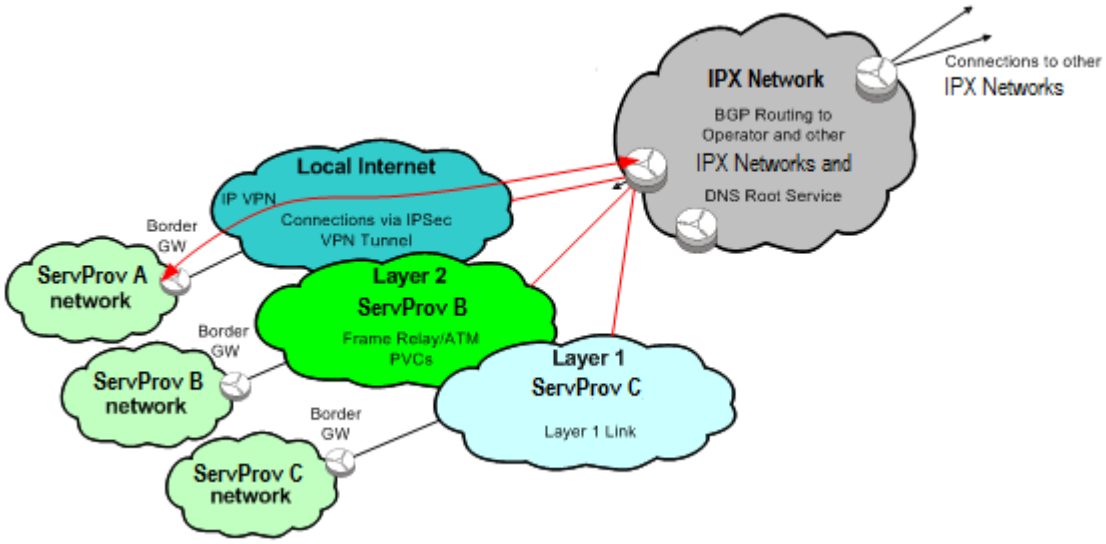

Figure 7: Hub Connectivity Option Scenario

6 QoS

6.1 SLA for IPX Network

The end-to-end QoS SLA in GSMA PRD AA.80 [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 section.

An SLA defines a service specification between a Service Provider and an IPX Provider (for example, access availability). An SLA can also define IPX Provider to IPX Provider service specifications depending on bilateral agreements between IPX 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 IPX Provider. The profile extends to the whole IPX network comprising IP IPX Providers' maintained networks and routers.

The following aspects should be considered for inclusion in the agreement between Service Provider and IPX Provider.

6.1.1 Service Guarantees

Service guarantees should be defined for each IP QoS parameters defined in section 6.3. Additionally, there should be a defined reporting and escalation procedure, that is, the backbone Provider takes responsibility to provide measurements and permits the Service Provider to analyse the results.

6.1.2 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 should be in scope for any future governance.

Help desk support and customer services should be considered.

6.2 Traffic classification

6.2.1 UMTS QoS parameters

There are four different UMTS QoS classes for the UMTS bearer service:

- 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 sensitive to delay and jitter, as long as packets are not dropped in network to avoid retransmissions and extra load to network.

The characteristic of each class is defined in [13] chapter 6.3.

- Traffic Classes attributes

It identifies the UMTS QoS Class applicable to the UMTS bearer service.

- Traffic Handling Priority

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

- Signalling Indication

The Signalling Indication identifies a bearer carrying signalling. It is applicable only to the interactive class.

6.2.2 EPS QoS Class Identifiers

3GPP TS 23.203 [28], table 6.1.7, provides the mapping of QCI to standardized characteristics listed below as well as some examples of applications:

1. Resource Type (Guarantied Bit Rate or Non-Guaranteed Bit Rate);

2. Priority;
3. Packet Delay Budget;
4. Packet Error Loss Rate.

Note that standardized characteristics are not stored in the subscriber profile nor are they carried on any EPS interfaces. QCI values are used as guidelines to configure the packet forwarding parameters of EPS equipment to provide an E2E QoS.

6.2.3 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].

6.2.4 IPX traffic classes

Warning: IPX traffic classes must not be confused with the UMTS QoS ones (see [13]) although they share the same names. IPX traffic classes are QoS classes valid in the IPX.

- Conversational class;
- Streaming class;
- Interactive class;
- Background class.

6.2.5 Differentiated Services Code Point

The 6-bit DSCP indicates the PHB that a packet belongs to. The DSCP values shown in Table 6 are specified in IETF RFC 3246 [15] and IETF RFC 2597 [16].

6.2.6 2G/3G/4G/5G marking

It is recommended that following traffic classes are available and marked by the MNO as presented in the table 5. Traffic classes are distinguished by Class of Service and Differential Service bits. The layer 2 CoS bits are seen in the PCP field of the Ethernet frame. The layer 3 bits are seen in IP CoS. Both are used for prioritizing traffic if needed, based on the mappings listed in table 5 below.

Note: the MNOs would mark the packets with the Diffserv values (layer 3 header information would remain unchanged end to end, unless IPX Providers choose to modify according to section 6.2.8). Then the various hops in the end to end path would be responsible to map these layer 3 values to the corresponding CoS markings (where applicable), in order to ensure consistent QoS parameters across the networks.

EPS QoS	GPRS/UMTS QoS Parameters			IP Transport		IPX QoS	Ethernet Transport	
QCI	Traffic Class	THP	Signaling indication	Diffserv PHB	DSCP	Traffic Class	CoS	Binary
1	Conversational	N/A	N/A	EF	101110	Conversational	5	101
2								
3								
4	Streaming	N/A	N/A	AF41	100010	Streaming	4	100
5	Interactive	1	Yes (see note)	AF31	011010	Interactive	3	011
6			No	AF32	011100		3	011
7		2	No	AF21	010010		2	010
8		3	No	AF11	001010		1	001
9	Background	N/A	N/A	BE	000000	Background	0	000

Table 5: 2G/3G/4G/5G EPS QoS information and their mapping to CoS & DSCP values

Note: The Signalling Indication QoS parameter has been introduced in 3GPP Release 5. SGSN supporting releases earlier than release 5 cannot manage it. They must mark Interactive Traffic Class with Priority 1 and PHB AF31.

6.2.7 Application traffic marking

It is recommended that the traffic is marked by the MNO as presented in the Table 6 according to the QoS required by the application.

Application	Protocol	PHB	IPX QoS class name
VideoShare	N/A	AF41	Streaming
VoIP/VoIMS/ VoLTE	RTP	EF	Conversational
Conversational video / ViLTE	RTP	EF	Conversational
Push to talk	N/A	AF41	Streaming
Video streaming	N/A	AF41	Streaming
Signalling (including capability discovery and Presence)	SIP SIGTRAN Diameter GTP-C HTTP/2	AF31	Interactive
DNS (inter-operator and IPX)	DNS	AF31	Interactive
Online gaming	N/A	AF32	Interactive
WAP browsing	N/A	AF21	Interactive
WEB browsing	N/A	AF21	Interactive

Instant messaging	N/A	AF11	Interactive
Image Share	MSRP	AF11	Interactive
Remote conn.	SSH, telnet	AF11	Interactive
File Transfer	MSRP	BE	Background
Email sync	N/A	BE	Background
MMS	SMTP	BE	Background

Table 6: Application mapping into DSCP

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

6.2.8 Packet marking rules

Service Providers are responsible for marking packets to correct traffic classes. They may outsource this functionality to IPX Provider when suitable.

If the DSCP marking from a Service Provider cannot be trusted (depending on the agreement between the Service Provider and its IPX Provider), its IPX Provider should correct the DSCP value to a static default value to be in line with pre-agreed levels (**Error! Reference source not found.**5) before sending to peer on the considered service VLAN (e.g. Voice, Data, Signalling, …).

The AF21 DSCP value should be used as default to correct untrusted DSCP values for Data Roaming VLAN.

At peering points, GRX Providers and IPX Providers will co-exist and will exchange GPRS Roaming traffic in a common VLAN for Data Roaming. It is the responsibility of the sending GRX/IPX Provider to ensure that DSCP marking can be trusted by the receiving IPX Provider.

6.2.9 5GS traffic marking

3GPP TS 23.501 [37] Table 5.7.4-1 provides the mapping of standardised 5QI values to 5G QoS characteristics, listed below as well as some examples of applications.

1. Resource Type (Guaranteed Bit Rate, Non-Guaranteed Bit Rate, Delay-critical Guranteed Bit Rate)
2. Default Priority Level
3. Packet Delay Budget
4. Packet Error Rate
5. Default Maximum Data Burst Volume
6. Default Average Window

5QI values are used as guidelines to configure the packet forwarding parameters of 5GS equipment to provide an E2E QoS. Such 5QI values are mapped to DSCP and CoS in Table 6 according to the above characteristics.

QoS	IP Transport		IPX QoS	Ethernet Transport	
5QI value	Diffserv PHB	DSCP	Traffic Class	CoS	Binary
1	EF	101110	Conversational	5	101
2					
3					
65					
66					
67					
71					
79					
80					
82					
83					
84					
85					
86					
87					
88					
89					
90					
4	AF41	100010	Streaming	4	100
72	AF42	100100		4	100
73	AF41	100010		4	100
74	AF41	100010		4	100
76	AF42	100100		4	100
5	AF31	011010	Interactive	3	011
6	AF32	011100		3	011
7	AF21	010010		2	010
8	AF11	001010		1	001
69	AF31	011010		3	011
70	AF32	011100		3	011
9	BE	000000	Background	0	000
10	BE	000000		0	000

Table 7: 5QI information and mapping to CoS & DSCP values

Note: Certain 5QI values (such as 79) may be indicated as 'Interactive' use case, however they're classified as traffic class 'conversational' in order to assign them DiffServ EF PHB capability to provide a robust service with low loss, low latency, low jitter, and assured bandwidth. The intent of this mapping table is mainly to recommend the DiffServ and CoS for the various services/use-cases represented by the 5QI values Note that only DiffServ and CoS values are the end results of this mapping table. 'Traffic Class' is just an intermediate step and is classified based on DSCP values.

6.3 IP QoS Definitions for IPX Network

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 sections, 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 IPX Providers PoP (Point-of-Presence).
- Local Loop size is 1 Gbit/s as minimum.

Following sections 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.

6.3.1 Availability

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

Service Providers should discuss with IPX 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:

- IPX Provider network, including peering/interworking functionality and possible DNS functionalities,
- Service Provider to IPX Network connection,
- Monitoring/measurement equipment (if supported).

Values for availability are following

- Availability of the IPX Provider network: 99,995%
- Service Providers connection to IPX Provider network with single connection: 99,7%
- Service Providers connection to IPX Provider network with dual connection: 99,9%

6.3.2 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)

Error! Reference source not found.5 and **Error! Reference source not found.**6 present roundtrip delay values between originating and terminating Service Provider premises at the transport layer.

It should be noted that actual performance of IPX Provider network could be better than given reference values in the **Error! Reference source not found.**5 and **Error! Reference source not found.**6.

For session based services, the round trip delay is greater due to processing time at the service layer.

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://unstats.un.org/unsd/methods/m49/m49regin.htm

6.3.3 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:

6.3.3.1 Definition

IP Packet Delay Variation is defined in IETF RFC 3393 [33], which 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 6.3.2.

The ipdv is the difference between the one-way-delay of the selected packets."

IETF RFC 3393 [33] 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.

6.3.3.2 Jitter Target Values

The following Jitter values shall only apply to conversational and streaming traffic classes (that is, EF and AF4 traffic classes).

Intra-continent Jitter Value – **5 ms** per GRX/IPX Provider network (maximum of two involved in the service delivery chain).

Inter-continent Jitter Value – **10 ms** per GRX/IPX Provider network (maximum of two involved in the service delivery chain).

6.3.3.3 Intra-Continent Traffic

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

6.3.3.4 Inter-Continent Traffic

In the case where traffic exchanged between Service Providers in different continents, and GRX/IPX network 1 is exchanging traffic with GRX/IPX network 2 in the same continent as the originating Service Provider, GRX/IPX network 1 would have a 5 ms Jitter target and GRX/IPX network 2 would have a 10 ms target to recognise that GRX/IPX network 2 traffic is inter-continental.

6.3.3.5 Service provider jitter requirements

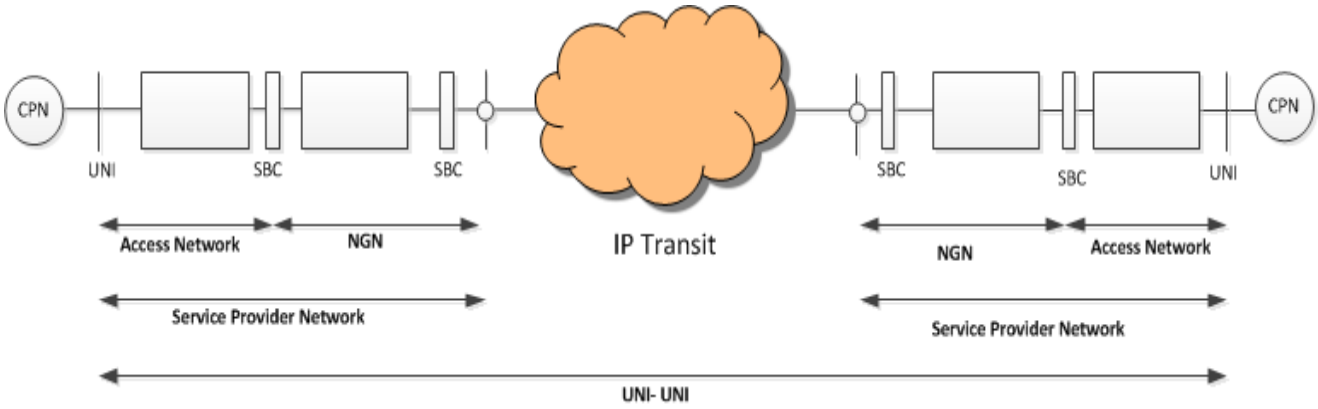

Figure 8: Jitter requirements

The limit for service provider jitter (IPDV) of GRX/IPX access links is as follows [ETSI TS 103 210; Y.1541 Appendix XII]:

Nature of Network	Application	Jitter Value
Service Provider Network (sending side)	EF Voice	< 40 ms
	EF Conversational Video	< 10 ms

Table 10: Limit on IPDV values

The target jitter value is the maximum occurring during one month.

6.3.4 Packet Loss Rate

Packet Loss is the ratio of dropped packets to all packets sent from the SOURCE to DESTINATION in per cents (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 11: Packet loss requirements

IPX Provider networks should be dimensioned so that packet drops do not occur (or occur relatively rarely).

7 Traffic Applications

The following sections describe some of the traffic applications for the IPX Provider networks.

7.1 GPRS/3G/4G 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. Transmission Control Protocol (TCP) carries GTP PDUs in the GPRS IP backbone network for protocols when a reliable data link is needed and User Datagram Protocol (UDP) carries GTP PDUs otherwise (see 3GPP TS 23.060 [3] for more information). Only Serving GPRS Support Node (SGSNs), Serving Gateways (SGWs), Gateway GPRS Support Node (GGSNs) and Packet Data Network Gateways (PGWs) implement the GTP protocol (see 3GPP TS 29.060 [3]). No other systems need to be aware of GTP.

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 IR.88 [25], WLAN roaming authentication (7.3), MMS Interworking (7.4) and IMS Interworking (7.5).

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

7.2 Service Provider Bilateral Services

The IPX Network may be used to transport any IP traffic on a bilateral basis as part of the IPX Transport Connectivity Option (see section 3.3.1 for more details), 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.

7.3 WLAN Roaming

The IPX Network can be used for WLAN roaming between Service Providers. At the first phase, Inter-Service Provider IP backbone is used only for transporting Remote Authentication Dial In User Service (RADIUS) messages that are used for authentication, accounting and authorization of the WLAN services. For further information, see IR.61 WLAN Roaming Guidelines.

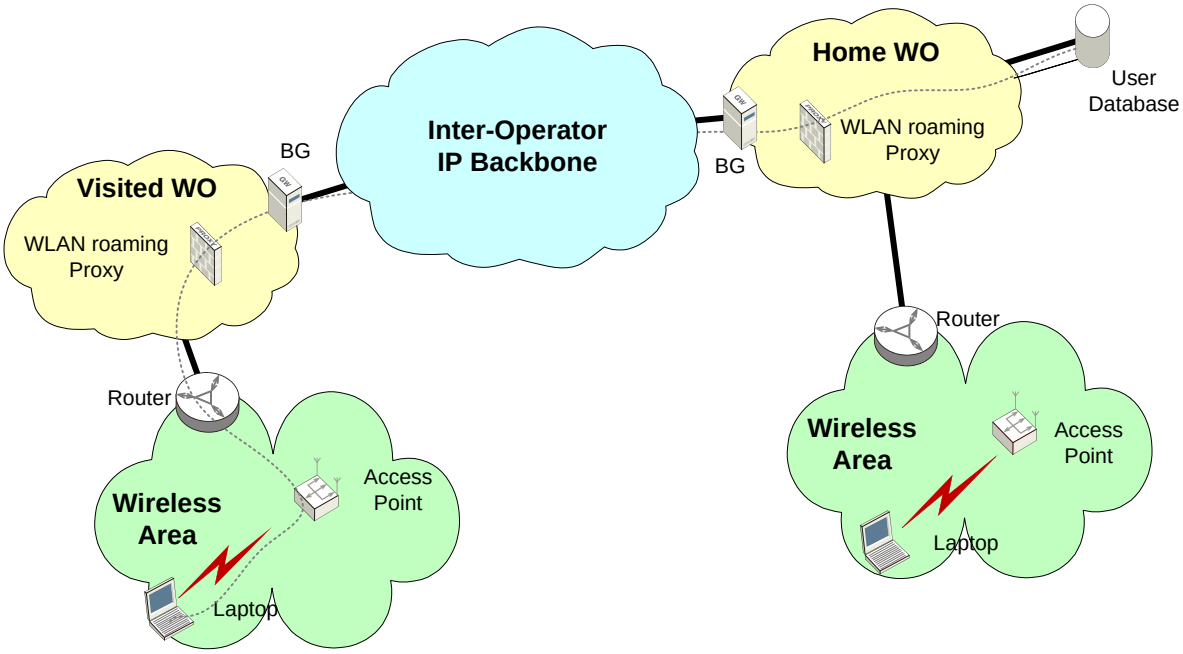

Figure 9: Inter-Service Provider IP Backbone used for the WLAN roaming

7.4 MMS Interworking

The IPX Network can be used to exchange MMS traffic between Service Providers utilizing SMTP protocols. For further information, see IR.52 MMS Interworking Guidelines.

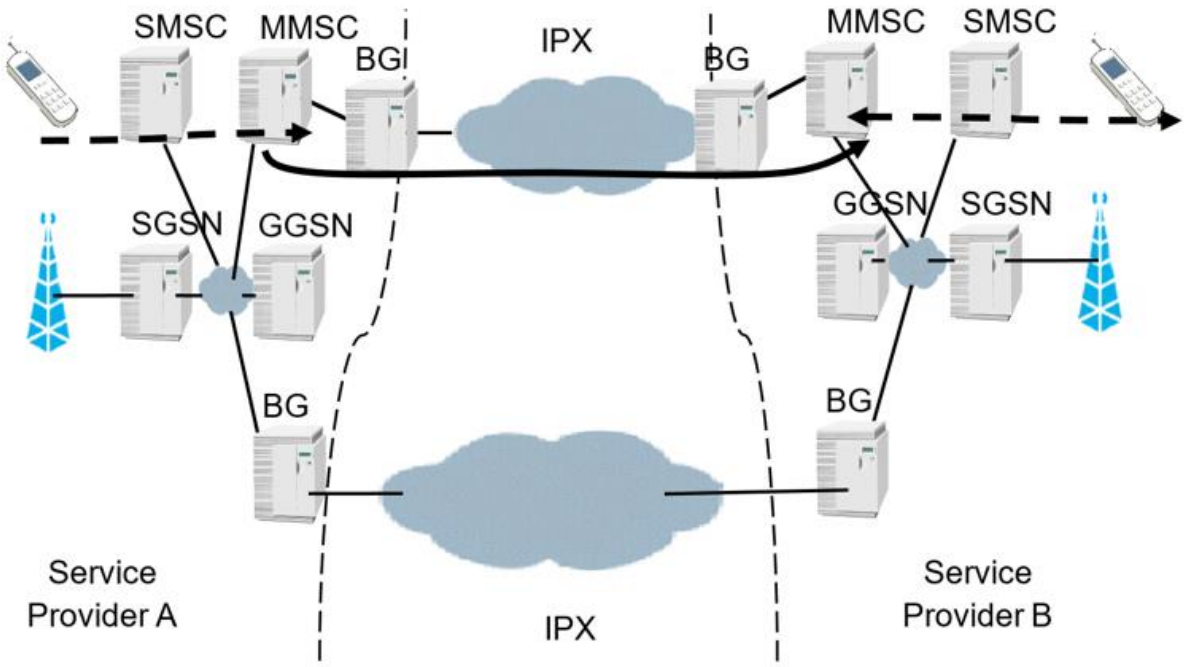

Figure 10: Inter-Service Provider IP Backbone used for MM4

7.5 IMS

The IPX Network can be used for IMS interworking between IMS networks as depicted in **Error! Reference source not found.** below. Note that User Plane traffic may or may not be sent through the IPX Proxy.

IMS interworking will introduce new protocols (for example, 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 GSMA

PRD IR.65 [20] - IMS Roaming and Interworking Guidelines – and 3GPP TS 23.228 [21].

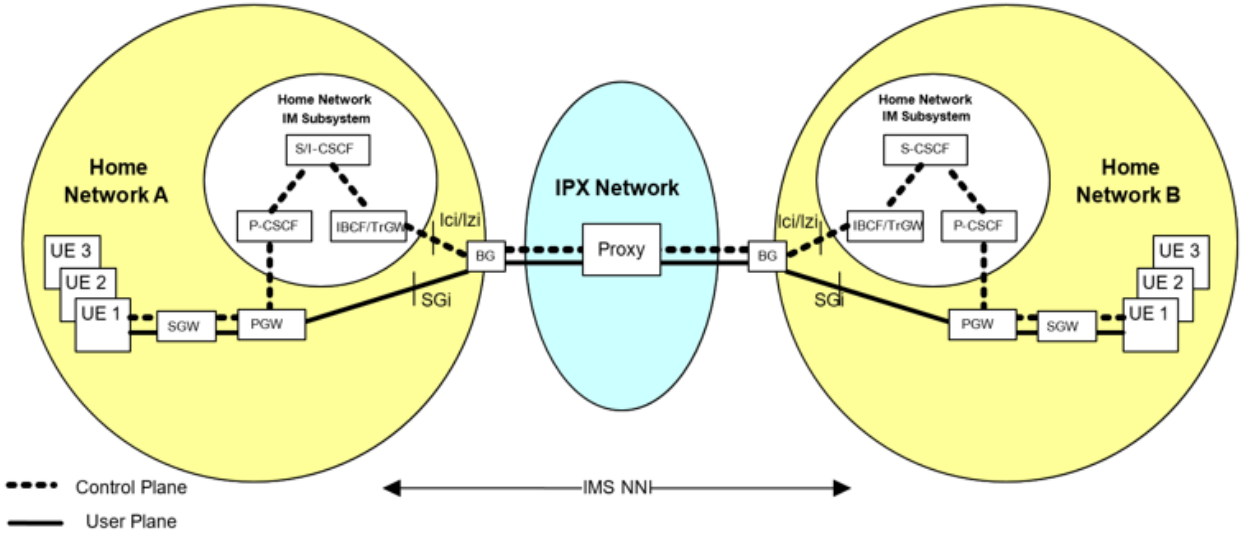

Figure 11: IPX Network used for the IMS Interworking

As stated in GSMA PRD IR.65 [20] section 5.7, the inter-connected networks in figure 10 can be, based on Operator deployment preference, either:

- a converged IMS core network supporting all IMS services,
- a separated IMS core network, with each supporting a sub-set of IMS services networks.

As described in GSMA PRD IR.95 [35] section 13, when there is a need to inter-connect between such different deployment options, then a suitable interworking capability is required between the IMS cores. Such interworking capability can be provided by the IPX network.

Furthermore, Operators can also deploy different mechanisms to realize the RCS Capability Exchange mechanism (i.e. Options versus Presence based) to negotiate the commonly supported service set,. If different mechanisms are deployed in inter-connected networks, then there is a need to provide an interworking function as described in GSMA PRD IR.90 [36] section 4.1.3. Such an interworking function can also be provided by the IPX network.

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

Annex A Considerations for implementation

A.1 A.1 Double IPX Provider network problem

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

Error! Reference source not found. shows example about asymmetric routing. In following case return packets could be blocked by Service Provider B Firewall (FW) if the FWs are not synchronized together.

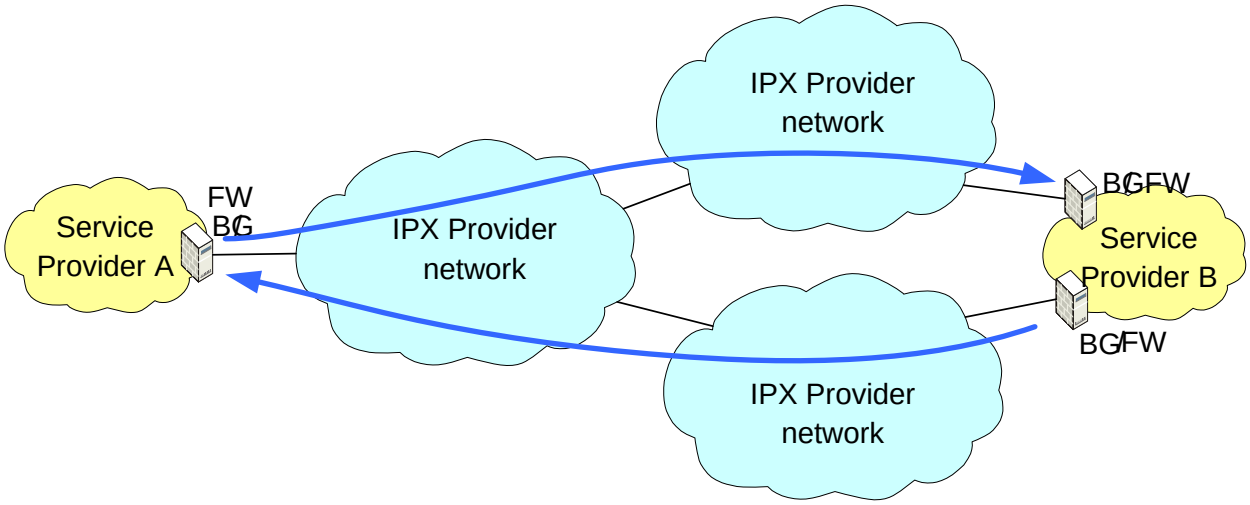

Figure 12: Asymmetric routing

It is recommended that Service Providers agree with their own IPX Providers how backbone addresses are advertised to the IPX 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 IPX Provider network 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 IPX network.

- 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.

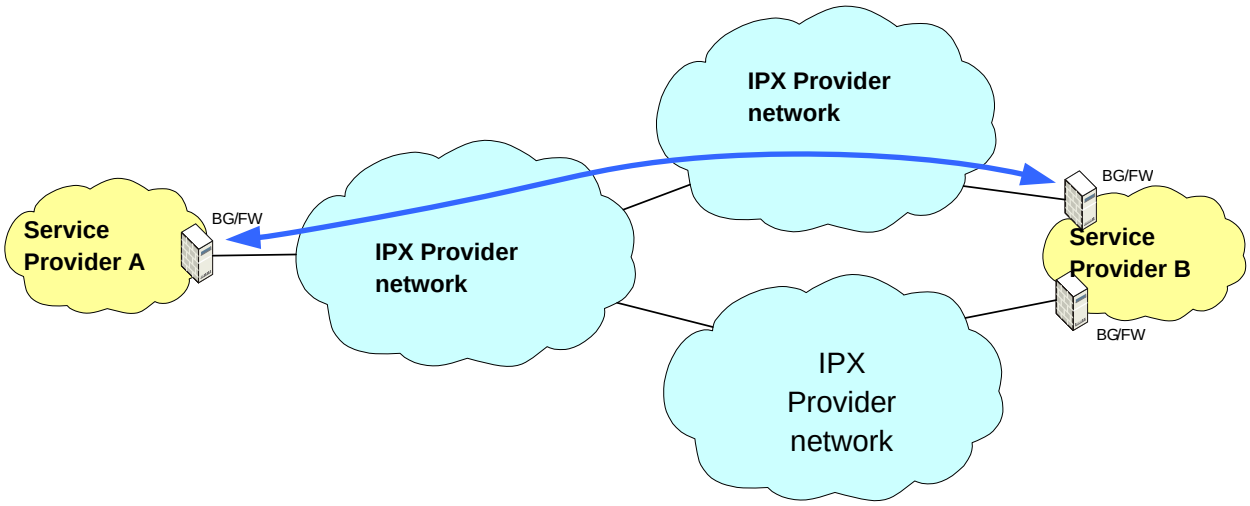

Figure 13: Avoiding of asymmetric routing using network configuration

A.1.2 Short-term solution disadvantages

- It is a "hot standby" solution. The IP traffic goes via the primary IPX Provider network only. Only in the case of failure of the primary IPX Provider network the traffic is routed via the other IPX Provider network.
- Avoids optimum path routing. That means, due to the BGP manipulation the selected path might not be the shortest one.
- IPX Provider commercial problem. The not preferred IPX Provider losses valuable traffic on the interface to the Service Provider. The traffic must be routed via the peering to another IPX Provider network.
- 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.1.3 Long-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.

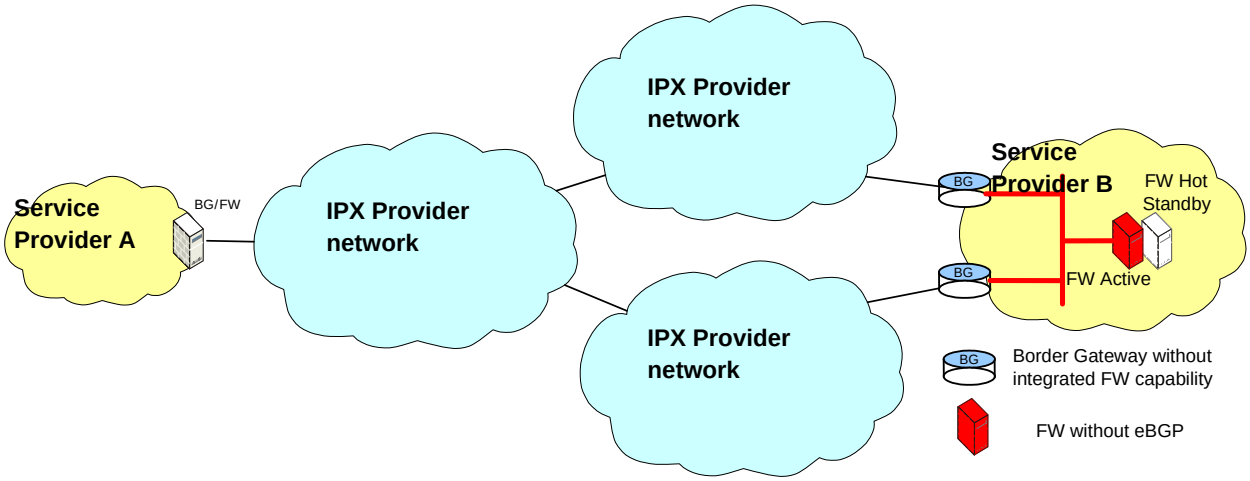

Figure 14: Proposal for network design to overcome the "IPX Provider network problem"

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

The IPX Provider network has QoS, the Service Providers need to define precise routing policy between Service Provider networks to account for this requirement

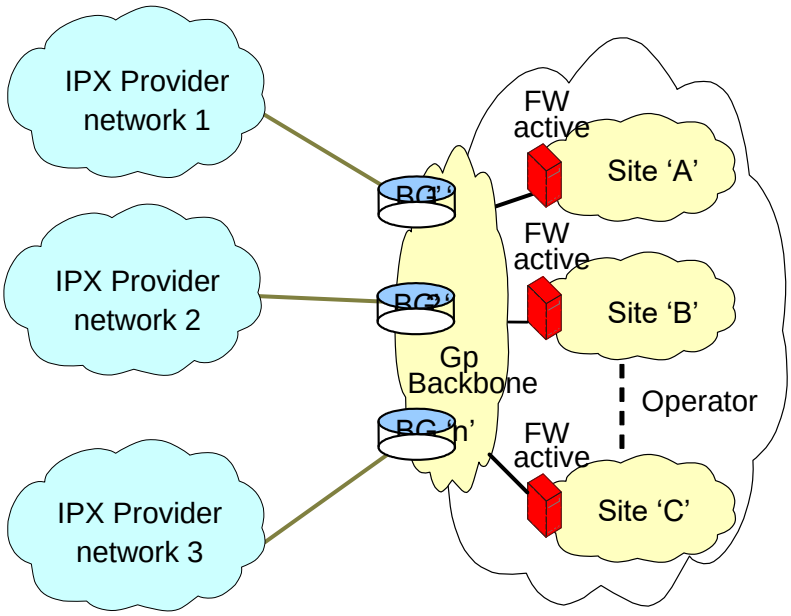

Figure 15: Future network growth

To overcome the "double IPX Provider network 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 IPX Provider network interconnection, which can be not cost efficient especially in

the early stages. The IPX Provider network IP ranges must be divided in two halves, for example "north" and "south".

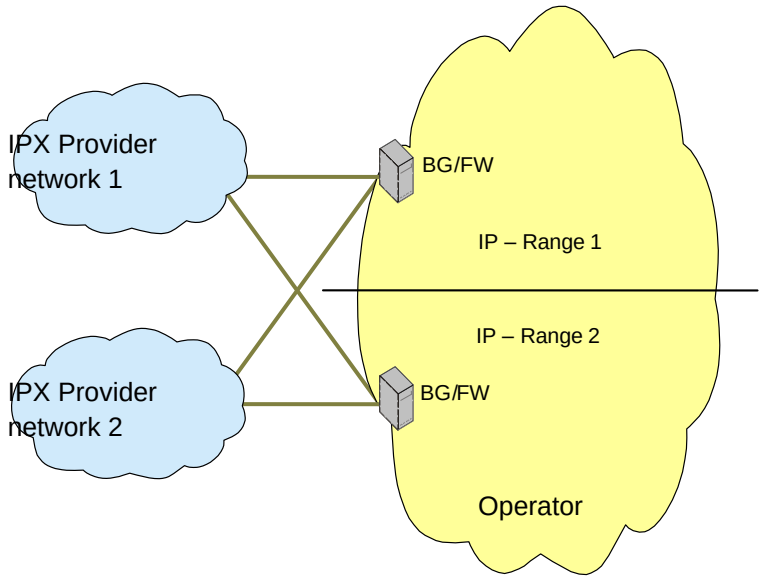

Figure 16: Full-meshed IPX Provider network interconnection

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

Annex B IPX Proxy Requirements

B.1 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.

B.2 Requirements for IPX Proxy

B.2.1 General

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

B.2.1.1 IPX 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 Service Providers (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 4.6 of this document and in GSMA PRD IR.77 [19].

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 (for example, 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 Port Address Translation (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 GSMA PRD AA.80 [22] 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 section 6 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 and 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 GSMA PRD IR.40 [26] and GSMA PRD IR.77 [19]. 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-tunnelled.

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 key Performance Indicators (KPI) parameters to end-to-end connections compared to when there is no IPX Proxy.

RI29. IPX Proxy shall be able to relay the Type of Service (ToS) 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 on-going 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.2.1.2 Operational Requirements

The set of Operational Requirements described in this section provides 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 GSMA PRD IR.40 [26] and GSMA PRD IR.77 [19].

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 signalling 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.

RO15. IPX Proxy may support an interworking capability between Service Providers who have opted for different IMS core network deployment options (i.e. converged IMS core network providing all IMS services versus separate IMS core networks, with each providing a sub-set of the overall set of services). This interworking functionality ensures consistency of SIP message routing to the correct IMS core network as well as the correct exchange of service capabilities between Service Provider networks. See section 13 of GSMA PRD IR.95 [35] for further details.

RO16. IPX Proxy may support inter-working of Options based and Presence based RCS Capability Exchange as described in GSMA PRD IR.90 [36] section 4.1.3. See section 14 of GSMA PRD IR.95 [35] for further details.

Annex C Document Management

C.1 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		

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
		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 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
5.0	December 2010	Packet Docs 046_10rev2, IREG Doc 059_14 and IREG Doc 059_18 incorporated	IREG Packet	Itsuma Tanaka / NTT DOCOMO, Nick Russell / Vodafone
6.0	March 2011	IREG Doc 60_061 incorporated	IREG 60/ DAG 79	Marko Onikki / Teliasonera
6.1	October 2011	Packet Doc 51 009 incorporated	IREG Packet 51	Gert Öster / Ericsson

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
7.0	January 2012	DAG Doc 88_035 incorporated	DAG 88	Michel van Veen /Sybase 365
8.0	December 2012	DAG Docs 99_012, 99_013 incorporated	DAG 99	Vincent Danno & Laurent Dubesset, Orange
9.0	February 2013	IREG Doc IR.34 CR1001	DAG #101	Jose Antonio Aranda (GSMA), Nicola Witney (GSMA), , Michael Van Veen (Sybase 365), Itsuma Tanaka (NTT DOCOMO, INC.), Document Approval Group (Co-ordinator), Document Approval Group (Director)
9.1	March 2013	IREG Doc IR.34 CR1002,CR1003		Vincent Danno (Orange France)
10.0	Oct. 2014	CR1005, CR1004	IREG	Marko Onikki (Telia Sonera)
11.0	November 2014	CR1006, CR1007	IREG	Marko Onikki (Telia Sonera)
11.1	March 2015	CR1008 IPX Network Connectivity - Adding Specific Language for which Options Allow for End to End SLAs and QoS	IREG	Marko Onikki (Telia Sonera)
12.0	January 2016	CR1010, CR1011, CR1012	NG	Marko Onikki (Telia Sonera)

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
13.0	18 October 2016	CR1013, CR1014, CR1015 (Class of Service consistency across IPX Network)	NG	Marko Onikki (Telia Company)
13.1	31 July 2017	CR1015 (ENUM Reference Correction) (duplication of CR No)	NG	Marko Onikki (Telia Company)
14.0	1 August 2018	CR1016, CR1017	NG	Marko Onikki (Telia Company)
15.0	11 May 2020	IR.34 CR1018 NNI Interworking Function	NG	Javier Sendin (GSMA)
16.0	30 October 2020	CR1019, CR1020, CR1021	NG	Marko Onikki (Telia Company)
17.0	18 May 2021	CR1022, CR1023, CR1024	NG	Marko Onikki (Telia Company)
18.0	13 Aug 2022`	IR.34 CR1025 DSCP class for application DNS	NG	Javier Sendin (GSMA)
19.0	June 2024	IR34 CR1027_N32 via NEW 5G Control Roaming N9 via DATA Roaming VLAN R0.3	NG-ISAG	Javier Sendin (GSMA)

Other Information

Type	Description
Document Owner	NG
Editor / Company	Eddy Goffin (Orange)

Feedback

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 prd@gsma.com

Your comments or suggestions & questions are always welcome.