International Interconnection forum for services over IP (i3 Forum)

(www.i3Forum.org)

Source:

Workstreams: "Technical Aspects", "Service Requirements"

Keywords: IPX

Common functionalities and capabilities of an IPX platform

(Release 1.2, May 2013)

Revision History

Date	Rel.	Subject/Comment
Dec. 12th 2012	1.1	First release of IPX Core document – First version
May 12th 2013	1.2	First release of IPX Core document – Second version after received comments

Executive Summary

The IPX model, as defined by the GSMA, is an international, trusted and QoS controlled IP backbone, consisting of a number of competing carriers (IPX Providers) that interconnects Service Providers according to mutually beneficial business models. The objective of this document is to provide a service and technical architecture that allows for both the Service Providers and the IPX Providers to enable a productive IPX business model. This document allows the following requirements to be realized.

- Service Providers (MNO, FNO, ASP, ISP, OTT Provider): Providing guaranteed service quality, reliability, and security for IP-based service delivery with other Service Providers in the IPX ecosystem.
- IPX Providers: Allowing for technical and economical efficiencies while providing IPX-based services to Service Providers.

This document describes principles and features common to all IPX networks. Topics specific to a given service can be found in separate documents, called Service Schedules.

The combination of the GSMA-defined IPX requirements, this Common Functionalities and Capabilities document, and the respective Service Schedules provides a set of IPX requirements that can be implemented, including:

- An IPX architecture and reference model;
- IP routing and forwarding with the identification of the proper standard/coding for routing, addressing, marking the IP packet;
- Session-based signalling support, e.g. SIP-I and SIP;
- Media with a list of supported codecs and their respective features;
- Security;
- Quality of service (QoS) measuring model encompassing the parameters' definition, guidelines for achieving these measurements, and their related metrics;
- Service Routing with the description and service impacts of the concepts of "confined routing" and "break-in/ break-out" scenarios.

Note that this document differentiates from that of the GSMA IPX requirements on some specific topics (such as break-in/break-out). However, this implementation specification document should not be considered as an alternative architecture with respect to the GSMA IPX model but as IPX Providers' contribution with the objective to provide a detailed technical guidance for the implementation of IPX-based services.

Services offered via private interconnection and/or via the Public Internet remain technical and commercial options outside the IPX environment, as per i3 Forum specifications [1], and Service Providers and IPX Providers are free to request and offer Internet-based services according to their own policies. Consequently, the existing interconnection model between Carriers and the new IPX model are both legitimate and will co-exist being that Service Provider and IPX Provider are free to request and to offer the model more suitable for their own commercial and technical policies.

The content of the document is based on the latest available version of the GSMA IPX specifications. The i3 Forum is ready to update the content of the document in next releases following the GSMA specification process.

Table of Contents

1 Scope and Objective of the document 1
2 Acronyms 2
3 References 3
4 Definitions 4
5 General Model & Architecture 5
5.1 Reference Business Framework 5
5.1.1 Break-in / break-out 6
5.1.2 Connectivity Options (as business models) 6
5.2 Reference Technical Architecture 7
6 IPX Agreements 9
7 Transport Functions 10
7.1 Generic Cases of Transport Configurations 10
7.1.1 Case 1- Layer 1 interconnection 10
7.1.2 Case 2- Local Layer 2 interconnection 10
7.1.3 Case 3 - Layer 3 interconnection via Public Internet 11
7.1.4 Applicability 11
7.2 Physical Interconnection Alternatives 11
7.2.1 SDH-based transport Systems 11
7.2.2 Ethernet-based transport Systems 12
7.2.3 Interconnection redundancy 12
7.3 VLAN 12
7.4 Internet Protocol 12
7.4.1 IP Addressing 12
7.4.2 IP Routing 12
7.4.3 Classes of Service 12
8 Signalling 14
9 Media/Data 15
10 Routing & addressing 16
10.1 General Service Routing Principles 16
10.2 Number of IPX Providers in the SP-SP communication 16
10.3 Routing Transparency 16
10.4 Break-in / break-out connectivity and notification 16
10.4.1 Break-in / break-out connectivity options 16
10.4.2 Break-in / break-out notification 17
10.5 Role of DNS and ENUM registry 17
10.6 Numbering and Addressing Scheme for E.164 number-based services 17
10.6.1 Tel-URI Addressing scheme 17
10.6.2 SIP-URI Addressing scheme 17
10.6.3 Number Portability Resolution 18
10.7 Other Addressing schemes 18
11 Security 19
11.1 General 19
11.2 Isolation From the Public Internet 19
11.3 Separation of Traffic by IP Addressing 19
11.4 Use of Proxy 19
12 QoS Measurement 20
12.1 QoS parameter definitions 20
12.2 Implementing GSMA quality requirements 21
12.2.1 Transport and Service Parameters 21
12.2.2 Service parameters 22
12.3 KPI computation for SLA / QoS reporting 22
12.4 QoS Enforcement 23
12.5 Penalties 23
13 Accounting principles 24
13.1 Transit fee 24
13.2 Charging transparency 24
14 Operational Practices 25
15 Annex A - Architecture of IPX platform 26

15.1 Reachability / Coverage: interconnection obligations for IPX Providers 26
15.2 Public Interconnect Locations 26

1 Scope and Objective of the document

This document, together with a set of separate, accompanying documents (called Service Schedules) deprecates and replaces i3Forum “Technical Specification for Voice over IPX service”.

The IPX model, as defined by the GSMA is an international, trusted and controlled IP backbone that interconnects Service Providers (SPs) according to mutually beneficial business models. It is designed to offer highly efficient and commercially attractive methods of establishing interworking and roaming interconnection arrangements for IP services [9]. The IPX environment consists of a number of IPX Providers (IPX Ps) in competition, selling interconnect services to SPs. The IPX Ps’ networks are mutually interconnected where there is demand by SPs.

The objective of this document is to provide a service and technical architecture that allows for both the SPs and the IPX Ps to enable a productive IPX business model. This document allows the following requirements to be realized.

- SPs: Providing guaranteed service quality, reliability, and security for IP-based service delivery with other SPs in the IPX ecosystem.
- IPX Ps: Allowing for technical and economical efficiencies while providing IPX-based services to SPs.

Consequently, the IPX would result in an evolution of the existing architectural model for voice, implying the transition from present local, mono-service (voice) interconnection model, towards a multi-service, converged, global, functionally-layered interconnection model.

This document describes features common to all IPX networks. Topics specific to a given service can be found in separate documents, called Service Schedules.

The combination of the GSMA-defined IPX requirements, this Common Functionalities and Capabilities document, and the respective Service Schedules provides a set of IPX requirements that can be implemented, including:

- An IPX architecture and reference model;
- IP routing and forwarding with the identification of the proper standard/coding for routing, addressing, marking the IP packet;
- Session-based signalling support, e.g. SIP-I and SIP;
- Media with a list of supported codecs and their respective features;
- Security;
- Quality of service (QoS) measuring model encompassing the parameters’ definition, guidelines for achieving these measurements, and their related metrics;
- Service Routing with the description and service impacts of the concepts of “confined routing” and “break-in/ break-out” scenarios.

Note that this document differentiates from that of the GSMA IPX requirements on some specific topics (such as break-in/break-out). However, this implementation specification document should not be considered as an alternative architecture with respect to the GSMA IPX model but as IPX Ps’ contribution with the objective to provide a detailed technical guidance for the implementation of IPX-based services.

Services offered via private interconnection and/or via the Public Internet remain a technical and commercial option outside the IPX environment, as per i3 Forum specifications [1], and SPs and IPX Ps are free to request and offer Internet-based services according their own policies.

The content of this document is based on the latest available version of the GSMA IPX specification. The i3 Forum is ready to update the content of the document in next releases following the GSMA specification updates.

2 Acronyms

ASP	Application Service Provider
BGP	Border Gateway Protocol
BFD	Bidirectional Forwarding Detection
CoS	Class of Service
DNS	Domain Name Server/Service
DSCP	Differentiated Service Code Point
ENUM	E.164 Number Mapping
EPS	Evolved Packet Sub-system
FNO	Fixed Network Operator
GSMA	GSM Association
GRX	GPRS Roaming eXchange
IANA	Internet Assigned Numbers Authority
IMS	IP Multimedia Subsystem
i3 Forum	International IP Interconnection Forum
IP	Internet Protocol
IPI	IP Interconnect
IPIA	IP Interworking Alliance
IPX	IP eXchange
IPX P	IPX Provider
IPsec	Internet Protocol Security
ISP	Internet Service Provider
ITU-T	International Telecommunications Union, Technical Working Group
KPI	Key Performance Indicator
MAP	Mobile Application Part
MD5	Message Digest 5
MNO	Mobile Network Operator
MPLS	Multi-Protocol Label Switching
MVNO	Mobile Virtual Network Operator
NDA	Non-Disclosure Agreement
NGN	Next Generation Network
NNI	Network to Network Interface
OSPF	Open Shortest Path First
PE	Provider Edge router
PHB	Per Hop Behaviour
PL	Packet Loss
QCI	QoS Class Indicator
QoS	Quality of Service
RFC	Request for Comments
RTD	Round Trip Delay
SBC	Session Border Controller
SDH POS	Synchronous Digital Hierarchy Packet Over Sonet
SIP	Session Initiation Protocol
SIP-I	SIP ISUP
SLA	Service Level Agreement
SP	Service Provider
SS7	Signalling System 7
TDM	Time Division Multiplexing
THP	Traffic Handling Priority
UE	User Equipment
URI	Uniform Resource Identifier
VLAN	Virtual Local Area Network
VoIPX	Voice over IPX
VPN	Virtual Private Network

3 References

[1] i3 Forum “Technical Interconnection Model for International Voice Services”, Release 5, May 2012

[2] i3 Forum White Paper “Voice Path Engineering in International IP based Voice Networks”, Release 3.0, May 2011

[3] i3 Forum “IP International Interconnections for Voice and other related services“, Release 3.0, June 2010

[4] i3 Forum “Routing and Addressing services for International Interconnections over IP”, Release 1.0, May 2010

[5] i3 Forum “ White Paper: Techniques for Carriers’ Advanced Routing and Addressing Schemes”, Release 1.0, May 2010

[6] i3 Forum “Technical White Paper on Security for IP Interconnections”, Release 1, May 2011

[7] i3 Forum “Interconnection IMS Signalling Profile”, Release 1.0, May 2012

[8] i3 Forum “Global SPID Whitepaper”, Release 1.0, May 2011

[9] GSMA IPXWP “IPX White Paper”, October 2006

[10] GSMA AA.80 “Agreement for IP Packet eXchange (IPX) Services”, Version 4.1, July 2011

[11] GSMA AA.81 “Packet Voice Interconnection Service Schedule to AA.80”, Version 2.1 and subsequent approved change requests.

[12] GSMA IR.34 “Inter-PLMN Backbone Guidelines”, Version 7.0, February 2012

[13] GSMA IR.40 “Guidelines for IPv4 Addressing and AS Numbering for GPRS Network Infrastructure and Mobile Terminals”, Version 7.0, September 2012

[14] IETF RFC 2328 “OSPF Version 2”, April 1998

[15] IETF RFC 2597 “Assured Forwarding PHB Group”, June 1999

[16] IETF RFC 3246 “Expedited Forwarding (Per-Hop Behavior)”, March 2002

[17] IETF RFC 3247 “Supplemental Information for the New Definition of the EF PHB (Expedited Forwarding Per-Hop Behaviour)”, March 2002

[18] IETF RFC 3261 “SIP: Session Initiation Protocol”, June 2002

[19] IETF RFC 3550 “RTP: A Transport Protocol for Real-Time Applications”, July 2003

[20] IETF RFC 3966 “The tel URI for Telephone Numbers”, December 2004

[21] IETF RFC 3986 “Uniform Resource Identifier (URI): Generic Syntax”, January 2005

[22] IETF RFC 4271 “A Border Gateway Protocol 4 (BGP-4)”, January 2006

[23] IETF RFC 5880 “Bidirectional Forwarding Detection”, June 2010

[24] IETF RFC 5881 “Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)”, June 2010

[25] ANSI T1.105 “SONET - Basic Description including Multiplex Structure, Rates and Formats”

[26] ITU-T Recommendation E.164 “The international public telecommunication numbering plan”, 1997

[27] ITU-T Recommendation G.707 “Network Node Interface for the Synchronous Digital Hierarchy(SDH)”, 01/2007

[28] ITU-T Recommendation Q.1912.5 “Interworking between Session Initiation Protocol and Bearer Independent Call Control or ISDN User Part”, 2004

[29] IEEE 802.3 “Telecommunications and Information Exchange Between Systems--Specific Requirements Part 3: CSMA/CD Access Method and Physical Layer Specifications”, 2008

4 Definitions

In this document the following definitions, discussed and agreed upon between GSMA, IPIA, and i3 Forum representatives in 2009, apply:

1) **IPX (IP eXchange)**: A private managed backbone providing guaranteed QoS, security and cascading payments. The IPX is a network of networks provided by the whole group of interconnected IPX Ps.

2) **Service Provider (SP)**: A business entity entering into a contractual relationship with IPX P(s) that offers services to final users providing termination (origin and destination) for IP services traffic. Thus, SPs include MNOs, FNOs (for example, fixed broadband operators and NGNs), ISPs, ASPs and similar entities.

   The business entity acts as an SP for its own contracted end users and those contracted through distribution entities with an exclusive commercial contract with the SP and that share the same access network of the SP (ex.: MVNOs).

3) **IPX Provider (IPX P)**: A business entity (such as an IP Carrier) offering IP interconnect capabilities to SPs, possibly through NNI with other IPX Ps for one or many IPX services compliant with the IPX operational criteria and compliant with the defined SLA and interconnect agreement for that end-to-end service.

4) **End-to-End (SP-to-SP)**: End-to-End means from SP premises to SP premises. Thus, SP core and access networks are excluded.

5 General Model & Architecture

5.1 Reference Business Framework

The IPX fulfills the following GSMA requirements:

1. Wide reachability: Allows an IPX P to provide services to any SP connected to the IPX domain and, provided certain conditions are met, any SP outside this domain (through break-in and break-out scenarios)
2. Security: Able to guarantee trusted communications.
3. Multiservice: An interconnection and services delivery solution supporting multiple services together, providing for economic efficiency, sustainability, and technically scalability
4. End-to-end QoS with cascaded responsibility: Able to support delivery of IPX Services with a controlled quality level by Service Level Agreements, tools, processes, and procedures agreed between all parties involved in the delivery chain.
5. End-to-end flexible payment models: Able to support different economic interconnection models and end-to-end business models, including those that need cascade payments.
6. End-to-end additional interconnection features: Able to support network transit features (i.e., routing, signalling interoperation, transcoding, addressing-portability-ENUM) as well as different arrangements for commercial agreements: bilateral and hubbing (multi-lateral relationship model, so an agreement with a hub is enough to terminate a service to and from multiple SPs).
7. Transparency: Able to support the capability and the willingness to disclose to other parties in the delivery chain, including SP, whether a terminating SP is compliant or not to the IPX Specification.

The specification is done from the point of view of a "Reference IPX P" that offers IPX features to a Customer SP for the interconnection of the IPX Services with its Target SPs, both for:

- Outbound traffic received from a Customer SP and routed through the Reference IPX P to the Target SP, possibly through another IPX P; and
- Inbound traffic received from a Target SP or possibly from another IPX P and routed through the Reference IPX P to the Customer SP.

The IPX interfaces (between two IPX Ps, or between an IPX P and an SP) are implemented commercially through bilateral agreements.

Figure 1 below provides a network reference model of the IPX domain, including compliant SPs, Non-Compliant SPs and IPX Ps.

Compliant SPs generate IP traffic towards IPX Ps across interfaces specified in Section 6. Each compliant SP can interconnect to one or more IPX Ps.

IPX Ps can implement both direct (i.e. bilateral) interconnections and shared (i.e. multilateral) interconnections. A shared multilateral interconnection can be implemented in private and/or public locations (i.e. telehouses/carrier hotels in the scope of this document) where IPX Ps can meet.

The private locations would be those set up by a group of IPX Ps and the public ones will be those created by a third party with open access to IPX Ps.

Note: in the GSMA IPX related documents, three public locations have been defined as private Peering Points (see 15Annex A - Architecture of IPX platform).

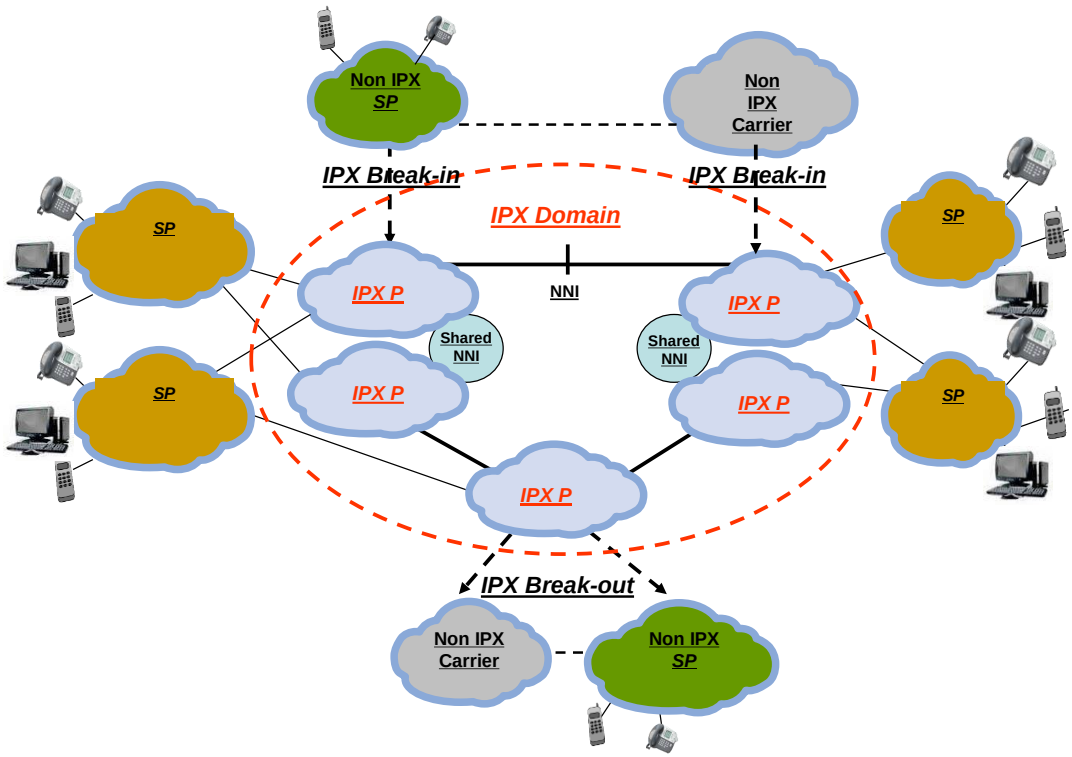

Figure 1: PX Domain Network Reference Model

5.1.1 Break-in / break-out

Allowing break-in/break-out via legacy networks, e.g. TDM and IP:

- Many destinations will remain reachable only via TDM and non IPX compliant IP connections for some considerable time. Not allowing TDM and IP break-in / break-out would exclude many destinations from a direct communication via the IPX domain and SPs would have to keep TDM interconnects operational in parallel to IPX-based interconnects in order to have access to these providers, and to receive calls from those SPs;
- Break-out / break-in NNIs support a faster deployment of IPX services as it breaks the dependency on all networks migrating to IP at the same time.

Break-in and break-out scenarios from both the SPs' and IPX Ps' perspective is allowed, and whether it will be used is dependent on market requirements.

The qualification process of carriers as IPX Ps as well as of SPs is outside the scope of this document. See also section 10.4.

5.1.2 Connectivity Options (as business models)

The IPX domain supports three commercial connectivity options: Transport Only, Service Transit and Service Hubbing. An IPX P is not obliged to offer all connectivity options.

Bilateral – Transport Only (transport without service awareness

According to GSMA IPX White Paper [9] section 6.2.1 *a bilateral connection between two Service Providers using the IPX transport layer with guaranteed QoS end-to-end. In this case, settlement is independent of the IPX Domain but connectivity still operates within IPI key business principles. Cascading of responsibilities (such as QoS) applies but not cascading of payments (Cascade billing).*

Note: the transport service will be addressed in an ad hoc Service Schedule.

Bilateral - Service Transit (transport with service awareness)

According to GSMA IPX White Paper section 6.2.2 *a bilateral connection between two Service Providers using the IPX Service layer and the IPX Transport layer with guaranteed QoS end-to-end. Within Service Transit, traffic is transited though IPX Providers but prices (termination charges) are agreed bilaterally between Service Providers and settlement of termination charges can be performed bilaterally between the Service Providers or via the IPX Providers (upon the Service Provider's choice).*

Multilateral - Hubbing (transport and hubbing with service awareness)

According to GSMA IPX White Paper [9] section 6.2.3 *a multilateral connection using Hub functionality: Hubbing/multilateral connectivity is where traffic is routed from one Service Provider to multiple destinations/Interworking partners through a single agreement with an IPX Provider. Cascading of responsibilities applies. Cascading of payments may be applied depending on the service.*

5.2 Reference Technical Architecture

The general IPX reference configuration is given in the following figure with two IPX Ps depicted.

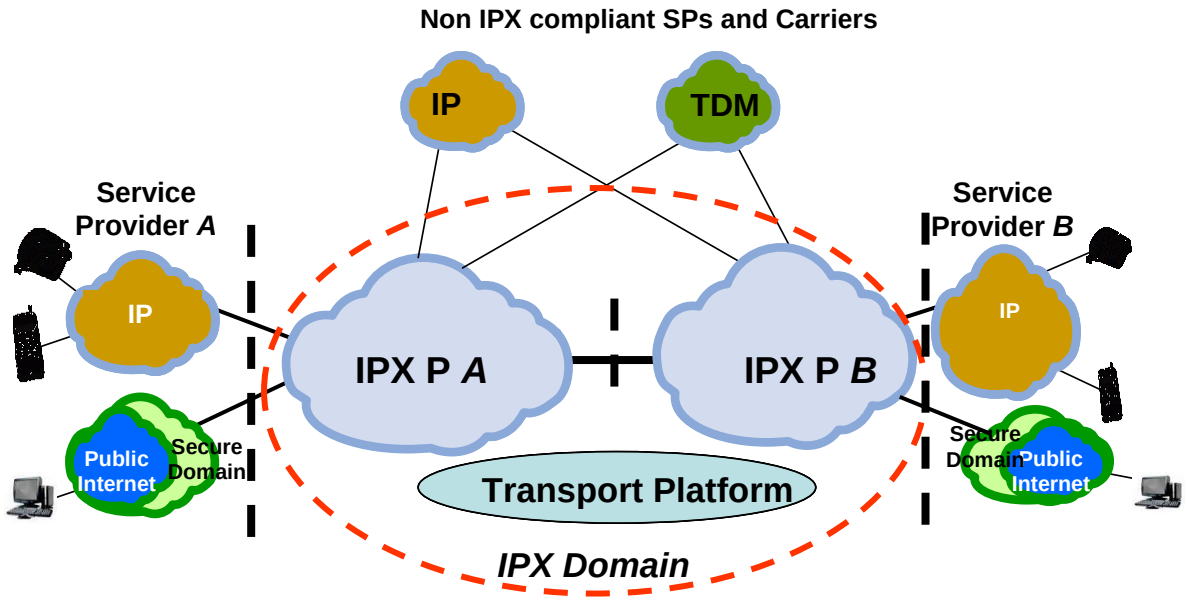

Figure 2: General IPX Reference Configuration

The IPX domain consists of all the IPX-P's networks and their interconnections. IPX Ps can connect to (non-IPX compliant) Carriers or SPs with the intent to either forward traffic (break-out) to destinations not reachable via the IPX, or to accept traffic destined to an IPX compliant SP (break-in). In both cases,

the rules of cascading responsibilities, QoS and security are defined by the service characteristics of the break-in/out SLA. Further details can be found in section 10.4.

Different types of transport functions for the interconnection of SPs with IPX-Ps, and between IPX-Ps are given in Section 7.

The geographical scope of the IPX domain is given in Fig. 2 . The end-to-end interconnection scope spans from egress port of the interconnecting element of the originating SP network towards its own IPX P, to the ingress port of the interconnecting element of the terminating SP (i.e. from SP to SP).

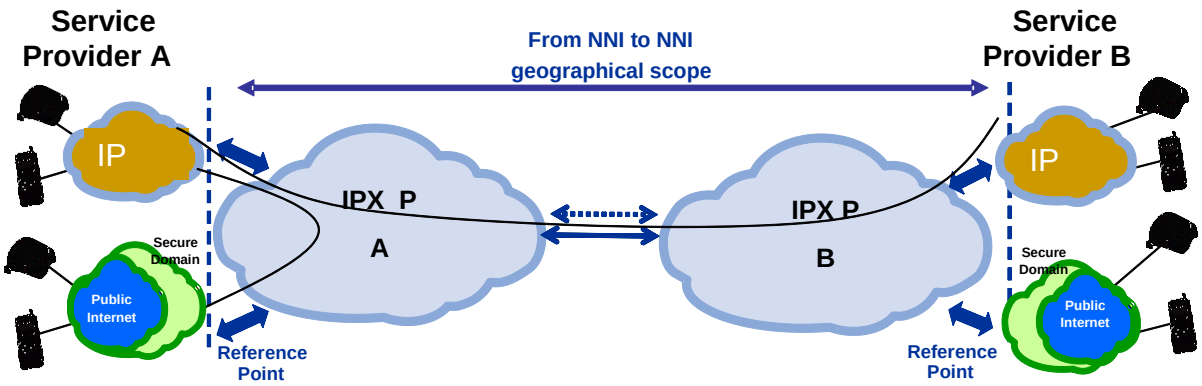

Figure 3 - Geographical scope of an IPX communication

The following basic requirements apply**:**

- More than one IPX P can be involved in the end-to-end (SP-to-SP) connection
- IPX being a multiservice platform, the interconnection functions are intended to be multiservice, capable of providing multiple quality levels and modular (i.e., some functions are not needed for specific service models and/or specific end-to-end services)
- The interconnection functions are intended to provide a “private communication path” (i.e., separated and protected from the Public Internet)
- Security functions shall be implemented among interconnection functions.
- The entity that provides the interconnecting physical line between SP and IPX P is responsible for ensuring the SLAs for that physical line (as described in AA.80 [10] annex 8)

6 IPX Agreements

Interconnected IPX-Providers have to enter into an IPX agreement describing common functionalities and capabilities as well as specific service schedules per service.

These agreements are the basis for a seamless service experience for Service Providers throughout the IPX domain, e.g. SLAs on technical performance or cascading charging process.

The recommended key parameters of such agreements will be included in future i3forum deliverables.

7 Transport Functions

This section recommends alternative transport configurations for implementing the NNI between a SP and an IPX-P or between two IPX-Ps.

Assuming the IPX domain as a global private infrastructure, interconnecting managed IP networks, carrying different types of traffic, the interconnections between these networks shall be private, i.e. no unidentified third parties are able to affect the service.

In order to retain the private interconnection feature the following conditions have to be satisfied:

- Only IPX services are exchanged across the respective NNI.
- All the involved IP addresses in the IPX address space (i.e., *PE router* interface, *P router* interface, border function interface) cannot be reached from unidentified entities via Public Internet and, as defined in GSMA IR.34 [12] have to be public, but they shall neither be announced onto nor be reachable from the Public Internet.
- The traffic, from the PE router to the border functions in a IPX P's or SP's domain, shall be secured, either physically or logically, from Internet Transit traffic.
- This security can be achieved:
  - **Physically**: by implementing separated and dedicated networks for the two types of traffic.
  - **Logically**: implementing different mechanisms such as MPLS/Virtual Private Network (at layer 2 and 3) or IP Sec tunnelling.

7.1 Generic Cases of Transport Configurations

7.1.1 Case 1- Layer 1 interconnection

In this configuration a dedicated physical link (provided by one involved operator (IPX P/SP), or by the two involved operators, or by an identified third party) is implemented between PE routers or layer 2 switches, or directly between border functions.

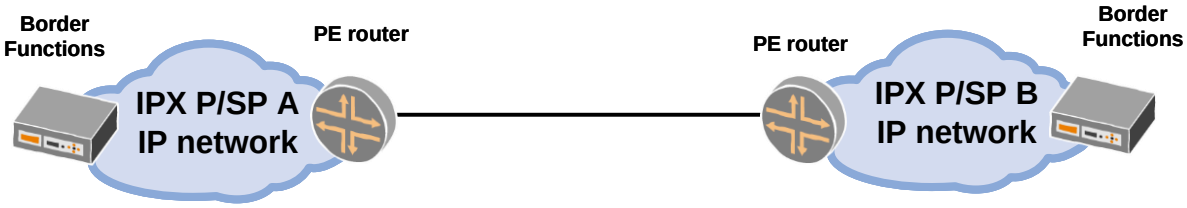

Figure 4 - Layer 1 Private-oriented Interconnection Configuration

7.1.2 Case 2- Local Layer 2 interconnection

In this configuration a dedicated physical link (provided by one involved operator (IPX-P/SP), or by the two involved operators, or by an identified third party) is implemented between PE routers or layer 2 switches, or directly between border functions passing through an Ethernet switch network run by a third party (e.g., telehouse/carrier hotel owner, Internet Exchange Point owner). The switch provider will assign specific *VLAN*s for each interconnection allowing for the aggregation of several interconnections over the same physical link.

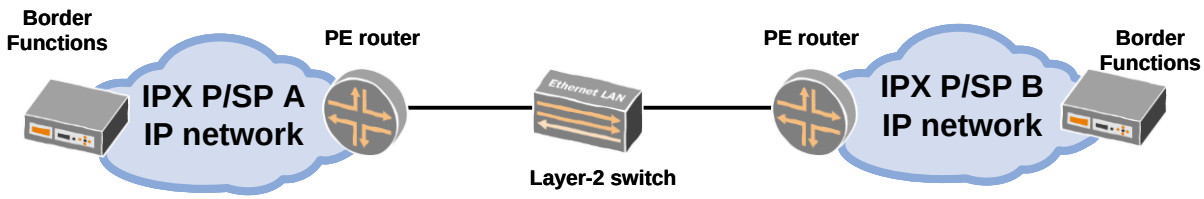

Figure 5 - Layer 2 Private-oriented Interconnection Configuration

A shared interconnection (see section 5.1.2) is a special case of this model in which multiple carriers are interconnected in the same layer 2 network as is described in [12] section 6.4.

7.1.3 Case 3 - Layer 3 interconnection via Public Internet

As a special case, in this configuration, an SP is connected to an IPX P via the Public Internet using either IPv4 or IPv6 by means of a VPN and using IPsec encryption for data services and signalling for session based services.

In agreement with GSMA IR.34 [12] this configuration should be used in case the previous configurations cannot be implemented due to technical and/or commercial reasons and it should never be used to interconnect two IPX Ps. Access connections over public Internet with IPsec are classified as break-in/out SP.

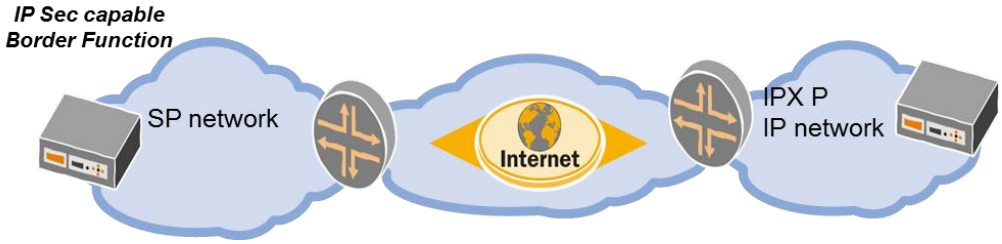

Figure 6 - Internet IP Sec SP/P Interconnection Configuration

7.1.4 Applicability

Referring to the cases above, the following transport configurations can be implemented:

	SP – IPX P interface	IPX P – IPX P interface
Case 1	Yes	Yes
Case 2	Yes possibly via a 3rd party interconnect location (see annex A).	Yes, possibly via a 3rd party interconnect location (see annex A). This Ethernet connection should physically be a local (or at most metropolitan) Ethernet interconnection. If this connection were to have a greater distance, its impact on the overall end-to-end QoS would be significant and this connection would become itself an IPX provider network.
Case 3	Yes	No

In all cases, it is desirable that the physical or virtual link interconnecting a SP with an IPX P to be as short as possible in order to minimise delay and in general to make the QoS monitoring processes simpler and representative of the SP-to-SP quality and end-user experience.

7.2 Physical Interconnection Alternatives

The physical interface of the interconnection can be SDH POS – based, or Ethernet-based (i.e., fast-Ethernet, gigabit-Ethernet or 10gigabit-Ethernet).

7.2.1 SDH-based transport Systems

The ITU-T Recommendations G. Series shall be considered as reference documents, among these the ITU T Recommendation ITU-T G.707 [27].

For North America another reference document is ANSI T1.105 [25].

7.2.2 Ethernet-based transport Systems

The IEEE recommendations 802.3 [29] for Ethernet communication together with enhanced Ethernet technologies such as fast-Ethernet, gigabit-Ethernet and 10gigabit-Ethernet have to be considered (e.g. ISO/CIE 8802-3).

7.2.3 Interconnection redundancy

The level of redundancy of a specific interconnection can be enhanced by increasing the number of involved Border Functions. Additional redundancy can be achieved by increasing the number of involved PE routers by geographical separation.

7.3 VLAN

VLAN multiservice sharing configuration at the interface between two IPX Providers will be defined in the corresponding Service Schedule for each type of traffic, and the bandwidth of each VLAN is not segregated and can fill the bandwidth of the physical link. It is strongly recommended to follow the same configuration at the interface between a Service Provider and an IPX Provider.

7.4 Internet Protocol

Bilateral IPX interconnections may occur using either IPv4 or IPv6 network protocols; in the context of this document IP refers to both IPv4 and IPv6 protocol versions.

There are currently no generally deployed solutions that allow transparent interworking between these two IP protocol versions. Therefore the scenarios described within this section can use either IPv4 or IPv6 protocol versions but versions cannot be mixed on the same logical interconnect; both parties in the interconnection shall be using the same protocol version. Border Function within each IPX Provider network will require to be able to perform interworking between logical interconnects operating on IPv4 and IPv6.

7.4.1 IP Addressing

The IPv4 addressing scheme shall be supported. The IPv6 addressing scheme is optional and can be agreed on a bilateral basis.

For the IPX address space IPX Ps will use only IP addresses assigned by IANA or related bodies as described in [13].

7.4.2 IP Routing

For all the above interconnection configurations, it is mandatory to announce only those IP addresses that need to be reached by the interconnecting IPX P.

The BGP protocol v4 should be used to exchange routes between different networks (both SP and IPX–P).

GSMA IR.34 [12] defines the use of specific BGP communities. The use of this capability does not make void the IPX definition and implementation as defined in this document.

It is recommended to tune timer parameters to appropriate values for the specific implementation, to ensure timely failure detection and convergence suitable for traffic. In addition, BFD [23][24] could also be used to speed up link failure detection and subsequent protocol convergence.

7.4.3 Classes of Service

Classes of Service are defined by means of DSCP marking, as defined in GSMA IR.34.

In IR.34 [12] section 6.2.6 the following traffic classification is described:

EPS	QoS Information			IP transport	
QCI	Traffic Class	THP	Signalling indication	Diff serv PHB	DSCP
1	Conversational	N/A	N/A	EF	101110
2					
3					
4	Streaming	N/A	N/A	AF41	100010
5	Interactive	1	Yes (see note)	AF31	011010
6			No	AF32	011100
7		2	No	AF21	010010
8		3	No	AF11	001010
9	Background	N/A	N/A	BE	000000

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.

DSCP marking at the interface between two IPX Providers will be defined in the corresponding Service Schedule for each type of traffic. It is strongly recommended to follow the same configuration at the interface between a Service Provider and an IPX Provider.

Within its own network, the IPX Provider is free to implement as it wants.

8 Signalling

For session based services, the signalling protocol in the IPX is SIP, including its different flavours, such as SIP-I. Details of the protocol can be found in each service schedules.

Some services may also make use of additional signalling protocol, including Diameter.

Legacy services rely on existing solutions. Refer to the service schedules for details.

9 Media/Data

Refer to the service schedules for details.

10 Routing & addressing

10.1 General Service Routing Principles

The network reference model depicted in Figure 1 shows IPX compliant SPs and IPX Ps as well as non-compliant SPs and Carriers. Because of the quality, security, and efficiency benefits of the IPX interconnection model, intra-IPX domain routing should always be the default routing option, with the exception of the following two scenarios:

- Business Agreement: A service request, e.g. a call, has to be routed towards a non-compliant carrier per agreement with between an SP and IPX P;
- Failover: A service request, e.g. a call, has to be routed towards a non-compliant carrier in because there are no available network resources within the IPX Domain that allow for the service request to be completed.

10.2 Number of IPX Providers in the SP-SP communication

The GSMA IPX [12] requires that not more than 2 IPX–Providers be involved in the SP-SP (end–to–end) communications, unless otherwise addressed by a specific GSMA Service Schedule., i3Forum recommends no more than two, but accepts more than 2 as long as this is disclosed to the customer and not service-affecting (unless commercially agreed).

10.3 Routing Transparency

The minimum set of information that the IPX P shall provide to the SP consists of the type of connectivity used to reach each terminating SP. These connections have to be classified into three groups depending on the nature of the connectivity:

- Direct connectivity: Only one IPX P from Originating SP to terminating SP,
- Indirect connectivity: More than one IPX P from originating SP to terminating SP,
- Break-out connectivity (or gateway connectivity) between the IPX Domain and the Non-IPX Domain.

The above information is provided in the commercial agreement between the IPX P and the SP and applies under normal operating conditions (i.e. no network failures and/or no network congestion).

10.4 Break-in / break-out connectivity and notification

10.4.1 Break-in / break-out connectivity options

IPX domain break-in and break-out can be implemented towards a SP and/or Carrier via service specific “break-in/out gateways” supporting three types of access technology options:

1. TDM interconnection
2. Private IP interconnection as defined in section 6 of this document. In this case, notwithstanding no identified third party is able to affect the service, other IPX requirements are not met.
3. Public IP access interconnections provided that:
    - All the traffic, entering the IPX P’s network, crosses IPX P’s border functions.
    - All other security requirements given in this document as well as in the relevant service schedule are met

10.4.2 Break-in / break-out notification

All SPs interconnected to the IPX domain via Public Internet in compliance with the access configuration described in section 6.3.1 have to be advertised to other SPs as break-in sources / break-out destinations.

All SPs and Carriers interconnected as described in section 9.4.1 have to be advertised to other SPs as break-in sources / break-out destinations.

10.5 Role of DNS and ENUM registry

GSMA IR.67 provides guidelines for DNS and ENUM in the GRX and IPX architecture. As defined in IR.67 DNS on the GRX and IPX backbone is completely separate from DNS on the Internet.

i3 Forum recognises that DNS/ENUM structure and capabilities can be used for addressing and routing purposes but, many different solutions are already in the market for providing routing and addressing capabilities to IPX Ps. Furthermore, these solutions are based on DNS/ENUM technology as well as other technologies (e.g. SS7/MAP protocol, SIP Re-direct protocol, Diameter protocol).

It is envisaged that advanced routing and addressing schemes (complementing ITU-T E.164 model or alternative to ITU-T E.164 model) will develop in the future and two i3 Forum deliverables ([4] and [5]) contain the first principles to be considered and the first guidelines to be followed. In any case, regardless the technical and market evolution, an IPXP has the right to select its own technical and commercial solution in order to successfully and appropriately route service requests.

10.6 Numbering and Addressing Scheme for E.164 number-based services

E.164 numbers are used as destination addresses for a number of services, such as voice, RCS, SMS. Using SIP, these numbers shall be used in telURI and SIP URI formats.

10.6.1 Tel-URI Addressing scheme

A tel-URI shall conform to IETF RFC 3966 [20], which state that global unique telephone numbers are identified by a leading “+” character so E.164 based addressing used in SIP INVITE message shall be as follows:

1. For geographical areas:	+CC NDC SN	maximum 15 digits.
2. For global services:	+CC GSN	maximum 15 digits.
3. For networks:	+CC IC SN	maximum 15 digits.
4. For groups of countries:	+CC GIC SN	maximum 15 digits.
An example of a tel-URI would be:	tel:+14085551212	

10.6.2 SIP-URI Addressing scheme

A SIP-URI shall conform to IETF RFC 3986 [21]. In order to setup an international voice call, the telephone number used in the SIP-URI shall be a valid E.164 number preceded with the “+” character and the user parameter value "phone" should be present as described in RFC 3261 [18] section 19.1.1.

An example of a SIP-URI would be: sip:+14085551212@domain.com;user=phone

10.6.3 Number Portability Resolution

GSMA IPX requirements indicate that the Service Provider to which the IPX-P terminates a call should not have to transit the call to another provider. Number portability complicates the satisfaction of this requirement. The i3 Forum Services WS [8] has also provided a requirement for number portability resolution by IPX-Ps.

GSMA plans for number portability resolution in the IPX based on the implementation of a global IPX ENUM system. Prior to the point at which this is achieved, IPX-Ps will need to make use of other methods for number portability resolution. These may include (but are not limited to):

- Queries of national number portability databases where they exist and where the IPX P has access to them
- Use of third party number portability resolution services
- Use of resolution service provided by the number block holding SPs

However, in the interim it is possible for an IPXP to send traffic to an SP, who, if needed, will transit the call to the recipient domestic SP.

10.7 Other Addressing schemes

Other addressing schemes may be used as defined in ad hoc Service Schedules.

11 Security

11.1 General

This section discusses the generic recommendations for security of interconnections to the IPX platform. Specific recommendations can be found in the respective Service Schedules.

For more information please refer to the i3forum – Technical White Paper on Security for IP Interconnections [6].

Any function processing traffic at the entry of the IPX network, and ensuring the right security level is called the Border Function in this document. Basic examples of possible Border Function include firewalls and SBCs.

To increase security, there are mechanisms recommended at the IP layer, such as access control lists, selective BGP announcements and BGP neighbour authentication encryption using MD5. In addition, IPX security is improved by the following methods:

- Isolation From the Public Internet within the IPX domain. In case of access configuration via public Internet, and in case of break-in/break-out, the IP addresses have to be advertised and security mechanisms have to be implemented [6][6].
- Separation of Traffic by IP Addressing
- Use of Proxy

Depending on the service, additional security features may be provided. They are described in the relevant Service Schedules.

11.2 Isolation From the Public Internet

From an IP routing perspective, the IPX has to be isolated from the public Internet, not advertising the related IP addresses to the public Internet.

Using only IANA registered IP address ranges, as defined in IR.40, we can prevent unidentified access ensuring only traffic from a valid IP address ranges can reach SPs and other IPX Ps. The use of private address space is not allowed.

11.3 Separation of Traffic by IP Addressing

This function is a recommendation for the SP, as the IPX P is not in control.

The IP addresses of the IPX shall not be advertised to the end user.

By keeping Infrastructure and UE IP ranges separate, 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 [IR.40], reducing the potential for an attack initiated from end users and subscribers.

11.4 Use of Proxy

Black and white lists provided by the SP shall be used by the IPX P to implement admission control of sessions from other SPs. Also, the IPX P shall block user plane traffic not related to on-going control plane sessions.

Note: some services may not allow the SP to define black and white lists. This will be reflected in the appropriate Service Schedule.

12 QoS Measurement

i3 Forum recognises a trend in the wholesale industry which calls for quality monitored and controlled services both from FNOs and MNOs Service Providers. This trend gets its most significant validation from the IPX (IP eXchange) model conceived and designed by GSMA.

GSMA, for the voice service over an IPX platform, identifies in AA.81 [11] the need:

- to measure and report the service-level KPIs
- to measure and report transport-level KPIs for packet loss, packet delay and packet jitter; the measurement is for the whole IPX Provider domain, i.e. from the first equipment in the IPX Providers network facing the originating Service Provider, to the last equipment in the Carriers network facing the terminating Service Provider.

  Note: SLA may also include the local tail, or not. This is a commercial decision for the IPX Provider – Service Provider relationship.

  Note: the service schedule may specify other measurement locations, e.g. when measurement is performed at the Border Function itself.

- to carry out the above measures following the forwarded path (dictated by the service) and not the shortest path driven by OSPF / BGP / other IP routing protocols; [14][22]

The figure below describes the reference configuration for QoS measurement.

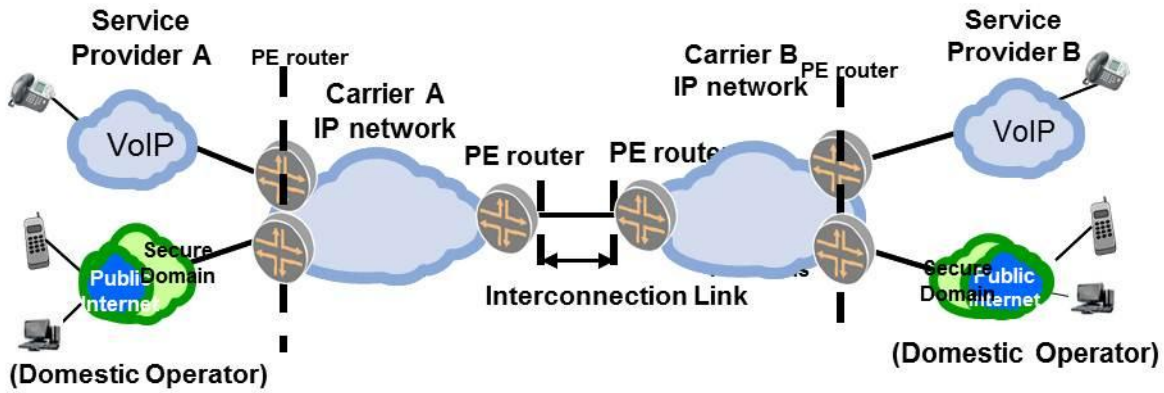

Figure 7: Reference configuration for QoS measurement

This section describes the transport QoS parameter definitions, their measurement configurations and KPI calculations pertaining to the international interconnection between IPX Ps and between IPX Ps and SPs. Additional specific QoS parameters can be found in the respective Service Schedules.

KPIs are defined for the purpose of:

- Monitoring (supervision) against pre-set thresholds
- SLA compliance and QoS reporting for IPX P to IPX P interconnections and IPX P to SP interconnections.

SLAs only apply provided that the load over the originating and terminating SP interconnections do not exceed a threshold as recommended by the GSMA. Any commercial agreement associated with SLA and/or QoS reporting is outside the scope of this document.

12.1 QoS parameter definitions

There are two categories of QoS parameters: transport QoS parameters; and service-level QoS parameters.

- Transport parameters
  - Round-Trip Delay (RTD): RTD is defined as the time it takes for a packet to go from one point to another and return
  - Jitter: Jitter is the absolute value of differences between the one-way delays of consecutive packets
  - Packet Loss: Packet loss is the ratio between the total lost packets (= total sent – total received) and the total sent packets over a given time period
- Service parameters are specific to each service, and described in the respective ad hoc Service Schedules.

Other parameters may be measured by IPX P and are out of scope of this document.

12.2 Implementing GSMA quality requirements

12.2.1 Transport and Service Parameters

The above described requirements call for the ability to measure the identified transport parameters for a specific segment reporting the collected data to the SP. This implies the need to:

- Measure the identified parameters for the identified end-to-end domain across downstream network(s) for QoS reporting;
- Analyse the call flow in order to locate and isolate faults.

When there are more than one IPX Ps involved in the end-to-end path, it is generally not possible to directly measure the end-to-end KPI. Instead, it is proposed that each IPX P will measure the performance of its own network, and measurements will subsequently be aggregated to reflect the end-to-end performance. As an example, in the figure below two IPX Ps are connected with the objective to produce an end-to-end report for originating SP-A across IPX Ps A and B.

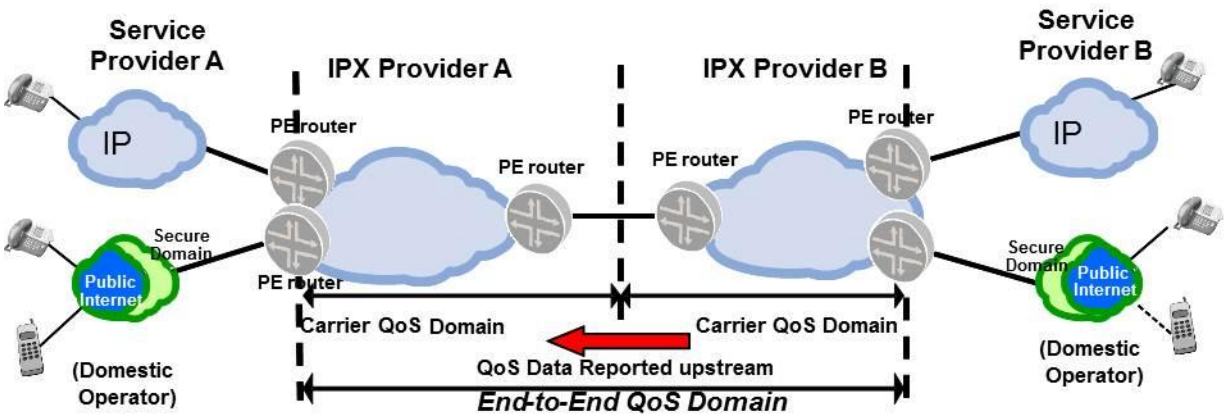

Figure 8: Aggregation based approach

The IPX P delay on the NNI between two IPX Ps in this document is assumed to be negligible because IPX Providers, in the vast majority of the cases, interconnect in TeleHouses / Carrier Hotels. If this condition is not met the transmission delay has to be added and considered an offset.

The performance across two domains is estimated by aggregating the performance across each domain. This can be computed as follows:

- Delay: each segment is measured by the IPX P. The total delay is estimated by adding up the delay over each domain.

With regard to delay measurements and reference values listed in IR.34 Sec. 6.3.2, i3f suggests that these values be reviewed and possibly updated for consistency.

- Loss: each segment is measured by the IPX P. The total Packet Loss is estimated by calculating the complement of the joint probability of a successful transmission on both networks:

  Packet Loss end-to-end = [1- (1- PL1)* (1-PL2)]

  where PL1 is the Placket Loss of the 1st network for the measured route

  and PL2 is the Packet Loss of the 2nd network for the measured route

- Jitter: no aggregation scheme can be applied since there is no mathematical model which can correlate the jitter data measured by each network in the end-to-end domain. Notwithstanding this technical difficulty, it is suggested the jitter measured by the last domain is passed to the originating Service Provider, since this measurement is the closest to the end of the IPX Providers' domain.

With regard to the measurement process of above parameters, there is a difference in the measured values for the two transmission directions due to different operating conditions of the crossed network equipment. This difference can be considered negligible for a symmetric path across the IPX domain (i.e. the two transmission paths follow the same route) but for specific cases, such as intercontinental communications, this difference could be significant.

It depends on the specific service to be provided whether this difference has to be retained in the SLA between SP and IPX P.

Consensus is required from the involved IPX Ps in order to report the requested QoS data to the originating SP. Multiple ways can be adopted (e.g. secure ftp, download and import from web portal) and IPX Ps are free to agree the most suitable way provided that security and integrity of the data is preserved.

12.2.2 Service parameters

The Service-level parameters of the downstream segment (from the interface between the originating SP / IPX Provider to the final user) can be affected by the quality of the terminating Service Provider network.

12.3 KPI computation for SLA / QoS reporting

As a general principle each IPX P can offer KPIs of QoS parameters according to its own commercial policy.

Let:

- T be the reporting period (e.g. T = one month)
- i be the index of the suite of measurements by the Border Function and/or probes and/or Call Handling Function (as applicable)
- KPIi be the measured value of the i-th sample for the considered KPI (e.g. RTD)
- N be the number of measurements over the period T (*i*=1..N)

KPIs are averaged values over a time period, the length of which is outside the scope of this document.

Generally speaking, the reported KPI is obtained as a function of all the measured samples $KPI = f(KPI_0, KPI_1,..., KPI_N)$. The following functions are suggested:

- RTD: 95 / 99 % percentile or average
- Packet loss: 95 / 99 % percentile or average
- Jitter: 95 / 99 % percentile or average

Note: as far as the above transport parameters are concerned, it has to be noticed that, from a commercial perspective, the function "*average*" is the preferred option.

12.4 QoS Enforcement

There are two possible general methods for QoS enforcement. Service schedules may give additional details.

- Enforcement through fault management.

  A QoS problem is raised upon SP Customer request: it is the responsibility of the SP to initiate a QoS problem request by opening a trouble ticket with its IPX P. The IPX Pand the SP customer will then work together to verify if there is an end-to-end QoS fault. For instance SP-A can open a trouble ticket to IPX P A and report that the commitment has been violated. In such case IPX P A will start troubleshooting within its own network and with IPX-P B's network. Each IPX P must at least offer this QoS cascading method. If the problem is identified, and if the repair duration is above the limits set in the SLAs, then the IPX Ps must pay the penalties negotiated in each SLA.

- Enforcement through constant monitoring and reporting of QoS and SLA values.

  In this option both IPX-P A and IPX-P B constantly measure the QoS in their network (RTD and PL per CoS) and report these values to their respective customers on a monthly basis. Alternatively, IPX Ps can also consistently monitor end-to-end RTD and PL between all end-to-end routes combinations sold to its customer (SPA to SPB, SPA to SPC, SPB to SPC etc). This last option can be very difficult to manage and not fully scalable for hundreds of routes. This solution is only optional and it is up to each IPX P to decide to offer it for one or several routes.

12.5 Penalties

This section provides an example of the penalty cascading principle, in the context given in Figure 7. Assuming that the end-to-end RTD or Packet Loss between the SP A PE and SP B PE is above the SLA negotiated by IPX-P X and SP A.

- IPX-P A must pay the penalties described in the SLAs with SP A, regardless of where the network problem is.
- If the network fault is within IPX-P A network, IPX-P A must bear all penalties on its own, no cascading.
- If the network fault is within IPX-P B network, then IPX-P A can request IPX-P B to pay penalties to IPX-P A as per the SLAs between IPX-P A and IPX-P B. To be noted that it is the commercial responsibility of IPX-P A to ensure (or to bear the risk) that SLAs negotiated with IPX-P B are consistent with IPX-P A SLAs negotiated with SP A.

However, it is matter of the bilateral discussion between parties to agree on the applicability of a penalty scheme.

13 Accounting principles

See also section 5.1.

13.1 Transit fee

Transit fee is defined as the compensation to the IPX P for network, connectivity, and service fulfilment services, excluding termination fees. Transit fees can vary depending on the service being facilitated as well as the destination.

13.2 Charging transparency

An IPX P is not obliged to provide separation of termination rate and transit fee unless commercially negotiated.

Separation of termination and transit fees is also omitted if disclosure of termination rates is not allowed by NDA or otherwise.

14 Operational Practices

This section contains some basic operational practices related to the provision of IPX services to Service Providers or between IPX Providers.

1. *Post-sale and provisioning process*:
    - Network design consolidation;
    - Network provisioning;
    - Service testing;

   have to be completed in a timely manner per contractual agreement.

2. *Trouble shooting and first level support*– It is recommended that each IPX Provider operates a central ticket/fault reporting process to ensure that each network issue is properly identified and escalated to the proper support team internally, to the customer Service Provider or to other IPX Providers, as needed. This customer service/fault desk shall be able to quickly identify the interconnection between SP – IPX P or between IPX Ps and review all network elements and devices to properly diagnose the issue and then transfer to the appropriate support team.
    - Team shall be available 7x24 with phone, fax and email access
    - Team shall have access to all relevant reports and alarms related to the network and IPX connections (IP, voice, signalling)
    - Team shall be trained on IPX

3. *2nd and 3rd level support* – The first level technician should have the tools and knowledge to properly diagnose the issue. Once that has taken place, if needed, they should escalate and transfer tickets to the correct internal support group responsible for the service or application (data/IP, Voice, signaling, etc).

4. *Reporting and communication*
    - Web portal: it is suggested that an automatic web portal be operational in order to facilitate the exchange of information between IPX P and SP and between IPX Ps. Typical data to be provided are QoS data, traffic exchanged, ASR, ALOC and other telecom measurements as well as planned outages and status of tickets. This portal can also be used to open up new capacity or network modification orders once commercially agreed.
    - Communication of tickets and status updates: it is suggested to have a process in place on how to communicate the status back to your IPX or SP partner. The first level support technician should be the primary lead on status updates related to the reported faults or network change requests. A streamlined approach will ensure that the communication reaches the IPX or SP partner correctly.

5. *Routing:* an IPX routing plan distinguished from the one for non IPX services shall be implemented. Break-out destinations can be routed according to the standard routing plans.

15 Annex A - Architecture of IPX platform

15.1 Reachability / Coverage: interconnection obligations for IPX Providers

Every IPX Provider will provide the list of SPs that can be reached through the IPX domain by an SP contracting it (with connectivity information as defined in 9.3). An SP may connect/contract more than one IPX Provider in order to reach all SPs that it is interested in by combination of the list of SPs of those IPX Ps.

In order to ensure that the IPX service develops in a way that is consistent with its core requirements of efficiency, QoS and security, it is important that a framework is defined that enabled IPX Providers to efficiently establish interconnection arrangements with other IPX Providers, in a manner that both minimises the physical distance that traffic has to travel between Service Providers, and is commercially sustainable to IPX Providers.

15.2 Public Interconnect Locations

It is expected that the IPX will re-utilise Interconnect locations that have already been established for GRX (IPX Zone Interconnect Locations in the following Table), as the IPX/GRX DNS has been deployed at these locations and it also minimises additional investment costs from IPX Providers.

IPX Zones	Shared Interconnection Location	Regions in each IPX Zone
Americas	Equinix Ashburn	North America (East Coast), North America (West Coast), Central America (incl. Caribbean), South America
Asia	Equinix Singapore	East Asia, South Central Asia, South East Asia, West Asia, Oceania
Europe & Africa	AMS-IX Amsterdam	West Europe, North Europe, East Europe, south Europe, Africa

Note: for the list of countries in each region please refer to section 6.3.2 of IR.34 [12].

i3f acknowledges the GSMA selection of the existing GRX interconnect locations but outlines that some delay requirements cannot always be met based on just these locations (e.g. communications within Africa, Latin America, Middle East).

IPX Provider Interconnection Evolution

In order to assure DNS resolution, an IPX Provider may initially have to connect to one of the above IPX Zone Interconnect Locations to enable it to offer an IPX Service to any of its perspective Service Providers.

When the IPX Provider has ten or more Service Providers within an IPX Zone, it shall interconnect in that zone to the other IPX Providers who are present at that IPX Zone, subject to the other IPX Provider(s) having at least 10 Service Providers in that same IPX Zone.

It should be noted that IPX Providers are free to negotiate Private Interconnection Terms with other IPX Providers in an IPX Zone, as it may be more efficient for an IPX Provider to do this rather than connect to the IPX Zone Interconnect Location.