International Interconnection forum for services over IP
(i3 Forum)

(www.i3 Forum.org)

Workstream "Technical Aspects"

Technical Specification for
Voice over IPX service

(Release 1.0, October 2010)

Executive Summary

In line with market trends which call for reliable, trusted, secure and quality controlled international voice service—i3 Forum Carriers endorse such a service evolution releasing this document as an implementation specification for the voice service within the framework of IP Packet Exchange (IPX) model conceived and specified by GSMA.

It is well known that the GSMA model defines the IPX as a global, trusted and controlled IP backbone, consisting of a number of competing IPX carriers (IPX Providers) that will interconnect Service Providers according to mutually beneficial business models.

In this scenario, the following needs/requirements can be recognised for the provision of voice over IPX services:

from Service Providers, as the entity offering services to final users, needing guaranteed quality (reliable and secure) IP-based services towards corresponding (terminating) Service Providers,

from Carriers (IPX Providers), as the entity offering interconnection services, serving any IPX compliant SP at the proper level of technical and economic efficiency,

with the common objective to implement a service and technical architecture that is business-sustainable for both Service Providers and Carriers.

This document, assuming and endorsing the basic GSMA technical / commercial requirements:

- focuses from the business perspective on the Multilateral Hubbing connectivity mode;
- provides a set of specifications which can be implemented achieving the basic requirements of GSMA IPX model for areas such as:
  - IP routing with the identification of the proper standard/coding for routing, addressing, marking the IP packet;
  - Signalling with the support of SIP-I (specified by ITU-T) and SIP (specified by IETF) signalling protocols;
  - Media with the listing of the codecs, and their features, to be used for narrowband, wideband and low bit rate communications;
  - Security with the support of the capabilities to be provided by Border Functions;
  - Quality of service control with the support of a comprehensive model encompassing the parameters' definition, their measurement process and proposed metrics;
  - Service Routing with the description and service impacts of the concepts of "confined routing" and "break-in/ break-out";
- differentiates from current GSMA specification on some specific topics which have been matter of analysis and study between MNO representatives and i3 Forum carriers in the past months.

Services offered via private interconnection and/or via the Public Internet remain as a technical and commercial options outside the IPX environment, as per i3 Forum specifications [*i3 Forum , "Technical Interconnection Model for International Voice Service", Release 3, May 2010*], and Service Providers/Carriers are free to request/offer Internet-based services according 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 (Carriers) are free to request / to offer the model more suitable for their own commercial / technical policies.

The content of the document is based on version June 2010 of the GSMA IPX specification. i3 Forum Carriers are 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

In line with market trends—which call for reliable, trusted, secure and quality controlled international voice service—i3 Forum Carriers endorse such a service evolution releasing this document as an implementation specification for the voice service within the framework of IP Packet Exchange (IPX) model conceived and specified by GSMA [10].

The GSMA model establishes the IPX as a global, trusted and controlled IP backbone that will interconnect Service Providers 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 [10]. The IPX environment will consist of a number of IPX carriers (IPX Providers) in competition, selling interconnect services to Service Providers. The IPX Providers' networks will be mutually interconnected where there is demand by Service Providers.

In the above scenario, the following needs/requirements can be recognised for the provision of voice over IPX services:

From Service Providers, as the entity offering services to final users, needing guaranteed quality (reliable and secure) IP-based services towards corresponding (terminating) Service Providers, using modular and transparent interconnection and functions provided by IPX Providers, in a global private network, and

From Carriers (IPX Providers), as the entity offering interconnection services, serving any IPX compliant SP at the proper level of technical and economic efficiency by means of the designing, implementation and operation of multi-service converged platform(s) for all types of IPX services,

with the common objective to implement a service and technical architecture that is business-sustainable for both Service Providers and Carriers.

As a result, 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, assuming and endorsing the basic GSMA technical / commercial requirements:

- focuses from the business perspective on the Multilateral Hubbing connectivity mode;
- provides a set of specifications which can be implemented achieving the basic requirements of GSMA IPX model for areas such as IP routing, signalling, media, security, quality of service control and service routing;
- differentiates from current GSMA specification on some specific topics which have been matter of analysis and study between MNO representatives and i3 Forum carriers in the past months.

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 Service Providers/Carriers are free to request/offer Internet-based services according their own policies.

The content of this document is based on the version June 2010 of the GSMA IPX specification. i3 Forum Carriers are ready to update the content of the document in next releases following the GSMA specification process.

2 Acronyms

3GPP	3rd Generation Partnership Project
3pcc	Third Party Call Control
3PTY	Three-Party conference
ACL	Access Control List
ACM	Address Complete Message
ACR	Anonymous Call Rejection
AF	Assured Forwarding
ALG	Application Level Gateway
ALOC	Average Length Of Conversation
AMR-NB	Adaptive Multi-Rate Narrow Band
AMR-WB	Adaptive Multi-Rate Wide Band
AMS-IX	AMSterdam Internet eXchange
ANM	Answer Message
AS	Autonomous System
ASP	Application Service Provider
ASR	Answer Seizure Rate
ATM	Asynchronous Transfer Mode
BA	Behavior Aggregate
BE	Best Effort
BFD	Bidirectional Forwarding Detection
BGCF	Breakout Gateway Control Function
BGP	Border Gateway Protocol
BSS	Business Support System
CBC	Cipher Block Chaining
CC	Country Code
CD	Call Deflection during alerting
CDR	Call Detail Record
CF	Call Forwarding
CHF	Call Handling Function
CIN	Calling Party's Number
CLI	Calling Line Identification
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
COLP	Connected Line identification Presentation
COLR	Connected Line identification Restriction
CPN	Called Party's Number
CPU	Central Processing Unit
CSCF	Call Session Control Function
CUG	Closed user Group
CUG	Closed User Group
CW	Call waiting
DdoS	Distributed Denial of Service
DES	Data Encryption Standard
Diffserv	Differentiated Services
DNS	Domain Name Service
DoS	Denial of Service
DPO	Dynamic Port Opening
DSCP	Differentiated Services Code Point
DTMF	Dual-Tone Multi-Frequency
DTX	Discontinuous Transmission
DWDM	Dense Wavelength Division Multiplexing
E2E	End to end
EF	Expedite Forwarding
ENUM	E.164 NUmber Mapping
EXP	MPLS header EXPerimental use field
FNO	Fixed Network Operator
FoIP	Fax over IP
GIC	Group Identification Code
GSDN	Global Software Defined Network
GSM	Groupe Speciale Mobile
GSMA	GSM Association

GSN	Global Subscriber Number
HW	Hardware
IAM	Initial Address Message
IANA	Internet Assigned Numbers Authority
IBCF	Interconnection Border Control Function
I-BGF	Interconnection Border Gateway Function
IC	Identification Code
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IFP	Internet Facsimile Protocol
IFT	Internet Facsimile Transfer
IKE	Internet Key Exchange
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPI	IP Interconnect
IPIA	IP Interworking Alliance
IPSec	IP Security
IPX	IP eXchange
IPX P	IPX Provider
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
ISUP	ISDN User Part
ITU	International Telecommunications Union
IVR	Interactive Voice Response
KPI	Key Performance Indicator
LBR	Low Bit rate codec
LBR	Low Bit Rate
MAP	Mobile Application Part
MF	Multi-Field Classifier
MGCF	Media Gateway Control Function
MGF	Media Gateway Function
MGW	Media Gateway
MIME	Multipurpose Internet Mail Extensions
MNO	Mobile Network Operator
MoIP	Modem over IP
MOS	Mean Opinion Scale
MOS_{CQE}	Mean Opinion Score, Communication Quality Estimated
MPIL	Multi-Party Interconnection Location
MPLS	Multi Protocol Label Switching
MTP	Message Transfer Part (SS7)
MVNO	Mobile Virtual Network Operator
NAPT	Network Address and Port Translation
NAT	Network Address Translation
NDC	National Destination Code
NDC	National Destination Code
NER	Network Efficiency Ratio
NGN	Next Generation Network
NN	National Number
NNI	Network to Network Interface
OCN	Original Called Number
OIP	Originating Identity Presentation
OIR	Originating Identity Restriction
OLO	Other Licensed Operator
OSS	Operations Support System
PDH	Plesiochronous Digital Hierarchy
PE-router	Provider Edge router
PGAD	Post Gateway Answer Delay
PGRD	Post Gateway Ringing Delay
PHB	Per-Hop Behaviour
POS	Packet Over Sonet
PP	Packetisation Period
P-router	Provider router
PSTN	Public Switched Telephone Network

PT	Payload Type
QoS	Quality of Service
REL	RELease
R-Factor	Rating-Factor
RFC	Request For Comments
RgN	Redirecting Number
RI	Redirecting Information
RR	Receiver Report
RTCP	Real Time Control Protocol
RTD	Round Trip Delay
RTP	Real-Time Protocol
SBC	Session Border Controller
SCCP	Signaling Connection Control Part (SS7)
SCTP	Stream Control Transmission Protocol
SDES	Source DEScription
SDH	Synchronous Digital Hierarchy
SDP	Session Description Protocol
SGF	Signaling Gateway Function
SIGTRAN	Signaling Transport suite of Protocols
SIP	Session Initiation Protocol
SIP URI	SIP protocol Uniform Resource Identifier
SIP-I	SIP with encapsulated ISUP
SIP-T	SIP for Telephones
SLA	Service Level Agreement
SN	Subscriber Number
SP	Service Provider
SPRT	Simple Packet Relay Transport
SR	Sender Report
TCAP	Transaction Capabilities Application Part
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TE MPLS	Traffic Engineering MPLS
tel-URI	Telephone Uniform Resource Identifier
THP	Traffic Handling Priority
TIP	Terminating Identification Presentation
TIR	Terminating Identification presentation Restriction
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking
TLS	Transport Layer Security
TOS	Type Of Service
TPKT	Transport protocol data-unit Packet
TSG	Trunk Group
TUP	Telephone User Part
UDP	User Datagram Protocol
UDPTL	facsimile UDP Transport Layer
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UUI	User-to-User Information
UUS1	User to user signalling 1
VAD	Voice Activity Detection
VBD	Voice Band Data
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VoIPX	Voice over IPX
VPN	Virtual Private Network
WB	Wideband codec

3 References

[1] i3 Forum "Technical Interconnection Model for International Voice Services" Release 3, June 2010

[2] i3 Forum "Interoperability Test Plan for Bilateral Voice services" Release 2.0, May 2009

[3] i3 Forum White Paper "Optimal Codec Selection in International IP based Voice Networks" Release 2.0, May 2010

[4] i3 Forum "Interconnection Form for International Voice Service" Release 2.0, May 2009

[5] i3 Forum White Paper "Mapping of Signaling protocols from ISUP to SIP, SIP-I" Release 1.0, May 2009

[6] i3 Forum "IP International Interconnections for Voice and other related services" Release 1.0, June 2009

[7] i3 Forum "Service Value and Process of Measuring QoS KPIs", Release 1.0, May 2010

[8] i3 Forum "Routing and Addressing services for International Interconnections over IP", Release 1.0, May 2010

[9] i3 Forum " White Paper: Techniques for Carriers' Advanced Routing and Addressing Schemes", Release 1.0, May 2010

[10] GSMA IPXWP "IPX White Paper", October 2006

[11] GSMA AA.80 "Agreement for IP Packet eXchange (IPX) Services", Version 3.2, July 2009

[12] GSMA AA.81 "PACKET VOICE INTERCONNECTION SERVICE SCHEDULE to AA.80", Version 1.2, July 2009

[13] GSMA IR.34 "Inter-PLMN Backbone Guidelines", Version 4.9, March 2010

[14] GSMA IR.40 "Guidelines for IPv4 Addressing and AS Numbering for GPRS Network Infrastructure and Mobile Terminals", Version 4.0, March 2007

[15] GSMA IR.67 "DNS/ENUM Guidelines for Service Providers & GRX/IPX Providers", Version 4.1, March 2010

[16] GSMA IR.77 "Inter-Operator IP Backbone Security Requirements For Service Providers and Inter-operator IP backbone Providers", Version 2.0, November 2007

[17] IETF RFC 768 "User Datagram Protocol", August 1980

[18] IETF RFC 1423: - Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers, February 1993

[19] IETF RFC 1918 "Address Allocation for Private Internets", February 1996

[20] IETF RFC 2246 "The TLS Protocol", January 1999

[21] IETF RFC 2396 "Uniform Resource Identifiers (URI): Generic Syntax", August 1998

[22] IETF RFC 2401 "Security Architecture for the Internet Protocol", November 1998

[23] IETF RFC 2474 "Definition of the Differentiated Services Field", December 1998

[24] IETF RFC 2475 "An Architecture for Differentiated Services", December 1998

[25] IETF RFC 2508 "Compressing IP/UDP/RTP Headers for Low-Speed Serial Links", February 1999.

[26] IETF RFC 2597 "Assured Forwarding PHB Group", June 1999

[27] IETF RFC 2663 "IP Network Address Translator (NAT) Terminology and Considerations", August 1999

[28] IETF RFC 2833 “RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals”, May 2000

[29] IETF RFC 2976 “The SIP INFO Method”, October 2000

[30] IETF RFC 3095 “Robust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed”, July 2001.

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

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

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

[34] IETF RFC 3262 “Reliability of Provisional Responses in the Session Initiation Protocol (SIP)”, June 2002

[35] IETF RFC 3265 “Session Initiation Protocol (SIP)-Specific Event Notification”, June 2002

[36] IETF RFC 3311 “The Session Initiation Protocol (SIP) UPDATE Method”, September 2002

[37] IETF RFC 3323 “A Privacy Mechanism for the Session Initiation Protocol (SIP)”, September 2002

[38] IETF RFC 3325 “SIP Extensions for Network-Asserted Caller Identity and Privacy within Trusted Networks”, September 2002

[39] IETF RFC 3332 & 4666 “Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) - User Adaptation Layer (M3UA)”, September 2006

[40] IETF RFC 3362 “Real-time Facsimile (T.38) – image/t38 MIME Sub-type Registration,”, August 2002

[41] IETF RFC 3389 “Real-time Transport Protocol (RTP) Payload for Comfort Noise (CN)” September 2002

[42] IETF RFC 3393 “IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)”, November 2002

[43] IETF RFC 3428 “Session Initiation Protocol (SIP) Extension for Instant Messaging”, December 2002

[44] IETF RFC 3515 “The Session Initiation Protocol (SIP) Refer Method”, April 2003

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

[46] IETF RFC 3551 “RTP Profile for Audio and Video Conferences with Minimal Control”, July 2003

[47] IETF RFC 3555 “MIME Type Registration of RTP Payload Formats”, July 2003

[48] IETF RFC 3555 “MIME Type Registration of RTP Payload Formats”, July 2003

[49] IETF RFC 3788 “Security Considerations for Signaling Transport (SIGTRAN) Protocols”, June 2004

[50] IETF RFC 3903 “Session Initiation Protocol (SIP) Extension for Event State Publication”, October 2004

[51] IETF RFC 3960 “Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)”, December 2004

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

[53] IETF RFC 4028 “Session Timers in the Session Initiation Protocol (SIP)”, April 2005

[54] IETF RFC 4040 “RTP Payload Format for a 64 kbit/s Transparent Call”, April 2005

[55] IETF RFC 4117 “Transcoding Services Invocation in the Session Initiation Protocol (SIP) Using Third Party Call Control (3pcc)” (June 2005).

[56] IETF RFC 4165 “Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) - User Peer-to-Peer Adaptation Layer (M2PA)“, September 2005

[57] IETF RFC 4166 “Telephony Signalling Transport over Stream Control Transmission Protocol (SCTP) Applicability Statement“, February 2006

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

[59] IETF RFC 4306 “Internet Key Exchange (IKEv2) Protocol”, December 2005

[60] IETF RFC 4458 “Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR)”, April 2006.

[61] IETF RFC 4566 “SDP: Session Description Protocol”, July 2006

[62] IETF RFC 4594 “Configuration Guidelines for Diffserv Service Classes”, August 2006

[63] IETF RFC 4733 “RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals” December 2006

[64] IETF RFC 4749 “RTP Payload Format for the G.729.1 Audio Codec” October 2006

[65] IETF RFC 4788 “Enhancements to RTP Payload Formats for EVRC Family Codecs”, January 2007

[66] IETF RFC 4856 “Media Type Registration of Payload Formats in the RTP Profile for Audio and Video Conferences”, March 2007

[67] IETF RFC 4867 “Real-Time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs April 2007

[68] IETF RFC 4960 “Stream Control Transmission Protocol”

[69] IETF RFC 5806 “Diversion Indication in SIP”, March 2010

[70] IETF draft-ietf-bfd-base-08.txt “Bidirectional Forwarding Detection”, March, 2008

[71] IETF draft-ietf-bfd-base-11 “Bidirectional Forwarding Detection”, January 2010

[72] ETSI 123.517 “TISPAN IP Multimedia Subsystem (IMS); Functional architecture”

[73] ITU-T T.38 Procedures for real-time Group 3 facsimile communication over IP networks, 1998

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

[75] ITU-T Recommendation G.729 “Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)”, 1996

[76] ITU-T Recommendation G.711 “Pulse Code Modulation (PCM) of Voice Frequencies”, 1988

[77] ITU-T Recommendation Q1912.5 “Interworking between Session Initiation Protocol and Bearer Independent Call Control or ISDN User Part”, 2004

[78] ITU-T Recommendation T.38 “Procedures for real-time Group 3 facsimile communication over IP networks” (04/2007)

[79] ITU-T Recommendation V.150 “Modem-over-IP networks: Foundation” (07/2003).

[80] ITU-T Recommendation G.729 “Coding of speech at 8 kbit/s using conjugate-structure algebraic code excited linear-prediction (CS-ALEP (01/07)

[81] ITU-T Recommendation G.729 Annex A “Reduced complexity 8kbit/s CS-ALEP codec” (11/96)

[82] ITU-T Recommendation G.729 Annex B Silence compression scheme for G.729 optimized for terminals conforming to Recommendation V.70” (11/96)

[83] ITU-T Recommendation G.729 Annex A and B

[84] ITU-T Recommendation. G.703 “Physical/electrical characteristics of hierarchical digital interfaces”, November 2001;

[85] ITU-T Recommendation. G.704 “Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical”, October 1998;

[86] ITU-T Recommendation. G.705 “Characteristics of plesiochronous digital hierarchy (PDH) equipment functional”, October 2000;

[87] ITU-T G.707: Network Node Interface for the Synchronous Digital Hierarchy(SDH), 01/2007

[88] ANSI T1.105: SONET - Basic Description including Multiplex Structure, Rates and Formats

[89] ITU-T Recommendation G.821 “Error Performance of an international digital connection operating at the bit rate below the primary rate and forming part of an Integrated Services Digital Network”, December 2002

[90] ITU-T Recommendation Y.1540 “Internet Protocol Data Communications Services - IP Packet Transfer and availability performance parameters”, November 2007

[91] ITU-T Recommendation E. 411 “International Network Management – Operational guidance”, March 2000

[92] ITU-T Recommendation E.425 “Network Management – Checking the quality of the international telephone service. Internal automatic observations”, March 2002

[93] ITU-T Recommendation E.437 “Comparative metrics for network performance management”, May 1999

[94] ITU-T Recommendation P.10 “Vocabulary of terms on telephone transmission quality and telephone sets”, December 1998

[95] ITU-T Recommendation G.107 “The E model, a computational model for use in transmission planning”, March 2005

[96] ETSI EG 202 057-2 “Speech processing transmission and quality aspects (STQ); user related QoS parameter definitions and measurements; Part 2: Voice Telephony, Group 3 Fax, modem data services and SMS”; October 2005

[97] ITU-T Recommendation V.152 “Procedures for supporting voice-band data over IP networks” , January 2005.

[98] ITU-T Recommendation Q.767, “Specification of Signalling System No.7, Application of the User Part of CCITT Signalling System No.7 for International Interconnection ISDN”, 1991

[99] 3GPP TS 23.107 “Quality of Service (QoS) concept and architecture”, 2009

[100]3GPP TS 29.163 “Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks” & TS 29.527 “TISPAN; Endorsement of the SIP-ISUP Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks”

[101] 3GPP TS 29.164 “Interworking between the 3GPP CS domain with BICC or ISUP as signalling protocol and external SIP-I networks”

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

[103]ITU-T Recommendation T.30 “Procedures for document facsimile transmission in the general switched telephone network“, September 2005

4 Basic Definitions

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

1) **IPX (IP Packet 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 Provider's networks.

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

   The business entity acts as Service Provider for the "numbers/user id's" of its own contracted end users and those contracted through distribution entities with an exclusive commercial contract with the Service Provider and that share the same access network of the SP (ex.: MVNOs).

   In the scope of this document, the first phase of implementation of VoIPX service only E.164 numbers shall be used as destination address. These numbers shall be used in tel-URI and SIP URI formats as described in section 11.

3) **IPX Provider (IPX P)**: A business entity (such as an IP Carrier) offering IP interconnect capabilities to Service Providers, possibly through interconnection with other IPX Providers for one or many IPX services compliant with the IPX operation 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 Service Provider premises to Service Provider premises. Thus, Service Provider core and access networks are excluded.

5) **VoIPX**: Identifies a specific logical subset of IPX devoted to manage voice service in terms of interfaces, features and capabilities. VoIPX confirms IPX concepts such as security, cascading and Service Provider to Service Provider responsibility.

   The above definition of Service Provider, IPX Provider and End-to-end are still valid in the VoIPX context.

6) **VoIPX Functional Architecture**: Identifies the set of VoIPX functions and options/features.

5 IPX Reference Configuration for Voice service

5.1 General Configuration

The general IPX reference configuration for Voice Services is given in the following figure with only 2 IPX Providers depicted.

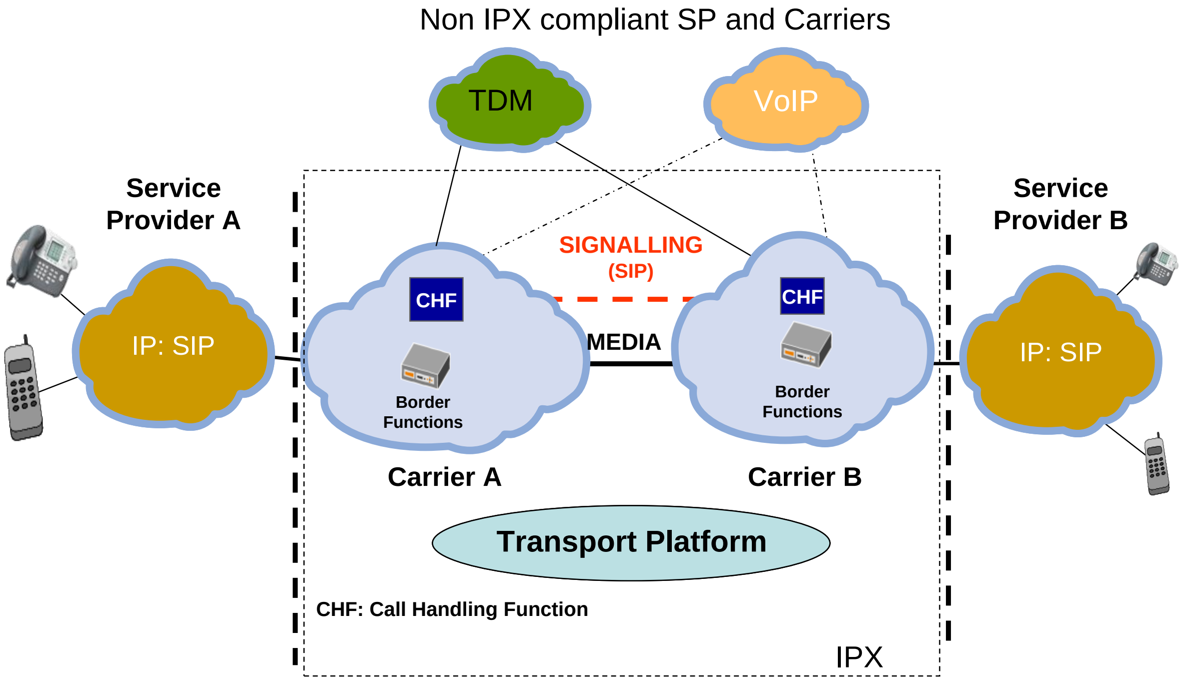


Figure 1 — General IPX Reference Configuration for Voice Services

The IPX domain consists of all the IPX Providers' networks and their interconnections. IPX Providers can connect to non-IPX compliant Carriers or Service Providers with the intent to either terminate traffic (break-out) to destinations not reachable via the IPX, or to accept traffic destined to an IPX compliant Service Provider (break-in). In both cases, the rules of cascading responsibilities, QoS and security shall be fulfilled. Further details can be found in section 12.5.

Different types of transport functions over the interconnection for both Service Provider to IPX Provider and between IPX Providers are given in Section 6.

The geographical scope of the IPX domain is given in figure 2. The end-to-end (E2E) interconnection responsibility (to be intended from SP-to-SP) is defined from egress port of the interconnecting element of the originating Service Provider network towards its own IPX Provider, to the ingress port of the interconnecting element of the terminating Service Provider. In this context, end-to-end corresponds to the above definition "from Service Provider premises to Service Provider premises".

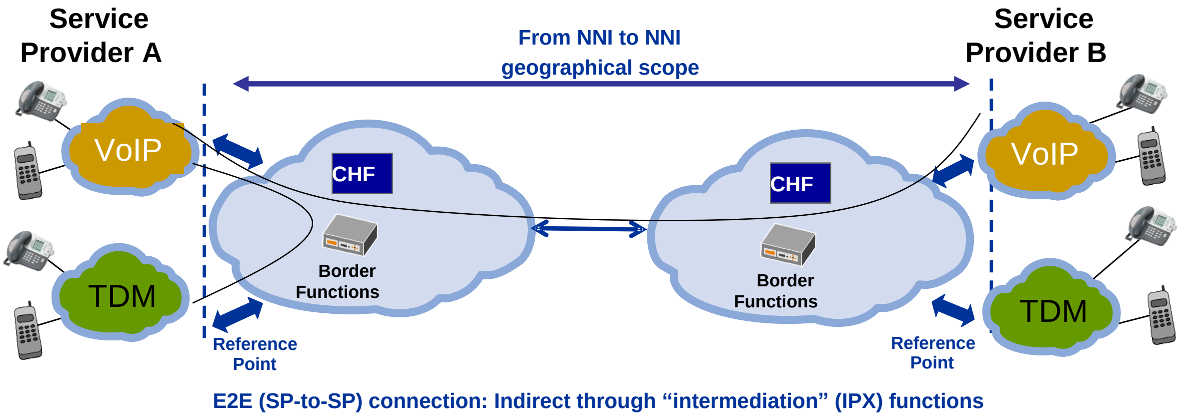


Figure 2 — Geographical scope of an IPX communication

The following basic requirements apply**:**

- More than one IPX Provider can be involved in the E2E (SP-to-SP) connection
- Even though the focus of this document is on voice service, being IPX a multiservice platform, the interconnection functions are intended to be multi-service, 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 Provider is responsible for ensuring the SLA's for that physical line (as described in AA.80 [11] annex 8)
- For services other than voice new requirements can be added.

5.2 Architecture of the IPX Domain for Voice Services

Figure 3 below provides an overall sketch of the IPX domain together with compliant Service Providers and Non-Compliant Service Providers and Carriers.

Compliant Service Providers generate IP traffic towards IPX providers across interfaces specified in the following sections. Each compliant SP can interconnect to one or more IPX Providers.

IPX Providers can implement both direct interconnections and interconnections via Multi–Party Interconnect Locations (MPIL) which are locations, private and/or public, where IPX Providers can meet. The private locations would be those set up by a group of IPX Providers and the public ones will be those created by a third party with open access to IPX Providers.

Note: in the GSMA IPX related documents, an MPIL is described as a Peering Point.

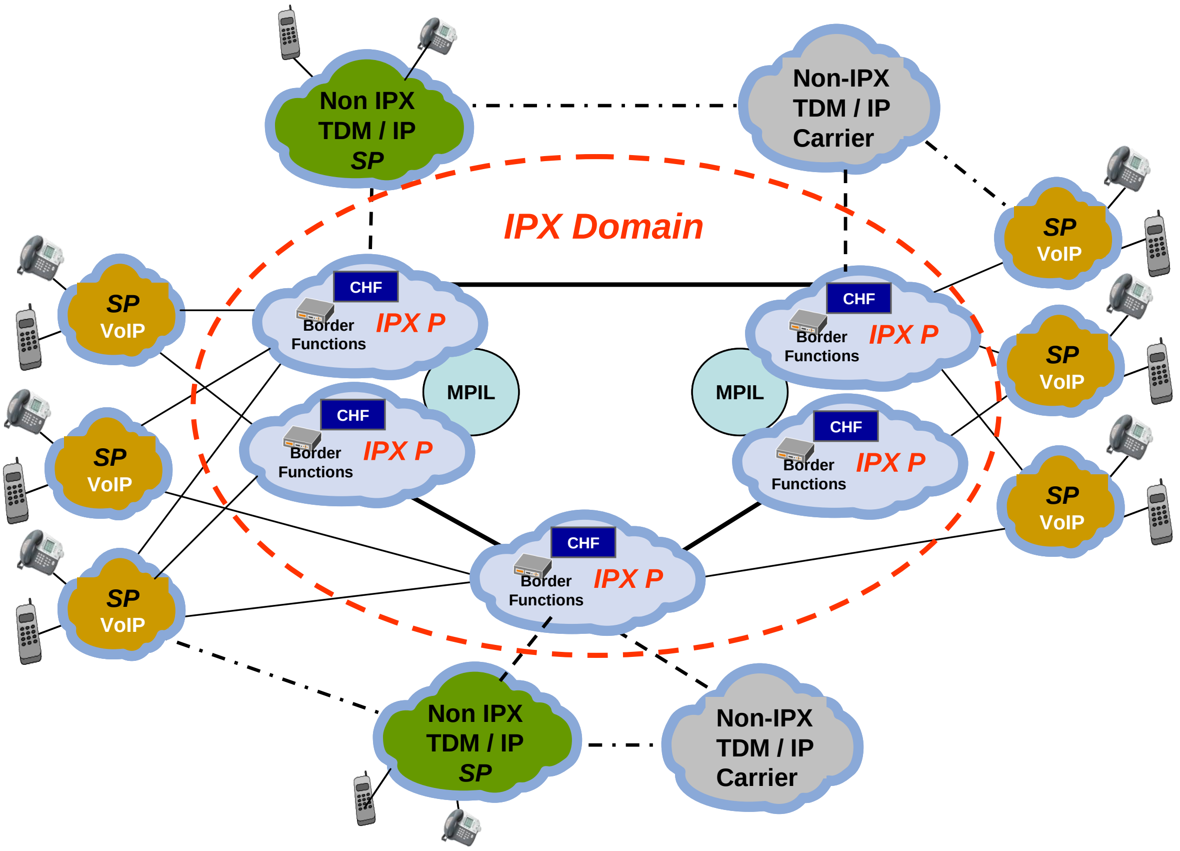


Figure 3 — Example IPX-network

As of early 2010, the GSMA has identified/set-up three public MPIL (Peering Points) in AMS-IX Amsterdam, Equinix Ashburn and Equinix Singapore for GRX/IPX services that can be used for VoIPX services. As the IPX/VoIPX traffic develops the number of MPILs could increase. See also Sec. 14 Annex A - Architecture of VoIPX platform.

5.2.1 Break-in / break-out Concepts

Allowing break-in/ break-out via TDM and IP for Voice Service between an IPX Provider and a Non-IPX compliant Service Provider has several advantages:

- many destinations will remain reachable only via TDM 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 MNOs would have to keep TDM interconnects operational in parallel to IPX-based interconnects in order to have access to these providers;
- Break-out / break-in interconnections support a faster deployment of IPX services for voice as it breaks the dependency on all networks migrating to IP at the same time.

5.2.1.1 Break-out from the IPX Domain (outgoing traffic)

In order to deliver traffic received from participating SPs towards non IPX destinations, the IPX Provider may be interconnected with non IPX Providers and non IPX compliant SPs as far as:

- those SPs reached through a break-out of the IPX domain are announced as reachable through a non IPX compliant interconnection. In this case the security and remaining capabilities of the E2E (SP-to-SP) connection are maintained unaffected and are compliant with the commercial agreement between originating SP and IPX Provider.

- due to network faults within the IPX domain which make the break-out route the only way to terminate the call. In this case the security is maintained unaffected. The remaining capabilities of the E2E (SP-to-SP) connection, as an objective, are compliant with the commercial agreement between originating SP and IPX Provider.

5.2.1.2 Break-in to the IPX Domain (incoming traffic)

The IPX Provider may inject traffic from other non IPX-compliant trusted SPs provided that the security of the IPX is not affected.

5.3 IPX Proxy in the VoIPX environment

The IPX proxy is a conceptual network element described in GSMA IR.34 [13] Annex B. Figure 4 below depicts the IPX proxy in a VoIPX environment. Inside one IPX Provider's network the IPX Proxy consists of all equipment and functions from the ingress Border Function up to and inclusive of the egress Border Function. This includes the Call Handling Function, but also other functions (e.g., media or signalling protocol conversion or IPv4/v6 translation, if required). The network between Provider Edge routers and Border Functions are not part of the IPX Proxy.

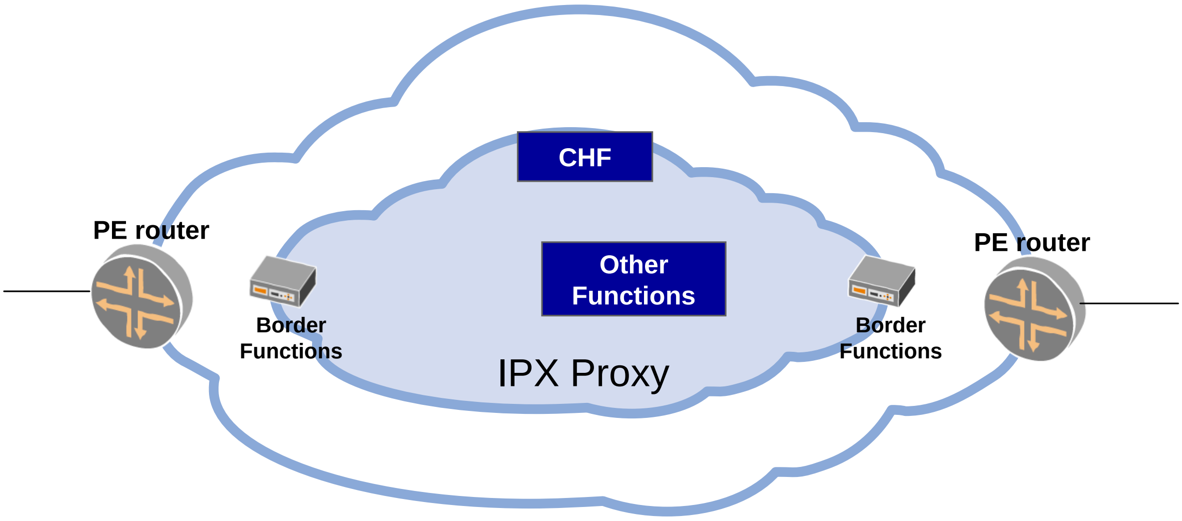


Figure 4 — IPX Proxy concept in VoIPX service

5.4 Connectivity Options

The IPX consists of two layers:

Transport or the Transport Layer provides connectivity between two Service Providers. This layer provides a guaranteed QoS bit-pipe function.

Service Awareness or the Service Layer provides establishment of connections and management of billing and settlements for a service.

The IPX Domain supports three interconnect models as detailed in the following sections.

5.4.1 Bilateral – Transport Only (transport without service awareness)

According to GSMA IPX White Paper 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). Each Service Provider will also pay their respective IPX Provider for the transport capacity, potentially depending on the level of QoS provided.*

This connectivity mode, being service agnostic, is considered out of scope for this document. Two Service Providers can set-up a voice interconnection between themselves if they receive the appropriate Transport Only connectivity mode from IPX Provider(s).

5.4.2 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).*

This connectivity mode is considered out of scope for this document being not clear some business and technical implications given by possible hybrid configurations (i.e. one SP requesting the Service Transit connectivity mode towards another SP requesting the Transport Only connectivity mode).

5.4.3 Multilateral - Hubbing (transport and hubbing with service awareness)

According to GSMA IPX White Paper 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.* [10]

This connectivity mode is the one in which the IPX Providers bring more value to the Service Providers and thus is the focus of this document.

5.4.4 Obligations for Connectivity Options for IPX Providers

The scope of this document is limited to the Multilateral – Hubbing connectivity mode.

An IPX provider is not obliged to offer all connectivity options: Transport, Service Transit and/or Service Hubbing.

5.5 Relationship to other IPX services

In document IR.34 [13], GSMA provides guidelines and technical information on how Inter Service Provider IP Backbone networks are set up, and how Service Providers will connect to it. The Inter Service Provider IP Backbone is defined as the collection of interconnected GRX and IPX Providers' networks, where the IPX is considered as an evolution of the GRX.

The IPX platform allows for the interconnection of any type of Service Providers (MNO, FNO, ISP, ASP, etc) and introduces the concept of end-to-end (i.e. from Service Provider premises to Service Provider premises) QoS as well as cascade billing.

The first release of this document, being dedicated to the specification of Voice over IPX, does not address some specific GSMA requirements pertaining to data services, but i3 Forum Carriers intend to expand the scope of this document to data services in next releases with the objective to address the whole set of GSMA requirements and to implement, as a target, a fully converged multiservice architecture.

As a result, the i3 Forum Carriers endorse the intrinsic value of the IPX model in terms of service integration and, notwithstanding the scope of this document is limited to voice service, each Carrier, acting as IPX Provider, can develop integrated service offerings encompassing one or more data services.

6 Transport Functions

This section recommends alternative reference transport configurations for implementing the NNI between a Service Provider and an IPX Provider and the NNI between two IPX Providers.

Assuming that the Public Internet is a global infrastructure, interconnecting managed IP networks and carrying mixed types of traffic with public announced IP addresses, two main sets of configurations are possible:

Private-oriented interconnection: when no unidentified third party is able to affect the bilateral VoIP service, and

Public-oriented interconnection: when the VoIP traffic is mixed with other IP traffic coming from the Public Internet, thus allowing the gateways' interfaces to be reached from unidentified third parties that can affect the service performance and quality.

In the following sections private-oriented scenarios are given which differentiate each other at the interconnection layer:

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

- Only VoIPX or other IPX services traffic is exchanged across the interconnection.
- All the involved IP addresses in the IPX address space (i.e., *PE router* interface, *P router* interface, border function interface) can not be reached from unidentified entities via Public Internet and as defined in GSMA IR.34 [13] have to be public, but they shall not be announced onto the Public Internet.
- The VoIP traffic, from the PE router to the border functions in a IPX Provider/SP 's domain, shall be secured, either physically or logically, from the Internet 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 native MPLS, Virtual Private Network (at layer 2 and 3) and Tunnelling (e.g. TE MPLS, IP Sec).

6.1 Generic Cases of Transport Configurations

6.1.1 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.

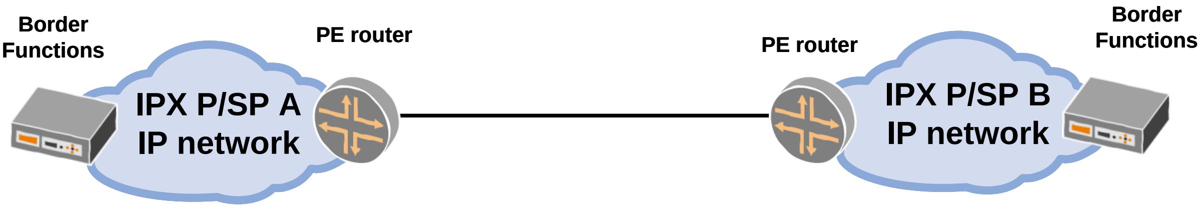


Figure 5 — Layer 1 Private-oriented Interconnection Configuration

6.1.2 Case 2- 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.

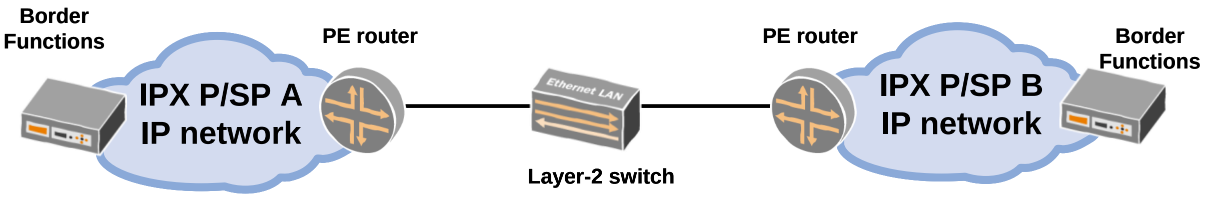


Figure 6 — Layer 2 Private-oriented Interconnection Configuration

MPILs are a special case of this model in which multiple carriers are interconnected in the same layer 2 network as is described in [13] section 6.4.

6.1.3 Case 3- Layer 3 interconnection

In this configuration, a dedicated virtual link is implemented between PE routers passing through a third party IP private network. The 3rd party IP network provider will establish a VPN between the carriers' networks and shall provide *QoS* mechanisms and shall guarantee appropriate SLAs.

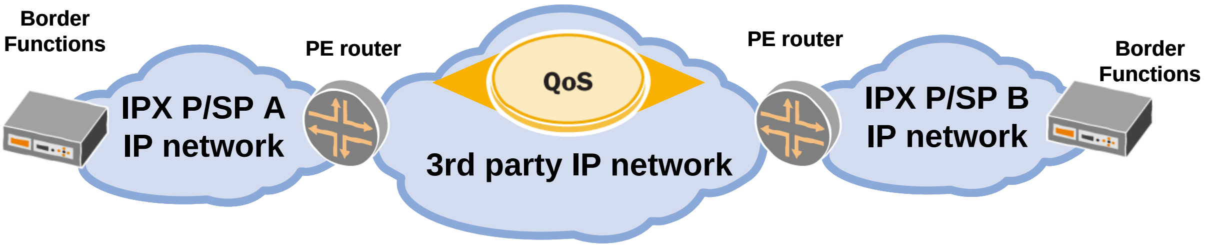


Figure 7 — Layer 3 Private-oriented Interconnection Configuration

6.1.4 Case 4- Layer 3 interconnection via Public Internet

In this configuration, an SP is connected to an IPX Provider via Public Internet by means of a VPN and using IP Sec encryption for signalling information.

In agreement with GSMA IR.34 [13] this configuration should be used in case the previous three configurations cannot be implemented both for technical and/or commercial reasons.

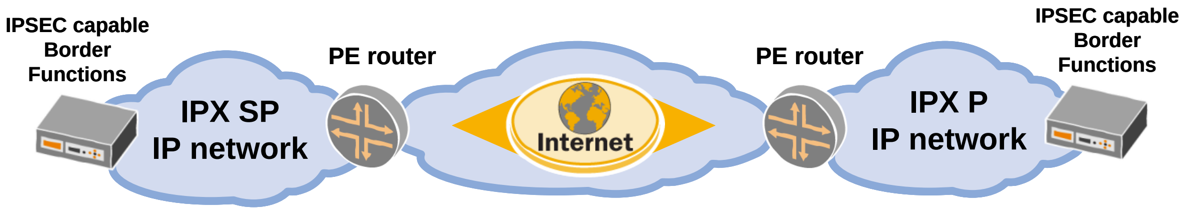

IPSEC capable Border Functions
IPX SP IP network
PE router
Internet
PE router
IPX P IP network
IPSEC capable Border Functions

Figure 8 — Internet IPSEC SP/P Interconnection Configuration

6.2 Transport Configurations for SP to IPX P interconnection

For Service Provider to IPX Provider interconnection, the following transport configurations (as illustrated in Section 6.1) can be implemented:

1) Case 1 as a direct layer 1 private interconnection (e. g., via a leased line).

2) Case 2 as layer 2 private interconnection (e.g., via an Ethernet switch).

3) Case 3 as layer 3 private interconnection (e.g., via a 3rd party private IP network using a Virtual Private Network connection).

4) Case 4 as a layer 3 interconnection via Virtual Private connection over the Public Internet using IPSec as the encryption scheme.

6.3 Transport Configurations for IPX-P to IPX P interconnection

For IPX to IPX Provider interconnection the following transport configurations (as illustrated in Section 6.1) can be implemented:

6.3.1 Direct Interconnection

For IPX Provider to IPX Provider interconnection the following transport functions can be implemented:

1) Case 1 as a direct layer 1 private interconnection (e. g. via a leased line).

2) Case 2 as layer 2 private interconnection (e.g. via an Ethernet switch).

6.3.2 Interconnection via MPIL

For IPX Provider to IPX Provider interconnection via MPIL, the case 2 transport function (section 6.1.2) is most attractive when a sufficient number of IPX Providers are willing to interconnect in it. Typically this MPIL will be set up by a third party such as a Telehouse or similar. As of early 2010 there are three: AMS-IX Amsterdam, Equinix Ashburn and Equinix Singapore.

6.4 Physical Interconnection Alternatives

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

6.4.1 SDH-based transport Systems

The ITU-T Recommendations G. Series shall be considered as reference documents, among these the ITU T Recc. ITU-T G.707 [87].

For North America another reference document is ANSI T1.105 [88].

6.4.2 Ethernet-based transport Systems

The IEEE recommendations 802.3 [102] for Ethernet communication together with enhanced ethernet technologies such as fast-ethernet, giga-ethernet and 10giga-ethernet have to be considered (e.g. ISO/CIE 8802-3).

6.4.3 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.

6.5 Dimensioning Requirements at the transport layer

In order to ensure that, at the interconnection, sufficient capacity is present with the highest level of confidence, a dimensioning scheme with an over-provisioning factor is suggested. In the following table, the bandwidth to be allocated per call is given for the most common codecs:

Codec	Packetisation (msec.)	IP Bandwidth (kbit/s)
G.711	20	104.720
G.729	20	43.120

G.729	40	25.960

Note: The IP bandwidth values of the above table consider the bandwidth of the codec plus the overhead of the Ethernet, IP, UDP and RTP protocols and assume a value equal to 10% as the over-provisioning factor. The signalling bandwidth is considered in the 10% over-provisioning factor.

6.6 IP Routing and IP Addressing

6.6.1 IP Routing

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

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

GSMA IR.34 [13] defines the use of BGP communities. This use does not affect the VoIPX as defined in this document.

It is recommended to tune timer parameters to appropriate values, which depend on specific implementation, to ensure optimum convergence after a link failure or topology change. Alternatively, BFD [70] could also be used to speed up link failure detection and subsequent protocol convergence.

6.6.2 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 Providers will use only IP addresses assigned by IANA or related bodies as described in [14] .

6.6.3 IP Packet Marking

In IR.34 ([13]) section 8.2 the following traffic classification, based on 3GPP's definitions in [99], is described:

QoS Information		**Diffserv PHB**	**DSCP**
Traffic Class	**THP**		
Conversational	N/A	EF	101110
Streaming	N/A	AF41	100010
Interactive	1	AF31	011010
	2	AF21	010010
	3	AF11	001010
Background	N/A	BE	000000

Note: Traffic Handling Priority (THP) specifies the relative importance of applications that belong to the Interactive traffic class

When comparing this table with the one from i3 Forum in [1]:

Traffic Type	**DSCP Marking**	**IP Precedence**	**802.1Q VLAN**
Voice Media	for configurations 6.1, 6.2., 6.31 DSCP 46/EF (101110).	5	5
	for configurations 6.2.24	5	5

Traffic Type	DSCP Marking	IP Precedence	802.1Q VLAN
	DSCP 46/EF (101110) or DSCP 00/DF (000000).	or 0	or 0
Voice Signalling	for configurations 6.1, 6.2.1, 6.3 DSCP 26/AF31 (011010) or DSCP 46/EF (101110)	3 or 5	3 or 5
	for configurations 6.2.24 DSCP 26/AF31 (011010) or DSCP 46/EF (101110) or DSCP 00/DF (000000)	3 or 5 or 0	3 or 5 or 0
SIGTRAN for **Mobile Signalling**	for configurations 6.1, 6.2. 6.3.1 DSCP 26/AF31 (011010) or DSCP 46/EF (101110)	3 or 5	3 or 5
	for configurations 6.2.24 DSCP 26/AF31 (011010) or DSCP 46/EF (101110) or DSCP 00/DF (000000)	3 or 5 or 0	3 or 5 or 0
Other traffic	DSCP 00/DF (000000).	0	0

and taking into account that the IPX Provider has to adapt to the common IP marking the following correspondence can be found:

Traffic Type	GSMA Traffic Class
Voice Media	Conversational
Voice Signalling	Conversational or Interactive
SIGTRAN for Mobile Signalling	Conversational or Interactive
Other Traffic	Background

Note: There is no agreement as whether the signalling has to be treated in the Expedited Forwarding ([31][32]) or Assured Forwarding ([26]) Per Hop Behaviours.

7 Signalling Functions

The interconnection model for VoIPX described in this document supports a SIP profile (as described in section 7.1) and an ISUP enabled SIP profile (as described in section 7.2).

7.1 Functions for supporting signalling protocol SIP (IETF RFC 3261)

7.1.1 Transport of SIP (IETF RFC 3261) signalling information

UDP is the default transport protocol for SIP. Usage of other transport protocols is discussed in the Interconnection Model [1]

7.1.2 SIP signalling protocol profile

The SIP profile shall comply with RFC 3261 [33] with the addition of the following considerations:

- The compact form of SIP shall not be used.
- The Request-URI shall be set in accordance to section 10.
- The support of IETF RFC 4028 [53] which addresses SIP Timers specification, is optional. The carrier receiving the INVITE message shall comply with IETF RFC 3261 [33] section 16.8 if IETF RFC 4028 [53] is not supported**.**
- The P-Asserted-Identity header defined in RFC 3325 [38] shall be supported.
- The Privacy header defined in RFC 3323 [37] shall be supported.
- The Diversion header defined in RFC 5806 [69] shall be supported.
- The following body types shall be supported:
  - application/sdp
- The following body types may be supported:
  - application/dtmf
  - application/dtmf-relay
  - multipart/mixed.

Subject to bilateral agreement, the carrier may or may not apply privacy before forwarding SIP messages over the interconnection interface. When applying privacy, it shall be applied as follows:

Originating User Privacy Request	**Originating Carrier behaviour**
CIN Known, Presentation not restricted	Forward CIN in From, Contact and P-Asserted-Identity headers
CIN Known, Presentation restricted	Use “Anonymous” in From and Contact headers.
CIN not known	Use “Unavailable” in From and Contact headers.

Note: when a SIP message is passed to an untrusted domain, the inclusion or removal of the P-Asserted-Identity header shall be determined by consulting the Privacy header. If a Privacy header is not present then it is recommended to include the P-Asserted-Identity header, but in this case bi-lateral agreement should dictate final treatment (IETF RFC 3323 [37], 3325 [38]). When the SIP message is passed to a trusted domain, the P-Asserted-Identity header should not be removed (IETF RFC 3325 [38]).

7.1.3 SIP Message support

SIP methods as listed in the Interconnection Model [1], section 7.1.3 shall be supported.

7.1.4 SIP Header support

SIP headers as listed in the Interconnection Model [1], section 7.1.4 shall be supported.

7.1.5 Alignment with 3GPP SIP definition

The i3 Forum is aware that there are differences between its basic SIP definition and the 3GPP SIP definition. These differences are under study and i3 Forum documentation will be upgraded when the study is concluded.

7.2 Functions for supporting signalling protocol SIP-I (ITU-T Rec. Q.1912.5)

7.2.1 Transport of SIP-I (ITU – T Q.1912.5) signalling information

UDP is the default transport protocol for SIP. Usage of other transport protocols is discussed in the Interconnection Model [1], section 7.2.1.

7.2.2 SIP-I (ITU – T Q.1912.5) signalling protocol profile

This signalling protocol profile shall be in accordance with ITU-T Recommendation Q.1912.5 [77] Annex C Profile C.

7.3 Mapping of ISUP to SIP or SIP-I signalling protocols

Mapping between ISUP and SIP or ISUP and SIP-I is a complex area that needs to be taken into account to ensure optimum behaviour for session control.

The most straightforward case is ISUP to SIP-I in accordance with specification ITU Q1912.5, Annex C Profile C [77]. Essentially, as the ISUP is encapsulated within the SIP message, correct conveyance of the ISUP information is guaranteed.

Where ISUP has to be mapped into SIP there are a number of standards but they differ and this has led to different vendors’ implementations.

For further information on this subject, refer to the i3 Forum White Paper “Mapping of Signalling Protocols from ISUP to SIP, SIP-I” [5].

8 Media Functions

Media functions in International voice IP interconnections should ensure the following:

- Transport for all the services
- Transcoding, where required and applicable.

An international IP voice interconnection shall support the following services:

- Voice phone calls using different codecs;
- DTMF support;
- Fax connections;
- Modem connections.

These above listed services shall be accessible for TDM and VoIP subscribers.

8.1 Voice calls – protocol profiles

For calls between two or more terminals the following protocol stack shall be used:

- RTP protocol for real time media;
- UDP protocol at the transport layer.

8.1.1 Real Time Protocol / Real Time Control Protocol

The Real Time transport Protocol (RTP) and Real Time transport Control Protocol (RTCP) shall be used for international voice services as defined in IETF RFC 3550 [45]. According to RFC 3550 for particular applications the following items should be additionally defined:

- Profile definition
- Payload format specification.

In order to guarantee measurements of QoS parameters, RTP and RTCP flows have to be passed through end-to-end for the voice over IP connection except when transcoding or packetisation period translation occurs.

The profile that shall be used for international voice interconnection is defined in IETF RFC 3551 [46]. The list of protocol parameters defined in this RFC [46] that shall be used is given below.

8.1.1.1 Real Time Protocol data header

The RTP data header is defined in Section 2 of RFC 3551 [46]. The content of this section is endorsed.

8.1.1.2 Real Time Protocol Payload types

The following RTP payload types shall be supported:

- G.711 A-law, G.711 µ-law, G.722, G.723, G.729, G.729a, b, ab, G.722 as defined in Section 6, Table 4 of RFC 3551 [46].
- Detailed definition of above mentioned and other supported codecs payload types in Sections 8.3-8.5 of this document.
- Comfort Noise is defined in Section 4 of RFC 3389 [41] (static PT 13 (8 kHz) or dynamic).
- Telephone Events (DTMF tones) as defined in the Section 3.3 of IETF RFC 2833 [28](dynamic)
    - Note: RFC 2833 has been superseded by RFC 4733 [63]. As a consequence, the latter should be considered as the target reference specification

- Telephone tones as defined in the Section 4.4 of IETF RFC 2833 [28] (dynamic)
    - Note: RFC2833 has been superseded by RFC 4733 [63]. As a consequence, the latter should be considered as the target reference specification

8.1.1.3 Real Time Protocol data header additions

No RTP header additions will be used.

8.1.1.4 Real Time Protocol data header extensions

Use of RTP data header extensions is not recommended.

8.1.1.5 Real Time Control Protocol report interval

Recommended bandwidth allocation to RTCP reports would be 1.25% of session bandwidth for senders and 3.75% for receivers. Other bandwidth allocations are possible as described in Section 2 of IETF RFC 3551 [46].

8.1.1.6 Sender Report/Receiver Report (SR/RR) extensions

Generally no SR/RR extensions will be used. Optional extensions may be used if agreed bilaterally.

8.1.1.7 Source Description (SDES) use

The SDES use is specified in IETF RFC 3551 [46] Section 2.

8.1.1.8 Security - security services and algorithms

According to RFC 3550 [45] Section 9.1, the default encryption algorithm is the Data Encryption Standard (DES) algorithm in Cipher Block Chaining (CBC) mode, as described in Section 1.1 of RFC 1423 [18], except that padding to a multiple of 8 octets is indicated as described for the P-bit.

In the scope of this document RTP (media) encryption is not recommended.

8.1.1.9 String-to-key mapping

No string to key will be used.

8.1.1.10 Congestion - the congestion control behaviour

RTP and this profile may be used in different contexts: enhanced network services, or best effort services. Some congestion control guidelines to be introduced are in Section 2 of IETF RFC 3551 [46]. Under normal operational conditions congestion should be avoided by network engineering techniques.

8.1.1.11 Transport protocol

The UDP as well as TCP protocols are defined in RFC 3551 [46] section 2 as transport layer. In the scope of this document only UDP protocol shall be used as RTP transport layer for voice services.

8.1.1.12 Transport mapping

The standard mapping of RTP and RTCP addresses and ports at transport layer is used as in RFC 3551 [46] Section 2 with the following recommendations:

- RTP should use an even destination port number and the corresponding RTCP stream should use the next higher (odd) destination port number as described in RFC 3550 [45] Section 11,
- Symmetrical UDP protocol should be used (the same port numbers).

8.1.1.13 Encapsulation of Real Time Protocol packets, multiple Real Time Protocol data packets

Encapsulation of RTP packets in UDP protocol shall be used as defined in [45].

8.1.1.14 IP/UDP/RTP Compression

Compressing IP/UDP/RTP Headers as described in RFC2508 [25] or RFC3095 [30] will reduce the bandwidth of the interconnection and is recommended when bandwidth is restricted.

When IP/UDP/RTP compression is used, the UDP checksum is not required for voice, hence compression to 2 bytes for RFC 2508 [25] (or 1 byte for RFC 3095 [30] if available) is recommended for this purpose.

8.2 Voice Codecs

Many different coding schemes have been defined, implemented and used for international voice service. In the scope of this document these codecs are divided into 2 categories:

Mandatory codecs: the carrier shall be able to carry all voice media flows encoded as per any of the i3 Forum recommended codecs, to be considered mandatory in this context, and shall allow the negotiation of these codecs between both originating and terminating Service Providers. As a result, a carrier has to support all mandatory codecs listed in Table 1 in Section 8.3 below. Provided at least one of the mandatory codecs is present in the session description protocol (SDP) offer, and provided at least one of the mandatory codecs is supported by both originating and terminating Service Providers, then codec negotiation is guaranteed to be successful. For any transcoding related matter see Section 8.6.2.

Optional codecs: other codecs which are considered with significant market relevance.

In next releases of this document, other codecs may be added to the list of mandatory and optional codecs.

8.3 Codecs Supported for Narrow Band Transmission

Narrow Band codecs reproduce the audio bandwidth of the PSTN and are expected to be used in IP based voice networks for some time. The codecs to be supported for Narrow Band transmission are:

Group 1. Mandatory Narrow band codecs	Group 2. Optional Narrow band codecs
G.711 A-law, μ-law 64 kbit/s	G.723.1 (quality impairments have to be considered using this codec)
G.729, G.729a, G.729b, G.729ab 8kbit/s	G.726
	AMR-NB

Table 1 Mandatory and Optional Narrow Band Codecs

Note: i3 forum recognises that the G:711 codec needs much higher bandwidth than other codecs like AMR-NB and confirms its willingness to review, in next release of this document, the content of Table 1 above in line with market developments.

8.3.1 Guidelines for Engineering

Packetisation period for mandatory Narrow Band codecs:

- for G.711 A-law and μ-law, packetisation period shall be 20 ms
- for G.729, G.729 a, G.729b, G.729ab, packetisation period shall be 20 ms

Payload type definition for mandatory Narrow Band codecs:

G.711 A-law	PT= 8 Static
G.711 μ-law	PT= 0 Static
G.729, G.729a	PT= 18 Static

•	G.729b,ab	PT= 18 Static. Optional parameter “annexb” may be used according to RFC 3555 [48] Section. 4.1.9.

Packetisation period for other (optional) Narrow Band codecs:

- for G.723.1 packetisation period shall be 30 ms
- for G.726 packetisation period shall be 20 ms
- For AMR-NB packetisation period shall be 20 ms.

Payload type definition for other Narrow Band codecs:

•	G.723.1	PT=4 Static Optional parameters "annexa" and "bitrate" may be used according to RFC3555 [48].
•	G.726	PT=Dynamic as defined in RFC 3555 [48]
•	AMR-NB	Dynamic as defined in RFC 4867 [67]

8.4 Codecs supported for Wideband Transmission

There is a general trend towards the increased use of wideband codecs. They provide superior voice quality and their use may reduce voice quality degradation due to transcoding. Support of wideband codecs by carriers is optional. However, when a carrier supports wideband codecs, this section applies and specifies what needs to be supported. The codecs to be supported for Wideband transmission are:

Group 1. Mandatory Wideband codecs (*)	Group 2. Optional WideBand codecs
G.722 (generally used by fixed network operators)	
AMR-WB (generally used by mobile network operators)	

Table 2 Mandatory and Optional Wideband Codecs

(*) The mandatory status is conditional on the support of wideband voice interconnection: if Wideband voice interconnection is supported, then the Group 1 codecs in Table 2 are mandatory as defined in Section 8.2.

8.4.1 Guidelines for Engineering

Packetisation period for mandatory Wideband codecs

- for G.722, packetisation period shall be 20 ms
- for AMR-WB, packetisation period shall be 20 ms

Payload type definition for mandatory Wideband codecs

•	G.722	PT=9 Static
•	AMR-WB	Dynamic as defined in RFC 4867 [67]

8.5 Codecs supported for Low Bit Rate transmission

In the case where transmission costs are high, such as for satellite links, minimal bandwidth use is an important design consideration.

8.5.1 Transmission (Occupied) Bandwidth

Factors affecting occupied bandwidth (or bandwidth demand) are: codec bit rate, Voice Activity Detection and Discontinuous Transmission (VAD/DTX), packetisation period (pp) and IP/UDP/RTP compression.

To transmit VoIP signals over satellite SDH bearers, 46 bytes of POS/IP/UDP/RTP headers are added to each VoIP packet payload. The 40 bytes of IP/UDP/RTP header can, for voice, be reduced to 2 bytes by implementing IP/UDP/RTP compression according to RFC 2508 [25] or to 1 byte if RFC 3095 [30] is implemented.

In network configurations where occupied bandwidth is important it is recommended to utilise transcoding (where unavoidable), packetisation period translation, and overhead reducing IP transmission techniques to gain control of transmission bandwidth (and hence link economics):

- select a Low Bit Rate (LBR) codec with low voice quality impairment factor (see [3]).
- select codecs with Discontinuous Transmission (DTX),
- Implement IP/UDP/RTP compression, and
- Consider translating the packetisation period to higher values, such as 40ms.

Note that the codec and packetisation period are (unless changed) set by the coder originating the media flow. Thus transcoding and packetisation translation capability may be needed by a satellite link carrier to guarantee that the occupied voice transmission bandwidth (hence cost) remains within acceptable limits.

An example of where transcoding may be avoided and occupied bandwidth contained is if a satellite link in an IPX primarily serves mobile SPs; then the IPX provider should consider supporting a common mobile codec on the satellite link (if bandwidth costs are acceptable after applying the last three criteria above) rather than transcoding to another low bit rate codec (of the satellite IPX provider's choice).

8.5.2 Voice Quality Considerations

As the codec bit rate decreases the voice quality also degrades, thus the balance between a LBR codec's contribution to link costs and its contribution to voice quality degradation must be considered with respect to the end-to-end voice quality required [3].

Where end-to-end performance is being bilaterally designed, inter-carrier cooperation in end-to-end design containing, say, a satellite hop, may allow other links in such an end-to-end connection to be engineered to minimize total quality impairment (such as by using a high quality codec in the remainder of the network). Such end-to-end design cooperation is strongly recommended.

8.5.3 Low Bit Rate Codecs

The codecs to be supported for Low Bit Rate transmission are:

Group 1. Mandatory LBR codecs (*)	Group 2. Optional LBR codecs
G.729a with VAD/DTX	AMR-NB with VAD/DTX

Table 3 Mandatory and Optional Low Bit Rate Codecs

(*) The mandatory status is conditional on the need for low bit rate voice interconnection: if low bit rate voice interconnection is needed, then the Group 1 codecs in Table 3 are mandatory as defined in Section 8.2.

8.5.4 Guidelines for Engineering

Packetisation period for mandatory Low Bit Rate codecs

- for G.729a packetisation period shall be 20 ms or 40ms (40ms lowers occupied bandwidth if extra latency is admissible, translation of packetisation period may be required [3])

Payload type definition for mandatory Low Bit Rate codecs

- G.729a PT= 18 Static

Packetisation period for other Low Bit Rate codecs

- for AMR-NB packetisation period shall be 20 ms or 40ms (40ms lowers occupied bandwidth if extra latency is admissible, translation of packetisation period may be required [3])

Payload type definition for other Low Bit Rate codecs

AMR-NB	Dynamic as defined in RFC 4867 [67]

Voice Activity Detection/Discontinuous Transmission (VAD/DTX)

- VAD/DTX (where available) shall be turned on.

IP/UDP/RTP Header Compression

- IP/UDP/RTP compression to 2 bytes [25] or 1 byte [30] shall be implemented on all restricted bandwidth links requiring low transmission bit rates, such as satellite links (this increases the voice payload capacity for a given transmission rate thus admitting higher codec bit rates to improve voice quality)

8.6 Codec/Packetisation period use and transcoding guidelines

Codec and packetisation period selection, and particularly transcoding, have a great impact on end-to-end voice quality in VoIP networks.

8.6.1 Voice quality estimation

It is necessary to ensure that voice transmission quality is acceptable for all IP interconnection configurations and designs. In case of a poor estimate result, the network configuration and/or codec/packetisation period choice should be redesigned.

The detailed rules as well as the method of end to end voice quality estimation for this purpose are given in the i3 Forum white paper “Optimal codec selection in international IP-based voice networks” [3].

Generally the design should take into consideration:

- the Codec/packetisation period parameters of all involved interconnected networks (e.g. originating SP and domestic network – international IPX providers’ networks – international carriers’ networks (break out case) – terminating SP and domestic network)
- the packetisation period latencies taken in conjunction with both originating and terminating domestic and local access networks latencies
- the international physical (distance) latency
- the expected packet loss and codec packet loss robustness
- the transmission bandwidth (cost)
- the voice quality (product) required.

8.6.2 General guidelines

The following general guidelines aim to provide default rules for codec choice and transcoding responsibility:

- transcoding should be avoided whenever possible, due to the impact on speech quality and delay;
- the order of codec/packetisation period preference is determined by the originating terminal and should be honoured wherever possible;
- if a call is to be routed to a TDM network and G.711 A-law/µ-law conversion is necessary, then the µ-law interfacing IPX provider/international carrier shall perform the companding conversion;
- if the call is to be routed to a TDM network, only one transcoding is recommended. If required, it should be performed during the voice over IP/TDM conversion;

- in case no common codec can be used between both end Service Providers, in the first instance it is the responsibility of Service Providers to support transcoding in order to ensure successful voice interoperability for their services;
- in the case of fixed-mobile interconnection, transcoding, if necessary, should always be performed by mobile service providers;
- if a satellite link serves mobile SP's, consider using the SP's mobile codec on the satellite link rather than transcoding to a different codec;
- it is recognized however that it is important for satellite link operators to keep occupied bandwidth of all signals under control for economic reasons and transcoding/pp translation capability will be required.

An extensive treatment of voice quality impairments generated by codec and/ or transcoding functions is given in [3].

8.7 Fax calls – protocol profiles

To enable sending and receiving fax messages from TDM to VoIP or TDM – TDM via VoIP the two following modes may be implemented:

- Mode 1: Voice Band Data (VBD = "pass through") as defined in ITU-T V.152 [97] Section 6.
- Mode 2: T.38 [78] Fax relay

In mode 1 the following stack shall be used:

- G.711 codec as described in Section 8.1.1, with the addition that it is also possible to use dynamic payload instead of static in SDP negotiation
- RTP as described in Section 8.1.1.
- UDP in transport layer as described in Section 8.1.1.

In mode 2, one of the three following stacks may be used:

- <u>Stack 1 (Recommended)</u>
    - IFT protocol for T.30 [103] media
    - UDPTL (Facsimile UDP Transport Layer)
    - UDP protocol in transport layer

- <u>Stack 2</u>
    - IFT for T.30 [103] media
    - RTP
    - UDP in transport layer
- <u>Stack 3</u>
    - IFT protocol for T.30 [103] media
    - TPKT (Transport Protocol Data Unit Packet)
    - TCP protocols in transport layer.

8.7.1 Fax over IP guidelines

T.38 fax relay should be supported (Version 0 mandatory, newer versions optional).

It is recommended to use T.38 fax relay method as first choice and fax pass–through (VBD) as second choice. In particular for satellite links the use of T.38 will greatly reduce the bandwidth of fax calls.

It is recommended to use stack 1 as described in Section 8.7 above for fax relay and G.711 codec for as described in section 8.5 above for modem pass–through.

It is recommended that Standard G3 Group facsimile shall be supported as mandatory. V.34 Group 3 facsimile support is optional according to bilateral agreement. Recommended target solution, i.e., is the implementation of the latest T.38 standard which allows full support of SG3 fax.

If a gateway has both T.38 and V.150.1 capabilities, the transitions from MoIP to FoIP mode shall be possible as described in T.38 Annex F. Figure F.1/T.38 [78].

8.8 Modem connections

To enable point to point modem connections TDM–IP–TDM the modem pass–through method or the modem relay method may be used:

- Voice Band Data (VBD) mode, as defined in ITU-T V.152 [97] section 6. with:
  - G.711 A-law or μ-law codec as described in Section 8.3.1, with the addition that it is also possible to use dynamic payload instead of static in SDP negotiation;
  - RTP as media protocol;
  - UDP as transport protocol.
- Modem relay mode, as defined in ITU-T V.150.1 [79] Section 9 with:
  - Simple Packet Relay Transport (SPRT) as specified in ITU-T V150.1 [79] Annex B;
  - UDP as transport protocol.

Call discrimination procedures in case of modem TDM–IP–TDM connection should be performed according to V.150.1 [79] Section 20. Interworking procedures between T.38 and V.150.1 should be as in T.38 Annex F [78].

8.9 MoIP Guidelines

For modem over IP transmission method 1 (Voice Band Data as described above) is recommended. Modem relay method may be optionally used when bilaterally agreed.

Modem Relay method is the recommended target solution when interconnection bandwidth must be minimized.

8.10 Support of 64k clear channel (ISDN)

64 kbit/s clear channels shall be supported. Payload type is dynamic as defined in IETF RFC 4040 [54].

8.11 Handling of early media

In this document the term "*early media*" encompasses ring–back tones, announcements, and in general, any type of media different than user–to–user communication (i.e., any media before the sending/receiving of the 200 OK message).

In TDM networks, ring–back tone is rendered by the called side whereas, in IP networks, it is usually rendered by the calling side. However, all scenarios which can be encountered by a carrier interconnecting, upstream and downstream, with ISUP, SIP and SIP-I based networks, need clarification. Handling of Early–Media is governed by the presence of the P-Early-Media header, when this header is supported. This is described in the Interconnection Model [1], section 9.1. When the P-Early-Media header is not supported, the behaviour of the IPX Provider is as described in the Interconnect Model [1], section 9.2.

9 Security Functions

9.1 Network elements for border function

It is mandatory that all voice traffic coming into / leaving a carrier's network passes through Border Function, e.g., SBC.

As a result, all IP packets (for signaling and media), crossing the bilateral voice interconnection, are originated and received by such Border Function.

In Section 5 the definitions of Border Function as well as the mapping with the corresponding functions for the control and user plane are given.

A typical example of Border Function is a SBC (Session Border Controller).

The main functions of the SBC are the following:

- Perform control functions by tightly integrating session signalling and media control.
- They (the SBC or border elements) are the source and destination for all signalling messages and media streams coming into and leaving the carrier's network.
- A Session Border Controller breaks down into two logically distinct pieces.
    - The Signalling SBC function controls access of SIP signalling messages to the core of the network, and manipulates the contents of these messages.
    - The Media SBC function controls access of media packets to the network, provides differentiated services and QoS for different media streams, and prevents service theft.

Furthermore, additional functionalities could be implemented in the SBC depending on the system supplier, e.g. Lawful Interception, media and control conversion, termination of secure (IPSec) connections.

The security related features and capabilities are described in more detail in Section 9.2.

9.2 Security features and capabilities

It is recommended that certain provisions be taken when using the public internet to ensure that the bilateral voice interconnection provides adequate protection against external intruders. If connected to the public Internet, it is recommended that adequate measures be implemented on those connections, and that incoming sessions initiated from the Internet from unidentified parties are blocked.

9.2.1 Topology Hiding and NAT/NAPT Translation

Topology hiding is the function which allows hiding Network Element addresses/names from third parties. Hiding IP addresses can be implemented by the NAT/NAPT mechanism, which is applied at the IP level and is defined in [27].

When SCTP will be used in the future, SCTP-NAT should be applied when necessary.

This IP topology hiding function is carried out for signalling traffic in the IBCF part of the Border Function, and for media traffic in the I-BGF part of Border Function.

Since voice traffic will be exchanged between Border Functions of two carriers, the addresses of the Border Functions will be the only visible IP endpoints.

The application of NAT/NAPT and SCTP–NAT (e.g. Multi–homing) shall have no impact on the interconnection functionality and shall be transparent to the interconnecting carriers.

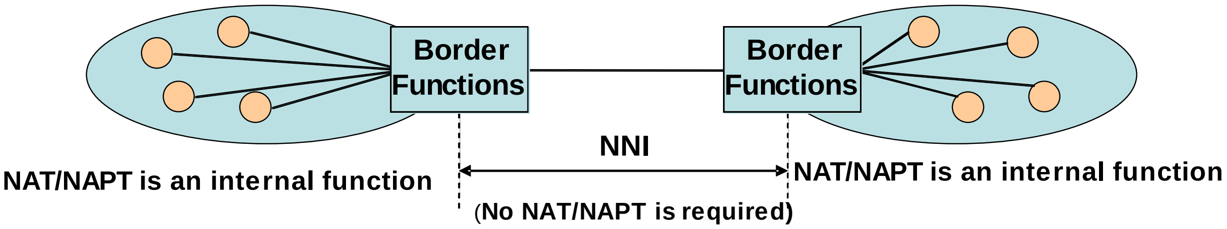

Border Functions
Border Functions
NNI
NAT/NAPT is an internal function
NAT/NAPT is an internal function
(No NAT/NAPT is required)

Figure 9 — NAT/NAPT Application

When NAT/NAPT is applied, IP addresses of IP packets are changed at IP level and ALG (Application Level Gateway) is the operation that changes IP addresses carried in SIP signaling accordingly.

9.2.2 Encryption

Two methods are used for encrypting information: IPSec as specified in [22] and TLS (Transport Layer Security) as specified in [20].

It is recommended to use the IPSec protocol when encryption is needed, since it is independent from the protocols used at the upper layer and it is more widely used (e.g., interconnection modes via the public Internet) with the following rules:

- Encryption for private interconnections
  In case of interconnection configurations described in Sections **Error! Reference source not found.**.1, 6.1.2 and 6.1.3, the use of encryption is not recommended for either the signalling or the media flows.

- Encryption for public interconnections

In case of interconnection configurations described in Section 6.1.4, the use of encryption is recommended for signalling flows. Encrypting the media flow is not required.

Whether the TLS scheme could be used in next versions of this document, is for further study.

9.2.3 Source Authentication

When IPSec is used (see Section 9.2.2), it shall be used also for source authentication. Exchange of keys should be based on IKEv2 as specified in [59].

9.2.4 Access Control lists

Access Control Lists are used to filter incoming packets in order to allow in only valid packets. ACL should apply as follows:

- Control on source IP address: only packets originating from the partner operator are allowed in;
- Control on destination IP address: optionally, only packets directed to Border Function are allowed in;
- It is recommended to use a HW (Hardware) based ACL. The use of HW based ACL is recommended because of CPU power consumption.

9.2.5 Traffic Policer

A traffic policer allows the application of rate limiting to streams of received signaling packets. Packets in excess of the permitted rate are deemed "nonconforming" and are discarded.

These policers protect the border function itself and the protected networks behind it against DoS attacks caused by overwhelming floods of packets.

9.2.6 Deep packet inspection

Deep packet inspection is the mechanism to protect against malformed, modified packets

9.2.7 Media traffic filtering

Media traffic filtering is used to make sure only those media packets pass for which the {source address & port - destination address & port} combination fully matches the one signaled in a successful call attempt.

9.2.8 Internet Control Message Protocol (ICMP) packet suppression

ICMP is part of the Internet Protocol Suite. ICMP messages are typically generated in response to errors in IP datagrams, or for diagnostic or routing purposes. ICMP suppression ignores ICMP messages other than ECHO, and suppresses the generation of ICMP responses other than ECHO REPLY.

Processing significant numbers of ICMP messages can be both CPU and memory resource intensive but, in most cases, provides no real operational benefit. By ignoring unnecessary ICMP messages, the border function mitigates the effect of certain DOS attacks.

10 Numbering and Addressing Scheme (E.164-based)

This first deliverable is E.164-based [74]. The objective of this section is to define the format of numbers and addresses which will be exchanged in signaling messages between operators in international IP interconnection for voice services.

10.1 Numbering and addressing in E.164-based International interconnection

International IP interconnection for voice services will be based on SIP [33] and SIP-I [77]. In the first phase of implementation only E.164 numbers shall be used as destination address. These numbers shall be used in tel-URI and SIP URI as described in sections 10.3 and 10.4 respectively.

10.2 International numbering scheme in TDM network

International number format used in International IP interconnect for voice shall conform to E.164 standard [74]. A telephone number is a string of decimal digits that uniquely indicates the network termination point. The number contains the information necessary to route the call to this point.

According to this standard full international number in global format contains a maximum of 15 digits starting from Country Code (E.164 [74] Section 6) and has the following format:

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.

Where:

• CC	Country Code for geographic area	1 – 3 digits
• NDC	National Destination Code	
• SN	Subscriber Number	
• GSN	Global Subscriber Number	
• IC	Identification Code	1 – 4 digits
• GIC	Group Identification Code	1 digit

Support of ISDN sub addressing as defined in E.164 [74] (Appendix B, Section B. 3.3) in international voice IP interconnect is OPTIONAL as it is very rarely used.

10.3 TEL-URI Addressing scheme

A Tel-URI shall conform to IETF RFC 3966 [52]. According to this RFC 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

10.4 SIP-URI Addressing scheme

A SIP-URI shall conform to IETF RFC 2396 [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 [33] section 19.1.1.

An example of a SIP-URI would be:

```
sip:+14085551212@domain.com;user=phone
```

11 Quality of Service Control

This section describes the QoS parameters pertaining to the international interconnection between IPX Providers and between IPX Providers and their customers (Service Providers).

KPIs of QoS parameters are defined for the purpose of:

- Monitoring (supervision) against given thresholds
- Troubleshooting
- Service Level Agreement (SLA) compliance and Quality of Service reporting (i.e., carrier with another carrier or carrier with a service provider)

Any commercial agreement associated with SLA and/or QoS reporting is outside the scope of this document. See [6] and [7] for any matter related to SLA compliance and/or management.

11.1 QoS parameter definitions

The following QoS parameters are considered the most relevant and they are divided in two sets pertinent to the transport layer, and the service, respectively.

- *Transport parameters*
    - round-trip delay
    - jitter
    - packet loss
- *Service parameters*
    - MOS_{CQE} / R-factor
    - ALOC
    - ASR
    - NER
    - PGRD

Note: PGRD is preferred over PGAD (Post Gateway Answer Delay) because the latter depends on the end-user behaviour.

Other parameters can be measured by carriers for the above listed actions.

No KPI specific to fax quality is defined in the scope of this document since fax quality is measured end-to-end in compliance with ETSI EG 202 057-2 [96].

Other KPIs which are outside the scope of this technical document are defined in [6] and [7].

CLI Management

CLI transparency is not considered a KPI in the scope of this document; however, it is strongly recommended and assumed that international carriers will pass on CLI unaltered.

Carriers, under normal operational conditions, are not expected to check CLI validity. Carriers can ensure that a CLI received is always passed on unmodified across their own domain except in the case to change CLI from national format to international format (if received over a TDM link at the originating international gateway). A CLI in SIP would normally be in the format specified in Section 10 of this report, and so no change of format would be necessary.

The carrier can also have an agreement with another interconnecting carrier that they will guarantee agreed CLI transparency levels.

There is no certainty that:

- CLI will be transmitted by Service Provider A;
- a CLI received from Service Provider A is a valid value, i.e., a value of a CLI ‘owned’ or ported to Service Provider, and indeed, is the correct CLI for the calling party;
- a CLI forwarded to an interconnecting carrier, even where that carrier has undertaken to guarantee transmission across its network, will be delivered to the terminating user, or delivered without any error being introduced beyond the interconnecting carrier.

In the following subsections the definitions of the QoS parameters listed above are given.

11.1.1 Parameters relevant to the transport layer

Round Trip Delay

Round Trip Delay is defined as the time it takes for a packet to go from one point to another and return [90].

Jitter

Jitter is the absolute value of differences between the delay of consecutive packets [90], [42].

Packet loss

Packet loss is the ratio between the total lost packets and the total sent packets over a given time period [90].

11.1.2 Parameters relevant to the service layer

For the following parameters en-bloc signaling is assumed. The case of overlap signaling is out-of-scope.

MOSCQE / R-factor for voice calls

MOS (Mean Opinion Score) is a subjective parameter defined in ITU-T Rec. P.10 [94] as follows “The mean of opinion scores, i.e., of the values on a predefined scale that subjects assign to their opinion of the performance of the telephone transmission system used either for conversation or for listening to spoken material.”

ITU-T Rec. G.107 [95] defines an objective transmission rating model (the E-model) for representing voice quality as an R-Factor, accounting for transmission impairments including lost packets, delay impairments and codecs. The impairment factors of the E-model are additive, thus impairments from different network segments may be added to obtain an end-to-end value.

The R-Factor may be converted into an estimated MOS which is called MOS Communication Quality Estimated or MOS_{CQE} (as defined in ITU-T Rec. P.10 [94]) using formula in ITU-T Rec G 107 Annex B [95]. As a result, MOS is thus an actual user opinion score, and all measurements done by equipment (including R-Factor and MOS_{CQE}) are estimates, and may differ from what actual customers would perceive.

ALOC

Average Length of Conversation (ALOC) expresses the average time in seconds of conversations for all the calls successfully setup in a given period of time. In a TDM environment ALOC has been defined in ITU-T Recc.E.437 [93]:

$$\textbf{ALOC} = \frac{\sum \textbf{ time periods between sending answer and release messages}}{\textbf{Total number of answers}}$$

In a Voice over IP environment, and for the purpose of this document, ALOC is defined as follows:

- SIP protocol: ALOC is measured from the time of SIP 200 OK (in response to an INVITE initiating a dialog) to the time of call release (SIP BYE).
- SIP-I protocol: ALOC is measured from the time of a SIP 200 OK with an encapsulated ANM to the time of receiving a BYE message with encapsulated REL.

ALOC depends on the user behaviour.

ASR

Answer Seizures Ratio (ASR) expresses the ratio of the number of calls effectively answered in a given period of time against the number of call session requests in that time. In a TDM environment, ASR has been defined in ITU-T Rec. E.411 [91] with the following formula:

$$\mathbf{ASR} = \frac{\textbf{Seizures resulting in answer signal}}{\textbf{Total Seizures}}$$

In a Voice over IP environment, and for the purpose of this document, ASR is defined as follows:

- SIP protocol: ASR is the ratio between the number of received 200 OK (in response to an INVITE initiating a dialog) and the number of sent INVITE initiating a dialog.
- SIP-I protocol: ASR is the ratio of the number of received 200 OK with an encapsulated ANM (in response to an INVITE with an encapsulated IAM initiating a dialog) to the number of INVITE sent with an encapsulated IAM.

ASR depends on the user behaviour.

NER

Network Efficiency Ratio (NER) expresses the ability of a network to deliver a call without taking into account user interferences (measure of network performance) in a given period of time. In a TDM environment, NER has been defined in ITU-T E.425 [92] released in 2002 with the following formula:

$$\mathbf{NER} = \frac{\textbf{Answer message or user failure}}{\textbf{Total Seizures}}$$

In a VoIP environment, and for the purpose of this document, NER is defined as follows:

- SIP protocol: NER is the ratio of the number of received responses amongst the following responses, with the number of sent INVITE initiating a dialog:
    - a response 200 OK INVITE or
    - a BYE response or
    - a 3xx response or
    - a 404 406 410 480 484 486 488 response or
    - a 6xx response
    - a CANCEL message (in forward direction i.e., from the calling party)
- SIP-I protocol: NER is the ratio of the number of received responses amongst the following responses, to the number of sent INVITE with an encapsulated IAM:
    - a response 200 OK INVITE with an ANM encapsulated or
    - a '410 GONE' with REL encapsulated and cause value 22 or
    - a BYE response or message type '486 Busy Here' or message type '600 Busy everywhere' with REL encapsulated and cause release 17 or

- a BYE response or message type ‘480 Temporarily unavailable’ with REL encapsulated with cause value 18 or 19 or 20 or 21 or 31, or
- a BYE response or message type ‘484 Address Incomplete’ with REL encapsulated with cause value 28 or
- a BYE response or message type ‘404 Not Found’ or message type ‘604 Does not exist anywhere’ with REL encapsulated with cause value 1 or
- a BYE response or message type 500 ‘Server Internal Error’ with REL encapsulated with cause value 50 or 55 or 57 or 87 or 88 or 90.
- a CANCEL message (in forward direction i.e., from the calling party)

Note: it is recognised that cause value 53 (outgoing calls barred within CUG) has to be considered as a user failure. Being the scope of this document limited to international interconnection it is assumed that no SIP message related to this cause value 53 will be received.

PGRD

Post Gateway Ringing Delay (PGRD) expresses the time elapsed between a request for a call setup and the alerting signal for that call. In a VoIP environment, and for the purpose of this document, PGRD is defined as follows:

- SIP protocol: PGRD is the average time between sending an INVITE initiating a dialog and the first received 18X message;
- SIP-I protocol: PGRD is the average time between sending an INVITE initiating a dialog with an encapsulated IAM and the first received 18X message with an encapsulated ACM.

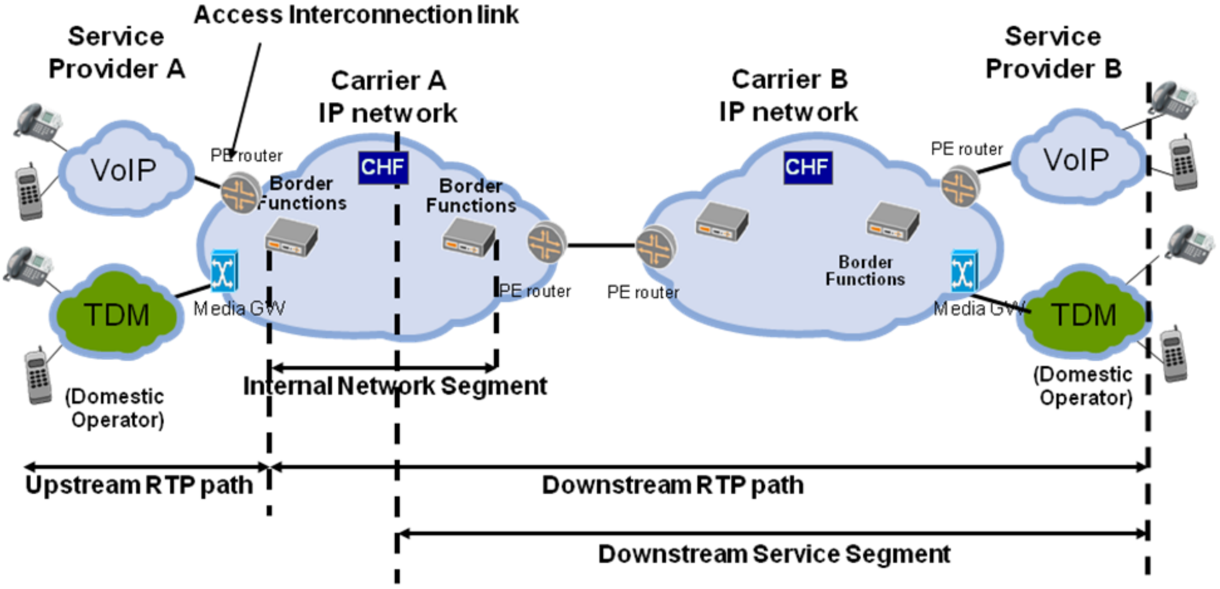
Note: only INVITEs initiating a dialog for which an alerting response is received are taken into account.

11.2 Reference points and measurement segments

Two reference configurations are defined, for the Carrier-to-Service Provider relationship and for the Carrier-to-Carrier relationship respectively.

11.2.1 For the Carrier-to-Service Provider relationship

The following Figure 10 applies to the Carrier–to–Service Provider relationship.



CHF: Call Handling Functions
Note: it is possible that more than two Carriers can be involved in the Service Provider-to-Service Provider communication.
If more than two Carriers are involved, Carrier B is meant to be the last in the path,
i.e. the Carrier interconnecting to Service Provider B. Consequently, Carrier A and Carrier B may not have a direct relationship.

Figure 10 — Reference configuration for the Carrier-to-Service Provider relationship

The following segments are defined:

- *the access interconnection link*: from egress interconnecting element of Service Provider A to ingress PE router of Carrier A. The entity that provides this link is responsible for ensuring the quality level for this link.

  The interconnection link may span a few metres in a telehouse / carrier hotel or some kilometres if a private circuit is leased or thousands of kilometres if the connection is made via the public Internet.

- *the internal network segment:* from Carrier A ingress Border Function to Carrier A egress Border Function.

  It is recognised that Border Function, either at network ingress or at network egress, might not be co-located with the PE router so identifying an internal network segment shorter than the real carrier's network domain. In these cases, Service Providers and Carriers can agree bilaterally the management of this geographical gap.

  Having the Border Function close to the PE router leads to more accurate measurement and is therefore advisable. However, it is also recognised that it may not be economically viable to have a Border Function co-located with each PE router. Therefore, a trade-off is required between the number of PE routers, the number of Border Function and the relevant economics.

  As traffic grows, it is expected that the number of Border Function entities will also grow, leading to increased co-location, implying more accurate measurements in the longer term.

- *the downstream service segment:* from Carrier Call Handling Function down to the terminal of the end user.

- downstream RTP path: from Carrier A ingress Border Function down to the equipment terminating the RTP flow (e.g. it could be the terminating end-user terminal for an end-to-end IP call, or could be the MGW if the call is broken out to TDM or could be a transcoding function).

- upstream RTP path: from the equipment originating the RTP flow (e.g. it could be the originating end-user terminal for an end-to-end IP call, or could be the MGW if the call is broken in from TDM or could be a transcoding function) to Carrier A ingress Border Function.

11.2.2 For the Carrier-to-Carrier relationship

The following Figure 11 applies to the inter-Carrier relationship. The SIGTRAN access type is included in the connections shown in the Figure 11 below.

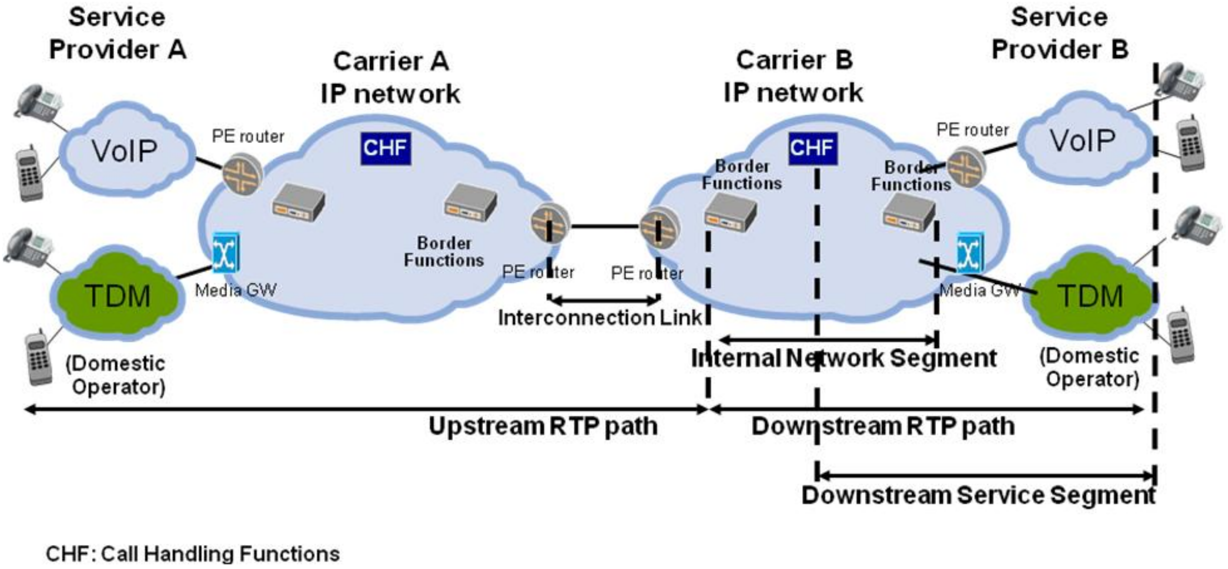


Figure 11 — Reference configuration for the Carrier-to-Carrier relationship

This Carrier-to-Carrier relationship is part of an originating SP – terminating SP communication which could involve more than 2 carriers.

The following segments are defined, assuming a flow of traffic from Carrier A to Carrier B:

- *the interconnection link:* from Carrier A egress PE router to Carrier B ingress PE router. The entity that provides the interconnection link is responsible for ensuring the quality level for the link.

  The interconnection link may span a few metres in a telehouse / carrier hotel or some kilometres if a private circuit is leased or thousand of kilometres if the connection is made via the public Internet.

- *the internal network segment:* from Carrier B ingress Border Function to Carrier B egress Border Function.

  It is recognised that Border Function, either at network ingress or at network egress, might not be co-located with the PE router so identifying an internal network segment shorter than the real carrier's network domain. In these cases, Carriers can agree bilaterally the management of this geographical gap.

  Having the Border Function close to the PE router leads to more accurate measurement and is therefore advisable. However, it is also recognised that it may not be economically viable to have a Border Function co-located with each PE router. Therefore, a trade-off is required between the number of PE routers, the number of Border Function and the relevant economics.

  As traffic grows, it is expected that the number of Border Function entities will also grow, leading to increased co-location, implying more accurate measurements in the longer term.

- *the downstream service segment:* from Carrier Call Handling Function down to the terminal of the end user.

- downstream RTP path: from Carrier B ingress Border Function down to the equipment terminating the RTP flow (e.g. it could be the terminating end-user terminal for an end-to-end IP call, or could be the MGW if the call is broken out to TDM or could be a transcoding function).
- upstream RTP path: from the equipment originating the RTP flow (e.g. it could be the originating end-user terminal for an end-to-end IP call, or could be the MGW if the call is broken in from TDM or could be a transcoding function) to Carrier B ingress Border Function.

11.2.3 Validity of the measurement mechanism

It has to be understood that a Carrier, for the parameters defined above, can detect a KPI degradation but cannot by itself identify the network responsible for such quality degradation.

It has to be noted that, if the Service Provider is not ready to commit to some level of service within its network, then it is not possible for the Carrier to control the QoS parameters that involve the Service Provider network, e.g., KPI for the Downstream Service segment.

11.2.4 Measurement points

The following tables in this subsection specify where each parameter can be measured.

11.2.4.1 For the transport parameters

Media traffic does not flow straight from the carrier ingress router to the carrier egress router; instead it flows through the ingress and egress Border Functions. Knowing that injected traffic from active probes would not follow such path, it is more relevant to take measurements on the path of the actual traffic. An appropriate location to take these measurements is at the Border Function. As a consequence, for the transport layer KPIs, measurements apply at Border Function based on actual RTP traffic. This allows for the possibility to have passive probes monitoring live traffic.

The geographical scope of one measure spans as far as the RTP end-point. If this flow is stopped by a network (see Section 8.1.1) or if an IP→TDM conversion takes place, the RTD, Jitter and Packet Loss values represent the performance over a limited geographical scope. As a result, for the quality control and monitoring, termination of the RTP flow before reaching the terminating Service Provider should be avoided, e.g., it is recommended not to perform any IP→TDM conversion before the destination Service Provider network.

Since an operator, in the SP-SP communication, could terminate RTP traffic without declaring it, and this is undetectable, there needs to be an understanding that no contrived termination of the RTP flows (i.e., early termination of the RTP flow not technically justified) takes place.

The value of a transport parameter over an Internal Network Segment can be obtained by subtracting the measure at egress Border Function to the measure at ingress Border Function.

	Monitoring		**Troubleshooting**	
KPI	***Carrier- SP***	***Carrier- Carrier***	***Carrier- SP***	***Carrier-Carrier***
RTD, Jitter, Packet Loss	Access Interc. Link Segment Internal Network Segment	Access Interc. Link Segment Internal Network Segment	Access Interc. Link Segment Internal Network Segment	Access Interc. Link Segment Internal Network Segment

	SLA / QoS Reporting	
KPI	***Carrier-SP***	***Carrier- Carrier***

RTD, Jitter, Packet Loss	Upstream RTP path Downstream RTP path	Upstream RTP path Downstream RTP path

Whether the parameters Round Trip Delay, Jitter and Packet loss are suitable for a SLA agreement is in the scope of [6] and [7].

11.2.4.2 For MOS$_{CQE}$

	Monitoring		**Troubleshooting**	
KPI	***Carrier- SP***	***Carrier- Carrier***	***Carrier- SP***	***Carrier-Carrier***
MOS$_{CQE}$	from ingress measuring equipment upstream to RTP end point (note 1) from ingress measuring equipment downstream to RTP end point (note 1)	from ingress measuring equipment upstream to RTP end point (note 1) from ingress measuring equipment downstream to RTP end point (note 1)	MOS$_{CQE}$ levels may indicate problems but they are not directly used for troubleshooting	MOS$_{CQE}$ levels may indicate problems but they are not directly used for troubleshooting

	SLA / QoS Reporting	
KPI	***Carrier- SP***	***Carrier- Carrier***
MOS$_{CQE}$	from ingress measuring equipment to downstream RTP end point (note 1)	from ingress measuring equipment to downstream RTP end point (note 1)

Note 1: It is to be noted that MOS$_{CQE}$ can be estimated by Border Function, or other equipment, relying on the information transported via RTCP protocol. If this flow is blocked by a network (see Section 8.1.1) or if an IP→TDM conversion takes place, MOS$_{CQE}$ values assume a limited geographical scope.

Whether the parameter MOS$_{CQE}$ is suitable for a SLA agreement is in the scope of [6] and [7]

11.2.4.3 For the service parameters

	Monitoring		**Troubleshooting**	
KPI	***Carrier- SP***	***Carrier- Carrier***	***Carrier- SP***	***Carrier-Carrier***
ALOC, ASR, NER, PGRD	At Call Handling Functions for the downstream direction	At Call Handling Functions for the downstream direction	KPI levels may indicate problems but they are not directly used for troubleshooting	KPI levels may indicate problems but they are not directly used for troubleshooting

	SLA / QoS Reporting	
KPI	***Carrier- SP***	***Carrier – Carrier***
ALOC, ASR, NER,	At Call Handling Functions for the downstream direction i.e., the	At Call Handling Functions for the downstream direction i.e., the

PGRD	downstream service segment	downstream service segment

Whether the parameters ALOC, ASR, NER and PGRD are suitable for a SLA agreement is in the scope of [6] and [7]

11.3 KPI computation for SLA / QoS reporting

As a general principle each Carrier can offer KPIs of QoS parameters according to its own commercial policy [7].

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)
- KPI_i 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
- 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.

- MOS: 95 / 99 % percentile
- ALOC: average (by definition)
- NER: average (by definition)
- ASR: average (by definition)
- PGRD: 95 / 99 % percentile.

11.4 Exchange of QoS data

The quality of a call consists of the quality provided both at the Transport layer and the Service Layer (see section 11.1). Neither only the Transport layer QoS parameters nor only the service layer QoS parameters can guarantee Service Providers the level of quality perceived by the final users (calls with IP delay, loss and jitter values compliant with target reference IP KPIs can result in poor service quality since multiple call cut-offs can occur, and, vice versa, calls with excellent service layer KPIs can still be rejected by final user due to packet loss and/or too long packet delay). As a result, a comprehensive and consistent approach has to be considered covering all aspects and all related parameters for the exchange of QoS data.

As far as the measurement and control of the Transport layer QoS parameters is concerned, considering the current alternatives to compute these parameters (i.e. either on real traffic or via external fake traffic injected by probes), i3 Forum Carriers, as presented above, support the first alternative using the Border Functions that can assure values are related to the real voice traffic, and can allow end-to-end monitoring at these network edge points.

The i3 Forum recognizes this approach is subject to the fulfilment of specific conditions (see above sections) and the current network implementation and IP migration might limit a wide use of this approach but suggests this method should be used avoiding the intrinsic complexity of summing up the measured performance of each network in the path.

With regard to service parameters, it has to be outlined that some parameters by definition include the end user behaviour (e.g., ASR, ALOC) and they should be considered for a service level agreement (SLA) only of the basis of a commercial decision taken by each IPX Provider, since the end user behaviour is not dependent on activities which are under the control of IPX Providers.

Some other service parameters (e.g. NER) by definition include the performance of all operators in the chain, both IPX Providers and Service Providers. Hence, all operators in the chain should commit on the target user-to-user value for these parameters, but this requirement is not compliant with the end-to-end scope of the IPX domain requested to IPX Providers, as per GSMA definition endorsed in section 5 of this document. Thus, IPX Providers, when they commit to a SLA/SLO for quality parameters, take on commercial risks that either cannot be fully cascaded downstream in the delivery chain or are cascaded with the implementation of a very complex and costly mechanism of certification, exchange and validation of QoS data.

Considering both the objectives to determine the end-to-end measurement required by customers and to identify the responsibility in case of dispute, the document [7] describes the measurement process for each operator in the chain. This process aims to compute the quality parameters from its points of measurement down to the end destination and to evaluate its contribution to the quality degradation. This approach does not support the need to share and aggregate each individual Network segment quality measurements in order to compute the end-to-end value, avoiding complex and more expensive solutions (e.g. exchange and post-elaboration of each internal network segment measure or a public database containing partial quality contributions from each operator for an end-to-end measurement).

12 Routing and Traffic Management

12.1 General Service Routing Principles

In section 5 a graphical example of an IPX domain for voice services has been described in figure 3. In addition to participating SPs, this figure shows IPX-Ps within the IPX domain, as well as Carriers and SPs outside this domain.

In agreement with GSMA White Paper on IPX which, in section 3.2, calls for a closed environment, in this document a routing confined within the IPX domain is always recommended unless:

- the call has to be routed towards a carrier in break-out in agreement with the contract signed between SP and IPX P;
- the call has to be routed towards a carrier in break-out since there are no available network resources which allow the call completion within the IPX domain.

The qualification process of carriers as IPX Provider as well as of Service Provider is outside the scope of this document.

12.2 Number of IPX Providers in the SP-SP communication

The GSMA IPX technical specifications recommend that not more than 2 IPX–Ps be involved in the SP-SP (end–to–end) communications, unless otherwise addressed by a specific service schedule. This limit is clarified for the voice service in AA.81 where it is written in section 2: *assume that any two PVI Service Providers are interconnected by at most two IPX networks unless this is not possible in exceptional cases. In the event that more than two IPX providers are needed to provide the connectivity, the QoS requirements shall remain unaltered*.

i3 Forum recognises the need to limit as much as possible the number of IPX Ps in the SP-SP communication to maximize the possibility of meeting quality requirements but, considering:

- the existing architecture of the voice network, very different from the GRX architecture, is based on hundreds of bilateral IP interconnections, and
- the intrinsic need of the wholesale business to route the call according the best price/quality trade-off,

the i3 Forum believes that the quality requirements can be achieved even if in some situations this GSMA IPX model constraint cannot always be met. Intercontinental calls are an example where the limit of 2 IPX–Ps cannot be guaranteed.

i3 Forum recognises that the number of involved IPX–Ps should not modify the quality requirements for a given SP-SP communication.

12.3 Routing Transparency

The minimum set of information that the IPX Provider shall provide to the Service Provider consists of the type of connectivity used to reach each terminating SP. These connections have to be classified into three groups depending if the connectivity is made through:

1) direct connectivity (i.e., there is only 1 IPX Provider from Originating Service Provider to terminating Service Provider),
2) indirect connectivity (i.e., there is more than 1 IPX Provider from Originating Service Provider to terminating Service Provider),
3) 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 provider and the service provider and applies under normal operating conditions (i.e., no network failures and/or no network congestion).

12.4 Opt-in / opt-out scheme

In compliance with GSMA doc AA.81 [12] section 6 no opt-in/opt-out scheme has to be supported for the VoIPX service.

12.5 Break-in / break-out connectivity

Break-in and break-out can be implemented via three technology options:

- via TDM interconnection
- via private IP interconnection as defined in section 6 of this document. This option implies that no unidentified third party is able to affect the bilateral voice over IPX service and hence:
    - only voice over IPX service or other IPX services traffic is exchanged across the interconnection;
    - only public IP addresses (provided by IANA) are used and they are not announced onto the Public Internet;
    - all the voice traffic, from the SP’s PE router to the IPX P’s border functions, shall be secured, either physically or logically, from Internet traffic.
- via public IP Interconnections as specified in section 6.1.4 of this document provided that
    - IPSec encryption is used for signalling information;
    - all the voice traffic, entering the IPX P network, crosses the IPX P’s border functions.

12.6 Role of DNS and ENUM registry

GSMA IR.67 provides guidelines for DNS and ENUM in the GRX/IPX architecture. As defined in IR.67 DNS on the GRX/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 for terminating a voice call but, as a matter of fact, many different solutions are already in the market for providing routing and addressing capabilities to carriers. 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 the spreading of advanced routing and addressing schemes (complementing ITU-T E.164 model or alternative to ITU-T E.164 model) will increase in the future and two i3 Forum deliverables ([8] and [9]) contain the first principles to be considered and the first guidelines to be followed. In any case, regardless the technical and market evolution, an IPX–P has the right to select its own technical and commercial solution in order to successfully route the call to destination.

12.7 Number Portability Resolution

GSMA IPX requirements indicate that the Service Provider to which the IPX Provider 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 [1] has also provided a requirement for number portability resolution by VoIPX providers. GSMA IPX plans for number portability resolution depend on the implementation of the PathFinder Carrier ENUM system. Prior to the point at which this achieved, VoIPX providers 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
- Queries or SIP INVITES directed to number block holding SPs

However, when the resolution of number portability is neither technically possible nor available, it is then possible for an IPX Provider to send traffic to a Service Provider, who, in turn, will transit the call to the recipient domestic Service Provider, if needed.

13 Accounting and Charging principles

13.1 Transit fee depending on destination

Transit fee (compensation charged by the IPX Provider for all the offered service excluding termination fee) for Multilateral Hubbing Service IPX connectivity options can vary and depends on 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 regulatory bodies or applicable law.

13.3 Accounting and Charging capabilities

The information flow to be exchanged from the transport and switching platforms with the relevant OSS/BSS systems is outside the scope of this document.

The information recorded in the Call Detail Record (CDR) shall support settlement and performance. The scope of this section includes only the data that require for exchange the information for settlement and performance. The CDR may also serve as a troubleshooting tool for certain information. This section does not address the format of the CDR in a carrier’s network nor the collecting method. Each carrier may have additional proprietary fields for internal uses, which is not in the scope of this section.

Since calls may be originated or terminated in TDM or VoIP network, the CDR shall support data attributes for these two types of calls and services. A comprehensive list of these attributes can be found on REF.

14 Annex A - Architecture of VoIPX platform

The following text is based on the joint GSMA's IPIA and i3 Forum activities carried out in 2009.

14.1 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. An SP may connect/contract more than one IPX P 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 Voice over IPX service develops in a way that is consistent with its core requirements of efficiency, quality of Service 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.

14.2 Global 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	IPX Zone – Multi -Party Interconnect Location	Regions in each IPX Zone
Americas	Equinish 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 8.3.2 of IR.34 [13]

The number of IPX Zones may increase as the IPX develops, and the level of commercial traffic over the IPX justifies this investment, but this shall be mutually agreed by a representative group of IPX Providers and Service Providers.

IPX Provider Interconnection Evolution

In order to assure DNS resolution, an IPX Provider will 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.