INTERNATIONAL INTERCONNECTION FORUM FOR SERVICES OVER IP

(i3 FORUM)

(www.i3forum.org)

Workstream "Technical Aspects"

Technical Interconnection Model for International Voice Services

(Release 3.0) May 2010

This document updates and replaces the i3 Forum document "Technical Interconnection Model for Bilateral Voice Services" (Release 2.0, May 2009).

EXECUTIVE SUMMARY

In order to allow a worldwide and unrestrained migration to IP of the thousands of existing TDM International voice interconnections, this document aims to specify, on the basis of existing standards/recommendations issued by international bodies (e.g. ITU-T, ETSI, IETF), a unique network architecture capable to support one (or a limited number of) interconnection model(s) for the implementation of trusted, secure and QoS compliant VoIP interconnection between International Wholesale Carriers.

In order to achieve this goal, the scope of the documents covers all the relevant technical issues e.g.:

- ✓ transport protocols/capabilities;
- ✓ signaling protocols (including SIGTRAN protocol for the support of mobile applications);
- ✓ media codec schemes;
- ✓ QoS levels with measurements and performance needs;
- ✓ E.164-based addressing schemes
- ✓ Security
- ✓ Accounting and Charging.

The specification of the VoIP and TDM interconnections of the international switching facilities with the domestic networks is outside the scope of this initiative.

Assuming a general reference configuration encompassing:

- ✓ switching platforms fed with TDM traffic as well as VoIP traffic from the domestic fixed and mobile networks and capable to manage signaling and media information onto an IP transport layer;
- ✓ border functions in order to separate IP domains enhancing service and network level of security;
- ✓ routing functions according to IP networking;
- ✓ transmission functions according to SDH/Ethernet –based systems and protocols;

and considering Public Internet as a global infrastructure, two main sets of configurations are recommended:

- ✓ *Private-oriented interconnection*: when no unidentified third party is able to affect the bilateral VoIP service;
- ✓ *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 which can affect the service performance and quality.

Though several signaling protocols are available on the market, two protocols have been selected as appropriate in this scenario: SIP protocol as defined in IETF RFC 3261 and complementing documents and ISUP enabled SIP profile as recommended in ITU-T Q.1912.5.

Media functions should assure transport for all the services and transcoding between different codecs. In the scope of this initiative the G.711 codec and the set of G.729 codec are considered mandatory.

Security, both from the network and service perspective, has been considered as a primary requirement for international VoIP interconnection. As a result, it is strongly recommended that all voice traffic coming into / leaving the network operator passes through Border Functions, i.e. all IP packets (for signaling and media), crossing this bilateral voice interconnection, are originated and received by such Border Functions.

Quality of Service parameters together with the relevant measurement points are defined for the Service Provider – Carrier relationship as well as for the Carrier to Carrier one. The identified parameters are pertinent to the transport layer (e.g., round trip delay, jitter, packet loss), to the service layer (e.g., MOS_{CQE}, ALOC, ASR, NER, PGRD) and to the call attributes (e.g., CLI transparency).

This deliverable is the third version of this technical interconnection document enhancing the sections related to quality of service control, coding (with the inclusion of LBR and WB codecs) and security (with the inclusion of a subsection devoted to discuss the most common threats in an IP environment). Future versions will be released encompassing new features / functions in order to consider the evolution of services, equipment capabilities and international standards.

Table of Contents

1 Scope of the document

The scope of this document is to address all the technical issues for the implementation of trusted, secure and QoS compliant IP-based interconnection of Voice Services (encompassing ISDN**,** fax and modem connections) between International Wholesale Operators considering:

- transport protocols/capabilities;
- signaling protocols
- media codec schemes;
- QoS levels with measurements and performance needs;
- E.164 addressing schemes;
- Security issues;
- Accounting and Charging Issues.

The support of applications based on the usage of the SIGTRAN suite of protocols is also considered in this document.

The results and deliverables of private and public standardisation/specification bodies, such as ITU-T, IETF, ETSI, GSMA, have been considered as well as it has been also verified the existence of any regulatory framework for international IP interconnection.

As far as the network platform is concerned, the present, and the short-term achievable, status of the art of the vendors' equipment has been considered.

All domestic legal rules and obligations are out of the scope of this document.

Though this document does not intend to address any specific IMS model, for the sake of consistency with widely used terminology, the IMS ETSI TISPAN naming conventions have been adopted for some functional blocks (e.g. border functions).

2 Objective of the document

The objective of the document is to define, on the basis of existing standards, a unique network architecture capable to support one (or a limited number of) interconnection model(s) for international voice over IP services encompassing bilateral interconnection as well as voice hubbing services.

Each interconnection model is fully described in terms of transport capabilities, signaling protocols, media codec schemes, available QoS levels, available numbering/addressing schemes, available security capabilities.

This deliverable is the third version of the document. Future versions will be released encompassing new features / capabilities to address the evolution of services, equipment capabilities and international standards.

The i3 Forum released a set of companion documents dealing with the service description [1], testing [3], codec selection [4], and migration template [5] for international voice over IP interconnection.

3 Acronyms

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
ANM	Answer Message
AS	Autonomous System
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
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
CW	Call waiting
DdoS	Distributed Denial of Service
DES	Data Encryption Standard
Diffserv	Differentiated Services
DoS	Denial of Service
DPO	Dynamic Port Opening
DSCP	Differentiated Services Code Point
DTMF	Dual-Tone Multi-Frequency
DWDM	Dense Wavelength Division Multiplexing
EF	Expedite Forward
EXP	MPLS header EXPerimental use field
FoIP	Fax over IP
GIC	Group Identification Code
GSDN	Global Software Defined Network
GSN	Global Subscriber Number
HW	Hardware
IAM	Initial Address Message
IBCF	Interconnection Border Control Function
I-BGF	Interconnection Border Gateway Function
IC	Identification Code
ICMP	Internet Control Message Protocol
IFP	Internet Facsimile Protocol
IFT	Internet Facsimile Transfer
IKE	Internet Key Exchange
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPSec	IP Security
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
IVR	Interactive Voice Response
KPI	Key Performance Indicator
LBR	Low Bit rate codec
MF	Multi-Field Classifier

MGCF	Media Gateway Control Function
MGF	Media Gateway Function
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
MPLS	Multiprotocol Label Switching
MTP	Message Transfer Part (SS7)
NAPT	Network Address and Port Translation
NAT	Network Address Translation
NDC	National Destination Code
NER	Network Efficiency Ratio
NNI	Network Network Interface
NN	National Number
OCN	Original Called Number
OIP	Originating Identity Presentation
OIR	Originating Identity Restriction
OLO	Other Licensed Operator
OSS	Operations Support System
P-router	Provider router
PDH	Plesiochronous Digital Hierarchy
PE-router	Provider Edge router
PGRD	Post Gateway Ringing Delay
PHB	Per-Hop Behaviour
POS	Packet Over SDH/Sonet
PSTN	Public Switched Telephone Network
QoS	Quality of Service
R-Factor	Rating-Factor
RgN	Redirecting Number
RI	Redirecting Information
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
SIP	Session Initiation Protocol
SIGTRAN	Signaling Transport suite of Protocols
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
SPRT	Simple Packet Relay Transport
SR/RR	Sender Report/Receiver Report
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TE MPLS	Traffic Engineering MPLS
tel-URI	Telephone Uniform Resource Identifier
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
TSG	Trunk Group
TUP	Telephone User Part
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UUI	User-to-User Information
UUS1	User to user signalling 1
VBD	Voice Band Data
VLAN	Virtual Local Area Network
VoIP	Voice over IP

VPN	Virtual Private Network
WB	Wideband codec

4 References

[1] i3 Forum “IP International Interconnections for Voice and other related services“ Release 1.0, June 2009
[2] i3 Forum “Service Value and Process of Measuring QoS KPIs“ Release 1.0, May 2010
[3] i3 Forum “Interoperability Test Plan for Bilateral Voice services” Release 2.0, May 2009
[4] i3 Forum White Paper “Optimal Codec Selection in International IP based Voice Networks” Release 2.0, May 2010
[5] i3 Forum “Interconnection Form for International Voice Service” Release 3.0, May 2010
[6] i3 Forum White Paper “Mapping of Signaling protocols from ISUP to SIP, SIP-I” Release 2.0, May 2010
[7] ETSI 123.517 “TISPAN IP Multimedia Subsystem (IMS); Functional architecture”
[8] IETF RFC 2474 “Definition of the Differentiated Services Field”, December 1998
[9] IETF RFC 2475 “An Architecture for Differentiated Services”, December 1998
[10] IETF RFC 3246 “Expedited Forwarding (Per-Hop Behavior)”, March 2002
[11] IETF RFC 3247 “Supplemental Information for the New Definition of the EF PHB (Expedited Forwarding Per-Hop Behavior)”, March 2002
[12] IETF RFC 2597 “Assured Forwarding PHB Group”, June 1999
[13] IETF RFC 4594 “Configuration Guidelines for Diffserv Service Classes”, August 2006
[14] IETF RFC 1918 “Address Allocation for Private Internets”, February 1996
[15] IETF draft-ietf-bfd-base-08.txt “Bidirectional Forwarding Detection”, March, 2008
[16] IETF RFC 4271 “A Border Gateway Protocol 4 (BGP-4)”, January 2006
[17] IETF RFC 3261 “SIP: Session Initiation Protocol”, June 2002
[18] IETF RFC 3966 “The tel URI for Telephone Numbers”, December 2004
[19] IETF RFC 3323 “A Privacy Mechanism for the Session Initiation Protocol (SIP)”, September 2002
[20] IETF RFC 3325 “SIP Extensions for Network-Asserted Caller Identity and Privacy within Trusted Networks”, September 2002
[21] IETF RFC 4028 “Session Timers in the Session Initiation Protocol (SIP)”, April 2005
[22] ITU-T Recommendation Q1912.5 “Interworking between Session Initiation Protocol and Bearer Independent Call Control or ISDN User Part, 2004
[23] IETF RFC 4566, “SDP: Session Description Protocol”, July 2006
[24] IETF RFC 3550 “RTP: A Transport Protocol for Real-Time Applications”, July 2003
[25] IETF RFC 3551, “RTP Profile for Audio and Video Conferences with Minimal Control”, July 2003
[26] IETF RFC 3555, “MIME Type Registration of RTP Payload Formats”, July 2003
[27] IETF RFC 2833, “RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals”, May 2000
[28] IETF RFC 4040, “RTP Payload Format for a 64 kbit/s Transparent Call”, April 2005
[29] IETF RFC 3362 “Real-time Facsimile (T.38) – image/t38 MIME Sub-type Registration,”, August 2002
[30] ITU-T T.38 Procedures for real-time Group 3 facsimile communication over IP networks, 1998
[31] IETF RFC 768 “User Datagram Protocol”, August 1980
[32] ITU-T Recommendation E.164 “The international public telecommunication numbering plan”, 1997
[33] ITU-T Recommendation G.729 “Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)”, 1996
[34] ITU-T Recommendation G.711 “Pulse Code Modulation (PCM) of Voice Frequencies”, 1988
[35] IETF RFC 5806 “Diversion Indication in SIP”, March 2010
[36] IETF RFC 4458 “Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR)”, April 2006.
[37] IETF RFC 3389 “Real-time Transport Protocol (RTP) Payload for Comfort Noise (CN)” September 2002
[38] IETF RFC 4733 “RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals” December 2006
[39] 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
[40] IETF RFC 4749 “RTP Payload Format for the G.729.1 Audio Codec” October 2006
[41] IETF RFC 3555 “MIME Type Registration of RTP Payload Formats”, July 2003
[42] IETF RFC 4117 “Transcoding Services Invocation in the Session Initiation Protocol (SIP) Using Third Party Call Control (3pcc)” (June 2005).
[43] ITU-T Recommendation T.38 “Procedures for real-time Group 3 facsimile communication over IP networks” (04/2007)
[44] ITU-T Recommendation V.150 “Modem-over-IP networks: Foundation” (07/2003).
[45] ITU-T Recommendation G.729 “Coding of speech at 8 kbit/s using conjugate-structure algebraic code excited linear-prediction (CS-ALEP (01/07)
[46] ITU-T Recommendation G.729 Annex A “Reduced complexity 8kbit/s CS-ALEP codec” (11/96)
[47] ITU-T Recommendation G.729 Annex B Silence compression scheme for G.729 optimized for terminals conforming to Recommendation V.70” (11/96)
[48] ITU-T Recommendation G.729 Annex A and B
[49] IETF RFC 2663 “IP Network Address Translator (NAT) Terminology and Considerations”, August 1999
[50] IETF RFC 2401 “Security Architecture for the Internet Protocol”, November 1998
[51] IETF RFC 2246 “The TLS Protocol”, January 1999
[52] IETF RFC 4306 “Internet Key Exchange (IKEv2) Protocol”, December 2005
[53] ITU-T Recommendation. G.703: “Physical/electrical characteristics of hierarchical digital interfaces”, November 2001;
[54] ITU-T Recommendation. G.704 “Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical”, October 1998;
[55] ITU-T Recommendation. G.705 “Characteristics of plesiochronous digital hierarchy (PDH) equipment functional”, October 2000;

[56] ITU-T G.707: Network Node Interface for the Synchronous Digital Hierarchy(SDH), 01/2007
[57] ANSI T1.105: SONET - Basic Description including Multiplex Structure, Rates and Formats
[58] IETF RFC 1423 - Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers, February 1993
[59] RFC 2396 “Uniform Resource Identifiers (URI): Generic Syntax”, August 1998
[60] 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
[61] ITU-T Recommendation Y.1540 “Internet Protocol Data Communications Services - IP Packet Transfer and availability performance parameters”, November 2007
[62] ITU-T Recommendation E. 411 “International Network Management – Operational guidance”, March 2000
[63] ITU-T Recommendation E.425 “Network Management – Checking the quality of the international telephone service. Internal automatic observations”, March 2002
[64] ITU-T Recommendation E.437 “Comparative metrics for network performance management”, May 1999
[65] ITU-T Recommendation P.10 “Vocabulary of terms on telephone transmission quality and telephone sets”, December 1998
[66] ITU-T Recommendation G.107 “The E model, a computational model for use in transmission planning”, March 2005
[67] 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
[68] ITU-T Recommendation V.152 “Procedures for supporting voice-band data over IP networks” , January 2005.
[69] ITU-T Recommendation Q.767, “Specification of Signaling System No.7, Application of the User Part of CCITT Signaling System No.7 for International Interconnection ISDN”, 1991
[70] IETF RFC 3393 “IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)”, November 2002
[71] IETF RFC 4960 “Stream Control Transmission Protocol”
[72] IETF RFC 4166 “Telephony Signaling Transport over Stream Control Transmission Protocol (SCTP) Applicability Statement“, February 2006
[73] IETF RFC 4165 “Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) - User Peer-to-Peer Adaptation Layer (M2PA)“, September 2005
[74] IETF RFC 3332 & 4666 “Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) - User Adaptation Layer (M3UA)”, September 2006
[75] IETF RFC 3788 “Security Considerations for Signaling Transport (SIGTRAN) Protocols”, June 2004
[76] IETF RFC 3960 “Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)”, December 2004
[77] 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”
[78] 3GPP TS 29.164 “Interworking between the 3GPP CS domain with BICC or ISUP as signaling protocol and external SIP-I networks”
[79] IETF RFC 2508 “Compressing IP/UDP/RTP Headers for Low-Speed Serial Links”, February 1999.
[80] IETF RFC 3095 “Robust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed”, July 2001.
[81] IETF RFC 3311 “The Session Initiation Protocol (SIP) UPDATE Method”, September 2002
[82] IETF RFC 2976 “The SIP INFO Method”, October 2000
[83] IETF RFC 3262 “Reliability of Provisional Responses in the Session Initiation Protocol (SIP)”, June 2002
[84] IETF RFC 3428 “Session Initiation Protocol (SIP) Extension for Instant Messaging”, December 2002
[85] IETF RFC 3903 “Session Initiation Protocol (SIP) Extension for Event State Publication”, October 2004
[86] IETF RFC 3515 “The Session Initiation Protocol (SIP) Refer Method”, April 2003
[87] IETF RFC 3265 “Session Initiation Protocol (SIP)-Specific Event Notification”, June 2002
[88] IETF RFC 3326 “The Reason Header Field for the Session Initiation Protocol (SIP)”, December 2002

5 General Reference Architecture

The general reference configuration for international voice interconnection based on IP protocol is given in Figure 1. Carriers operate switching facilities which are fed with TDM traffic as well as VoIP traffic from the domestic fixed and mobile networks. The interconnection between two Carriers makes use of signaling protocol (see Section 7) and media (see Section 8) flows carried onto an IP transport layer (see Section 6).

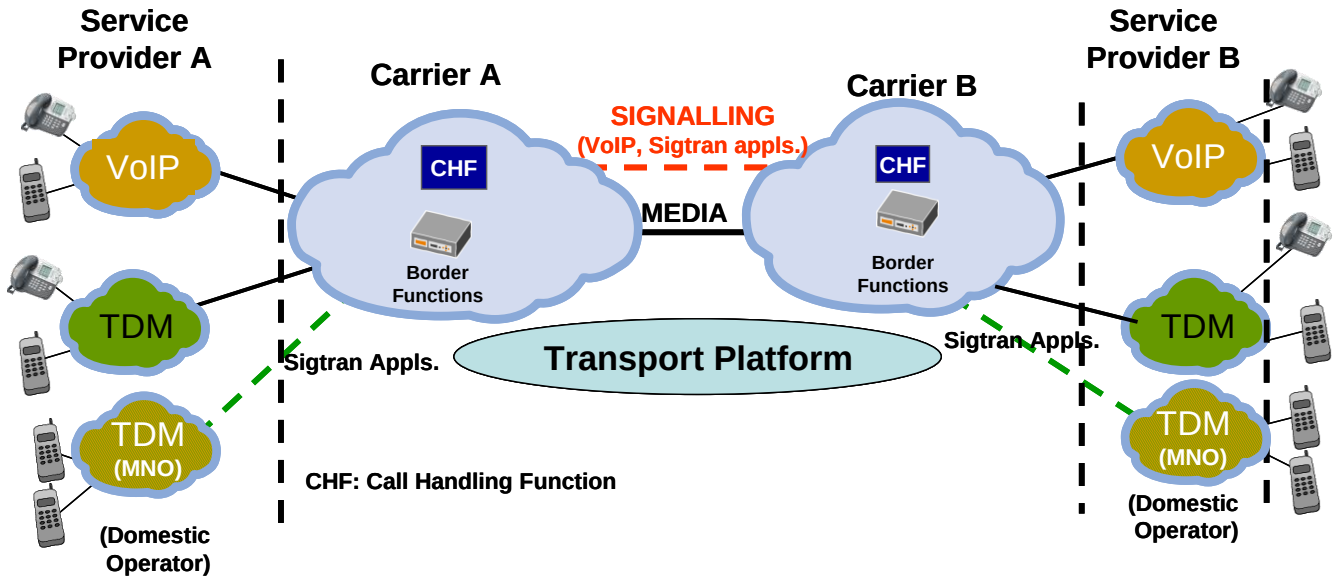


Figure 1 – General Reference Configuration

The above general reference configuration also supports:

- ISDN services (see Section 7 for the relevant characteristics)
- legacy Signaling System #7-based applications over an IP transport making use of the SIGTRAN suite of protocols. Specific applications considered in this document are SMS, Camel and roaming mobile signaling applications [1].

5.1 Service reference configuration

The service reference configuration is depicted in Figure 2.

Four basic functional blocks have been identified:

1) the Call Handling Function which performs the functions related to signaling management, call routing, control of the Media Gateways and redirection of signaling and media to the Border Functions. For the sake of consistency with IMS TISPAN terminology, in Figure 2 the Call Handling Function encompasses some capabilities of the functional blocks “Call Session Control Function” (CSCF), the Media Gateway Control Function (MGCF) and the Breakout Gateway Control Function (BGCF).
2) the Media Gateway Function (MGF) which is devoted to the transcoding of the media flow from/to TDM domain and IP domain;
3) the Signaling Gateway Function (SGF) which is devoted to manage the SIGTRAN connections and to interwork SIGTRAN with MTP;
4) the Border Function which is devoted to separate the IP domain of the two carriers in order to implement trusted and secure VoIP interconnections. The border function applies to both the control plane and the user plane. For the sake of consistency with IMS TISPAN terminology, in Figure 2:
   - The control plane border function is identified with the Interconnection Border Control Function (IBCF) [7];
   - The user plane border function is identified with I-Border Gateway Function (I-BGF) [7].

The implementation of integrated Border Function (i.e co-located IBCF and I-BGF) vs. distributed Border Function (i.e. IBCF geographically separated from I-BGF) depends on the specific carrier’s implementation and it is not the subject of this document.

Additional information on how to use the border function for security purposes is given in Section 9 of this document.

The Call Handling Function of the Carrier's international switching facility receives VoIP and TDM signaling from the domestic network. The specification of the VoIP and TDM interconnections of the international switching facilities with the domestic networks is outside the scope of this document.

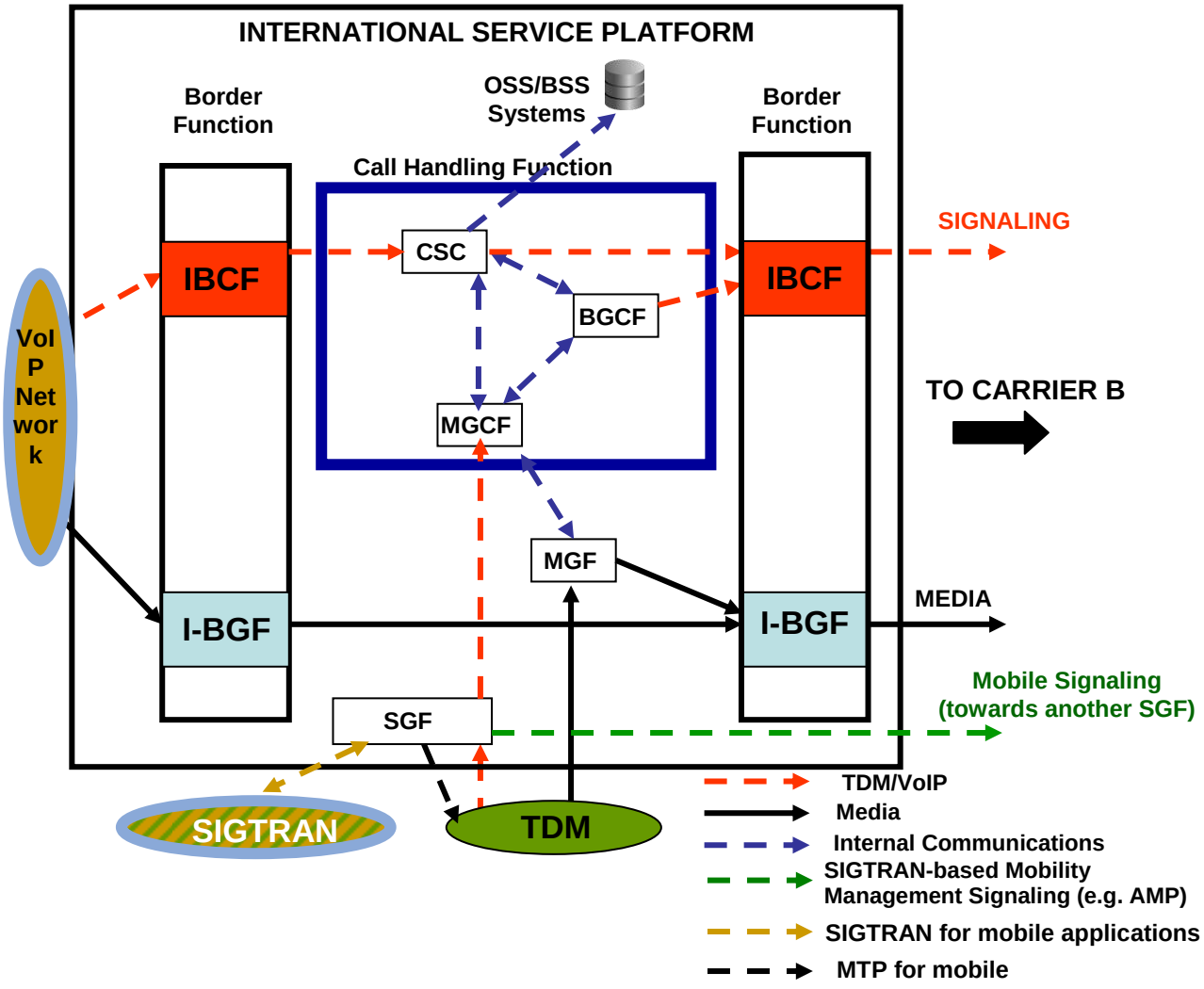


Figure 2 – Service Reference Configuration

The specification of the Signaling and Media information is given in Sections 7 and 8 of this document, respectively.

The specification of the minimum set of information elements produced by OSS/ BSS systems for accounting and charging functions is given in Section 12.

5.1.1 Functions to be performed for the incoming domestic voice traffic

For the TDM traffic, the Call Handling Function:

- receives the Common Channel Signaling #7
- converts in suitable protocols for VoIP traffic;
- identifies the proper routing towards the egress port;
- controls the Media Getaways, which, in turn, convert the TDM media flows to RTP media flows;
- the signaling is sent to the IBCF which controls I-BGF identifying the involved I-BGF resources where the RTP media flow has to be directed.

For VoIP traffic, the Call Handling Function:

- receives the proper signaling information (e.g. SIP, SIP-I);
- converts, if needed, to suitable protocols for VoIP traffic;
- identifies the proper routing towards the egress port;
- sends signaling to the IBCF identifying the I-BGF resources where the RTP media flow has to be directed.

5.1.2 Functions to be performed for the incoming voice international traffic

IBCF receives the signaling information (e.g. SIP, SIP-I) from the corresponding carrier and forwards this signaling information to the Call Handling Function.

The Call Handling Function:

- identifies the proper routing towards the egress port;
- performs signaling interworking, if needed;
- in case of delivering towards a TDM-based network, controls the identified Media Gateway Functions for delivering the media information;
- in case of delivering towards a VoIP-based network, the signaling information is sent to the IBCF which controls I-BGF identifying the involved I-BGF resources where the RTP media flow has to be directed.

5.1.3 Functions to be performed for the SIGTRAN traffic

For the SIGTRAN traffic, the Signaling Gateway Function:

- receives the proper signaling information;
- identifies the proper routing towards the egress port;
- performs, if needed, interworking between MTP and SIGTRAN;
- handles mobility protocols for interworking with wireless networks.

5.2 Transport reference configuration

Different transport configurations can be identified distinguishing between Private IP Interconnection and Public IP Interconnection. In turn, different options are viable for these two main categories. The definition of Private and Public IP Interconnection is given in Section 6 of this document.

At the transmission layer either SDH transmission system or Ethernet-based systems are possible solutions. Additional information of these transmission systems are given in Section 6 of this document.

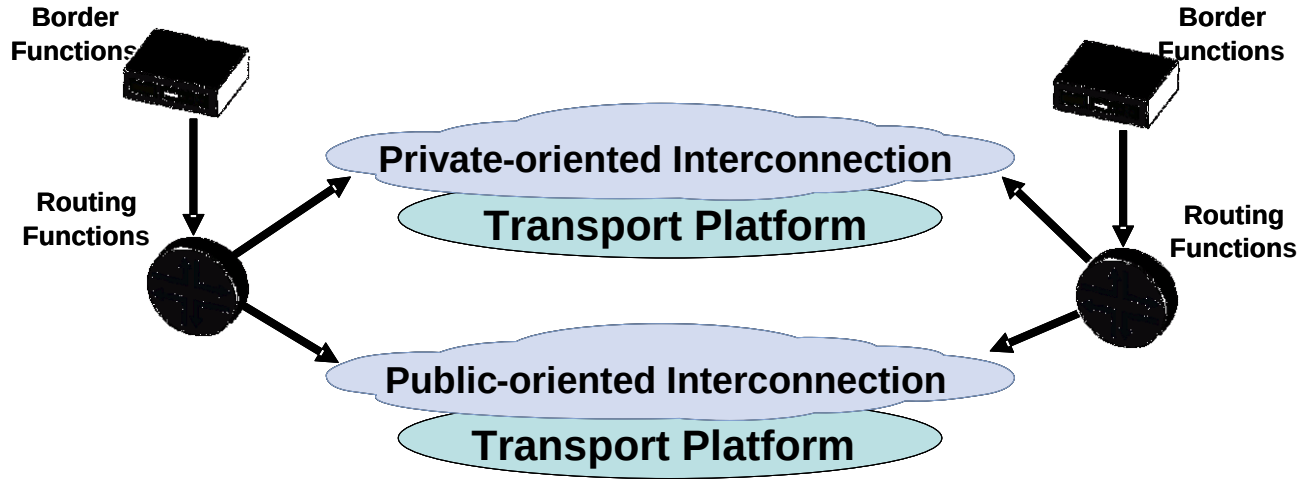


Figure 3 – Transport Reference Configuration

6 Transport Functions

This section recommends alternative reference transport configurations for implementing bilateral international VoIP interconnections.

Assuming as Public Internet a global infrastructure, interconnecting managed *IP* networks, 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;
- *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 which can affect the service performance and quality.

This section exclusively deals with the Transport Functions. Signalling Functions and Media Functions are discussed in Sections 7 and 8, respectively.

6.1 Transport functions for private-oriented interconnections

In the following subsections three 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:

1) Only VoIP and/or private data services traffic is exchanged across the interconnection;

2) All the involved IP addresses (i.e. *PE router* interface, *P router* interface, border function interface) can not be reached from unidentified entities via Public Internet. As a result, these IP addresses can be private or public, but they shall not be announced onto the Public Internet.

A hybrid configuration (i.e. carrier A using public not announced IP addresses and carrier B using private IP addresses), though technically feasible, is not recommended since it implies additional operational efforts for the management of the address spaces.

3) The VoIP traffic, from the PE router to the border function in a carrier's domain, shall be secured, either physically or logically, from the Internet Transit traffic.

This security can be achieved:

- *physically*: by implementing separated and dedicated networks for the two types of traffic.
- *logically*: implementing different mechanism such as native MPLS, Virtual Private Network (at layer 2 and 3) and Tunneling (e.g. TE MPLS, IP Sec).

The QoS issues are dealt with in Section 10.

6.1.1 Layer 1 interconnection

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

Figure 4 – Layer 1 Private-oriented Interconnection Configuration

6.1.2 Layer 2 interconnection

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

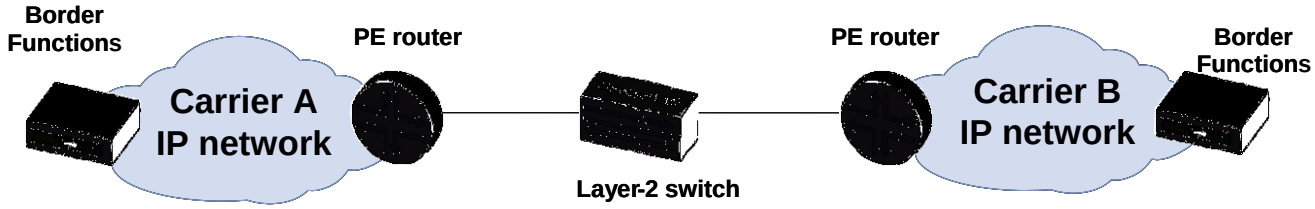


Figure 5 – Layer 2 Private-oriented Interconnection Configuration

6.1.3 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.

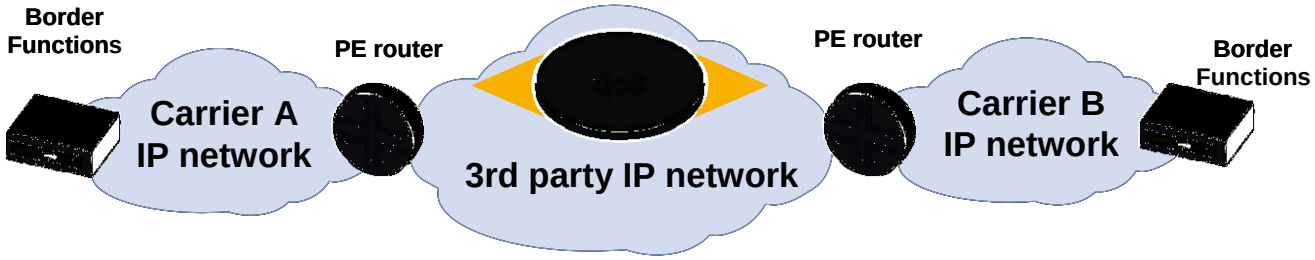


Figure 6 – Layer 3 Private-oriented Interconnection Configuration

6.2 Transport functions for public-oriented interconnection

In the following subsections two public-oriented scenarios are given which differentiate each other at the interconnection layer.

In order to retain the public interconnection feature it is assumed that some IP addresses to be used in these configurations can be reached from unidentified entities via Public Internet.

6.2.1 Layer 1 / layer 2 direct interconnection sharing data+VoIP

In this configuration Internet traffic as well as VoIP traffic is exchanged directly:

1) over the same physical link;
2) via a layer 2 switch.

In both cases, layer-2 traffic encapsulation can be used by configuring VLAN based on IEEE 802.1q standard. Carriers may use QoS mechanisms (e.g. Diffserv) to guarantee VoIP traffic performance over the interconnection. The IP addresses of the involved PE routers interfaces shall be public and they may be announced over the Public Internet. Border function IP addresses shall be exchanged only by the two carriers (i.e., using the no-export BGP community attribute).

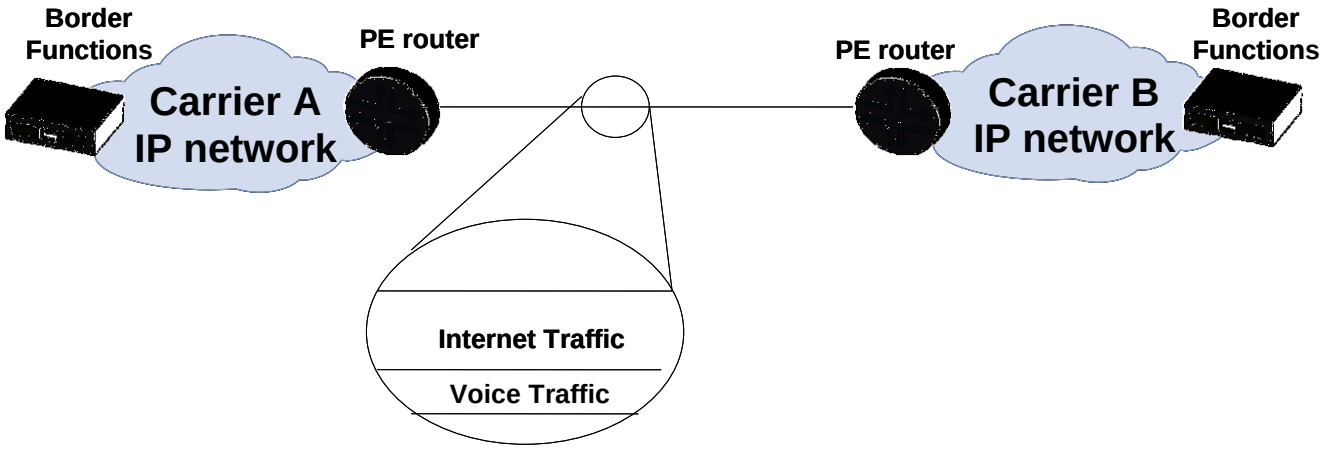


Figure 7 – Layer 1 / 2 Public-oriented Direct Interconnection Configuration

6.2.2 Indirect interconnection via public Internet

In this configuration the VoIP traffic passes through Public Internet, i.e. through a third (or multiple) Internet Transit providers.

The IP addresses of the PE routers as well as those of the Border functions shall be public and they shall be announced over the Public Internet.

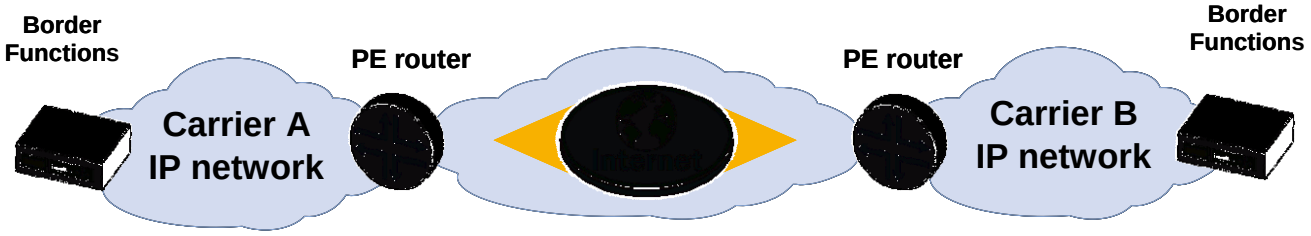


Figure 8 – Indirect Public-oriented Interconnection Configuration

This configuration includes the case where PE routers are interconnected via an IPSec tunnel onto the public Internet. More information on encryption requirements are given in Section 10.

This scenario implies lower values of QoS parameters than the interconnection configurations described in Section 6.1 since uncontrolled network segments are present from origin to destination of the call, but allows simpler and faster interconnection provisioning.

6.3 Physical interconnection alternatives

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

6.3.1 PDH-based transport systems

The ITU-T Recommendations G. Series shall be considered as reference documents: ITU-T Rec. G.703 [53], G.704 [54] and G.705 [55].

6.3.2 SDH-based transport systems

The ITU-T Recommendations G. Series shall be considered as reference documents: ITU T Rec. G.707 [56]

For North America another reference document is ANSI T1.105 [57]

6.3.3 Ethernet-based transport systems

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

6.3.4 DWDM-based transport systems

For the public interconnection configurations, a DWDM channel can be provisioned for interconnecting two carries.

6.3.5 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.

6.4 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 over-provisioning factor.

6.5 IP Routing and IP Addressing

6.5.1 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 [16] or a static routing protocol can be used to exchange routes between carriers' networks.

If the BGP protocol is used, two cases have to be considered:

a) direct AS (Autonomous System) connection (see Sections 6.1.1, 6.1.2, 6.2.1): the NO_EXPORT communities attribute shall be set;
b) indirect AS connection (see Sections 6.1.3, 6.2.2): the NO_EXPORT communities attribute shall not be set.

It is recommended to tune timer parameters at proper values, which depend on specific implementation, to ensure better convergence for recovering needs. Alternatively, BFD [15] could also be used to speed up link failure detection and subsequent protocol convergence.

6.5.2 IP Addressing

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

If public addresses are used, then the carriers will use only IP addresses assigned by IANA or related bodies. If private addresses [14] are used, the bilateral agreement has to specify the IP addressing scheme.

6.6 IP Packet marking

The following table describes the traffic classes defined for all the interconnection configurations described above:

Traffic class	Traffic type
Voice Media	Speech / Voice bearer.
Voice Signaling	Voice Control Traffic (SIP, SIP-I signaling protocols)I
Mobile Signaling	SMS and roaming (TCAP signaling protocol)
Other Customer Traffic	Internet traffic, other data traffic

Other control/management traffic such as BGP traffic crosses the interface.

6.6.1 Distinguishing traffic classes

In order to distinguish between traffic classes, the use of the DSCP marking scheme in Behaviour Aggregation mode [9] is recommended.

Using classification based on the DSCP value, packet marking is pre-agreed by both operators. The receiving operator assumes that the sending operator has marked the packet correctly according to the pre-agreed scheme described above.

If there is a mix of Internet and VoIP traffic across the interconnection or the recommended marking cannot be guaranteed, an alternative solution is to classify packets using the Multi-Field classification method [9]. Using this scheme, ingress traffic is classified by the receiving Operator PE Router based on any field in the IP header, e.g. destination address, source address, port numbers or other IP packet header fields.

6.6.2 IP Marking table

The following table recommends the packet marking guideline for the link/network for all above interconnection configurations making use of the DiffServ (IETF RFC and IP Precedence TOS marking scheme plus the coding scheme at the MPLS and Ethernet layers, respectively. It applies to the traffic to be transmitted.

Traffic Type	DSCP Marking	IP Precedence	802.1Q VLAN
Voice Media	for configurations 6.1, 6.2.1 DSCP 46/EF (101110).	5	5
	for configurations 6.2.2 DSCP 46/EF (101110) or DSCP 00/DF (000000).	5 or 0	5 or 0
Voice Signaling,	for configurations 6.1, 6.2.1 DSCP 26/AF31 (011010) or DSCP 46/EF (101110)	3 or 5	3 or 5
	for configurations 6.2.2 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 Signaling	for configurations 6.1, 6.2.1 DSCP 26/AF31 (011010) or DSCP 46/EF (101110)	3 or 5	3 or 5
	for configurations 6.2.2 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

The marking for the other control/management traffic depends on the specific network implementation.

6.6.3 Traffic treatment

For interconnection configurations specified in Sections 6.1 and 6.2.1, voice media traffic leaving the sending Border Function towards the receiving operator Border Function should be treated according to the Expedited Forwarding Per-Hop Behavior [10], [11].

For the interconnection configuration specified in Section 6.2.2, voice media traffic leaving the sending Border Function towards the sending PE router is treated either according to the Expedited Forwarding Per-Hop Behavior [10], [11] or according to Default forwarding Per-Hop Behavior [1] that is, it becomes 'best effort' forwarding.

For interconnection configurations specified in Sections 6.1 and 6.2.1, voice signaling traffic leaving the sending Border Function towards the receiving operator Border Function should be treated according to the Expedite Forwarding Per-Hop Behavior [10], [11], or alternatively according to the Assured Forwarding Per-Hop Behavior [12].

The industry uses both AF and EF PHB for signaling traffic. Where one carrier internally uses AF and the other interconnecting carrier internally uses EF, then bilateral agreement is needed on how to configure the interconnection to re-mark the packets as required in both directions. Further if different DSCP markings within the AF class are used, bilateral agreement will be required regarding whether the different marking is maintained or traffic re-marked as described for AF / EF marking.

For the interconnection configuration specified in Section 6.2.2, signalling traffic leaving the sending Border Function towards the sending PE router is treated either according to:

- the Expedite Forwarding Per-Hop Behavior, as specified in RFC 3246 [10] and 3247 [11];
- the Assured Forwarding Per-Hop Behavior as specified in RFC 2597 [12];
- the Default forwarding PHB , as specified in IETF RFC 2474 [8].

7 Signaling Functions

The interconnections described in this document shall support either a basic SIP profile (as described in Section 7.1) or an ISUP enabled SIP profile (as described in Section 7.2) or SIGTRAN for additional signaling purposes such as SMS, Camel and mobile roaming (as described in Section 7.4).

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

This subsection describes the basic SIP profile.

7.1.1 Transport of SIP (IETF RFC 3261) signaling information

The SIP protocol can be transported over UDP [31], TCP or SCTP. IETF RFC 3261 [17] defines that UDP is the default for SIP.

In the scope of this document UDP shall be used as default. If a non-reliable transport implementation is used then TCP may be used based on bilateral agreements.

There is also the possibility to use the newer transport protocol SCTP. Since support from vendors is not widely available at the date when this document is published, the use of SCTP is left as part of the specific bilateral agreement.

7.1.2 SIP signaling protocol profile

The basic SIP profile shall comply with RFC 3261 [17] 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 112.
- The support of IETF RFC 4028 [21], which addresses SIP Timers specification, is optional. The carrier receiving the INVITE message shall comply with IETF RFC 3261 [17] section 16.8 if IETF RFC 4028 [21] is not supported**.**
- The P-Asserted-Identity header defined in RFC 3325 [20] shall be supported.
- The Privacy header defined in RFC 3323 [19] shall be supported.
- The Diversion header defined in RFC 5806 [35] 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 3325, 3323). When the SIP message is passed to a trusted domain, the P-Asserted-Identity header should not be removed ([IETF RFC 3325]).

7.1.3 SIP Message support

The following table specifies how the SIP messages shall be supported.

#	SIP Message	Observations

#	SIP Message	Observations
1	REGISTER	The REGISTER message is not needed in the scope of this document.
2	INVITE	The INVITE message shall be supported as described in IETF RFC 3261 [17].
3	ACK	The ACK message shall be supported as described in IETF RFC 3261 [17].
4	CANCEL	The CANCEL message shall be supported as described in IETF RFC 3261 [17].
5	BYE	The BYE message shall be supported as described in IETF RFC 3261 [17].
6	OPTIONS	The OPTIONS messages shall be supported as described in IETF RFC 3261 [17]. SIP message OPTIONS can be used to probe reachability and availability as follows: periodic SIP OPTIONS messages are sent to the other party to check if the route is still valid; after several unanswered messages the route gets dropped. The use of this feature is subject to bilateral agreement.
7	UPDATE	The UPDATE message described in IETF RFC 3311 [81] may be used subject to bilateral agreement
8	INFO	The INFO message described in IETF RFC 2976 [82] may be used subject to bilateral agreement
9	PRACK	The PRACK message described in IETF RFC 3262 [83] may be used subject to bilateral agreement
10	MESSAGE	The MESSAGE message described in IETF RFC 3428 [84] may be used subject to bilateral agreement
	PUBLISH	The PUBLISH message described in IETF RFC 3903 [85] may be used subject to bilateral agreement
11	REFER	The REFER message described in IETF RFC 3515 [86] may be used subject to bilateral agreement
12	SUBSCRIBE	The SUBSCRIBE message described in IETF RFC 3265 [87] may be used subject to bilateral agreement
13	NOTIFY	The NOTIFY message described in IETF RFC 3265 [87] may be used subject to bilateral agreement

7.1.4 SIP Header support

The following table specifies how the SIP header shall be supported.

#	Header	Observations
1	Accept	The Accept header shall be used as defined in section 20.1 of RFC 3261 [17] with the addition that accepting application/sdp is mandatory.
2	Accept-Encoding	The Accept-Encoding header shall be used as defined in section 20.2 of RFC3261 [17].
3	Accept-Language	The Accept-Language header shall be used as defined in section 20.3 of RFC 3261 [17]. Standard English language (en) is mandatory.
4	Alert-Info	The Alert-Info header is not applicable in the scope of this document.
5	Allow	The Allow header shall be used as defined in section 20.5 of RFC 3261 [17] with the addition that it should be mandatory in all response messages (it reduces the number of messages exchanged).
6	Authentication-Info	The Authentication-Info header is not applicable in the scope of this document.
7	Authorization	The Authorization header is not applicable in the scope of this document.
8	Call-ID	The Call-ID header shall be used as defined in section 20.8 of RFC 3261 [17].
9	Call-Info	The support of Call-Info header is optional and should be agreed between the interconnecting Carriers.
10	Contact	The Contact header shall be used as defined in section 20.10 of RFC 3261 [17]. Privacy considerations might modify its value.
11	Content-Disposition	The Content-Disposition header shall be used as defined in section 20.11 of RFC 3261 [17].
12	Content-Encoding	The Content-Encoding header shall be used as defined in section 20.12 of RFC 3261 [17].
13	Content-Language	The Content-Language header shall be used as defined in section 20.13 of RFC 3261 [17].
14	Content-Length	The Content-Length header shall be used as defined in section 20.14 of RFC 3261 [17].
15	Content-Type	The Content-Type header shall be used as defined in section 20.15 of RFC

#	Header	Observations
		3261 [17]. Support for Content-Type of application/sdp is mandatory.
16	Cseq	The Cseq header shall be used as defined in section 20.16 of RFC 3261 [17].
17	Date	The Date header shall be used as defined in section 20.17 of RFC 3261 [17].
18	Error-Info	The Error-Info header shall be used as defined in section 20.18 of RFC 3261 [17].
19	Expires	The Expires header shall be used as defined in section 20.19 of RFC 3261 [17].
20	From	The From header shall be used as defined in section 20.20 of RFC 3261. Privacy considerations might modify its value.
21	In-Reply-To	The In-Reply-To header shall be used as defined in section 20.21 of RFC 3261 [17].
22	Max-Forwards	The Max-Forwards header shall be used as defined in section 20.22 of RFC 3261 [17].
23	Min-Expires	The Min-Expires header shall be used as defined in section 20.23 of RFC 3261 [17].
24	MIME-Version	The MIME-Version header shall be used as defined in section 20.24 of RFC 3261 [17].
25	Organization	The Organization header shall be used as defined in section 20.25 of RFC 3261 [17].
26	P-Asserted-Identity	The P-Asserted-Identity shall be used as defined in RFC 3325 [20].
27	Priority	The Priority header shall be used as defined in section 20.26 of RFC 3261 [17].
28	Privacy	The Privacy header shall be used as defined in RFC 3323 [19].
29	Proxy-Authenticate	The Proxy-Authenticate header is not applicable in the scope of this document.
30	Proxy-Authorization	The Proxy-Authorization header is not applicable in the scope of this document.
31	Proxy-Require	The Proxy-Require header is not applicable in the scope of this document.
32	Reason Header	The Reason Header should be used as defined in IETF RFC 3326 [88].
33	Record-Route	The Record-Route header is not applicable in the scope of this document.
34	Reply-To	The Reply-To header shall be used as defined in section 20.31 of RFC 3261 [17]. Privacy considerations might modify its value.
35	Require	The Require header shall be used as defined in section 20.32 of RFC 3261 [17].
36	Retry-After	The Retry-After header shall be used as defined in section 20.33 of RFC 3261 [17].
37	Route	The Route header is not applicable in the scope of this document.
38	Server	The Server header shall be used as defined in section 20.35 of RFC 3261 [17].
39	Subject	The Subject header shall be used as defined in section 20.36 of RFC 3261 [17].
40	Supported	The Supported header shall be used as defined in section 20.37 of RFC 3261 [17].
41	Timestamp	The Timestamp header shall be used as defined in section 20.38 of RFC 3261 [17].
42	To	The To header shall be used as defined in section 20.39 of RFC 3261 [17]. Privacy considerations might modify its value.
43	Unsupported	The Unsupported header shall be used as defined in section 20.40 of RFC 3261 [17].
44	User-Agent	The User-Agent header shall be used as defined in section 20.41 of RFC 3261 [17].
45	Via	The Via header shall be used as defined in section 20.42 of RFC 3261 [17].
46	Warning	The Warning header shall be used as defined in section 20.43 of RFC 3261 [17].
47	WWW-Authenticate	The WWW-Authenticate header is not applicable in the scope of this document.

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

This subsection describes the ISUP-enabled SIP profile.

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

See Section 7.1.1.

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

This signaling protocol profile shall be in accordance with ITU-T Recommendation Q.1912.5 [22] Annex C Profile C.

7.2.3 ISDN Supplementary service support for SIP-I

The implementation of SIP-I based interconnection is transparent for the support of ISDN bearer services, including video services, as well as ISDN Supplementary Services.

Assuming ITU-T Q.767 [69] as the reference document for the identification of the ISDN bearer services to be supported onto an international circuit; namely:

Category: Circuit mode

- 64 kbit/s unrestricted
- Speech
- 3,1 kHz audio

it is recommended that the same bearer capabilities are supported on an international IP link.

The following listed Supplementary Services are part of the ISUP encapsulation mechanism and there is no need of additional interworking function:

- Calling Line Identification Presentation (CLIP)
- Calling Line Identification Restriction (CLIR)
- Connected Line Identification Presentation (COLP)
- CLIP no screening
- COLP no screening
- Connected line Identification Restriction (COLR)
- Call Deflection during alerting (CD)
- Call Forwarding (CF)´
- Anonymous Call Rejection (ACR)
- Reject Forward call (only if Call Forwarding indication is provided by ISUP)
- Call waiting (CW)
- Three-Party conference (3PTY) (depending on special situation via destination IP-network)
- Closed user Group (CUG)
- User to user signaling 1(UUS1)

As some ISDN services are delay sensitive, in order to meet standard quality levels, it is preferable to provide ISDN services via private-oriented interconnections (see Section 6.1).

Video services based on 64 kbit/s unrestricted channel bearer capability are supported.

7.3 Mapping of ISUP to SIP or SIP-I signaling 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 behavior for session control.

The most straightforward case is ISUP to SIP-I in accordance with specification ITU Q1912.5, Annex C Profile C [22]. 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.

It is the view of the i3 Forum that these problems are sufficiently acute that the industry needs to address the issue as a matter of urgency to agree one common standard for mapping between SIP and ISUP and then implement this on all relevant vendor platforms as quickly as possible.

As a partial solution, the support of the Reason Header field in SIP is recommended since it can alleviate the majority of mapping issues where ISUP disconnect cause values can be retrieved.

For further information on this subject, refer to the i3 Forum White Paper “Mapping of Signaling Protocols from ISUP to SIP, SIP-I” [6].

7.4 Functions for supporting signaling protocol SIGTRAN

The suite of SIGTRAN protocols enable the transport of Signaling System #7 (SS7) messages over an IP transport layer as defined in Section 6. This section provides guidelines on the implementation of the following SIGTRAN protocols for inter-carrier connectivity.

7.4.1 Identification of SIGTRAN adaptation protocol stack

Among the various SIGTRAN adaptation protocol stacks, for the interconnection between Signaling Gateways Functions (SGF), for the inter-carrier connectivity, the Message Transfer Part 2 Peer-to-Peer Adaptation Layer (M2PA) should be considered as the preferred solution since it is the only one with relaying capabilities (i.e. it is possible to continue SS#7 MTP traffic routing beyond the end-point of the M2PA connection).

The Message Transfer Part 3 User Adaptation Layer (M3UA) may be used in the case when no relaying capability is needed (i.e. a SCCP connection with the corresponding carrier).

In all cases, the Stream Control Transmission Protocol (SCTP) shall be used between the IP layer and the SIGTRAN adaptation layers.

7.4.2 SCTP

SCTP shall be supported as defined by IETF RFC 4960 [71] and IETF RFC 4166 [72]**.**

7.4.3 M2PA

If the transport of SS7 MTP3 signaling messages is required in a peer to peer architecture, such as SGF to SGF, then M2PA shall be implemented as defined by IETF RFC 4165 [73]**.**

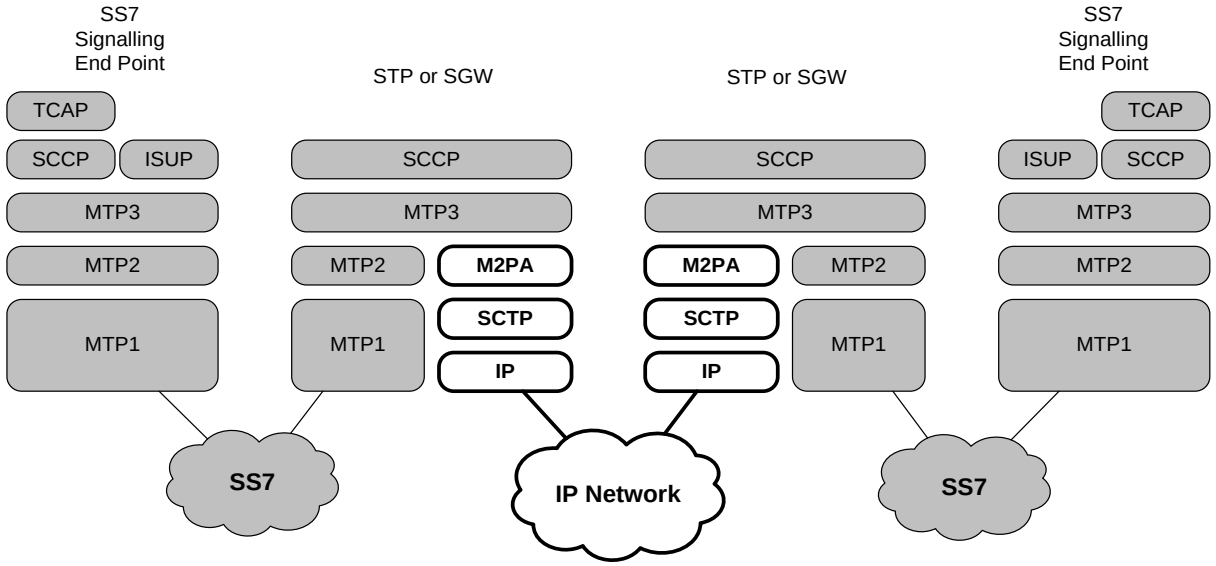


Figure 9 – M2PA Adaptation Layer

7.4.4 M3UA

If the transport of any SS7 MTP3-User signaling, (e.g. SCCP) is required, then M3UA shall be implemented as defined by also IETF RFC 3332 [74] as short term implementation and IETF RFC 4666 [74] as target implementation.

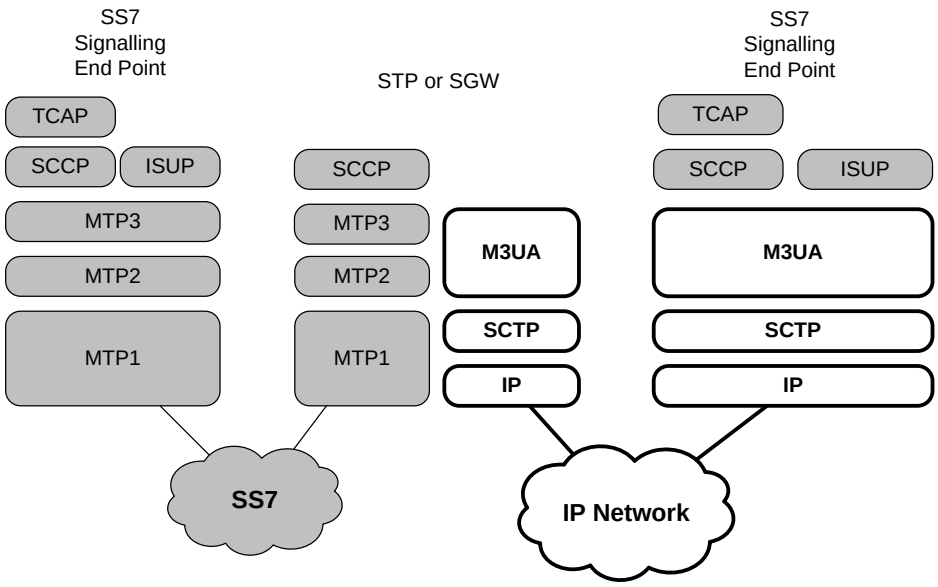


Figure 10 – M3UA Adaptation Layer

7.4.5 Security

For private interconnection configurations (Section 6.1), as these interconnections are by definition secure, no encryption is necessary.

For public interconnection configurations (Section 6.2), as per IETF RFC 3788 [75], the support of IPsec is mandatory for all nodes running SIGTRAN protocols. TLS support is optional, see Section 11.2.

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 [24]. 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 [25]. The list of protocol parameters defined in this RFC [25] that shall be used is given below.

8.1.1.1 Real Time Protocol data header

RTP data header is defined in Section 2 of RFC 3551. 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.729a, b, ab, G.722, WB AMR, as defined in Section 6, Table 4 of RFC 3551.
- Detailed definition of above mentioned and other supported codecs payload types in Sections 8.3-8.5 of this document.
- Comfort Noise as defined in Section 4 of RFC 3389 [37]. (static PT 13 (8 kHz) or dynamic).
- Telephone Events (DTMF tones) as defined in the Section 3.3 of IETF RFC 2833 [27] (dynamic)
  Note: RFC 2833 has been superseded by RFC 4733 [38]. 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 (dynamic)
  Note: RFC2833 has been superseded by RFC 4733. 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.

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 [25] Section 2.

8.1.1.8 Security - security services and algorithms

According to RFC 3550 [24] 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 [58], except that padding to a multiple of 8 octets is indicated as described for the P-bit.

In the scope of this document RTP 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 [25]. Under normal operational conditions congestion should be avoided by network engineering technique.

8.1.1.11 Transport protocol

The UDP as well as TCP protocols are defined in RFC 3551 [25] 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 [25] 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 [24] 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 [24].

8.1.1.14 IP/UDP/RTP Compression

Compressing IP/UDP/RTP Headers as described in RFC2508 [79] or RFC3095 [80] 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 (or 1 byte for RFC 3095 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 as 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 Sec. 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 recommended due to their significant market relevance.

In future 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
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: as far as the conversion between G.711 A-law with G.711 μ-law is concerned, the existing conventions apply.

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.729a, 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 “[41]” Section. 4.1.9.

Packetisation period for other 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 [41].
- G.726 PT=Dynamic as defined in RFC 3555 [41]
- AMR-NB Dynamic as defined in RFC 4867 [39]

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 this can 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 [39]

8.5 Codecs supported for low bit rate transmission

Where transmission costs are high, such as for satellite links, low occupied bandwidth is an important design consideration.

8.5.1 Transmission (occupied) bandwidth

Factors affecting occupied bandwidth are: codec bit rate, Voice Activity Detection and Discontinuous Transmission (VAD/DTX), packetisation period 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 to RFC 2508 [79] or to 1 byte if RFC3095 [80] 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):

a. select a Low Bit Rate (LBR) codec with low voice quality impairment factor (see [4]);

b. select codecs with Discontinuous Transmission (DTX);

c. Implement IP/UDP/RTP compression on the satellite link, and

d. 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 voice transmission bandwidth (hence cost) remains within acceptable limits.

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 [4].

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 Sec. 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 [4])

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 [4])

Payload type definition for other Low Bit Rate codecs:

- AMR-NB Dynamic as defined in RFC 4867 [39]

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 [79] or 1 byte [80] shall be implemented on all 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” [4].

Generally the design should take into consideration:

1. the codec/packetisation period parameters of all involved interconnected networks (e.g. originating domestic network – international carriers’ networks – terminating domestic network)
2. the packetisation period latencies taken in conjunction with both originating and terminating domestic and local access networks latencies
3. the international physical distance latency
4. the expected packet loss and codec packet loss robustness
5. the transmission bandwidth (cost)
6. 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:

1. transcoding should be avoided whenever possible, due to the impact on speech quality and delay;

2. the order of codec/packetisation period preference is determined by the originating terminal and should be honoured wherever possible;
3. 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 international carrier shall perform the companding conversion;
4. 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;
5. 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;
6. in the case of fixed-mobile interconnection, transcoding, if necessary, should always be performed by mobile service providers.
7. 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 code
8. 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 [4].

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 [68] Section 6.
- Mode 2: T.38 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:

Stack 1

- IFT protocol for T.30 media
- UDPTL (Facsimile UDP Transport Layer)
- UDP protocol in transport layer

Stack 2

- IFT for T.30 media
- RTP
- UDP in transport layer

Stack 3

- IFT protocol for T.30 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 passthrough (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 modem passthrough.

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 [43].

8.8 Modem connections

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

I. Voice Band Data (VBD) mode, as defined in ITU-T V.152 [68]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.

II. Modem relay mode, as defined in ITU-T V.150.1 [44] Section 9 with
   - Simple Packet Relay Transport (SPRT) as specified in ITU-T V150.1 [44] Annex B;
   - UDP as transport protocol.

Call discrimination procedure in case of modem TDM- IP –TDM connection should be performed according to V.150.1 [44] Section 20. Interworking procedure between T.38 and V.150.1 should be as in T.38 Annex F [43].

8.9 MoIP guidelines

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

Modem Relay method as target solution is recommended 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 [28].

9 Handling of early media

In this document the term "*early media*" encompasses ringback 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 ringback tone is rendered by the called side whereas, in IP network it is usually rendered by the calling side for SIP-based signaling. These two specifications, however, do not cover every scenario which can be encountered by a carrier interconnecting, upstream and downstream, with ISUP, SIP and SIP-I –based networks.

This section assumes a node perspective and hence focuses on the action to be performed in the Call Handling Function. It provides operational guidelines in order to ensure that a caller always hears a ringback tone or any other announcement.

If in some interworking configurations detailed below, the carrier has to generate a ringback tone, it is the carrier's decision to select this tone.

9.1 Support of P-early media header

The support and handling of P-early media header is documented in IETF RFC 3960 [76]. However, this RFC does not address interworking between different types of networks.

Details of the interworking between different types of networks are specified in 3GPP TS 29.163 & TS 29.527 [77] and TS 29.164 [78]. The following describes the actions to be performed by the carrier's Call Handling Functions for all possible interworking configurations.

TDM (ISUP) -> SIP, SIP-I: the carrier shall generate the ringback tone at reception of a 180 RINGING message, except when the value of the P-early media header indicates the presence of early media.

SIP, SIP-I -> TDM (ISUP): the carrier receives the ringback tone generated downstream and transmits it upstream with a 18x message with the P-early media header according to 3GPP TS 29.163 [77] for SIP and 3GPP TS 29.164 [78].for SIP-I.

SIP, SIP-I - > SIP-I: if the carrier receives early media it transmits it upstream (together with the relevant received signaling messages e.g. 18x type); if the carrier does not receive any early media then it passes back the message received and it does not generate any ringback tone.

SIP, SIP-I -> SIP: if the carrier receives early media it transmits it upstream (together with the relevant received signaling messages e.g. 18x type); if the carrier does not receive any early media then it passes back the message received and it does not generate any ringback tone.

9.2 No support of P-early media header

TDM (ISUP) -> SIP, SIP-I: the carrier generates a ringback tone at reception of a 180 RINGING message. In case early media is received (e.g. for coloured ringback tone) then it transmits it upstream. Early media may be indicated by the existence of an SDP in the 180 RINGING or 18x message.

SIP, SIP-I -> TDM (ISUP): the carrier receives the ringback tone generated downstream and transmits it upstream with 18x message.

SIP, SIP-I - > SIP-I: if the carrier receives early media it transmits it upstream (together with the relevant received signaling messages e.g. 18x type); if the carrier does not receive any early media then it passes back the message received and it does not generate any ringback tone.

SIP, SIP-I -> SIP: if the carrier receives early media it transmits it upstream (together with the relevant received signaling messages e.g. 18x type); if the carrier does not receive any early media then it passes back the message received and it does not generate any ringback tone.

10 Security Issues

10.1 Network elements for border function

It is strongly recommended that all voice traffic coming into / leaving a carrier's network passes through Border Function.

As a result, all IP packets (for signalling and media), crossing this 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 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 functions:
  - The Signaling SBC function controls access of SIP signaling 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 optional functions could be implemented in the SBC.

The security related features and capabilities are described in more detail in Section 10.2.

10.2 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.

10.2.1 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 [49].

This IP topology hiding function is carried out for signaling traffic in the IBCF part of 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 shall have no impact on the interconnection functionality and shall be transparent to the interconnecting carriers.

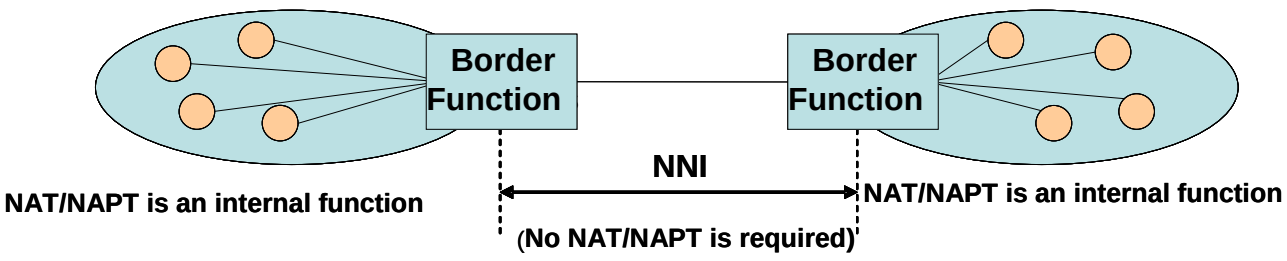


Figure 11 – NAT/NAPT Application

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.

10.2.2 Encryption

Two methods are used for encrypting information: IPSec as specified in [50] and TLS (Transport Layer Security) as specified in [51].

It is recommended to use the IPSec protocol when the encryption is needed, since it is independent from the protocols used at the upper layer and it is more widely used. Whether the TLS scheme could be used in next versions of this document, is for further study.

- Encryption for private interconnections
  In case of interconnection configurations described in Section 6.1, the use of encryption is not recommended for either the signaling or the media flows.
- Encryption for public interconnections
  In case of interconnection configurations described in Section 6.2, the use of encryption is recommended for signalling flows. Encrypting the media flow is not required.

10.2.3 Source authentication

When IPSec is used (see Section 10.2.2), it shall be used also for source authentication. Exchange of keys should be based on IKEv2 as specified in [52].

10.2.4 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.

10.2.5 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.

10.2.6 Deep packet inspection

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

10.2.7 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 signalled in a successful call attempt.

10.2.8 Internet control message protocol 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.

10.3 Attacks / misbehaviour to be protected from

Security or Fraud issues can basically be divided into two categories being “internal” and “external”. Internal issues are basically configuration related fraud and are caused by internal personnel of a carrier. External issues are attacks performed by the external world.

The subsections below only deal with “external” issues

10.3.1 DoS attack

Traffic is received from a not trustworthy IP-address from carrier C

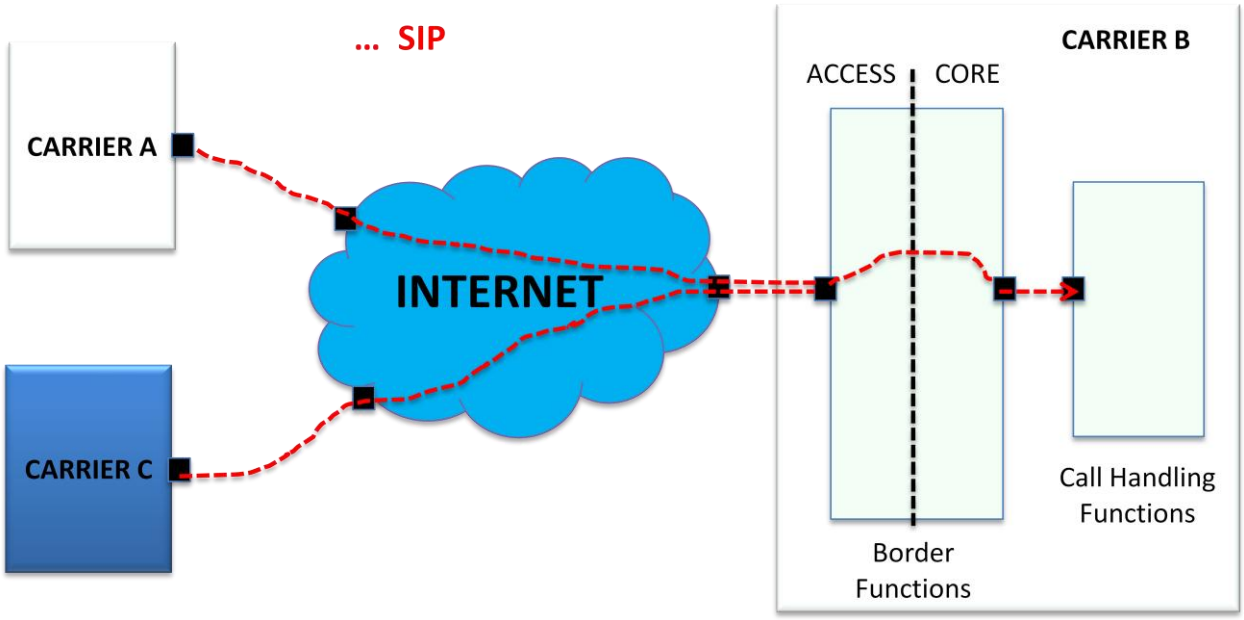


Figure 12 – DoS attack from not trustworthy IP-addresses

Impact

- Regular traffic between carrier A and carrier B can be impacted because of traffic overload caused by carrier C.

Proposed security functions as remedy:

- Use of ACL in the SBC which blocks the traffic coming from not trustworthy IP-addresses.

10.3.2 Protocol fuzzing

Protocol fuzzing is a technique which consists of manipulating a network protocol (e.g. SIP). The manipulated messages are then sent to a carrier with the aim to jeopardize the SBC functions (SBC might not be able to handle properly unexpected data, it may lead to memory corruption and even crashes of the SBC).

Carrier C sends a high amount of invalid or malformed SIP messages.

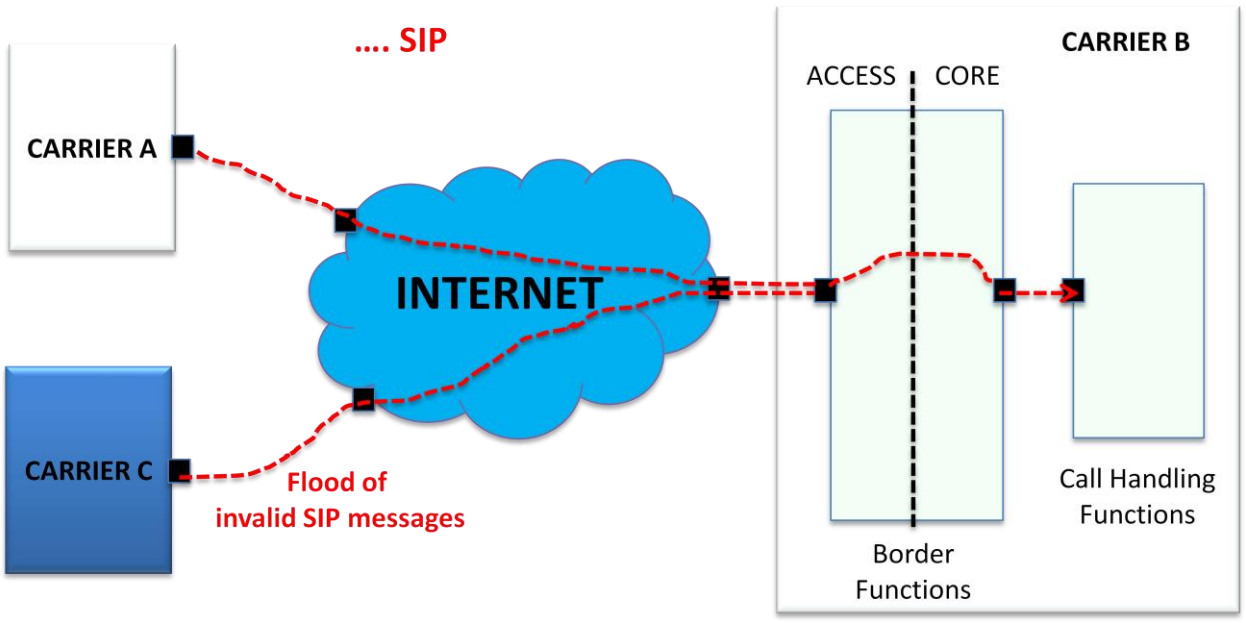


Figure 13 – Protocol Fuzzing

Impact

- These malformed messages can cause overload, memory violation or even crash of the SBC.
- Risk public/private connection: Risk is higher for public connection.

Proposed security functions as remedy:

- Deep packet inspection.

10.3.3 Address spoofing

Case A

In this case, the spoofer uses the source IP-address of Carrier A and sends a high amount of valid SIP messages.

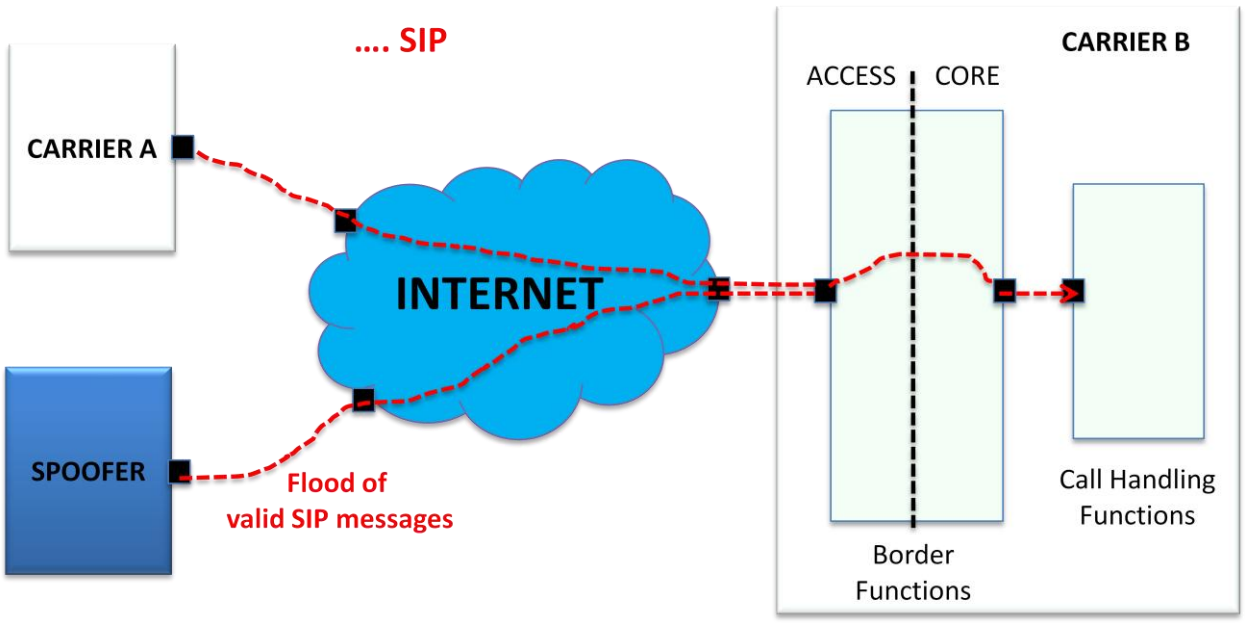


Figure 14 – Address spoofing with high amount of valid SIP messages

Impact

- The high amount of SIP messages can overload the SBC.
- QoS is reduced.

Proposed security functions as remedy:

- Traffic policer. Difficulty is to define the threshold as of when to reject calls because this must be based on the traffic profile which is dynamic.
- Source authentication via IPSec.

Case B

In this case, the spoofer uses the source IP-address of Carrier A and sends systematically a low amount of valid SIP messages towards random destination telephone numbers.

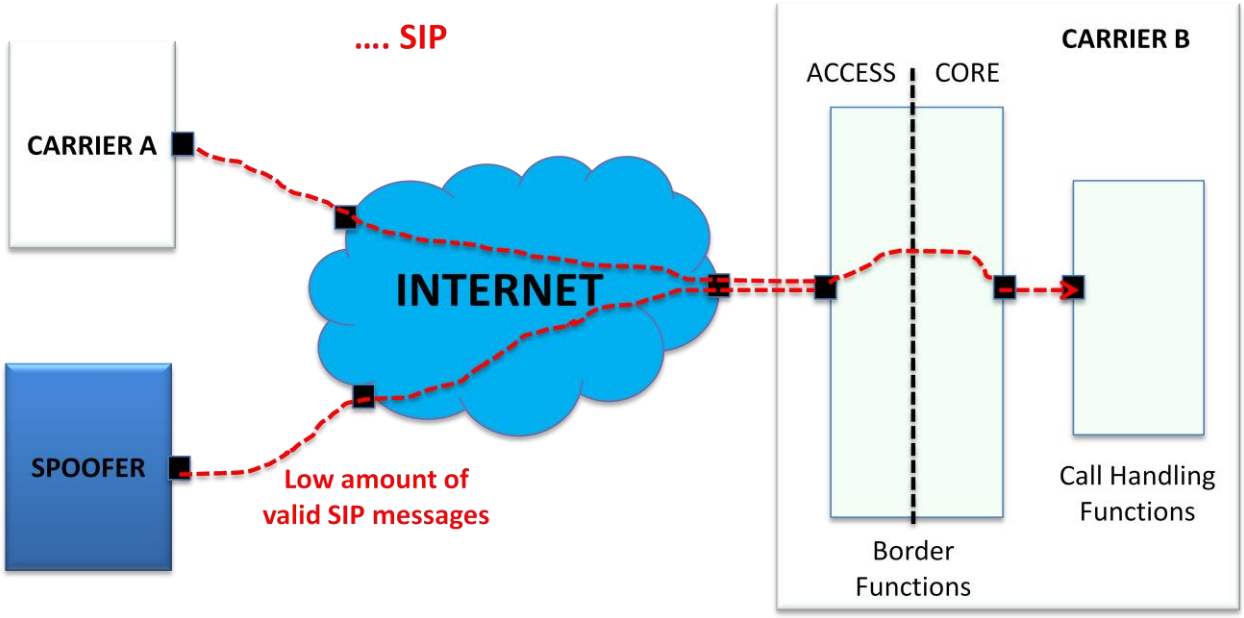


Figure 15 – Address spoofing with low amount of valid SIP messages

Impact

- In this case, the spoofer uses resources of Carrier A. Since the amount of traffic sent is rather low, this type of fraud is difficult to detect.
- Risk public/private connection: Risk is higher for public connection.

Proposed security functions as remedy:

- Source authentication via IPSec

10.3.4 Theft of service (bandwidth consumption)

Real time use of the service is different than the one indicated in the SIP signaling.

Impact

- More bandwidth is consumed than indicated in the SIP signaling. E.g. in the SIP signaling it is negotiated that a voice call will be established but in reality a video call is established.
- Commercial Fraud: CDRs will indicate a service which does not correspond to reality.

Proposed security functions as remedy:

- Deep packet inspection

10.3.5 Rogue media

A “rogue RTP stream” consists of media packets that are not associated with any active call (e.g. a RTP stream that starts too early or ends too late according to the SIP signaling.)

Impact

- Commercial Fraud: CDRs will indicate a call duration which does not correspond to reality.

Proposed security functions as remedy:

- Media traffic filtering

10.3.6 CLI manipulation

Altering the CLI may result in the displayed caller ID misleading the called party as to the identity and/or location of the calling party.

It is expected that international carriers pass on CLI unaltered. Carriers, under normal operational conditions, are not required to check CLI validity. If the CLI is already manipulated at the ingress side, it will be sent unaltered to the egress side (except that it shall be changed from National format to International format if received over a TDM link at the originating international gateway).

11 Quality of Service parameters

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

KPIs are defined for the purpose of:

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

Any commercial agreement associated with SLA and/or QoS reporting is subject to agreement between parties and outside the scope of this document. See in [1], [2] for any matter related to SLA 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 [67].

Other KPIs which are outside the scope of this technical document, such as maximum time to restore service, are defined in [1], [2].

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 12 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 [61].

Jitter
Jitter is the absolute value of differences between the delay of consecutive packets [61], [70].

Packet loss
Packet loss is the ratio between the total lost packets and the total sent packets over a given time period [61].

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.

MOS_{CQE} / R-factor for voice calls
MOS (Mean Opinion Score) is a subjective parameter defined in ITU-T Rec. P.10 [65] 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 [66] 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 [65]) using formula in ITU-T Rec G 107 Annex B [66]. 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 [64]:

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

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 [62] with the following formula:

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

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 [63] released in 2002 with the following formula:

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

Note: user failure includes caller abandonment

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.

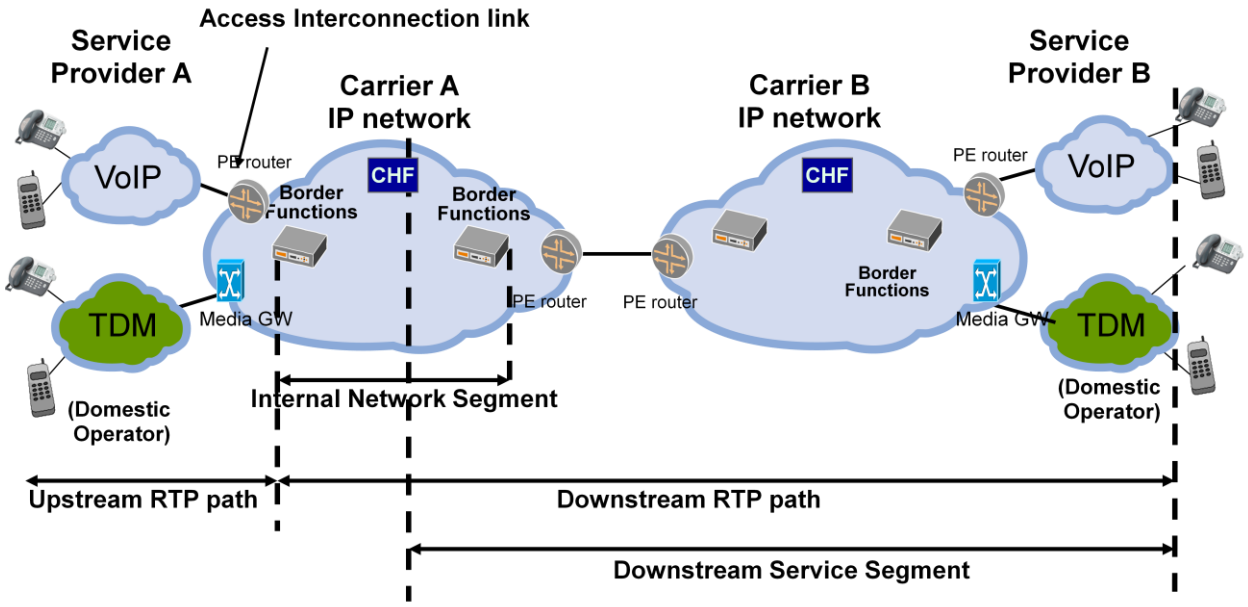
Note: only INVITEs initiating a dialog for which an alerting response is received are taken into account.

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 16 applies to the Carrier–to–Service Provider relationship. The SIGTRAN access type is included in the connections shown in the Figure 16 below.



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 16 – Reference configuration for the Carrier-to-Service Provider relationship

The following segments are defined:

1. *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.

2. *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 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.

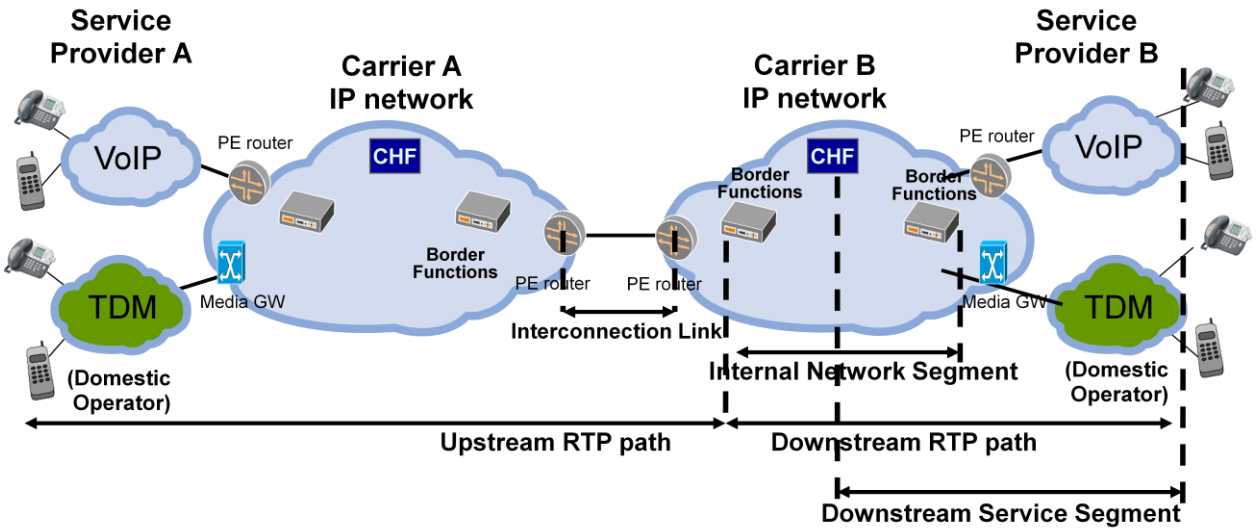
3. *the downstream service segment:* from Carrier Call Handling Function down to the terminal of the end user.

4. 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).

5. 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 17 applies to the inter-Carrier relationship. The SIGTRAN access type is included in the connections shown in the Figure 17 below.



CHF: Call Handling Functions

Figure 17 – 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:

1. *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.

2. *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 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.

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

4. 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).

5. 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.

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,.

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 ✓Internal Network Segment	✓Access Interc. Link ✓Internal Network Segment	✓Access Interc. Link ✓Internal Network Segment	✓Access Interc. Link ✓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 in [1], [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 in [1], [2].

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, PGRD	✓ At Call Handling Functions for the downstream direction i.e. the downstream service segment	✓ At Call Handling Functions for the downstream direction i.e. the downstream service segment

Whether the parameters ALOC, ASR, NER and PGRD are suitable for a SLA agreement is in the scope of in [1], [2].

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 [1], [2].

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

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

11.4 Exchange of QoS data

This issue is dealt with in [1], [2].

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

This deliverable is E.164-based [32]. 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.

12.1 Numbering and addressing in E.164-based international interconnection

International IP interconnection for voice services will be based on SIP [17] and SIP-I [22]. 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 11.3and 11.4 respectively.

12.2 International numbering scheme in TDM network

International number format used in International IP interconnect for voice shall conform to E.164 standard [32]. 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 [32] 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 ([32] Appendix B, Section B. 3.3) in international voice IP interconnect is OPTIONAL as it is very rarely used.

12.3 TEL URI addressing scheme

Tel-URI shall conform to IETF RFC 3966 [18] “The tel URI for Telephone Numbers”. According to this RFC global unique telephone numbers are identified by 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.

12.4 SIP URI Addressing scheme

SIP-URI shall conform to IETF RFC 2396 [59]. 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 [17] section 19.1.1. As an example of SIP URI the following format is given:

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

13 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.

13.1 Call detail record format

The CDR shall support the following information or the data that can derive the following information. Optional information is identified in the column.

#	Information	Note
1.	Originating Carrier	Mandatory. This field includes the country of the carrier. The originating carrier may be: ▪ A domestic carrier for calls originating in a domestic location ▪ Int'l carrier for calls originating in an int'l location ▪ The carrier itself for calls originating in its own network.
2.	Terminating Carrier	Mandatory. This field includes the country of the carrier. The terminating carrier may be: ▪ A domestic carrier for calls terminating in a domestic location. ▪ Int'l carrier for calls terminating in an int'l location ▪ The carrier itself for calls terminating in its own network.
3.	Ingress TSG Number / virtual TSG Number / IP Address	Mandatory. Source IP address/Port Number
4.	Egress TSG Number / virtual TSG Number / IP Address	Mandatory. Destination IP address/Port Number
5.	Call Identifier	Mandatory. If the SIP protocol is used, Call-ID and CSeq are recorded.
6.	Ingress Protocol	Mandatory. SIP, SIP-I, ITU-T C7, TUP, etc.
7.	Egress Protocol	Mandatory. SIP, SIP-I, ITU-T C7, TUP, etc.
8.	Dialed Digit in CC+NN format	Mandatory. It is assumed the called number is an E.164 number.
9.	Caller Number in CC+NN format, if available	Optional. A caller number may not be received. CLIR indicator, if CLI is received.
10.	Service Information (e.g., Toll Free, Int'l Long Distance, etc.)	Mandatory. This information is used for determining the billing direction. For example, outgoing Int'l Toll Free Service is foreign billed.
11.	Ingress Codec	See Section 8.
12.	Egress Codec	See Section 8.
13.	Original Called Number (OCN)	Optional. This information is used for call forwarding, e.g., Mobile's voice mail.
14.	Redirecting Information (RI)	Optional. This information is used for call forwarding, e.g., Mobile's voice mail.
15.	Redirecting Number (RgN)	Optional. This information is used for call forwarding, e.g., Mobile's voice mail.
16.	Call Disposition (Cause Code, SIP Status Code)	Mandatory. For example, Cause Code 34 for ISUP signaling; 404 for SIP protocol.

#	Information	Note
17.	Time of Seizure [Indicator, Year, Month, Date, Hour, Minutes, Seconds]: IAM, INVITE	Mandatory. Note this field shall include a Time Zone indication if local time is used otherwise use GMT.
18.	Time of Alert [Indicator, Year, Month, Date, Hour, Minutes, Seconds]: ACM, 18X	Optional. Note this field shall include a Time Zone indication if local time is used otherwise use GMT.
19.	Time of Answer [Indicator, Year, Month, Date, Hour, Minutes, Seconds]: ANM, 200, OK	Optional Note this field shall include a Time Zone indication if local time is used otherwise use GMT.
20.	Time of Termination [Indicator, Year, Month, Date, Hour, Minutes, Seconds]: REL, BYE, CANCEL	Mandatory Note this field shall include a Time Zone indication if local time is used otherwise use GMT.
21.	LANG/Language Digit	Optional. For TDM operator-to-operator calls.
22.	Origination Access Type: e.g., mobile, fixed, payphone	Optional. For TDM ITU-T SS#7 and SIP-I signaling protocols.
23.	Bearer Capability	Optional. For TDM ITU-T SS#7 and SIP-I signaling protocols.
24.	GSDN/Global Software Defined Network Call Type	Optional. For TDM ITU-T SS#7 and SIP-I signaling protocols.
25.	ISDN Supplementary Services	Optional. For TDM ITU-T SS#7 and SIP-I signaling protocols.
26.	UUI Rejection/Subsequent UUI Received Indicator	Optional. For TDM ITU-T SS#7 and SIP-I signaling protocols.
27.	RTP Lost Packets	Optional. For media traffic quality of service
28.	RTP Jitter	Optional. For media traffic quality of service
29.	RTCP Lost Packets	Optional. For media traffic quality of service
30.	RTCP Jitter	Optional. For media traffic quality of service
31.	MOS	Optional. For media traffic quality of service
32.	Total octets received	Optional. Total traffic received
33.	Total octets sent	Optional. Total traffic sent

1 Annex on Network Interconnection Examples

On the basis of the content of the main part of this document, various interconnection models can be implemented for a bilateral international Voice service depending on the transport configurations, adopted signaling protocol and media codec and additional, interconnection models that imply different quality levels.

In order to better address carriers' needs, it has been recognised useful to complete the specification describing two network examples covering different market scenarios:

1) *direct private-oriented interconnection (dedicated to voice service)*
2) *indirect public-oriented interconnection (via Public Internet)*

in terms of transport configuration, IP protocol parameters, suggested signaling protocol, suggested codec, suggested network security features.

1.1 Direct private-oriented interconnection (dedicated to voice service)

Transport Characteristics
Transport configuration: as specified in Section 6.1.1
Transmission Interface: either SDH/Sonet- based or Ethernet-based
Type of the IP addresses (of the PE router and Border Function): Public not announced onto the Internet
IP TOS field marking: DSCP = 46/EF or IP Precedence = 5
IP Dimensioning Criterion: with a 15% over-provisioning factor taking into account IP packet payload and protocols overhead

Service Characteristics
Signaling Protocol: SIP-I as specified in ITU-T Rec. Q.1912.5 Annex C Profile C transported over UDP protocol (specified in IETF RFC 768)
Voice Codec: as specified in ITU-T Rec. G.711 with RTP protocol as specified in IETF RFC 3550
Fax Protocol: as specified in ITU-T Rec. T.38
DTMF Support:: as specified in IETF RFC 2833
Numbering and Addressing: as specified in ITU-T Rec. E.164

Security Characteristics
Border Function: required
Signaling Encryption: no encryption needed
Media Encryption: no encryption needed

1.2 Indirect public-oriented interconnection (via public Internet)

Transport Characteristics
Transport configuration: as specified in Section 6.2.2
Transmission Interface: either SDH/Sonet- based or Ethernet-based
Type of the IP addresses (of the PE router and Border Function): Public announced onto the Internet
IP TOS field marking: (DSCP = 46/EF / IP Precedence=5) or (DSCP DF/CS0 / IP Precedence=0)
IP Dimensioning Criterion: with a 15% over-provisioning factor taking into account IP packet payload and protocols overhead

Service Characteristics
Signaling Protocol: SIP as SIP signaling profile specified in Section 7.1 based on IETF RF3261 transported over UDP protocol (specified in IETF RFC 768)
Voice Codec: as specified in ITU-T Rec. G.729a with RTP protocol as specified in IETF RFC 3550
Fax Protocol: as specified in ITU-T Rec. T.38
DTMF Support:: as specified in IETF RFC 2833
Numbering and Addressing: as specified in ITU-T Rec. E.164

Security Characteristics
Border Function: required
Signaling Encryption: encryption required by means of IPSec protocol
Media Encryption: no encryption needed.

1.3 Comparison of the interconnection examples

The two given examples of bilateral international interconnection are intended to meet different market requirements.

The first example (private-oriented) describes a possible interconnection configuration to be implemented between two carriers with co-located IP backbones nodes, or that are willing to build a transmission circuit. This interconnection configuration, providing the highest level of quality both in terms of voice call quality, service quality, network availability and network security, can replace existing TDM-based ones and, the more the number of channels is high, the more the suitability of this configuration is high.

The second example (via Public Internet) is more suitable for cases where the two carriers are not co-located and accept the lower quality levels generated by the Public Internet. This interconnection implies a lower cost (resources shared with other services) and, in general, lower provisioning time (no need to set-up an ad-hoc link).

The two examples can both be used to transport International voice traffic, however due to the lower quality levels achievable onto the public internet, carriers that want to provide a high and stable quality of voice services should favour a private and dedicated interconnection solution.

Two tables below provide *target values* for the two discussed network scenarios.

Relevant to Voice Service layer

	Case 1) Private-oriented	**Case 2) via Public Internet**
ASR	**Higher** (on the basis of historical data) ASR includes customer behaviour and is route dependant	**Lower** (on the basis of historical data) ASR includes customer behaviour and is route dependant
NER	**NER values depend on destination and type of destination (fixed/mobile).** **The same values of the existing TDM interconnection should be achieved.**	**Lower than Private-oriented case**
MOS (model E)	**Higher than 4**	**Higher than 3,6**
PGRD (POST GATEWAY RINGING DELAY)	**Under Evaluation**	**Under Evaluation**
ALOC	**Higher** (on the basis of historical data) ALOC includes customer behaviour and is route dependant	**Lower** (on the basis of historical data) ALOC includes customer behaviour and is route dependant
ISUP information transport	**Supported**	**Partly Supported**

Relevant to Network Platform layer

	Case 1) Private-oriented	**Case 2) via Public Internet**
Network availability (including the	**99.99%** monthly with dual access, **99.95%** monthly with single access	**99.99%** monthly with dual access, **99.95%** monthly with single access

int. segment)		
RTD (for the int. segment)	**Depending on geographical areas** Indicative RTD values for specific regions are given in GSMA IR34 V.4.2 (Oct. 2007) pg. 31	**Depending on geographical areas** **Higher values than private-oriented interconnection** Indicative RTD values for specific regions are given in GSMA IR34 V.4.2 (Oct. 2007) pg. 31
Packet Loss (for the int. segment	**<0.1%**	**> = 0.1%**
Packet Jitter (for the int. segment	**Under Evaluation**	**Under Evaluation**