INTERNATIONAL INTERCONNECT FORUM FOR SERVICES OVER IP

i3 FORUM

Technical Interconnection Model for Bilateral Voice Services

(V.1.0) May 2008

Table of Contents

Annexes

1 Scope of the document

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

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

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 in 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, for naming some functional blocks (e.g. border functions) the IMS ETSI TISPAN model has been assumed.

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 bilateral VoIP services.

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

This deliverable is the first version of the document. Future versions will be released encompassing new features / capabilities to address the evolution of services, equipment capabilities and international standards. A companion document [1] deals with the testing of bilateral international VoIP interconnection.

This deliverable has been produced in parallel with the international VoIP service description given in [2].

3 Acronyms

3pcc	Third Party Call Control
ACL	Access Control List
ACM	Address Complete Message
AF	Assured Forwarding
ALG	Application Level Gateway
ALOC	Average Length of Call
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
CDR	Call Detail Record
CLI	Calling Line Identity
CLIR	Calling Line ID Restriction
CPN	Calling Party Number
CSCF	Call Session Control Function
DES	Data Encryption Standard
Diffserv	Differentiated Services
DSCP	Differentiated Services Code Point
DTMF	Dual-Tone Multi-Frequency
EF	Expedite Forward
EXP	Experimental Use field MPLS header
FoIP	Fax over IP
GIC	Group Identification Code
GSDN	Global Software Defined Network
GSN	Global Subscriber Number
IAM	Initial Address Message
IBCF	Interconnection Border Control Function
I-BGF	Interconnect Border Gateway Function
IC	Identification Code
IFP	Internet Facsimile Protocol
IFT	Internet Facsimile Transfer
IKE	Internet Key Exchange
IMS	IP Multimedia Subsystem
IPSec	IP Security
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
IVR	Interactive Voice Response
KPI	Key Performance Indicator
MF	Multi-Field Classifier
MGCF	Media Gateway Control Function
MGF	Media Gateway Function
MIME	Multipurpose Internet Mail Extensions
MoIP	Modem over IP
MOS	Mean Opinion Scale
MPLS	Multiprotocol Label Switching
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

OLO	Other Licensed Operator
OSS	Operations Support System
P-router	Provider router
PE-router	Provider Edge router
PGRD	Post Gateway Ringing Delay
PHB	Per-Hop Behavior
POS	Packet Over Sonet
PSTN	Public Switched Telephone Network
R-Factor	Rating-Factor
RgN	Redirecting Number
RI	Redirecting Information
RTCP	Real Time Control Protocol
RTD	Round Trip Delay
RTP	Real-Time Protocol
SCTP	Stream Control Transmission Protocol
SDES	Source Description
SDH	Synchronous Digital Hierarchy
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SIP URI	SIP protocol Uniform Resource Identifier
SIP-I	SIP with encapsulated ISUP
SIP-T	SIP for Telephones
SLA	Service Level Agreement
SN	Subscriber Number
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
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
VBD	Voice Band Data
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network

4 References

[1] IP-IP Forum “Interoperability Test Plan for Bilateral Voice services” Version 1.0, May 2008
[2] IP-IP Forum “Bilateral Voice Service Description“ Version 1.0, May 2008
[3] IETF RFC 2474 “Definition of the Differentiated Services Field”
[4] IETF RFC 2475 “An Architecture for Differentiated Services”
[5] IETF RFC 3246 “Expedited Forwarding Per-Hop Behavior”
[6] IETF RFC 3247 “Supplemental Information for the New Definition of the EF PHB”
[7] IETF RFC 2597 “Assured Forwarding PHB Group”
[8] IETF RFC 4594 “Configuration Guidelines for Diffserv Service Classes”
[9] IETF RFC 1918 “Address Allocation for Private Internets”
[10] IETF draft-ietf-bfd-base-08.txt “Bidirectional Forwarding Detection”
[11] IETF RFC 4271 “A Border Gateway Protocol 4 (BGP-4)”
[12] IETF RFC 3261 “SIP: Session Initiation Protocol”, June 2002
[13] IETF RFC 3966 “The tel URI for Telephone Numbers”, December 2004
[14] IETF RFC 3323 “A Privacy Mechanism for the Session Initiation Protocol (SIP)”, September 2002
[15] IETF RFC 3325 “SIP Extensions for Network-Asserted Caller Identity and Privacy within Trusted Networks”, September 2002
[16] IETF RFC 4028 “Session Timers in the Session Initiation Protocol (SIP)”, April 2005
[17] ITU-T Recommendation Q1912.5 “Interworking between Session Initiation Protocol and Bearer Independent Call Control or ISDN User Part, 2004
[18] IETF RFC 4566, “SDP: Session Description Protocol”, July 2006
[19] IETF RFC 3550 “RTP: A Transport Protocol for Real-Time Applications”, July 2003
[20] IETF RFC 3551, “RTP Profile for Audio and Video Conferences with Minimal Control”, July 2003
[21] IETF RFC 3555, “MIME Type Registration of RTP Payload Formats”, July 2003
[22] IETF RFC 2833, “RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals”, May 2000
[23] IETF RFC 3362 “Real-time Facsimile (T.38) – image/t38 MIME Sub-type Registration,”, August 2002
[24] ITU-T T.38 Procedures for real-time Group 3 facsimile communication over IP networks, 1998
[25] IETF RFC 768 “User Datagram Protocol”, August 1980
[26] ITU-T Recommendation E.164 “The international public telecommunication numbering plan”, 1997
[27] ITU-T Recommendation G.729 “Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)”, 1996
[28] ITU-T Recommendation G.711 “Pulse Code Modulation of Voice Frequencies”, 1988
[29] IETF draft-levy-sip-diversion-08 “Diversion Indication in SIP”, August 2004
[30] IETF RFC 4458 “Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR)”, April 2006.
[31] IETF RFC 3389 “Real-time Transport Protocol (RTP) Payload for Comfort Noise (CN)” September 2002
[32] IETF RFC 4733 “RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals” December 2006
[33] 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
[34] IETF RFC 4749 “RTP Payload Format for the G.729.1 Audio Codec” October 2006
[35] IETF RFC 3555 “MIME Type Registration of RTP Payload Formats”
[36] IETF RFC 4117 “Transcoding Services Invocation in the Session Initiation Protocol (SIP) Using Third Party Call Control (3pcc)” (June 2005).
[37] ITU-T Recommendation T.38 “Procedures for real-time Group 3 facsimile communication over IP networks” (04/2007)
[38] ITU-T Recommendation V.150 “Modem-over-IP networks: Foundation” (01/2003).
[39] ITU-T Recommendation G.711 “Pulse Code Modulation (PCM) of voice frequencies”
[40] ITU-T Recommendation G.729 “Coding of speech at 8 kbit/s using conjugate-structure algebraic code excited linear-prediction (CS-ALEP (03/96)
[41] ITU-T Recommendation G.729 Annex A “Reduced complexity 8kbit/s CS-ALEP codec” (11/96)
[42] ITU-T Recommendation G.729 Annex B Silence compression scheme for G.729 optimized for terminals conforming to Recommendation V.70” (11/96)
[43] ITU-T Recommendation G.729 Annex A and B
[44] IETF RFC 2663 “IP Network Address Translator (NAT) Terminology and Considerations”
[45] IETF RFC 2401 “Security Architecture for the Internet Protocol”
[46] IETF RFC 2246 “The TLS Protocol”
[47] IETF RFC 4306 “Internet Key Exchange (IKEv2) Protocol”
[48] ITU-T Recc. G.703: “Physical/electrical characteristics of hierarchical digital interfaces”, November 2001;

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

[50] ITU-T Recc. G.705 "Characteristics of plesiochronous digital hierarchy (PDH) equipment functional", October 2000;

[51] ITU-T G.707: Network Node Interface for the Synchronous Digital Hierarchy(SDH)

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

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

[54] RFC 2396 "Uniform Resource Identifiers (URI): Generic Syntax"

[55] 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

[56] ITU-T Recommendation Y.1540 "Internet Protocol Data Communications Services - IP Packet Transfer and availability performance parameters", December 2002

[57] ITU-T Recommendation E. 411 "International Network Management – Operational guidance", March 2000

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

[59] ITU-T Recommendation G.100 "Definitions used in recommendations on general characteristics of international telephone connections and circuits", February 2001

[60] ITU-T Recommendation E.437 "Comparative metrics for network performance management", May 1999

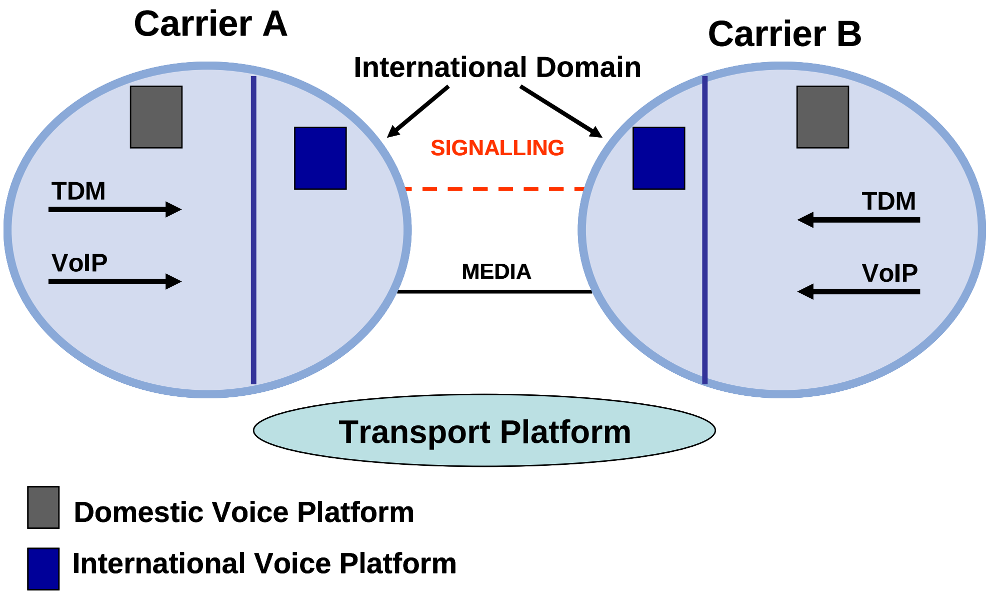
[61] ITU-T Recommendation P.10 "Vocabulary of terms on telephone transmission quality and telephone sets", December 1998

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

[63] 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

5 General Reference Architecture

The general reference configuration for international bilateral 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 signalling protocols (see section 7) and media (see section 8) flows carried onto an IP transport layer (see section 6).



Note: The interface between the domestic environment and the international one can be either an intra-carrier interface or an interface between a domestic operator and an OLO. The specification of such interface is outside the scope of this document.

Figure 1 – General Reference Configuration

5.1 Service Reference Configuration

The service reference configuration is depicted in figure 2.

Three basic functional blocks have been identified:

1) Call Handling Function which performs the functions related to signalling 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 Functions encompass the Call Session Control Functions (CSCF), the Media Gateway Control Functions (MGCF) and the Breakout Gateway Control Function (BGCF).
2) Media Gateway Functions (MGF) devoted to the transcoding of the media flow from/to TDM domain and IP domain;
3) Border Functions devoted to separate the IP domain of the two carriers in order to implement trusted and secure VoIP Interconnections. The border functions apply both to the control plane and 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) whereas the user plane border functions is identified with I-Border Gateway Function (I-BGF). Additional information on how to use the border functions for security purposes are given in section 9 of this document.

The Call Handling Function of the Carrier's international switching facility receives VoIP and TDM signalling 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.

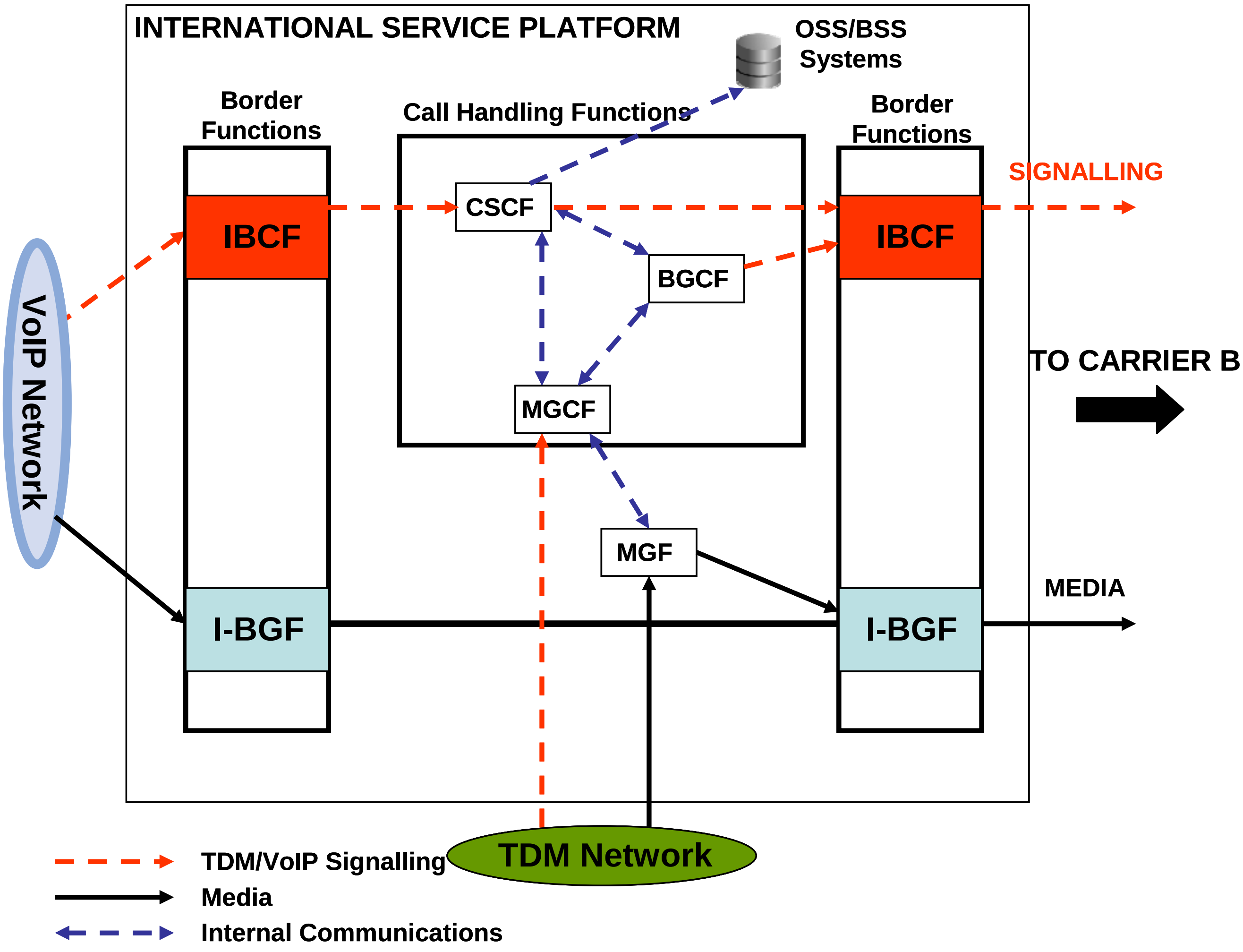


Figure 2 – Service Reference Configuration

The specification of the Signalling and Media information are 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 traffic

For the TDM traffic, the Call Handling Function:

- receives the Common Channel Signalling #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 flow in RTP media flow;
- the signalling 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 the VoIP traffic, the Call Handling Function:

- receives the proper signalling information (e.g. H.323, SIP, SIP-T, SIP-I)
- converts, if needed, in suitable protocols for VoIP traffic;
- identifies the proper routing towards the egress port;
- the signalling is sent to the IBCF which controls I-BGF identifying the involved I-BGF resources where the RTP media flow has to be directed.

5.1.2 Functions to be performed for the incoming international traffic

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

The Call Handling Function:

- identifies the proper routing towards the egress port;
- performs signalling 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 signalling 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.

5.2 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.

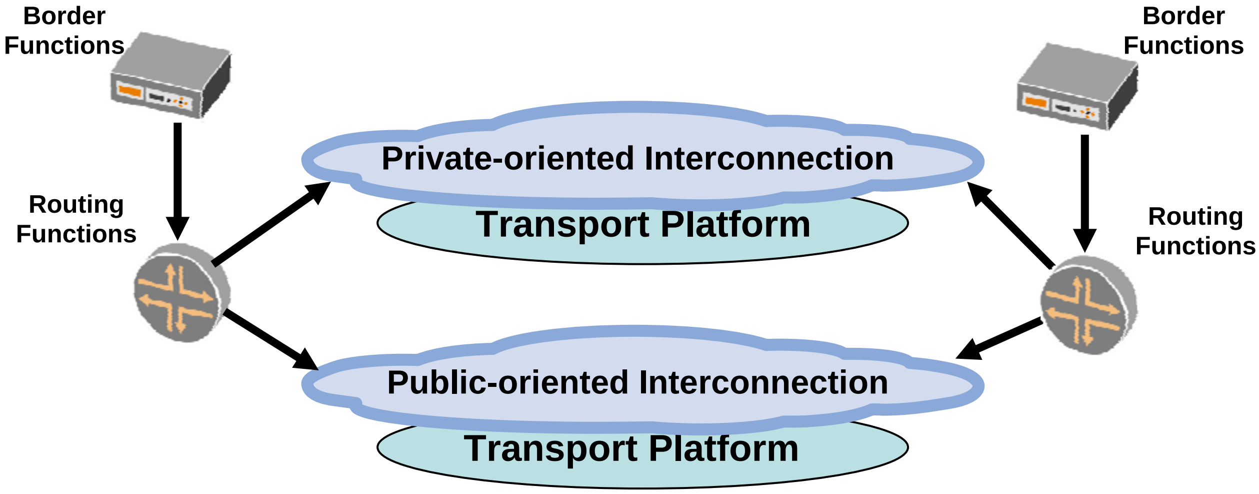


Figure 3 – Transport Reference Configuration

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 sections 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 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 functions 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 border functions.

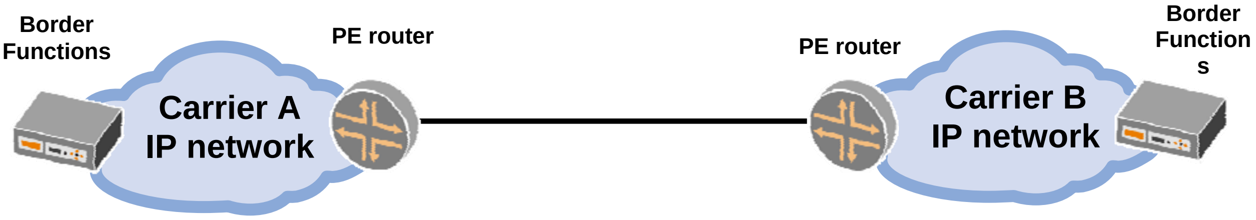


Figure 4 – Layer 1 Private-oriented Interconnection Configuration

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 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.

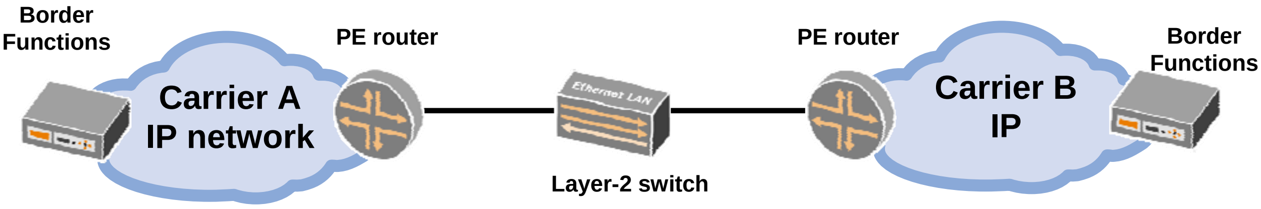


Figure 5 – Layer 2 Private-oriented Interconnection Configuration

6.1.3 Layer 3 interconnection

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

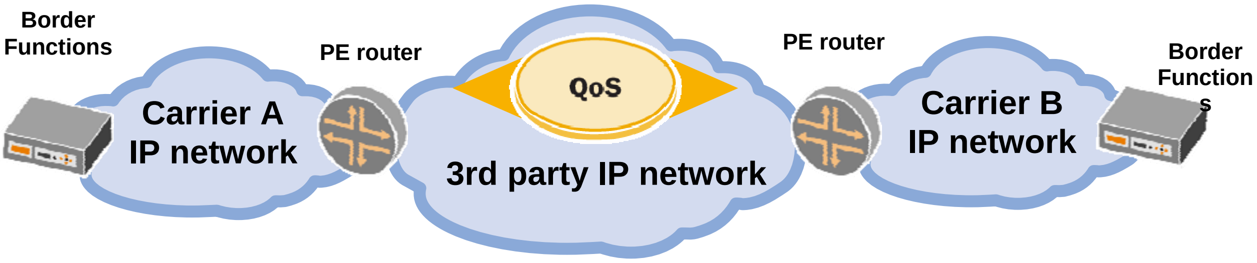


Figure 6 – Layer 3 Private-oriented Interconnection Configuration

6.2 Transport Functions for Public-oriented Interconnection

In the following sections 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 have to be public and they may be announced over the Public Internet. Border function IP addresses have to be exchanged only by the two carriers (ie : using no-export BGP community).

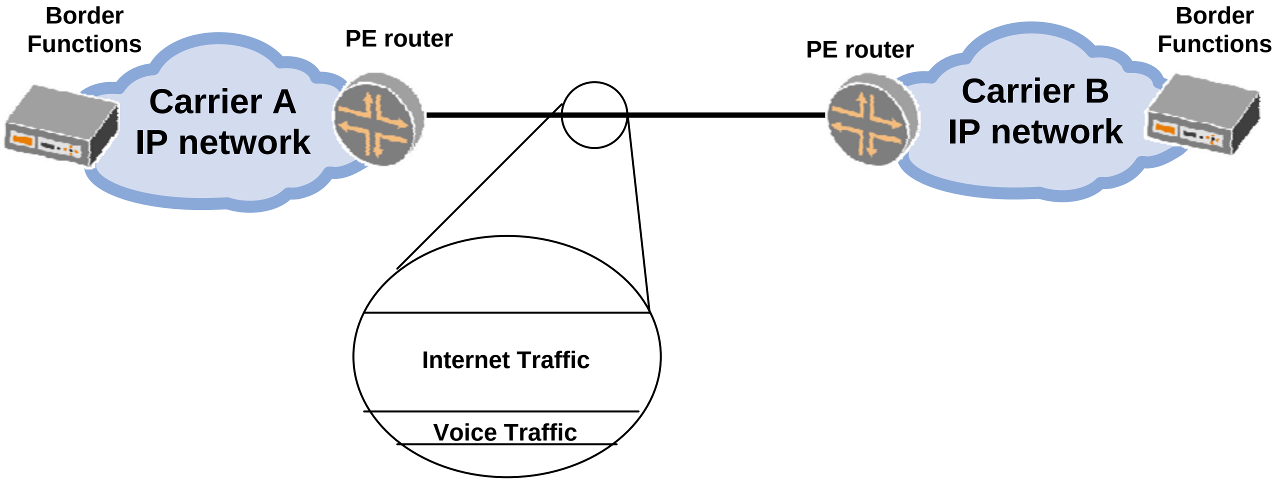


Figure 7 – Layer 1 / 2 Public-oriented Direct Interconnection Configuration

6.2.2 Non direct 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 of the Border functions shall be public and they shall be announced over the Public Internet.

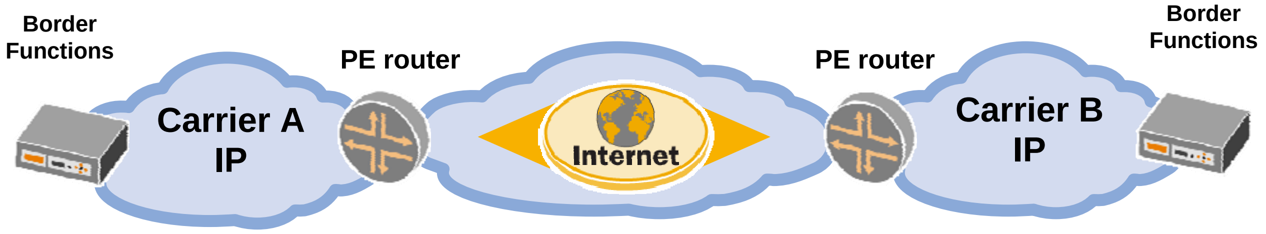


Figure 8 – Non Direct Public-oriented Interconnection Configuration

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 9.

This scenario implies lower values of QoS parameters than the interconnection configurations described in sec. 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 or PDH, SDH POS – based or Ethernet-based (i.e. fast-ethernet, gigabit-ethernet or 10gigabit-ethernet).

6.3.1 Transport Systems PDH-based

The ITU-T Recommendations G. Series shall be considered as reference documents, among these the ITU T Recc. ITU-T G.703, G.704, G.705 [48], [49], [50].

6.3.2 Transport Systems SDH-based

The ITU-T Recommendations G. Series shall be considered as reference documents, among these the ITU T Recc. ITU-T G.707 [51]

For US other reference document is ANSI T1.105 [52]

6.3.3 Transport Systems Ethernet-based

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

6.3.4 Transport Systems DWDM-based

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. Considering the IP overhead and assuming a value equal to 15% as over-provisioning factor, the following table, for the most common codecs, provides the bandwidth per call to be allocated:

Codec	Packetisation (msec.)	Bandwidth (kbit/s)
G.711	20	100.280
G.711	40	86.940
G.729	20	35.880
G.729	40	22.540

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 [11] 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 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 desirable to tune timers parameters at proper values, which depend on specific implementation, to ensure better convergence for recovering needs. Alternatively, BFD [10] 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 [9] 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)l
Other Customer Traffic	Internet traffic, other data traffic

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

The following table recommends the packet marking guideline for the link/network for all above interconnection configurations making use of the DiffServ 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	DCSP Marking	IP Precedence	EXP	802.1Q VLAN
Voice Media	for configurations 6.1, 6.2.1 DSCP 46/EF (101110).	5	5	5
	for configurations 6.2.2 DSCP 46/EF (101110) or DSCP DF/CS0 (000000).	5 or 0	5 or 0	5 or 0
Voice Signaling	for configurations 6.1, 6.2.1 DSCP 46/EF (101110) or DSCP 40/CS5 (101000).	5	5	5
	DSCP 46/EF (101110) or DSCP 40/CS5 (101000) or DSCP DF/CS0 (000000)	5 or 0	5 or 0	5 or 0
Other traffic	DSCP DF/CS0 (000000).	0	0	0

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

6.6.1 Distinguishing traffic classes

In order to distinguish between traffic classes, the use of the DSCP marking scheme in Behaviour Aggregation mode [4] 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 [2]. 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 Traffic treatment

For interconnection configurations specified in sections 6.1 and 6.2.1, voice media traffic leaving the sending Border Functions towards the receiving operator Border Functions should be treated according to the Expedite Forwarding Per-Hop Behaviour [5][6].

For the interconnection configuration specified in section 6.2.2, voice media traffic leaving the sending Border Functions towards the sending PE router is treated either according to the Expedite Forwarding Per-Hop Behaviour [5][6] or according to Default forwarding Per-Hop Behaviour[1].

For interconnection configurations specified in sections 6.1 and 6.2.1, voice signalling traffic leaving the sending Border Functions towards the receiving operator Border Functions should be treated according to the Expedite Forwarding Per-Hop Behaviour [5][6], or alternatively according to the Assured Forwarding Per-Hop Behaviour [7].

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

- the Expedite Forwarding Per-Hop Behaviour, as specified in RFC 3246 [5] and 3247 [6];
- the Assured Forwarding Per-Hop Behaviour as specified in RFC 2597 [7].
- the Default forwarding PHB , as specified in IETF RFC 2474 [3]

7 Signalling Functions

The bilateral 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).

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

This subsection describes the basic SIP profile.

7.1.1 Transport of SIP (IETF RFC 3261) signalling information

The SIP protocol can be transported over UDP [25], TCP or SCTP. RFC 3261[12] 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 could 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 signalling protocol profile

The basic SIP profile shall comply with RFC 3261 [12] 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 11.
- The support of IETF RFC 4028 [16], which addresses SIP Timers specification, is optional. The carrier receiving the INVITE message shall comply with IETF RFC 3261 [12] section 16.8 if IETF RFC 4028 [16] is not supported**.**
- The P-Asserted-Identity header defined in RFC 3325 [15] shall be supported.
- The Privacy header defined in RFC 3323 [14] shall be supported.
- The Diversion header defined in draft-levy-sip-diversion-08 [29] 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
CPN Known, Presentation not restricted	Forward CPN in From, Contact and P-Asserted-Identity headers
CPN Known, Presentation restricted	Use “Anonymous” in From and Contact headers. Neither P-Asserted-Identity or Privacy headers shall be used.
CPN not known	Use “Unavailable” in From and Contact headers. Neither P-Asserted-Identity or Privacy headers shall be used.

7.1.3 SIP Message support

The following table specifies how the SIP messages have to be supported.

#	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 RFC3261 [12].
3	ACK	The ACK message shall be supported as described in IETF RFC3261 [12].
4	CANCEL	The CANCEL message shall be supported as described in IETF RFC3261 [12].
5	BYE	The BYE message shall be supported as described in IETF RFC3261 [12].
6	OPTIONS	The OPTIONS messages shall be supported as described in IETF RFC3261 [12]. 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 may be used subject to bilateral agreement
8	INFO	The INFO message described in IETF RFC 2976 may be used subject to bilateral agreement
9	PRACK	The PRACK message described in IETF RFC 3262 may be used subject to bilateral agreement
10	MESSAGE	The MESSAGE message described in IETF RFC3428 may be used subject to bilateral agreement
	PUBLISH	The PUBLISH message described in IETF RFC3903 may be used subject to bilateral agreement
11	REFER	The REFER message described in IETF RFC3515 may be used subject to bilateral agreement
12	SUBSCRIBE	The SUBSCRIBE message described in IETF RFC3265 may be used subject to bilateral agreement
13	NOTIFY	The NOTIFY message described in IETF RFC3265 may be used subject to bilateral agreement

7.1.4 SIP Header support

The following table specifies how the SIP header has to be supported.

#	Header	Observations
1	Accept	The Accept header shall be used as defined in section 20.1 of RFC 3261 [12] 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 [12].
3	Accept-Language	The Accept-Language header shall be used as defined in section 20.3 of RFC 3261 [12]. 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 [12] 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 [12].
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 [12]. 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 [12].
12	Content-Encoding	The Content-Encoding header shall be used as defined in section 20.12 of RFC 3261 [12].
13	Content-Language	The Content-Language header shall be used as defined in section 20.13 of RFC 3261 [12].
14	Content-Length	The Content-Lenght header shall be used as defined in section 20.14 of RFC 3261 [12].
15	Content-Type	The Content-Type header shall be used as defined in section 20.15 of RFC 3261 [12]. 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 [12].
17	Date	The Date header shall be used as defined in section 20.17 of RFC 3261 [12].
18	Error-Info	The Error-Info header shall be used as defined in section 20.18 of RFC 3261 [12].
19	Expires	The Expires header shall be used as defined in section 20.19 of RFC 3261 [12].
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 [12].
22	Max-Forwards	The Max-Forwards header shall be used as defined in section 20.22 of RFC 3261 [12].
23	Min-Expires	The Min-Expires header shall be used as defined in section 20.23 of RFC 3261 [12].
24	MIME-Version	The MIME-Version header shall be used as defined in section 20.24 of RFC 3261 [12].
25	Organization	The Organization header shall be used as defined in section 20.25 of RFC 3261 [12].
26	P-Asserted-Identity	The P-Asserted-Identity shall be used as defined in RFC 3325 [15].
27	Priority	The Priority header shall be used as defined in section 20.26 of RFC 3261 [12].
28	Privacy	The Privacy header shall be used as defined in RFC 3323 [14].
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	Record-Route	The Record-Route header is not applicable in the scope of this document.

33	Reply-To	The Reply-To header shall be used as defined in section 20.31 of RFC 3261 [12]. Privacy considerations might modify its value.
34	Require	The Require header shall be used as defined in section 20.32 of RFC 3261 [12].
35	Retry-After	The Retry-After header shall be used as defined in section 20.33 of RFC 3261 [12].
36	Route	The Route header is not applicable in the scope of this document.
37	Server	The Server header shall be used as defined in section 20.35 of RFC 3261 [12].
38	Subject	The Subject header shall be used as defined in section 20.36 of RFC 3261 [12].
39	Supported	The Supported header shall be used as defined in section 20.37 of RFC 3261 [12].
40	Timestamp	The Timestamp header shall be used as defined in section 20.38 of RFC 3261 [12].
41	To	The To header shall be used as defined in section 20.39 of RFC 3261 [12]. Privacy considerations might modify its value.
42	Unsupported	The Unsupported header shall be used as defined in section 20.40 of RFC 3261 [12].
43	User-Agent	The User-Agent header shall be used as defined in section 20.41 of RFC 3261 [12].
44	Via	The Via header shall be used as defined in section 20.42 of RFC 3261 [12].
45	Warning	The Warning header shall be used as defined in section 20.43 of RFC 3261 [12].
46	WWW-Authenticate	The WWW-Authenticate header is not applicable in the scope of this document.

7.2 ISUP enabled SIP signalling profile

This subsection describes the ISUP-enabled SIP profile.

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

See section 7.1.1.

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

This signalling protocol profile shall be in accordance with ITU-T Recommendation Q.1912.5 [17] Annex C Profile C.

8 Media Functions

Media functions in International voice IP interconnect should assure as follows:

- Transport for all the services
- Transcoding

In the scope of international IP voice Interconnect the following services shall be supported:

- Voice phone calls and conference 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 phone calls and conference calls

For phone calls between two terminals as well as for conference calls with more than 2 participants the following protocol stack shall be used:

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

8.1.1 RTP / RTCP Protocols

The Real Time media Protocol (RTP) that shall be used for international voice services is defined in RFC 3550 [19]. According to [19] for particular applications the following items SHOULD be additionally defined:

- Profile definition
- Payload format specification.

The profile that shall be used for international voice interconnection is defined in IETF RFC 3551 [20]. Below the list of protocol parameters defined in this RFC that SHALL be used with some additional updates for different codecs:

8.1.1.1 RTP data header

RTP data header is defined in RFC 3551 [20] Section 2. The content of this section is endorsed.

8.1.1.2 RTP Payload types

The following RTP payload types shall be supported:

- G.711 A-law, G.711 µ-law, G.722, G.723, G.729, G.729a,b,ab, G.722 as defined in RFC 3551 [20] section 6, Table 4.
- Detailed definition of above mentioned and other supported codecs payload types in section 8.1.2 below.
- Comfort Noise as defined in RFC 3389 [31] section 4. (static PT 13 (8 kHz) or dynamic)
- Telephone Events (DTMF tones) as defined in IETF RFC 2833 [22] section 3.3 (dynamic)
- Telephone tones as defined in IETF RFC 2833 [22] section 4.4 (dynamic)

8.1.1.3 RTP data header additions

No RTP header additions will be used.

8.1.1.4 RTP data header extensions

Use of RTP data header extensions is not recommended.

8.1.1.5 RTCP 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 RFC 3551 [20] section 2.

8.1.1.6 SR/RR extension

No SR/RR extensions will be used.

8.1.1.7 SDES use

The SDES use is specified in IETF RFC 3551 section 2.

8.1.1.8 Security - security services and algorithms

According to RFC 3550 [19] 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 [53], except that padding to a multiple of 8 octets.

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 [20]. 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 [20] 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 [20] 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 [19] section 11;
- symmetrical UDP protocol should be used (the same port numbers).

8.1.1.13 Encapsulation - of RTP packets, multiple RTP data packets

Standard encapsulation of RTP packets in UDP protocol shall be used.

8.1.2 Codecs supported in international voice interconnection

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: provided at least one of the mandatory codecs is present in session description protocol (SDP) offer, and provided at least one of the mandatory codecs is supported by the end side, then codec negotiation is guaranteed to be successful. As a result, the carrier shall be able to carry all flows encoded as per any of the mandatory codecs, and to transcode the media flow if needed.

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

Group 1. Mandatory	Group 2. Optional
G.711 A-law, µ-law 64 kbit/s	G.722
G.729, G.729a, G.729b, G.729ab 8kbit/s	G.723.1
	G.729.1
	AMR
	WB-AMR

Packetization time for mandatory codecs:

- for G.711 A-law and µ-law packetization time will be 20 ms
- for G.729, G.729 a, G.729b, G.729 ab packetization time will be 20 ms or 40 ms

Payload definition for mandatory codecs:

- G.711 A-law PT= 8 Static or dynamic
- G.711 µ-law PT= 0 Static or dynamic
- G.729, G.729a PT= 18 Static or dynamic
- G.729b,ab PT= 18 Static or dynamic. Optional parameter "annexb" may be used according to RFC 3555 [21] : MIME Type Registration of RTP Payload Formats" (section. 4.1.9).".

Payload definition for other codecs:

G.722	PT=9 Static or dynamic
G.723.1	PT=4 Static or dynamic
G.729.1	Dynamic as defined in RFC 4749 [34]
AMR	Dynamic as defined in RFC 4867 [33]
WB-AMR	Dynamic as defined in RFC 4867 [33]

In next releases of this document, other codecs can be considered as mandatory as well as other codecs can be added to the list of optional codecs.

8.1.3 Transcoding Functions

In general transcoding should be avoided whenever possible, due to the impact on speech quality and delay. It is a commercial decision which carrier has to take care of this function.

For the sake of completeness, the transcoding functions are specified in RFC 4117 [36]. Appropriate scenarios are presented in sections 3.2 and 3.3 of this RFC.

8.1.4 Fax connections

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

- Mode 1: G.711 pass through
- Mode 2: T.38 Fax relay

In mode 1 the following stack SHALL be used:

- G.711 codec
- RTP as described in sec. 8.1.1.
- UDP in transport layer as described in sec. 8.1.1.11

In mode 2 one of two following stacks shall be used:

<u>Stack 1</u>

- IFT protocol for T.30 media
- UDP or TCP protocols in network layer.

<u>Stack 2</u>

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

T.38 fax coding should be supported (Version 0 mandatory, newer versions optional).All gateway VoIP to FoIP and back transitions in voice and facsimile over IP environment described in T.38 Annex D and E are allowed.

8.1.5 Modem connections

To enable point to point modem connections TDM – IP - TDM the following stack according to ITU-T V.150.1 [38] sections 8 shall be supported:

- **Voice Band Data (VBD) mode with**
  - G.711 A-law or µ-law codec;
  - RTP as media protocol;
  - UDP as transport protocol.

Additional modes which may be supported are:

- **Audio mode with**
  - DTMF&Tones as specified in RFC 2833 [22];
  - RTP as media protocol;
  - UDP as transport protocol;

- **Modem relay mode with**
  - Simple Packet Relay Transport (SPRT) as specified in ITU-T V150.1 [38] 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 [38] Section 20. Interworking procedure between T.38 and V.150,1 should be as in T.38 Annex F [37].

8.2 Media Security

Media information shall not be encrypted. Additional media security information are given in section 9.

9 Security Issues

It is strongly recommended that all voice traffic coming into / leaving the network operator passes through Border Functions. As a result, all IP packets (for signalling and media), crossing this bilateral voice interconnection, are originated and received by such Border Functions.

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

9.1 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 [44].

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

Since voice traffic will be exchanged between Border Functions, 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.

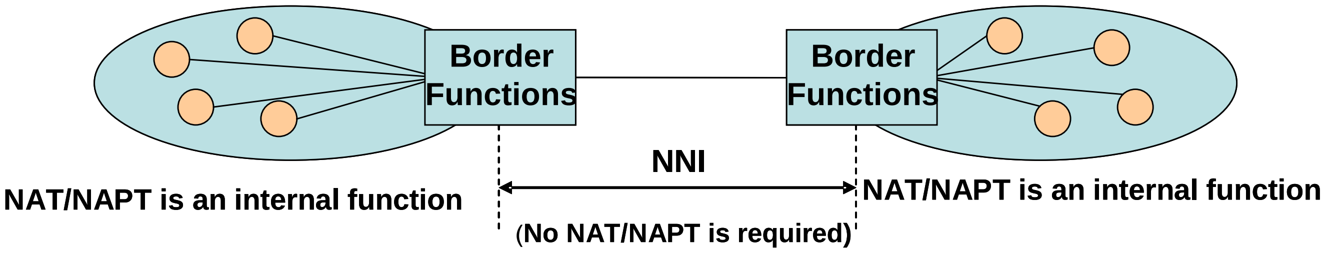

Border Functions
Border Functions
NNI
NAT/NAPT is an internal function
NAT/NAPT is an internal function
(No NAT/NAPT is required)

Figure 9 – NAT/NAPT Application

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

9.2 Encryption

Two methods are used for encrypting information: IPSec as specified in [45] and TLS (Transport Layer Security) as specified in [46] .

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, it is for further study.

9.2.1 Encryption for private interconnections

In case of interconnection configurations described in section 6.1, the use of encryption is not recommended either for the signalling or for the media flows.

9.2.2 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.

9.3 Source Authentication

When IPSec is used (see section 9.2), it shall be used also for source authentication. Exchange of keys should be based on IKEv2 [47].

9.4 Access Control

For carriers to protect their networks from the following threats:

- Distributed Denial of Service (DDoS) attack
- Theft of Service
- Protocol Fuzzing

is recommended to implement IP packet access control based on the following mechanisms:

- packet screening based on Access Control Lists (ACL);
- rate limiting.

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 Functions are allowed in.

Other techniques, such as Dynamic Port Opening (DPO), may be applied depending on specific carrier implementation.

Rate limiting implies that the overall bandwidth allocated to service requests coming from a specific source is limited, so that source can not flood the voice platform with call setups.

9.5 Functionalities for compliance with international legal framework

No specific regulatory obligation related to security in international IP interconnection exists so far.

10 Quality of Service parameters.

This section describes the QoS parameters pertaining to the international interconnection between carriers. The following QoS parameters are considered the most important in this first deliverable and they are divided in 3 different sets relevant to the transmission/IP layer, the voice/media quality and the network, respectively. Other parameters can be measured and/or monitored by carriers.

Transmission/IP parameters:

- Bit Error Rate
- RTP round-trip delay
- RTP jitter
- RTP packet loss

Voice/media parameters

- MOS / R-factor for voice quality
- Fax quality

Network parameters

- ALOC
- ASR
- NER
- PGRD

10.1 Parameters relevant to the Transmission/ IP layer

Bit Error Rate
The Bit Error Rate is defined in ITU-T Recc. G.821 [55] as the ratio between the number of bit errors to the total number of bits transmitted in a given time interval.

It should be measured between the PE router of a carrier and the corresponding PE router of the interconnected carrier.

RTP Round Trip Delay
The RTP Round Trip Delay is defined as the time it takes for a packet to go from one point to another and come back [56].

It should be measured between the PE router (in case of an IP-based domestic network) / Media Gateway (in case of a TDM-based domestic network) of the first carrier where the domestic operator is interconnected and the PE router (in case of an IP-based domestic network) / Media Gateway (in case of a TDM-based domestic network) of the second carrier where the other domestic operator is interconnected.

RTP jitter
The RTP jitter is defined as the absolute value of differences between the delay of consecutive packets**.**

It should be measured between the PE router (in case of an IP-based domestic network) / Media Gateway (in case of a TDM-based domestic network) of the first carrier where the domestic operator is interconnected and the PE router (in case of an IP-based domestic network) / Media Gateway (in case of a TDM-based domestic network) of the second carrier where the other domestic operator is interconnected.

RTP packet loss
The RTP packet loss is defined as the ratio between the total lost packets and total sent packets.

It should be measured between the PE router (in case of an IP-based domestic network) / Media Gateway (in case of a TDM-based domestic network) of the first carrier where the domestic operator is interconnected and the PE router (in case of an IP-based domestic network) / Media Gateway (in case of a TDM-based domestic network) of the second carrier where the other domestic operator is interconnected.

As an example, the following figure describes the reference points in the measurement configuration for the 3 identified IP layer parameters.

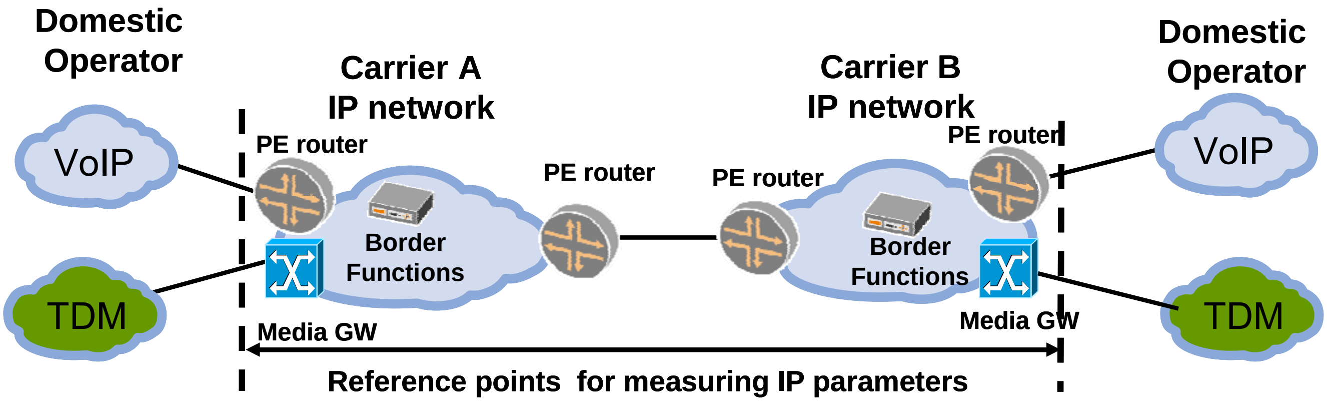


Figure 10 – Example of reference measurement configuration for private-oriented interconnection

10.2 Parameters relevant to the voice/media quality

MOS / R-factor for voice calls

The MOS (Mean Opinion Score) is subjective parameter defined in ITU-T Rec. P.10 [61]/G.100 [59] 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*."

In ITU-T Recc. G.107 Annex B [62] defines a mathematical model to assess the MOS figure, including lost packets delay impairments and codec. This figure is derived from the R-factor whose values, in turn, are computed according to the same ITU-T Recc. G.107.

It can be evaluated by Border Functions and/or Call Handling Functions. Separate measurement equipment may also be used to collect R-factor. It should be measured from originating RTP/RTCP end-point to terminating RTP/RTCP end-point. It is desirable to measure from Border Functions to Border Functions.

Fax quality

Fax quality is defined in ETSI EG 202 057-2 [63] as the ratio of successful fax transactions to the total number of fax transactions.

This parameter has an end-to-end validity.

10.3 Parameters relevant to network quality

ALOC

The Average Length of Call (ALOC) expresses the average time of conversation 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 [60]. In a VoIP 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 or a new transaction) to the time of call release (SIP BYE or CANCEL).

- 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.

It should be measured at the Border Function and/or Call Handling Functions.

ASR

The Answer Seizures Ratio (ASR) expresses the ratio between the number of call session requests and the number of calls effectively answered in a given period of time. In a TDM environment, ASR has been defined in ITU-T Recc. E.411 [57] with the following formula:

$$\text{ASR} = \frac{\text{Seizures resulting in answer signal}}{\text{Total seizures}} \times 100$$

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

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

It should be measured by Call Handling Function, on a monthly basis.

NER

The Network Efficiency Ratio (NER) expresses the ability of a network to deliver a call without taking into account user interferences in a given period of time. In a TDM environment, NER has been defined in ITU-T E.411 [57] and E.425 [58] with the following formula:

$$\text{NER} = \frac{\text{Seizures delivered to the far-end terminal}}{\text{Total Seizures}} \text{ x } 100$$

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 or a new transaction:
    - 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

- 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 BYE response or message type ‘486 Busy Here’ with REL encapsulated and cause release 17 or
    - a BYE response or message type ‘600 Busy everywhere’ with REL encapsulated with 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’ with REL encapsulated with cause value 1 or
    - a BYE response 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.

It should be measured by the Call Handling Function.

PGRD

The 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 or a new transaction and receiving a 180 'Ringing'.

- SIP-I protocol: PGRD is the average time between sending an INVITE with an encapsulated IAM and receiving an alerting signal.

It should be measured by the Call Handling Function.

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

This first deliverable is E.164-based [26]. ENUM addressing scheme will be considered in future releases of this deliverable on the basis of the output of the Work Stream "Service and Requirements". The target of this section is to define the format of numbers and addresses which will be exchanged in signaling messages between operators in international IP interconnect for voice services.

11.1 Numbering and addressing in international interconnect E.164-based

International IP interconnection for voice services will be based on SIP [12] and SIP-I [17]. 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 11.3 and 11.4 respectively.

11.2 International numbering scheme in TDM network

International number format used in International IP interconnect for voice shall conform to E.164 standard [26]. 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 maximum 15 digits starting from Country Code (E.164 [26] 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 ([26] Appendix B, Section B. 3.3) in international voice IP interconnect is OPTIONAL as it is very rarely used.

11.3 TEL URI Addressing scheme

Tel-URI SHALL conform to RFC 3966 “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.

11.4 SIP URI Addressing scheme

SIP-URI shall conform to RFC 2396 [54]. In order to setup an international voice call, the telephone number used in the SIP URI shall be a valid E.164 number preceded by “+”character and the user parameter value "phone" should be present as described in RFC 3261 [12] section 19.1.1.. As an example of SIP URI the following format is given:

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

12 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 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.

12.1 Call Data 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	Mandatory. G.711 A, G.711 u, G.729, etc.
12.	Egress Codec	Mandatory. G.711 A, G.711 u, G.729, etc.
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 signalling protocols.
23.	Bearer Capability	Optional. For TDM ITU-T SS#7 and SIP-I signalling protocols.
24.	GSDN/Global Software Defined Network Call Type	Optional. For TDM ITU-T SS#7 and SIP-I signalling protocols.
25.	ISDN Supplementary Services	Optional. For TDM ITU-T SS#7 and SIP-I signalling protocols.
26.	UUI Rejection/Subsequent UUI Received Indicator	Optional. For TDM ITU-T SS#7 and SIP-I signalling 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 signalling 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 signalling protocol, suggested codec, suggested network security features.

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

Transport Characteristics
Transport configuration: as specified in sec. 6.1.1
Transmission Interface: either SDH/Sonet- based or Ethernet-based
Type of the IP addresses (of the PE router and Border Functions): 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
Signalling Protocol: SIP-I as specified in ITU-T Recc. Q.1912.5 Annex C Profile C transported over UDP protocol (specified in IETF RFC 768)
Voice Codec: as specified in ITU-T Recc. G.711 with RTP protocol as specified in IETF RFC 3550
Fax Protocol: as specified in ITU-T Recc. T.38
DTMF Support:: as specified in IETF RFC 2833
Numbering and Addressing: as specified in ITU-T Recc. E.164

Security Characteristics
Border Functions: required
Signalling 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 sec. 6.2.2
Transmission Interface: either SDH/Sonet- based or Ethernet-based
Type of the IP addresses (of the PE router and Border Functions): 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 5% over-provisioning factor taking into account IP packet payload and protocols overhead

Service Characteristics

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

Security Characteristics

Border Functions: required
Signalling 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 int. segment)	**99.99%** monthly with dual access, **99.95%** monthly with single access	**99.99%** monthly with dual access, **99.95%** monthly with single access
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**