Anhang 1 zum Handbuch Technik

VoIP Interkonnektion – Public Network-to-Network Interface

Version	2-2
Ausgabedatum	16.05.2023
Ersetzt Version	2-1
Gültig ab	01.09.2023
Vertrag	Vertrag betreffend Verbindung von VoIP Fernmeldeanlagen und -diensten

Table of Contents

1 Scope and Objectives

1. The objective of this document is to provide a specification of the SIP Network-to-Network Interface (NNI) used between two SIP telephony service providers to exchange voice traffic.

2. The scope of this document is to describe general parameters and procedures for basic call establishment, call control and a common set of telephony features.

3. The functionality specified herein, covers the functional layers from the network layer of the NNI up to and including RTP and SIP.

2 VoIP Interconnection Reference Architecture

2.1 Introduction

1. The Swisscom VoIP Interconnection architecture is built on the principal of individual point to point peerings (hereafter referred to as interconnection) with another Provider of Telecommunication Services (PTS).

2. The architecture principals are close to the ITU-T Rec. Q.3401 and take benefits of the specifications made and described by the IETF Speermint Project (Draft Hancock) as well as the Technical Recommendations published by the International IP Interconnection Forum (i3 Forum).

2.2 Key Words

1. This document uses the same key words as IETF drafts and RFCs when defining levels of requirements. In particular, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", “SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY" and “OPTIONAL" are to be interpreted as described in BCP 14, RFC 2119 to indicate requirement levels for compliant SIP signaling interworking.

2.3 Technical Principals

1. The NNI reference architecture consist of 4 physical IP Point of Interconnect (IP-POI) and 2 logical SIP Point of Interconnect (SIP-POI) as depicted by figure 1 below.

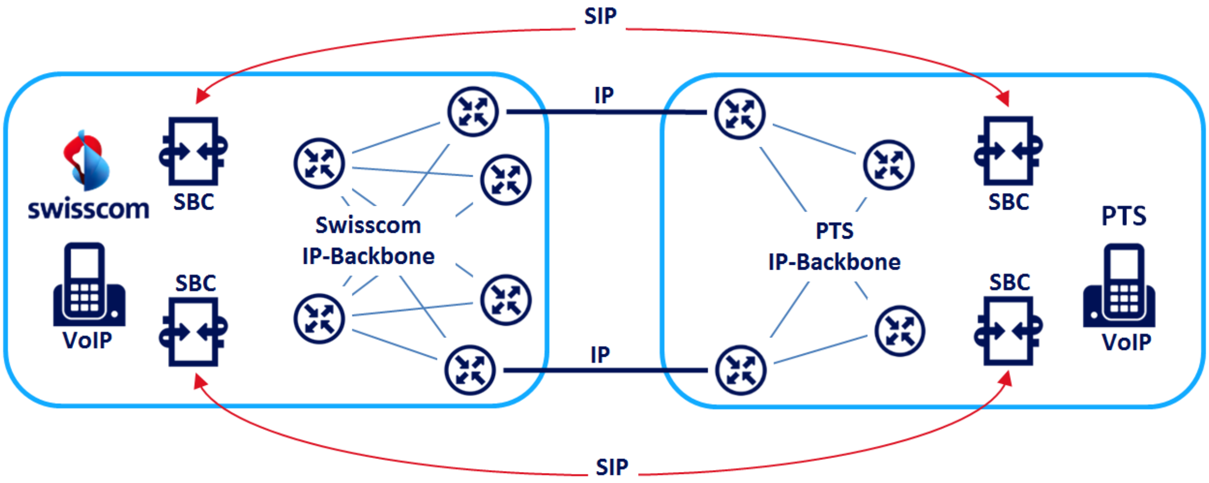

Figure 1 Reference Architecture for VoIP Interconnection – Public NNI

2. Each interconnection partner (PTS) can choose two IP-POIs where VoIP traffic is handed over. IP interconnection at more than two IP-POIs is subjected to bilateral agreements. Further details about the IP-POIs and the network connection can be found in the contract document 'Leistungsbeschreibung Netzdienste VoIP'.

3. Independent of the IP-POI, each interconnection partner MUST peer with the two Swisscom interconnection SBCs. Swisscom likewise expect to send traffic to two different interconnection SBCs in the PTS network. The interconnection SBC (border SBC) MUST be configured as B2BUA (Back-to-Back User Agent) for signaling and media termination.

4. Interconnection SBCs SHALL be configured with a one-to-one association to each other. They SHALL NOT fail over to the other interconnection partner SBCs if reachability to the associated SBC has been lost. Instead, if the associated interconnection partner SBC becomes unavailable, the interconnection SBC SHALL crank back to its own core network which MUST then re-route via the second VoIP NNI path. This concept is intended to simplify the re-routing cases and avoid unnecessary post-dial delay.

5. To achieve optimal load sharing and minimal service impact in the event of a major network outage, both SIP paths SHALL be equally used, hence the partner SHALL distribute traffic equally among both interconnection SBCs. Either path MUST support the full set of agreed services and (E.164) numbers. Each path SHALL be able to handle 100% of the agreed traffic even in the event of a single POI failure. Therefore, each path SHALL never be operated at more than 50% traffic load under normal conditions. This is true for the IP transit network as well as for the SIP sessions network and the interconnection SBCs.

   Further details concerning the dimensioning guidelines for VoIP interconnection, including the maximum capacity utilization of an interconnection link, can be found in the contract document 'Handbuch Technik'.

6. Figures 2 and 3 below depict the logic behind this concept; the two upper interconnection SBCs have a direct relation (association) with each other and the two lower interconnection SBCs also have a direct relation with each other.

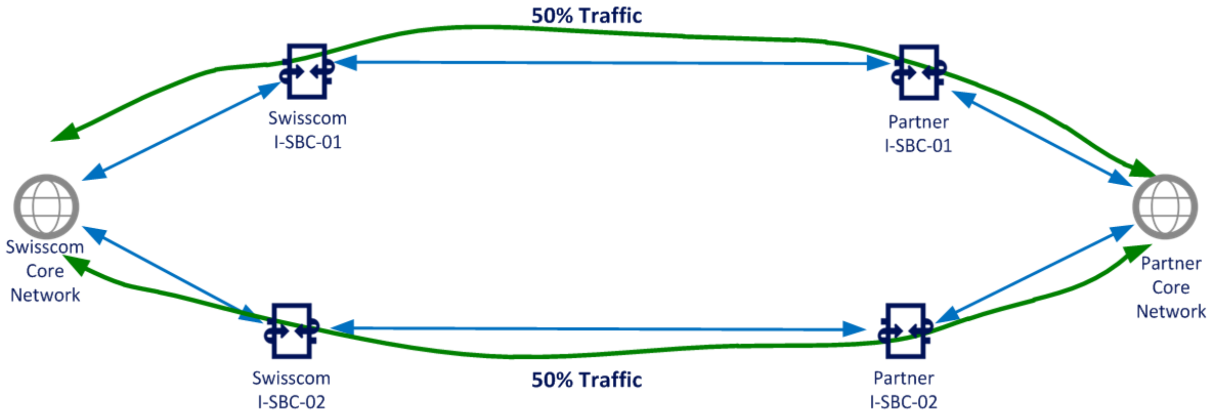

Figure 2 SIP Routing Concept – Normal Condition

7. In the event of a POI failover, the interconnection SBC cranks back and the core network re-routes to the 2nd interconnection SBC (figure 3 below).

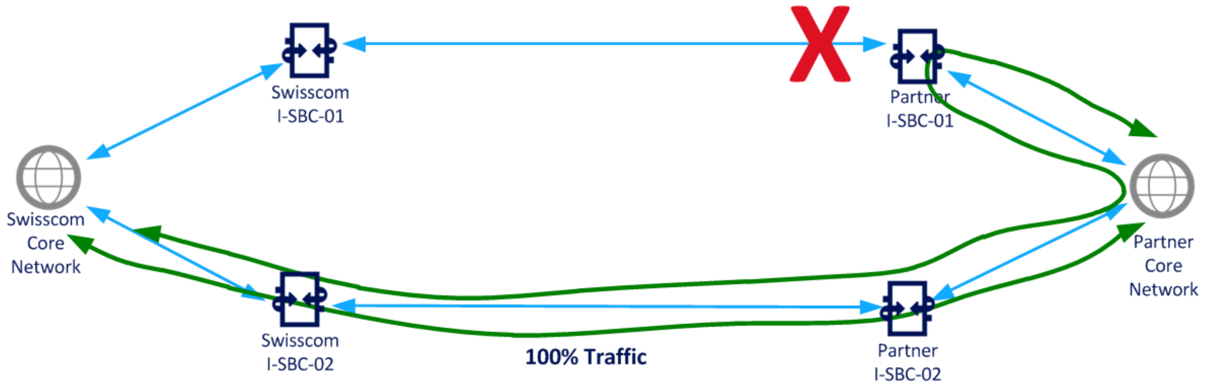

Figure 3 SIP Routing Concept – Single POI Outage & Crankback

8. As depicted by figure 4 below, inbound and outbound traffic SHALL be sent across different, logical SIP interfaces. Media traffic SHALL use a (at least 1) different IP-address than signaling traffic. All IP-addresses exposed by a single SBC SHALL reside in the same logical subnet. Therefore, each interconnection SBC MUST offer at least 4 public IP-addresses of a single, logical IP-subnet.

9. As also shown in figure 4 below, the top-two blue and red "SIP-interfaces" are used for traffic from left

to right while the bottom blue and red Interfaces are used for traffic in the opposite direction. This way it is possible to properly control and monitor inbound and outbound traffic.

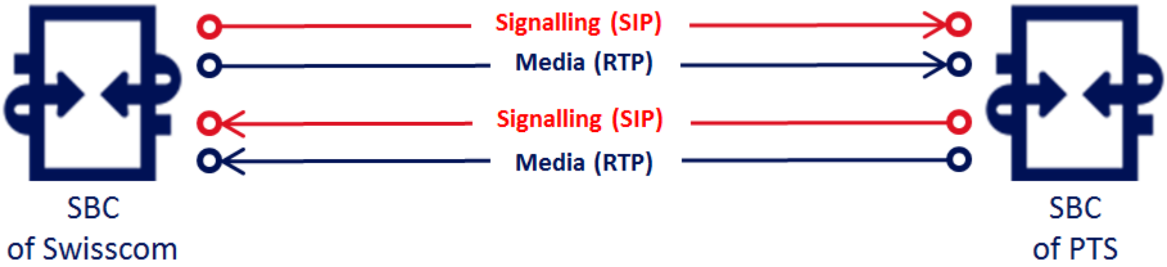

Figure 4 Interconnection SBC Association and IP Addressing Scheme

10. Interconnection SBCs SHALL monitor partner interconnection SBCs using SIP OPTIONS as described later in this document.

3 Technical Specifications

3.1 SIP Signaling

1. IETF SIP (RFC 3261) is used as the base signaling protocol for VoIP Interconnection. For efficiency reasons, UDP SHALL be used as the default layer 4 transport protocol to carry SIP signaling packets. TCP fallback SHALL NOT be used across the NNI. Instead, interconnection SBCs SHALL insure that the MTU packet size does not exceed the maximum SIP-UDP transfer unit of 1500 bytes. Larger SIP packets MUST be fragmented by the interconnection SBCs. The network elements SHALL transmit the UDP packets from the SBC without further fragmentation, i.e. SHALL support the max. Ethernet frame size of 1518 bytes that is needed to include the header entries for MPLS and Queue-in-Queue.

2. A SIP message length of up to 9k MUST be supported. A larger message length MAY be supported. If larger messages can not be supported, the peer SHALL respond with a 513 Message Too Large.

3. Header compression (as described in RFC 2508 or RFC 3095) SHALL NOT be used in IP/UDP/TCP/RTP headers.

4. SCTP (Stream Control Transmission Protocol) MUST NOT be used.

5. ISUP headers and messages SHALL be mapped into the corresponding SIP headers and header values according to ITU-T Rec. Q.1912.5.

3.1.1 SIP Methods Supported

1. The following SIP messages MUST be supported by the interconnection SBCs:

INVITE

ACK

CANCEL

BYE

PRACK

OPTIONS NOTE1

UPDATE NOTE2

2. NOT supported are the following SIP methods:

REFER

REGISTER

SUBSCRIBE

NOTIFY

PUBLISH

INFO

MESSAGE

3. The REQUIRE header SHALL NOT be used whenever possible. Instead, the SUPPORTED header SHALL be used identifying supported SIP extensions. If REQUIRE header must be sent by an interconnection partner for some reason, the receiving partner MAY reject the call with an appropriate reason code if the method is not supported in his network. Only extensions defined in a standard RFC track SHALL be used as specified in RFC 3261 [8.1.1.9]. Unless otherwise specified, all methods supported MUST be used as described in RFC 3261.

NOTE1 OPTIONS SHALL be used to probe reachability and availability of the VoIP Interconnection peers: periodic SIP OPTIONS messages SHALL be sent to the other party to check if the peer is still alive; after 3 unanswered messages, the peer SHALL be marked as out-of-service until the next positive response has been received.

NOTE2 UPDATE MAY be used to refresh the SIP session as an alternative to Re-INVITE.

3.1.2 SIP Header Support

1. The following SIP headers MUST (m) be supported both on the sending and receiving side:

Allow	[RFC 3261, chapter 20.5]
Call-ID	[RFC 3261, chapter 20.8]
Contact	[RFC 3261, chapter 20.10]
Content-Length	[RFC 3261, chapter 20.14]
Content-Type	[RFC 3261, chapter 20.15]
CSeq	[RFC 3261, chapter 20.16]
From	[RFC 3261, chapter 20.20]
History-Info NOTE3	[RFC 4244, chapter 4.1]
Max-Forwards NOTE4	[RFC 3261, chapter 20.22]
P-Asserted-Identity NOTE5	[RFC 3325, chapter 9.1]
P-Charging-Vector NOTE6	[RFC 3455, chapter 4.6]
Privacy NOTE7	[RFC 3323, chapter 4.2]

Reason	[RFC 3326, chapter 2]
To	[RFC 3261, chapter 20.39]
Via	[RFC 3261, chapter 20.42]

2. The following SIP headers MAY (o) be supported, i.e. they MAY be received but can be ignored if the receiving side does not support them:

Accept	[RFC 3261, chapter 20.1]
Alert-Info	[RFC 3261, chapter 20.4]
Call-Info [NOTE 9]	[RFC 3261, chapter 20.9]
Content-Disposition	[RFC 3261, chapter 20.11]
Expires	[RFC 3261, chapter 20.19]
Geolocation [NOTE 9]	[RFC 6442, chapter 4.1]
Geolocation-Error [NOTE 9]	[RFC 6442, chapter 4.4]
Geolocation-Routing [NOTE 9]	[RFC 6442, chapter 4.2]
Info-Package	[RFC 2976, chapter 4]
MIME-Version	[RFC 3261, chapter 20.24]
Min-SE	[RFC 4028, chapter 5]
P-Early-Media	[RFC 5009, chapter 9]
RAck	[RFC 3262, chapter 7.2]
Record-Route	[RFC 3261, chapter 20.30]
Recv-Info	[RFC 2976, chapter 5]
Retry-After	[RFC 3261, chapter 20.33]
Route	[RFC 3261, chapter 20.34]
RSeq	[RFC 3262, chapter 7.1]
Session-Expires [NOTE8]	[RFC 4028, chapter 4]
Supported	[RFC 3261, chapter 20.37]
Timestamp	[RFC 3261, chapter 20.38]
Unsupported	[RFC 3261, chapter 20.40]
User-Agent	[RFC 3261, chapter 20.41]
Warning	[RFC 3261, chapter 20.43]

3. The following SIP headers SHALL NOT (n/a) be used, i.e. neither sent nor received:

Accept-Contact	[RFC 3841, chapter 9.2]
Accept-Encoding	[RFC 3261, chapter 20.2]
Accept-Language	[RFC 3261, chapter 20.3]
Allow-Events	[RFC 3265, chapter 7.2.2]
Authentication-Info	[RFC 3261, chapter 20.6]
Authorization	[RFC 3261, chapter 20.7]
Call-Info	[RFC 3261, chapter 20.9]
Content-Encoding	[RFC 3261, chapter 20.12]
Content-Language	[RFC 3261, chapter 20.13]
Date	[RFC 3261, chapter 20.17]
Error-Info	[RFC 3261, chapter 20.18]
Event	[RFC 3265, chapter 7.2.1]
Flow-Timer	[RFC 5626, chapter 10]
Geolocation	[RFC 6442, chapter 4.1]
Geolocation-Error	[RFC 6442, chapter 4.4]

Geolocation-Routing	[RFC 6442, chapter 4.2]
In-Reply-To	[RFC 3261, chapter 20.21]
Join	[RFC 3911, chapter 7.1]
Min-Expires	[RFC 3261, chapter 20.23]
Organization	[RFC 3261, chapter 20.25]
P-Access-Network-Info	[RFC 3455, chapter 4.4]
P-Answer-state	[RFC 4964, chapter 7.1]
P-Asserted-Service	[RFC 6050, chapter 4.1]
P-Associated-URI	[RFC 3455, chapter 5.1]
P-Called-Party-ID	[RFC 3455, chapter 4.2]
P-Charging-Function-Addresses	[RFC 3455, chapter 4.5]
P-Media-Authorization	[RFC 3313, chapter 5.1]
P-Preferred-Identity	[RFC 3325, chapter 9.2]
P-Preferred-Service	[RFC 6050, chapter 4.2]
P-Profile-Key	[RFC 5002, chapter 5]
P-Served-User	[RFC 5502, chapter 6]
P-User-Database	[RFC 4457, chapter 4]
P-Visited-Network-ID	[RFC 3455, chapter 4.3]
Path	[RFC 3327, chapter 4]
Permission-Missing	[RFC 5360, chapter 5.9.3]
Priority	[RFC 3261, chapter 20.26]
Priv-Answer-Mode	[RFC 5373, chapter 2]
Proxy-Authenticate	[RFC 3261, chapter 20.27]
Proxy-Authorization	[RFC 3261, chapter 20.28]
Proxy-Require	[RFC 3261, chapter 20.29]
Referred-By	[RFC 3892, chapter 3]
Refer-Sub	[RFC 4488, chapter 4]
Refer-To	[RFC 3515, chapter 2.1]
Reject-Contact	[RFC 3841, chapter 9.2]
Replaces	[RFC 3891, chapter 6.1]
Reply-To	[RFC 3261, chapter 20.31]
Request-Disposition	[RFC 3841, chapter 9.1]
Require	[RFC 3261, chapter 20.32]
Security-Client	[RFC 3329, chapter 2.2]
Security-Server	[RFC 3329, chapter 2.2]
Security-Verify	[RFC 3329, chapter 2.2]
Server	[RFC 3261, chapter 20.35]
Service-Route	[RFC 3608, chapter 5]
SIP-ETag	[RFC 3903, chapter 11.3.1]
SIP-If-Match	[RFC 3903, chapter 11.3.2]
Subject	[RFC 3261, chapter 20.36]
Subscription-State	[RFC 3265, chapter 7.2.3]
Trigger-Consent	[RFC 5360, chapter 5.11.2]
WWW-Authenticate	[RFC 3261, chapter 20.44]

NOTE3 History-Info header as defined in RFC 4244 SHALL be used to reflect Call

Deflection/Forwarding.
Diversion header as described in the historic (obsolete) RFC 5806 MAY be used as well for backward compatibility with older systems who have not yet depreciated the use of the Diversion header. If both headers are present in a single call, the History-Info header takes precedence over the Diversion header. If an interconnection partner chooses to perform interworking between Diversion and History-Info at the border of his network, RFC 6044 SHALL be used to do so.

NOTE4 For SIP OPTIONS, if possible/supported by the partner interconnection SBC, the Max-Forwards header parameter SHALL be set to 0 to terminate SIP probing right at the ingress point. For all other SIP messages, the Max-Forwards header SHALL be left to the default value. Interconnection SBCs SHALL respond with a 200 OK or 483 Too Many Hops in case the hop count has been set to 0 by the partner interconnection SBC. SIP OPTIONS requests are specified in section 11 of RFC 3261.

NOTE5 P-Asserted-Identity: The transmission of a trusted identity in form of a calling party number in the SIP header field P-Asserted-Identity among interconnection partners is mandatory. The originating network SHALL ensure that the subscriber's information in the P-Asserted Identity (user part and host portion) are verified, screened and hence can uniquely be assigned to a certain subscriber. The P-Asserted-Identity header shall be set up by the originating network operator and SHALL be transmitted transparently through the networks. For calls originating from a circuit switched network, the P-Asserted-Identity header is set up in general from the interworking network.

NOTE6 P-Charging-Vector: If not already created in the interconnection partner network, the interconnection partner SBC MAY generate and insert an ICID value along with its own IP-address in the icid-generated-at field and the orig-ioi specifying the carriers origin domain. Already existing P-Charging information MAY be transparently sent by the interconnection SBCs.

NOTE7 The Privacy header MUST be used as defined in RFC 3323 if a subscriber has requested privacy (CLIR).

NOTE8 The Session-Expires header as per RFC 4028 SHALL be set to 1800 in all relevant SIP messages (INVITE, 200 OK).

NOTE9 Geolocation SHALL be used for the transport of references for the regulated emergency call localisation.

Call-Info SHALL be used for the transport of references for regulated special applications in the area of emergency calls, e.g. eCall or NGeCall.

In any case, either Geolocation or Call-Info SHALL be populated, i.e. the headers are mutually exclusive.

If the PTS does not have a URL, i.e. there is no localisation for the concerned call, then Call-Info, Geolocation, Geolocation-Error and Geolocation-Routing SHALL be left empty.

3.1.3 SIP Response Codes

1. Unless otherwise specified, SIP response codes SHALL be used according to RFC 3261.

2. In the context of the VoIP NNI, the following response codes SHALL be used for specific scenarios:

   – If a number has been sent across the NNI which is not expected/agreed to be routed across the VoIP NNI, the terminating network SHALL respond with a 403 Forbidden and the originating network SHALL NOT repeat the request across the 2nd VoIP NNI path.
   – If the partner interconnection network can not support any of the offered codecs even though G.711 A-law has been specified as mandatory, it SHALL respond with a 415 Unsupported Media Type or a 488 Not Acceptable Here.
   – If the partner interconnection network can not support a method requested (e.g. due to REQUIRE header), it SHALL respond with a 405 Method Not Allowed.

3. All other responses SHALL follow the intended purpose as described in RFC 3261.

4. The exact definition of proper SIP response codes MAY require adoption on a bilateral agreement.

3.1.4 SDP Requirements

1. The SBC MUST support the SDP requirements defined in RFC 4566. If an interconnection SBC receives an SDP offer containing multiple media descriptors, it MUST act on the media descriptors and include all of them in the same order in the response, including non-zero ports and zero ports for the offered media according to its capabilities as specified in RFC 3264.

2. While a Content-Type of application/sdp MAY be appropriate for basic telephony calls, SIP MIME types along with a Content-Type of multipart/mixed MUST be supported across the NNI to support future services and functions such as emergency calls or other media types. If an interconnection partner does not support this within his network, he MAY decide to strip these messages at the interconnection SBC until support has been agreed and ratified in a future release of the VoIP Interconnection NNI described in this document.

3.1.5 Call Flow Scenarios

1. The following call flow scenarios are in reference to the IETF Speermint Working Group Draft “draft-hancock-sip-interconnect-guidelines” and have been used as the guiding principal for the VoIP Interconnection NNI.

2. Where applicable, call flows have been adapted or removed to adopt to the VoIP Interconnection NNI.

3.1.5.1 Basic Call Setup

1. This section describes the procedures required to establish a 2-way session for a basic voice call between two users. In this case it is assumed that no originating or terminating features are applied (no call blocking, forwarding, etc.), and that the called line is available to accept the call.

2. Both, early- and delayed offer MUST be supported by the interconnection SBCs to setup a basic call as per RFC 3261. In the case of an early offer (which is the preferred method over the VoIP Interconnection NNI), the originating SBC MUST include an SDP offer in the initial INVITE.

3. Likewise, unreliable- and reliable call setup MUST be supported by the interconnection SBCs. However, SIP provisional acknowledgement (PRACK) as per RFC 3262 SHALL be used as the preferred method. In the case of PRACK, the terminating SBC MUST include an SDP answer in the first reliable response to INVITE. The terminating SBC MAY also include an SDP body in a non-reliable provisional 18x response to the INVITE. The SDP contained in a non-reliable 18x provisional response can be considered a "preview" of the actual SDP answer to be sent in the 200 OK to INVITE. The originating SBC can act on this "preview" SDP to establish an ‘early media’ session. The terminating SBC MUST ensure that the "preview" SDP matches the actual SDP answer contained in the 200 OK response to INVITE.
4. The SBC SHALL always set the SDP mode attribute in the initial offer/answer to "a=sendrecv". Setting the mode to "a=sendrecv" on the initial SDP offer/answer exchange avoids an additional SDP offer/answer exchange to update the mode to send-receive after the call is answered. This should help mitigate the problem of voice-clipping on answer.
5. Interconnection SBCs that advertise support for different but overlapping sets of codecs in the SDP offer/answer exchange for a given call SHALL negotiate a common codec for the call to avoid transcoding. Codec negotiation SHALL occur according to the RFC 3264 and RFC 4317. A minimal set of mandatory codecs are described later in this document.
6. If no common codec can be agreed, the terminating SBC SHALL respond with a SIP 415 “Unsupported Media Type” or SIP 488 “Not Acceptable Here”.
7. An SDP offer/answer exchange occurs within the context of a single dialog. Therefore, the requirement for matching SDPs in the provisional and final responses to INVITE applies only when the provisional and final response are in the same dialog. If the provisional and final response are on different dialogs (say, when the INVITE is forked), the requirement for matching SDPs does not apply.

3.1.5.2 Session Refresh

1. If a SIP session is refreshed by sending a Re-INVITE and the SDP is identical to the SDP in the previous INVITE, the answerer SHALL NOT interpret this as a new offer and thus SHALL respond with the same SDP as the previous SDP from the answerer.

   If the answerer nevertheless responds with a different SDP (e.g. because the answerer deliberately wants to modify the characteristics of the session), then the offerer is strongly RECOMMENDED to forward the new SDP answer to the originating (calling) user agent.

   This behaviour should reduce the risk of asymmetric codec usage which ultimately may cause loss of end-to-end media.

3.1.5.3 Call Hold

1. To avoid dropped calls or calls that can not be retrieved after Call Hold, Call Hold MUST be based on the RFC 3264 (Offer/Answer in SDP) method. The obsolete RFC 2543 using a null address (c=IN IP 0.0.0.0) MUST NOT be used at the NNI.
2. The interconnection SBC (on behalf of the calling party) that wishes to place a media stream "on hold" MUST offer an updated SDP to its peer network with an attribute of "a=inactive" or "a=sendonly" in the media description block.
3. An SBC that receives an SDP offer with an attribute of "a=inactive" in the media description block MUST

place the media stream "on hold" and MUST answer with an updated SDP containing a media attribute of "a=inactive". It MUST NOT set the connection data of the answer SDP to c=0.0.0.0.

3.1.5.4 Call Transfer

1. A user can perform the various forms of Call Transfer (consultive transfer, blind transfer).
2. SIP Re-INVITE is the supported method to be used for Call Transfer across the VoIP Interconnection NNI.
3. The SIP REFER method according to RFC 3515 MUST NOT be used at the NNI. If the SIP REFER method is used within the partner network, the REFER MUST be interworked latest at the NNI into Re-INVITE.
4. Call Transfer using Re-INVITE is based on the Call Hold model explained further above in this document. To transfer the call, the B-party (called party) puts the A-party (calling party) on hold using the method for Call Hold above and establishes a new call to party C. After the call between the B- and C-Parties is established, the B-party modifies both call legs media information to connect A and C together while the B-party’s proxy remains in the signaling path.
5. Whenever possible, the media path SHALL be optimized by the originating SBC.

3.1.5.5 Call Diversion/Deflection

1. If a user’s endpoint is configured for Call Diversion and the forwarded destination is outside the originating network , then the forwarding proxy/SBC SHALL remain in the signaling path of the forwarded call in order to support separate billing of forward-from and forward-to legs.
2. The History-Info header SHALL be used as defined in RFC 4244 to reflect call forwarding condition and detect call forwarding loops. A reason cause SHALL be presented if known.
3. For backward compatibility reasons, the Diversion header as described in RFC 5806 MUST be supported as well.
4. A partner interconnection SBC MAY apply interworking functions between the two methods as described in RFC 6044.

3.1.5.6 CANCEL Message

1. A CANCEL message MAY contain a reason header (RFC 3326) to indicate the reason for the CANCEL message. The interconnection SBC SHALL transparently transport this reason header.

3.1.5.7 Ringback Tone and Early Media

1. During the call setup phase, while the originating network is waiting for the terminating network to answer the call, the originating line is either playing local ringback tone to the calling user or connected to a receive-only or bi-directional early-media session with the terminating network. For example, early media can be supplied by the terminating endpoint (e.g. custom ringback tone) while waiting for answer.
2. During session establishment, an SBC MUST use the following procedures in the following paragraphs to control whether the originating line applies local ringback tone or establishes an early media session while waiting for the call to be answered.

3. The terminating user (network node) MUST send the following provisional response to a call-initiating INVITE:

   - a 180 (Alerting) response containing no SDP if the call scenario requires the originating network to apply local ringback tone,
   - a 183 (Progressing) response containing SDP that describes the terminating media endpoint if the call scenario requires the originating network to establish an early-media session with the terminating media endpoint.

4. The originating user (network node) MUST perform the following action on receipt of a provisional response to a call-initiating INVITE:

   - on receiving a 180 (Ringing) response containing no SDP, apply local ringback tone,
   - on receiving a 180 (Ringing) or 183 (Progressing) response containing SDP, establish an early media session with the media endpoint described by the SDP,
   - on receiving any other provisional response (with or without SDP) do nothing (e.g. continue to apply local ringback tone if it was already being applied when response was received).

5. The above complies with the emerging IETF Proposal RFC 3960.

6. The use of the P-Early-Media header field as described in IETF RFC 5009 to control the flow of media in the early dialog state may be useful in any SIP network that is interconnected with other SIP networks, but the support by the partner network is OPTIONAL.

3.1.5.8 Early Media with Multiple Terminating Endpoints

1. There are some call scenarios that require media sessions to be established (serially) between the originating user agent and one or more intermediate media endpoints before the call is connected to the final target called user agent. For example, the terminating network can insert a media server in the call to interact with the calling user in some way (e.g. to collect a blocking-override PIN) before offering the call to the called user. Another case occurs when the called user fails to answer within an allotted time and the call is redirected to voice-mail, or forwarded to another user via Call Forwarding Don't Answer (CFDA). These different cases can be combined in the same call.

2. For each terminating media endpoint that is associated with a call before the call is answered, the terminating network must decide whether to establish an early media session or apply ringback tone at the originating user agent. For example, consider the case where the called user has call blocking with PIN override, and CFDA. First, an early-media session is established with the call-blocking server to collect the PIN, next the originating user agent is instructed to play local ringback tone while waiting for the called user to answer, and finally an early media session is established with the forward-to party to play custom ringback tone.

3.1.5.9 Forking the INVITE

1. Forking is a mechanism for supporting multiple terminating media endpoints before answer. For each terminating media endpoint that requires an early media session to be established with the originating media endpoint, the terminating SBC MUST signal the attributes of the terminating media endpoint to the originating SBC within the SDP of a 183 (Progressing) response. The terminating SBC MUST ensure

that 18x responses containing different SDP copies are not sent within the same dialog. The terminating SBC does this by specifying a different To: tag for each provisional response that contains a unique SDP, as if the INVITE had been sequentially forked. The originating SBC MUST honour the most recently received 18x response to INVITE, based on the procedures defined above in the Basic Call section.

3.1.5.10 Calling Name and Number Delivery (with Privacy support)

1. An originating SBC MUST pass the network-provided, verified number of the originating user in the P-Asserted-Identity (PAI) header of dialog-initiating requests. The calling number is contained in the telephone-subscriber syntax form of the SIP URI, containing an E.164 number as described in the SIP URI format section of this document.
2. In addition to the above mentioned PAI header, a second PAI header containing the tel URI (Telephone number URI) MAY be present (as described in RFC 3325 chapter 9.1).
3. The originating SBC SHOULD also pass the calling number in the From header, which generally contains the originating user identity to be presented to the called user. The number in the From header MAY be user-provided and unverified to support Special Arrangement.
4. Delivery of the calling name as part of the Display-Info header is OPTIONAL and the support by the terminating endpoint is equally OPTIONAL. The calling name is contained in the display-name component of the P-Asserted-Identity header or From Header.
5. Privacy (CLIR) MUST be signaled by the originating user indicated by the Privacy header containing the value “id” as specified in RFC 3323 and RFC 3325. Both SBC’s MUST honour and transparently pass the privacy settings as requested. Swisscom does not support and honour the values “user” or “critical” for the Privacy header.

   In addition and if not already properly set by the originating user, the originating SBC SHALL obscure the identity of the originating user in other headers as follows:

   – Set the identity information in the 'From' header to "Anonymous” using the following URI Syntax : sip:anonymous@anonymous.invalid",

   – Obscure any information from the Call-ID and Contact headers, such as the originating FQDN (Fully Qualified Domain Name), that could provide a hint to the originating user's identity.
6. In cases where privacy is requested by the originating user indicated by a SIP identity equal to “sip:anonymous@anonymous.invalid" in the From header but not properly indicated in the Privacy header as explained above, the originating SBC SHALL insert the proper Privacy header containing the value “id” on behalf of the originating user.
7. If privacy (CLIR) is signaled by the originating user as described above, the identity of the originating user SHALL NOT be presented to the terminating user by the terminating network. Beside the common headers like From and PAI, also other SIP elements (e.g. Call-ID and Contact headers) indicating the identity of the originating user SHALL be obscured.

3.1.5.11 Detecting Call Forwarding Loops

1. Partner network nodes and/or interconnection SBCs MUST be able to detect call forwarding loops.

2. A call forwarding loop is defined to be the scenario that occurs when a targeted subscriber for a call routes or forwards the call to another destination. If the forwarded-to destination also has call forwarding configured or a misconfigured routing table exists, the call can forward back (directly or indirectly) to the original targeted subscriber. When a loop is detected, the network that performs the detection MUST reject the call.

3. In the context of VoIP Interconnection, interconnection SBCs MUST support a configurable limit on the number of times an individual call may be subject to forwarding. If the number of forwarding attempts for a single call exceeds this limit, the SBC MUST reject the call.

4. Loop detection can occur in various ways and is lacking on proper standardisation. Hereafter and in the context of VoIP Interconnection, three methods are described how interconnection partners can detect loops.

5. Method 1: As a minimum, every interconnection partner SBC (or network) MUST support the basic loop detection built-in based on the Max-Forward Header as specified in RFC 3261. Partner SIP Application Servers and partner interconnection SBCs MUST therefore support the Max-Forward Header and MUST NOT reset the value to a new upper limit while a call is in transit. Instead, each SIP node MUST decrement the Hop-Count by one (1) as defined in the RFC. When the Max-Forward counter reaches a value of zero (0), the next node MUST respond back with a 483 Too Many Hops and the call MUST be cancelled. Problems may occur if an intermediate node does not support SIP and protocol conversion in TDM (e.g. ISUP) or H.323 occurs. In that case, Hop-based loop prevention is not possible.

6. Method 2: Additionally, a SBC MAY detect call forwarding loops and limit the number of times a call is forwarded by supporting the History-Info header field as defined in RFC 4244, and by analysing the History-Info entries as described in this section. If the SBC supports the prevention of forwarding loops via analysis of the History-Info header present in the INVITE, then it MUST compare the forward-to address with the set of targeted-to URI (hi-targeted-to-uri) entries from the History-Info header. If there is a match then a loop has occurred. If no History-Info header is present then it is not possible to perform loop detection via this mechanism. If an SBC supports the prevention of forwarding loops by enforcing a maximum number of forwarding attempts, then it MUST calculate the number of forwarding attempts by counting the number of entries in the History-Info header that were added due to call forwarding (i.e. entries containing a nested Reason header which includes a protocol-cause parameter and a reason-text parameter that indicate the call was forwarded. If no History-Info header is present then it is not possible to determine the number of forwarding attempts via this mechanism.

7. Method 3: Finally, loop prevention may occur, based on the Via header analysis. Every SBC (SIP proxy) adds himself in the Via header. If a node detects his own IP-address in a previous Via header entry, a loop may have occurred.

8. If a loop has been detected by method 2 (History-Info header) or method 3 (Via header), the partner SBC SHALL respond with a 482 Loop Detected.

3.2 Media and Other Payload

1. Media traffic is carried using the RTP protocol as specified in the IETF RFC 3550. RTCP (RTP Control Protocol) SHALL be used along with RTP for each media session carried across the NNI. RTP MUST be transported using UDP/IP.

2. SRTP (Secure Real-time Transport Protocol) MUST NOT be used.

3.2.1 Audio Codecs

1. G.711 A-law with 20m packetisation SHALL be used among all interconnection partners as a base codec for VoIP calls across the NNI and MUST be offered in the SDP negotiation in every basic telephony call.
2. Further codecs MAY be offered by the partner network in the SDP offer but the support by the partner network is OPTIONAL.
3. Payload Types (PT) used MUST comply with RFC 3551 (chapter 6). Dynamic payload SHALL NOT be used for standard codecs unless explicitly foreseen in the codec standards reference documentation.
4. Voice Activity Detection (VAD) SHALL NOT be used unless mandatory by the codec profile.
5. Asymmetric packetisation MAY be used for all none-mandatory codecs (all except G.711 A-law), but the support by the partner network is OPTIONAL. Calls MAY be rejected with an appropriate response (415, 488,) if the partner network can not support asymmetric packetisation.
6. If transcoding or transrating is required, it is in the responsibility of the terminating network.

3.2.2 Video Codecs

1. Video codecs (active or inactive) MAY be offered in an INVITE. The support by the other network or endpoints, however, is OPTIONAL. To signal no support for Video, the other party MUST indicate this by setting the port number in the corresponding stream to zero as per RFC 3264 section 6.
   Swisscom currently does not support Video Calling.

3.2.3 DTMF

1. It is strongly RECOMMENDED to transmit DTMF digits according to the IETF RFC 4733, or its predecessor RFC 2833 if compatible to RFC 4733. In cases where compressed audio codecs (e.g. G.722) are being offered, the aforementioned RFC method MUST be used to transmit DTMF digits.
2. In cases where DTMF tones are transmitted in-band in a G.711 RTP Stream, it is transparent to the network. A proper DTMF transmission can however not be guaranteed end-to-end.
3. An SDP offer with no telephone-event codec included MUST NOT be rejected for this reason, unless DTMF transmission is absolutely necessary for the session.
4. Out-of-band transmission of DTMF digits with SIP INFO or SIP NOTIFY MUST NOT be used across the NNI.

3.3 Number Format / URI Structure

1. A Number is a string of decimal digits that uniquely indicates the network termination point (hereafter called dial string). The dial string contains the information necessary to route the call to this point. Over-decadic Numbers MUST NOT be used. A dial string may include only the following characters: 0-9,*,# ('#' character is represented as "%23", based on RFC 2396). Dial string is expressed in the User-URI portion of the SIP URI according to RFC 3966.
2. A Name is a string of characters acting as a more readable alias for a given Number. It MAY be

presented to the terminating user depending on the target system. Characters used for Name strings SHALL use the ISO 10646 character set in UTF-8 encoding (RFC 2279).

3.3.1 Operator Number Portability (ONP)

1. ONP MUST also be supported on the VoIP Interconnection NNI.
2. The mechanism used to route ported numbers between operators in today's TDM (ISUP) network is described in the TelDaS "Technical specification for Number Portability in fixed networks".
3. The main attribute behind the concept remains the Number Portability Routing Number (NPRN), which is in essence a 5 digit routing prefix assigned to operators by the OFCOM.
4. A network operator may use the NPRN internally within his own network to perform proper billing and routing.
5. For calls to non-ported numbers, the NPRN SHALL be removed by the originating network operator at the network boundary (egress interconnection SBC).

   It is in the responsibility of the terminating network operator to perform an All Call Query (ACQ) at the ingress interconnection SBC and insert the NPRN in a local network specific element of choice if he requires to use the NPRN to perform proper billing and routing within his own network.
6. Unless otherwise agreed between the two interconnection partners, for calls to ported numbers the NPRN SHALL be sent by the originating network operator as a 5-digit prefix in front of the National Significant Number (NSN) (i.e. sip:NPRN-NSN or sip:+41-NPRN-NSN).

3.3.2 SIP URI Addressing Scheme

1. Numbering and addressing scheme used by the SBC SHALL be E.164-based and follow the format defined in RFC 3966 (chapter 5.1.4 Global Number format). These numbers MUST be expressed using SIP URI. Tel URI (Telephone number URI) is NOT supported for routing.
2. The SIP URI SHALL conform to IETF RFC 3966. In order to setup a call, the telephone number used in the SIP URI SHALL be a valid E.164 number preceded by the "+"character and the user parameter value "phone" SHOULD be present as described in RFC 3261 section 19.1.1.
3. If an interconnection partner network uses international numbers without the leading "+" sign (such as sip:41582219911) internally within its network , it MUST prefix the number with a "+" at the egress interconnection SBC to comply with RFC 3966. Likewise, an interconnection partner MAY strip the "+" at his ingress SBC if he does not wish to see the "+" within his own network.
4. If an interconnection partner network requires to obtain the NPRN for ported numbers, numbers MAY be sent prefixed with the corresponding NPRN either in national format or global number format. If sent in global number format, the Swiss country code (+41) MUST be sent in front of the NPRN to avoid potential overlap with country codes (+CC) matching certain NPRN prefixes.
5. The host portion of the SIP URI can either be an IPv4 address or a domain name, as agreed bilaterally between the two interconnection partners (see also following examples and footnotes).
6. Examples of a valid SIP URI are:

   sip:+41582219911@xxx.xxx.xxx.xxx;user=phone NOTE9 sip:+41582219911@domain.com;user=phone NOTE10

sip:anonymous@anonymous.invalid; NOTE11

sip:"NPRN"582219911@domain.com;user=phone NOTE12

sip:+41"NPRN"582219911@xxx.xxx.xxx.xxx.;user=phone NOTE12

7. Examples of invalid SIP URI are:

sip:+41582219911@domain.com;

sip:0041582219911@domain.com;user=phone

sip:41582219911@domain.com;user=phone

NOTE9 xxx.xxx.xxx.xxx = represents a valid IPv4 address and SHALL be the public IP-address of the originating or Interconnection SBC interface, depending on the SIP header (e.g. R-URI, From, To, PAI).

NOTE10 domain.com represents the domain name that matches the corresponding SIP domain of the originating or the terminating network (depending on the header) and is subject to bilateral interconnection agreement. In the PAI header, domain.com SHALL reflect the origin domain of the calling-party if applicable.

NOTE11 This format is only valid for a calling party number.

NOTE12 This format is only valid for a called party number.

3.4 Synchronisation and Clocking

1. Both Parties MUST make sure their core network equipment is properly clocked and synchronised as recommended by the ITU-T and described in the various G.8xx standards. since IP-based equipment can not use the same clock synchronisation concept as TDM based networks, it is important pure VoIP devices such as the interconnection SBCs use a highly precise clock source to reduce slips and other clocking issues in VoIP transmission. Proper clocking is also important to insure billing consistency.
2. All interconnection SBCs and other involved VoIP devices MUST be synchronised against a stable Stratum 1 time server.

3.5 Services

3.5.1 Supplementary Services

1. The following basic telephony or supplementary services are supported across the NNI. Please note that services with a local network relevance only (i.e. UNI services) are not explicitly listed here.

Caller ID Presentation (CLIP)

Caller ID Restriction (CLIR)

Call Hold (HOLD)

Call Transfer Consultive (CTC)

Call Transfer Blind (CTB)

Call Deflection / Call Forwarding (CD / CF)

Call Waiting (CW)

Three Party conference (3PTY)

3.5.2 Facsimile

1. To enable sending and receiving faxes over the NNI, the following modes are supported with Best Effort:

   – T.38 Fax Relay (Version 0) according to ITU-T Rec. T.38
   – „Pass through“

2. It is up to the A- and B-party to negotiate the appropriate transport.

3. Standard G3 Group facsimile MUST be supported. ITU-T Rec. V.34 Group 3 MUST be supported up to 7’200bps. Higher speeds MAY be supported and are subject of bilateral testing.

4. In “pass through” mode, fax is transmitted “in-band” as voice payload through a normal VoIP call using the G.711 A-law voice codec. VAD SHALL be disabled and jitter buffer SHALL allow for larger values (>80ms) to avoid dropped calls. Fax “pass-through” mode SHALL be used with the following guiding principles:

   – G.711 A-law, 20ms packetisation, no VAD.

5. In T.38 mode, the following stack SHALL be used:

   – IFT (Internet Facsimile Transfer) for T.30 media
   – UDPTL (facsimile UDP Transport Layer).

6. It is RECOMMENDED that all SIP devices that support both modes for fax transmission, support fallback to G.711.

7. The Swisscom SIP devices support either “G.711 only” or both T.38 and G.711 for fax transmission. All Swisscom SIP devices that support both modes for fax transmission, support fallback to G.711.

8. Transcoding between the two modes SHALL NOT be used, unless the service provider is using SIP devices supporting T.38 only.

3.5.3 Data Services (Modem)

1. Data services (modem data) across the NNI are carried at best effort and cannot be guaranteed. Modem Traffic SHALL be transmitted “in-band” as voice payload using the G.711 A-law voice codec. This technique is often referred to as Voice Band Data (VBD).

2. ITU-T Rec. V.150.1 Data-Relay MUST NOT be used.

3.6 Quality of Service

1. Quality of Service parameters together with the relevant measurement points MUST be agreed at the NNI interface.

2. The following parameter is relevant to the transport layer:
   - round-trip delay time (RTD)
3. The following parameters are relevant to the service layer:
   - ALOC
   - ASR
   - NER
   - PGRD
4. The following parameter is relevant to the call attributes:
   - CLI transparency

3.6.1 Transport Layer QoS

1. ITU-T Rec. G.114 defines a maximum of 150ms one-way delay for any given call and a total delay budget of 400ms. Therefore, any given national call SHALL NOT exceed the above values for calls originated and terminated between two partner networks.

   A more reasonable value for calls originated and terminated between two interconnection partner networks, assuming both parties are located within the Swiss network boundaries (i.e. not software abroad), is an RTD of 45ms. It should be noted that actual performance across the NNI and the interconnection partner IP backbone could be even better.
2. In the context of the NNI specification, RTD is the total time that it takes to transmit an IP packet from a given source (phone/gateway) in the partner network to the destination (phone/gateway) in the other partner's network and receive the reply packet from the same destination at the origin source.
3. A best practice for a more accurate RTD for International calls has been defined by the GSMA in the IR.34 reference document and SHALL be used as a reference for transit- and international calls carried across the NNI.

3.6.2 Service Layer QoS

1. The following service layer KPIs have been taken from the i3 Forum interconnect proposal and are essentially translations from the old SS7 TDM world. However, SIP is a more flexible protocol and has a wider range of response messages. Accordingly, IETF has defined a set of new KPIs described in the IETF draft "draft-ietf-pmol-sip-perf-metrics-xx.txt". Due to lack of standardisation and missing implementation, however, legacy TDM KPIs have currently been chosen for VoIP Interconnection.

3.6.2.1 ALOC

1. The Average Length of Conversation (ALOC) expresses the average time in seconds of conversations for all the calls successfully set up in a given period of time. In a TDM environment ALOC has been defined in ITU-T Rec. E.437 with the following formula:

   ALOC = [Time periods between sending answer and release messages / Total number of answers]
2. In the context of the SIP NNI and for the purpose of this document, ALOC is defined as follows:

   ALOC is measured from the time of SIP message 200 OK (in response to an INVITE initiating a dialog) to the time of call release (SIP BYE message).

3.6.2.2 ASR

1. Answer Seizure 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 = [Seizures resulting in answer signal / Total seizures]

2. In the context of the SIP NNI and for the purpose of this document, ASR is defined as follows:

   ASR is the ratio between the number of received 200 OK SIP messages (in response to an INVITE initiating a dialog) and the number of sent INVITE initiating a dialog.

3.6.2.3 NER

1. 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 Rec. E.425 released in 2002 with the following formula:

   NER= [Answer message or user failure / Total seizures]

2. In the context of the SIP NNI and for the purpose of this document, NER is defined as follows:

   NER is the ratio of the number of received responses amongst the following responses, with the number of sent INVITE initiating a dialog:

   – a 200 OK response to an initial INVITE or
   – a BYE response or
   – a 3xx response or
   – a 404, 406, 410, 433, 480, 483, 484, 485, 486 or 488 response
   – a 600, 603 or 606 response
   – a CANCEL message (in forward direction i.e. from the calling party)

   Note that 403 is not included because it is categorized as both Network and User events.

3.6.2.4 PGRD

1. 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:

   The PGRD is the elapsed time after INVITE until media is available to the remote device.

2. It can be calculated with the average time between sending an INVITE initiating a dialog and the first received message of the following SIP responses:

   – 180 resulting in local ringing at the remote device.
   – The first 200 OK without preceding 180 or 183, resulting in the call/session being answered.
   – 183 with SDP and if there is no 180, resulting in media being available from the far end to the remote device. The media from the far end to the remote device will typically be ringing, but there are scenarios where the media would be either a tone or an announcement.

3.7 Billing

1. Since signaling delay in a VoIP network, and especially if TDM Interworking is involved, can be more lengthy compared to a legacy TDM backbone using SS7 ISUP, it is RECOMMENDED that interconnection billing CDRs are taken by both parties from their respective interconnection SBCs to insure the least discrepancy in call duration values.
2. Trigger point for a successful call and hence starting point for billing SHALL be the 200 OK SIP message sent by the interconnection SBC (in response to an INVITE initiating a dialog). The billing SHALL end at call release (SIP BYE message sent be either party).
3. Call setup MUST be cancelled latest after 4 minutes as per ITU-T Rec. Q.118 “Abnormal Conditions – Special Release”.
4. The IMS Charging Identity (ICID) carried in the P-Charging-Vector MAY be used for billing correlation between the two parties, unless missing in CDR due to certain call flows or for other reasons.

4 Referenced Documents

Reference	Title
E.164	ITU-T Recommendation E.164 (11/2010) “The international public telecommunication numbering plan”
E.411	ITU-T Recommendation E.411 (03/2000) “International network management – Operational guidance”
E.425	ITU-T Recommendation E.425 (03/2002) “Internal automatic observations”
E.437	ITU-T Recommendation E.437 (05/99) “Comparative metrics for network performance management”
G.114	ITU-T Recommendation G.114 (05/2003) “One-way transmission time”
Q.118	ITU-T Recommendation Q.118 (09/97) “Abnormal conditions – Special release arrangements”
Q.1912.5	ITU-T Recommendation Q.1912.5 (03/2004) “Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control protocol or ISDN User Part”
Q.3401	ITU-T Recommendation Q.3401 (03/2007) “NGN NNI signalling profile (protocol set 1)”
T.38	ITU-T Recommendation T.38 (09/2010) “Procedures for real-time Group 3 facsimile communication over IP networks”
V.34	ITU-T Recommendation V.34 (02/98) “A modem operating at data signalling rates of up to 33 600 bit/s for use on the general switched telephone network and on leased point-to-point 2-wire telephone-type circuits”
V.150.1	ITU-T Recommendation V.150.1 (01/2003) “Modem-over-IP networks: Procedures for the end-to-end connection of V-series DCEs”

RFC 1889	“RTP: A Transport Protocol for Real-Time Applications” (January 1996)
RFC 2119 a.k.a. BCP 14	“Key words for use in RFCs to Indicate Requirement Levels” (March 1997)
RFC 2279	“UTF-8, a transformation format of ISO 10646” (January 1998)
RFC 2396	“Uniform Resource Identifiers (URI): Generic Syntax” (August 1998)
RFC 2508	“Compressing IP/UDP/RTP Headers for Low-Speed Serial Links” (February 1999)
RFC 2543	“SIP: Session Initiation Protocol” (March 1999)
RFC 2833	“RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals” (May 2000)
RFC 2976	“The SIP INFO Method” (October 2000)
RFC 3095	“RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed” (July 2001)
RFC 3261	“SIP: Session Initiation Protocol” (June 2002)
RFC 3262	“Reliability of Provisional Responses in Session Initiation Protocol (SIP)” (June 2002)
RFC 3264	“An Offer/Answer Model with Session Description Protocol (SDP)” (June 2002)
RFC 3265	“Session Initiation Protocol (SIP)-Specific Event Notification” (June 2002)
RFC 3313	“Private Session Initiation Protocol (SIP) Extensions for Media” (January 2003)
RFC 3323	“A Privacy Mechanism for the Session Initiation Protocol (SIP)” (November 2002)
RFC 3325	“Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks” (November 2002)
RFC 3326	“The Reason Header Field for the Session Initiation Protocol (SIP)” (December 2002)
RFC 3327	“Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts” (December 2002)
RFC 3329	“Security Mechanism Agreement for the Session Initiation Protocol (SIP)” (January 2003)
RFC 3455	“Border Gateway” (August 2002)
RFC 3515	“The Session Initiation Protocol (SIP) Refer Method” (April 2003)
RFC 3550	“RTP: A Transport Protocol for Real-Time Applications” (July 2003)
RFC 3551	“RTP Profile for Audio and Video Conferences with Minimal Control” (July 2003)
RFC 3608	“Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration” (October 2003)
RFC 3841	“Caller Preferences for the Session Initiation Protocol (SIP)” (August 2004)
RFC 3891	“The Session Initiation Protocol (SIP) "Replaces" Header” (September 2004)
RFC 3892	“The Session Initiation Protocol (SIP) Referred-By Mechanism” (September 2004)
RFC 3903	“Session Initiation Protocol (SIP) Extension for Event State Publication” (October 2004)
RFC 3911	“The Session Initiation Protocol (SIP) "Join" Header” (October 2004)

RFC 3960	“Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)” (December 2004)
RFC 3966	“The tel URI for Telephone Numbers” (December 2004)
RFC 4028	“Session Timers in the Session Initiation Protocol (SIP)” (April 2005)
RFC 4244	“An Extension to the Session Initiation Protocol (SIP) for Request History Information” (November 2005)
RFC 4317	“Session Description Protocol (SDP) Offer/Answer Examples” (December 2005)
RFC 4457	“The Session Initiation Protocol (SIP) P-User-Database Private-Header (P-Header)” (April 2006)
RFC 4488	“Suppression of Session Initiation Protocol (SIP) REFER Method Implicit Subscription” (May 2006
RFC 4566	“SDP: Session Description Protocol“ (July 2006)
RFC 4733	“RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals” (December 2006)
RFC 4964	“The P-Answer-State Header Extension to the Session Initiation Protocol for the Open Mobile Alliance Push to Talk over Cellular” (September 2007)
RFC 5002	“The Session Initiation Protocol (SIP) P-Profile-Key Private Header (P-Header)” (August 2007)
RFC 5009	“Private Header (P-Header) Extension to the Session Initiation Protocol (SIP) for Authorization of Early Media” (September 2007)
RFC 5360	“A Framework for Consent-Based Communications in the Session Initiation Protocol (SIP)” (October 2008)
RFC 5373	“Requesting Answering Modes for the Session Initiation Protocol (SIP)” (November 2008)
RFC 5502	“The SIP P-Served-User Private-Header (P-Header) for the 3GPP IP Multimedia (IM) Core Network (CN) Subsystem” (April 2009)
RFC 5626	“Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)“ (October 2009)
RFC 5806	“Diversion Indication in SIP“ (March 2010)
RFC 6044	“Mapping and Interworking of Diversion Information between Diversion and History-Info Headers in the Session Initiation Protocol (SIP)” (October 2010)
RFC 6050	“A Session Initiation Protocol (SIP) Extension for the Identification of Services” (November 2010)
RFC 6442	“Location Conveyance for the Session Initiation Protocol” (December 2011)
PRD IR.34 Version 4.9 (4 March 2010)	GSMA rerefence document “Inter-Service Provider IP Backbone Guidelines”

SR 784.101.112/1	Anhang 1 zur Verordnung der ComCom - Technische und administrative Vorschriften für Nummernportabilität zwischen Fernmeldedienstanbieterinnen
IETF Speermint Working Group; Draft Hancock SIP Interconnect Guidelines “draft-hancock-sip-interconnect-guidelines-03” (March 8, 2010)	
i3 Forum “Technical Interconnection Model for International Voice Services” (Release 5.0) May 2012	
TelDaS “Technical specification for Number Portability in fixed networks” Edition 13.0 (25.11.2002)	

5 Abbreviations and Acronyms

ALOC	Average Length of Call Average Length of Conversation
ASR	Answer Seizure Ratio
BCP	Best Current Practice
CDR	Call Data Record Call Detail Record
CFDA	Call Forwarding Don’t Answer
CLI	Caller ID Calling Line Identification
CLIR	Caller ID Restriction Calling Line Identification Restriction
DTMF	Dual-Tone Multi-Frequency signalling
GSMA	GSM Association
ICID	IMS Charging Identity
IETF	Internet Engineering Task Force
IP	Internet Protocol
IMS	IP Multimedia Subsystem
I-SBC	Interconnection SBC
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISUP	ISDN User Part
ITU	International Telecommunication Union
KPI	Key Performance Indicator
MIME	Multipurpose Internet Mail Extensions
NER	Network Efficiency Ratio

NNI	Network-to-Network Interface
NPRN	Number Portability Routing Number
NSN	National Significant Number
OFCOM	Federal Office of Communications L'Office Fédéral de la Communication
ONP	Operator Number Portability
PAI	P-Asserted-Identity
PGRD	Post Gateway Ringing Delay
PIN	Personal Identification Number
POI	Point of Interconnect
PTS	Provider of Telecommunication Services
R-URI	Request-URI
RFC	Request for Comments
RTD	Round-Trip Delay Time
RTP	Real-Time Transport Protocol
SBC	Session Border Controller
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SS7	Signalling System No. 7
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TelDaS	Telecom Data Services
UDP	User Datagram Protocol
UNI	User-Network Interface
URI	Uniform Resource Identifier
UTF	Unicode Transformation Formats
VAD	Voice Activity Detection
VoIP	Voice over IP