INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2001-2004

COM 11 – LS 10 – E

Original: English

Question(s):	11 & 12/11	Geneva, 11 - 22 November 2002

Ref. : TD 35R2 (PLEN)

Source:	ITU-T Study Group 11, WP 3 Questions 11 & 12/11 (SIP-ISUP/BICC interworking)
Title:	In response to your views and requirements concerning SIP-ISUP/BICC interworking

LIAISON STATEMENT

To:	**ETSI (for 3GPP CN, 3GPP CN WG3)**
Approval:	**Study Group 11, November 2002**
For:	**Information**
Deadline:	**June 2003**

Contact: Alf Heidermark
LM Ericsson
Sweden

Tel:+ 46 872 73894
Email : alf.heidermark@uab.ericsson.se

SG 11 thanks you for your “liaison statement” regarding your views and requirement concerning SIP-BICC/ISUP interworking and in particular the draft Q.1912.sip recommendation.

On the requirement level three different profiles are defined. Profile A makes reference to 3GPP TS 24.229. The three profiles are the basis for the protocol work (on draft Q.1912.SIP).

The earliest date that Q.1912-sip can be consented is 2003-09-12. After that an approval procedure is initiated. Therefore the earliest date, assuming successful approval, that recommendation can be approved is November 2003.

It is planned to have an interim Rapporteurs meeting scheduled on 7-11 April 2003 and one electronic meeting later for possible line by line review, which will deal with SIP-BICC/ISUP interworking.

The recommendation Q.1912.sip will be a document encompassing the protocol for the three SIP-ofiles. The text related to profile A constitutes an integrated part of Q.1912.sip.

For your information, please find attached the 2 documents that constitutes the current baselines for draft Recommendation Q.1912.sip.

If you find it helpful, we will be pleased to keep you informed of our work progress.

Attachments:

Draft Q.1912.sip (TD.3/11-38 & 39)

TD **[38-WP3]** /11
http://www.itu.int/md/meetingdoc.asp?type=mitems&lang=e&parent=T01-SG11-021111-TD-WP3-0038

TD **[39-WP3]**/11
http://www.itu.int/md/meetingdoc.asp?type=mitems&lang=e&parent=T01-SG11-021111-TD-WP3-0039

INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2001-2004

STUDY GROUP 11

TD 38 (WP 3/11)

Original: English

Question(s): 11,12/11 Geneva, 11 - 22 November 2002

TEMPORARY DOCUMENT

Source: Editor Q.1912.SIP

Title: Draft Q.1912.SIP: Agreed Output from ITU-T SG11 Meeting, November-2002, Geneva, Switzerland.

Abstract

This TD is an agreed output Draft Q.1912.SIP from Question 11/12 in this SG11 Meeting at Geneva (11-22 November 2002) after reviewing the Editor’s proposed output draft (TD WP3/11-34). This TD is based on agreements or decisions on certain Delayed Contributions to revise the draft Q.1912.SIP (TD WP3/11-16 or OTW-107) output from Ottawa 2002-September meeting. TD WP3/11-16 has been agreed at the beginning of the Question 11 & 12/11 meeting to be the baseline for revision. The clean version of TD WP3/11-16 (without revision marks) was re-distributed as TD3/11-23 in this SG11 Meeting at Geneva (11-22 November 2002). The revision marks within the main text body in this TD reflect changes from TD 3/11-23. Due to document comparison software problem, not all the revision marks for tables in clauses 6.1.3.6, 6.1.3.7, and 7.1.3 that deal with CLI are shown.

Reproduction of the contents of this document

TSB Note: First few pages of this voluminous document are reproduced for paper copy distribution. Full copy is available electronically from current meeting documents in SG 11 Web page.

A limited number of the full paper copies may be available in the meeting room(s) of the relevant question(s) by prior arrangement with the Rapporteur(s)/Author(s) who should inform the TSB Secretariat of any specific requirements sufficiently in advance.

Contact: Koan S. Chong Tel: +1-732-420-4557
AT&T Fax: +1-732-368-6703
U.S.A. Email: kschong@att.com

Draft New Recommendation Q.1912.SIP

Interworking Between Session Initiation Protocol (SIP) and Bearer Independent Call Control Protocol~~INTERWORKING BETWEEN SESSION INITIATION PROTOCOL (SIP) AND THE BEARER INDEPENDENT CALL CONTROL PROTOCOL~~ or ISDN User Part

Summary

This Recommendation defines the signalling interworking between the Bearer Independent Call Control (BICC) or ISDN User Part (ISUP) protocols and SIP in order to support services that can be commonly supported by BICC or ISUP and SIP based network domains.

1 Scope

This Recommendation defines the signalling interworking between the Bearer Independent Call Control (BICC) or ISDN User Part (ISUP) protocols and Session Initiation Protocol (SIP) with its associated Session Description Protocol (SDP) at an Interworking ~~Functional entity~~Unit (IWU). ISUP is defined in accordance with Q.761 to Q.764 and BICC is defined in accordance with Q.1902.1 to Q.1902.4. SIP and SDP are defined by the IETF. The capabilities of SIP and SDP that are needed to interwork with BICC or ISUP are defined in Annex E of this Recommendation.~~The services that can be supported through the use of the signalling interworking are limited to the services that are supported by BICC or ISUP and SIP based network domains.~~

~~ISUP is defined in accordance with Q.761 to Q.764 and BICC is defined in accordance with Q.1902.1 to Q.1902.4. BICC is the call control protocol used between "Serving Nodes" in a network that incorporates separate call and bearer control. An Interface Serving Node (ISN) provides the interface between BICC network domains and non-BICC network domains. The BICC/ISUP capabilities or signalling information defined for national use is outside the scope of this Recommendation. It does not imply interworking for national-specific capabilities is not feasible.~~

~~SIP and SDP are defined by the IETF. The capabilities of SIP and SDP that are interworking with BICC or ISUP in ITU are defined in Q.SIPPROF.~~

An IWU may be stand-alone or may be combined with an ISUP exchange or BICC Interface Serving Node (ISN). It is assumed in this Recommendation that the initial service requests must be forwarded and/or delivered via a trusted Adjacent SIP Node (ASN) within a SIP network domain. The ASN is viewed as a trusted network entity rather than untrusted user entity, and thus the interface between the IWU and the ASN is a Network-to-Network interface (NNI). Where SIP with Encapsulated ISUP (SIP-I) is used, it is assumed that the remote SIP User Agent is able to process ISUP. Support for SIP interworking at a User-Network Interface (UNI) is for further study.

The services that can be supported through the use of the signalling interworking are limited to the services that are supported by BICC or ISUP and SIP based network domains. Services that are common in SIP and BICC or ISUP network domains will seamlessly interwork by using the function of an ~~ISN~~Interworking Unit (IWU). The ~~ISN~~ IWU will also handle (through default origination or graceful termination) services or capabilities that do not interwork seamlessly across domains.

Editor's Note: Specific services or capabilities for interworking and types of interworking treatment will be identified by Question-6/9.

~~It is assumed in this Recommendation that the initial service requests must be forwarded and/or delivered via a trusted Adjacent SIP Node (ASN) within a SIP network domain. Specifically speaking, a standalone IWU or ISN consider this interface as Network-to-Network Interface (NNI). Support for SIP operating in User-Network (UNI) Interface is for further study.~~

~~Editor's Note: A figure illustrating the scope of this Recommendation may be available from Question 6/9. The figure in the input document is deleted to avoid confusion.~~

~~The interworking between BICC or ISUP and SIP occurs in a standalone IWU or an ISN. The scope of this Recommendation is as shown in Figure 1.~~

The scope of this Recommendation is shown in Figure 1~~Figure 1Figure 11~~ and Figure 3~~Figure 2Figure 22~~, respectively.

Note (in Figure 1~~Figure 1Figure 11~~ and Figure 3~~Figure 2Figure 22~~): The content consists of the SIP headers and message body.

Figure 1~~Figure 1Figure 11~~ shows the scope of interworking between SIP and ISUP.

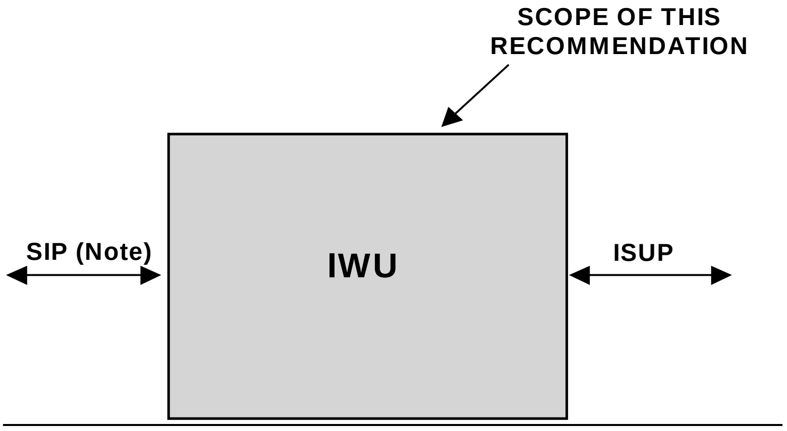


Figure 1/Q.1912.SIP - Scope of Interworking between SIP and ISUP

Figure 3~~Figure 2Figure 22~~ shows the scope of interworking between SIP and BICC.

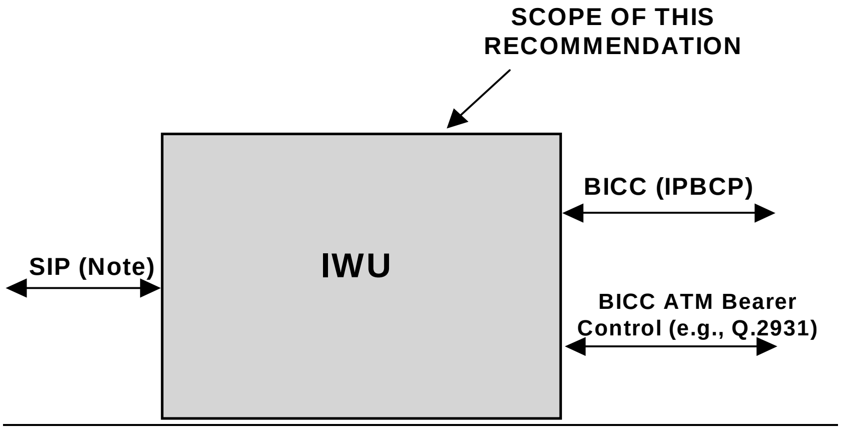

SCOPE OF THIS RECOMMENDATION
IWU
SIP (Note)
BICC (IPBCP)
BICC ATM Bearer Control (e.g., Q.2931)

Figure 3~~2~~/Q.1912.SIP - Scope of Interworking between SIP and BICC

TRQ.BICC/ISUP-SIP specifies the set of common capabilities supported by the interworking between SIP and BICC/ISUP for three different profiles (A, B, and C) in forms of Tables. Tables 1 and 2 of TRQ.BICC/ISUP-SIP specify interworking capabilities for Profile A, Tables 3 and 4 specify interworking capabilities for Profile B, and Tables 5 and 6 specify interworking capabilities for SIP-I, respectively.

2 References

The following ITU-T Recommendations and other references constitute provisions of this Recommendation. At the time of publication, the editions indicated were considered valid. All Recommendations and other references are subject to revisions and therefore all users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. All IETF Standard Track RFC directly referenced by this Recommendation are listed in the ~~Q.SIPPROF~~Annex-E.1.

~~Editor's note: Q.SIPPROF is a planned Recommendation. Some of the references in Q.SIPPROF are currently Internet drafts. Those references will be made to comply with Recommendation A.5~~

[1] ITU-T Recommendations Q.761 to Q.764 (2000) – Specifications of Signalling System No.7 ISDN User Part (ISUP).

[2] ITU-T Recommendations Q.1902.1 to Q.1902.4 (2001) – Specifications of the Bearer Independent Call Control Protocol (BICC).

~~[3] ITU-T Recommendations Q.SIPPROF (200X) – Profile of Session Initiation Protocol (SIP) and Session Description Protocol (SDP) for Interworking Between SIP/SDP and BICC/ISUP.~~

~~.~~[3] ITU-T TRQ.BICC/ISUP-SIP.

3 Definitions

For BICC or ISUP specific terminology, reference shall be made to ITU-T Recommendation Q.1902.2. For SIP and SDP specific terminology, reference shall be made to ~~RFC2543~~ RFC 3261 and RFC 2327 respectively. Definitions for additional terminology used in this interworking Recommendation are as follows:

Incoming or Outgoing: This term is used in this Recommendation to indicate the direction of a call (not signalling information) with respect to a reference point.

Incoming Interworking Unit (I-IWU): This physical entity, which can ~~co-locate~~be combined with ~~the~~ a BICC ISN or ISUP exchange, terminates incoming calls using SIP and originates outgoing calls using the BICC or ISUP protocols.

Incoming SIP or BICC/ISUP [Network]: The network, from which the incoming calls are received, uses the SIP or BICC/ISUP protocol. Without the term “network”, it simply refers to the protocol.

Outgoing Interworking Unit (O-IWU): This physical entity, which can ~~co-locate~~be combined with ~~the~~ a BICC ISN or ISUP exchange, terminates incoming calls using BICC or ISUP protocols and originates outgoing calls using the SIP.

Adjacent SIP Node (ASN): A SIP node (SIP Proxy or Back-to-Back User Agent) that has established a direct trust relation (association) with Incoming or Outgoing IWU entities. ~~A~~ The SIP Proxy and Back-to-Back User Agent are ~~is~~ defined in accordance with ~~RFC2543~~RFC 3261.

~~Editor’s Note: The trust relation referred in the definition of ASN require further study, which should result in defining criteria for a “trusted node” or trust relation referred in this Recommendation.~~

Outgoing SIP or BICC/ISUP [Network]: The network, to which the outgoing calls are sent, uses the SIP or BICC/ISUP protocol. Without the term “network”, it simply refers to the protocol.

SIP ~~Pre-condition~~Precondition: Indicates the support of the SIP “precondition procedure” as defined in ~~draft-ietf-sip-manyfolks-resource~~RFC 3312.

SIP with Encapsulated ISUP (SIP-I): This phrase refers to the use of SIP with a message body that encapsulates the BICC/ISUP information according to the requirements in this Recommendation. SIP-I is only used in Profile-C.

Editor’s Note: The above definitions still need to be reviewed by Question 6/9.

In addition, this Recommendation makes use of the terms **header field**, **message**, **message body**, **method**, **provisional response**, and **User Agent**, which are defined in RFC 3261 clause 6. It uses the term **payload type** as defined in RFC 1889, and **static** and **dynamic** payload type as defined in that RFC. Finally, it uses the terms **attribute** and **session** as defined in RFC 2327.

4 Abbreviations

Editor's Note: Unused acronyms will be deleted when this draft is going for Consent.

APM	Application Transport Message
ASN	Adjacent SIP Node
BCF-N	Bearer Control Nodal Function
BICC	Bearer Independent Call Control
BIWF	Bearer Interworking Function
CSF-N	Call Service Nodal Function
DSN	Destination Serving Node
DTMF	Dual Tone Multi Frequency
IWU	Interworking Unit
ISDN	Integrated Services Digital Network
ISN	Interface Serving Node
ISUP	ISDN User Part
OSN	Originating Serving Node
SCN	Switched Circuit Network
SIP	Session Initiation Protocol
SIP-I	SIP with Encapsulated ISUP
UA	User Agent (i.e. UAC and UAS)

5 Methodology

5.1 Conventions for Representation of BICC/ISUP PDU

1) The first letter of a name for each signalling information element for the following classes of terms is capitalised:

indicators,

parameters,

information elements,

messages.

Examples: Called Party Number parameter, Initial Address Message.

2) The definition of a parameter value is written in *italics* and is inserted between quotation marks.

Example: Nature of Address value 0000011 – "*national (significant) number*".

5.2 Conventions for Representation of SIP/SDP Information[1]

1) All letters of a SIP method name are capitalised; and will follow the word "method".

   Example: Method=INVITE

2) The first letter of a SIP header name is capitalised and the header name is followed with a colon (i.e., "Via:").

   Examples: To: and From:

3) Syntactic fields of a SIP header are represented by the names of the field and are enclosed in "<" and ">".

   Examples: <tag>, <maddr>, etc.

4) The names of SIP parameters will be followed with an equal symbol.

   Examples: transport=

5) The textual representation of response will consist of numeric status code and the name of the associated method.

   Examples: 415 INVITE

6) An SDP information description will consist of a number of lines of text of the form:

   <type>=<value>

   where:

   <*type*> will be exactly one case-significant character, examples: s= (session name), m= (media name and transport address), etc. and

   <*value*> will be structured text whose format will depend on <*type*>,

   examples:

   s=SDP seminar,

   m=video 51372 RTP/AVP 31, etc.

5.3 General Principles

At the SIP interface the IWU shall act as a UA and shall support the standards as defined in ~~Q.SIPPROFILE~~Annex-E. The ISUP interface shall support the protocol as defined in the ISUP Recommendations Q.761 to Q.764 (2000). The BICC interface shall support the protocol as defined in the BICC Recommendations Q.1902.1 to Q.1902.4.

The ~~CSF-N~~IWU shall act as a Type A exchange for the purposes of ISUP and BICC Compatibility procedures.

[1] Based on input from OTW051.

Only the procedures, methods, and elements of information (messages, parameters, indicators, headers, etc.) relevant to interworking are described. Therefore, the procedures, methods, and elements of information that are of local significance (i.e. only relevant to either one of the signalling systems: SIP, ISUP or BICC), are outside the scope of this ~~recommendation~~Recommendation, as they ~~can not~~cannot be interworked.

Editor's Note: Need additional text on handling other services that do not cross the IWU. Further contributions are sought.

The IWU combined with a BICC ISN or an ISUP exchange shall provide interworking between the bearer network connections on the SIP and ISUP or BICC network domain sides.

~~1)~~ 5.3.1 Identification of Call, ~~Call Leg~~Dialog and Call Control Association

The ~~ISN~~ IWU shall establish a one-to-one relationship between a SIP Dialog and a BICC/ISUP call/bearer control instance so that signalling information associated with the same call interwork.

~~Editor's note: The text dealing with (a) ISUP and BICC segmentation and (b) APM segmentation is deleted. New text may be needed at some where in this Recommendation to deal with this segmentation capability that does interwork across the interworking node.~~

~~2)~~ 5.3.2 Encapsulation of ISUP information.[2]

The following general principles of ISUP encapsulation apply within this Recommendation.

a) An IWU receiving a SIP message shall remove the ISUP body from the SIP message. Any differences between the SIP message (e.g. header fields and SDP) and the ISUP message shall be resolved as defined by the procedures within this document. In all cases the resultant ISUP information shall be passed to the relevant ISUP procedures.

b) An IWU receiving ISUP information shall consult its local trust policy to determine if the subsequent node to which the outgoing SIP request is directed is trusted to receive ISUP information. Upon determination that adjacent SIP node (ASN) is trusted to receive ISUP information the IWU shall encapsulate the ISUP message within the body of the SIP message. There are some exclusions as to which ISUP messages may be encapsulated within a SIP message. Clause 5.4 gives details of ISUP encapsulation procedures. These detailed procedures include a list of ISUP messages that are not encapsulated within SIP.

In all cases whereby the IWU inspects a SIP message and discovers that there is no encapsulated ISUP then the IWU is required to construct an appropriate ISUP message using the information received within the SIP header fields and SDP body (if present). Clauses 6 and 7 of this Recommendation provide all the information that the IWU requires to be able to perform this task.

~~NOTE~~Note: The interworking specifications in Clauses 6 and 7 are of use whether or not the received SIP message contained encapsulated ISUP. In the case that the received SIP messages contain encapsulated ISUP information, they provide any necessary interworking between SIP headers and the relevant ISUP parameters thus enabling encapsulated ISUP information to be modified/updated prior to ISUP procedures being applied as detailed in bullet point 1 above. In the case that the received SIP messages do not contain any encapsulated ISUP, they provide the means for the IWU

[2] Based on input from NWB038.

to construct the appropriate ISUP messages purely based on the SIP header (and SDP body) information available.

~~3)~~5.3.3~~–~~ Interworking of ISUP overlap signalling

If an individual ~~gateway~~ IWU is connected to a part of the network which is known through configuration to use overlap signalling then this clause (and associated sub-clauses) are valid. ~~Sections (i) to (iii) present some additional procedures which result whenever overlap signalling is propagated from a BICC/ISUP network into a SIP network. Detailed overlap procedures are provided within the appropriate sections in Clause 6 and 7 of this Recommendation.~~

~~(i) Approach to interworking of ISUP overlap signalling~~

This Recommendation provides the interworking procedures for the case when overlap signalling is propagated into the SIP network and the case where overlap signalling is converted to en-bloc signalling at the O-~~IWF~~IWU. Additionally, procedures are outlined (in Clause ~~7~~6) to address situations where overlap signalling is received on the SIP side of the I-~~IWF~~IWU. While this document covers all four overlap interworking scenarios (viz. ISUP overlap to SIP en-bloc, ISUP overlap to SIP overlap, SIP overlap to ISUP en-bloc and SIP overlap to ISUP overlap) it is recommended that SIP en-bloc signalling is used, i.e. the use of overlap signalling within the SIP network should be avoided. Thus, the preferred scenario is to convert ISUP overlap signalling to SIP en-bloc signalling at the O-~~IWF~~IWU. The decision regarding how to configure a particular ~~IWF~~ IWU with respect to overlap signalling is therefore a matter of local policy/network configuration.

Detailed overlap procedures are provided within the appropriate sections in Clause 6 and 7 of this Recommendation.

~~***Note***:~~

Note-1: when an O-~~IWF~~ IWU knows that a SIP network will be used as a transit network between two PSTN endpoints, it may find it appropriate to propagate overlap signalling through the SIP network, so that ISUP overlap signalling appears in the destination ISUP network.

Note-2 an O-~~IWF~~IWU, connecting to a PSTN that nominally supports overlap signalling, may convert, if it has sufficient knowledge to do so from ISUP overlap signalling to SIP en-bloc signalling.

5.4 ISUP encapsulation - Detailed procedures[3]

This section is relevant only to the profile where ISUP information is encapsulated (or is expected to be encapsulated) in SIP messages sent or received on the SIP interface of an IWU. This section builds on the general principles of ISUP encapsulation outlined in clause 5.3 -(2).

5.4.1 Sending of ISUP information to Adjacent SIP Nodes~~ at O-IWU~~

[3] Based on input from OTW046.

5.4.1.1 Determination of Trust policy

Prior to sending out the INVITE message with encapsulated ISUP the O-IWU shall consult its trust policy to determine whether the ISUP information can be passed to the ASN. If the ASN is trusted to receive ISUP information the O-IWU shall proceed to encapsulate any ISUP information received (with the exception of the excluded messages detailed in clause 5.4.~~4~~3) in a relevant SIP message (see clause 5.4.1.3). Setting of header fields relating to the handling of the ISUP body is specified in clause 5.4.1.2.

Similarly, for the backwards direction an I-IWU receiving backwards ISUP information shall encapsulate any ISUP information received (with the exception of the excluded messages detailed in clause 5.4.3) in a relevant SIP message (see clause 5.4.1.3) only if the node to which the SIP message is being sent is trusted to receive ISUP information. Setting of header fields relating to the handling of the ISUP body is specified in clause 5.4.1.2.

Editor's Note: Deletion of old 5.4.1.2 from TD 3/11-23 dealing with 'Content-disposition" header is based on decision on D.351 and D.405.

~~5.4.1.2 Interworking ISUP Parameter compatibility information (PCI) with "content-disposition" header field (handling-parameter field) for ISUP MIME bodies~~

~~For each instance of a parameter containing PCI the O-IWU shall run the following logic algorithm. If, for any PCI field the algorithm evaluates to "true" then the "handling parameter" in the ISUP message body shall be set to "required" otherwise the "handling parameter" shall be set to "optional".~~

~~***Algorithm for determining value for ISUP body "handling parameter"***~~

~~(Release Call Indicator = Release Call)~~

~~OR~~

~~(Discard Parameter Indicator = Pass On~~
~~AND~~
~~Pass On Not possible indicator = Release Call.)~~

~~OR~~

~~(Discard Message Indicator = Pass on.~~
~~AND~~
~~Pass on Not possible Indicator = Release Call)~~

~~ED. Note: Contributions are invited to address the algorithm of handling "handling parameter".~~

Editor's Note: Content and title of Clause number "5.4.1.2" in this TD is based on decision on D.406.

5.4.1.2 "Content-Type" header field (version parameter) for ISUP MIME bodies

For the purpose of this specification the "Content-Type" header field within the ISUP MIME body shall be supplied as follows:

```
Content-Type: application/ISUP; version= itu-t92+;
```

Note: itu-t92+ means ISUP ’92 plus every higher ISUP Version. However, no action is taken by the IWU on the “version” parameter.

5.4.1.3 Determination of which SIP message to use to encapsulate the ISUP message

For basic call setup the SIP message used to encapsulate the ISUP message is the SIP message that was first triggered to be sent from the ~~O-~~IWU as a result of the interworking specified within ~~chapter 7~~ the main body of this Recommendation and any ISUP specific annexes.

As an example, this means that an ISUP IAM received in clause 7.1.1 (B) will be encapsulated within the INVITE message that is sent out immediately from the O-IWU.

For messages that do not form part of basic call set up or for which no SIP message is generated as a result of receipt of the ISUP message, see section 5.4.3.

5.4.2 Receipt of ISUP information ~~at the I-IWU~~

5.4.2.1 De-encapsulation of ISUP information

On receipt of a SIP message containing encapsulated ISUP the I-IWU shall de-encapsulate the ISUP message body from the SIP message. The ISUP message then goes through a number of stages of additional processing before being sent into the BICC/ISUP network. This processing is specified in clauses 5.4.2.1.1 and 5.4.2.1.2.

5.4.2.1.1 ~~Precedence of~~Alignment of SIP headers ~~over~~ and ISUP body contents

On receipt of a SIP message containing encapsulated ISUP the I-IWU shall use the procedures outlined in this Recommendation with regard to interworking from SIP headers to ISUP parameters to ~~overwrite~~ align any parameters in the ISUP message ~~which~~ that are in conflict with SIP header fields (e.g. due to service invocation within the SIP network) when the SIP ~~request~~ message reaches the I-IWU. The alignment rules regarding which header overrides which ISUP/BICC parameter and vice versa will depend on application/service related aspects.

For example, on receipt of an encapsulated IAM the procedures in chapter 6 relating to the population of the Called party number from the Request-URI would be used to re-write the Called Party number parameters/fields in the de-encapsulated ISUP message.

Once all ~~re-writing~~alignment of these ISUP parameters (and any related fields) has completed the I-IWU shall then pass the resulting ISUP message onto the ISUP procedures (see clause 5.4.2.1.2).

5.4.2.1.2 Passing resulting ISUP message to ISUP procedures / Sending of ISUP message

On receipt of an ISUP message resulting from the actions taken in clause 5.4.2.1 the ISUP message shall be passed to the relevant ISUP procedures. The ISUP message (if any) which results from this step is the ISUP message which is sent on the outgoing BICC/ISUP interface.

5.4.3 Exclusions/Special considerations

The following ISUP messages are either not encapsulated within any SIP message or receive a special treatment with regards to ISUP encapsulation.

Note~~.~~: This table shows only those messages within Recommendation Q.763 which are not marked "national use" and for which ISUP encapsulation is not appropriate. For messages marked "national use" (in Recommendation Q.763) it is up to the relevant national standards bodies to decide whether or not these messages shall be encapsulated within SIP and/or any special encapsulation behaviour that is required for the message.

Editor's Note: Contribution is invited on encapsulation handling of COT.

Table 1/Q.1912.SIP – ISUP Messages for Special Consideration

ISUP message	Reference
Reset Circuit	Note 1
Circuit Group Blocking	Note 1
Circuit Group Blocking Acknowledgement	Note 1
Group Reset	Note 1
Circuit Group Reset Acknowledgement	Note 1
Confusion (?)	Note 2
Facility reject (?)	Note 2
User to User information	Note 2
Forward Transfer	Note 2
Suspend	Note 2
Resume	Note 2
Blocking	Note 1
Blocking Acknowledgement	Note 1
Continuity Check Request	Note 1
Continuity	Note 1
Unblocking	Note 1
Unblocking Acknowledgement	Note 1
Circuit Group Unblocking	Note 1
Circuit Group Unblocking Acknowledgement	Note 1
Facility Accepted	Note 2
Facility Request	Note 2
User part test	Note 1
User part available	Note 1
Facility	Note 2
Network Resource management	Note 2
Identification Request	Note 2
Identification response	Note 2

ISUP message	Reference
Segmentation	Note 3
Loop prevention	Note 2
Application Transport	Note 2
Pre-Release information	Note 2
Release Complete	Note 4
Note 1: see clause 5.4.3.1 Note 2: See clause 5.4.3.2 Note 3: See clause 5.4.3.3 Note 4 See clause 5.4.3.4	

5.4.3.1 ISUP side procedures only

These messages are not encapsulated within SIP messages since they relate to procedures that are relevant only for the ISUP side of the call. Typically these messages are related to maintenance of ISUP circuits. If these ISUP messages are received encapsulated within a SIP messages, the ISUP information shall be discarded.

5.4.3.2 Transparent messages

In these cases, the ISUP message is transported through the SIP network encapsulated in the following SIP messages:

(a) “183” provisional response if this is the first SIP backward message.

(b) ~~a SIP~~ INFO message in all other cases.

These messages are ~~transported within the SIP INFO message since they are~~ deemed important to transport transparently in order to maintain end-to-end service.

~~Ed. Note: Concept is agreed but editorial actions are needed.~~

5.4.3.3 ISUP Segmentation and ISUP encapsulation

The Segmentation message itself is not encapsulated within SIP. Instead the I-IWU (ISUP side interface) will re-assemble the original ISUP message with its segmented part and encapsulate this within the SIP message body.

5.4.3.4 Handling of RLC

A RLC message shall be encapsulated into a 200 (Ok) message sent as a response to a SIP BYE method with encapsulated ISUP REL message.

6 Incoming Call Interworking from SIP to BICC/ISUP at I-IWU

An ~~incoming~~ Incoming ~~Interface Serving node~~Interworking Unit (I-IWU) entity is used to transport calls originated from a SIP network domain to a BICC or ISUP network domain.

The “incoming SIP” refers to the SIP protocol, which is used between the Incoming ~~Interface Serving Node~~IWU and the call originating entity (entities) supported in the SIP network domain. Similarly, the “outgoing BICC/ISUP” refers to the BICC or ISUP protocol supported between the Incoming Interface Serving Node and the next-hop entity (entities) in the BICC or ISUP network domain.

The Incoming ~~Interface Serving Node~~IWU receives forward and backward signalling information from the “incoming SIP” and “outgoing BICC/ISUP” sides, respectively. After receiving this signalling information and performing appropriate call/service processing, the Incoming ~~Interface Serving Node~~IWU may signal forward to subsequent BICC/ISUP nodes or backward to preceding SIP entities. This clause specifies the signalling interworking requirements for basic call at the incoming ~~ISN~~IWU. The chapter is split into sub-clauses based upon the messages sent or received on the outgoing (BICC/ISUP) interface of the ~~ISN~~IWU. Only messages that are generated as a result of interworking to/from the incoming SIP side of the ~~ISN~~ IWU are considered in this interworking. Messages that are generated as a result of a local protocol state machine are not re-described in this specification.

The scope of this ~~section~~ clause is based on the key assumptions: (a) the Incoming ~~Interface Serving Node~~IWU supports originating basic calls only; and (b) calls originated from SIP network domain do not require equivalent PSTN/ISDN service interworking. The service annexes of this document will cover additional interworking specification related to specific PSTN/ISDN services, which may be required by other interworking network architectures.

~~Editor’s Note: The service policies are derived from the operators’ obligation to their subscribers or regulatory agencies. Their obligation to provide certain service grades may cover end-to-end, PSTN/ISDN domain or SIP domain.~~

In the case of Type 2 or Type 4 Gateways as defined in TRQ.BICC/ISUP.SIP, the I-IWU shall (in addition to the procedures outlined within this clause) follow the BICC specific procedures outlined in clause A.2 of Annex A.

~~Editor’s Note: The IWU considered in the following Recommendation shall have the capability to control the timers T7 and T9 as specified in Q.764 and Q.1902.4, respectively.~~

6.1 Sending of Initial Address Message (IAM)

~~Outgoing ISUP procedures apply, with the following clarifications and exceptions with regards to when ISUP IAM and Continuity messages are to be sent.~~The procedures for sending of the IAM message depend on whether the INVITE received from the SIP network contains an SDP Offer. See clauses 6.1.1 and 6.1.2.

The IAM parameters are coded according to clause 6.1.3.

6.1.1 INVITE received without an SDP Offer.

Upon receipt of the INVITE, the I-IWU shall determine if the received INVITE indicates support for reliable provisional responses.

1) If reliable provisional responses are supported, the I-IWU shall immediately send an SDP Offer including media description within a 183 Session Progress message.

   (a) If SIP preconditions are not in use, the I-IWU shall send the IAM upon receipt of the SDP Answer with media description.

   (b) If SIP preconditions are in use, the I-IWU will send the IAM by continuing on to procedure in clause 6.1.2 (2) below.

2) If reliable provisional responses are not supported, the I-IWU shall immediately send out the IAM using local policy to set the TMR/USI mandatory parameters. Depending on any necessary transcoding resulting from the selected TMR/USI, the I-IWU shall send the SDP Offer including media description within the first 18X message backwards towards the SIP endpoint and may repeat this SDP Offer within any subsequent provisional responses until the 200 OK (INVITE) is sent. The 200 INVITE shall contain the same Offer as that sent in all provisional responses.

6.1.2 INVITE received with an SDP Offer or continuation from Clause 6.1.1 (1)

1) If SIP preconditions are not in use, the IAM shall be sent immediately.

2) If SIP preconditions are in use, then:

   (a) If outgoing BICC/ISUP signaling on subsequent network supports the use of the continuity check procedure:

      (i) If the subsequent network is a BICC network: The Continuity indicator of the Nature of Connection indicators field shall be set to “COT to be expected”.

      (ii) If the subsequent network is an ISUP network: The Continuity check indicator in the Nature of Connection Indicators parameter is set to "continuity check performed on previous circuit", or "continuity check required on this circuit". The latter setting shall be used if the continuity check is to be performed on the outgoing circuit.

   (b) If outgoing BICC/ISUP signaling on subsequent network does not support the use of the continuity check procedure, the IAM shall be sent when the I-IWU determines that all preconditions have been met.

In all cases, sub-clause 6.1.1 gives specific details related to the population of specific parameters of the IAM. Table 2~~Table 2Table 2Table 2~~ below gives a summary of parameters within the IAM message that are interworked from the INVITE message along with a reference to the sub-clauses of 6.1.1, in which the specific interworking is described.

Editor’s Note: Replacement of old 6.1.1 to 6.1.4, 6.3, 6.4 and 6.5 from TD 3/11-23 dealing with precondition signaling with a general precondition clause based on Offer-Answer terminology in Clause 6.1 is based on decision on D.376 and D.377. Interworking procedure with sending COT is revised in a new sub-clause.

~~6.1.1 Sending ISUP IAM for INVITE without Pre-Condition~~

~~The ISUP IAM is sent when the INVITE is received and the incoming procedure decides that the call can be routed.~~

~~6.1.2 Sending ISUP IAM for INVITE with Pre-Condition~~[4]

~~Two cases are supported:~~

1. ~~Sending an ISUP IAM, using the continuity check protocol to withhold call completion untilthe I-IWU determines (using the procedures outlined in [3- (manyfolks)]) that session establishment can continue and hence the ISUP COT can be sent on the outgoing BICC/ISUP side to continue call completion on the ISUP side.~~
2. ~~Withholding the sending of the ISUP IAM until the I-IWU determines (using the procedures outlined in [3- (manyfolks)]) that session establishment can continue and hence the IAM can be sent from the outgoing BICC/ISUP side.~~

~~Where the subsequent network supports the continuity check protocol the ISUP IAM is sent when the incoming procedure decides that the call can be routed. The Continuity Check indicator in the Nature of Connection Indicators parameter is set to indicate “continuity check performed on previous circuit”, or “continuity check required on this circuit” may alternatively be sent if the continuity check is to be performed on the outgoing circuit.~~

~~The Continuity message, with the Continuity Indicators parameter set to “continuity check successful” is sent when both of the following conditions are satisfied.~~

1. ~~The I-IWU determines (based upon the procedures outlined in [3-(manyfolks)]) that sufficient pre-conditions have been met on the SIP side of the call for session establishment to continue (on both SIP and ISUP sides of the I-IWU).~~
2. ~~If the continuity check is being performed on the outgoing ISUP circuit, the test shall be successfully completed.~~

~~Where the subsequent network does not support the continuity check protocol the sending of the ISUP IAM is delayed until the I-IWU determines (based upon the procedures outlined in [3- (Manyfolks)]) that sufficient pre-conditions have been met on the SIP side of the call for session establishment to continue (on both SIP and ISUP sides of the I-IWU).~~

~~6.1.3 Sending BICC IAM for INVITE without Pre-Condition~~

~~Outgoing BICC procedures apply, with the following clarifications and exceptions:~~

~~□When sending the IAM the Continuity indicator in the Nature of Connection Indicators parameter is set to “no COT to be expected”.~~

~~6.1.4 Sending BICC IAM for INVITE with Pre-Condition~~

~~Outgoing BICC, (as defined in Q.1902.4) procedures apply, with the following clarifications and exceptions:~~

~~□When sending the IAM the Continuity indicator in the Nature of Connection Indicators parameter is set to “COT to be expected”.~~

~~The Continuity message, with the Continuity Indicators parameter set to “continuity” is sent when the I-IWU determines (based upon procedures outlined in [3- (Manyfolks)]) that sufficient pre-conditions~~

~~have been met on the SIP side of the call for session establishment to continue (on both the SIP and ISUP sides of the I-IWU).~~

6.1.~~5~~3~~-~~ IAM Parameters

Table 2~~Table 2Table 2Table 2~~ indicates the IAM parameters that interwork from SIP.

Table 2/Q.1912.SIP ~~—~~- Interworked Contents of the Initial Address Message

Parameter	Section
Nature of Connection indicators	Section 6.1.~~5~~3.3
Forward Call Indicators	Section 6.1.~~5~~3.4
Calling Party Category	Section 6.1.~~5~~3.2
Transmission medium requirement	Section 6.1.~~5~~3.5
Called Party Number	Section 6.1.~~5~~3.1
Calling Party Number	Section 6.1.~~5~~3.6
User service information	Section 6.1.~~5.7~~3.8
Application transport: BAT (BICC only)	Section 6.1.~~5.8~~3.9
Hop Counter	Section 6.1.~~5.9~~3.10
Generic Number	Section 6.1.~~5.10~~3.7

6.1.~~5~~3.1 -Called Party Number

The information contained in the userinfo component of the Request-URI with user=phone shall be mapped to the called party number parameter of the IAM message.

Support of other URI schemas such as TEL: URI or SIPS-URI, URI component values and URI parameters is optional.

Table 4~~3~~/Q.1912.SIP – Coding of the Called Party Number

INVITE→	IAM→
Request-~~Uri~~URI	**Called Party Number**
Userinfo (SIP URI with user=phone)	Address Signal

6.1.~~5~~3.2 Calling Party Category (Mandatory)

The following codes should be set by the I-IWU as default in the calling party category field

Bits/Codes	Meaning
0000 1010	ordinary calling subscriber

6.1.~~5~~3.3 Nature of Connection Indicators (Mandatory)

The indicators of the Nature of connection parameters, which are set by the IWU, are as follows:

Bits	Indicators in Nature of connection parameter
AB	Satellite indicator
DC	Continuity check indicator (ISUP) / Continuity indicator (BICC)
E	Outgoing echo control device

Other ~~FCI~~ Nature of Connection indicators should follow the current ISUP/BICC Recommendation.

The following codes should be set by the I-IWU as default in the nature of connection indicators parameter field:

Bits	Codes	Meaning	Conditions
AB	00	No satellite circuit in the connection (Note-1)	
	01	One satellite circuit in the connection	
DC~~:=~~ ~~DC:=~~ ~~DC:=~~	00	Continuity check not required (ISUP) / no COT to be expected (BICC)	Without ~~pre-condition~~precondition request.
	10	Continuity check performed on a previous circuit (ISUP) / COT to be expected (BICC)	With ~~pre-condition~~precondition request.
	~~00~~	~~Continuity check not required (ISUP) / no COT to be expected (BICC)~~	~~Pre-condition has been met.~~
E	1	Outgoing echo control device included~~"~~ (Note-1)	

Note-1: Applicable to Profile-A only.

~~Ed. Note: Default bit E setting of "1" is for Profile A & B only. Contributions are invited to address whether bit E should have a default.~~

6.1.~~5~~3.4 Forward call indicators (Mandatory)

The indicators of the FCI parameters, which are set by the IWU, are as follows:

Bits	Indicators in FCI parameter
D	Interworking indicator
F	ISUP/BICC indicator
HG	ISUP/BICC preference indicator
I	ISDN access indicator

Other FCI indicators should follow the current ISUP/BICC Recommendation.

~~IWU~~

For Profiles B and C, ~~The~~ the appropriate values of the FCI are determined based on analysis of various information (signalling, internal states and/or local policies) at the IWU.

For Profile A, the following indicators should be set by the I-IWU as default in the FCI parameter:

Bits	Codes	Meaning	Conditions
D	1	Interworking encountered.	
F	0	ISDN user part/BICC not used all the way.	
HG	01	ISDN user part/BICC not required all the way	
I	0	Originating access non-ISDN	

~~Ed. Note: Contributions are invited to provide further guidelines on the setting of FCI values.~~

6.1.~~5~~3.5 Transmission medium requirement (Mandatory)

The coding of TMR/USI is described in this clause assuming that transcoding is not used by the IWU. Interworking relations between any SDP information and TMR/USI become irrelevant if transcoding is used.

The SDP within the SIP message body shall be used to derive the TMR codes, and USI.

Note: If the outgoing signalling is BICC, the SDP will also interwork with other BICC parameters (APP with BAT) relating to the bearer control signalling information of the selected outgoing bearer. This additional interworking specification is addressed in the BICC-specific Annex.

The SDP Media Description Part received by the incoming ISN should indicate only one media stream.

Only the “m=”, “b=” and “a=” lines of the SDP Media Description Part are considered to interwork with the IAM parameters, TMR and USI.

The first sub-field (i.e., <media>) of “m=” line will indicate one of the currently defined values: “audio”, “video”, “application”, “data”, “image” or “control”.

Further studies are needed if <media> of the “m=” line is “video”, “application” or “control”.

If <media> of the “m=” line is “audio”, then <transport>, <fmt-list> and the optional “b=” line should be evaluated to determine the TMR/USI value used in the outgoing signalling. The bandwidth proposed by the “b=” line should be rounded up to the nearest values of Nx64 kbit/s, where N is an integer starting from 1. If the round-up bandwidth is between 128 and 1920 kbit/s (i.e., $2 \leq N \leq 30$), then the TMR should indicate the corresponding values (kbit/s) for unrestricted digital information. If the bandwidth proposed by the optional “b=” line is greater than 1920 kbit/s, then there is interworking failure.

If the round-up bandwidth for <media> equal to audio is 64 Kbps or “b=” line is absent, then TMR should be set to “3.1 KHz”, and the <transport> and <fmt-list> are evaluated to determine whether User information layer 1 protocol indicator of USI parameter should be set to “G.711 µ–law” or “G.711 A-law”.

The following Table 5~~Table 4Table 4Table 4~~ ~~table~~ provides the mapping relations based on the above procedure.

For Profile A, the TMR parameter is set to 3.1 kHz audio and transcoding is applied when required.

~~Editor note: Are the USI coding for G.722 and FAX correct?~~

Table 5~~4~~/Q.1912.SIP - Coding of TMR/USI from SDP: SIP to ISUP/BICC

m= line			b= line	a= line	TMR parameter	USI parameter		HLC parameter
<media>	<transport>	<fmt-list>	<modifier>:<bandwidth-value>	rtpmap:<dynamic-PT> <encoding name>/<clock rate>[/encoding parameters>	TMR codes	Information Transport Capability	User information layer 1 protocol indicator	High layer characteristics identification
			Note: <bandwidth value> for <modifier> of AS is evaluated to be B kbit/s.					
audio	RTP/AVP	0	N/A or up to 64 kbit/s	N/A	3.1KHz audio	3.1KHz audio	G.711 µ-law	Telephony
audio	RTP/AVP	Dynamic PT	N/A or up to 64 kbit/s	rtpmap:<dynamic-PT> PCMU/8000	3.1KHz audio	3.1KHz audio	G.711 µ-law	Telephony
audio	RTP/AVP	8	N/A or up to 64 kbit/s	N/A	3.1KHz audio	3.1KHz audio	G.711 A-law	Telephony
audio	RTP/AVP	Dynamic PT	N/A or up to 64 kbit/s	rtpmap:<dynamic-PT> PCMA/8000	3.1KHz audio	3.1KHz audio	G.711 A-law	Telephony
audio	RTP/AVP	9	AS:64 kbit/s	rtpmap:9 G.722/8000~~N/A~~	64 kbit/s unrestricted	Unrestricted digital inf. w/tones/ann.	~~G722~~	
audio	RTP/AVP	Dynamic PT	AS:64 kbit/s	rtpmap:<dynamic-PT> ~~G722~~CLEARMODE/8000 (Note-2)	64 kbit/s unrestricted	Unrestricted digital information	~~G722~~	
Image	udptl	t38	N/A or up to 64 kbit/s	~~?~~Based on T.38	3.1 KHz audio	3.1KHz audio	~~FAX (?)~~	Facsímile Group 2/3
Image	tcptl	t38	N/A or up to 64 kbit/s	~~?~~Based on T.38	3.1 KHz audio	3.1KHz audio	~~FAX (?)~~	Facsímile Group 2/3
~~Data~~audio	~~Don't Care~~RTP/AVP	~~Don't Care~~Dynamic PT	0 < B ≤ N × 64 kbit/s	~~Don't care~~rtpmap;dynamic-PT>CLEARMODE/8000 (Note-2)	N × 64 kbit/s unrestricted, where N is a positive integer and N × 64 kbit/s is the smallest multiple greater than or equal to B (evaluated from "b=" line).	Unrestricted digital information		

Note-1: In this table the codec G.711 is used only as an example. Other codec is possible.

Note-2: CLEARMODE has not yet been standardized; and its usage is FFS.

6.1.~~5~~3.6 Calling party number

Table 7~~5~~/Q.1912.SIP - Mapping of SIP From/P-Asserted-Identity/Privacy headers to BICC/ISUP CLI parameters

Has a "P-Asserted-Identity" header field containing a URI (Note 2) with an identity in the format "+CC"+"NCD"+"SN" been received?	**Has a "From" header field (Note 3) containing a URI with an identity in the format "+CC"+"NCD"+" SN" been received?**	**Calling Party Number parameter** **Address signals**	**Calling Party Number parameter** **APRI**	**Generic Number (additional calling party number) address signals**	**Generic Number parameter APRI**
No	No	Network option to either include a network provided E.164 number (See Table 8~~Table 6Table 6Table 6~~) or omit the CgPN parameter	Network option to set APRI to either "presentation restricted" or "presentation allowed" (See Table 8~~Table 6Table 6Table 6~~)	Parameter not included	Not applicable
No	Yes	Network Option to either include a network provided E.164 number (See Table 8~~Table 6Table 6Table 6~~) or omit the CgPN parameter	Network option to set APRI to either "presentation restricted" or "presentation allowed" (See Table 8~~Table 6Table 6Table 6~~)	Network Option to either derive from the "From" header or omit the parameter (See Table 11~~Table 8Table 8Table 8~~) (Note 1)	APRI = "presentation restricted" or "presentation allowed" depending on SIP Privacy header. (See Table 11~~Table 8Table 8Table 8~~)
Yes	No	Derive from P-Asserted-Identity (See Table 7~~Table 7Table 7Table 7~~)	APRI = "presentation restricted" or "presentation allowed" depending on SIP Privacy header. (See Table 7~~Table 7Table 7Table 7~~)	Not included	Not applicable
Yes	Yes	Derived from P-Asserted-Identity (See Table 7~~Table 7Table 7Table 7~~)	APRI = "presentation restricted" or "presentation allowed" depending on SIP Privacy header. (See Table 7~~Table 7Table 7Table 7~~)	Not included	Not applicable

Note 1: This mapping effectively gives the equivalent of Special Arrangement to all SIP UAC with access to the I-IWU.

Note 2: It is possible that the P-Asserted-Identity header field includes both a tel URI and a sip or sips URI. The handling of this case is for further study.

Note 3: The “From” header may contain an “Anonymous URI”. An “Anonymous URI” includes information that does not point to the calling party. RFC 3261 recommends that the display-name component contain "Anonymous". RFC [privacy] recommends that the Anonymous URI itself have the value "anonymous@anonymous.invalid".

Table 8~~6~~/Q.1912.SIP - Setting of the Network-provided BICC/ISUP Calling Party Number parameter with a CLI (Network Option)

BICC/ISUP CgPN Parameter field	**Value**
Screening Indicator	*“network provided”*
Address signals	If NOA is *“national (significant) number”* no country code should be included. If NOA is “*international number”*, then the country code of the network-provided number should be included.

Table 7/Q.1912.SIP - Mapping of P-Asserted-Identity and Privacy Headers to the ISUP/BICC Calling Party Number Parameter

SIP Component	Value	BICC/ISUP Parameter / field	Value
P-Asserted-Identity header field (Note 1)	name-addr / addr-spec	Calling Party Number	
		Number incomplete indicator	*"Complete"*
		Numbering Plan Indicator	*"ISDN/Telephony (E.164)"*
		Nature of Address Indicator	If +CC is equal to the CC of the country where ISN is located AND the next BICC/ISUP node is located in the same country then set to *"national (significant) number"* else set to *"international number"*
		Address Presentation Restricted Indicator (APRI)	depends on priv-value in Privacy header.
		Screening indicator	Network Provided
addr-spec	"+CC" "NCD" "SN" from the URI	Address signal	if NOA is *"national (significant) number"* then set to "NCD" + "SN" If NOA is *"international number"* Then set to "CC"+"NCD"+"SN"
Privacy header field is not present		APRI	Presentation allowed
Privacy header field	priv-value	APRI	*"Address Presentation Restricted Indicator"*
priv-value	"header"	APRI	Presentation restricted
	"user"~~ (when P-Asserted-Identity header does not exist)~~	APRI	Presentation restricted~~Address not available~~
	"none"	APRI	Presentation allowed
	"id" (Note 2)	APRI	Presentation restricted

Note 1: It is possible that a P-Asserted –Identity header field includes both a ~~tel~~ TEL URI and a sip or ~~sips~~ SIPS URI.~~ Processing in this case is for further study.~~ The SIP URI is given priority.

~~Note 2: P-Asserted-Identity header must exist if Privacy header with "id" is included.~~

6.1.~~1~~3.7 Generic number

Table 11~~8~~/Q.1912.SIP Mapping of SIP From Header Field to BICC/ISUP Generic Number (additional calling party number) parameter (Network option)

SIP Component	Value	BICC/ISUP Parameter / field	Value
From header field	name-addr or addr-spec	Generic Number Number Qualifier Indicator	*"Additional Calling Party number"*
from-spec	(name-addr / addr-spec)		
		Nature of Address Indicator	If +CC is equal to the CC of the country where IWU is located AND the next BICC/ISUP node is located in the same country then Set to *"national (significant) number"* Else set to *"international number"*
		Number incomplete indicator	*"Complete"*
		Numbering Plan Indicator	*"ISDN/Telephony (E.164)"*
		APRI	Depends on priv-value
		Screening indicator	*"user provided not verified"*
Addr-spec	"+CC" "NCD" "SN" from the URI	Address signal	if NOA is *"national (significant) number"* then set to "NCD" + "SN" If NOA is *"international number"* Then set to "CC"+"NCD"+"SN"
Privacy header field	priv-value	APRI	*"Address Presentation Restricted Indicator"*
Privacy header field is absent		APRI	*"presentation allowed"*
priv-value	"header	APRI	*"presentation restricted"*
	"user"	APRI	*"presentation restricted"*
	"none"	APRI	*"presentation allowed"*
	"id"	no mapping to Generic No	

6.1.~~5.7~~3.8~~-~~ User service information

See sub clause on TMR.

6.1.~~5.8~~3.9~~-~~ Application transport: BAT (BICC only)

Refer to BICC specific Annex in this Recommendation.

6.1.~~5.9~~3.10– Hop counter

For SIP-I, the I-IWU acting as an independent exchange shall perform the normal BICC/ISUP Hop Counter procedure using the Hop Counter taken from the encapsulated IAM.

For Profile A and B, the I-IWU shall perform the following interworking procedure if Hop counter procedure is supported.

At the I-IWU the Max-Forwards SIP header shall be used to derive the Hop Counter parameter if applicable. Due to the different default values (that are based on network demands/provisions) of the SIP Max-Forwards header and the Hop Counter, a factor shall be used to adapt the Max Forwards to the Hop Counter at the I-IWU. For example, the following guidelines could be applied.

~~1~~Max-Forwards for a given message should be monotone decreasing with each successive visit to a SIP entity, regardless of intervening interworking, and similarly for Hop Counter.

~~2~~The initial and successively mapped values of Max-Forwards should be large enough to accommodate the maximum number of hops that might be expected of a validly routed call.

~~Note: For the BICC/ISUP call passing through the SIP network, the Hop Counter value at the I-IWU should be lower than at the O-IWU to avoid circular routing. This must apply also when the Hop Counter/Max Forwards passes different network domains. The adaptation mechanism could be a direct mapping of the values, the use of an adaptation factor or fixed rules (e.g. multiply by 2 or increase by 20…) due to the network demands.~~

The following table shows the principle of the mapping:

Max-Forwards	= X	Hop Counter	= INTEGER part of (X /Factor)

Note:- The Mapping of value X to Y should be done with the used (implemented) adaptation mechanism.

The Principle of adoption could be implemented on a basis of the network provision, trust domain rules and bilateral agreement.

6.2 Receipt of Subsequent INVITE and handling of ~~Sending of~~ Subsequent Address Message (SAM)

The applicable procedure depends upon whether the succeeding PSTN/ISDN supports overlap signalling.~~[5]~~

6.2.1 Overlap Signalling Supported

If the I-IWU receives a subsequent INVITE with the same Call-ID and From tag as the previous one and an updated Request-URI, then a SAM message shall be generated using the interworking specified in clause 6.2.1.1. Upon sending of the SAM message, the INVITE received previously is answered with a 484 Address Incomplete.

[5] Based on input from OTW-046.

6.2.1.1 Address signal parameters

The SAM message contains only the address signals parameter. The I-IWU populates the address signals parameters by comparing the user part of the Request-URI of the INVITE just received with the cumulative digits sent so far to the ISUP/BICC network (using IAM/SAMs). Only the extra digits received in this INVITE compared with the digits sent so far to the ISUP/BICC are sent within the SAM.

6.2.2 Overlap Signalling Not Supported

Upon receipt of an INVITE, if the I-IWU can determine that the INVITE has too few digits for an IAM to be sent "en-bloc" to the PSTN/ISDN the I-IWU shall immediately generate a 484 Address Incomplete response.

~~Subsequent Address Message (SAM) may only be sent by I-IWUs which connect to PSTN which support overlap sending..~~

~~The procedures for interworking forward INVITEs from the SIP network to overlap signalling in the PSTN are as follows:~~

~~□An I-IWU does not have any means to know whether SIP overlap signalling is being used or not. So, upon reception of an INVITE, the gateway generates an IAM following the procedures described in clause 6.1.1 (and associated sub-clauses). If a gateway receives a subsequent INVITE with the same Call-ID and From tag as the previous one and an updated Request-URI, a SAM shall be generated, not a new IAM. Upon reception of a subsequent INVITE, the INVITE received previously is answered with a 484 Address Incomplete.~~

~~If the I-IWU is not connected to an area of the PSTN where overlap signalling is in use then upon receipt of subsequent INVITEs with the same Call-ID and From tag as the previous one and an updated Request-URI the I-IWU shall generate:~~

~~□A REL for the previous IAM and a new IAM should be generated, or~~

~~□a 484 Address Incomplete response, if the I-IWU can determine that the INVITE it receives has too few digits for an IAM to be sent "en-bloc" to the PSTN~~

~~In all cases, IAM messages are sent using the interworking procedures specified in clause 6.1 and the SAM messages are sent using the interworking specified in clause 6.x.x.~~

~~6.2.1 Address signal parameters~~

~~The SAM message contains only the address signals parameter. The I-IWU populates the address signals parameters by comparing the user part of the Request-URI of the INVITE just received with the cumulative digits sent so far to the ISUP/BICC network (using IAM/SAMs). Only the extra digits received in this INVITE compared with the digits sent so far to the ISUP/BICC are sent within the SAM.~~

~~6.3 Receipt of PRACK (to 183 Session Progress)~~

~~The I-IWU should evaluate the SDP content of the received PRACK (to 183 session Progress INVITE) message to determine if interworking is needed to send out any BICC/ISUP message. Coding of the PRACK message with pre-condition signalling information is specified in the following sub-clause.~~

~~If the received PRACK contains indication of a pre-condition being met, then the I-IWU should generate BICC/ISUP message, the I-IWU will generate the BICC/ISUP message in the following circumstances:~~

~~(A) If no IAM has been sent due to conditions set forth in Clause 6.1.1 Case (3-b-I), the I-IWU will send out an IAM. Refer to Clause 6.1.1 for coding of the IAM using the information from the previously received INVITE.~~

~~(B) If an IAM has already been sent under Clause 6.1.1 Case (3-b-ii), the I-IWU will send out the COT. Coding of the COT is specified in clause 6.1.7.~~

~~6.4 Sending of COT on receipt of UPDATE (with pre-condition met)~~

~~When an INVITE has previously been received by the I-IWU and contains an SDP-Offer requesting the pre-condition to be met, the I-IWU will wait for UPDATE to indicate if the pre-condition has been met. Coding of the UPDATE for pre-condition signalling is specified in the following sub-clause.~~

~~If the I-IWU receives the UPDATE message indicating a confirmation of pre-condition being met, the I-IWU will generate the BICC/ISUP message in the following circumstances:~~

~~(A) If no IAM has been sent due to conditions set forth in Clause 6.1.1 Case (3-b-I), the I-IWU will send out an IAM. Refer to Clause 6.1.1 for coding of the IAM using the information from the previously received INVITE.~~

~~(B) If an IAM has already been sent under Clause 6.1.1 Case (3-b-ii), the I-IWU will send out the COT. Coding of the COT is specified in this clause.~~

~~Bits~~	~~Indicators in Continuity Indicators parameter~~
~~A~~	~~Continuity indicator~~

~~The following codes should be set by the I-IWU in the Continuity indicators parameter field:~~

~~Bits~~	~~Codes~~	~~Meaning~~	~~Conditions~~
~~A: =~~	~~1~~	~~Continuity check successful (ISUP)/continuity (BICC)~~	~~With pre-conditions~~

~~6.5 Sending of COT on receipt of forward 200 OK (UPDATE) (with pre-condition met)~~

~~A forward 200 OK (UPDATE) response is generated in response to a backward UPDATE request sent from the I-IWU to the UAC. This forward 200 OK (UPDATE) response contains the SDP-Answer to the SDP-Offer in backward UPDATE request previously sent by the I-IWU. The SIP side of the I-IWU must handle with the 200 OK (UPDATE) with the associated SDP-Answer according to the protocol and procedures defined/referenced within Q.SIPPROFILE.~~

~~This 200 OK (UPDATE) will indicate if the pre-condition has been met. Coding of the 200 OK (UPDATE) for pre-condition signalling is specified in the following sub-clause.~~

~~If the I-IWU receives the 200 OK (UPDATE) message indicating a confirmation of pre-condition being met, the I-IWU will generate the BICC/ISUP message in the following circumstances:~~

~~(A) If no IAM has been sent due to conditions set forth in Clause 6.1.1 Case (3-b-I), the I-IWU will send out an IAM. Refer to Clause 6.1.1 for coding of the IAM using the information from the previously received INVITE.~~

~~(B) If an IAM has already been sent under Clause 6.1.1 Case (3-b-ii), the I-IWU will send out the COT. Coding of the COT is specified in Clause 6.4.~~

6.3 Sending of COT

When the I-IWU determines that all the preconditions on the incoming SIP side have been met and any continuity tests on the outgoing ISUP/BICC side have been successfully completed, the I-IWU shall send the COT message coded as follows:

1) If subsequent network is BICC network, the Continuity Indicator in the COT message shall be set to "Continuity".

2) If subsequent network is ISUP network, the Continuity Indicator in the COT message shall be set to "Continuity check successful".

6.~~6~~4 Receipt of Connect Message (CON)

If the CON is received, then the ~~200 OK (INVITE)~~200 INVITE is sent.

Table 10~~9~~/Q.1912.SIP - Method sent to SIP upon receipt of CON

←Message sent to SIP	←Message Received from ISUP/BICC
~~200 OK (INVITE)~~200 INVITE	CON

6.~~7~~5 Receipt of ACM

Table 11~~Table 10Table 10Table 10~~ provides a summary of how the ACM message is interworked to the SIP side by an I-IWU.

On receipt of the ACM, the backward SIP response sent on the incoming side of the I-IWU depends upon the value of the "Backwards Call Indicator - Called party's status indicator" parameter of the ACM.

(1) BCI (called party status indicator) = "subscriber free": If this parameter is set to "subscriber-free" then the 180 Ringing SIP response is sent from the I-IWU. Coding of ACM and 180 Ringing is specified in this clause.

(2) BCI (called party status indicator) = "no indication" or any value other than "subscriber-free": If this parameter is not set to "subscriber-free" then the 183 Session Progress response is sent from the I-IWU. (See Table 11~~Table 10Table 10Table 10~~).

Encapsulating of ACM with Called party's status indicator of "no indication" within the 183 Session Progress is applicable at the I-IWU if SIP with MIME encoding of ISUP is used.

However, ACM with called party's status indicator of no indication is not mapped to 183 Session Progress at the I-IWU if SIP with MIME encoding of ISUP is not used.

If timer T9 expires, the ISUP/BICC connection is released and ~~504 Gateway Time-out~~480 Temporary Unavailable is sent.

Editor Note: NWB051 pointed out the case of receiving ACM with cause parameter but there was no discussion on the interworking implication. This may need a separate clause under third level heading. Contribution is needed.

Table 11~~10~~/Q1912.SIP – Method sent to SIP upon receipt of ACM

←Message sent to SIP	←ACM
	Backward call indicators parameter **Called party's status indicator**
183 Session Progress	00 *No indication*
180 Ringing	01 *Subscriber free*

6.~~8~~6 Receipt of CPG

On receipt of a CPG message, either a 180 Ringing or 183 Session Progress SIP response shall be sent from the SIP side of the I-IWU. Table 13~~Table 11Table 1111Table 9~~ provides a summary of the mapping between the received CPG message and the 180 and 183 SIP responses.

Encapsulating of CPG with event indicator of progress or in-band information within the 183 Session Progress is applicable at the I-IWU if SIP with MIME encoding of ISUP is used.

However, CPG with event indicator of progress or in-band information is not mapped to the 183 Session Progress at the I-IWU if SIP with MIME encoding of ISUP is not used.

Table 13~~11~~/Q.1912.SIP - Receipt of CPG at the I-IWU

←Message sent to the SIP	←CPG
	Event information parameter **Event indicator**
180 Ringing	000 0001 (*alerting*)
183 Session Progress	000 0010 (*progress*) or 000 0011 (*in-band information or an appropriate pattern is now available*)

6.~~9~~7 Receipt of Answer Message (ANM)

On receipt of BICC/ISUP ANM, the IWU shall indicate to the SIP protocol to send a ~~200 OK (INVITE)~~200 INVITE to the UAC.

Ed. Note: The interworking of the SIP network putting the media stream inactive before ANM raises concerns that this may impact adversely upon the ISDN/PSTN services. Contributions are invited.

6.~~10~~8~~-~~ Through connection of the bearer path

Through connection of bearer path is applicable to Type 1 or Type 3 Gateways only.

6.~~10~~8.1 Through connection of the bearer path (ISUP)

Through connection at the I-IWU shall follow the Q.764 through connection procedures for the originating exchange~~ in Q.764 procedure~~.

For the SIP-I case, the I-IWU shall follow the through connection procedures in Q.764 procedure for the transit exchange.

6.~~10~~8.2 Through connection of the bearer path (BICC)

The bearer path shall be connected in both directions when both of the following conditions are satisfied:

- The BICC outgoing bearer set-up procedure, (Q.1902.4) is successfully completed, and;
- The I-IWU determines (using the procedures defined in ~~[manyfolks]~~RFC 3312) that sufficient ~~pre-condition~~preconditions have been satisfied on the SIP side for session establishment to proceed.(if applicable).

In addition, if BICC is performing the “Per-call bearer set-up in the forward direction” Outgoing bearer set-up procedure and the Connect Type is “notification not required”, the bearer path shall be connected in both directions when the Bearer Set-up request is sent (and the I-IWU determines (through the procedures defined in RFC 3312~~[manyfolks]~~ that sufficient ~~pre-condition~~preconditions have been met for the session to proceed).

6.~~11~~9 Receipt of Suspend Message (SUS) network initiated[6]

The actions taken on the ISUP/BICC side upon receipt of the suspend message (SUS) are described in ~~Section~~ Clause 2.4.1c/Q.764 and 10.2.1c/Q.1902.4.

No action is taken on the SIP side.

Note: The above ISUP/BICC actions are taken at the IWU of controlling exchange.

In the case of I-IWU that use SIP with MIME, the SUS is encapsulated in the MIME body of an INFO request.

Table 15~~12Table 15~~/Q1912.SIP - INFO sent to SIP upon receipt of SUS

←Message sent to SIP	←Message Received from ISUP/BICC
INFO	SUS

6.~~12~~10 Receipt of Resume Message (RES) network initiated[7]

The actions taken on the ISUP/BICC side upon receipt of the resume message (RES) are described in ~~Section~~ Clause 2.4.2c/Q.764 and 10.2.2c/Q.1902.4.

No action is taken on the SIP side.

Note: The above ISUP/BICC actions are taken at the IWU of controlling exchange.

~~In the case of I-IWU that use SIP with MIME~~For SIP-I, the I-IWU shall encapsulate the RES ~~is encapsulated~~ in an INFO ~~request~~method.

Table 16~~13~~/Q1912.SIP - Receipt of Resume Message (RES) network initiated~~Table 15a/Q1912.SIP~~

←Message sent to SIP	←Message Received from ISUP/BICC
INFO	RES

6.~~13~~ 11 Release Procedures at the I-IWU

6.~~13~~11.1 Receipt of BYE/CANCEL

~~Editor's note: The release procedure for BICC/ISUP is common to both I-IWU and O-IWU. And, therefore 7.1.2 may be moved to a clause applicable to both nodes.~~

On receipt of SIP BYE or CANCEL, the I-IWU shall send an ISUP REL to the ISUP side.

On receipt of SIP BYE or CANCEL, the I-IWU shall invoke the BICC Release sending procedure [Q.1902.4] on the BICC side.

Table 17~~Table 14Table 1414Table 10~~ shows the coding of the cause value in the REL.

Table 17~~14~~/Q1912.SIP – ~~Table 10 Release from SIP side~~Receipt of BYE or CANCEL

SIP Message →	**REL →**
	cause parameter
BYE	Cause value No. 16 (normal clearing)
CANCEL	Cause value No. 31 (normal unspecified)

6.~~13~~11.2 Receipt ~~of REL~~of REL

On receipt of an ISUP REL, the I-IWU immediately requests the disconnection of the internal bearer path. When the ISUP circuit is available for re-selection, an ISUP RLC is returned to the ISUP side.

On receipt of a BICC REL, the ~~ISN~~ I-IWU invokes the BICC Release reception procedures [Q.1902.4, subclause 11.6] on the BICC side.

Editor's note: The above paragraphs are applicable to Type 1 or 3 Gateways only.

~~The I-IWU shall send SIP BYE on receipt of ISUP/BICC REL with cause value No. 16 (normal clearing). On receipt of REL with other cause values, the I-IWU shall send Status-Code 4xx (Client Error), 5xx(Server Error) or 6xx (Global Failure). A list is shown in Table .~~

On receipt of REL before receiving ANM or CON, the I-IWU shall send the appropriate SIP status-code in Table 19~~Table 15Table 1515~~. See Table 19~~Table 15Table 1515~~ for the mapping from ISUP/BICC cause code to SIP status code. ISUP/BICC cause codes not appearing in Table 19~~Table 15Table 1515~~ shall have the same mapping as the appropriate Q.850 class defaults.

For SIP-I, the appropriate SIP status code of the SIP response that encapsulates the REL message should be same as the default mapping shown in Table 19~~Table 15Table 15~~ for Profile A and B.

On receipt of REL after receiving ANM or CON, the I-IWU shall send BYE.

"In the case that the REL message is received and a final response (e.g. ~~200 OK(INVITE)~~200 INVITE) has already been sent (but no ACK has been received) on the incoming side of the I-IWU then the I-IWU shall NOT send a 487 Request terminated and instead wait until the ACK is received before sending a BYE message."

~~Editors Note: The yellow highlighted cause code or SIP statuses imply?~~

Table 19~~15~~/Q.1912.SIP - Receipt of the Release message (REL)

←SIP Message	← REL
	Cause parameter
404 Not Found	Cause value No. 1 (unallocated (unassigned) number)
503 Service unavailable~~404 Not Found~~	Cause value No 2 (no route to network)
503 Service unavailable ~~404 Not Found~~	Cause value No 3 (no route to destination)
503 Service unavailable (SIP-I only)	Cause value No. 8 (Preemption)
503 Service unavailable SIP-I only)	Cause value No. 9 (Preemption-circuit reserved for reuse)
486 Busy Here	Cause value No. 17 (user busy)
480 Temporarily unavailable~~408 Request Timeout~~	Cause value No (18 no user responding)
480 Temporarily unavailable	Cause value No 19 (no answer from the user)
480 Temporarily unavailable	Cause value No. 20 (subscriber absent)
480 Temporarily unavailable~~403 Forbidden~~	Cause value No 21 call rejected
410 Gone	Cause value No 22 number changed ~~(w/o diagnostic)~~
~~302 Moved Temporarily~~No mapping	Cause value No 23 (redirection to new destination)
480 Temporarily unavailable~~483Too many hops~~	Cause value No 25 (Exchange routing error)
502 Bad Gateway	Cause value No 27 (destination out of order)
484 Address Incomplete	Cause value No. 28 invalid number format (address incomplete)
503 Service unavailable~~501 Not implemented~~	Cause value No 29 (facility rejected)
480 Temporarily unavailable	Cause value No 31 (normal unspecified) (Class default)
486 Busy here if Diagnostics indicator includes the (CCBS indicator = CCBS possible) else 480 Temporarily unavailable~~503 Service unavailable~~ ~~Editors Note (RJ): this solution has to be discussed.~~	Cause value in the Class 010 (resource unavailable, Cause value No 34)
503 Service unavailable	Cause value in the Class 010 (resource unavailable, Cause value No 38-47) (47 is class default)
503 Service unavailable	Cause value No 50 (requested facility not subscribed)
503 Service unavailable (SIP-I only)~~403 Forbidden~~	Cause value No 55 (incoming calls barred within CUG)
503 Service unavailable~~403 Forbidden~~	Cause value No 57 (bearer capability not authorized)
503 Service unavailable	Cause value No 58 (bearer capability not presently)
503 Service unavailable	Cause value No 63 (service option not available, unspecified) (Class default)
503 Service unavailable~~501 Not implemented~~	Cause value in the Class 100 (service or option not implemented Cause value No 65 - 79) (79 is class default)
503 Service unavailable (SIP-I only)	Cause value No 87 (user not member of CUG)
503 Service unavailable	Cause value No 88 (incompatible destination)
503 Service unavailable (SIP-I only)	Cause value No 90 (Non-existent CUG)
404 Not Found	Cause value No 91 (invalid transit network selection)
503 Service unavailable	Cause value No 95 (invalid message) (Class default)
503 Service unavailable	Cause value No 97 (Message type non-existent or not implemented)

←SIP Message	← REL
	Cause parameter
503 Service unavailable~~501 Not implemented~~	Cause value No 99 (information element/parameter non-existent or not implemented))
480 Temporarily unavailable~~504 Gateway timeout~~	Cause value No. 102 (recovery on timer expiry)
503 Service unavailable~~501 Not implemented~~	Cause value No 103 (Parameter non-existent or not implemented, pass on)
503 Service unavailable~~501 Not implemented~~	Cause value No 110 (Message with unrecognized Parameter, discarded)
400 Bad Request	Cause value No. 111 (protocol error, unspecified) (Class default)
480 Temporarily unavailable~~500 Server internal error~~	127 (interworking unspecified) (Class default)

6.~~13~~11.3 Autonomous Release at I-IWU

~~**Error! Reference source not found.**~~ Table 21~~Table 16Table 16~~16 shows the trigger events at the IWU and the release initiated by the IWU when the call is traversing from SIP to ISUP/BICC.

If an automatic repeat attempt initiated by the I-IWU is not successful (because the call is not routable), the I-IWU shall send a ~~503 Service~~480 Temporarily ~~Available~~ Unavailable response to the SIP side. No actions on the ISUP (BICC) side are required.

If, after answer, ISUP/BICC procedures result in autonomous REL from the IWU then a BYE shall be sent on the SIP side.

If the I-IWU receives unrecognized backward ISUP or BICC signalling information and determines that the call needs to be released based on the coding, the I-IWU shall send a ~~400 Bad Request~~503 Service unavailable response on the SIP side.

Table 21~~16~~/Q.1912.SIP - Autonomous Release at I-IWU

← SIP	Trigger event	REL →
		cause parameter
484 Address Incomplete~~ or 490 Request Updated~~ ~~(Response to be sent determined by overlap procedures - see section 7.x.x.x.)~~	Determination that insufficient digits received See 6.2.2. ~~call should be released as a result of overlap procedures.~~ Receipt of subsequent INVITE within overlap procedure, see 6.2.1.	Not sent.
~~503 Service~~480 Temporarily Unavailable	Congestion at the IWU.	Not sent.

← SIP	Trigger event	REL →
		cause parameter
BYE	ISUP/BICC procedures result in release after answer,	
~~502 Bad Gateway~~503 Service Unavailable	Call release due to the ISUP/BICC compatibility procedure (Note 1)	
NOTE 1– IWU receives unrecognized ISUP or BICC signalling information and determines that the call needs to be released based on the coding of the compatibility indicators, refer to Q.764 and Section Q.1902.4.		

6.~~13~~11.4 Receipt of RSC, GRS or CGB (ISUP)

~~Table 13~~ Table 23~~Table 17Table 17~~17 shows the message sent by the IWU upon receipt of an ISUP RSC message, GRS message or CGB message with the Circuit Group Supervision Message Type Indicator coded as “hardware failure oriented”, when at least one backward ISUP message relating to the call has already been received. The IWU sends BYE if it has already received an ACK for the INVITE. If it has sent ~~200 OK (INVITE)~~200 INVITE but has not yet received an ACK for the ~~200OK(INVITE)~~200 INVITE then the IWU shall wait until it receives the ACK for the ~~200OK(INVITE)~~200 INVITE before sending the BYE. Otherwise, it sends 503 Service Unavailable. On receipt of a GRS or CGB message, one SIP message is sent for each call association. Therefore, multiple SIP messages may be sent on receipt of a single GRS or CGB message.

In the case that ISUP encapsulation is being used the RSC, GRS or CGB ISUP messages shall not be encapsulated within the SIP BYE or 503 Service Unavailable response.

~~Editor's note: The lack of encapsulation of the RSC/GRS/CGB messages within SIP is because these messages have significance only within the local ISUP domain from which they originated hence do not make sense to transit over SIP to another ISUP domain. In the case of an ISUP-SIP-ISUP call whereby the destination ISUP end issues a RSC/GRS/CGB then a 503 or BYE will be issued to the SIP side which is subsequently converted into a REL message with appropriate cause code (see section 8).~~

Table 23~~17~~/Q.1912.SIP - Receipt of RSC, GRS or CGB messages (ISUP)~~Table13. - Receipt of RSC, GRS or CGB messages (ISUP)~~

← SIP	← Message received from ISUP
503 Service Unavailable or BYE	reset circuit message (RSC)
503 Service Unavailable or BYE	circuit group reset message (GRS)
503 Service Unavailable or BYE	circuit group blocking message (CGB) with the circuit group supervision message type indicator coded *"hardware failure oriented"*

6.~~13~~11.5 Receipt of RSC or GRS (BICC)

~~**Error! Reference source not found.**~~ Table 25~~Table 18Table 1818~~ shows the message sent by the IWU upon receipt of a BICC RSC message or GRS message, when at least one backward BICC message relating to the call has already been received. The IWU sends BYE if it has already received an ACK for the INVITE. If it has sent 200 OK but has not yet received an ACK for the ~~200OK(INVITE)~~200 INVITE then the IWU shall wait until it receives the ACK for the ~~200OK(INVITE)~~200 INVITE before sending the BYE. . Otherwise, it sends 503 Service Unavailable. On receipt of a GRS message, one SIP message is sent for each call association. Therefore, multiple SIP messages may be sent on receipt of a single GRS message.

In the case that ISUP encapsulation is being used the RSC or GRS messages shall not be encapsulated within the SIP BYE or 503 Service Unavailable response.

Table 25~~18~~/Q.1912.SIP - ~~Table14 –~~Receipt of RSC or GRS messages (BICC)

← SIP	← Message received from BICC
503 Service Unavailable or BYE	reset CIC message (RSC)
503 Service Unavailable or BYE	CIC group reset message (GRS)

7 Outgoing Call Interworking from BICC/ISUP to SIP at O-IWU

An Outgoing ~~Interface Serving~~interworking Unit (O-IWU) ~~Node~~ is used to transport calls from a BICC or ISUP network domain to a SIP network domain.

The “outgoing SIP” refers to the SIP protocol, which is used between the Outgoing ~~Interface Serving Node~~IWU and the call terminating entity (entities) in the SIP network domain. Similarly, by definition, “incoming BICC/ISUP” refers to the BICC or ISUP protocol supported between the Outgoing ~~Interface Serving Node~~IWU and the preceding BICC or ISUP entity.

The Outgoing ~~Interface Serving Node~~IWU receives forward and backward signalling information from the “incoming BICC/ISUP” and “outgoing SIP” sides, respectively. After receiving this signalling information and performing appropriate call/service processing, the Outgoing ~~Interface Serving Node~~IWU may signal to subsequent SIP nodes or preceding BICC/ISUP entities. This clause specifies the signalling interworking requirements for basic call at the outgoing ~~ISN~~IWU. The chapter is split into clauses based upon the messages sent or received on the outgoing (SIP) interface of the ~~ISN~~IWU. Only messages that are generated as a result of interworking to/from the incoming BICC/ISUP side of the ~~ISN~~ IWU are considered in this interworking. Messages that are generated as a result of a local protocol state machine are not re-described in this specification.

In the case of Type 2 or 4 Gateways as defined in TRQ.BICC/ISUP.SIP, the I-IWU shall (in addition to the procedures outlined within this clause) follow the BICC specific procedures outlined in clause A.2 of Annex A.

7.1 Sending of INVITE

The O-IWU can receive an IAM from ~~either~~ the ISUP or BICC network. After performing the normal ISUP/BICC handling for incoming IAM and ~~selecting~~ choosing to route the call to the SIP network domain, the O-IWU determines from configuration whether en-bloc addressing is to be applied on the SIP side.

1) If en-bloc addressing is to be used, the O-IWU shall determine the end of address signalling from the earlier of the following criteria a) to d) and invoke the appropriate outgoing SIP signalling procedure as described in this clause.

   End of address signalling is determined by the following criteria:

   a) by receipt of an end-of-pulsing (ST) signal; or

   b) by receipt of the maximum number of digits used in the national numbering plan; or

   c) by analysis of the called party number to indicate that a sufficient number of digits has been received to route the call to the called party; or

   d) 4-6 seconds (T_{OIW1}) after the receipt of the latest address message and the minimum number of digits required for routing the call has been received.

Note: En-bloc is preferred, and is required for Profile A.

2) If overlap addressing is to be used toward the SIP network, then the O-IWU shall:

- start timer T_{OIW3}~~,~~
- invoke the appropriate outgoing SIP signalling procedure as described in this clause, and
- process SAM as described in clause 7.2.1.

The O-IWU will invoke the outgoing SIP signalling procedure using one of the following scenarios. Which scenario is used depends upon whether preconditions are used in the SIP network:

(A) Send INVITE without ~~pre-condition~~precondition upon receipt of ISUP IAM.

(B) Send INVITE with ~~pre-condition~~precondition upon receipt of ISUP IAM.

(C) Send INVITE without ~~pre-condition~~precondition upon receipt of BICC IAM.

(D) Send INVITE with ~~pre-condition~~precondition upon receipt of BICC IAM.

Details of the procedures are described in this sub clause. Coding of the IAM received and the INVITE sent by the O-IWU are specified in the following sub clauses.

Timer (T_{OIW2}) is started when the initial INVITE is sent.

If timer (T_{OIW2}) expires, an early ACM is sent to the ISUP or BICC network. See clause 7.5.

(A) Sending INVITE without Pre-~~C~~condition for ISUP IAM

Outgoing SIP procedures apply with the following clarifications and exceptions with regards to when INVITE is to be sent.

INVITE is sent when the ISUP IAM is received, the incoming procedure decides that the call can be routed and the Continuity Check indicator in the Nature of Connection Indicators parameter in the IAM is set to indicate “continuity check not required”.

Sending of INVITE is delayed if the Continuity Check indicator in the Nature of Connection Indicators parameter in the IAM is set to indicate either “continuity check required on this circuit” or “continuity check performed on previous circuit”. INVITE shall be sent on receipt of the Continuity message with the Continuity Indicators parameter set to “continuity check successful”.

(B) Sending INVITE with Pre-~~C~~condition for ISUP IAM

INVITE with ~~pre-condition~~precondition is sent on receipt of ISUP IAM. Incoming ISUP procedures apply, with the following clarifications and exceptions as to when a confirmation of the ~~pre-condition~~precondition being met is to be sent.

The O-IWU should initiate the ~~pre-condition~~precondition signalling procedure using the SDP-Offer in the INVITE. The ~~pre-condition~~precondition signalling is concluded upon sending (within an SDP Offer-Answer exchange)~~-~~ the confirmation of a ~~pre-condition~~precondition being met. The ~~UPDATE message~~SDP Offer or Answer carrying the confirmation of a ~~pre-condition~~precondition being met is sent when both of the following conditions are satisfied.

1. If the Continuity Check indicator in the Nature of Connection Indicators parameter in the incoming IAM is set to indicate either “continuity check required on this circuit” or “continuity check performed on previous circuit”, the Continuity message with the Continuity Indicators parameter set to “continuity check successful” shall be received.
2. The requested ~~pre-condition~~preconditions are met in the SIP network.

Note: For Profile-A, the signaling of “preconditions being met” always occurs within the SDP Offer in the UPDATE message.

(C) INVITE without Pre-~~C~~condition for BICC IAM

Incoming BICC procedures apply, with the following clarifications and exceptions as to when the INVITE is to be sent.

The sending of the INVITE is delayed until all the following conditions are satisfied:

1. If the incoming IAM indicated “COT to be expected”, a Continuity message, with the Continuity Indicators parameter set to “continuity” shall be received.
2. One of the following events, which indicate successful completion of bearer set-up, shall be received by the Incoming bearer set-up procedure, (Q.1902.4 [6] subclause 7.5):

    2.1. Bearer Set-up indication – for the forward bearer set-up case where the incoming Connect Type is “notification not required”.

    2.2. APM with Action indicator set to “Connected” – for the forward bearer set-up cases (with, or without bearer control tunnelling) where the incoming Connect Type is “notification required”, and for the fast set-up(backward) case.

    2.3. Bearer Set-up Connect indication – for the backward bearer set-up case.

    2.4. BNC set-up success indication for cases using bearer control tunnelling, except as identified in item 2.2 above.

(D) INVITE with Pre-Condition for BICC IAM

INVITE with ~~pre-condition~~precondition is sent on receipt of BICC IAM. Incoming BICC procedures apply, with the following clarifications and exceptions as to when a confirmation of the ~~pre-condition~~precondition being met is to be sent.

The O-IWU should initiate the ~~pre-condition~~precondition signalling procedure using the SDP-Offer in the INVITE. The ~~pre-condition~~precondition signalling is concluded upon sending the (within an SDP Offer-Answer exchange) confirmation of a ~~pre-condition~~precondition being met. The SDP Offer or Answer~~UPDATE message~~ carrying the confirmation of a ~~pre-condition~~precondition being met is sent when both of the following conditions are satisfied.

1. If the incoming IAM indicated “COT to be expected”, a Continuity message, with the Continuity Indicators parameter set to “continuity” shall be received.
2. One of the following events, which indicate successful completion of bearer set-up, shall also be received by the Incoming bearer set-up procedure, (Q.1902.4 [6] subclause 7.5), depending on the procedure being applied:

    2.1. Bearer Set-up indication – for the forward bearer set-up case where the incoming Connect Type is “notification not required”.

    2.2. APM with Action indicator set to “Connected” – for the forward bearer set-up cases (with, or without bearer control tunnelling) where the incoming Connect Type is “notification required”, and for the fast set-up (backward) case.

    2.3. Bearer Set-up Connect indication – for the backward bearer set-up case.

    2.4. BNC set-up success indication for cases using bearer control tunnelling, except as identified in item 2.2 above.

3. The requested ~~pre-condition~~preconditions are met in the SIP network.

Note: For Profile-A, the signaling of “preconditions being met” always occurs within the SDP Offer in the UPDATE message.

For all cases of sending INVITE(A, B, C and D), Table 27~~Table 19Table 1919table 15~~ provides a summary of how the header fields within the outgoing INVITE message are populated.

Table 27~~19~~/Q.1912.SIP – Interworked Contents of the INVITE message

IAM→	INVITE→
Called Party Number	Request~~-uri ~~URI (NOTE 1)
Calling Party Number	P-Asserted-Identity (NOTE 2)
	Privacy (NOTE 2)
Hop Counter	Max-Forwards (NOTE 3)
TMR/USI	Message Body (application/SDP) (NOTE 4)
NOTE 1 – See 7.1.2 NOTE 2 – See 7.1.3 NOTE 3 – See 7.1.4 NOTE 4 – See 7.1.1	

7.1.1 Coding of SDP Media Description Lines from TMR/USI~~Transmission medium requirement (Mandatory)~~

The TMR parameter plus the optional User Service Information parameter of the IAM received by the O-IWU indicate the user-requested bearer service characteristics. Their codes should be mapped to the SDP information. The Recommendations Q.1902.3/Q.763 provide exhaustive listing of the available codes in the TMR and USI parameters. In principle, any combination of those codes can be mapped into any SDP information as long as transcoding is available.

Editor's Note: The deleted table does not provide any more information than Table 16. Clause 7.1.2 (TD 3/11-23) is merged into clause 7.1.1 and 7.1.1 should be re-named.

~~The following Table shows some of the common TMR and USI code combinations that can be mapped into SDP without the support of transcoding.~~

~~7.1.2 Coding of SDP Media Description Lines from TMR/USI~~[8]

The coding of SDP media description lines is described in this clause assuming that transcoding is not used by the IWU. Interworking relations between any SDP information and TMR/USI become irrelevant if transcoding is used.

~~Editor note: FFS is needed if TMR indicating unrestricted digital information at any rate is received.~~

~~The~~ Table 29~~Table 20Table 2021~~ ~~following table~~ provides the mapping relations from TMR/USI codes to SDP media description lines.

The O-IWU for Profile-A shall be capable of encoding the SDP for the AMR codec, which is specified in RFC 3267: "RTP payload format and file storage format for the Adaptive Multi-Rate (AMR) Adaptive Multi-Rate Wideband (AMR-WB) audio codec".

~~Editor note: Are the USI coding correct for FAX and G.722?~~

Table 29~~202021~~/Q.1912.SIP ~~Table 16~~ - Coding of SDP Media Description Lines from TMR/USI: ISUP/BICC to SIP

TMR parameter	USI parameter	USI parameter	HLC IE in ATP	m= line			b= line	a= line
TMR codes	**Information Transport Capability**	**User information layer 1 protocol indicator**	**High layer characteristics identification**	**<media>**	**<transport>**	**<fmt-list>**	**<modifier>:<bandwidth-value>**	**rtpmap:<dynamic-PT> <encoding name>/<clock rate>[/encoding parameters>**
speech	Speech	G.711 μ-law	“Ignore”	audio	RTP/AVP	0	AS:64	~~N/A~~rtpmap:0 PCMU/8000
speech	Speech	G.711 μ-law	“Ignore”	audio	RTP/AVP	Dynamic PT	AS:64	rtpmap:<dynamic-PT> PCMU/8000
speech	Speech	G.711 A-law	“Ignore”	audio	RTP/AVP	8	AS:64	rtpmap:8 PCMA/8000~~N/A~~
speech	Speech	G.711 A-law	“Ignore”	audio	RTP/AVP	Dynamic PT	AS:64	rtpmap:<dynamic-PT> ~~PCMU~~PCMA/8000
3.1 KHz audio	“USI Absent”		“Ignore”	audio	RTP/AVP	0 or 8	AS:64	rtpmap:0 PCMU/8000 or rtpmap:8 PCMA/8000
3.1 KHz audio	3.1 KHz audio	G.711 μ-law	Telephony or ”HLC absent”	audio	RTP/AVP	0	AS:64	rtpmap:0 PCMU/8000
3.1 KHz audio	3.1 KHz audio	G.711 A-law	Telephony or HLC absent”	audio	RTP/AVP	8	AS:64	rtpmap:8 PCMA/8000
3.1 KHz audio	3.1 KHz audio	~~FAX (?)~~	Facsimile Group 2/3	image	udptl	t38	AS:64	~~?~~Based on T.38.
3.1 KHz audio	3.1 KHz audio	~~FAX (?)~~	Facsimile Group 2/3	image	tcptl	t38	AS:64	Based on T.38.~~?~~
64 kbit/s unrestricted	Unrestricted digital inf. W/tone/ann.	N/A	“Ignore”	audio	RTP/AVP	9	AS:64	Rtpmap:9 G.722/8000
64 kbit/s unrestricted	Unrestricted digital information	N/A ~~(FFS)~~	“Ignore”	audio~~Data (FFS)~~	RTP/AVP~~UDP (FFS)~~	Dynamic PT~~N/A~~	AS:64	~~N/A (FFS)~~rtpmap:<dynamic-PT> CLEARMODE/8000
2 × 64 kbit/s unrestricted	Unrestricted digital information	N/A ~~(FFS)~~	“Ignore”	audio~~Data (FFS)~~	RTP/AVP~~UDP (FFS)~~	Dynamic PT~~N/A~~	AS:128	rtpmap:<dynamic-PT> CLEARMODE/8000~~N/A (FFS)~~
384 kbit/s unrestricted	Unrestricted digital information	N/A ~~(FFS)~~	“Ignore”	audio~~Data (FFS)~~	RTP/AVP~~UDP (FFS)~~	Dynamic PT~~N/A~~	AS:384	rtpmap:<dynamic-PT> CLEARMODE/8000~~N/A (FFS)~~
1536 kbit/s unrestricted	Unrestricted digital information	N/A ~~(FFS)~~	“Ignore”	audio~~Data (FFS)~~	RTP/AVP~~UDP (FFS)~~	Dynamic PT~~N/A~~	AS:1536	rtpmap:<dynamic-PT> CLEARMODE/8000~~N/A (FFS)~~
1920 kbit/s unrestricted	Unrestricted digital information	N/A ~~(FFS)~~	“Ignore”	audio~~Data (FFS)~~	RTP/AVP~~UDP (FFS)~~	Dynamic PT~~N/A~~	AS:1920	rtpmap:<dynamic-PT> CLEARMODE/8000~~N/A (FFS)~~
N × 64 kbit/s unrestricted, N from 3 to 29	Unrestricted digital information	N/A	“Ignore”	audio	RTP/AVP	Dynamic PT	AS:N × 64	rtpmap:<dynamic-PT> CLEARMODE/8000 (Note 1)

Note-1: CLEARMODE has not yet been standardized; and its usage is FFS.

~~Note:~~

~~(1) FFS is needed for <media> equal to data.~~

7.1.~~3~~2 -Request-URI

The called party number parameter of the IAM message contains the forward address information to derive the userinfo component of the INVITE Request-URI.

Note~~: ~~: The O-IWU follows existing BICC/ISUP procedure to select the outgoing route. If a new called party number is derived for the outgoing route, then the newly derived called party number should be mapped into the userinfo component of the INVITE Request URI.

For the basic call the telephone number contained in the called party number parameter is also considered as the identification of the called party. This information is mapped to the userinfo component of ~~SIP~~Request-URI and is used as the addr-spec component of the To: header field.

7.1.~~5~~3~~-~~ P-Asserted-Identity and privacy header fields

Table 31~~212122~~/Q.1912.SIP - Mapping BICC/ISUP CLI Parameters to SIP Header fields

Has a Calling Party Number parameter with complete E.164 number, with Screening Indicator = UPVP or NP (See Note 1), and with APRI = "presentation allowed" or "presentation restricted" been received?	**Has a Generic Number (additional calling party number) with a complete E.164 number, with Screening Indicator = UPNV, and with APRI = "presentation allowed" been received?**	**P-Asserted-Identity header field**	**From header field: display-name (optional) and addr-spec**	**Privacy header field**
N	N	Header field not included	Unavailable@ Hostportion	Header field not included
N (Note 2).	Y	Header field not included	display-name derived from Generic Number (ACgPN) if possible.	Header field not included
			addr-spec derived from Generic Number (ACgPN) address signals (See Table 32~~Table 22Table 22Table 23~~) or uses network provided value	
Y (See Note 1)	N	Derived from Calling Party Number parameter address signals (See Table 34~~Table 23Table 23Table 24~~)	if APRI = "allowed", display-name may be derived from Calling Party Number (~~A~~CgPN) if possible . if APRI = "restricted", display-name is "Anonymous"	If Calling Party Number parameter APRI = "restricted" then priv-value =; "id". For other APRI settings Privacy header is not included or if included, "id" is not included (See Table 37~~Table 25Table 25Table 26~~)
			if APRI = "allowed", addr-spec is derived from Calling Party Number parameter address signals (See Table 24~~Table 24Table 24Table 25~~) or uses network provided value if APRI = "restricted", addr-spec is set to the "Anonymous URI" (Note 3)	
Y	Y	Derived from Calling Party Number parameter address signals (See Table 34~~Table 23Table 23Table 24~~)	display-name may be derived from Generic Number (ACgPN) if possible	If Calling Party Number parameter APRI = "restricted" then priv-value =; "id" . For other APRI settings Privacy header is not included or if included, "id" is not included (See Table 37~~Table 25Table 25Table 26~~)

Has a Calling Party Number parameter with complete E.164 number, with Screening Indicator = UPVP or NP (See Note 1), and with APRI = “presentation allowed” or “presentation restricted” been received?	**Has a Generic Number (additional calling party number) with a complete E.164 number, with Screening Indicator = UPNV, and with APRI = “presentation allowed” been received?**	**P-Asserted-Identity header field**	**From header field: display-name (optional) and addr-spec**	**Privacy header field**
			addr-spec is derived from Generic Number (ACgPN) address signals (See Table 32~~Table 22Table 22Table 23~~) or uses network provided value	

Note-1: A Network Provided CLI in the CgPN parameter may occur on a call from an analogue access line. Therefore in order to allow the “display” of this Network Provided CLI at a SIP UAS it must be mapped into the SIP From header ~~(not discarded as shown in NWB- 030)~~. It is also considered suitable to map into the P-Asserted-Identity header since it is a fully authentic CLI related exclusively to the calling line, and therefore equally as good a User Provided Verified and Passed CLI for this purpose.

Note 2: It is not clarified if the IWU is possible to set the From Header and the Display name derived form the Generic Number Parameter. This case is FFS because it may not be possible.

Note 3: The “From” header may contain an “Anonymous URI”. An “Anonymous URI” includes information that does not point to the calling party. RFC 3261 recommends that the display-name component contains "Anonymous". RFC [privacy] recommends that the Anonymous URI itself have the value "anonymous@anonymous.invalid".

Table 32~~222223~~/Q.1912.SIP - Mapping of Generic Number (additional calling party number) to SIP From header fields

BICC/ISUP Parameter / field	**Value**	**SIP Component**	**Value**
Generic Number Number Qualifier Indicator	*"additional calling party number"*	From header field	display-name (optional) and addr-spec
Nature of Address Indicator	*"national (significant) number"*	Addr-spec	Add CC (of the country where the ISN is located) to GN address signals then map to SIP URI
	"international number"		Map complete GN address signals to SIP URI
Address signal	if NOA is *"national (significant) number"* then the format of the address signals is: NCD + SN If NOA is *"international number"* then the format of the address signals is: CC + NCD + SN	Display-name	Displayname may be mapped from Address Signal, if possible and network policy allows it.
		Addr-spec	"+CC" "NCD" "SN" mapped to user portion of URI scheme used

Table 34~~232324~~/Q.1912.SIP - Mapping of Calling Party Number parameter to SIP P-Asserted-Identity header fields

BICC/ISUP Parameter / field	**Value**	**SIP Component**	**Value**
Calling Party Number		P-Asserted-Identity header field	display-name (optional) and addr-spec
Nature of Address Indicator	*"national (significant) number"*	addr-spec	Add CC (of the country where the ~~ISN~~ IWU is located) to CgPN address signals then map to SIP URI
	"international number"		Map complete CgPN address signals to SIP URI
Address signal	If NOA is *"national (significant) number"* then the format of the address signals is: NCD + SN If NOA is *"international number"* then the format of the address signals is: CC + NCD + SN	display-name	display-name may be mapped from Address Signal, if possible and network policy allows it
		addr-spec	"+CC" "NCD" "SN" mapped to user portion of URI scheme used

Table 24~~242425~~/Q.1912.SIP - Mapping of BICC/ISUP Calling Party Number parameter to SIP From header fields

BICC/ISUP Parameter / field	**Value**	**SIP Component**	**Value**
Calling Party Number		From header field	display-name (optional) and addr-spec
Nature of Address Indicator	*"national (significant) number"*	addr-spec	Add CC (of the country where the ~~ISN~~ IWU is located) to CgPN address signals then map to SIP URI
	"international number"		Map complete CgPN address signals to SIP URI
Address signal	If NOA is "*national (significant) number"* then the format of the address signals is: NCD + SN If NOA is *"international number"* then the format of the address signals is: CC + NCD + SN	display-name	Display-name may be mapped from Address Signal, if possible and network policy allows it. ~~;user=phone"~~
		addr-spec	"+CC" "NCD" "SN" mapped to user portion of URI scheme used

Table 37~~252526~~/Q.1912.SIP - Mapping of BICC/ISUP APRIs into SIP Privacy header fields

BICC/ISUP Parameter / field	**Value**	**SIP Component**	**Value**
Calling Party Number or Generic Number (additional calling party number)		Privacy header field	priv-value
APRI (See Table 31~~Table 21Table 21Table 22~~ to determine which APRI to use for this mapping)	*"presentation restricted"*	Priv-value	"id" ("id" included only if the P-Asserted-Identity header is included in the SIP INVITE)
	"presentation allowed"	Priv-value	omit Privacy header or Privacy header without "id" if other privacy service is needed~~)~~

Note: When Calling Party Number parameter exists, P-Asserted-Identity header is always derived from it as in Table 31~~Table 21Table 21Table 22~~.

7.1.~~6~~4 Max Forwards header

For SIP-I, the O-IWU acting as independent exchange shall perform the normal BICC/ISUP Hop Counter procedure if the Hop Counter parameter is available.

For Profile A and B, the I-IWU shall perform the following interworking procedure in this clause if Hop Counter procedure is supported.

At the O-IWU the Hop Counter parameter ~~-~~shall be used to derive the Max-Forwards SIP header. Due to the different default values (that are based on network demands/provisions) of the SIP Max-Forwards header and the Hop Counter, an adaptation mechanism shall be used to adopt the Hop Counter to the Max Forwards at the O-IWU. For example, the following guidelines could be applied.

~~3~~a) Max-Forwards for a given message should be monotone decreasing with each successive visit to a SIP entity, regardless of intervening interworking, and similarly for Hop Counter.

~~4~~b) The initial and successively mapped values of Max-Forwards should be large enough to accommodate the maximum number of hops that might be expected of a validly routed call.

~~Note: For the BICC/ISUP call passing through the SIP network, the Hop Counter value at the I-IWU should be lower than at the O-IWU to avoid circular routing. This must apply also when the Hop Counter/Max Forwards passes different network domains. The adaptation mechanism could be a direct mapping of the values, the use of an adaptation factor or fixed rules (e.g. multiply by 2 or increase by 20…) due to the network demands.~~

~~O-IWU~~The following table shows the principle of the mapping:

Hop Counter	= Y	Max-Forwards	= X

Note:~~-~~ The Mapping of value X to Y should be done with the used (implemented) adaptation mechanism.

The Principle of adaptation could be implemented on a basis of the network provision, trust domain rules and bilateral agreement

7.1.5 Coding of Encapsulated ISUP IAM Parameters in Outgoing INVITE for SIP-I

This clause is used to specify coding of certain encapsulated BICC/ISUP information based on appropriate BICC/ISUP procedures. For computation of certain parameter/indicator values, the IWU is assumed to be an ISDN/PSTN exchange.

7.1.5.1 Nature of connection parameter

The O-IWU shall increment the satellite indicator by 1 in the nature of connection parameter if the selected outgoing connection is using SIP-I.

7.1.5.2 Propagation Delay Counter parameter

The O-IWU should increase the Propagation Delay Counter by an appropriate value based on available network configuration data that represents the delay of the IP net.

7.2 ~~Sending of Subsequent INVITE (?) on r~~Receipt of SAM

If en bloc addressing is used toward the SIP network, subsequent SAM messages received after the O-IWU has sent the INVITE are ignored.

7.2.1 Overlap procedures upon receipt of SAM

If timer T_{OIW3} is running, the O-IWU shall:

1) Restart timers T_{OIW2} and T_{OIW3} upon receipt of a SAM.

2) Invoke the appropriate outgoing signalling procedure A), B), C), or D) as described in clause 7.1, with the following additional procedures:

- The Request-URI and the To header field of the new INVITE shall contain all digits received so far for this call.
- If the initial INVITE has not yet been sent, as is possible in cases A) and C), then in the SIP-I case the IAM message encapsulated within the initial INVITE shall incorporate all digits received so far for this call into the Called Party Number.
- If the initial INVITE has already been sent, then:

  a) A new INVITE with the same call-ID and From header (including tag) as the previous INVITE is sent. In the SIP-I case, the SAM is encapsulated in the new INVITE.

  b) The new INVITE shall contain a new SDP offer. The O-IWU may re-use any resources that have already been reserved for this call. This re-use of existing reserved resources shall be reflected within the precondition attributes for the SDP parameters in question.

  c) The remaining contents of the new INVITE are interworked from the parameters of the original IAM as per clause 7.1 of this Recommendation.

If timer T_{OIW3} has expired, subsequent SAM messages received after the O-IWU has sent the INVITE are ignored.

~~FFS.~~

Editor Note: Clause 7.3 (Sending UPDATE) of TD 3/11-23 is deleted based on decision on D378 and D389.

~~7.3 Receipt of COT message / Sending of UPDATE message with "confirmation" preconditions met~~

~~Editor's note: This section is expected to explain how and when receipt of a COT and the O-IWU determining that all preconditions for which the ASN has requested confirmation is met results in the sending of an UPDATE message on the SIP side.~~

~~7.4 Receipt of 1xx Response~~

Ed. Note: This Clause at level-2 heading can simply be used to deal with the receipt of 18X response. Any other non-18X provisional responses requiring interworking in the future could be added as separate level-2 clauses.

7.~~4~~3~~.1~~ Receipt of ~~18x~~ 18X response

The following table (Table 27~~Table 26Table 2627Table 19~~) provides a summary of the interworking of ~~18x~~ 18X messages to ISUP messages. For further details please see the reference sub-clause given in each table row.

Table 27~~262627~~/Q.1912.SIP - ~~Table 19:~~ Receipt of ~~18x~~ 18X Response

←ISUP message	←~~18x~~ 18X response
ACM or CPG (Note 1)	180 Ringing
ACM or CPG (Note 2)	183 Session Progress
NOTE 1 – See 7.~~4~~3.1~~.1~~ NOTE 2 – See 7.~~4~~3.~~1.~~2	

~~Upon receipt of the 180 Ringing response, the O-IWU should send backward (map it to) the ACM with called party's status of "subscriber free" or CPG with event indicator of "alerting". The ISUP/BICC procedure at the O-IWU should determine whether ACM or CPG is to be sent backward. This is applicable to O-IWU in Profile A, B and C. In the case of Profile C, the encapsulated ACM or CPG will be evaluated by ongoing ISUP/BICC procedure to send back appropriate message. See sub-clause for details.~~

Note: Local ISUP/BICC procedures may provide for generation of a backward early ACM (no indication) based upon timer expiry. These procedures operate independently of SIP interworking.

~~If 183 Session Progress response is received without any encapsulated ISUP/BICC message, no ISUP/BICC is sent backward and ISUP/BICC procedures should continue.~~

~~If 183 Session Progress response is received with encapsulated ISUP/BICC message, the encapsulated ACM or CPG will be evaluated by ongoing ISUP/BICC procedure to send back the appropriate message. See sub-clause for details.~~

~~Ed. Note: The following sub-clauses may need further revision if the above principle can be stabilized first.~~

~~Note: The above procedures (and related sub-clauses) describe what message should be sent when a SIP 18x response is received on the SIP side of the O-IWU with no encapsulated ISUP. In the case that ISUP encapsulation is in use in the SIP network then the General Principles of ISUP encapsulation apply regarding what message shall be sent on the BICC/ISUP side and the setting of parameters within that message.~~

7.43.1~~.1~~ Receipt of 180 Ringing

If a 180 Ringing is received without any encapsulated BICC/ISUP message, the IWU shall send either the ACM or CPG message as determined by BICC/ISUP procedures related to whether or not an ACM has previously been sent for this call. If the ACM is to be sent the Called Party’s Status indicator in the Backward Call Indicators parameter is coded as “subscriber free”. If the CPG is to be sent the event indicator shall be set to "alerting".

7.43.1.1~~.1~~ Setting for ACM Backwards Call Indicators

The table within this sub-clause presents the default values of Backward Call Indicator parameters that are set by the O-IWU when ACM is sent~~ as a result of clause 7.4.1.1~~. Other Backwards Call Indicator parameters are set according to ISUP/BICC procedures.

The indicators of the BCI parameters, which are set by the IWU, are as follows:

Bits	Indicators in BCI parameter
DC	Called Party's status indicator
I	Interworking indicator
K	ISDN User part/BICC indicator
M	ISDN access indicator

For all profiles, Called Party's status indicator (Bit DC) is set to "subscriber free".

For Profile A, these are the default settings.

Parameter	Bits	Codes	Meaning
Interworking Indicator	I	1	interworking encountered
ISDN User part/BICC indicator	K	0	ISDN user part/BICC not used all the way
ISDN access indicator	M	0	terminating access non-ISDN

For Profile-B and C, the O-IWU shall set the appropriate values of other BCI indicators (other than Called Party's status indicator) based on analysis of various information such as signalling, internal states and/or local policies.

Ed. Note: Aligned with section 6.1.5.4 based on the decision taken in Ottawa with respect to FCI.

7.~~4~~3.1.~~1.1~~2 Settings for CPG

The table within this sub-clause presents the default values of the Event Information parameter that are set by the O-IWU when CPG is sent. Other Event Information parameters are set according to ISUP/BICC procedures. ~~Event Information parameter~~

Bits	Indicators in Event Information parameter
G F E D C B A	Event indicator

The following codes ~~should~~ shall be set by the O-~~IWF~~ IWU in the Event ~~information~~ Information parameter field on receipt of 180 Ringing:

Bits	Codes	Meaning
G F E D C B A: =	0 0 0 0 0 0 1	Alerting

~~Ed. Note: The following text doesn't seem to belong to this clause. A table describing the CPG parameters is needed.~~

~~The interworking procedure of the O-IWU is dependent on the following scenario:~~

~~(A) SIP Profile-A: Pre-conditions are being used on the SIP network.~~

~~If an ACM has not been sent and a 180 Ringing is received without any encapsulated BICC/ISUP message, the IWU shall send the ACM with Called Party's Status indicator in the Backward Call Indicators parameter coded as "subscriber free".~~

~~Coding of ACM to be sent by the O-IWU is specified in this clause.~~

~~Coding of CPG to be sent by the O-IWU is specified in clause 7.1.12.~~

~~(B) SIP Profile-B: Pre-conditions are not used on the SIP network.~~

~~Interworking procedure is same as Profile-A.~~

~~Note: Interworking with 180 Ringing is independent from the use of pre-condition signalling.~~

~~(C) SIP Profile-C: BICC/ISUP messages are encapsulated in SIP.~~

~~If an ACM has not been sent and a 180 Ringing is received with an encapsulated ACM, the IWU shall send the encapsulated ACM.~~

~~Coding of ACM to be sent by the O-IWU specified in this clause does not apply.~~

7.~~4~~3.~~1.~~2 Receipt of 183 Session Progress

If 183 Session Progress is received without any encapsulated ISUP/BICC message, no ISUP/BICC message is sent backward and ISUP/BICC procedures should continue.

For SIP-I, if 183 Session Progress is received with encapsulated ISUP/BICC message, the O-IWU shall determine the appropriate backward BICC/ISUP message based on the encapsulated ISUP message and existing BICC/ISUP signaling state.

~~Ed. Note: Any mapping from 183 Session Progress response may be limited to case of Profile C. In that case, the encapsulated ISUP/BICC message cannot be ignored. And it should be dependent on ongoing ISUP/BICC signaling state at the O-IWU with the encapsulated ISUP/BICC information as additional input. Contributions are invited.~~

~~7.4.1.2.1 Default settings for ACM Backwards Call Indicators parameters~~

~~The table within this sub-clause presents the default values of Backward Call Indicator parameters that are set by the O-IWU when ACM is sent as a result of clause 7.4.1.2. Other Backwards Call Indicator parameters are set according to ISUP/BICC procedures.~~

~~7.4.1.2.2 Default settings for CPG Backwards Call Indicators parameters~~

~~Note: Interworking with 183 Session Progress is dependent on the use of pre-condition signalling.~~

~~The interworking procedure of the O-IWU is dependent on the following scenario:~~

~~(A) SIP Profile-A: Pre-conditions are being used on the SIP network.~~

~~An ACM message shall not be generated on receipt of the **first** 183 Session Progress response for this call.~~

~~Subsequently 183 Session Progress messages are mapped to either an ACM or a CPG message as determined by the call state (?) and the relevant BICC/ISUP procedures. If an ACM has not been sent and a 183 Session Progress is received without any encapsulated BICC/ISUP message, the IWU shall send the ACM with Called Party's Status indicator in the Backward Call Indicators parameter coded as "no indication"~~

~~Coding of ACM to be sent by the O-IWU is specified in this clause.~~

~~Coding of CPG to be sent by the O-IWU is specified in clause 7.1.13.~~

~~(B) SIP Profile-B: Pre-conditions are not used on the SIP network.~~

~~If an ACM has not been sent and a 183 Session Progress is received without any encapsulated BICC/ISUP message, the IWU shall send the ACM according to the call state (?) and the relevant BICC/ISUP procedures.~~

~~Coding of ACM or CPG to be sent by the O-IWU specified in this clause does not apply?~~

~~(C) SIP Profile-C: BICC/ISUP messages are encapsulated in SIP.~~

~~If an ACM has not been sent and a 183 Session Progress is received with an encapsulated ACM, the IWU shall send the encapsulated ACM.~~

~~Coding of ACM to be sent by the O-IWU specified in this clause does not apply.~~

~~7.4.2 Sending of CPG on receipt of 180 Session Progress~~

~~The interworking procedure of the O-IWU is dependent on the following scenario:~~

~~(A) SIP Profile-A: Pre-conditions are being used on the SIP network.~~

~~If an ACM has been sent and a 180 Ringing without any encapsulated ISUP message is received, then the O-IWU shall send backward a CPG with event indicator (of event information parameter) indicating alerting.~~

~~Coding of CPG is specified in this clause.~~

~~(B) SIP Profile-B: Pre-conditions are not used on the SIP network.~~

~~Interworking procedure is same as Profile-A.~~

~~Note: Interworking with 180 Ringing is independent from the use of pre-condition signalling.~~

~~(C) SIP Profile-C: BICC/ISUP messages are encapsulated in SIP.~~

~~If an ACM has been sent and a 180 Ringing is received with an encapsulated CPG, the IWU shall send the encapsulated CPG.~~

~~Coding of CPG to be sent by the O-IWU specified in this clause does not apply.~~

~~7.4.3 Sending of CPG on receipt of 183 Session Progress~~

~~The interworking procedure of the O-IWU is dependent on the following scenario:~~

~~(A) SIP Profile-A: Pre-conditions are being used on the SIP network.~~

~~If an ACM has been sent and a 183 Session Progress without any encapsulated ISUP message is received, then the O-IWU shall send backward a CPG with event indicator (of event information parameter) indicating progress.~~

~~Coding of CPG to be sent by the O-IWU is specified in this clause.~~

~~(B) SIP Profile-B: Pre-conditions are not used on the SIP network.~~

~~If an ACM has not been sent and a 183 Session Progress is received without any encapsulated BICC/ISUP message, the IWU shall send the CPG according to the call state (?) and the relevant BICC/ISUP procedures.~~

~~Coding of CPG to be sent by the O-IWU specified in this clause does not apply?~~

~~(C) SIP Profile C: BICC/ISUP messages are encapsulated in SIP.~~

~~If an ACM has not been sent and a 183 Session Progress is received with an encapsulated CPG, the IWU shall send the encapsulated CPG.~~

~~Coding of CPG to be sent by the O-IWU specified in this clause does not apply.~~

7.4 Expiry of Timer T_{OIW2} and Sending of Early ACM

When timer T_{OIW2} expires, the O-IWU shall return ACM.

For Profile A and B, the O-IWU shall return awaiting answer indication (e.g., ringing tone) to the calling party.

The Called Party's status indicator (Bit DC) of BCI parameter is set to "no indication". The other BCI indicators shall be set as described in clause 7.3.1.1.

7.~~5~~5~~-~~ Receipt of ~~200 OK (INVITE)~~200 INVITE

~~The following conditions must be satisfied before the ANM or CON message is sent from the O-IWU.~~ When the O-IWU receives a 200 INVITE for this call, it shall:

- Send ~~Which ISUP/BICC message (~~ANM or CON~~) is to be sent when these conditions are satisfied, is~~ as determined by ISUP/BICC procedures.

~~200 OK(INVITE) for this call must be received by the O-IWU.~~

- Stop any existing “awaiting answer indication” (e.g. ringing tone).

7.~~5~~5.1 Setting of Backwards Call Indicators

Editor note: Contributions are invited on generating parameters for ANM or CON.

7.~~6~~6 Through connection of BICC/ISUP bearer path

Through connection of bearer path is applicable to Type 1 or Type 3 Gateway only.

For Profile A and B, through connection at the O-IWU shall follow the Q.764 procedures for the destination exchange if this functionality is not available at the related SIP entity.

For SIP-I, the following procedures shall apply.

Through connection of the bearer path shall be completed dependent upon whether or not ~~pre-condition~~preconditions are in use on the SIP side of the call.

The bearer path shall be connected in both directions on completion of the bearer setup on the SIP side. This event is indicated by the receipt of SDP~~-answer~~ Answer acceptable to the O-IWU; and an indication that all mandatory ~~pre-condition~~preconditions (if any) have been met.

The bearer path shall be connected in the forward direction no later than on receipt of ~~200 OK (INVITE)~~200 INVITE.

Editor note: Contributions are invited to clarify the case without preconditions.

~~Editor's note: This text is accepted for the SIP-T case. Contributions invited are invited to address possible fraud in backwards path for a call from ISUP to SIP.~~

7.~~6~~6.1 Tone and announcement (backward)

For Profile A and B, ~~The~~ the following conditions result in ringing tone being played from the O-IWU:

1) 180 Ringing received AND

2) ISUP procedures indicate that ringing tone can be applied.

Note: ~~SDP indicates that media is on hold (i.e. the media attribute for the media stream that is being inter-worked to the ISDN/PSTN is set to a=inactive or a=recvonly (from the point of view of the SIP endpoint)).~~

It is possible that ringing tone is already being played as a result of T_{OIW2} expiry. See clause 7.4.

Editor's note: Is ringing tone the only tone to be signalled in backward direction? Are there any other signalling conditions required for other tone and announcement?

7.~~7~~7~~-~~ Release Procedures at the O-IWU

7.~~7~~7.1 Receipt of Forward REL during user-initiated SUS/RES

7.~~7~~7.2 Receipt of Forward REL

Upon receipt of a BICC or ISUP REL:

(1) REL message received at O-IWU before ~~200 OK (INVITE)~~200 INVITE received on SIP side.

On receipt of the REL message the "outgoing SIP" side of the O-IWU must:

- Send a CANCEL request to the ASN. SIP procedures at the ASN indicate how this request is dealt with. SIP procedures also apply to any subsequent protocol action on the SIP side as a result of any responses from the ASN and any "glare" ~~conditions which~~conditions, which may occur.

(2) REL message received at O-IWU after ~~200 OK(INVITE)~~200 INVITE received and ACK sent on SIP side

On receipt of the REL message the "outgoing SIP" side of the O-IWU must:

- Send a BYE request to the ASN. SIP procedures at the ASN indicate how this request is dealt with ~~(~~normally by sending a 200 OK (BYE)~~)~~.

In the case that the state of the SIP side of the call does not fall into the circumstances described within (1) or (2), the following procedures must be followed instead:

- If the REL message is received after the ~~200 OK(INVITE)~~200 INVITE but before the outgoing side of the O-IWU has sent the ACK, then the O-IWU shall send the ACK before sending a BYE.
- If CANCEL request has been sent before the ~~200 OK (INVITE)~~200 INVITE has been received and the CANCEL and ~~200 OK (INVITE)~~200 INVITE "cross on the wire", then the O-IWU shall send an ACK for the ~~200 OK (INVITE)~~200 INVITE and subsequently send a BYE request after the ACK has been sent.

Editor's note: This note refers to the second bullet dealing with 200 INVITE and CANCEL “cross on the wire’. The CANCEL Request will be answered with a 481 (Call Leg/Transaction Does Not Exist), but nevertheless the connection on the SIP side is still established and has to be released. Therefore the ACK and BYE shall be sent. The text and the above clarification seem to belong the realm of SIP procedure; and is not clear on the interworking procedure. If this has not been explicitly specified in SIP and CANCEL is triggered autonomously, then it should be captured somewhere else. If this CANCEL is triggered by receipt of forward REL before 200 INVITE, then this bullet item should be moved to item (1). What is the group’s opinion?

7.~~7~~7.3 Receipt of Backward BYE

~~Editor’s note: The release procedure for BICC/ISUP is common to both I-IWU and O-IWU. And, therefore 7.1.24.4 may be moved to a clause applicable to both nodes.~~

~~Editor's note: This section used to be titled interworking with BYE/CANCEL, however for an O-IWU (outgoing SIP) it does not make sense to send a CANCEL from the ASN to the O-IWU since the O-IWU in this case is the UAC and this effectively means the UAS (ASN) is asking the UAC to cancel a request (Yet the request is being processed at the UAS). To "cancel" a session prior to 200 OK being sent , the ASN would need to send a 487 Request terminated to the O-IWU (i.e. it would not send a CANCEL). The action to take on receipt of a 487 at the O-IWU is described in a later section on 4xx/5xx/6xx responses.~~

~~(The only time that receiving a CANCEL at the O-IWU would make sense is if you wanted to CANCEL a re-INVITE sent from the ASN - this scenario does not fit in with the ISUP-SIP interworking).~~

On receipt of SIP BYE, the O-IWU shall send an ISUP REL to the ISUP side.

On receipt of SIP BYE, the O-IWU shall invoke the BICC Release sending procedure [Q.1902.4] on the BICC side.

Table 29~~Table 27Table 27~~28~~Table 20~~ shows the coding of the cause value in the REL.

Table 29~~2727~~28/Q.1912.SIP ~~Table 20~~ - Release from SIP side at O-IWU

←REL	←SIP Message
cause parameter	
Cause value No. 16 (normal clearing)	BYE

7.~~7~~7.4 Autonomous Release at O-IWU

Table 31~~Table 28Table 28~~29 ~~Table 21~~shows the trigger events at the IWU and the release initiated by the IWU when the call is traversing from ISUP/BICC to SIP.

If, after answer, ISUP/BICC procedures result in autonomous REL from the IWU then a BYE shall be sent on the SIP side.

Table 31~~2828~~29/Q.1912.SIP - Autonomous Release at O-IWU

REL ←	Trigger event	→ SIP
cause parameter		
As determined by ISUP/BICC procedure.	ISUP/BICC procedures result in generation of autonomous REL on ISUP/BICC side.	CANCEL or BYE

7.~~7~~7.5. Receipt of RSC, GRS or CGB (ISUP)

Table 33~~Table 29Table 29~~30~~Table 22~~ shows the message sent by the IWU upon receipt of an ISUP RSC message, GRS message or CGB message with the Circuit Group Supervision Message Type Indicator coded as "hardware failure oriented". The IWU sends BYE if it has already received an ACK for the INVITE. If it has received ~~200 OK (INVITE)~~200 INVITE but has not yet sent an ACK for the INVITE then the IWU shall first send the ACK before sending the BYE. Otherwise, it sends CANCEL. On receipt of a GRS or CGB message, one SIP message is sent for each call association. Therefore, multiple SIP messages may be sent on receipt of a single GRS or CGB message.

In the case that ISUP encapsulation is being used the RSC, GRS or CGB ISUP messages shall not be encapsulated within the SIP BYE or CANCEL.

~~Editor's note: The lack of encapsulation of the RSC/GRS/CGB messages within SIP is because these messages have significance only within the local ISUP domain from which they originated hence do not make sense to transit over SIP to another ISUP domain. In the case of an ISUP-SIP-ISUP call whereby the destination ISUP end issues a RSC/GRS/CGB then a CANCEL or BYE will be issued to the SIP side which is subsequently converted into a REL message with appropriate cause code (see section 7).~~

Table 33~~292930~~/Q.1912.SIP - Receipt of RSC, GRS or CGB messages (ISUP) at O-IWU

Message received from ISUP →	SIP →
reset circuit message (RSC)	CANCEL or BYE
circuit group reset message (GRS)	CANCEL or BYE
circuit group blocking message (CGB) with the circuit group supervision message type indicator coded *"hardware failure oriented"*	CANCEL or BYE

7.~~7~~7.6 Receipt of RSC or GRS (BICC)

~~**Error! Reference source not found.**~~Table 35~~Table 30Table 3031~~ shows the message sent by the IWU upon receipt of a BICC RSC message or GRS message.The IWU sends BYE if it has already received an ACK for the INVITE. If it has received 200 OK but has not yet sent an ACK for the INVITE then the IWU shall first send the ACK for the INVITE before sending the BYE. . Otherwise, it sends CANCEL. On receipt of a GRS message, one SIP message is sent for each call association. Therefore, multiple SIP messages may be sent on receipt of a single GRS message.

In the case that ISUP encapsulation is being used the RSC or GRS messages shall not be encapsulated within the SIP BYE or CANCEL response.

~~Table23. - Receipt of RSC or GRS messages (BICC)~~Table 35~~303031~~/Q.1912.SIP - Receipt of RSC or GRS (BICC) at O-IWU

Message received from BICC →	SIP →
reset CIC message (RSC)	CANCEL or BYE
CIC group reset message (GRS)	CANCEL or BYE

7.~~7~~7.7 Receipt of 4XX, 5XX, 6XX

~~Editor's note: The following mappings have been taken from draft-ietf-sipping-isup-01.txt.~~

~~The 487 Request terminated value has been added in here since it is needed and appears to be missing from draft-ietf-sipping-isup-01.txt. (Is the mapping used here ok?)~~

The behaviour of the O-IWU on receipt of a ~~4xx~~ 4XX~~/~~, ~~5xx~~ 5XX or ~~6xx~~ 6XX final response to the INVITE on the SIP side is described within Table 37~~Table 31Table 3132table 24~~. If no further reference is given in the "Remarks" column then this means that the SIP response is interworked to an ISUP REL message sent on the incoming ISUP side of the O-IWU with the cause code indicated within the table. In cases where further reference is indicated the behaviour of the O-IWU is described within the referred to section, however the table indicates the "eventual" behaviour of the O-IWU in the case that further measures taken on the SIP side of the call (to try and sustain the call) fail resulting in the ISUP half call being released by sending a REL with the cause code indicated.

Table 37~~3131~~32/Q.1912.SIP - Receipt of 4XX, 5XX or 6XX at O-IWU~~Table 24 4xx/5xx/6xx Received on SIP side of O-IWU~~

←REL (cause code)	~~← 4xx/5xx/6xx~~4XX/5XX/6XX SIP Message	Remarks
127 Interworking~~41 Temporary Failure~~	400 Bad Request	
127 Interworking~~21 Call rejected~~	401 Unauthorised	(i)
127 Interworking~~21 Call rejected~~	402 Payment Required	
127 Interworking~~21 Call rejected~~	403 Forbidden	
1 Unallocated number	404 Not Found	
127 Interworking~~63 Service or option unavailable~~	405 Method Not Allowed	
127 Interworking~~79 Service/Option not implemented~~	406 Not Acceptable	
127 Interworking~~21 Call Rejected~~	407 Proxy authentication required	(i)
127 Interworking~~102 Recovery on timer expiry~~	408 Request Timeout	
22 Number changed (without diagnostic)	410 Gone	
127 Interworking	413 Request Entity too long	(ii)
127 Interworking	414 Request-uri too long	(ii)
127 Interworking~~79 Service/option not implemented~~	415 Unsupported Media type	(ii)
127 Interworking	416 Unsupported URI scheme	(ii)
127 Interworking	420 Bad Extension	(ii)

←REL (cause code)	~~← 4xx/5xx/6xx~~4XX/5XX/6XX SIP Message	Remarks
127 Interworking	421 Extension required	(ii)
127 Interworking	423 Interval Too Brief	
18 No user responding	480 Temporarily Unavailable	
127 Interworking~~41 Temporary Failure~~	481 Call/Transaction does not exist	
127 Interworking	482 Loop Detected	
127 Interworking~~25 Exchange routing error~~	483 Too many hops	
28 Invalid Number format	484 Address Incomplete	~~(v)~~
127 Interworking~~1 Unallocated number~~	485 ~~Ambigous~~Ambiguous	
17 User busy	486 Busy Here	
~~31 Normal unspecified~~No mapping.	487 Request terminated	
127 Interworking~~31 Normal unspecified~~	488 Not acceptable here	~~(iii)~~
~~28 Invalid number format.~~	~~490 Request Updated~~	~~(v)~~
No mapping.	490 Request Updated	
No mapping.	491 Request Pending	
127 Interworking	493 Undecipherable	
127 Interworking~~41 Temporary failure~~	500 Server Internal error	
127 Interworking~~38 Network out of order~~	501 Not implemented	
127 Interworking~~38 Network out of order~~	502 Bad Gateway	
127 Interworking~~41 Temporary failure~~	503 Service Unavailable	
127 Interworking~~102 Recovery on timer expiry~~	504 Server timeout	
127 Interworking	505 Version not supported	(ii)
127 Interworking	513 Message too large	(ii)
127 Interworking~~?~~	580 Precondition failure	(~~iv~~iii)
17 User busy	600 Busy Everywhere	
21 Call rejected	603 Decline	
1 Unallocated number	604 Does not exist anywhere	
127 Interworking~~31 Normal unspecified~~	606 Not acceptable	~~(iii)~~

Editor Note: Contributions are invited to revise the following remarks.

~~Editor's note: The above table needs to be re-visited. Agreed on the principle that any SIP condition not related to service maps "interworking" unless there is an obvious alternative. Contributions invited.~~

Remarks in Table 37~~Table 31Table 3132~~:

(i)~~-~~ Provision of authorization from O-IWU to ASN.

If the SIP entity is unable to carry through authorisation.

(ii)~~-~~ Session Re-origination as a preference to Release.

The O-IWU should react ~~to~~ to this result by attempting to re-originate the session. If protocol error response codes are still received after this then the O-IWU shall send a REL message on the BICC/ISUP side with the cause code appropriate to the SIP response received~~ (as indicated in the table xx)~~.

~~(iii) Use of "Warning" headers received with SIP responses.~~

~~These SIP responses are accompanied by "warning headers" raising the prospect that the warning header itself may provide additional information as to what REL message cause code the SIP message should be inter worked to. Presently, given the current set of defined warning headers, assigning the cause code as "31, normal unspecified" shall suffice.~~

(~~iv~~iii) Special handling of 580 ~~Pre-condition~~Precondition failure response to an INVITE message.

Receipt of the 580 ~~Pre-condition~~Precondition failure response only causes the REL message to be issued on the ISUP side of the O-IWU in the case whereby the 580 is in direct response to an INVITE message. In all other cases receipt of a 580 ~~Pre-condition~~Precondition failure response by the O-IWU does NOT result in a REL message being sent on the ISUP side.

~~Editor's note: The above sections (7.1.24.1, 7.1.24.2, 7.1.24.3, 7.1.24.4) are NOT ACCEPTED in this meeting. Contributions however are invited. If the text is accepted in a future meeting then the text needs to be re-formatted as notes to the table instead of separate sections referenced out of the table.~~

~~Editor's note: 8.2.X.4 arises because the 580 can be sent in response to an UPDATE message in order to refuse an offer which contains pre-conditions which the ASN is un-willing or unable to fulfill. Thus the O-IWU can re-attempt with a new offer later in the session (i.e. the session is not terminated). This is not the case when the 580 is in direct response to an offer contained within an INVITE message since the 580 is a final response to the INVITE and hence terminates both the offer and the session.~~

7.8 Timers at O-IWU

Table 39~~323233~~/Q.1912.SIP - Interworking Timers

Symbol	**Time-out value**	**Cause for initiation**	**Normal termination**	**At expiry**	**Reference**
T_{OIW1}	4-6 seconds (default of 4 seconds)	When latest digit is received after the minimum number of digits required for routing the call has been received.	At the receipt of fresh address information.	Send the initial INVITE, Return an ACM and send the awaiting answer indication (e.g. ring tone) to the calling party.	7.1
T_{OIW2}	4-6 seconds (default of 4 seconds)	When latest digit is received after the minimum number of digits required for routing the call has been received.	On reception of 180 Ringing or 200 INVITE	Send early ACM and send the awaiting answer indication (e.g. ring tone) to the calling party.	7.1, 7.2, 7.5.
T_{OIW3}	4-6 seconds (default of 4 seconds)	When latest digit is received after the minimum number of digits required for routing the call has been received.	At the receipt of fresh address information.	Send the initial or subsequent INVITE. Return an ACM and send the awaiting answer indication (e.g. ring tone) to the calling party.	7.1, 7.2

ANNEX-A

ANNEX-A. BICC Specific Interworking for Basic Call

Editor Note: The following text for Annex-A is taken from NWB061. Some key technical issues (e.g., does it require any capability beyond BICC CS2?) still remain that may result in major change to this text. Instead of integrating some of the proposed text into the COMMON PART, they are left in this annex for the ease of further contribution.

Editor Note: Modify section 6.0. Shaded text is the proposed new text.

A.1 Interworking Requirements at the I-IWU

An incoming Interface Serving node entity is used to transport calls originated from a SIP network domain to a BICC or ISUP network domain.

The "incoming SIP" is qualified as SIP which is used between the Incoming Interface Serving Node and the call originating entity (entities) supported in the SIP network domain. Similarly, the "outgoing BICC/ISUP" is qualified as the BICC or ISUP protocol supported between the Incoming Interface Serving Node and the next-hop entity (entities) in the BICC or ISUP network domain.

Editor Note: The following paragraph is proposed by NWB061.

In the specific case that the outgoing side of the I-IWU is BICC and that both incoming (SIP) and outgoing BICC sides of the I-IWU use the same media bearer technology with no media intermediary and with Bearer Control Tunnelling on the BICC side, then the I-IWU shall (in addition to the procedures outlined within this section) follow the additional BICC specific procedures outlined in section 2.0 of Annex A.

Editor Note: Modify section 7.0. Shaded text is the proposed new text.

A.2 Interworking Requirements at the O-IWU

An Outgoing Interface Serving (O-IWU) Node is used to transport calls from a BICC or ISUP network domain to a SIP network domain.

By definition, "outgoing SIP" is qualified as SIP which is used between the Outgoing Interface Serving Node and the call terminating entity (entities) in the SIP network domain. Similarly, by definition, "incoming BICC/ISUP" is qualified as the BICC or ISUP protocol supported between the Outgoing Interface Serving Node and the preceding BICC or ISUP entity.

Editor Note: The following paragraph is proposed by NWB061.

In the specific case that the incoming side of the O-IWU is BICC and that both outgoing (SIP) and incoming (BICC) sides of the O-IWU use the same media bearer technology with no media intermediary and with Bearer Control Tunnelling on the BICC side then the O-IWU shall (in addition to the procedures outlined within this section) follow the additional BICC specific procedures outlined in section 2.0 of annex A.

The Outgoing Interface Serving Node receives forward and backward signalling information from the "incoming BICC/ISUP" and "outgoing SIP" sides, respectively. After receiving this signalling information and performing appropriate call/service processing, the Outgoing Interface Serving Node may signal to subsequent SIP nodes or preceding BICC/ISUP entities for further call processing. In order to capture the signalling requirements, this subclause is organized into two subclauses for forward and backward signalling interworking.

The scope of this section is based on the key assumptions: (a) the Outgoing Interface Serving Node delivers basic calls only; and (b) the calls are delivered to a SIP network domain that does not require equivalent PSTN/ISDN service interworking. The service annexes of this document will cover additional interworking specification related to specific PSTN/ISDN services, which may be required by other interworking network architectures.

Editor Note: The following text is all new text for Annex-A.

1.0 Introduction

This annex contains additional inter workings to/from SIP which are particular to the BICC protocol.

2.0 Inter working BICC to/from SIP with common media bearer technology and BICC supports "Bearer Control Tunnelling"

If both BICC and SIP networks use the same media bearer technology, there is no media intermediary and the BICC side uses bearer control tunnelling then the following procedures apply.

For BICC CS2, the only defined Bearer Control Protocol carried by the Bearer Control Tunnelling mechanism is IP BCP (Q.1990). However, the procedures below apply equally to any future Bearer Control Protocol for which interworking with SDP and the SDP offer/answer procedures is defined.

2.1 Bearer Control Interworking

A Bearer Control Interworking function is assumed to exist which performs interworking between Bearer Control information (in the BICC Bearer Control Tunnelling Information Element) and SDP message bodies (in SIP messages). For IP BCP, the procedures for this interworking function are defined in section 3.1 of this annex ?..

2.1.1 Interworking from SDP offers to BICC Bearer Control Tunnelling information

On receipt of a SIP message containing an SDP offer, the Bearer Control Interworking function is used to generate a Bearer Control Protocol Data Unit for inclusion in a BICC message. The particular BICC message used depends on the procedures defined below.

The procedures of [SDP offer/answer] are used to determine the SIP message which should contain the SDP answer corresponding to this offer. Sending of this message is delayed until a BICC message has been received containing a Bearer Control Product Data Unit as described in 2.1.3.

2.1.2 Interworking from SDP answers to BICC Bearer Control Tunnelling information

On receipt of a SIP message containing an SDP answer, the Bearer Control Interworking function is used to generate a Bearer Control Protocol Data Unit for inclusion in a BICC message. The particular BICC message used depends on the procedures defined below.

2.1.3 Interworking from BICC Bearer Control Tunnelling information to SDP

On receipt of a BICC message containing a Bearer Control Protocol Data Unit, the Bearer Control Interworking Function is used to generate an SDP offer or answer for inclusion within a SIP message.

If the SDP is an SDP offer, then the particular SIP message used depends on the procedures defined below.

If the SDP is an SDP answer, then the SIP message sent is as identified in section 2.1.1 above.

2.2 Message mapping procedures

2.2.1 SIP to BICC

2.2.1.1 Initial INVITE

On receipt of the INVITE, the I-IWU determines the Bearer Setup Procedure to be used on the BICC side. This depends on whether the INVITE contains an SDP offer:

> If the INVITE contains an SDP offer, then the I-IWU uses the ‘Per call bearer setup using bearer control tunnelling – fast forwards’ procedures defined in Q.1902.4. The INVITE is mapped to an IAM as described in Section 7 of the main body of this Recommendation.?.
>
> If the INVITE does not contain an SDP offer, then the I-IWU uses the ‘Per call bearer setup using bearer control tunnelling – backwards’ procedures defined in Q.1902.4. The INVITE is mapped to an IAM as described in Section 7? of the main body of this Recommendation..

2.2.1.2 APM

Subsequently, an APM message is received according to the procedures of Q.1902.4. This is mapped to a SIP 183 response to the initial INVITE.

2.2.1.3 PRACK

On receipt of a PRACK message responding to the 183 response sent in section 2.2.1.2, containing SDP the I-IWU shall send an APM message on the BICC side.

2.2.1.4 Further APM messages

On receipt of further APM messages on the BICC side, containing Bearer Control Tunnelling information which maps to an SDP offer, the I-IWU shall send an UPDATE request on the SIP side.

2.2.1.5 UPDATE requests

On receipt of an UPDATE request on the SIP side, containing SDP, the I-IWU shall send an APM message on the BICC side.

2.2.1.6 200 OK(UPDATE) response

On receipt of a 200 OK(UPDATE) message in response to the UPDATE request sent as a result of section 2.2.1.4, containing SDP the I-IWU shall send an APM message on the BICC side.

2.2.2 BICC to SIP

2.2.2.1 Initial IAM

On receipt of an IAM, the O-IWU action depends on the Bearer Setup Procedure requested

2.2.2.1.1 Fast Forwards setup

In this case, the IAM contains Bearer Control Tunnelling information which maps to an SDP offer. An INVITE is sent containing this SDP offer.

2.2.2.1.2 Backwards

In this case, the IAM does not contain Bearer Control Tunnelling information. An INVITE is sent without SDP.

2.2.2.1.3 Delayed Forwards

In this case, the IAM does not contain Bearer Control Tunnelling information. An APM is returned according to the procedures of Q.1902.4.

Subsequently, an APM message is received containing Bearer Control Tunnelling information which maps to an SDP offer. An INVITE is sent containing this SDP offer.

2.2.2.2 Provisional response to INVITE

A provisional response to the INVITE may be received containing SDP which maps to a Bearer Control Protocol Data Unit. This is included as Bearer Control Tunnelling data within an APM message.

2.2.2.3 Subsequent APMs

On receipt of an APM message containing Bearer Control Tunnelling information, this information is mapped to an SDP offer or answer. In the case of an SDP offer, this is sent in an UPDATE message. In the case of an SDP answer, the procedures of 2.1.3 determine the SIP message to send.

2.3 ~~Pre-condition~~Preconditions

~~Pre-condition~~Preconditions refer to the mechanisms used to determine when bearer setup is complete, including completion of any procedures within the bearer network not visible to the IWU.

Two forms of ~~pre-condition~~precondition exist: (i) relating to the set up of the bearer on the particular bearer link in question (ii) related to the set up of the bearer on previous links.

~~Pre-condition~~Preconditions of both kinds are handled on the SIP side using the mechanisms of [3 – (manyfolks)] which are based on attributes within the SDP.

~~Pre-condition~~Preconditions of type (i) are handled on the BICC side as follows:

- For fast/delayed forwards setup with Bearer Control Tunnelling, the existence of ~~pre-condition~~preconditions can be signalled forwards by indicating ‘notification required’ in the initial IAM. Subsequently, an APM message indicating ‘Connected’ is used to indicate that the bearer setup is complete.
- For backwards setup with Bearer Control Tunnelling, fulfilment of the precondition is assumed to be detected by the Bearer Control Protocol and reported to the terminating CSF.

~~Pre-condition~~Preconditions of type (ii) are handled on the BICC side by means of the COT mechanism as described in Q.1902.4.

Note that BICC provides mechanisms to indicate the existence and completion of ~~pre-condition~~preconditions from the O-IWU to the T-ISN, but not in the reverse direction – it is assumed that there are no (pre-ACM) procedures at the O-IWU that need to be delayed pending the completion of actions at the T-ISN.

The Bearer Control Interworking Function is responsible for processing precondition indications within the SDP and indicating to the BICC procedures when the above BICC mechanisms are required. The following indications may be passed from the Bearer Control Interworking Function to the BICC protocol procedures:

- Type (i) precondition required
- Type (i) precondition met
- Type (ii) precondition required
- Type (ii) precondition met

Similarly, when the BICC mechanism require preconditions to be signalled, a request is made to the Bearer Control Interworking Function to add the appropriate indications to SDP. The following indications mat be passed from the BICC protocol procedures to the Bearer Control Interworking Function:

- Type (i) precondition required
- Type (i) precondition met
- Type (ii) precondition required
- Type (ii) precondition met

2.3.1 Interworking type (i) preconditions

2.3.1.1 SIP to BICC

2.3.1.1.1 Fast-forwards setup

On receipt of the indication *Type (i) preconditions required* from the Bearer Control Interworking Function, the indication ‘Notification required’ shall be included in the outgoing IAM. (Note: this indication should not be received at any other time)

Subsequently, on receipt of the indication *Type (i) preconditions met* from the Bearer Control Interworking Function, an APM message shall be sent containing the indication ‘Connected’.

Editor’s note: The Bearer Control Interworking Function will need to take care of the following things: (i) on receipt of the SDP offer containing preconditions, generate the *Type (i) preconditions required* indication (ii) on generation of the SDP answer, indicate that the IWU’s end of the preconditions have been met in that SDP and (iii) on receipt of SDP indicating that the preconditions have been completely met, it should generate the *Type (i) preconditions met indication*.

Editor’s note: For backwards setup, preconditions could appear in the SDP answer received from the SIP side in the PRACK. In this case the Bearer Control Interworking Function will just wait until

SDP indicating ~~pre-condition~~preconditions met is received before actually mapping to IP BCP and forwarding to the BICC side.

2.3.1.2 BICC to SIP

2.3.1.2.1 Fast forwards setup

If the indication ‘notification required’ is received in the IAM, then the indication *Type (i) precondition required* is sent to the Bearer Control Interworking Function along with the Bearer Control Tunnelling Information in the IAM.

Subsequently, on receipt of an APM indicating ‘Connected’, then the indication *Type (i) precondition met* is sent to the Bearer Control Interworking Function.

Editor’s note: These indications will cause the BCIWU to include/generate the appropriate SDP precondition attributes.

2.3.1.2.2 Backwards setup

No action is taken on receipt of the indications Type (i) preconditions required and Type (i) preconditions met.

Editor’s note: The BCIWU may receive an SDP offer (say in 183) indicating preconditions, which it would signal to the BICC side (which does nothing, as above). The BCIWU can indicate ~~pre-condition~~preconditions met in the SDP answer, since on the BICC side receipt of the Bearer Control PDU indicates ~~pre-condition~~preconditions met.

2.3.1.2.3 Delayed Forwards

If the indication ‘notification required’ is received in the IAM, then the indication *Type (i) precondition required* is sent to the Bearer Control Interworking Function along with the Bearer Control Tunnelling Information received in the subsequent APM.

Subsequently, on receipt of an APM indicating ‘Connected’, then the indication *Type (i) precondition met* is sent to the Bearer Control Interworking Function.

2.3.2 Interworking type (ii) preconditions

2.3.2.1 SIP to BICCC

2.3.2.1.1 Fast forwards setup

On receipt of the indication *Type (ii) preconditions required* from the Bearer Control Interworking Function, the Nature of Connection indicators in the outgoing IAM shall be set to "Continuity check required on outgoing circuit". (Note: this indication should not be received at any other time).

Subsequently, on receipt of the indication *Type (ii) preconditions met* from the Bearer Control Interworking Function, a COT message shall be sent with the continuity indicators set to "continuity check successful".

Editor’s note: The Bearer Control Interworking Function will need to take care of the following things: (i) on receipt of the SDP offer containing preconditions, generate the *Type (ii) preconditions required* indication (ii) on generation of the SDP answer, indicate that the IWU’s end of the preconditions have been met in that SDP and (iii) on receipt of SDP indicating that the preconditions have been completely met, it should generate the *Type (ii) preconditions met indication*.

Editor’s note: For backwards setup, preconditions could appear in the SDP answer received from the SIP side in the PRACK. In this case the Bearer Control Interworking Function will just wait until

SDP indicating ~~pre-condition~~preconditions met is received before actually mapping to IP BCP and forwarding to the BICC side.

2.3.2.2 BICC to SIP

2.3.2.2.1 Fast forwards setup

If the indication ‘continuity check required on outgoing circuit’ is received in the IAM, then the indication *Type (ii) preconditions required* is sent to the Bearer Control Interworking Function along with the Bearer Control Tunnelling Information in the IAM.

Subsequently, on receipt of COT message with continuity indicators indicating "continuity check successful", then the indication *Type (ii) precondition met* is sent to the Bearer Control Interworking Function.

Editor’s note: These indications will cause the BCIWU to include/generate the appropriate SDP precondition attributes.

2.3.2.2.2 Backwards setup

No action is taken on receipt of the indications Type (ii) preconditions required and Type (ii) preconditions met.

Editor’s note: The BCIWU may receive an SDP offer (say in 183) indicating preconditions, which it would signal to the BICC side (which does nothing, as above). The BCIWU can indicate ~~pre-condition~~preconditions met in the SDP answer, since on the BICC side receipt of the Bearer Control PDU indicates ~~pre-condition~~preconditions met.

2.3.2.2.3 Delayed Forwards

If the indication ‘continuity check required on the outgoing circuit’ is received in the IAM, then the indication *Type (ii) precondition required* is sent to the Bearer Control Interworking Function along with the Bearer Control Tunnelling Information received in the subsequent APM.

Subsequently, on receipt of a COT message with continuity indicators indicating "continuity check successful", then the indication *Type (ii) precondition met* is sent to the Bearer Control Interworking Function.

3.0 Bearer Control Interworking Function

3.1 IPBCP/ SDP Bearer Control interworking function (BC-IWU)

This section defines the procedures associated with a Bearer Control Interworking Function which interworks IPBCP to/from SDP. In all cases the BC-IWU is a call stateful device. This is particularly important in enabling the BC-IWU to manipulate precondition information it receives within SDP offers/answers and IPBCP messages.

The IPBCP/SDP Bearer Control Interworking function (BC-IWU) shall behave as follows:

3.1.1. SDP to IPBCP

3.1.1.1 Receipt of SDP offer.

On receipt of an SDP offer (as determined by the procedures within [(3-(RFCoffer-ans)]) the BC-IWU shall send a REQUEST message on the IPBCP side. The REQUEST message contents shall be formatted as per the procedures in section 6 of Recommendation Q.1970. Any SDP fields that cannot be directly carried within the SDP allowed within the IPBCP REQUEST message shall not be sent to the BICC side. In addition, if the SDP offer contained any precondition media level attributes these shall be removed from the SDP sent to the IPBCP side. Instead, if the BC-IWU receives a type (i) preconditions required indication (as defined by the procedures in section 2.3) then the procedures outlined in section 2.3.1 shall be followed with respect to the setting of indicators within the BICC IAM. Furthermore, if SDP offer instead resulted in the BC-IWU receiving a type (i) preconditions met indication then the BC-IWU shall correlate receipt of this indication with receipt of a type (i) preconditions required indication in a previous offer for this call and the procedures outlined within section 2.3.1. with respect to type (i) preconditions met shall be followed.

3.1.1.2 Receipt of SDP answer

(i) IPBCP has previously sent a REQUEST message for which it has not yet received an answer.

On receipt of an SDP answer (as determined by the procedures within [3-(RFCoffer-ans)] the BC-IWU shall send an ACCEPTED message to the IPBCP side. The ACCEPTED message contents shall be formatted as per the procedures of section 6 of Recommendation Q.1970. With the exception of media level attributes describing preconditions, if the SDP field is allowed to be included in the ACCEPTED message, it shall be included.

If the SDP answer is received and the port number of the media stream that was being offered in the SDP offer is set to 0 then the BC-IWU shall send a REJECTED message to the IPBCP side. The REJECTED message contents shall be formatted as per the procedures of section 6 of Recommendation Q.1970. With the exception of media level attributes describing preconditions, if the SDP field is allowed to be included in the REJECTED message, it shall be included.

(ii) IPBCP has not previously sent a REQUEST message or has sent a REQUEST message for which an answer has been received.

On receipt of an SDP answer (as determined by the procedures within [3-(RFCoffer-answer)] the BC-IWU shall not send any message to the IPBCP side.

Editor's note: This deals with the situation whereby a call is from BICC to SIP and conformation of SIP preconditions is requested in the 18x. This results in an UPDATE being generated at the O-IWU with an SDP offer. This SDP offer will produce an answer at the ASN which should not be inter-worked to the BICC side (since the SDP offer simply reports updates the status of preconditions).

3.1.2 IPBCP to SDP

3.1.2.1 Receipt of Request message

On receipt of an IPBCP REQUEST message, the BC-IWU shall construct and send an SDP offer in the first SIP message sent as a result of the interworking procedures defined in this Recommendation and as per the procedures relating to the sending of SDP offers in SIP defined within [3-(RFCoffer-ans)] [3-(RFC3261)]. The SDP fields contained within the IPBCP REQUEST message shall be included within the SDP offer. If the BC-IWU receives a type (ii) preconditions required indication then the BC-IWU shall ensure that the SDP offer sent from the BC-IWU contains a "local" precondition (in the language of (3-(Manyfolks))). The current status of this "local" precondition shall have a strength tag of "none" and a direction tag of "none". The desired status of the local precondition shall be set to a strength of "mandatory" and a direction value of "sendrecv". Additionally, the BC-IWU shall insert a corresponding remote precondition with a desired status of strength-tag = none and direction-tag = none. The BC-IWU is responsible for storing the state of all preconditions during the duration of the call.

If, in the period between sending this offer and sending the last offer, the BC-IWU receives a type (ii) precondition met indication then the BC-IWU shall correlate receipt of this precondition status information with the value of the "local" precondition tag which it inserted on receipt of the type (ii) precondition required indication received in a previous IPBCP REQUEST message. The BC-IWU shall set the current status of this precondition equal to the desired status before sending out the SDP offer containing the updated current status.

3.1.2.2 Receipt of Accepted message

On receipt of an IPBCP ACCEPTED message, the BC-IWU shall construct and send an SDP answer in the first SIP message sent as a result of the interworking procedures defined in this Recommendation and as per the procedures relating to the sending of SDP answers defined within [3-(RFCoffer-ans)] and [3-(RFC3261)]. The SDP fields contained within the IPBCP ACCEPTED message shall be included within the SDP answer. Additionally, the BC-IWU shall include any SDP relating to the status of the preconditions SDP sent within the SDP offer that was interworked to the REQUEST message responsible for generating this ACCEPTED message. In particular, if the BC-IWU has received a type (i) preconditions required indication in the SDP offer which generated the REQUEST message responsible for this ACCEPTED message then the BC-IWU shall add in precondition SDP to update the current (and desired status (if necessary)) of the type (i) preconditions. The procedures used to respond to the SDP received in the previous SDP offer correlated with this answer are described fully in (3-[Manyfolks]).

3.1.2.3 Receipt of Confused message

On receipt of the CONFUSED message, the BC-IWU shall follow the procedures outlined within Q.1970.

Editor's note: The "confused" message is a compatibility mechanism which is part of the IPBCP protocol itself and has no parallel in SDP. The procedures in IPBCP say that on receipt of this message the BC-IWU could re-attempt the bearer establishment or may instead report the compatibility problem to a control entity to decide what action (e.g. releasing the call) to take. This may result in autonomous REL resulting at the BICC layer - the REL would of course effect the SIP network and would be covered in the procedures relating to autonomous release at the IWU.

3.1.2.4 Receipt of Rejected message.

On receipt of the REJECTED message, the BC-IWU shall send an SDP answer in the first available SIP message. The SDP answer shall be constructed using the SDP fields present in the REJECTED message however, the BC-IWU shall set the port number for the media stream to the value 0.

ANNEX-B

ANNEX-B. ISUP Specific Interworking for Basic Call

Editor Note: This Annex is reserved for ISUP specific interworking.

ANNEX-C.1~C.N

Interworking for ISDN Supplementary Services

Editor's Note: There are ~~probably~~ multiple service-specific annexes, which can be Annex C.1, Annex C.2, etc.

ANNEX C.1

ANNEX C.1 Interworking of CLIP/CLIR Supplementary service to SIP networks.

The CLIP/CLIR services are only to be interworked between trusted nodes - that is before passing any CLIP/CLIR information over the SIP/ISUP boundary the IWU must satisfy itself that the nodes to which the information is to be passed are trusted.

The inter working between the Calling Party Number and the P-Asserted-ID header and vice versa used for the CLIP-CLIR service is defined in the clauses 6.1.5.6 and 7.1.5. This inter working is essentially the same as for basic call and differs only in that if the CLIR service is invoked the "Address Presentation Restriction Indicator (APRI)" (in the case of ISUP to SIP calls) or the “priv value” of the "calling" Privacy header field (in the case of SIP to ISUP calls) is set to the appropriate "restriction/privacy" value.

In the specific case of ISUP originated calls, use of the CLIP service additionally requires the ability to determine whether the number was network provided or provided by the access signalling system. Due to the possible SIP indication of the P-Asserted-Identity the Screening indicator is set to network provided as default. For the CLIP-CLIR service the mapping of the APRI is described within clauses 6.1.5.6 and 7.1.5.

At the O-IWU the presentation restricted indication shall be mapped to the privacy header = “id” and “header”

With the use SIP-I (encapsulated ISUP) all parameters needed for the interworking of the CLIP-CLIR services shall be taken from the encapsulated ISUP. Using SIP-I signalling causes no impact on the CLIP-CLIR service.

ANNEX C.2

ANNEX C.2 Interworking of COLP/COLR Supplementary service to SIP networks.

Editor Note: This procedure is clear for SIP-I but not clear for Profile A and B.

For the SIP-I case all parameters related to the COLP/COLR service shall be taken from the encapsulated ISUP to process the COLP/COLR service. No impact on SIP and ISUP/BICC.

ANNEX C.3

ANNEX C.3 Interworking of Direct-Dialing-In (DDI) Supplementary service to SIP networks.

SIP-I:

The processing of the service is not impacted due to the fact that SIP-I is used.

All parameters can be taken from the encapsulated ISUP MIME.

ANNEX C.4

ANNEX C.4 Interworking of Malicious Call Identification (MCID) Supplementary service to SIP networks.

In accordance with the procedures described within Q.731.7, the service shall be terminated at the IWU.

SIP-I:

Impact: IP bearer can not be hold after the release of the call.

All parameters can be taken from the encapsulated ISUP MIME.

ANNEX C.5

ANNEX C.5 Interworking of Sub-addressing (SUB) Supplementary service to SIP networks.

SIP-I:

The processing of the service is not impacted due to the fact that SIP-I is used.

All parameters can be taken from the encapsulated ISUP MIME.

ANNEX C.6

ANNEX C.6 Interworking of Call Forwarding Busy (CFB)/ Call Forwarding No Reply (CFNR) / Call Forwarding Unconditional (CFU) Supplementary service to SIP networks.

In accordance with the procedures described within regarding recommendation (Q.732.2, Q.732.3 or Q.732.4), the service shall be terminated at the IWU.

SIP-I:

The processing of the service is not impacted due to the fact that SIP-I is used.

All parameters can be taken from the encapsulated ISUP MIME.

A call forwarding within the SIP network is FFS.

Editor Note: In forwarding case within SIP network, not all needed indications can be send to the IWU.

ANNEX C.7

ANNEX C.7 Interworking of Call Deflection (CD) Supplementary service to SIP networks.

In accordance with the procedures described within Q.732.5, the service shall be terminated at the IWU.

SIP-I:

The processing of the service is not impacted due to the fact that SIP-I is used.

All parameters can be taken from the encapsulated ISUP MIME.

Interworking SIP-BICC/ISUP:

Service is terminated at the IWU.

Interworking is FFS.

ANNEX C.8

ANNEX C.8 Interworking of Explicit Call Transfer (ECT) Supplementary service to SIP networks.

In accordance with the procedures described within Q.732.7, the service shall be terminated at the IWU.

SIP-I:

The processing of the service is not impacted due to the fact that SIP-I is used.

All parameters can be taken from the encapsulated ISUP MIME.

ANNEX C.9

ANNEX C.9 Interworking of Call Waiting (CW) Supplementary service to SIP networks.

In accordance with the procedures described within Q.733.1, the service shall be terminated at the IWU.

SIP-I:

The processing of the service is not impacted due to the fact that SIP-I is used.

All parameters can be taken from the encapsulated ISUP MIME.

ANNEX C.10

ANNEX C.10 Interworking of Call HOLD (HOLD) Supplementary service to SIP networks.

Call Hold is defined as an ISUP supplementary service within Q.733.2.

A call may be placed on hold by the calling user, at any time after the call has been answered or additionally as a service provider option:

1) after alerting has commenced, or
2) after the calling user has provided all of the information necessary for processing the call.

A call may be placed on hold by the called user, at any time after the call has been answered and before call clearing has begun.

For the Call Hold supplementary service, the Call Progress message containing the Generic Notification Indicator parameter is used to send the appropriate notification towards the remote party.

The following notification descriptions are used:

- Remote-hold
- Remote-retrieval

The Event Indicator is set to "Progress".

The same service is also available within SIP networks and is defined in RFC 3264. If a party in a call wants to put the other party "on hold", i.e., request that it temporarily stops sending one or more unicast media streams, a party offers the other an updated SDP. The stream to be placed on hold will be marked with the following attribute:

- "a=sendonly", if the stream was previously a sendrecv media stream
- "a=inactive", if the stream was previously a recvonly media stream

If the party wants to retrieve the call, then the stream to be retrieved will be marked as:

- "a=sendrecv", if the stream was previously a sendrecv media stream, or the attribute may be omitted, since sendrecv is the default
- "a=recvonly", if the stream was previously an inactive media stream

The mapping between the ISUP and SIP flows is shown in the following table.

Table 40~~33~~/Annex C.10 - A Mapping between ISUP and SIP for Call Hold supplementary service

Call state	**ISUP message**	**Mapping**	**SIP message**
Answered	CPG with "Remote-hold"	<==>	INVITE with the attribute line "a=sendonly" or "a=inactive" for the offered media stream (see above).
Answered	CPG with "Remote-retrieval"	<==>	INVITE with the attribute line "a=sendrecv", or omitted attribute line, or "a= recvonly" for the offered media stream (see above)
before answer	CPG with "Remote-hold"	==>	UPDATE with the attribute line "a=sendonly" or "a=inactive" for the offered media stream (see above).
before answer	CPG with "Remote- retrieval "	==>	UPDATE with the attribute line "a=sendrecv", or omitted attribute line, or "a= recvonly" for the offered media stream (see above)
Mapping: <==> : Mapping in both directions, i.e. from ISUP to SIP and vice versa ==> : Mapping from ISUP to SIP only			

In case of SIP with encapsulated ISUP (SIP-I) the Call Progress message is not generated from the SIP message but extracted from the SIP message at the I-IWU.

In case of SIP with encapsulated ISUP (SIP-I) the Call Progress message is encapsulated in the SIP message at the O-IWU.

The mapping between the ISUP and SIP-I flows is shown in the following table.

Table 41~~34~~/Annex C.10 - Mapping between ISUP and SIP-I for Call Hold supplementary service

Call state	ISUP message	Mapping	SIP message
Answered	CPG with "Remote-hold" CPG with "Remote-hold" extracted from the body of the SIP message	==> <==	INVITE with the attribute line "a=sendonly" or "a=inactive" for the offered media stream (see above) and encapsulated ISUP CPG message
Answered	CPG with "Remote-retrieval" CPG with "Remote-retrieval" extracted from the body of the SIP message	==> <==	INVITE with the attribute line "a=sendrecv", or omitted attribute line, or "a= recvonly" for the offered media stream (see above) and encapsulated ISUP CPG message
before answer	CPG with "Remote-hold" CPG with "Remote-hold" extracted from the body of the SIP message	==> <==	UPDATE with the attribute line "a=sendonly" or "a=inactive" for the offered media stream (see above) and encapsulated ISUP CPG message
before answer	CPG with "Remote- retrieval " CPG with "Remote-retrieval" extracted from the body of the SIP message	==> <==	UPDATE with the attribute line "a=sendrecv", or omitted attribute line, or "a= recvonly" for the offered media stream (see above) and encapsulated ISUP CPG message
Mapping: <== : Mapping from SIP to ISUP ==> : Mapping from ISUP to SIP			

Note: the Interworking of the Call Hold (HOLD) Supplementary service between BICC and SIP networks is for further study since BICC CS2 does not support media suspension.

SIP-I:

The processing of the service is not impacted due to the fact that SIP-I is used.

All parameters can be taken from the encapsulated ISUP MIME

Interworking SIP-BICC/ISUP:

See contribution written by Siemens.

ANNEX C.11

ANNEX C.11 Interworking of Completion of Calls to Busy Subscriber (CCBS) Supplementary service to SIP networks.

In accordance with the procedures described within Q.733.3, the service shall be terminated at the IWU.

SIP-I:

Impact: SCCP connectivity between originating and terminating network is needed. This connectivity could be available as a by-pass to the SIP network.

All parameters can be taken from the encapsulated ISUP MIME.

Interworking of CCBS without SCCP by-pass is FFS.

ANNEX C.12

ANNEX C.12 Interworking of Completion of Calls on No Reply (CCNR) Supplementary service to SIP networks.

In accordance with the procedures described within Q.733.5, the service shall be terminated at the IWU.

SIP-I:

Impact: SCCP connectivity between originating and terminating network is needed. This connectivity could be available as a by-pass to the SIP network.

All parameters can be taken from the encapsulated ISUP MIME.

Interworking of CCBS without SCCP by-pass is FFS.

ANNEX C.13

ANNEX C.13 Interworking of Terminal Portability (TP) Supplementary service to SIP networks.

Terminal Portability is defined as an ISUP supplementary service within Q.733.4.

For the Terminal Portability supplementary service, the Suspend and Resume messages containing the Suspend/Resume indicators set to “ISDN subscriber initiated” are used.

The Suspend message indicates a temporary cessation of communication without releasing the call. It can only be accepted during the conversation/data phase. A Resume message indicates a request to recommence communication.

Although there is no similar service in SIP networks, it is appropriate to map the flows for ISUP Terminal Portability supplementary service onto the flows for Call Hold in SIP networks in order to request media suspension at the remote SIP user agent.

In the case of SIP with encapsulated ISUP (SIP-I), the Call Progress message is not generated from the SIP message but extracted from the SIP message at the I-IWU.

In the case of SIP with encapsulated ISUP (SIP-I), the Call Progress message is encapsulated in the SIP message at the O-IWU.

Note: the Interworking of Terminal Portability (TP) Supplementary service between BICC and SIP networks is for further study since BICC CS2 does not support media suspension.

ANNEX C.14

ANNEX C.14 Interworking of Conference calling (CONF) Supplementary service to SIP networks.

In accordance with the procedures described within Q.734.1, the service shall be terminated at the IWU.

SIP-I:

The processing of the service is not impacted due to the fact that SIP-I is used.

All parameters can be taken from the encapsulated ISUP MIME.

ANNEX C.15

ANNEX C.15 Interworking of Three-Party Service (3PTY) Supplementary service to SIP networks.

In accordance with the procedures described within Q.734.2, the service shall be terminated at the IWU.

SIP-I:

The processing of the service is not impacted due to the fact that SIP-I is used.

All parameters can be taken from the encapsulated ISUP MIME.

ANNEX C.16

ANNEX C.16 Interworking of Closed User Group (CUG) Supplementary service to SIP networks.

In accordance with the procedures described within Q.735.1, the service shall be terminated at the IWU.

SIP-I:

The processing of the service is not impacted due to the fact that SIP-I is used.

All parameters can be taken from the encapsulated ISUP MIME.

ANNEX C.17

ANNEX C.17 Interworking of Multi-Level Precedence and Preemption (MLPP) Supplementary service to SIP networks.

In accordance with the procedures described within Q.735.3, the service shall be terminated at the IWU.

SIP-I:

Impact: the priority cannot be supported for the availability for an SIP bearer.

All parameters can be taken from the encapsulated ISUP MIME.

ANNEX C.18

ANNEX C.18 Interworking of Global Virtual Network Service (GVNS) Supplementary service to SIP networks.

In accordance with the procedures described within Q.735.6, the service shall be terminated at the IWU.

SIP-I:

The processing of the service is not impacted due to the fact that SIP-I is used.

All parameters can be taken from the encapsulated ISUP MIME.

ANNEX C.19

ANNEX C.19 Interworking of International telecommunication charge card (ITCC) Supplementary service to SIP networks.

In accordance with the procedures described within Q.736.1, the service shall be terminated at the IWU.

SIP-I:

Impact: SCCP connectivity between originating and terminating network is needed. This connectivity could be available as an by-pass to the SIP network.

All parameters can be taken from the encapsulated ISUP MIME.

Interworking of ITCC without SCCP by-pass is FFS.

ANNEX C.20

ANNEX C.20 Interworking of Reverse charging (REV) Supplementary service to SIP networks.

In accordance with the procedures described within Q.736.3, the service shall be terminated at the IWU.

SIP-I:

The processing of the service is not impacted due to the fact that SIP-I is used.

All parameters can be taken from the encapsulated ISUP MIME.

ANNEX C.21

ANNEX C.21 Interworking of User-to-User Signalling (UUS) Supplementary service to SIP networks.

In accordance with the procedures described within Q.737.1, the service shall be terminated at the IWU.

SIP-I:

The impact with regard to the full functionality of the UUS is for further study.

All parameters can be taken from the encapsulated ISUP MIME.

ANNEX-E.1~E.N

Editor’s Note: All the E.X Annexes contain references to normative IETF RFC and materials originally sourced from IETF but are deemed normative to this Recommendation.

ANNEX-E.1

ANNEX-E.1 List of Normative References (normative)

[1] RFC 1890, "RTP Profile for Audio and Video Conferences with Minimal Control", Internet Engineering Task Force, January 1996.

[2] RFC 2046, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", Internet Engineering Task Force, November 1996.

[3] RFC 2327, "SDP: Session Description Protocol", Internet Engineering Task Force, April 1998.

[4] RFC 2806, "URLs for Telephone Calls", Internet Engineering Task Force, April 2000.

Editor's note: RFC 2806 is new, but seems to be needed.

[5] RFC 2833, "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals", May 2000.

Editor's note: present in TRQ BICC/ISUPSIP, but not clear whether the requirement to support it affects the IWU.

[6] RFC 2976, “The SIP INFO method”, Internet Engineering Task Force, October 2000.

[7] RFC 3204, “MIME media types for ISUP and QSIG objects”, Internet Engineering Task Force, December 2001.

[8] RFC 3261, “SIP: Session Initiation Protocol”, Internet Engineering Task Force, June 2002.

[9] RFC 3262, "Reliability of Provisional Responses in SIP", Internet Engineering Task Force, June 2002.

[10] RFC 3264, "An Offer/Answer Model with SDP", Internet Engineering Task Force, June 2002.).

[11] RFC 3267, "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", Internet Engineering Task Force. June 2002

[12] RFC 3312, “Integration of Resource Management and Session Initiation Protocol (SIP)”, Internet Engineering Task Force, October 2002.

[13] RFC 3311, "The Session Initiation Protocol UPDATE Method", Internet Engineering Task Force, September 2002.

[14] RFC AAAA, "A Privacy Mechanism for the Session Initiation Protocol (SIP)", Internet Engineering Task Force. Approved, but not yet published. (Available as draft-ietf-sip-privacy-general-01.txt).

[15] RFC CCCC, "RTP Payload Format for a 64 kbit/s voice band data call", Internet Engineering Task Force. Work in progress. (Available as draft-kreuter-avt-rtp-clearmode-00.txt).

Editor's note: The IETF will provide a RFC number for this document as soon as we need it for the consent process.

ANNEX-E.2

ANNEX-E.2 The P-Asserted-Identity: SIP header extension (normative)

This Annex reproduces the content of RFC YYYY (to be published, available as draft-ietf-sip-asserted-identity-02). That RFC was made Informational rather than Standards Track because IETF policy is to standardize open rather than closed networks. Its domain of applicability is defined in the opening section of the document. Interworking Units covered by this Recommendation shall support the P-Asserted-Identity header field as defined in this Annex, and shall additionally conform to the trust conditions applicable to the SIP network within which this header field is used.

Copyright Notice

Abstract

This document describes private extensions to SIP that enable a network of trusted SIP servers to assert the identity of authenticated users, and the application of existing privacy mechanisms to the identity problem. The use of these extensions is only applicable inside an administrative domain with previously agreed-upon policies for generation, transport and usage of such information. This document does NOT offer a general privacy or identity model suitable for use between different trust domains, or use in the Internet at large.

A.1 Applicability statement

This document describes private extensions to SIP [1] that enable a network of trusted SIP servers to assert the identity of end users or end systems, and to convey indications of end-user requested privacy.

The use of these extensions is only applicable inside a 'Trust Domain' as defined in Short term requirements for Network Asserted Identity [5]. Nodes in such a Trust Domain are explicitly trusted by its users and end-systems to publicly assert the identity of each party, and to be responsible for withholding that identity outside of the Trust Domain when privacy is requested. The means by which the network determines the identity to assert is outside the scope of this document (though it commonly entails some form of authentication).

A key requirement of [5] is that the behavior of all nodes within a given Trust Domain 'T' is known to comply to a certain set of specifications known as 'Spec(T)'. Spec(T) MUST specify behavior for the following:

1. The manner in which users are authenticated
2. The mechanisms used to secure the communication among nodes within the Trust Domain
3. The mechanisms used to secure the communication between UAs and nodes within the Trust Domain
4. The manner used to determine which hosts are part of the Trust Domain
5. The default privacy handling when no Privacy header field is present
6. That nodes in the Trust Domain are compliant to SIP [1]

8. Privacy handling for identity as described in Section 7.

An example of a suitable Spec(T) is shown in Section 11.

This document does NOT offer a general privacy or identity model suitable for inter-domain use or use in the Internet at large. Its assumptions about the trust relationship between the user and the network may not apply in many applications. For example, these extensions do not accommodate a model whereby end users can independently assert their identity by use of the extensions defined here. Furthermore, since the asserted identities are not cryptographically certified, they are subject to forgery, replay, and falsification in any architecture that does not meet the requirements of [5].

The asserted identities also lack an indication of who specifically is asserting the identity, and so it must be assumed that the Trust Domain is asserting the identity. Therefore, the information is only meaningful when securely received from a node known to be a member of the Trust Domain.

Despite these limitations, there are sufficiently useful specialized deployments that meet the assumptions described above, and can accept the limitations that result, to warrant informational publication of this mechanism. An example deployment would be a closed network which emulates a traditional circuit switched telephone network.

A.2 Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [3].

Throughout this document requirements for or references to proxy servers or proxy behavior apply similarly to other intermediaries within a Trust Domain (ex: B2BUAs).

The terms Identity, Network Asserted Identity and Trust Domain in this document have meanings as defined in [5].

A.3 Introduction

Various providers offering a telephony service over IP networks have selected SIP as a call establishment protocol. Their environments require a way for trusted network elements operated by the service providers (for example SIP proxy servers) to communicate the identity of the subscribers to such a service, yet also need to withhold this information from entities that are not trusted when necessary. Such networks typically assume some level of transitive trust amongst providers and the devices they operate.

These networks need to support certain traditional telephony services and meet basic regulatory and public safety requirements. These include Calling Identity Delivery services, Calling Identity Delivery Blocking, and the ability to trace the originator of a call. While baseline SIP can support each of these services independently, certain combinations cannot be supported without the extensions described in this document. For example, a caller that wants to maintain privacy and consequently provides limited information in the SIP From header field will not be identifiable by recipients of the call unless they rely on some other means to discover the identity of the caller. Masking identity information at the originating user agent will prevent certain services, e.g., call trace, from working in the Public Switched Telephone Network (PSTN) or being performed at intermediaries not privy to the authenticated identity of the user.

This document attempts to provide a network asserted identity service using a very limited, simple mechanism, based on requirements in [5]. This work is derived from a previous attempt, [6], to solve several problems related to privacy and identity in Trust Domains . A more comprehensive mechanism, [7] which uses cryptography to address this problem is the subject of current study by the SIP working group.

Providing privacy in a SIP network is more complicated than in the PSTN. In SIP networks, the participants in a session typically are normally able to exchange IP traffic directly without involving any SIP service provider. The IP addresses used for these sessions may themselves reveal private information. A general purpose mechanism for providing privacy in a SIP environment is discussed in [2]. This document applies that privacy mechanism to the problem of network asserted identity.

A.4 Overview

The mechanism proposed in this document relies on a new header field called 'P-Asserted-Identity' that contains a URI (commonly a SIP URI) and an optional display-name, for example:

P-Asserted-Identity: "Cullen Jennings" <sip:fluffy@cisco.com>

A proxy server which handles a message can, after authenticating the originating user in some way (for example: Digest authentication), insert such a P-Asserted-Identity header field into the message and forward it to other trusted proxies. A proxy that is about to forward a message to a proxy server or UA that it does not trust MUST remove all the P-Asserted-Identity header field values if the user requested that this information be kept private. Users can request this type of privacy as described in Section 7.

The formal syntax for the P-Asserted-Identity header is presented in Section 9.

A.5 Proxy behavior

A proxy in a Trust Domain can receive a message from a node that it trusts, or a node that it does not trust. When a proxy receives a message from a node it does not trust and it wishes to add a P-Asserted-Identity header field, the proxy MUST authenticate the originator of the message, and use the identity which results from this authentication to insert a P-Asserted-Identity header field into the message.

If the proxy receives a message (request or response) from a node that it trusts, it can use the information in the P-Asserted-Identity header field, if any, as if it had authenticated the user itself.

If there is no P-Asserted-Identity header field present, a proxy MAY add one containing at most one SIP or SIP URIs, and at most one tel URL. If the proxy received the message from an element that it does not trust and there is a P-Asserted-Identity header present which contains a SIP or SIP URI, the proxy MUST replace that SIP or SIPS URI with a single SIP or SIP URI or remove it. Similarly, if the proxy received the message from an element that it does not trust and there is a P-Asserted-Identity header present which contains a tel URI, the proxy MUST replace that tel URI with a single tel URI or remove it.

When a proxy forwards a message to another node, it must first determine if it trusts that node or not. If it trusts the node, the proxy does not remove any P-Asserted-Identity header fields that it generated itself, or that it received from a trusted source. If it does not trust the element, then the proxy MUST examine the Privacy header field (if present) to determine if the user requested that asserted identity information be kept private.

A.6 Hints for multiple identities

If a P-Preferred-Identity header field is present in the message that a proxy receives from an entity that it does not trust, the proxy MAY use this information as a hint suggesting which of multiple valid identities for the authenticated user should be asserted. If such a hint does not correspond to any valid identity known to the proxy for that user, the proxy can add a P-Asserted-Identity header of its own construction, or it can reject the request (for example, with a 403 Forbidden). The proxy MUST remove the user-provided P-Preferred-Identity header from any message it forwards.

A user agent only sends a P-Preferred-Identity header field to proxy servers in a Trust Domain; user agents MUST NOT populate the P-Preferred-Identity header field in a message that is not sent directly to a proxy that is trusted by the user agent. Were a user agent to send a message containing a P-Preferred-Identity header field to a node outside a Trust Domain, then the hinted identity might not be managed appropriately by the network, which could have negative ramifications for privacy.

A.7 Requesting privacy

Parties who wish to request the removal of P-Asserted-Identity header fields before they are transmitted to an element that is not trusted may add the "id" privacy token to the Privacy header field. The Privacy header field is defined in [6]. If this token is present, proxies MUST remove all the P-Asserted-Identity header fields before forwarding messages to elements that are not trusted. If the Privacy header field value is set to "none" then the proxy MUST NOT remove the P-Asserted-Identity header fields.

When a proxy is forwarding the request to an element that is not trusted and there is no Privacy header field, the proxy MAY include the P-Asserted-Identity header field or it MAY remove it. This decision is a policy matter of the Trust Domain and MUST be specified in Spec(T). It is RECOMMENDED that unless local privacy policies prevent it, the P-Asserted-Identity header fields SHOULD NOT be removed, since removal may cause services based on Asserted Identity to fail.

However, it should be noted that unless all users of the Trust Domain have access to appropriate privacy services, forwarding of the P-Asserted-Identity may result in disclosure of information which was not requested by and could not be prevented by the user. It is therefore STRONGLY RECOMMENDED that all users have access to privacy services as described in this document.

Formal specification of the "id" Privacy header priv-value is described in Section 9.3. Some general guidelines for when users require privacy are given in [2].

If multiple P-Asserted-Identity headers field values are present in a message, and privacy of the P-Asserted-Identity header field is requested, then all instances of the header field values MUST be removed before forwarding the request to an entity that is not trusted.

A.8 User Agent Server behavior

Typically, a user agent renders the value of a P-Asserted-Identity header field that it receives to its user. It may consider the identity provided by a Trust Domain to be privileged, or intrinsically more trustworthy than the From header field of a request. However, any specific behavior is specific to implementations or services. This document also does not mandate any user agent handling for multiple P-Asserted-Identity header field values that happen to appear in a message (such as a SIP URI alongside a tel URL).

However, if a User Agent Server receives a message from a previous element that it does not trust, it MUST NOT use the P-Asserted-Identity header field in any way.

If a UA is part of the Trust Domain from which it received a message containing a P-Asserted-Identity header field, then it can use the value freely but it MUST ensure that it does not forward the information to any element that is not part of the Trust Domain.

If a UA is not part of the Trust Domain from which it received a message containing a P-Asserted-Identity header field, then it can assume this information does not need to be kept private.

A.9 Formal syntax

The following syntax specification uses the augmented Backus-Naur Form (BNF) as described in RFC-2234 [4].

A.9.1 The P-Asserted-Identity header

The P-Asserted-Identity header field is used among trusted SIP entities (typically intermediaries) to carry the identity of the user sending a SIP message as it was verified by authentication.

PAssertedID = "P-Asserted-Identity" HCOLON PAssertedID-value

*(COMMA PAssertedID-value)

PAssertedID-value = name-addr / addr-spec

A P-Asserted-Identity header field value MUST consist of exactly one name-addr or addr-spec. There may be one or two P-Asserted-Identity values. If there is one value, it MUST be a sip, sips, or tel URI. If there are two values, one value MUST be a sip or sips URI and the other MUST be a tel URI. It is worth noting that proxies can (and will) add and remove this header field.

This document adds the following entry to Table 2 of [1]:

Header field	where	proxy	ACK	BYE	CAN	INV	OPT	REG	SUB	NOT	REF	INF	UPD	PRA
P-Asserted-Identity		adr	-	o	-	o	o	-	o	o	o	-	-	-

A.9.2 The P-Preferred-Identity header

The P-Preferred-Identity header field is used from an user agent to a trusted proxy to carry the identity the user sending the SIP message wishes to be used for the P-Asserted-Header field value that the trusted element will insert.

PPreferredID = "P-Preferred-Identity" HCOLON PPreferredID-value

*(COMMA PPreferredID -value)

PPreferredID-value = name-addr / addr-spec

A P-Preferred-Identity header field value MUST consist of exactly one name-addr or addr-spec. There may be one or two P-Preferred-Identity values. If there is one value, it MUST be a sip, sips, or tel URI. If there are two values, one value MUST be a sip or sips URI and the other MUST be a tel URI. It is worth noting that proxies can (and will) remove this header field.

This document adds the following entry to Table 2 of [1]:

Header field	where	proxy	ACK	BYE	CAN	INV	OPT	REG	SUB	NOT	REF	INF	UPD	PRA
P-Preferred-Identity		adr	-	o	-	o	o	-	o	o	o	-	-	-

A.9.3 The "id" privacy type

This specification adds a new privacy type ("priv-value") to the Privacy header, defined in [2]. The presence of this privacy type in a Privacy header field indicates that the user would like the Network Asserted Identity to be kept private with respect to SIP entities outside the Trust Domain with which the user authenticated. Note that a user requesting multiple types of privacy MUST include all of the requested privacy types in its Privacy header field value.

priv-value = "id"

Example:

Privacy: id

A.10 Examples

A.10.1 Network Asserted Identity passed to trusted gateway

In this example, proxy.cisco.com creates a P-Asserted-Identity header field from an identity it discovered from SIP Digest authentication. It forwards this information to a trusted proxy which forwards it to a trusted gateway. Note that these examples consist of partial SIP messages that illustrate only those headers relevant to the authenticated identity problem.

```
   * F1   useragent.cisco.com -> proxy.cisco.com

   INVITE sip:+14085551212@cisco.com SIP/2.0
   Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-123
   To: <sip:+14085551212@cisco.com>
   From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
   Call-ID: 245780247857024504
   CSeq: 1 INVITE
   Max-Forwards: 70
   Privacy: id

   * F2   proxy.cisco.com -> useragent.cisco.com

   SIP/2.0 407 Proxy Authorization
   Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-123
   To: <sip:+14085551212@cisco.com>;tag=123456
   From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
   Call-ID: 245780247857024504
   CSeq: 1 INVITE
   Proxy-Authenticate: .... realm="sip.cisco.com"

   * F3   useragent.cisco.com -> proxy.cisco.com

   INVITE sip:+14085551212@cisco.com SIP/2.0
   Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-124
   To: <sip:+14085551212@cisco.com>
   From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
   Call-ID: 245780247857024504
   CSeq: 2 INVITE
   Max-Forwards: 70
   Privacy: id
   Proxy-Authorization: .... realm="sip.cisco.com" user="fluffy"

   * F4   proxy.cisco.com -> proxy.pstn.net (trusted)

   INVITE sip:+14085551212@proxy.pstn.net SIP/2.0
   Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-124
   Via: SIP/2.0/TCP proxy.cisco.com;branch=z9hG4bK-abc
   To: <sip:+14085551212@cisco.com>
   From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
   Call-ID: 245780247857024504
   CSeq: 2 INVITE
   Max-Forwards: 69
   P-Asserted-Identity: "Cullen Jennings" <sip:fluffy@cisco.com>
   P-Asserted-Identity: tel:+14085264000
   Privacy: id

   * F5   proxy.pstn.net -> gw.pstn.net (trusted)

   INVITE sip:+14085551212@gw.pstn.net SIP/2.0
   Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-124
   Via: SIP/2.0/TCP proxy.cisco.com;branch=z9hG4bK-abc
   Via: SIP/2.0/TCP proxy.pstn.net;branch=z9hG4bK-a1b2
   To: <sip:+14085551212@cisco.com>
   From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
   Call-ID: 245780247857024504
   CSeq: 2 INVITE
   Max-Forwards: 68
   P-Asserted-Identity: "Cullen Jennings" <sip:fluffy@cisco.com>
   P-Asserted-Identity: tel:+14085264000
   Privacy: id
```

A.10.2 Network Asserted Identity Withheld

In this example, the User Agent sends an INVITE that indicates it would prefer the identity sip:fluffy@cisco.com to the first proxy, which authenticates this with SIP Digest. The first proxy creates a P-Asserted-Identity header field and forwards it to a trusted proxy (outbound.cisco.com). The next proxy removes the P-Asserted-Identity header field, and the request for Privacy before forwarding this request onward to the biloxi.com proxy server which it does not trust.

```
   * F1    useragent.cisco.com -> proxy.cisco.com

   INVITE sip:bob@biloxi.com SIP/2.0
   Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-a111
   To: <sip:bob@biloxi.com>
   From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
   Call-ID: 245780247857024504
   CSeq: 1 INVITE
   Max-Forwards: 70
   Privacy: id
   P-Preferred-Identity: "Cullen Jennings" <sip:fluffy@cisco.com>

   * F2    proxy.cisco.com -> useragent.cisco.com
   SIP/2.0 407 Proxy Authorization
   Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-a111
   To: <sip:bob@biloxi.com>;tag=123456
   From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
   Call-ID: 245780247857024504
   CSeq: 1 INVITE
   Proxy-Authenticate: .... realm="cisco.com"

   * F3    useragent.cisco.com -> proxy.cisco.com

   INVITE sip:bob@biloxi.com SIP/2.0
   Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-a123
   To: <sip:bob@biloxi.com>
   From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
   Call-ID: 245780247857024504
   CSeq: 2 INVITE
   Max-Forwards: 70
   Privacy: id
   P-Preferred-Identity: "Cullen Jennings" <sip:fluffy@cisco.com>
   Proxy-Authorization: .... realm="cisco.com" user="fluffy"

   * F4    proxy.cisco.com -> outbound.cisco.com (trusted)

   INVITE sip:bob@biloxi SIP/2.0
   Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-a123
   Via: SIP/2.0/TCP proxy.cisco.com;branch=z9hG4bK-b234
   To: <sip:bob@biloxi.com>
   From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
   Call-ID: 245780247857024504
   CSeq: 2 INVITE
   Max-Forwards: 69
   P-Asserted-Identity: "Cullen Jennings" <sip:fluffy@vovida.org>
   Privacy: id

   * F5   outbound.cisco.com -> proxy.biloxi.com (not trusted)

   INVITE sip:bob@biloxi SIP/2.0
   Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-a123
   Via: SIP/2.0/TCP proxy.cisco.com;branch=z9hG4bK-b234
   Via: SIP/2.0/TCP outbound.cisco.com;branch=z9hG4bK-c345
   To: <sip:bob@biloxi.com>
   From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
   Call-ID: 245780247857024504
   CSeq: 2 INVITE
   Max-Forwards: 68
   Privacy: id

   * F6   proxy.biloxi.com -> bobster.biloxi.com

   INVITE sip:bob@bobster.biloxi.com SIP/2.0
   Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-a123
   Via: SIP/2.0/TCP proxy.cisco.com;branch=z9hG4bK-b234
   Via: SIP/2.0/TCP outbound.cisco.com;branch=z9hG4bK-c345
   Via: SIP/2.0/TCP proxy.biloxi.com;branch=z9hG4bK-d456
   To: <sip:bob@biloxi.com>
   From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
   Call-ID: 245780247857024504
   CSeq: 2 INVITE
   Max-Forwards: 67
   Privacy: id
```

A.11 Example of Spec(T)

The integrity of the mechanism described in this document relies on one node knowing (through configuration) that all of the nodes in a Trust Domain will behave in a predetermined way. This requires the predetermined behavior to be clearly defined and for all nodes in the Trust Domain to be compliant. The specification set that all nodes in a Trust Domain T must comply with is termed 'Spec(T)'.

The remainder of this section presents an example Spec(T), which is not normative in any way.

A.11.1 Protocol requirements

The following specifications MUST be supported:

1. SIP [1]
2. This document.

A.11.2 Authentication requirements

Users MUST be authenticated using SIP Digest Authentication.

A.11.3 Security requirements

Connections between nodes within the Trust Domain and between UAs and nodes in the Trust Domain MUST use TLS using a cipher suite of RSA_WITH_AES_128_CBC_SHA1. Mutual authentication between nodes in the trust domain MUST be performed and confidentiality MUST be negotiated.

A.11.4 Scope of Trust Domain

The Trust Domain specified in this agreement consists of hosts which possess a valid certificate which is

a) signed by examplerootca.org;

b) whose subjectAltName ends with one of the following domain names:

trusted.div1.carrier-a.net,

trusted.div2.carrier-a.net,

sip.carrier-b.com;

and

c) whose domain name corresponds to the hostname in the subjectAltName in the certificate.

A.11.5 Implicit handling when no Privacy header is present

The elements in the trust domain must support the 'id' privacy service therefore absence of a Privacy header can be assumed to indicate that the user is not requesting any privacy. If no Privacy header field is present in a request, elements in this Trust Domain MUST act as if no privacy is requested.

A.12 Security considerations

The mechanism provided in this document is a partial consideration of the problem of identity and privacy in SIP. For example, these mechanisms provide no means by which end users can securely share identity information end-to-end without a trusted service provider. Identity information which the user designates as 'private' can be inspected by any intermediaries participating in the Trust Domain. This information is secured by transitive trust, which is only as reliable as the weakest link in the chain of trust.

When a trusted entity sends a message to any destination with that party's identity in a P-Asserted-Identity header field, the entity MUST take precautions to protect the identity information from eavesdropping and interception to protect the confidentiality and integrity of that identity information. The use of transport or network layer hop-by-hop security mechanisms, such as TLS or IPSec with appropriate cipher suites, can satisfy this requirement.

A.13 IANA considerations

A.13.1 Registration of new SIP header fields

This document defines two new private SIP header fields, "P-Asserted-Identity" and "P-Preferred-Identity". As recommended by the policy of the Transport Area, these headers should be registered by the IANA in the SIP header registry, using the RFC number of this document as its reference.

```
   Name of Header:          P-Asserted-Identity

   Short form:              none

   Registrant:              Cullen Jennings
                            fluffy@cisco.com

   Normative description:
   Section 9.1 of this document

   Name of Header:          P-Preferred-Identity

   Short form:              none

   Registrant:              Cullen Jennings
                            fluffy@cisco.com

   Normative description:
   Section 9.2 of this document
```

A.13.2 Registration of "id" privacy type for SIP Privacy header

```
   Name of privacy type:    id

   Short Description:       Privacy requested for Third-Party Asserted Identity

   Registrant:              Cullen Jennings
                            fluffy@cisco.com
   Normative description:
   Section 9.3 of this document
```

A.14 Acknowledgements

Thanks to Bill Marshall and Flemming Andreason[6], Mark Watson[5], and Jon Peterson[7] for authoring drafts which represent the bulk of the text making up this document. Thanks to many people for useful comments including Jonathan Rosenberg, Rohan Mahy and Paul Kyzivat.

Normative References

[1] Rosenberg, J. and H. Schulzrinne, "SIP: Session Initiation Protocol", draft-ietf-sip-rfc2543bis-09 (work in progress), February 2002. Now published as RFC 3261.

[2] Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)", draft-ietf-sip-privacy-general-00 (work in progress), May 2002. To be published as RFC xxxx.

[3] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[4] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, November 1997.

Informational References

[5] Watson, M., "Short term requirements for Network Asserted Identity", draft-ietf-sipping-nai-reqs-01 (work in progress), May 2002.

[6] Andreasen, F., "SIP Extensions for Network-Asserted Caller Identity and Privacy within Trusted Networks", draft-ietf-sip-privacy-04 (work in progress), March 2002.

[7] Peterson, J., "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", draft-peterson-sip-identity-00 (work in progress), April 2002.

Authors' Addresses

Cullen Jennings
Cisco Systems
170 West Tasman Drive
MS: SJC-21/3
San Jose, CA 95134
USA

Phone: +1 408 527-9132
EMail: fluffy@cisco.com

Jon Peterson
NeuStar, Inc.
1800 Sutter Street, Suite 570
Concord, CA 94520
USA

Phone: +1 925/363-8720
EMail: Jon.Peterson@NeuStar.biz

Mark Watson
Nortel Networks
Maidenhead Office Park (Bray House)
Westacott Way
Maidenhead, Berkshire
England

Phone: +44 (0)1628-434456
EMail: mwatson@nortelnetworks.com

Full Copyright Statement

Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

~~ANNEX C.1~~

~~ANNEX C.1 Interworking of CLIP/CLIR Supplementary service to SIP networks.~~

~~CLIP/CLIR is defined within Q.731.3 and Q.731.4 respectively. As per the interworking recommendations sections of Q.731.3 and Q.731.4, CLIP/CLIR services are only to be interworked between trusted nodes - that is before passing any CLIP/CLIR information over the SIP/ISUP boundary the IWU must satisfy itself that the nodes to which the information is to be passed are trusted. Tables C.1A and C.1B below specify the inter working required when the caller invokes CLIR and/or when the called party invokes the CLIP service. This inter working is essentially the same as that defined in section 8.1.1 table 22 and section 7.1.1.2 table 17 for basic call and differs only in that if the CLIR service is invoked the "Address Presentation Restriction Indicator (APRI)" (in the case of ISUP to SIP calls) or the privacy tag of the "calling" Remote-Party-ID header field (in the case of SIP to ISUP calls) is set to the appropriate "restriction/privacy" value. In the specific case of ISUP originated calls, use of the CLIP service additionally requires the ability to determine whether the number was network provided or provided by the access signalling system. These differences and how they modify the "basic call" interworking previously described are shown in Table C.1A (for ISUP to SIP calls) and Table C.1B (for SIP to ISUP calls).~~

~~Table C.1B INVITE to IAM Mapping for CLIP/CLIR Supplementary services~~

~~Comment: delete complete table.~~

~~Table C.1A IAM (Calling Party Number parameter) to INVITE Mapping for CLIP/CLIR Supplementary services~~

~~Comment: delete complete table.~~

~~ANNEX C.2~~

~~ANNEX C.2 Interworking of COLP/COLR Supplementary service to SIP networks.~~

~~COLP/COLR IS DEFINED WITHIN Q.731.5 AND Q.731.6 RESPECTIVELY.~~

~~C.2.1 Forwards inter working~~

~~C.2.1.1 IAM to INVITE inter working (ISUP to SIP calls)~~

~~The BICC/ISUP to SIP inter working node determines that the COLP service has been requested by the calling party by parsing the "Optional Forward Call Indicators" field of the incoming IAM. If the "Connected Line Identity Request indicator" is set to "requested" then the BICC/ISUP to SIP inter working node SHALL ensure that any backwards "called party" information is inter worked to the appropriate parameters of the ISUP ANM or CON message sent backwards to the calling party as detailed within this service annex. No additional mapping (over and above that of "basic call") is specified within this service annex for IAM to INVITE mapping.~~

~~C.2.1.1 INVITE to IAM inter working (SIP to ISUP calls).~~

~~In the case of SIP to ISUP calls the incoming SIP outgoing ISUP node shall determine (via local) policy whether or not the calling subscriber is subscribed to the COLP service (e.g. via database dip). If the calling subscriber has indeed subscribed to the COLP service then the SIP toBICC/ISUP inter working node shall invoke the COLP service on behalf of the SIP node by setting the "Connected Line Identity Request indicator" parameter of the "Optional forward call indicator" of the IAM to "requested". No additional mapping (over and above that of "basic call") is specified within this service annex for INVITE to IAM mapping.~~

~~C.2.2 Backwards inter working~~

~~C.2.2.1 200 OK (INVITE) to ANM inter working~~

~~Table C.2A specifies the inter working required in the case when the calling party has invoked the COLP service. The table also indicates the inter workings (in addition to those specified within the "basic call" section of this document) required if the calling party has invoked the COLP service and the called party may or may not invoke the COLR service.~~

~~C.2.2.2 ANM to 200 OK (INVITE)~~

~~Table C.2B specifies the inter working required in the case when the COLP has been automatically requested on behalf of the originating SIP node. The table also indicates the inter workings (in addition to those specified within the "basic call" section of this document) required if the COLP service has been invoked and the called party may or may not have invoked the COLR service.~~

~~Editor's note: Pages in this Section Break are Landscape for tables.~~

~~Editor's note: Contents of the following tables should be reformatted to the new format. Please do not contribute using the old table format~~

~~Table C.2A 200 OK (INVITE) to ANM - Additional Mapping for COLP/COLR Supplementary services~~

~~Table C.2B ANM to 200 OK (INVITE) - Additional Mapping for COLP/COLR Supplementary services~~

~~ANNEX D~~APPENDIX-1

~~ANNEX D~~APPENDIX-~~.1~~A Interworking scenarios between SIP and BICC

A.1 Scope

This annex defines typical interworking scenarios between BICC/ISUP and SIP. ISDN Access flows are included for informational purposes only.

A.2 Definitions

The vertical boxes represent two entities: BICC and IWU (SIP-BICC Interworking Function).

The vertical dashed lines represent the access interface. Each access interface supports a single access type: ISDN or SIP-NNI.

Solid horizontal arrows represent signalling messages and indicate their direction of propagation, i.e. to or from the interworking function. The interaction of messages shown along the vertical represent increasing time in the downward direction. All events on the same vertical line are related, e.g. an incoming message causes voice-path connections and triggers an outgoing message. Events on different vertical lines are not related unless connected by dashed lines. A dashed line indicates that an incoming message may trigger an event at a later time.

Wavy horizontal arrows (~~>) represent tones or announcements sent in-band.

Timers are represented as vertical arrows.

For call control the following symbols are used within the vertical boxes to indicate the relationship between the incoming and outgoing messages and the call control action taken.

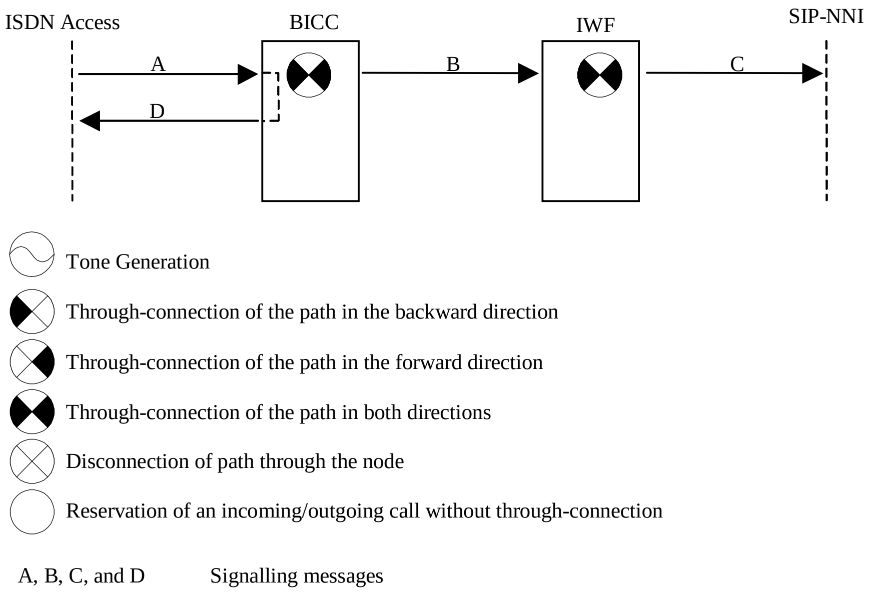

ISDN Access
BICC
IWF
SIP-NNI
A
B
C
D
Tone Generation
Through-connection of the path in the backward direction
Through-connection of the path in the forward direction
Through-connection of the path in both directions
Disconnection of path through the node
Reservation of an incoming/outgoing call without through-connection
A, B, C, and D
Signalling messages

Figure A.1/Q.1912.SIP – Example of a call flow or "arrow" diagram

A.3 Abbreviations

A.4 Methodology

Call flow or "arrow" diagrams are provided to show the temporal relationships between signalling messages during execution of a call control procedure. The general format of an arrow diagram is shown in Figure A.1.

The main part of the Recommendation takes precedence over this annex.

A.5 Interworking of SIP accesses to BICC

Subclauses A.5.1 and A.5.2 contain information relevant to basic call control. The call flow diagrams are divided into functional subclauses:

successful call set-up procedures;

unsuccessful call set-up procedures;

release procedures;

simple message segmentation procedures.

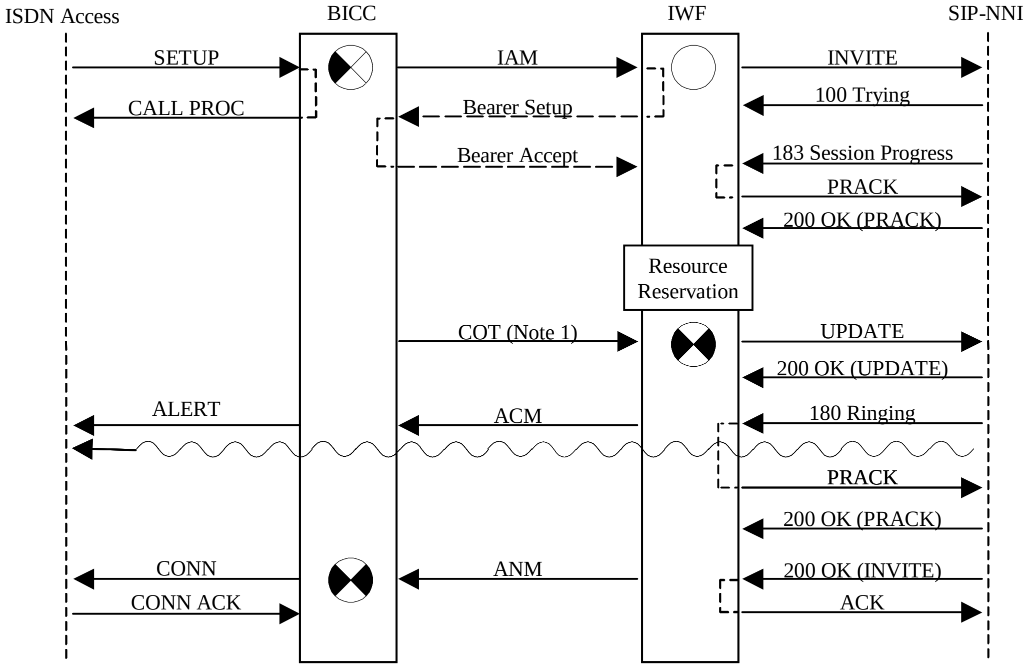
Editor’s Note: The following subsections show possible sequences of messages. Other scenarios may be added later as identified.

A.5.1 Incoming Call – BICC to SIP

A.5.1.1 Successful call set-up procedures/call flow diagrams for basic call control

A.5.1.1.1 Backwards BICC Bearer Setup, SIP Preconditions used

Figure A.2 shows a sequence of messages for successful call set-up for an incoming call from BICC to SIP. In this example, the IWU indicates mandatory local sendrecv preconditions in the INVITE. The IWU then sends the UPDATE message upon completion of bearer setup, any local resource reservation and reception of a COT message (if the IAM indicated 'COT on Previous'). The UPDATE message will confirm that local preconditions have been met. It is assumed that a SIP "Proxy" will be responsible for protecting against fraudulent use of the user plane.



Note 1 – This message is optional, depending on the indication in the IAM.

Figure A.2/Q.1912.SIP – Successful basic call setup from BICC to SIP

A.5.1.2 Unsuccessful call set-up procedures/call flow diagrams for basic call control

FFS

A.5.1.3 Release procedures/call flow diagrams for basic call control

A.5.1.3.1 Normal call release procedure, backwards bearer set-up

Figure A.3 shows a normal call release procedure initiated from the BICC side of the call. This call flow assumes that no resource reservation teardown signalling is required on the SIP side of the call.

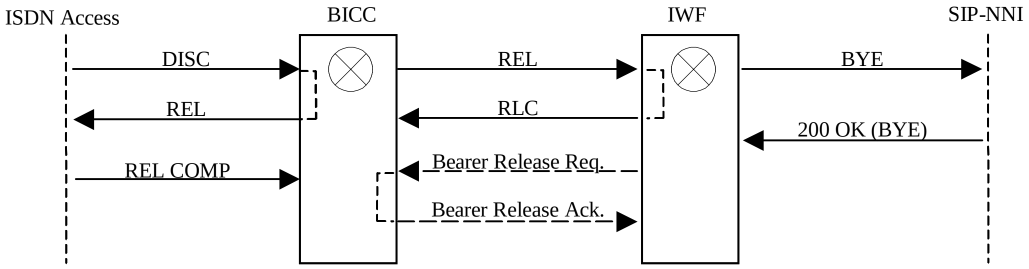


Figure A.3/Q.1912.SIP – Normal call release from BICC to SIP

A.5.1.4 Simple segmentation procedures/call flow diagrams for basic call control

FFS

A.5.2 Outgoing Call – SIP to BICC

A.5.2.1 Successful call set-up procedures/call flow diagrams for basic call control

A.5.2.1.1 SIP Preconditions used, backwards BICC bearer setup, non-automatic answer

Figure A.4 shows the sequence of messages for successful call set-up for an outgoing call from SIP to BICC. In this sequence, the SIP side indicates mandatory local resource reservation (such as sendrecv) in the INVITE. The IAM (with ‘COT on Previous’ indication) is sent by the IWU once the initial INVITE is received, and a COT message is sent once the SIP side has reserved resources for the call (confirmed in the UPDATE). It is assumed that a SIP “Proxy” will be responsible for protecting against fraudulent use of the user plane.

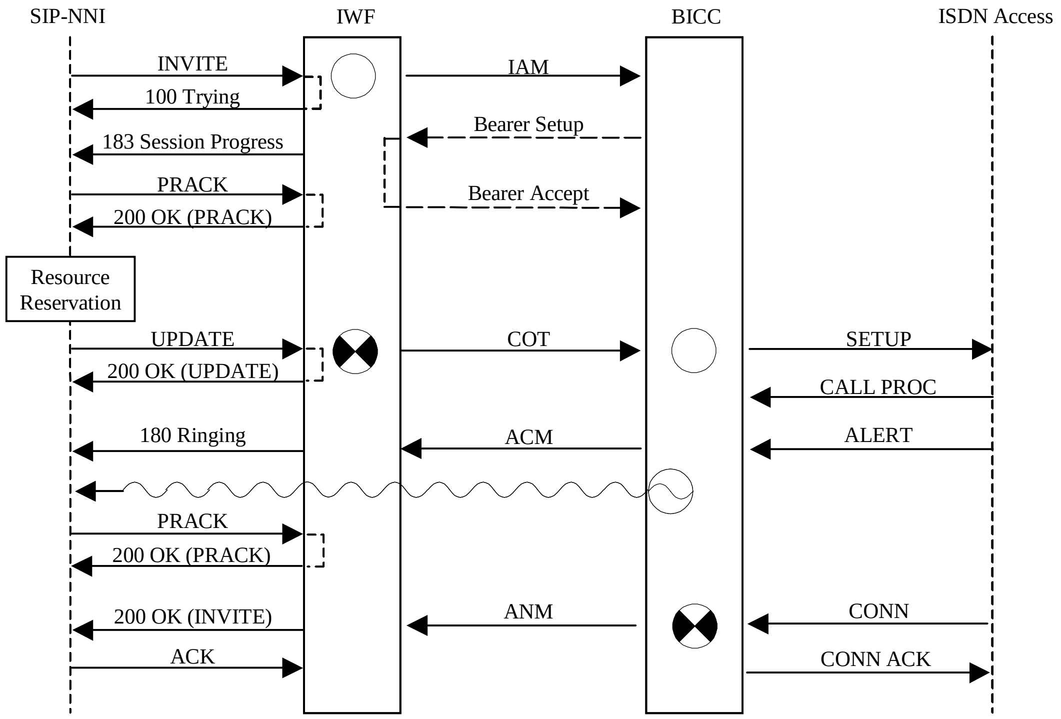


Figure A.4/Q.1912.SIP - Successful basic call setup from SIP to BICC

A.5.2.2 Unsuccessful call set-up procedures/call flow diagrams for basic call control

FFS

A.5.2.3 Release procedures/call flow diagrams for basic call control

A.5.2.3.1 Normal call release procedure, backward bearer set-up

Figure A.5 shows a normal call release procedure initiated from the SIP side of the call. This call flow assumes that no resource reservation teardown signalling is required on the SIP side.

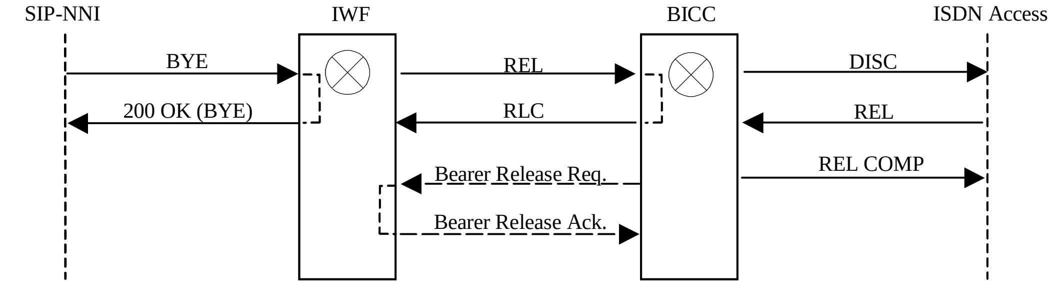


Figure A.5/Q.1912.SIP – Normal call release from SIP to BICC

A.5.2.4 Simple segmentation procedures/call flow diagrams for basic call control

FFS

APPENDIX-B

APPENDIX-B Interworking scenarios between SIP and ISUP

B.1 Scope

B.2 Definitions

B.3 Abbreviations

B.4 Methodology

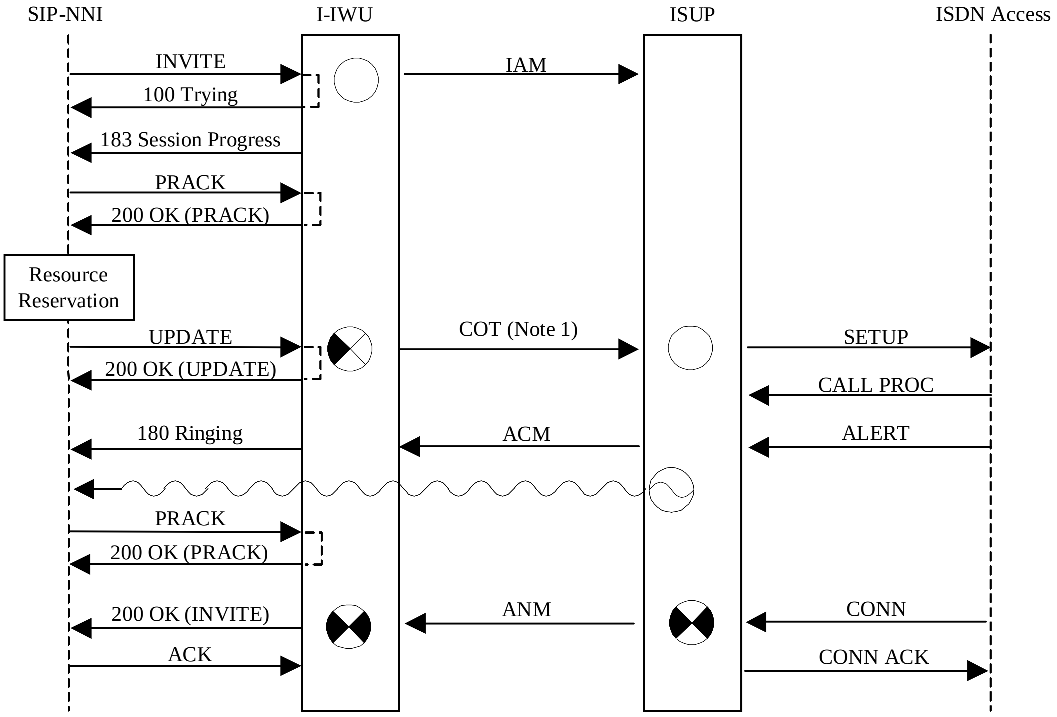
B.5 Interworking of SIP Access to ISUP

B.5.1 Incoming Call – SIP to ISUP

B.5.1.1 Successful Call Set-Up Procedures/Call Flow Diagrams for Basic Call Control

B.5.1.1.1 SIP Preconditions Used

Figure B.5~~Figure B.3Figure B.3~~ shows the sequence of messages for successful call set-up for an outgoing call from SIP to ISUP. In this sequence, the SIP side indicates mandatory local resource reservation (such as sendrecv) in the INVITE. The IAM (with 'continuity check performed on previous circuit' or 'continuity check required on this circuit' indication) is sent by the IWU once the initial INVITE is received, and a COT message (with 'continuity check successful' indication) is sent once the SIP side has reserved resources for the call (confirmed in the UPDATE).



Note 1 – This message is optional, depending on the indication in the IAM.

Figure B.5~~3~~/Q.1912.SIP - Successful Basic Call Set-Up from SIP to ISUP (SIP Preconditions and Continuity Check Protocol Used)

B.5.1.1.2 SIP Preconditions Not Used

Figure B.7~~Figure B.4Figure B.4~~ shows the sequence of messages for successful call set-up for an outgoing call from SIP to ISUP. The IAM (with 'continuity check not required' indication) is sent by the IWU once the initial INVITE is received.

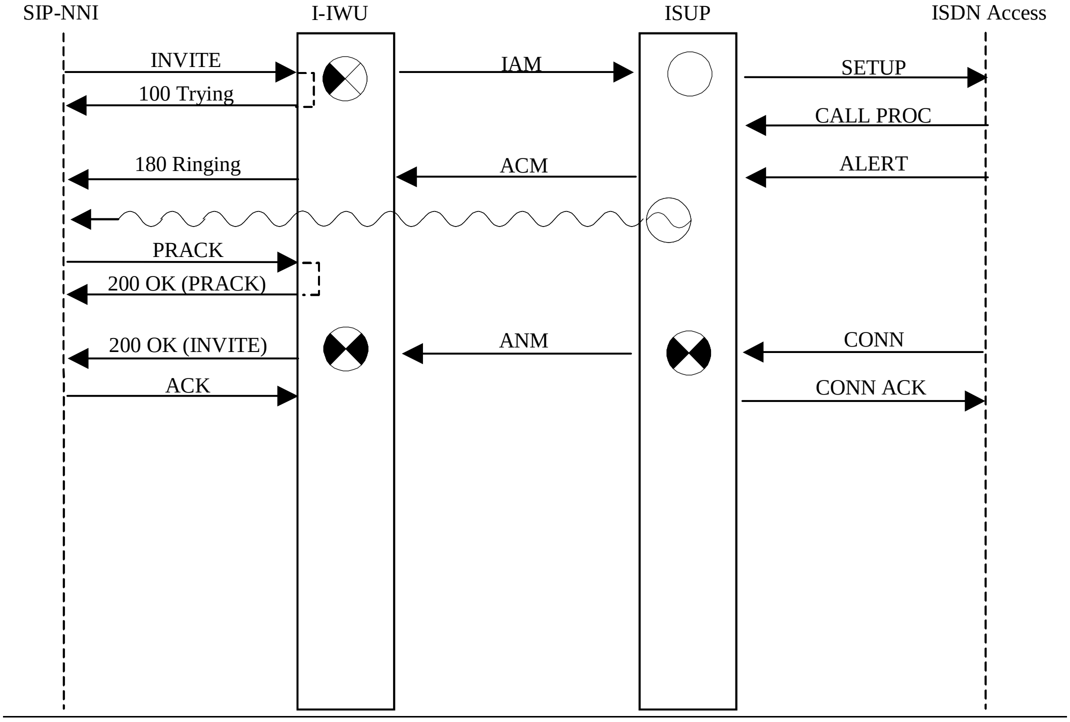
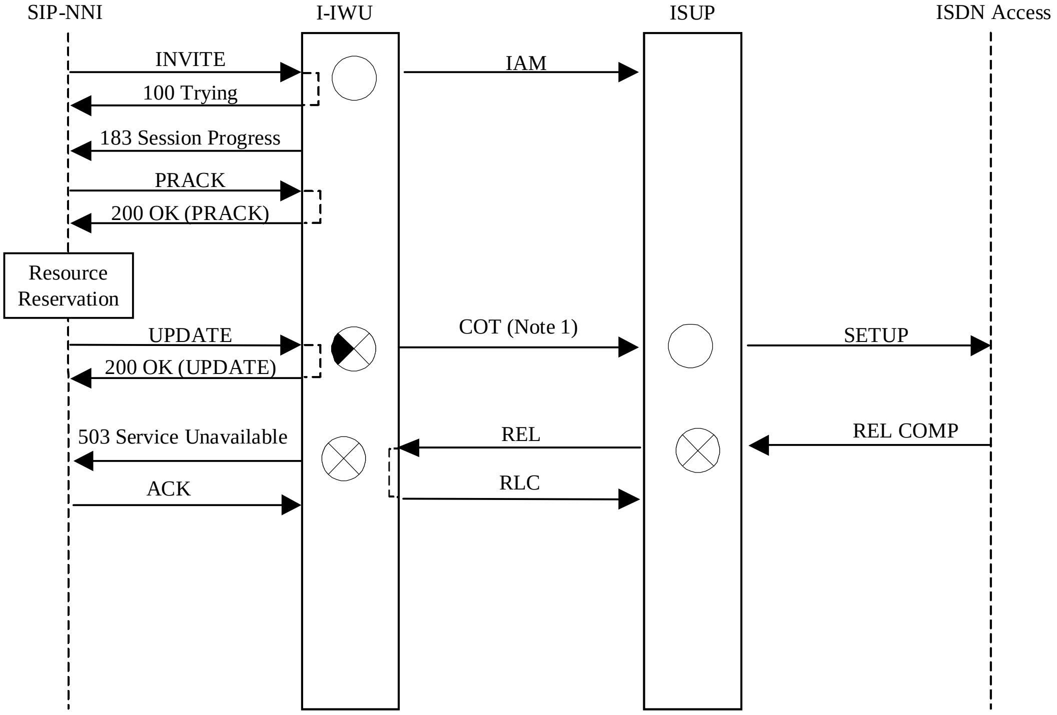


Figure B.74/Q.1912.SIP – Successful Basic Call Set-Up from SIP to ISUP (SIP Preconditions and Continuity Check Protocol Not Used)

B.5.1.2 Unsuccessful Call Set-Up Procedures/Call Flow Diagrams for Basic Call Control

Figure B.9~~Figure B.5Figure B.5~~ shows the sequence of messages for unsuccessful call set-up for an outgoing call from SIP to ISUP. In this sequence, the IWU sends the 503 Service Unavailable message upon reception of the REL message (with Cause Value No. 34 (resource unavailable)) from the ISUP side of the call



Note 1 – This message is optional, depending on the indication in the IAM.

Figure B.9~~5~~/Q.1912.SIP - Unsuccessful Basic Call Set-Up from SIP to ISUP

B.5.1.3 Normal Call Release Procedure

Figure B.12~~Figure B.7Figure B.7~~ shows a normal call release procedure initiated from the SIP side of the call. This call flow assumes that no resource reservation teardown signaling is required on the SIP side.

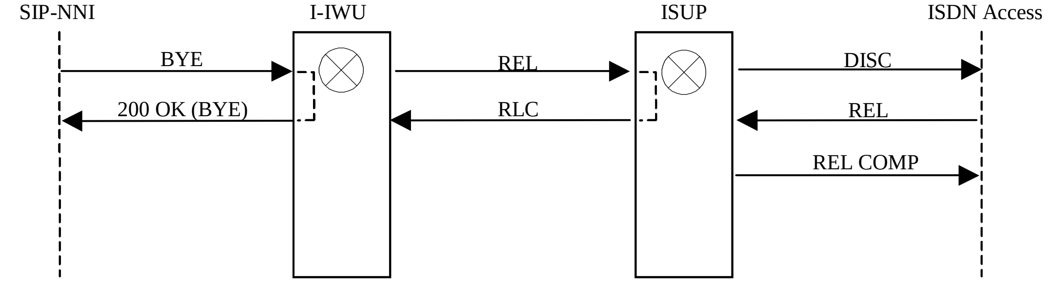


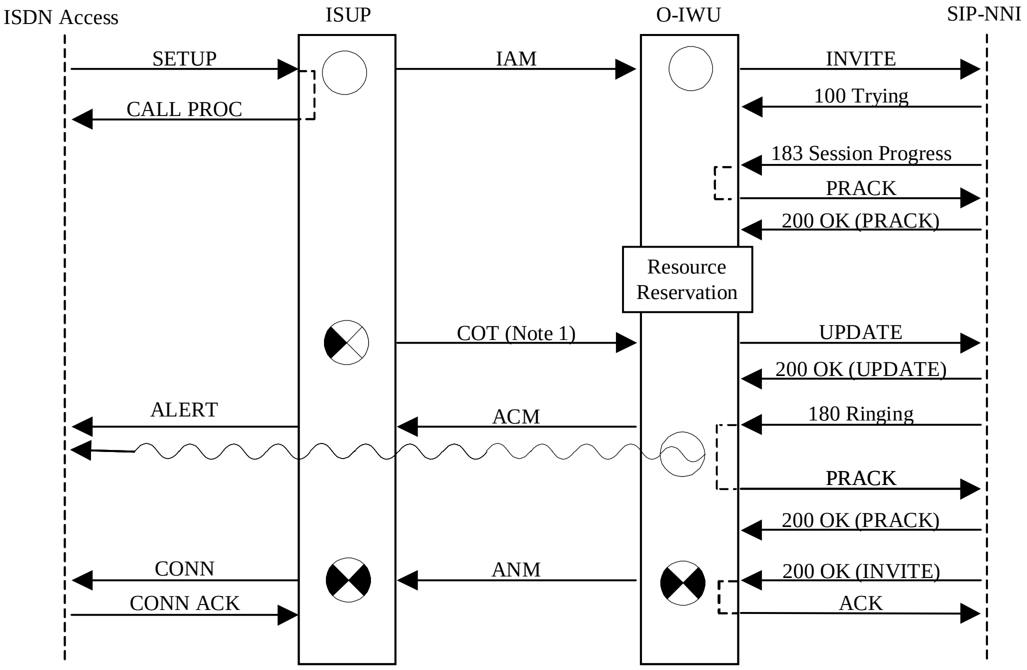
Figure B.6/Q.1912.SIP - Normal Call Release from SIP to ISUP

B.5.2 Outgoing Call – ISUP to SIP

B.5.2.1 Successful Call Set-Up Procedures/Call Flow Diagrams for Basic Call Control

B.5.2.1.1 SIP Preconditions Used

Figure B.12~~Figure B.7Figure B.7~~ shows a sequence of messages for successful call set-up for an incoming call from ISUP to SIP. In this example, the IWU indicates mandatory local sendrecv preconditions in the INVITE. The IWU then sends the UPDATE message upon reception of a COT message (if the IAM indicated 'continuity check performed on previous circuit' or 'continuity check required on this circuit') and completion of any local resource reservation. The UPDATE message will confirm that the local preconditions have been met.



Note 1 – This message is optional, depending on the indication in the IAM.

Figure B.12~~7~~/Q.1912.SIP - Successful Basic Call Set-Up from ISUP to SIP (SIP Preconditions and Continuity Check Protocol Used)

B.5.2.1.2 SIP Preconditions Not Used

Figure B.8~~Figure B.8Figure B.8~~ shows a sequence of messages for successful call set-up for an incoming call from ISUP to SIP. In this example, the IWU sends the INVITE message upon reception of an IAM (since the IAM indicated 'continuity check not required').

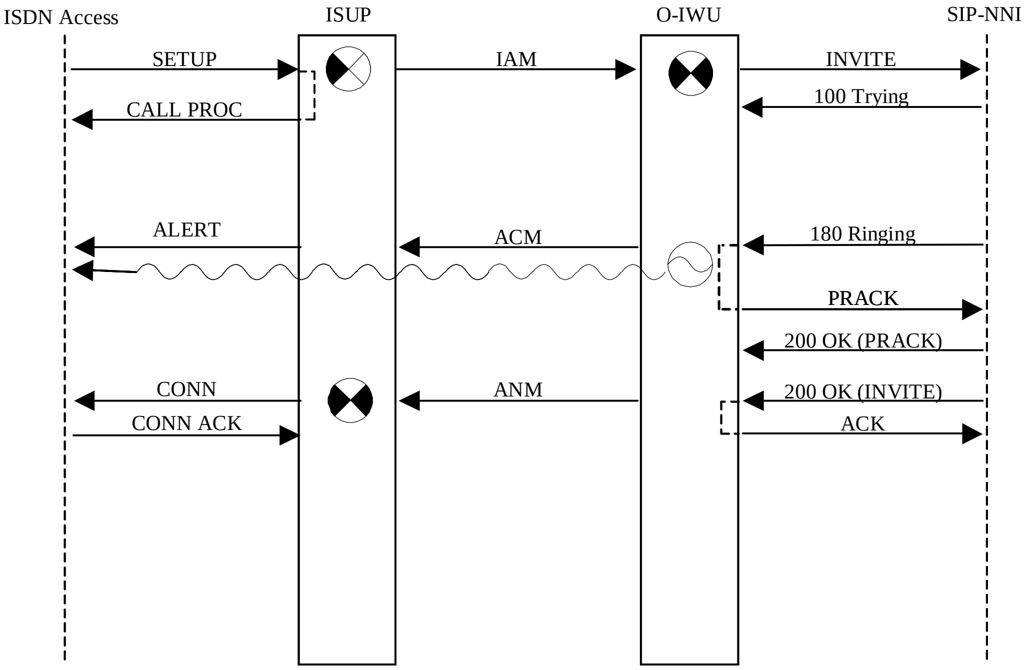


Figure B.8/Q.1912.SIP - Successful Basic Call Set-Up from ISUP to SIP (SIP Preconditions and Continuity Check Protocol Not Used)

B.2.2.2 Unsuccessful Call Set-Up Procedures/Call Flow Diagrams for Basic Call Control

Figure B.10~~Figure B.9Figure B.9~~ shows a sequence of messages for unsuccessful call set-up for an incoming call from ISUP to SIP. In this example, the IWU sends the REL message upon reception of the 484 Address Incomplete message from the SIP side of the call.

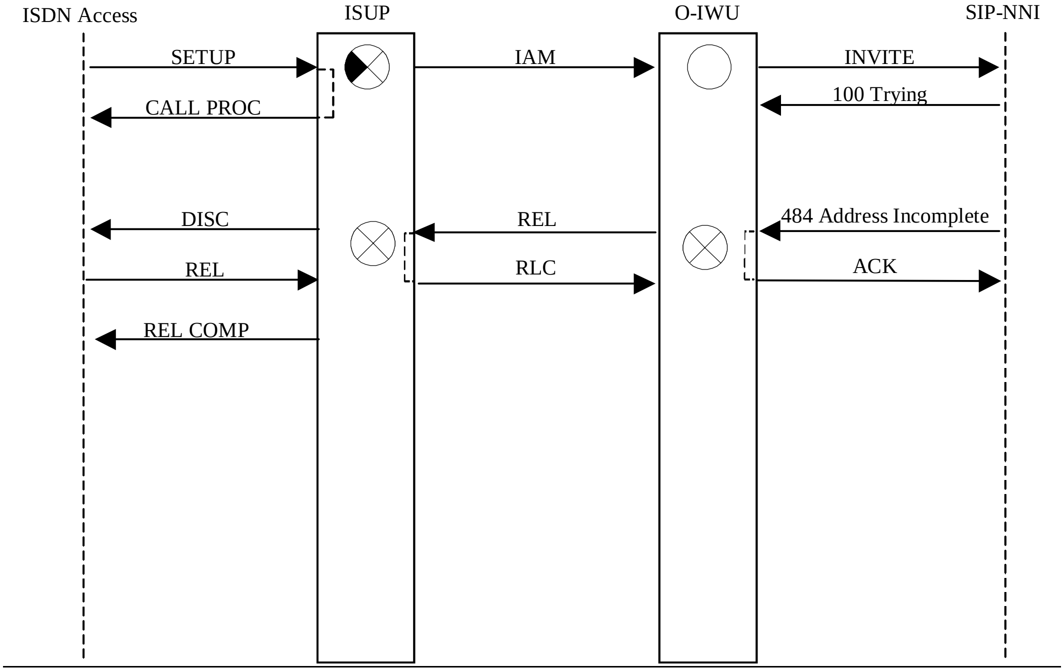


Figure B.10~~9~~/Q.1912.SIP - Unsuccessful Basic Call Set-Up from ISUP to SIP

B.5.2.3 Normal Call Release Procedure

Figure B.12~~Figure B.10Figure B.10~~ shows a normal call release procedure initiated from the ISUP side of the call. This call flow assumes that no resource reservation teardown signaling is required on the SIP side of the call.

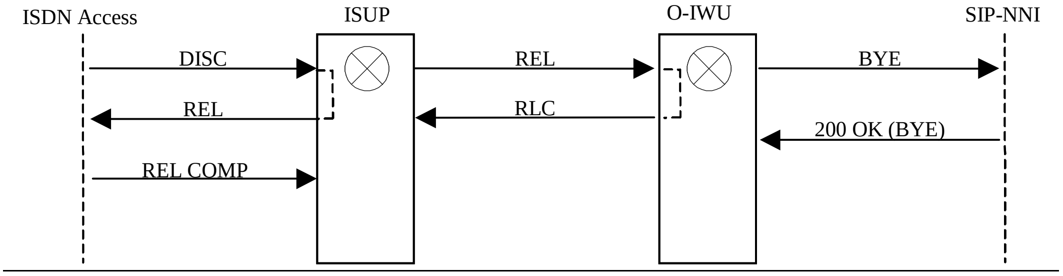


Figure B.12~~10~~//Q.1912.SIP - Normal Call Release from ISUP to SIP

~~APPENDIX 1~~

~~Appendix 1 Capabilities and Services Supported by ISUP and BICC~~

~~Editor's Note: The capabilities and services supported by ISUP and BICC have been documented in various normative ITU-T Recommendations. They are listed in this appendix to aid the editor tracking the interworking specification. This appendix will be removed prior to determination.~~

~~The BICC/ISUP protocols provide a large set of signalling capabilities to support a diverse set of PSTN/ISDN/IN services. These signalling capabilities or procedures are in turn supported by sets of signalling information, which may be encoded in a number of messages, parameters and indicators. Grouping the signalling information by the signalling procedures provide the initial step to determine if the signalling information need to interwork across different signalling system. See Table 11 for the list of services or procedures to be used in this Recommendation for grouping the BICC/ISUP signalling information. The capabilities acronyms will be used to tag various signalling information under consideration for interworking.~~

~~In addition to defining supported capability sets, another factor of determining the relevance of signalling information for interworking depends on the network architecture where the interworking nodes locate. The main text of this Recommendation (Q.1912.SIP) documents the interworking for "Profile-A" presented in the TRQ.BICCSIP. The scope of Profile-A is limited to architecture of interconnecting the BICC/ISUP network with the SIP network serving as an access network for terminal end-points. It should be possible to provide additional interworking specification annexes to the main text of this Recommendation as more service profiles are studied for various architectural applications.~~

~~Table 11: Listing of Capabilities Supported by BICC/ISUP~~

The whole Appendix C is a new Appendix to Q.1912.SIP.

APPENDIX C

APPENDIX-C Interworking scenarios between SIP-I and ISUP

1 General

1.1 Scope

This appendix defines some typical interworking scenarios between ISUP and SIP-I. ISDN Access flows are included for informational purposes only. The IWU knows that it operates in trunking mode through reconfiguration or analysis of received signalling information.

1.2 Methodology

Call flow or "arrow" diagrams are provided to show the temporal relationships between signalling messages during execution of a call control procedure. The general format of an arrow diagram is shown in Figure 1. The main part of the Recommendation takes precedence over this appendix.

1.3 Symbols and abbreviations

The vertical boxes represent originating/terminating exchanges and outgoing/incoming interworking service nodes. The intermediate exchange presentation is omitted as it has no impact on the call flows.

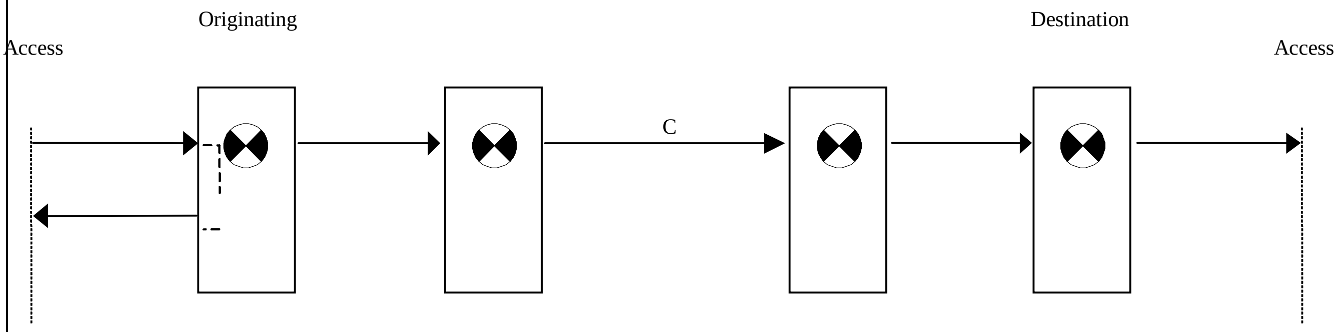
The vertical dashed lines represent the access interface. Each access interface supports a single access type: ISDN or non-ISDN.

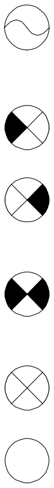
Solid horizontal arrows represent signalling messages and indicate their direction of propagation, i.e. to or from the interworking function. The interaction of messages shown along the vertical represent increasing time in the downward direction. All events on the same vertical line are related, e.g. an incoming message causes voice-path connections and triggers an outgoing message. Events on different vertical lines are not related unless connected by dashed lines. A dashed line indicates that an incoming message may trigger an event at a later time.

Wavy horizontal arrows (~~>) represent tones or announcements sent in-band.

Timers are represented as vertical arrows.

For call control the following symbols are used within the vertical boxes to indicate the relationship between the incoming and outgoing messages and the call control action taken.





A, B, C, D, E and F

[G, H]

i, j, k and l

X and Y

Figure 1/Q.1912.SIP – Example of a call flow or "arrow" diagram

2 Interworking of ISUP over SIP-I

Subclauses 2.1 and 2.2 contain information relevant to basic call control. The call flow diagrams are divided into functional subclauses:

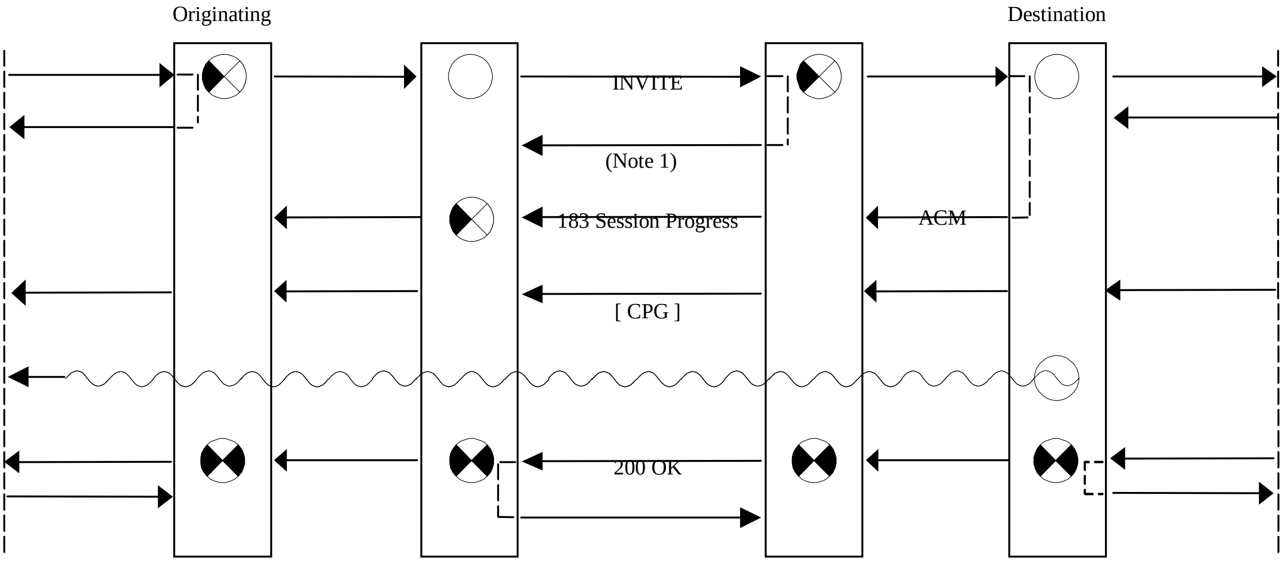
- successful call set-up procedures;
- unsuccessful call set-up procedures;
- release procedures;
- suspend/resume procedures

2.1 Successful call set-up procedures/call flow diagrams for basic call control

2.1.1 En bloc, non automatic answering terminal sending of address complete independent from access

See 2.1/Q.764 and xyz/RFC 3261

Figure 2 shows the sequence of messages for successful call set-up for an incoming ISUP call over SIP-I. At the I-ISN the ACM message is mapped and encapsulated to 183 provisional response preserving the ISUP signalling transparency. The O-IWU performs the through-connection of the path in the backward direction after the receipt of SDP information in 183 response.



NOTE 1 – The generation of the 100 (Trying) response is necessary if the I-IWU knows that it will not generate a provisional or final response within 200 ms.

NOTE 2 – The method of ACM generating independent of access is termed *Early* ACM. The ACM is independently generated at the destination exchange with the following parameters: called party satus = no indication; ISDN Access Indicator = ISDN access.

/Q.1912.SIP – En bloc, non-automatic answering terminal sending of address complete independent from access

For detailed messages and parameter mapping, refer to:

– IAM message – subclauses xyz and xyz

– ACM message – subclauses xyz and xyz

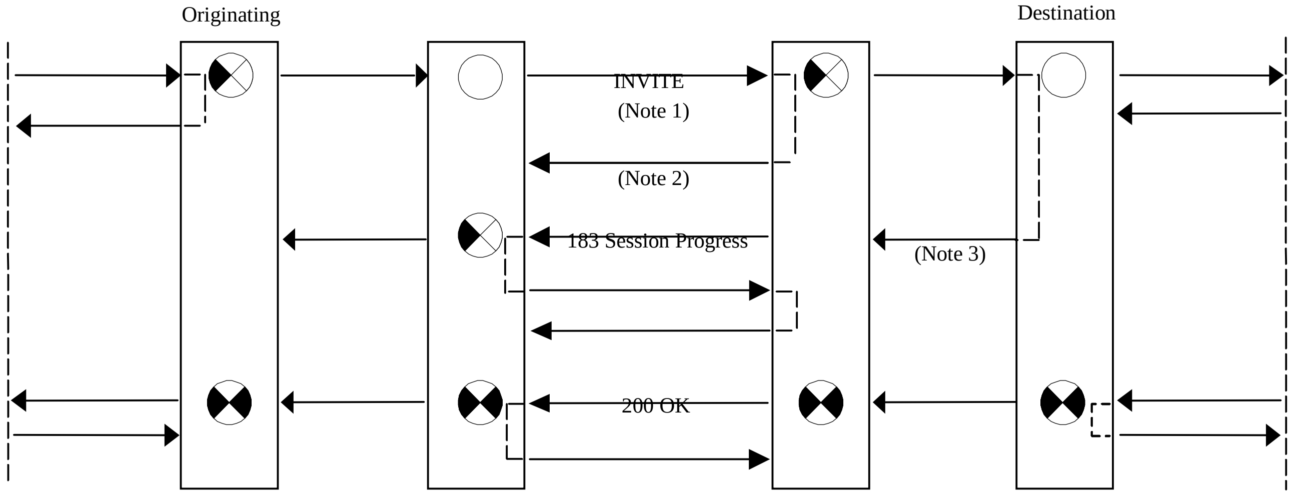
– CPG message – subclauses xyz and xyz

– ANM message – subclauses xyz and xyz

2.1.2 En bloc, automatic answering terminal sending of address complete independent from access

See 2.1/Q.764 and xyz/RFC 3261

Figure 3 shows the sequence of messages for successful call set-up for an incoming ISUP call over SIP-I. The O-IWU indicates the support of reliability of provisional responses in the INVITE. At the I-ISN the ACM message is mapped and encapsulated to 183 response preserving the ISUP signalling transparency. The O-IWU confirms the receipt of provisional response with the PRACK request. The O-IWU performs the through-connection of the path in the backward direction after the receipt of SDP information in 183 response.



NOTE 1 – INVITE contains the Supported header field with the option tag 100rel

NOTE 2 – The generation of the 100 (Trying) response is necessary if the I-IWU knows that it will not generate a provisional or final response within 200 ms.

NOTE 3 – The ACM is generated with following parameters: called party satus = no indication; ISDN Access Indicator =ISDN access.

/Q.1912.SIP – En bloc, automatic answering terminal sending of address complete independent from access

For detailed messages and parameter mapping, refer to:

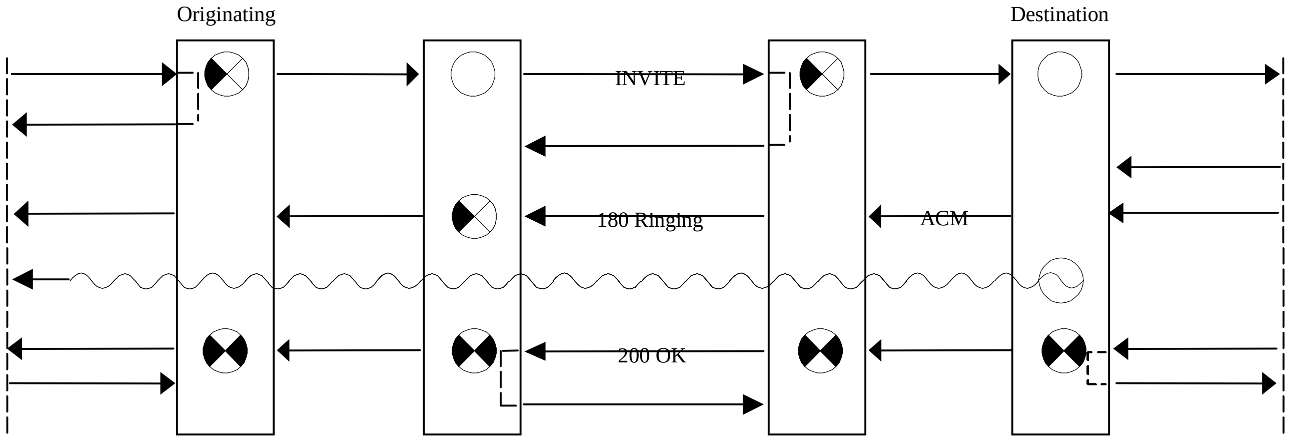
- IAM message – subclauses xyz and xyz
- ACM message – subclauses xyz and xyz
- ANM message – subclauses xyz and xyz

2.1.3 En bloc, non-automatic answering terminal

See 2.1/Q.764 and xyz/RFC 3261

NOTE – Termed *Late* ACM.

Figure 4 shows the sequence of messages for successful call set-up for an incoming ISUP call over SIP-I. The O-IWU performs the through-connection of the path in the backward direction after the receipt of SDP information in 180 response.



NOTE 1 – The generation of the 100 (Trying) response is necessary if the I-IWU knows that it will not generate a provisional or final response within 200 ms.

NOTE 2 – The ACM is generated with following parameters: called party satus = subscriber free; ISDN Access Indicator = ISDN access

/Q.1912.SIP – En bloc, non-automatic answering terminal

For detailed messages and parameter mapping, refer to:

– IAM message – subclauses xyz and xyz

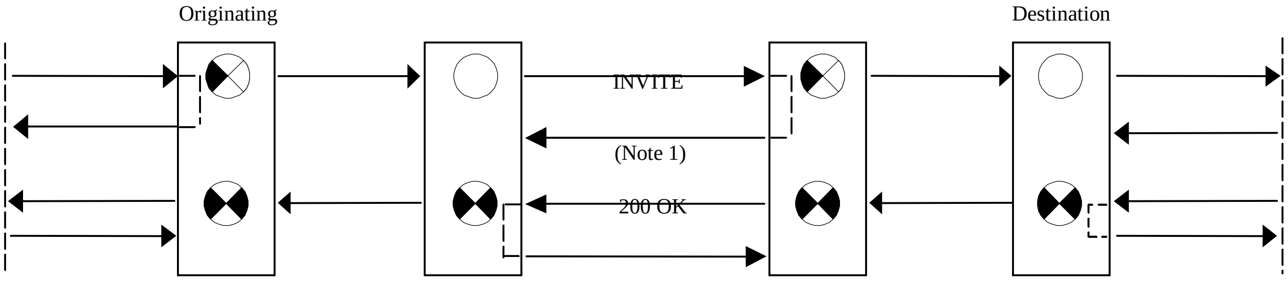
– ACM message – subclauses xyz and xyz

– ANM message – subclauses xyz and xyz

2.1.4 En bloc, automatic answering terminal

See 2.1/Q.764 and xyz/RFC 3261

Figure 5 shows the sequence of messages for successful call set-up for an incoming ISUP call over SIP-I. The I-ISN sends the 200 OK response on the receipt of CONNECT message containing the address complete and the connect indication. Both IWUs perform the through-connection of the path in both directions on the receipt of connect indication.



NOTE 1 – The generation of the 100 (Trying) response is necessary if the I-IWU knows that it will not generate a provisional or final response within 200 ms.

/Q.1912.SIP – En bloc, automatic answering terminal

For detailed messages and parameter mapping, refer to:

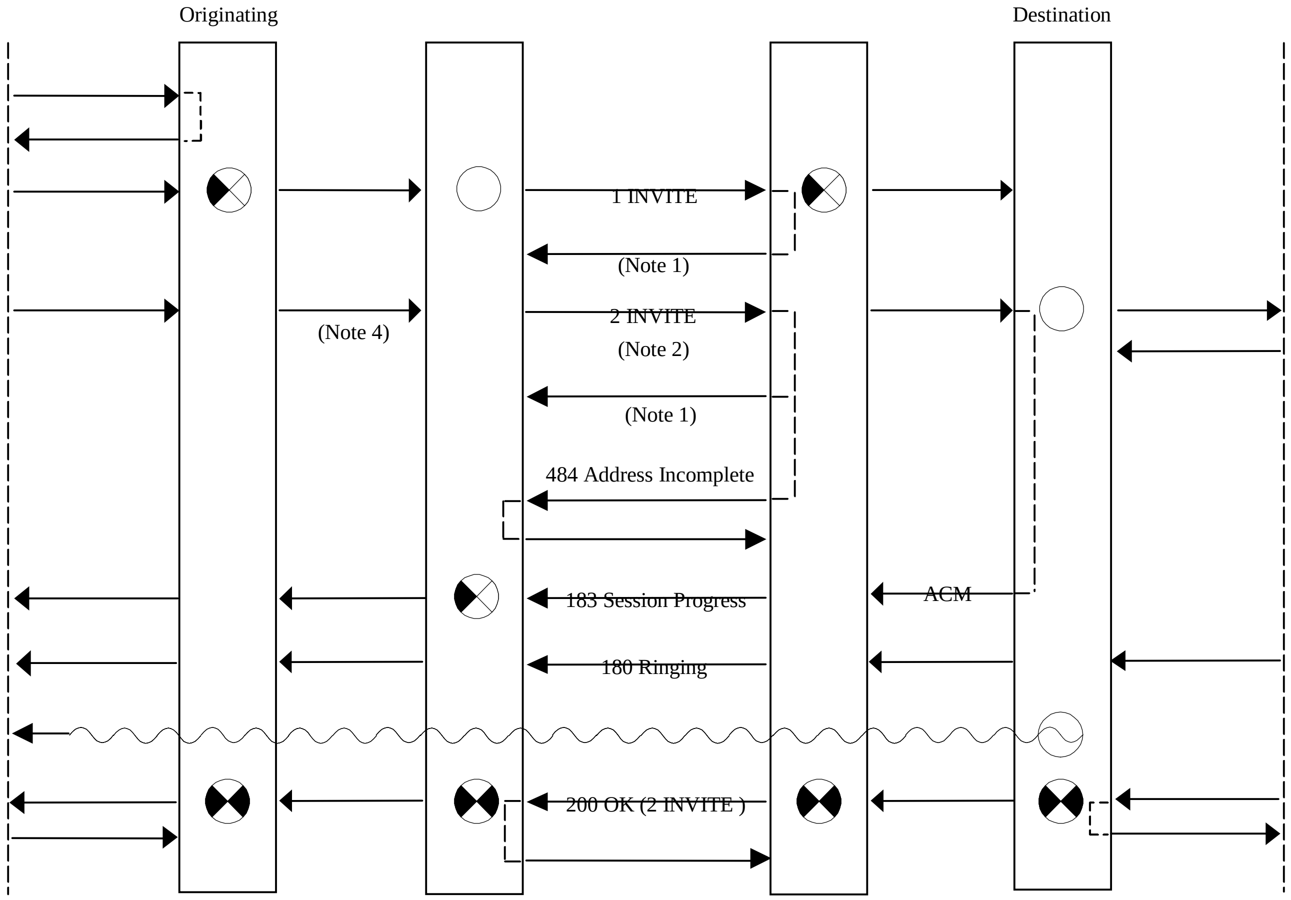
– IAM message – subclauses xyz and xyz

– CON message – subclauses xyz and xyz

2.1.5 Overlap addressing, originating, intermediate and terminating network , non-automatic answering terminal

See 2.1/Q.764 and xyz/RFC 3261

Figure 6 shows the sequence of messages when overlap sending is in use at the incoming , transit and destination network. In this case the ACM through the network informs the originating exchange that enough address information has been received, and the exchange can therefore indicate call proceeding to the calling party. The O-IWU sends the subsequent INVITE requests on the receipt of SAM messages. are At the I-ISN the ACM message is mapped and encapsulated to



NOTE 1 – The generation of the 100 (Trying) response is necessary if the I-IWU knows that it will not generate a provisional or final response within 200 ms.

NOTE 2 – The subsequent INVITE is generated by O-IWU with the same Call-ID and the same From header field including the tag as the first INVITE sent, but has an updated Request-URI. For details see xyz/Q.1912.SIP.

NOTE 3 – The ACM is independently generated at the destination exchange with the following parameters: called party satus = no indication; ISDN Access Indicator = ISDN access

NOTE 5 – The number of SAM messages shown for example only. In practice the number may be zero or more.

183 response preserving the ISUP signalling transparency. ACM The O-IWU performs the through-connection of the path in the backward direction after the receipt of SDP information in 183 response.

/Q.1912.SIP – Overlap addressing, originating access and network, non-automatic answering terminal

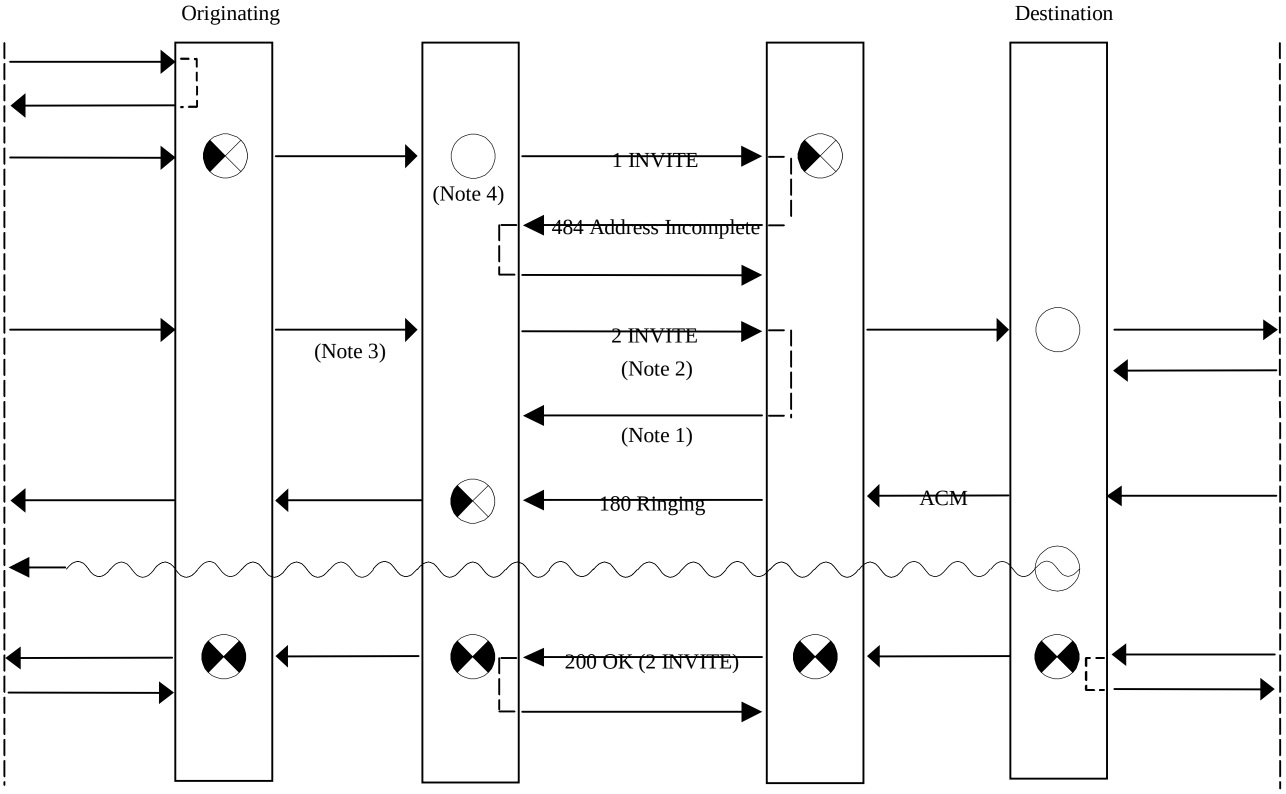
For detailed messages and parameter mapping, refer to:

- IAM message – subclauses xyz and xyz
- SAM message – subclauses xyz and xyz
- ACM message – subclauses xyz and xyz
- CPG message – subclauses xyz and xyz
- ANM message – subclauses xyz and xyz

2.1.7 Overlap addressing, originating and intermediate network only

See 2.1/Q.764 and xyz/RFC 3261

Figure 7 shows the sequence of messages when overlap sending is in use at the incoming and transit network only. The O-IWU sends the subsequent INVITE requests on the receipt of SAM messages. The ACM message contains the address complete and “subscriber free” indication and is mapped and encapsulated in to the 180 response at the I-IWU. The O-IWU performs the through-connection of the path in the backward direction after the receipt of SDP information in 180 response.



/Q.1912.SIP – Overlap addressing, originating and transit network only

For detailed messages and parameter mapping, refer to:

– IAM message – subclauses xyz and xyz

– SAM message – subclauses xyz and xyz

– ACM message – subclauses xyz and xyz

– ANM message – subclauses xyz and xyz

NOTE 1 – The generation of the 100 (Trying) response is necessary if the I-IWU knows that it will not generate a provisional or final response within 200 ms.

NOTE 2 – The subsequent INVITE is generated by O-IWU with the same Call-ID and the same From header field including the tag as the first INVITE sent, but has an updated Request-URI. For details see xyz/Q.1912.SIP.

NOTE 3 – The number of SAM messages shown for example only. In practice the number may be zero or more.

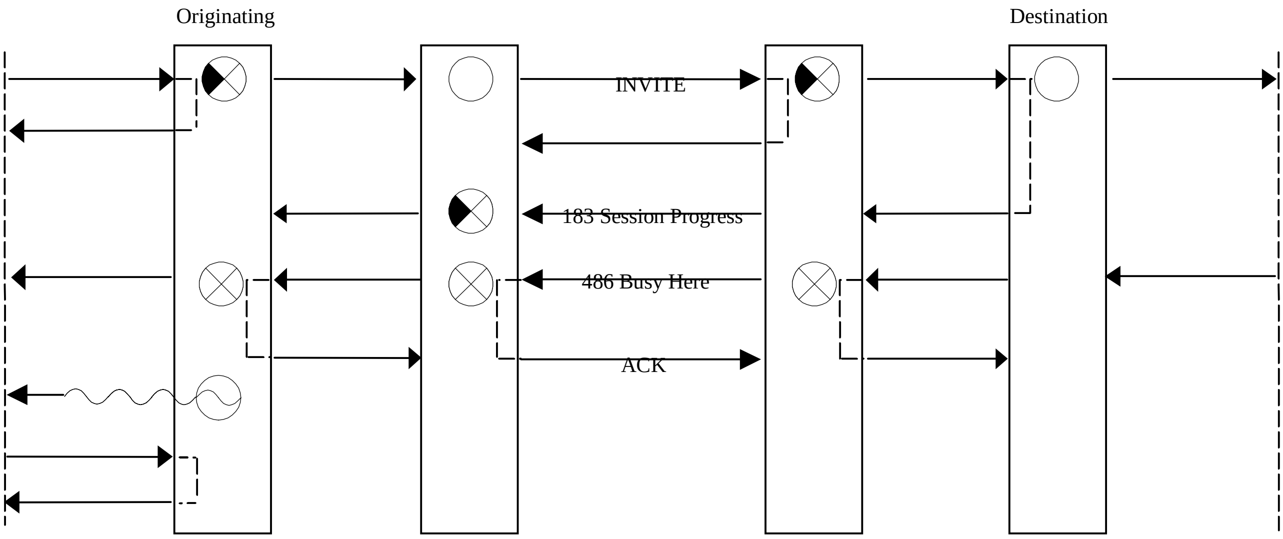
NOTE 4 – The timer Txx is started each time the INVITE is sent, this prevents the call from being released by the receipt of 484 Address Incomplete.

2.2 Unsuccessful cal set-up procedures/call flow diagrams for basic call control

2.2.1 Tone/announcement applied at the originating exchange

See 2.1/Q.764 and xyz/RFC 3261

Figure 8 shows the unsuccessful call set-up procedure where tones or announcements are generated in the originating exchange. The REL message is mapped and encapsulated into the appropriate SIP unsuccessful response status code depending on the cause value.



NOTE 1 – The generation of the 100 (Trying) response is necessary if the I-IWU knows that it will not generate a provisional or final response within 200 ms.

NOTE 2 – If *Early* ACM is used, the ACM is independently generated with the following parameters: called party satus = no indication; ISDN Access Indicator = ISDN access

NOTE 3 – See the table/section xyz for the mapping of ISUP release causes to the SIP error responses

NOTE 4 – Timer T306 is started after tone is sent in the Q.931 protocol block.

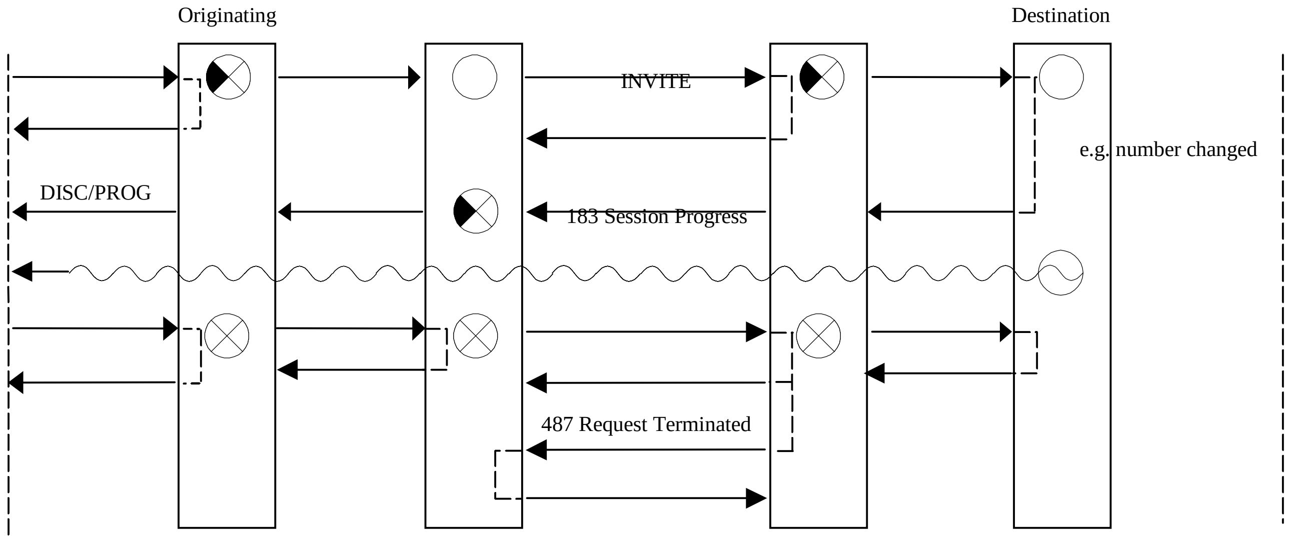
/Q.1912.SIP – Unsuccessful cal set-up, point-to-point data link, ACM generated independent of access

For detailed messages and parameter mapping, refer to:

- IAM message – subclauses xyz and xyz
- ACM message – subclauses xyz and xyz
- REL message – subclauses xyz and xyz

2.2.2 Tone/announcement applied by at the destination exchange

See 2.1/Q.764 and xyz/RFC 3261



NOTE 1 – The generation of the 100 (Trying) response is necessary if the I-IWU knows that it will not generate a provisional or final response within 200 ms.

NOTE 2 – The ACM is not mapped from a message from the destination user. It is independently generated at the destination exchange.

NOTE 3 – If tones/announcements are applied, the DISCONNECT message containing progress indicator No. 8 may be mapped from the ACM message with an appropriate cause indicators parameter. As an alternative, a PROGRESS message may also be sent containing progress indicator No. 8 when the cause indicators parameter is not contained in an ACM message.

NOTE 4 – Customised announcements can only be provided by the destination exchange

Figure 9 shows an unsuccessful call set-up where certain tones and announcements can only be generated in the destination exchange or (intermediate exchange) during call establishment. The REL message is mapped into the CANCLE request to terminate SIP session set-up procedure.

/Q.1912.SIP – Unsuccessful call set-up tone/announcement applied by destination exchange

For detailed messages and parameter mapping, refer to:

– IAM message – subclauses xyz and xyz

– ACM message – subclauses xyz and xyz

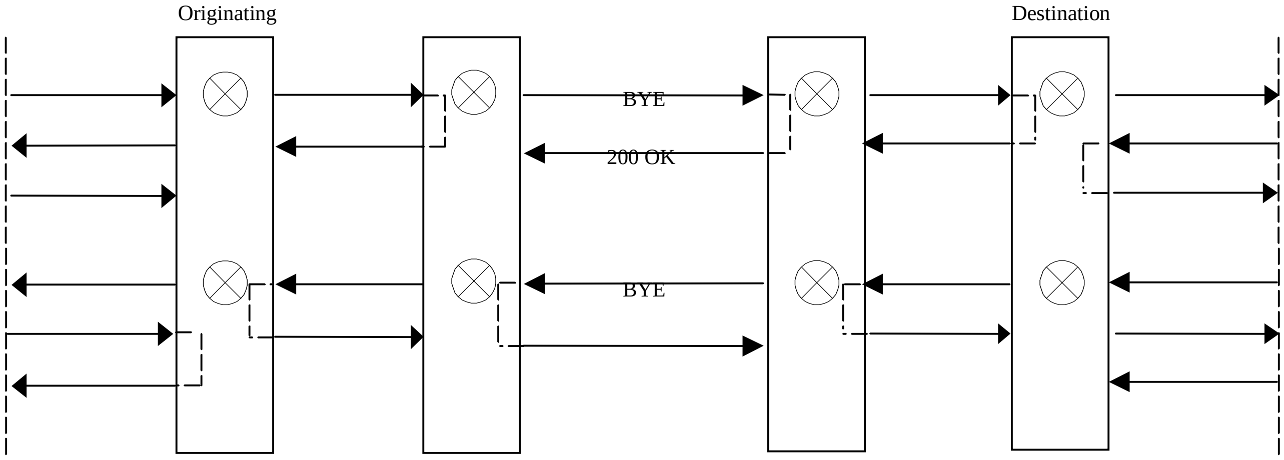
– REL message – subclauses xyz and xyz

2.3 Release procedures/call flow diagrams for basic call control

2.3.1 Normal call release procedure without tone provision

See 2.1/Q.764 and xyz/RFC 3261

Figure 10 shows the normal call release interworking procedures without tone provision. A REL message is mapped and encapsulated into BYE request to preserve the ISUP signalling transparency.



NOTE 1 – This procedure is applicable in those cases where in band tone/announcements are not provided, e.g. 64 kbit/s unrestricted bearer service.

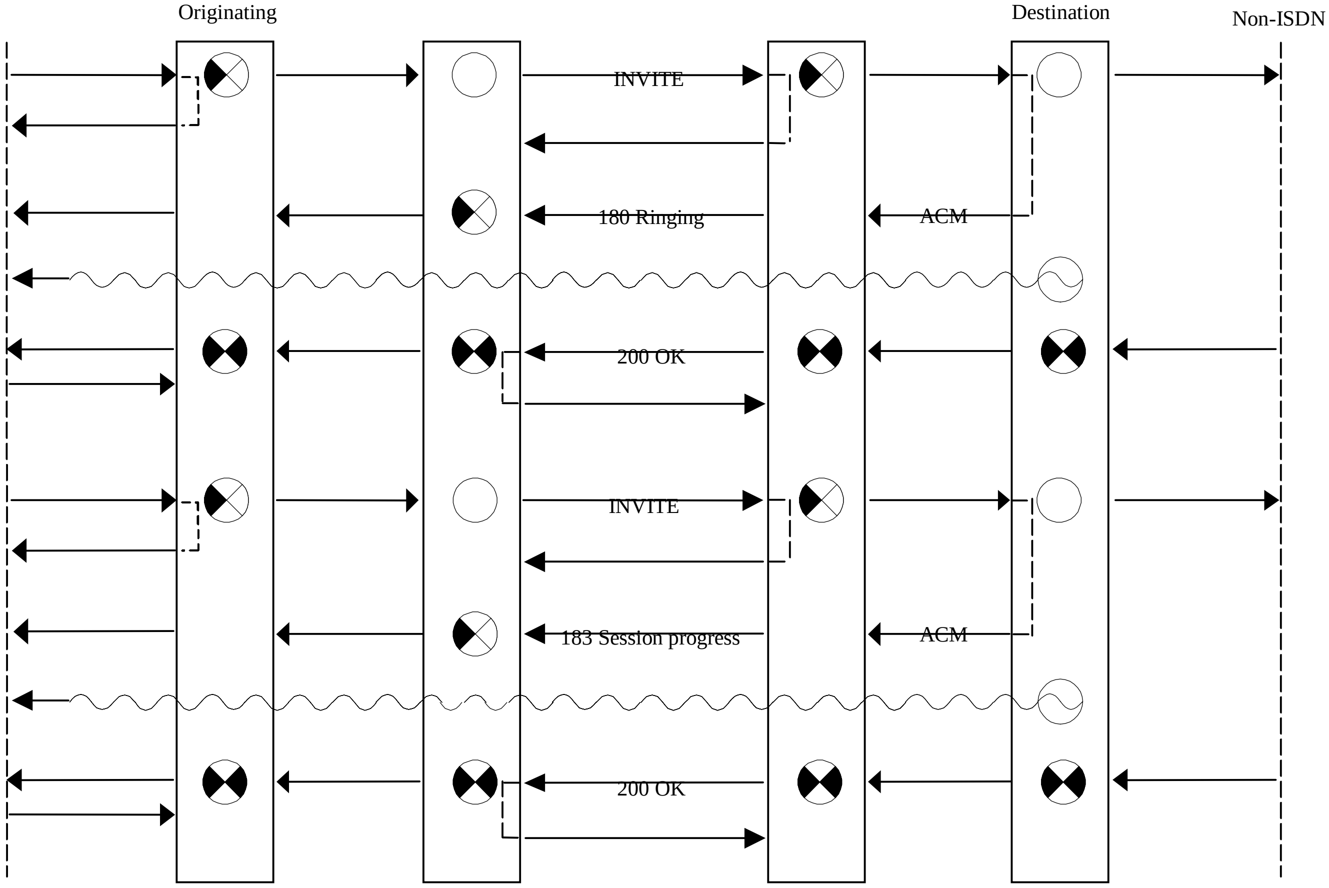
/Q.1912.SIP – Normal call release procedure without tone provision (Note 1)

3.1 Successful call set-up procedures/call flow diagrams

3.1.1 ISDN Access to non-ISDN access

See 2.1/Q.764 and xyz/RFC 3261

Figure 11 shows the sequence of messages for a call from an ISDN access to a non-ISDN access.



NOTE 1 – The generation of the 100 (Trying) response is necessary if the I-IWU knows that it will not generate a provisional or final response within 200 ms.

NOTE 2 – The ACM is independently generated at the destination exchange with the following parameters: called party satus = subscriber free; ISDN Access Indicator = non-ISDN access

NOTE 3 – The ACM is independently generated at the destination exchange with the following parameters: called party satus = no indication; ISDN Access Indicator = non-ISDN access. In order to support user-generated in-band information (e.g from PBX. See 2.1.4.1b/Q.764), the destination exchange may include in the ACM optional backward call indicators = in-band information available and through-connect in the backward direction.

/Q.1912.SIP – ISDN access to non-ISDN access

For detailed messages and parameter mapping, refer to:

– IAM message – subclauses xyz and xyz

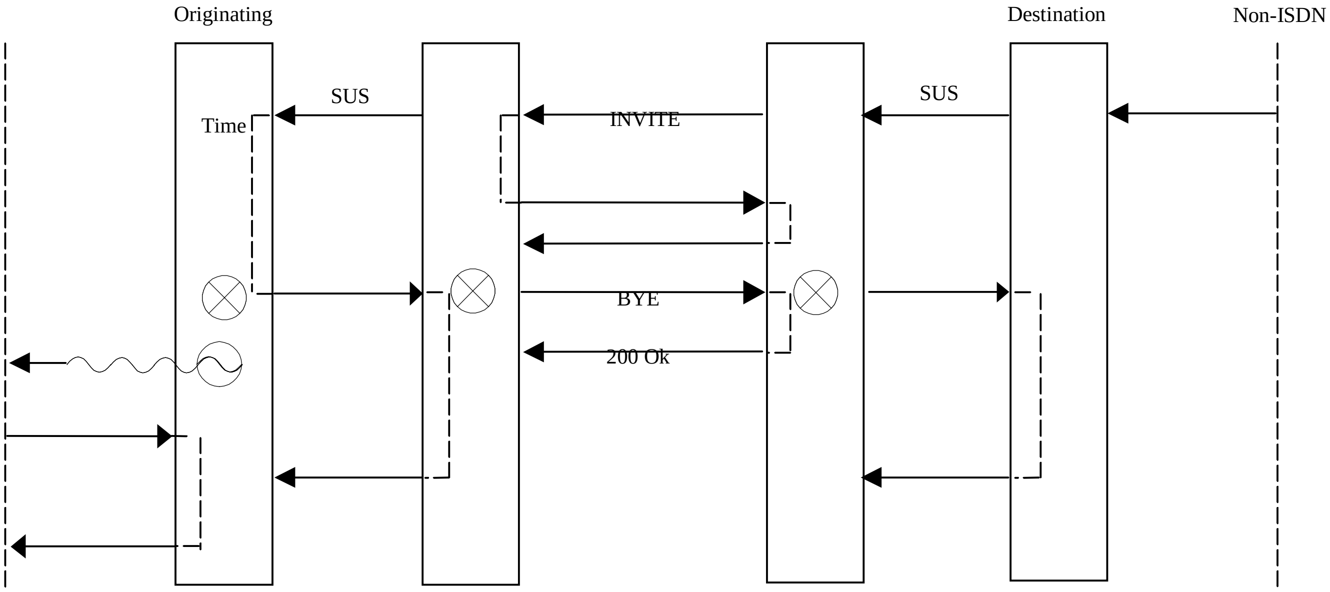
- ACM message – subclauses xyz and xyz
- ANM message – subclauses xyz and xyz

3.2 Release procedures/call flow diagrams

3.2.1 Normal release for ISDN access to non-ISDN access

See 2.1/Q.764 and xyz/RFC 3261

Figure 12 shows the normal call release procedure being initiated from the terminating non-ISDN access by means of a clear-back signal. At the destination exchange, the clear-back signal is mapped into a SUS with suspend/resume indicator (network initiated). At the I-IWU the SUS message is mapped and encapsulated into INVITE request. The originating ISDN exchange start the timer. Upon expiry of the timer, if the originating exchange has not received a RES message, the originating exchange initiates clearing by a REL to the preceding exchange.



NOTE 1 – This procedure is applicable in those cases where in band tone/announcements are not provided, e.g. 64 kbit/s unrestricted bearer service.

NOTE 2 – The transparent transmission of SUS (network initiated)message is possible only in the case of ISUP encapsulation.

/Q.1912.SIP – Normal release procedures for ISDN access to non-ISDN access interworking

For detailed messages and parameter mapping, refer to:

– SUS message – subclauses xyz and xyz

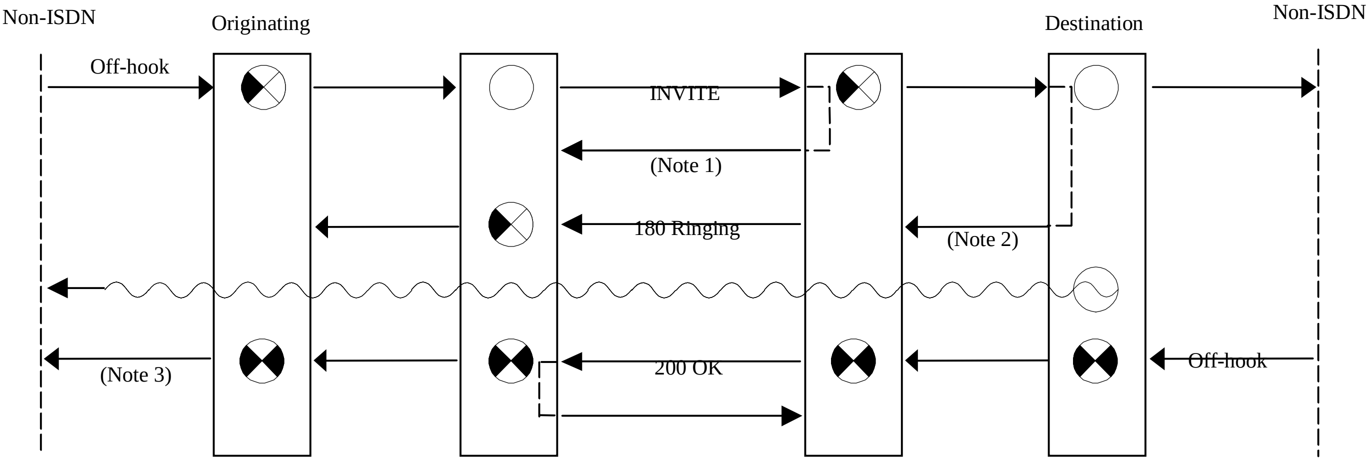
– REL message – subclauses xyz and xyz

4.1 Successful cal set-up procedures/call flow diagrams

4.1.1 Non-ISDN access to non-ISDN access

See 2.1/Q.764 and xyz/RFC 3261

Figure 13 shows the sequence of messages for a call from non-ISDN access to a non-ISDN access. The arrows between the exchanges and non-ISDN accesses indicate signals that may vary with the access protocol.



NOTE 1 – The generation of the 100 (Trying) response is necessary if the I-IWU knows that it will not generate a provisional or final response within 200 ms.

NOTE 2 – The ACM is independently generated at the destination with the following parameters: called party satus = subscriber free; ISDN Access Indicator =non-ISDN access, interworking encountered = no.

NOTE 3 – Conditioinal on type of access

/Q.1912.SIP – Non-ISDN access to non-ISDN access

For detailed messages and parameter mapping, refer to:

– IAM message – subclauses xyz and xyz

– ACM message – subclauses xyz and xyz

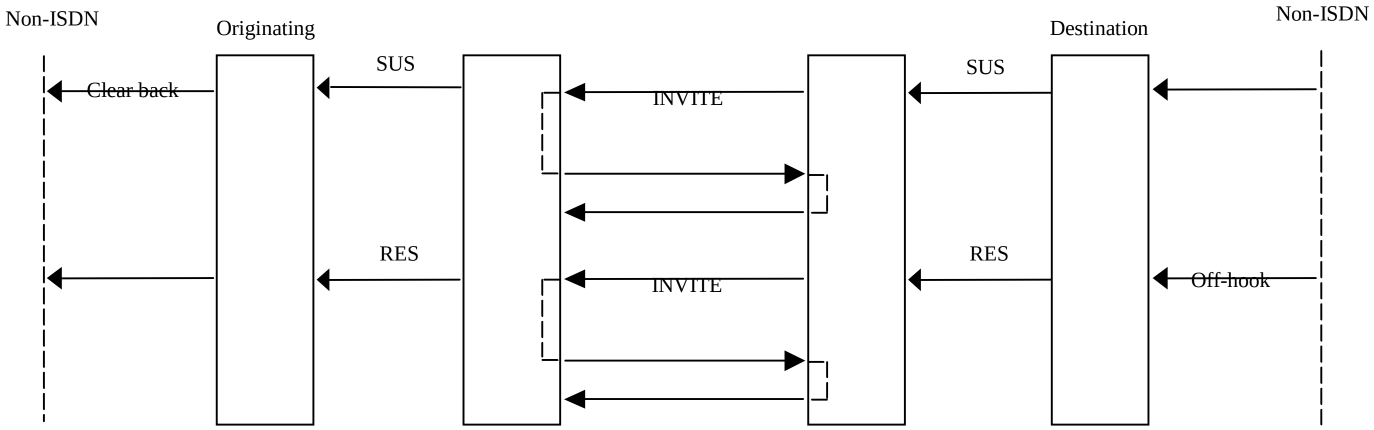
– ANM message – subclauses xyz and xyz

4.1 Suspend/resume procedures/call flow diagrams

4.1.1 Suspend/resume non-ISDN access to non-ISDN access

See 2.1/Q.764 and xyz/RFC 3261

Figure 14 illustrates the suspend and resume procedures for non-ISDN access – non-ISDN access interworking. At the I-IWU the SUS message is mapped and encapsulated into INVITE request. At the O-IWU the RES message is also mapped and encapsulated into INVITE request.



NOTE – Supervision Control in controlling exchange
NOTE 1 – The transparent transmission of SUS/RES (network initiated) messages is possible only in case of ISUP encapsulation.

/Q.1912.SIP – Suspend/resume non-ISDN access to non-ISDN access

For detailed messages and parameter mapping, refer to:

– SUS message – subclauses xyz and xyz

– RES message – subclauses xyz and xyz

INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2001-2004

STUDY GROUP 11

TD 39 (WP 3/11)

Original: English

Question(s): 11,12/11 Geneva, 11 - 22 November 2002

TEMPORARY DOCUMENT

Source: Editor Q.1912.SIP

Title: Draft Q.1912.SIP Annex A: Agreed Output from ITU-T SG11 Meeting, November-2002, Geneva, Switzerland.

Abstract

This TD is Annex A of the agreed output Draft Q.1912.SIP from Question 11/12 in this SG11 Meeting at Geneva (11-22 November 2002). This TD is based on agreements or decisions on Delayed Contributions D.385 to revise the draft Q.1912.SIP (TD WP3/11-16 or OTW-107) output from Ottawa 2002-September meeting. TD WP3/11-16 has been agreed at the beginning of the Question 11 & 12/11 meeting to be the baseline for revision. The clean version of TD WP3/11-16 (without revision marks) was re-distributed as TD3/11-23 in this SG11 Meeting at Geneva (11-22 November 2002).

Contact: Koan S. Chong Tel: +1-732-420-4557
AT&T Fax: +1-732-368-6703
U.S.A. Email: kschong@att.com

ANNEX-A. BICC Specific Interworking for Basic Call

Editor Note: The following text for Annex-A ~~is~~ was originally taken from NWB061. Some key technical issues (e.g., does it require any capability beyond BICC CS2?) still remain that may result in major change to this text. Instead of integrating some of the proposed text into the COMMON PART, they are left in this annex for the ease of further contribution.

~~**Editor Note: Modify section 6.0. Shaded text is the proposed new text.**~~

~~A.1 Interworking Requirements at the I-IWU~~

~~An incoming Interface Serving node entity is used to transport calls originated from a SIP network domain to a BICC or ISUP network domain.~~

~~The "incoming SIP" is qualified as SIP which is used between the Incoming Interface Serving Node and the call originating entity (entities) supported in the SIP network domain. Similarly, the "outgoing BICC/ISUP" is qualified as the BICC or ISUP protocol supported between the Incoming Interface Serving Node and the next-hop entity (entities) in the BICC or ISUP network domain.~~

~~**Editor Note: The following paragraph is proposed by NWB061.**~~

~~In the specific case that the outgoing side of the I-IWU is BICC and that both incoming (SIP) and outgoing BICC sides of the I-IWU use the same media bearer technology with no media intermediary and with Bearer Control Tunnelling on the BICC side, then the I-IWU shall (in addition to the procedures outlined within this section) follow the additional BICC specific procedures outlined in section 2.0 of Annex A.~~

~~**Editor Note: Modify section 7.0. Shaded text is the proposed new text.**~~

~~A.2 Interworking Requirements at the O-IWU~~

~~An Outgoing Interface Serving (O-IWU) Node is used to transport calls from a BICC or ISUP network domain to a SIP network domain.~~

~~By definition, "outgoing SIP" is qualified as SIP which is used between the Outgoing Interface Serving Node and the call terminating entity (entities) in the SIP network domain. Similarly, by definition, "incoming BICC/ISUP" is qualified as the BICC or ISUP protocol supported between the Outgoing Interface Serving Node and the preceding BICC or ISUP entity.~~

~~Editor Note: The following paragraph is proposed by NWB061.~~

~~In the specific case that the incoming side of the O-IWU is BICC and that both outgoing (SIP) and incoming (BICC) sides of the O-IWU use the same media bearer technology with no media intermediary and with Bearer Control Tunnelling on the BICC side then the O-IWU shall (in addition to the procedures outlined within this section) follow the additional BICC specific procedures outlined in section 2.0 of annex A.~~

~~The Outgoing Interface Serving Node receives forward and backward signalling information from the "incoming BICC/ISUP" and "outgoing SIP" sides, respectively. After receiving this signalling information and performing appropriate call/service processing, the Outgoing Interface Serving Node may signal to subsequent SIP nodes or preceding BICC/ISUP entities for further call processing. In order to capture the signalling requirements, this subclause is organized into two subclauses for forward and backward signalling interworking.~~

~~The scope of this section is based on the key assumptions: (a) the Outgoing Interface Serving Node delivers basic calls only; and (b) the calls are delivered to a SIP network domain that does not require equivalent PSTN/ISDN service interworking. The service annexes of this document will cover additional interworking specification related to specific PSTN/ISDN services, which may be required by other interworking network architectures.~~

~~Editor Note: The following text is all new text for Annex A.~~

A.1~~.0~~ Introduction

This annex contains additional inter workings to/from SIP which are particular to the BICC protocol.

A.2~~.0~~ ~~-~~Inter working BICC to/from SIP with common media bearer technology and BICC supports "Bearer Control Tunnelling"

If both BICC and SIP networks use the same media bearer technology~~, there~~, there is no media intermediary and the BICC side uses bearer control tunnelling then the following procedures apply.

For BICC CS2, the only defined Bearer Control Protocol carried by the Bearer Control Tunnelling mechanism is IP BCP (Q.1990). However, the procedures below apply equally to any future Bearer Control Protocol for which interworking with SDP and the SDP offer/answer procedures is defined.

A.2.1 Bearer Control Interworking

A Bearer Control Interworking function is assumed to exist which performs interworking between Bearer Control information (in the BICC Bearer Control Tunnelling Information Element) and SDP message bodies (in SIP messages). For IP BCP, the procedures for this interworking function are defined in section 3.1 of this ~~a~~Annex~~ ?~~.

A.2.1.1 Interworking from SDP offers to BICC Bearer Control Tunnelling information

On receipt of a SIP message containing an SDP offer, the Bearer Control Interworking function is used to generate a Bearer Control Protocol Data Unit for inclusion in a BICC message. The particular BICC message used depends on the procedures defined below.

The procedures of [~~SDP offer/answer~~RFC 3264] are used to determine the SIP ~~message which~~message, which should contain the SDP answer corresponding to this offer. Sending of this message is delayed until a BICC message has been received containing a Bearer Control Product Data Unit as described in 2.1.3.

A.2.1.2 Interworking from SDP answers to BICC Bearer Control Tunnelling information

On receipt of a SIP message containing an SDP answer, the Bearer Control Interworking function is used to generate a Bearer Control Protocol Data Unit for inclusion in a BICC message. The particular BICC message used depends on the procedures defined below.

A.2.1.3 Interworking from BICC Bearer Control Tunnelling information to SDP

On receipt of a BICC message containing a Bearer Control Protocol Data Unit, the Bearer Control Interworking Function is used to generate an SDP offer or answer for inclusion within a SIP message.

If the SDP is an SDP offer, then the particular SIP message used depends on the procedures defined below.

If the SDP is an SDP answer, then the SIP message sent is as identified in ~~section~~ clause 2.1.1 above in this Annex.

A.2.2 Message mapping procedures

A.2.2.1 SIP to BICC

A.2.2.1.1 Initial INVITE

On receipt of the INVITE, the I-IWU determines the Bearer Setup Procedure to be used on the BICC side. This depends on whether the INVITE contains an SDP offer:

If the INVITE contains an SDP offer, then the I-IWU uses the ‘Per call bearer setup using bearer control tunnelling – fast forwards’ procedures defined in Q.1902.4. The INVITE is mapped to an IAM as described in ~~Section~~ clause 7 of the main body of this Recommendation~~.?~~.

If the INVITE does not contain an SDP offer, then the I-IWU uses the ‘Per call bearer setup using bearer control tunnelling – backwards’ procedures defined in Q.1902.4. The INVITE is mapped to an IAM as described in clause~~Section~~ 7? of the main body of this Recommendation..

A.2.2.1.2 APM

Subsequently, an APM message is received according to the procedures of Q.1902.4. This is mapped to a SIP 183 response to the initial INVITE.

A.2.2.1.3 PRACK

On receipt of a PRACK message responding to the 183 response sent in ~~section~~ clause 2.2.1.2, containing SDP the I-IWU shall send an APM message on the BICC side.

A.2.2.1.4 Further APM messages

On receipt of further APM messages on the BICC side, containing Bearer Control Tunnelling information which maps to an SDP offer, the I-IWU shall send an UPDATE request on the SIP side.

A.2.2.1.5 UPDATE requests

On receipt of an UPDATE request on the SIP side, containing SDP, the I-IWU shall send an APM message on the BICC side.

A.2.2.1.6 200 ~~OK(~~UPDATE~~)~~ response

On receipt of a 200 ~~OK(~~UPDATE~~)~~ message in response to the UPDATE request sent as a result of section 2.2.1.4, containing SDP the I-IWU shall send an APM message on the BICC side.

A.2.2.2 BICC to SIP

A.2.2.2.1 Initial IAM

On receipt of an IAM, the O-IWU action depends on the Bearer Setup Procedure requested

A.2.2.2.1.1 Fast Forwards setup

In this case, the IAM contains Bearer Control Tunnelling ~~information which~~information, which maps to an SDP offer. An INVITE is sent containing this SDP offer.

A.2.2.2.1.2 Backwards

In this case, the IAM does not contain Bearer Control Tunnelling information. An INVITE is sent without SDP.

A.2.2.2.1.3 Delayed Forwards

In this case, the IAM does not contain Bearer Control Tunnelling information. An APM is returned according to the procedures of Q.1902.4.

Subsequently, an APM message is received containing Bearer Control Tunnelling ~~information which~~information, which maps to an SDP offer. An INVITE is sent containing this SDP offer.

A.2.2.2.2 Provisional response to INVITE

A provisional response to the INVITE may be received containing SDP which maps to a Bearer Control Protocol Data Unit. This is included as Bearer Control Tunnelling data within an APM message.

A.2.2.2.3 Subsequent APMs

On receipt of an APM message containing Bearer Control Tunnelling information, this information is mapped to an SDP offer or answer. In the case of an SDP offer, this is sent in an UPDATE message. In the case of an SDP answer, the procedures of 2.1.3 determine the SIP message to send.

A.2.3 ~~Pre-condition~~Preconditions

~~Pre-condition~~Preconditions refer to the mechanisms used to determine when bearer setup is complete, including completion of any procedures within the bearer network not visible to the IWF.

~~Two forms of pre-condition exist: (i) relating to the set up of the bearer on the particular bearer link in question (ii) related to the set up of the bearer on previous links.~~

~~Pre-conditions of both kinds~~ Preconditions are handled on the SIP side using the mechanisms of [~~3 – (manyfolks)~~RFC 3312] which are based on attributes within the SDP.

~~Pre-conditions of type (i) a~~Preconditions re handled on the BICC side using the continuity mechanism as described in Q.1902.4 to delay continuation of call setup until all preconditions to call setup have been met~~using the continuity mechanism as described in Q.1902.4 to delay continuation of call setup until all preconditions to call setup have been met~~. ~~as follows:~~

~~For fast/delayed forwards setup with Bearer Control Tunnelling, the existence of pre-conditions can be signalled forwards by indicating 'notification required' in the initial IAM. Subsequently, an APM message indicating 'Connected' is used to indicate that the bearer setup is complete.~~

~~For backwards setup with Bearer Control Tunnelling, fulfilment of the precondition is assumed to be detected by the Bearer Control Protocol and reported to the terminating CSF.~~

~~Pre-conditions of type (ii) are handled on the BICC side by means of the COT mechanism as described in Q.1902.4.~~

Note that BICC provides mechanisms to indicate the existence and completion of ~~pre-condition~~preconditions from the O-ISN to the T-ISN, but not in the reverse direction – it is assumed that there are no (pre-ACM) procedures at the O-ISN that need to be delayed pending the completion of actions at the T-ISN.

The Bearer Control Interworking Function is responsible for processing precondition indications within the SDP and indicating to the BICC procedures when the above BICC mechanisms are required. The following indications may be passed from the Bearer Control Interworking Function to the BICC protocol procedures:

~~I.~~• ~~Type (i)~~ precondition required

~~I.~~• ~~Type (i)~~ precondition met

~~I.Type (ii) precondition required~~

~~I.Type (ii) precondition met~~

Similarly, when the BICC mechanism require preconditions to be signalled, a request is made to the Bearer Control Interworking Function to add the appropriate indications to SDP. The following indications may~~t~~ be passed from the BICC protocol procedures to the Bearer Control Interworking Function:

• ~~Type (i)~~ precondition required

• ~~Type (i)~~ precondition met

~~Type (ii) precondition required~~

~~Type (ii) precondition met~~

A.2.3.1 Interworking ~~type (i)~~ preconditions

A.2.3.1.1 SIP to BICC

A.2.3.1.1.1 Fast-forwards setup

~~On receipt of the indication *Type (i) preconditions required* from the Bearer Control Interworking Function, the indication 'Notification required' shall be included in the outgoing IAM. (Note: this indication should not be received at any other time)~~

On receipt of the indication *preconditions required* from the Bearer Control Interworking Function, the "Continuity indicator" in the IAM shall be set to "COT to be expected". Subsequently, on receipt of the indication *preconditions met* from the Bearer Control Interworking Function (and on the determination that all preconditions local to the BICC side are also met) a COT message with "continuity indicators" set to "Continuity" shall be sent.~~On receipt of the indication *preconditions required* from the Bearer Control Interworking Function, the "Continuity indicator" in the IAM shall be set to "COT to be expected". Subsequently, on receipt of the indication *preconditions met* from the Bearer Control Interworking Function (and on the determination that all preconditions local to the BICC side are also met) a COT message with "continuity indicators" set to "Continuity" shall be sent.~~

~~Subsequently, on receipt of the indication *Type (i) preconditions met* from the Bearer Control Interworking Function, an APM message shall be sent containing the indication 'Connected'.~~

Editor's note: The Bearer Control Interworking Function will need to take care of the following things: (i) on receipt of the SDP offer containing preconditions, generate the ~~*Type (i)*~~ *preconditions required* indication (ii) on generation of the SDP answer, indicate that the IWF's end of the preconditions have been met in that SDP and (iii) on receipt of SDP indicating that the preconditions have been completely met, it should generate the ~~*Type (i)*~~ *preconditions met indication*.

Editor's note: For backwards setup, preconditions could appear in the SDP answer received from the SIP side in the PRACK. In this case the Bearer Control Interworking Function will just wait until SDP indicating ~~pre-condition~~preconditions met is received before actually mapping to IP BCP and forwarding to the BICC side.

A.2.3.1.2 BICC to SIP

A.2.3.1.2.1 Fast forwards setup

If the indication "COT to be expected" is received in an IAM~~If the indication "COT to be expected" is received in an IAM, If the indication 'notification required' is received in the IAM~~, then the indication ~~*Type (i)*~~ *precondition required* is sent to the Bearer Control Interworking Function along with the Bearer Control Tunnelling Information in the IAM.

Subsequently, on receipt at the O-IWF~~ at the O-IWF~~ of a COT message indicating "continuity"~~ COT message indicating "continuity"n APM indicating 'Connected'~~, then the indication ~~*Type (i)*~~ *precondition met* is sent to the Bearer Control Interworking Function.

Editor's note: These indications will cause the BCIWF to include/generate the appropriate SDP precondition attributes.

A.2.3.1.2.2 Backwards setup

No action is taken on receipt of the indications ~~Type (i)~~ *preconditions required* and ~~Type (i)~~ *preconditions met*.

Editor's note: The BCIWF may receive an SDP offer (say in 183) indicating preconditions, which it would signal to the BICC side (which does nothing, as above). The BCIWF can indicate ~~pre-condition~~preconditions met in the SDP answer, since on the BICC side receipt of the Bearer Control PDU indicates ~~pre-condition~~preconditions met.

A.2.3.1.2.3 Delayed Forwards

If the indication "COT to be expected"~~"COT to be expected" 'notification required'~~ is received in the IAM, then the indication ~~*Type (i)*~~ *precondition required* is sent to the Bearer Control Interworking Function along with the Bearer Control Tunnelling Information received in the subsequent APM.

Subsequently, on receipt of a~~n APM~~ COT message indicating '~~Connected~~Continuity', then the indication ~~*Type (i)*~~ *precondition met* is sent to the Bearer Control Interworking Function.

~~2.3.2 Interworking type (ii) preconditions~~

~~2.3.2.1 SIP to BICCC~~

~~2.3.2.1.1 Fast forwards setup~~

~~On receipt of the indication *Type (ii) preconditions required* from the Bearer Control Interworking Function, the Nature of Connection indicators in the outgoing IAM shall be set to "Continuity check required on outgoing circuit". (Note: this indication should not be received at any other time).~~

~~Subsequently, on receipt of the indication *Type (ii) preconditions met* from the Bearer Control Interworking Function, a COT message shall be sent with the continuity indicators set to "continuity check successful".~~

~~Editor's note: The Bearer Control Interworking Function will need to take care of the following things: (i) on receipt of the SDP offer containing preconditions, generate the *Type (ii) preconditions required* indication (ii) on generation of the SDP answer, indicate that the IWF's end of the preconditions have been met in that SDP and (iii) on receipt of SDP indicating that the preconditions have been completely met, it should generate the *Type (ii) preconditions met indication.*~~

~~Editor's note: For backwards setup, preconditions could appear in the SDP answer received from the SIP side in the PRACK. In this case the Bearer Control Interworking Function will just wait until SDP indicating pre-met is received before actually mapping to IP BCP and forwarding to the BICC side.~~

~~2.3.2.2 BICC to SIP~~

~~2.3.2.2.1 Fast forwards setup~~

~~If the indication 'continuity check required on outgoing circuit' is received in the IAM, then the indication *Type (ii) preconditions required* is sent to the Bearer Control Interworking Function along with the Bearer Control Tunnelling Information in the IAM.~~

~~Subsequently, on receipt of COT message with continuity indicators indicating "continuity check successful", then the indication *Type (ii) precondition met* is sent to the Bearer Control Interworking Function.~~

~~Editor's note: These indications will cause the BCIWF to include/generate the appropriate SDP precondition attributes.~~

~~2.3.2.2.2 Backwards setup~~

~~No action is taken on receipt of the indications Type (ii) preconditions required and Type (ii) preconditions met.~~

~~Editor's note: The BCIWF may receive an SDP offer (say in 183) indicating preconditions, which it would signal to the BICC side (which does nothing, as above). The BCIWF can indicate pre-met in the SDP answer, since on the BICC side receipt of the Bearer Control PDU indicates pre-met.~~

~~2.3.2.2.3 Delayed Forwards~~

~~If the indication 'continuity check required on the outgoing circuit' is received in the IAM, then the indication *Type (ii) precondition required* is sent to the Bearer Control Interworking Function along with the Bearer Control Tunnelling Information received in the subsequent APM.~~

~~Subsequently, on receipt of a COT message with continuity indicators indicating "continuity check successful", then the indication *Type (ii) precondition met* is sent to the Bearer Control Interworking Function.~~

A.3.0 Bearer Control Interworking Function

A.3.1 IPBCP/ SDP Bearer Control interworking function (BC-IWF)

This section defines the procedures associated with a Bearer Control Interworking Function which interworks IPBCP to/from SDP. In all cases the BC-IWF is a call stateful device. This is particularly important in enabling the BC-IWF to manipulate precondition information it receives within SDP offers/answers and IPBCP messages.

The IPBCP/SDP Bearer Control Interworking function (BC-IWF) shall behave as follows:

A.3.1.1. SDP to IPBCP

A.3.1.1.1 Receipt of SDP offer.

On receipt of an SDP offer (as determined by the procedures within [~~(3 (RFCoffer-ans)~~RFC 3264]) the BC-IWF shall send a REQUEST message on the IPBCP side. The REQUEST message contents shall be formatted as per the procedures in section 6 of Recommendation Q.1970. Any SDP fields that cannot be directly carried within the SDP allowed within the IPBCP REQUEST message shall not be sent to the BICC side. In addition, if the SDP offer contained any precondition media level attributes indicating that preconditions to session establishment are present on the SIP side of the call these shall be removed from the SDP sent to the IPBCP side. Instead, ~~if the BC-IWF receives~~ a ~~type (i)~~ *preconditions required* indication (as defined by the procedures in section 2.3) is sent to the BC-IWF. Subsequently ~~then~~ the procedures outlined in section 2.3.1.1~~1~~ shall be followed with respect to the setting of indicators within the BICC IAM. Furthermore, if the SDP offer instead resulted in the BC-IWF receiving a ~~type (i)~~ *preconditions met* indication (as a result of the precondition SDP indicating that all mandatory preconditions had been met) then the BC-IWF shall correlate receipt of this indication with receipt of a ~~type (i)~~ *preconditions required* indication in a previous offer for this call and the procedures outlined within section 2.3.1.1~~1.~~ with respect to ~~type (i)~~ preconditions met shall be followed.

A.3.1.1.2 Receipt of SDP answer

(i) IPBCP has previously sent a REQUEST message for which it has not yet received an answer.

On receipt of an SDP answer (as determined by the procedures within [RFC 3264~~3 (RFCoffer-ans)~~] the BC-IWF shall send an ACCEPTED message to the IPBCP side. The ACCEPTED message contents shall be formatted as per the procedures of section 6 of Recommendation Q.1970. With the exception of media level attributes describing preconditions, if the SDP field is allowed to be included in the ACCEPTED message, it shall be included. If the SDP received in the answer indicates a change in status of the preconditions from any previous SDP received at the I-IWF then this change in precondition status shall be reported to the BC-IWF using precondition indications as defined in section 2.3.~~If the SDP received in the answer indicates a change in status of the preconditions from any previous SDP received at the I-IWF then this change in precondition status shall be reported to the BC-IWF using precondition indications as defined in section 2.3.~~

If the SDP answer is received and the port number of the media stream that was being offered in the SDP offer is set to 0 then the BC-IWF shall send a REJECTED message to the IPBCP side. The REJECTED message contents shall be formatted as per the procedures of section 6 of Recommendation Q.1970. With the exception of media level attributes describing preconditions, if the SDP field is allowed to be included in the REJECTED message, it shall be included.

(ii) IPBCP has not previously sent a REQUEST message or has sent a REQUEST message for which an answer has been received.

On receipt of an SDP answer (as determined by the procedures within [RFC 3264~~3 (RFCoffer-answer)~~] the BC-IWF shall not send any message to the IPBCP side.

Editor's note: This deals with the situation whereby a call is from BICC to SIP and conformation of SIP preconditions is requested in the ~~18x~~18X. This results in an UPDATE being generated at the O-IWF with an SDP offer. This SDP offer will produce an answer at the ASN which should not be inter-worked to the BICC side (since the SDP offer simply reports updates the status of preconditions).

A.3.1.2 IPBCP to SDP

A.3.1.2.1 Receipt of Request message

On receipt of an IPBCP REQUEST message, the BC-IWF shall construct and send an SDP offer in the first SIP message sent as a result of the interworking procedures defined in this Recommendation and as per the procedures relating to the sending of SDP offers in SIP defined within [RFC 3264~~3 (RFCoffer-ans)~~] [~~3 (~~RFC3261~~)~~]. The SDP fields contained within the IPBCP REQUEST message shall be included within the SDP offer. If the BC-IWF receives a ~~type (ii)~~ *preconditions required* indication then the BC-IWF shall ensure that the SDP offer sent from the BC-IWF contains a "local" precondition (in the language of ~~(3-(Manyfolks))~~RFC 3312). The current status of this "local" precondition shall have a strength tag of "none" and a direction tag of "none". The desired status of the local precondition shall be set to a strength of "mandatory" and a direction value of "sendrecv". Additionally, the BC-IWF shall insert a corresponding remote precondition with a desired status of strength-tag = none and direction-tag = none. The BC-IWF is responsible for storing the state of all preconditions during the duration of the call.

If, in the period between sending this offer and sending the last offer, the BC-IWF receives a~~ type (ii)~~ *precondition met* indication then the BC-IWF shall correlate receipt of this precondition status information with the value of the "local" precondition tag which it inserted on receipt of the ~~type (ii)~~ *precondition required* indication received in a previous IPBCP REQUEST message. The BC-IWF shall set the current status of this precondition equal to the desired status before sending out the SDP offer containing the updated current status.

A.3.1.2.2 Receipt of Accepted message

On receipt of an IPBCP ACCEPTED message, the BC-IWF shall construct and send an SDP answer in the first SIP message sent as a result of the interworking procedures defined in this Recommendation and as per the procedures relating to the sending of SDP answers defined within [~~3 (RFCoffer-ans)~~RFC 3264] and [3-(RFC3261)]. The SDP fields contained within the IPBCP ACCEPTED message shall be included within the SDP answer. Additionally, the BC-IWF shall include any SDP relating to the status of the preconditions SDP sent within the SDP offer that was interworked to the REQUEST message responsible for generating this ACCEPTED message. In particular, if the BC-IWF has received a ~~type (i)~~ *preconditions required* indication ~~–~~in the SDP offer which generated the REQUEST message responsible for this ACCEPTED message then the BC-IWF shall add in precondition SDP to update the current (and desired status (if necessary)) of the ~~type (i)~~ preconditions. The procedures used to respond to the SDP received in the previous SDP offer correlated with this answer are described fully in ~~(3-[Manyfolks])~~RFC 3312.

A.3.1.2.3 Receipt of Confused message

On receipt of the CONFUSED message, the BC-IWF shall follow the procedures outlined within Q.1970.

Editor's note: The "confused" message is a compatibility mechanism which is part of the IPBCP protocol itself and has no parallel in SDP. The procedures in IPBCP say that on receipt of this message the BC-IWF could re-attempt the bearer establishment or may instead report the compatibility problem to a control entity to decide what action (e.g. releasing the call) to take. This may result in autonomous REL resulting at the BICC layer - the REL would of course effect the SIP network and would be covered in the procedures relating to autonomous release at the IWF.

A.3.1.2.4 Receipt of Rejected message.

On receipt of the REJECTED message, the BC-IWF shall send an SDP answer in the first available SIP message. The SDP answer shall be constructed using the SDP fields present in the REJECTED message however, the BC-IWF shall set the port number for the media stream to the value 0.