INTERNATIONAL TELECOMMUNICATION UNION

ITU-T Q.1912.5

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(03/2004)

SERIES Q: SWITCHING AND SIGNALLING

Specifications of signalling related to Bearer Independent Call Control (BICC)

Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control protocol or ISDN User Part

ITU-T Recommendation Q.1912.5

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2	Q.120–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	Q.800–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	**Q.1900–Q.1999**
BROADBAND ISDN	Q.2000–Q.2999
General aspects	Q.2000–Q.2099
Signalling ATM adaptation layer (SAAL)	Q.2100–Q.2199
Signalling network protocols	Q.2200–Q.2299
Common aspects of B-ISDN application protocols for access signalling and network signalling and interworking	Q.2600–Q.2699
B-ISDN application protocols for the network signalling	Q.2700–Q.2899
B-ISDN application protocols for access signalling	Q.2900–Q.2999

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation Q.1912.5

Interworking between Session Initiation Protocol (SIP) and 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.

Source

ITU-T Recommendation Q.1912.5 was approved on 12 March 2004 by ITU-T Study Group 11 (2001-2004) under the ITU-T Recommendation A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

ITU-T Recommendation Q.1912.5

Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control protocol or ISDN User Part

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 Unit (IWU). ISUP is defined in accordance with ITU-T Recs Q.761 to Q.764 and BICC is defined in accordance with ITU-T Recs 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 C.

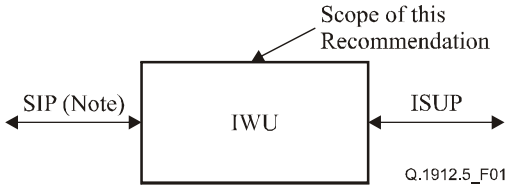
An IWU may be stand-alone or may be combined with an ISUP exchange or BICC Interface Serving Node (ISN). It is assumed in this Recommendation that the initial service requests are forwarded and/or delivered via a trusted Adjacent SIP Node (ASN) within a SIP network domain. The ASN is viewed as a trusted 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 Profile C (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 out of scope of this Recommendation. Interworking with forking in the SIP network is not specified in this Recommendation and 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 interwork by using the function of an Interworking Unit (IWU). The IWU will also handle (through default origination or graceful termination) services or capabilities that do not interwork across domains.

The scope of this Recommendation is shown in Figures 1 and 2, respectively.

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

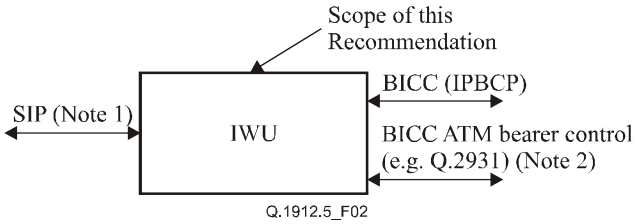
Items relating to security when interworking between two signalling systems in this Recommendation are for further study.



NOTE – The content consists of the SIP headers and message body.

Figure 1/Q.1912.5 – Scope of interworking between SIP and ISUP

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



NOTE 1 – The content consists of the SIP headers and message body.

NOTE 2 – Interworking with ATM bearer control is not specified in this Recommendation.

Figure 2/Q.1912.5 – Scope of interworking between SIP and BICC

ITU-T Supplement 45 to Q-series Recommendations (TRQ.2815) 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 Supplement 45 (TRQ.2815) 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 Profile C (SIP-I), respectively. The details on the capabilities supported by the different profiles, and all profiles in common, are shown in Annex C.1.1.2.

Administrations may require operators to take into account national requirements in implementing this Recommendation, and in particular, in determining the local trust policy for the IWU.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; 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. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

– All IETF Standards Track RFC directly referenced by this Recommendation are listed in Annex C.1.

– ITU-T Recommendation Q.731.7 (1997), *Stage 3 description for number identification supplementary services using Signalling System No. 7: Malicious call identification (MCID)*.

– ITU-T Recommendation Q.732.2 (1999), *Stage 3 description for call offering supplementary services using Signalling System No. 7: Call diversion services: Call forwarding busy, call forwarding no reply, call forwarding unconditional, call deflection.*

– ITU-T Recommendation Q.732.3 (1993), *Stage 3 description for call offering supplementary services using Signalling System No. 7: Call forwarding no answer*.

– ITU-T Recommendation Q.732.4 (1993), *Stage 3 description for call offering supplementary services using Signalling System No. 7: Call forwarding unconditional*.

– ITU-T Recommendation Q.732.5 (1993), *Stage 3 description for call offering supplementary services using Signalling System No. 7: Call deflection*.

– ITU-T Recommendation Q.732.7 (1996), *Stage 3 description for call offering supplementary services using Signalling System No. 7: Explicit call transfer*.

– ITU-T Recommendation Q.733.1 (1992), *Stage 3 description for call completion supplementary services using Signalling System No. 7: Call waiting (CW)*.

– ITU-T Recommendation Q.733.2 (1993), *Stage 3 description for call completion supplementary services using Signalling System No. 7: Call hold (HOLD)*.

– ITU-T Recommendation Q.733.3 (1997), *Stage 3 description for call completion supplementary services using Signalling System No. 7: Completion of calls to busy subscriber (CCBS)*.

– ITU-T Recommendation Q.733.4 (1993), *Stage 3 description for call completion supplementary services using Signalling System No. 7: Terminal portability (TP)*.

– ITU-T Recommendation Q.733.5 (1999), *Stage 3 description for call completion supplementary services using Signalling System No. 7: Completion of calls on no reply*.

– ITU-T Recommendation Q.734.1 (1993), *Stage 3 description for multiparty supplementary services using Signalling System No. 7: Conference calling*.

– ITU-T Recommendation Q.734.2 (1996), *Stage 3 description for multiparty supplementary services using Signalling System No. 7: Three-party service*.

– ITU-T Recommendation Q.735.1 (1993), *Stage 3 description for community of interest supplementary services using Signalling System No. 7: Closed user group (CUG)*.

– ITU-T Recommendation Q.735.3 (1993), *Stage 3 description for community of interest supplementary services using Signalling System No. 7: Multi-level precedence and preemption*.

– ITU-T Recommendation Q.735.6 (1996), *Stage 3 description for community of interest supplementary services using Signalling System No. 7: Global virtual network service (GVNS)*.

– ITU-T Recommendation Q.736.1 (1995), *Stage 3 description for charging supplementary services using Signalling System No. 7: International Telecommunication Charge Card (ITCC)*.

– ITU-T Recommendation Q.736.3 (1995), *Stage 3 description for charging supplementary services using Signalling System No. 7: Reverse charging (REV)*.

– ITU-T Recommendation Q.737.1 (1997), *Stage 3 description for additional information transfer supplementary services using Signalling System No. 7: User-to-user signalling (UUS)*.

– ITU-T Recommendations Q.761 to Q.764 (1999), *Specifications of Signalling System No. 7 ISDN User Part (ISUP)*.

– ITU-T Recommendation Q.850 (1998), *Usage of cause and location in the Digital Subscriber Signalling System No. 1 and the Signalling System No. 7 ISDN user part*.

– ITU-T Recommendations Q.1902.1 to Q.1902.4 (2001), *Specifications of the Bearer Independent Call Control (BICC) protocol*.

3 Definitions

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

3.1 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.

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

3.3 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.

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

3.5 Adjacent SIP Node (ASN): A SIP node (e.g., SIP Proxy or Back-to-Back User Agent or the SIP side of an IWU) that has established a direct trust relation (association) with Incoming or Outgoing IWU entities. The SIP Proxy and Back-to-Back User Agent are defined in accordance with RFC 3261.

3.6 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.

3.7 SIP precondition: Indicates the support of the SIP "precondition procedure" as defined in RFC 3312.

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

3.9 Type 1 gateway: An interworking unit (IWU) capable of bearer control as well as call control. The IWU interworks between SIP and BICC or ISUP. Bearer control interworking is an internal operation.

NOTE – Because it is internal, bearer control interworking for Type 1 gateways is not specified in this Recommendation.

3.10 Type 2 gateway: An interworking unit capable of call control but not bearer control. The IWU interworks between SIP and BICC. Bearer control interworking is between the external bearer control protocol on the BICC side and SDP within SIP.

NOTE – Bearer control interworking for Type 2 gateways in the particular case of IP Bearer Control (IPBCP) is specified in Annex A.

3.11 Type 3 gateway: An interworking unit capable of bearer control as well as call control. The IWU interworks between SIP-I and BICC or ISUP. Bearer interworking is an internal operation.

NOTE – Because it is internal, bearer control interworking for Type 3 gateways is not specified in this Recommendation.

3.12 Type 4 gateway: An interworking unit capable of call control but not bearer control. The IWU interworks between SIP-I and BICC. Bearer control interworking is between the external bearer control protocol on the BICC side and SDP within SIP.

NOTE – Bearer control interworking for Type 4 gateways in the particular case of IP Bearer Control (IPBCP) is specified in Annex A.

In addition, this Recommendation makes use of the terms **header field**, **message**, **message body**, **method**, **request, provisional** and **final response**, **dialog** and **User Agent**, which are defined in section 6/RFC 3261. It uses the term **payload type** as defined in RFC 3550, and **static** and **dynamic** payload type as defined in that RFC. Finally, it uses the terms **attribute** and **session** as defined in RFC 2327.

Within this Recommendation the following terminology is used:

– **pass to BICC/ISUP procedures** describes an operation internal to the IWU;

– **send** describes the transmission of a message on the applicable external network interface.

4 Abbreviations

This Recommendation uses the following abbreviations:

General

ABNF	Augmented Backus-Naur Form (see RFC 2234)
AMR	Adaptive Multirate (codec)
ASN	Adjacent SIP Node
ATM	Asynchronous Transfer Mode
B2BUA	Back-to-Back User Agent
BICC	Bearer Independent Call Control
BC-IWF	Bearer Control-Interworking Function
BNC	Backbone Network Connection
BNF	Backus-Naur Form
CC	Country Code
CLI	Calling Line Identification
CONN	CONNECT message (see ITU-T Rec. Q.931)
DISC	DISCONNECT message (see ITU-T Rec. Q.931)
FFS	For further study.
IANA	Internet Assigned Numbers Authority
IETF	Internet Engineering Task Force
I-IWU	Incoming (to BICC/ISUP) InterWorking Unit
IPBCP	Internet Protocol Bearer Control Protocol
ISDN	Integrated Services Digital Network
ISN	Interface Serving Node
ISUP	ISDN User Part
IWU	InterWorking Unit
MIME	Multi-purpose Internet Mail Extensions
NDC	National Destination Code
NNI	Network-to-Network Interface
O-IWU	Outgoing (from BICC/ISUP) InterWorking Unit
PSTN	Public Switched Telephone Network
PT	Payload Type
RFC	Request For Comments
RTP	Real-time Transport Protocol
SCCP	Signalling Connection Control Part
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SIP-I	SIP with encapsulated ISUP
SN	Subscriber Number
TLS	Transport Layer Security

UA User Agent
UAC User Agent Client
UAS User Agent Server
UNI User-to-Network Interface
URI Universal Resource Identifier

BICC/ISUP messages

ACM Address Complete Message
ANM Answer Message
APM Application Transport Mechanism
BAT Bearer Association Transport
CGB Circuit Group Blocking
CON Connect message
COT Continuity message
CPG Call progress
GRS Circuit Group Reset message
IAM Initial Address Message
REL Release message
RES Resume message
RLC Release Complete
RSC Reset Circuit message
SGM Segmentation Message
SAM Subsequent Address Message
SUS Suspend message

BICC/ISUP parameters and values

ACgPN *"additional calling party number"* (value of Number Qualifier indicator within Generic Number)
APP Application Transport Parameter
APRI Address Presentation Restricted Indicator
ATP Access Transport Parameter
BCI Backward Call Indicator
CgPN Calling Party Number
CIC Circuit Identification Code (ISUP)
CIC Call Instance Code (BICC)
FCI Forward Call Indicator
HLC High Layer Compatibility
NOA Nature of Address indicator
NP *"network provided"* (Screening Indicator value)
TMR Transmission Medium Requirement
UPVP *"user provided, verified and passed"* (Screening Indicator value)
USI User Service Information

5 Methodology

5.1 Conventions for representation of BICC/ISUP PDU

1) The first letter of each major word is capitalized in the names of BICC/ISUP:
   - messages (e.g., Initial Address Message, User-to-user Information);
   - parameters (e.g., Nature of Connection Indicators, Calling Party's Category); and
   - parameter information (e.g., Nature of Address Indicator, Address Signals, Cause Value).

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) All letters of SIP method names are capitalized.

   Example: INVITE, INFO.

2) SIP header fields are identified by the unabbreviated header field name as defined in the relevant RFC, including capitalization and enclosed hyphens but excluding the following colon.

   Examples: To, From, Call-ID.

3) Where it is necessary to refer with finer granularity to components of a SIP message, the component concerned is identified by the ABNF rule name used to designate it in the defining RFC (generally section 25/RFC 3261), in plain text without surrounding angle brackets.

   Examples: Request-URI, the userinfo portion of a sip: URI.

4) URI schemes are represented by the lower-case identifier followed by a colon and the abbreviation "URI"

   Examples: sip: URI, tel: URI.

5) SIP provisional and final responses other than 2XX are represented by the status code followed by the normal reason phrase for that status code, with initial letters capitalized.

   Examples: 100 Trying, 484 Address Incomplete.

6) Because of potential ambiguity within a call flow about which request a 200 OK final response answers, 200 OK is always followed by the method name of the request.

   Examples: 200 OK INVITE, 200 OK PRACK.

7) A particular line of an SDP session description is identified by the two initial characters of the line, that is, the line type character followed by "="

   Examples: m= line, a= line.

8) Where it is necessary to refer with finer granularity to components of a session description, the component concerned is identified by its rule name in the ABNF description of the SDP line concerned, delimited with angle brackets.

   Examples: the <media> and <fmt> components of the m= line.

5.3 General principles

At the SIP interface, the IWU shall act as a UA and shall support the applicable RFCs as indicated in Annex C.1. The ISUP interface shall support the protocol as defined in the ISUP ITU-T Recs Q.761 to Q.764 (1999). The BICC interface shall support the protocol as defined in the BICC ITU-T Recs Q.1902.1 to Q.1902.4.

The following rules apply to the handling of unrecognized BICC/ISUP information:

– For Profiles A and B, the IWU shall act as a Type A exchange for the purposes of ISUP and BICC Compatibility procedures.

– For Profile C (SIP-I): for the mapping of BICC/ISUP to and from SIP header fields and SDP, the IWU behaves as a Type A exchange. However, when handling ISUP information before encapsulating it or after it has been de-encapsulated, the IWU can act as a Type A or Type B exchange depending on the role (e.g., gateway between operators, transit) the IWU is performing for that particular call.

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, as they cannot be interworked.

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

Before sending any information on the SIP side, the IWU shall consult its local trust policy to determine if the subsequent node to which the outgoing SIP message is directed is trusted to receive that information. Upon determining that the adjacent SIP node (ASN) is not trusted to receive that information, the IWU shall take appropriate action (e.g., omit the information, provide another value or release the call).

Similarly, before accepting any information on the SIP side, the IWU shall consult its local trust policy to determine if the node from which the incoming SIP message came is trusted to originate or pass on that information. Upon determining that the adjacent SIP node (ASN) is not trusted to provide that information, the IWU shall take appropriate action (e.g., ignore the information, use a default value, or release the call).

5.3.1 Identification of call, dialog and call control association

The IWU shall establish a one-to-one relationship between a SIP dialog and a BICC/ISUP call/bearer control instance so that interworking is between signalling information related to the same call. For overlap sending, the same BICC/ISUP call/bearer control instance at the IWU may be associated with a succession of SIP dialogs until address signalling is complete.

5.3.2 General principles specific to Profile C (SIP-I)

In the case of Profile C (SIP-I), the following ISUP timers defined in ITU-T Rec. Q.764 shall not be supported by ISUP procedures on the SIP side of the IWU: T1, T4, T5, T10, T12 through T32, T36 and T37.

Where the SIP dialog terminates and the ISUP state machine is still running (except as provided by clauses 6.2 and 7.2.1, dealing with overlap sending), an implementation-dependent function will release the call.

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 Recommendation. In all cases, the resultant ISUP information shall be passed to the relevant ISUP procedures.

b) An IWU receiving an ISUP message shall, if appropriate, 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, the IWU may be required to construct an appropriate ISUP message using the SIP information received. Clauses 6 and 7 provide all the information that the IWU requires to be able to perform this task.

5.3.3 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-IWU. Additionally, procedures are outlined (in clause 6) to address situations where overlap signalling is received on the SIP side of the I-IWU. While this Recommendation covers procedures for propagating overlap signalling across the SIP network, 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-IWU. Nevertheless, the decision regarding how to configure a particular IWU with respect to overlap signalling is a matter of local policy/network configuration.

In the particular case of SIP overlap to ISUP overlap signalling interworking at the I-IWU, the SIP network must deliver all INVITEs with the same Call-ID and From tag which have enough addressing information to reach an I-IWU to the same I-IWU.

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

NOTE 1 – When an O-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 – It is expected that INVITEs will be delivered in order to the I-IWU. The I-IWU does not buffer and re-order INVITEs that it receives as part of an overlapped call; instead, by analysing the Request-URI, it determines if the INVITE received is the most recent INVITE based upon the number of digits present compared with the number of digits that have already been received at the I-IWU. Procedures within clause 6 outline how the I-IWU processes any INVITEs that are received out of sequence.

5.4 ISUP encapsulation – detailed procedures

This clause is relevant to Profile C (SIP-I) only. It builds on the general principles of ISUP encapsulation outlined in 5.3.2.

5.4.1 Sending of ISUP information to adjacent SIP nodes

5.4.1.1 Introduction

The O-IWU shall apply any interworking procedures detailed within clause 7 affecting parameters within the ISUP, and then proceed to encapsulate any ISUP information received (with the exception of the excluded messages detailed in 5.4.3) in a relevant SIP message (see 5.4.1.3). Setting of header fields relating to the handling of the ISUP body is specified in 5.4.1.2.

Similarly, an I-IWU receiving backwards ISUP information which is not excluded from encapsulation (see 5.4.3) shall apply any interworking procedures detailed in clause 6 affecting the ISUP and then encapsulate the ISUP output in a relevant SIP message (see 5.4.1.3). Setting of header fields relating to the handling of the ISUP body is specified in 5.4.1.2.

5.4.1.2 Header fields for ISUP MIME bodies

For the purpose of this Recommendation the Content-Type header field associated with the ISUP MIME body shall be supplied as follows:

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

NOTE – itu-t92+ means ISUP '92 plus every later ISUP Version. However, no action is taken by the IWU on the "version" parameter.

The Content-Disposition header field associated with the ISUP MIME body shall be set as follows:

Content-Disposition: signal; handling = required.

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 IWU as a result of the interworking specified within the main body of this Recommendation and any ISUP-specific annexes.

As an example, this means that an ISUP IAM received in 7.1 B will be encapsulated within the INVITE message that is sent out from the O-IWU.

For other messages see 5.4.3.

5.4.2 Receipt of ISUP information

5.4.2.1 De-encapsulation of ISUP information

On receipt of a SIP message containing encapsulated ISUP, the IWU shall de-encapsulate the ISUP message from the SIP message body. 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 through 5.4.2.1.3.

5.4.2.1.1 Alignment of SIP headers and ISUP body contents

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

Where a default value is defined to be set in the subclauses of clauses 6 and 7, this shall apply to profiles A and/or B as described. For profile C (SIP-I) the ISUP field shall be derived from the encapsulated ISUP MIME body and local policy.

Where a SIP header mapping to ISUP field(s) is defined (for example the mapping of Request-URI to Called Party Number in 6.1.3.1), the SIP header should be given precedence over the encapsulated ISUP value in the alignment process unless otherwise stated.

5.4.2.1.2 Setting of ISUP parameters by IWU

After following the procedures in 5.4.2.1.1, the IWU will follow any procedures outlined within clause 6 (for the I-IWU) or clause 7 (in the case of the O-IWU) with respect to setting any parameters in the de-encapsulated ISUP message that are required to be autonomously set by the IWU in order to facilitate the interworking.

5.4.2.1.3 Passing resulting ISUP message to BICC/ISUP procedures and sending of message

After following the procedures in 5.4.2.1.2, the IWU shall pass the ISUP information to the relevant BICC/ISUP procedures. The message (if any) which results from the application of the relevant BICC/ISUP procedures is the message which is sent on the BICC/ISUP interface.

5.4.3 Exclusions and special considerations

The ISUP messages listed in Table 1 are either not encapsulated within any SIP message, or receive a special treatment with regard to ISUP encapsulation. The clause number shown in the reference column for each message contains the procedures applicable to that message. This table applies not only to messages received on the BICC/ISUP side and interworked but also to messages generated internally.

NOTE – Table 1 shows only those messages within ITU-T Rec. Q.763 which are not marked "national use". Messages marked "national use" (in ITU-T Rec. Q.763) are outside the scope of this Recommendation.

Table 1/Q.1912.5 – ISUP messages for special consideration

ISUP message	Reference
Reset Circuit	5.4.3.1 (Note 1)
Circuit Group Blocking	5.4.3.1
Circuit Group Blocking Acknowledgement	5.4.3.1
Group Reset	5.4.3.1
Circuit Group Reset Acknowledgement	5.4.3.1
Confusion	5.4.3.1 or 5.4.3.2 (Note 2)
Facility reject	5.4.3.1 or 5.4.3.2 (Note 2)
User to User information	5.4.3.2
Forward Transfer	5.4.3.2
Suspend	5.4.3.2
Resume	5.4.3.2
Blocking	5.4.3.1
Blocking Acknowledgement	5.4.3.1
Continuity Check Request	5.4.3.1
Continuity	5.4.3.1
Unblocking	5.4.3.1
Unblocking Acknowledgement	5.4.3.1
Circuit Group Unblocking	5.4.3.1
Circuit Group Unblocking Acknowledgement	5.4.3.1
Facility Accepted	5.4.3.2
Facility Request	5.4.3.2
User part test	5.4.3.1
User part available	5.4.3.1
Facility	5.4.3.2
Network Resource management	5.4.3.2
Identification Request	5.4.3.2
Identification response	5.4.3.2
Segmentation	5.4.3.3
Loop prevention	5.4.3.2

Table 1/Q.1912.5 – ISUP messages for special consideration

ISUP message	Reference
Application Transport	5.4.3.2
Pre-Release information	5.4.3.2
Release Complete	5.4.3.4
NOTE 1 – Where the ISUP procedures would send reset circuit (RSC) to an ISUP exchange, the IWU shall send an encapsulated REL with release cause 31 (Normal, unspecified). NOTE 2 – These messages are either locally terminated or sent transparently depending on whether they are destined for the IWU or for another exchange.	

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 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 Session Progress provisional response if this is sent by the I-IWU in the backward direction before a confirmed dialog is established.

b) INFO message in all other cases.

These messages are deemed important to transport transparently in order to maintain end-to-end service.

5.4.3.3 ISUP segmentation and ISUP encapsulation

The Segmentation message itself is not encapsulated within SIP. Instead the IWU (BICC/ISUP side interface) will reassemble the original message with its segmented part and check the Optional Forward Call Indicators or Optional Backward Call Indicators parameter.

The actions taken by the IWU on the Optional Forward Call Indicators or Optional Backward Call Indicators depend on whether the Simple Segmentation Indicator is the only indicator to be set in the parameter.

If no other indicator is set within the Optional Forward Call Indicators or Optional Backward Call Indicators parameter, the entire parameter is discarded.

If another indicator is set within the Optional Forward Call Indicators or Optional Backward Call Indicators parameter, the IWU shall set the Simple Segmentation Indicator to indicate that no additional information will be sent.

The IWU shall then encapsulate the resulting message within the SIP message body.

5.4.3.4 Encapsulation of RLC

If a BYE is received containing an encapsulated REL, the 200 OK BYE sent in response shall encapsulate the RLC generated by BICC/ISUP procedures.

5.5 sip: and sips: URIs

Wherever this Recommendation makes reference to a sip: URI as defined in RFC 3261 the text applies equally to sips: URIs. The difference between the two URI types is of significance only in the SIP network, and does not affect interworking.

6 Incoming call interworking from SIP to BICC/ISUP at I-IWU

An Incoming 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 call originating entity (entities) supported in the SIP network domain and the I-IWU. Similarly, the "outgoing BICC/ISUP" refers to the BICC or ISUP protocol supported between the I-IWU and the next-hop entity (entities) in the BICC or ISUP network domain.

The I-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 I-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 I-IWU. This clause is split into subclauses based upon the messages sent or received on the outgoing BICC/ISUP interface of the I-IWU. Only messages that are generated as a result of interworking to/from the incoming SIP side of the I-IWU are considered in this interworking.

The scope of this clause is based on the key assumptions that:

a) the I-IWU supports originating basic calls only; and

b) calls originated from the SIP network domain do not require equivalent PSTN/ISDN service interworking.

The service annexes of this Recommendation will cover additional interworking specifications related to specific PSTN/ISDN services.

In the case of Type 2 or Type 4 Gateways, as defined in ITU-T Supplement 45 to Q-series Recommendations (TRQ.2815), the I-IWU shall (in addition to the procedures outlined within this clause) follow the BICC-specific procedures outlined in A.2.

The I-IWU shall include a To tag in the first backward non-100 provisional response, in order to establish an early dialog as described in section 12/RFC 3261.

For Profile C (SIP-I) operation, ISUP message segmentation must be handled as described in 5.4.3.3.

6.1 Sending of Initial Address Message (IAM)

If an INVITE is received which has enough digits to route to the BICC/ISUP network and which cannot be associated with an existing call, the IAM resulting from the "receipt of INVITE" interworking procedures (see 6.1.1 and 6.1.2) or (in the case of Profile C operation) the de-encapsulated IAM (as updated by the SIP-ISUP interworking procedures within 6.1.3 and associated subclauses) shall be passed to BICC/ISUP procedures. For overlap operation only, if an INVITE is received with the same Call-Id and From tag values as the previous INVITE for which a call is currently active, the procedures of 6.2 apply.

NOTE – If an INVITE is received which does not have enough digits to route to the BICC/ISUP network, normal SIP procedures apply and the INVITE is not interworked.

Clauses 6.1.1 and 6.1.2 address the receipt of the first INVITE for which an IAM is sent. The procedures for sending of the IAM then depend on whether the INVITE received from the SIP network contains an SDP Offer. See 6.1.1 and 6.1.2.

The IAM parameters are coded according to 6.1.3.

6.1.1 INVITE received without an SDP offer

Upon receipt of the first INVITE with sufficient digits for an IAM to be sent, 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 a media description the content of which is determined using local policy within a 183 Session Progress message, subject to the following rules if the I-IWU operates as an international incoming gateway and if G.711 encoding is used:

   i) If the call is to be routed to an A-law PSTN network, then it shall send an SDP offer with A-law (PCMA), but not μ-law (PCMU) included in the media description.

   ii) If the call is to be routed to a μ-law PSTN network, then it shall send an SDP offer with both A-law (PCMA) and μ-law (PCMU) included in the media description and μ-law (PCMU) shall take precedence over A-law (PCMA).

   These procedures reflect the requirement that transcoding between A-law and μ-law must occur in μ-law networks only.

   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 the procedure described in item 2 of 6.1.2.

2) If reliable provisional responses are not supported, the I-IWU shall immediately send out the IAM.

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

If the I-IWU operates as an international incoming gateway, and if G.711 encoding is used, then the following procedures apply. These procedures reflect the requirement that transcoding between A-law and μ-law must occur in μ-law networks only.

i) If the call is to be routed to an A-law PSTN network then it shall delete μ-law (PCMU), if present, from the media description that it will send back in the SDP answer.

ii) If the call is to be routed to a μ-law PSTN network, and if both A-law (PCMA) and μ-law (PCMU) were present in the offer, then the I-IWU shall delete A-law (PCMA) from the media description that it will send back in the SDP answer.

The processing continues as follows:

1) If SIP preconditions are not in use, the I-IWU shall immediately send out the IAM.

2) If SIP preconditions are in use, then:

   a) If outgoing BICC/ISUP signalling on the subsequent network supports the use of the continuity check procedure, the IAM shall be sent out immediately on the BICC/ISUP side with the following coding of the Nature of Connection Indicators parameter:

      i) If the subsequent network is a BICC network: The Continuity indicator of the Nature of Connection Indicators parameter 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 signalling on subsequent network does not support the use of the continuity check procedure, sending of the IAM shall be deferred until all preconditions have been met.

In all cases, 6.1.3 gives specific details related to the population of specific parameters of the IAM. Table 2 gives a summary of parameters within the IAM that are interworked from the INVITE along with a reference to the subclauses of 6.1.3 in which the specific interworking is described.

6.1.3 IAM parameters

Table 2 indicates the IAM parameters that interwork from SIP.

Table 2/Q.1912.5 – Interworked contents of the Initial Address Message

Parameter	Clause
Called Party Number	6.1.3.1
Calling Party's Category	6.1.3.2
Nature of Connection Indicators	6.1.3.3
Forward Call Indicators	6.1.3.4
Transmission Medium Requirement	6.1.3.5
Calling Party Number	6.1.3.6.1
Generic Number	6.1.3.6.2
User Service Information	6.1.3.7
Application Transport: BAT (BICC only)	6.1.3.8
Hop Counter	6.1.3.9

6.1.3.1 Called Party Number (mandatory)

It is required that the Request-URI contain a sip: URI with the user = phone parameter, where the userinfo part of the URI is an E.164 number encoded as specified by the telephone-subscriber rule of RFC 2806. Support of any other URI schemes in the Request-URI is for further study.

The information contained in the userinfo component of the Request-URI shall be mapped to the Called Party Number parameter of the IAM. The Internal Network Number Indicator shall be coded to "*routing to internal network number not allowed"*. Table 3 summarizes this mapping.

Table 3/Q.1912.5 – Coding of the Called Party Number

INVITE→	IAM→
Request-URI	Called Party Number
userinfo (sip: URI with user = phone)	Address Signals

6.1.3.2 Calling Party's Category (mandatory)

For Profiles A and B, the following codes should be set by the I-IWU as default in the Calling Party's Category parameter.

Bits/Codes	Meaning
0000 1010	"*Ordinary calling subscriber*"

For Profile C (SIP-I) the Calling Party's Category value shall be generated from the Calling Party's Category parameter present in the encapsulated ISUP.

6.1.3.3 Nature of Connection Indicators (mandatory)

The indicators of the Nature of Connection Indicators parameter which are set by the I-IWU are as follows:

Bits	Indicators in Nature of Connection Indicators parameter
AB	Satellite Indicator
DC	Continuity Check Indicator (ISUP)/ Continuity Indicator (BICC)
E	Outgoing Echo Control Device

Other fields in the Nature of Connection Indicators should follow the current BICC/ISUP Recommendation.

The codes in Table 4 should be set by the I-IWU as default in the Nature of Connection Indicators parameter fields:

Table 4/Q.1912.5 – Default Nature of Connection Indicator values

Bits	Codes	Meaning	Conditions
AB			
	01	"*One satellite circuit in the connection*"	Profiles A and B
DC (Note)	00	*"Continuity check not required (ISUP)/no COT to be expected (BICC)"*	Without pending precondition request (all profiles).
	10	*"Continuity check performed on a previous circuit (ISUP)/COT to be expected (BICC)"*	With pending precondition request (all profiles).
E	1	*"Outgoing echo control device included"*	Profile A
NOTE – In applying these values, the I-IWU shall ignore the Continuity setting received in an encapsulated IAM. COT is not encapsulated; the I-IWU creates COT as required. See 6.3.			

For Profile C (SIP-I), with the exception of Continuity Indicator (BICC)/Continuity Check Indicator (ISUP) which receives a special treatment in 6.1.1 and 6.1.2, the Nature of Connection Indicators should be generated by the I-IWU using the Nature of Connection Indicators received in the encapsulated IAM message.

6.1.3.4 Forward Call Indicators (mandatory)

The indicators of the FCI parameter which are set by the I-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 fields in the FCI parameter should follow the current BICC/ISUP Recommendation.

For Profile A, the indicator values in Table 5 should be set by the I-IWU as default in the FCI parameter:

Table 5/Q.1912.5 – Default values for Forward Call Indicators

Bits	Codes	Meaning
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"*

For Profile B, the appropriate values of the FCI parameter are determined based on analysis of various parameters (from signalling, internal states or configuration) at the I-IWU.

For Profile C (SIP-I), the Forward Call Indicators parameter shall be generated by the I-IWU using the Forward Call Indicators parameter present within the received encapsulated ISUP message.

6.1.3.5 Transmission Medium Requirement (mandatory), User Service Information (optional), and Higher Layer Compatibility information element within Access Transport Parameter (optional)

For Profile A, the TMR parameter is set to 3.1 kHz audio, the USI parameter is not sent and transcoding is applied when required. The remainder of this clause applies to Profiles B and C.

For Profile B

If SDP is received from the remote peer before the IAM is sent, and if transcoding is not supported at the I-IWU, then the TMR, USI and HLC shall be derived from SDP as described in 6.1.3.5.1. Otherwise, they shall be set in accordance with local policy.

If G.711 is used, the I-IWU is an international gateway, and the incoming call is treated as an ISDN originated call, then the User Information Layer 1 Protocol indicator of the USI parameter shall be set in accordance with the encoding law of the subsequent BICC/ISUP network.

For Profile C (SIP-I)

The TMR, USI and HLC shall be taken from the encapsulated ISUP.

If the USI parameter is present in the encapsulated ISUP, G.711 is used, and the I-IWU is an international gateway, then the User Information Layer 1 Protocol indicator of the USI parameter shall be set in accordance with the encoding law of the subsequent BICC/ISUP network.

6.1.3.5.1 Transcoding not available at the I-IWU (Profile B only)

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 Annex A.

The SDP Media Description Part received by the I-IWU 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, USI and HLC.

The first subfield (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 the round-up bandwidth for <media> equal to audio is 64 kbit/s 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*".

Table 6 provides the default mapping relations based on the above procedure.

Table 6/Q.1912.5 – Coding of TMR/USI/HLC from SDP: SIP to BICC/ISUP

m= line			b= line	a= line	TMR parameter	USI parameter (Note 1)		HLC parameter
<media>	<transport>	<fmt-list>	<modifier>: <bandwidth-value> NOTE – <bandwidth value> for <modifier> of AS is evaluated to be B kbit/s.	a = rtpmap: <payload type> <encoding name>/ <clock rate> [/<encoding parameters>]	TMR codes	Information Transport Capability	User Information Layer 1 Protocol Indicator	High Layer Characteristics Identification
audio	RTP/AVP	0	N/A or up to 64 kbit/s	N/A	*"3.1 kHz audio"*	*"3.1 kHz audio"*	*"G.711 μ-law"*	(Note 3)
audio	RTP/AVP	Dynamic PT	N/A or up to 64 kbit/s	rtpmap: <payload type> PCMU/8000	*"3.1 kHz audio"*	*"3.1 kHz audio"*	*"G.711 μ-law"*	(Note 3)
audio	RTP/AVP	8	N/A or up to 64 kbit/s	N/A	*"3.1 kHz audio"*	*"3.1 kHz audio"*	*"G.711 A-law"*	(Note 3)
audio	RTP/AVP	Dynamic PT	N/A or up to 64 kbit/s	rtpmap: <payload type> PCMA/8000	*"3.1 kHz audio"*	*"3.1 kHz audio"*	*"G.711 A-law"*	(Note 3)
audio	RTP/AVP	9	AS:64 kbit/s	rtpmap:9 G722/8000	*"64 kbit/s unrestricted"*	*"Unrestricted digital inf. w/tones/ann"*		
audio	RTP/AVP	Dynamic PT	AS:64 kbit/s	rtpmap: <payload type> CLEARMODE/8000 (Note 2)	*"64 kbit/s unrestricted"*	*"Unrestricted digital information"*		
image	udptl	t38	N/A or up to 64 kbit/s	Based on T.38	*"3.1 kHz audio"*	*"3.1 kHz audio"*		*"Facsimile Group 2/3"*
image	tcptl	t38	N/A or up to 64 kbit/s	Based on T.38	*"3.1 kHz audio"*	*"3.1 kHz audio"*		*"Facsimile Group 2/3"*

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.

NOTE 3 – HLC is normally absent in this case. It is possible for HLC to be present with the value "Telephony", although 6.3.1/Q.939 indicates that this would normally be accompanied by a value of "Speech" for the Information Transfer Capability element.

6.1.3.6 BICC/ISUP Calling Line Identification (CLI) parameters

Table 7 summarizes the cases for mapping from the SIP INVITE header fields to the BICC/ISUP CLI parameters. Table 8 provides details when the Calling Party Number parameter is given a network provided value. Table 9 provides details for Calling Party Number parameter mapping in other cases. Finally, Table 10 provides details for mapping to Generic Number parameter when this is possible.

For Profile C (SIP-I)

If the address within the Calling Party Number or Generic Number after application of the mapping in this clause and processing by BICC/ISUP procedures is the same as the respective value contained in the encapsulated ISUP, no additional interworking is needed for that parameter beyond use of ISUP encapsulation. The contrary case is treated in the same way as for Profiles A and B.

Should any discrepancy occur in privacy settings during the alignment process the strongest privacy shall prevail.

Table 7/Q.1912.5 – Mapping of SIP From/P-Asserted-Identity/Privacy header fields to BICC/ISUP CLI parameters

Has a SIP P-Asserted-Identity containing a URI (Note 2) with an identity in the format "+" CC + NDC + SN been received?	**Has a SIP From (Note 3) containing a URI with an identity in the format "+" CC + NDC + 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) or omit the Address Signals. (Note 4)	If a Privacy header field was received, set APRI as indicated in Table 9, otherwise, network option to set APRI to "*presentation restricted*" or "*presentation allowed*" (Note 4)	Parameter not included	Not applicable
No	Yes	Network option to either include a network provided E.164 number (See Table 8) or omit the Address Signals. (Note 4)	If a Privacy header field was received, set APRI as indicated in Table 9, otherwise, network option to set APRI to either "*presentation restricted*" or "*presentation allowed*" (Note 4)	Network option to either omit the parameter (if CgPN has been omitted) or derive from the SIP From (see Table 10) (Note 1)	See Table 10
Yes	No	Derive from SIP P-Asserted-Identity (See Table 9)	APRI = *"presentation restricted*" or "*presentation allowed*" depending on SIP Privacy header. (See Table 9)	Not included	Not applicable
Yes	Yes	Derived from SIP P-Asserted-Identity (See Table 9)	APRI = "*presentation restricted*" or "*presentation allowed*" depending on SIP Privacy. (See Table 9)	Network Option to either omit the parameter or derive from the SIP From (Note 1) (See Table 10)	APRI = "*presentation restricted*" or "*presentation allowed*" depending on SIP Privacy. (See Table 10)

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: URI. The handling of this case is for further study.

NOTE 3 – The SIP From header field 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 3323 recommends that the Anonymous URI itself have the value "*anonymous@anonymous.invalid*".

NOTE 4 – A national option exists to set the APRI to "*Address not available"*.

6.1.3.6.1 Calling Party Number

Table 8/Q.1912.5 – 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"*
Number Incomplete Indicator	*"complete"*
Numbering Plan Indicator	*"ISDN/Telephony (E.164)"*
Address Presentation Restricted Indicator	*"Presentation allowed/restricted*" (see Table 7)
Nature of Address Indicator	If next BICC/ISUP node is located in the same country set to "*national (significant) number*" else set to "*international number*".
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 9/Q.1912.5 – Mapping of P-Asserted-Identity and Privacy header fields to the BICC/ISUP Calling Party Number parameter

Source SIP header field and component	Source component value	Calling Party Number parameter field	Derived value of parameter field
–	–	Number Incomplete Indicator	"*complete*"
–	–	Numbering Plan Indicator	"*ISDN (Telephony) numbering plan (Recommendation E.164)*"
P-Asserted-Identity, appropriate global number portion of the URI, assumed to be in form "+" CC + NDC + SN (Note 1)	CC	Nature of Address Indicator	If CC is equal to the country code of the country where I-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*"
Privacy, priv-value component (Note 2)	Privacy header field absent	Address Presentation Restricted Indicator (APRI)	"*presentation allowed*"
	"*none*"		"*presentation allowed*"
	"*header*"		"*presentation restricted*"
	"*user*"		"*presentation restricted*"
	"*id*"		"*presentation restricted*"
–	–	Screening Indicator	"*network provided*"

Table 9/Q.1912.5 – Mapping of P-Asserted-Identity and Privacy header fields to the BICC/ISUP Calling Party Number parameter

Source SIP header field and component	Source component value	Calling Party Number parameter field	Derived value of parameter field
P-Asserted-Identity, appropriate global number portion of the URI, assumed to be in form "+" CC + NDC + SN (Note 1)	CC, NDC, SN	Address Signals	If NOA is "*national (significant) number*" then set to NDC + SN. If NOA is "*international number*" then set to CC + NDC + SN
NOTE 1 – It is possible that the P-Asserted-Identity header field includes both a tel: URI and a sip: URI. The handling of this case is for further study. NOTE 2 – It is possible to receive two priv-values, one of which is "*none*", the other "*id*". In this case, APRI shall be set to "*presentation restricted*".			

6.1.3.6.2 Generic Number

Table 10/Q.1912.5 – Mapping of SIP From header field to BICC/ISUP Generic Number (*"additional calling party number"*) parameter (network option)

Source SIP header field and component	Source component value	Generic Number parameter field	Derived value of parameter field
–	–	Number Qualifier Indicator	"*additional calling party number*"
From, userinfo component of URI assumed to be in form "+" CC + NDC + SN	CC	Nature of Address Indicator	If CC is equal to the country code of the country where I-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) numbering plan (Recommendation E.164)*"
–	–	Address Presentation Restricted Indicator (APRI)	Use same setting as for calling party number.
–	–	Screening Indicator	"*user provided, not verified*"
From, userinfo component assumed to be in form "+" CC + NDC + SN	CC, NDC, SN	Address Signals	If NOA is "*national (significant) number*" then set to NDC + SN. If NOA is "*international number*" then set to CC + NDC + SN

6.1.3.7 User Service Information (Optional)

See 6.1.3.5.

6.1.3.8 Application Transport: BAT (BICC only)

See Annex A.

6.1.3.9 Hop Counter (Optional)

For Profile C (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 if the Hop Counter parameter is available. The procedure applicable to Profiles A and B shall also be used for Profile C, if no Hop Counter parameter is received in the encapsulated IAM and the succeeding network supports the Hop Counter procedure.

For Profiles A and B, the I-IWU shall derive the Hop Counter parameter value from the Max-Forwards header field value by applying a factor to the latter as shown in Table 11, where the factor is constructed according to the following principles:

a) Hop Counter for a given message should never increase and should decrease by at least 1 with each successive visit to an IWU, regardless of intervening interworking, and similarly for Max-Forwards in the SIP domain.

b) The initial and successively mapped values of Hop Counter should be large enough to accommodate the maximum number of hops that might be expected of a validly routed call.

Table 11/Q.1912.5 – Mapping from Max-Forwards to Hop Counter

Max-Forwards value	Hop Counter value
X	Y = Integer part of (X/Factor)

NOTE – The preceding rules imply that the mapping from Max-Forwards to Hop Counter will take account of the topology of the networks traversed. Since call routing, and thus the number of hops taken, will depend on the origin and destination of the call, the mapping factor used to derive Hop Counter from Max-Forwards should be similarly dependent on call origin and destination. Moreover, when call routing crosses administrative boundaries, the operator of the I-IWU will coordinate with adjacent administrations to provide a mapping at the I-IWU which is consistent with the initial settings or mapping factors used in the adjacent networks.

In summary, the factor used to map from Max-Forwards to Hop Counter for a given call will depend on call origin and call destination, and will be provisioned at the I-IWU based on network topology, trust domain rules, and bilateral agreement.

6.2 Receipt of subsequent INVITE

This clause applies when overlap operation is supported across the I-IWU. Other configurations are handled by the SIP or BICC/ISUP state machines operating separately.

If the I-IWU receives an INVITE with the same Call-ID and From tag as a previous INVITE which was associated with a BICC/ISUP call/bearer control instance currently existing on the BICC/ISUP side, then:

a) If the number of digits in the Request-URI is greater than the number of digits already accumulated for the call, the I-IWU shall generate a SAM and pass it to outgoing BICC/ISUP procedures. The SAM shall contain in its Subsequent Number parameter only the additional digits received in this Request-URI compared with the digits already accumulated for the call. For Profile C (SIP-I), any encapsulated IAM is ignored during this process and is not used. Any earlier INVITE is replied to with a 484 Address Incomplete response if this has not already been done.

b) If the number of digits in the Request-URI is fewer than the number of digits already accumulated for the call, then the I-IWU shall immediately send a 484 Address Incomplete response for this INVITE. In this case, no SAM is sent to BICC/ISUP procedures.

6.2.1 Independence of session negotiation and receipt of address information

As a general principle, the overlap procedures allow for session negotiation (and, in particular, the negotiation and confirmation of preconditions) to continue independently of the receipt of address information. On sending of a 484 Address Incomplete message for an INVITE transaction, the I-IWU considers any offer-answer exchange initiated by the INVITE to be terminated. The new INVITE initiates a new offer-answer exchange. However, if resources have already been reserved and they can be reused within the new offer-answer exchange, the precondition signalling shall reflect the current status of the affected preconditions.

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 procedures on the outgoing BICC/ISUP side have been successfully completed, the I-IWU shall send the COT message coded as follows:

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

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

6.4 Receipt of Connect message (CON)

Table 12 indicates the mapping of the Connect message.

Table 12/Q.1912.5 – Message sent to SIP upon receipt of CON

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

When Profile C (SIP-I) is applicable, the Connect message is encapsulated in a 200 OK INVITE final response.

6.5 Receipt of ACM

Table 13 provides a summary of how the ACM 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 Called Party's Status Indicator in the Backward Call Indicators parameter of the ACM.

1) If the BCI (Called Party's Status Indicator) is set to "*subscriber free*" then :
   - in case of Profile A or Profile B, the 180 Ringing SIP response is sent from the I-IWU;
   - in the case of Profile C (SIP-I), a 180 Ringing SIP response is sent from the I-IWU. The ACM is encapsulated within this response.

2) BCI (Called Party's Status Indicator) = "*no indication*" or any value other than "*subscriber-free*": If this parameter is not set to "*subscriber-free*" then:
   - in the case of Profile A or Profile B, the ACM is not interworked;

     NOTE 1 – A backward path is available as soon as the IAM is sent and appropriate SDP is received from the calling end.

– in the case of Profile C (SIP-I), a 183 Session Progress response is sent from the I-IWU. (See Table 13). The ACM is encapsulated within this response.

NOTE 2 – ACM with Cause parameter is not interworked (except for encapsulation in Profile C (SIP-I) operation). Protection against indefinite prolongation of the call is provided by T9 and other timers.

Table 13/Q.1912.5 – Message sent to SIP upon receipt of ACM

← Message sent to SIP	← ACM
	Backward Call Indicators parameter Called Party's Status Iindicator
183 Session Progress in case of Profile C otherwise not interworked.	00 "*No indication"*
180 Ringing	01 "*Subscriber free"*

6.6 Receipt of CPG

For Profiles A and B, CPG with Event indicator of "*progress*" or "*in-band information*" is not interworked. CPG with Event Indicator of "*alerting*" is interworked as shown in Table 14.

For Profile C (SIP-I), 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 as shown in Table 14. This response shall encapsulate the CPG message.

Table 14/Q.1912.5 – 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 in case of Profile C (SIP-I) otherwise not interworked.	000 0010 (*"progress"*) or 000 0011 (*"in-band information or an appropriate pattern is now available"*)

6.7 Receipt of Answer Message (ANM)

The mapping of ANM is shown in Table 15. On receipt of BICC/ISUP ANM, the I-IWU shall indicate to the SIP protocol to send a 200 OK INVITE to the UAC. If no offer was received in the initial INVITE, and reliable provisional responses were not supported, the 200 OK INVITE shall include an SDP offer consistent with the TMR/USI used on the BICC/ISUP side.

Table 15/Q.1912.5 – Receipt of ANM at the I-IWU

← Message sent to SIP	← Message received from BICC/ISUP
200 OK INVITE	ANM

When Profile C is applicable, the Answer message is encapsulated in a 200 OK INVITE final response.

6.8 Through connection of the bearer path

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

6.8.1 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.

For the Profile C (SIP-I) case, the I-IWU shall follow the through connection procedures in ITU-T Rec. Q.764 for the transit exchange.

6.8.2 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 (ITU-T Rec. Q.1902.4) is successfully completed, and;
- The I-IWU determines (using the procedures defined in RFC 3312) that sufficient 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) that sufficient preconditions have been met for the session to proceed.

6.9 Receipt of Suspend message (SUS) network initiated

If the I-IWU is the controlling exchange for the Suspend procedure, the actions taken on the BICC/ISUP side upon receipt of the Suspend message (SUS) are described in 2.4.1c/Q.764 and 10.2.1c/Q.1902.4.

SUS is not interworked in Profile A or B operation. In the Profile C (SIP-I) case, the SUS is encapsulated in the MIME body of an INFO request. This is summarized in Table 16.

Table 16/Q.1912.5 – INFO sent to SIP upon receipt of SUS (Profile C only)

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

6.10 Receipt of Resume message (RES) network initiated

If the I-IWU is the controlling exchange for the Resume procedure, the actions taken on the BICC/ISUP side upon receipt of the Resume message (RES) are described in 2.4.2c/Q.764 and 10.2.2c/Q.1902.4.

RES is not interworked in Profile A or B operation. In the Profile C (SIP-I) case, the I-IWU shall encapsulate the RES in an INFO method. This is summarized in Table 17.

Table 17/Q.1912.5 – Receipt of Resume message (RES) network initiated (Profile C only)

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

6.11 Release procedures at the I-IWU

6.11.1 Receipt of BYE/CANCEL

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 (ITU-T Rec. Q.1902.4) on the BICC side.

In the case of Profile C (SIP-I), the encapsulated REL received in a BYE message shall be passed to BICC/ISUP procedures without modification. A received CANCEL message shall be treated as described for Profile A or B below.

For Profile A or B

If the Reason header field with Q.850 Cause Value is included in the BYE or CANCEL, then the Cause Value may be mapped to the ISUP Cause Value field in the ISUP REL depending on local policy. The mapping of the Cause Indicators parameter to the Reason header is shown in Table 18. Table 19 shows the coding of the Cause Value in the REL if it is not available from the Reason header field. In both cases, the Location Field shall be set to "*network beyond interworking point*".

Table 18/Q.1912.5 – Mapping of SIP Reason header fields into Cause Indicators parameter

Component of SIP Reason header field	Component value	BICC/ISUP Parameter field	Value
protocol	"*Q.850*"	Cause Indicators parameter	–
protocol-cause	"*cause = XX*" (Note 1)	Cause Value	"*XX*" (Note 1)
–	–	Location	*"network beyond interworking point"*
NOTE 1 – "XX" is the Cause Value as defined in ITU-T Rec. Q.850.			

Table 19/Q.1912.5 – Coding of Cause Value if not taken from the Reason header field (except when encapsulated REL received)

SIP Message →	REL → Cause Indicators parameter
BYE	Cause Value No. 16 (normal call clearing)
CANCEL	Cause Value No. 31 (normal, unspecified)

6.11.2 Receipt 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 reselection, an ISUP RLC is returned to the ISUP side.

On receipt of a BICC REL, the I-IWU invokes the BICC Release reception procedures (11.6/Q.1902.4), on the BICC side.

The above paragraphs are applicable to Type 1 or 3 Gateways only.

Depending on local policy, a Reason header field containing the received (Q.850) Cause Value of the REL may be added to the SIP final response or BYE sent as a result of this clause. The mapping of the Cause Indicators parameter to the Reason header is shown in Table 20.

Table 20/Q.1912.5 – Mapping of Cause Indicators parameter into SIP Reason header fields

Cause indicators parameter field	Value of parameter field	component of SIP Reason header field	component value
–	–	protocol	"*Q.850*"
Cause Value	"*XX*" (Note 1)	protocol-cause	"*cause = XX*" (Note 1)
–	–	reason-text	Should be filled with the definition text as stated in ITU-T Rec. Q.850 (Note 2)
NOTE 1 – "XX" is the Cause Value as defined in ITU-T Rec. Q.850. NOTE 2 – Due to the fact that the Cause Indicators parameter does not include the definition text as defined in Table 1/Q.850, this is based on provisioning in the O-IWU.			

On receipt of REL before receiving ANM or CON, the I-IWU shall send the appropriate SIP status code in a final response to the SIP peer. See Table 21 for the mapping from BICC/ISUP Cause Value to SIP status code. BICC/ISUP Cause Value not appearing in Table 21 shall have the same mapping as the appropriate Q.850 class defaults.

For Profile C (SIP-I), the appropriate SIP status code of the SIP response that encapsulates the REL message should be the same as the default mapping shown in Table 21 for Profiles A and B.

Table 21/Q.1912.5 – Receipt of the Release message (REL)

← SIP Message	← REL Cause Indicators parameter
404 Not Found	Cause Value No. 1 ("*unallocated (unassigned) number*")
500 Server Internal Error	Cause Value No. 2 ("*no route to network*")
500 Server Internal Error	Cause Value No. 3 ("*no route to destination*")
500 Server Internal Error	Cause Value No. 4 ("*Send special information tone*")
404 Not Found	Cause Value No. 5 ("*Misdialled trunk prefix*")
500 Server Internal Error (SIP-I only)	Cause Value No. 8 ("*Preemption*")
500 Server Internal Error (SIP-I only)	Cause Value No. 9 ("*Preemption-circuit reserved for reuse*")
486 Busy Here	Cause Value No. 17 ("*user busy*")
480 Temporarily unavailable	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	Cause Value No. 21 ("*call rejected*")
410 Gone	Cause Value No. 22 ("*number changed*")
No mapping	Cause Value No. 23 ("*redirection to new destination*")
480 Temporarily unavailable	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*"))
500 Server Internal Error	Cause Value No. 29 ("*facility rejected*")

Table 21/Q.1912.5 – Receipt of the Release message (REL)

← SIP Message	← REL Cause Indicators parameter
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	Cause Value in the Class 010 (resource unavailable, Cause Value No. 34)
500 Server Internal Error	Cause Value in the Class 010 (resource unavailable, Cause Value No. 38-47) (47 is class default)
500 Server Internal Error	Cause Value No. 50 ("*requested facility not subscribed*")
500 Server Internal Error (SIP-I only)	Cause Value No. 55 ("*incoming calls barred within CUG*")
500 Server Internal Error	Cause Value No. 57 ("*bearer capability not authorized*")
500 Server Internal Error	Cause Value No. 58 ("*bearer capability not presently available*")
500 Server Internal Error	Cause Value No. 63 ("*service or option not available, unspecified*") (Class default)
500 Server Internal Error	Cause Value in the Class 100 (service or option not implemented Cause Value No. 65-79) (79 is class default)
500 Server Internal Error (SIP-I only)	Cause Value No. 87 ("*user not member of CUG*")
500 Server Internal Error	Cause Value No. 88 ("*incompatible destination*")
500 Server Internal Error (SIP-I only)	Cause Value No. 90 ("*Non-existent CUG*")
404 Not Found	Cause Value No. 91 ("*invalid transit network selection*")
500 Server Internal Error	Cause Value No. 95 ("*invalid message, unspecified*") (Class default)
500 Server Internal Error	Cause Value No. 97 ("*Message type non-existent or not implemented*")
500 Server Internal Error	Cause Value No. 99 ("*information element/parameter non-existent or not implemented*")
480 Temporarily unavailable	Cause Value No. 102 ("*recovery on timer expiry*")
500 Server Internal Error	Cause Value No. 103 ("*Parameter non-existent or not implemented, passed on*")
500 Server Internal Error	Cause Value No. 110 ("*Message with unrecognized parameter, discarded*")
500 Server Internal Error	Cause Value No. 111 ("*protocol error, unspecified*") (Class default)
480 Temporarily unavailable	Cause Value No. 127 (*"interworking, unspecified*") (Class default)

On receipt of REL after receiving ANM or CON, the I-IWU shall send BYE. For Profile C (SIP-I), this BYE message shall encapsulate the received REL message.

6.11.3 Autonomous release at I-IWU

Table 22 shows the trigger events at the I-IWU and the release initiated by the I-IWU when the call is traversing from SIP to BICC/ISUP.

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 480 Temporarily Unavailable response to the SIP side. No actions on the ISUP (BICC) side are required.

If, after answer, BICC/ISUP procedures result in autonomous REL from the I-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 500 Server Internal Error response on the SIP side. Depending on local policy, a Reason header field containing the (Q.850) Cause Value of the REL message sent by the I-IWU may be added to the SIP Message (BYE or final response) sent by the SIP side of the I-IWU.

For Profile C (SIP-I), depending on the trigger event, a BYE or the appropriate SIP status code of the SIP response that encapsulates the REL message should be the same as the default mapping shown in Table 21 for Profiles A and B.

Table 22/Q.1912.5 – Autonomous release at I-IWU

← SIP	Trigger event	REL →
		Cause Indicators parameter
484 Address Incomplete	Determination that insufficient digits are received. See Note in 6.1. Receipt of subsequent INVITE within overlap procedure, see 6.2.	Not applicable.
480 Temporarily Unavailable	Congestion at the IWU.	Not applicable.
BYE	BICC/ISUP procedures result in release after answer.	According to BICC/ISUP procedures.
500 Server Internal Error	Call release due to the BICC/ISUP compatibility procedure (Note)	According to BICC/ISUP procedures.
484 Address Incomplete	Call release due to expiry of T7 within the BICC/ISUP procedures	According to BICC/ISUP procedures.
480 Temporarily Unavailable	Call release due to expiry of T9 within the BICC/ISUP procedures	According to BICC/ISUP procedures.
480 Temporarily Unavailable	Other BICC/ISUP procedures result in release before answer	According to BICC/ISUP procedures.
NOTE – If the I-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, then see 2.9.5.2/Q.764 and 13.4.3/Q.1902.4.		

6.11.4 Receipt of RSC, GRS or CGB (ISUP)

Table 23 shows the message sent by the I-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.

a) The I-IWU sends BYE if it has already received an ACK for the 200 OK INVITE it had sent.

b) If I-IWU has sent 200 OK INVITE but has not yet received an ACK for the 200 OK INVITE, then the I-IWU shall wait until it receives the ACK for the 200 OK INVITE before sending the BYE.

c) In all other cases the I-IWU sends 500 Server Internal Error.

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 Profile C (SIP-I) case, the SIP BYE or 500 Server Internal Error message shall encapsulate the REL generated by ISUP procedures, rather than the RSC, GRS or CGB message which caused it to be generated.

Table 23/Q.1912.5 – Receipt of RSC, GRS or CGB messages (ISUP)

← SIP	← Message received from ISUP
500 Server Internal Error or BYE	Reset Circuit message (RSC)
500 Server Internal Error or BYE	Circuit Group Reset message (GRS)
500 Server Internal Error or BYE	Circuit Group Blocking message (CGB) with the Circuit Group Supervision Message Type indicator coded *"hardware failure oriented"*

6.11.5 Receipt of RSC or GRS (BICC)

Table 24 shows the message sent by the I-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.

a) The I-IWU sends BYE if it has already received an ACK for the 200 OK INVITE it had sent.

b) If the I-IWU has sent 200 OK but has not yet received an ACK for the 200 OK INVITE, then the I-IWU shall wait until it receives the ACK for the 200 OK INVITE before sending the BYE.

c) In all other cases, the I-IWU sends 500 Server Internal Error.

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 Profile C (SIP-I) case, the SIP BYE or 500 Server Internal Error message shall encapsulate the REL generated by BICC procedures, rather than the RSC or GRS message which caused it to be generated.

Table 24/Q.1912.5 – Receipt of RSC or GRS messages (BICC)

← SIP	← Message received from BICC
500 Server Internal Error or BYE	Reset CIC message (RSC)
500 Server Internal Error or BYE	CIC Group Reset message (GRS)

7 Outgoing call interworking from BICC/ISUP to SIP at O-IWU

An Outgoing Interworking Unit (O-IWU) 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 O-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 O-IWU and the preceding BICC or ISUP entity.

The O-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 O-IWU may signal to subsequent SIP nodes or preceding BICC/ISUP entities.

If the address information received from the preceding BICC/ISUP exchange is not in the form of an E.164 international public telecommunication number, the O-IWU shall add the country code or the country code and national destination code of the preceding exchange to form the international public telecommunication number.

This clause specifies the signalling interworking requirements for a basic call at the O-IWU. It is split into subclauses based upon the messages sent or received on the outgoing (SIP) interface of the O-IWU. Only messages that are generated as a result of interworking to/from the incoming BICC/ISUP side of the O-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 Recommendation.

In the case of Type 2 or 4 Gateways as defined in ITU-T Supplement 45 to Q-series Recommendations (TRQ.2815), the O-IWU shall (in addition to the procedures outlined within this clause) follow the BICC-specific procedures outlined in clause A.2.

For Profile C (SIP-I) operation, ISUP message segmentation must be handled as described in 5.4.3.3.

7.1 Sending of the first INVITE

After performing the normal BICC/ISUP handling for incoming address messages (IAM possibly followed by SAMs) and 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 then 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) by observing that timer T_{OIW1} has expired.

   If end of address signalling is determined in accordance with criteria a, b and c above, timer T_{OIW2} shall be started on sending of the INVITE.

NOTE 1 – *En bloc* is preferred, and is required for Profile A.

2) If overlap addressing is to be used toward the SIP network, then, after the minimum number of digits required for routing the call has been received, the O-IWU shall:

   – start timer T_{OIW2} and invoke the appropriate outgoing SIP signalling procedure as described in this clause; and

– be prepared to process SAM as described in 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 precondition upon receipt of ISUP IAM/SAM.

B) Send INVITE with precondition upon receipt of ISUP IAM/SAM.

C) Send INVITE without precondition upon receipt of BICC IAM/SAM.

D) Send INVITE with precondition upon receipt of BICC IAM/SAM.

Details of the procedures are described in this clause. Coding of the INVITE sent by the O-IWU is specified in 7.1.1 through 7.1.5.

For Profile C (SIP-I), the IAM resulting from the application of BICC/ISUP procedures and the procedures of this clause is encapsulated in the outgoing INVITE.

If timer T_{OIW2} expires, an early ACM is sent to the ISUP or BICC network. See 7.4.

A) Sending INVITE without precondition for ISUP IAM/SAM

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

INVITE is sent when the ISUP IAM (possibly followed by SAMs) is received 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*". INVITE shall not be sent if the Continuity message is received with the Continuity Indicators parameter set to "*continuity check failed*" or the ISUP timer T8 expires.

B) Sending INVITE with precondition for ISUP IAM/SAM

INVITE with precondition is sent on receipt of ISUP IAM (possibly followed by SAMs). Incoming ISUP procedures apply, with the following clarifications and exceptions as to when a confirmation of the precondition being met is to be sent.

NOTE 2 – Configured procedures may delay the INVITE until local resources have been reserved on the outgoing bearer path.

The O-IWU should initiate the precondition signalling procedure using the SDP offer in the INVITE. The precondition signalling is concluded upon sending (within an SDP offer-answer exchange) the confirmation of a precondition being met. The SDP offer or answer carrying the confirmation of a 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 preconditions are met in the SIP network.

   NOTE 3 – For Profile A, the signalling of "preconditions being met" always occurs within the SDP offer in the UPDATE message.

CANCEL or BYE (according to the rule in 7.7.1) shall be sent if the Continuity message is received with the Continuity Indicators parameter set to "*continuity check failed*" or the ISUP timer T8 expires.

REL with Cause Value 47 (resource unavailable, unspecified) shall be sent on the ISUP side of the O-IWU and CANCEL or BYE (according to the rule in 7.7.1) shall be sent on the SIP side if internal resource reservation was unsuccessful. See 7.7.3 for further details.

C) INVITE without precondition for BICC IAM/SAM

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 (7.5/Q.1902.4):

   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.

INVITE shall not be sent if the Continuity message is not received, i.e., the BICC timer T8 expires.

D) INVITE with precondition for BICC IAM/SAM

INVITE with precondition is sent on receipt of BICC IAM (possibly followed by SAMs). Incoming BICC procedures apply, with the following clarifications and exceptions as to when a confirmation of the precondition being met is to be sent.

NOTE 4 – Configured procedures may delay the INVITE until local resources have been reserved on the outgoing bearer path.

The O-IWU should initiate the precondition signalling procedure using the SDP offer in the INVITE. The precondition signalling is concluded upon sending the (within an SDP offer-answer exchange) confirmation of a precondition being met. The SDP offer or answer carrying the confirmation of a precondition being met is sent when all 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 (7.5/Q.1902.4), 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 preconditions are met in the SIP network.

NOTE 5 – For Profile A, the signalling of "preconditions being met" always occurs within the SDP offer in the UPDATE message.

CANCEL or BYE (according to the rule in 7.7.1) shall be sent if the Continuity message is not received, i.e., the BICC timer T8 expires.

REL with Cause Value 47 (resource unavailable, unspecified) shall be sent on the ISUP side of the O-IWU and CANCEL or BYE (according to the rule in 7.7.1) shall be sent on the SIP side if internal resource reservation was unsuccessful. See 7.7.3 for further details.

For all cases of sending INVITE (A, B, C and D), Table 25 provides a summary of how the header fields within the outgoing INVITE message are populated.

Table 25/Q.1912.5 – Interworked contents of the INVITE message

IAM→	INVITE→
Called Party Number	Request-URI (see 7.1.2 and 7.2)
	To (see 7.1.2)
Calling Party Number	P-Asserted-Identity (see 7.1.3)
	Privacy (see 7.1.3)
	From (see 7.1.3)
Generic Number (*"additional calling party number"*)	From (see 7.1.3)
Hop Counter	Max-Forwards (see 7.1.4)
TMR/USI	Message Body (application/SDP) (see 7.1.1)
ISUP Message	Message Body (application/ISUP) (Note)
NOTE – Profile C only. See 5.4.1.2	

7.1.1 Coding of SDP media description lines from TMR/USI

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. ITU-T Recs Q.1902.3 and Q.763 provide exhaustive listing of the available codes in the TMR and USI parameters. Generally, any combination of those codes can be mapped into any SDP information as long as transcoding is available.

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) and Adaptive Multi-Rate Wideband (AMR-WB) audio codec".

If the O-IWU operates as an international outgoing gateway and if G.711 encoding is offered then the following cases apply. These procedures reflect the requirement that transcoding between A-law and μ-law has to occur in a μ-law network only.

– If the call is coming from an A-law PSTN network, the O-IWU shall send an SDP Offer with A-law (PCMA), but not μ-law (PCMU) included in the media description.

– If the call is coming from a μ-law PSTN network, the O-IWU shall send an SDP Offer with both μ-law (PCMU) and A-law (PCMA) included in the media description and PCMU shall take precedence over PCMA.

7.1.1.1 Transcoding not available at the O-IWU

Table 26 provides the mapping relations from TMR/USI codes to SDP media description lines when transcoding is not available at the O-IWU.

Table 26/Q.1912.5 – Coding of SDP media description lines from TMR/USI: BICC/ISUP to SIP

TMR 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>	a=rtpmap:<payload type> <encoding name>/ <clock rate> [/<encoding parameters>]
"speech"	*"Speech"*	*"G.711 μ-law"*	Ignore	audio	RTP/AVP	0 (and possibly 8) (Note 1)	AS:64	rtpmap:0 PCMU/8000 (and possibly rtpmap:8 PCMA/8000) (Note 1)
"speech"	*"Speech"*	*"G.711 μ-law"*	Ignore	audio	RTP/AVP	Dynamic PT (and possibly a second Dynamic PT) (Note 1)	AS:64	rtpmap:<payload type> PCMU/8000 (and possibly rtpmap:<payload type> PCMA/8000) (Note 1)
"speech"	*"Speech"*	*"G.711 A-law"*	Ignore	audio	RTP/AVP	8	AS:64	rtpmap:8 PCMA/8000
"speech"	*"Speech"*	*"G.711 A-law"*	Ignore	audio	RTP/AVP	Dynamic PT	AS:64	rtpmap:<payload type> PCMA/8000
"3.1 kHz audio"	USI Absent		Ignore	audio	RTP/AVP	0 and/or 8 (Note 1)	AS:64	rtpmap:0 PCMU/8000 and/or rtpmap:8 PCMA/8000 (Note 1)
"3.1 kHz audio"	*"3.1 kHz audio"*	*"G.711 μ-law"*	(Note 3)	audio	RTP/AVP	0 (and possibly 8) (Note 1)	AS:64	rtpmap:0 PCMU/8000 (and possibly rtpmap:8 PCMA/8000) (Note 1)
"3.1 kHz audio"	*"3.1 kHz audio"*	*"G.711 A-law"*	(Note 3)	audio	RTP/AVP	8	AS:64	rtpmap:8 PCMA/8000
"3.1 kHz audio"	*"3.1 kHz audio"*		*"Facsimile Group 2/3"*	image	udptl	t38	AS:64	Based on ITU-T Rec. T.38.
"3.1 kHz audio"	*"3.1 kHz audio"*		*"Facsimile Group 2/3"*	image	tcptl	t38	AS:64	Based on ITU-T Rec. T.38.

Table 26/Q.1912.5 – Coding of SDP media description lines from TMR/USI: BICC/ISUP to SIP

TMR 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>	a=rtpmap:<payload type> <encoding name>/ <clock rate> [/<encoding parameters>]
"64 kbit/s unrestricted"	*"Unrestricted digital inf. W/tone/ann."*	N/A	Ignore	audio	RTP/AVP	9	AS:64	rtpmap:9 G722/8000
"64 kbit/s unrestricted"	*"Unrestricted digital information"*	N/A	Ignore	audio	RTP/AVP	Dynamic PT	AS:64	rtpmap:<payload type> CLEARMODE/8000 (Note 2)
"2 x 64 kbit/s unrestricted"	*"Unrestricted digital information"*	N/A	Ignore	FFS	FFS	FFS	FFS	FFS
"384 kbit/s unrestricted"	*"Unrestricted digital information"*	N/A	Ignore	FFS	FFS	FFS	FFS	FFS
"1536 kbit/s unrestricted"	*"Unrestricted digital information"*	N/A	Ignore	FFS	FFS	FFS	FFS	FFS
"1920 kbit/s unrestricted"	*"Unrestricted digital information"*	N/A	Ignore	FFS	FFS	FFS	FFS	FFS
"N × 64 kbit/s unrestricted", N from 3 to 29	*"Unrestricted digital information"*	N/A	Ignore	FFS	FFS	FFS	FFS	FFS

NOTE 1 – Both PCMA and PCMU required under the conditions stated in 7.1.1.

NOTE 2 – Since CLEARMODE has not yet been standardized, its use is for further study.

NOTE 3 – HLC normally absent in this case. It is possible for HLC to be present with the value "Telephony", although 6.3.1/Q.939 indicates that this would normally be accompanied by a value of "Speech" for the Information Transfer Capability element.

7.1.2 Request-URI and To header field

The Called Party Number parameter of the IAM and possibly the Address Signals indicators in the Subsequent Number parameter of SAMs contain the forward address information to derive the userinfo component of the INVITE Request-URI.

NOTE – The O-IWU follows existing BICC/ISUP procedures 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 address information contained in the Called Party Number parameter (and Subsequent Number parameters, if any) is also considered as the identification of the called party. This information is used to derive the addr-spec component of the To header field.

If the Request-URI or the To header field contains a sip: URI, it shall include the "user=phone" URI parameter.

7.1.3 P-Asserted-Identity, From and Privacy header fields

Table 27 shows the mapping from Calling Party Number and Generic Number to the SIP P-Asserted-Identity, From, and Privacy header fields in the INVITE. Table 28 provides details for mapping Generic Number to the From header field. Table 29 provides details for the mapping from Calling Party Number to P-Asserted-Identity, while Table 30 provides details for the mapping from Calling Party Number to the From header field. Finally, Table 31 provides details for mapping from the APRI subfields of Calling Party Number and Generic Number into the Privacy header field.

If the From or the P-Asserted-Identity header field contains a sip: URI, it shall include the "user=phone" URI parameter.

Table 27/Q.1912.5 – Mapping of 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 = "UPVP", 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 4)	Y	Header field not included	display-name derived from Generic Number (ACgPN) if possible addr-spec derived from Generic Number (ACgPN) address signals or uses network provided value	Header field not included
Y (Note 1)	N	Derived from Calling Party Number parameter Address Signals (See Table 29)	if APRI = "*presentation allowed*", display-name may be derived from Calling Party Number (CgPN) if possible if APRI = "*presentation restricted*", display-name is "Anonymous"	If Calling Party Number parameter APRI = "*presentation restricted*" then priv-value includes "*id*". For other APRI settings Privacy header is not included or if included, "id" is not included (See Table 31)
			if APRI = "*presentation allowed*", addr-spec is derived from Calling Party Number parameter Address Signals (see Table 30) or uses network provided value if APRI = "*presentation restricted*", addr-spec is set to the "Anonymous URI" (Note 3)	
Y	Y	Derived from Calling Party Number parameter Address Signals (See Table 29)	display-name may be derived from Generic Number (ACgPN) (Note 2)	If Calling Party Number parameter APRI = "*presentation restricted*" then priv-value includes "id" . For other APRI settings Privacy header is not included or if included, "id" is not included (See Table 31)
			addr-spec is derived from Generic Number (ACgPN) Address Signals (see Table 28)	

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. It is also considered suitable to map into the P-Asserted-Identity header since, in this context, it is a fully authenticated CLI related exclusively to the calling line and, therefore, as valid as a User Provided Verified and Passed CLI for this purpose.

NOTE 2 – Whether it is possible to derive the display-name from the Generic Number Parameter is FFS.

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". The Anonymous URI itself should have the value "anonymous@anonymous.invalid".

NOTE 4 – This combination of CgPN and ACgPN is an error case but is shown here to ensure consistent mapping across different implementations.

Table 28/Q.1912.5 – Mapping of Generic Number (*"additional calling party number"*) to SIP From header field

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 IWU is located) to Generic Number Address Signals then map to user portion of URI scheme used.
	"*international number"*		Map complete GenericNumber Address Signals to user portion of URI scheme used.
Address Signals	if NOA is "*national (significant) number"* then the format of the address signals is: NDC + SN If NOA is "*international number"* then the format of the address signals is: CC + NDC + SN	Display-name	display-name may be mapped from Address Signals, if possible and network policy allows it.
		Addr-spec	"+" CC NDC SN mapped to user portion of URI scheme used

Table 29/Q.1912.5 – Mapping of Calling Party Number parameter to SIP P-Asserted-Identity header field

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 IWU is located) to CgPN Address Signals then map to URI
	"international number"		Map complete CgPN Address Signals to URI
Address Signals	If NOA is "*national (significant) number"* then the format of the Address Signals is: NDC + SN If NOA is "*international number"* then the format of the address signals is: CC + NDC + SN	display-name	display-name may be mapped from Address Signals, if possible and network policy allows it
		addr-spec	"+" CC NDC SN mapped to the appropriate global number portion of URI scheme used

Table 30/Q.1912.5 – Mapping of BICC/ISUP Calling Party Number parameter to SIP From header field

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 IWU is located) to CgPN Address Signals then map to user portion of URI scheme used.
	"international number"		Map complete CgPN Address Signals to user portion of URI scheme used.
Address Signals	If NOA is "*national (significant) number"* then the format of the Address Signals is: NDC + SN If NOA is "*international number"* then the format of the Address Signals is: CC + NDC + SN	display-name	Display-name may be mapped from Address Signals, if possible and network policy allows it.
		addr-spec	"+" CC NDC SN mapped to userinfo portion of URI scheme used

Table 31/Q.1912.5 – Mapping of BICC/ISUP APRIs into SIP Privacy header field

BICC/ISUP Parameter/field	Value	SIP component	Value
Calling Party Number		Privacy header field	priv-value
APRI (See Table 27 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 is received, P-Asserted-Identity header is always derived from it as in Table 27.			

7.1.4 Hop Counter (Optional)

For Profile C (SIP-I), if the Hop Counter parameter is available, then the O-IWU acting as an independent exchange shall perform the normal BICC/ISUP Hop Counter procedure as it constructs the outgoing encapsulated IAM.

For Profiles A and B the O-IWU shall derive the Max-Forwards header field value from the Hop Counter value when that is available. It shall do so by applying a factor to the Hop Counter value as shown in Table 32, where the factor is constructed according to the following principles:

a) Max-Forwards for a given message should never increase, and should decrease by at least 1 with each successive visit to an IWU, regardless of intervening interworking, and similarly for Hop Counter in the BICC/ISUP domain.

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.

Table 32/Q.1912.5 – Mapping from Hop Counter to Max-Forwards

Hop Counter value	Max-Forwards value
X	Y = Integer part of (X * Factor)

NOTE – The preceding rules imply that the mapping between Max-Forwards and Hop Counter will take account of the topology of the networks traversed. Since call routing and thus the number of hops taken will depend on the origin and destination of the call, the mapping factor used to derive Max-Forwards from Hop Counter should be similarly dependent on call origin and destination. Moreover, when call routing crosses administrative boundaries, the operator of the O-IWU will coordinate with adjacent administrations to provide a mapping at the O-IWU which is consistent with the initial settings or mapping factors used in the adjacent networks.

In summary, the factor used to map from Hop Counter to Max-Forwards for a given call will depend on call origin and call destination, and will be provisioned at the O-IWU based on network topology, trust domain rules, and bilateral agreement.

7.1.5 Coding of encapsulated ISUP IAM parameters in outgoing INVITE (Profile C (SIP-I) only)

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

7.1.5.1 Nature of Connection Indicators

The O-IWU shall increment the satellite indicator in the Nature of Connection Indicators parameter.

7.1.5.2 Propagation Delay Counter

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

7.2 Receipt of SAM after INVITE has been sent

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

7.2.1 Overlap procedures upon receipt of SAM

On receipt of a SAM from the BICC/ISUP procedures running at the incoming side of the O-IWU, the O-IWU shall:

1) Stop timer T_{OIW3} (if it is running).

2) T_{OIW2} shall be restarted and the O-IWU shall invoke the appropriate outgoing signalling procedure A, B, C, or D as described in 7.1, with the following additional procedures:

   a) The Request-URI and the To header field of the new INVITE shall contain all digits received so far for this call.

b) A new INVITE with the same Call-ID and From header (including tag) as the previous INVITE is sent. In the Profile C (SIP-I) case, the IAM which was sent with the original INVITE is also encapsulated in the new INVITE.

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

d) All other contents of the new INVITE are interworked from the parameters of the original IAM as per 7.1.

If timer T_{OIW2} has expired, subsequent SAMs received after the O-IWU has sent the INVITE are ignored.

7.3 Receipt of 18X response

Table 33 provides a summary of the interworking of 18X messages to ISUP messages. For further details please see the reference clause given in each table row.

Table 33/Q.1912.5 – Receipt of 18X response

← ISUP message	← 18X response
ACM or CPG (Note 1)	180 Ringing
ACM or CPG (Note 2) for Profile C (SIP-I) only	183 Session Progress with encapsulated ACM or CPG
NOTE 1 – See 7.3.1. NOTE 2 – See 7.3.2.	

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

7.3.1 Receipt of 180 Ringing

On receipt of a 180 Ringing message, timer T_{OIW2} (if running) is stopped. If a 180 Ringing is received without any encapsulated ISUP message, the O-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.

For Profile C (SIP-I), if 180 Ringing is received with encapsulated ACM or CPG message, the O-IWU shall determine the appropriate backward BICC/ISUP message and parameters based on the encapsulated ISUP message and existing BICC/ISUP signalling state. Timer T_{OIW2} shall be stopped (if running).

7.3.1.1 Setting for ACM Backward Call Indicators (mandatory) (Profiles A and B only)

The table within this clause presents the default values of Backward Call Indicators parameter that are set by the O-IWU when ACM is sent. Other values of the Backward Call Indicators parameter are set according to BICC/ISUP procedures.

The indicators of the BCI parameter, which are set by the O-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 profiles A and B, Called Party's Status Indicator (Bit DC) is set to "*subscriber free*".

For Profile A, the default settings are shown in Table 34.

Table 34/Q.1912.5 – Default Backward Call Indicators settings for Profile A

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, the O-IWU shall set the appropriate values of other indicators in the Backward Call Indicators parameter (other than Called Party's Status Indicator) based on analysis of various information such as signalling, internal states and/or local policies.

7.3.1.2 Settings for Event Information (mandatory) in CPG (Profiles A and B only)

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

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

The code in Table 35 shall be set by the O-IWU in the Event Information parameter on receipt of 180 Ringing.

Table 35/Q.1912.5 – Coding of Event Indicator for Profiles A and B

Bits	Codes	Meaning
G F E D C B A	0 0 0 0 0 0 1	*"alerting"*

7.3.2 Receipt of 183 Session Progress

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

For Profile C (SIP-I), if 183 Session Progress is received with encapsulated ISUP, the O-IWU shall determine the appropriate backward BICC/ISUP message based on the encapsulated ISUP message and existing BICC/ISUP signalling state. Timer T_{OIW2} shall be stopped in this case.

7.4 Expiry of timers and sending of early ACM

When either timer T_{OIW1} (in the case of calls converted to *en bloc* at the outgoing SIP interface) or timer T_{OIW2} expires, the O-IWU shall return ACM. In the case that the continuity check is performed (ISUP) or COT is expected (BICC), the O-IWU shall withhold sending ACM until a successful continuity indication has been received. For Profiles 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 indicators of the BCI parameter shall be set as described in 7.3.1.1.

7.5 Receipt of 200 OK INVITE

When the O-IWU receives a 200 OK INVITE for this call, it shall stop timer T_{OIW2} (if running).

For Profiles A and B the O-IWU shall:

1) Send ANM or CON as determined by BICC/ISUP procedures.

2) Stop any existing awaiting answer indication (e.g., ringing tone).

For Profile C (SIP-I), if 200 OK INVITE is received with encapsulated CON or ANM message, the O-IWU shall determine the appropriate backward BICC/ISUP message and parameters based on the encapsulated ISUP message and existing BICC/ISUP signalling state.

7.5.1 Setting of Backward Call Indicators in the CON message (Profiles A and B only)

The Called Party's Status Indicator (Bit DC) of BCI parameter is set to *"no indication"*. The other indicators of the BCI parameter shall be set as described in 7.3.1.1.

7.6 Through connection of BICC/ISUP bearer path

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

For Profiles 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 ASN. If the ASN supports the Q.764 procedures for through connection at a destination exchange, the O-IWU shall follow the procedures specified for Profile C (SIP-I).

For Profile C (SIP-I), the following procedures shall apply.

Through connection of the bearer path shall be completed dependent upon whether or not 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 acceptable to the O-IWU and an indication that all mandatory 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.

7.6.1 Tone and announcement (backward)

For Profiles A and B, 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; and

3) the local arrangements assign the role of destination exchange to the O-IWU rather than the associated SIP entity.

NOTE 1 – It is possible that ringing tone or a progress announcement is already being played as a result of T_{OIW1} or T_{OIW2} expiry. See 7.4.

NOTE 2 – In the case that the associated SIP entity performs the functions of the destination exchange, other tones or announcements may be received from the SIP network.

7.7 Release procedures at the O-IWU

7.7.1 Receipt of forward REL

Upon receipt of a BICC or ISUP REL message:

1) REL received before INVITE has been sent: no action is required on the SIP side other than to terminate local procedures if any are in progress.

2) REL message received before any response has been received to the INVITE: The O-IWU shall hold the REL message until a SIP response has been received. At that point, it shall take action 3 or 4 as appropriate.

3) REL message received at O-IWU before a response has been received which establishes a confirmed dialogue or early dialogue:

The O-IWU shall send a CANCEL request. If the O-IWU subsequently receives a 200 OK INVITE, then it shall send an ACK for the 200 OK INVITE and subsequently send a BYE request after the ACK has been sent.

4) REL message received at O-IWU after a response has been received which establishes a confirmed dialogue or early dialogue:

The O-IWU shall send a BYE request. For Profiles A and B, for an early dialog only, CANCEL may be used instead.

For Profile C (SIP-I), if a BYE message is sent, it shall encapsulate the received REL message.

Depending on local policy, a Reason header field containing the received (Q.850) Cause Value of the REL message may be added to the CANCEL or BYE request. The mapping of the Cause Indicators parameter to the Reason header is shown in Table 20 (see 6.11.2).

7.7.2 Receipt of backward BYE

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

On receipt of SIP BYE, the O-IWU shall invoke the BICC Release sending procedure (ITU-T Rec. Q.1902.4) on the BICC side.

In the case of Profile C (SIP-I), the encapsulated REL shall be passed to ISUP/BICC procedures without modification.

For Profile A or B

If a Reason header field with Q.850 Cause Value is included in the BYE, then the Cause Value may be mapped to the ISUP Cause Value field in the ISUP REL depending on local policy. The mapping of the Reason header to the Cause Indicators parameter is shown in Table 18 (see 6.11.1). Table 36 shows the coding of the Cause Value in the REL message if it is not available from the Reason header field.

Table 36/Q.1912.5 – Release from SIP side at O-IWU

←REL Cause Indicators parameter	**←SIP message**
Cause Value No. 16 ("*normal call clearing*")	BYE

7.7.3 Autonomous release at O-IWU

Table 37 shows the trigger events at the O-IWU and the release initiated by the O-IWU when the call is traversing from BICC/ISUP to SIP.

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

Depending on local policy, a Reason header field containing the (Q.850) Cause Value of the REL message sent by the O-IWU may be added to the SIP Message (BYE or CANCEL) to be sent by the SIP side of the O-IWU.

Table 37/Q.1912.5 – Autonomous Release at O-IWU

REL ← Cause Indicators parameter	Trigger event	→ SIP
As determined by BICC/ISUP procedure.	COT received with the Continuity Indicators parameter set to "*continuity check failed*" (ISUP only) or the BICC/ISUP timer T8 expires.	Send CANCEL or BYE according to the rule described in 7.7.1.
REL with cause value 47 (resource unavailable, unspecified).	Internal resource reservation unsuccessful	As determined by SIP procedure
As determined by BICC/ISUP procedure.	BICC/ISUP procedures result in generation of autonomous REL on BICC/ISUP side.	CANCEL or BYE according to the rule described in 7.7.1.
Depending on the SIP release reason.	SIP procedures result in a decision to release the call.	As determined by SIP procedure.

7.7.4 Receipt of RSC, GRS or CGB (ISUP)

Table 38 shows the message sent by the O-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*".

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.

The O-IWU shall send CANCEL or BYE according to the rule described in 7.7.1.

Depending on local policy, a Reason header field containing the (Q.850) Cause Value of the REL message sent by the O-IWU may be added to the SIP message (BYE or CANCEL) to be sent by the SIP side of the O-IWU.

In the Profile C (SIP-I) case the RSC, GRS or CGB ISUP messages shall not be encapsulated, but if a BYE request is sent, it shall encapsulate the REL message that would be sent towards a forward ISUP node.

Table 38/Q.1912.5 – 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

7.7.5 Receipt of RSC or GRS (BICC)

Table 39 shows the message sent by the O-IWU upon receipt of a BICC RSC message or GRS message.

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.

The O-IWU shall send CANCEL or BYE according to the rule described in 7.7.1.

Depending on local policy, a Reason header field containing the (Q.850) Cause Value of the REL message sent by the O-IWU may be added to the SIP message (BYE or CANCEL) to be sent by the SIP side of the O-IWU. In the Profile C (SIP-I) case the RSC or GRS messages shall not be encapsulated, but if a BYE request is sent, it shall encapsulate the REL message that would be sent towards a forward ISUP node.

Table 39/Q.1912.5 – Receipt of RSC or GRS (BICC) at O-IWU

Message received from BICC →	SIP →
Reset Circuit/CIC message (RSC)	CANCEL or BYE
Circuit/CIC Group Reset message (GRS)	CANCEL or BYE

7.7.6 Receipt of 4XX, 5XX, 6XX responses to INVITE

If a Reason header is included in a 4XX, 5XX, 6XX, then the Cause Value of the Reason header should be mapped to the ISUP Cause Value field in the ISUP REL message. The mapping of the Reason header to the Cause Indicators parameter is shown in Table 18 (see 6.11.1). Otherwise, the mapping from status code to Cause Value on receipt of a 4XX, 5XX or 6XX final response to the INVITE on the SIP side is described within Table 40.

For Profile C, if an encapsulated REL is received it shall be passed to BICC/ISUP procedures without modification. In all other cases the procedures in the remainder of this clause apply.

In all cases where SIP itself, or subclauses to this clause specify additional SIP side behaviour related to the receipt of a particular INVITE response, these procedures should be followed in preference to the immediate sending of a REL message to BICC/ISUP.

If there are no SIP side procedures associated with this response, the REL shall be sent immediately.

NOTE – Depending upon the SIP side procedures applied at the O-IWU, it is possible that receipt of certain 4XX/5XX/6XX responses to an INVITE may in some cases not result in any REL message being sent to the BICC/ISUP network. For example, if a 401 Unauthorized response is received and the O-IWU successfully initiates a new INVITE containing the correct credentials, the call will proceed.

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 Value 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 to sustain the call) fail, resulting in the ISUP half call being released by sending a REL message with the Cause Value indicated.

When the response to the INVITE results in the BICC/ISUP REL message with cause 127 "*Interworking*" being sent, then the location should be set to (BI) "*network beyond interworking point*".

Table 40/Q.1912.5 – Receipt of 4XX, 5XX or 6XX at O-IWU

← REL (Cause Value)	← 4XX/5XX/6XX SIP message	Remarks
127 Interworking	400 Bad Request	
127 Interworking	401 Unauthorized	(Note 1)
127 Interworking	402 Payment Required	
127 Interworking	403 Forbidden	
1 Unallocated number	404 Not Found	
127 Interworking	405 Method Not Allowed	
127 Interworking	406 Not Acceptable	
127 Interworking	407 Proxy authentication required	(Note 1)
127 Interworking	408 Request Timeout	
22 Number changed (without diagnostic)	410 Gone	
127 Interworking	413 Request Entity too long	(Note 1)
127 Interworking	414 Request-uri too long	(Note 1)
127 Interworking	415 Unsupported Media type	(Note 1)
127 Interworking	416 Unsupported URI scheme	(Note 1)
127 Interworking	420 Bad Extension	(Note 1)
127 Interworking	421 Extension required	(Note 1)
127 Interworking	423 Interval Too Brief	
20 Subscriber absent	480 Temporarily Unavailable	
127 Interworking	481 Call/Transaction does not exist	
127 Interworking	482 Loop Detected	
127 Interworking	483 Too many hops	
28 Invalid Number format	484 Address Incomplete	(Note 1)
127 Interworking	485 Ambiguous	
17 User busy	486 Busy Here	
127 Interworking or no mapping (Note 3)	487 Request terminated	(Note 2)
127 Interworking	488 Not acceptable here	
No mapping	491 Request Pending	(Note 2)
127 Interworking	493 Undecipherable	
127 Interworking	500 Server Internal error	
127 Interworking	501 Not implemented	
127 Interworking	502 Bad Gateway	
127 Interworking	503 Service Unavailable	(Note 1)
127 Interworking	504 Server timeout	

Table 40/Q.1912.5 – Receipt of 4XX, 5XX or 6XX at O-IWU

← REL (Cause Value)	← 4XX/5XX/6XX SIP message	Remarks
127 Interworking	505 Version not supported	(Note 1)
127 Interworking	513 Message too large	(Note 1)
127 Interworking	580 Precondition failure	(Note 1)
17 User busy	600 Busy Everywhere	
21 Call rejected	603 Decline	
1 Unallocated number	604 Does not exist anywhere	
127 Interworking	606 Not acceptable	
NOTE 1 – This response may be handled entirely on the SIP side; if so, it is not interworked. NOTE 2 – This response does not terminate a SIP dialog, but only a specific transaction within it. NOTE 3 – No mapping if the O-IWU previously issued a CANCEL request for the INVITE.		

7.7.6.1 Special handling of 484 Address Incomplete response when T_{OIW3} is in use

On receipt of a 484 Address Incomplete response for the current INVITE (i.e., there are no other pending INVITE transactions for this call), if the O-IWU is configured to propagate overlap signalling into the SIP network, the O-IWU shall not send a REL message immediately and shall instead start timer T_{OIW3}. The REL message shall only be sent if T_{OIW3} expires. If the O-IWU is not configured to propagate overlap signalling into the SIP network, then the timer shall not be started and the REL shall be sent immediately to the BICC/ISUP network.

7.7.6.2 Special handling of 580 Precondition Failure received in response to either an INVITE or UPDATE

A 580 Precondition failure response may be received as a response either to an INVITE or to an UPDATE request.

7.7.6.2.1 580 Precondition Failure response to an INVITE

Release with Cause Value, as indicated in Table 40, is sent immediately to the BICC/ISUP network.

7.7.6.2.2 580 Precondition Failure response to an UPDATE within an early dialog

Release with Cause Code 127 "*Interworking*" is sent immediately to the BICC/ISUP network. A BYE request is sent for the INVITE transaction within which the UPDATE was sent.

7.8 Timers at O-IWU

Table 41 defines the interworking timers introduced in clause 7.

Table 41/Q.1912.5 – Interworking timers

Symbol	Timeout value	Cause for initiation	Normal termination	At expiry	Reference
T_{OIW1}	4-6 seconds (default of 4 seconds)	On receipt of an IAM or SAM after the minimum number of digits required for routing the call has been received, if the end of address signalling has not been determined.	At the receipt of fresh address information.	Send the initial INVITE, return an ACM. For profiles A and B only, send the awaiting answer indication (e.g., ring tone) or appropriate progress announcement to the calling party.	7.1, 7.4 (Note 1)
T_{OIW2}	4-14 seconds (default of 4 seconds)	Sending of INVITE unless the ACM has already been sent.	On receipt of 484 Address Incomplete for the current INVITE, 180 Ringing, 183 Session Progress with encapsulated ACM, or 200 OK INVITE	Send early ACM. For profiles A and B only, send the awaiting answer indication (e.g. ring tone) or appropriate progress announcement to the calling party.	7.1, 7.2.1, 7.3.1, 7.4, 7.5 (Note 2)
T_{OIW3}	4-6 seconds (default of 4 seconds)	On receipt of 484 Address Incomplete for the current INVITE if there are no other pending INVITE transactions for this call.	At the receipt of fresh address information.	Send REL with Cause Value 28 to the BICC/ISUP side.	7.2.1, 7.7.6.1 (Note 3)

NOTE 1 – This timer is used for ISUP overlap to SIP *en bloc* conversion.

NOTE 2 – This timer is used to send an early ACM if a delay is encountered in receiving a response from the subsequent SIP network.

NOTE 3 – This timer is known as the "SIP dialog protection timer". This timer is only used where the O-IWU is configured to propagate ISUP overlap signalling into the SIP network.

8 Bibliography (informative)

[1] ITU-T Q-series Recommendations – Supplement 45 (2003), *Technical Report TRQ.2815*: *Requirements for interworking BICC/ISUP network with originating/destination networks based on SIP and SDP*.

[2] ITU-T Recommendation Q.939 (1993), *Typical DSS1 service indicator codings for ISDN telecommunications services*.

Annex A

BICC specific interworking for basic call

A.1 Introduction

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

A.2 Interworking 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 CS-2, the only defined Bearer Control Protocol carried by the Bearer Control Tunnelling mechanism is IPBCP (ITU-T Rec. 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 IPBCP, the procedures for this interworking function are defined in A.3.1.

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 RFC 3264 and RFC 3261 are used to determine the SIP message that 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 Protocol Data Unit as described in A.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 A.2.1.1.

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 ITU-T Rec. Q.1902.4. The INVITE is mapped to an IAM as described in 7.1.

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 ITU-T Rec. Q.1902.4. The INVITE is mapped to an IAM as described in 7.1.

A.2.2.1.2 APM

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

A.2.2.1.3 PRACK

On receipt of a PRACK message, responding to the 183 Session Progress response sent in A.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 A.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 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 Q.1902.4 procedures.

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.

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 A.2.1.3 determine the SIP message to send.

A.2.3 Preconditions

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.

Preconditions are handled on the SIP side using the mechanisms of RFC 3312 which are based on attributes within the SDP.

Preconditions are handled on the BICC side using the continuity mechanism as described in ITU-T Rec. Q.1902.4 to delay continuation of call setup until all preconditions to call setup have been met.

Note that BICC provides mechanisms to indicate the existence and completion of 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:

– precondition required;

– precondition met.

Similarly, when the BICC mechanism requires 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 be passed from the BICC protocol procedures to the Bearer Control Interworking Function:

• precondition required;

• precondition met.

A.2.3.1 Interworking preconditions

A.2.3.1.1 SIP to BICC

A.2.3.1.1.1 Fast Forwards setup

On receipt of the indication precondition 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 precondition 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 Indicator set to "*Continuity*" shall be sent.

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, then the indication 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 of a COT message indicating "*continuity*", then the indication precondition met is sent to the Bearer Control Interworking Function.

A.2.3.1.2.2 Backwards setup

No action is taken on receipt of the indications preconditions required and preconditions met.

A.2.3.1.2.3 Delayed Forwards

If the indication "*COT to be expected*" is received in the IAM, then the indication 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 indicating "*Continuity*", then the indication precondition met is sent to the Bearer Control Interworking Function.

A.3 Bearer Control Interworking Function

A.3.1 IPBCP/SDP Bearer Control Interworking Function (BC-IWF)

This clause defines the procedures associated with a Bearer Control Interworking Function (BC-IWF) 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 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 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 clause 6/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, a preconditions required indication (as defined by the procedures in A.2.3) is sent to the BC-IWF. Subsequently, the procedures outlined in A.2.3.1.1 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 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 preconditions required indication in a previous offer for this call and the procedures outlined within A.2.3.1.1, with respect to 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), the BC-IWF shall send an ACCEPTED message to the IPBCP side. The ACCEPTED message contents shall be formatted as per the procedures of clause 6/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 A.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 clause 6/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), the BC-IWF shall not send any message to the IPBCP side.

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 and RFC 3261. The SDP fields contained within the IPBCP REQUEST message shall be included within the SDP offer. If the BC-IWF receives a 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 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 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 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 RFC 3264 and RFC 3261. 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 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 status (and desired status if necessary) of the preconditions. The procedures used to respond to the SDP received in the previous SDP offer, correlated with this answer, are fully described in 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 ITU-T Rec. Q.1970.

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.

Annex B

Interworking for ISDN supplementary services

This annex describes service interworking of ISDN supplementary services between SIP and BICC/ISUP.

Except where otherwise stated, services in Profile C (SIP-I) operation use the parameters of the (de)encapsulated ISUP, and no other interworking is required. Accordingly, the service interworking descriptions below are only for Profile A and B operation unless Profile C (SIP-I) is specifically indicated.

B.1 Interworking of CLIP/CLIR supplementary service to SIP networks

Profiles A and B

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 sent are trusted.

The interworking between the Calling Party Number and the P-Asserted-Identity header and vice versa used for the CLIP-CLIR service is defined in 6.1.3.6 and 7.1.3. This interworking is essentially the same as for basic call and differs only in that if the CLIR service is invoked, the Address Presentation Restricted 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 6.1.3.6 and 7.1.3.

At the O-IWU the *"presentation restricted"* indication shall be mapped to the Privacy header field with priv-value containing *"id"* and *"header"*.

Profile C (SIP-I)

At the O-IWU: the service shall be supported by encapsulation.

At the I-IWU: If the address within the Calling Party Number after application of the interworking rules in 6.1.3.6 and processing by BICC/ISUP procedures is the same as the value contained in the encapsulated ISUP, no additional interworking is needed beyond use of ISUP encapsulation. In the contrary case the Calling Party Sub-address is deleted from the ATP.

B.2 Interworking of COLP/COLR supplementary service to SIP networks

Profiles A and B

FFS.

Profile C (SIP-I)

No additional interworking beyond use of ISUP encapsulation.

B.3 Interworking of Direct-Dialling-In (DDI) supplementary service to SIP networks

Profiles A and B

FFS.

Profile C (SIP-I)

No additional interworking beyond use of ISUP encapsulation.

B.4 Interworking of Malicious Call Identification (MCID) supplementary service to SIP networks

Profiles A and B

The IWU shall act in accordance with the procedures described in 7.7/Q.731.7 under the sub clause "Interactions with other networks".

Profile C (SIP-I)

All parameters can be taken from the encapsulated ISUP MIME as usual. However, the IP bearer cannot be held after the release of the call.

B.5 Interworking of Sub-addressing (SUB) supplementary service to SIP networks

Profiles A and B

FFS.

Profile C (SIP-I)

At the O-IWU: the service shall be supported by encapsulation.

At the I-IWU: If the address within the Called Party Number after application of the interworking rules in 6.1.3.6 and processing by BICC/ISUP procedures is the same as the value contained in the encapsulated ISUP, no additional interworking is needed beyond use of ISUP encapsulation. In the contrary case the Called Party Sub-address is deleted from the ATP.

B.6 Interworking of Call Forwarding Busy (CFB)/Call Forwarding No Reply (CFNR)/Call Forwarding Unconditional (CFU) supplementary services to SIP networks

Profiles A and B

The IWU shall act in accordance with the procedures described within 2.7/Q.732.2-5, under the clause heading "Interactions with other networks".

Profile C (SIP-I)

Call forwarding in the PSTN requires no additional interworking beyond use of ISUP encapsulation.

B.7 Interworking of Call Deflection (CD) supplementary service to SIP networks

Profiles A and B

The IWU shall act in accordance with the procedures described within 2.7/Q.732.2-5, under the clause heading "Interactions with other networks".

Profile C (SIP-I)

No additional interworking beyond use of ISUP encapsulation.

B.8 Interworking of Explicit Call Transfer (ECT) supplementary service to SIP networks

Profiles A and B

The IWU shall act in accordance with the procedures described within 7.7/Q.732.7, under the clause heading "Interactions with other networks".

Profile C (SIP-I)

No additional interworking beyond use of ISUP encapsulation.

B.9 Interworking of Call Waiting (CW) supplementary service to SIP networks

Profiles A and B

The IWU shall act in accordance with the procedures described within 1.7/Q.733.1, under the clause heading "Interactions with other networks".

Profile C (SIP-I)

No additional interworking beyond use of ISUP encapsulation.

B.10 Interworking of Call Hold (HOLD) supplementary service to SIP networks

Profiles A and B

Call Hold is defined as an ISUP supplementary service within ITU-T Rec. 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 Table B.10-1.

Table B.10-1/Q.1912.5 – 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"*	↔ (Note)	UPDATE with the attribute line "a=sendonly" or "a=inactive" for the offered media stream (see above)
before answer	CPG with *"remote retrieval "*	↔ (Note)	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. NOTE – For the "before answer" scenarios, mapping applies only for hold requests sent by the calling party to the called party as the called party cannot put the calling party on hold before answer.			

Profile C (SIP-I)

Interworking is via the encapsulated CPG message. No additional interworking is required.

The mapping between the ISUP and SIP-I flows is shown in Table B.10-2.

Table B.10-2/Q.1912.5 – Mapping between ISUP and SIP-I 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) and encapsulated ISUP CPG message
	CPG with *"remote hold"* extracted from the body of the SIP message	←	
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) and encapsulated ISUP CPG message
	CPG with *"remote retrieval"* extracted from the body of the SIP message	←	
before answer	CPG with *"remote hold"*	→ (Note)	UPDATE with the attribute line "a=sendonly" or "a=inactive" for the offered media stream (see above) and encapsulated ISUP CPG message
	CPG with *"remote hold"* extracted from the body of the SIP message	←	
before answer	CPG with *"remote retrieval"*	→ (Note)	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
	CPG with *"remote retrieval"* extracted from the body of the SIP message	←	
Mapping: ← : Mapping from SIP to ISUP. → : Mapping from ISUP to SIP. NOTE – For the "before answer" scenarios, mapping applies only for hold requests sent by the calling party to the called party as the called party cannot put the calling party on hold before answer.			

NOTE – The Interworking of the Call Hold (HOLD) Supplementary service between BICC and SIP networks is for further study since BICC CS-2 does not support media suspension.

B.11 Interworking of Completion of Calls to Busy Subscriber (CCBS) supplementary service to SIP networks

Profiles A and B

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

Profile C (SIP-I)

No additional interworking beyond the use of ISUP encapsulation and SCCP connectivity between originating and terminating ISDN networks.

B.12 Interworking of Completion of Calls on No Reply (CCNR) supplementary service to SIP networks

Profiles A and B

The IWU shall act in accordance with the procedures described within 11/Q.733.5, under the clause heading "Interactions with other networks".

Profile C (SIP-I)

No additional interworking beyond the use of ISUP encapsulation and SCCP connectivity between originating and terminating ISDN networks.

B.13 Interworking of Terminal Portability (TP) supplementary service to SIP networks

Profiles A and B

Terminal Portability is defined as an ISUP supplementary service within ITU-T Rec. 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. A Suspend message containing the Suspend/Resume indicators set to "*ISDN subscriber initiated*" shall be treated like a CPG with "*remote hold*" in Table B.10. A Resume message containing the Suspend/Resume indicators set to "*ISDN subscriber initiated*" shall be treated like a CPG with "*remote retrieval*" in Table B.10.

Profile C (SIP-I)

Interworking is via the encapsulated SUS and RES messages. No additional interworking is required.

NOTE – The Interworking of Terminal Portability (TP) Supplementary service between BICC and SIP networks is for further study since BICC CS-2 does not support media suspension.

B.14 Interworking of Conference Calling (CONF) supplementary service to SIP networks

Profiles A and B

The IWU shall act in accordance with the procedures described within 2.7/Q.734.1, under the clause heading "Interactions with other networks".

Profile C (SIP-I)

No additional interworking beyond use of ISUP encapsulation.

B.15 Interworking of Three-Party Service (3PTY) supplementary service to SIP networks

Profiles A and B

The IWU shall act in accordance with the procedures described within 2.7/Q.734.2, under the clause heading "Interactions with other networks".

Profile C (SIP-I)

No additional interworking beyond use of ISUP encapsulation is required.

B.16 Interworking of Closed User Group (CUG) supplementary service to SIP networks

Profiles A and B

The IWU shall act in accordance with the procedures described within 1.5.2.4.2/Q.735.1, under the clause heading "Exceptional procedures".

Profile C (SIP-I)

No additional interworking beyond use of ISUP encapsulation.

B.17 Interworking of Multi-Level Precedence and Preemption (MLPP) supplementary service to SIP networks

Profiles A and B

The IWU shall act in accordance with the procedures described within 3.7/Q.735.3, under the clause heaading "Interactions with other networks".

Profile C (SIP-I)

No additional interworking beyond use of ISUP encapsulation is required.

B.18 Interworking of Global Virtual Network Service (GVNS) supplementary service to SIP networks

Profiles A and B

The IWU shall act in accordance with the procedures described within 6.7/Q.735.6, under the clause heading "Interactions with other networks".

Profile C (SIP-I)

No additional interworking beyond use of ISUP encapsulation is required.

B.19 Interworking of International Telecommunication Charge Card (ITCC) supplementary service to SIP networks

Profiles A and B

The IWU shall act in accordance with the procedures described within 1.7/Q.736.1, under the clause heading "Interactions with other networks".

Profile C (SIP-I)

SCCP connectivity between originating and terminating ISDN networks is needed. This connectivity could be available as a bypass to the SIP network.

All parameters can be taken from the encapsulated ISUP MIME.

Interworking of ITCC without SCCP by-pass is FFS.

B.20 Interworking of Reverse Charging (REV) supplementary service to SIP networks

Profiles A and B

The IWU shall act in accordance with the procedures described within 3.7/Q.736.3, under the clause heading "Interactions with other networks".

Profile C (SIP-I)

No additional interworking beyond use of ISUP encapsulation is required.

B.21 Interworking of User-to-User Signalling (UUS) supplementary service to SIP networks

Profiles A and B

The IWU shall act in accordance with the procedures described within ITU-T Rec. Q.737.1, under the clause heading "Interactions with other networks".

Profile C (SIP-I)

All parameters can be taken from the encapsulated ISUP MIME.

The impact with regard to the full functionality of the UUS is for further study.

Annex C

This annex contains references to normative Internet Engineering Task Force (IETF) RFCs and materials originally sourced from the IETF but deemed normative to this Recommendation.

C.1 SIP/SIP-I references (normative)

C.1.1 SIP/SIP-I signalling references and profile

C.1.1.1 References

See also C.2.

- IETF RFC 2046 (1996), *Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types*.
- IETF RFC 2327 (1998), *SDP: Session Description Protocol*.
- IETF RFC 2806 (2000), *URLs for Telephone Calls*.
- IETF RFC 2976 (2000), *The SIP INFO Method*.
- IETF RFC 3204 (2001), *MIME media types for ISUP and QSIG Objects*.
- IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*.
- IETF RFC 3262 (2002), *Reliability of Provisional Responses in the Session Initiation Protocol (SIP)*.
- IETF RFC 3264 (2002), *An Offer/Answer Model with the Session Description Protocol (SDP)*.
- IETF RFC 3311 (2002), *The Session Initiation Protocol UPDATE Method*.
- IETF RFC 3312 (2002), *Integration of Resource Management and Session Initiation Protocol (SIP).*
- IETF RFC 3323 (2002), *A Privacy Mechanism for the Session Initiation Protocol (SIP)*.
- IETF RFC 3326 (2002), *The Reason Header Field for the Session Initiation Protocol (SIP).*

C.1.1.2 SIP/SIP-I Signalling Profiles

Reference	Profile A	Profile B	Profile C
RFC 2046 *Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types*	Supported	Supported	Supported
RFC 2327 *SDP: Session Description Protocol*	Supported	Supported	Supported
RFC 2806 *URLs for Telephone Calls*	Supported	Supported	Supported
RFC 2976 *The SIP INFO Method*	Not Supported	Not Supported	Supported
RFC 3204 *MIME media types for ISUP and QSIG Objects*	Not Supported	Not Supported	Supported
RFC 3261 *SIP: Session Initiation Protocol*	Supported	Supported	Supported
RFC 3262 *Reliability of Provisional Responses in the Session Initiation Protocol (SIP)*	Supported	Optional	Optional
RFC 3264 *An Offer/Answer Model with the Session Description Protocol (SDP)*	Supported	Supported	Supported
RFC 3311 *The Session Initiation Protocol UPDATE Method*	Supported	Supported	Supported
RFC 3312 *Integration of Resource Management and Session Initiation Protocol (SIP)*	Supported	Optional	Optional
RFC 3323 *A Privacy Mechanism for the Session Initiation Protocol (SIP)*	Supported	Supported	Supported
RFC 3325 *Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks (Note)*	Supported	Supported	Supported
RFC 3326 *The Reason Header Field for the Session Initiation Protocol (SIP)*	Supported	Supported	Supported
NOTE – C.2 shall be taken as the normative reference replacing RFC 3325.			

C.1.2 SIP/SIP-I media references

C.1.2.1 References

– IETF RFC 2833 (2000), *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*.

– IETF RFC 3267 (2002), *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*.

– IETF RFC 3389 (2002), *RTP Payload for Comfort Noise*.

– IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.

– IETF RFC 3551 (2003), *RTP Profile for Audio and Video Conferences with Minimal Control*.

– ITU-T Recommendation T.38 (2004), *Procedures for real-time Group 3 facsimile communication over IP networks*.

C.2 The P-Asserted-Identity SIP header extension (normative)

This clause reproduces the content of RFC 3325. 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.

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.

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].
7) That nodes in the Trust Domain are compliant to this document.
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.

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].

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.

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.

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 SIPS URI, the proxy MUST replace that SIP or SIPS URI with a single SIP or SIPS URI or remove this header field. 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 the header field.

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.

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.

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, unless local privacy policies prevent it, because 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 the user has not requested and cannot prevent. 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.

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 the user has requested that asserted identity information be kept private.

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.

9 Formal syntax

The following syntax specification uses the augmented Backus-Naur Form (BNF) as described in RFC 2234 [4].

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
P-Asserted-Identity		adr	-	o	-	o	o	-

	SUB	NOT	REF	INF	UPD	PRA
	o	o	o	-	-	-

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
P-Preferred-Identity		adr	-	o	-	o	o	-

	SUB	NOT	REF	INF	UPD	PRA
	o	o	o	-	-	-

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
```

10 Examples

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
```

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
```

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.

11.1 Protocol requirements

The following specifications MUST be supported:

1) SIP [1].

2) This document.

11.2 Authentication requirements

Users MUST be authenticated using SIP Digest Authentication.

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.

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.

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.

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.

13 IANA considerations

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

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

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, Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[2] Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)", RFC 3323, November 2002.

[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", RFC 3324, November 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

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

Appendix I

Interworking scenarios between SIP and BICC

I.1 Scope

This appendix defines typical interworking scenarios between SIP and BICC. ISDN Access flows are included for informational purposes only. The main body of the Recommendation takes precedence over this appendix.

I.2 Definitions

The vertical boxes represent two entities: a BICC SN and the IWU (SIP-BICC Interworking Unit).

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 unit. 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.

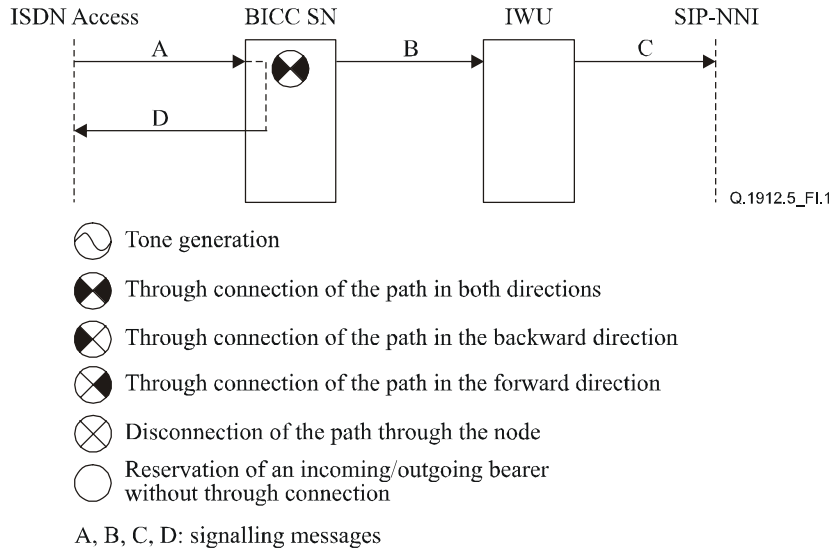


Figure I.1/Q.1912.5 – Example of a call flow or "arrow" diagram

I.3 Abbreviations

See clause 4.

I.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 I.1.

I.5 Interworking of SIP accesses to BICC

Clauses I.5.1 and I.5.2 contain information relevant to basic call control. The call flow diagrams are divided into functional subclauses:

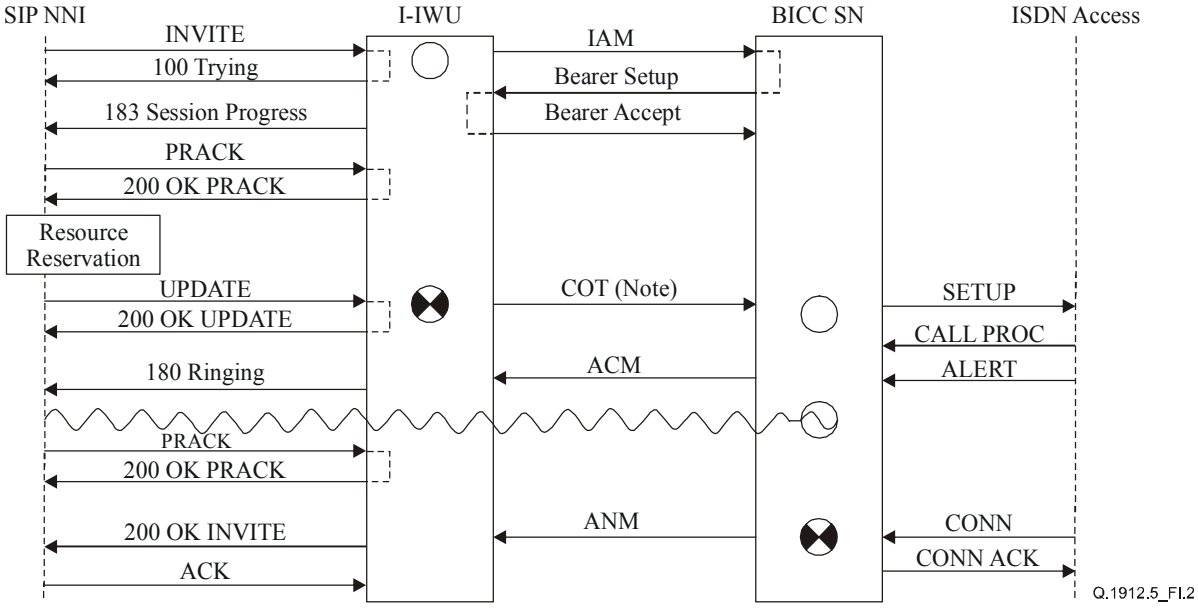
– successful call set-up procedures;
– unsuccessful call set-up procedures;
– release procedures;
– simple message segmentation procedures.

I.5.1 Example scenarios for incoming call interworking from SIP to BICC at I-IWU

I.5.1.1 Successful call set-up procedures/call flow diagrams for basic call control

I.5.1.1.1 SIP preconditions used, backwards BICC bearer setup, non-automatic answer

Figure I.2 shows the sequence of messages for successful call set-up for an incoming 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 to be expected"* indication) is sent by the I-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 the ASN will be responsible for protecting against fraudulent use of the user plane.

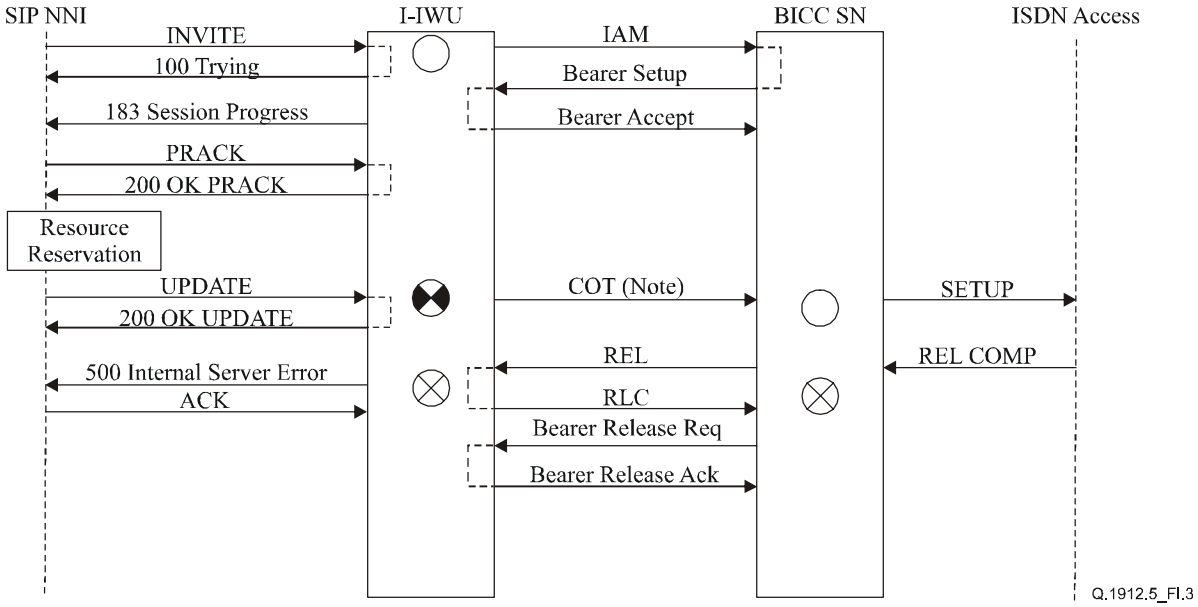


NOTE – The IAM contained the indication "*COT to be expected*".

Figure I.2/Q.1912.5 – Successful basic call setup from SIP to BICC

I.5.1.2 Unsuccessful call set-up procedures/call flow diagrams for basic call control

Figure I.3 shows the sequence of messages for unsuccessful call set-up for an incoming call from SIP to BICC. In this sequence, the I-IWU sends the 500 Server Internal Error message upon reception of the REL message (with Cause Value No. 34 (resource unavailable)) from the BICC side of the call.



NOTE – The IAM contained the indication *"COT to be expected"*.

Figure I.3/Q.1912.5 – Unsuccessful basic call set-up from SIP to BICC

I.5.1.3 Release procedures/call flow diagrams for basic call control

I.5.1.3.1 Normal call release procedure, backward bearer set-up

Figure I.4 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.

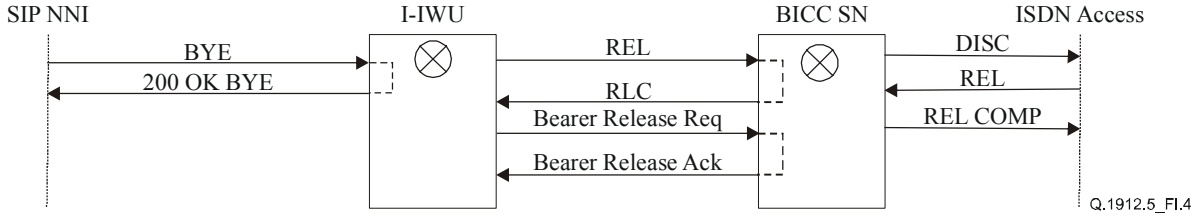
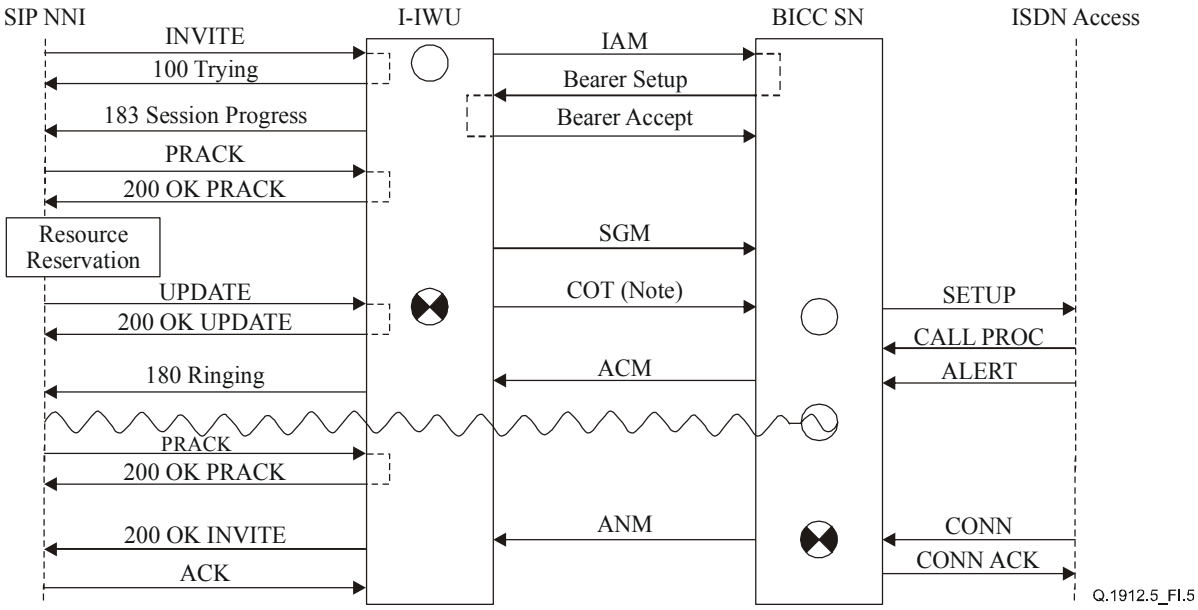


Figure I.4/Q.1912.5 – Normal call release from SIP to BICC

I.5.1.4 Simple segmentation procedures/call flow diagrams for basic call control

Figure I.5 shows a sequence of messages for successful call set-up for an incoming call from SIP to BICC using the segmentation procedures on the BICC side. In this example, the IWU sends the SGM independent of a message from the SIP side, and hence there is no interworking significance.



NOTE – The IAM contained the indication *"COT to be expected"*.

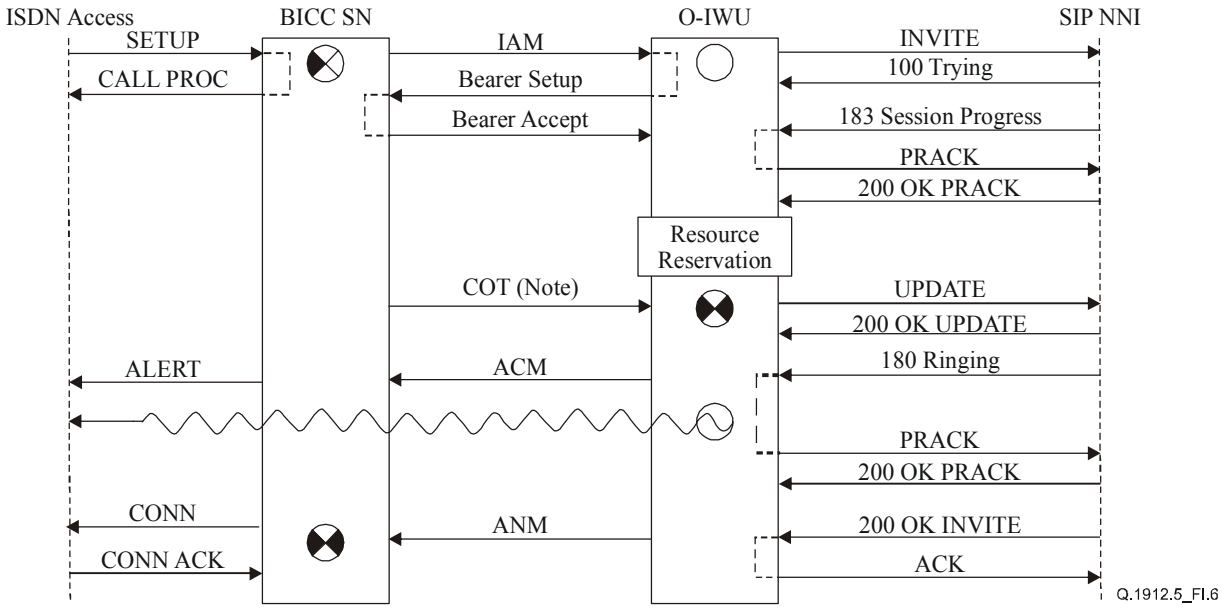
Figure I.5/Q.1912.5 – Basic call set-up using segmentation procedures from SIP to BICC

I.5.2 Example scenarios for outgoing call interworking from BICC to SIP at O-IWU

I.5.2.1 Successful call set-up procedures/call flow diagrams for basic call control

I.5.2.1.1 Backwards BICC bearer setup, SIP preconditions used

Figure I.6 shows a sequence of messages for successful call set-up for an outgoing call from BICC to SIP. In this example, the O-IWU indicates mandatory local sendrecv preconditions in the INVITE. The O-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 to be expected*"). 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 – This message is optional, depending on the indication in the IAM.

Figure I.6/Q.1912.5 – Successful basic call setup from BICC to SIP

I.5.2.2 Unsuccessful call set-up procedures/call flow diagrams for basic call control

Figure I.7 shows a sequence of messages for unsuccessful call set-up for an outgoing call from BICC to SIP. In this example, the O-IWU sends the REL message upon reception of the 484 Address Incomplete message from the SIP side of the call.

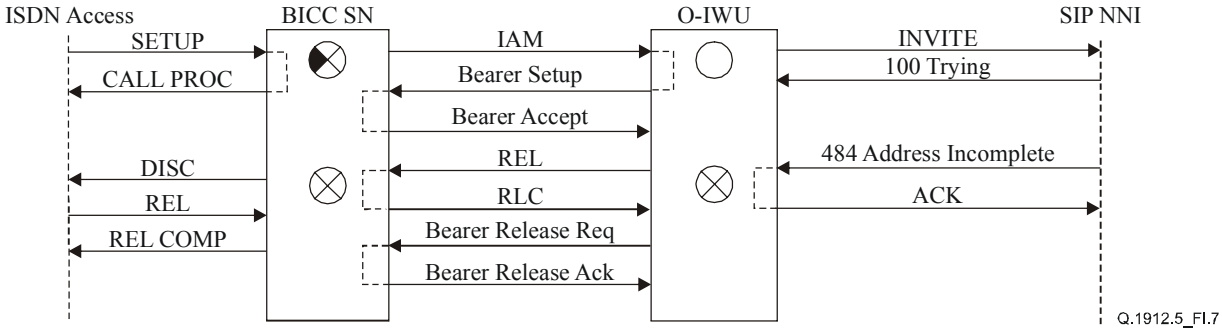


Figure I.7/Q.1912.5 – Unsuccessful basic call set-up from BICC to SIP

I.5.2.3 Release procedures/call flow diagrams for basic call control

I.5.2.3.1 Normal call release procedure, backwards bearer set-up

Figure I.8 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.

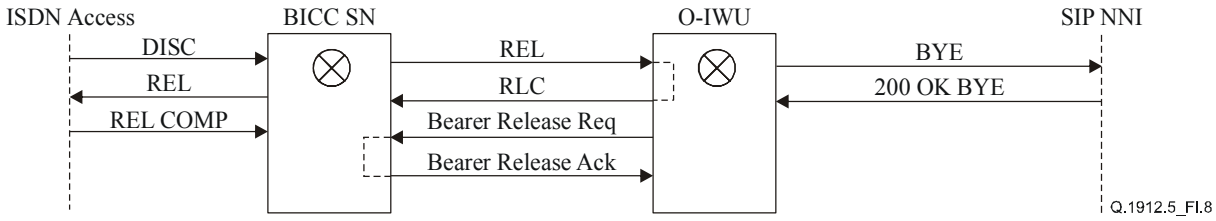


Figure I.8/Q.1912.5 – Normal call release from BICC to SIP

I.5.2.4 Simple segmentation procedures/call flow diagrams for basic call control

Figure I.9 shows a sequence of messages for successful call set-up for an outgoing call from BICC to SIP using the segmentation procedures. In this example, the O-IWU sends the INVITE message upon reception of the SGM from the BICC side of the call.

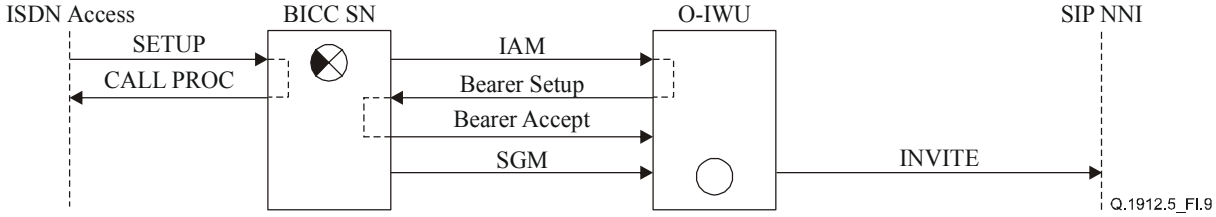


Figure I.9/Q.1912.5 – Basic call set-up using segmentation procedures from BICC to SIP

Appendix II

Interworking scenarios between SIP and ISUP

II.1 Scope

This appendix defines typical interworking scenarios between SIP and ISUP. ISDN Access flows are included for informational purposes only. The main body of the Recommendation takes precedence over this appendix.

II.2 Definitions

The vertical boxes represent two entities: an ISUP exchange and IWU (SIP-ISUP Interworking Unit).

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 unit. 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 actions taken.

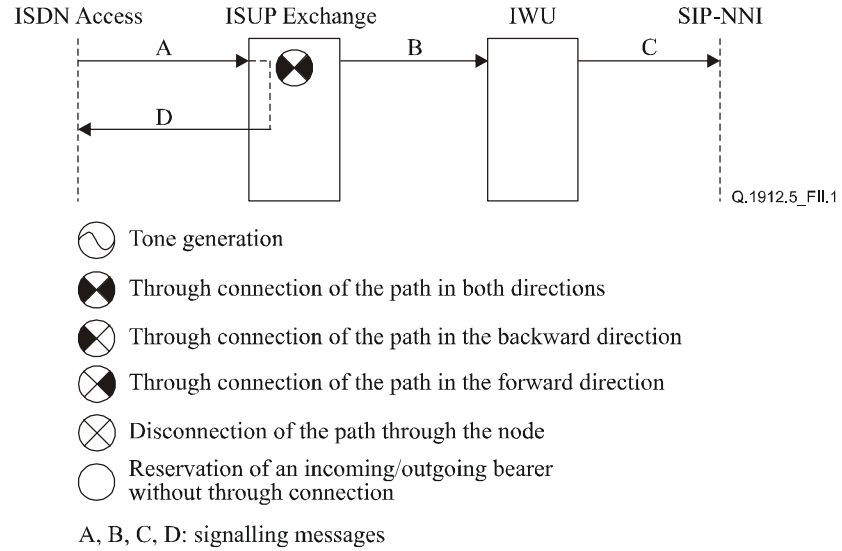


Figure II.1/Q.1912.5 – Example of a call flow or "arrow" diagram

II.3 Abbreviations

See clause 4.

II.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 II.1.

II.5 Interworking of SIP Access to ISUP

Clauses II.5.1 and II.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;

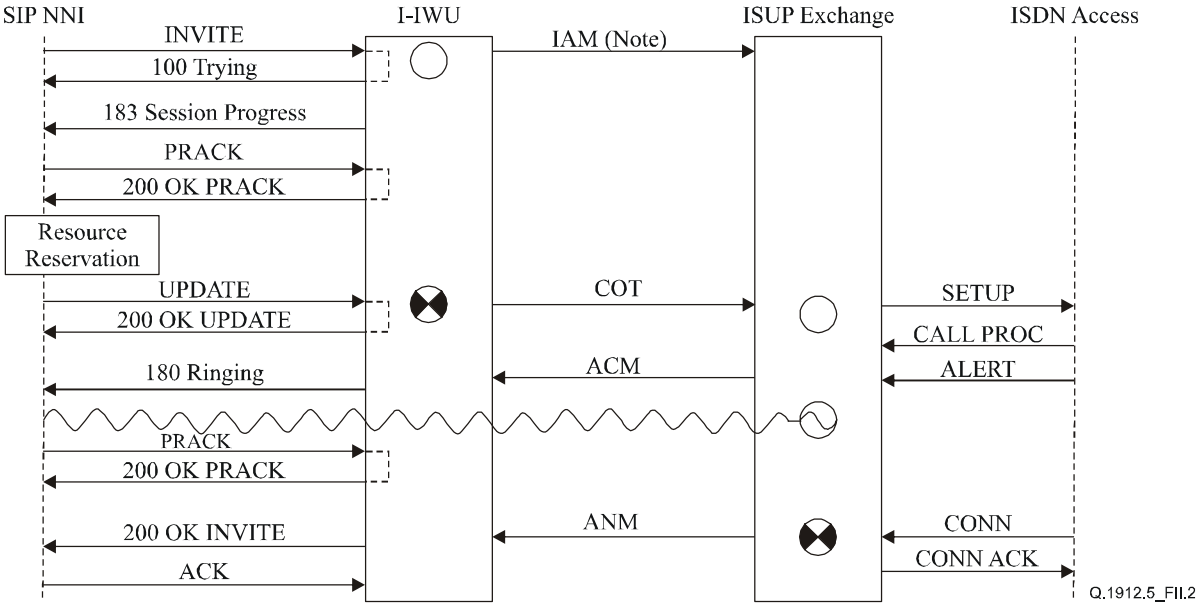
– release procedures.

II.5.1 Example scenarios for incoming call interworking from SIP to ISUP at I-IWU

II.5.1.1 Successful call set-up procedures and call flow diagrams for basic call control

II.5.1.1.1 SIP preconditions used

Figure II.2 shows the sequence of messages for successful call set-up for an incoming 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 I-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).

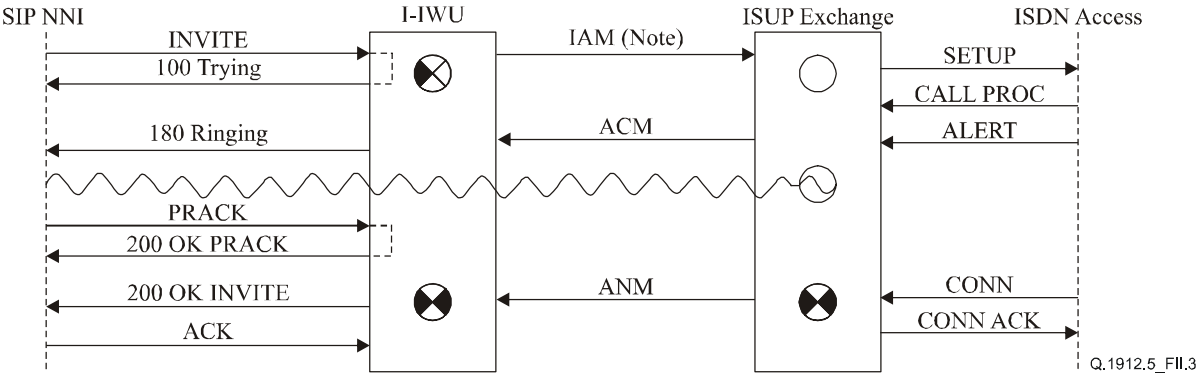


NOTE – The IAM contained the indication *"continuity check performed on previous circuit"* or *"continuity check required on this circuit"*.

Figure II.2/Q.1912.5 – Successful basic call set-up from SIP to ISUP (SIP preconditions and continuity check protocol used)

II.5.1.1.2 SIP preconditions not used

Figure II.3 shows the sequence of messages for successful call set-up for an incoming call from SIP to ISUP. The IAM (with *"continuity check not required"* indication) is sent by the I-IWU once the initial INVITE is received.

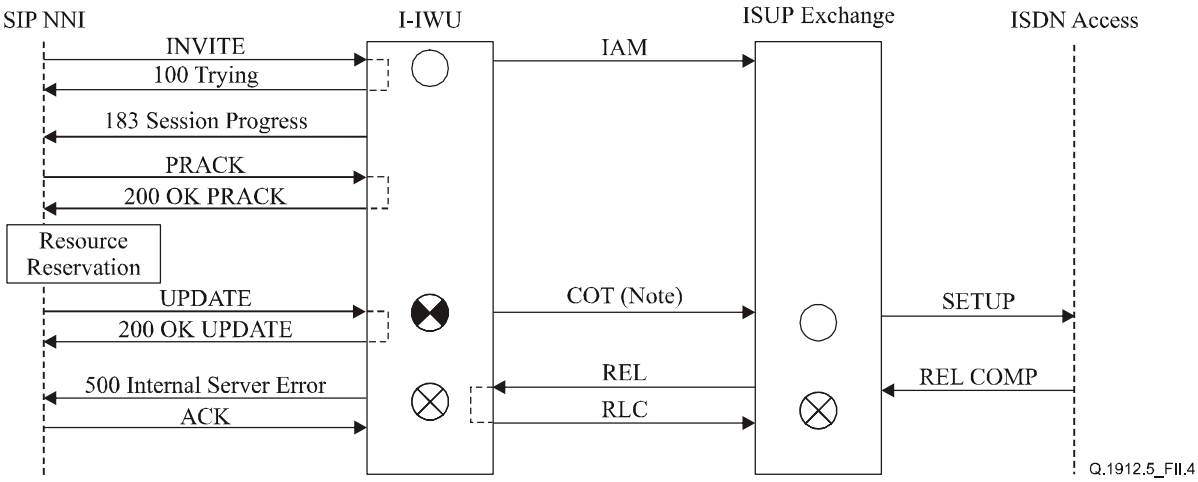


NOTE – The IAM contained the indication *"continuity check not required"*.

Figure II.3/Q.1912.5 – Successful basic call set-up from SIP to ISUP (SIP preconditions and continuity check protocol not used)

II.5.1.2 Unsuccessful call set-up procedures and call flow diagrams for basic call control

Figure II.4 shows the sequence of messages for unsuccessful call set-up for an incoming call from SIP to ISUP. In this sequence, the I-IWU sends the 500 Server Internal Error message upon reception of the REL message (with Cause Value No. 34 (resource unavailable)) from the ISUP side of the call.



NOTE – This message is optional, depending on the indication in the IAM.

Figure II.4/Q.1912.5 – Unsuccessful basic call set-up from SIP to ISUP

II.5.1.3 Normal call release procedure

Figure II.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.

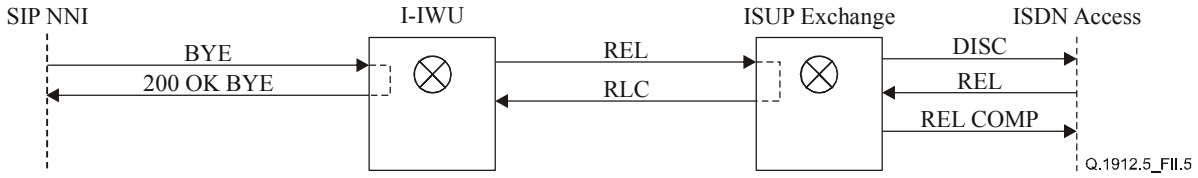


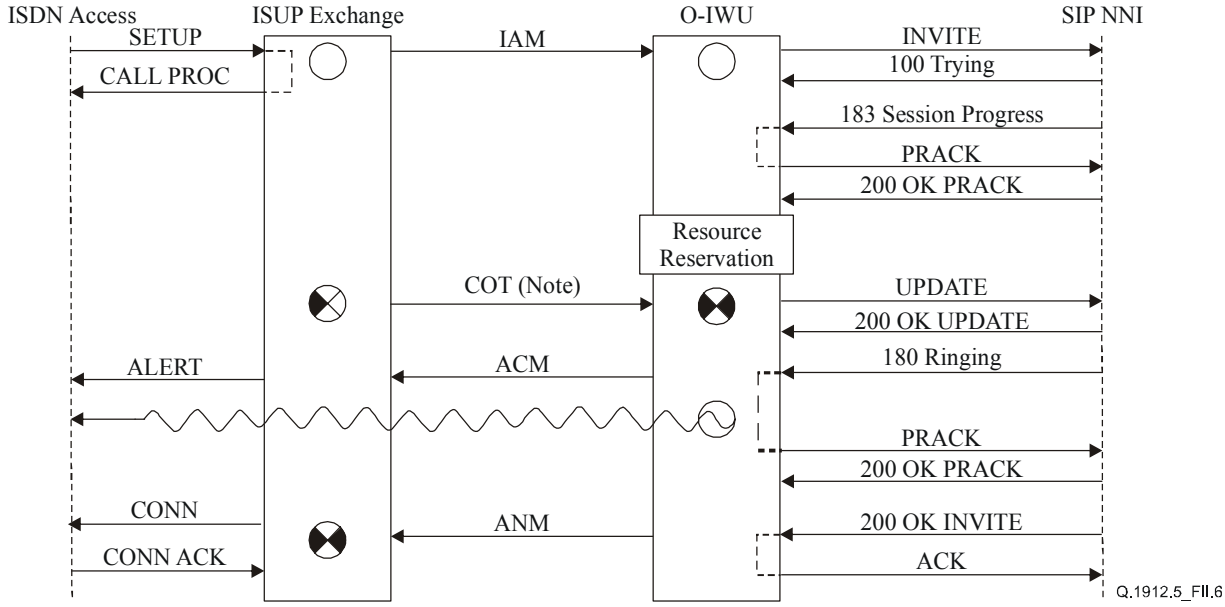
Figure II.5/Q.1912.5 – Normal call release from SIP to ISUP

II.5.2 Example scenarios for outgoing call interworking from ISUP to SIP at O-IWU

II.5.2.1 Successful call set-up procedures and call flow diagrams for basic call control

II.5.2.1.1 SIP preconditions used

Figure II.6 shows a sequence of messages for successful call set-up for an outgoing call from ISUP to SIP. In this example, the O-IWU indicates mandatory local sendrecv preconditions in the INVITE. The O-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.

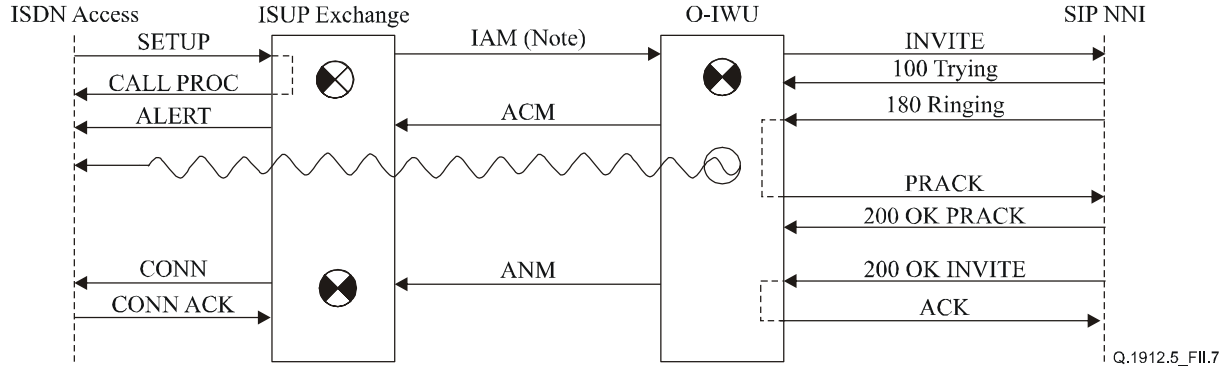


NOTE – This message is optional, depending on the indication in the IAM.

Figure II.6/Q.1912.5 – Successful basic call set-up from ISUP to SIP (SIP preconditions and continuity check protocol used)

II.5.2.1.2 SIP preconditions not used

Figure II.7 shows a sequence of messages for successful call set-up for an outgoing call from ISUP to SIP. In this example, the O-IWU sends the INVITE message upon reception of an IAM (since the IAM indicated "*continuity check not required*").



NOTE – The IAM contained the indication *"continuity check not required"*.

Figure II.7/Q.1912.5 – Successful basic call set-up from ISUP to SIP (SIP preconditions and continuity check protocol not used)

II.5.2.2 Unsuccessful call set-up procedures and call flow diagrams for basic call control

Figure II.8 shows a sequence of messages for unsuccessful call set-up for an outgoing call from ISUP to SIP. In this example, the O-IWU sends the REL message upon reception of the 484 Address Incomplete message from the SIP side of the call.

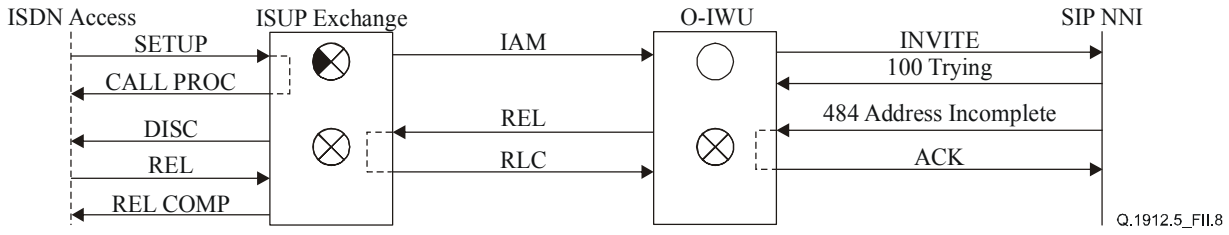


Figure II.8/Q.1912.5 – Unsuccessful basic call set-up from ISUP to SIP

II.5.2.3 Normal call release procedure

Figure II.9 shows a normal call release procedure initiated from the ISUP side of the call. This call flow assumes that no resource reservation teardown signalling is required on the SIP side of the call.

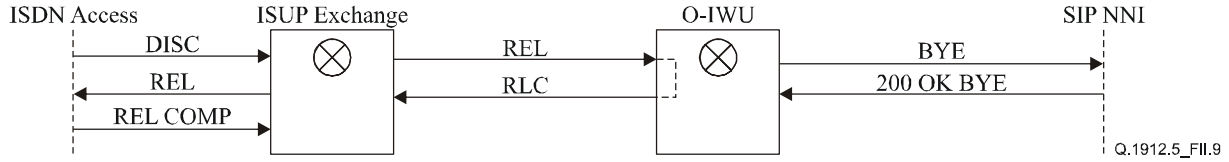


Figure II.9//Q.1912.5 – Normal call release from ISUP to SIP

Appendix III

Interworking scenarios between Profile C (SIP-I) and ISUP

III.1 General

III.1.1 Scope

This appendix defines some typical interworking scenarios between ISUP and SIP when Profile C (SIP-I) is in use. ISDN Access flows are included for informational purposes only. The operation of IWUs as a transit exchange is prearranged through configuration or analysis of received signalling information. The main body of the Recommendation takes precedence over this appendix.

III.1.2 Definitions

The vertical boxes represent originating and destination ISUP exchanges and outgoing and incoming IWUs (SIP-ISUP Interworking Units). Intermediate ISUP exchanges are not shown, since they do not change the basic call flows.

The vertical dashed lines represent the access interface, ISDN or non-ISDN depending on the example.

Solid horizontal arrows represent signalling messages and indicate their direction of propagation, i.e., to or from the interworking unit. 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.

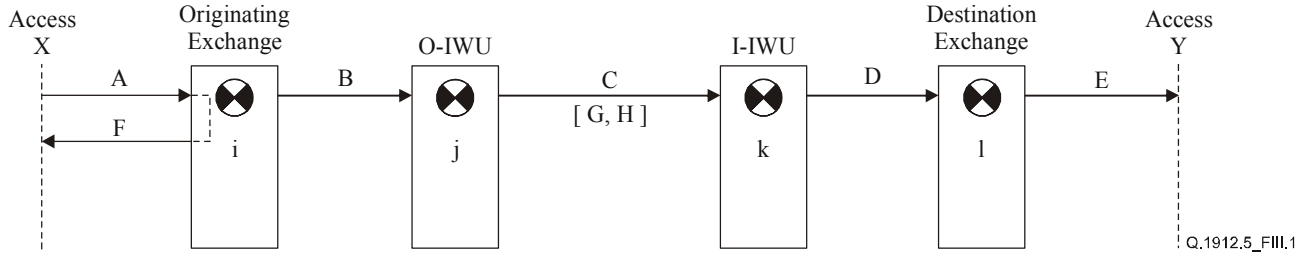
For call control, the following symbols are used within the vertical boxes to indicate the relationship between the incoming and outgoing messages and the call control action taken.

III.1.3 Abbreviations

See clause 4.

III.1.4 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 III.1.



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 bearer channel without through-connection

A, B, C, D, E and F	Signalling messages
[G, H]	Encapsulated information
i, j, k and l	Call control actions
X and Y	Access type

Figure III.1/Q.1912.5 – Example of a call flow or "arrow" diagram

III.2 Interworking of ISUP with SIP using Profile C (SIP-I)

Clauses III.2.1 to III.2.4 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.

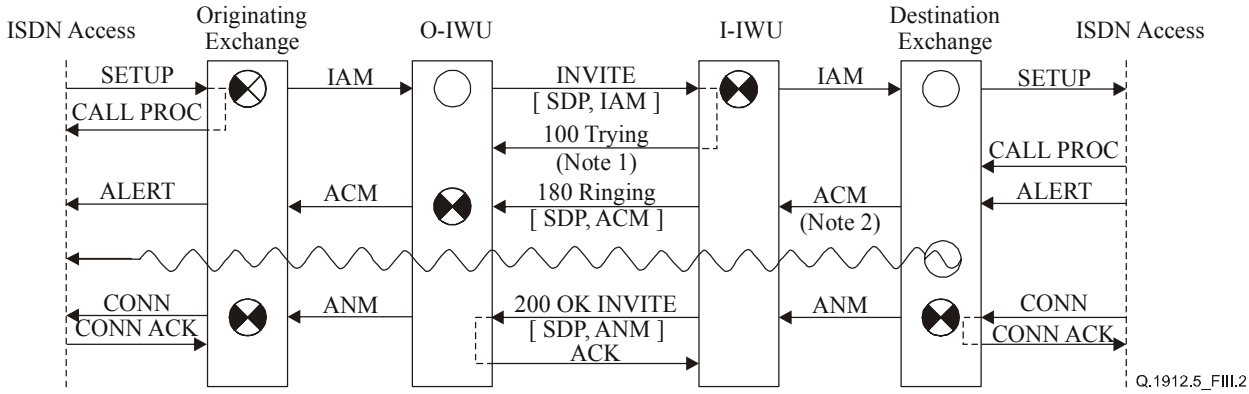
III.2.1 Successful call set-up procedures/call flow diagrams for basic call control

III.2.1.1 *En bloc*, subscriber free indication

See 2.1/Q.764 and RFC 3261.

NOTE – Termed Late ACM.

Figure III.2 shows the sequence of messages for successful call set-up for an incoming ISUP call in the case of Profile C (SIP-I) operation. The O-IWU performs the through-connection of the bearer path in both directions after the receipt of SDP answer in the 180 Ringing response.



NOTE 1 – Any SIP entity along the signalling path to the I-IWU, or the I-IWU itself, may return a 100 Trying provisional response either by configuration or because it determines that a further response will take longer than 200 ms to generate. This is a purely SIP matter with no interworking significance, but is depicted for realism in this and subsequent figures.
NOTE 2 – ACM contained the following indicators:
Called Party Status = *"subscriber free"*, ISDN Access Indicator = *"ISDN access"*

Figure III.2/Q.1912.5 – *En bloc*, subscriber free indication

For detailed messages and parameter mapping, refer to:

– IAM – clauses 6.1.3 and 7.1.1 through 7.1.5.

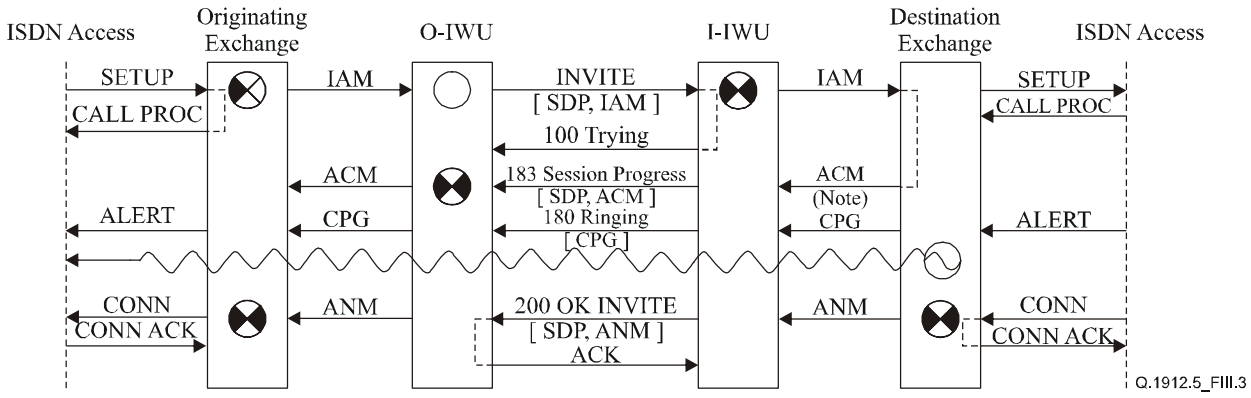
– ACM – clauses 6.5 1) and 7.3.1.

– ANM – clauses 6.7 and 7.5.

III.2.1.2 *En bloc*, early ACM

See 2.1/Q.764 and RFC 3261.

Figure III.3 shows the sequence of messages for successful call set-up for an incoming ISUP call in the case of Profile C (SIP-I) operation. At the I-IWU the ACM is mapped and encapsulated to 183 Session Progress provisional response preserving the ISUP signalling transparency. The O-IWU performs the through-connection of the bearer path in both directions after the receipt of SDP answer in the 183 Session Progress response.



NOTE – The method of ACM generating independent of access is termed *Early* ACM. The ACM is independently generated at the destination exchange with the following indicators: Called Party Status = "*no indication*"; ISDN Access Indicator = "*ISDN access*".

Figure III.3/Q.1912.5 – *En bloc*, early ACM encapsulation

For detailed messages and parameter mapping, refer to:

– IAM – clauses 6.1.2 and 7.1.

– ACM – clauses 6.5 2) and 7.3.2.

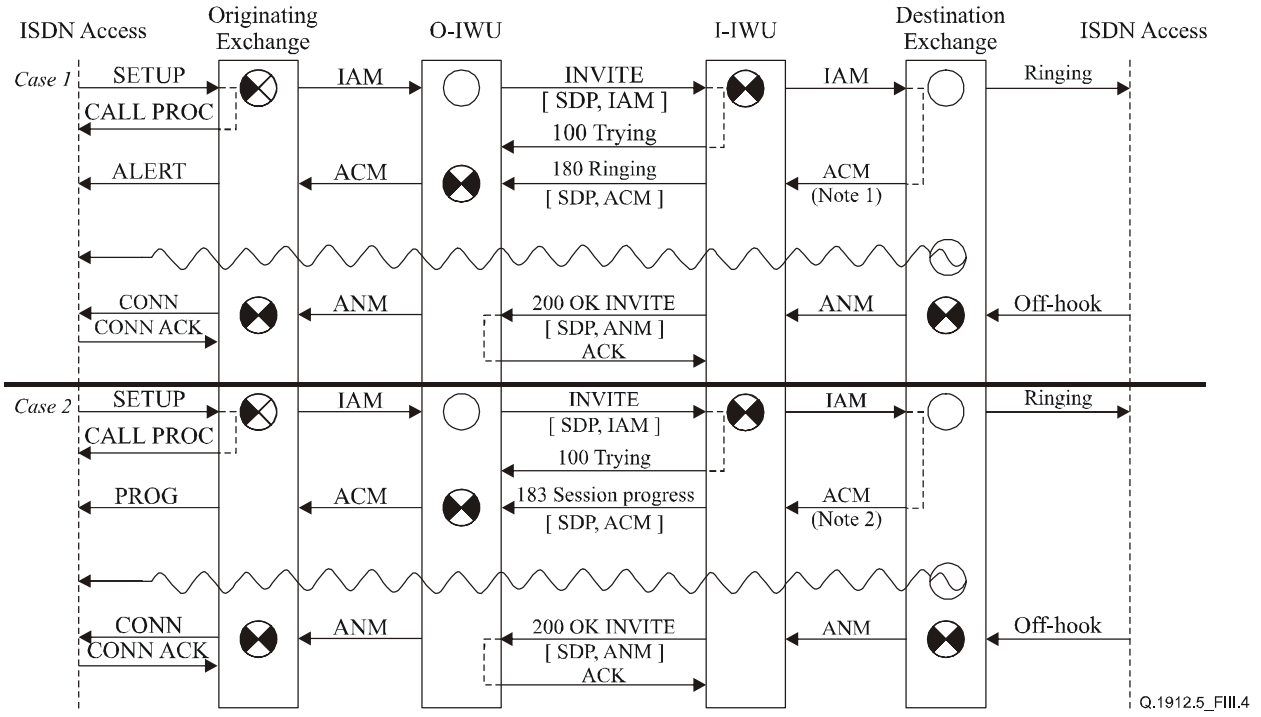
– CPG message – clauses 6.6 and 7.3.1.

– ANM – clauses 6.7 and 7.5.

III.2.1.3 *En bloc*, early media scenarios

See 2.1/Q.764 and RFC 3261.

Figure III.4 Cases 1 and 2 show sequences of messages for a call from an ISDN access to a non-ISDN access. The two cases differ based on the contents of the ACM generated at the destination exchange.



NOTE 1 – The ACM in case 1 is independently generated at the destination exchange with the following indicators: Called Party Status = *"subscriber free"*, ISDN Access Indicator = *"non-ISDN access"*.
NOTE 2 – The ACM in case 2 is independently generated at the destination exchange with the following indicators: Called Party Status = *"no indication"*, ISDN Access Indicator = *"non-ISDN access"*. In order to support user-generated in-band information (e.g., from a PBX, see 2.1.4.1 b/Q.764), the destination exchange may through-connect in the backward direction and include in the ACM the Optional Backward Call Indicators parameter indicating *"in-band information or an appropriate pattern is now available"*.

Figure III.4/Q.1912.5 – Early media call-flows

For detailed messages and parameter mapping, refer to:

– IAM – clauses 6.1.2 and 7.1.

– ACM – clauses 6.5 1)/6.5 2) and 7.3.1/7.3.2.

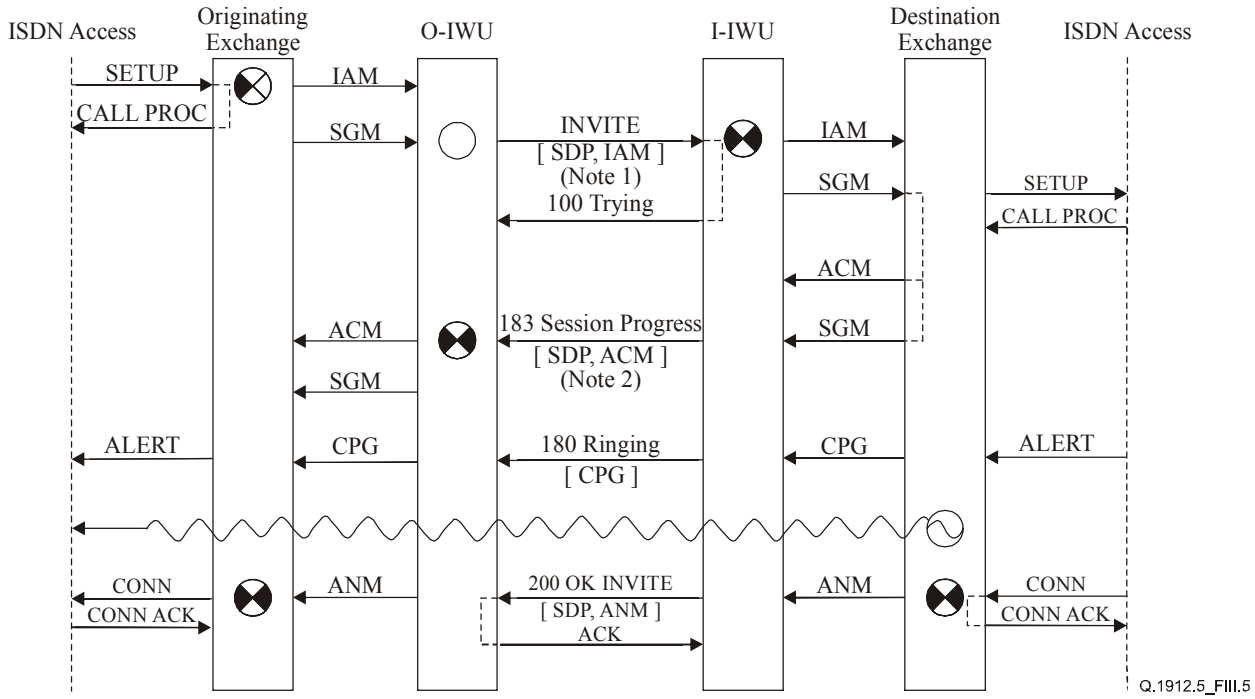
– CPG message – clauses 6.6 and 7.3.1.

– ANM – clauses 6.7 and 7.5.

III.2.1.4 *En bloc*, simple segmentation procedures

See 2.1.12/Q.764 and RFC 3261.

Figure III.5 indicates the simple segmentation procedures in the forward and backward directions. Before the encapsulation, the IWU reassembles the incoming ISUP message with its segmented part (see 5.4.3.3). After de-encapsulation, the IWU applies ISUP segmentation procedures, if needed.



NOTE 1 – The complete re-assembled IAM message is encapsulated in the INVITE request.
NOTE 2 – The complete re-assembled ACM message is encapsulated in the 183 provisional response.

Figure III.5/Q.1912.5 – *En bloc*, simple segmentation in both directions

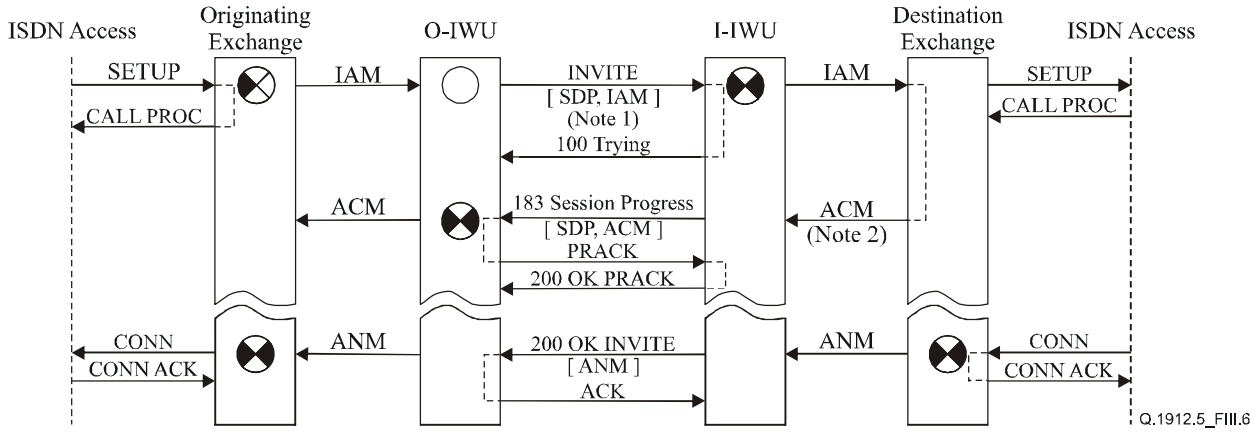
For detailed messages and parameter mapping, refer to:

– IAM – clauses 6.1.2 and 7.1.
– SGM – clause 5.4.3.3.
– ACM – clauses 6.5 2) and 7.3.2.
– CPG message – clauses 6.6 and 7.3.1.
– ANM – clauses 6.7 and 7.5.

III.2.1.5 *En bloc*, reliable provisional responses

See 2.1/Q.764 and 4/RFC 3262.

Figure III.6 shows the sequence of messages for successful call set-up for an incoming ISUP call in the case of Profile C (SIP-I) operation. The O-IWU indicates the required support of reliable provisional responses by adding option tag 100rel to the Required header field of the INVITE request. At the I-ISN, the ACM is mapped and encapsulated in a 183 Session Progress response preserving the ISUP signalling transparency. The O-IWU confirms the receipt of provisional response with the PRACK request. Typically there will be an alerting phase, not shown here, with mapping of ISUP CPG message to 180 Ringing. The 200 OK INVITE contains no SDP, since the offer-answer exchange is completed during the preceding steps. This is only possible where the provisional responses are transmitted reliably.



NOTE 1 – INVITE contains the Required header field with the option tag 100rel.
NOTE 2 – ACM contained the following indicators:
Called Party Status = *"no indication"*, ISDN Access Indicator = *"ISDN access"*.

Figure III.6/Q.1912.5 – *En bloc*, use of reliable provisional responses

For detailed messages and parameter mapping, refer to:

– IAM – clauses 6.1.2 and 7.1.

– ACM – clauses 6.5 2) and 7.3.2.

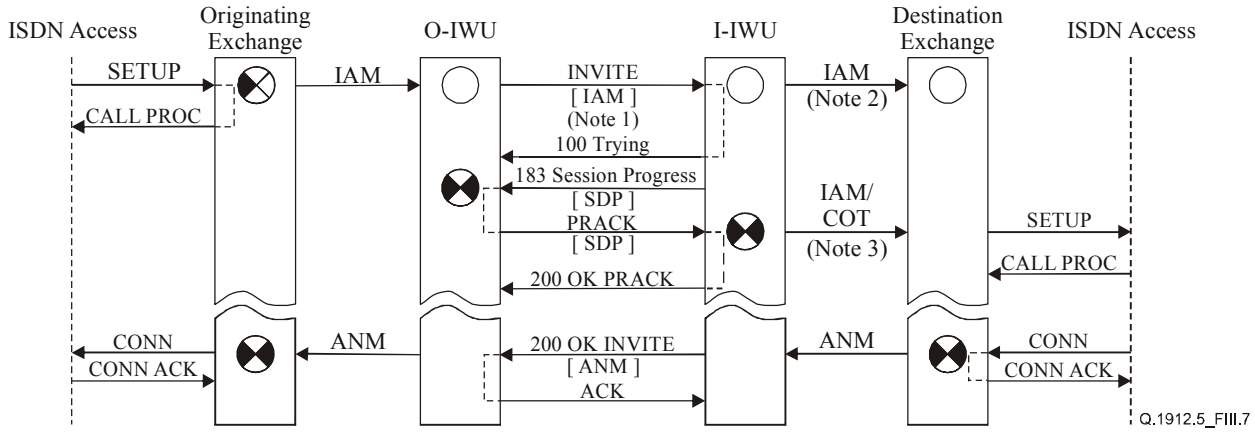
– ANM – clauses 6.7 and 7.5.

III.2.1.6 *En bloc*, backward SDP offer

See 2.1/Q.764 and RFC 3261.

Figure III.7 shows the sequence of messages for successful call set-up for an incoming ISUP call in the case of Profile C (SIP-I) operation. Depending on configuration, the O-IWU can omit the SDP in the initial INVITE, thus asking I-IWU to provide the SDP offer. The indication of reliable provisional responses support is included. If the I-IWU supports the procedure, it can transfer an SDP offer via a 183 Session Progress response. The O-IWU responds with SDP answer and performs the through-connection of the bearer path in both directions after the receipt of SDP answer in the 183 Session Progress response.

Depending on configuration, I-IWU can directly send IAM with *"COT on previous circuit"* indication and continue the call setup by sending COT after receipt of SDP answer. As an alternative, it can delay the sending of IAM until the receipt of SDP answer. See 6.1.1 1). In any scenario, the I-IWU through-connects the bearer path on the receipt of SDP answer. The alerting phase is omitted from the figure for simplicity.



NOTE 1 – INVITE contains the Supported header field with the option tag 100rel.
NOTE 2 – In the case of immediate sending of IAM, it will contain *"COT on previous circuit"* indication.
NOTE 3 – The choice between deferred IAM and COT depends on the I-IWU configuration.

Figure III.7/Q.1912.5 – *En bloc*, backward session description initiation

For detailed messages and parameter mapping, refer to:

– IAM – clauses 6.1.1 1) and 7.1.

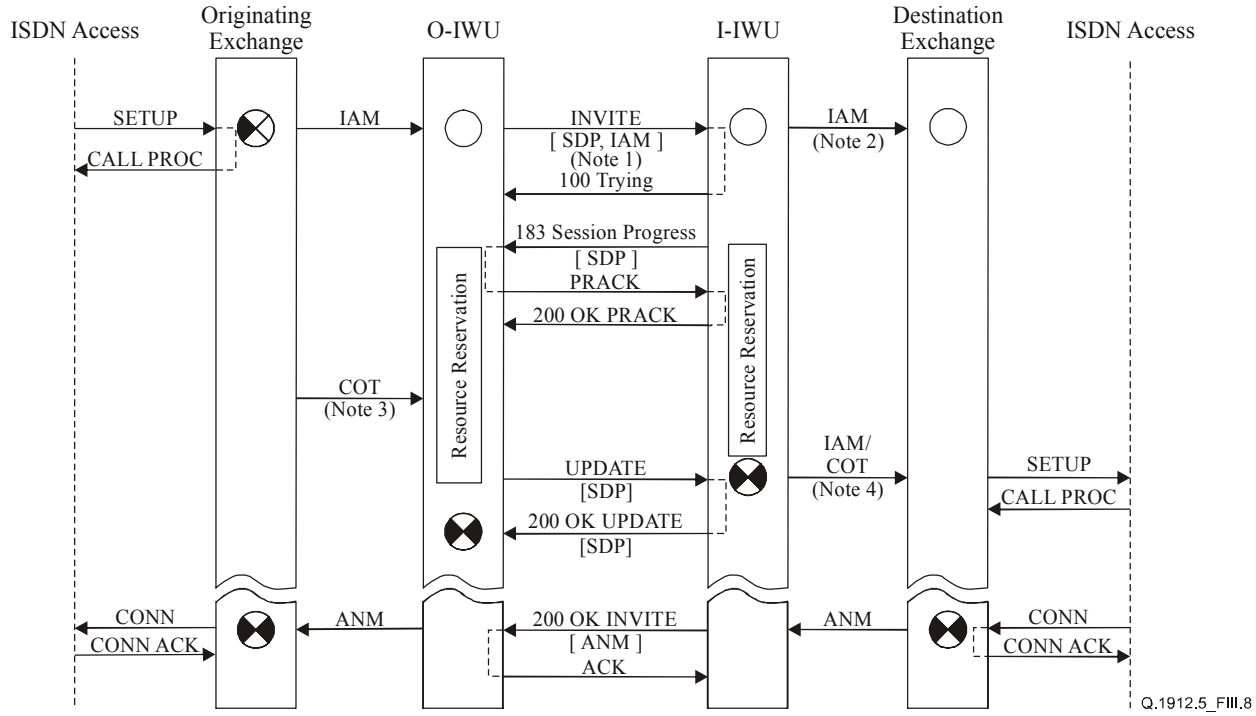
– ANM – clauses 6.7 and 7.5.

III.2.1.7 *En bloc*, end-to-end resource reservation

See 2.1/Q.764 and 13.1/RFC 3312.

Figure III.8 shows the sequence of messages for successful call set-up for an incoming ISUP call in the case of Profile C (SIP-I) operation. The O-IWU indicates mandatory end-to-end sendrecv quality of service preconditions in the SDP of initial INVITE and also the required use of reliable provisional responses. The I-IWU requests confirmation from the O-IWU of end-to-end network resource reservation in the SDP of 183 Session Progress response and begins with its own network resource reservation. After successful network resource reservation and reception of a COT message (if the IAM from originating exchange indicated "*COT on previous circuit*"), the O-IWU indicates its status in the SDP of an UPDATE request. Having already reserved network resources, I-IWU confirms the achieved end-to-end sendrecv precondition in the SDP of 200 OK UPDATE.

Depending on configuration, I-IWU can directly send IAM with *"COT on previous circuit"* indication and continue the call setup by sending COT after meeting the preconditions. As an alternative, it can delay the sending of IAM until the meeting of preconditions. See 6.1.2 2).



NOTE 1 – INVITE contains mandatory end-to-end sendrecv preconditions and the Required header field with the option tag 100rel.
NOTE 2 – In the case of immediate sending of IAM, it will contain *"COT on previous circuit"* indication.
NOTE 3 – COT on the originating side is optional, depending on the indication in the IAM.
NOTE 4 – The choice between deferred IAM and COT depends on the I-IWU configuration, see 6.1.2.

Figure III.8/Q.1912.5 – *En bloc*, end-to-end preconditions for resource reservation

For detailed messages and parameter mapping, refer to:

– IAM – clauses 6.1.2 2) and 7.1 B).

– COT message – clauses 6.3 and 7.1 B).

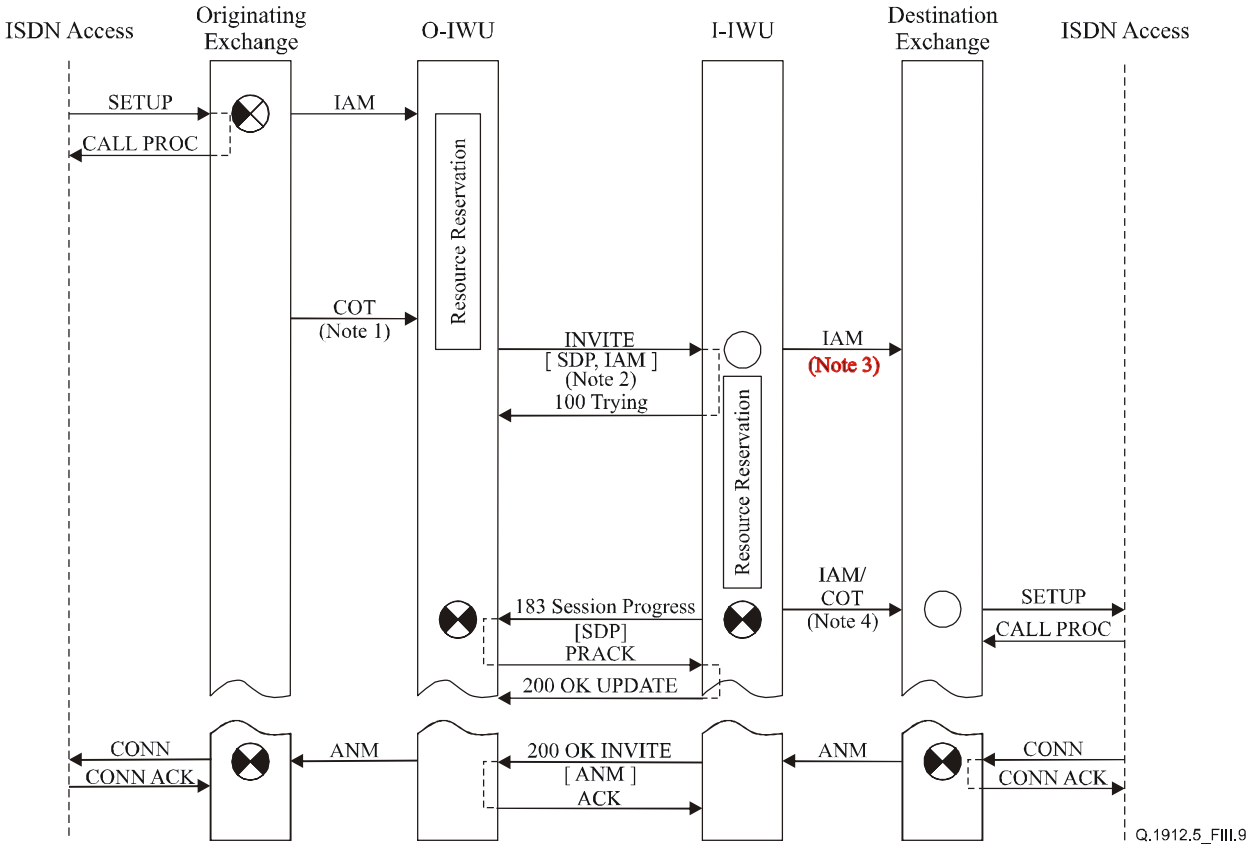
– ANM – clauses 6.7 and 7.5.

III.2.1.8 *En bloc*, segmented resource reservation

See 2.1/Q.764 and 13.2/RFC 3312.

Figure III.9 shows the sequence of messages for successful call set-up for an incoming ISUP call in the case of Profile C (SIP-I) operation. On the receipt of IAM, the O-IWU reserves resources in its local network branch. On successful reservation and reception of a COT message (if the IAM from originating exchange indicated "*COT on previous circuit*"), the O-IWU includes the request for the reservation of the local network resource at I-IWU and also the required use of reliable provisional responses in the SDP of the initial INVITE. After local network resource reservation the I-IWU notifies the O-IWU with SDP in 183 Session Progress response that all preconditions are met.

Depending on configuration, I-IWU can directly send IAM with *"COT on previous circuit"* indication and continue the call setup by sending COT after meeting the preconditions. As an alternative, it can delay the sending of IAM until the meeting of preconditions.



NOTE 1 – COT on the originating side is optional, depending on the indication in the IAM.
NOTE 2 – INVITE contains mandatory segmented sendrecv preconditions and the Required header field with the option tag 100rel.
NOTE 3 – In the case of immediate sending of IAM, it will contain *"COT on previous circuit"* indication.
NOTE 4 – The choice between deferred IAM and COT depends on the I-IWU configuration, see 6.1.2.

Figure III.9/Q.1912.5 – *En bloc*, segmented preconditions for resource reservation

For detailed messages and parameter mapping, refer to:

– IAM – clauses 6.1.2 2) and 7.1 B).

– COT message – clauses 6.3 and 7.1 B).

– ANM – clauses 6.7 and 7.5.

III.2.1.9 *En bloc*, automatic call answering

See 2.1/Q.764 and RFC 3261.

Figure III.10 shows the sequence of messages for successful call set-up for an incoming ISUP call in the case of Profile C (SIP-I) operation. The I-IWU 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 bearer path in both directions on the receipt of connect indication.

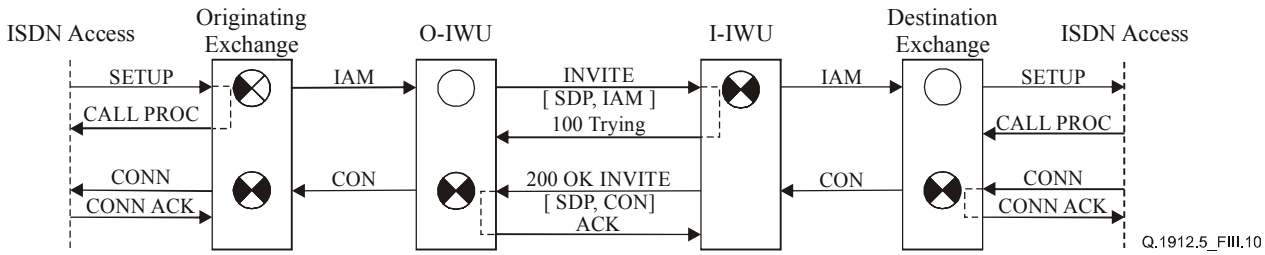


Figure III.10/Q.1912.5 – *En bloc*, automatic answering terminal

For detailed messages and parameter mapping, refer to:

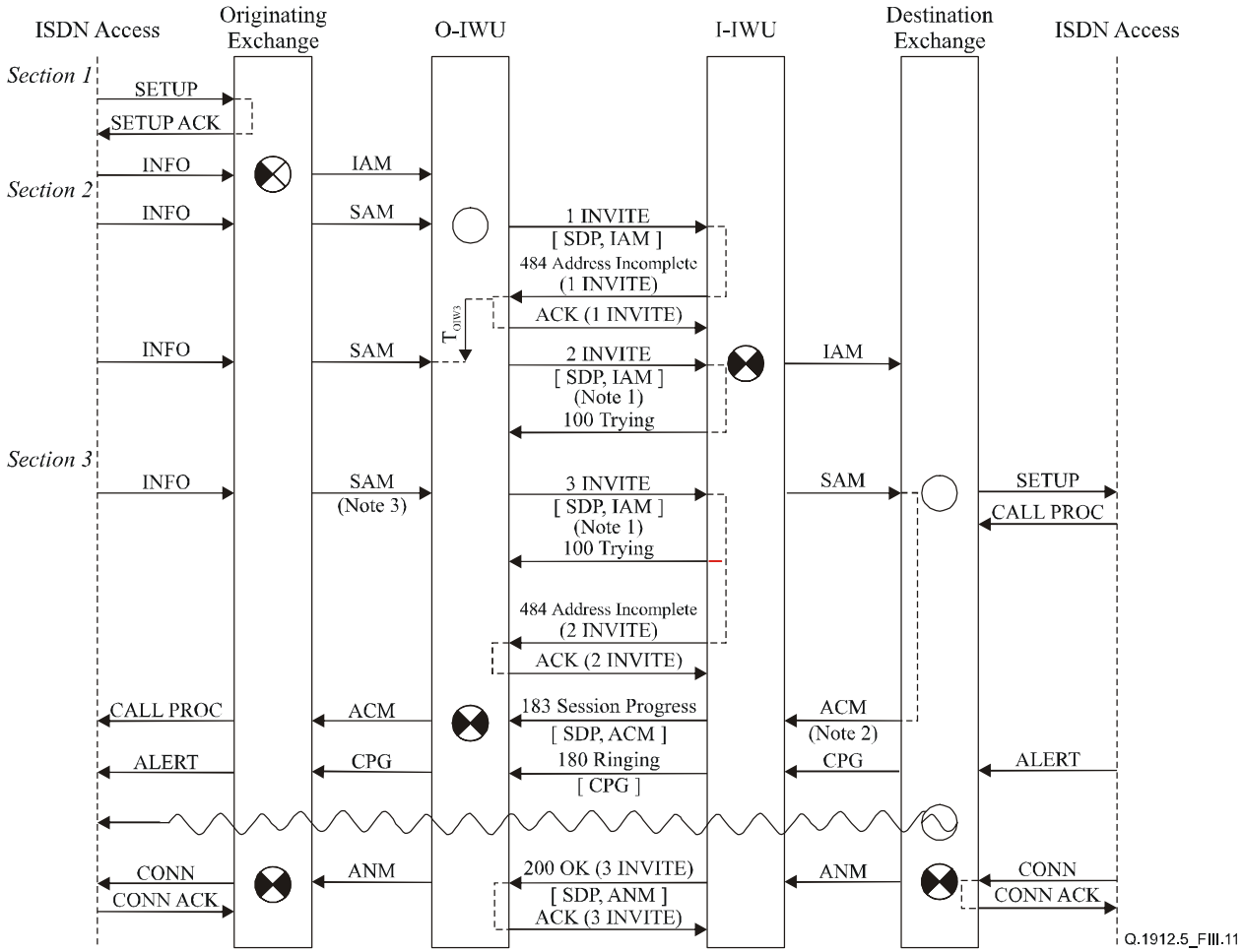
– IAM – clauses 6.1.1 1) and 7.1 A).

– CON message – clauses 6.4 and 7.5.

III.2.1.10 Overlap signalling

See 2.1/Q.764 and RFC 3261.

Figure III.11 shows the sequence of messages when overlap sending is in use. The figure is divided into three sections where, in the first section, the O-IWU did not receive enough digits to progress the call. In the second section, O-IWU receives enough digits, but the I-IWU cannot progress the call and sends a 484 Address Incomplete final response. Since the O-IWU is configured to perform overlap sending, it does not release the call but starts the timer T_{OIW3}. Before timer T_{OIW3} expires a following SAM triggers the sending of subsequent INVITE 2 and clears the timer T_{OIW3}. In the third section, the next SAM triggers the sending of subsequent INVITE 3. On the reception of INVITE 3, the I-IWU sends the SAM to the destination exchange and terminates the INVITE 2 transaction with a 484 Address Incomplete final response. The O-IWU clears the transaction 2 INVITE, but does not start timer T_{OIW3} and does not release the call as the INVITE 3 transaction is still pending.



NOTE 1 – INVITE 2 and INVITE 3 have the same Call-ID and From tag as INVITE 1, but have Request-URIs updated to include all digits received to that point. For details see 7.2.
NOTE 2 – The ACM is independently generated at the destination exchange with the following indicators: Called Party Status = *"no indication"*, ISDN Access Indicator = *"ISDN access"*.
NOTE 3 – The number of SAMs shown is for illustration only. In practice there may be zero or more SAMs.

Figure III.11/Q.1912.5 – Overlap addressing

For detailed messages and parameter mapping, refer to:

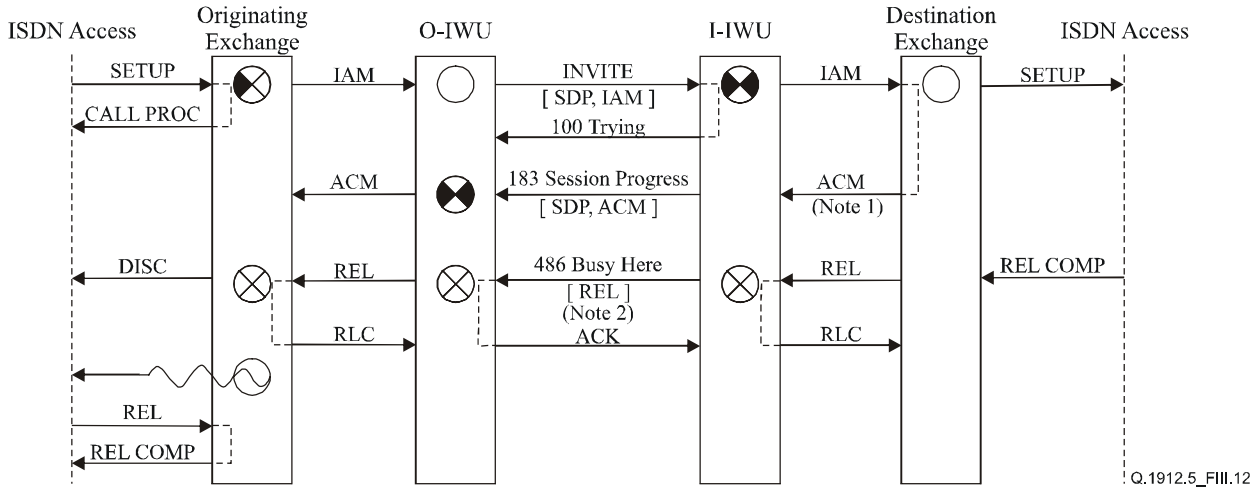
– IAM – clauses 6.1.2 and 7.1.
– SAM – clauses 6.2.1 and 7.2.1.
– ACM – clauses 6.5 2) and 7.3.2.
– CPG message – clauses 6.6 and 7.3.1.
– ANM – clauses 6.7 and 7.5.

III.2.2 Unsuccessful call set-up procedures/call flow diagrams for basic call control

III.2.2.1 Backward release during call setup

See 2.2/Q.764 and RFC 3261.

Figure III.12 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 – If early ACM is used, the ACM is independently generated at the destination exchange with the following indicators: Called Party Status = *"no indication"*, ISDN Access Indicator = *"non-ISDN access"*.
NOTE 2 – See Tables 21 and 40 for mapping between release causes and SIP status codes.

Figure III.12/Q.1912.5 – Backward release during call setup

For detailed messages and parameter mapping, refer to:

– IAM – clauses 6.1.2 and 7.1.

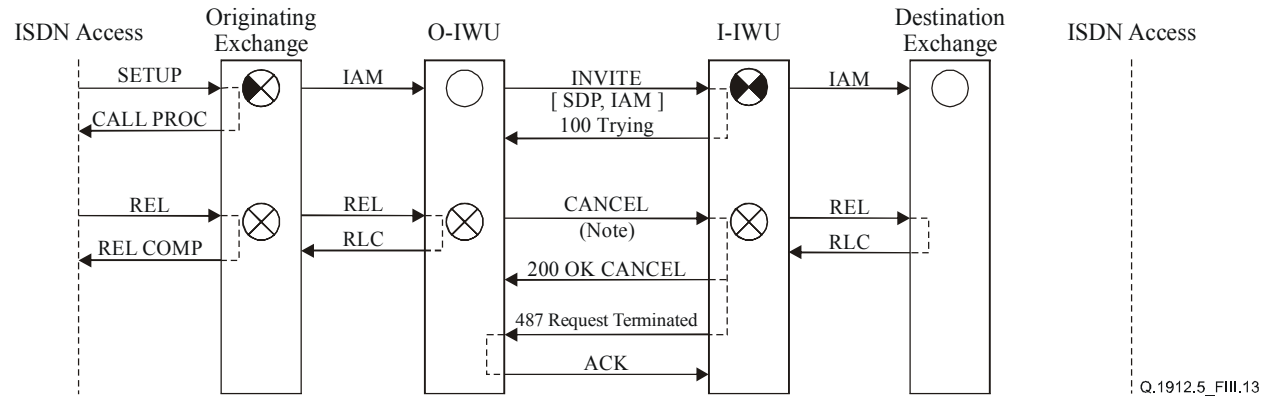
– ACM – clauses 6.5 2) and 7.3.2.

– REL message – clauses 6.11.2 (Table 21) and 7.7.6 (Table 40).

III.2.2.2 Forward release during call setup, no early dialog

See 2.2/Q.764 and RFC 3261.

Figure III.13 shows a premature release situation where a Release message is received at the O-IWU prior to successful early dialog setup. In this situation, a CANCEL request is sent to the I-IWU and the normal release procedure is started.



NOTE – REL is not encapsulated in CANCEL because the latter is a hop-by-hop request. If the O-IWU supports the Reason header field the Cause Value is mapped to that field. See 6.11.1 and 7.7.1.

Figure III.13/Q.1912.5 – Forward release during call setup, no early dialog is established

For detailed messages and parameter mapping, refer to:

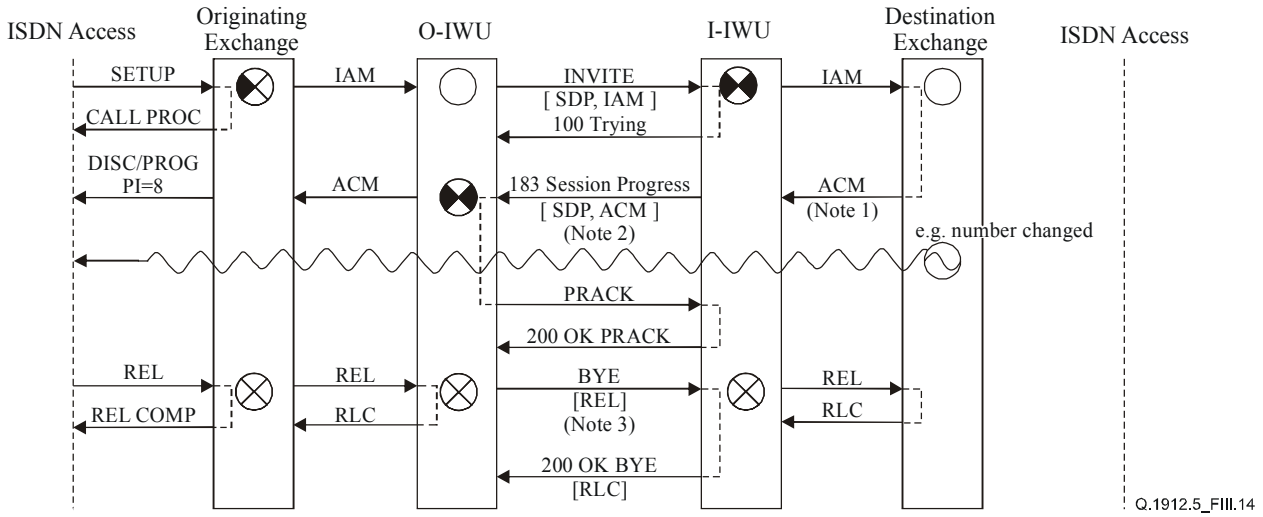
– IAM – clauses 6.1.2 and 7.1.

– REL message – clauses 6.11.1 and 7.7.1 1).

III.2.2.3 Forward release during call setup, early dialog is established

See 2.2/Q.764 and RFC 3261.

Figure III.14 shows an unsuccessful call set-up where certain tones and announcements are generated in the destination exchange during call establishment. The O-IWU indicates the required support of reliable provisional responses by adding option tag 100rel to the Required header field of the INVITE request. The REL message is mapped and encapsulated in the BYE request as an early dialog is already established through the reception of a To tag in the 183 Session Progress response.



NOTE 1 – The ACM is not mapped from a message from the destination user. It is independently generated at the destination exchange.
NOTE 2 – The 183 Session Progress response contains the To header field tag which creates an early dialogue.
NOTE 3 – Since an early dialogue has been established, the O-IWU can release the call with a BYE rather than a CANCEL. Since BYE is end-to-end, it can encapsulate the REL.

Figure III.14/Q.1912.5 – Forward release during call setup, early dialog is already established

For detailed messages and parameter mapping, refer to:

– IAM – clauses 6.1.2 and 7.1.

– ACM – clauses 6.5 2) and 7.3.2.

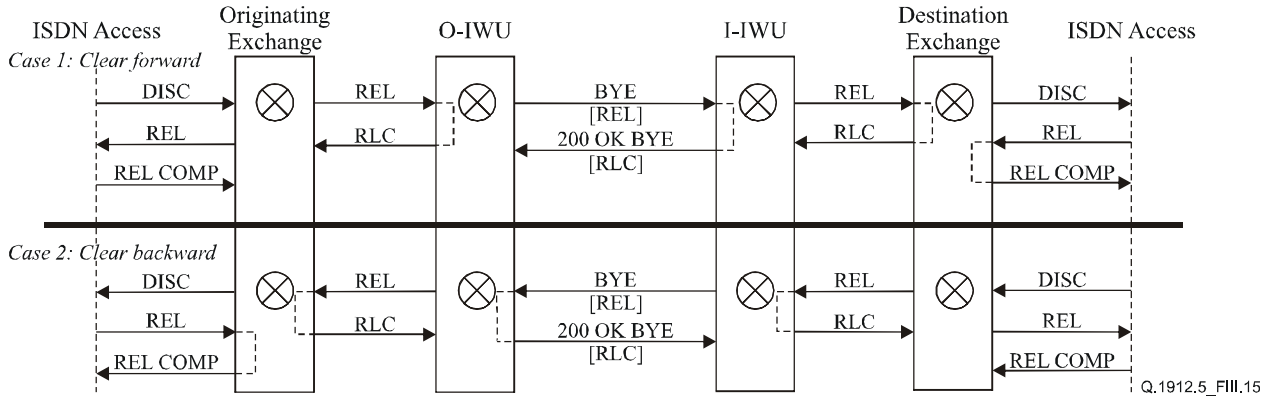
– REL message – clauses 6.11.1 and 7.7.1 2).

III.2.3 Release procedures/call flow diagrams for basic call control

III.2.3.1 Normal call release procedure without tone provision

See 2.3/Q.764 and RFC 3261.

Figure III.15 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 – This procedure is applicable where in-band tones or announcements are not provided, e.g., 64 kbit/s unrestricted bearer.

Figure III.15/Q.1912.5 – Normal call release procedure without tone provision

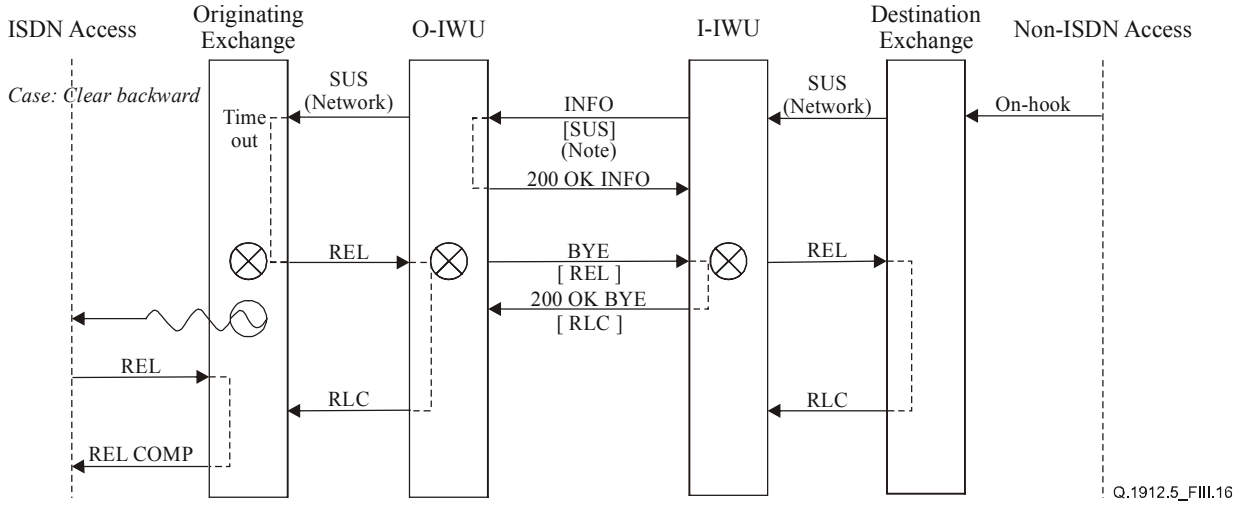
For detailed messages and parameter mapping, refer to:

– REL message – clauses 6.11.2 and 7.7.3.

III.2.3.2 Normal release with SUS message encapsulation

See 2.3/Q.764 and RFC 3261.

Figure III.16 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 an INFO request.



NOTE – The transparent transport of SUS is possible only in the case of Profile C (SIP-I) operation.

Figure III.16/Q.1912.5 – Normal release with SUS message encapsulation

For detailed messages and parameter mapping, refer to:

– SUS message – clause 6.9 (no special interworking at O-IWU).

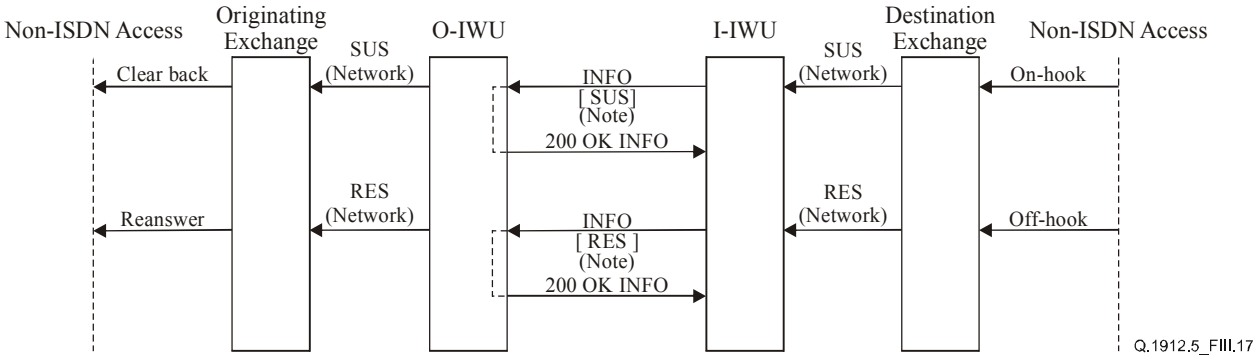
– REL message – clauses 6.11.1 and 7.7.1 2).

III.2.4 Suspend/resume procedures/call flow diagrams for basic call control

III.2.4.1 Suspend/resume non-ISDN access to non-ISDN access

See 2.4/Q.764 and RFC 3261.

Figure III.17 illustrates suspend and resume procedures for non-ISDN access – non-ISDN access interworking in the case of Profile C (SIP-I) operation. At the I-IWU the SUS message is mapped and encapsulated into an INFO request. At the O-IWU, the RES message is also mapped and encapsulated into an INFO request.



NOTE – The transparent transport of SUS and RES is possible only in the case of Profile C (SIP-I) operation.

Figure III.17/Q.1912.5 – Suspend/resume non-ISDN access to non-ISDN access

For detailed messages and parameter mapping, refer to:

– SUS message – clause 6.9.

– RES message – clause 6.10.

Neither message requires interworking beyond de-encapsulation at the O-IWU.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	**Switching and signalling**
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communications
Series Y	Global information infrastructure, Internet protocol aspects and Next Generation Networks
Series Z	Languages and general software aspects for telecommunication systems

Geneva, 2004