STATUS OF THIS MEMO

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as work in progress.

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Abstract

SIP-T (earlier referred to as the SIP-BCP-T) is a mechanism that uses SIP to facilitate the interconnection of the PSTN with IP. This document explains the context and the architectures in which SIP-T may be used. This document has to be studied in conjunction with the existing SIP-T (referred to in some older documents as SIP-BCP-T) literature.

1. Introduction

The Session Initiation Protocol (SIP) is an application-layer control protocol that can establish, modify and terminate multimedia sessions or calls. These multimedia sessions include multimedia conferences, Internet telephony and similar applications. SIP is one of the key protocols used to implement VoIP. Although performing telephony call signaling and transporting the associated audio media over IP beget
significant advantages, a VoIP network cannot exist in isolation. It is vital for a SIP network to be smoothly interfaced to the PSTN.

An important characteristic of any VoIP SIP network is FEATURE TRANSPARENCY with respect to the PSTN. Traditional telecom services such as call waiting, 800 numbers, etc. implemented in SS7 should be offered by a SIP network in a manner that precludes any debilitating difference in the user experience. It is necessary that SIP support the primitives for the delivery of such services where the terminating point is a regular SIP-phone (see definition in section 2 below). However, it is essential that SS7 information be available at the points of PSTN inter-connection to ensure transparency of features not otherwise supported in SIP. SS7 information should be available in its entirety and without any loss to the SIP network across the PSTN-IP interface. A compelling need to do so also arises from the fact that certain networks utilize proprietary ISUP parameters to transmit certain information through their networks. Another requirement is ROUTABILITY in the SIP network - a SIP message that is used to set up a telephone call should bear sufficient information that would enable it to be appropriately routed to its destination by proxy servers in the SIP network. The SIP-T (SIP for Telephones) effort provides a framework for the integration of legacy telephony signaling into SIP messages. SIP-T fulfils the above two requirements through ENCAPSULATION and TRANSLATION respectively. At the point of inter-connection SS7 ISUP messages are encapsulated within SIP in order that information necessary for services is not discarded. Also, certain information is translated from an SS7 ISUP message to generate the corresponding SIP header information in order to facilitate the routing of SIP messages.

While pure SIP has all the requisite instruments for the establishment and termination of calls, it does not have any mechanism to carry any MID-CALL CONTROL INFORMATION along the SIP signaling path during the session. This mid-call information does not result in any change in the state of SIP calls or the parameters of the sessions that SIP initiates. A provision to transmit such optional application layer information is also needed. Thus, SIP-T also has to cater to this requirement of transferring mid-call signaling information.

Problem definition: To provide ISUP transparency across PSTN-IP inter-connections

<table>
<thead>
<tr>
<th>PSTN-IP Inter-connection Requirements</th>
<th>SIP-T Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability of ISUP information</td>
<td>Encapsulation of ISUP in the SIP body</td>
</tr>
</tbody>
</table>
**Routability of SIP messages with ISUP dependencies**

**Translation of ISUP information into the SIP header**

**Transfer of mid-call ISUP signaling messages**

**Use of the INFO Method for mid-call signaling**
(See section 4.d)

Table 1: SIP-T features that fulfill PSTN-IP inter-connection requirements

**Note:**

1. Many modes of signaling are used in telephony (SS7 ISUP, BTNUP, ISDN, etc.). This document concentrates only on SS7 ISUP and aims to specify the behavior across ISUP-SIP interfaces only.

2. SIP-T details the methods and tools necessary for the PSTN and VoIP networks to inter-operate via the SIP protocol. This paper provides a context for the usage of SIP-T and characterizes architectures that employ SIP-T. It also highlights the functions of the different elements in a SIP-T-enabled network. This document is to be assessed in conjunction with the SIP-BCP-T (presently known as SIP-T) document-set.

### 2. SIP-T for PSTN-IP Interconnections

SIP-T is not a new protocol. It embodies the manner in which SIP must be used to provide ISUP transparency across PSTN-IP inter-connections. It is to be used in situations where an IP network (SIP network, for the purposes of our discussion) interfaces with the PSTN. Such a network may frequently need to hand a call over to another network in order to terminate it. Therefore, such networks do not normally exist in isolation. They have business relationships with each other resulting in them being peered together in order to terminate calls. Thus, SIP-T originates from networks and it terminates at other sites within the network or at a peer network. It is therefore an intra-network or inter-network mechanism that uses SIP. Networks that are peered together adhere to certain rules as specified in their agreements with each other. Thus, SIP-T may not traverse networks arbitrarily. The originator of a SIP-T message could have a relationship with the receiver of the message.

It follows that a network should have PSTN access in order to originate SIP-T (PSTN origination). However, a network need not have PSTN access in order to receive SIP-T. A network can terminate calls directed at IP-based end-user devices that are homed to it or to the PSTN. Or, a network may just serve as a transit network with IP inter-connections to other networks that have PSTN interfaces. Such a
transit network will accept VoIP calls from one network and hand them off to another network where they may be terminated. And, the originating network most often will not know whether the receiving (i.e. next-hop) network is a terminating network or a transit network. (See Note 1.)

The PSTN interfaces that a particular network is associated with define the ISUP variants that that network supports. This capability of a network to be able to support a particular version of ISUP determines whether it can provide feature transparency while terminating a call.

The following are the components of a SIP-T-enabled network.

1. PSTN: This is the Public Switched Telephone Network. It may either refer to the entire inter-connected collection of local, long-distance and international phone companies or some subset thereof.

2. IP-endpoint: Any sort of device that originates SIP-calls to the network may be considered an IP end-point for the purposes of this document. Thus, the following devices may classify as

   IP-end-points: a. MGC UA: A Media Gateway Controller (MGC) is an entity used to control a gateway (that is typically used to provide conversion between the audio signals carried on telephone circuits and data packets carried over packet networks). The term MGC is thus used in this document to typify entities that control the point of inter-connection between the PSTN and the IP-network. An MGC speaks ISUP to the PSTN and SIP to the IP-network and converts between the two.

   b. SIP-phone: The term used to represent all end-user devices that originate SIP calls.

   c. Firewalls or edge-elements through which calls may enter the network from that of a peer network.

3. Proxy: A proxy is a SIP entity that helps route SIP signaling messages to their destinations. Consequently, a proxy might route SIP messages to other proxies (some of which may be co-located with firewalls), MGCs and SIP-phones.
In the above figure the IP network (see Note 2) bridges two LECs together. SIP is employed as the VoIP protocol used to set up and tear down VoIP sessions and calls. The VoIP network receives SS7 messages from one PSTN interface (the PSTN origination) and sends them out on another (PSTN termination). Let a call originate from LEC1 and be terminated by LEC2. The originator is defined as the generator of the SIP setup signaling and the terminator is defined as the consumer of the SIP setup signaling. MGC1 is thus the originator and MGC2, the terminator. One or more proxies may be used to route the call from the originator to the terminator.

In order to seamlessly integrate the IP network with the PSTN, it is important to retain the SS7 information at the points of inter-connection and use this information for the purpose of call establishment. By including ISUP information in the SIP signaling the network automatically leverages the call establishment capability of SIP while trying to establish a session whose attributes may be influenced by the ISUP information.

SIP-T is employed in order to leverage the intrinsic benefits of utilizing SIP: call control and establishment via proxies, capability to enable new services, etc. However, if only the transportation of ISUP was relevant here, any protocol for the transport of signaling information may be used to achieve this, obviating the need for SIP and consequently that of SIP-T. SIP-T thus facilitates call establishment and the enabling of new services over the IP network while simultaneously providing a method of inter-connection with the PSTN.

SIP-T preserves the ISUP information received by the originator by
encapsulating it in the SIP messages that it uses to establish a session with the terminator. Translation of information from the received ISUP messages to the SIP header fields enables these messages to be effectively routed to the terminator. The terminator then generates the ISUP message from the received SIP message and sends it to the PSTN at the terminating end.

Voice calls do not always have to originate and terminate in the PSTN (via MGCs). They may either originate and/or terminate in SIP phones. The alternatives for call origination and termination suggest the following possibilities for calls that traverse through an IP network:

Note: The words originator and terminator used in the following text are used with reference to the SIP setup signaling (as explained above). The words origination and termination as in ‘PSTN origination’, ’IP termination’, etc. are used to refer to the call from the actual, physical origination to the termination, i.e., between the two end-users that communicate.)

1. PSTN origination - PSTN termination: The originator (ingress-MGC) receives ISUP from the PSTN and it retains this information (via encapsulation and translation) in the SIP messages that it transmits towards the terminator (egress-MGC). The terminator extracts the ISUP content from the SIP message that it receives and it dispatches this to the PSTN.

2. PSTN origination - IP termination: The originator (MGC) receives ISUP from the PSTN and it preserves this ISUP information in the SIP messages (via encapsulation and translation) that it directs towards the terminator (SIP-phone). The terminator has no use for the encapsulated ISUP and ignores it.

3. IP origination - PSTN termination: A SIP-phone originates the call towards the network. A SIP message is thus received at the point of entry to the IP network and is routed to the appropriate terminating end-point (terminator). The terminator (MGC) tries to terminate the call to the appropriate PSTN interface, based on information that is present in the received SIP header. The ISUP message that is to be sent to the LEC must be generated from information gleaned from the SIP header.

4. IP origination - IP termination: This is a case for pure SIP. SIP-T does not come into play as there is no PSTN involvement.

Thus, there are three distinct elements (from a functional point of view) in a SIP VoIP network offering PSTN inter-connection:
1. The originator of SIP signaling
2. The terminator of SIP signaling
3. The network of proxies that routes calls from the originator to the terminator.

The capabilities required of these entities are ascertained by exploring the path that a SIP message takes from its generation to its final consumption. This is discussed in the next section.

3. SIP-T Configurations and Roles

For the purposes of this document, an MGC is the point of interconnection between the PSTN and the IP network and ISUP is the protocol used for call signaling in SS7 networks. SIP is the protocol used for the establishment and termination of sessions in the IP world. The IP body (as portrayed in all the illustrations in this document) may encompass a mass of distinct SIP-enabled IP networks, inter-connected to each other through SIP proxies and a firewall infrastructure. Proxies are employed to facilitate the routing of the SIP messages, both within and across the IP networks. Firewalls may be deployed at the point of inter-connection in order to insure that the transfer of calls does not constitute a security breach for either network.

The different configurations that are possible in a SIP-T network are presented in section 3.1 below. Originator, terminator and proxy requirements are addressed in section 3.2.

3.1 SIP-T Configurations

The different configurations that are possible in PSTN-IP interconnections are presented below.

3.1.1 SIP bridging (PSTN - IP - PSTN)
A situation in which a SIP network connects two instances of the telephone network is an example of ‘SIP bridging’. A telephone call originates in the PSTN and an SS7 ISUP message is dispatched to the MGC that is the point of interconnection with the PSTN network. This MGC is the point of origination (or ingress) for message flows over the IP network for this call. The call progresses in the IP network (through proxies that route the call) until it is terminated at the appropriate PSTN interface. The MGC that interconnects to the PSTN at the egress is the point of termination of the IP message flow. This egress-MGC then uses ISUP to communicate with the PSTN at the terminating end. SIP is used in the IP network to determine the appropriate point of termination and to establish a session between the origination and termination in order to carry the call through the IP network.

A very elementary call-flow for SIP bridging is as shown below.

```
PSTN            MGC#1   Proxy    MGC#2          PSTN
--------IAM------> |-------INVITE------>
                  |         |----IAM------>
                  |<--100 TRYING-->
                  |<-----18x-------
                  |<----ACM------>
                  |<----ANM------>
                  |<----200 OK----->
                  |<-----ACK------>
====================Conversation================
```
3.1.2 PSTN origination - IP termination

A call originates from the PSTN and terminates at a SIP-phone.

A simple call-flow depicting the ISUP and SIP signaling for a PSTN-originated call terminating in IP as follows:

<table>
<thead>
<tr>
<th>PSTN</th>
<th>MGC</th>
<th>VoIP Network</th>
<th>Proxy</th>
<th>SIP-phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>-----</td>
<td>IAM</td>
<td></td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>&lt;---</td>
<td>INV</td>
<td>---------INV</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;-----</td>
<td>TRYING---</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&lt;---</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&lt;---</td>
</tr>
<tr>
<td></td>
<td>&lt;---</td>
<td>ACM------</td>
<td></td>
<td>&lt;-----</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&lt;-----</td>
</tr>
<tr>
<td></td>
<td>&lt;---</td>
<td>ANM------</td>
<td></td>
<td>&lt;------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&lt;-------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&lt;-------</td>
</tr>
<tr>
<td></td>
<td>-----</td>
<td>REL------</td>
<td></td>
<td>&lt;-------</td>
</tr>
</tbody>
</table>

Figure 3: PSTN origination - IP termination
3.1.3 IP origination - PSTN termination

A call originates from a SIP-phone and terminates in the PSTN. There is no telephony interface at call-origination.

A simple call-flow illustrating the different legs in the call is as shown below.

```
SIP-phone         Proxy                    MGC          PSTN
|-----INVITE------>|                       |                 |
|<---100 TRYING---|<--------100 TRYING------|-------IAM------>|
|<------18x-------|<--------18x---------|<------ACM-------|
|<------200 OK-----|<--------200 OK-------|<------ANM-------|
|<------ACK-------|-----------ACK---------|                |
|<------BYE-------|-----------BYE---------|
```

Figure 4: IP origination - PSTN termination
3.2 SIP-T Roles

Originator and terminator requirements are derived in sections 3.2.1 and 3.2.2 respectively. Proxy requirements are described in section 3.2.3.

3.2.1 Originator

The fundamental function of the originator is to generate the SIP call-setup signaling. The MGC is the originator for PSTN originations, while the SIP-phone is the originator for IP-originations. In either case, it should be noted that the originator is not certain of the nature of the termination, i.e. whether it is in IP or the PSTN.

In the case of calls originating in the PSTN (figures 2 and 3), the originator (MGC) takes the necessary steps to preserve the ISUP information. It formulates the SIP INVITE from the ISUP that it has received from the PSTN. The originator is entrusted with the responsibility of identifying the nature of the ISUP (ETSI, ANSI, etc.) that it has received, depending on the nature of the PSTN interface. This ISUP is correctly classified to be a particular ISUP variant that the originating network supports. The MGC then translates certain ISUP information into the SIP headers (see Note 3), so as to enable the SIP message to be routed. This might, for instance, involve setting the ‘To’ field in the INVITE to the dialed number (Called Party Number) of the ISUP IAM. The MGC then encapsulates the ISUP IAM into the SIP INVITE and ships it out.

The originator is not certain of the entity that will terminate the call - the fact that the terminating entity could be a SIP-phone that does not need ISUP is not known to the originator, and it proceeds with ISUP encapsulation. It is the responsibility of the terminator to determine whether it wants to utilize the encapsulated ISUP or not.

In case of an IP-origination (figure 4) the SIP-phone is the originator. The SIP-phone issues the SIP signaling that is directed to a SIP proxy that allows it entry into the network. There is no ISUP to encapsulate, as there is no PSTN interface. Although the call may terminate in the telephone network and need ISUP in order that that may take place, the originator may not be aware of this and consequently, should not be burdened with the task of generating the ISUP. It is the responsibility of the terminator to generate ISUP if
necessary (i.e. for PSTN terminations only, and not for IP terminations).

Thus, an originator must generate the SIP signaling while performing ISUP encapsulation and translation (ISUP to SIP) wherever possible (PSTN originations). This must be done irrespective of the nature of the termination (whether SIP or SS7).

Originator requirements: encapsulate ISUP, translate information from ISUP to SIP

3.2.2 Terminator

The terminator is the consumer of the SIP signaling. The terminator is a SIP UA that must be capable of standard SIP processing. The MGC is the terminator in case of PSTN terminations and is responsible for terminating the call to the LEC via ISUP. The SIP-phone is the terminator for IP terminations.

In case of PSTN terminations (figures 2 and 4) the MGC at the egress tries to terminate the call to the appropriate PSTN interface. The terminator generates the ISUP from the incoming SIP message. The ISUP may either be extracted directly from the SIP message that encapsulates it or gleaned from the SIP headers. In order to make the determination about the PSTN termination the terminator looks either into the encapsulated ISUP that it has received, or the SIP header. In some instances the ISUP that has been retrieved from the SIP message may need to be modified before it is sent out to the LEC. (See Note 4)

In case of an IP termination (figure 3) the SIP-phone that receives ISUP-encapsulated SIP messages from the network disregards the ISUP as it does not hold any significance for an IP-termination.

Terminator requirements: standard SIP processing, interpretation of encapsulated ISUP (multi-part MIME; see 4.b.1), ignorance of unknown MIME content (specifically ISUP)

3.2.3 Proxy

Proxies are entrusted with the task of routing messages to other proxies, both within and at the edges of the network (the latter may be co-located with firewalls that monitor the point of interconnection with external elements), MGCs and SIP-phones.

A call that enters a given network (say network A) may be terminated at the appropriate PSTN interface (MGC) or SIP-phone homed to network A (intra-network), or, it may be handed off to a peer network for
termination through an edge proxy (inter-network). The proxies make this determination based on their evaluation of the routable elements in the SIP message. The routable elements could be the dialed number or the ISUP variant or any other parameter (See Note 5.) The edge elements (both MGCs and proxies) must be cognizant of the potential (capabilities) of their interfaces (PSTN interfaces and peer proxies respectively) in order to facilitate routing.

Feature transparency of ISUP is central to the notion of SIP-T. Compatibility between the ISUP variants of the originating and terminating PSTN interfaces automatically leads to feature transparency. The termination of a call at a point that results in greater proximity to the final destination (rate considerations) is also preferable. The preference of one over the other results in a trade-off between simplicity of operation and cost. (See Note 6.) The requirement of procuring a reasonable rate may dictate that a SIP-T call spans dissimilar PSTN interfaces (SIP bridging across different ISUP variants). Two different possibilities arise here:

a) The need for ISUP feature transparency may necessitate ISUP translation (conversion), i.e. conversion from one version of ISUP to another in order to facilitate the termination of that call over an interface (MGC) that does not support the ISUP variant of the originating PSTN interface. (See Note 7.) Although in theory conversion may be performed at any point in the path, it is viable to perform it at a point that is at the greatest proximity to the terminating MGC. This may be accomplished by transferring the call to an Application Server (See Note 8) that spawns an application to perform the conversion. Feature transparency in this case is contingent on the availability of resources to perform ISUP conversion, and, is secured as a result of an increase in the call-set up time.

b) The alternative would be to sacrifice ISUP transparency by handing the call off to an interface (MGC) that does not support the version of the originating ISUP. The terminating MGC would then just ignore the encapsulated ISUP and use the information in the SIP header to terminate the call.

Thus, the proxy must have the intelligence to make a judicious choice given the options available to it. The task of determining which peer proxy or MGC to hand off the call to is a routing problem that is contingent upon the choice of the routable elements.

Proxy requirements: ability to route based on choice of routable elements

In summary:
The ORIGINATOR must try to perform ISUP encapsulation and translation irrespective of the nature of the termination.

The TERMINATOR must either interpret the multipart MIME or ignore it while performing standard SIP processing. The TERMINATOR must regenerate the ISUP if the call terminates in the PSTN. Two possibilities arise:

a) The ISUP may be extracted from the SIP message body, or,

b) The ISUP may be generated from information in the SIP headers.

The TERMINATOR must ignore any ISUP present in the SIP-T message in case of IP termination.

A PROXY must be able to route a call based on the choice of routable elements.

4. Components of the SIP-T proposal:

The key items of the specification that would address each of the requirements in detail are as follows:

a. Core SIP SIP-T uses the methods and procedures of pure SIP as defined by RFC 2543.

b. Encapsulation

b.1 The ISUP MIME type

Encapsulation of the PSTN signaling is one of the major requirements of SIP-T. SIP-T uses MIME multi-part to enable SIP messages to contain multiple payloads (SDP, ISUP, etc.). Numerous ISUP variants are in existence today and the ISUP MIME type should be such that it enables ISUP recognition in the simplest manner possible. The ISUP nomenclature scheme should meet the design goals of simplicity and extensibility while providing a complete ISUP description. A scheme for performing ISUP encapsulation using multi-part MIME has been described in [2].

c. Translation

ISUP is used between the IP network and the PSTN, while SIP is used within the IP network. The MGC acts as a protocol converter between SIP and ISUP. This dictates that signaling information be shared across the two protocols so that VoIP sessions and SS7 connections may be established appropriately.

c.1 ISUP SIP message mapping
This describes a mapping between ISUP and SIP. At the PSTN-IP interface the MG is entrusted with the task of generating an ISUP message for each SIP message received and vice versa. It is necessary to specify the rules that govern the mapping between ISUP and SIP messages (i.e., what ISUP messages may be encapsulated in a particular SIP message: an IAM must be encapsulated in an INVITE, a REL in a BYE, etc.).

A potential mapping between ISUP and SIP messages has been described in draft-camarillo-sip-isup-bcp-00.txt (Best Current Practice for ISUP to SIP mapping).

c.2 ISUP parameter-SIP header mapping

A SIP message that is used to set up a telephone call should contain sufficient information that would enable it to be appropriately routed to its destination by proxy servers in the SIP network. This implies that a certain amount of ISUP information would have to be present in the SIP headers. It is important to lay down a set of rules that defines the procedure for translation of information from ISUP to SIP (for example, the Called Party Number in an ISUP IAM must be mapped onto the SIP To field, etc.) and also the interpretation of both elements (SIP headers and encapsulated ISUP) at the terminating entity. This issue becomes inherently more complicated by virtue of the fact that a message (especially an INVITE) may undergo transformation at the hands of an Application Server (AS), and consequently, one or both of the following may result:

a) the SIP headers and ISUP content are in conflict (an example in the Future Work section), or, b) a part of the encapsulated ISUP may be rendered irrelevant and obsolete.

Rules that delineate the preferred behavior of the entities in question (whether originating or terminating) and under the specific circumstances surrounding each such case need to be outlined.

d. Support for mid-call signaling

The INFO method

Pure SIP does not have any provision for carrying any mid-call control information that is generated during a session. The INFO method (defined in draft-ietf-sip-info-method-04.txt (The SIP INFO Method) should be used for this purpose.
5. SIP Content Negotiation

The originator of a SIP-T request might package both SDP and ISUP elements into the same SIP message by using the MIME multipart format. If the terminator device did not support a multipart payload (multipart/mixed) or the ISUP MIME type, it would reject the SIP request with a 415 Unsupported Media Type specifying the media types it supports (default - SDP). The originator would then have to re-send the SIP request after stripping out the ISUP payload (i.e. with only the SDP payload) and this would then be accepted.

This is a rather cumbersome flow and it is highly desirable to have a mechanism by which the originator could signify which bodies are required and which are optional so that the terminator can silently discard optional bodies that it does not understand (like a SIP-phone ignoring the ISUP payload). This is contingent upon the terminator having support for a Content-type of multipart/mixed. The Content-Disposition header referenced in [1] should be applied to each of the MIME bodies in a MIME multipart to correctly specify how a given body must be interpreted by the UAS. The ISUP MIME type using the Content-Disposition header has been defined in [2]. An INVITE with a multipart payload (such as SDP and ISUP) can thus specify how each of the payloads may be processed, leading to call-flows such as the following:

1. Support for ISUP is optional. Therefore, UA2 accepts the INVITE irrespective of whether it can process the ISUP.

   UA1                   UA2
   INVITE-->
   (Content-type:multipart/mixed;
    Content-type: application/sdp;
    Content-disposition: session; handling=required;
    Content-type: application/isup;
    Content-disposition: signal; handling=optional;)

   <--18x

2. Support for ISUP is preferred. UA2 does not support the ISUP and rejects the INVITE with a 415 Unsupported Media Type. UA1 strips off the ISUP and re-sends the INVITE with SDP only and this is then accepted.

   UA1                   UA2
   INVITE-->
   (Content-type:multipart/mixed;
    Content-type: application/sdp;
    Content-disposition: session; handling=required;
    Content-type: application/isup;
3. Support for ISUP is mandatory for call establishment. UA2 does not support the ISUP and rejects the INVITE with a 415 Unsupported Media type. UA1 then directs its request to UA3.

UA1 to UA2
INVITE-->
(Content-type: multipart/mixed;
  Content-type: application/sdp;
  Content-disposition: session; handling=required;
  Content-type: application/isup;
  Content-disposition: signal; handling=required;)

UA1 to UA3
INVITE-->
(Content-type: multipart/mixed;
  Content-type: application/sdp;
  Content-disposition: session; handling=required;
  Content-type: application/isup;
  Content-disposition: signal; handling=required;)

Note: 1. These call-flows are not complete. Only the messages relevant to this discussion are shown. 2. Specifics of the ISUP MIME type can be obtained from [2]. The accordance with the rules of [2].

6. Security

SIP-T is an intra-network or inter-network signaling mechanism that may be subject to pre-existing relationships between the networks. The originator of a SIP-T message could have a relationship with the receiver of the message. Each network should have the adequate
security apparatus (firewalls, etc.) in place to ensure that the transfer of calls does not result in any security violations.

It has to be noted that the transit of ISUP in SIP bodies may provide opportunities for abuse and fraud, especially by untrusted SIP endpoints that are potential recipients of SIP-T traffic. Different solutions to this problem are most likely applicable to different networks. Completely trusted networks obviously need not be concerned with this matter. For networks with many untrusted elements, encapsulated ISUP MIME bodies could be encrypted to alleviate this problem — although this requires the maintenance of a public key infrastructure, it affords significant protection without any additional element costs. Alternatively, encapsulated ISUP could also be deleted by some entity within the originating network (an Application Server, for example) before any SIP messages are transmitted to untrusted elements or networks; however, this requires some foresight into the destination of signaling traffic. It would also help if networks that have untrusted SIP elements homed to them managed the registration of these end-points and enforced trust relationships and policy with users. (See Note 9.)

7. Future Work

There are many issues associated with SIP-T that need resolution. Some of these have been identified and are presented below. This is in no way an exhaustive list. Additions to this list are anticipated as study progresses in the SIP-T space.

7.1 Network inter-connection architecture:

The SIP-T mechanism may be used between peer networks. The structure of inter-connection of the peers (use of a NAP architecture, etc.) may affect the manner in which an edge-proxy selects the next-hop network, and consequently, the routing process.

7.2 Application architecture:

A SIP-T message is a SIP message produced as a result of ISUP encapsulation and translation via a PSTN-originated call. Not only does it enclose ISUP within its body, but it also has some of its header fields populated with information that has been translated from the ISUP message. When a call invokes a number translating application in an AS (Application Server) the application would normally only modify the fields in the SIP-T header to reflect a change in the call-destination. This could result in a SIP-T message in which the information in the header does not agree with the encapsulated ISUP and this is a violation. A possible solution
is to have the application alter the encapsulated ISUP (or even delete it in case of termination to a SIP-phone) in addition to amending the SIP-T header.

8. List of notes:

1. A call that originates in the IP domain (IP origination) and terminates in the PSTN (PSTN termination) needs special consideration and is explored in detail in a subsequent section of this document.

2. The IP network depicted here is representative of an interconnected mesh of SIP-enabled networks. Call hand-off procedures between any two networks that are inter-connected are subject to the terms and conditions of the contractual agreements between them.

3. This document only details the functions of the different entities in the SIP-T signaling path. The specifics of the translation from ISUP to SIP and vice versa are to be addressed in the forthcoming ISUP parameter-SIP header mapping and other associated documents. See the SIP-T Components section for details.

4. Some terminating MGCs may alter the encapsulated ISUP (or might even delete it if necessary (see Note 7 below)) in order to remove any conditions specific to the originating circuit; for example, continuity test flags in the Nature of Connection Indicators, etc.

5. Routable elements are to be addressed in depth in the forthcoming ISUP parameter-SIP header draft.

6. It is not the intention of this document to lay down rules for inter-network call hand-off. This document attempts only to assess the relative merits and demerits of a routing policy based on each choice.

7. Even so, the relevance of ANSI-specific information in an ETSI network (or vice versa) is questionable. Clearly, the strength of SIP-T is realized when the encapsulated ISUP involves the usage of proprietary parameters.

8. An Application Server (AS) is an entity that hosts applications that offer calls enhanced services. An AS receives SIP signaling from the network and invokes applications that produce certain application-layer responses to the signaling, before transferring the call back to the network.

9. These and other security-related issues will be explored in a draft (forthcoming) dealing with security in networks that employ SIP-T.
9. Revision history

9.1 Changes from the 00 version: 1. Addition of a section on SIP content negotiation. 2. Several editorial changes.

9.2 Changes from the 01 version: 1. Changes in the security section (encryption, presentation restriction, etc.). 2. Several editorial changes.

10. References:


11. Acknowledgements:

We thank Andrew Dugan, Rob Maidhof, Dave Martin, Adam Roach, Jonathan Rosenberg and Dean Willis for their valuable comments.

12. Authors’ addresses

Aparna Vemuri
Jon Peterson
1025 Eldorado Blvd,
Broomfield,
CO 80021.
Aparna.Vemuri@level3.com
Jon.Peterson@level3.com

Full Copyright Statement

Copyright (c) The Internet Society (2000). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for
copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.