Internet Engineering Task Force
Internet Draft
draft-ietf-sip-isup-mime-09.txt
Jan 2001
Expires: Jul 2001

Eric Zimmerer
LongBoard
Jon Peterson, Aparna Vemuri
Level 3 Communications
Lyndon Ong
Ciena Networks
F. Audet, M. Watson, M. Zonoun
Nortel Networks

MIME media types for ISUP and QSIG Objects

Status of this Memo

Abstract

This document describes MIME types for application/ISUP and application/QSIG objects for use in SIP applications, according to the rules defined in RFC 2048 [1]. These types can be used to identify ISUP and QSIG objects within a SIP message such as INVITE or INFO, as might be implemented when using SIP between legacy systems.

1. Introduction

ISUP (ISDN User part) defined in the ITU-T recommendations Q.761-4 is a signaling protocol used between telephony switches. There exists a need to transport ISUP-encoded signaling information between SIP entities as part of the payload of SIP [2] messages, in order to access ISUP-based legacy service logic. For example, this may be implemented when using SIP to control sessions between two systems

that support legacy telephony services or gateway between legacy systems.

QSIG is the analogous signaling protocol used between private branch exchanges to support calls within private telephony networks. There is a similar need to transport QSIG-encoded signaling information between SIP entities to support legacy services or gateway between legacy systems.

The following discussion is specific to this usage and would not apply to the transportation of ISUP or QSIG messages in other applications. These media types are intended for ISUP or QSIG application information that is used within the context of a SIP session, and not as general purpose transport of SCN signaling.

The definition of media types for ISUP and QSIG application information does not address fully how the entities exchanging messages determine or negotiate compatibility. It is assumed that this is addressed by alternative means such as configuration or routing protocols.

This is intended to be an IETF approved MIME type, and to be defined through an RFC. NOTE: usage of Q.SIG within SIP is neither endorsed nor recommended as a result of this MIME registration.

3. Proposed new media types

ISUP and QSIG messages are composed of arbitrary binary data that is transparent to SIP processing. The best way to encode these is to use binary encoding. This is in conformance with the restrictions imposed on the use of binary data for MIME (RFC 2045 [3]). It should be noted that the rules mentioned in the RFC 2045 apply to Internet mail messages and not to SIP messages. Binary has been preferred over Base64 encoding because the latter would only result in adding bulk to the encoded messages and possibly be more costly in terms of processing power.

3.1 ISUP Media Type

This media type is defined by the following information:

Media type name: application
Media subtype name: ISUP

Required parameters: version
Optional parameters: base
Encoding scheme: binary
Security considerations: See section 5.

The ISUP message is encapsulated beginning with the Message Type Code (i.e., omitting Routing Label and Circuit ID Code).

The use of the 'version' parameter allows network administrators to identify specific versions of ISUP that will be exchanged on a bilateral basis. This enables a particular client such as a SoftSwitch/Media Gateway Controller to recognize and parse the message correctly, or (possibly) to reject the message if the specified ISUP version is not supported. This specification places no constraints on the values that may be used in 'version'; these are left to the discretion of the network administrator.

specific implementation of ISUP, e.g., X-NetxProprietaryISUPv3, or to identify a well-known standard version of ISUP, e.g., itu-t or ansi.

A 'base' parameter can optionally be included in some cases (e.g., if the receiver may not recognize the 'version' string) to specify that the encapsulated ISUP can also be processed using the identified 'base' specification. Table 1 provides a list of 'base' values supported by the 'application/ISUP' media type, including whether or not the forward compatibility mechanism defined in ITU-T 1992 ISUP is supported.

Table 1: ISUP 'base' values

base	protocol	compatibility
itu-t88	ITU-T Q.761-4 (1988)	no
itu-t92+	ITU-T Q.761-4 (1992)	yes
ansi88	ANSI T1.113-1988	no
ansi00	ANSI T1.113-2000	yes
etsi121	ETS 300 121	no
etsi356	ES 300 356	yes
gr317	BELLCORE GR-317	no
ttc87	JT-Q761-4(1987-1992)	no
ttc93+	JT-Q761-4(1993-)	yes

The Content-Disposition header [5] may be included to describe how the encapsulated ISUP is to be processed, and in particular what the handling should be if the received Content-Type is not recognized. The default disposition-type for an ISUP message body is "signal". This type indicates that the body part contains signaling information associated with the session, but does not describe the session.

The following is how a typical header would look ('base' may be omitted):

```
Content-Type: application/ISUP; version=nxv3; base=etsi121
```



```
Content-Disposition: signal; handling=optional
```

3.2 QSIG Media Type

The application/QSIG media type is defined by the following information:

Media type name: application
Media subtype name: QSIG
Required parameters: none
Optional parameters: version
Encoding scheme: binary
Security considerations: See section 5.

The use of the 'version' parameter allows identification of different QSIG variants. This enables the terminating Connection Server to recognize and parse the message correctly, or (possibly) to reject the message if the particular QSIG variant is not supported.

Table 2 is a list of protocol versions supported by the 'application/QSIG' media type.

Table 2: QSIG versions

version	protocol
iso	ISO/IEC 11572 (Basic Call) and ISO/IEC 11582 (Generic Functional Protocol)

The following is how a typical header would look (Content-Disposition not included in this instance):

```
  Content-Type: application/QSIG; version=iso
```

The default disposition-type is "signal" as in an ISUP body part.

4. Illustrative examples

4.1 ISUP

SIP message format requires a Request line followed by Header lines followed by a CRLF separator followed by the message body. To illustrate the use of the 'application/ISUP' media type, below is an INVITE message which has the originating SDP information and an encapsulated ISUP IAM.

Note that the two payloads are demarcated by the boundary parameter (specified in RFC 2046 [4]) which in the example has the value

"unique-boundary-1". This is part of the specification of MIME multipart and is not related to the

```
INVITE sip:13039263142@Den1.level3.com SIP/2.0
Via: SIP/2.0/UDP den3.level3.com
From: sip:13034513355@den3.level3.com
To: sip:13039263142@Den1.level3.com
Call-ID: DEN123199902171209550099@Den1.level3.com
CSeq: 8348 INVITE
Contact: <sip:jpeterson@level3.com>
Content-Length: 436
Content-Type: multipart/mixed; boundary=unique-boundary-1
MIME-Version: 1.0

--unique-boundary-1
Content-Type: application/SDP; charset=ISO-10646

v=0
o=jpeterson 2890844526 2890842807 IN IP4 126.16.64.4
s=SDP seminar
c=IN IP4 MG122.level3.com
t= 2873397496  2873404696
```

```
m=audio 9092 RTP/AVP 0 3 4
--unique-boundary-1
Content-Type: application/ISUP; version=nxv3;
base=etsi121
Content-Disposition: signal; handling=optional

01 00 49 00 00 03 02 00 07 04 10 00 33 63 21
43 00 00 03 06 0d 03 80 90 a2 07 03 10 03 63
53 00 10 0a 07 03 10 27 80 88 03 00 00 89 8b
0e 95 1e 1e 1e 06 26 05 0d f5 01 06 10 04 00
--unique-boundary-1--
```

Note: Since binary encoding is used for the ISUP payload, each byte is encoded as a byte, and not as a two-character hex representation. Hex digits were used in the draft because a literal encoding of those bytes would have been confusing and unreadable.

4.2 QSIG

To illustrate the use of the 'application/QSIG' media type, below is an INVITE message which has the originating SDP information and an encapsulated QSIG SETUP message.

Note that the two payloads are demarcated by the boundary parameter (specified in RFC 2046 [4]) which in the example has the value "unique- boundary-1". This is part of the specification of MIME

multipart and is not related to the 'application/QSIG' media type.

```
INVITE sip:14084955072@sc1.nortelnetworks.com SIP/2.0
Via: SIP/2.0/UDP sc10.nortelnetworks.com
From: sip:14085655675@sc10.nortelnetworks.com
To: sip:14084955072@sc1.nortelnetworks.com
Call-ID: 12319990217120955009990sc12.nortelnetworks.com
CSeq: 1234 INVITE
Contact: <sip:14085655675@sc10.nortelnetworks.com>
Content-Length: 358
Content-Type: multipart/mixed; boundary=unique-boundary-1
MIME-Version: 1.0

--unique-boundary-1
Content-Type: application/SDP; charset=ISO-10646
```

```
v=0
o=audet 2890844526 2890842807 5 IN IP4 134.177.64.4
s=SDP seminar
c=IN IP4 MG141.nortelnetworks.com
t= 2873397496 2873404696
m=audio 9092 RTP/AVP 0 3 4

--unique-boundary-1
Content-type:application/QSIG; version=iso

08 02 55 55 05 04 02 90 90 18 03 a1 83 01
70 0a 89 31 34 30 38 34 39 35 35 30 37 32
--unique-boundary-1--
```

5. Security considerations

Information contained in ISUP and QSIG bodies may include sensitive customer information, potentially requiring use of encryption. Security mechanisms are provided in RFC 2543 (SIP - Session Initiation Protocol) and should be used as appropriate for both the SIP message and the encapsulated ISUP or QSIG body.

6. IANA considerations

Registrations for the 'version' symbols used within the ISUP and QSIG MIME types must specify a definitive specification reference, identifying a particular issue of the specification, to which the new symbol shall refer. Identifying a definite specification reference requires a review process; the authors recommend that a subject matter expert be designated as described in RFC 2434 [6] under Expert Review.

Note that where a specification is fully peer-to-peer backwards compatible with a previous issue (i.e., the compatibility mechanism is supported by both), then there is no need for separate symbols to be registered. The symbol for the original specification should be used to identify backwards-compatible upgrades of that specification as well.

Symbols beginning with the characters 'X-' are reserved for non-

standard usage (e.g., cases in which a token other than a string representing an issue of an ISUP specification is appropriate for characterizing ISUP within an administrative domain). Such non-standard version can only be transmitted between administrative domains in accordance with a bilateral agreement. These symbols should be administered under the Private Use policy described in RFC 2434.

7. Authors

Eric Zimmerer
LongBoard, Inc.
3103 North First St. #200
San Jose, CA 95133, USA
EZimmerer@lboard.com

M. Zonoun, F. Audet
Nortel Networks
Santa Clara, CA 95054
mzonoun@nortelnetworks.com

Aparna Vemuri
Jon Peterson
Level 3 Communications
Broomfield, CO, USA
aparna.vemuri@level3.com
jon.peterson@level3.com

M. Watson
Nortel Networks
Maidenhead, UK
mwatson@nortelnetworks.com

Lyndon Ong
Point Reyes Networks
San Jose, CA, USA
lyndon_ong@yahoo.com

8. References

[1] Freed, Klensin, Postel, "Multipart Internet Mail Extensions (MIME) Part Four: Registration Procedures" RFC 2048, Internet Engineering Task Force, November 1996.

[2] Handley, Schulzrinne, Schooler and Rosenberg, "Session Initiation Protocol (SIP)" RFC 2543, Internet Engineering Task Force, March 1999.

[3] Freed, Borenstein, "Multipart Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies" RFC 2045, Internet

Engineering Task Force, November 1996.

[4] Freed, Borenstein, "Multipart Internet Mail Extensions (MIME) Part Two: Media Types" RFC 2046, Internet Engineering Task Force, November 1996.

[5] Troost, Dorner, Moore, "Communicating Presentation Information in Internet Messages: The Content-Disposition Header Field", RFC 2183, Internet Engineering Task Force, August 1997.

[6] Narten, Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", RFC2434, BCP26, Internet Engineering Task Force, October 1998.