SIPPING Working Group
Internet Draft
Document: draft-ietf-sipping-torture-tests-00.txt
Expires: February 2003

A. Johnston
WorldCom
J. Rosenberg
dynamicsoft
H. Schulzrinne
Columbia U.

August 2002

Session Initiation Protocol Torture Test Messages

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

This informational document gives examples of Session Initiation Protocol (SIP) test messages designed to exercise and "torture" a parser. They were developed as part of the SIPit SIP interoperability testing events.

Conventions used in this document

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 [1].

Table of Contents

1. Overview.....3

2. SIP Test Messages....3
2.1 INVITE Parser Torture Test Message....3
2.2 INVITE with Proxy-Require and Require....4
2.3 INVITE with Unknown Schemes in URIs....5
2.4 REGISTER with Y2038 Test....5
2.5 INVITE with inconsistent Accept and message body....6
2.6 INVITE with non-SDP message body....6
2.7 Unknown Method Message....7
2.8 Unknown Method with CSeq Error....7
2.9 REGISTER with Unknown Authorization Scheme....8
2.10 Multiple SIP Request in a Single Message....8
2.11 INVITE missing Required Headers....9
2.12 INVITE with Duplicate Required Headers....10
2.13 INVITE with Illegal Expires Header....10
2.14 200 OK Response with Broadcast Via Header....11
2.15 INVITE with Invalid Via and Contact Headers....12
2.16 INVITE with Incorrect Content-Length Header....12
2.17 INVITE with Invalid Value for Content-Length....13
2.18 INVITE with Garbage after Message Body....14
2.19 INVITE with Error in Display Name in To Header....14
2.20 INVITE with a Semicolon-Separated Parameter in the "user" Part....15
2.21 INVITE with Illegal Enclosing of Request-URI in "<>"....15
2.22 INVITE with Illegal LWS within Elements of Request-URI...16
2.23 INVITE with illegal >1 SP between elements of Request URI17
2.24 INVITE with a legal SIP URI containing escaped characters17
2.25 INVITE with the illegal use of escaped headers in Request-URI 18
2.26 INVITE containing an unknown scheme in the Request URI...19
2.27 OPTIONS with no LWS between display name and <....19
2.28 OPTIONS with extran LWS between display name and <....20
2.29 INVITE with an illegal SIP Date format....20
2.30 INVITE with Passed Expries Time....21
2.31 INVITE with Max-Forwards Set to Zero....21
2.32 REGISTER with a Escaped Header in a Legal SIP URI of a Contact....22
2.33 REGISTER with a Escaped Header in a Illegal SIP URI of a Contact....22
2.34 INVITE with Long Values in Headers....23
2.35 OPTIONS with multiple headers....24
2.36 INVITE with large number of SDP attributes and telephone subscriber Request-URI....25
2.37 REGISTER with a contact parameter....26
2.38 REGISTER with a url parameter....26
2.39 INVITE with an Unquoted Display Name Containing Multiple Tokens....26
2.40 INVITE with an Unquoted Display Name Containg Non-Token Characters....27

2.41 INVITE with Unknown (Higher) Protocol Version in Start Line27

2.42 INVITE with RFC2543 syntax.....28
Security Considerations.....28
References.....28
Acknowledgments.....29
Author's Addresses.....29

1. Overview

These SIP test messages are based on the current version 2.0 of SIP in RFC 3261[2] with SDP usage described in RFC 3264[3].

Note that this document is informational, and is NOT NORMATIVE on any aspect of SIP syntax.

2. SIP Test Messages

The files in here are test messages for SIP servers to exercise various functions. They have been used in SIPit interoperability events. All messages shown here are valid, unless otherwise noted. The correct behavior of servers and clients is also described.

2.1 INVITE Parser Torture Test Message

This message is a correctly formatted SIP message. It contains:

line folding all over
escaped characters within quotes
LWS between colons, semicolons, headers, and other fields
both comma separated and separate listing of headers
mix or short and long form for the same header
unknown header field
unusual header ordering
unknown parameters of a known header

Proxies should forward message and clients should respond as to a normal INVITE message.

Message Details

```
INVITE sip:vivekg@chair.dnrc.bell-labs.com SIP/2.0
TO :
 sip:vivekg@chair.dnrc.bell-labs.com ;   tag    = 1918181833n
From   : "J Rosenberg \\\"" <sip:jdrosen@lucent.com>
  ;
  tag = 98asjd8
Max-Forwards: 6
Call-ID: 0ha0isndaksdj@10.1.1.1
```

```
cseq: 8
  INVITE
Via  : SIP  /   2.0
 /UDP
    135.180.130.133;branch=z9hG4bKkdjuw
Subject :
NewFangledHeader:   newfangled value
 more newfangled value
Content-Type: application/sdp
v:  SIP  / 2.0  / TCP     1192.168.156.222   ;
  branch  =   9ikj8  ,
 SIP  /    2.0   / UDP  192.168.255.111   ; hidden
m:"Quoted string \"\"" <sip:jdrosen@bell-labs.com> ; newparam =
newvalue ;
  secondparam = secondvalue  ; q = 0.33,
 tel:4443322

v=0
o=mhandley 29739 7272939 IN IP4 126.5.4.3
s=-
c=IN IP4 135.180.130.88
t=0 0
m=audio 492170 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

2.2 INVITE with Proxy-Require and Require

This message tests support for Proxy-Require and Require. It is a request that contains both headers, listing new features.

Proxies and clients should respond with a 420 Bad Extension, and an Unsupported header listing these features.

Message Details

```
INVITE sip:user@company.com SIP/2.0
To: sip:j_user@company.com
From: sip:caller@university.edu;tag=242etr
Max-Forward: 6
Call-ID: 0ha0isndaksdj@10.1.1.1
Require: newfeature1, newfeature2
Proxy-Require: newfeature3, newfeature4
CSeq: 8 INVITE
Via: SIP/2.0/UDP 135.180.130.133;branch=z9hG4bKkdjuw
```

2.3 INVITE with Unknown Schemes in URIs

This message contains unknown schemes in the Request URI, To, From and Contact headers of a request.

A server should probably return a not found error; but other behaviors are acceptable.

Message Details

```
INVITE name:John_Smith SIP/2.0
To: isbn:2983792873
From: <http://www.cs.columbia.edu>;tag=3234233
Call-ID: 0ha0isndaksdj@10.1.2.3
CSeq: 8 INVITE
Max-Forward: 7
Via: SIP/2.0/UDP 135.180.130.133:5060;branch=z9hG4bKkdjuw
Content-Type: application/sdp

v=0
o=mhandley 29739 7272939 IN IP4 126.5.4.3
s=-
c=IN IP4 135.180.130.88
t=0 0
m=audio 492170 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

2.4 REGISTER with Y2038 Test

This message is a registration request with an expiration year of 2040. This makes sure that a server doesn't crash on seeing a date past Y2038.

The correct behavior is probably to limit the lifetime to some configured maximum.

Message Details

```
REGISTER sip:company.com SIP/2.0
To: sip:user@company.com
From: sip:user@company.com;tag=3411345
Max-Forwards: 8
Contact: sip:user@host.company.com
Call-ID: 0ha0isndaksdj@10.0.0.1
```

```
CSeq: 8 REGISTER
Via: SIP/2.0/UDP 135.180.130.133;branch=z9hG4bKkdjuw
Expires: Sat, 01 Dec 2040 16:00:00 GMT
```

2.5 INVITE with inconsistent Accept and message body

This is a UAS test. It is a request that includes an Accept header without SDP. The UAS should respond with an error.

Message Details

```
INVITE sip:user@company.com SIP/2.0
To: sip:j_user@company.com
From: sip:caller@university.edu;tag=234
Max-Forwards: 5
Call-ID: 0ha0isndaksdj@10.0.0.1
Accept: text/newformat
CSeq: 8 INVITE
Via: SIP/2.0/UDP 135.180.130.133;branch=z9hG4bKkdjuw
Content-Type: application/sdp

v=0
c=IN IP4 135.180.130.88
m=audio 492170 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

2.6 INVITE with non-SDP message body

This is a test of a user agent server. It is a request that includes a body of a non-SDP type.

The user agent server should respond with an error.

Message Details

```
INVITE sip:user@comapny.com SIP/2.0
To: sip:j.user@company.com
From: sip:caller@university.edu;tag=8
Max-Forwards: 70
Call-ID: 0ha0isndaksdj@10.0.0.1
CSeq: 8 INVITE
Via: SIP/2.0/UDP 135.180.130.133;branch=z9hG4bKkdjuw
Content-Type: application/newformat
```

```
<audio>
 <pcmu port="443"/>
</audio>
```

2.7 Unknown Method Message

This request message contains a new unknown method, NEWMETHOD.

A proxy should forward this using the same retransmission rules as BYE. A UAS should reject it with an error, and list the available methods in the response.

Message Details

```
NEWMETHOD sip:user@comapny.com SIP/2.0
To: sip:j.user@company.com
From: sip:caller@university.edu;tag=34525
Max-Forwards: 6
Call-ID: 0ha0isndaksdj@10.0.0.1
CSeq: 8 NEWMETHOD
Via: SIP/2.0/UDP 135.180.130.133;branch=z9hG4bKkdjuw
Content-Type: application/sdp

v=0
o=mhandley 29739 7272939 IN IP4 126.5.4.3
c=IN IP4 135.180.130.88
m=audio 492170 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

2.8 Unknown Method with CSeq Error

This message is nearly identical to the Unknown Method message. It is a request with a new unknown method, but with a CSeq method tag which does not match.

A proxy should either respond with an error, or correct the method tag. The user agent should reject it with an error, and list the available methods in the response.

Message Details

```
NEWMETHOD sip:user@comapny.com SIP/2.0
To: sip:j.user@company.com
From: sip:caller@university.edu;tag=23411413
Max-Forwards: 3
Call-ID: 0ha0isndaksdj@10.0.1.1
CSeq: 8 INVITE
Via: SIP/2.0/UDP 135.180.130.133;branch=z9hG4bKkdjuw
Content-Type: application/sdp

v=0
o=mhandley 29739 7272939 IN IP4 126.5.4.3
s=-
c=IN IP4 135.180.130.88
t=0 0
m=audio 492170 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

2.9 REGISTER with Unknown Authorization Scheme

This message is a REGISTER request with an unknown authorization scheme.

The server should do something reasonable, such as rejecting the request.

Message Details

```
REGISTER sip:company.com SIP/2.0
To: sip:j.user@company.com
From: sip:j.user@company.com;tag=87321hj23128
Max-Forwards: 8
Call-ID: 0ha0isndaksdj@10.0.1.1
CSeq: 8 REGISTER
Via: SIP/2.0/UDP 135.180.130.133;branch=z9hG4bKkdjuw
Authorization: Super-PGP ajsohdaosdh0asyhdaind08yasdknasd09asidhas0d8
```

2.10 Multiple SIP Request in a Single Message

This message contains two requests, separated by a bunch of whitespace. Since the message exceeds the length indicated in the Content-Length header, the message should be rejected. (Multiple SIP requests per UDP packet are no longer allowed.)

Message Details

```
REGISTER sip:company.com SIP/2.0
To: sip:j.user@company.com
From: sip:j.user@company.com;tag=43251j3j324
Max-Forwards: 8
Call-ID: 0ha0isndaksdj@10.0.2.2
Contact: sip:j.user@host.company.com
CSeq: 8 REGISTER
Via: SIP/2.0/UDP 135.180.130.133;branch=z9hG4bKkdjuw
Content-Length: 0
```

```
INVITE sip:joe@company.com SIP/2.0
To: sip:joe@company.com
From: sip:caller@university.edu;tag=141334
Max-Forwards: 8
Call-ID: 0ha0isnda977644900765@10.0.0.1
CSeq: 8 INVITE
Via: SIP/2.0/UDP 135.180.130.133;branch=z9hG4bKkdjuw
Content-Type: application/sdp

v=0
o=mhandley 29739 7272939 IN IP4 126.5.4.3
s=-
c=IN IP4 135.180.130.88
t=0 0
m=audio 492170 RTP/AVP 0 12
m =video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

2.11 INVITE missing Required Headers

This message contains no Call-ID, From, or To header.

The server should not crash, and ideally should respond with an error.

Message Details

```
INVITE sip:user@company.com SIP/2.0
CSeq: 0 INVITE
Via: SIP/2.0/UDP 135.180.130.133;branch=z9hG4bKkdjuw
```

```
Content-Type: application/sdp

v=0
o=mhandley 29739 7272939 IN IP4 126.5.4.3
s=-
c=IN IP4 135.180.130.88
t=0 0
m=audio 492170 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

2.12 INVITE with Duplicate Required Headers

The message contains a request with an extra Call-ID and To field.

The server should not crash, and should ideally respond with an error.

Message Details

```
INVITE sip:user@company.com SIP/2.0
Via: SIP/2.0/UDP 135.180.130.133;branch=z9hG4bKkdjuw
Max-Forwards: 70
CSeq: 0 INVITE
Call-ID: 98asdh@10.1.1.1
Call-ID: 98asdh@10.1.1.2
From: sip:caller@university.edu;tag=3413415
From: sip:caller@organization.org
To: sip:user@company.com
Content-Type: application/sdp

v=0
o=mhandley 29739 7272939 IN IP4 126.5.4.3
s=-
c=IN IP4 135.180.130.88
t=0 0
m=audio 492170 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

2.13 INVITE with Illegal Expires Header

This message contains an Expires header which has illegal values for a number of components, but otherwise is syntactically correct.

Message Details

```
INVITE sip:user@company.com SIP/2.0
Via: SIP/2.0/UDP 135.180.130.133;branch=z9hG4bKkdjuw
Max-Forwards: 88
CSeq: 0 INVITE
Call-ID: 98asdh@10.1.1.2
Expires: Thu, 44 Dec 19999 16:00:00 EDT
From: sip:caller@university.edu;tag=3651
To: sip:user@company.com
Content-Type: application/sdp

v=0
o=mhandley 29739 7272939 IN IP4 126.5.4.3
s=-
c=IN IP4 135.180.130.88
t=0 0
m=audio 492170 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

2.14 200 OK Response with Broadcast Via Header

This message is a response with a 2nd Via header of 255.255.255.255.

On receiving this response, the top Via header is stripped and the packet forwarded. Since the next address is the broadcast address, it causes the packet to be broadcast onto the network. A smart server should ignore packets with 2nd Via headers that are 255.255.255.255 or 127.0.0.1. At the very least it should not crash.

Message Details

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 135.180.130.57;branch=0
Via: SIP/2.0/UDP 255.255.255.255;branch=0
Max-Forwards: 70
Call-ID: 0384840201@10.1.1.1
CSeq: 0 INVITE
From: sip:user@company.com;tag=11141343
To: sip:user@university.edu;tag=2229
Content-Type: application/sdp

v=0
```

```
o=mhandley 29739 7272939 IN IP4 126.5.4.3
s=-
c=IN IP4 224.2.17.12/127
t=0 0
m=audio 492170 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

2.15 INVITE with Invalid Via and Contact Headers

This is a request with the Via and Contact headers incorrect. They contain additional semicolons and commas without parameters or values.

The server should respond with a Bad Request error.

Message Details

```
INVITE sip:user@company.com SIP/2.0
To: sip:j.user@company.com
From: sip:caller@university.edu;tag=134161461246
Max-Forwards: 7
Call-ID: 0ha0isndaksdj@10.0.0.1
CSeq: 8 INVITE
Via: SIP/2.0/UDP 135.180.130.133;;,;
Contact: "" <> ;,"Joe" <sip:joe@org.org>;;,,;;
Content-Type: application/sdp

v=0
o=mhandley 29739 7272939 IN IP4 126.5.4.3
s=-
c=IN IP4 135.180.130.88
t=0 0
m=audio 492170 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

2.16 INVITE with Incorrect Content-Length Header

This is a request message with a Content Length that is much larger than the length of the body.

When sent UDP, the server should respond with an error. With TCP, there's not much you can do but wait...

Message Details

```
INVITE sip:user@company.com SIP/2.0
Max-Forwards: 80
To: sip:j.user@company.com
From: sip:caller@university.edu;tag=93942939o2
Call-ID: 0ha0isndaksdj@10.0.0.1
CSeq: 8 INVITE
Via: SIP/2.0/UDP 135.180.130.133
Content-Type: application/sdp
Content-Length: 9999

v=0
o=mhandley 29739 7272939 IN IP4 126.5.4.3
s=-
c=IN IP4 135.180.130.88
t=0 0
m=audio 492170 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

2.17 INVITE with Invalid Value for Content-Length

This is a request message with a negative value for Content-Length.

The server should respond with an error.

Message Details

```
INVITE sip:user@company.com SIP/2.0
Max-Forwards: 254
To: sip:j.user@company.com
From: sip:caller@university.edu;tag=3
Call-ID: 0ha0isndaksdj@10.0.0.1
CSeq: 8 INVITE
Via: SIP/2.0/UDP 135.180.130.133;branch=z9hG4bKkdjuw
Content-Type: application/sdp
Content-Length: -999

v=0
o=mhandley 29739 7272939 IN IP4 126.5.4.3
s=-
c=IN IP4 135.180.130.88
t=0 0
```

```
m=audio 492170 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

2.18 INVITE with Garbage after Message Body

This is a request message with garbage after the end of the SDP included in the body.

The servers should reject the request as the body is longer than the Content-Length.

Message Details

```
INVITE sip:user@company.com SIP/2.0
To: sip:j.user@company.com
From: sip:caller@university.edu;tag=3223
Max-Forwards: 7
Call-ID: 0ha0isndaksdj@10.0.0.1
CSeq: 8 INVITE
Via: SIP/2.0/UDP 135.180.130.133
Content-Type: application/sdp
Content-Length: 138

v=0
o=mhandley 29739 7272939 IN IP4 126.5.4.3
s=-
c=IN IP4 135.180.130.88
t=0 0
m=audio 492170 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
asdpasd08asdsdk:;;asd
 a0sdjhg8a0''...'';;;;
```

2.19 INVITE with Error in Display Name in To Header

This is a request with an unterminated quote in the display name of the To field.

The server can either return an error, or proxy it if it is successful parsing without the terminating quote.

Message Details

```
INVITE sip:user@company.com SIP/2.0
To: "Mr. J. User <sip:j.user@company.com>
From: sip:caller@university.edu;tag=93334
Max-Forwards: 10
Call-ID: 0ha0isndaksdj@10.0.0.1
CSeq: 8 INVITE
Via: SIP/2.0/UDP 135.180.130.133:5050;branch=z9hG4bKkdjuw
Content-Type: application/sdp
Content-Length: 138

v=0
o=mhandley 29739 7272939 IN IP4 126.5.4.3
s=-
c=IN IP4 135.180.130.88
t=0 0
m=audio 492170 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

2.20 INVITE with a Semicolon-Separated Parameter in the "user" Part

This is an INVITE request with a semicolon-separated parameter in the "user" part.

Outbound proxies should direct it appropriately.

Message Details

```
INVITE sip:user;par=u%40h.com@company.com SIP/2.0
To: sip:j_user@company.com
From: sip:caller@university.edu;tag=33242
Max-Forwards: 3
Call-ID: 0ha0isndaksdj@10.1.1.1
CSeq: 8 INVITE
Via: SIP/2.0/UDP 135.180.130.133;branch=z9hG4bKkdjuw
```

2.21 INVITE with Illegal Enclosing of Request-URI in "<>"

This INVITE is illegal because the Request-URI has been enclosed within in "<>".

An intelligent server may be able to deal with this and fix up athe Request-URI if acting as a Proxy. If not it should respond 400 with an appropriate reason phrase.

Message Details

```
INVITE <sip:user@company.com> SIP/2.0
To: sip:user@company.com
From: sip:caller@university.edu;tag=39291
Max-Forwards: 23
Call-ID: 1@10.0.0.1
CSeq: 1 INVITE
Via: SIP/2.0/UDP 135.180.130.133
Content-Type: application/sdp
Content-Length: 174

v=0
o=mhandley 29739 7272939 IN IP4 126.5.4.3
s=-
c=IN IP4 135.180.130.88
t=3149328700 0
m=audio 492170 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

2.22 INVITE with Illegal LWS within Elements of Request-URI

This INVITE has illegal LWS within the SIP URI.

An intelligent server may be able to deal with this and fix up the Request-URI if acting as a Proxy. If not it should respond 400 with an appropriate reason phrase.

Message Details

```
INVITE sip:user@company.com; transport=udp SIP/2.0
To: sip:user@company.com
From: sip:caller@university.edu;tag=231413434
Max-Forwards: 5
Call-ID: 2@10.0.0.1
CSeq: 1 INVITE
Via: SIP/2.0/UDP 135.180.130.133:5060;branch=z9hG4bKkdjuw
Content-Type: application/sdp
Content-Length: 174
```

```
v=0
o=mhandley 29739 7272939 IN IP4 126.5.4.3
s=-
c=IN IP4 135.180.130.88
t=3149328700 0
m=audio 492170 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

2.23 INVITE with illegal >1 SP between elements of Request URI

This INVITE has illegal >1 SP between elements of the Request-URI.

An intelligent server may be able to deal with this and fix up the Request-URI if acting as a Proxy. If not it should respond 400 with an appropriate reason phrase.

Message Details

```
INVITE sip:user@company.com  SIP/2.0
Max-Forwards: 8
To: sip:user@company.com
From: sip:caller@university.edu;tag=8814
Call-ID: 3@10.0.0.1
CSeq: 1 INVITE
Via: SIP/2.0/UDP 135.180.130.133:5060;branch=z9hG4bKkdjuw
Content-Type: application/sdp
Content-Length: 174

v=0
o=mhandley 29739 7272939 IN IP4 126.5.4.3
s=-
c=IN IP4 135.180.130.88
t=0 0
m=audio 492170 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

2.24 INVITE with a legal SIP URI containing escaped characters

This INVITE is legal and has a Request-URI with a SIP URI containing escaped characters.

Message Details

```
INVITE sip:sip%3Auser%40example.com@company.com;other-param=summit
SIP/2.0
To: sip:user@company.com
From: sip:caller@university.edu;tag=938
Max-Forwards: 87
Call-ID: 4@10.0.0.1
CSeq: 1 INVITE
Via: SIP/2.0/UDP 135.180.130.133:5060;branch=z9hG4bKkdjuw
Content-Type: application/sdp
Content-Length: 174

v=0
o=mhandley 29739 7272939 IN IP4 126.5.4.3
s=-
c=IN IP4 135.180.130.88
t=0 0
m=audio 492170 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

2.25 INVITE with the illegal use of escaped headers in Request-URI

This INVITE is illegal as it the Request-URI contains a SIP URI containing
escaped headers.

An intelligent server may be liberal enough to accept this. A server acting as a proxy should remove the escaped header before processing.

Message Details

```
INVITE sip:user@company.com?Route=%3Csip:sip.example.com%3E SIP/2.0
To: sip:user@company.com
From: sip:caller@university.edu;tag=341518
Max-Forwards: 7
Call-ID: 5@10.0.0.1
CSeq: 1 INVITE
Via: SIP/2.0/UDP 135.180.130.133:5060;branch=z9hG4bKkdjuw
Content-Type: application/sdp
Content-Length: 174

v=0
o=mhandley 29739 7272939 IN IP4 126.5.4.3
s=-
```

```
c=IN IP4 135.180.130.88
t=0 0
m=audio 492170 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

2.26 INVITE containing an unknown scheme in the Request URI

This INVITE contains an unknown URI scheme in the Request-URI.

A server should reject this message with a 400 response plus an appropriate reason phrase despite being able to understand the To header as a SIP URI.

Message Details

```
INVITE name:user SIP/2.0
To: sip:user@company.com
From: sip:caller@university.edu;tag=384
Max-Forwards: 3
Call-ID: 6@10.0.0.1
CSeq: 1 INVITE
Via: SIP/2.0/UDP 135.180.130.133;branch=z9hG4bKkdjuw
Content-Type: application/sdp
Content-Length: 174

v=0
o=mhandley 29739 7272939 IN IP4 126.5.4.3
s=-
c=IN IP4 135.180.130.88
t=0 0
m=audio 492170 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

2.27 OPTIONS with no LWS between display name and <

This OPTIONS request is legal despite there being no LWS between the display name and < in the From header.

Message Details

```
OPTIONS sip:user@company.com SIP/2.0
```

```
To: sip:user@company.com
From: "caller"<sip:caller@example.com>;tag=323
Max-Forwards: 70
Call-ID: 1234abcd@10.0.0.1
CSeq: 1 OPTIONS
Via: SIP/2.0/UDP 135.180.130.133:5060;branch=z9hG4bKkdjuw
```

2.28 OPTIONS with extran LWS between display name and <

This OPTIONS request is legal despite there being extra LWS between the display name and < in the From header.

Message Details

```
OPTIONS sip:user@company.com SIP/2.0
To: sip:user@company.com
From: "caller"    <sip:caller@example.com>;tag=32
Max-Forwards: 70
Call-ID: 1234abcd@10.0.0.1
CSeq: 2 OPTIONS
Via: SIP/2.0/UDP 135.180.130.133:5060;branch=z9hG4bKkdjuw
```

2.29 INVITE with an illegal SIP Date format.

This INVITE is illegal as it contains a non GMT time zone in the SIP Date header.

An intelligent server may be able to fix this up and correct the time to GMT. Alternatively this message may illicit a 400 response with an appropriate reason phrase.

Message Details

```
INVITE sip:user@company.com SIP/2.0
To: sip:user@company.com
From: sip:caller@university.edu;tag=2
Max-Forwards: 70
Call-ID: 7@10.0.0.1
CSeq: 1 INVITE
Via: SIP/2.0/UDP 135.180.130.133:5060;branch=z9hG4bKkdjuw
Date: Fri, 01 Jan 2010 16:00:00 EST
Content-Type: application/sdp
Content-Length: 174
```

```
v=0
o=mhandley 29739 7272939 IN IP4 126.5.4.3
s=-
c=IN IP4 135.180.130.88
t=0 0
m=audio 492170 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

2.30 INVITE with Passed Expries Time

This is a legal INVITE but the message content has long since expired.

A server should respond 408 (Timeout).

Message Details

```
INVITE sip:user@company.com SIP/2.0
To: sip:user@company.com
From: sip:caller@university.edu;tag=3843
Max-Forwards: 70
Call-ID: 8@10.0.0.1
CSeq: 1 INVITE
Via: SIP/2.0/UDP 135.180.130.133:5060;branch=z9hG4bKkdjuw
Expires: Thu, 01 Dec 1994 16:00:00 GMT
Content-Type: application/sdp
Content-Length: 174

v=0
o=mhandley 29739 7272939 IN IP4 126.5.4.3
s=-
c=IN IP4 135.180.130.88
t=0 0
m=audio 492170 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

2.31 INVITE with Max-Forwards Set to Zero

This is a legal SIP request with the Max-Forwards header set to zero.

A proxy or gateway should not forward the request and respond 483 (Too Many Hops).

Message Details

```
INVITE sip:user@company.com SIP/2.0
To: sip:user@company.com
From: sip:caller@university.edu;tag=3ghsd41
Call-ID: 9@10.0.0.1
CSeq: 1 INVITE
Via: SIP/2.0/UDP 135.180.130.133:5060;branch=z9hG4bKkdjuw
Max-Forwards: 0
Content-Type: application/sdp
Content-Length: 174

v=0
o=mhandley 29739 7272939 IN IP4 126.5.4.3
s=-
c=IN IP4 135.180.130.88
t=0 0
m=audio 492170 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

2.32 REGISTER with a Escaped Header in a Legal SIP URI of a Contact

This is a legal REGISTER message where the Contact header contains a SIP URI with an escaped header within it.

Message Details

```
REGISTER sip:company.com SIP/2.0
To: sip:user@company.com
From: sip:user@company.com;tag=8
Max-Forwards: 70
Contact: sip:user@host.company.com
Call-ID: k345asrl3fdbv@10.0.0.1
CSeq: 1 REGISTER
Via: SIP/2.0/UDP 135.180.130.133:5060;branch=z9hG4bKkdjuw
Contact: <sip:user@example.com?Route=%3Csip:sip.example.com%3E>
```

2.33 REGISTER with a Escaped Header in a Illegal SIP URI of a Contact

This is an illegal message as the REGISTER request contains a SIP

URI with an escaped header but it is not enclosed in <>

A server should respond 400 with an appropriate reason phrase.

Message Details

```
REGISTER sip:company.com SIP/2.0
To: sip:user@company.com
From: sip:user@company.com;tag=998332
Max-Forwards: 70
Contact: sip:user@host.company.com
Call-ID: k345asrl3fdbv@10.0.0.1
CSeq: 1 REGISTER
Via: SIP/2.0/UDP 135.180.130.133:5060;branch=z9hG4bKkdjuw
Contact: sip:user@example.com?Route=%3Csip:sip.example.com%3E
```

2.34 INVITE with Long Values in Headers

This is a legal message that contains long values in many headers.

Message Details

```
INVITE sip:user@company.com SIP/2.0
To: "I have a user name of extreme proportion"
<sip:user@company.com:6000;other-
param=1234567890somethingelselong1234567890>
From: sip:caller@university.edu;tag=12481841982424
Call-ID:
kl24ahsd546folnyt2vbak9sad98u23naodiunzds09a3bqw0sdfbsk34poouymnae004
3nsed09mfkvc74bd0cuwnms05dknw87hjpobd76f
CSeq: 1 INVITE
P-My-State: sldkjflzdsfaret0803adgaasd0afds0asdaasd
Via: SIP/2.0/TCP sip33.example.com
Via: SIP/2.0/TCP sip32.example.com
Via: SIP/2.0/TCP sip31.example.com
Via: SIP/2.0/TCP sip30.example.com
Via: SIP/2.0/TCP sip29.example.com
Via: SIP/2.0/TCP sip28.example.com
Via: SIP/2.0/TCP sip27.example.com
Via: SIP/2.0/TCP sip26.example.com
Via: SIP/2.0/TCP sip25.example.com
Via: SIP/2.0/TCP sip24.example.com
Via: SIP/2.0/TCP sip23.example.com
Via: SIP/2.0/TCP sip22.example.com
Via: SIP/2.0/TCP sip21.example.com
```

```
Via: SIP/2.0/TCP sip20.example.com
Via: SIP/2.0/TCP sip19.example.com
Via: SIP/2.0/TCP sip18.example.com
Via: SIP/2.0/TCP sip17.example.com
Via: SIP/2.0/TCP sip16.example.com
Via: SIP/2.0/TCP sip15.example.com
Via: SIP/2.0/TCP sip14.example.com
Via: SIP/2.0/TCP sip13.example.com
Via: SIP/2.0/TCP sip12.example.com
Via: SIP/2.0/TCP sip11.example.com
Via: SIP/2.0/TCP sip10.example.com
Via: SIP/2.0/TCP sip9.example.com
Via: SIP/2.0/TCP sip8.example.com
Via: SIP/2.0/TCP sip7.example.com
Via: SIP/2.0/TCP sip6.example.com
Via: SIP/2.0/TCP sip5.example.com
Via: SIP/2.0/TCP sip4.example.com
Via: SIP/2.0/TCP sip3.example.com
Via: SIP/2.0/TCP sip2.example.com
Via: SIP/2.0/TCP sip1.example.com
Via: SIP/2.0/TCP
host.example.com;received=135.180.130.133;branch=C1C3344E2710000000E2
99E568E7potato10potato0potato0
Content-Type: application/sdp

v=0
o=mhandley 29739 7272939 IN IP4 126.5.4.3
s=-
c=IN IP4 135.180.130.88
t=0 0
m=audio 492170 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

2.35 OPTIONS with multiple headers.

This is an illegal and badly mangled message.

A server should respond 400 with an appropriate reason phrase if it can. It may just drop this message.

Message Details

```
OPTIONS sip:135.180.130.133 SIP/2.0
Via: SIP/2.0/UDP company.com:5604
Max-Forwards: 70
```

```
From: sip:iuser@company.com;tag=74345345
To: sip:user@135.180.130.133
Call-ID: 1804928587@company.com
CSeq: 1 OPTIONS
Expires: 0 0l@company.com
To: sip:user@135.180.130.133
Call-ID: 1804928587@company.com
CSeq: 1 OPTIONS
Contact: sip:host.company.com
Expires: 0xpires: 0sip:host.company.com
Expires: 0
Contact: sip:host.company.com
```

2.36 INVITE with large number of SDP attributes and telephone subscriber Request-URI

This is a legal message with a large number of SDP attributes and a long telephone subscriber Request-URI

Message Details

```
INVITE sip:+19725552222;phone-
context=name%40domain;new=user?%22Route%3a%20X%40Y%3bZ=W%22@gw1.atlan
ta.com;user=phone SIP/2.0
Via: SIP/2.0/UDP iftgw.biloxi.com:5060;branch=z9hG4bKjeefr3
Max-Forwards: 70
From:
<sip:+13035551111@ift.client.atlanta.com;user=phone>;tag=332lflke
To: sip:+16555552222@ss1.atlanta.com;user=phone
Call-ID: 1717@ift.client.atlanta.com
CSeq: 56 INVITE
Content-Type: application/sdp
Content-Length: 320

v=0
o=faxgw1 2890844527 2890844527 IN IP4 iftgw.biloxi.com
s=-
c=IN IP4 iftmg.biloxi.com
t=0 0
m=image 49172 udptl t38
a=T38FaxVersion:0
a=T38maxBitRate:14400
a=T38FaxFillBitRemoval:0
a=T38FaxTranscodingMMR:0
a=T38FaxTranscodingJBIG:0
a=T38FaxRateManagement:transferredTCF
```

```
a=T38FaxMaxBuffer:260
a=T38FaxUdpEC:t38UDPR
```

2.37 REGISTER with a contact parameter.

This REGISTER contains a contact where the 'user' parameter should be interpreted as being a contact-param and not a url-param.

The register should succeed but a subsequent retrieval of the registration must not include "user=phone" as a url-parameter.

Message Details

```
REGISTER sip:bell-tel.com SIP/2.0
Via: SIP/2.0/UDP saturn.bell-tel.com:5060;branch=z9hG4bKkdjuw
Max-Forwards: 70
From: sip:watson@bell-tel.com;tag=DkfVgjkrtMwaerKKpe
To: sip:watson@bell-tel.com
Call-ID: 70710@saturn.bell-tel.com
CSeq: 2 REGISTER
Contact: sip:+19725552222@gw1.atlanta.com;user=phone
```

2.38 REGISTER with a url parameter.

This register contains a contact where the 'user'parameter is a url-param.

The register should succeed and a subsequent retrieval of the registration must
include "user=phone" as a url-parameter.

Message Details

```
REGISTER sip:bell-tel.com SIP/2.0
Via: SIP/2.0/UDP saturn.bell-tel.com:5060;branch=z9hG4bKkdjuw
Max-Forwards: 70
From: sip:watson@bell-tel.com;tag=838293
To: sip:watson@bell-tel.com
Call-ID: 70710@saturn.bell-tel.com
CSeq: 3 REGISTER
Contact: <sip:+19725552222@gw1.atlanta.com;user=phone>
```

2.39 INVITE with an Unquoted Display Name Containing Multiple Tokens

This is a legal INVITE where the To and From header contain display names that contain multiple tokens but are unquoted.

Message Details

```
INVITE sip:t.watson@ieee.org SIP/2.0
Via:     SIP/2.0/UDP c.bell-tel.com:5060;branch=z9hG4bKkdjuw
Max-Forwards:    70
From:    A. Bell <sip:a.g.bell@bell-tel.com>;tag=459843
To:      T. Watson <sip:t.watson@ieee.org>
Call-ID: 31414@c.bell-tel.com
CSeq:    1 INVITE
```

2.40 INVITE with an Unquoted Display Name Containg Non-Token Characters

This is an illegal invite at the display names in the To and From headers contain non-token characters but are unquoted.

A server may be intelligent enough to cope with this but may also return a 400 response with an appropriate reason phrase.

Message Details

```
INVITE sip:t.watson@ieee.org SIP/2.0
Via:     SIP/2.0/UDP c.bell-tel.com:5060;branch=z9hG4bKkdjuw
Max-Forwards:      70
From:    Bell, Alexander <sip:a.g.bell@bell-tel.com>;tag=43
To:      Watson, Thomas <sip:t.watson@ieee.org>
Call-ID: 31415@c.bell-tel.com
CSeq:    1 INVITE
```

2.41 INVITE with Unknown (Higher) Protocol Version in Start Line

This is an illegal INVITE as the SIP Protocol version is unknown.

The server should respond to the request with a bad version error.

Message Details

```
INVITE sip:t.watson@ieee.org SIP/7.0
Via:     SIP/2.0/UDP c.bell-tel.com;branch=z9hG4bKkdjuw
Max-Forwards:     70
```

```
From:    A. Bell <sip:a.g.bell@bell-tel.com>;tag=qweoiqpe
To:      T. Watson <sip:t.watson@ieee.org>
Call-ID: 31417@c.bell-tel.com
CSeq:    1 INVITE
```

2.42 INVITE with RFC2543 syntax

This is a legal message per RFC 2543 which should be accepted by RFC 3261 elements which want to maintain backwards compatibility.

Message Details

```
INVITE sip:UserB@biloxi.com SIP/2.0
Via: SIP/2.0/UDP iftgw.biloxi.com
From: <sip:+13035551111@ift.client.atlanta.com;user=phone>;tag=93752
Record-Route: <sip:UserB@biloxi.com;maddr=ss1.wcom.com>
To: sip:+16505552222@ss1.atlanta.com;user=phone
Call-ID: 1717@ift.client.atlanta.com
CSeq: 56 INVITE
```

Security Considerations

Since this document represents NON NORMATIVE examples of SIP session establishment, the security considerations in RFC 3261 [2] apply.

References

1 Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997

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

3 J.Rosenberg and H.Schulzrinne, "An Offer/Answer Model with SDP", Internet Engineering Task Force, RFC 3264, April 2002.

Acknowledgments

Thanks to Rohan Mahy, Adam Roach, Gonzalo Camarillo, Cullen Jennings, and Tom Taylor for their detailed comments during the final final review. Thanks to Vijay Gurbani for his comments.

The authors wish to thank Neil Deason for his additions to the Torture Test messages and Kundan Singh for performing parser validation of messages.

The authors wish to thank the following individuals for their participation in the final review of this call flows document: Aseem Agarwal, Rafi Assadi, Ben Campbell, Sunitha Kumar, Jon Peterson, Marc Petit-Huguenin, Vidhi Rastogi, and Bodgey Yin Shaohua.

The authors also wish to thank the following individuals for their assistance: Jean-Francois Mule, Hemant Agrawal, Henry Sinnreich, David Devanatham, Joe Pizzimenti, Matt Cannon, John Hearty, the whole MCI WorldCom IPOP Design team, Scott Orton, Greg Osterhout, Pat Sollee, Doug Weisenberg, Danny Mistry, Steve McKinnon, and Denise Ingram, Denise Caballero, Tom Redman, Ilya Slain, Pat Sollee, John Truetken, and others from MCI WorldCom, 3Com, Cisco, Lucent and Nortel.

Author's Addresses

Alan Johnston
WorldCom
100 South 4th Street
St. Louis, MO 63102
USA

EMail: alan.johnston@wcom.com

Jonathan Rosenberg
dynamicsoft
72 Eagle Rock Ave
East Hanover, NJ 07936
USA

EMail: jdrosen@dynamicsoft.com

Henning Schulzrinne
Dept. of Computer Science
Columbia University
1214 Amsterdam Avenue
New York, NY 10027
USA

EMail: schulzrinne@cs.columbia.edu

Copyright Notice

"Copyright (C) The Internet Society 2002. 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.

Acknowledgement

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