Network Working Group
Internet-Draft
Expires: May 18, 2006

R. Sparks, Ed.
Estacado Systems
A. Hawrylyshen
Ditech Communications Corp.
A. Johnston
Tello Corporation
J. Rosenberg
Cisco Systems
H. Schulzrinne
Columbia University
November 14, 2005

Session Initiation Protocol Torture Test Messages
draft-ietf-sipping-torture-tests-09

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

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.

This Internet-Draft will expire on May 18, 2006.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

This informational document gives examples of Session Initiation

Protocol (SIP) test messages designed to exercise and "torture" a SIP implementation.

Table of Contents

1. Overview 4
2. Document Conventions 4
  2.1. Representing Long Lines 4
  2.2. Representing Non-printable Characters 5
  2.3. Representing Long Repeating Strings 6
3. SIP Test Messages 6
  3.1. Parser tests (syntax) 6
    3.1.1. Valid messages 6
      3.1.1.1. A short tortuous INVITE 6
      3.1.1.2. Wide range of valid characters 8
      3.1.1.3. Valid use of the % escaping mechanism 9
      3.1.1.4. Escaped nulls in URIs 10
      3.1.1.5. Use of % when it is not an escape 11
      3.1.1.6. Message with no LWS between display name and < . . 11
      3.1.1.7. Long values in header fields 12
      3.1.1.8. Extra trailing octets in a UDP datagram 14
      3.1.1.9. Semicolon separated parameters in URI user part . 15
      3.1.1.10. Varied and unknown transport types 15
      3.1.1.11. Multipart MIME message 16
      3.1.1.12. Unusual reason phrase 17
      3.1.1.13. Empty reason phrase 18
    3.1.2. Invalid messages 19
      3.1.2.1. Extraneous header field separators 19
      3.1.2.2. Content length larger than message 19
      3.1.2.3. Negative Content-Length 20
      3.1.2.4. Request scalar fields with overlarge values . . . 21
      3.1.2.5. Response scalar fields with overlarge values . . . 22
      3.1.2.6. Unterminated quoted string in display-name 22
      3.1.2.7. <> enclosing Request-URI 23
      3.1.2.8. Malformed SIP Request-URI (embedded LWS) 24
      3.1.2.9. Multiple SP separating Request-Line elements . . . 25
      3.1.2.10. SP characters at end of Request-Line 26
      3.1.2.11. Escaped headers in SIP Request-URI 27
      3.1.2.12. Invalid timezone in Date header field 27
      3.1.2.13. Failure to enclose name-addr URI in <> 28
      3.1.2.14. Spaces within addr-spec 29
      3.1.2.15. Non-token characters in display-name 29
      3.1.2.16. Unknown protocol version 30
      3.1.2.17. Start line and CSeq method mismatch 30
      3.1.2.18. Unknown Method with CSeq method mismatch 30
      3.1.2.19. Overlarge response code 31
  3.2. Transaction layer semantics 31

3.2.1. Missing transaction identifier 31
3.3. Application layer semantics 32
3.3.1. Missing Required Header Fields 32
3.3.2. Request-URI with unknown scheme 33
3.3.3. Request-URI with known but atypical scheme 33
3.3.4. Unknown URI schemes in header fields 34
3.3.5. Proxy-Require and Require 34
3.3.6. Unknown Content-Type 35
3.3.7. Unknown authorization scheme 35
3.3.8. Multiple values in single value required fields . . . 36
3.3.9. Multiple Content-Length values 37
3.3.10. 200 OK Response with broadcast Via header field value 37
3.3.11. Max-Forwards of zero 38
3.3.12. REGISTER with a contact header parameter 38
3.3.13. REGISTER with a url parameter 39
3.3.14. REGISTER with a url escaped header 39
3.3.15. Unacceptable Accept offering 40
3.4. Backward compatibility 41
3.4.1. INVITE with RFC2543 syntax 41
4. Security Considerations 42
5. IANA Considerations 42
6. Acknowledgments 42
7. Informative References 43
Appendix A. Bit-exact archive of each test message 43
A.1. Encoded Reference Messages 44
Authors' Addresses 49
Intellectual Property and Copyright Statements 50

1. Overview

This document is informational, and is NOT NORMATIVE on any aspect of SIP.

This document contains test messages based on the current version (2.0) of the Session Initiation Protocol as defined in [RFC3261]. Some messages exercise SIP's use of SDP as described in [RFC3264].

These messages were developed and refined at the SIPIt interoperability test events.

The test messages are organized into several sections. Some stress only a SIP parser and others stress both the parser and the application above it. Some messages are valid, and some are not. Each example clearly calls out what makes any invalid messages incorrect.

This document does not attempt to catalog every way to make an invalid message, nor does it attempt to be comprehensive in exploring unusual, but valid, messages. Instead, it tries to focus on areas that have caused interoperability problems or have particularly unfavorable characteristics if they are handled improperly. This document is a seed for a test plan, not a test plan in itself.

The messages are presented in the text using a set of markup conventions to avoid ambiguity and meet Internet-Draft layout requirements. To resolve any remaining ambiguity, a bit-accurate version of each message is encapsulated in an appendix.

2. Document Conventions

This document contains many example SIP messages. Although SIP is a text-based protocol, many of these examples cannot be unambiguously rendered without additional markup due to the constraints placed on the formatting of RFCs. This document defines and uses the markup defined in this section to remove that ambiguity. This markup uses the start and end tag conventions of XML, but does not define any XML document type.

The appendix contains an encoded binary form of all the messages and the algorithm needed to decode them into files.

2.1. Representing Long Lines

Several of these examples contain unfolded lines longer than 72 characters. These are captured between <allOneLine/> tags. The

single unfolded line is reconstructed by directly concatenating all lines appearing between the tags (discarding any line-feeds or carriage returns). There will be no whitespace at the end of lines. Any whitespace appearing at a fold-point will appear at the beginning of a line.

The following represent the same string of bits:

```
Header-name: first value, reallylongsecondvalue, third value
```

```
<allOneLine>
Header-name: first value,
 reallylongsecondvalue
, third value
</allOneLine>
```

```
<allOneLine>
Header-name: first value,
 reallylong
second
value,
 third value
</allOneLine>
```

Note that this is NOT SIP header line folding where different strings of bits have equivalent meaning.

2.2. Representing Non-printable Characters

Several examples contain binary message bodies or header field values containing non-ascii range UTF-8 encoded characters. These are rendered here as a pair of hexadecimal digits per octet between <hex/> tags. This rendering applies even inside quoted-strings.

The following represent the same string of bits:

```
Header-name: value one
```

```
Header-name: value<hex>206F6E</hex>e
```

The following is a Subject header field containing the euro symbol:

```
Subject: <hex>E282AC</hex>
```

2.3. Representing Long Repeating Strings

Several examples contain very large data values created with repeating bit strings. Those will be rendered here using <repeat count=some_integer>value</repeat>. As with <hex> this rendering applies even inside quoted-strings.

For example, the value "abcabcabc" can be rendered as <repeat count=3>abc</repeat>. A display name of "1000000 bottles of beer" could be rendered as

```
To: "1<repeat count=6><hex>30</hex></repeat> bottles of beer"
    <sip:beer.example.com>
```

and a Max-Forwards header field with a value of one google will be rendered here as

```
Max-Forwards: 1<repeat count=100>0</repeat>
```

3. SIP Test Messages

3.1. Parser tests (syntax)

3.1.1. Valid messages

3.1.1.1. A short tortuous INVITE

This short, relatively human-readable message contains:

- o line folding all over
- o escaped characters within quotes
- o an empty subject
- o LWS between colons, semicolons, header field values, and other fields
- o both comma separated and separate listing of header field values
- o mix of short and long form for the same header field name
- o unkown Request-URI parameter
- o unknown header fields
- o unknown header field with a value that would be syntactically invalid if it were defined in terms of generic-param
- o unusual header field ordering
- o unusual header field name character case
- o unknown parameters of a known header field
- o uri parameter with no value
- o header parameter with no value
- o integer fields (Max-Forwards and CSeq) with leading zeros

All elements should treat this as a well-formed request.

The UnknownHeaderWithUnusualValue header field deserves special attention. If this header field were defined in terms of comma separated values with semicolon separated parameters (as many of the existing defined header fields), this would be invalid. However, since the receiving element does not know the definition of the syntax for this field, it must parse it as a header-value. Proxies would forward this header field unchanged. Endpoints would ignore the header field.

Message Details : wsinv

```
INVITE sip:vivekg@chair-dnrc.example.com;unknownparam SIP/2.0
TO :
 sip:vivekg@chair-dnrc.example.com ;   tag    = 1918181833n
from   : "J Rosenberg \\\""       <sip:jdrosen@example.com>
  ;
  tag = 98asjd8
MaX-fOrWaRdS: 0068
Call-ID: wsinv.ndaksdj@192.0.2.1
Content-Length   : 150
cseq: 0009
  INVITE
Via  : SIP  /   2.0
 /UDP
    192.0.2.2;branch=390skdjuw
s :
NewFangledHeader:   newfangled value
 continued newfangled value
UnknownHeaderWithUnusualValue: ;;,,;;,;
Content-Type: application/sdp
Route:
 <sip:services.example.com;lr;unknownwith=value;unknown-no-value>
v:  SIP  / 2.0  / TCP     spindle.example.com   ;
  branch  =   z9hG4bK9ikj8  ,
 SIP  /    2.0   / UDP  192.168.255.111   ; branch=
 z9hG4bK30239
m:"Quoted string \"\"" <sip:jdrosen@example.com> ; newparam =
      newvalue ;
  secondparam ; q = 0.33

v=0
o=mhandley 29739 7272939 IN IP4 192.0.2.3
s=-
c=IN IP4 192.0.2.4
t=0 0
m=audio 49217 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

3.1.1.2. Wide range of valid characters

This message exercises a wider range of characters in several key syntactic elements than implementations usually see. Of particular note:

- o The Method contains non-alpha characters from token. Note that % is not an escape character for this field. A method of IN%56ITE is an unknown method. It is not the same as a method of INVITE
- o The Request-URI contain unusual, but legal, characters
- o A branch parameter contains all non-alphanum characters from token
- o The To header field value's quoted-string contains quoted-pair expansions, including a quoted NULL character
- o The name part of name-addr in the From header field value contains multiple tokens (instead of a quoted string) with all non-alphanum characters from the token production rule. That value also has an unknown header parameter whose name contains the non-alphanum token characters and whose value is a non-ascii range UTF-8 encoded string. The tag parameter on this value contains the non-alphanum token characters
- o The Call-ID header field value contains the non-alphanum characters from word. Notice that in this production:
  - * % is not an escape character. (It is only an escape character in productions matching the rule "escaped")
  - * " does not start a quoted-string. None of ',` or " imply that there will be a matching symbol later in the string
  - * The characters []{}()<> do not have any grouping semantics. They are not required to appear in balanced pairs
- o There is an unknown header field (matching extension-header) with non-alphanum token characters in its name and a UTF8-NONASCII value

If this unusual URI has been defined at a proxy, the proxy will forward this request normally. Otherwise a proxy will generate a 404. Endpoints will generate a 501 listing the methods they understand in an Allow header field.

```
Message Details : intmeth

<allOneLine>
!interesting-Method0123456789_*+`.%indeed'~
 sip:1_unusual.URI~(to-be!sure)&isn't+it$/crazy?,/;;*
:&it+has=1,weird!*pas$wo~d_too.(doesn't-it)
@example.com SIP/2.0
</allOneLine>
Via: SIP/2.0/TCP host1.example.com;branch=z9hG4bK-.!%66*_+`'~
<allOneLine>
To: "BEL:\<hex>07</hex> NUL:\<hex>00</hex> DEL:\<hex>7F</hex>"
 <sip:1_unusual.URI~(to-be!sure)&isn't+it$/crazy?,/;;*
@example.com>
</allOneLine>
<allOneLine>
From: token1~` token2'+_ token3*%!.- <sip:mundane@example.com>
;fromParam''~+*_!.-%=
"<hex>D180D0B0D0B1D0BED182D0B0D18ED189D0B8D0B9</hex>"
;tag=_token~1'+`*%!-.
</allOneLine>
Call-ID: intmeth.word%ZK-!.*_+'@word`~)(><:\/"][?}{
CSeq: 139122385 !interesting-Method0123456789_*+`.%indeed'~
Max-Forwards: 255
<allOneLine>
extensionHeader-!.%*+_`'~:
<hex>EFBBBFE5A4A7E5819CE99BBB</hex>
</allOneLine>
Content-Length: 0
```

3.1.1.3. Valid use of the % escaping mechanism

This INVITE exercises the % HEX HEX escaping mechanism in several places. The request is syntactically valid. Interesting features include:

- o The request-URI has sips:user@example.com embedded in its userpart. What that might mean to example.net is beyond the scope of this document.
- o The From and To URIs have escaped characters in their userparts.
- o The Contact URI has escaped characters in the URI parameters. Note that the "name" uri-parameter has a value of "value%41" which is NOT equivalent to "valueA". Per [RFC2396], unescaping URI components is never performed recursively.

A parser must accept this as a well-formed message. The application using the message must treat the % HEX HEX expansions as equivalent to the character being encoded. The application must not try to interpret % as an escape character in those places where % HEX HEX

("escaped" in the grammar) is not a valid part of the construction. In [RFC3261], "escaped" only occurs in the expansions of SIP-URI, SIPS-URI, and Reason-Phrase.

```
Message Details : esc01

INVITE sip:sips%3Auser%40example.com@example.net SIP/2.0
To: sip:%75se%72@example.com
From: <sip:I%20have%20spaces@example.net>;tag=938
Max-Forwards: 87
i: esc01.239409asdfakjkn23onasd0-3234
CSeq: 234234 INVITE
Via: SIP/2.0/UDP host5.example.net;branch=z9hG4bKkdjuw
C: application/sdp
Contact:
  <sip:cal%6Cer@host5.example.net;%6C%72;n%61me=v%61lue%25%34%31>
Content-Length: 150

v=0
o=mhandley 29739 7272939 IN IP4 192.0.2.1
s=-
c=IN IP4 192.0.2.1
t=0 0
m=audio 49217 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

3.1.1.4. Escaped nulls in URIs

This register request contains several URIs with nulls in the userpart. The message is well formed - parsers must accept this message. Implementations must take special care when unescaping the Address-of-Record (AOR) in this request to not prematurely shorten the username. This request registers two distinct contact URIs.

```
Message Details : escnull

REGISTER sip:example.com SIP/2.0
To: sip:null-%00-null@example.com
From: sip:null-%00-null@example.com;tag=839923423
Max-Forwards: 70
Call-ID: escnull.39203ndfvkjdasfkq3w4otrq0adsfdfnavd
CSeq: 14398234 REGISTER
Via: SIP/2.0/UDP host5.example.com;branch=z9hG4bKkdjuw
Contact: <sip:%00@host5.example.com>
Contact: <sip:%00%00@host5.example.com>
L:0
```

3.1.1.5. Use of % when it is not an escape

Most of the places % can appear in a SIP message, it is not an escape character. This can surprise the unwary implementor. The following well-formed request has these properties:

- o The request method is unknown. It is NOT equivalent to REGISTER
- o The display-name portion of the To and From header fields is "%Z%45". Note that this is not the same as %ZE
- o This message has two Contact header field values, not three. <sip:alias2@host2.example.com> is a C%6Fntact header field value

A parser should accept this message as well formed. A proxy would forward or reject the message depending on what the Request-URI meant to it. An endpoint would reject this message with a 501.

Message Details : esc02

```
RE%47IST%45R sip:registrar.example.com SIP/2.0
To: "%Z%45" <sip:resource@example.com>
From: "%Z%45" <sip:resource@example.com>;tag=f232jadfj23
Call-ID: esc02.asdfnqwo34rq23i34jrjasdcnl23nrlknsdf
Via: SIP/2.0/TCP host.example.com;branch=z9hG4bK209%fzsnel234
CSeq: 29344 RE%47IST%45R
Max-Forwards: 70
Contact: <sip:alias1@host1.example.com>
C%6Fntact: <sip:alias2@host2.example.com>
Contact: <sip:alias3@host3.example.com>
l: 0
```

3.1.1.6. Message with no LWS between display name and <

This OPTIONS request is not valid per the grammar in RFC 3261 since there is no LWS between the token in the display name and < in the From header field value. This has been identified as a specification bug that will be removed when RFC 3261 is revised. Elements should accept this request as well formed.

Message Details : lwsdisp

```
OPTIONS sip:user@example.com SIP/2.0
To: sip:user@example.com
From: caller<sip:caller@example.com>;tag=323
Max-Forwards: 70
Call-ID: lwsdisp.1234abcd@funky.example.com
CSeq: 60 OPTIONS
Via: SIP/2.0/UDP funky.example.com;branch=z9hG4bKkdjuw
l: 0
```

3.1.1.7. Long values in header fields

This well-formed request contains header fields with many values and values that are very long. Features include:

- o The To header field has a long display name, and long uri parameter names and values
- o The From header field has long header parameter names and values, in particular a very long tag
- o The Call-ID is one long token

Message Details : longreq

```
INVITE sip:user@example.com SIP/2.0
<allOneLine>
To: "I have a user name of
 <repeat count=10>extreme</repeat> proportion"
<sip:user@example.com:6000;
unknownparam1=very<repeat count=20>long</repeat>value;
longparam<repeat count=25>name</repeat>=shortvalue;
very<repeat count=25>long</repeat>ParameterNameWithNoValue>
</allOneLine>
<allOneLine>
F: sip:
<repeat count=5>amazinglylongcallername</repeat>@example.net
;tag=12<repeat count=50>982</repeat>424
;unknownheaderparam<repeat count=20>name</repeat>=
unknowheaderparam<repeat count=15>value</repeat>
;unknownValueless<repeat count=10>paramname</repeat>
</allOneLine>
Call-ID: longreq.one<repeat count=20>really</repeat>longcallid
CSeq: 3882340 INVITE
<allOneLine>
Unknown-<repeat count=20>Long</repeat>-Name:
 unknown-<repeat count=20>long</repeat>-value;
 unknown-<repeat count=20>long</repeat>-parameter-name =
 unknown-<repeat count=20>long</repeat>-parameter-value
</allOneLine>
Via: SIP/2.0/TCP sip33.example.com
v: SIP/2.0/TCP sip32.example.com
V: 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
```

```
V :  SIP/2.0/TCP sip22.example.com
v :  SIP/2.0/TCP sip21.example.com
V  : SIP/2.0/TCP sip20.example.com
v  : 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
<allOneLine>
Via: SIP/2.0/TCP
 host.example.com;received=192.0.2.5;
branch=very<repeat count=50>long</repeat>branchvalue
</allOneLine>
Max-Forwards: 70
<allOneLine>
Contact: <sip:
<repeat count=5>amazinglylongcallername</repeat>
@host5.example.net>
</allOneLine>
Content-Type: application/sdp
l: 150

v=0
o=mhandley 29739 7272939 IN IP4 192.0.2.1
s=-
c=IN IP4 192.0.2.1
t=0 0
m=audio 49217 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

3.1.1.8. Extra trailing octets in a UDP datagram

This message contains a single SIP REGISTER request, which ostensibly arrived over UDP in a single datagram. The packet contains extra octets after the body (which in this case has zero length). The extra octets happen to look like a SIP INVITE request, but (per section 18.3 of [RFC3261]) they are just spurious noise that must be ignored.

A SIP element receiving this datagram would handle the REGISTER request normally and ignore the extra bits that look like an INVITE request. If the element is a proxy choosing to forward the REGISTER, the INVITE octets would not appear in the forwarded request.

```
Message Details : dblreq

REGISTER sip:example.com SIP/2.0
To: sip:j.user@example.com
From: sip:j.user@example.com;tag=43251j3j324
Max-Forwards: 8
I: dblreq.0ha0isndaksdj99sdfafnl3lk233412
Contact: sip:j.user@host.example.com
CSeq: 8 REGISTER
Via: SIP/2.0/UDP 192.0.2.125;branch=z9hG4bKkdjuw23492
Content-Length: 0


INVITE sip:joe@example.com SIP/2.0
t: sip:joe@example.com
From: sip:caller@example.net;tag=141334
Max-Forwards: 8
Call-ID: dblreq.0ha0isnda977644900765@192.0.2.15
CSeq: 8 INVITE
Via: SIP/2.0/UDP 192.0.2.15;branch=z9hG4bKkdjuw380234
Content-Type: application/sdp
Content-Length: 150

v=0
o=mhandley 29739 7272939 IN IP4 192.0.2.15
s=-
c=IN IP4 192.0.2.15
t=0 0
m=audio 49217 RTP/AVP 0 12
m =video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

3.1.1.9. Semicolon separated parameters in URI user part

This request has a semicolon-separated parameter contained in the "user" part of the Request-URI (whose value contains an escaped @ symbol). Receiving elements will accept this as a well formed message. The Request-URI will parse such that the user part is "user;par=u@example.net".

Message Details : semiuri

```
OPTIONS sip:user;par=u%40example.net@example.com SIP/2.0
To: sip:j_user@example.com
From: sip:caller@example.org;tag=33242
Max-Forwards: 3
Call-ID: semiuri.0ha0isndaksdj
CSeq: 8 OPTIONS
Accept: application/sdp, application/pkcs7-mime,
        multipart/mixed, multipart/signed,
        message/sip, message/sipfrag
Via: SIP/2.0/UDP 192.0.2.1;branch=z9hG4bKkdjuw
l: 0
```

3.1.1.10. Varied and unknown transport types

This request contains Via header field values with all known transport types and exercises the transport extension mechanism. Parsers must accept this message as well formed. Elements receiving this message would process it exactly as if the 2nd and subsequent header field values specified UDP (or other transport).

Message Details : transports

```
OPTIONS sip:user@example.com SIP/2.0
To: sip:user@example.com
From: <sip:caller@example.com>;tag=323
Max-Forwards: 70
Call-ID:  transports.kijh4akdnaqjkwendsasfdj
Accept: application/sdp
CSeq: 60 OPTIONS
Via: SIP/2.0/UDP t1.example.com;branch=z9hG4bKkdjuw
Via: SIP/2.0/SCTP t2.example.com;branch=z9hG4bKklasjdhf
Via: SIP/2.0/TLS t3.example.com;branch=z9hG4bK2980unddj
Via: SIP/2.0/UNKNOWN t4.example.com;branch=z9hG4bKasd0f3en
Via: SIP/2.0/TCP t5.example.com;branch=z9hG4bK0a9idfnee
l: 0
```

3.1.1.11. Multipart MIME message

This MESSAGE request contains two body parts. The second part is binary encoded and contains null (0x00) characters. Receivers must take care to properly frame the received message.

Parsers must accept this message as well formed, even if the application above the parser does not support multipart/signed.

Additional examples of multipart/mime messages, in particular S/MIME messages, are available in the security call flow examples draft [I-D.jennings-sip-sec-flows].

```
Message Details : mpart01

MESSAGE sip:kumiko@example.org SIP/2.0
<allOneLine>
Via: SIP/2.0/UDP 127.0.0.1:5070
;branch=z9hG4bK-d87543-4dade06d0bdb11ee-1--d87543-;rport
</allOneLine>
Max-Forwards: 70
Route: <sip:127.0.0.1:5080>
<allOneLine>
Identity: r5mwreLuyDRYBi/0TiPwEsY3rEVsk/G2WxhgTV1PF7hHuL
IK0YWVKZhKv9Mj8UeXqkMVbnVq37CD+813gvYjcBUaZngQmXc9WNZSDN
GCzA+fWl9MEUHWIZo1CeJebdY/XlgKeTa0Olvq0rt70Q5jiSfbqMJmQF
teeivUhkMWYUA=
</allOneLine>
Contact: <sip:fluffy@127.0.0.1:5070>
To: <sip:kumiko@example.org>
From: <sip:fluffy@example.com>;tag=2fb0dcc9
Call-ID: 3d9485ad0c49859b@Zmx1ZmZ5LW1hYy0xNi5sb2NhbA..
CSeq: 1 MESSAGE
Content-Transfer-Encoding: binary
Content-Type: multipart/mixed;boundary=7a9cbec02ceef655
Date: Sat, 15 Oct 2005 04:44:56 GMT
User-Agent: SIPimp.org/0.2.5 (curses)
Content-Length: 553

--7a9cbec02ceef655
Content-Type: text/plain
Content-Transfer-Encoding: binary

Hello
--7a9cbec02ceef655
Content-Type: application/octet-stream
Content-Transfer-Encoding: binary
```

```
<hex>
3082015206092A86
4886F70D010702A08201433082013F02
01013109300706052B0E03021A300B06
092A864886F70D010701318201203082
011C020101307C3070310B3009060355
04061302555331133011060355040813
0A43616C69666F726E69613111300F06
03550407130853616E204A6F7365310E
300C060355040A130573697069743129
3027060355040B132053697069742054
657374204365727469666961746520
417574686F72697479020801950071 02
330113300706052B0E03021A300D0609
2A864886F70D01010105000481808EF4
66F948F0522DD2E5978E9D95AAE9F2FE
15A06659716292E8DA2AA8D8350A68CE
FFAE3CBD2BFF1675DDD5648E593DD647
28F26220F7E941749E330D9A15EDABDB
93D10C42102E7B7289D29CC0C9AE2EFB
C7C0CFF9172F3B027E4FC027E1546DE4
B6AA3ABB3E66CCCB5DD6C64B8383149C
B8E6FF182D944FE57B65BC99D005
</hex>
--7a9cbec02ceef655--
```

3.1.1.12. Unusual reason phrase

This 200 response contains a reason phrase other than "OK". The reason phrase is intended for human consumption, and may contain any string produced by

```
Reason-Phrase   =  *(reserved / unreserved / escaped
                   / UTF8-NONASCII / UTF8-CONT / SP / HTAB)
```

This particular response contains unreserved and non-ASCII UTF-8 characters. This response is well formed. A parser must accept this message.

```
Message Details : unreason

<allOneLine>
SIP/2.0 200 = 2**3 * 5**2 <hex>D0BDD0BE20D181D182
D0BE20D0B4D0B5D0B2D18FD0BDD0BED181D182D0BE20D0B4
D0B5D0B2D18FD182D18C202D20D0BFD180D0BED181D182D0
BED0B5</hex>
</allOneLine>
Via: SIP/2.0/UDP 192.0.2.198;branch=z9hG4bK1324923
Call-ID: unreason.1234ksdfak3j2erwedfsASdf
CSeq: 35 INVITE
From: sip:user@example.com;tag=11141343
To: sip:user@example.edu;tag=2229
Content-Length: 154
Content-Type: application/sdp
Contact: <sip:user@host198.example.com>

v=0
o=mhandley 29739 7272939 IN IP4 192.0.2.198
s=-
c=IN IP4 192.0.2.198
t=0 0
m=audio 49217 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

3.1.1.13. Empty reason phrase

This well formed response contains no reason phrase. A parser must accept this message. The space character after the reason code is required. If it were not present, this message could be rejected as invalid (a liberal receiver would accept it anyway).

```
Message Details : noreason

SIP/2.0 100<hex>20</hex>
Via: SIP/2.0/UDP 192.0.2.105;branch=z9hG4bK2398ndaoe
Call-ID: noreason.asndj203insdf99223ndf
CSeq: 35 INVITE
From: <sip:user@example.com>;tag=39ansfi3
To: <sip:user@example.edu>;tag=902jndnke3
Content-Length: 0
Contact: <sip:user@host105.example.com>
```

3.1.2. Invalid messages

This section contains several invalid messages reflecting errors seen at interoperability events and exploring important edge conditions that can be induced through malformed messages. This section does not attempt to be a comprehensive list of all types of invalid messages.

3.1.2.1. Extraneous header field separators

The Via header field of this request contains additional semicolons and commas without parameters or values. The Contact header field contains additional semicolons without parameters. This message is syntactically invalid.

An element receiving this request should respond with a 400 Bad Request error.

```
Message Details : badinv01

INVITE sip:user@example.com SIP/2.0
To: sip:j.user@example.com
From: sip:caller@example.net;tag=134161461246
Max-Forwards: 7
Call-ID: badinv01.0ha0isndaksdjasdf3234nas
CSeq: 8 INVITE
Via: SIP/2.0/UDP 192.0.2.15;;,;,,
Contact: "Joe" <sip:joe@example.org>;;;;
Content-Length: 152
Content-Type: application/sdp

v=0
o=mhandley 29739 7272939 IN IP4 192.0.2.15
s=-
c=IN IP4 192.0.2.15
t=0 0
m=audio 49217 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

3.1.2.2. Content length larger than message

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

When sent over UDP (as this message ostensibly was), the receiving element should respond with a 400 Bad Request error. If this message arrived over a stream-based transport such as TCP, there's not much

the receiving could do but wait for more data on the stream and close the connection if none is forthcoming in a reasonable period of time.

Message Details : clerr

```
INVITE sip:user@example.com SIP/2.0
Max-Forwards: 80
To: sip:j.user@example.com
From: sip:caller@example.net;tag=93942939o2
Contact: <sip:caller@hungry.example.net>
Call-ID: clerr.0ha0isndaksdjweiafasdk3
CSeq: 8 INVITE
Via: SIP/2.0/UDP host5.example.com;branch=z9hG4bK-39234-23523
Content-Type: application/sdp
Content-Length: 9999

v=0
o=mhandley 29739 7272939 IN IP4 192.0.2.155
s=-
c=IN IP4 192.0.2.155
t=0 0
m=audio 49217 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

3.1.2.3. Negative Content-Length

This request has a negative value for Content-Length.

An element receiving this message should respond with an error. This request appeared over UDP, so the remainder of the datagram can simply be discarded. If a request like this arrives over TCP, the framing error is not recoverable and the connection should be closed. The same behavior is appropriate for messages that arrive without a numeric value in the Content-Length header field such as:

```
Content-Length: five
```

Implementors should take extra precautions if the technique they choose for converting this ascii field into an integral form can return a negative value. In particular, the result must not be used as a counter or array index.

Message Details : ncl

```
INVITE sip:user@example.com SIP/2.0
Max-Forwards: 254
To: sip:j.user@example.com
From: sip:caller@example.net;tag=32394234
Call-ID: ncl.0ha0isndaksdj2193423r542w35
CSeq: 0 INVITE
Via: SIP/2.0/UDP 192.0.2.53;branch=z9hG4bKkdjuw
Contact: <sip:caller@example53.example.net>
Content-Type: application/sdp
Content-Length: -999

v=0
o=mhandley 29739 7272939 IN IP4 192.0.2.53
s=-
c=IN IP4 192.0.2.53
t=0 0
m=audio 49217 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

3.1.2.4. Request scalar fields with overlarge values

This request contains several scalar header field values outside their legal range.

- o the CSeq sequence number is >2**32-1.
- o the Max-Forwards value is >255.
- o the Expires value is >2**32-1.
- o the Contact expires parameter value is >2**32-1.

An element receiving this request should respond with a 400 Bad Request due to the CSeq error. If only the Max-Forwards field were in error, the element could choose process the request as if the field were absent. If only the expiry values were in error, the element could treat them as if they contained the default values for expiration (3600 in this case).

Other scalar request fields that may contain aberrant values include, but are not limited to, the Contact q value, the Timestamp value, and the Via ttl parameter.

```
Message Details : scalar02

REGISTER sip:example.com SIP/2.0
Via: SIP/2.0/TCP host129.example.com;branch=z9hG4bK342sdfoi3
To: <sip:user@example.com>
From: <sip:user@example.com>;tag=239232jh3
CSeq: 36893488147419103232 REGISTER
Call-ID: scalar02.23o0pd9vanlq3wnrlnewofjas9ui32
Max-Forwards: 300
Expires: 1<repeat count=100>0</repeat>
Contact: <sip:user@host129.example.com>
  ;expires=280297596632815
Content-Length: 0
```

3.1.2.5. Response scalar fields with overlarge values

This response contains several scalar header field values outside their legal range.

- o the CSeq sequence number is >2**32-1.
- o The Retry-After field is unreasonably large (note that RFC 3261 does not define a legal range for this field).
- o The Warning field has a warning-value with more than 3 digits

An element receiving this response will simply discard it.

```
Message Details : scalarlg

SIP/2.0 503 Service Unavailable
<allOneLine>
Via: SIP/2.0/TCP host129.example.com
;branch=z9hG4bKzzxdiwo34sw
;received=192.0.2.129
</allOneLine>
To: <sip:user@example.com>
From: <sip:other@example.net>;tag=2easdjfejw
CSeq: 9292394834772304023312 OPTIONS
Call-ID: scalarlg.noase0of0234hn2qofoaf0232aewf2394r
Retry-After: 949302838503028349304023988
Warning: 1812 overture "In Progress"
Content-Length: 0
```

3.1.2.6. Unterminated quoted string in display-name

This is a request with an unterminated quote in the display name of the To field. An element receiving this request should return an 400 Bad Request error.

An element could attempt to infer a terminating quote and accept the message. Such an element needs to take care that it makes a reasonable inference when it encounters

```
To: "Mr J. User <sip:j.user@example.com> <sip:realj@example.net>
```

Message Details : quotbal

```
INVITE sip:user@example.com SIP/2.0
To: "Mr. J. User <sip:j.user@example.com>
From: sip:caller@example.net;tag=93334
Max-Forwards: 10
Call-ID: quotbal.aksdj
Contact: <sip:caller@host59.example.net>
CSeq: 8 INVITE
Via: SIP/2.0/UDP 192.0.2.59:5050;branch=z9hG4bKkdjuw39234
Content-Type: application/sdp
Content-Length: 152

v=0
o=mhandley 29739 7272939 IN IP4 192.0.2.15
s=-
c=IN IP4 192.0.2.15
t=0 0
m=audio 49217 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

3.1.2.7. <> enclosing Request-URI

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

It is reasonable to always reject a request with this error with a 400 Bad Request. Elements attempting to be liberal with what they accept may choose to ignore the brackets. If the element forwards the request, it must not include the brackets in the messages it sends.

Message Details : ltgtruri

```
INVITE <sip:user@example.com> SIP/2.0
To: sip:user@example.com
From: sip:caller@example.net;tag=39291
Max-Forwards: 23
Call-ID: ltgtruri.1@192.0.2.5
CSeq: 1 INVITE
Via: SIP/2.0/UDP 192.0.2.5
Contact: <sip:caller@host5.example.net>
Content-Type: application/sdp
Content-Length: 159

v=0
o=mhandley 29739 7272939 IN IP4 192.0.2.5
s=-
c=IN IP4 192.0.2.5
t=3149328700 0
m=audio 49217 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

3.1.2.8. Malformed SIP Request-URI (embedded LWS)

This INVITE has illegal LWS within the Request-URI.

An element receiving this request should respond with a 400 Bad Request.

An element could attempt to ignore the embedded LWS for those schemes (like sip) where that would not introduce ambiguity.

Message Details : lwsruri

```
INVITE sip:user@example.com; lr SIP/2.0
To: sip:user@example.com;tag=3xfe-9921883-z9f
From: sip:caller@example.net;tag=231413434
Max-Forwards: 5
Call-ID: lwsruri.asdfasdoeoi2323-asdfwrn23-asd834rk423
CSeq: 2130706432 INVITE
Via: SIP/2.0/UDP 192.0.2.1:5060;branch=z9hG4bKkdjuw2395
Contact: <sip:caller@host1.example.net>
Content-Type: application/sdp
Content-Length: 159

v=0
o=mhandley 29739 7272939 IN IP4 192.0.2.1
s=-
c=IN IP4 192.0.2.1
t=3149328700 0
m=audio 49217 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

3.1.2.9. Multiple SP separating Request-Line elements

This INVITE has illegal multiple SP characters between elements of the start line.

It is acceptable to reject this request as malformed. An element that is liberal in what it accepts may ignore these extra SP characters while processing the request. If the element forwards the request, it must not include these extra SP characters in the messages it sends.

Message Details : lwsstart

```
INVITE  sip:user@example.com  SIP/2.0
Max-Forwards: 8
To: sip:user@example.com
From: sip:caller@example.net;tag=8814
Call-ID: lwsstart.dfknq234oi243099adsdfnawe3@example.com
CSeq: 1893884 INVITE
Via: SIP/2.0/UDP host1.example.com;branch=z9hG4bKkdjuw3923
Contact: <sip:caller@host1.example.net>
Content-Type: application/sdp
Content-Length: 150

v=0
o=mhandley 29739 7272939 IN IP4 192.0.2.1
s=-
c=IN IP4 192.0.2.1
t=0 0
m=audio 49217 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

3.1.2.10. SP characters at end of Request-Line

This OPTIONS request contains SP characters between the SIP-Version field and the CRLF terminating the Request-Line.

It is acceptable to reject this request as malformed. An element that is liberal in what it accepts may ignore these extra SP characters while processing the request. If the element forwards the request, it must not include these extra SP characters in the messages it sends.

Message Details : trws

```
OPTIONS sip:remote-target@example.com SIP/2.0<hex>2020</hex>
Via: SIP/2.0/TCP host1.examle.com;branch=z9hG4bK299342093
To: <sip:remote-target@example.com>
From: <sip:local-resource@example.com>;tag=329429089
Call-ID: trws.oicu34958239neffasdhr2345r
Accept: application/sdp
CSeq: 238923 OPTIONS
Max-Forwards: 70
Content-Length: 0
```

3.1.2.11. Escaped headers in SIP Request-URI

This INVITE is malformed as the SIP Request-URI contains escaped headers.

It is acceptable for an element to reject this request with a 400 Bad Request. An element could choose to be liberal in what it accepts and ignore the escaped headers. If the element is a proxy, the escaped headers must not appear in the Request-URI of forwarded request (and most certainly must not be translated into the actual header of the forwarded request).

```
Message Details : escruri

INVITE sip:user@example.com?Route=%3Csip:example.com%3E SIP/2.0
To: sip:user@example.com
From: sip:caller@example.net;tag=341518
Max-Forwards: 7
Contact: <sip:caller@host39923.example.net>
Call-ID: escruri.23940-asdfhj-aje3br-234q098w-fawerh2q-h4n5
CSeq: 149209342 INVITE
Via: SIP/2.0/UDP host-of-the-hour.example.com;branch=z9hG4bKkdjuw
Content-Type: application/sdp
Content-Length: 150

v=0
o=mhandley 29739 7272939 IN IP4 192.0.2.1
s=-
c=IN IP4 192.0.2.1
t=0 0
m=audio 49217 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

3.1.2.12. Invalid timezone in Date header field

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

It is acceptable to reject this request as malformed (though an element shouldn't do that unless the contents of the Date header field were actually important to its processing). An element wishing to be liberal in what it accepts could ignore this value altogether if it wasn't going to use the Date header field anyhow. Otherwise, it could attempt to interpret this date and adjust it to GMT.

RFC 3261 explicitly defines the only acceptable timezone designation as "GMT". "UT", while synonymous with GMT per [RFC2822], is not

valid. "UTC" and "UCT" are also invalid.

Message Details : baddate

```
INVITE sip:user@example.com SIP/2.0
To: sip:user@example.com
From: sip:caller@example.net;tag=2234923
Max-Forwards: 70
Call-ID: baddate.239423mnsadf3j23lj42--sedfnm234
CSeq: 1392934 INVITE
Via: SIP/2.0/UDP host.example.com;branch=z9hG4bKkdjuw
Date: Fri, 01 Jan 2010 16:00:00 EST
Contact: <sip:caller@host5.example.net>
Content-Type: application/sdp
Content-Length: 150

v=0
o=mhandley 29739 7272939 IN IP4 192.0.2.5
s=-
c=IN IP4 192.0.2.5
t=0 0
m=audio 49217 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

3.1.2.13. Failure to enclose name-addr URI in <>

This REGISTER request is malformed. The SIP URI contained in the Contact Header field has an escaped header, so the field must be in name-addr form (which implies the URI must be enclosed in <>).

It is reasonable for an element receiving this request to respond with a 400 Bad Request. An element choosing to be liberal in what it accepts could infer the angle brackets since there is no ambiguity in this example. In general, that won't be possible.

Message Details : regbadct

```
REGISTER sip:example.com SIP/2.0
To: sip:user@example.com
From: sip:user@example.com;tag=998332
Max-Forwards: 70
Call-ID: regbadct.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
l: 0
```

3.1.2.14. Spaces within addr-spec

This request is malformed since the addr-spec in the To header field contains spaces. Parsers receiving this request must not break. It is reasonable to reject this request with a 400 Bad Request response. Elements attempting to be liberal may ignore the spaces.

```
Message Details : badaspec

OPTIONS sip:user@example.org SIP/2.0
Via: SIP/2.0/UDP host4.example.com:5060;branch=z9hG4bKkdju43234
Max-Forwards: 70
From: "Bell, Alexander" <sip:a.g.bell@example.com>;tag=433423
To: "Watson, Thomas" < sip:t.watson@example.org >
Call-ID: badaspec.sdf0234n2nds0a099u23h3hnnw009cdkne3
Accept: application/sdp
CSeq: 3923239 OPTIONS
l: 0
```

3.1.2.15. Non-token characters in display-name

This OPTIONS request is malformed since the display names in the To and From header fields contain non-token characters but are unquoted.

It is reasonable to always reject this kind of error with a 400 Bad Request response.

An element may attempt to be liberal in what it receives and infer the missing quotes. If this element were a proxy, it must not propagate the error into the request it forwards. As a consequence, if the fields are covered by a signature, there's not much point in trying to be liberal - the message should be simply rejected.

```
Message Details : baddn

OPTIONS sip:t.watson@example.org SIP/2.0
Via:     SIP/2.0/UDP c.example.com:5060;branch=z9hG4bKkdjuw
Max-Forwards:      70
From:    Bell, Alexander <sip:a.g.bell@example.com>;tag=43
To:      Watson, Thomas <sip:t.watson@example.org>
Call-ID: baddn.31415@c.example.com
Accept: application/sdp
CSeq:    3923239 OPTIONS
l: 0
```

3.1.2.16. Unknown protocol version

To an element implementing [RFC3261], this request is malformed due to its high version number.

The element should respond to the request with a 505 Version Not Supported error.

```
Message Details : badvers

OPTIONS sip:t.watson@example.org SIP/7.0
Via:     SIP/7.0/UDP c.example.com;branch=z9hG4bKkdjuw
Max-Forwards:     70
From:    A. Bell <sip:a.g.bell@example.com>;tag=qweoiqpe
To:      T. Watson <sip:t.watson@example.org>
Call-ID: badvers.31417@c.example.com
CSeq:    1 OPTIONS
l: 0
```

3.1.2.17. Start line and CSeq method mismatch

This request has mismatching values for the method in the start line and the CSeq header field. Any element receiving this request will respond with a 400 Bad Request.

```
Message Details : mismatch01

OPTIONS sip:user@example.com SIP/2.0
To: sip:j.user@example.com
From: sip:caller@example.net;tag=34525
Max-Forwards: 6
Call-ID: mismatch01.dj0234sxdfl3
CSeq: 8 INVITE
Via: SIP/2.0/UDP host.example.com;branch=z9hG4bKkdjuw
l: 0
```

3.1.2.18. Unknown Method with CSeq method mismatch

This message has an unknown method in the start line, and a CSeq method tag which does not match.

Any element receiving this response should respond with a 501 Not Implemented. A 400 Bad Request is also acceptable, but choosing a 501 (particularly at proxies) has better future-proof characteristics.

```
Message Details : mismatch02

NEWMETHOD sip:user@example.com SIP/2.0
To: sip:j.user@example.com
From: sip:caller@example.net;tag=34525
Max-Forwards: 6
Call-ID: mismatch02.dj0234sxdfl3
CSeq: 8 INVITE
Contact: <sip:caller@host.example.net>
Via: SIP/2.0/UDP host.example.net;branch=z9hG4bKkdjuw
Content-Type: application/sdp
l: 138

v=0
o=mhandley 29739 7272939 IN IP4 192.0.2.1
c=IN IP4 192.0.2.1
m=audio 49217 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

3.1.2.19. Overlarge response code

This response has a response code larger than 699. An element receiving this response should simply drop it.

```
Message Details : bigcode

SIP/2.0 4294967301 better not break the receiver
Via: SIP/2.0/UDP 192.0.2.105;branch=z9hG4bK2398ndaoe
Call-ID: bigcode.asdof3uj203asdnf3429uasdhfas3ehjasdfas9i
CSeq: 353494 INVITE
From: <sip:user@example.com>;tag=39ansfi3
To: <sip:user@example.edu>;tag=902jndnke3
Content-Length: 0
Contact: <sip:user@host105.example.com>
```

3.2. Transaction layer semantics

This section contains tests that exercise an implementation's parser and transaction layer logic.

3.2.1. Missing transaction identifier

This request indicates support for RFC 3261-style transaction identifiers by providing the z9hG4bK prefix to the branch parameter, but it provides no identifier. A parser must not break when receiving this message. An element receiving this request could

reject the request with a 400 Response (preferably statelessly, as other requests from the source are likely to also have a malformed branch parameter), or it could fall back to the RFC 2543 style transaction identifier.

Message Details : badbranch

```
OPTIONS sip:user@example.com SIP/2.0
To: sip:user@example.com
From: sip:caller@example.org;tag=33242
Max-Forwards: 3
Via: SIP/2.0/UDP 192.0.2.1;branch=z9hG4bK
Accept: application/sdp
Call-ID: badbranch.sadonfo23i420jv0as0derf3j3n
CSeq: 8 OPTIONS
l: 0
```

3.3. Application layer semantics

This section contains tests that exercise an implementation's parser and application layer logic.

3.3.1. Missing Required Header Fields

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

An element receiving this message must not break because of the missing information. Ideally, it will respond with a 400 Bad Request error.

Message Details : insuf

```
INVITE sip:user@example.com SIP/2.0
CSeq: 193942 INVITE
Via: SIP/2.0/UDP 192.0.2.95;branch=z9hG4bKkdj.insuf
Content-Type: application/sdp
l: 152

v=0
o=mhandley 29739 7272939 IN IP4 192.0.2.95
s=-
c=IN IP4 192.0.2.95
t=0 0
m=audio 49217 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

3.3.2. Request-URI with unknown scheme

This OPTIONS contains an unknown URI scheme in the Request-URI. A parser must accept this as a well-formed SIP request.

An element receiving this request will reject it with a 416 Unsupported URI Scheme response.

Some early implementations attempt to look at the contents of the To header field to determine how to route this kind of request. That is an error. Despite the fact that the To header field and the Request URI frequently look alike in simplistic first-hop messages, the To header field contains no routing information.

Message Details : unkscm

```
OPTIONS nobodyKnowsThisScheme:totallyopaquecontent SIP/2.0
To: sip:user@example.com
From: sip:caller@example.net;tag=384
Max-Forwards: 3
Call-ID: unkscm.nasdfasser0q239nwsdfasdkl34
CSeq: 3923423 OPTIONS
Via: SIP/2.0/TCP host9.example.com;branch=z9hG4bKkdjuw39234
Content-Length: 0
```

3.3.3. Request-URI with known but atypical scheme

This OPTIONS contains an Request-URI with an IANA registered scheme that does not commonly appear Request-URIs of SIP requests. A parser must accept this as a well-formed SIP request.

If an element will never accept this scheme as meaningful in a request-URI, it is appropriate to treat it as unknown and return a 416 Unsupported URI Scheme response. If the element might accept some URIs with this scheme, then a 404 Not Found is appropriate for those URIs it doesn't accept.

Message Details : novelsc

```
OPTIONS soap.beep://192.0.2.103:3002 SIP/2.0
To: sip:user@example.com
From: sip:caller@example.net;tag=384
Max-Forwards: 3
Call-ID: novelsc.asdfasser0q239nwsdfasdkl34
CSeq: 3923423 OPTIONS
Via: SIP/2.0/TCP host9.example.com;branch=z9hG4bKkdjuw39234
Content-Length: 0
```

3.3.4. Unknown URI schemes in header fields

This message contains registered schemes in the To, From and Contact header fields of a request. The message is syntactically valid. Parsers must not fail when receiving this message.

Proxies should treat this message as they would any other request for this URI. A registrar would reject this request with a 400 Bad Request response since the To: header field is required to contain a SIP or SIPS URI as an AOR.

```
Message Details : unksm2

REGISTER sip:example.com SIP/2.0
To: isbn:2983792873
From: <http://www.example.com>;tag=3234233
Call-ID: unksm2.daksdj@hyphenated-host.example.com
CSeq: 234902 REGISTER
Max-Forwards: 70
Via: SIP/2.0/UDP 192.0.2.21:5060;branch=z9hG4bKkdjuw
Contact: <name:John_Smith>
l: 0
```

3.3.5. Proxy-Require and Require

This request tests proper implementation of SIP's Proxy-Require and Require extension mechanisms.

Any element receiving this request will respond with a 420 Bad Extension response containing an Unsupported header field listing these features from either the Require or Proxy-Require header field depending on the role in which the element is responding.

```
Message Details : bext01

OPTIONS sip:user@example.com SIP/2.0
To: sip:j_user@example.com
From: sip:caller@example.net;tag=242etr
Max-Forwards: 6
Call-ID: bext01.0ha0isndaksdj
Require: nothingSupportsThis, nothingSupportsThisEither
Proxy-Require: noProxiesSupportThis, norDoAnyProxiesSupportThis
CSeq: 8 OPTIONS
Via: SIP/2.0/TLS fold-and-staple.example.com;branch=z9hG4bKkdjuw
Content-Length: 0
```

3.3.6. Unknown Content-Type

This INVITE request contains a body of unknown type. It is syntactically valid. A parser must not fail when receiving it.

A proxy receiving this request would process it just like any other INVITE. An endpoint receiving this request would reject it with a 415 Unsupported Media Type error.

```
Message Details : invut

INVITE sip:user@example.com SIP/2.0
Contact: <sip:caller@host5.example.net>
To: sip:j.user@example.com
From: sip:caller@example.net;tag=8392034
Max-Forwards: 70
Call-ID: invut.0ha0isndaksdjadsfij34n23d
CSeq: 235448 INVITE
Via: SIP/2.0/UDP somehost.example.com;branch=z9hG4bKkdjuw
Content-Type: application/unknownformat
Content-Length: 40

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

3.3.7. Unknown authorization scheme

This REGISTER request contains an Authorization header field with an unknown scheme. The request is well-formed. A parser must not fail when receiving it.

A proxy will treat this request as any other REGISTER. If it forwards the request, it will include this Authorization header field unmodified in the forwarded messages.

A registrar that does not care about challenge-response authentication will simply ignore the Authorization header field, processing this registration as if the field were not present. A registrar that does care about challenge-response authentication will reject this request with a 401, issuing a new challenge with a scheme it understands.

Endpoints choosing not to act as registrars will simply reject the request. A 405 Method Not Allowed is appropriate.

```
Message Details : regaut01

REGISTER sip:example.com SIP/2.0
To: sip:j.user@example.com
From: sip:j.user@example.com;tag=87321hj23128
Max-Forwards: 8
Call-ID: regaut01.0ha0isndaksdj
CSeq: 9338 REGISTER
Via: SIP/2.0/TCP 192.0.2.253;branch=z9hG4bKkdjuw
Authorization: NoOneKnowsThisScheme opaque-data=here
Content-Length:0
```

3.3.8. Multiple values in single value required fields

The message contains a request with multiple Call-ID, To, From, Max-Forwards and CSeq values. An element receiving this request must not break.

An element receiving this request would respond with a 400 Bad Request error.

```
Message Details : multi01

INVITE sip:user@company.com SIP/2.0
Contact: <sip:caller@host25.example.net>
Via: SIP/2.0/UDP 192.0.2.25;branch=z9hG4bKkdjuw
Max-Forwards: 70
CSeq: 5 INVITE
Call-ID: multi01.98asdh@192.0.2.1
CSeq: 59 INVITE
Call-ID: multi01.98asdh@192.0.2.2
From: sip:caller@example.com;tag=3413415
To: sip:user@example.com
To: sip:other@example.net
From: sip:caller@example.net;tag=2923420123
Content-Type: application/sdp
l: 154
Contact: <sip:caller@host36.example.net>
Max-Forwards: 5

v=0
o=mhandley 29739 7272939 IN IP4 192.0.2.25
s=-
c=IN IP4 192.0.2.25
t=0 0
m=audio 49217 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
```

```
a=rtpmap:31 LPC
```

3.3.9. Multiple Content-Length values

Multiple conflicting Content-Length header field values appear in this request.

From a framing perspective, this situation is equivalent to an invalid Content-Length value (or no value at all).

An element receiving this message should respond with an error. This request appeared over UDP, so the remainder of the datagram can simply be discarded. If a request like this arrives over TCP, the framing error is not recoverable and the connection should be closed.

Message Details : mcl01

```
OPTIONS sip:user@example.com SIP/2.0
Via: SIP/2.0/UDP host5.example.net;branch=z9hG4bK293423
To: sip:user@example.com
From: sip:other@example.net;tag=3923942
Call-ID: mcl01.fhn2323orihawfdoa3o4r52o3irsdf
CSeq: 15932 OPTIONS
Content-Length: 13
Max-Forwards: 60
Content-Length: 5
Content-Type: text/plain
```

There's no way to know how many octets are supposed to be here.

3.3.10. 200 OK Response with broadcast Via header field value

This message is a response with a 2nd Via header field value's sent-by containing 255.255.255.255. The message is well formed - parsers must not fail when receiving it.

Per [RFC3261] an endpoint receiving this message should simply discard it.

If a proxy followed normal response processing rules blindly, it would forward this response to the broadcast address. To protect against this being used as an avenue of attack, proxies should drop such responses.

```
Message Details : bcast

SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.2.198;branch=z9hG4bK1324923
Via: SIP/2.0/UDP 255.255.255.255;branch=z9hG4bK1saber23
Call-ID: bcast.0384840201234ksdfak3j2erwedfsASdf
CSeq: 35 INVITE
From: sip:user@example.com;tag=11141343
To: sip:user@example.edu;tag=2229
Content-Length: 154
Content-Type: application/sdp
Contact: <sip:user@host28.example.com>

v=0
o=mhandley 29739 7272939 IN IP4 192.0.2.198
s=-
c=IN IP4 192.0.2.198
t=0 0
m=audio 49217 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

3.3.11. Max-Forwards of zero

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

A proxy should not forward the request and respond 483 (Too Many Hops). An endpoint should process the request as if the Max-Forwards field value were still positive.

```
Message Details : zeromf

OPTIONS sip:user@example.com SIP/2.0
To: sip:user@example.com
From: sip:caller@example.net;tag=3ghsd41
Call-ID: zeromf.jfasdlfnm2o2l43r5u0asdfas
CSeq: 39234321 OPTIONS
Via: SIP/2.0/UDP host1.example.com;branch=z9hG4bKkdjuw2349i
Max-Forwards: 0
Content-Length: 0
```

3.3.12. REGISTER with a contact header parameter

This register request contains a contact where the 'unknownparam' parameter must be interpreted as being a contact-param and not a url-param.

This REGISTER should succeed. The response must not include "unknownparam" as a url-parameter for this binding. Likewise, "unknownparam" must not appear as a url-parameter in any binding during subsequent fetches.

Behavior is the same, of course, for any known contact-param parameter names.

Message Details : cparam01

```
REGISTER sip:example.com SIP/2.0
Via: SIP/2.0/UDP saturn.example.com:5060;branch=z9hG4bKkdjuw
Max-Forwards: 70
From: sip:watson@example.com;tag=DkfVgjkrtMwaerKKpe
To: sip:watson@example.com
Call-ID: cparam01.70710@saturn.example.com
CSeq: 2 REGISTER
Contact: sip:+19725552222@gw1.example.net;unknownparam
l: 0
```

3.3.13. REGISTER with a url parameter

This register request contains a contact where the URI has an unknown parameter.

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

Behavior is the same, of course, for any known url-parameter names.

Message Details : cparam02

```
REGISTER sip:example.com SIP/2.0
Via: SIP/2.0/UDP saturn.example.com:5060;branch=z9hG4bKkdjuw
Max-Forwards: 70
From: sip:watson@example.com;tag=838293
To: sip:watson@example.com
Call-ID: cparam02.70710@saturn.example.com
CSeq: 3 REGISTER
Contact: <sip:+19725552222@gw1.example.net;unknownparam>
l: 0
```

3.3.14. REGISTER with a url escaped header

This register request contains a contact where the URI has an escaped header.

The register should succeed and a subsequent retrieval of the registration must include the escaped Route header in the contact URI for this binding.

Message Details : regescrt

```
REGISTER sip:example.com SIP/2.0
To: sip:user@example.com
From: sip:user@example.com;tag=8
Max-Forwards: 70
Call-ID: regescrt.k345asrl3fdbv@192.0.2.1
CSeq: 14398234 REGISTER
Via: SIP/2.0/UDP host5.example.com;branch=z9hG4bKkdjuw
M: <sip:user@example.com?Route=%3Csip:sip.example.com%3E>
L:0
```

3.3.15. Unacceptable Accept offering

This request indicates the response must contain a body in an unknown type. In particular, since the Accept header field does not contain application/sdp, the response may not contain an SDP body. The recipient of this request could respond with a 406 Not Acceptable with a Warning/399 indicating that a response cannot be formulated in the formats offered in the Accept header field. It is also appropriate to respond with a 400 Bad Request since all SIP User-Agents (UAs) supporting INVITE are required to support application/sdp.

Message Details : sdp01

```
INVITE sip:user@example.com SIP/2.0
To: sip:j_user@example.com
Contact: <sip:caller@host15.example.net>
From: sip:caller@example.net;tag=234
Max-Forwards: 5
Call-ID: sdp01.ndaksdj9342dasdd
Accept: text/nobodyKnowsThis
CSeq: 8 INVITE
Via: SIP/2.0/UDP 192.0.2.15;branch=z9hG4bKkdjuw
Content-Length: 150
Content-Type: application/sdp

v=0
o=mhandley 29739 7272939 IN IP4 192.0.2.5
s=-
c=IN IP4 192.0.2.5
t=0 0
m=audio 49217 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

3.4. Backward compatibility

3.4.1. INVITE with RFC2543 syntax

This is a legal message per RFC 2543 (and several bis versions) which should be accepted by RFC 3261 elements which want to maintain backwards compatibility.

- There is no branch parameter at all on the Via header field value
- There is no From tag
- There is no explicit Content-Length (The body is assumed to be all octets in the datagram after the null-line)
- There is no Max-Forwards header field

```
Message Details : inv2543

INVITE sip:UserB@example.com SIP/2.0
Via: SIP/2.0/UDP iftgw.example.com
From: <sip:+13035551111@ift.client.example.net;user=phone>
Record-Route: <sip:UserB@example.com;maddr=ss1.example.com>
To: sip:+16505552222@ss1.example.net;user=phone
Call-ID: inv2543.1717@ift.client.example.com
CSeq: 56 INVITE
Content-Type: application/sdp

v=0
o=mhandley 29739 7272939 IN IP4 192.0.2.5
s=-
c=IN IP4 192.0.2.5
t=0 0
m=audio 49217 RTP/AVP 0
```

4. Security Considerations

This document presents NON NORMATIVE examples of SIP session establishment. The security considerations in [RFC3261] apply.

Parsers must carefully consider edge conditions and malicious input as part of their design. Attacks on many Internet systems use crafted input to cause implementations to behave in undesirable ways. Many of the messages in this draft are designed to stress a parser implementation at points traditionally used for such attacks. This document does not, however, attempt to be comprehensive. It should be considered a seed to stimulate thinking and planning, not simply a set of tests to be passed.

5. IANA Considerations

This document has no actions for IANA.

6. Acknowledgments

The final detailed review of this document was performed by: Diego Besprosvan, Vijay Gurbani, Shashi Kumar, Derek MacDonald, Gautham Narasimhan, Nils Ohlmeier, Bob Penfield, Reinaldo Penno, Marc Petit-Huguenin, Richard Sugarman, and Venkatesh Venkataramanan.

Earlier versions of this document were reviewed by: Aseem Agarwal, Rafi Assadi, Gonzalo Camarillo, Ben Campbell, Cullen Jennings, Vijay

Gurbani, Sunitha Kumar, Rohan Mahy, Jon Peterson, Marc Petit-Huguenin, Vidhi Rastogi, Adam Roach, Bodgey Yin Shaohua and Tom Taylor.

Thanks to Cullen Jennings and Eric Rescorla for their contribution to the multipart/mime sections of this document and their work constructing S/MIME examples in [I-D.jennings-sip-sec-flows]. Thanks to Neil Deason for contributing several messages and Kundan Singh for performing parser validation of messages in earlier versions.

The following individuals provided significant comments during the early phases of the development of this document: Jean-Francois Mule, Hemant Agrawal, Henry Sinnreich, David Devanatham, Joe Pizzimenti, Matt Cannon, John Hearty, the whole MCI 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, 3Com, Cisco, Lucent and Nortel.

7. Informative References

[I-D.jennings-sip-sec-flows]
Jennings, C. and K. Ono, "Example call flows using SIP security mechanisms", draft-jennings-sip-sec-flows-03 (work in progress), July 2005.

[RFC2396] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", RFC 2396, August 1998.

[RFC2822] Resnick, P., "Internet Message Format", RFC 2822, April 2001.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[RFC3264] Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)", RFC 3264, June 2002.

Appendix A. Bit-exact archive of each test message

The following text block is an encoded, gzip compressed TAR archive of files that represent each of the example messages discussed in Section 3.

To recover the compressed archive file intact, the text of this document may be passed as input to the following Perl script (the output should be redirected to a file or piped to "tar -xzvf -").

```
#!/usr/bin/perl
use strict;
my $bdata = "";
use MIME::Base64;
while(<>) {
 if (/-- BEGIN MESSAGE ARCHIVE --/ .. /-- END MESSAGE ARCHIVE --/) {
     if ( m/^\s*[^\s]+\s*$/) {
         $bdata = $bdata . $_;
     }
  }
}
print decode_base64($bdata);
```

Figure 58

Alternatively, the base-64 encoded block can be edited by hand to remove document structure lines and fed as input to any base-64 decoding utility.

A.1. Encoded Reference Messages


```
-- BEGIN MESSAGE ARCHIVE --
H4sIAEDwcEMCA+xdW2zc2Hm2nexNG6UN3LRF0QfaiKJdyxwdnkMOhyOPVrIt
27It22tdvHYTeM8MDzWc4ZAjkqORvK2bbIAAedmHtEHRdlvkoUCLFAjSlyLF
9rJPLYoWrTdAg6JFHwp0i+5D0SIoEAQFuj2HnAuH5GgoW3PxmgcazYU/b4f/
//3Xc04Rq9ipk1JGxe6xITVAW1YUvXc5K/W8syYheEygP0lIECWJ0gkSkMAx
DhwbQWs4LrY57phdcerYrjr96AZtb91L5/0paTdvbazevLHOOXo933CIvUT2
cK1ukIxlb3Prq7fmYQZMT23pON/+Nr958RZXthxXzLRpS1YtL4EsWCja2CyV
Cw+U8mWxeK2qVhoigkicnlrDe/wly25iW3XynEwPecmmO3GnzxPDOMstG/RQ
pkrs09w5diU4s50p0i1LgTMsLrh4uyAiJEI0PbVh0Z3vYNexzLPcRtmqYYfu
692Gm2l6v/fcyuL01AVsGPzqxTxXbPO8o2qAXp4JTdUBGChKA6IyKptmEwCl
pFZNQs+0XCqRupvncL1u6CXs6pY576h1erx1spPnkALpLSpcqyOnp4w8R29v
eurpeP60L/yHNkQAGCT/IsiG5R8KMJX/sco/lbiu/DNpi6NoizHbVqLi1Ysf
nsAiBEUYBgAUAymCQj9lYEYIochBEhiQ6BYXO1i1TM2CSBchqOwC7AAKKxqq
ILMtsbmnVVaHJP9U8Mkw1f8g+RcAFI+xf6IIBJRFVP7FbDbV/yNpqze2VjdW
jl78TeJ64g+pflWYwo5aAEHp9XiQqlGq22smlWEqsBAZFRHyvENUzax5VoQv
vwJVuQoSOf/S+xgnQdskxixpTk9dpKfMc5ds/SwHBO4qNjlIWZETsnkA6B+3
sr5Bz2iZLi5R7DkXuEd2fCkTuNNFn5CYLr+xXydxSNXafJ2Y226Z3oPk4c5u
gb5ZhVqZGj8G2eegIlNTQoYyvUGF3iC3ekvsAKM0PeUU+OmpUiG6wS0AhmS1
Am6ousXRLhdk7vbGrfnlrVscvSnItu3qKrE4BGF3ExKmp3DBdus1XM8jgbt+
```

68KzjIbPJv6bQ0X/BP6fgEL2n4gkKcX/Udt/sY5Trw/IWhBqS0l8wGYY/b3W
dQJpC7mBg71AXyl5rdcL9HeNu5WQC0jZnvKbIC313MNAf4+2Pi7f0yr/urkL
hHHGf2QEwvafDFAq/xNn/1Uyj2EBCkgUstSiF6CYjZiBvSLpcyIoY6A7poqr
jlrBDrUFWYwGO13/ra/l1/EhpYWFswtnzwYMuNNXLdKKLlUs0oMLC7TFmWhw
oFl3SAtO6GvCCeOy4Wiv7xLbGaf/B0QxqP8lT/5RNpX/idH/ckT/y3H6P6nq
79H8yxlP+Q/S+DtNYuk7dRLQ+xuZlupPrPI9TmdKXw4r/Y5uF56x4FCxhKmz
PFb7n4p+JP6Dsqn8j6S1tCcHAeBuXjtIpSq5kHwLCPqhncg+UJIygVd4PwcX
ic127Mqmx4UA5cScCCAQqMKnyl/DVVSBxG4SVXOW11Wtk3OROiZA1/wImya+
8SFQaUdtdyFCRtRGK0oFlTgLQEwU2OkGiLyDs/AQzAXxZfHwloKS62sqsE1p
vCdtR4P/ZM8drveXIP4jS2H7T4RCiv+Tl/+r3H+cFIAIiWuHDcFsEP59Juxx
/KanbpOdhm5T0DUtt6yb2+uNet2yXWejrDtn435c0d0yoSe6ZVt7+3xgd/aD
TpwWbXt/+6K1bO5Ht8XkCXs03Mb1dU6zDJWnQM5T7vEUySArOKxbJsWyLOrb
JUsda/4PSIIY8f/S+M9o7T8RKqKSlREQqDS6LrGZgHFFm+AqR6WKs0mJ6LtM
uvpbiCBs6UGk5Kg4WyQo6y2Gw45qaahRgQDRj6aG6BU06Keyhh1Eyl7gBzuK
3rX5kKiIIbvvXBxs+Q4jUrDpaHrL8jsXZ/r5hAqAFVM1q6zWJ0ZK+xh49GYj
Ft7TqP9LFLHtMed/5CwM+3/UaE/lf2Liv72aO/ekEWGF5fnpPwv2S7A3zG17
P5xhbyOIz7I9xkKT6JiihVpFCYLEven7qMbmWX5H5CGSIDp0Yl+h7THiwgcE
hocbGS5Rpsa18eZ/JCBE9b+cyv8o2u2Vy6vrGyu3PXmNFf6I/DjYbdjmYyV+
u5FfdrpQvLYds7lY1ba2K1XbXWtiYl+71g76xu8SBIY2L1PuEcBS9Drb4AC5
9m0HAIgdfk5QZEhZENK2tN0UghC00DCrptU0vZN8YqLDrT6D45R/MStH5B+m
+v9Zlf8cylEleTiZhwNlHsXJ/LlDCf3iJzAnpBYNm+yMNf4nICkbtv+ltP5r
UuQ/makf3doq1IKSUEEVBCODgHLTU6t5rsV/Pda8ojDfXzMNZFQhQqIAQ2q6
dbJwnW/X9u+Kev9oBZTiEMsrV+4TrqMX3PWWgkUkPf3Vvsbe7UkKZajTi+K6
qQN24c5SZJnKleJJ01KwlOQwhTIxnYBywK+3Hn5R85OXxHCJPZ800xVtxCkN
O/0zOP+P5DD+wzT+M/L4D305M2iZQeuMCALYFUSqqF6YkSWHzMgwDu08+2p1
BlLE2iX0jXZhiTjB47VisCgXwT15ekrPcz5/spEhQPFCwtVK1YTIMukXwKPA
sBDIBoaKScM+DHTjEzUHJPmnp7hOnGomeyFuKMgC/Z12xoI5kxVqpLBL34wG
vXVpBokzSFg8ItTsC5ppaUDaDov/cMzx/2zU/6eSnOL/aOz/GVGmtvKMKPk+
gE22dce1sZ3p6w2cnrlHyVvF1DZxrIZd6jF2FzvD+wdSevCvQQQrWNUqPUVh
Pmsy0Dd3mhYS7R2IdCRWbJYbLJkGRKZtVE2H1YX1JugvDBwDCIEyoz1wTGIE
NYiCRJEL9kjssMWe4AE2dOwIfkowlBC8MJO9FCGFfnlYmDR6TOQRohDhkccf
aCebDcMYb/5fjMb/sun4/wnz/xmb8DMA8OxDP9e2L1Ersqco0J+/44DhwG2W
RAoEyFS13WpFxY5W3UFN0XLtHYBVR6OggHfVzpBgESk5Zv0d4PgPSvsFCnW6
okhvZSmy42IMVT/C6/nJjhfSzrYbtj7e8f9iJP4nS6n+H7X/Fw7gvXbbarik
MIMuhLBhBq0cydwASBQkIRc3JqzfqHsPP/rVBbRZ2XMWeWY3lCs8rhBUtHmK
DTtAyTV5DTeJXYY7fFk0pS58UKihyh8e7D3ylsa7ZcKXqRmTvOJvmMGz1A1M
25M13XQa2pj9PzEbGf8rpvnfseN/F+NbKOnVbQ3OKSgxOYWMx2cDQdFoDbs9
JA4qfZMISjo3yiD5d2vELY/V/oM99V9Z3/5L/b+RtFOUAYhNHFc3t/k1ygmW
6g2/k7JyTrl/Zu7NzIxuqoSosw89kBDuN8yG08BGZvP26sNXXIsvklNOwyav
flF3zFl3Tne/MF+y8YP9187OLyycyX9Rd+fK2CkIZ5tEt9VTZ+rY+ULTeqje
dy0r84pqEbYbr7uvLg0uP2lHdoSDyjczp2ay2TP3596cfdiKV51fuZ7/0gvc
jU36doy7yL79aisoddj7iQ1zuVaVmMLDN/0PcHbuvv8JnZk5leH9E9UaporN
UPBLo7vfYqUls7MP587cp8QzhdMffOXR9x790aM//+DtR9/74J0PvvHo+4/+
5LRnMN/3jvpQmJ17kx6ZzwSM37YcNy1bnbl3jT+VoT0wu8S+vvnw1VcWz+W/
NH/6y7/02q+8FZhGS4AQ5STuEDwQNtYhK08lexTTHQriVwhWiU3PPXNm7j7t
/vx/vfcXH/7e73/41Xc/+u33JncMzLNt/+1CSURjjf9lvfF/IfsvHf83avtv
k9p/55eS1QDqmrvdzPTL+M4JCCBJkgTalihppmToVPB7C+vo2Qr1smWSRTbU
r0SBivcCDq1jRK5moYZV1S44TjjO3o5AzAlZCbTr+IJkvafrAU2f+QVZkOOu

M1BTJGU7hu/Rzgnz+LP6HQl20i5ouOPO/wE5bP+J6fyfk+T/JZ0F84mGBeW8
gL94YG7AZ9feGaJUR9MrbBZvpHZrQSRRPKD8zbFqJNksof2FvVUZrFl2DbtR
40b0rJtznuTSnuHO1Uu1BsfGGBdOiyI6PU9/PDff3jy2529Y5vawC4AHyH82
K6NI/D/N/02Q/HtO1CrHirg4zDE6zsQ1wlkaR21/m9TIE75xddtiokHl6nTs
mN58lvZpTzG+UNgl9j5j36N87WKjQRbYJ+8k7C6H/So4ZXrn/omHcUtxL8/n
JNTpu0Hf7uhu+Ya1xS6AebQ+RuMafkDdQcO7HB+w2cUO8+doQTRUcpP4J0Kx
zYplz+MdCq8U/FMEzuDxyNH8a1+/99QN4jidWzjyDwHt3VY21Aq3Cf1xf/T/
2yynd2wFlGOVA6BjLGz6PcNfp5RH+eKZrOW5VsfzRy3SvP9ch3f8ehszeA/7
C6M4k3dPMTFAilAI9bppu1EK2EuxFaUQQhRx5wFhmuUIDVRCNKvR4/TOCMZo
Yo4jh+4p5npgNkwTcxwpRBN3PWKYJuY4oT7e4vJchCbUy7txNOF+5rjouUD4
OFEaQYk8rxiiXJQohkoe/OiFbAIaKQGNmIAGJaCBCWgSsLQABtMog0lyg0kS
dHKCPk7QxQl6OEEHJ+nfASQRr7I1cY5a6MR12o7mqIy9Ubz8W2rB9cCa2THY
lo+xZofxLBTlGO62O+wCwIHz/0Tmf5WEtP5vpP5//ERaR1Plp0BFiOQNg4X+
HR4UlgLB71aWcnC9iTTMZXqUIw7oI0FUEMzJYEKAwGg6qu7Ux5r/QzKL/7OB
3jKbDNqP/6X1XyNpR7P+ny9x52JQoDsf34Cq/zYjssIDXCypSxr1L/fjUnFZ
0GdiTgYKkb3iw/rpwn9d+R9//T8K5/8lANL5P8Yd/1/gDHswBPjCvacRXqFK
LJdD/ANFSzIrMPJnZo/k+6ReUPC4058MVLWIpbOll7zi/qZt+p9ySLSr3qCi
VvJPQNSkzIooQa2q0HfqIoiUgwwLYfSGxcGOxaQZFml7WvCfAaA7Vv9PhhH/
T07rP0aJ//H2X98ZYJ/IIczlBLEX41scqFXNHWr9UYwXEVAUrLKh37hJ0FKM
FSjkFJTLDZjvQxhkCSKlPcfrcFB+4sNHtZIx7vl/gCRnw/Vf6fwPE+X/HXoy
HTaVAkTJYMJiqzbEhY3YcKMAUPisqpVNZgJatl7GTU21MLJEW4IW0m2nu0IQ
ta+o+ddxEyOCGfFFsyBKJYUF3iV77nzdwLrJxHqDXjaZdTjT4pp4n3MtjuVD
adc0uRo29zmr5BLX4bBNOIetLuEQlREVCcd2zEyG+1nTnRp2S+VhgsDA+I8k
huRfgmn95yTGfx6rrhOJEpQOWv4lyIMVNvOgs6dqRtKp3NNgz5HIPxyf/Mve
+L8e+59+SeV/FO3Gyp21lY0rNy9OBgLAAQjQ11IPGeoHI0X/yf8GZ4TZTIWH
N+njrPmJiNHUKFMPewG4AfIPRYH5/wjK9Mkj4M3/JKX6fzRtbWV9ffmyHwCu
Nmp61Yqs/hvvAQhQpowMvAiqHI6g8mpOlkTEiypWCciqoKgWBYEQXuDbmxZs
VvAdlxIKjgILniUHqGCvqlQ+dXc/z9lSrWmT6439i7fvntfnwYZ+q7ni3EX2
ypZTnb8M7+yVtze2hFuX5PKVxvXVa+Duna1r98rXdpW1Sm6TvLFTXdsqmls7
SL5wcS4noO3du5XS+U18z9x+vfZGSblz4976xRuXLzxYntPuGMrayuaVO6v3
LOECuUqK6t35N4zta2QDg5vG7g6wXRm8LlX0da24s3a19vollxB9d7NcXbtz
d3O5EAYuzWho2v5Sbx8uBpaqij6KxZ4Rdq0DRLJsUCsCtVRSAtiKVEXMSVgF
JVHJSUpx6V5tT7hXuyddvyOU7+6DvRu65BThjXJxOZPppt1bjBHARJstqEVs
fsUsWapubrO1vExs74dhs9YwXJ3BynxN3yPqQtFiQ5/t/YKMlVKRlAAsEaJl
2cjhi5g96XXsnqUeG3ez5LJ1aCUOiHlRzEtZ7vLaxvQUGwnIL2/TE3gcqNfq
rD/mvZQ690qpYTvEeTXGe5MQQ2qej562v1eX4Ganp64Qw7CSHDmoQDxvkHdc
m7DVQxKdB7x9/PbzL535+pWv/3j6+Asnvv328Qv0p9dOHD8uvAReeP65uc9+
6sQvgJe7JMeFt49zlOQXKQn4ZVAXXgYvPf+pzU8/f/LE5rpwEnyOfXnxJOMN
XbNsU8fC58BPsR9fOPniOja5q9RJFT4LPsN+mjr5HOU03RVeBbPs+8snuXX2
ndsgjstdILara+zmCLfccMvUH3f3T7x4/FvHdk6g4ye7lzfdubzjx5879umv
fuWd/9F+cuW/b/M/+PA33vmdb33nox/93+e/rd3dKX7zP/7pzB/8ozRV/ruP
v3vuz+Y+/tnGv/yD+s7dwg8vv/KjIvfjj5bd30XTv/X5//zDf/61Dz5z/qcz
b9nf+MG77//1dzP/+1fv//1Pfm5+4cTDm+/P/utG7d/++Dv59xa1v/2bL//w
L6997Ws/8+73//3jn+d//eaHb5E//c1Hz8U9OJ5/Vr0DT1jHq/8FCILjv0Rf
/6frP40l/0s1SR2b+wnHf0JpkN3dtnfjV1uIrQjxx1t3Tf6Ok9BiVSXHlolc
CljSrV2UxPvAA5yWTk6bpafZIgT9Y5jtLZEIZpL8tzcTJptnI1khqnjQtHjZ
0GOIZNQP6bHAvkVs8KgnVErDMmNtZskYcvYnQfynZ/5PD/9BWv83HvxPsP4n
ZFj0ZPEgL7WDgllgxoc9w/qh4KWQbEmETdQpBwYJyoFRkol9e69MQk+W6OUf

Z9VP5p/0qRRGIxsqYFrUIXEsc6zr/0EYyP/IXv0HSuV/JK29/jftf+6J1/bu
MBOmUsxW9tbZ7PyKAiGbx7u7kne6ivfk6H9rlxhOaaz1/yKUQvKf1v+PPP9r
4XqmSEg9Pz/fFXqURwDAoxkGlItU+qIe6PD50K/0pYcHOxRhzKZf+Fs1uqt0
IH8JgT5jANpjMJUklV9iOifhTsNyi3i863/IohS2/+V0/c8Jsv+9+X/W7Ax3
NcOxaLyvRaOm/2ICHFBQzCKXQnAkUJslPTfgoLF9SthoT7rqpaTkJSCBBLCQ
uNATjmHly6PIEdtkGzeGnABONv97r/4X0/k/R9KGvP5vTkZQKFcgEmDuoJVt
O2zYEwNoizTFjL5r+jKF3w1O9vH9WxmqB54I57kb1k2TXDOtprNR1p31UplN
QWbV8U6D8FQOcIEVaEak/BNpGtCOL2K15I5X/lHY/wdp/mfS5P8g6Y+VfUXJ
IQQPHPTb4b4qEiXs2AbS1OLukgD8sohuNcJBC3ojKSPkKDViL9R3QF9oDfGD
Vzuir0zvikef0DJS+gTYuknjlX8pG43/pfWfT7v85waJvs94IdEPZ3X/v72j
2W3bBt8L9B2IALsEcUqRki05c9Fi2LB2a7I169JDgUKxKFv+oRxSspqctp4H
7F2G9bjtFZI3Gj9RdiXZlpN2tZNVbFLHlCjJ9Pf/+x+29nu2wtS4DvXvQBu/
Dx5SKVSu+LQtgNfq/9RckP9Jjf+3BP+XN2AhVQY2ahLp+eFqs33eVlBh/Seg
jZNBfx4ITpu2Q01IIFUKogMxw5TkCMOcuMyhmtAQTzxn6vLRGU24GHGWhP7A
lU4cLMomFKvP+/WbSSBYapTYwFjtmijuMJQQRwdMP1uH2Jg4LctpNimxDesj
zJh6p0a9beJ/U+d/ENLEoCim8n9t/9us/8/CFB0zMQ26DL3g7tQNRu7piH0Q
+l9cvPEC6Ngtk8Xyh2rptanCQlxVRhaYK72BzwbJ3EBA0mxRm5qtFqHYhEQC
I5//WSQMCtx56EqGQx+STfqcnIV+6MIb4rLEh2sJ6EoSifPGYz9iQt3CdCgm
NrXVTsErvIX7OLaSc05cwdPgXcNWtw2nTESxYGjnCUc/iLCnUFbu3E5fg/Qm
W8//blkL8T+E1vr/7bL/p0a+14tKwOraCeXY0GuUBKosBqRBNTMNQnCQp8iA
d//e426XTaIsjp+Hp6F3Prft3cApYFjVOWGFog63pQfQRzsCJBsHW67/ha1W
Tv5vZvX/mjX+b2KU878P1IfsxF+YOIecNycKK1E9FD0dDUCJSariAWZwudQf
YL/n7DPkL6HgXmFiMuzKVmMcjNkeiNF6lNKU9nITMuhxNZM7VzFwt8fUAXXl
3BtfuL0qknL789EjJj91+6/19r98/ReN/6RV+/82zf+VZMwfKdU4HAdZesMR
UohVntW4LdzRpF9E+mfuy4Z/JE7c596xgnDczDv4UjgrIHPe1Pfy/OLivEHU
aYpnI/WjBH/E4/EpE2olRzpCQJ9F23Nenk4UFHX1FMzVorgfhuhUfbXqa4On
DkN4I9KXJUzdvi5Pj3Sf1E6auHH37X8RJCBCJq7cYv2HZquE/5ZV2/+3w/8/
rP7vR1X+RTkYHAaDvukOPe6eDYYJ4550pQ+MfwWfv1ZN4PVl4EqLjr/6Sa0i
VatGrhx4fb9sH/n+GEW0Yh1xbBxzDz5R8TEPvzs8OjlEkVmxWKk72KeMLzHK
VLo/sOsEns8ZWyJ6RCKR2+b/Fi7jv0lxjf8bx3/BxmHEGmo/esuFfoQq+7Gv
gHhQ1bGT9wWsvFHR/DcKFUlpCCbDWHTZMsLimMTBdr7aQQrPYdCNqelYNoQQ
Mx8iiPsCGpqLtYSEUNvJBxcv72Xy/4kYjvlQdseflgKslf9NWsb/Zo3/m8X/
kt1Mx8S1ozCCpnk6NK6rAX8T2QAZVPI6G2AT+D8mW8Z/Ssr4b5Fa/78l/n/A
8kCe8raSXWnLIXaLzrl0P4ogYShJkv1lYr9CzDJWp7CWqv/980mfcTdiXqNc
xvE9MzYdnHfwL3Lj1QUnjOtEAn4JzcHaT8M+f308DqL+w8+tWmTMt57/a2Cj
7P+zDFrXf9vImEn2BGPUQWR3l6JdZO3uEnT51+Xf6OrXq7fq5fLPy3eXf1z9
DnOlqau3V7+hBrr85+qX2bHLd1U2cccu4aRBiemQIqHIgBKaAQ2B6Q/pgDCR
MM+Xj48rUolXBiMahm43skJqYV6sXZAEwhMWXX7XSwlaFsbj2AsZxjdLE3Ls
lXlCcOj2tRSsxx0aiQz4dLvxH0bLMsrxH0oArOn/hv0/02DKhr1H3b4biIbH
RbegNGXdvtPe3Dnh8Ai1799bvxwdIIQUgQVnakcRMMOGf5Ty+/d8AZ1GUBvt
PEXPQ8n4KRM99OrVq52dzPuqs009AQcfLcREwn9w5Q6CIl8Dz17jidIQv8QJ
VaT66SOlsR5dmVaewdiBW+XiSLK20gg9UCen24GA1Wm38VwOnXE76mCZiZ8S
Nu2QJd+4vDdi3rfM9SDEDCHOEl/PoayXLgKtO+Cxmlk8mLWq1+tPlPj6gscy
dkc/w+E2OjjY21O/B2t5l664qm6W7rTUYYCy8PWPxAwCEnWfjm42P+sAz0Pd
qf1h2oZ9tiepwfABAh0chpwEwO4KUJF9fXqHADIQyoQCJxgObITABz/fYn1F
9SfIE+kGG017n1jWvuLucK3sQh21aBaJDBF6igO2d36MQ6VqIBmJgCvw2gHw
WglY6lJqtzWsd2ZhAGom/ZT6mSXYQzx9ygE6U8+O9ym9MXtfWQPI3Axrv2AK
/fwt6/8EL9r/av3/Dvn/qix9vb70TCNHgDOQG4Apb+TzMQnJyKTCirE29xVM

e5QYFZ69a/V4AitCULYd4Lr0Rz3qUY/PfPwLcaRGXQDwAAA=
-- END MESSAGE ARCHIVE --

Authors' Addresses

Robert J. Sparks (editor)
Estacado Systems

Email: RjS@estacado.net

Alan Hawrylyshen
Ditech Communications Corp.
602 - 11 Ave SW
Suite 310
Calgary, Alberta T2R 1J8
Canada

Phone: +1 403 561 7313
Email: ahawrylyshen@ditechcom.com

Alan Johnston
Tello Corporation
999 Baker Way, Suite 250
San Mateo, CA 94404

Email: ajohnston@tello.com

Jonathan Rosenberg
Cisco Systems
600 Lanidex Plaza
Parsippany, NJ 07052

Phone: +1 973 952 5000
Email: jdrosen@cisco.com
URI: http://www.jdrosen.net

Henning Schulzrinne
Columbia University
Department of Computer Science
450 Computer Science Building
New York, NY 10027
US

Phone: +1 212 939 7042
Email: hgs@cs.columbia.edu
URI: http://www.cs.columbia.edu

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM 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.

Copyright Statement

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

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