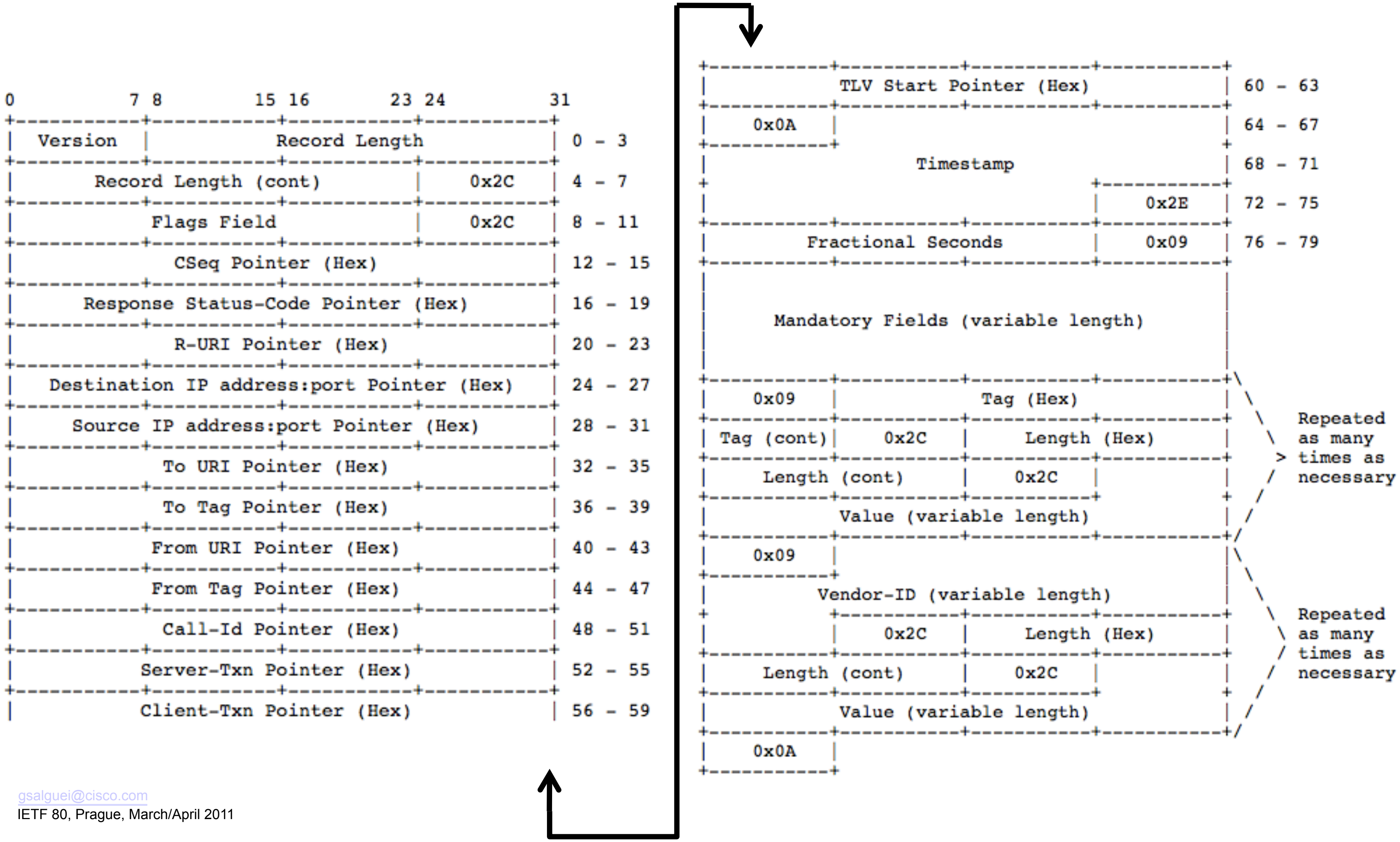
Format for the Session Initiation Protocol (SIP) Common Log Format (CLF)

draft-ietf-sipclf-format-01
(G. Salgueiro, V. Gurbani, and A. B. Roach)

Presenter: Vijay Gurbani
IETF 80, Prague, Czech Republic
April 1, 2011

Current CLF Format

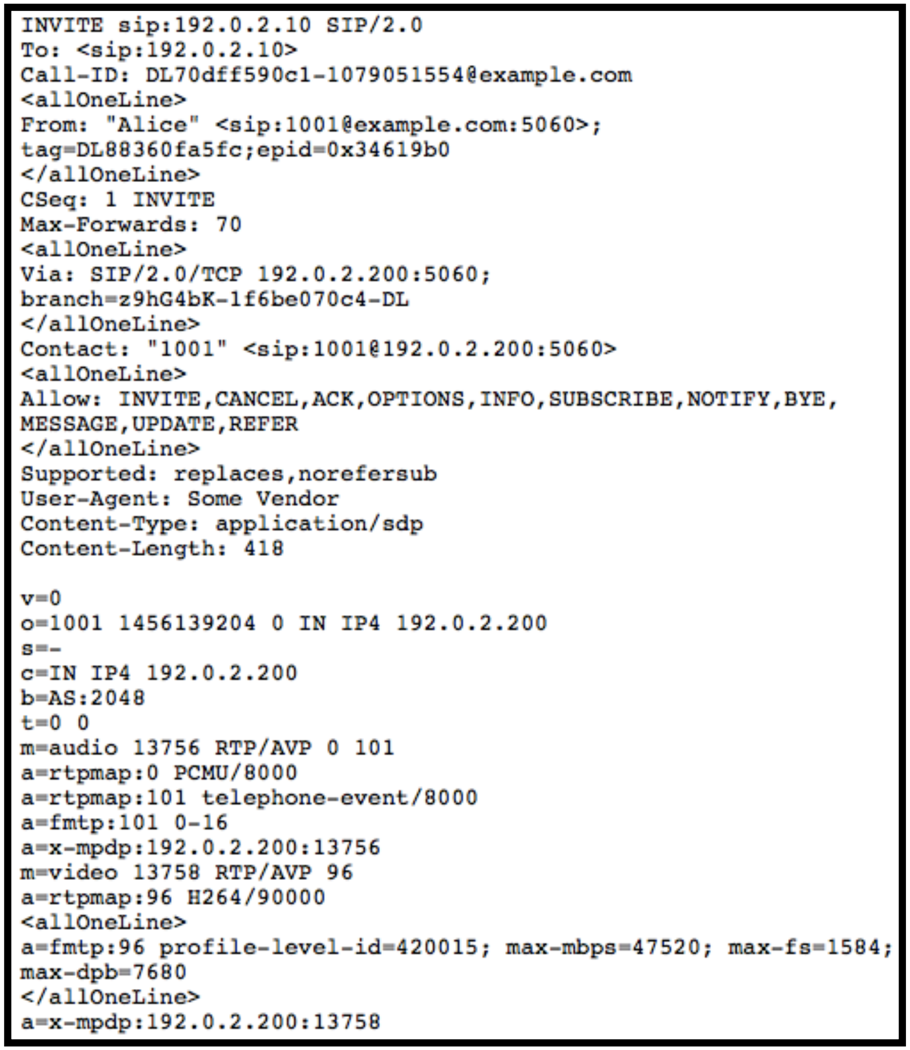


```
 0           7 8          15 16         23 24          31
+-----------+-----------+-----------+-----------+
| Version   |         Record Length             | 0 - 3
+-----------+-----------+-----------+-----------+
|       Record Length (cont)        |   0x2C    | 4 - 7
+-----------+-----------+-----------+-----------+
|           Flags Field             |   0x2C    | 8 - 11
+-----------+-----------+-----------+-----------+
|             CSeq Pointer (Hex)                | 12 - 15
+-----------+-----------+-----------+-----------+
|     Response Status-Code Pointer (Hex)        | 16 - 19
+-----------+-----------+-----------+-----------+
|             R-URI Pointer (Hex)               | 20 - 23
+-----------+-----------+-----------+-----------+
|  Destination IP address:port Pointer (Hex)    | 24 - 27
+-----------+-----------+-----------+-----------+
|    Source IP address:port Pointer (Hex)       | 28 - 31
+-----------+-----------+-----------+-----------+
|            To URI Pointer (Hex)               | 32 - 35
+-----------+-----------+-----------+-----------+
|            To Tag Pointer (Hex)               | 36 - 39
+-----------+-----------+-----------+-----------+
|           From URI Pointer (Hex)              | 40 - 43
+-----------+-----------+-----------+-----------+
|           From Tag Pointer (Hex)              | 44 - 47
+-----------+-----------+-----------+-----------+
|            Call-Id Pointer (Hex)              | 48 - 51
+-----------+-----------+-----------+-----------+
|          Server-Txn Pointer (Hex)             | 52 - 55
+-----------+-----------+-----------+-----------+
|          Client-Txn Pointer (Hex)             | 56 - 59
```

```
+-----------+-----------+-----------+-----------+
|            TLV Start Pointer (Hex)            | 60 - 63
+-----------+-----------+-----------+-----------+
|   0x0A    |                                   | 64 - 67
+-----------+                                   +
|                   Timestamp                   | 68 - 71
+                                   +-----------+
|                                   |   0x2E    | 72 - 75
+-----------+-----------+-----------+-----------+
|       Fractional Seconds          |   0x09    | 76 - 79
+-----------+-----------+-----------+-----------+
|                                               |
|                                               |
|      Mandatory Fields (variable length)       |
|                                               |
|                                               |
+-----------+-----------+-----------+-----------+\
|   0x09    |           Tag (Hex)               | \
+-----------+-----------+-----------+-----------+  \   Repeated
| Tag (cont)|   0x2C    |     Length (Hex)      |   \  as many
+-----------+-----------+-----------+-----------+    > times as
|    Length (cont)      |   0x2C    |           |   /  necessary
+-----------+-----------+-----------+           +  /
|            Value (variable length)            | /
+-----------+-----------+-----------+-----------+/
|   0x09    |                                   |\
+-----------+                                   | \
|          Vendor-ID (variable length)          |  \
+           +-----------+-----------+-----------+   \  Repeated
|           |   0x2C    |     Length (Hex)      |    \ as many
+-----------+-----------+-----------+-----------+    / times as
|    Length (cont)      |   0x2C    |           |   /  necessary
+-----------+-----------+-----------+           +  /
|            Value (variable length)            | /
+-----------+-----------+-----------+-----------+/
|   0x0A    |
+-----------+
```

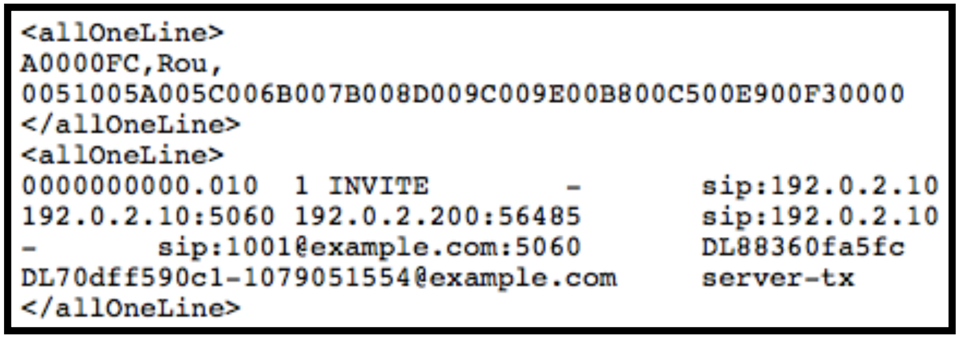
Sample CLF Record

- Example:



```
INVITE sip:192.0.2.10 SIP/2.0
To: <sip:192.0.2.10>
Call-ID: DL70dff590c1-1079051554@example.com
<allOneLine>
From: "Alice" <sip:1001@example.com:5060>;
tag=DL88360fa5fc;epid=0x34619b0
</allOneLine>
CSeq: 1 INVITE
Max-Forwards: 70
<allOneLine>
Via: SIP/2.0/TCP 192.0.2.200:5060;
branch=z9hG4bK-1f6be070c4-DL
</allOneLine>
Contact: "1001" <sip:1001@192.0.2.200:5060>
<allOneLine>
Allow: INVITE,CANCEL,ACK,OPTIONS,INFO,SUBSCRIBE,NOTIFY,BYE,
MESSAGE,UPDATE,REFER
</allOneLine>
Supported: replaces,norefersub
User-Agent: Some Vendor
Content-Type: application/sdp
Content-Length: 418

v=0
o=1001 1456139204 0 IN IP4 192.0.2.200
s=-
c=IN IP4 192.0.2.200
b=AS:2048
t=0 0
m=audio 13756 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=x-mpdp:192.0.2.200:13756
m=video 13758 RTP/AVP 96
a=rtpmap:96 H264/90000
<allOneLine>
a=fmtp:96 profile-level-id=420015; max-mbps=47520; max-fs=1584;
max-dpb=7680
</allOneLine>
a=x-mpdp:192.0.2.200:13758
```



```
<allOneLine>
A0000FC,Rou,
0051005A005C006B007B008D009C009E00B800C500E900F30000
</allOneLine>
<allOneLine>
0000000000.010  1 INVITE        -       sip:192.0.2.10
192.0.2.10:5060 192.0.2.200:56485       sip:192.0.2.10
-       sip:1001@example.com:5060       DL88360fa5fc
DL70dff590c1-1079051554@example.com     server-tx
</allOneLine>
```

Major Changes Since IETF 79

- Three versions released since then:
  1. draft-salgueiro-sipclf-indexed-ascii-03
  2. draft-ietf-sipclf-format-00
  3. draft-ietf-sipclf-format-01
- Introduced the <allOneLine/> notation from RFC 4475 to better represent within the confines of I-D formatting the long lines seen in a SIP CLF record.

Major Changes Since IETF 79

- To improve document organization and simplify syntax discussion, the SIP CLF record format is logically subdivided into three component parts:

    1) <IndexPointers>
    2) <MandatoryFields>
    3) <OptionalFields>

- Changed all the ip addresses and DNS names to be documentation friendly.

Major Changes Since IETF 79

- Introduced mechanism for treatment of empty and unparsable fields (both how they are represented and escaped).

- Logging of optional fields is now divided into two sections:

  1) Pre-Defined Optional Fields
  2) Vendor-Specific Optional Fields

Major Changes Since IETF 79

- Added an additional tag to the pre-defined optional fields to log message bodies
- Added text about what body types we will log and the mechanism to do so
- Added an example of an optionally logged body

Major Changes Since IETF 79

- Added the section on logging vendor-specific optional fields
- Introduced the notion of a Vendor-ID and defined its syntax (based on Syslog SD-ID format)
- Fixed minor issues raised on SIPCLF list
- Very extensive formatting changes

Open Issues

- Proposal #1: If there are no optional fields the <TLV Start Pointer> points to the terminating line-feed (0x0A) at the end of the record instead of being set to 0x0000. This is intended to simplify length calculation for final mandatory element (i.e. client-txn).

Open Issues

Proposal #2: Move the Flag Field from the <IndexPointers> to <MandatoryFields>. This is to ensure that <IndexPointers> is purely meta-data and can be ignored if desired. This maintains all the real “data” on the second line of the record.

Open Issues

- Proposal #3: Separate protocol and send/ receive from the current Sent/Received Flag.

Current (1 Byte)

u = received UDP message
t = received TCP message
l = received TLS message
U = sent UDP message
T = sent TCP message
L = sent TLS message

Proposed (2 Bytes)

Sent/Received:	S = sent message
	R = received message
Transport Protocol:	U = UDP
	T = TCP
	S = SCTP
	L = TLS

- Question: Do we separate encryption from plain text (i.e. another byte)?

Open Issues

- Proposal #4: Both IPv4 and IPv6 address:port SHALL be logged with the syntax:

[address]:port

This square bracket notation is the recommended format [RFC 5952] for IPv6 address and port and is perfectly suitable for IPv4.

Open Issues

- Proposal #5: Currently there are two formats to log pre-defined and vendor-specified optional fields. This should be simplified:

1) A single TLV format for both pre-defined and vendor-specified optional fields

2) This single format is still syslog-like using tag@PEN format for the "Tag" in the TLV. PEN=0 used if it is not a vendor-specified optional field.

Open Issues

- If an optional field occurs more than once in a SIP message (e.g. Contact), how should this be logged? As several optional fields with the same tag? Or as a single concatenated value?

Preference: multiple TLVs with the same tag

Open Issues

- Do we specify that pre-defined optional fields MUST be logged in ascending tag order? Or allow any order?

- If pre-defined optional fields exist MUST they be logged before the vendor-specified optional fields as shown in the format diagram? Or allow any order?

Open Issues

- Need to make a final determination of what other fields we think could be useful and need to be added to the list of pre-defined optional fields (e.g. Reason-Phrase, Refer, History-Info, Session-ID, etc.). This might become a bit of a long list that could virtually include all fields in a SIP message. Is this the desired purpose or does it become counter-productive and unwieldy to sweep everything in as a pre-defined optional field?

Thanks!