SIP ADVENTURES

ABOUT ANDREW

A unified communications blog by Andrew Prokop

UNDERSTANDING SESSION DESCRIPTION PROTOCOL (SDP)

September 30, 2013 · *by* Andrew Prokop · *in SIP* · *42 Comments*

It's impossible to truly understand SIP without understanding its cousin, Session Description Protocol (SDP). While SIP deals with establishing, modifying, and tearing down sessions, SDP is solely concerned with the media within those sessions. That SIP would relegate media to another protocol is not accidental. The creators of SIP set out to make it media agnostic and this separation of church and state reinforces that. SIP does what it does best and leaves media to SDP.

So, what is SDP? Well, it's exactly what its name says it is. It's a protocol that describes the media of a session. It is important to realize that it doesn't negotiate the media. It isn't used by SIP clients to go back and forth asking "can you do this?" before finally settling on a common media protocol like G.711. Instead, one party tells the other party, "here are all the media types I can support — pick one and use it."

SDP is comprised of a series of <character>=<value> lines, where <character> is a single case-sensitive alphabetic character and <value> is structured text.

SDP consists of three main sections – session, timing, and media descriptions. Each message may contain multiple timing and media descriptions, but only one session description.

The definition of those sections and their possible contents are as follows. It's important to know that not every character/value may

Follow me on Twitter at @ajprokop
Email me at ajprokop@gmail.com

TOP POSTS & PAGES

 Understanding

be present in an SDP message.

Session description

v= (protocol version number, currently only 0)

o= (originator and session identifier : username, id, version number, network address)

s= (session name : mandatory with at least one UTF-8-encoded character)

i=* (session title or short information)

u=* (URI of description)

e=* (zero or more email address with optio

p=* (zero or more phone number with opti

c=* (connection information—not require

b=* (zero or more bandwidth information

One or more Time descriptions ("t=" and "r=" lines; see below)

z=* (time zone adjustments)

k=* (encryption key)

a=* (zero or more session attribute lines)

Zero or more Media descriptions (each one starting by an "m=" line; see below)

Time description (mandatory)

t= (time the session is active)

r=* (zero or more repeat times)

Media description (if present)

m= (media name and transport address)

Session Description Protocol (SDP)


Understanding SIP Timers Part I


Understanding SIP Timers Part II


Understanding SIP Re-INVITE


Understanding SIP CANCEL


Understanding the SIP Via Header


An Introduction to the SIP Diversion Header


SIP Media Management: Early Offer vs. Late Offer


Understanding SIP Authentication


Understanding the SIP OPTIONS Request

ARCHIVES

- October 2015
- September 2015
- August 2015

i=* (media title or information field)

c=* (connection information — optional if included at session level)

b=* (zero or more bandwidth information lines)

k=* (encryption key)

a=* (zero or more media attribute lines — overriding the Session attribute lines)

For Example

The following is an example of an actual SDP message.

v=0

o=Andrew 2890844526 2890844526 IN IP4 10.120.42.3

s= SDP Blog

c=IN IP4 10.120.42.3

t=0 0

m=audio 49170 RTP/AVP 0 8 97

a=rtpmap:0 PCMU/8000

a=rtpmap:8 PCMA/8000

a=rtpmap:97 iLBC/8000

m=video 51372 RTP/AVP 31 32

a=rtpmap:31 H261/90000

Unless you've been working with SIP and SDP for a while, this probably looks pretty undecipherable. However, it's really not that bad if you know what to look for and what you can safely ignore. This is what I pay attention to in an SDP message.

c= This will tell me the IP address where the media will come from and where it should be sent to.

- July 2015
- June 2015
- May 2015
- April 2015
- March 2015
- February 2015
- January 2015
- December 2014
- November 2014
- October 2014
- September 2014
- August 2014
- July 2014
- June 2014
- May 2014
- April 2014
- March 2014
- February 2014
- January 2014
- December 2013
- November 2013
- October 2013
- September 2013
- August 2013
- July 2013
- June 2013

CATEGORIES

- 9-1-1
- AudioCodes
- Avaya
- Blogging
- Call Recording
- CEBP
- Cloud Communications
- Codec

m= There will be a media line for each media type. For example, if your client can support real-time audio there will be an m= audio line. If your client can support real-time video there will be a separate m=video line. Each media line indicates the number the codecs that will be defined in attribute lines.

a= There will be an attribute line for each codec advertised in the media line.

Looking at the example above I immediately see this.

The client will use IP version 4 with an address of 10.120.42.3. It can support three audio codecs and one video codec. The audio codecs are G.711 uLaw (PCMU), G.711 aLaw (PCMA), and iLBC. The audio codecs will use port 49170 and all have a sample rate of 8000 Hz. The video codec is H.261 on port 51327. 99.9% of the time I can safely ignore any of the other SDP values that might be present.

After receiving a SIP message with the above SDP in the message body, the recipient will respond with SDP of its own identifying its IP address, ports, and codec values. The recipient will also pick from the list of the sender's codecs which ones it will use and potentially start real-time media flows. The unwritten rule of SDP is that if possible you use the first codec of a type listed, but you don't have to. If the sender says he can do something, he had better be prepared to handle media of that type no matter in what order it was listed.

I hope this helps makes sense of what might be seen as a difficult subject. If possible, take some Wireshark traces of a few SIP calls and see if you can figure out how media is being described and used.

By the way, this is the 50th article I've written for this blog. Congratulations to me.

- Collaboration Environment
- Contact Center
- ENUM
- Flowroute
- FoIP
- History
- IAUG
- Interoperability
- IPv6
- Microsoft Lync
- Mobility
- Networking
- Nortel
- PPM
- Presence
- Privacy
- Real-Time Protocol
- RFC 2833
- RFC 3833
- RFC 4733
- RTP
- Security
- Session Border Controller
- Session Management
- SIP
- SIP Trunks
- SIPREC
- Social Media
- Toll-Free
- TR/87
- traceSM
- Unified Communications
- Video
- Virtual
- Voice Mail