Implementation Lessons using WebRTC in Asterisk

Astricon, October 2013

Moisés Silva <moy@sangoma.com>
Manager, Software Engineering

Hiastar.com
星昊通科技

Sangoma 中国总代理

SANGOMA

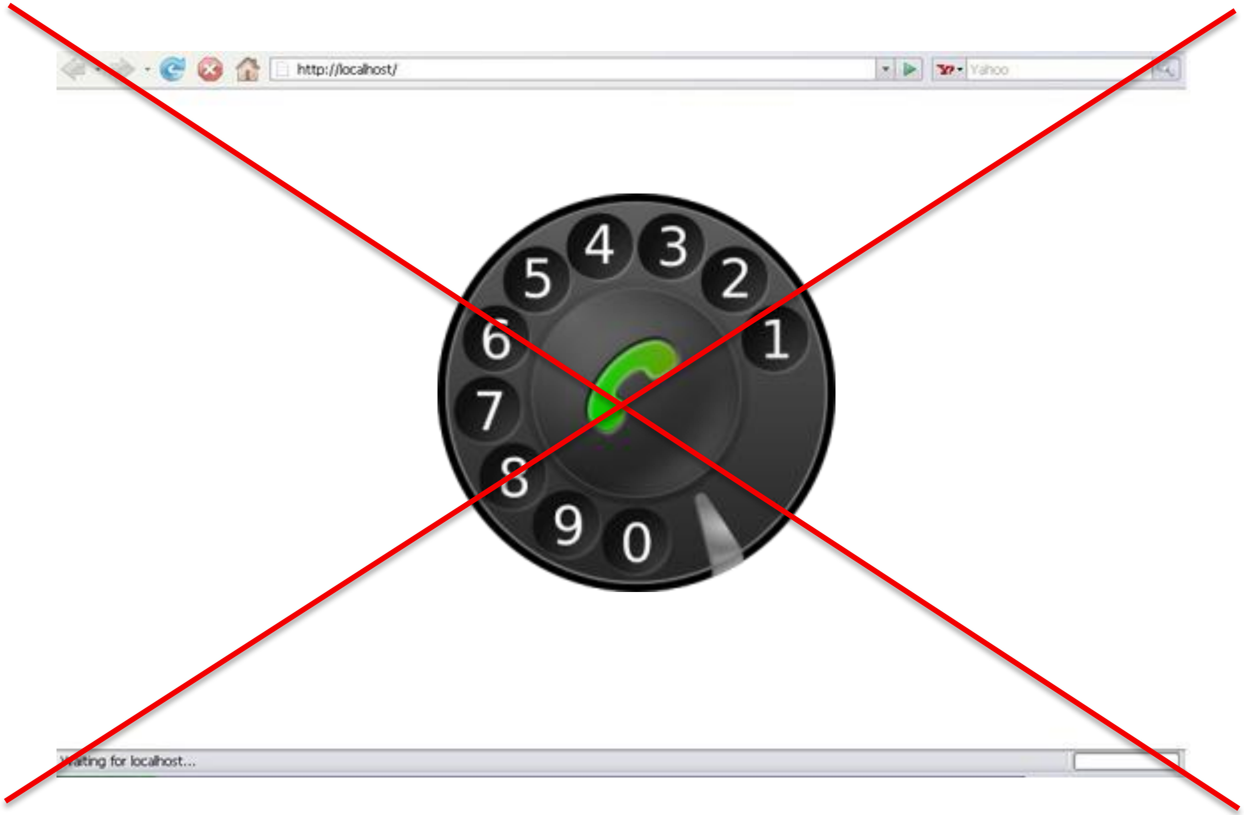
CONNECT WITH SANGOMA

Agenda

- WebRTC Intro
- WebRTC Asterisk Architecture
- Install & Config
- Troubleshooting

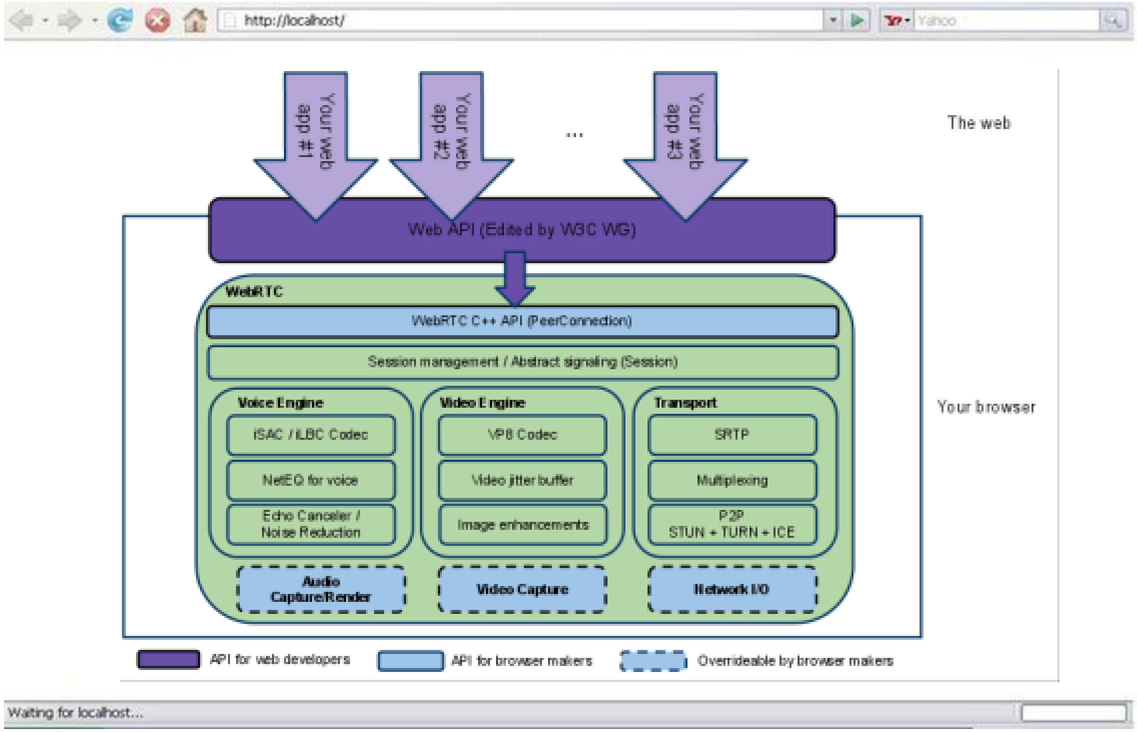
WebRTC Intro

- It is not a phone in the browser!



WebRTC Intro

- It is a full RTC engine in the browser!



Your web app #1

Your web app #2

...

Your web app #3

The web

Web API (Edited by W3C WG)

WebRTC

WebRTC C++ API (PeerConnection)

Session management / Abstract signaling (Session)

Voice Engine

iSAC / iLBC Codec

NetEQ for voice

Echo Canceler / Noise Reduction

Video Engine

VP8 Codec

Video jitter buffer

Image enhancements

Transport

SRTP

Multiplexing

P2P STUN + TURN + ICE

Audio Capture/Render

Video Capture

Network I/O

Your browser

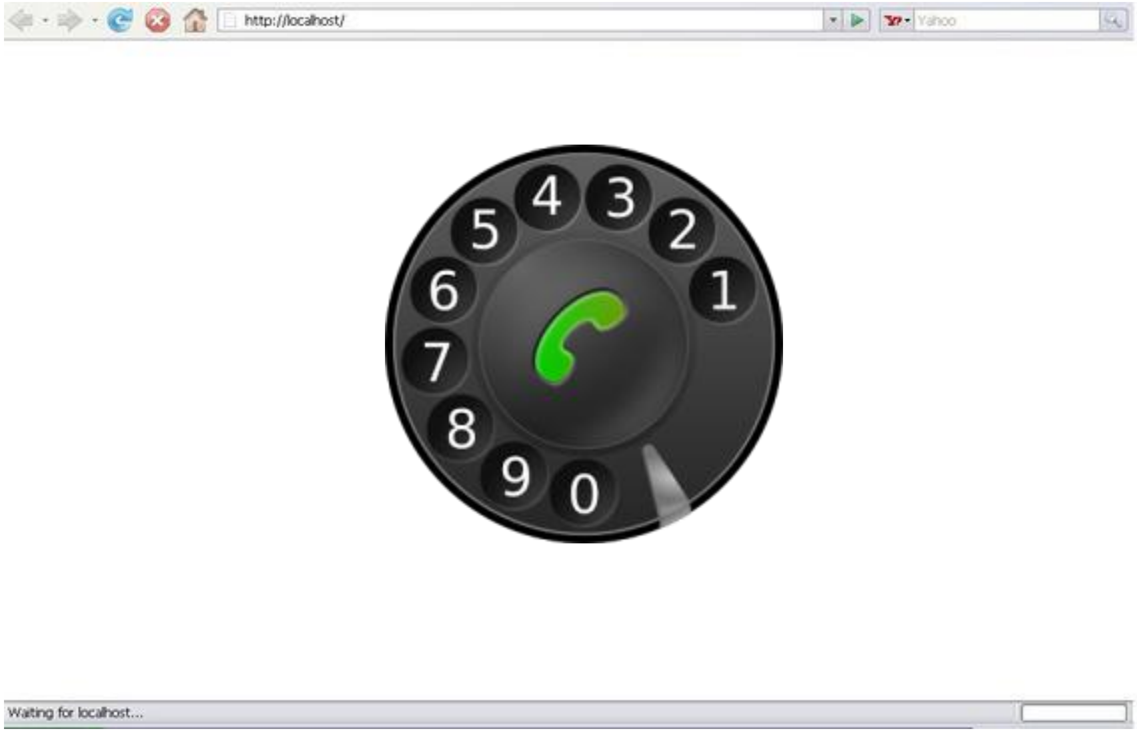
🟪 API for web developers

🟦 API for browser makers

▭ Overrideable by browser makers

WebRTC Intro

- Yes, it can be used for a phone in the browser ☺



http://localhost/

Waiting for localhost...

WebRTC Intro

- Full media engine API in the web browser
- No “call” or “session” signaling defined
- Generic data interchange between browsers, peer to peer
- State of the art NAT traversal techniques

WebRTC Intro

- WebRTC comes with multiple APIs, ie:
    - Peer-to-Peer Connections (RTCPeerConnection)
    - Peer-to-Peer Data API (RTCDataChannel)
    - Statistics (RTCStats)
    - Media Stream (getUserMedia)

WebRTC Intro

- WebRTC uses established protocols:
  - SRTP/SRTCP for media exchange (secure RTP)
  - SDP (its use is controversial and currently challenged)
  - ICE, STUN, TURN for NAT Traversal
  - DTLS for key exchange
  - G.711, Opus, VP8/H.264 etc; for voice and video

WebRTC Intro

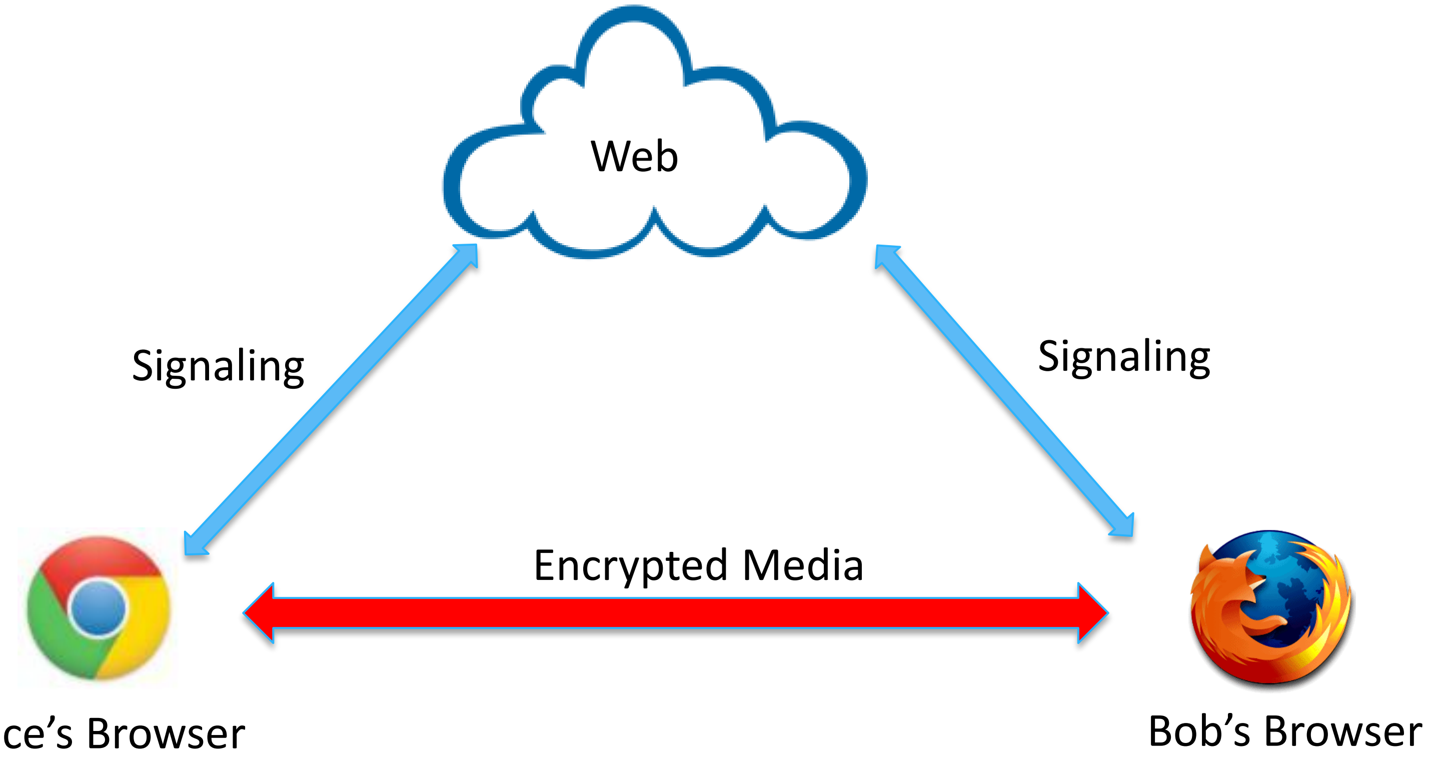
- What signaling to use is up to you:
  - SIP
  - XMPP/Jingle
  - RESTful API (json)
  - OpenPeer ….

WebRTC Intro

- Applications
  - A phone, video calls, conferencing etc!
  - Video games
  - P2P Video Streaming (Chromecast)
  - Motion-detecting Baby Monitor (https://github.com/webrtcHacks/webrtc_baby_monitor)

WebRTC Intro

- WebRTC Web Triangle



Web

Signaling

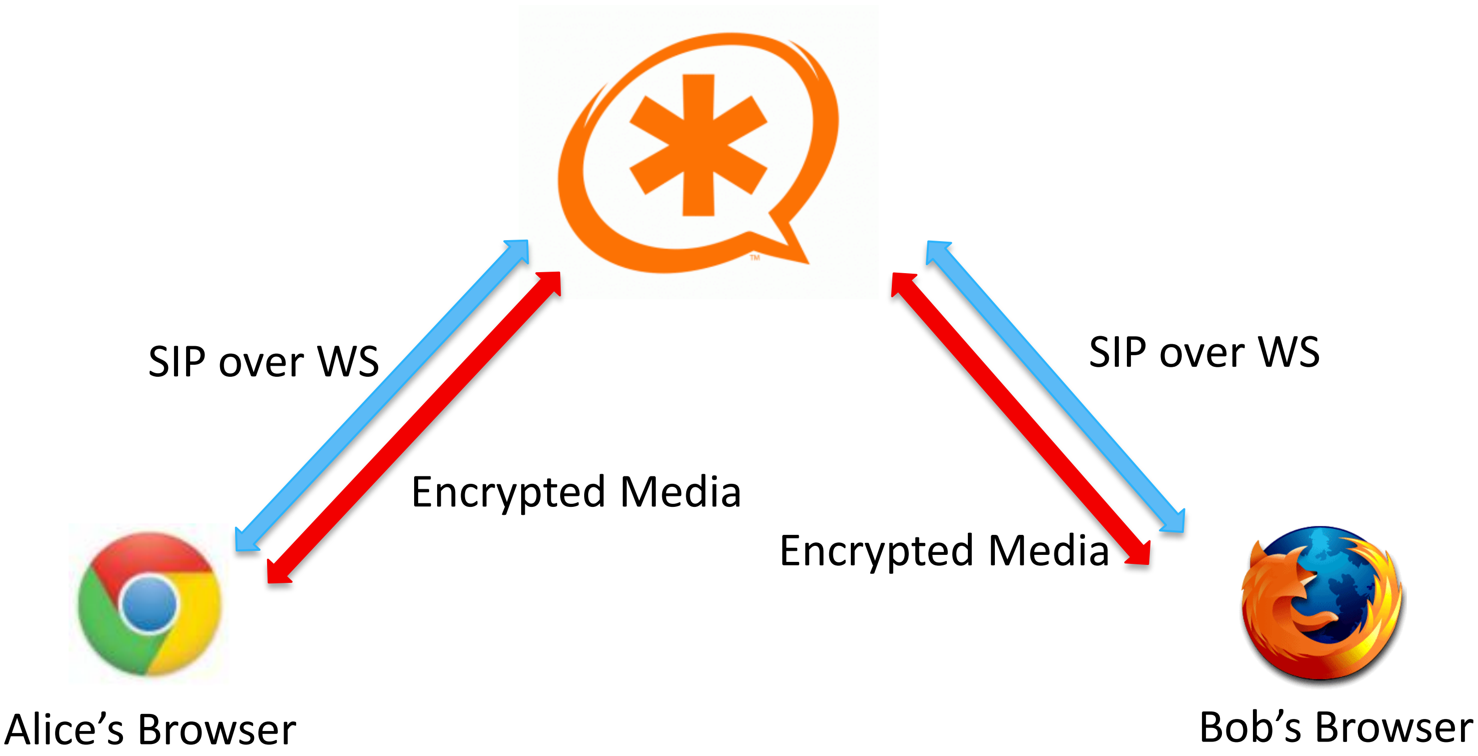
Signaling

Encrypted Media

Alice’s Browser

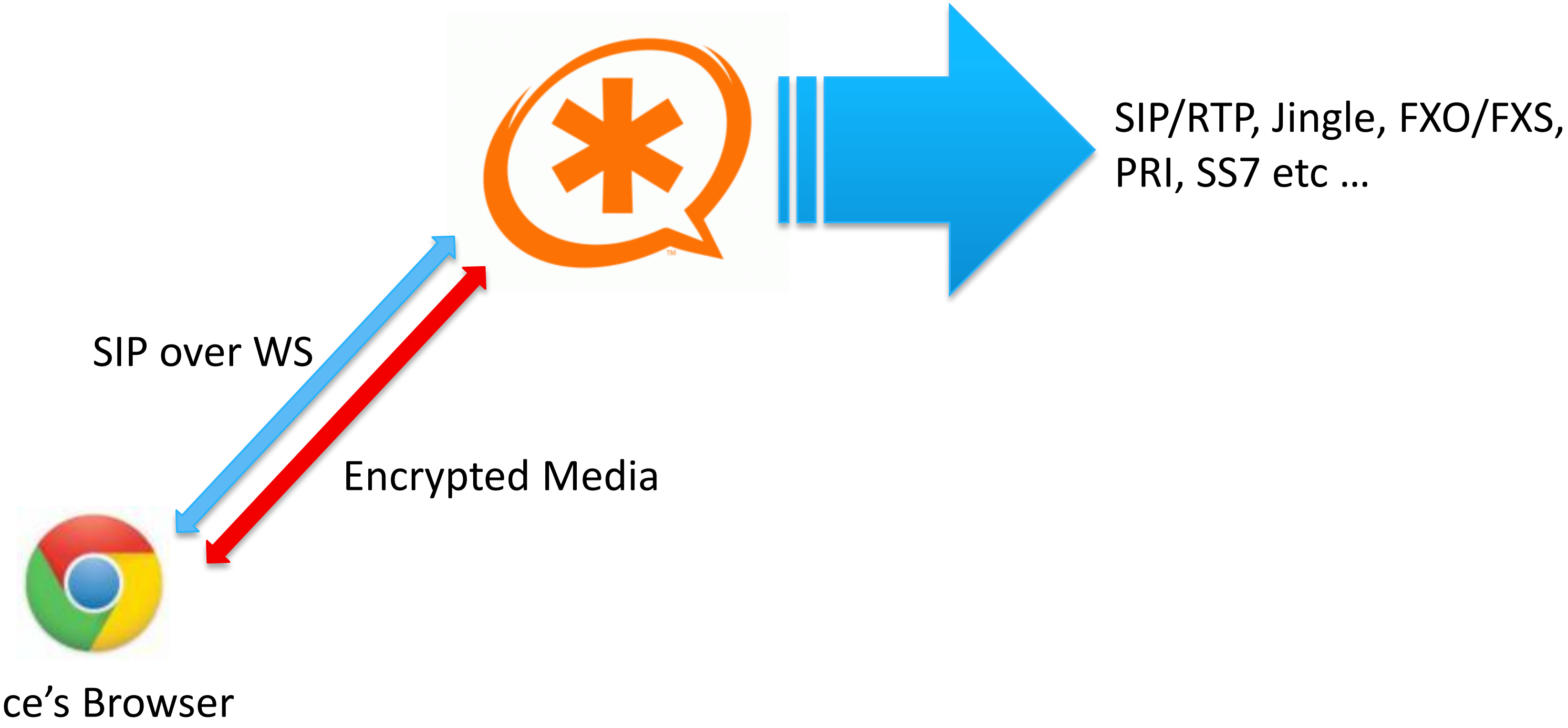
Bob’s Browser

WebRTC in Asterisk

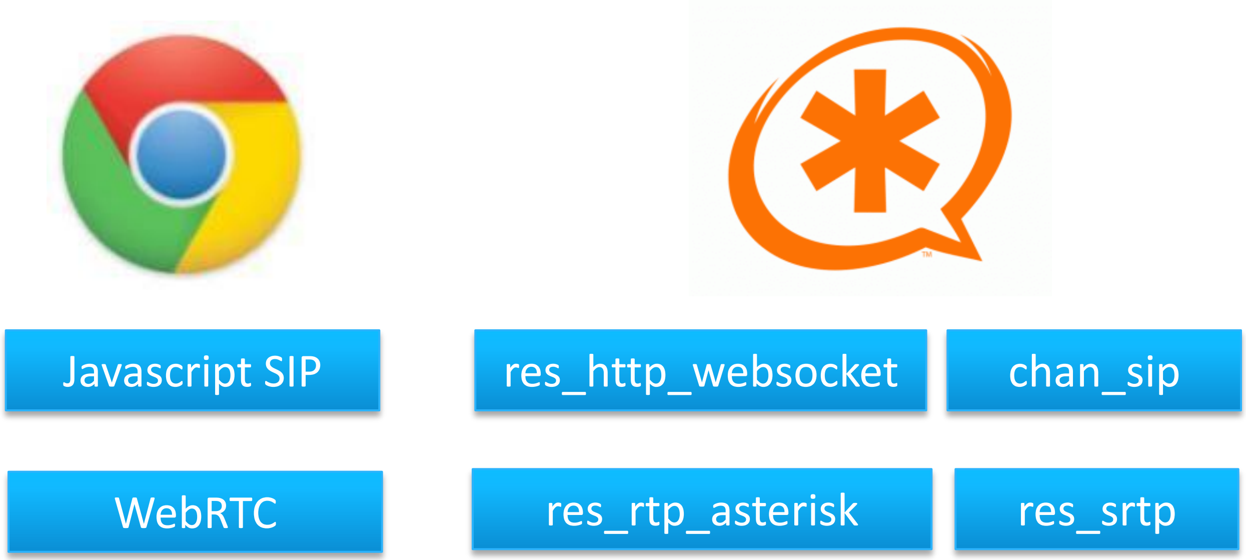


WebRTC in Asterisk

- WebRTC Gateway



WebRTC in Asterisk



Javascript SIP

WebRTC

res_http_websocket

chan_sip

res_rtp_asterisk

res_srtp

WebRTC in Asterisk

sipml5

Chrome 30

Asterisk 11

Installing WebRTC Support

- Make sure you have:
  - libuuid-devel (required by res_rtp_asterisk)
  - OpenSSL w/ DTLS support (1.0.1e has SSL_CTX_set_tlsext_use_srtp)
  - libsrtp-devel

Installing WebRTC Support

- Easy usual steps …
  - ./configure
  - make menuselect:
    - res_http_websocket
    - res_rtp_asterisk
  - make install

Configuring WebRTC Support

- Enable the websockets server (http.conf)
  - enabled=yes
  - bindaddr=0.0.0.0
  - bindport=8088

Configuring WebRTC Support

- Good idea to use secure websockets (http.conf)
  - tlsenable=yes
  - tlsbindaddr=0.0.0.0:8089
  - tlscertfile=localhost.crt
  - tlsprivatekey=localhost.key

Configuring WebRTC Support

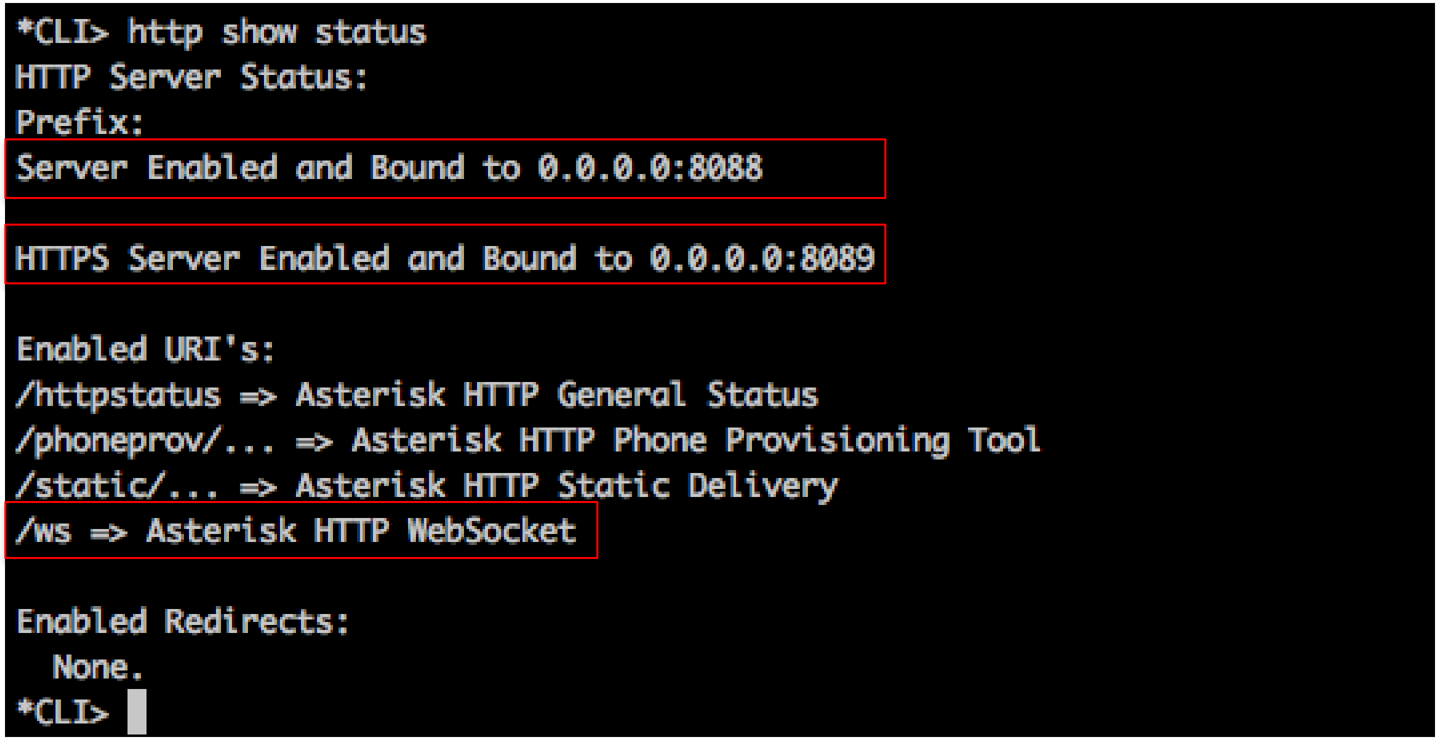
- But … Asterisk currently seems to have issues with secure WebSockets, patches available to fix them

  - https://issues.asterisk.org/jira/browse/ASTERISK-21930

  - http://svnview.digium.com/svn/asterisk/team/moy/webrtc-11/

Configuring WebRTC Support

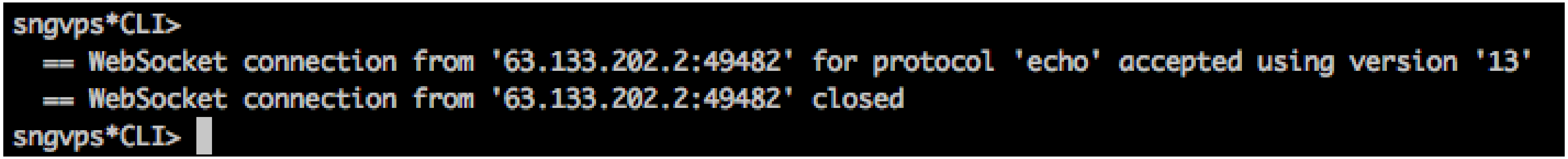
- Verify the HTTP server status



```
*CLI> http show status
HTTP Server Status:
Prefix:
Server Enabled and Bound to 0.0.0.0:8088

HTTPS Server Enabled and Bound to 0.0.0.0:8089

Enabled URI's:
/httpstatus => Asterisk HTTP General Status
/phoneprov/... => Asterisk HTTP Phone Provisioning Tool
/static/... => Asterisk HTTP Static Delivery
/ws => Asterisk HTTP WebSocket

Enabled Redirects:
  None.
*CLI>
```

Configuring WebRTC Support

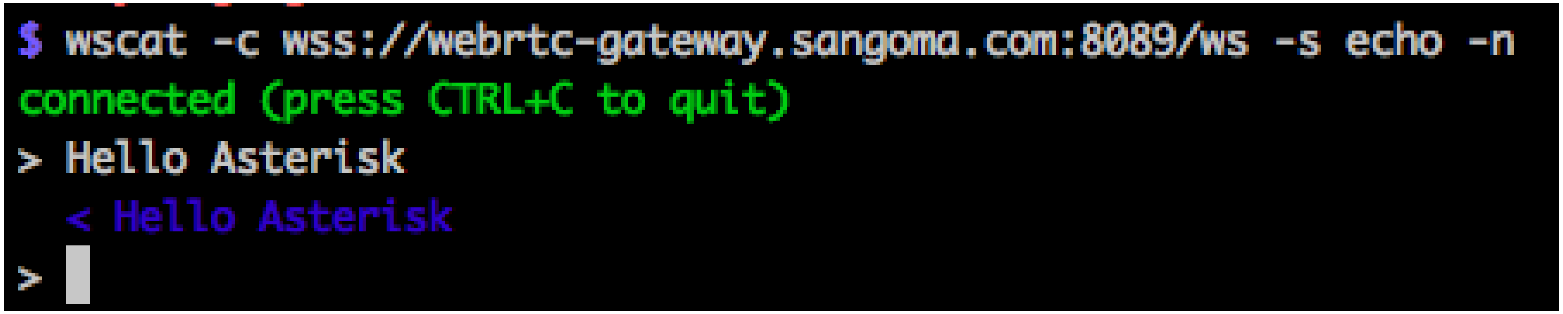
- Test websockets connectivity
  - npm install –g ws
  - wscat –s echo –c ws://<host>:<port>/ws
    wscat –s echo –c wss://<host>:<port>/ws



```
sngvps*CLI>
  == WebSocket connection from '63.133.202.2:49482' for protocol 'echo' accepted using version '13'
  == WebSocket connection from '63.133.202.2:49482' closed
sngvps*CLI>
```

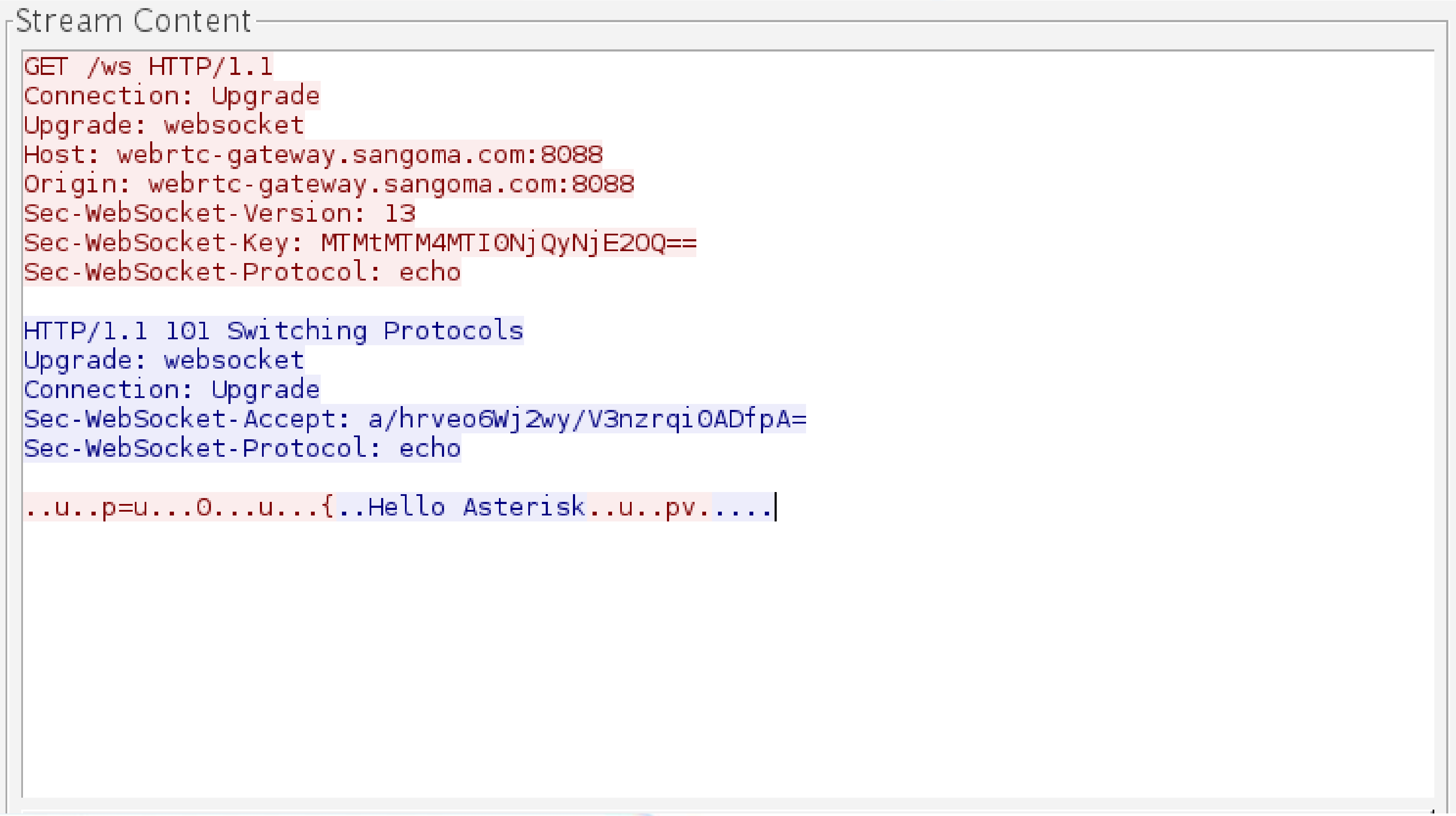
Configuring WebRTC Support

- Test websockets connectivity



```
$ wscat -c wss://webrtc-gateway.sangoma.com:8089/ws -s echo -n
connected (press CTRL+C to quit)
> Hello Asterisk
  < Hello Asterisk
> 
```

Configuring WebRTC Support



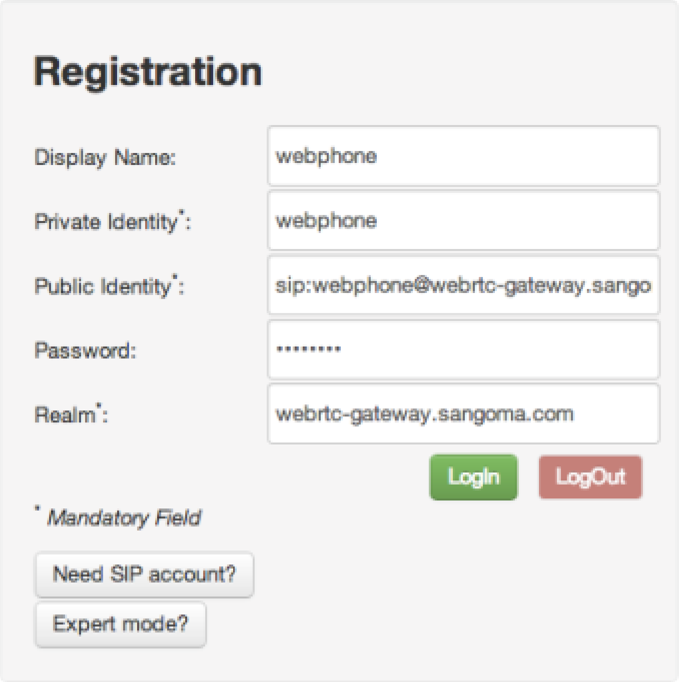
```
GET /ws HTTP/1.1
Connection: Upgrade
Upgrade: websocket
Host: webrtc-gateway.sangoma.com:8088
Origin: webrtc-gateway.sangoma.com:8088
Sec-WebSocket-Version: 13
Sec-WebSocket-Key: MTMtMTM4MTI0NjQyNjE2OQ==
Sec-WebSocket-Protocol: echo

HTTP/1.1 101 Switching Protocols
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Accept: a/hrveo6Wj2wy/V3nzrqi0ADfpA=
Sec-WebSocket-Protocol: echo

..u..p=u...0...u...{..Hello Asterisk..u..pv.....
```

Configuring WebRTC Support

- Enable SIP over websockets (sip.conf)
  - transport=ws,wss
  - Make sure you use the /ws URL when connecting from JavaScript
  - Create a SIP account to receive ws/wss calls

Configuring WebRTC Support

- Testing using sipml5.org/call.htm



Registration

Display Name: webphone

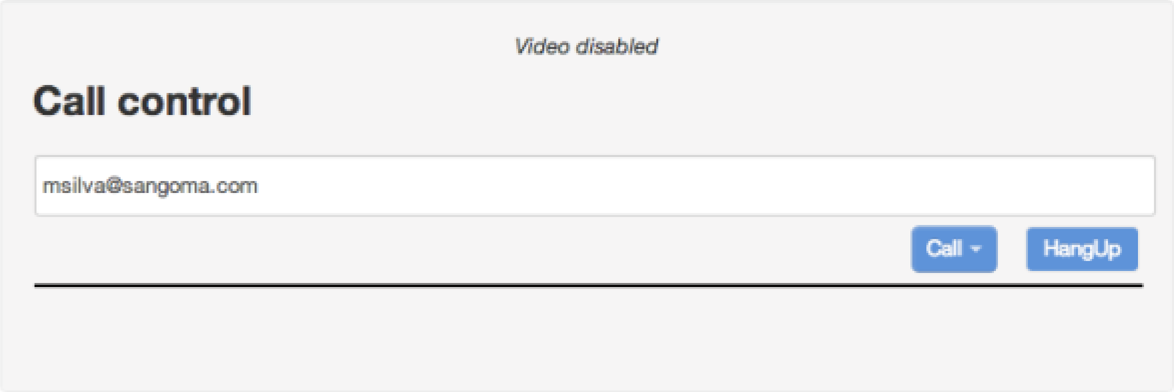
Private Identity*: webphone

Public Identity*: sip:webphone@webrtc-gateway.sango

Password: *********

Realm*: webrtc-gateway.sangoma.com

* *Mandatory Field*

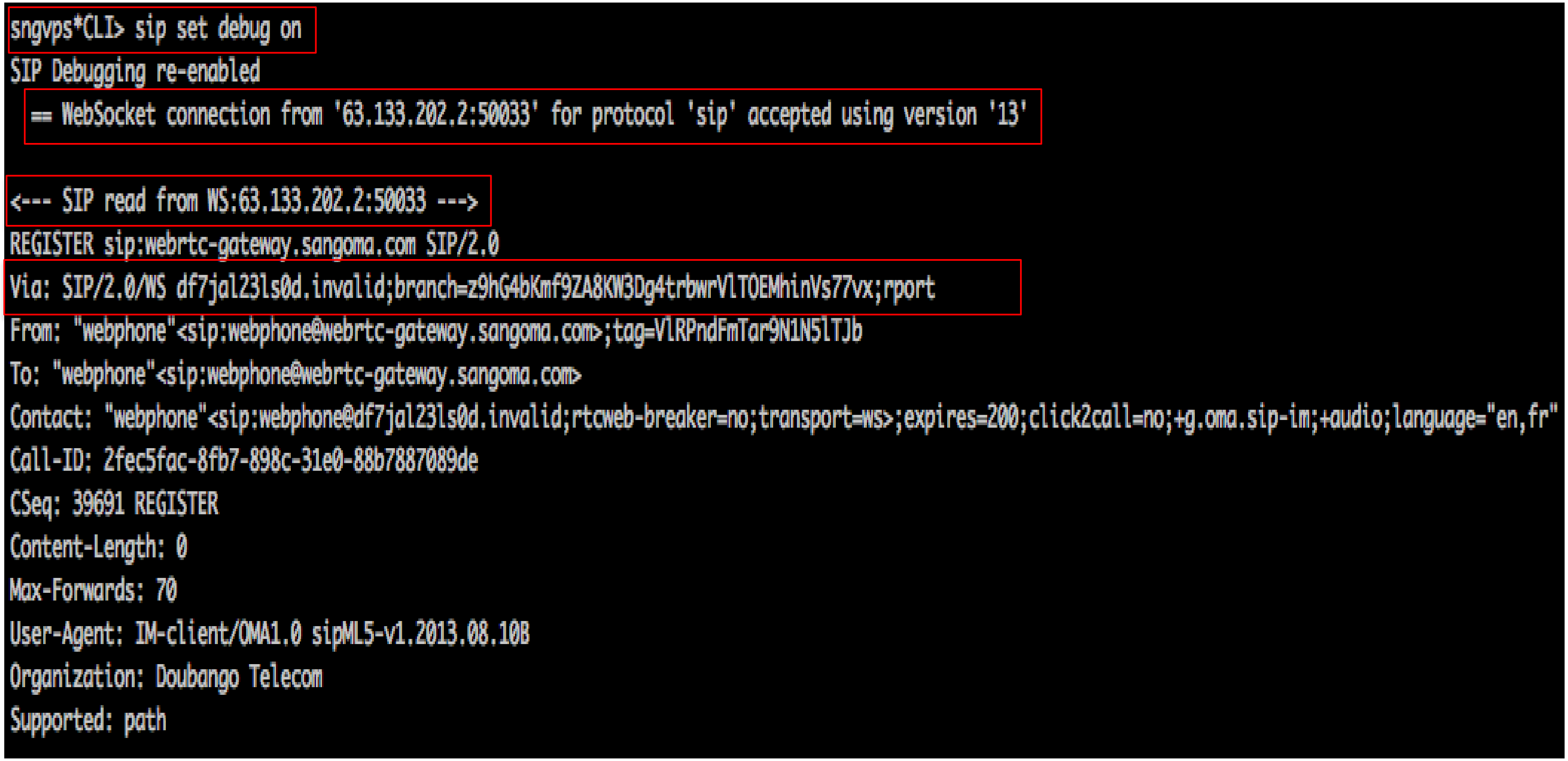


Video disabled

Call control

msilva@sangoma.com

Configuring WebRTC Support



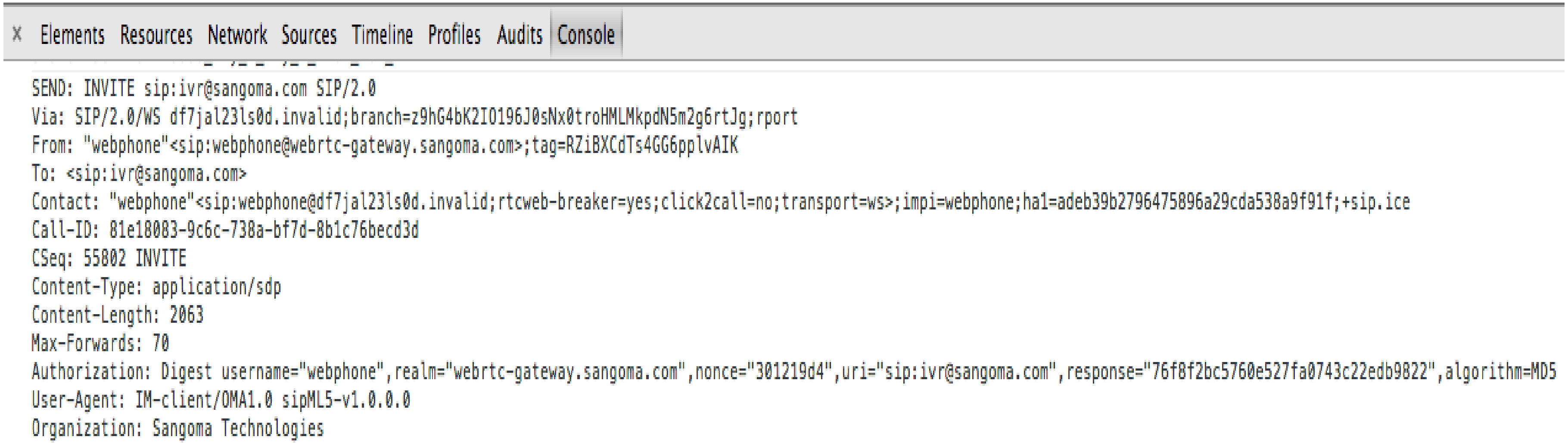
```
sngvps*CLI> sip set debug on
SIP Debugging re-enabled
  == WebSocket connection from '63.133.202.2:50033' for protocol 'sip' accepted using version '13'

<--- SIP read from WS:63.133.202.2:50033 --->
REGISTER sip:webrtc-gateway.sangoma.com SIP/2.0
Via: SIP/2.0/WS df7jal23ls0d.invalid;branch=z9hG4bKmf9ZA8KW3Dg4trbwrVlTOEMhinVs77vx;rport
From: "webphone"<sip:webphone@webrtc-gateway.sangoma.com>;tag=VlRPndFmTar9N1N5lTJb
To: "webphone"<sip:webphone@webrtc-gateway.sangoma.com>
Contact: "webphone"<sip:webphone@df7jal23ls0d.invalid;rtcweb-breaker=no;transport=ws>;expires=200;click2call=no;+g.oma.sip-im;+audio;language="en,fr"
Call-ID: 2fec5fac-8fb7-898c-31e0-88b7887089de
CSeq: 39691 REGISTER
Content-Length: 0
Max-Forwards: 70
User-Agent: IM-client/OMA1.0 sipML5-v1.2013.08.10B
Organization: Doubango Telecom
Supported: path
```

Troubleshooting

- Troubleshooting Toolkit
  - javascript console
  - chrome://webrtc-internals
  - Node ws (test websockets)
  - Wireshark!

Troubleshooting

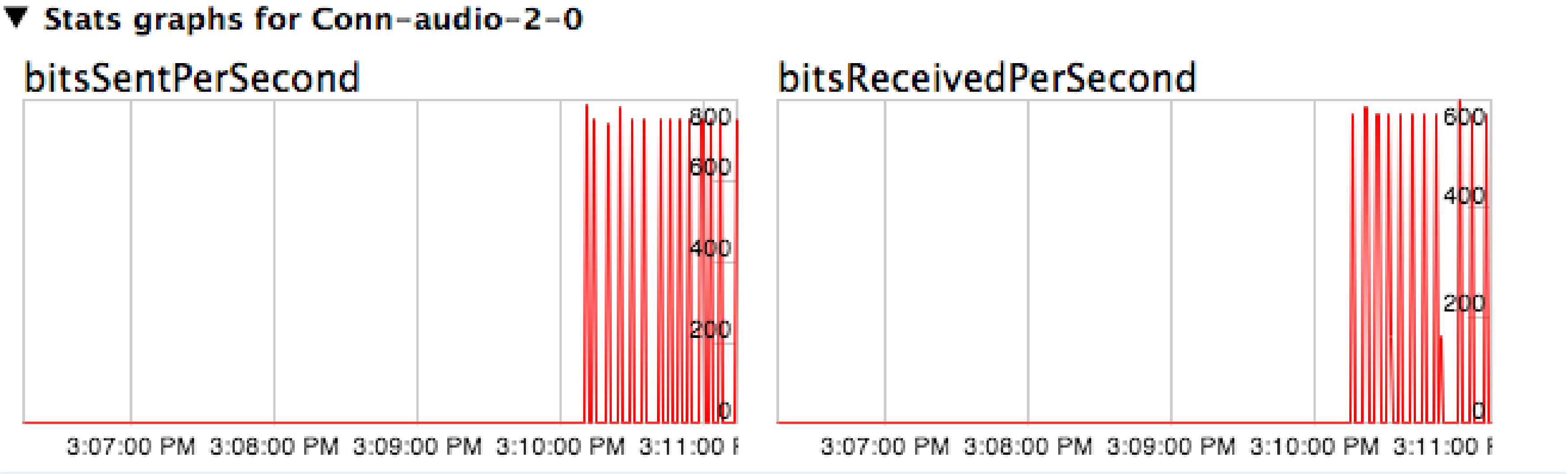
- The javascript console is your friend



```
SEND: INVITE sip:ivr@sangoma.com SIP/2.0
Via: SIP/2.0/WS df7jal23ls0d.invalid;branch=z9hG4bK2IO196J0sNx0troHMLMkpdN5m2g6rtJg;rport
From: "webphone"<sip:webphone@webrtc-gateway.sangoma.com>;tag=RZiBXCdTs4GG6pplvAIK
To: <sip:ivr@sangoma.com>
Contact: "webphone"<sip:webphone@df7jal23ls0d.invalid;rtcweb-breaker=yes;click2call=no;transport=ws>;impi=webphone;ha1=adeb39b2796475896a29cda538a9f91f;+sip.ice
Call-ID: 81e18083-9c6c-738a-bf7d-8b1c76becd3d
CSeq: 55802 INVITE
Content-Type: application/sdp
Content-Length: 2063
Max-Forwards: 70
Authorization: Digest username="webphone",realm="webrtc-gateway.sangoma.com",nonce="301219d4",uri="sip:ivr@sangoma.com",response="76f8f2bc5760e527fa0743c22edb9822",algorithm=MD5
User-Agent: IM-client/OMA1.0 sipML5-v1.0.0.0
Organization: Sangoma Technologies
```

Troubleshooting

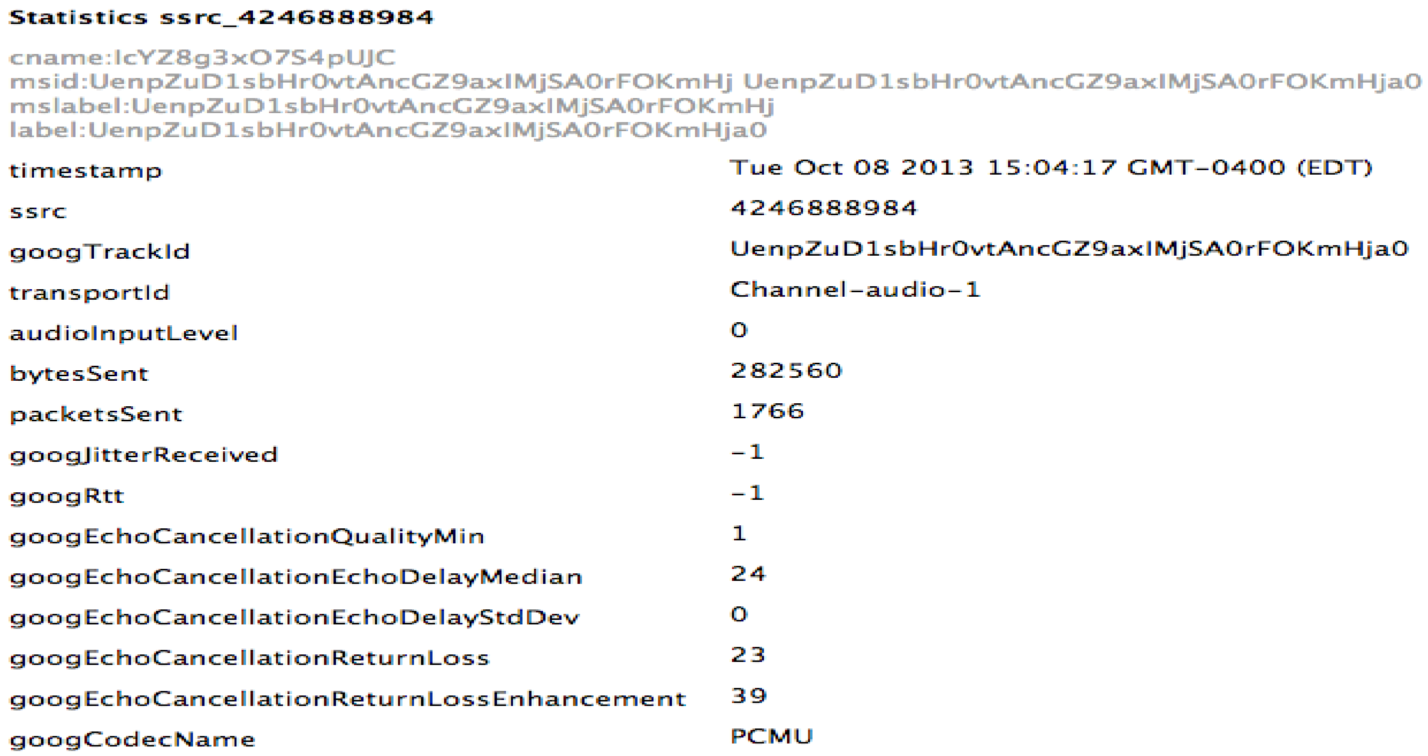
- Checking out chrome://webrtc-internals



▼ Stats graphs for Conn-audio-2-0

Troubleshooting

- Checking out chrome://webrtc-internals



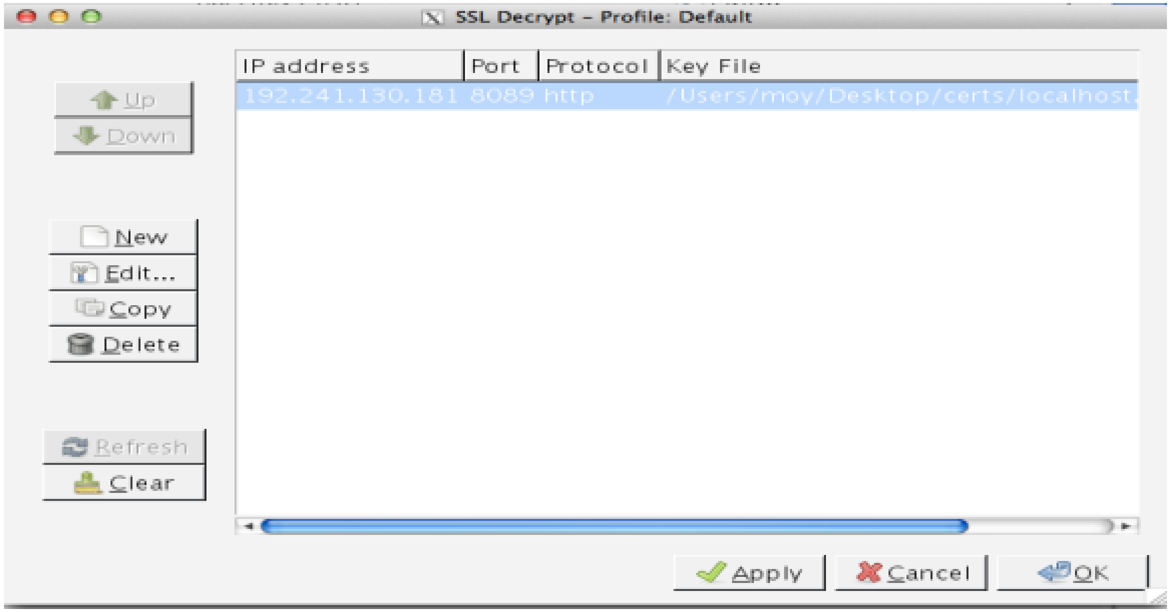
```
Statistics ssrc_4246888984

cname:lcYZ8g3xO7S4pUJC
msid:UenpZuD1sbHr0vtAncGZ9axIMjSA0rFOKmHj UenpZuD1sbHr0vtAncGZ9axIMjSA0rFOKmHja0
mslabel:UenpZuD1sbHr0vtAncGZ9axIMjSA0rFOKmHj
label:UenpZuD1sbHr0vtAncGZ9axIMjSA0rFOKmHja0

timestamp                                  Tue Oct 08 2013 15:04:17 GMT-0400 (EDT)
ssrc                                       4246888984
googTrackId                                UenpZuD1sbHr0vtAncGZ9axIMjSA0rFOKmHja0
transportId                                Channel-audio-1
audioInputLevel                            0
bytesSent                                  282560
packetsSent                                1766
googJitterReceived                         -1
googRtt                                    -1
googEchoCancellationQualityMin             1
googEchoCancellationEchoDelayMedian        24
googEchoCancellationEchoDelayStdDev        0
googEchoCancellationReturnLoss             23
googEchoCancellationReturnLossEnhancement  39
googCodecName                              PCMU
```

Troubleshooting

- Note that Wireshark VoIP calls menu won’t work for calls over websockets
- You can however use “Follow TCP stream” and see the entire SIP signaling flow
- RTP decoding will not work either (rtcp-mux)

Troubleshooting

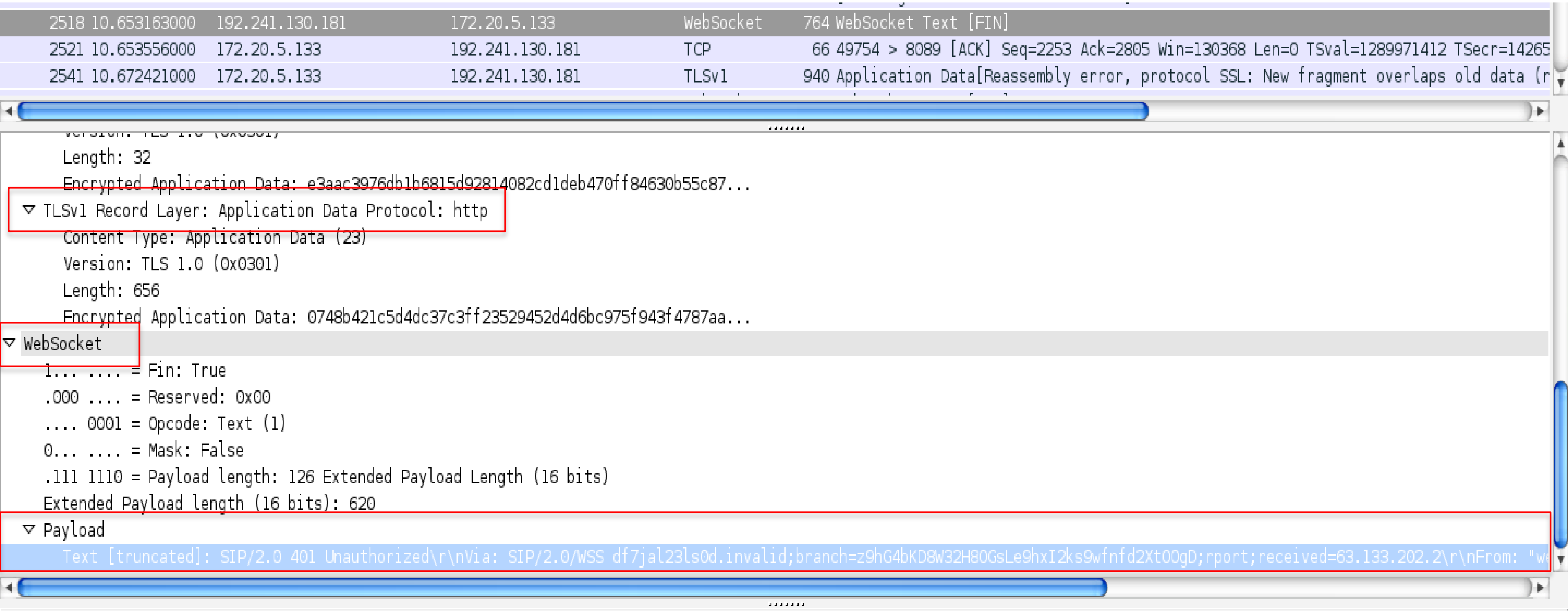
- TLS decryption can be achieved by installing the private key on Wireshark
  - Preferences -> Protocols -> SSL -> RSA Key List



IP address	Port	Protocol	Key File
192.241.130.181	8089	http	/Users/moy/Desktop/certs/localhost

Troubleshooting

- Wireshark decrypted secure WebSocket payload



```
2518 10.653163000  192.241.130.181   172.20.5.133      WebSocket   764 WebSocket Text [FIN]
2521 10.653556000  172.20.5.133      192.241.130.181   TCP          66 49754 > 8089 [ACK] Seq=2253 Ack=2805 Win=130368 Len=0 TSval=1289971412 TSecr=14265
2541 10.672421000  172.20.5.133      192.241.130.181   TLSv1       940 Application Data[Reassembly error, protocol SSL: New fragment overlaps old data (r
```

```
    Version: TLS 1.0 (0x0301)
    Length: 32
    Encrypted Application Data: e3aac3976db1b6815d92814082cd1deb470ff84630b55c87...
 ▽ TLSv1 Record Layer: Application Data Protocol: http
    Content Type: Application Data (23)
    Version: TLS 1.0 (0x0301)
    Length: 656
    Encrypted Application Data: 0748b421c5d4dc37c3ff23529452d4d6bc975f943f4787aa...
▽ WebSocket
  1... .... = Fin: True
  .000 .... = Reserved: 0x00
  .... 0001 = Opcode: Text (1)
  0... .... = Mask: False
  .111 1110 = Payload length: 126 Extended Payload Length (16 bits)
  Extended Payload length (16 bits): 620
 ▽ Payload
    Text [truncated]: SIP/2.0 401 Unauthorized\r\nVia: SIP/2.0/WSS df7jal23ls0d.invalid;branch=z9hG4bKD8W32H80GsLe9hxI2ks9wfnfd2Xt00gD;rport;received=63.133.202.2\r\nFrom: "w
```

Things to test in the near Future

- Trickle Ice
- Use of other codecs (ie Opus, iSAC)
- Video (VP8)
- Use libwebsockets in res_http_websocket?

Conclusion

- Asterisk + WebRTC gateway is easy to setup!
- Know your debugging tools
- Understand the protocols involved
- Have fun and hack away!

QUESTIONS

SANGOMA

CONNECT WITH SANGOMA

Contact Us

- Sangoma Technologies

  100 Renfrew Drive, Suite 100
  Markham, Ontario L3R 9R6
  Canada

- Website

  http://www.sangoma.com/

- Telephone

  +1 905 474 1990 x2 (for Sales)

- Email

  sales@sangoma.com

Hiastar.com
星昊通科技

Sangoma 中国总代理

f /Sangoma

/Sangoma

You Tube /SangomaTechnologies

blog.sangoma.com

THANK YOU

SANGOMA

CONNECT WITH SANGOMA