Seneca | SCHOOL OF INFORMATION TECHNOLOGY, ADMINISTRATION AND SECURITY

DCN704 – Collaborative Communications Laboratory Report

Lab # 5 (5%): VoIP protocols

Student Name: Fatjon Dauti
Student ID #: 151413192

Total marks: 5

Learning outcomes

- To identify the protocols needed for Collaboration Services
- To analyze the protocol operations when different VoIP services run across the network
- To compare protocols and architectures in terms of quality of service

Part 1. SIP

Open the following capture files using Wireshark and perform the indicated steps:
SIP-RTP on G.711
SIP-RTP on G.729

I have appended my name to the .pcap files for the screenshots, so that it will show in each window title below.

1. **[0.25 marks]** Display the complete Protocol Hierarchy for each capture file.

Insert the screenshot of these windows here.

Wireshark · Protocol Hierarchy Statistics · sip-rtp-g711-fatjondauti.pcap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	852	100.0	185175	87k	0	0	0
Ethernet	100.0	852	6.4	11928	5645	0	0	0
Internet Protocol Version 4	100.0	852	9.2	17040	8064	0	0	0
User Datagram Protocol	100.0	852	3.7	6816	3225	0	0	0
Session Initiation Protocol	1.2	10	2.7	5069	2399	10	5069	2399
Real-Time Transport Protocol	98.8	842	77.9	144322	68k	839	144308	68k
Data	0.4	3	0.0	14	6	3	14	6

Wireshark · Protocol Hierarchy Statistics · sip-rtp-g729a-fatjondauti.pcap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	433	100.0	34784	32k	0	0	0
Ethernet	100.0	433	17.4	6062	5700	0	0	0
Internet Protocol Version 4	100.0	433	24.9	8660	8143	0	0	0
User Datagram Protocol	100.0	433	10.0	3464	3257	0	0	0
Session Initiation Protocol	1.4	6	8.6	2989	2810	6	2989	2810
Real-Time Transport Protocol	98.6	427	39.1	13609	12k	425	13600	12k
Data	0.5	2	0.0	9	8	2	9	8

2. **[0.25 marks]** What are the Transport Layer and Application Layer protocols involved in these captures?

   The transport layer protocol involved is UDP, the application layer protocols are RTP and SIP

3. **[0.25 marks]** Identify the SIP flows in each capture. How many different SIP conversations are included in these captures?

Insert the screenshot of these windows here.

2 conversations in the first capture (g711), 1 in the second capture (g729a)

Wireshark · SIP Flows · sip-rtp-g711-fatjondauti.pcap

Start Time	Stop Time	Initial Speaker	From	To	Protocol	Duration	Packets	State	Comments
0.000000	8.504283	10.0.2.20	"PCMU/8000" <sip:sipp@10.0.2.20:5060>	test <sip:test@10.0.2.15:5060>	SIP	00:00:08	6	COMPLETED	INVITE 200
8.619801	8.624534	10.0.2.20	"PCMA/8000" <sip:sipp@10.0.2.20:5060>	test <sip:test@10.0.2.15:5060>	SIP	00:00:00	4	IN CALL	INVITE 200

Wireshark · SIP Flows · sip-rtp-g729a-fatjondauti.pcap

Start Time	Stop Time	Initial Speaker	From	To	Protocol	Duration	Packets	State	Comments
0.000000	8.506934	10.0.2.20	"G729/8000" <sip:sipp@10.0.2.20:5060>	test <sip:test@10.0.2.15:5060>	SIP	00:00:08	6	COMPLETED	INVITE 200

4. **[0.25 marks]** Play and compare the SIP streams. How can you compare them? How similar or different are they?

   Regarding SIP, we can apply "sip" in Wireshark as a filter, to filter only SIP related traffic. From Telephony window - SIP Flows, I can check the flow sequence for each SIP stream. They are similar in terms that there is a sequence that follows each call, for instance first packet is a SIP INVITE packet which initiates the telephone call. We see default SIP port 5060 UDP being used. For the first g711 file, I can see that the second SIP stream was interrupted without the BYE method to end the SIP session properly, so the call might have been disconnected. Also I noticed that some SIP Requests have a protocol of SIP/SDP in the Protocol column and be searching online it is the Session Description Protocol which is used for session invitation and parameter negotiation.

5. **[0.25 marks]** What stream offers the best quality? How do you measure the quality of a SIP-RTP stream?

Insert the screenshot of these windows showing the time graph of the streams here.

The see statistics that helps us determine the quality of SIP-RTP streams I used the RTP Stream Analysis in Wireshark.

Wireshark · RTP Stream Analysis · sip-rtp-g711-fatjondauti.pcap

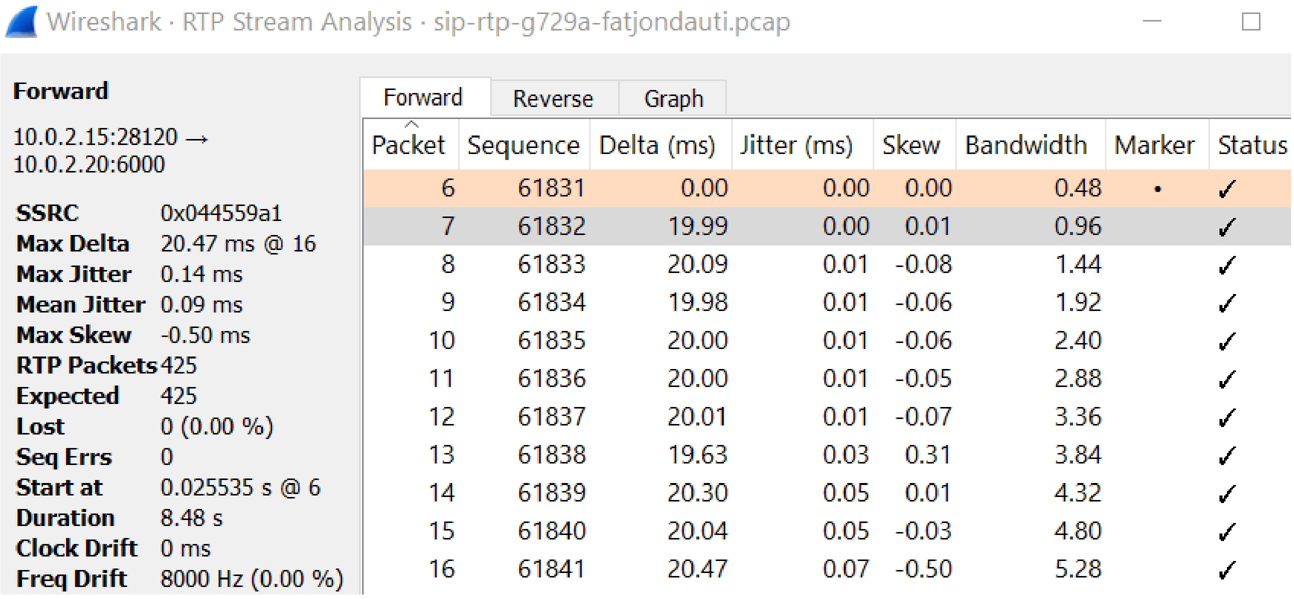
Forward

10.0.2.15:27942 → 10.0.2.20:6000

SSRC	0x343da99b
Max Delta	20.05 ms @ 310
Max Jitter	0.01 ms
Mean Jitter	0.01 ms
Max Skew	-0.03 ms
RTP Packets	425
Expected	425
Lost	0 (0.00 %)
Seq Errs	0
Start at	0.022690 s @ 6
Duration	8.48 s
Clock Drift	0 ms
Freq Drift	8000 Hz (0.00 %)

Forward | Reverse | Graph

Packet	Sequence	Delta (ms)	Jitter (ms)	Skew	Bandwidth	Marker	Status
6	37595	0.00	0.00	0.00	1.60	•	✓
7	37596	19.98	0.00	0.02	3.20		✓
8	37597	20.01	0.00	0.01	4.80		✓
9	37598	20.01	0.00	-0.00	6.40		✓
10	37599	19.98	0.00	0.02	8.00		✓
11	37600	20.02	0.00	-0.00	9.60		✓
12	37601	19.99	0.00	0.01	11.20		✓
13	37602	20.00	0.00	0.01	12.80		✓
14	37603	20.00	0.00	0.00	14.40		✓
15	37604	19.98	0.01	0.02	16.00		✓
16	37605	20.02	0.01	0.00	17.60		✓

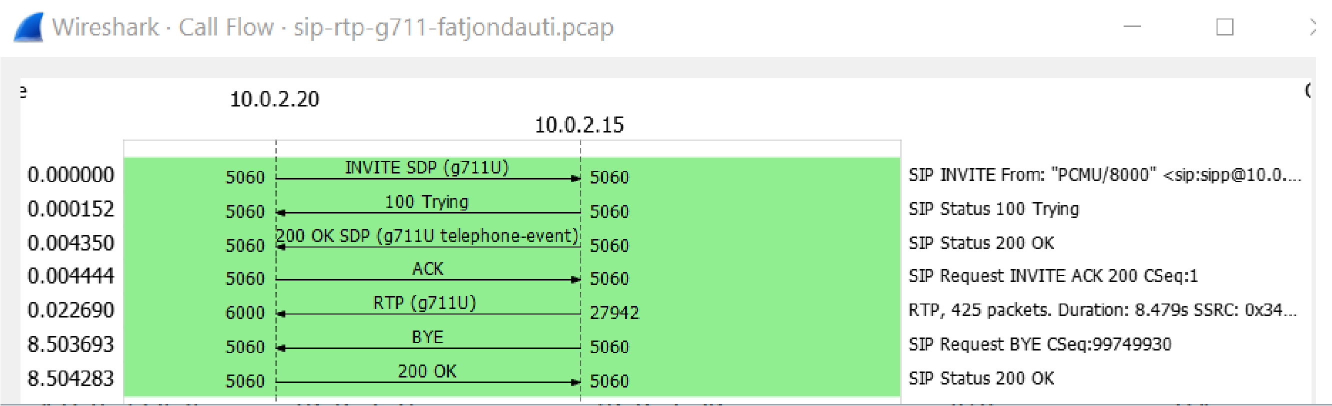


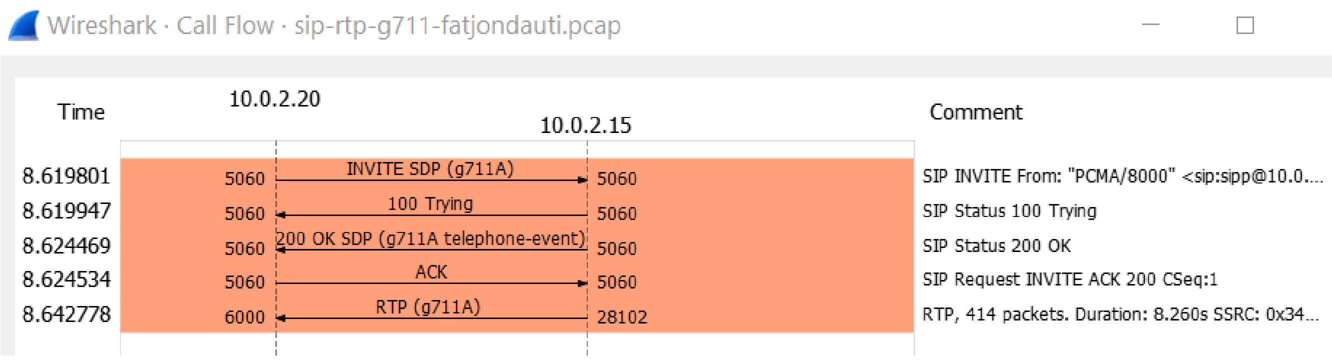
Packet	Sequence	Delta (ms)	Jitter (ms)	Skew	Bandwidth	Marker	Status
6	61831	0.00	0.00	0.00	0.48	•	✓
7	61832	19.99	0.00	0.01	0.96		✓
8	61833	20.09	0.01	-0.08	1.44		✓
9	61834	19.98	0.01	-0.06	1.92		✓
10	61835	20.00	0.01	-0.06	2.40		✓
11	61836	20.00	0.01	-0.05	2.88		✓
12	61837	20.01	0.01	-0.07	3.36		✓
13	61838	19.63	0.03	0.31	3.84		✓
14	61839	20.30	0.05	0.01	4.32		✓
15	61840	20.04	0.05	-0.03	4.80		✓
16	61841	20.47	0.07	-0.50	5.28		✓

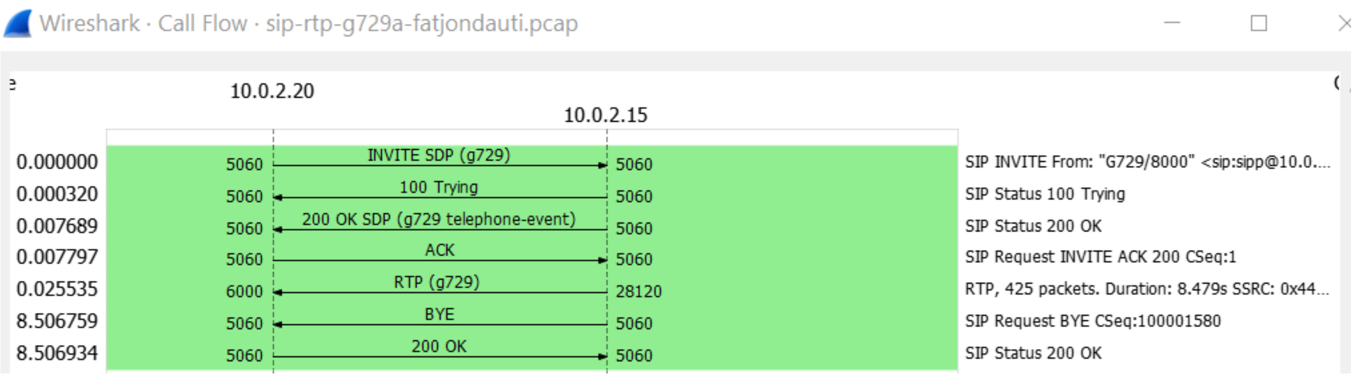
As we can see by comparing the rtp stream from each codec, with G729a we incur more Jitter (variation in packet delays), and this can be problematic for voice calls. As expected, G729a which uses compression, requires much less bandwidth as we see in the RTP stream above.

6. **[0.25 marks]** Display the call flow sequence of each call.

Insert the screenshot of these windows here.







7. **[0.25 marks]** Describe a typical SIP call sequence. How does it start? How does it finish?

As seen in the flow sequences above, a SIP call sequence starts with an INVITE request sent by the caller phone. The other SIP phone responds with Trying, meaning that it is attempting the connection. When the other phone responds with SIP Status 200 OK, the call has been answered. The caller phone acknowledges the successful invite with INVITE ACK. Voice packets will start to be transmitted through RTP. In the sequence above we can see RTP flow direction and the codec being used. When the other phone hangs up, a BYE request is sent to the caller phone. The caller phone confirms the end of the session with a SIP Status 200 OK.

8. **[0.25 marks]** What advice can be given to an end user, if you have to recommend one particular compression algorithm?

When deciding what codec to use I would balance between the quality of voice calls desired and bandwidth available on WAN links. If bandwidth is not a problem I would recommend the user to use a codec that does little compression, this way the quality of voice calls would be superior.
In case the user or business, needs to make a high number of calls at the same time while sacrificing quality without it being noticeable on voice conversations a codec that provide more compression can be used.

Part 2. H.248

Open the following Packet Tracer capture and perform the following steps:

[Fax call from TDM to SIP over Mediagateway with declined T38 request, megaco H.248.]

1. **[0.25 marks]** What end-user service is this capture about?

   This capture is about sending Fax data over IP network.

2. **[0.25 marks]** Display the complete Protocol Hierarchy on each capture file.

Insert the screenshot of these windows here.

Wireshark · Protocol Hierarchy Statistics · FAX-Call-t38-CA-TDM-SIP-FB-1-fatjondauti.pcap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	7217	100.0	1471433	107k	0	0	0
Ethernet	100.0	7217	6.9	101038	7398	0	0	0
Internet Protocol Version 4	100.0	7217	9.8	144340	10k	0	0	0
User Datagram Protocol	100.0	7217	3.9	57736	4227	0	0	0
T.38	27.9	2010	23.5	345720	25k	0	0	0
Malformed Packet	27.9	2010	0.0	0	0	2010	0	0
Session Initiation Protocol	1.3	92	3.3	48987	3587	92	48987	3587
Real-Time Transport Protocol	69.1	4985	51.3	754679	55k	4982	754631	55k
RFC 2833 RTP Event	0.0	3	0.0	12	0	3	12	0
MEGACO	1.8	130	1.2	18110	1326	130	18110	1326

3. **[0.25 marks]** What are the Transport Layer and Application Layer protocols involved in this capture?

   UDP is the transport layer protocol, T.38, SIP, RTP and MEGACO are the application layer protocols

4. **[0.25 marks]** Identify the VoIP calls in this capture. How many different calls are included in these captures?

Insert the screenshot of these windows here.

Based on the Telephony - VOIP Calls section in Wireshark, the following 5 different calls are displayed, 2 related to SIP and 3 to H.248

Wireshark · VoIP Calls · FAX-Call-t38-CA-TDM-SIP-FB-1-fatjondauti.pcap

Start Time	Stop Time	Initial Speaker	From	To	Protocol	Duration	Packets	State	Comments
20.988792	20.988792	10.35.40.22	10.23.1.42 : fffffffe		H.248	00:00:00	2		
21.006905	104.773232	10.35.40.22	10.23.1.42 : 000000bf		H.248	00:01:23	15		
21.020256	104.814347	10.35.60.72	<sip:unavailable@hostportion>	<sip:061963177@italtel.it;user=phone>	SIP	00:01:23	69	COMPLETED	INVITE 200 488 200
21.026253	104.811532	138.132.169.101	<sip:unavailable@hostportion>	<sip:061963177@italtel.it;user=phone>	SIP	00:01:23	23	COMPLETED	INVITE 200 488 200
21.193159	104.758664	10.35.40.22	10.23.1.42 : 000000bf		H.248	00:01:23	13		

5. **[0.25 marks]** Analyze each RTP stream. What is the maximum bandwidth used in the entire stream? Insert the screenshot of these windows here.

Maximum bandwidth used in the streams is 98.02 and 84.80 bytes

Wireshark · RTP Stream Analysis · FAX-Call-t38-CA-TDM-SIP-FB-1-fatjondauti.pcap

Forward

10.23.1.52:16756 →
10.35.60.100:15580

SSRC	0x17d90134
Max Delta	179.65 ms @ 3521
Max Jitter	33554432.97 ms
Mean Jitter	170598.08 ms
Max Skew	536827226.94 ms
RTP Packets	3147
Expected	3147
Lost	0 (0.00 %)
Seq Errs	0
Start at	29.970889 s @ 184
Duration	74.79 s
Clock Drift	14609996 ms
Freq Drift	1570768 Hz (19534.61 %)

Forward | Reverse | Graph

Packet	Sequence	Delta (ms)	Jitter (ms)	Skew	Bandwidth	Marker	Status
1627	953	6.18	0.76	5.12	98.02		Payloac
1623	950	6.16	0.59	5.10	97.66		Payloac
1631	955	19.98	1.26	-4.94	97.38		✓
1620	948	9.96	0.37	5.10	97.31		✓
1625	952	3.73	0.56	5.02	97.06		Payloac
341	100	9.98	0.37	5.14	96.96		✓
342	101	10.01	0.34	5.13	96.96		✓
344	102	9.99	0.32	5.14	96.96		✓
345	103	10.06	0.31	5.08	96.96		✓
347	104	9.92	0.29	5.16	96.96		✓
354	109	8.93	0.95	5.14	96.96		✓

Wireshark · RTP Stream Analysis · FAX-Call-t38-CA-TDM-SIP-FB-1-fatjondauti.pcap

Forward

10.35.60.100:15580 →
10.23.1.52:16756

SSRC	0x0eaf0eaf
Max Delta	140.44 ms @ 3131
Max Jitter	7.01 ms
Mean Jitter	0.64 ms
Max Skew	-64.46 ms
RTP Packets	1838
Expected	1844
Lost	6 (0.33 %)
Seq Errs	1
Start at	27.803285 s @ 45
Duration	36.91 s
Clock Drift	-1 ms
Freq Drift	8000 Hz (-0.00 %)

Forward | Reverse | Graph

Packet	Sequence	Delta (ms)	Jitter (ms)	Skew	Bandwidth	Marker	Status
340	157	20.16	0.61	0.34	84.80		✓
337	156	19.66	0.64	0.50	83.20		✓
2208	1077	20.36	0.59	-0.34	83.20		✓
3070	1819	20.30	0.39	-0.44	83.20		✓
110	51	19.66	0.35	-0.20	81.60		✓
112	53	19.62	0.36	-0.25	81.60		✓
113	54	19.92	0.34	-0.17	81.60		✓
114	55	19.50	0.35	0.33	81.60		✓
115	56	20.84	0.38	-0.50	81.60		✓
117	58	20.23	0.35	-0.69	81.60		✓
118	59	19.42	0.37	-0.11	81.60		✓

6. **[0.25 marks]** Other than the OK status (check mark symbol), what are the other statuses of the packets in the same stream?

Other status are "Payload changed", "Wrong sequence number", "Incorrect timestamp", "Comfort noise".

7. **[0.5 marks]** Study the RFC3389 standard. How can you apply this standard in VoIP services?

The RFC 3389 standard, defines a standard for distributing comfort noise information in VoIP systems. Real-time Transport Protocol (RTP) is the protocol used for transporting comfort noise (CN). CN is used with audio codecs that do not support comfort noise as part of the codec itself such as G.711 in this example. This standard is applied in VoIP services to avoid prolong periods of total silence, which might make the listener think that the transmission has been lost and hang up prematurely. CN will fill those silent portions of transmissions with artificial noise.

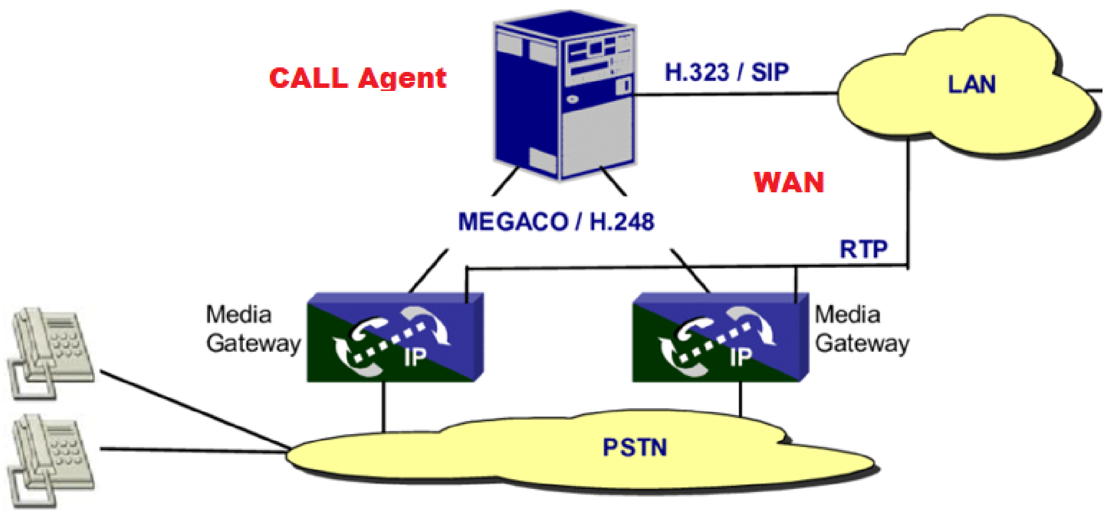
Part 3. Conclusion

1. **[0.5 marks]** Make a comparison between SIP and H.248. In which cases do you use one or the other? Or Both?

   As defined in the Soft-switch architecture big picture, H.248 would be used to provide gateway-to-gateway (Media Gateway to Media Gateway Controller or Call Agent) interface for SIP (signaling between call agents or call processors). SIP and Megaco used together allows fax, video, and data to flow from PSTN to IP networks and back to PSTN.

2. **[0.5 marks]** Illustrate your answer with a network example, including a diagram of the network in each case.

   The image I found below offers a good example of illustrating the answer above, in a scenario that includes both MEGACO-H248 and SIP.



References

https://www.ucpros.net/using-wireshark-sip-analysis-for-voip-scenarios/
https://www.onsip.com/voip-resources/voip-solutions/sip-call-flow-explained
https://www.nextiva.com/blog/voip-codecs.html#types
https://en.wikipedia.org/wiki/Comfort_noise
Protocol Convergence - 9 : Megaco / H.248
https://www.researchgate.net/figure/General-Scenario-for-MEGACO-H248-Usage_fig7_240257066