Aalto University

Department of Communications and Networking
ELEC-E7330 Laboratory Course in Internet Technologies

29 - VoIP

Student Instructions

Juha Järvinen 02.12.2020
Dancun Ogenda & Abbas Waqar 20.08.2019

1 Preliminary Exercises

1.1 Introduction

Voice over Internet Protocol (VoIP) has been a popular technology as it seeks to replace the aging Public Switched Telephone Networks (PSTN). It enables the transfer of both voice and data over IP. It has the benefits that one for example does not have to be restricted to a given geographical location as an internet connection is all that is needed to make phone calls.

There are different implementations in which VoIP can be implemented. Examples include Skype. But for this laboratory exercise, FreeSWITCH, which is an open source VoIP solution will be used.

The laboratory will cover, registering users on the FreeSWITCH and making calls between users in one domain, making calls between users in different domain, session initiation protocol (SIP) security and traffic monitoring to see the important details that are involved in the communication.

1.2 VoIP, SIP and FreeSWITCH Preliminary questions

PQ1:
What is the difference between VoIP and SIP? List a few examples of the popular VoIP solutions that you might have heard of

PQ2:
Draw the protocol stack and show the level at which SIP operates

PQ3:
What is a CODEC. Provide three different examples of audio codes that can be used in SIP. Provide the main characteristics such as sampling rate, bit rate and frame size for each of the codecs. Provide two functions of codecs?

PQ4:
What are the major differences between VoIP and Public Switched Telephone Network? Provide four features that comes with implementing VoIP that makes it commonly referred to as a killer application of traditional phone systems?

PQ5:
Provide an example of codec negotiation in FreeSWITCH in a call between Alice and Bob. Assume Alice has phone with codecs (G722 and PCMU), Bob has codecs (PCMU and PCMA) and the FreeSWITCH has an inbound codec preference of (G722, G722.1, PCMU, PCMA, G729)

PQ6:
Provide the directories that you can use to register a user in FreeSWITCH. In that directory, there are default users. Provide your configuration for a user with username 2000 and password PASS. Show the additional configurations that you have to make in the diaplan file so that calls made to 2000 can be successful.

PQ7:
How would you access the FreeSWITCH CLI after it has been installed? How would you save changes to the user files? How would you prove that users have been successfully registered to the FreeSwitch? How would you exit the FreeSWITCH CLI? Provide the commands with explanations.

PQ8:
By default, in FreeSWITCH everything is transmitted unencrypted. What are the possible disadvantages that exist and how can security be implemented? Provide the directory that can be used to configure security, for example TLS. Provide an exact way in which the media stream can be encrypted.

2 Laboratory Work

2.1 Introduction

This labwork is done both at “home” and at a lab room. We use in this work an ESXi platform installed in an APU4 AMD64 computer. Delete old virtual computers at its datastore before going further. Download images at Mycourses portal.

In addition, your group needs to two computers with wired Ethernet connection. If you do not have ones, please contact Juha.Tapio.Jarvinen@aalto.fi

The laboratory exercise is based on the SIP protocol. The server application used in this exercise is FreeSWITCH, which is installed in Debian 10 servers. There are two laboratory scenarios, one in which calls are made between users which exist in a single domain, the other is between users on different domains. To make calls after registering the users, you will have to configure two physical VoIP phones and at least one softphone that is installed already on the workstation.

To confirm whether users are registered, and any changes made to the configuration files are working, you will need to SSH into the FreeSWITCH servers. The IP addresses are 10.38.0.100 and 10.38.10.200. The username is *lab*. The password is *voip*.

SSH will not work when trying to configure the VoIP phones. For this you will have to configure them according to the instructions that will be given in the appendix section. You will after, give them the IP address, point to that IP on a web browser and from there configure the users/user registration.

All the questions mark with (AT THE LAB) are done at the lab, others at “home”.

2.2 Environment

The topology of the first part of the laboratory exercise is as shown below in figure one. As a gateway address use 10.38.0.254.

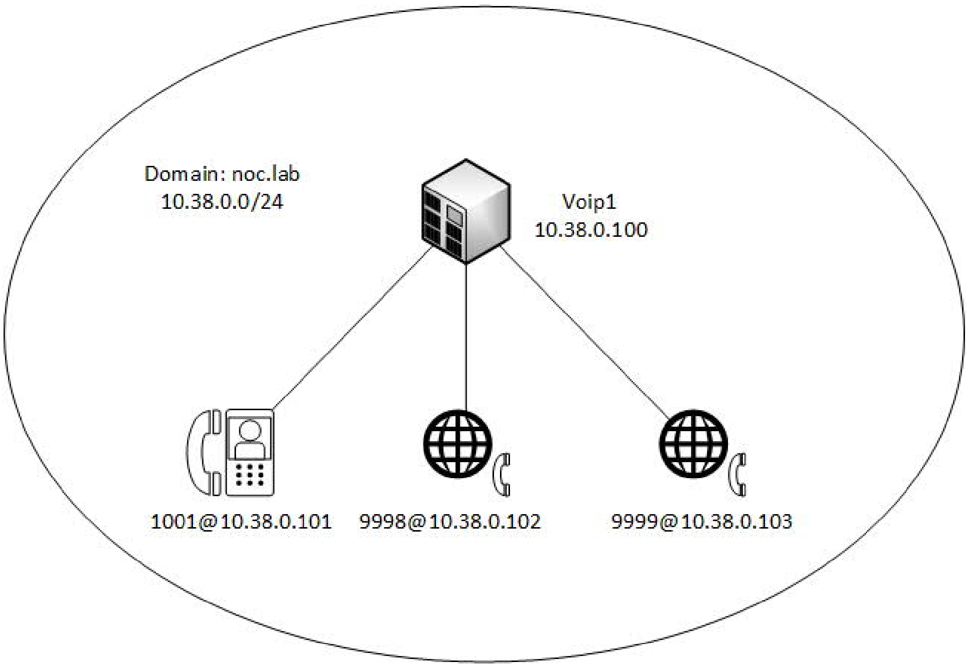

Figure 1. VoIP Laboratory Topology.

Now install one Freeswitch appliance in the APU computer. Configure it similarly as in Figure 1.

- In ESXi connect two physical connections (vmnic1 and vmnic2) to same network with voip1.
- Install Jitsi softphones (https://desktop.jitsi.org/Main/Download) to your computers with IPs 10.38.0.102 and 10.38.0.103
- A separate phone (10.38.0.101) will be connected at the room to your installation

2.3 Configuration of SIP Components

Q1.
SSH into voip1**.** The username is **lab** and the password is **lab.**

A guideline for configurations will be found at:
https://freeswitch.org/confluence/display/FREESWITCH/Configuration

First you have to configure two new users namely 9998 and 9999 to Jitsi softphones. Create xml files for the new users and then register them using the Jitsi softphone. The username has to be that of the created user.

Take a look at how the default user xml files have been configured to know what to include to make the new users that you are going to create work

After creating the xml file, you have to give file ownership to freeswitch otherwise it won’t load the xml files. You can do that by following commands.

chmod 000 <filename> // remove all rights from the file
chmod gu+wr <filename> // give the group and user read and write permissions to the file
chown -R freeswitch:freeswitch <filename> // change the ownership of the file to

freeswitch

After creating the xml file for both users, you can access the FreeSWITCH CLI, by using command fs_cli, reload all the xml configurations by using reloadxml command. To check the registered users, use show registrations command. Hopefully, you can see the users that you have created registered.

If no registrations can be found for users, then something might be wrong with your user configuration. Try it by yourself and if you do not succeed you can ask for help from the assistant(s).

Then go back to the FreeSWITCH CLI and confirm using the command show registrations. If from the console, you can see the total number of registrations to be two then everything is working as it should be.

Go ahead and make a call between user 9998 and 9999. Before making a call, start tcpdump on ethernet interface of voip1. Capture the packets for a small period between the call.

At the lab: make a call between user 9998 and 1001. Before making a call, start tcpdump on ethernet interface of voip1. Capture the packets for a small period between the call.

Transfer the pcap file to your lab computer. Open the file, using wireshark <path to/or filename> on the CLI terminal.

Q2.
Analyze the file and describe everything that is happening. What sort of packets and protocols can be seen from the capture? Can you be able to see the origin and the destination of the call? What CODECS are being used if any?

Provide short and concise descriptions with Wireshark call flow to back up your answers.

3 SIP Trunking

3.1 Environment

Add voip2 and NetEm servers to installation as presented in Figure 2. Configure voip2 on the similar way as Voip1. And configure the rest of network as in the figure; 10.38.200.0/30 is internal link in ESXi. Move the 9999 laptop to the other domain. Remember to IP route networks between VoIP hosts.

NetEm is “an enhancement of the Linux traffic control facilities that allow to add delay, packet loss, duplication and more other characteristics to packets outgoing from a selected network interface. NetEm is built using the existing Quality Of Service (QOS) and Differentiated Services (diffserv) facilities in the Linux kernel.”[1]. In an image there is a bridge with two interfaces. “Cut” a link between voip1 and voi2 servers and add Netem server between them. Remember to name links with different names. The just start the NetEm image in ESXi and leave it running so long as told to something with that computer.

1 https://man7.org/linux/man-pages/man8/tc-netem.8.html

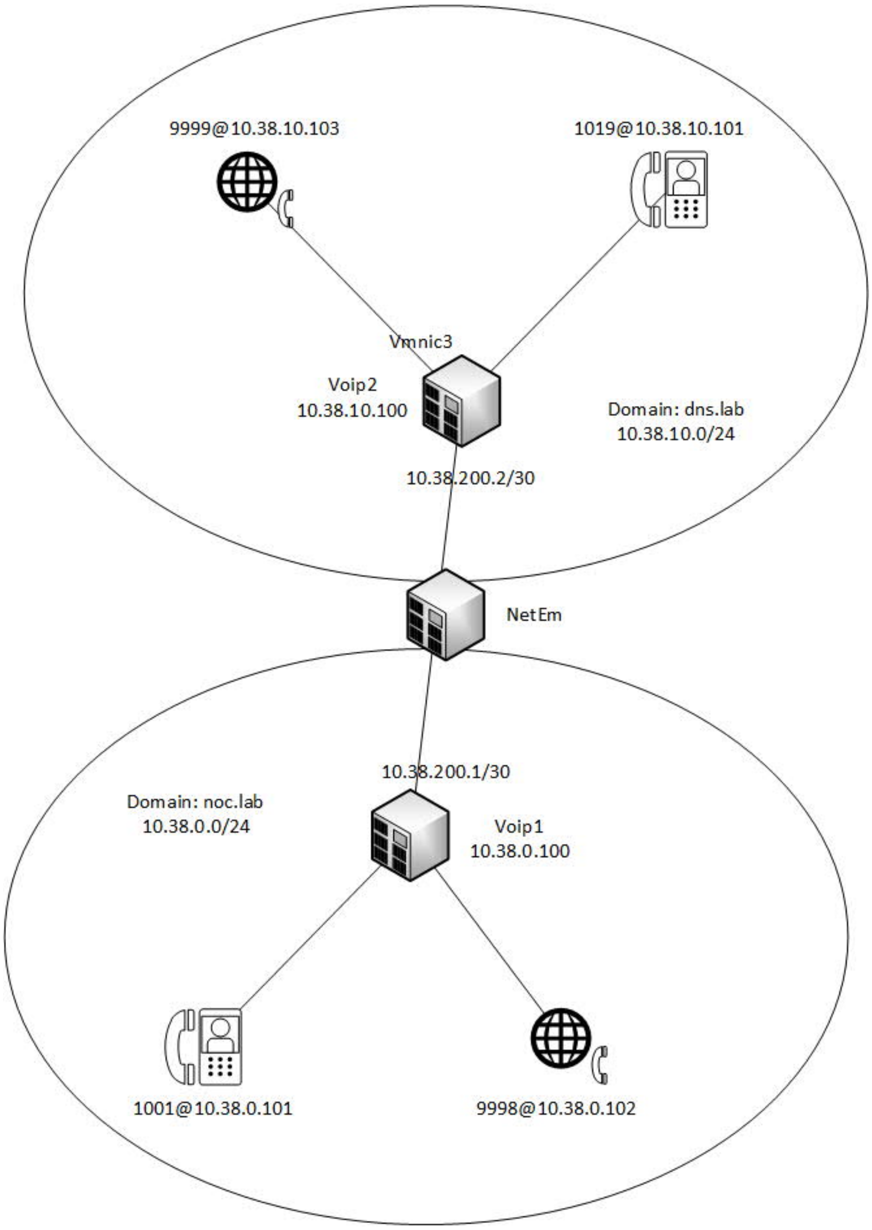

Figure 2. VoIP Laboratory Topology for the second section.

Q3. (4 points)
Next remove user 9999 from voip1 and configure it on voip2 server (10.38.10.100). You can SSH into voip 2 by using username **lab** and password **lab** Show that your registration is successful on voip2. Make a call from 9998 to 9999. Is the call successful? If not, why?

3.2 Towards to SIP Trunking

SIP Trunking refers to the interconnection between two domains to enable end point's Phone Exchange Systems (PBX) to send and receive calls via the internet. The SIP protocol is able to control voice, video and even messaging applications.

As you might have noticed from the previous question, a call from user 9998 (voip1) to 9999 (voip2) was not successful because SIP Trunking was not implemented and the first SIP server did not know how to route calls that were destined for users in another different domain. (outbound and inbound calls).

To configure outbound calls, we need a gateway that will allow our SIP servers to route outbound calls. A simple SIP trunking that will enable users **1001 and 9998** in voip1 server to call user **1019 and 9999** on voip2 server.

- Firstly, edit the **/etc/freeswitch/sip_profiles/external.xml**, and locate the section that has **ext-rtp-ip** and **ext-sip-ip**. Change from the default value to the IP address of that domain. Do the same on both files in the different domains.

- Secondly, enable the gateway configuration in **/etc/freeswitch/sip_profiles/external/<gateway.xml>,** which requires the DID, gateway IP, username and password if configured on the gateway for incoming calls. The codecs that will be used for outbound and inbound calls can also be configured in this file.

- Thirdly, we need to configure an DID (like country or area code) which will indicate the call being placed is outbound (another domain) and will also tell our server to route this call to specified gateway.

  This is configured in **/etc/freeswitch/dialplan/default/outbound.xml**. This provides a way in which calls to the outbound destination number have to be reached/routed. For this to work, it has to be configured in both domains, as a one domain configuration only is not sufficient.

- Finally, we need to set up our sip server to also receive incoming calls. This is configured in **/etc/freeswitch/diaplan/public/00_inbound_did.xml**. Here we specify which dialplan to refer to if we receive something from another domain, then look for the specified dial plan against incoming DID.
  This shows that if the destination number matches the number configured in this file, then the call is inbound and should be handled as such.

Do same for the voip1 server with gateway (**10.38.10.100**), and inbound number 61001. Any caller dialing 61001 from outside the voip1.noc.lab domain, will be transferred to user/extension 1001. Voip1 is also configured to make an outbound call with number 51003.

The task is for you to configure both voip1 and voip2 servers. Configure **voip2.dns.lab** for outbound calls with number 61001, and outbound calls from **voip1.noc.lab domain**. And for voip1, which is using the outbound number 51019. Make sure in the end that if 51019 is dialed from user 9998, the call with go through to the user 9999 etc. Same should apply for calls made to 61001 from 1001 etc., which should go through as well.

After successful configuration, you can check if the both servers are therefore able to communicate with each other. This can be tested by opening the FreeSWITCH CLI and entering the command sofia status. You should be able to see the external registration that will handle outbound and inbound calls between the two FreeSWITCH servers in different domain.

Q4. (4 points)
Make a successful call from user 9998 in voip1 domain to user 9999 in voip2 domain and vice versa.

Q5. (AT THE LAB)
Make a successful call from user 1001 in voip1 domain to user 1019 in voip2 domain and vice versa.

Q5.
Start tcpdump to capture packets, on any of the FreeSWITCH servers (voip1 or voip2). Make and outbound call from any domain (e.g. dial 51003 from extension 9998). Accept the call at the other end and talk with you group member for few seconds. Transfer the captured file to lab computer and open it using Wireshark.

Analyze the file and describe everything that is happening. What sort of packets and protocols can be seen from the capture? Can you be able to see the origin and the destination of the call? What CODECS are being used if any?

Provide short and concise descriptions with Wireshark call flow to back up your answers.

Q6 (AT THE LAB)
Repeat the test with 1001 and 1019. Is there any difference in dumps?

4 QoS and codecs

In most VoIP networks, there are challenges that always affect the quality of calls between different endpoints. An example of the challenges are latencies, jitter, delays among others. Various audio codecs have been designed to support VoIP calls under different network conditions

Q6.
Which codec would you consider useful in low and high bandwidth conditions? Provide the reasoning behind the choice. What is the best solution and the sacrifice that has to be taken in order to make calls in situation where the bandwidth is limited?

Real network consists of limited bandwidth along with latency, jitter, delays. These can be introduced in our network using tc, netem and wondershaper.

There is a dummy pc to emulate wide area network using netem (Network Emulation). It allows to test protocols by emulating variable delays, loss, duplication and reordering. Netem is used with command line tool tc (traffic control).

Some useful commands for the lab are as below:

To add a fixed amount of delay to all the packets that go out of the local interface, the command used is: -
#tc qdisc add dev ens160 root netem delay 100msecs

After the command has been executed, the results of the ping before and after should be different in how long they take. A new ping should show an increase in the deal with a figure of about 100 milliseconds.

It is also possible to introduce random variation to the network. The command used to introduce this variation is as shown: -
#tc qdisc change dev ens160 root netem delay 100msec 10msecs

For packet loss, in the tc command it has to be specified using the percentage sign. An example command that will drop 1 out of 1000 packets is as shown: -
#tc qdisc change dev ens160 root netem loss 1%

Apart from the packet loss, it is also possible to duplicate the number of packets. The command used is as follows: -
#tc qdisc change dev ens160 root netem duplicate 1%

To corrupt packets through the introduction of random noise, the command used is as follows: -
#tc qdisc change dev ens160 root netem corrupt 1%

NOTE: Read the reference about the use of netem in addition to the commands that have been given above.

For bandwidth limiting, another traffic shaping script called wondershaper. Wondershaper allows you to dictate what amount of bandwidth you want in a link in both the uplink and the downlink directions. An example is shown as follows: -

#wondershaper ens160 1024 512

This will configure on the link ens160, a downlink speed of 1024 Kbit/sec and a uplink speed of 512 Kbits/sec

Q7.
You can configure the outgoing codec in any of the FreeSWITCH servers by adding a variable tag in the gateway configuration file. The file is located at
/etc/freeswitch/sip_profiles/external/<gateway>.xml.

```
<variables>
  <variable name="absolute_codec_string" value="insert_codec_here"
  direction="outbound" />
</variables>
```

Force FreeSWITCH to use one of the codecs supported by the IP phones (G722 or G711) for outgoing calls. Restart FreeSWITCH after the changes made to the gateway configuration files. Introduce a delay, and then constantly increase it until the point at which the VoIP calls will no longer be audible.

NOTE: Remove any configured network limitations that are introduced earlier before going to the next task

Check man pages for the commands (**man wondershaper**).

You can analyse calls with VoIPmonitor, an open source network packet sniffer designed for VoIP applications. VoIPmonitor can analyze quality of VoIP calls according to ITU-T G.107 E-model and predicts quality on MOS (Mean Opinion Score) scale with values ranging from 1 for unacceptable to 5 for perfect communication.

The other tool that is used to monitor VoIP traffic and offer a graphical insight on what is happening is the VoIPmonitor. It has been configured and you just have to point to the IP address

10.38.0.100 (voip1) or 10.38.10.100 (voip2) on a web browser. The username is **admin** and the password are **admin12345**.

So, after logging in, click to the **dashboard**, and you will be able to see parameters such as the Mean Opinion Score (MOS) about the call. From this part, any other changes that will be made to reflect/simulate bad networking conditions has to be all shown in this graphical user interface (GUI).

Any active calls that are currently undergoing can be seen from **Active Calls** button. There is a way in which all calls are recorded without encryption. All calls that are made, are recorded and can be viewed and listened from the **CDR** button.

Feel free to play around with the VoIP monitor GUI and then see what capabilities it has apart from the ones mentioned above.

Q8.
Induce varying delays and random jitter in the network. At least use values 0ms, 200ms, 500ms and 1000ms to simulate calls from local call to a satellite call. Check the quality of call between phones and its MOS value. Analyse the results in few sentences. Mention highest delay for acceptable VoIP call and the effect of delay and jitter in the call.

Q9.
Change the delay to zero and then alter the packet loss values. Use values 0, 0.0, 0.1, 0.16 and 0.25. Check the quality of call between phones and its MOS value. Analyse the results in few sentences and also write the highest loss value for acceptable VOIP call. How does packet duplication and corruption affect in the VOIP call?

5 VoIP Security and threats

VoIP hasn’t survived without security problems. Companies implementing VoIP services tend to be concerned about quality issues and ignore security. The threats are mostly similar as for any of the data and the securing methods doesn’t differ from the securing methods of the other data either. The differences concern mostly about architecture and some service features. This part scratches only the surface of VoIP-security. The idea of this part is to show how unsecured VoIP-traffic may be.

Q11. (3 pts)
Capture a voip call from any of the voip server. (call between 1001@voip1 and 1019@voip2) Decode the RTP traffic in Wireshark. Are you able to successfully tap the voip call?

6 The Lab Room Session

Reserve a 1-2 h lab session by emailing to Juha.Tapio.Jarvinen@aalto.fi or at the Mycourses portal.

7 Final Report

Answer all the questions marked Q from the previous sections. Additionally, answer the questions below in the final report.

FQ1.
There are many more codecs involved with the VoIP technology. Find and list here at least four more along with their basic properties: sampling rate, bit rate, frame size (if frame-based).

FQ2.
What security threats can be found for VoIP traffic or system? Mention at least four of them. (One of them may be closer than you thought)

FQ3.
Give few tips to improve VoIP security.

8 Useful References

Wondershaper: http://ubuntuforums.org/showthread.php?t=25911

Netem: http://www.linuxfoundation.org/collaborate/workgroups/networking/netem

SIP Protocol: http://tools.ietf.org/html/rfc3665

APPENDIX A: CONFIGURING YEALINK VOIP PHONES (AT THE LAB)

VOIP Phones checking or configuring via keypad:

	Check	Configure
IP Address	****90#**	****80# then <ip address>#**
Subnet Mask	****91#**	****81# then <subnet mask>#**
Gateway	****92#**	****82# then <gateway>#**
DNS1	****93#**	****83# then <dns1>#**
DNS2	****94#**	****84# then <dns2>#**
DHCP		****88# then 0# to disable DHCP** ****88# then 1# to enable DHCP**

VOIP Phones checking or configuring via web:
Dial **90# to get ip address of the phone. Then enter the address in address bar of browser.
Login: admin
Password: admin
In the account settings, activate the account and change the required parameters.

Note: PC used for login should be on the same network as the of phone.

REFERECES:

[1] https://tandisrayan.co/files/UGT18.pdf