Institute of Telecommunications
Warsaw University of Technology
Jan 2021

EINTE LAB EXERCISES

VOIP SERVICE LAB (SIP, RTP/RTCP)

INTRODUCTION

This exercise covers the basic aspects of VoIP service, related to multimedia data transport (**RTP**) and session control (**SIP**). This exercise is executed offline, using the provided VirtualBox virtual machine containing the SIP server and the free SIP client software.

The exercise can be done individually or in the groups (groups of more that 3 persons have to be agreed with the course supervisor). To execute the exercise you will need a PC/laptop with Internet access and Windows 7 or higher OS (please make sure that the relevant virtualization support options are on in the PC BIOS).

Note: *the exercise can be also executed under Linux OS – there are Linux versions of all the required software except the 3CX client, but the Windows client can be successfully installed and run under Wine.*

Before starting the exercise it is advised to refresh your knowledge related to the following protocols:

- SIP (http://tools.ietf.org/html/rfc3261)
- SDP (https://tools.ietf.org/html/rfc4566)
- RTP/RTCP (https://www.ietf.org/rfc/rfc3550.txt)

PREPARATION

The preparation activities consist of installation and configuration of the required software.

1. Download the **IPlab-3cx.ova** file containing the image of the VM with the VoIP server and save on a local storage.The file can be retrieved from the files repository in the MS Teams EINTE group. **Note!** The file size is about 900MB.

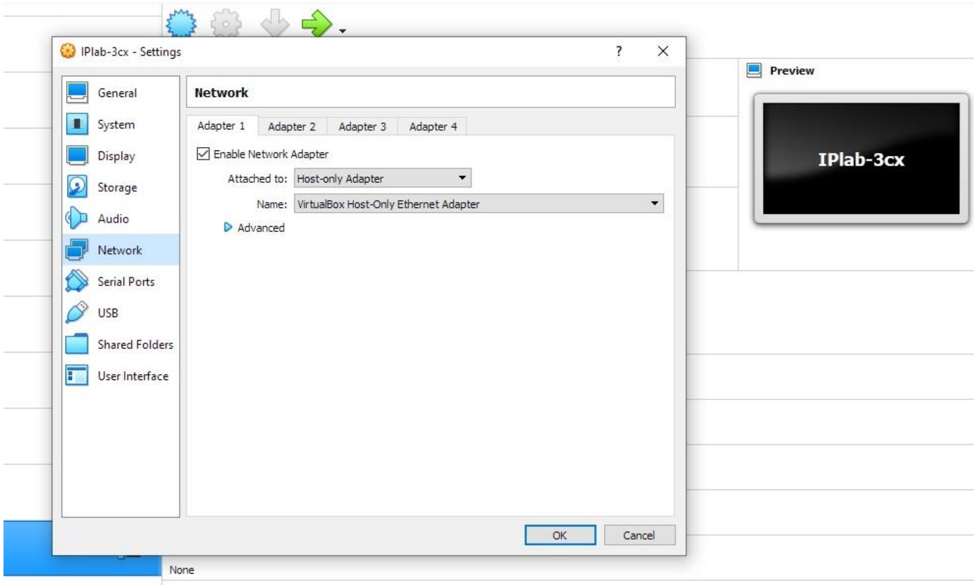
2. Install the **WireShark** software

   The software is available for download fom http://www.wireshark.org/ After downloading, install WireShark with the default options.

3. Import the VoIP server VM into **VirtualBox** environment

   Start the VirtualBox, choose the ***File/Import Appliance*** option from the main menu and select the VoIP server *IPlab-3cx.ova* VM image file from a local disk. Start the VM import process (leave all import settings on default values) – this may take a few minutes.

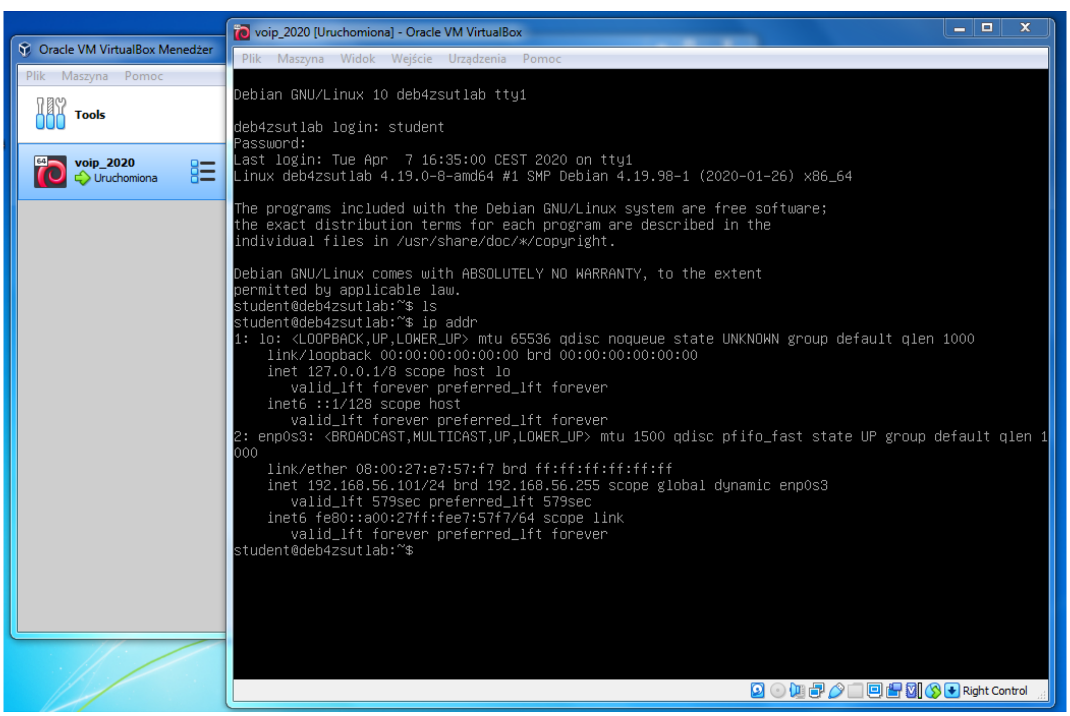
   After importing the VM, select it and click on *Settings* button, select the *Network* tab and make sure that there is a network adapter attached to the host-only network (*Virtual Box Host Only Ethernet Adapter*).



In case of problems, please first check if there exists a host-only network using the *Files/ Host Network Manager* from the main menu. If not, create a new one using *Create* option and then select an appropriate network adapter in VM settings.

4. Starting the 3CX server

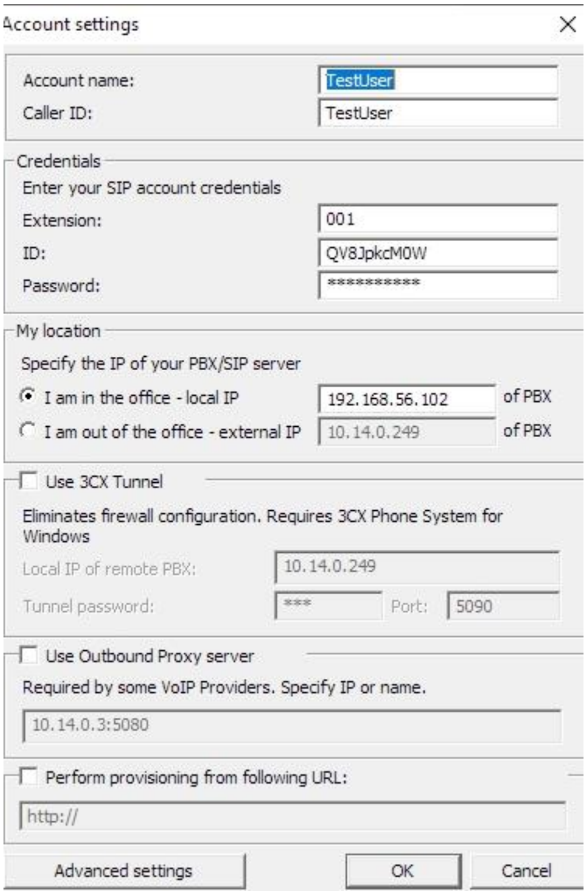
Next, start the VM (e.g. using *Start* button). After the VM Linux console shows up, login using the following credentials (user, password): *test*, *test2020*. After successful login, issue the *ip addr* command and read the IP address that was assigned to the VM by the host-only network DHCP server



In the above example, you can see that the „enp0s3" interface IP address is 192.168.56.101 (the interface name „enp0s3" may be different in some cases, but the VM should have only 2 interfaces – loopback and the one related to the host-only network). You can then verify the connectivity running the ping command to the VM interface address from the command-line terminal on the host PC. After successful ping, you can minimize the VM (but keep it running through the whole exerercise). The VirtualBox window can be closed.

5. Installing and starting 3CX client

3CX communicator can be downloaded from: https://www.3cx.com/downloads/3CXPhone6.msi
After download, install the client software using standard options. Run the communicator, select option *Create Profile* and create a new account using the *New* button. If the 3CX software was already installed earlier, you can enter the same context clicking the right mouse button over the „phone" window and selecting *Accounts*.



Next, fill the account data as shown on the picture above (the account name and *Caller ID* can be changed as you will). The IP adress in *My location* panel should be the same as the IP address read from the VM console (this was discussed in section 5 above). The ID and password in *Credentials* panel are respectively: *QV8JpkcM0W* (with zero before W) and *qIgueuFEB6* (with capital *I* as Irene).

After closing the configuration window and returning to phone application, the main window should display the account name and *On Hook* notification that confirm a successful registration.

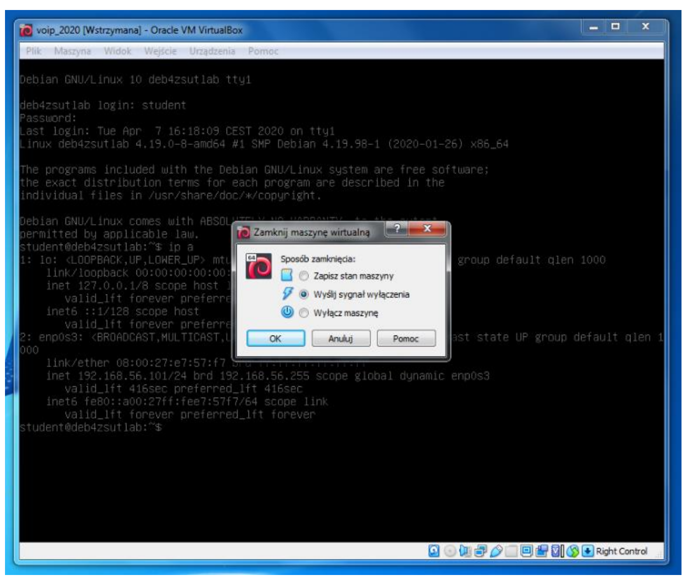
EXECUTION

Note: before starting the exercise, run **WireShark** and make sure that it captures packets on the ***VirtualBox Host-Only Network*** interface.

1. Connection to the VoIP server

   The main task of the exercise consists of connecting with the VoIP server and hearing the audio messages using 3CX softphone. To accomplish this, you need to do the following steps:

   a) Connect with the 801 number, using numerical keys of the application and a button with green handset.
   b) Hear the welcome message. After the message ends, press one of the numerical keys on the PC keyboard and hear another message. After that, the call will be disconnected. **Note**: if you can't hear the message, first make sure that the proper sound output device is selected in the 3CX client *Preferences*).
   c) Enter the *Accounts* menu of the 3CX communicator, select an active account and click the *Edit* button and then *Advanced Settings*. In the audio codec options change the codec on top of the list (e.g. exchange PCMA/PCMU for GSM or vice-versa). Also, deselect the *Support RFC2833 DTMF* option and select *Support SIPINFO DTMF*.
   d) Repeat the connection with 801.
   e) Stop the Wireshark capture and save the captured data in the .*pcap* file (<u>that has to be attached to the report</u>).
   f) Close the VoIP server VM (by closing the window and selecting *Send the Shutdown Signal* option).



2. Analysis of the captured data

Analyze the captured data flow between the 3CX SIP client and the VoIP server, paying special attention to the sequence and content of the SIP messages, and the SDP session descriptions carried inside INVITE and 200 OK, as well as to the content of the RTP packets (especially the RTP EVENT packets).

Prepare the report (**in PDF format**), containing at least the following:

- Wireshark window screenshot showing the sequence of SIP messages exchanged between the 3CX client and VoIP server during the exercise (obtained by *Flow Sequence* option in *Telephony/VoIP Calls* menu of Wireshark).
- Answers to the following questions related to the first call:
    - What is the meaning of *407 Proxy Authentication Required* response received after the first INVITE?
    - What is the content of Media Description line in SDP descriptions sent within the SIP INVITE and 200 OK messages? Attach the relevant screenshots and explain the meaning of the most important fields.
    - What is the voice codec used in the session?
    - In some RTP packets the *Mark* field in the packet header has the value of 1 – why?
    - How the information about the pressed key is sent by the SIP client to the VoIP server?
    - What is the sequence number and timestamp of the first RTP packet sent by the server to the client, and why they are not 0 or 1?
- Answers to the following questions related to the second call:
    - Which voice codec was used in the second session?
    - How the information about the pressed key is now sent to the VoIP server?

Please note that some answers require extending the VoIP-related knowledge beyond what was discussed during the lecture.

DELIVERY

- Prepare a zip archive containing the report and the Wireshark pcap file.
- Rename the archive in the following manner: COURSE_Semester_FirstAuthorSurname.zip (example: EINTE_2021Z_Kowalski.zip).
- Upload the archive archive in response to the assignment before deadline.

Do not forget to add a header with the names of lab group members to the title page of the report.