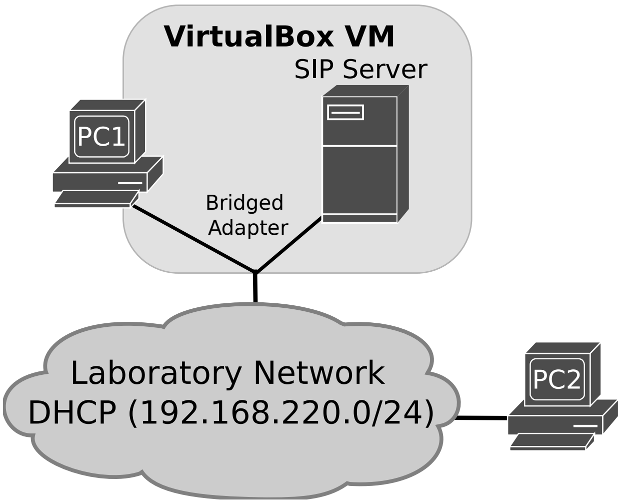
Arquitetura de Redes Avançadas

Laboratory Guide

VoIP

SIP, RTP and RTCP protocols and H323 protocol stack



SIP, RTP and RTCP Protocols

1. The SIP server must be implemented as a virtual Ubuntu/Debian server. A VirtualBox appliance (with all required services and files) is available to download here (login/password: ubuntu/reverse). Connect VM to your PC (PC1) Ethernet interface using a Bridged Adapter. Boot the SIP Server and identify the DHCP acquired IPv4 address (assuming from now on 192.168.220.x). If necessary release the previous acquired address and restart DHCP client process:

```
 # sudo dhclient -r eth0
 # sudo dhclient eth0
```

Identify the DHCP acquired IPv4 address of your PC1. From your PC1, test the connectivity with your SIP Server (using the command ping). Connect to your server using SSH (`ssh ubuntu@192.168.220.x`), in order to make future configurations easier by command line copy and paste. Change to root terminal with the command `sudo su`.

Note: The server should have installed the VoIP gateway and conference server (Asterisk) with default configuration.

Editing the /etc/asterisk/sip.conf file add a new user:

```
        [PintoDaCosta]
        type=friend
        host=dynamic
        secret=labcom
        context=phones
        allow=all
```

And editing the /etc/asterisk/extensions.conf file add a phone extension (2000) to deliver a welcome message:

```
        [phones]
        exten => 2000,1,Answer(500)
        exten => 2000,n,Playback(demo-congrats)
        exten => 2000,n,PlayBack(vm-goodbye)
        exten => 2000,n,Hangup()
```

Restart Asterisk:

```
        service asterisk restart
```

2. In your PC1, start a VoIP softphone (Ekiga) and add a new SIP account (Edit → Accounts → Accounts → Add a SIP Account) with the credentials defined before and **without enabling the account**, e.g.:

```
        Name: SIPServer
        Registrar: 192.168.220.x
        User: PintoDaCosta
        Password: labcom
```

Start a Wireshark capture and enable the SIP account. Analyze the exchanged SIP request and status messages and identify the purpose of the following messages: REGISTER and SUBSCRIBE (and if present PUBLISH).

3. Start new Wireshark capture (in your Ethernet interface in non-promiscuous mode) and change the status in your VoIP softphone to AWAY. Change the status back to ONLINE. Analyze the exchanged SIP messages and identify the purpose of the PUBLISH messages (based on the XML contents of the message body).

4. Start new Wireshark capture, make an audio call to extension 2000 (sip:2000@192.168.220.x) for a welcome message from server, and wait for the end of the message:

- Analyze the exchanged SIP request and status messages and identify the purpose of the following request messages: INVITE, ACK and BYE.
- Analyze the exchanges RTP messages and identify the purpose of the fields Payload Type, SSRC, Sequence, Timestamp and flags.
- Analyze the exchanges RTCP messages and identify the purpose of the message fields.

5. Test different audio codecs: Speex 16kHz, PCMU, PCMA, gsm and G722. By selecting one at time in Ekiga Audio → Codec preferences. Make an an audio call to extension 2000 for each audio codec. Analyze SIP, RTP and RTCP packets.

6. Editing the /etc/asterisk/sip.conf file add a new user:

```
[Vieira]
type=friend
host=dynamic
secret=labcom
context=phones
allow=all
```

Editing the /etc/asterisk/extensions.conf file define extension numbers for all users:

```
[phones]
...
exten => 2001,1,Dial(SIP/PintoDaCosta,10)

exten => 2002,1,Dial(SIP/Vieira,10)
```

Restart Asterisk: `service asterisk restart`

7. Using a second PC (PC2) or making arrangements with a neighbor group, register the second user with your Asterisk server. On your PC1, start new Wireshark capture and make an audio call to the second user extension (2002@192.168.220.x). After a few seconds hang up the call. Analyze the exchanged SIP request and status messages, identify the purpose of the following messages: INVITE, ACK, BYE, Trying, Ringing and OK.

8. Create a conference room (101) editing the file /etc/asterisk/meetme.conf:

```
        conf => 101
```

Edit the /etc/asterisk/extensions.conf file define an new extension number to access conference room 101:

```
        [phones]
        exten => 1101,1,Answer
        exten => 1101,2,Wait(1)
        exten => 1101,3,Authenticate(1234)
        exten => 1101,4,MeetMe(101,p,1234)
        exten => 1101,5,Playback(vm-goodbye)
        exten => 1101,6,Hangup
```

Restart Asterisk:

```
        service asterisk restart
```

On your PC1, **change the DTMF Mode to RFC2833 in Ekiga Preferences → Protocols → SIP Settings.** Start new Wireshark capture and make an audio call to the conference room (extension 1101@192.168.220.x). Authenticate with PIN 1234# and after a few seconds hang up the call with the # key. Analyze the exchanged SIP and RTP messages, identify the purpose of the following messages: SIP INVITE, ACK, BYE, Trying and OK, and RTP EVENT.

On your PC1, **change the DTMF Mode to INFO in Ekiga Preferences → Protocols → SIP Settings.** Make a second audio call to the conference room (extension 1101@192.168.220.x). Analyze the exchanged SIP and RTP messages, identify the purpose of the SIP INFO messages.

9. Create voicemail boxes (with password 1212) editing the /etc/asterisk/voicemail.conf file:

```
        [ara_voicemail]
        2001 => 1212,PintoDaCosta,2001@araxvoip.com
        2002 => 1212,Vieira,2002@araxvoip.com
```

Associate the new voicemail boxes with the previously created users, edit /etc/asterisk/sip.conf file:

```
        [PintoDaCosta]
        ...
        mailbox=2001@ara_voicemail

        [Vieira]
        ...
        mailbox=2002@ara_voicemail
```

Update the /etc/asterisk/extensions.conf file to activate the voicemail is no one answer an extension:

```
        exten => 2001,1,Dial(SIP/PintoDaCosta,10)
        exten => 2001,2,VoiceMail(2001@ara_voicemail)
        exten => 2001,3,PlayBack(vm-goodbye)
        exten => 2001,4,HangUp()

        exten => 2002,1,Dial(SIP/Vieira,10)
        exten => 2002,2,VoiceMail(2002@ara_voicemail)
        exten => 2002,3,PlayBack(vm-goodbye)
        exten => 2002,4,HangUp()
```

And update the /etc/asterisk/extensions.conf file to define extensions to access voicemail boces (9001 → 2001 and 9002 → 2002):

```
        exten => 9001,1,VoiceMailMain(2001@ara_voicemail)
        exten => 9002,1,VoiceMailMain(2002@ara_voicemail)
```

Restart Asterisk:

```
        service asterisk restart
```

Unregister the user Vieira with the server, make a call from PintoDaCosta to Vieira (2002) and leave a message on the voice mail. Unregister PintoDaCosta with the server.

Use DTMF Mode as INFO in Ekiga Preferences → Protocols → SIP Settings.

Start new Wireshark, register Vieira with the server and access the voicemail box (call 9002, and use password 1212). Analyze the exchanged SIP request and status messages, identify the purpose of the following messages: NOTIFY and INFO.

10. Activate video call support by editing the file /etc/asterisk/sip.conf:

```
[general]
videosupport=yes
```

Using a second PC or making arrangements with a neighbor group, register the second user with your Asterisk server. On your PC1, start new Wireshark capture, connect your web cameras and make a video call to the second user extension (2002@192.168.220.x). After a few seconds hang up the call.

- Analyze the exchanged SIP request and status messages, identify the purpose of the following messages: INVITE, ACK, BYE, Trying, Ringing and OK.
- Analyze the exchanges RTP messages and identify the purpose of the fields Payload Type, SSRC, Sequence, Timestamp and flags.
- Analyze the exchanges RTCP messages and identify the purpose of the message fields.

H.323 Protocol Stack

11. Start a new Wireshark capture. To establish a audio/video call between two terminal using H.323, start Ekiga on both terminals and in one of them define the destination as “h323:<ip_address>” and press the call button. Analyze the exchanged Q.931, H.225, H.245 (and H.261 if present) messages.