

# TP Réseaux Multimédia

## Téléphonie sur IP avec le protocole SIP

NOM et PRENOM : [BONNET Ludivine](#)

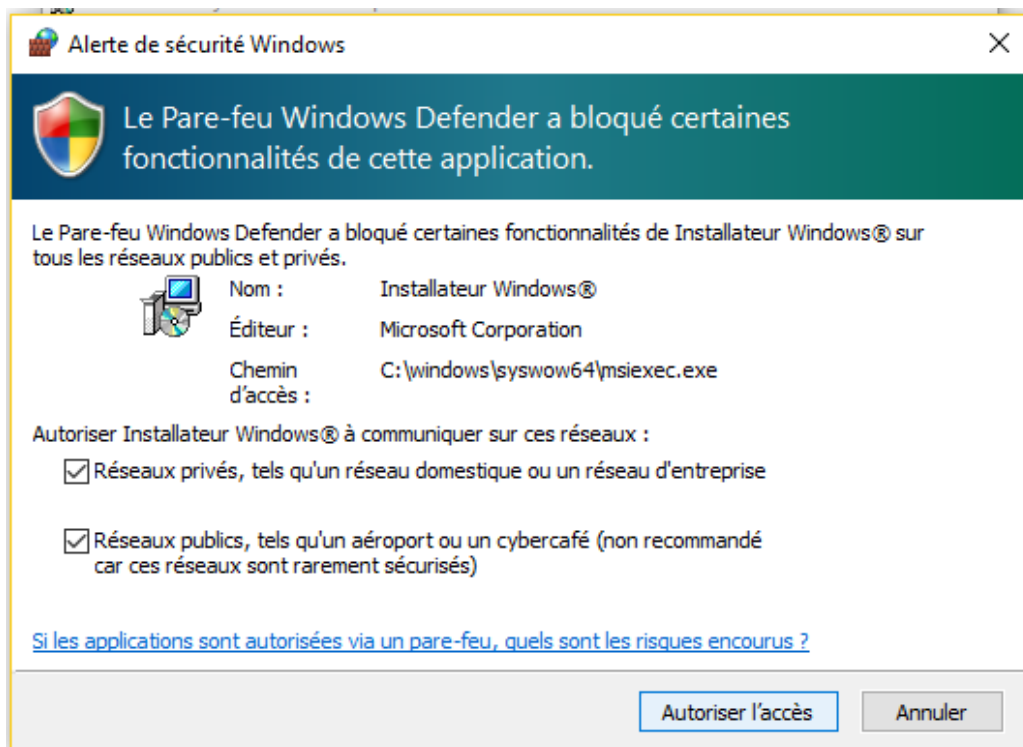
NOM et PRENOM : [GUARDIA Quentin](#)

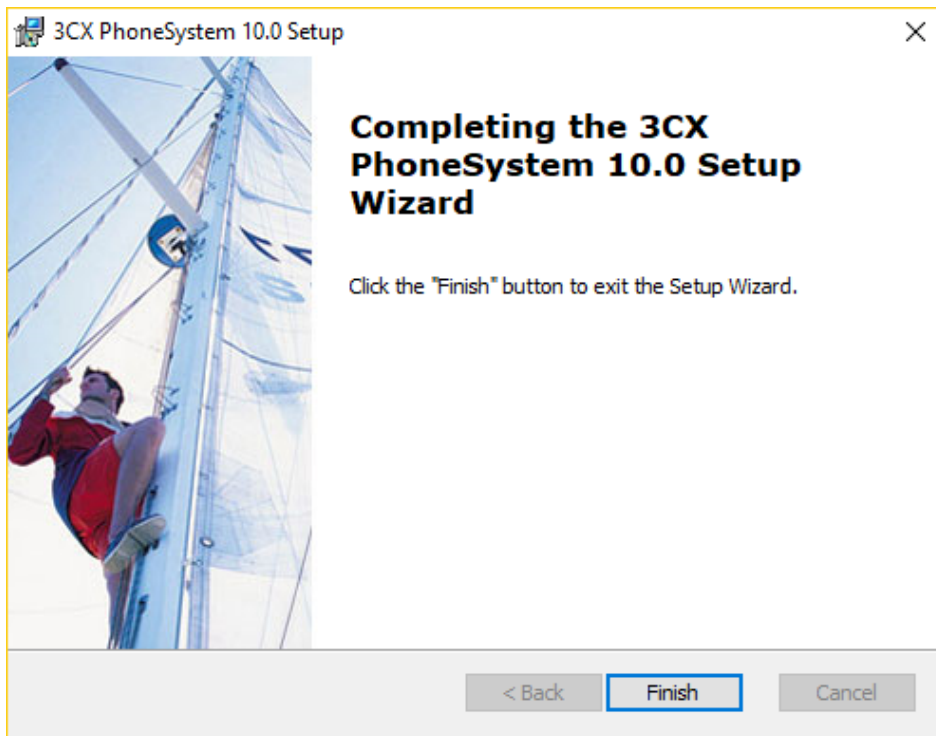
**Objectif** : installer, configurer et analyser le fonctionnement d'un système de téléphonie sur IPv4 compatible avec le protocole SIP (Session Initiation Protocol) et couplant Téléphonie, Vidéoconférence et messagerie électronique.

- Répondre aux questions et reportez vos réponses sur ce document. Les captures d'écran sont appréciées pour illustrer/valider vos réponses. Convertir votre document en PDF si possible avant envoi par email : [master2srs.dir@gmail.com](mailto:master2srs.dir@gmail.com) en précisant dans le sujet du mail : « **M1 Cyber – TP3 ToIP** ».
- Date limite de remise de votre rapport par email : 21 avril 17h00
- Pour répondre aux questions suivantes veuillez installer les logiciels fournis et utiliser la documentation associée. Aidez vous si besoin d'Internet.

### - Partie 1 : Téléphonie sur IP avec le protocole SIP en mode de communication via un serveur téléphonique (SIP proxy) et authentification des clients

10. **install** the 3CX SIP proxy server. **Create** three (3) user accounts (BOB (100), ALICE (101) and PAUL (102)) in the SIP server administration console to authenticate each SIP client during the calling process. <https://www.3cx.fr>






Ajouter l'extension d'un utilisateur

Ajouter une extension utilisateur

Veillez saisir le nom et l'adresse e-mail de l'utilisateur de l'extension. Spécifiez l'adresse MAC et le modèle du téléphone pour le configurer automatiquement.  
[Veillez consulter les guides de configuration du téléphone pour plus](#)

Numéro d'extension:	<input type="text" value="100"/>	?
Prénom:	<input type="text" value="BOB"/>	?
Nom:	<input type="text"/>	?
Adresse e-mail:	<input type="text"/>	?
ID d'authentification:	<input type="text" value="100"/>	?
Mot de passe d'authentification:	<input type="text" value="y2spebg"/>	?
PIN de la messagerie vocale:	<input type="text" value="7978"/>	?
Adresse MAC (Facultatif)	<input type="text"/>	?
Modèle (Facultatif)	<input type="text" value="No model"/>	?
Sélectionnez une Interface:	<input type="text" value="10.188.153.206"/>	?

Welcome to 3CX User Settings Wizard


Software based PBX for Windows®

**Paramètres généraux**  
Langue  
Local IP  
Public IP  
Paramètres  
Nb. de chiffres pour les numéros d'extensions  
Serveur de messagerie  
Connexion de l'administrateur  
**Paramètres des téléphones**  
**Extensions**  
Extensions des opérateurs  
Passerelles VoIP  
**Terminer**  
Enregistrer la configuration  
Enregistrement  
Terminer

**Création des extensions utilisateurs**

Maintenant, créez une ou plusieurs extensions sur le système téléphonique 3CX. Si vous utilisez des téléphones SIP supportés et que vous suivez le guide approprié, les téléphones pourront être configurés automatiquement.

Extension	Prénom	Nom	E-mail
100	BOB		
101	ALICE		
102	PAUL		

< >

Ajout ext. Suppr. ext.

< Retour Suivant > Terminer

11. **Configure** your first SIP softphone clients to create a profile using BOB account to log on to your SIP proxy server. **Configure** your second SIP 3CX VoIP softphone to create another profile using ALICE account to log on to the SIP proxy server of your student mate. You may use a laptop or your mobile/Tablet devices to setup your lab.

- Beware : we may need to update your hosts file on server and client systems
- Beware : use PCMA or PCMU audio codec in your VoIP clients.
- Beware : use only numbers (no letters or special characters) for the password
- Beware : deactivate or reconfigure your windows firewall to open the voip tcp/udp ports.

Account settings

Account name: BOB

Caller ID: 100

Credentials

Enter your SIP account credentials

Extension: 100

ID: 100

Password: \*\*\*\*\*

My location

Specify the IP of your PBX/SIP server

☒ I am in the office - local IP 192.168.137.101 of PBX

☐ I am out of the office - external IP 192.168.137.101 of PBX

☐ Use 3CX Tunnel

Eliminates firewall configuration. Requires 3CX Phone System for Windows

Local IP of remote PBX: 10.188.153.206

Tunnel password: \*\*\*\*\* Port: 5000

☐ Use Outbound Proxy server

Required by some VoIP Providers. Specify IP or name.

☐ Perform provisioning from following URL:

http://

Advanced settings OK Cancel

Account advanced settings

PBX voicemail:

STUN server: stun.3cx.com

Registration time: 2 minutes

SIP transport: UDP Certificates

RTP mode: Normal

☒ Support RFC2833 DTMF

Payload number: 101

☐ Support INBAND DTMF

☐ Support SIPINFO DTMF

Audio codecs

PCMU

PCMA

GSM

Up

Down

Video codecs

H.263 (ffdsnow)

Up

Down

Video formats

176 x 144

352 x 288

128 x 96

704 x 576

Up

Down

OK Cancel



host:5000/management/MainForm.wgx

mètres Liens Aide

l'activité du serveur | Ajout. extension | Ajout. passerelle RTC | Assistant opérateur VoIP | Créer une règle sortante | Cré

**Etat des extensions**

✖ Déconnecter l'appel | 🗖 Afficher le filtre

	Etat	Extension	Statuts utilisateurs	Files d'attente	Nom
●	Enregistré (inoccupé)	100	Disponible	Appel	BOB
●	Non enregistré	101	Disponible	Appel	ALICE
●	Non enregistré	102	Disponible	Appel	PAUL
●	Non enregistré	103	Disponible	Appel	

Using Wireshark, answers the following questions :

- **Capture, display and insert in this document the SIP sequence when the terminal is registering at the server (user authentication and registration procedures).**

Source	Destination	Protocol	Length	Info
192.168.137.101	192.168.137.101	SIP	596	Request: REGISTER sip:192.168.137.101:5060 (1 binding)
192.168.137.101	192.168.137.101	SIP	565	Status: 407 Proxy Authentication Required
192.168.137.101	192.168.137.101	SIP	812	Request: REGISTER sip:192.168.137.101:5060 (1 binding)
192.168.137.101	192.168.137.101	SIP	486	Status: 200 OK (1 binding)
192.168.137.101	192.168.137.101	SIP	640	Request: SUBSCRIBE sip:100@192.168.137.101:5060;transport=UDP
192.168.137.101	192.168.137.101	SIP	566	Status: 407 Proxy Authentication Required
192.168.137.101	192.168.137.101	SIP	874	Request: SUBSCRIBE sip:100@192.168.137.101:5060;transport=UDP
192.168.137.101	192.168.137.101	SIP	439	Status: 489 Event Package Not Supported

- **Are the UserID and password transmitted in cleartext between your terminal and the server (yes/no) ? If not, explain how it does ?**

```

▼ Message Header
  > Via: SIP/2.0/UDP 0.0.0.0:62779;branch=z9hG4bK-d8754z-e513df58bd745346-1---d8754z-;rport
    Max-Forwards: 70
  > Contact: <sip:100@0.0.0.0:62779;rinstance=e70f827219e8e9e8>
  > To: "100"<sip:100@192.168.137.101:5060>
  > From: "100"<sip:100@192.168.137.101:5060>;tag=48324d09
    Call-ID: OGUXMDQxZDlhZTllZDVhZWl5MjZjhlNmJmOGIyYWE.
    [Generated Call-ID: OGUXMDQxZDlhZTllZDVhZWl5MjZjhlNmJmOGIyYWE.]
  > CSeq: 1 REGISTER
    Expires: 120
    Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REGISTER, SUBSCRIBE, NOTIFY, REFER, INFO, MESS.
    Supported: replaces
    User-Agent: 3CXPhone 6.0.20943.0

```

No, we can only see the UserID which is same as extension number, but password is encrypted. We can't find it in cleartext.

#### – What is the server port number ?

Port 5060 is used

```

> Internet Protocol Version 4, Src: 192.168.137.101, Dst: 37.171.169.38
> User Datagram Protocol, Src Port: 64815, Dst Port: 5060
▼ Session Initiation Protocol (REGISTER)
  > Request-Line: REGISTER sip:37.171.169.38:5060 SIP/2.0
  ▼ Message Header
    > Via: SIP/2.0/UDP 192.168.137.101:64815;branch=z9hG4bK-d8754z-3d62

```

#### – What is the SIP method used to register to the server ?

Client send first a "REGISTER" request, with important data like server address, its own IP, extension number, connection time, protocol (UDP)... Then the server returns a 407 Authentication required so the client send his credentials.

```

▼ Session Initiation Protocol (REGISTER)
  > Request-Line: REGISTER sip:37.171.169.38:5060 SIP/2.0
  ▼ Message Header
    > Via: SIP/2.0/UDP 192.168.137.101:64815;branch=z9hG4bK-d8754z-3d62424bd0437302-1---d8754z-;rport
      Max-Forwards: 70
    ▼ Contact: <sip:101@37.173.92.71:50557;transport=UDP;rinstance=428366dbe9b286a7>
      > Contact URI: sip:101@37.173.92.71:50557;transport=UDP;rinstance=428366dbe9b286a7
    > To: "101"<sip:101@37.171.169.38:5060>
    > From: "101"<sip:101@37.171.169.38:5060>;tag=1972f017
      Call-ID: NjNlYTQ2MTQyZTBiMGE5ZjU3ZWYzYTk2NTBhOWEyZDc.
      [Generated Call-ID: NjNlYTQ2MTQyZTBiMGE5ZjU3ZWYzYTk2NTBhOWEyZDc.]
    ▼ CSeq: 1 REGISTER
      Sequence Number: 1
      Method: REGISTER
      Expires: 120
      Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REGISTER, SUBSCRIBE, NOTIFY, REFER, INFO, MESSAGE
      Supported: replaces
      User-Agent: 3CXPhone 6.0.20943.0
      Content-Length: 0

```



#### – What is the SIP code number used to register ?

We can't find code number in the REGISTER request.

#### – What is the SIP code number used by the server to confirm your registration ?

Code "200" is returned by server to tell everything has been successful, like for HTTP protocol.

11 **Initiate** a call between 2 SIP Softphones (example BOB -> ALICE) through your SIP server using an extension number (example "100"). Using Wireshark, **capture** the sequence of SIP messages between the 2 terminals and the server from the beginning to the end of your voip session.

	Etat	Extension	Statuts utilisateurs	Files d'attente	Nom
	Enregistré (inoccupé)	100	Disponible	Appel	BOB
	Enregistré (inoccupé)	101	Disponible	Appel	ALICE

- Using Wireshark options, display and insert in this document, the flow chart of the SIP signalling messages exchanged between the two terminals from Registration to End call. Use advanced wireshark options. Look at the

Time	Source	Destination	Protocol	Length	Info
7 3.370624	192.168.137.101	192.168.137.101	SIP/SDP	1252	Request: INVITE sip:101@192.168.137.101:5060
267 3.479680	192.168.137.101	192.168.137.101	SIP	339	Status: 100 Trying
373 3.836975	192.168.137.101	192.168.137.101	SIP	435	Status: 180 Ringing
585 8.245267	192.168.137.101	192.168.137.101	SIP/SDP	809	Status: 200 OK
586 8.354027	192.168.137.101	192.168.137.101	SIP	698	Request: ACK sip:101@192.168.137.101:5060
1414 13.007213	192.168.137.101	192.168.137.101	SIP	698	Request: BYE sip:101@192.168.137.101:5060
1535 13.115828	192.168.137.101	192.168.137.101	SIP	427	Status: 200 OK

- Are the source and destination port numbers used by the clients identical to the ones used with the direct voice call procedure (Partie 1)?

No, they are not the same.

Port used in Part 1:

1414 13.007213	192.168.137.101	192.168.137.101	SIP	698	Request: BYE s
----------------	-----------------	-----------------	-----	-----	----------------

Frame 1414: 698 bytes on wire (5584 bits), 698 bytes captured (5584 bits) on interface \De  
Null/Loopback  
Internet Protocol Version 4, Src: 192.168.137.101, Dst: 192.168.137.101  
User Datagram Protocol, Src Port: 62779 Dst Port: 5060  
Session Initiation Protocol (BYE)  
> Request-Line: BYE sip:101@192.168.137.101:5060 SIP/2.0  
v Message Header  
> Via: SIP/2.0/UDP 192.168.137.101:62779;branch=z9hG4bK-d8754z-9a073d4bd54ca55f-1---d8

Ports used during call:

758 11.704673	127.0.0.1	127.0.0.1	TCP	44	53
759 11.704776	127.0.0.1	127.0.0.1	TCP	52	53

Null/Loopback  
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  
Transmission Control Protocol, Src Port: 53373, Dst Port: 5482, Seq: 1, Ack: 9  
Source Port: 53373  
Destination Port: 5482

- Are the voice IP packets passing through the SIP server or directly between the 2 clients ?

Voice IP packets are communicated directly between both clients.

- What is the role of the SIP server during this test ?

The SIP server is used to manage sessions and allow connexion between two phones.



Les parties 2, 3, 4, et 5 ci-dessous vous permettront d'implémenter et tester des fonctionnalités CTI (couplage téléphonie et informatique) :

## Partie 2 : Call transfert and Call redirection

12. BOB (100), ALICE (101) and PAUL (102) are logged on to your SIP server. Establish a voice call between BOB and ALICE, and after ALICE hangs-up, she **Transfers** the active call to PAUL.

Source	Destination	Protocol	Length	Info
192.168.137.101	192.168.137.174	SIP/SDP	1060	Request: INVITE sip:101@192.168.137.174:59083;rinstance=5ed004e40b
192.168.137.174	192.168.137.101	SIP	464	Status: 180 Ringing
192.168.137.174	192.168.137.101	SIP/SDP	996	Status: 200 OK
192.168.137.101	192.168.137.174	SIP	502	Request: ACK sip:101@192.168.137.174:59083;rinstance=5ed004e40b2f4
192.168.137.174	192.168.137.101	SIP/SDP	1063	Request: INVITE sip:100@192.168.137.101:5060, in-dialog
192.168.137.101	192.168.137.174	SIP	362	Status: 100 Trying
192.168.137.101	192.168.137.174	SIP/SDP	1014	Status: 200 OK
192.168.137.174	192.168.137.101	SIP	496	Request: ACK sip:100@192.168.137.101:5060
192.168.137.174	192.168.137.101	SIP	587	Request: REFER sip:100@192.168.137.101:5060, in-dialog
192.168.137.101	192.168.137.174	SIP	458	Status: 202 Accepted
192.168.137.101	192.168.137.174	SIP/si...	613	Request: NOTIFY sip:101@192.168.137.174:59083;rinstance=5ed004e40b
192.168.137.101	192.168.137.78	SIP	653	Request: INVITE sip:102@192.168.137.78:59654;rinstance=2b163319c4b
192.168.137.101	192.168.137.78	SIP	653	Request: INVITE sip:102@192.168.137.78:43974;rinstance=9048adf5f50
192.168.137.78	192.168.137.101	SIP	347	Status: 100 Trying
192.168.137.174	192.168.137.101	SIP	459	Status: 200 OK
192.168.137.78	192.168.137.101	SIP	575	Status: 180 Ringing
192.168.137.101	192.168.137.78	SIP	653	Request: INVITE sip:102@192.168.137.78:43974;rinstance=9048adf5f50
192.168.137.101	192.168.137.78	SIP	653	Request: INVITE sip:102@192.168.137.78:43974;rinstance=9048adf5f50
192.168.137.101	192.168.137.78	SIP	653	Request: INVITE sip:102@192.168.137.78:43974;rinstance=9048adf5f50
192.168.137.78	192.168.137.101	SIP/SDP	1038	Status: 200 OK
192.168.137.101	192.168.137.174	SIP/si...	622	Request: NOTIFY sip:101@192.168.137.174:59083;rinstance=5ed004e40b
192.168.137.174	192.168.137.101	SIP	459	Status: 200 OK
192.168.137.174	192.168.137.101	SIP	536	Request: BYE sip:100@192.168.137.101:5060
192.168.137.101	192.168.137.78	SIP/SDP	798	Request: ACK sip:102@192.168.137.78:59654;rinstance=2b163319c4b7a2
192.168.137.101	192.168.137.174	SIP	437	Status: 200 OK
192.168.137.101	192.168.137.78	SIP	653	Request: INVITE sip:102@192.168.137.78:43974;rinstance=9048adf5f50
192.168.137.78	192.168.137.101	SIP	566	Request: BYE sip:100@192.168.137.101:5060
192.168.137.101	192.168.137.78	SDP	428	Status: 200 OK

- What is the SIP message/method used to do this call transfer ?

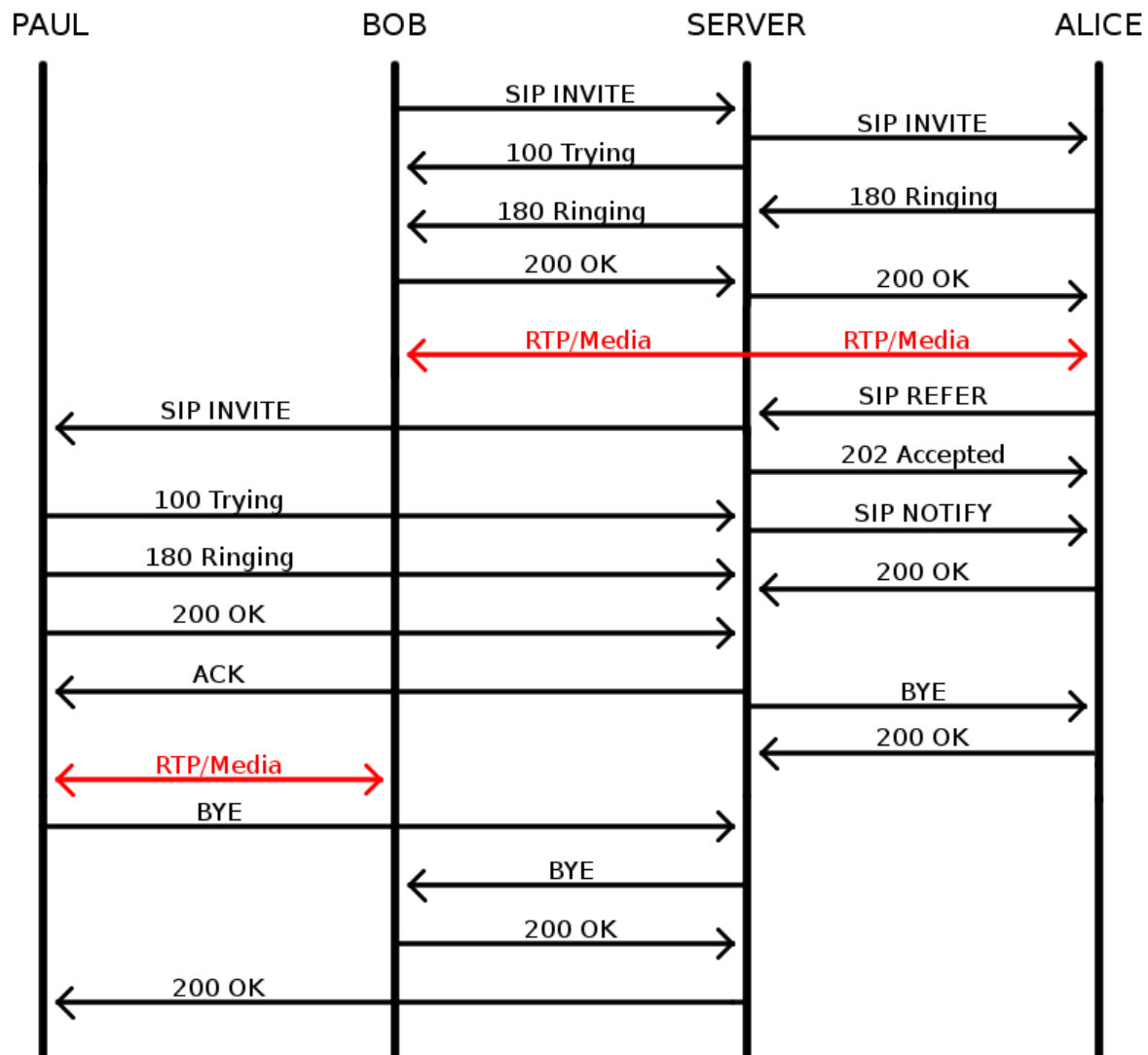
During the call, ALICE sends a request REFER to the server. Then the server requests INVITE to PAUL and tell ALICE the REFER is OK (200). Then PAUL is Trying (100) to call so ALICE receives a SIP NOTIFY. After that, PAUL and ALICE both send OK (200) to the server to tell they're ready. So the server transmits an ACK to PAUL and BYE to ALICE. ALICE answers OK (200). Finally, the call between PAUL and BOB is launched.

- What is the SIP code used ?

Server sends "202 Accepted" to ALICE to notify her that the refer has been accepted, PAUL sends "100 Trying" and "180 Ringing" to the server to initiate the second call and PAUL and ALICE send "200 OK" to tell they are ready.

Below there is a diagram showing SIP packets sent from the first call to the end of the second call.





13. Modify the SIP server and the ALICE profile, to automatically redirect an incoming call to ALICE to PAUL when ALICE is not answering after 10 secondes ringing.

- capture the server configuration screen for setting up this functionality. Insert this picture in this document.

### Modifier une extension-101

Modifiez les paramètres de l'extension et cliquez sur 'OK' ou 'Appliquer' pour enregistrer les modifications.

Général	Règles de transfert	Téléconfiguration des téléphones	Autre	Horaires de bureau
<div> <div>Disponible</div> <div>Absent</div> <div>En dehors de l'entreprise</div> <div>Personnalisé #1</div> <div>Personnalisé #2</div> <div>Exceptions</div> </div>				
Configurez où les appels seront redirigés lorsque l'utilisateur sera en ligne ou qu'il ne répondra pas.				
<b>Pas de réponse</b>				
Si l'appel n'est pas répondu dans <input type="text" value="10"/> Secondes, puis:				
<input type="radio"/> Envoyer l'appel vers ma messagerie vocale <input type="radio"/> Envoyer l'appel vers mon numéro de mobile <input checked="" type="radio"/> Envoyer l'appel vers <div> <input type="text" value="extension - 102 PAUL"/> </div>				
<input type="radio"/> Un numéro externe ou un ID skype <input type="checkbox"/> Rebond™ (Offrir l'option de confirmer à accepter) <input type="radio"/> Déconnecter l'appel				

### Partie 3 : Voice Messaging and Voice Mail

14. **modify** the SIP server and ALICE profile to redirect an inbound call to the voice messaging system if ALICE is not responding after 10 seconds.

- capture a picture of your screen configuration and insert it in this document.

Général Règles de transfert Téléconfiguration des téléphones Autre Horaires de bureau

Disponible Absent En dehors de l'entreprise Personnalisé #1 Personnalisé #2 Exceptions

Configurez ou les appels seront redirigés lorsque l'utilisateur sera en ligne ou qu'il ne répondra pas.

Pas de réponse

Si l'appel n'est pas répondu dans  Secondes, puis:

☒ Envoyer l'appel vers ma messagerie vocale

☐ Envoyer l'appel vers mon numéro de mobile

- Capture the SIP message/method sequence of this scenario and insert it in this document.

Time	Source	Destination	Protocol	Length	Info
2.868468	192.168.137.101	192.168.137.174	SIP/SDP	1060	Request: INVITE sip:101@192.168.137.174:64050;rins
2.988822	192.168.137.174	192.168.137.101	SIP	464	Status: 180 Ringing
12.893336	192.168.137.101	192.168.137.174	SIP	515	Request: CANCEL sip:101@192.168.137.174:64050;rins
13.012160	192.168.137.174	192.168.137.101	SIP	459	Status: 200 OK
13.012160	192.168.137.174	192.168.137.101	SIP	406	Status: 487 Request Terminated
13.013179	192.168.137.101	192.168.137.174	SIP	420	Request: ACK sip:101@192.168.137.174:64050;rinstan

- What is the SIP message and code number used by the server to indicate that ALICE is not available ?

The SIP message from ALICE is a CANCEL request, where BOB answer with a 200 OK and 487 Request Terminated packets.

- What is the phone number to dial to access to the voice messages recorded in the Server ?

This is 999 (and 99 if we had only 2 digits extensions). We have then to enter the PIN written in extension's profile in the server.

- With wireshark, identify the network protocols that are used to access and listen to this voice messages ? Do you use RTSP/RTP/RTCP (yes/no) ?

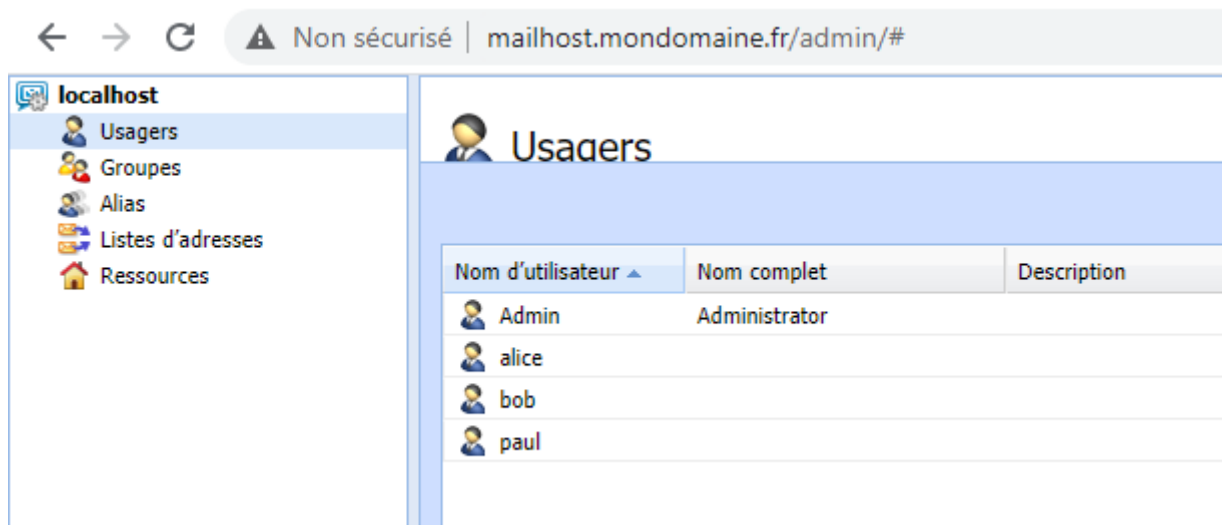
Based on Wireshark, only RTP is used. We couldn't find RTSP or RTCP packet.

Time	Source	Destination	Protocol	Length	Info
2197 53.223780	192.168.137.101	192.168.137.174	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x2213, Seq=13873, Time=
2198 53.231681	192.168.137.174	192.168.137.101	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x3D6C, Seq=20253, Time=
2199 53.238613	192.168.137.101	192.168.137.174	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x2213, Seq=13874, Time=
2200 53.251740	192.168.137.174	192.168.137.101	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x3D6C, Seq=20254, Time=
2201 53.266687	192.168.137.174	192.168.137.101	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x3D6C, Seq=20255, Time=
2202 53.272917	192.168.137.101	192.168.137.174	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x2213, Seq=13875, Time=
2203 53.279460	192.168.137.101	192.168.137.174	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x2213, Seq=13876, Time=
2204 53.286679	192.168.137.174	192.168.137.101	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x3D6C, Seq=20256, Time=
2205 53.306200	192.168.137.101	192.168.137.174	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x2213, Seq=13877, Time=
2206 53.306554	192.168.137.174	192.168.137.101	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x3D6C, Seq=20257, Time=
2207 53.318307	192.168.137.101	192.168.137.174	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x2213, Seq=13878, Time=
2208 53.331623	192.168.137.174	192.168.137.101	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x3D6C, Seq=20258, Time=
2209 53.337477	192.168.137.101	192.168.137.174	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x2213, Seq=13879, Time=
2210 53.346562	192.168.137.174	192.168.137.101	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x3D6C, Seq=20259, Time=
2211 53.363453	192.168.137.101	192.168.137.174	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x2213, Seq=13880, Time=
2212 53.371582	192.168.137.174	192.168.137.101	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x3D6C, Seq=20260, Time=
2213 53.380570	192.168.137.101	192.168.137.174	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x2213, Seq=13881, Time=
2214 53.386578	192.168.137.174	192.168.137.101	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x3D6C, Seq=20261, Time=
2215 53.403029	192.168.137.101	192.168.137.174	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x2213, Seq=13882, Time=

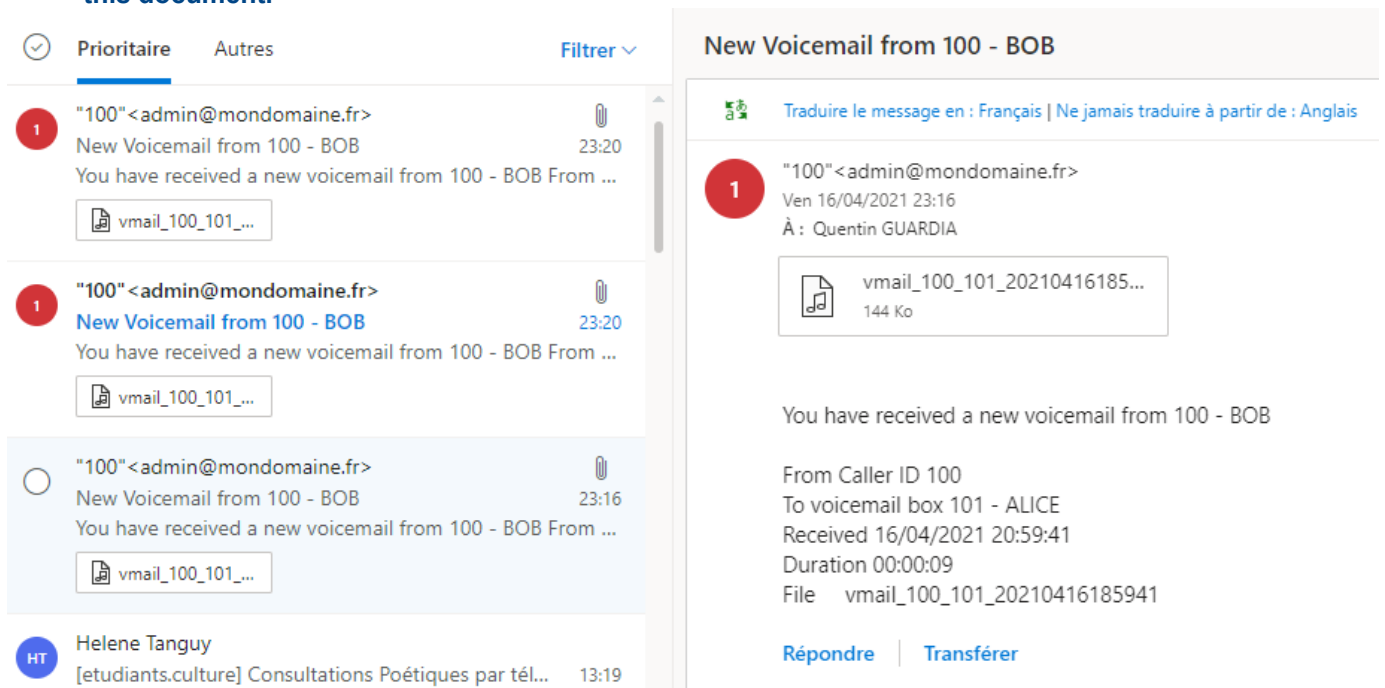
15. Install and configure an Email Server and configure it with 4 accounts (ADMIN, BOB, ALICE & PAUL)

In the VOIP Server, **Configure** the ALICE profile to automatically receive an email notification with the attached voice message using an external SMTP server (your webmail or your university email account)

We used kerio mailserver:



- capture a screen picture of your email message with the attached voice mail. Insert this picture in this document.



- **What is the audio format of this voice message ?**  
The audio file is a .wav file.
- **What is the email protocol to send this message to the client (POP3, IMAP4, SMTP) ?**  
The protocol SMTP is used as shown below:

smtp					
o.	smtp	Source	Destination	Protocol	Length Info
3118	16.048456	192.168.137.101	192.168.137.101	SMTP	100 S: 220 DESKTOP-JNTG6MS Kerio MailServer 6.7.2 ESMTP ready
3120	16.048557	192.168.137.101	192.168.137.101	SMTP	66 C: EHLO DESKTOP-JNTG6MS
3122	16.048738	192.168.137.101	192.168.137.101	SMTP	210 S: 250-DESKTOP-JNTG6MS   AUTH CRAM-MD5 PLAIN LOGIN DIGEST-MD5 NTLM
3124	16.049816	192.168.137.101	192.168.137.101	SMTP	112 C: AUTH ntlm TlRMTVNTUAAABAAAAB4IIogAAAAAAAAAAAAAAAAAAAAKA0SCAAADw==
3126	16.050759	192.168.137.101	192.168.137.101	SMTP	370 S: 334 TlRMTVNTUAAACAAAAGhAeADgAAAFgoqi4q4azDiV9ekAAAAAAAAAAJgAmABWAA
3128	16.052232	192.168.137.101	192.168.137.101	SMTP	690 C: TlRMTVNTUAAADAAAAGAAAYIAAAAABKAUoBmAAAAAAAAABYAAACgAKAFgAAAAeAB4AYg
3133	19.055481	192.168.137.101	192.168.137.101	SMTP	77 S: 535 5.7.0 Authentication failed
3135	19.055742	192.168.137.101	192.168.137.101	SMTP	65 C: AUTH login User: QWRtaW4=
3137	19.055970	192.168.137.101	192.168.137.101	SMTP	62 S: 334 UGFzc3dvcmQ6
3139	19.056113	192.168.137.101	192.168.137.101	SMTP	54 C: Pass: QWRtaW4x
3141	19.056549	192.168.137.101	192.168.137.101	SMTP	81 S: 235 2.0.0 Authentication successful
3143	19.056747	192.168.137.101	192.168.137.101	SMTP	77 C: MAIL FROM:<admin@mondomaine.fr>

#### Partie 4 : Interactive Voice Assistant

16. Modify ALICE profile to activate an Interactive Voice Assistant when an incoming call is not answered after 10 sec. Record a "Welcome voice message" in audio WAVE format that propose the following interactive scenario to the caller:

Please dial #1 : to transfer your call to BOB

Please dial #2 : to transfer your call to the voice messaging

Please dial #3 : to repeat listen this message again

- capture a screen picture of your email message with the attached voice mail. Insert this picture in this document.

Número d'extension virtuelle (Ne peut pas être utilisé comme extension)	<input type="text" value="800"/>	?
Nom	<input type="text" value="Bienvenue"/>	?
Rediriger vers MS Exchange	<input type="checkbox"/>	?
Directive	<input type="text" value="bienvenue.wav"/>	

---

Options du menu

Touche	Touche	Numéro de l'extension
0	<input type="text"/>	<input type="text"/>
1	Connect to Extension	100 BOB
2	Transférer à la boîte vocale	101 ALICE
3	Répéter la directive	
4	<input type="text"/>	
5	<input type="text"/>	
6	<input type="text"/>	
7	<input type="text"/>	
8	<input type="text"/>	
9	<input type="text"/>	
Délai	<input type="text" value="60"/>	

## Modifier une extension-101

Modifiez les paramètres de l'extension et cliquez sur 'OK' ou 'Appliquer' pour enregistrer les modifications.

Général Règles de transfert Téléconfiguration des téléphones Autre Horaires de bureau

Disponible Absent En dehors de l'entreprise Personnalisé #1 Personnalisé #2 Exceptions

Configurez où les appels seront redirigés lorsque l'utilisateur sera en ligne ou qu'il ne répondra pas.

Pas de réponse

Si l'appel n'est pas répondu dans  Secondes, puis: ?

☐ Envoyer l'appel vers ma messagerie vocale

☐ Envoyer l'appel vers mon numéro de mobile

☒ Envoyer l'appel vers  ?

☐ Un numéro externe ou un ID skype  ?

☐ Rebond™ (Offrir l'option de confirmer à accepter)

☐ Déconnecter l'appel

## Partie 5 : VOIP and VideoConferencing with 3CX clients and server

17 Configure the **3CX VOIP clients** to use Video-Conferencing without any security options.

Account advanced settings

PBX voicemail:

STUN server:

Registration time:  minutes

SIP transport:  Certificates

RTP mode:

☒ Support RFC2833 DTMF  
Payload number:

☐ Support INBAND DTMF

☐ Support SIPINFO DTMF

Audio codecs

PCMU Up

PCMA Down

GSM

Video codecs

H.263 (ffdsnow) Up

Down

Video formats

176 x 144 Up

352 x 288 Down

128 x 96

704 x 576

OK Cancel

Preferences

Sound devices

Configure sound devices used by the phone

Microphone:

Speaker:

Ringin:

Video

Video source:  Configure

☒ Allow video calls

☒ Start sending video when call is established

☐ Do not send video when phone is inactive or hidden

General network settings

RTP ports:

Local SIP port:  ☒ Any

Behavior

Define behavior of your 3CXPhone

☐ Automatically starts at Windows logon

☒ Automatically check for updates

☒ Expand + sign to 00

☐ Prevent answering pop-up from stealing focus on ringing

☐ Microphone noise reduction

When computer is locked:

When screensaver starts:

Visual look

Set the visual look of your 3CXPhone

Skin:

Language:  Download others

OK Cancel



- **What is the video codec type used ? What is the video resolution (pixels) ?**  
The H.263 ffdshow codec is used, with a resolution of 176\*144 pixels.
- **What is the audio codec type used ?**  
PCMA audio codec is used.
- **How many sockets (TCP and UDP ports) at the client side are used for this videoconference ?**  
Ports from 40 000 to 40 049 are used during videoconference, looking at the preferences window and Wireshark

## Partie 6 : VOIP and Security with 3CX

### 18. VOIP vulnerabilities :

- search on the internet about the different vulnerabilities and threats on TOIP services. List these on a table below.

Man-In-The-Middle and replay
Denial of Service
Hijacking and theft data which can cost lots of fees when hacker use them to do expansive acts
Intrusion on the organism, to put viruses and trojan
Internet Bound Traffic: packets can be sniffed
Spoofing: a hacker can act with society's properties to ask credentials to customers
Call tampering: the hacker send lots of datas to affect clarity of call
Eavesdropping (ex:VOMIT,...)
Spams (ex:SPIT,...)
Gateway, Firewall, Application, Phones can be also victims of vulnerabilities and so on...

- initiate a voice call (without security using PCMA or PCMU codec) and capture the voice packets with wireshark. Record the voice packet into a file with .wav file extension. Play this file with your media player to listen to the conversation.



Fichier Editer Vue Aller Capture Analyser Statistiques **Telephonie** Wireless Outils Aide

rtp

o.	Time	Source	Destination
14	5.818215	192.168.137.78	192.168.
15	5.818215	192.168.137.78	192.168.
16	5.818544	192.168.137.78	192.168.
17	5.818544	192.168.137.78	192.168.
18	5.818544	192.168.137.78	192.168.
19	5.818544	192.168.137.78	192.168.
20	5.818544	192.168.137.78	192.168.
21	5.818544	192.168.137.78	192.168.
22	5.818544	192.168.137.78	192.168.
23	5.818544	192.168.137.78	192.168.
24	5.818544	192.168.137.78	192.168.
25	5.818544	192.168.137.78	192.168.
30	6.284430	192.168.137.101	192.168.
31	6.304449	192.168.137.101	192.168.
32	6.324551	192.168.137.101	192.168.
33	6.344363	192.168.137.101	192.168.
34	6.364379	192.168.137.101	192.168.
35	6.384370	192.168.137.101	192.168.
36	6.393119	192.168.137.78	192.168.137.101

Appels VoIP  
ANSI  
GSM  
IAX2 Stream Analysis  
Messages ISUP  
LTE  
MTP3  
Osmux  
**RTP**  
RTSP  
SCTP  
Opérations SMPP  
Messages UCP  
H.225  
SIP Flux  
SIP Statistics  
WAP-WSP Packet Counter

Flux RTP  
Analyse de Flux

Frame 14: 54 bytes on wire (432 bits). 54 bytes captured (432 bits) on interface \Device\NPF {B7389593-8B1

Wireshark - Analyse flux RTP - Wi-Fi

Forward

192.168.137.78:54408 → 192.168.137.101:40018

SSRC 0xeaafd04a  
Max Delta 179.02 ms @ 463  
Max Jitter 65011677.08 ms  
Mean Jitter 1478985.85 ms  
Max Skew 536870336.97 ms  
RTP Packets 363  
Expected 363  
Lost 0 (0.00 %)  
Seq Errs 0  
Start at 5.818215 s @ 14  
Duration 7.43 s  
Clock Drift -7969360 ms  
Freq Drift -8572412 Hz (-107255.15 %)

Reverse

:0 → :0

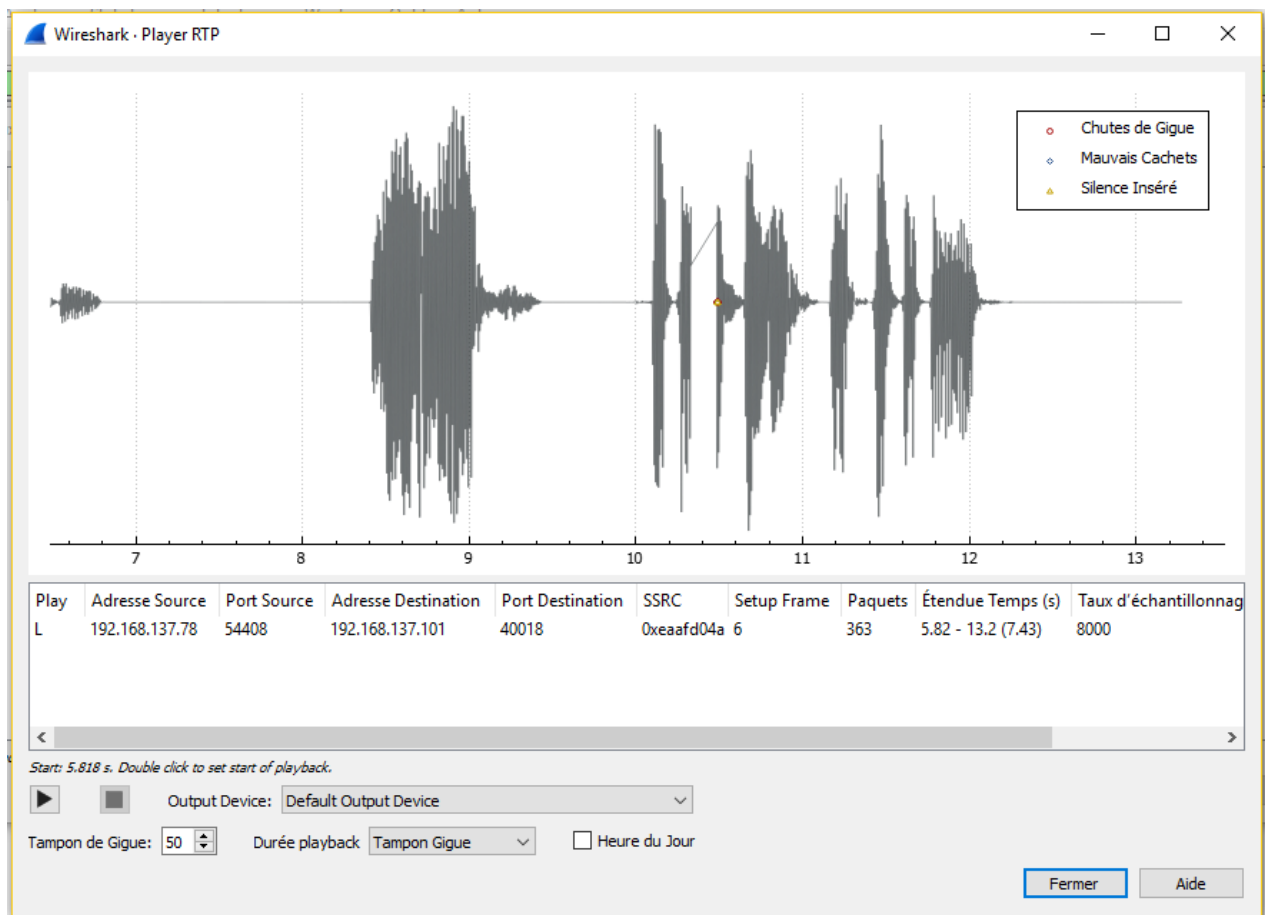
SSRC 0x00000000  
Max Delta 0.00 ms @ 0  
Max Jitter 0.00 ms  
Mean Jitter 0.00 ms  
Max Skew 0.00 ms  
RTP Packets 0  
Expected 1  
Lost 1 (100.00 %)  
Seq Errs 0  
Start at 0.000000 s @ 0  
Duration 0.00 s  
Clock Drift 0 ms  
Freq Drift 1 Hz (0.00 %)

1 flux trouvés.

Paquet	Séquence	Delta(ms)	Gigue(ms)	Déviation	Bande passante	Marqueur	Etat
14	30317	0.00	0.00	0.00	0.32		✓
15	30318	0.00	0.00	0.00	0.64		✓
16	30319	0.33	0.00	0.00	0.96		✓
17	30320	0.00	0.00	0.00	1.28		✓
18	30321	0.00	0.00	0.00	1.60		✓
19	30322	0.00	0.00	0.00	1.92		✓
20	30323	0.00	0.00	0.00	2.24		✓
21	30324	0.00	0.00	0.00	2.56		✓
22	30325	0.00	0.00	0.00	2.88		✓
23	30326	0.00	0.00	0.00	3.20		✓
24	30327	0.00	0.00	0.00	3.52		✓
25	30328	0.00	0.00	0.00	3.84		✓
36	30329	574.57	33554396.08	536870336.97	5.44	*	Payload changed to ...
37	30330	0.00	65011677.08	-555.03	7.04		✓
38	30331	0.21	60948448.50	-535.24	8.64		✓
39	30332	0.00	57139171.71	-515.24	10.24		✓
40	30333	0.00	53567974.73	-495.24	11.84		✓
41	30334	0.00	50219977.56	-475.24	13.44		✓
42	30335	0.00	47081230.21	-455.24	15.04		✓
43	30336	0.00	44138654.58	-435.24	16.64		✓
45	30337	17.81	41379988.80	-433.05	18.24		✓
47	30338	18.01	38793739.63	-431.06	19.84		✓
49	30339	21.04	36369130.96	-432.10	21.44		✓
51	30340	20.96	34096060.34	-433.06	23.04		✓
53	30341	18.00	31965056.69	-431.06	24.64		✓
55	30342	21.02	29967240.71	-432.07	26.24		✓
57	30343	18.62	28094288.26	-430.69	27.84		✓
59	30344	22.35	26338395.39	-433.04	29.44		✓

Enregistrer Fermer Jouer Flux Aide





We want now to secure the TOIP communications by configuring both the VOIP clients and the server to establish a secured (encrypted) authentication between the clients and the server AND a secured (encrypted) voice call between the two VOIP client.

Configure the 3CX Client with security options : TLS for SIP signalling and SRTP for voice media.

The image shows three screenshots of the 3CX Client configuration interface.

**Account advanced settings:** This window shows various configuration options. Under 'SIP transport', 'TLS' is selected. Under 'RTP mode', 'Only secure' is selected. The 'Support RFC2833 DTMF' checkbox is checked, and the 'Payload number' is set to 101. The 'Audio codecs' section shows 'PCMU', 'PCMA', and 'GSM'. The 'Video codecs' section shows 'H.263 (ffdsnow)'. The 'Video formats' section shows '176 x 144', '352 x 288', '128 x 96', and '704 x 576'.

**Account settings:** This window shows the account configuration. The 'Account name' is 'BOB' and the 'Caller ID' is '100'. The 'Credentials' section shows the 'Extension' as '100', the 'ID' as '100', and the 'Password' as '\*\*\*\*\*'. The 'My location' section shows the 'Specify the IP of your PBX/SIP server' with 'I am in the office - local IP' selected, and the IP address '192.168.137.101:5061' of PBX. The 'Use 3CX Tunnel' checkbox is checked, and the 'Local IP of remote PBX' is '10.188.153.206'. The 'Tunnel password' is '\*\*\*\*\*' and the 'Port' is '5000'. The 'Use Outbound Proxy server' checkbox is unchecked. The 'Perform provisioning from following URL' checkbox is unchecked, and the URL is 'http://'. There are buttons for 'Advanced settings', 'OK', and 'Cancel'.

**Certificates:** This window shows the 'Installed certificates' section. The 'Certificate' list contains 'root\_cert\_3CXPHONE.pem'. There are buttons for 'Import', 'Remove', and 'Close'.

Configure the 3CX Server with secure SIP (SIPS) using “SimpleCA” to generate an X.509 SSL certificate for this server. Use the instructions presented in the “security user guide”.

**74 Set Up Root CA**

Country	Cyprus
State or Province Name (full name)	Nicosia
Locality Name (eg. City)	Nicosia
Organization (eg. company) *	3CX Ltd.
Organizational Unit (eg. section)	Telecommunications PBX
Common Name (eg. Root CA) *	3CXPHONE
Email Address	info@3cx.com
CA Key Password	XXXXXX
Repeat Password	XXXXXX

Ok Cancel

**74 New Server Certificate Request**

Country *	Cyprus
State or Province Name (full name) *	Nicosia
Locality Name (eg. City) *	Nicosia
Organization (eg. company) *	3CX PBX
Organizational Unit (eg. section) *	PBX
Common Name (eg. www.domain.com) *	192.168.137.101
Email Address *	info@3cx.com

Ok Cancel

avancé | Codes de raccourcis | Exchange 2007/2010 | Conférence téléphonique | Sécurité | Anti-Hacking | IP Blacklist | Paramètres personnalisés | Sortie CDR

**Sécurité**

Si vous le souhaitez, 3CX peut établir des connexions SIP sécurisées. Pour activer cela, vous devez créer une clé et un certificat pour chaque interface suivant cette FAQ. Notez que ça ne fonctionne pas avec tous les téléphones. Important - Le Service 3CX PhoneSystem doit être redémarré pour que les modifications soient prises en compte.

Sélectionnez l'interface: 192.168.137.101 ?

**Certificat**




```
-----BEGIN CERTIFICATE-----
MIIDETCCAnoCAQEWdQYJKoZIhvcNAQEEBQAwZzQxZjBjNVBAYTAkNZMRAw
wDgYDQVQIEwdOaWVnc2lhMRawDgYDVQQHEwdOaWVnc2lhMRawDgYDVQQKEwZz
Q1ggTHRkLjEeMBwGA1UECxmVGVsZWVnbW11bmJlYXRpb24gUEYMRawDgYDVQQDE
wZzQ1hQSE9ORTEbMBkGCSqGSIb3DQEQJARYMaW5mb0AzY3guY29tMB4XDTEw
MDIwMloXDTEwMDUxNjIwMDUwMlowYgZzQxZjBjNVBAYTAkNZMRAwDgYDVQQIDA
dOaWVnc2lhMRawDgYDVQQHDAwWVnc2lhMRawDgYDVQQKDAczQ1ggUEYMQwZz
Q1ggYDVQQLDANQZQlGxGDAWBgNVBAMMDzE5Mi4xNjguMTM3LjEwMTEbMBkGCS
qGSIb3DQEQJARYMaW5mb0AzY3guY29tMBIIBjANBgkqhkiG9w0BAQEFAAOCAQ
8AMIIBCAQEAatIqmhzdNtVPTscsYHxUdnbfoJyFQ2WUoOFuEvXptq2GIWfX
TnAsmZ+TudDq9sky7puKvAnuHeFVz+idNkopj4mCt90EAt5vmO3//Yt9yqM6x
kJeif8Uo4ypfQpy9LLsUNP6HqTZAYWWoJdT6QZIk13isnCvQwMgjd2J8OQD
HFgsY6d/CafpuH0wpYy91Et+z7azAEqioO9OmNmcRnPYMqctQzbZQF5DAAK
IOOxpYC4J5WHvoplZ22xiHivRvhOB/hpB6HrvrmIZ9NmrF5y+r2AuWTKcrAW
Stcbwz+CODcgO/l6k8T9IgrLi0byVUK2U3kmU3+JdawdZ7VNSfKwIDAQABA
oIBADoJE+x/rbiw+oz9IzXuoj2P362sdPvdG6e6K5pnCLB9wtUaJL0tK/kaJdY
4DT/Vf2zaTSeTHZs3U0lp1hhQkLmWX5HRFZgA3ujPTIoVDBO2ku8maJN9j
tngHp+WW0uztGlRkszs+uEVW002OAABSBUvKe9ob75f4/gWjgAEm8dhOmpO
wttBUN8llh/8Py0Xn+TKL+rr+Wfj10eNGBwCvWwms/cOuKBZWdQeeIP8yL
QbLu93dqigjHYD6DyHppjxSFIT0T6ROVvADGwd7WR0rhcvP5BRokp1oc1x
11qaSxd1tQdxryehNbtakoTU7v3+g2t2aqDIQuS7RGL
```

**Clé**

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAatIqmhzdNtVPTscsYHxUdnbfoJyFQ2WUoOFuEvXptq2GI
WfXtTnAsmZ+TudDq9sky7puKvAnuHeFVz+idNkopj4mCt90EAt5vmO3//Yt9yq
M6xkJeif8Uo4ypfQpy9LLsUNP6HqTZAYWWoJdT6QZIk13isnCvQwMgjd2J8O
QDHFgsY6d/CafpuH0wpYy91Et+z7azAEqioO9OmNmcRnPYMqctQzbZQF5DAAK
IOOxpYC4J5WHvoplZ22xiHivRvhOB/hpB6HrvrmIZ9NmrF5y+r2AuWTKcrAWSt
cbwz+CODcgO/l6k8T9IgrLi0byVUK2U3kmU3+JdawdZ7VNSfKwIDAQABAoIB
ADoJE+x/rbiw+oz9IzXuoj2P362sdPvdG6e6K5pnCLB9wtUaJL0tK/kaJdY4DT
/Vf2zaTSeTHZs3U0lp1hhQkLmWX5HRFZgA3ujPTIoVDBO2ku8maJN9jtngHp+
WW0uztGlRkszs+uEVW002OAABSBUvKe9ob75f4/gWjgAEm8dhOmpOwttBUN8ll
h/8Py0Xn+TKL+rr+Wfj10eNGBwCvWwms/cOuKBZWdQeeIP8yLQbLu93dqigj
HYD6DyHppjxSFIT0T6ROVvADGwd7WR0rhcvP5BRokp1oc1x11qaSxd1tQdxryeh
NbtakoTU7v3+g2t2aqDIQuS7RGL
```

Activer le SIP sécurisé Désactiver le SIP sécurisé

Ce PC > Disque local (C:) > SimpleCA > certificats

Nom	Modifié le	Type
 request	17/04/2021 18:30	Certificat de sécur...
 request.csr	17/04/2021 18:30	Fichier CSR
 request	17/04/2021 18:30	Fichier KEY

Using Wireshark, answer the following questions.

### 19. VoIP signalling security :

Détail du paquet ▾ UTF-8 / ASCII / UTF-16 ▾ ☐ Sensible à la casse Chaîne de Caractères ▾ sip

Time	Source	Destination	Protocol	Length	Info
57 6.470606	192.168.137.101	192.168.137.101	TCP	44	53850 → 5061 [ACK] Seq=965 Ack=1517 Win=525568 Len=0
58 6.681485	192.168.137.101	192.168.137.101	TLSv1	918	Application Data, Application Data
59 6.681547	192.168.137.101	192.168.137.101	TCP	44	5061 → 53850 [ACK] Seq=1517 Ack=1839 Win=525568 Len=0
60 6.704742	127.0.0.1	127.0.0.1	TCP	52	52844 → 5485 [PSH, ACK] Seq=1 Ack=1 Win=2053 Len=8
61 6.704806	127.0.0.1	127.0.0.1	TCP	44	5485 → 52844 [ACK] Seq=1 Ack=9 Win=2051 Len=0
62 6.704850	127.0.0.1	127.0.0.1	TCP	66	52844 → 5485 [PSH, ACK] Seq=9 Ack=1 Win=2053 Len=22

[TCP Segment Len: 874]  
Sequence Number: 965 (relative sequence number)  
Sequence Number (raw): 491815631  
[Next Sequence Number: 1839 (relative sequence number)]  
Acknowledgment Number: 1517 (relative ack number)  
Acknowledgment number (raw): 3229762657  
0101 .... = Header Length: 20 bytes (5)  
> Flags: 0x018 (PSH, ACK)  
Window: 2053  
[Calculated window size: 525568]  
[Window size scaling factor: 256]  
Checksum: 0xd844 [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
> [SEQ/ACK analysis]  
> [Timestamps]  
TCP payload (874 bytes)  
Transport Layer Security  
▼ TLSv1 Record Layer: Application Data Protocol: sip.tcp  
Content Type: Application Data (23)  
Version: TLS 1.0 (0x0301)  
Length: 32  
Encrypted Application Data: 7136c591dd1af44a718823d976c22477eabe9b5177a3da939725872a1c651b68  
[Application Data Protocol: sip.tcp]  
> TLSv1 Record Layer: Application Data Protocol: sip.tcp

- **Explain How the SIP messages are secured between clients and Server ? and between Client and Client ?**

Between clients and server, SIPS is used to secure SIP. It's a SIP version using TLS/SSL. Between two clients, SRTP is used to ensure media exchange. On the same way, it's RTP with data encryption. We explain in the next answers how it works.

- **What is the transport protocol used (TCP/UDP) with SIP security ? Explain Why, you don't have the same protocole than the non-secured SIP call ?**

TLSv1 protocol is used. This is a protocol only used for secured exchange, a special handshake is done at the beginning. It's not the case for a non-secured communication, where this protocol is not asked. We could also have used a SSL tunnel.

- **Explain what is SIPS (SIP over SSL)**

SIPS gives more security during a client/server exchange than standard SIP. First, client and server check each other certificate, then they exchange key, and to finish they choose the cipher mode. After that, the SIP/RTP exchanges are fully encrypted, using the keys and the cipher mode.

- **What is the port number of SIPS ?**

SIPS requires port 5061 instead of 5060

## 20. VoIP data security :

- Are the default voice/RTP packets encrypted (yes/no) ?

No, as we saw before, RTP packets are not encrypted by default and we can listen to the call using Wireshark

- what is the encryption algorithm used to secure voice data ?

AES in CBC mode has been used (cf screen below)

- Explain what is Secure RTP (SRTP). Find the IETF RFC number for SRTP.

RFC 3711 explains what Secure Real-Time Transfer Protocol is. This is a protocol based on RTP, with more security strength, like message authentication, confidentiality or protection against replay.

- What is the transport protocol used (TCP/UDP) with SIP security ?

We can see TCP packets on Wireshark. It must be the SRTP data

- How the SRTP secret key is exchanged between the two systems ?

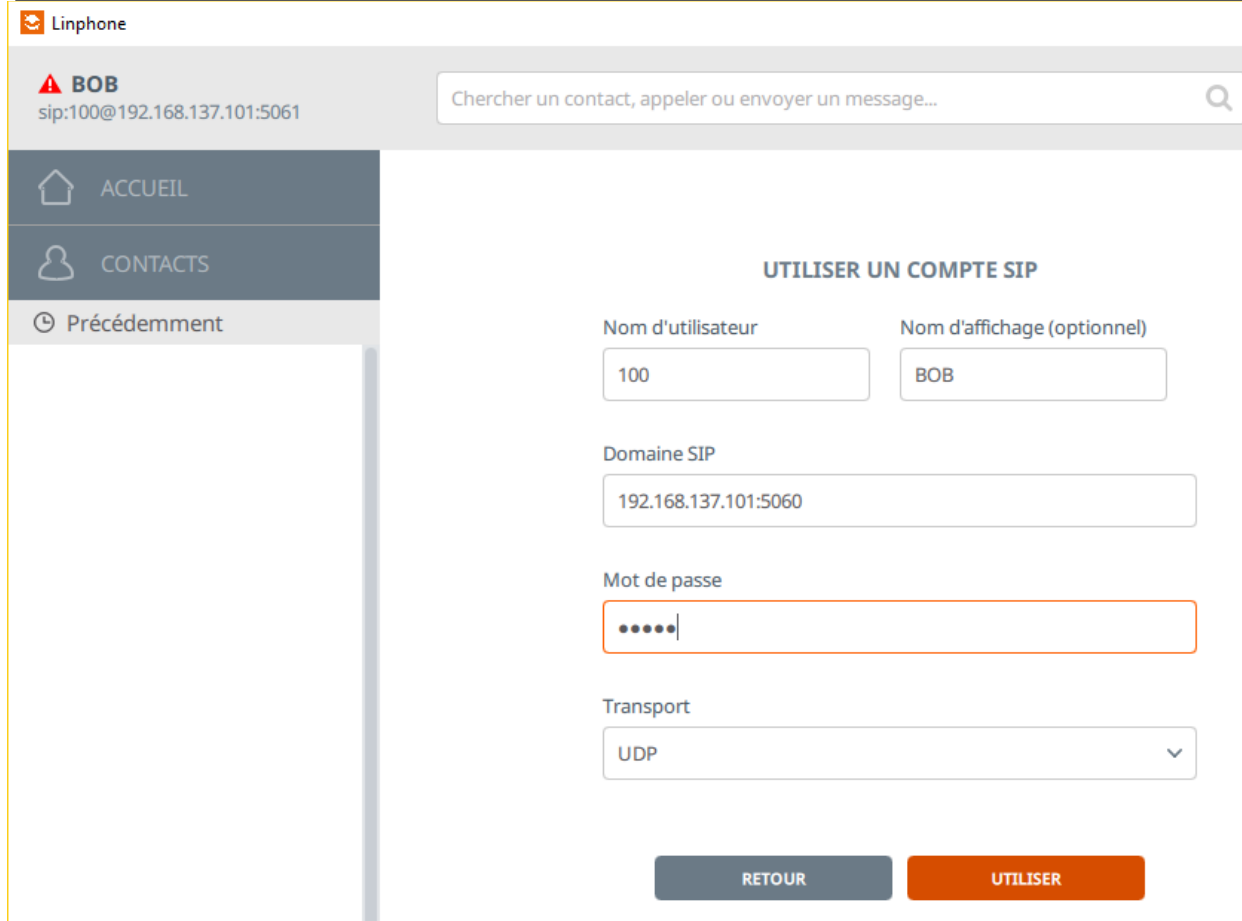
Key management protocol allows secret key to be known by both systems. Actually, one single master key is exchanged, then keys are derived from this master key on both sides.

- Insert the pictures of the captured packets with Wireshark to justify your answers.

Time	Source	Destination	Protocol	Length	Info
43 6.259049	192.168.137.101	192.168.137.101	TLSv1	144	Client Hello
44 6.259102	192.168.137.101	192.168.137.101	TCP	44	5061 → 53850 [ACK] Seq=1 Ack=101 Win=525568 Len=0
45 6.260432	192.168.137.101	192.168.137.101	TLSv1	915	Server Hello, Certificate, Server Hello Done
46 6.260506	192.168.137.101	192.168.137.101	TCP	44	53850 → 5061 [ACK] Seq=101 Ack=872 Win=524544 Len=0
47 6.263255	192.168.137.101	192.168.137.101	TLSv1	242	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
48 6.263319	192.168.137.101	192.168.137.101	TCP	44	5061 → 53850 [ACK] Seq=872 Ack=299 Win=525312 Len=0
49 6.267948	192.168.137.101	192.168.137.101	TLSv1	103	Change Cipher Spec, Encrypted Handshake Message
50 6.268013	192.168.137.101	192.168.137.101	TCP	44	53850 → 5061 [ACK] Seq=299 Ack=931 Win=524544 Len=0
51 6.268433	192.168.137.101	192.168.137.101	TLSv1	710	Application Data, Application Data
52 6.268472	192.168.137.101	192.168.137.101	TCP	44	5061 → 53850 [ACK] Seq=931 Ack=965 Win=524544 Len=0
Version: TLS 1.0 (0x0301)					
Length: 74					
Handshake Protocol: Server Hello					
Handshake Type: Server Hello (2)					
Length: 70					
Version: TLS 1.0 (0x0301)					
Random: 607b1849c9627f1541d83831550b66c85f691023383e37dcf0153d36c6f0eb90					
Session ID Length: 32					
Session ID: dcec888c40d1a493f43444b55d6f9fbdfe9e7498557986fa915528f26595842f					
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)					
Compression Method: null (0)					
TLSv1 Record Layer: Handshake Protocol: Certificate					
Content Type: Handshake (22)					
Version: TLS 1.0 (0x0301)					
Length: 778					
Handshake Protocol: Certificate					
Handshake Type: Certificate (11)					
Time	Source	Destination	Protocol	Length	Info
46 6.260506	192.168.137.101	192.168.137.101	TCP	44	53850 → 5061 [ACK] Seq=101 Ack=872 Win=524544 Len=0
47 6.263255	192.168.137.101	192.168.137.101	TLSv1	242	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
48 6.263319	192.168.137.101	192.168.137.101	TCP	44	5061 → 53850 [ACK] Seq=872 Ack=299 Win=525312 Len=0
49 6.267948	192.168.137.101	192.168.137.101	TLSv1	103	Change Cipher Spec, Encrypted Handshake Message
50 6.268013	192.168.137.101	192.168.137.101	TCP	44	53850 → 5061 [ACK] Seq=299 Ack=931 Win=524544 Len=0
51 6.268433	192.168.137.101	192.168.137.101	TLSv1	710	Application Data, Application Data
52 6.268472	192.168.137.101	192.168.137.101	TCP	44	5061 → 53850 [ACK] Seq=931 Ack=965 Win=524544 Len=0
53 6.317205	127.0.0.1	127.0.0.1	TCP	56	53851 → 5000 [SYN] Seq=0 Win=64240 Len=0 MSS=65495 WS=256 SACK_PERM=1
54 6.317292	127.0.0.1	127.0.0.1	TCP	56	5000 → 53851 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256
55 6.317400	127.0.0.1	127.0.0.1	TCP	44	53851 → 5000 [ACK] Seq=1 Ack=1 Win=525568 Len=0
56 6.470538	192.168.137.101	192.168.137.101	TLSv1	630	Application Data, Application Data
57 6.470606	192.168.137.101	192.168.137.101	TCP	44	53850 → 5061 [ACK] Seq=965 Ack=1517 Win=525568 Len=0
58 6.681485	192.168.137.101	192.168.137.101	TLSv1	918	Application Data, Application Data
59 6.681547	192.168.137.101	192.168.137.101	TCP	44	5061 → 53850 [ACK] Seq=1517 Ack=1839 Win=525568 Len=0
60 6.704742	127.0.0.1	127.0.0.1	TCP	52	52844 → 5485 [PSH, ACK] Seq=1 Ack=1 Win=2053 Len=8
61 6.704806	127.0.0.1	127.0.0.1	TCP	44	5485 → 52844 [ACK] Seq=1 Ack=9 Win=2051 Len=0
62 6.704850	127.0.0.1	127.0.0.1	TCP	66	52844 → 5485 [PSH, ACK] Seq=9 Ack=1 Win=2053 Len=22
63 6.704882	127.0.0.1	127.0.0.1	TCP	44	5485 → 52844 [ACK] Seq=1 Ack=31 Win=2051 Len=0
64 6.704921	127.0.0.1	127.0.0.1	TCP	48	52844 → 5485 [PSH, ACK] Seq=31 Ack=1 Win=2053 Len=4
65 6.704953	127.0.0.1	127.0.0.1	TCP	44	5485 → 52844 [ACK] Seq=1 Ack=35 Win=2051 Len=0
66 6.704986	127.0.0.1	127.0.0.1	TCP	517	52844 → 5485 [PSH, ACK] Seq=35 Ack=1 Win=2053 Len=473
67 6.705018	127.0.0.1	127.0.0.1	TCP	44	5485 → 52844 [ACK] Seq=1 Ack=508 Win=2049 Len=0
68 6.705249	127.0.0.1	127.0.0.1	TCP	52	5485 → 52844 [PSH, ACK] Seq=1 Ack=508 Win=2049 Len=8
69 6.705302	127.0.0.1	127.0.0.1	TCP	44	52844 → 5485 [ACK] Seq=508 Ack=9 Win=2053 Len=0
70 6.705470	127.0.0.1	127.0.0.1	TCP	60	5485 → 52844 [PSH, ACK] Seq=9 Ack=508 Win=2049 Len=16
71 6.705534	127.0.0.1	127.0.0.1	TCP	44	52844 → 5485 [ACK] Seq=508 Ack=25 Win=2053 Len=0
72 6.705582	127.0.0.1	127.0.0.1	TCP	48	5485 → 52844 [PSH, ACK] Seq=25 Ack=508 Win=2049 Len=4

## Partie 7 : VOIP and Security with Linephone

- Install the TOIP Linephone client in your terminals. Beware to unistall 3CX TOIP clients first. <https://www.linphone.org>
- Configure first the Linephone SIP accounts to connect to your 3CX server



The screenshot shows the Linphone application interface for configuring a SIP account. On the left is a sidebar with navigation options: 'ACCUEIL' (Home), 'CONTACTS', and 'Précédemment' (Previously). The main area is titled 'UTILISER UN COMPTE SIP' (Use a SIP account). It contains several input fields: 'Nom d'utilisateur' (Username) with the value '100', 'Nom d'affichage (optionnel)' (Optional display name) with the value 'BOB', 'Domaine SIP' (SIP domain) with the value '192.168.137.101:5060', 'Mot de passe' (Password) which is masked with dots, and a 'Transport' dropdown menu currently set to 'UDP'. At the bottom of the form are two buttons: 'RETOUR' (Return) and 'UTILISER' (Use).

- Configure then the Linephone audio codec. Explain what audio codec you selected. What is your audio bit rate ?

I selected the opus audio codec with a bitrate of 50 Kbit/s. Screenshot is available on the next page.

Activer l'annulation d'écho ☒

## Codecs audio

Nom	Description	Fréquence (Hz)	Débit (Kbit/s)	Paramètres	Status
opus	An opus encoder.	48000	50	useinbandfec=1	<input checked="" type="checkbox"/>
speex	The free and wonderful speex codec	16000	40	vbr=on	<input type="checkbox"/>
speex	The free and wonderful speex codec	8000	32	vbr=on	<input type="checkbox"/>
PCMU	ITU-G.711 ulaw encoder	8000	80		<input type="checkbox"/>
PCMA	ITU-G.711 alaw encoder	8000	80		<input type="checkbox"/>
GSM	The GSM full-rate codec	8000	30		<input type="checkbox"/>
G722	The G.722 wideband codec	8000	80		<input type="checkbox"/>
iLBC	WebRtc's iLBC encoder	8000	24	mode=30	<input type="checkbox"/>
G729	G729 audio encoder filter	8000	24	annexb=yes	<input type="checkbox"/>
speex	The free and wonderful speex codec	32000	40	vbr=on	<input type="checkbox"/>

- **Configure then the Linephone video codec. Explain what video codec you selected (Cisco H.264 or google VP8). What is your video resolution (pixels) ? What is your video bitrate ?**

I selected Google VP8 video codec, which can be used with a 640\*480 pixels resolution. The bitrate is 1500 Kbit/s.

## Paramètres de capture vidéo

Périphérique de capture vidéo 

Directshow capture: HP Truevision HD

Profil vidéo

Définition 

vga (640x480)

## Codecs vidéo

Nom	Description	Fréquence (Hz)	Débit (Kbit/s)	Paramètres	Status
VP8	A VP8 video encoder using libvpx library.	90000	1500		<input checked="" type="checkbox"/>
H264	Provided by CISCO SYSTEM,INC				<input type="checkbox"/>

- **Configure then the Linephone Security options to select SRTP (data) and SIPS (signaling).**

Appels

Chiffrement

AucunSRTPZRTPTLS

Chiffrement obligatoire

Répondre automatiquement

Délai (en ms)

0

Répondre autom. (avec vidéo)

Afficher le clavier tél. automatiq...

Fenêtre d'appels en tâche de fo...

Enregistrer auto. les appels

Chat

Activer le son des notifications

Son des notifications

C:\Program Files (x86

Serveur de partage

https://www.linphone.org:444/ift.php

Paramètres principaux du compte SIP

Adresse SIP\*

"BOB" <sip:100@192.168.137.101>

Adresse du serveur SIP\*

<sip:192.168.137.101;transport=tls>

Durée d'enregistrement

3600

+

-

Transport

TLS

▼

Route

Paramètres de contact

message-expires=604800

Intervalle standard RTCP AVPF (...)

1

+

-

S'enregistrer

ANNULER

CONFIRMER

Port d'écoute SIP UDP

5061

+

-

Port d'écoute SIP TCP

5061

+

-

Port Audio RTP UDP

7078

Port Vidéo RTP UDP

9078

NAT et Pare-feu



- **What is ZRTP ? what are the differences with SRTP ?**

ZRTP is a protocol which provides security between two end points in a VoIP network. To do so, Secure RTP (SRTP) is used, with the help of a Diffie-Hellman key exchange before any data communication.

- **What is Datagram TLS (DTLS). Find the RFC number for DTLS. What are the differences with SRTP ?**

DTLS is defined in the RFC 4347 and in RFC 6347 for the version 1.2. It is a communication protocol, preventing from attacks like message forgery, tampering or eavesdropping. This is based on the TLS protocol and it's similar to it. Actually, SRTP uses DTLS for the handshake and so the key exchange. Then, RTP data are encrypted using SRTP method during the communication between both end points.

- **Configure then the Linephone network options to setup your UDP/TCP port numbers for facilitating your firewall configurations**

We didn't understand what was expecting here, but we disabled fixed ports and we have activated ICE and TURN in the NAT and firewall options.

### Protocole réseau et ports

---

Port d'écoute SIP UDP	<input type="checkbox"/>
Port d'écoute SIP TCP	<input type="checkbox"/>
Port Audio RTP UDP	<input type="checkbox"/>
Port Vidéo RTP UDP	<input type="checkbox"/>

### NAT et Pare-feu

---

Activer ICE	<input checked="" type="checkbox"/>
Activer TURN	<input checked="" type="checkbox"/>

- **What is STUN/TURN protocols ? Why we need these protocols with TOIP ? Provide the name and IP address of two public STUN/TURN servers available online.**

STUN protocol allows NAT clients in a local network to pass through firewall to communicate with an external VoIP operator. To do so, information like public IP, NAT router type or port used must be known and exchanged by the clients. So two VoIP end points can connect with the help of a STUN server. TURN is an extension of STUN, which aims to facilitate NAT traversal for media traffic. Media traffic is more heavy than network discovery packets, so it is relayed by a dedicated server: the STUN server.

These protocols are important for TOIP because clients sometimes need to join another client in an external network. So handshake and then media traffic need to traverse firewall, with the help of STUN and TURN servers.

Here are two public STUN/TURN servers available online:

---

- [stun.3cx.com:3478](https://stun.3cx.com:3478) with IP 54.39.182.217
  - [stun.12voip.com:3478](https://stun.12voip.com:3478) with IP 77.72.169.212
- We can register to them online.

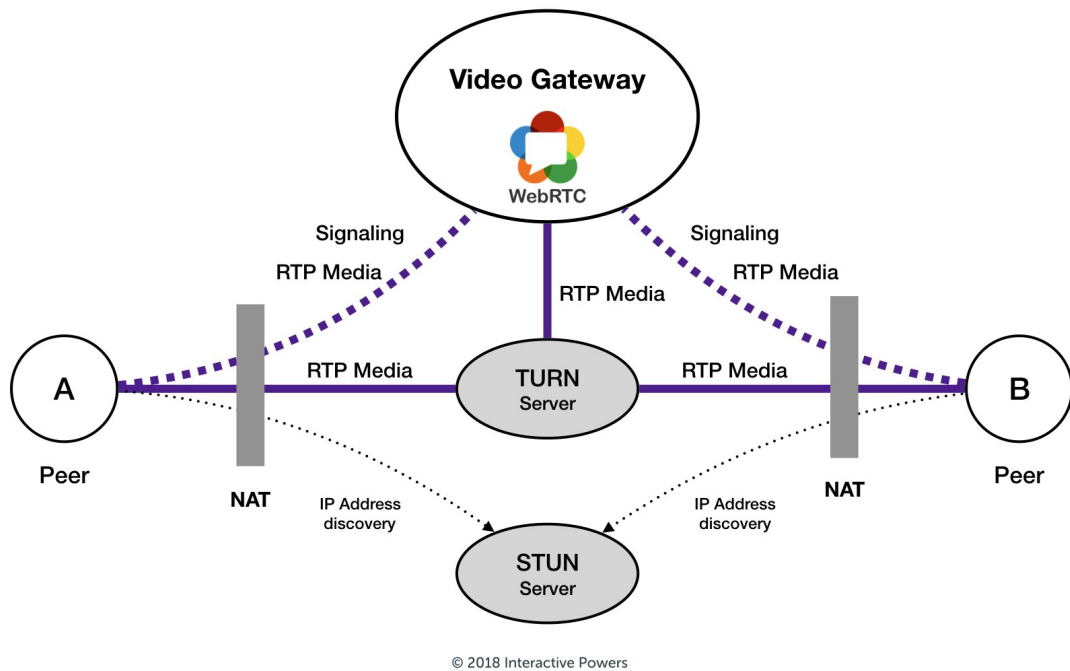


Diagram showing the roles of TURN and STUN servers from  
<https://blog.ivrpowers.com/post/technologies/what-is-stun-turn-server/>