

TP IPBX 12 : TP ANALYSE DE TRAMES PAR SNIFFER (WIRESHARK)

Objectif : Etre capable d'analyser les trames d'une conversation en ToIP

Ce sujet comporte 7 pages

1. MISE EN SITUATION :

En tant que technicien en SE vous souhaitez analyser les trames SIP échangées entre le poste 405 (softphone) et le poste 401 (poste standard dédié) afin de vérifier leur bon fonctionnement.

2. INSTALLATION

La configuration de départ est :

Obox + 1 poste dédié (401 standard) + 1 poste analogique (402) + 1 poste IP(407) + 1 softphone Xlite (405 sur eepc)

2.1. On vous demande de réaliser cette installation aussi bien matériel, que logiciel. Ainsi que la configuration de l'obox et des postes associés.

2.2. Tester la configuration dans les situations suivante :

Appel de 401 vers 402, vers 405, vers 407 et vice versa.

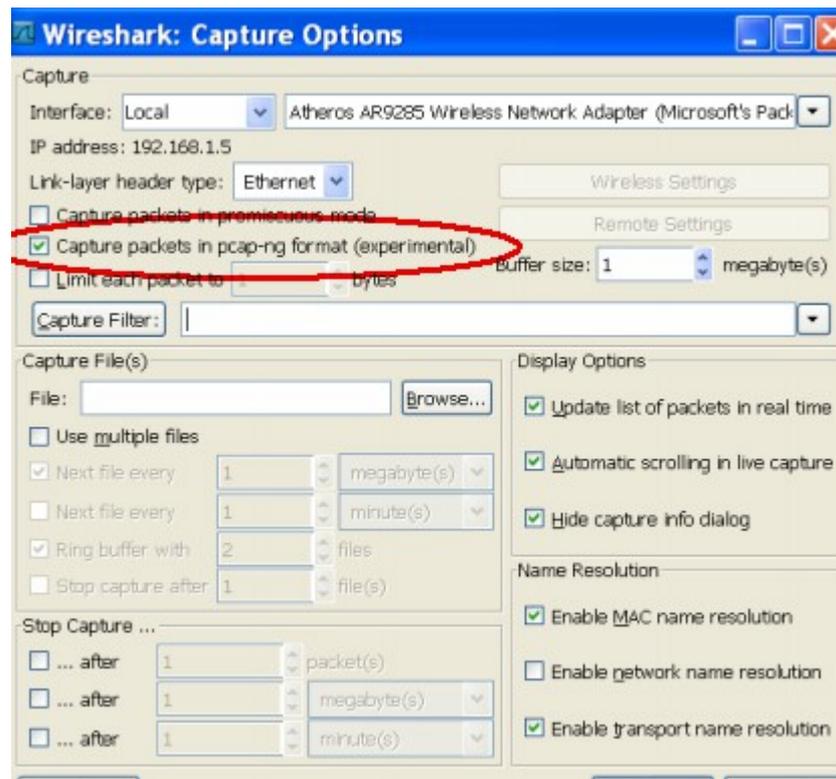
Attention : le pc softphone doit être sur le réseau wifi de l'obox.

3. ETUDE D'UN APPEL ENTRE UN POSTE ANALOGIQUE ET IP

3.1. Mesure par sniffer

Afin de visualiser les informations échangées lors de la communication IP nous utilisons un sniffer Wireshark disponible gratuitement sur internet.

- Installer wireshark avec les options par défaut sur l'eepc si nécessaire.
- Démarrer l'application « wireshark »
- Choisir la carte réseau wireless (attention choisir l'option capture packet...
-

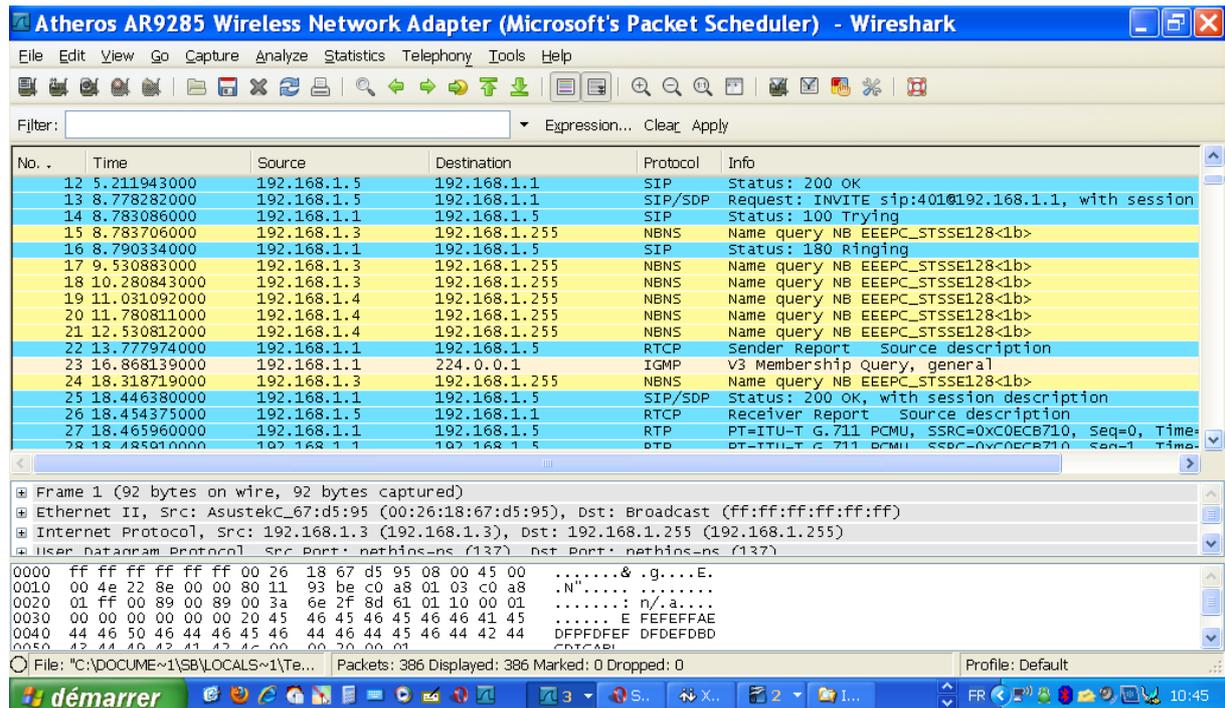


- Lancer la capture lorsque vous êtes prêt à faire un appel.
- Appeler avec le poste 405 (softphone) le poste 401
- Le poste 401 sonne
- décrocher et parler.
- Raccrocher.
- Arrêter la capture.

3.2. Analyse des trames.

Repérage du protocole de communication.

A partir de votre capture répondre aux questions suivantes :



Quels protocoles sont utilisés lors des échanges téléphoniques ?

Quelle est l'adresse du poste appelant ?

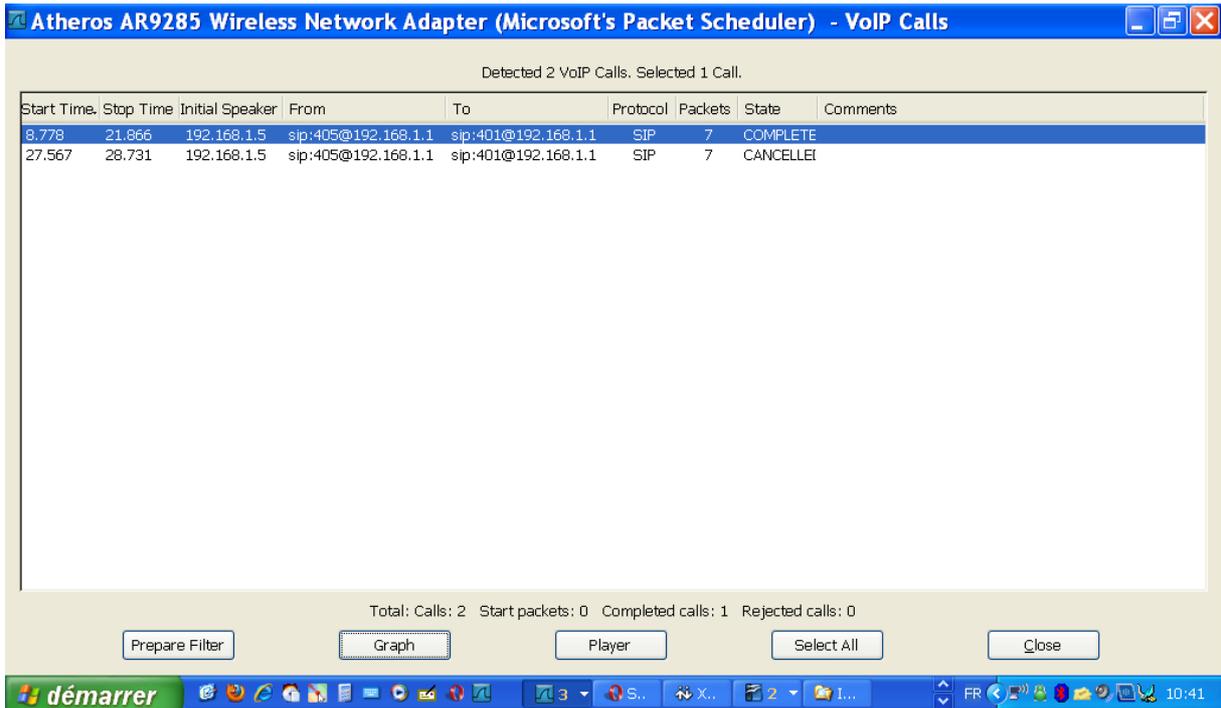
Quelle est l'adresse du poste appelé ?

Quelle est l'adresse de la passerelle

Que remarquez vous (vous pourrez répondre plus facilement à la fin du TP)?

Afin d'analyser les trames de téléphonies, passer le sniffer en mode TELEPHONY.

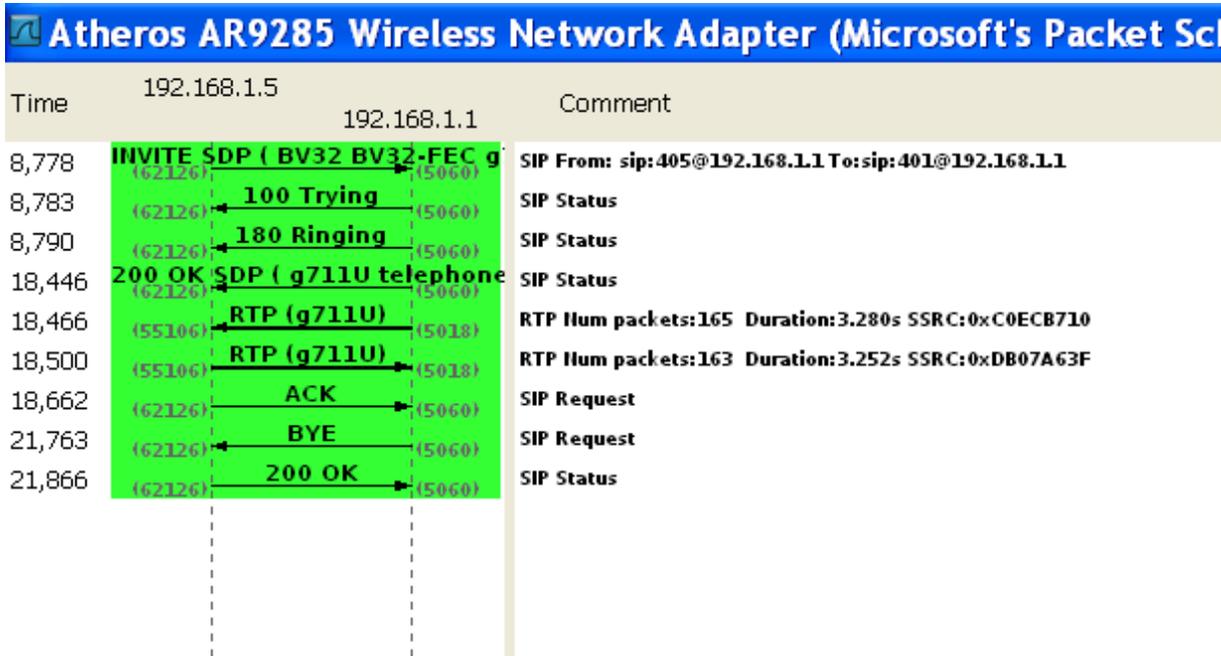
Puis choisir : la conversation à analyser



Ici 2 appels VoIP sont détectés parmi les trames acquises.

On choisit la première qui est complète.

Appuyer sur Graph afin de visualiser les échanges entre les postes :



A partir de cet échange répondre aux questions suivantes :

Donner le protocole de codage (codec) utilisé ?

Retrouver les numéros des postes présents dans cette communication ?

Donner l'adresse du serveur SIP ?

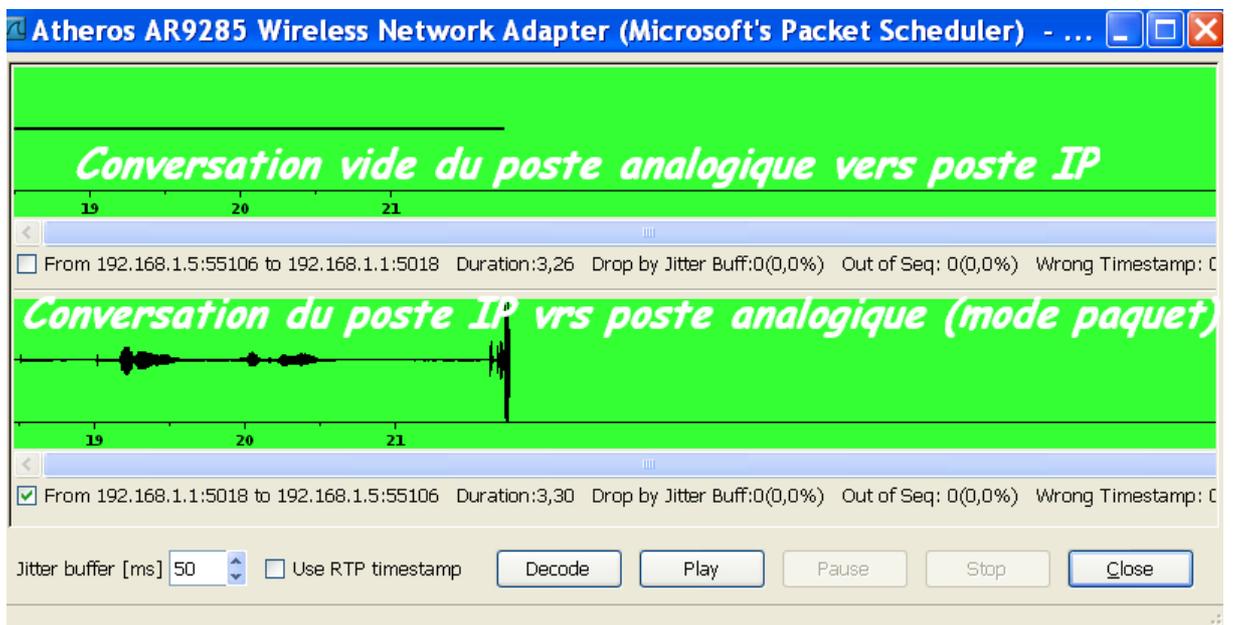
Pourquoi ne voit on pas le poste appelé (401) ?

Reconstitution de la conversation.

Il est possible de reconstituer la conversation en choisissant :

- Choisir la conversation à reconstituer
- Choisir « player »
- puis « decode »

Ecouter la conversation sélectionnée en choisissant : **Play**

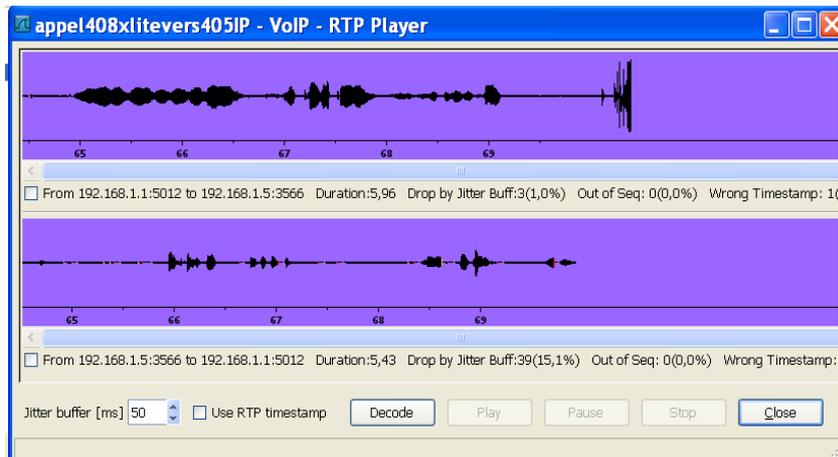
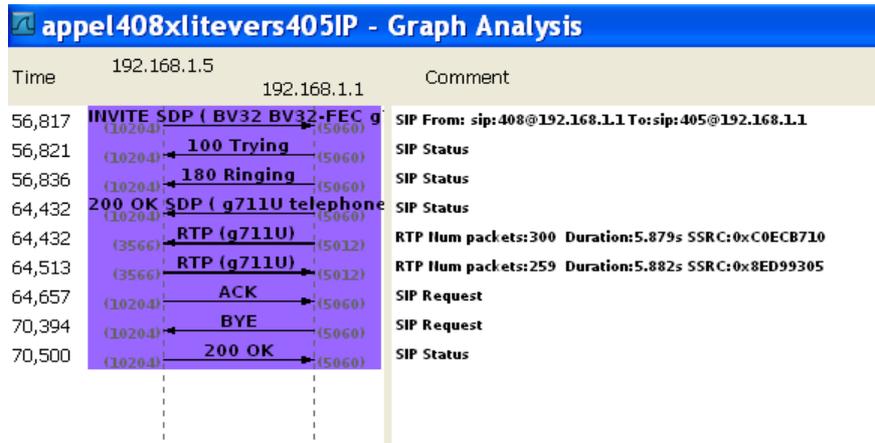


On ne peut reconstituer que la conversation dans un sens !!! A VERIFIER

4. ETUDE D'UN APPEL ENTRE DEUX POSTES IP.

Refaire l'étude et l'analyse précédente dans les conditions suivantes :
appel entre un softphone et un téléphone IP.

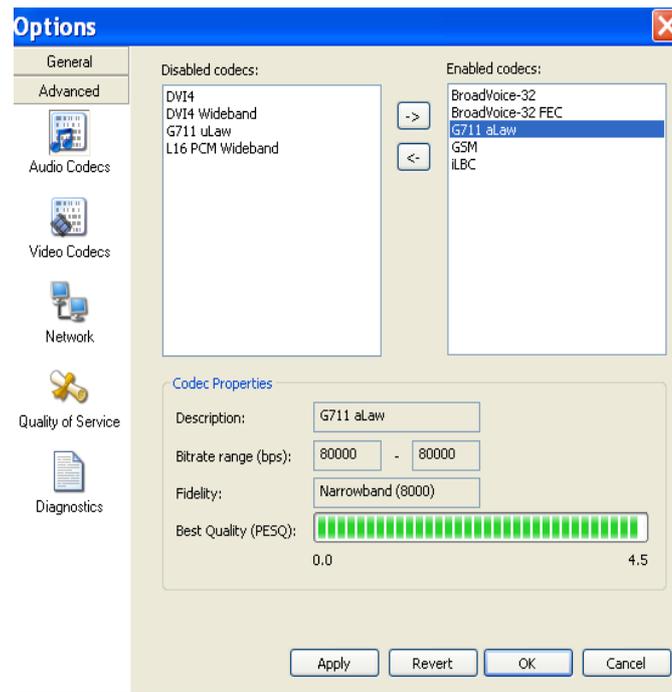
Après analyse :



Que remarquez vous (vous pourrez répondre plus facilement à la fin du TP)?

5. ETUDE D'UNE PANNE : CODEC MAL CONFIGURÉ

On vous demande de modifier le codec supporté par le softphone.
 Modifier les codecs autorisés dans Xlite :



5.1. Eliminer les codecs compatibles avec obox

5.2. Réessayer un appel en capturant les trames.

5.3. Analyser les trames.

6. CORRECTION

7. MISE EN SITUATION :

En tant que technicien en SE vous souhaitez analyser les trames SIP échangées entre le poste 405 (softphone) et le poste 401 (poste standard dédié) afin de vérifier leur bon fonctionnement.

8. INSTALLATION

La configuration de départ est :

Obox + 1 poste dédié (401 standard) + 1 poste analogique (402) + 1 poste IP(407) + 1 softphone Xlite (405 sur eeepc)

8.1. On vous demande de réaliser cette installation aussi bien matériel, que logiciel. Ainsi que la configuration de l'obox et des postes associés.

8.2. Tester la configuration dans les situations suivante :

Appel de 401 vers 402, vers 405, vers 407 et vice versa.

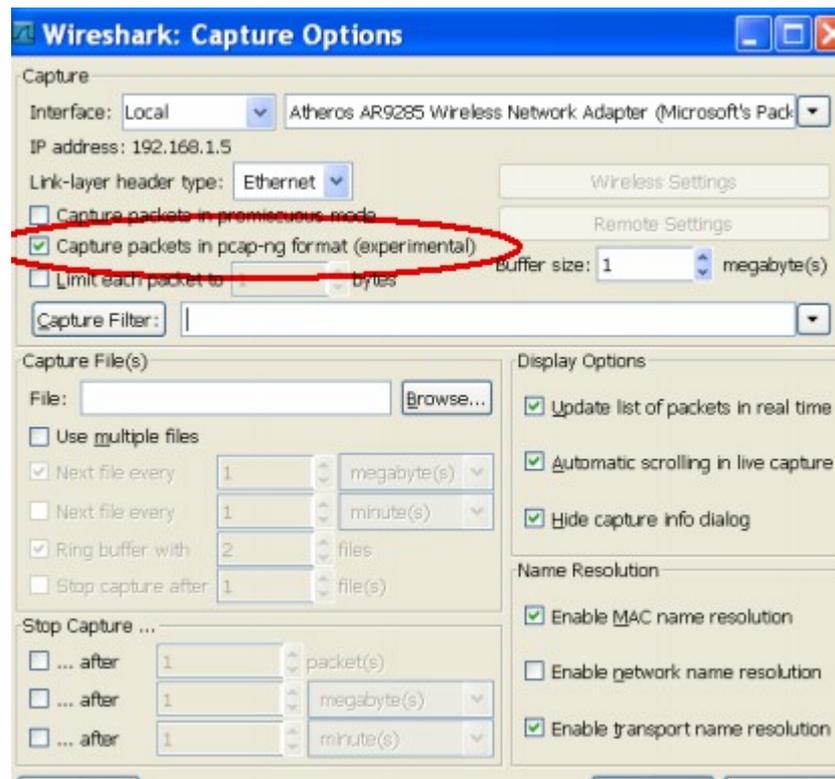
Attention : le pc softphone doit être sur le réseau wifi de l'obox.

9. ETUDE D'UN APPEL EN POSTE ANALOGIQUE ET IP

9.1. Mesure par sniffer

Afin de visualiser les informations échangées lors de la communication IP nous utilisons un sniffer Wireshark disponible gratuitement sur internet.

- Installer wireshark avec les options par défaut sur l'eeepc si nécessaire.
- Démarrer l'application « wireshark »
- Choisir la carte réseau wireless (attention choisir l'option capture packet...
-

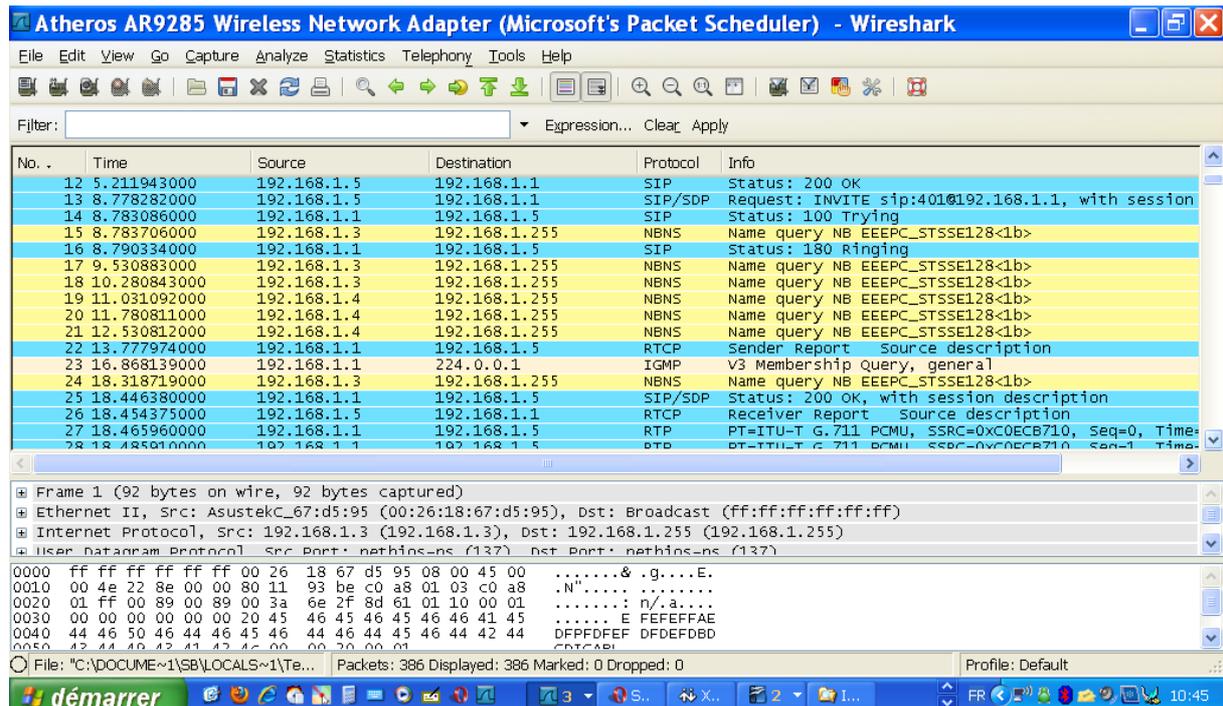


- Lancer la capture lorsque vous êtes prêt à faire un appel.
- Appeler avec le poste 405 (softphone) le poste 401
- Le poste 401 sonne
- décrocher et parler.
- Raccrocher.
- Arrêter la capture.

9.2. Analyse des trames.

Repérage du protocole de communication.

A partir de votre capture répondre aux questions suivantes :



Quels protocoles sont utilisés lors des échanges téléphoniques ?

(SIP et RTP) coté IPphone et NBNS(analogique phone)

Quelle est l'adresse du poste appelant ?

192.168.1.5

Quelle est l'adresse du poste appelé ?

192.168.1.3

Quelle est l'adresse de la passerelle

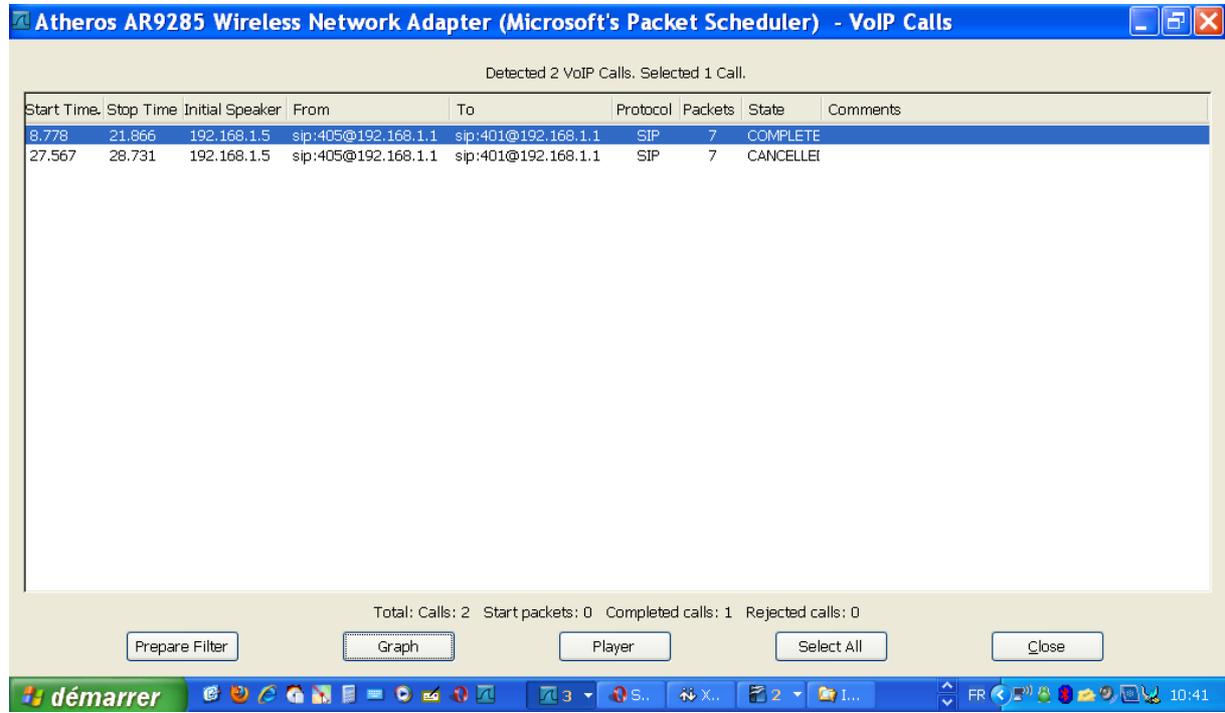
192.168.1.1

Que remarquez vous (vous pourrez répondre plus facilement à la fin du TP)?

Le poste analogique ne voit pas le protocole SIP/RTP normal c'est de l'analogique. Les paquets IP sont arrêtés par la passerelle 192.168.1.1 et sont transformé en voix versle poste analogique.

Afin d'analyser les trames de téléphonies, passer le sniffer en mode TELEPHONY.

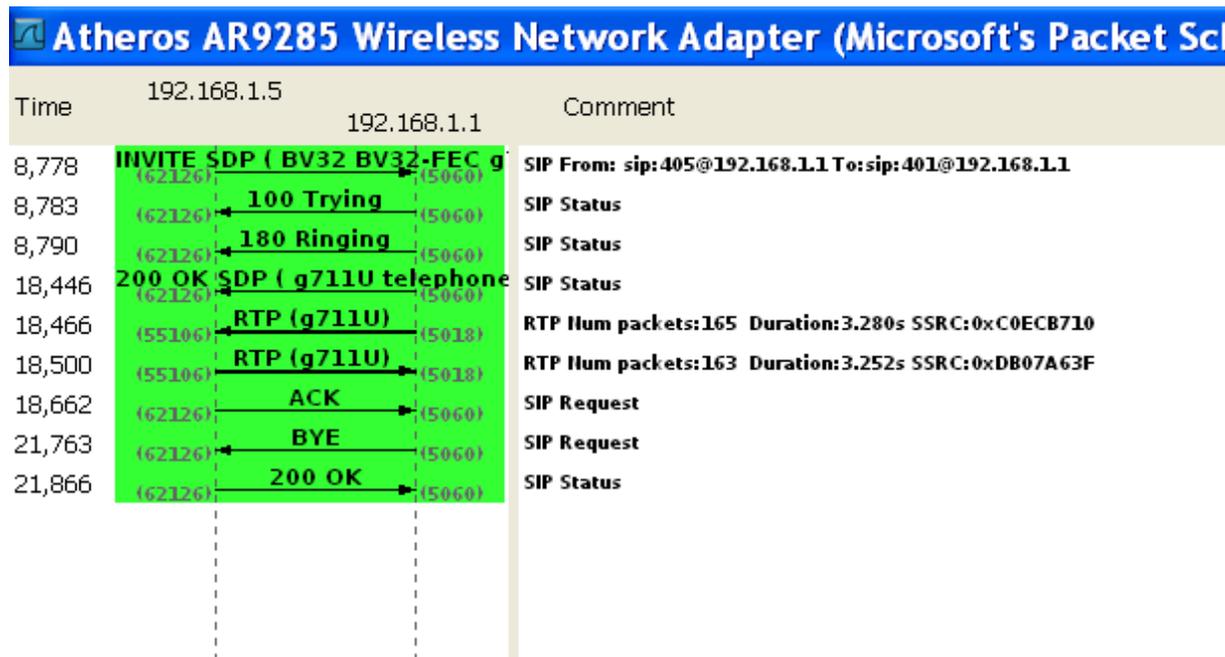
Puis choisir : la conversation à analyser



Ici 2 appels VoIP sont détectés parmi les trames acquises.

On choisit la première qui est complète.

Appuyer sur Graph afin de visualiser les échanges entre les postes :



A partir de cet échange répondre aux questions suivantes :

Donner le protocole de codage (codec) utilisé ?

G711U

Retrouver les numéros des postes présents dans cette communication ?

Poste 405 et 401

Donner l'adresse du serveur SIP ?

192.168.1.1

Pourquoi ne voit-on pas le poste appelé (401) ?

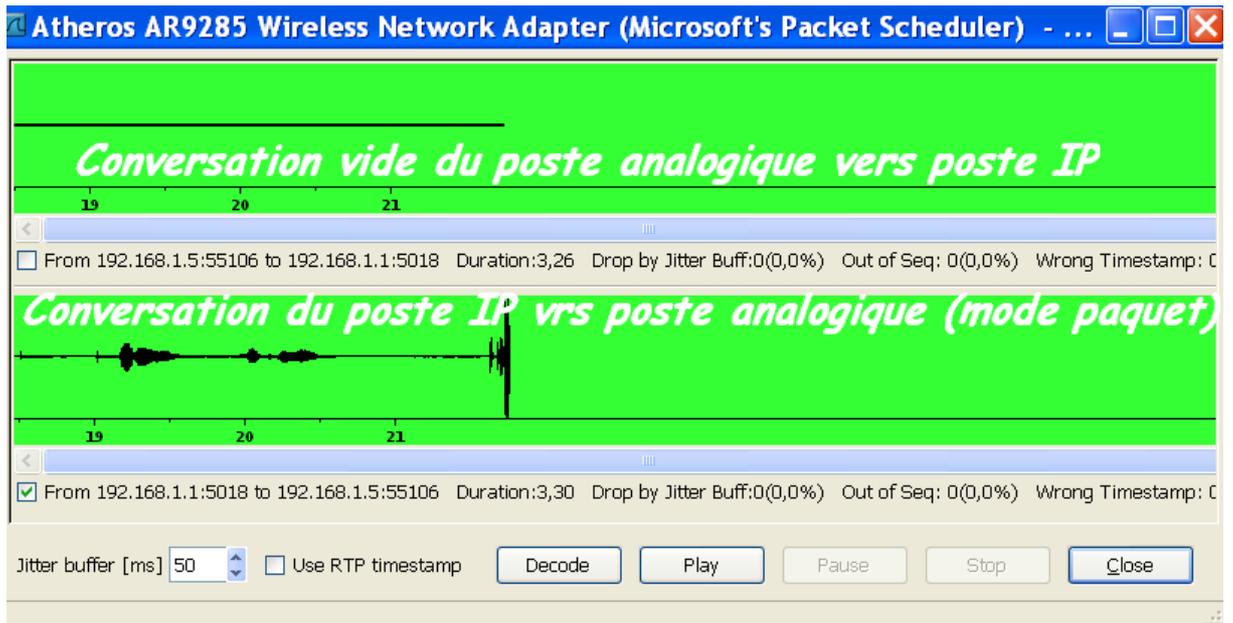
on analyse uniquement la partie SIP transmission par paquet. Le poste 401 est analogique donc pas de transmission par paquet mais de l'analogique classique.

Reconstitution de la conversation.

Il est possible de reconstituer la conversation en choisissant :

- Choisir la conversation à reconstituer
- Choisir « player »
- puis « decode »

Ecouter la conversation sélectionnée en choisissant : **Play**

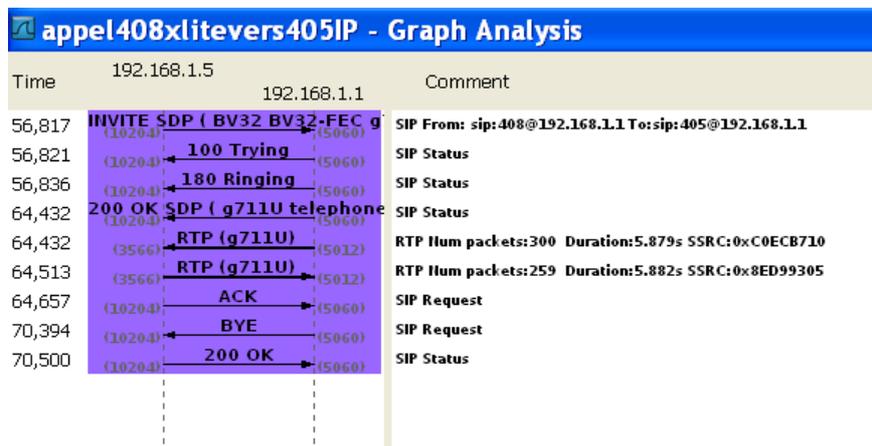


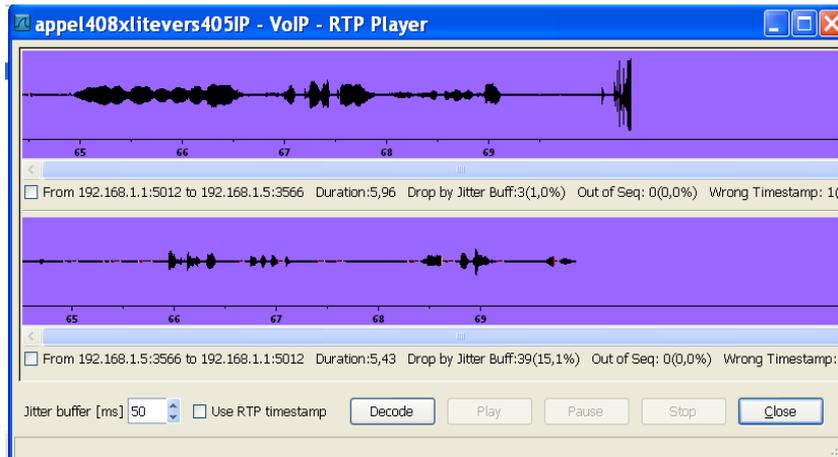
On ne peut reconstituer que la conversation dans un sens !!! A VERIFIER

10. ETUDE D'UN APPEL ENTRE DEUX POSTES IP.

Refaire l'étude et l'analyse précédente dans les conditions suivantes :
appel entre un softphone et un téléphone IP.

Après analyse :





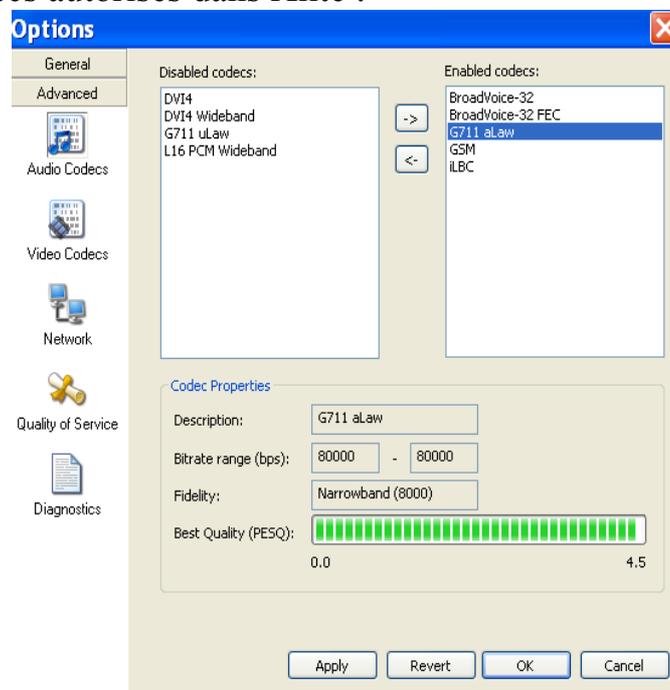
Que remarquez vous (vous pourrez répondre plus facilement à la fin du TP)?

A VERIFIER : On doit pouvoir voir les 2 conversations et les paquets ne sont entre les 2 postes transitant par la passerelle.

11. ETUDE D'UNE PANNE : CODEC MAL CONFIGURÉ

On vous demande de modifier le codec supporté par le softphone.

Modifier les codecs autorisés dans Xlite :



Eliminer les codecs compatibles avec obox
Réessayer un appel en capturant les trames.

Analyser les trames.

-