



Découverte de la Convergence VDI



Pré req

Matériel nécessaire :

- Laboratoire DIDAVDI+
- Station étudiante complète

Durée : 28 heures

SOMMAIRE

TP 1 : Protocole FTP

TP 2 : Protocole HTTP

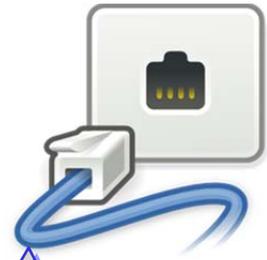
TP 3 : Service Vidéo, Protocoles RTSP et IGMP

TP 4 : Protocole Voix, fonction téléphonique

TP 5 : Voix, Protocoles SIP et RTP

TP 6 : Protocole ARP

TP 7 : Protocole DHCP



Baie DidaVDI

TP5 – Protocoles SIP et RTP



Voix

Le protocole SIP (Session Initiation Protocol) est un protocole Client/Server de Localisation Voix sur IP. Il est utilisé conjointement avec le protocole RTP (Real Time Transport Protocol) qui assure les transport des flux médias Voix et Vidéo.

La plupart des services réseaux sont normalisés par l'organisme IETF (Internet Engineering Task Force) dans des documents appelés RFC (Request For Comments). Le service SIP est normalisé RFC3261 de juin 2002 et le protocole RTP est le RFC 3550 de juillet 2003. Le service SIP utilise le port UDP 5060 pour l'analyse des écoutes SIP et RTP, dans le TP5, ce TP4 permet d'introduire des fonctionnalités téléphoniques courantes.

Prérequis :

- Utilisation Système d'exploitation
- Protocoles : IP, TCP

Matériel nécessaire :

- Serveur DidaVDI
- Routeur
- Commutateur
- PC Client (minimum 1)
- Videophone (minimum 1)

Extrait

Extrait

Mise en place de la plateforme



A travers l'interface LCD du Serveur DidaVDI, déterminez son adresse IP :

```
DidaVDI > Serveur DidaVDI > Info. Interf. Réseau
```



Depuis le poste PC Client, vérifiez la connectivité réseau avec le serveur DidaVDI à l'aide d'une requête d'écho ICMP :

```
ping 192.168.1.100
```

1 Démarrage du service Voix



Depuis le Poste PC Client, vérifiez l'état du port associé par défaut au service Voix SIP sur le serveur DidaVDI :

```
nmap 192.168.1.100 -sU -p 5060
Starting Nmap 5.21 ( http://nmap.org ) at 2011-09-07 15:38 CEST
Nmap scan received for 192.168.1.100: 5060
Host is up (0.0075s latency).
PORT      STATE SERVICE
5060/udp  CLOS
MAC Address: 00:05:B7:DB:48:D0 (Arbor Technology)

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```



A travers l'interface LCD du Serveur DidaVDI, activez le service Voix SIP :

```
DidaVDI > Services Donnees > Service Voix > Demarrage Voix
```



A travers l'interface LCD du Serveur DidaVDI, vérifiez l'état du port associé au service Voix SIP :

```
DidaVDI > Serveur DidaVDI > Etat des services
```



Depuis le Poste PC Client, vérifiez l'état du port associé par défaut au service Voix SIP sur le serveur DidaVDI :

```
nmap 192.168.1.100 -sU -p 5060
Starting Nmap 5.21 ( http://nmap.org ) at 2011-09-07 15:37 CEST
Nmap scan received for 192.168.1.100
Host is up (0.0077s latency).
PORT      STATE SERVICE
5060/udp  OPEN|FILTERED sip
MAC Address: 00:05:B7:DB:48:D0 (Arbor Technology)

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
```

2 Etude du protocole de signalisation SIP



**PC Client
Multimédia**

192.168.1.20

Appel Direct



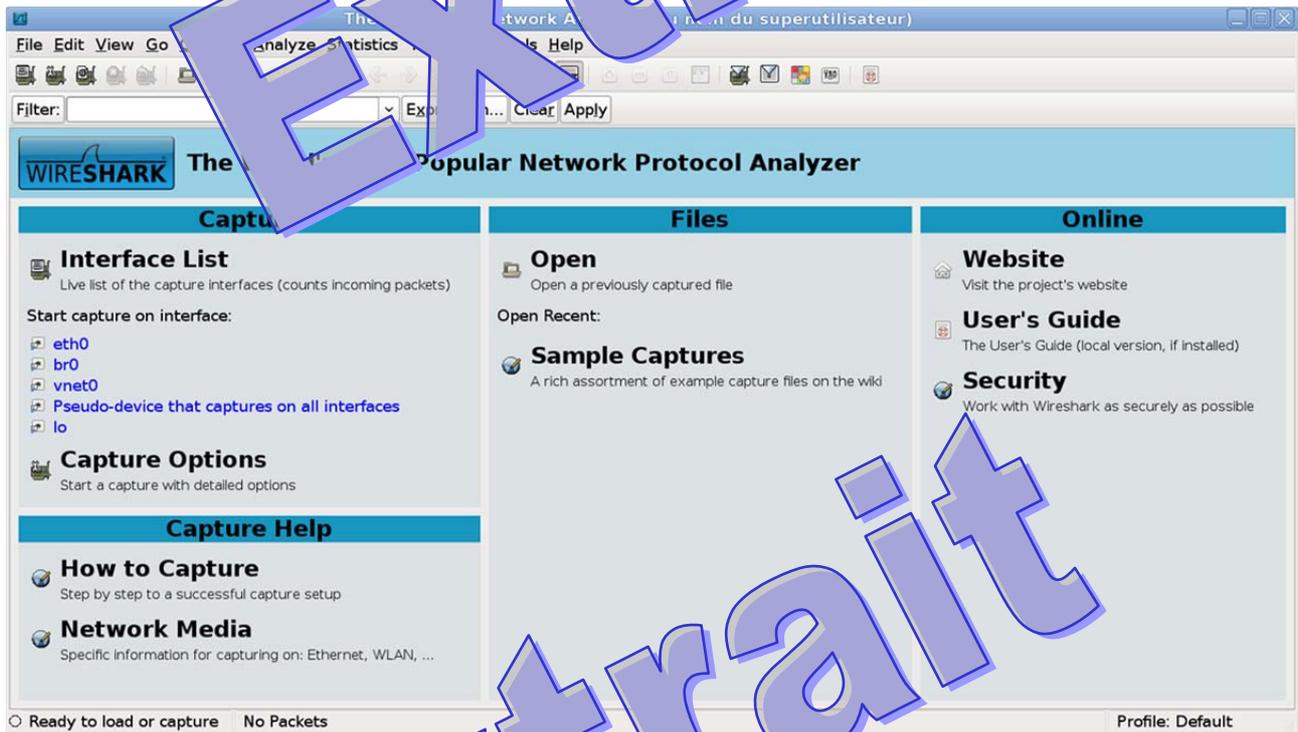
**Serveur
DidaVDI**

192.168.1.100

Il s'agit d'un appel direct entre un téléphone logiciel et un IPBX. L'IPBX joue le rôle d'un second téléphone avec un échange et diffusion audio automatiques. L'ordinateur qui héberge le téléphone logiciel dispose également d'un logiciel de capture et d'analyse du trafic réseau (Wireshark).

2.1 Capture du trafic

Sur le poste client DidaVDI, lancez le logiciel de capture et d'analyse du trafic réseau en à l'aide de l'icône Wireshark :



Dans la fenêtre « Capture », cliquez sur « Start capture on interface : eth0 ».

Sur le téléphone, numérotez « sip:3@192.168.1.100 », puis lancez l'appel. Ensuite, simulez un appel complet.

Dans le logiciel de capture et d'analyse du trafic réseau, sélectionnez le menu déroulant « Capture », puis « Stop ».

2.2 Analyse du trafic

2.2.1 Filtrage des paquets VoIP : simulation SIP et Media RTP

- Dans le champs « Filter », appliquer l'expression « sip (ip) »
- Sauvegardez les paquets résultants de filtrage dans un fichier « CaptureAppelDirect.pcap » en sélectionnant le menu déroulant « Save as », puis « Save as ».

Analyse des paquets de signalisation SIP

- Dans le logiciel de capture et d'analyse du trafic réseau, sélectionnez le menu déroulant « Telephony », puis « VoIP Calls ».

CaptureAppelDirect.pcap - VoIP Calls

Detected 1 VoIP Call. Selected 0 Calls.

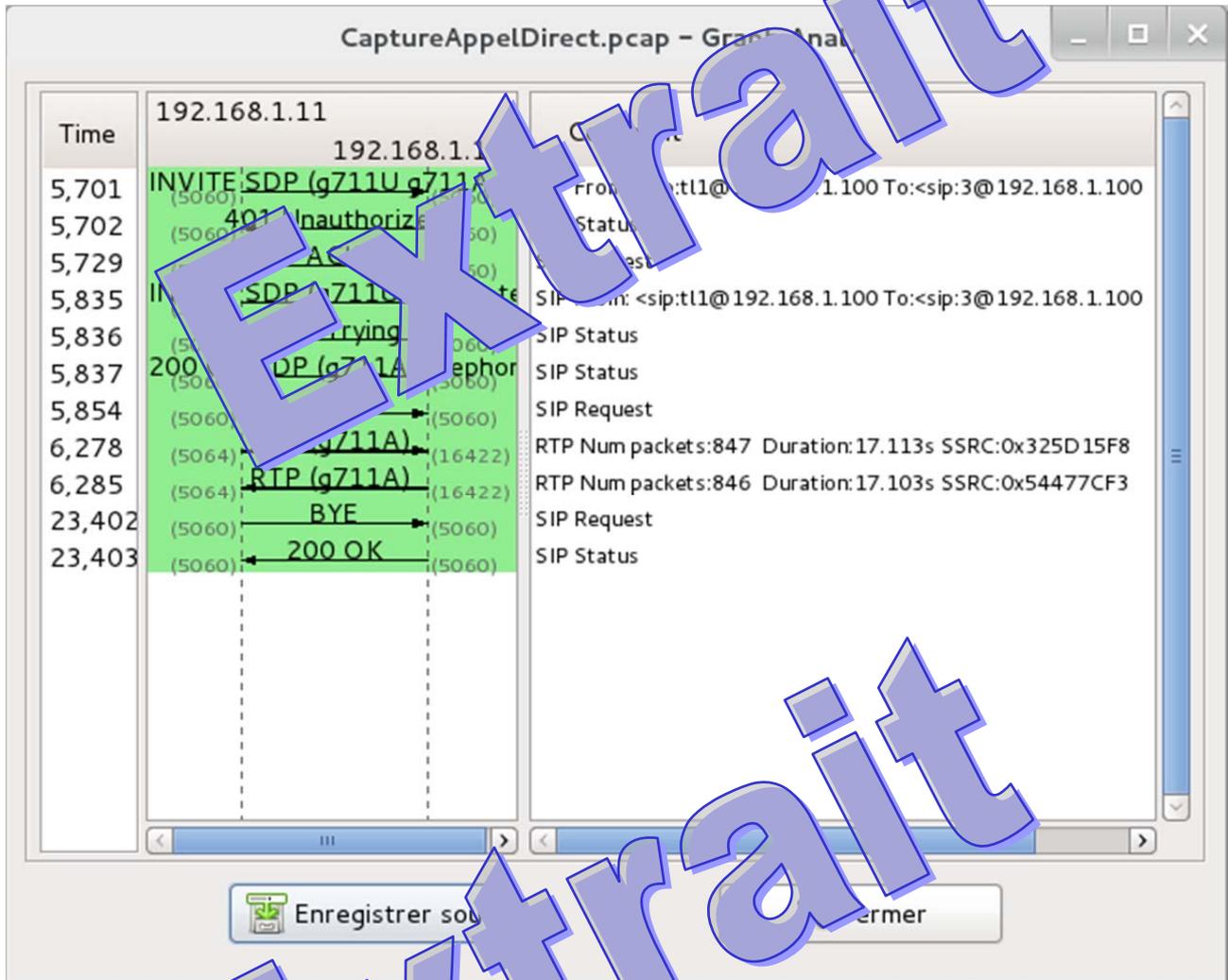
Start Time	Stop Time	Initial Sp	From	To	Protoco	Packets	State	Comments
5,701343	23,402839	192.168.1.	< sip:tl1@192.168.1.100	< sip:3@192.168.1.100	SIP	9	COMPLETE	

Total: Calls: 1 Start packets: 0 Complete: 1

Prepare Filter Flow Sélectionner Fermer



Cliquez sur la ligne concernant votre appel, puis sur le bouton Filtrer

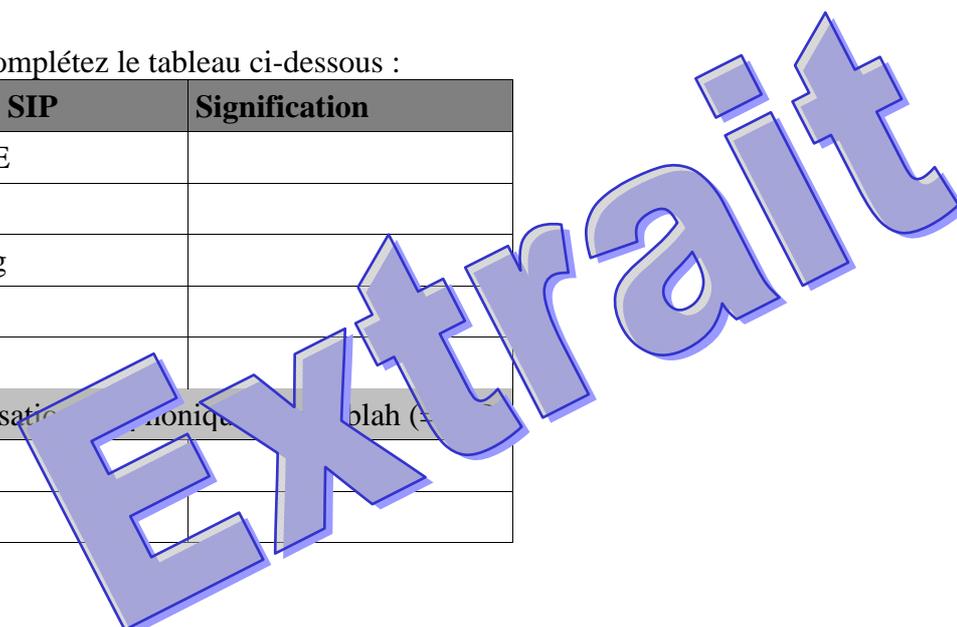


Cette fenêtre propose une représentation graphique des échanges de paquets SIP à travers le temps (axe vertical) et des adresses IP des machines impliquées (axe horizontal). Lorsque l'on clique sur une des flèches, le paquet correspondant est sélectionné dans la fenêtre principale.

Le premier échange 401/Unauthorized correspond au mécanisme d'authentification, nous n'en tiendrons pas compte dans le tableau suivant.

 Complétez le tableau ci-dessous :

Paquet SIP	Signification
INVITE	
Trying	
Ringing	
OK	
ACK	
Conversations téléphoniques (SIP)	
BYE	
OK	



1.1.1.1 Analyse de la négociation SDP des codecs

Codecs proposés par l'appelant

 Sélectionnez le paquet SIP INVITE sur le graph, et retrouvez ce même paquet marqué dans la fenêtre principale.

 Dans la partie basse de la fenêtre principale, on trouve le contenu du paquet.

 Développez la dernière ligne qui concerne « Session Description Protocol » (=SIP)

 Développez la dernière ligne de la partie « corps » du paquet SIP « Message Body »

 Développez la dernière ligne de la partie « Session Description Protocol » (=SDP)

 Listez les codecs présents dans les champs « media attributes (a) » :

 Indiquez les codecs qui correspondent à cette liste de codecs :

.....

.....

.....

 Comparez cette liste avec celle présente dans le menu « Edition > Préférences > Audio > Codecs du téléphone logiciel appelant.

☞ Modifiez cette liste dans le téléphone logiciel appelant et refaite une capture pour visualisez la nouvelle partie SDP du paquet SIP INVITE.

Sélection des codecs par l'appelé

Appelant : téléphone logiciel		Appelé : ...	
Audio		Audio	
Ordre	Codec	re	Codec
1	G.711 loi A		G.711 loi μ
2	G.711 loi μ	2	G.729
3		3	G.711 loi A

☞ Expliquez le principe du choix des codecs réalisé par le téléphone qui recoit l'appel et donnez le codec audio issue de cette sélection :

Explications :

.....

.....

.....

Codec Audio sélectionné par l'appelant

Codec sélectionné par l'appelé

☞ Sélectionnez le paquet SIP OK dans le graphique et retrouvez le même paquet marqué dans la fenêtre principale.

- ☞ Dans la fenêtre principale, trouvez le contenu du paquet.
- ☞ Développez la dernière ligne qui concerne « Session Initiation Protocol » (=SIP)
- ☞ Développez la ligne qui contient le corps du paquet SIP « Message Body »
- ☞ Développez la dernière ligne « Session Description Protocol » (=SDP)
- ☞ Listez les codecs présentés dans les champs « media attributes (a) » :

☞ Indiquez à quoi correspond ce codec :

3 Etude du protocole de Transport RTP

3.1 Analyse de la qualité du trafic RTP : delay et jitter

- Dans le menu déroulant « Telephony », sélectionnez « RTP », puis « Show All Streams ».
- Sélectionnez un flux RTP (communication dans un sens) et son correspondant dans l'autre sens), puis cliquez « Analyse ».
- Pour chaque onglet (« Forward Direction » et « Reverse Direction »), dans le résumé au bas de la fenêtre, les valeurs suivantes :

Pack	Sequen	Delta(n)	Jitter	Jitter (previous)	IP BW(k)	Mark	Status
17	45534	0.00	0.00	0.00	1.60	SET	[Ok]
19	45535	20.05	0.00	-0.05	3.20		[Ok]
21	45536	20.02	0.00	-0.08	4.80		[Ok]
23	45537	20.18	0.02	-0.26	6.40		[Ok]

Max delta = 140.23 ms at packet no. 640
 Max jitter = 0.25 ms. Mean jitter = 0.08 ms.
 Max skew = -3.19 ms.
 Total RTP packets = 856 (expected 856) Lost RTP packets = 10 (1.17%) Sequence error = 3
 Duration 17.10 s (-80 ms clock drift, corresponding to 7963 Hz (-0.47%))

Paramètre	Valeur maximale acceptée	Valeur recommandée
Latence maximale	150 ms	
Gigue maximale	20 ms	
Taux max de perte de paquets	2,6%	

1.1.1.2 Qualité de service

Les équipements de commutation (niveau 2) ou de routage (niveau 3) permettent aujourd'hui de garantir la qualité de service (latence max, gigue max...) en priorisant les flux voix ou video. Pour ce faire, les téléphones marquent ces paquets voix ou video aux niveaux 2 (802.1p) et/ou 3 (diffserv).

Par défaut, le videophone ekiga marque les paquets au niveau 3 avec la valeur par défaut 46 (=0x2E).

➤ Dans la fenêtre principale du logiciel de capture et d'analyse du trafic réseau, sélectionner un paquet **RTP** G.711 partant de ekiga, puis développez ce paquet au niveau « Internet Protocol » (=IP), puis développez les champs « Differentiated Service Code Point ».

➤ Retrouvez la valeur 46 dans ces champs « DiffServ Code Point ».

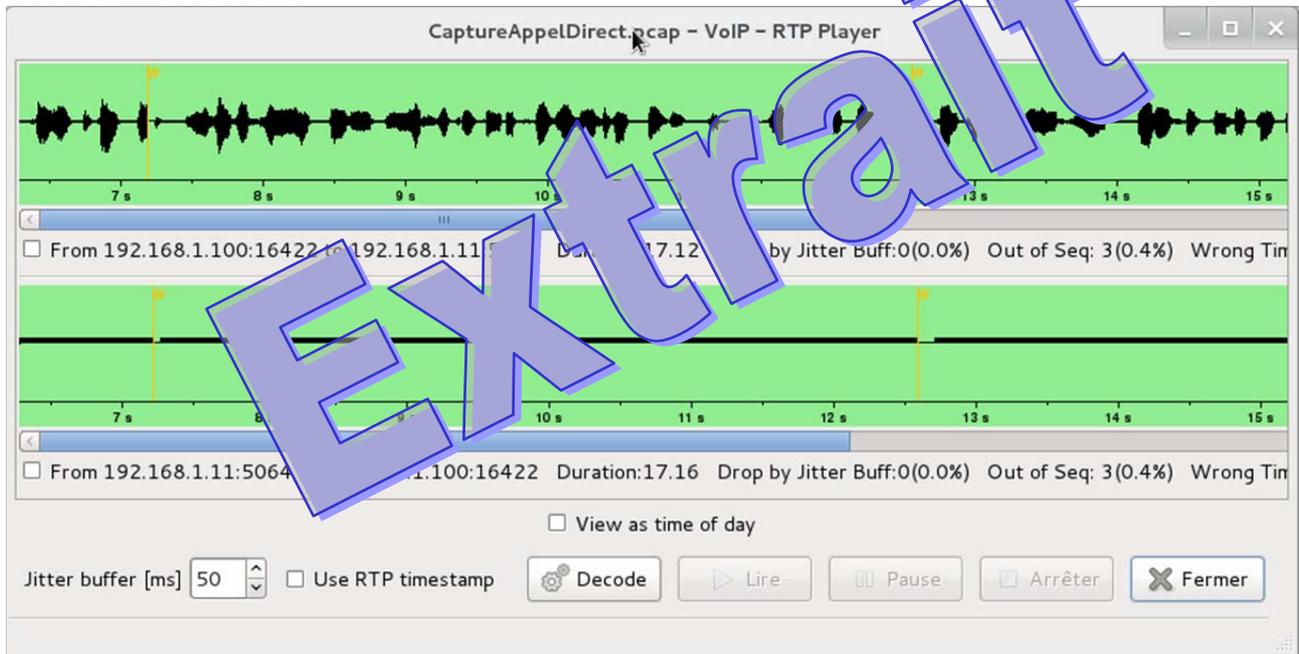
➤ Dans la fenêtre principale du logiciel de capture et d'analyse du trafic réseau, sélectionner un paquet **SIP** partant de ekiga puis développez ce paquet au niveau « Internet Protocol » (=IP), puis développez les champs « Differentiated Service Code Point ».

➤ Indiquez les paquets SIP et marqués (« taggés ») de la même manière que les paquets RTP :

Extrait

3.2 Ecoute des paquets RTP

☞ Dans la fenêtre « RTP Stream Analysis », cliquez sur « Player » puis comment écouter la conversation.



☞ Dans la fenêtre « RTP Stream Analysis », sélectionner « Save & Load » pour enregistrer le contenu des paquets RTP dans un fichier « Conversation.au ».

☞ Relisez le fichier « Conversation.au » à l'aide de la commande `play Conversation.au`

✍ Expliquez comment éviter les écouteurs :