

Introduction :

Le but de ce TP sera de nous familiariser avec le logiciel de captures de trames réseaux Wireshark ainsi que de connaître quelques commandes de base pour le réseau.

I. Récupération des paramètres réseaux et vérification du fonctionnement de celui-ci

1. Récupération des paramètres

Nous avons commencé le TP en identifiant les paramètres réseaux pré-établis à l'aide de la commande :

- ipconfig /all – Sous Windows
- ifconfig – Sous Linux

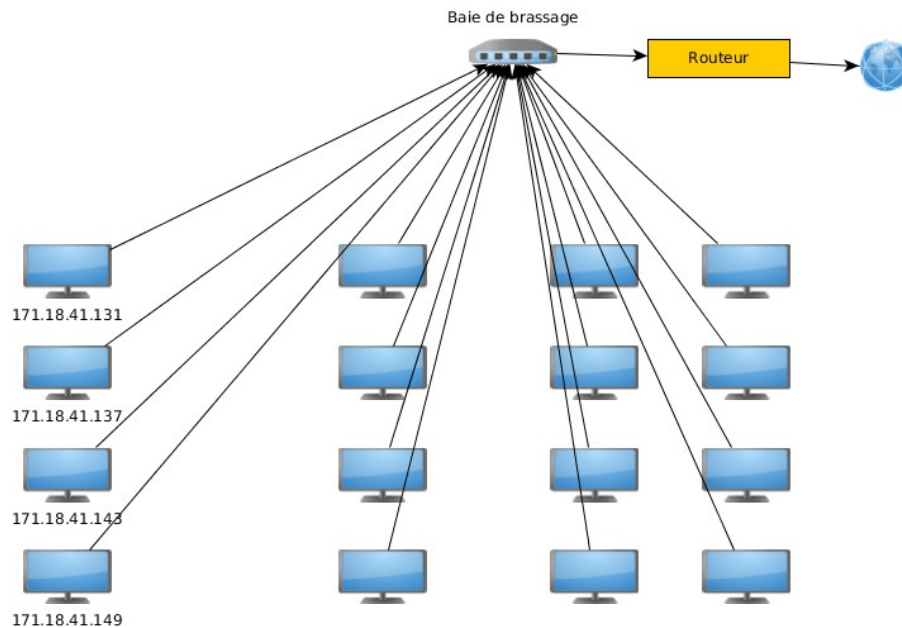
Voici les information recueillies :

	Poste avec Wireshark	Poste classique
Adresse IP	172.18.41.139	172.18.41.140
Masque sous-réseau	255.255.248.0	255.255.248.0
Passerelle	172.18.41.1	172.18.41.1
Adresse MAC	00:24:81:1A:21:88	00:24:81:1A:19:5C

Topologie du réseau

On remarque que le premier PC de la salle possède une adresse IP de 172.18.41.131 et que toutes les adresses IP des PC suivant se suivent.

Voici donc la topologie du réseau :



On a 5 PC (ici réduit à 4 pour la place) par rangée et toutes les adresses IP se suivent

2. Vérification du fonctionnement du réseau

Nous avons vérifié le fonctionnement du réseau à l'aide de la commande « ping » qui nous permet de vérifier qu'on obtient bien une réponse des PC auxquels on envoie les requêtes.

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrateur>ping 172.18.41.140

Envoi d'une requête 'ping' sur 172.18.41.140 avec 32 octets de données :

Réponse de 172.18.41.140 : octets=32 temps=1 ms TTL=64
Réponse de 172.18.41.140 : octets=32 temps<1ms TTL=64
Réponse de 172.18.41.140 : octets=32 temps<1ms TTL=64
Réponse de 172.18.41.140 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 172.18.41.140:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
C:\Documents and Settings\Administrateur>
```

On fait suivre la commande ping de l'adresse IP du PC à tester

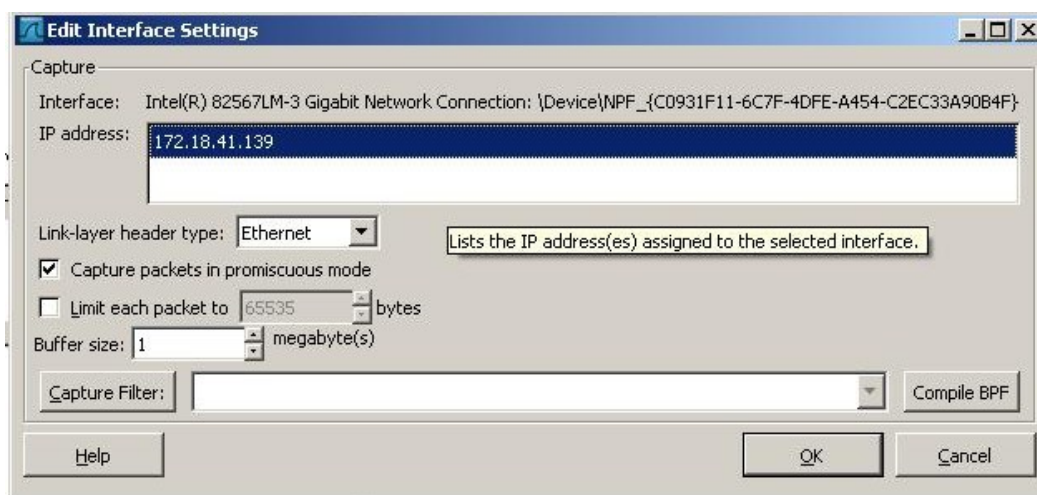
II. Réalisation des captures Wireshark

Le réseau ayant été étudié nous avons réalisé des captures des flux réseaux à l'aide du logiciel Wireshark.

Grâce à des filtres de captures il a été possible de sélectionner quel type de trafic nous souhaitions récupérer.

Leurs utilisation est décrite dans les chapitres suivant.

Tout d'abord nous avons réalisé une capture sans aucun filtrage afin de voir comment fonctionnait le logiciel.



Options de filtrage (ici aucune option)

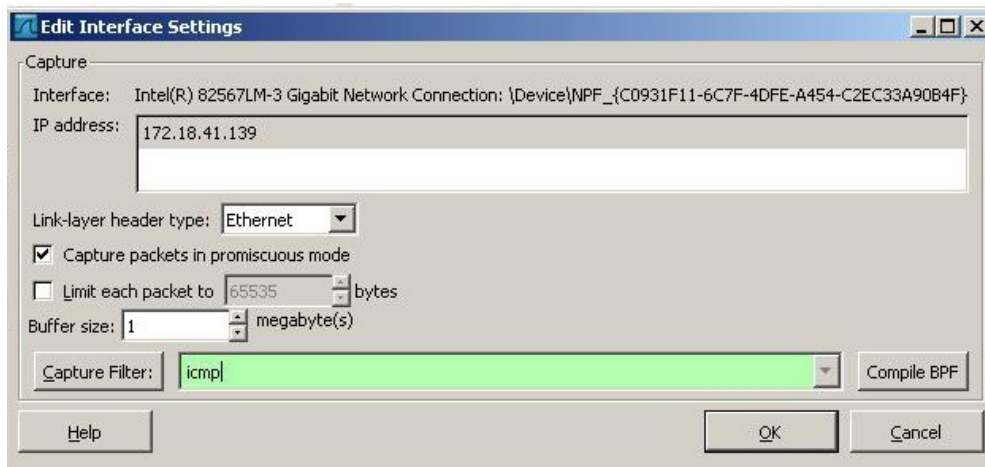
9	2.746617000	172.18.41.38	172.18.47.255	NBNS	92	Name query NB MSHOME<Id>	
10	2.747123000	172.18.41.23	172.18.47.255	NBNS	92	Name query NB MSHOME<Id>	
11	3.058998000	172.18.41.139	172.18.47.255	BROWSER	243	Host Announcement IC2S122-09, workstation, Server, NT workstation, Potential Bro	
12	4.000193000	Alcatel-_f3:f7:98	Spanning-tree-(for-br:STP	60	RST. Root = 0/0/00:e0:b1:ae:25:7c Cost = 3 Port = 0x7407		
13	4.060485000	172.18.41.38	172.18.47.255	NBNS	92	Name query NB MSHOME<Id>	
14	4.060933000	172.18.41.23	172.18.47.255	NBNS	92	Name query NB MSHOME<Id>	
15	6.000435000	Alcatel-_f3:f7:98	Spanning-tree-(for-br:STP	60	RST. Root = 0/0/00:e0:b1:ae:25:7c Cost = 3 Port = 0x7407		
16	8.000475000	Alcatel-_f3:f7:98	Spanning-tree-(for-br:STP	60	RST. Root = 0/0/00:e0:b1:ae:25:7c Cost = 3 Port = 0x7407		
17	10.000570000	Alcatel-_f3:f7:98	Spanning-tree-(for-br:STP	60	RST. Root = 0/0/00:e0:b1:ae:25:7c Cost = 3 Port = 0x7407		
18	12.000687000	Alcatel-_f3:f7:98	Spanning-tree-(for-br:STP	60	RST. Root = 0/0/00:e0:b1:ae:25:7c Cost = 3 Port = 0x7407		
19	14.000839000	Alcatel-_f3:f7:98	Spanning-tree-(for-br:STP	60	RST. Root = 0/0/00:e0:b1:ae:25:7c Cost = 3 Port = 0x7407		
20	14.226738000	Alcatel-_ae:25:7c	Broadcast	ARP	60	who has 172.18.41.87? Tell 172.18.41.1	
21	14.621980000	Alcatel-_ae:25:7c	Broadcast	ARP	60	who has 172.18.41.84? Tell 172.18.41.1	
22	16.000875000	Alcatel-_f3:f7:98	Spanning-tree-(for-br:STP	60	RST. Root = 0/0/00:e0:b1:ae:25:7c Cost = 3 Port = 0x7407		
23	18.001010000	Alcatel-_f3:f7:98	Spanning-tree-(for-br:STP	60	RST. Root = 0/0/00:e0:b1:ae:25:7c Cost = 3 Port = 0x7407		
24	18.410618000	172.18.41.127	224.0.0.251	MDNS	308	Standard query 0x0000 AAAA 1c2s120-01.local, "QM" question A 1c2mac-13.local,	

Résultat de la capture

1. Application de filtres pour les captures

Les options de filtrage (à la capture) sont définies dans les options de l'interface de capture, et plus exactement dans le champs « Filtre de capture » (Capture Filter) de cette fenêtre.

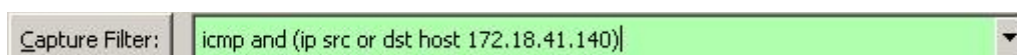
a) Filtrage ICMP



1	0.000000000	172.18.41.139	172.18.41.139	ICMP	98 Echo (ping) request	id=0x0925, seq=1/256, ttl=64
2	0.000372000	172.18.41.139	172.18.41.140	ICMP	98 Echo (ping) reply	id=0x0925, seq=1/256, ttl=128
3	1.000659000	172.18.41.139	172.18.41.139	ICMP	98 Echo (ping) request	id=0x0925, seq=2/512, ttl=64
4	1.000684000	172.18.41.139	172.18.41.139	ICMP	98 Echo (ping) reply	id=0x0925, seq=2/512, ttl=128
5	2.000463000	172.18.41.139	172.18.41.139	ICMP	98 Echo (ping) request	id=0x0925, seq=3/768, ttl=64
6	2.000481000	172.18.41.139	172.18.41.140	ICMP	98 Echo (ping) reply	id=0x0925, seq=3/768, ttl=128
7	5.110777000	172.18.41.138	172.18.41.139	ICMP	74 Echo (ping) request	id=0x0200, seq=15872/62, ttl=128
8	5.110798000	172.18.41.139	172.18.41.138	ICMP	74 Echo (ping) reply	id=0x0200, seq=15872/62, ttl=128
9	6.101545000	172.18.41.138	172.18.41.139	ICMP	74 Echo (ping) request	id=0x0200, seq=16128/63, ttl=128
10	6.101572000	172.18.41.139	172.18.41.138	ICMP	74 Echo (ping) reply	id=0x0200, seq=16128/63, ttl=128
11	7.101692000	172.18.41.138	172.18.41.139	ICMP	74 Echo (ping) request	id=0x0200, seq=16384/64, ttl=128
12	7.101719000	172.18.41.139	172.18.41.138	ICMP	74 Echo (ping) reply	id=0x0200, seq=16384/64, ttl=128
13	8.101543000	172.18.41.138	172.18.41.139	ICMP	74 Echo (ping) request	id=0x0200, seq=16640/65, ttl=128
14	8.101563000	172.18.41.139	172.18.41.138	ICMP	74 Echo (ping) reply	id=0x0200, seq=16640/65, ttl=128
15	10.056203000	172.18.41.140	172.18.41.139	ICMP	98 Echo (ping) request	id=0x0926, seq=1/256, ttl=64
16	10.056228000	172.18.41.139	172.18.41.140	ICMP	98 Echo (ping) reply	id=0x0926, seq=1/256, ttl=128
17	11.056300000	172.18.41.140	172.18.41.139	ICMP	98 Echo (ping) request	id=0x0926, seq=2/512, ttl=64

On peut donc capture les ping de différentes adresses

b) Filtrage ICMP sur 2 adresses

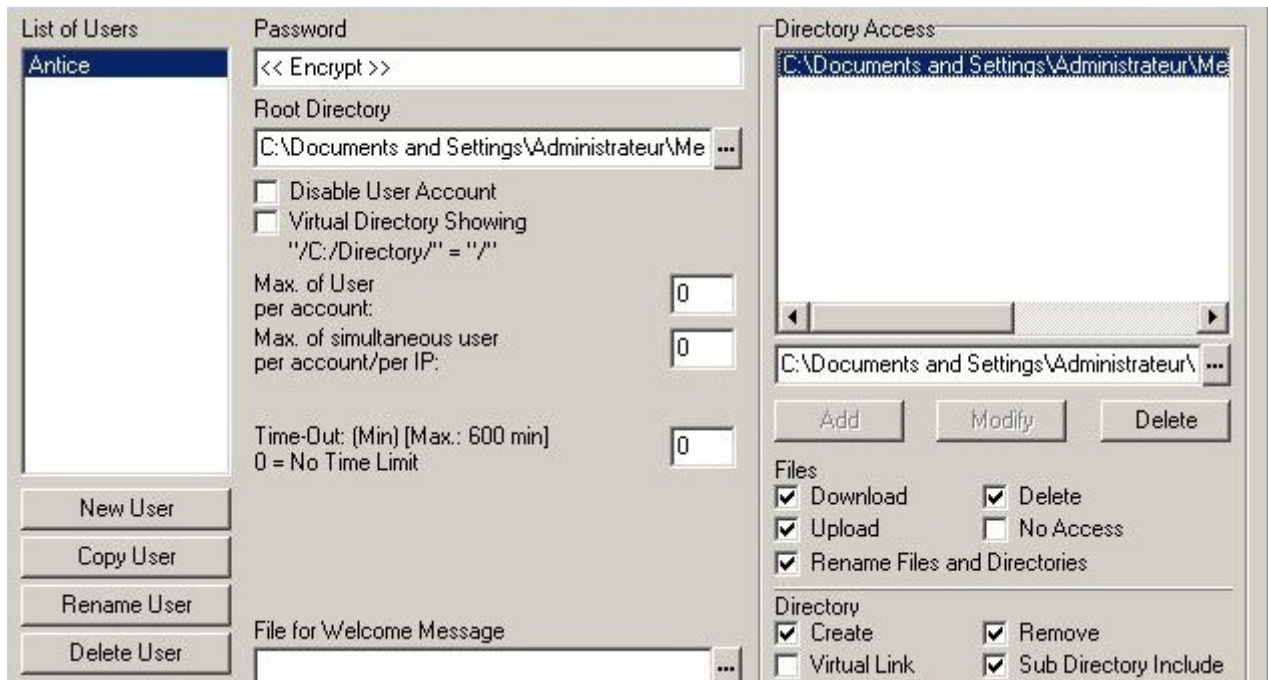


1	0.000000000	172.18.41.140	172.18.41.139	ICMP	98 Echo (ping) request	id=0x09d1, seq=1/256, ttl=64
2	0.000375000	172.18.41.139	172.18.41.140	ICMP	98 Echo (ping) reply	id=0x09d1, seq=1/256, ttl=128
3	1.000193000	172.18.41.140	172.18.41.139	ICMP	98 Echo (ping) request	id=0x09d1, seq=2/512, ttl=64
4	1.000217000	172.18.41.139	172.18.41.140	ICMP	98 Echo (ping) reply	id=0x09d1, seq=2/512, ttl=128
5	2.000110000	172.18.41.140	172.18.41.139	ICMP	98 Echo (ping) request	id=0x09d1, seq=3/768, ttl=64
6	2.000133000	172.18.41.139	172.18.41.140	ICMP	98 Echo (ping) reply	id=0x09d1, seq=3/768, ttl=128

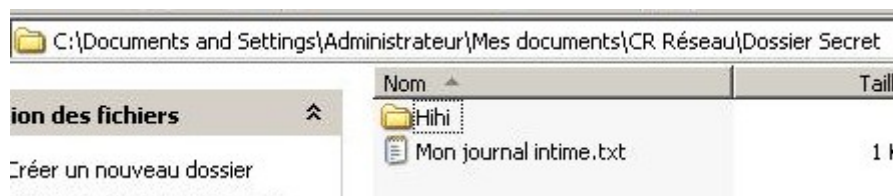
On obtient donc seulement les pings de l'adresse IP spécifiée

c) Filtrage FTP

Pour effectuer le filtrage FTP nous avons installé le serveur FTP *TYPsoft FTP Server* et l'avons configuré comme suit :



Droits de l'utilisateur Antice sur le "Dossier Secret" et ses fichiers/sous-dossiers



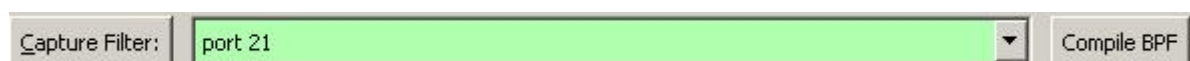
Organisation des fichiers au sein de dossier partagé "Dossier Secret"

On a donc un utilisateur :

- ID : Antice
- Mot de passe : azerty

Qui possède les tous les droits (sauf la création de liens symboliques) sur le « Dossier Secret »

Suite à notre configuration nous avons effectué une capture du trafic à l'aide du filtre suivant :



Puis nous avons réalisé une connexion :

Compte rendu de Réseau

```
ftp> open 172.18.41.139
Connecté à 172.18.41.139.
220 TYPSoft FTP Server 1.10 ready...
Utilisateur <172.18.41.139:(none)> : Antice
331 Password required for Antice.
Mot de passe :
230 User Antice logged in.
ftp> _
```

Connexion à un serveur FTP depuis le terminal
Windows

Voici une connexion non fructueuse au serveur vue par Wireshark :

30	31.61578400(172.18.41.139)	172.18.41.140	FTP	68	Response: 221 Goodbye!
31	31.61581300(172.18.41.139)	172.18.41.140	TCP	54	ftp > jllcelmd [FIN, ACK] Seq=110 Ack=33 win=65503 Len=0
32	31.61650600(172.18.41.140)	172.18.41.139	TCP	60	jllcelmd > ftp [ACK] Seq=33 Ack=111 win=65426 Len=0
33	31.61716800(172.18.41.140)	172.18.41.139	TCP	60	jllcelmd > ftp [FIN, ACK] Seq=33 Ack=111 win=65426 Len=0
34	31.61717900(172.18.41.139)	172.18.41.140	TCP	54	ftp > jllcelmd [ACK] Seq=111 Ack=34 win=65503 Len=0
35	33.47103000(172.18.41.140)	172.18.41.139	TCP	62	tssmap > ftp [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
36	33.47108900(172.18.41.139)	172.18.41.140	TCP	62	ftp > tssmap [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1460 SACK_PERM=1
37	33.47142800(172.18.41.140)	172.18.41.139	TCP	60	tssmap > ftp [ACK] Seq=1 Ack=1 win=65535 Len=0
38	33.47354000(172.18.41.139)	172.18.41.140	FTP	92	Response: 220 TYPSoft FTP Server 1.10 ready...
39	33.60721900(172.18.41.140)	172.18.41.139	TCP	60	tssmap > ftp [ACK] Seq=1 Ack=39 win=65497 Len=0
40	35.17498700(172.18.41.140)	172.18.41.139	FTP	67	Request: USER Antice
41	35.17549200(172.18.41.139)	172.18.41.140	FTP	89	Response: 331 Password required for Antice.
42	35.31720300(172.18.41.140)	172.18.41.139	TCP	60	tssmap > ftp [ACK] Seq=14 Ack=74 win=65462 Len=0
43	39.39904100(172.18.41.140)	172.18.41.139	FTP	78	Request: PASS antoine je t'aime
44	39.40143400(172.18.41.139)	172.18.41.140	FTP	76	Response: 530 Login incorrect.
45	39.54173400(172.18.41.140)	172.18.41.139	TCP	60	tssmap > ftp [ACK] Seq=38 Ack=96 win=65440 Len=0

On remarque dans le cadre vert, l'établissement de la connexion entre le serveur et le client puis la phase d'authentification en rouge qui se solde par un échec

2. Filtrages sur le protocole Ethernet

a) Filtrage IP

ether proto 0x800

Le protocole IP a pour valeur 0x800 dans une trame Ethernet

b) Filtrage sur les adresses MAC

ether dst or src 00:24:81:1A:19:5C

c) Filtrages conjugués

ether dst or src 00:24:81:1A:19:5C and host 172.18.41.140

On a un filtrage sur l'adresse MAC ainsi que sur l'adresse IP

d) Filtrage DNS

Nous avons effectué une capture d'une requête DNS sur le nom google.fr, voici la commande utilisée ainsi que le résultat dans Wireshark :

```
C:\Documents and Settings\Administrateur>nslookup google.fr
Serveur : dns2.univ-lemans.fr
Address: 195.221.244.106

Réponse ne faisant pas autorité :
Nom : google.fr
Addresses: 193.51.224.185, 193.51.224.187, 193.51.224.144, 193.51.224.148
193.51.224.152, 193.51.224.154, 193.51.224.155, 193.51.224.159, 193.51.224.163
193.51.224.165, 193.51.224.166, 193.51.224.170, 193.51.224.174, 193.51.224.176
193.51.224.177, 193.51.224.181
```

On remarque que le serveur "dns2.univ-lemans.fr" appartient à l'université

1	0.000000000	172.18.41.139	195.221.244.106	DNS	88	Standard query	0x0001	PTR 106.244.221.195.in-addr.arpa
2	0.000327000	195.221.244.106	172.18.41.139	DNS	189	Standard query response	0x0001	PTR dns2.univ-lemans.fr
3	13.375657000	172.18.41.139	195.221.244.106	DNS	88	Standard query	0x0001	PTR 106.244.221.195.in-addr.arpa
4	13.375994000	195.221.244.106	172.18.41.139	DNS	189	Standard query response	0x0001	PTR dns2.univ-lemans.fr
5	13.377709000	172.18.41.139	195.221.244.106	DNS	84	Standard query	0x0002	A google.fr.univ-lemans.fr
6	13.378035000	195.221.244.106	172.18.41.139	DNS	133	Standard query response	0x0002	No such name
7	13.379517000	172.18.41.139	195.221.244.106	DNS	69	Standard query	0x0003	A google.fr
8	13.380285000	195.221.244.106	172.18.41.139	DNS	471	Standard query response	0x0003	A 193.51.224.185 A 193.51.224.187 A 193.51.224.144 A

Jeu de requêtes/réponses entre le PC et le serveur DNS.

On remarque que les adresses de résultat dans le dernier paquet reçu sont celles utilisées dans la réponse du terminal au-dessus.

Le serveur nous répond « Réponse ne faisant pas autorité » car ce n'est pas lui qui possède directement les adresses associées au nom google.fr.

III. Capture des flux TCP lors d'une interaction entre un client et un serveur FTP

On a capturé plusieurs trames concernant la connexion d'un client à un serveur FTP, le dépôt d'un fichier sur le serveur puis la déconnexion de celui-ci.

Le capture est disponible en « Annexe1.pcapng » car sa taille est trop important pour réaliser des captures images.

IV. Affichage de la table ARP

Pour finir le TP nous avons affiché la table ARP à l'aide de la commande « arp -a » dans le terminal Windows.

Cette table associe des adresses MAC aux adresses IP du réseau afin d'éviter une nouvelle recherche de l'adresse de la machine réceptrice à chaque envoi de données.

Les entrées de la table peuvent être dynamiques (ajout d'une adresse automatiquement lors des jeu de requêtes/réponses du réseau) ou bien statiques (entrée en « dur » depuis le clavier).

```
C:\Documents and Settings\Administrateur>arp -a

Interface : 172.18.41.139 --- 0x10003
Adresse Internet    Adresse physique    Type
172.18.41.1         00-e0-b1-ae-25-7c   dynamique
172.18.41.140       00-24-81-1a-19-5c   dynamique
```

Exemple de l'exécution de la commande "arp -a" dans un terminal Windows.

Conclusion :

Ce TP a permis de découvrir l'analyseur réseau Wireshark ainsi que les interactions de bases entre différents équipements réseaux.

Une approche de la configuration des serveur FTP a également été effectuée lors de la séance.