Khomany Anice
Antoine Foucault

Compte rendu de Réseau

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

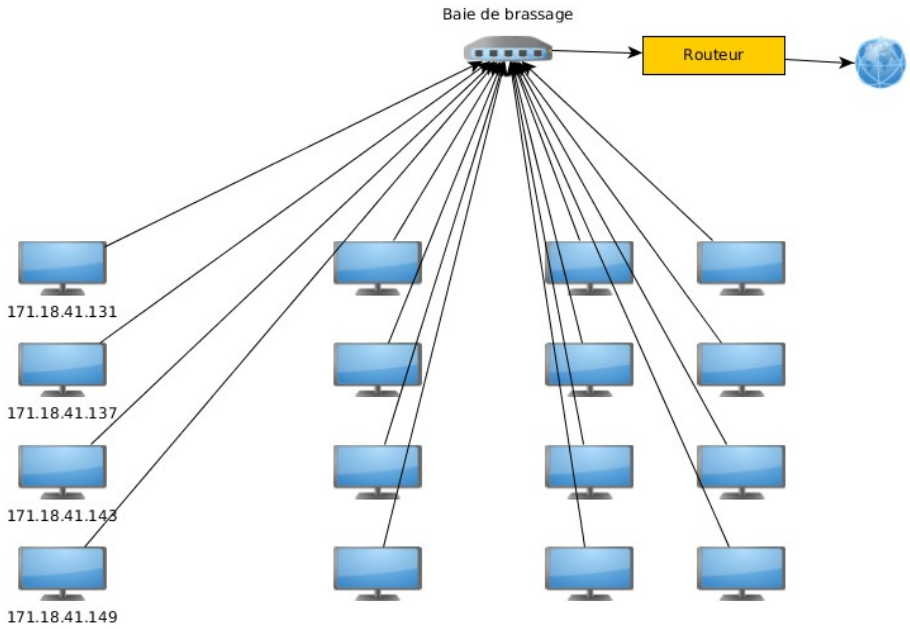
Khomany Anice
Antoine Foucault

Compte rendu de Réseau

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

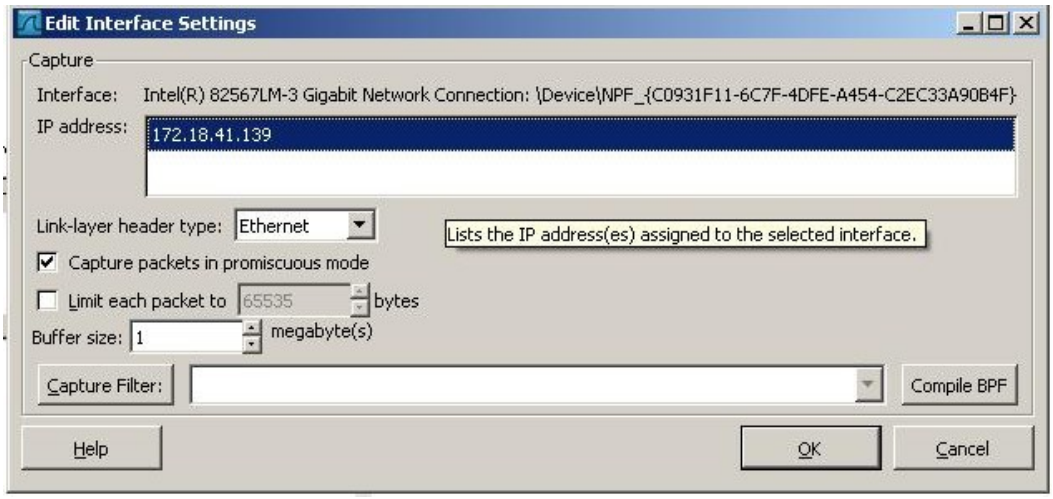
Nous avons vérifié le fonctionnement du réseau à l'aide de la commande « ping » qui nous permet de vérifier qu'on obtient bien une réponse des PC auxquels on envoi les requêtes.

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

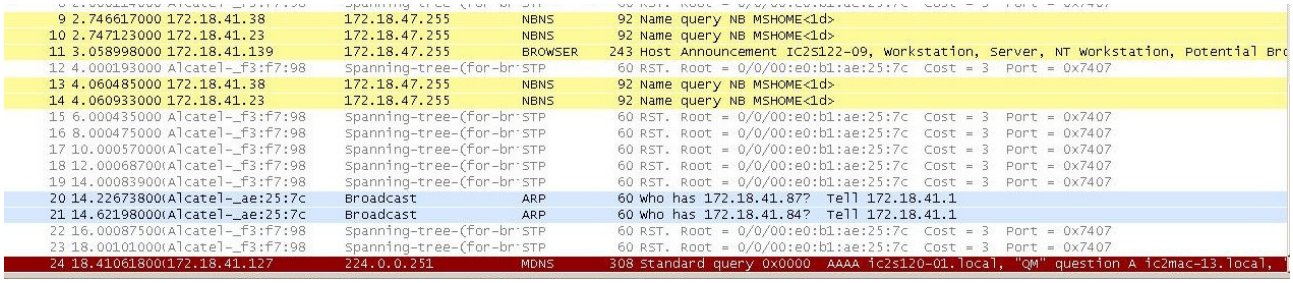
II. Réalisation des captures Wireshark

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)



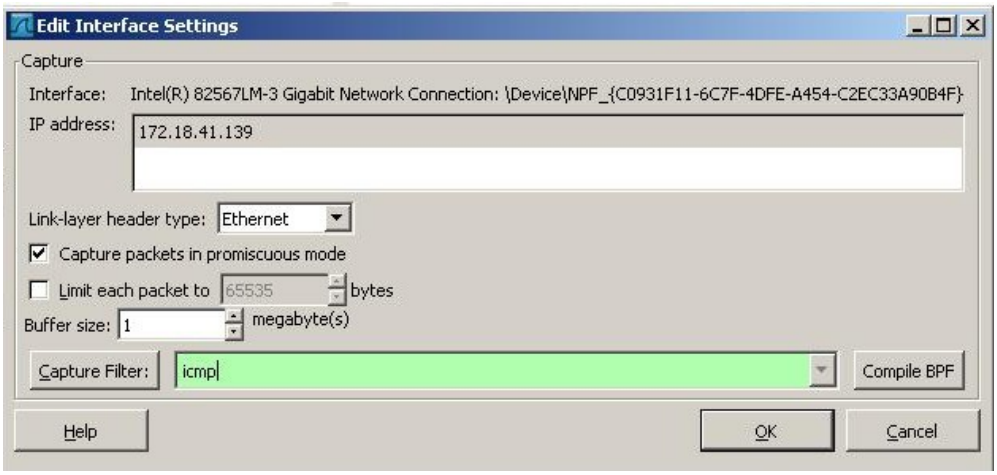
Résultat de la capture

1. Application de filtres pour les captures

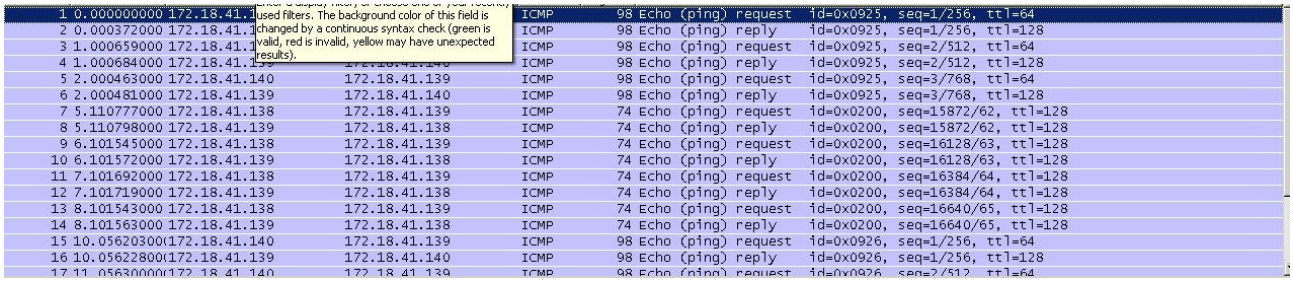
Les options de filtrage (à la capture) sont définies dans les options de l'interface de capture, et plus exactement dans le champs « Filtre de capture » (Capture Filter) de cette fenêtre.

Compte rendu de Réseau

a) Filtrage ICMP

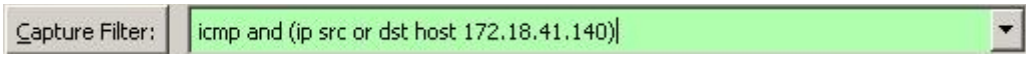


On applique ici le filtre icmp

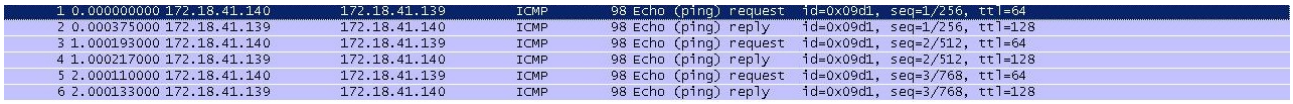


On peut donc capture les ping de différentes adresses

b) Filtrage ICMP sur 2 adresses



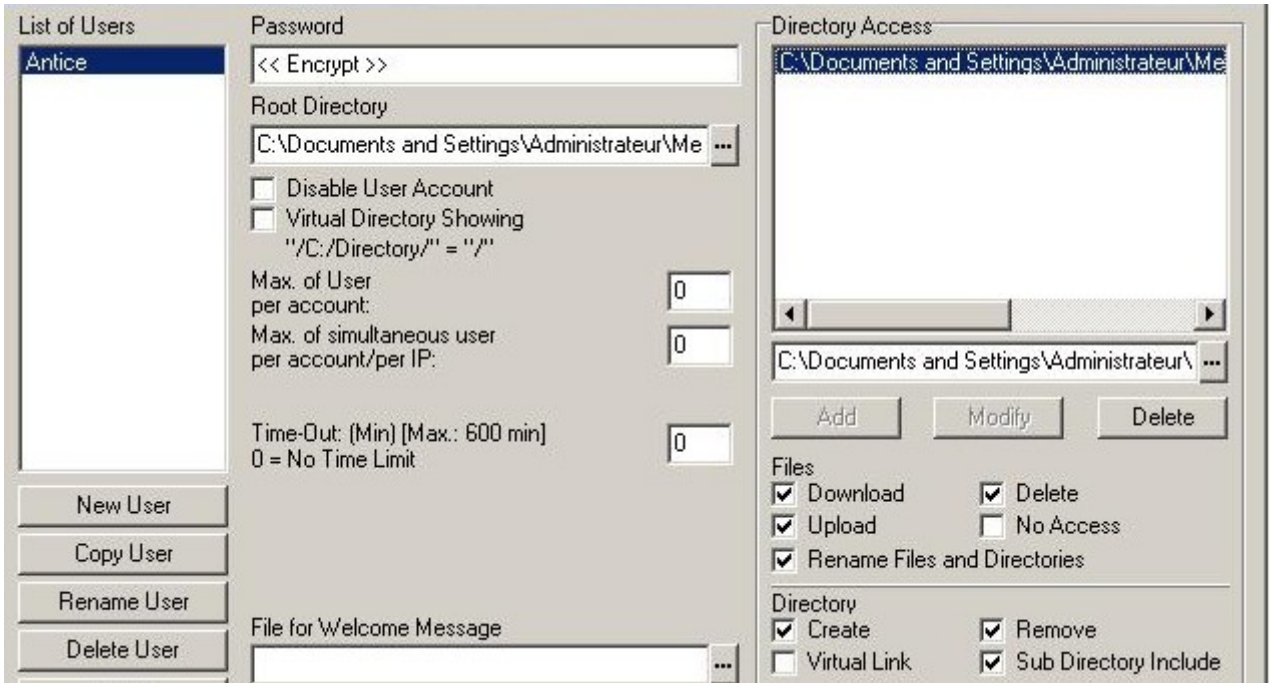
On applique le filtre de capture du protocole ICMP ainsi qu'une restriction sur l'adresse IP



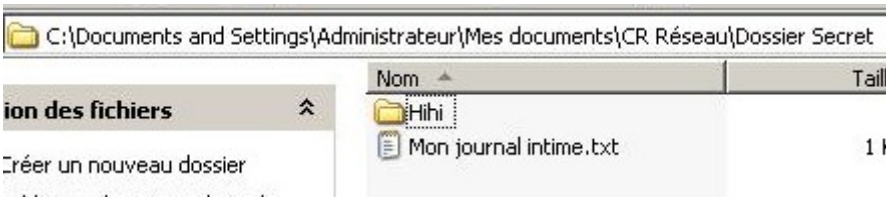
On obtient donc seulement les pings de l'adresse IP spécifiée

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 :

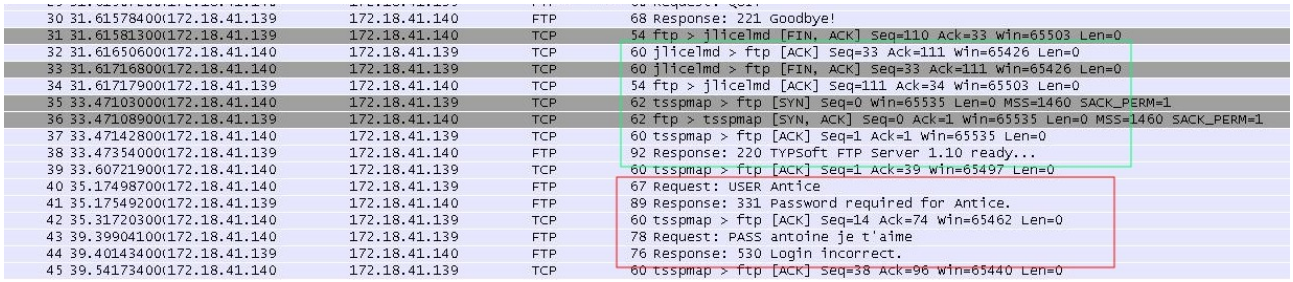
Puis nous avons réalisé une connexion :

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 une serveur FTP depuis le terminal Windows

Voici une connexion non fructueuse au serveur vue par WireShark :



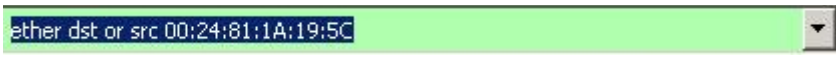
On remarque dans le cadre vert, l'établissement de la connexion entre le serveur et le client puis la phase d'authentification en rouge qui se solde par un échec

2. <u>Filtrages sur le protocole Ethernet</u>

a) Filtrage IP

Le protocol IP à pour valeur 0x800 dans une trame Ethernet

b) Filtrage sur les adresses MAC



c) Filtrages conjugués

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'exexcution de la commande "arp -a" dans un terminal Windows.

Khomany Anice
Antoine Foucault

Compte rendu de Réseau

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.