

TP 4 : Prise en Main de Wireshark et DHCP

Partie I : Prise en main de Wireshark

Objectif :

Être capable d'utiliser un analyseur de protocoles

Découvrir les caractéristiques générales et l'encapsulation des protocoles du modèle "TCP/IP"

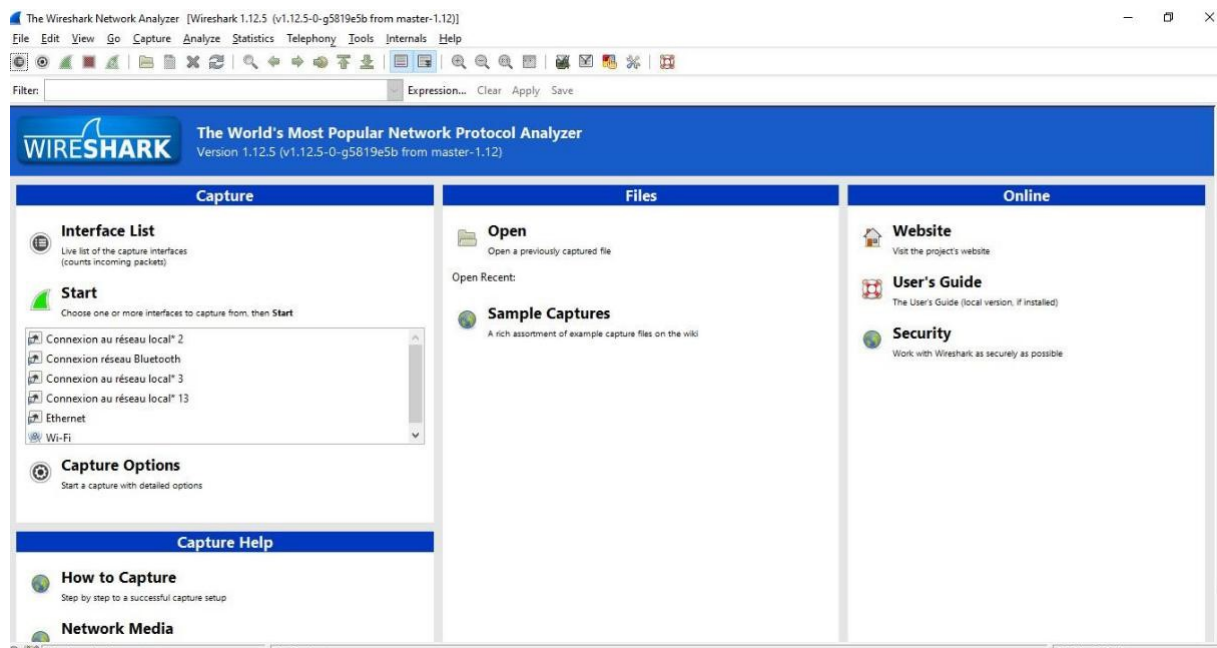
Wireshark est un analyseur de protocole réseau. Il permet de visualiser et de capturer les trames, les paquets de différents protocoles réseau, filaire ou pas.

Télécharger le logiciel Wireshark du site officiel de l'éditeur : <https://www.wireshark.org/>

Capture des trames sur le réseau

- 1- Lancer le logiciel Wireshark (double clic sur l'icône  sur le bureau)

Le logiciel s'ouvre sur cette page de menu :



- 2- Sélectionner capture / Interfaces....(ou cliquer sur interface List ci-dessus)
- 3- Repérer une entrée ayant du trafic réseau. Cliquer sur son bouton Start
- 4- Sélectionner une trame et faire son analyse

L'affichage se décompose en trois cadres :

The screenshot shows the Wireshark interface with the following components:

- Cadre 1 : trames capturées (capture en temps réel possible)**: A table listing captured packets. The table has columns: No., Time, Source, Destination, Protocol, and Info. It shows 11 packets, including TCP SYN, ACK, and HTTP GET requests.
- Cadre 2 : contenu décodé (couche par couche) de la trame sélectionnée dans le cadre 1**: Details of the selected packet (Frame 1). It shows the Ethernet II, Internet Protocol, and Transmission Control Protocol layers.
- Cadre 3 : "dump" en hexadécimale du protocole sélectionné dans le cadre 2**: A hex dump of the selected packet data, showing the raw bytes in hexadecimal and ASCII.

Cadre 1 : liste l'ensemble des paquets capturés

Cadre 2 : affiche le détail d'un paquet sélectionné dans la liste des paquets du cadre supérieur.

Cadre 3 : présente l'ensemble du paquet sous forme octale et ASCII. Ces octets contiennent les en-têtes des différentes couches de l'architecture TCP/IP ainsi que les données transmises par le processus à l'origine du message.



Analyse d'un paquet

Encapsulation d'un paquet

Lorsqu'un paquet est sélectionné, la zone centrale (cadre 2) permet de visualiser clairement les différentes couches d'encapsulation du paquet.

Les 5 entrées présentées correspondent à différentes encapsulations, ordonnées de la couche la plus basse à la couche la plus haute :

1. Données sur le média de capture : Wire = filaire
2. Trame relative à la couche liaison de donnée : Ethernet II
3. Paquet relatif à la couche réseau : Internet Protocol
4. Datagramme relatif à la couche transport : User Datagram Protocol
5. Données de l'application : regroupe généralement les couches session, présentation, application.

```

> Frame 5765 (65 bytes on wire, 65 bytes captured)
> Ethernet II, Src: Dell_b3:04:ee (00:1d:09:b3:04:ee), Dst: CompalIn_41:3e:16 (00:1b:38:41:3e:16)
> Internet Protocol, Src: 193.52.236.243 (193.52.236.243), Dst: 193.52.236.247 (193.52.236.247)
> User Datagram Protocol, Src Port: 55056 (55056), Dst Port: terabase (4000)
> Data (23 bytes)

```

Détail de chaque niveau d'encapsulation

Sur l'exemple présenté en Figure ci-dessous, nous avons étendu les entrées correspondant aux couches réseau, transport et application en cliquant sur les triangles correspondants. Nous pouvons voir entre autre que :

```

> Frame 5765 (65 bytes on wire, 65 bytes captured) (1)
> Ethernet II, Src: Dell b3:04:ee (00:1d:09:b3:04:ee), Dst: CompalIn 41:3e:16 (00:1b:38:41:3e:16)
▼ Internet Protocol, Src: 193.52.236.243 (193.52.236.243), Dst: 193.52.236.247 (193.52.236.247)
    Version: 4 (2)
    Header length: 20 bytes (3)
    > Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total length: 51 (4)
    Identification: 0x0000 (0)
    > Flags: 0x04 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (0x11) (5)
    > Header checksum: 0xde65 [correct]
    Source: 193.52.236.243 (193.52.236.243) (6)
    Destination: 193.52.236.247 (193.52.236.247) (7)
▼ User Datagram Protocol, Src Port: 55056 (55056), Dst Port: terabase (4000)
    Source port: 55056 (55056)
    Destination port: terabase (4000)
    Length: 31 (8)
    > Checksum: 0x5c85 [validation disabled]
▼ Data (23 bytes) (9)
    Data: 74657374206427656E766F6920646520657373616765
    [Length: 23]

0000  00 1b 38 41 3e 16 00 1d 09 b3 04 ee 08 00 45 00  ..BA>.....E.
0010  00 33 00 00 40 00 40 11 de 65 c1 34 ec f3 c1 34  .3..@. .e4..4 (10)
0020  ec f7 d7 10 0f a0 00 1f 5c 85 74 65 73 74 20 64  .... \.test d
0030  27 65 6e 76 6f 69 20 64 65 20 6d 65 73 73 61 67  'envoi d e messag (11)
0040  65
    e
  
```

Le paquet est de type IP v4 : ref (2)

Le type de données de ce paquet IP est un datagramme UDP : ref (5)

L'IP de la machine source est 193.52.236.243 : ref (6)

L'IP de la machine destination est 193.52.236.247 : ref (7)

Nous pouvons également faire un point sur la taille des données et des-en-têtes à différents niveaux d'encapsulation :

La taille des données envoyée par le processus est de 23 octets : ref (9)

La taille totale du datagramme UDP est de 31 octets - ref (8) - Cette valeur est la somme entre la taille réelle des données (23 octets) et 8 octets d'en-tête du paquet (8 étant une valeur fixe pour un paquet UDP)

La taille des en-têtes du paquet IP est de 20 octets : ref (3)

Le paquet IP contient un en-tête (20 octets) ainsi que le datagramme UDP (31 octets).

Sa taille totale est de 51 octets, taille rappelée en ref (4)

La taille totale du paquet IP est de (flèche). Cette valeur somme la taille du paquet UDP à la taille de l'en-tête IP.

Si l'on ajoute 12 octets d'en-tête pour la couche Ethernet II (taille fixe), la taille totale de la trame est de 65 octets, comme présentée en ref (1) sur Figure 5.

Notons ainsi que pour transférer 23 octets de données brutes, il nous a fallu transférer au total 65 octets (en fait il nous a même fallu transférer des octets supplémentaires avant la trame Ethernet. Ces octets seront ici passés sous silence).

- ***Visualisation octale de la trame***

La zone inférieure (cadre 3) permet de visualiser la trame capturée sous forme octale. Un clic sur n'importe lequel des niveaux d'encapsulation permet de visualiser la portion d'octets correspondante dans la zone inférieure de l'analyseur.

Partie II : Réseaux Sans Fils

Etre capable d'installer, de configurer et de mettre en place un Routeur/Point d'accès WiFi

Le WiFi (norme IEEE 802.11) a été conçu pour mettre en oeuvre des réseaux locaux s'affranchissant des fils. On parle donc de Wireless Lan (WLAN), c'est à dire « LAN sans Fil ».

Il existe plusieurs variantes du WiFi :

- **802.11b, 802.11g et 802.11n** compatibles entre eux, et fonctionnent tous deux avec une fréquence de 2.4Ghz. Le 802.11b atteint un débit maximal théorique de 11Mbit/s, le 802.11g monte à 54 Mbit/s et le 802.11n à 270 ou 300 Mbit/s.
- **802.11a** incompatible avec les 3 autres. Fréquence de 5GHz , débit de 54Mbit/s.

Il existe plusieurs modes de fonctionnement :

- ☐ Mode infrastructure (mode de point d'accès)
- ☐ Mode Client sans fil
- ☐ Mode Répéteur
- ☐ Mode Bridge (mode Pont)
- ☐ Mode Ad-Hoc (peer-to-peer)

Dans ce TP, on va se limiter sur le mode point d'accès :

1- Installation et Configuration du routeur / point d'accès

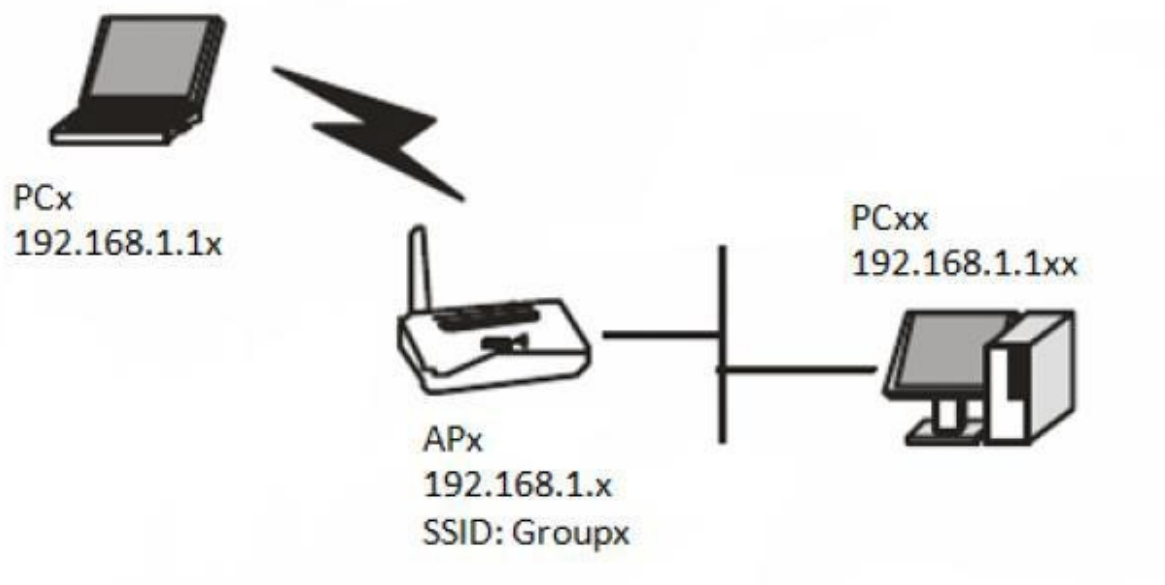


S1-2021/2022

1

- Utilisez un câble Ethernet pour connecter le port Ethernet du point d'accès au port de la carte réseau situé sur le poste.
- accéder à l'utilitaire web depuis votre poste (Ouvrez votre navigateur internet, et, dans la barre d'URL saisissez 192.168.1.1).
- À l'invite, tapez le nom d'utilisateur **admin** et le mot de passe **admin**. Cliquez sur **OK**.

2- Mode Point d'Accès

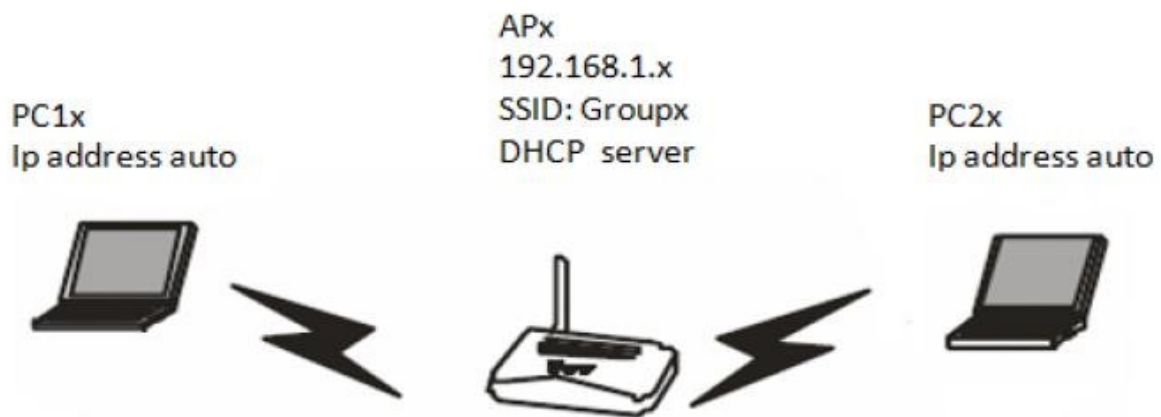


x = 1, 2, 3, 4, 5,6 (x est le nombre de groupe)

- Donner les adresses IP des machines PCx et PCxx
- Exécuter le PING entre PCx et PCxx (que dire de la TTL et qu'est ce qu'il signifie)

Partie II : Serveur DHCP

Les paramètres du serveur DHCP définissent la plage d'adresses IP qui peuvent être automatiquement attribuées aux stations du réseau.



Attribution des adresses automatiques pour le PC1x et PC2x.

Exécuter Wireshark et visualiser le message DHCP

Utiliser la commande 'ipconfig' pour vérifier la configuration

Exécuter la commande 'Ping' entre les deux PC

Vérifier la connexion des PCs sur le PA

