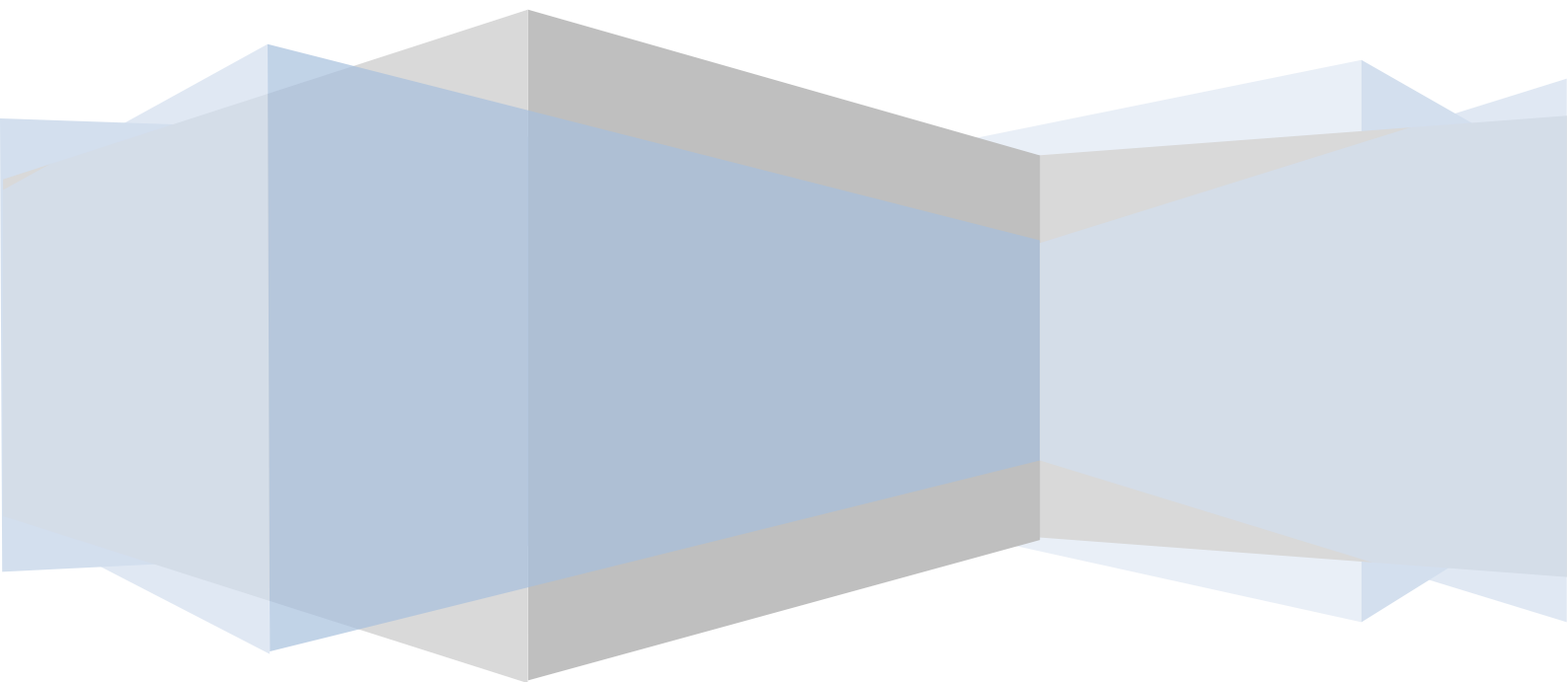


NSI – Classe de première

# Encapsulation, routage & protocoles

NSI - Réseaux informatiques

Courtois, Duffaud



## TABLE DES MATIERES

1.	Prérequis et thème .....	3
2.	Tests du réseau réel .....	3
2.1.	Déterminer ses adresses .....	3
2.2.	Communiquer avec son voisin .....	4
2.3.	Capturer des trames.....	5
3.	Tests d'un réseau virtuel.....	<b>Erreur ! Signet non défini.</b>
3.1.	Mode simulation .....	<b>Erreur ! Signet non défini.</b>
3.2.	Modification de l'infrastructure .....	<b>Erreur ! Signet non défini.</b>

---

## 1. PREREQUIS ET THEME

**Prérequis** : adressage IPv4, notions de protocole, adresse logique, physique, port, modèle OSI

**Objectif** : Se familiariser avec le parcours de séquence par la pratique

**Durée** : ~2h

**Matériel** : Salle d'info, PC sous Linux et/ou Windows, logiciels Packet Tracer, Wireshark

## 2. TESTS DU RESEAU REEL

L'objectif ici est de faire quelques manipulations simples sur notre machine afin de commencer à appréhender comment les machines communiquent sur un réseau.

### 2.1. DETERMINER SES ADRESSES



Sous Linux

Il vous faut lancer un terminal. A l'invite de commande, tapez :

```
ifconfig
```

Ou bien :

```
ip
```

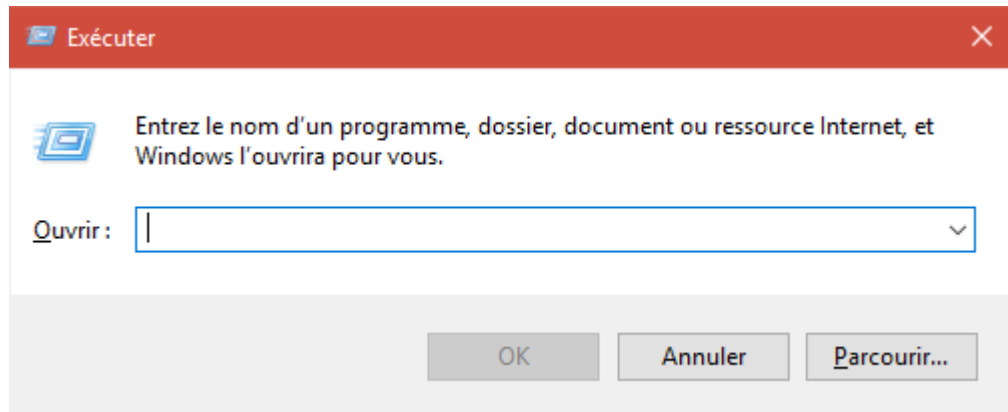
En résultat, vous devriez trouver toutes les informations concernant votre appareil, son ou ses adresses sur le réseau. En effet, votre ordinateur peut disposer de plusieurs interfaces réseaux (wifi, câble) et bien sûr, il dispose d'adresse IPv4 ou IPv6 et d'adresse MAC. Notez ces adresses avec le nom des interfaces correspondantes.

La commande `ifconfig` peut nécessiter d'être super utilisateur suivant les distributions, auquel cas, on utilisera la commande `ip`.



## Sous Windows

C'est quasiment la même chose. Lancez la commande Exécuter (Windows+R) et tapez dans le champ Ouvrir cmd. Un terminal Windows devrait s'ouvrir.



Dans ce terminal, il suffit de taper la commande

```
ipconfig
```

Cette commande seule ne vous fournira pas les mêmes informations que le ifconfig de Linux. Pour avoir les adresses physiques, il faut lui passer l'option /all comme ceci :

```
ipconfig /all
```

Notez les adresses avec le nom des interfaces correspondantes.

## 2.2. COMMUNIQUER AVEC SON VOISIN

Pour communiquer avec son voisin, on a besoin de son adresse IP. Ensuite, dans un premier temps, il suffit de faire un « ping » sur cette adresse. La commande ping est disponible sur Linux et Windows mais sous Linux, elle ne s'arrête pas d'elle-même. Du coup, 2 solutions, la barbare avec la combinaison Ctrl+C ou la civilisée en lui passant l'option -c (-n sous Windows) et en spécifiant le nombre de ping à faire.

```
ping -c 4 xxx.xxx.xxx.xxx
```

xxx.xxx.xxx.xxx est bien sur l'adresse IP de votre voisin.



## Point cours

La commande ping utilise le protocole ICMP (Internet Control Message Protocol) qui sert comme son nom l'indique, à contrôler les erreurs de transmission.

Pour vérifier que les services réseaux sont bien installés sur votre machine, vous pouvez pinguer votre adresse de boucle locale (adresse réservée) :

```
ping -c 4 127.0.0.1
```

Si ping n'est pas reconnu, vos services réseaux sont HS. C'est probablement un conflit entre anti-virus, firewall ou autre et une MAJ de l'OS. 127.0.0.1 doit TOUJOURS répondre, sinon.

## 2.3. CAPTURER DES TRAMES

### 2.3.1. LE VOISIN

Pour capturer des trames, rien ne vaut Wireshark. C'est un logiciel d'analyse de trame. Il peut capturer les trames réseaux tout comme, avec le bon plug in, les trames USB.



## Sous Windows

Suivant la version de Windows et de Wireshark, il vous faut être administrateur pour pouvoir capturer des trames sur vos interfaces réseau.

Pour le lancer en administrateur (en admettant que vous puissiez le faire), il suffit de lancer la commande Exécuter, de taper wireshark dans le champ Ouvrir et de faire la combinaison de touches Ctrl+Shift+Entrée. Cela lance le logiciel en mode administrateur.



## Sous Linux

Le problème peut aussi se poser ici. Dans un terminal, si vous passez en mode super utilisateur, soit par la commande `su`, soit par la commande `sudo -s`, il vous suffira ensuite de taper :

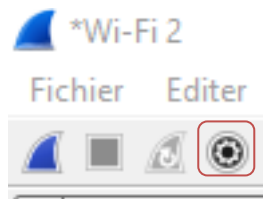
```
wireshark &
```

Ou bien restez sur votre compte utilisateur et tapez :

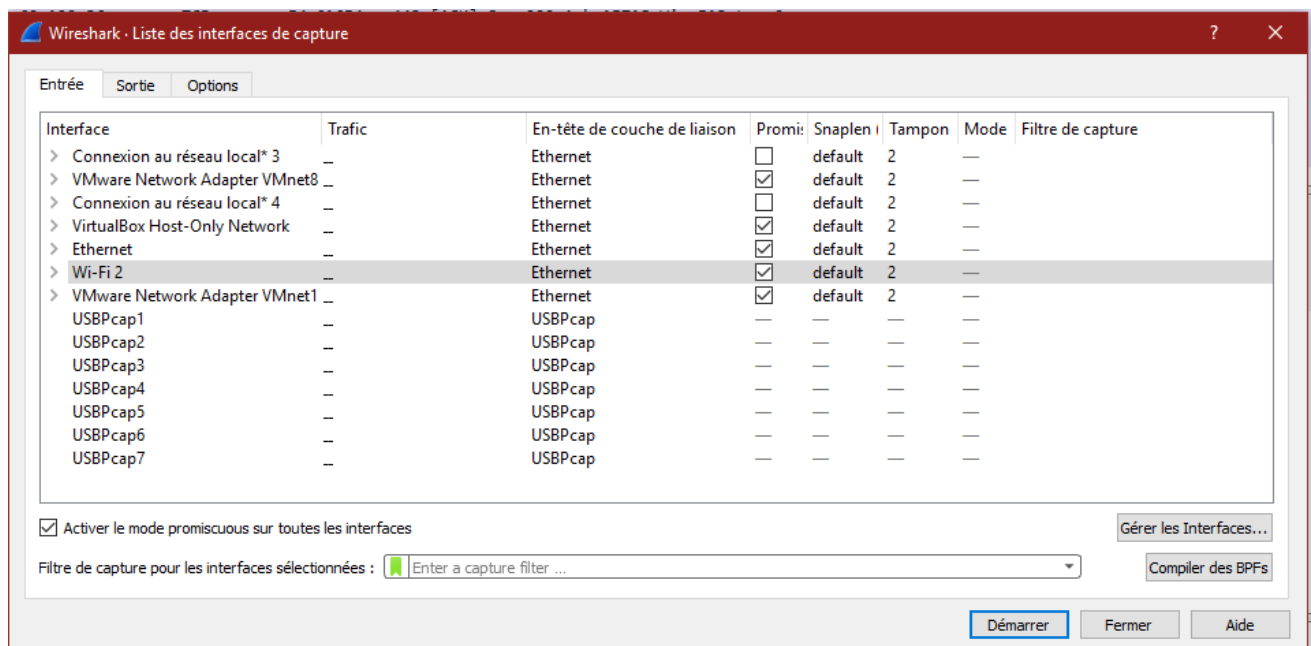
```
sudo wireshark &
```

Le `&` vous permet de reprendre la main sur votre terminal. Si vous l'oubliez, ce n'est pas grave, ouvrez en un autre.

Une fois Wireshark lancé, vous devez choisir l'interface à écouter en cliquant sur l'icône ronde Options de capture en haut à gauche de la fenêtre.



La fenêtre suivante apparaît, il suffit de choisir votre interface à écouter en la sélectionnant puis clic sur le bouton démarrer.



Sur votre terminal, pinguez à nouveau votre voisin. Si un navigateur est ouvert, vous allez voir énormément de trames. Pour la suite du TP, il suffit de mettre un filtre ICMP dans le champ filter.

Arrêtez la capture.

**Quelle est l'adresse MAC de votre voisin ?**

Toujours sur le même principe, pinguez quelques autres ordinateurs vous entourant. Notez les adresses MAC.

### 2.3.2. LES GAFA

Toujours sur le même principe, pinguez maintenant les GAFA (Google, Apple, Facebook et Amazon).

Vous ne connaissez pas l'adresse IP de leurs serveurs ? Pas de problème.



#### Point cours

La commande ping peut également utiliser une adresse telle qu'on les utilise dans un navigateur.

```
ping -n 4 google.fr
```

La commande ping vous retournera la réponse d'un des serveurs de Google (dans cet exemple) grâce au service DNS (Domain Name Server). Ce service fait le lien entre adresse IP et adresse web. Il vous est généralement fourni par votre fournisseur d'accès.

Capturez vos pings pour chacun des GAFA.

**Quelles sont leurs adresses IP ?**

**Leurs adresses MAC ?**

**Que peut-on remarquer ?**



## Point cours

Votre machine a besoin des adresses MAC pour pouvoir communiquer sur le réseau.

Elle stocke de manière temporaire les adresses qu'elle connait dans une table dite table ARP (Address Resolution Protocol).

Cette table fait la correspondance entre adresse IP et adresse MAC.

Vous allez regarder dans la table ARP de votre PC



## Sous Windows

Dans votre terminal, tapez

```
arp -a
```

Vous devriez retrouver quelques adresses IP connues, notamment celles de vos voisins directs.



## Sous Linux

C'est normalement la même commande que sous Windows. Mais il se peut que votre Linux n'accepte pas arp -a directement. Il vous faut soit taper

```
sudo arp -a
```

soit le chemin complet :

```
/usr/sbin/arp -a
```

RETROUVEZ-VOUS L'ADRESSE MAC DE VOS GAFA DANS CETTE TABLE ?

SI OUI, QUELLE ADRESSE IP Y EST ASSOCIEE ?



## Point cours

Votre machine est dans un réseau. Pour communiquer avec d'autres machines de ce réseau, elle n'a à priori besoin d'aucun intermédiaire et peut même se contenter de connaître uniquement une adresse MAC. Par contre, pour aller sur les sites comme ceux des GAFAs, il vous faut sortir du réseau. Vous passerez dès lors par une passerelle (un routeur) qui fera la jonction entre votre réseau local et les autres réseaux.

C'est ce que fait votre box chez vous.

Vous allez déterminer l'adresse de la passerelle de votre réseau.



## Sous Windows

Dans votre terminal, tapez

```
route PRINT
```

La commande vous retourne obligatoirement l'adresse de votre passerelle.



## Sous Linux

La commande est plus courte mais vous pouvez y accoler l'option `-n` pour n'afficher que les résultats numériques

```
route -n
```

CETTE ADRESSE EST ELLE DANS VOTRE TABLE ARP ?

QU'A-T-ELLE DE SIGNIFICATIVE PAR RAPPORT A NOS MANIPULATIONS CONCERNANT LES GAFAs ?

QUE PEUT-ON EN CONCLURE ?

Vous pouvez récupérer les adresses des routeurs par lequel un ping sur Google par exemple passera.



## Sous Windows

Dans votre terminal, tapez

```
tracert
```

La commande vous retourne le nombre de routeurs traversés et leurs adresses.



## Sous Linux

La commande est plus explicite ici

```
traceroute
```

Vous pouvez prendre chacune des adresses IP qui vous est retournée par cette commande et apprendre où elle est localisée géographiquement dans le monde grâce au site <https://www.iplocation.net/>.