Travaux pratique TCP_IP

Exercice 1 – Structure de l'adresse IP

A – Configuration réseau

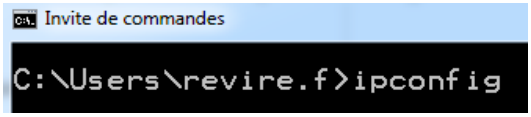
- Connectez-vous sur la machine DESKTOP-OV84LGJ, sous le compte

administrateur : Utilisateur : TSSR-07

Mot de passe : formation

Ouvrir une *Invite de commandes* (dans votre barre des taches), et exécutez la commande **ipconfig**

Icône de l'*Invite de commandes*



NB : Ignorez la carte réseau muni d'une adresse IP commençant par 169.X.X.X

Votre adresse IP : **192.168.2.17**

Masque de Sous-Réseau : **255.255.255.0**

Passerelle par défaut : **192.168.2.254**

Serveur DNS : **192.168.2.254**

- Analyse de la configuration :

Classe de votre NetID : **C**

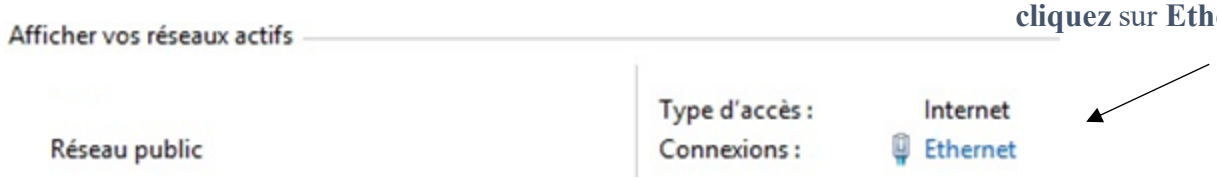
Présence de SubNetID : **Non, le masque respecte la classe donc pas de sous-réseaux**

Qui a fournit cette configuration IP : **Le DHCP**

- Afin de vous apprendre à configurer manuellement une carte réseau, vous allez appliquer vous-même cette configuration, pour cela ouvrez le **Panneau de configuration / Centre Réseau et partage**

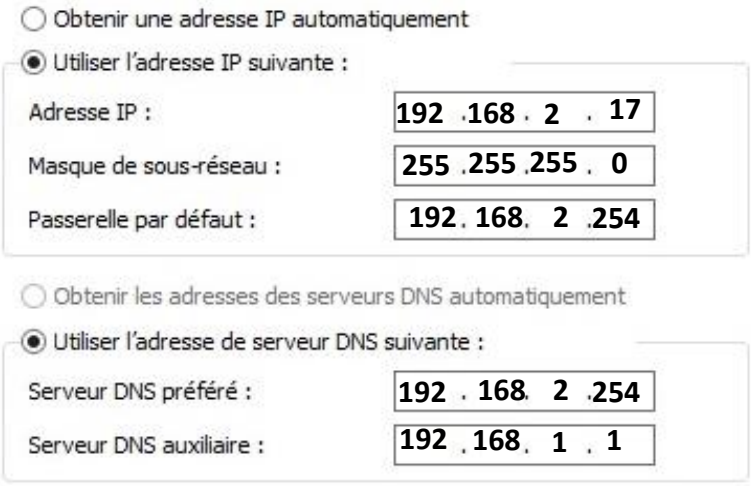
Centre Réseau et partage

Puis sur la ligne **cliquez** sur **Ethernet**



- Cliquez sur le bouton **Propriétés**.
- Sélectionnez le protocole **TCP/IPv4** et cliquez sur le bouton **Propriétés** :

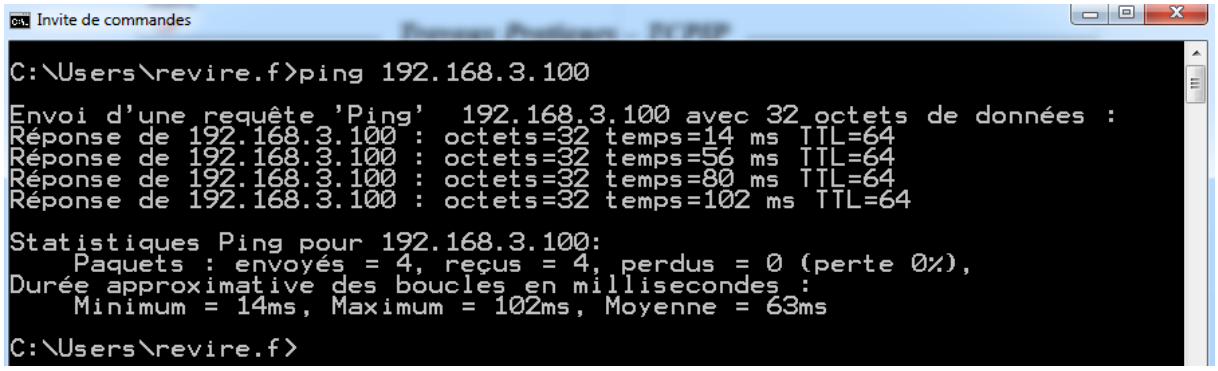
- Sélectionnez l'option **Utiliser l'adresse IP suivante**.



Saisissez la configuration précédemment relevé.

Puis validez par le bouton **OK**.

- Utilisez la commande de diagnostic **PING**, qui va vous permettre de vérifier la communication entre deux équipements situés sur un réseau.
- Vous pouvez effectuer la commande **ping** (dans une *Invite de commandes*), sur l'adresse IP d'un voisin ou sur une passerelle de votre centre de formation X.X.X.X



Question ouverte avec le formateur : Si deux interfaces réseau disposent d'une même adresse IP sur un même réseau, quelles sont les conséquences ?

-Situation impossible.

B – Masque de sous-réseau

Que représente une adresse IP ? Il s'agit de l'adresse d'une machine sur un réseau

Adresse logique de la machine, permettant de communiquer avec d'autres machines

@IP d'un Host	Masque	Classe de réseau	Nombre de SubNet
192.93.205.24	**255.255.255.0**	C	0
3.1.6.10	**255.0.0.0**	A	**non**
11.1.0.12	~~**255.0.0.0**~~ **255.255.0.0**	256 sous-réseau donc classless	**256 (8 Bits)**
129.39.1.15	**255.255.0.0**	B	
128.45.4.8	~~**255.255.0.0v**~~ **255.255.248.0**	32 sous-réseau donc classless	**32 (5 Bits)**
194.26.203.0	255.0.0.0	ERREUR	

Si j'utilise un masque de sous-réseau 255.255.255.240 (pour un NetID Classe C)

- Quel est le nombre de sous-réseau dont je dispose ? _

256 - 240 = 16 Le pas est de 16 adresses par sous-réseaux

- Quelles sont les deux premières plages d'adresses des hôtes ?

(0 - 16) et (17 - 32)

- Quelles sont les adresses réseaux, pour les deux premières plages ?

15 , 31,

- Quelles sont les adresses de diffusions, pour les deux premières plages ?

0 , 17

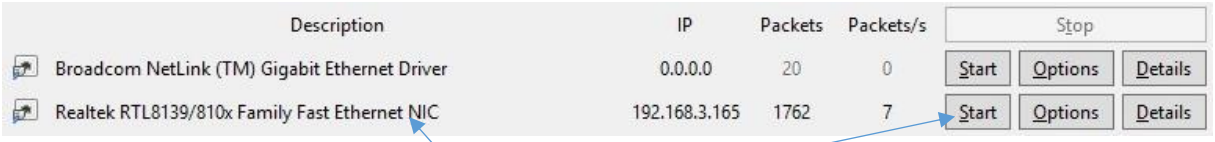
Exercice 2 – Couche Network Access

A – Sniffer

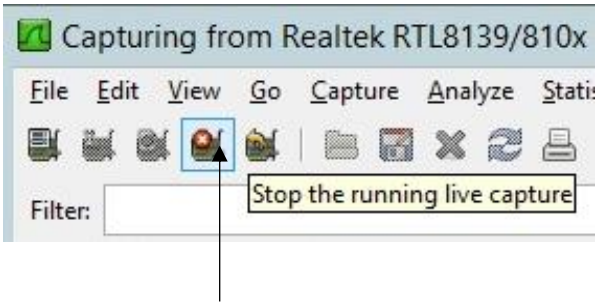
Le rôle d'un sniffer est de capturer les trames qui arrivent uniquement sur ses cartes réseaux.

- Installez **Wireshark**
- Le programme **Wireshark** est un logiciel sniffer gratuit.
- Démarrez le programme **Wireshark**, puis cliquez dans le menu *Capture / Interfaces…*

- Votre PC dispose d'un ou plusieurs cartes réseaux, une de marque Broadcom et une autre Realtek dans mon cas.
- Vous devriez constater des échanges de paquets à travers le compteur de Packets sur la carte Realtek dans mon cas toujours.



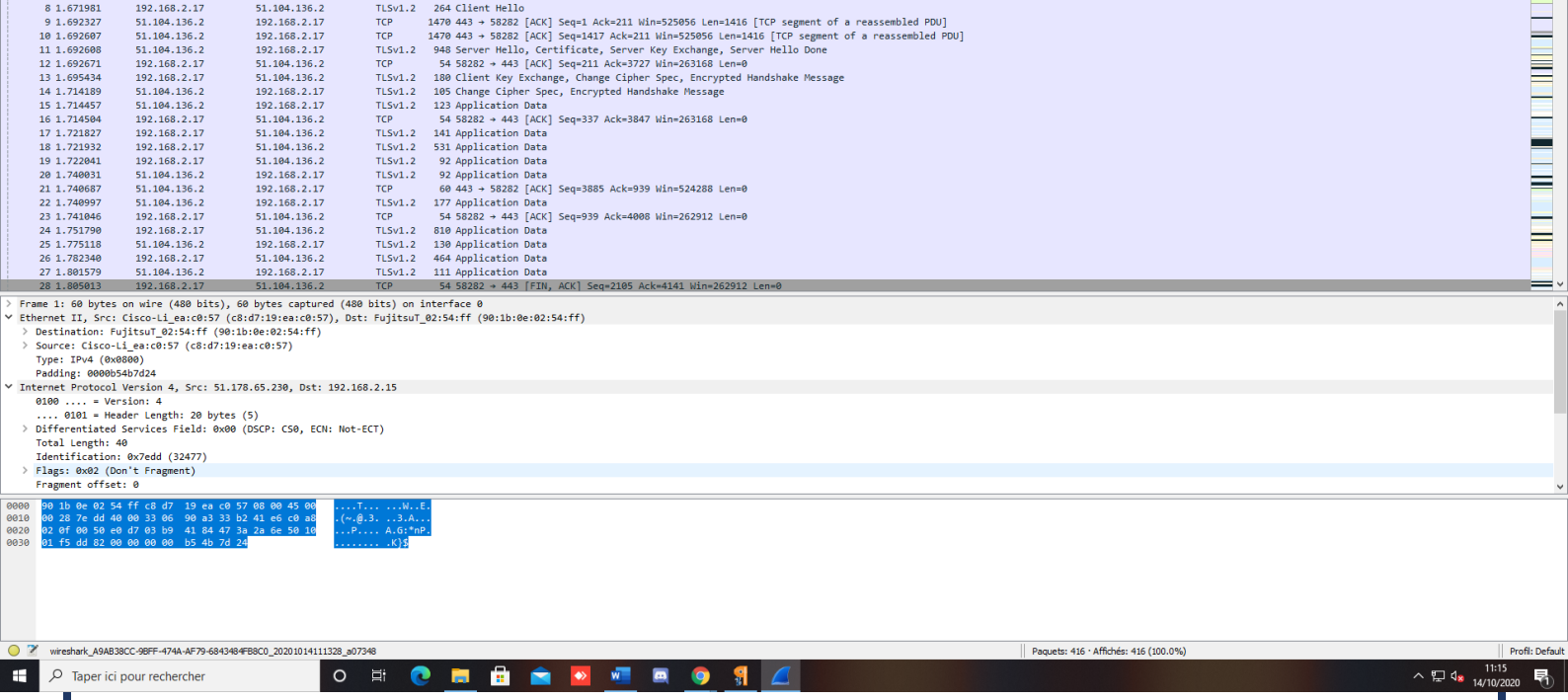
- Sur la ligne **Realtek**, cliquez sur le bouton **Start** afin de lancer la capture.
- Laissez quelques instants, puis arrêtez la capture en cliquant sur le bouton **Stop**.



Bouton pour stopper la capture

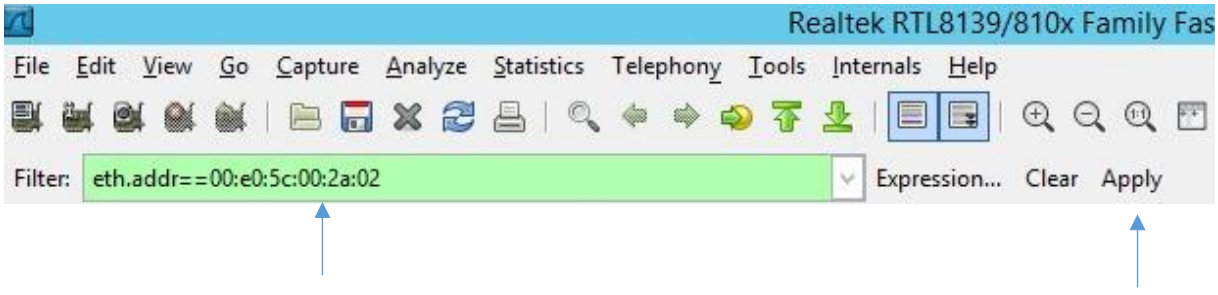
- Quel est le trafic essentiellement capturer ?

Le traffic essentiellement capturé est celui de mon adresse IP



Relevez l'adresse physique de votre carte Realtek : **90-1B-0E-02-56-77**

Retournez sur **Wireshark** et saisissez dans le champs **Filter** la ligne suivante :



Saisissez votre adresse physique

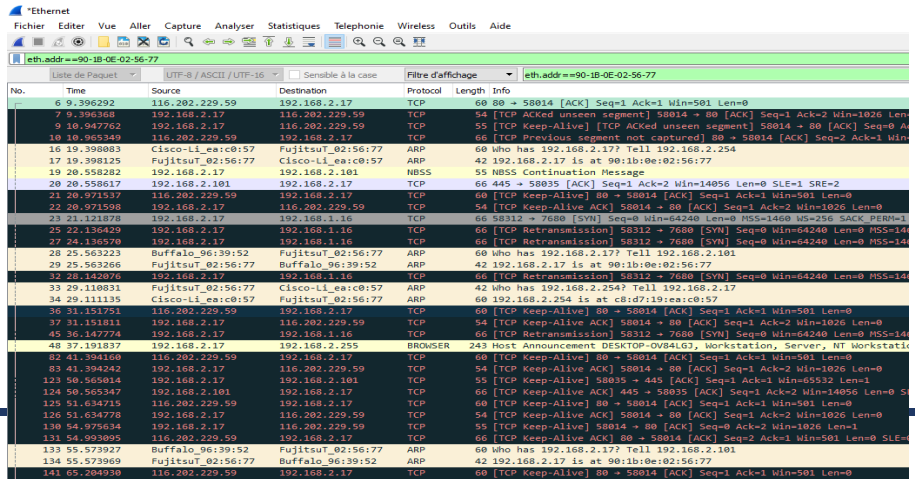
Puis validez votre filtre en cliquant sur le bouton **Apply**

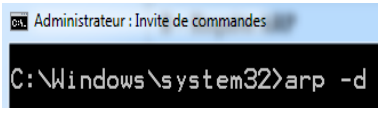
Après avoir appliqué le filtre, vous visualisez uniquement les trames traitées par cette interface.

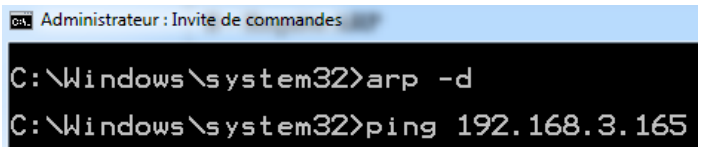
B – Requête ARP

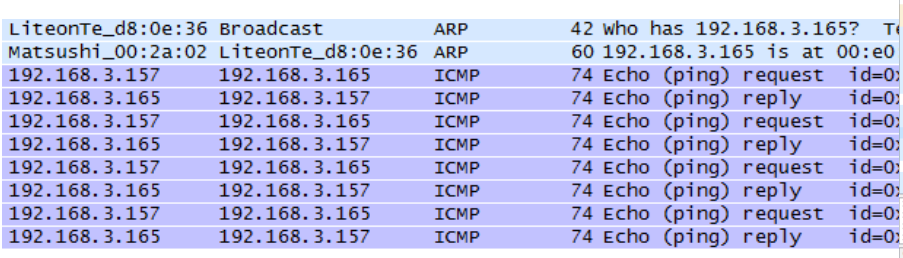
Pour faciliter cet exercice travaillez par deux, voisin A et voisin B.

Sur Wireshark gardez le filtre que vous avez appliqué précédemment.









- Le voisin A demande l'adresse IP du voisin B.

  IP Voisin B : 192.168.2.22

- Voisin A **et** Voisin B, ouvrent une *Invite de commandes* et tous deux exécutent la commande **arp –d.**

```
Administrateur : Invite de commandes
C:\Windows\system32>arp -d
```

Cette commande a pour fonction de vider le cache ARP, qui contient la résolution des adresses physiques et adresses IP récemment contactées (par ping ou autre action système)

- Voisin A **et** Voisin B, lancent tous deux la capture de trame avec **Wireshark**.

- Une fois la capture de trame en route le Voisin A, exécute dans *Invite de commandes* :**ping *ip_voisinB***

```
Administrateur : Invite de commandes
C:\Windows\system32>arp -d
C:\Windows\system32>ping 192.168.3.165
```

- Une fois le **ping** terminé, Voisin A **et** Voisin B arrêtent leur capture et analyser les trames échangées.
  Exemple :

```
LiteonTe_d8:0e:36 Broadcast         ARP    42 Who has 192.168.3.165?  Te
Matsushi_00:2a:02 LiteonTe_d8:0e:36 ARP    60 192.168.3.165 is at 00:e0
192.168.3.157     192.168.3.165     ICMP   74 Echo (ping) request  id=0x
192.168.3.165     192.168.3.157     ICMP   74 Echo (ping) reply    id=0x
192.168.3.157     192.168.3.165     ICMP   74 Echo (ping) request  id=0x
192.168.3.165     192.168.3.157     ICMP   74 Echo (ping) reply    id=0x
192.168.3.157     192.168.3.165     ICMP   74 Echo (ping) request  id=0x
192.168.3.165     192.168.3.157     ICMP   74 Echo (ping) reply    id=0x
192.168.3.157     192.168.3.165     ICMP   74 Echo (ping) request  id=0x
192.168.3.165     192.168.3.157     ICMP   74 Echo (ping) reply    id=0x
```

Exercice 3 – Couche Internet

A – Table de routage

- Analyse d'une table de routage, ouvrez une *Invite de commande* et lancez la commande **route print**

```
IPv4 Table de routage
===========================================================================
Itinéraires actifs :
Destination réseau    Masque réseau  Adr. passerelle   Adr. interface Métrique
          0.0.0.0          0.0.0.0    192.168.3.100    192.168.3.165     20
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
      169.254.0.0      255.255.0.0         On-link   169.254.183.240    286
  169.254.183.240  255.255.255.255         On-link   169.254.183.240    286
  169.254.255.255  255.255.255.255         On-link   169.254.183.240    286
      192.168.3.0    255.255.255.0         On-link     192.168.3.165    276
    192.168.3.165  255.255.255.255         On-link     192.168.3.165    276
    192.168.3.255  255.255.255.255         On-link     192.168.3.165    276
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link     192.168.3.165    276
        224.0.0.0        240.0.0.0         On-link   169.254.183.240    286
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link     192.168.3.165    276
  255.255.255.255  255.255.255.255         On-link   169.254.183.240    286
===========================================================================
```

Que représentent les colonnes suivantes :

Destination réseau : Ce sont toutes les adresses réservées à l'utilisateur
Adresse de la machine que l'on veut joindre

Masque de réseau : taille + important
Les types de masques de réseaux Subdivision logique d'un réseau de
Masque de réseau de l'adresse qu'on veut joindre (comme un code postal de destination)

Adr. Passerelle : l'adresse du routeur - PORTE DE SORTIE

Adr. Interface : l'adresse par laquelle passent les données afin d'aller d'un réseau à un autre adresse IP de la machine émettrice

métrique : Dans un protocole de routage, la **métrique** est une mesure de la « distance » qui sépare un routeur d'un réseau de destination. (nombre de noeuds qu'on traverse)

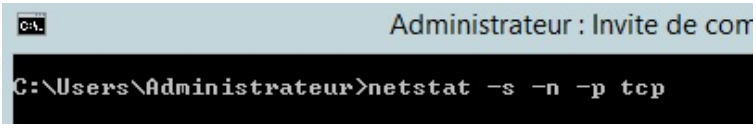
Exercice 4 – Couche Host To Host

A – Analyse du trafic TCP

Utilisation de la commande **netstat**

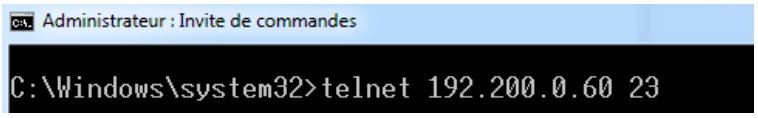
La commande **nestsat** peut permettre de tester l'accès aux ports d'une machine distante.
Exemple dans une *Invite de commandes*, lancez la commande **telnet 192.200.0.xx 5555 (l'adresse IP du voisin)**

- Et dans une deuxième fenêtre d'*Invite de commandes*, lancez la commande **netstat –s –n –p tcp**

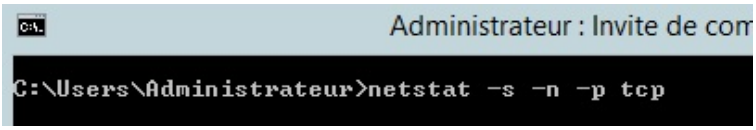


- Manipulation 2

Dans une *Invite de commandes*, lancez la commande **telnet 192.200.0.xx 23 (l'adresse IP du voisin)**



Et dans une deuxième fenêtre d'*Invite de commandes*, lancez la commande **netstat –s –n –p tcp**

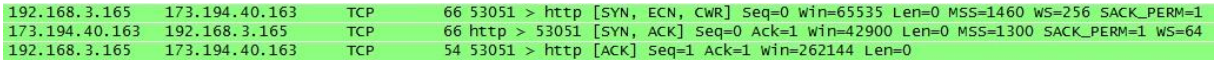


- Manipulation 3

Capture les trames sur une phase de SYN via une connexion TCP.

Méthode :

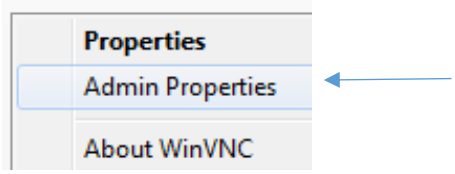
- Lancer une capture sur Wireshark.
- Puis ouvrir application en TCP (page web ou telnet…).
- Arrêtez la capture, et analysez les trames de synchro.



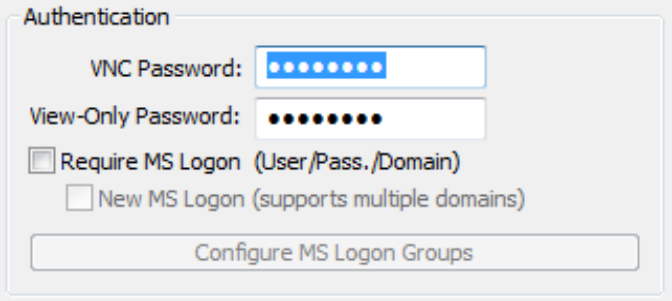
Exercice 5 – Couche Application A – Outil de connexion à distance

Utilisons l'application VNC, afin de prendre le contrôle à distance.

- Afin de permettre le contrôle à distance vous devez configurer le serveur VNC, cliquez droit sur l'agent VNC Serveur, icône bleu dans la zone de notification.
- Sélectionnez **Admin Properties**



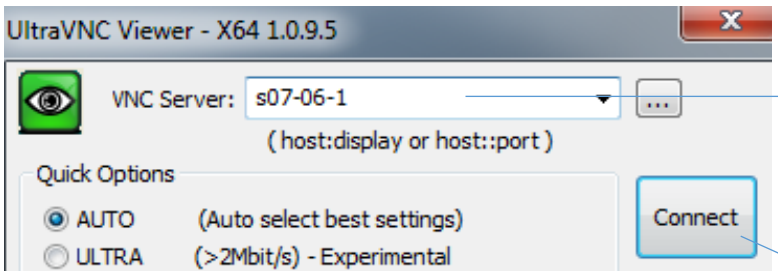
- Placez-vous dans le cadre **Authentication** et saisissez un mot de passe dans **VNC Password**.



- Puis validez sur **OK**.

- Utilisez maintenant l'application cliente de VNC pour prendre le contrôle, sur les routeurs des voisins (en leur demandant bien évidement le mot de passe qu'ils ont configuré sur leur Serveur VNC).

  L'application cliente est VNC Viewer (icône verte).

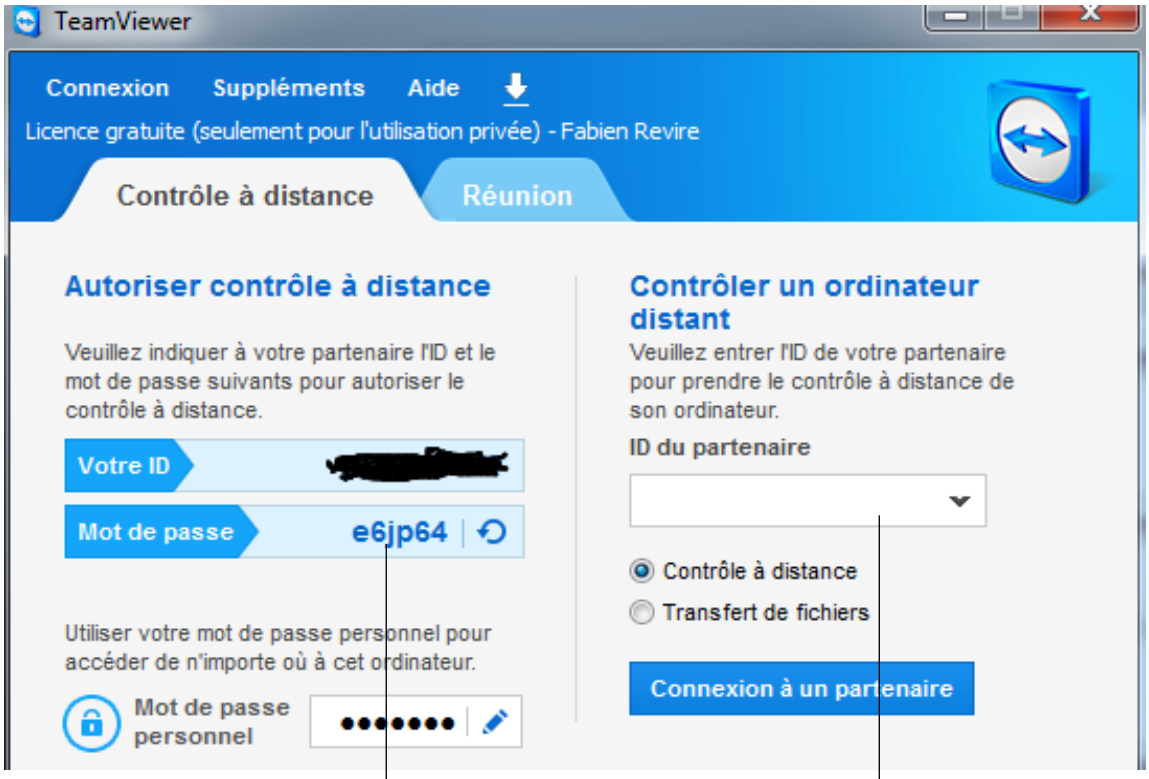


Saisissez le nom ou adresse IP du serveur VNC, que vous souhaitez prendre le contrôle.

Puis cliquez sur le bouton **Connect**.

Prendre la main sur une machine domestique, depuis un réseau extérieur via VNC:

- Autre solution Teamviewer, il s'agit du même outil, qui joue le rôle à la fois de client et de serveur :



Partie Serveur de l'outil Teamviewer

Partie Client de l'outil Teamviewer.

Exercice 6 – Résolution de nom

- **Résolution locale par fichier hosts**
- Placez-vous via l'explorateur de fichier, dans le dossier suivant :

C:\Windows\System32\drivers\etc

- Editez le fichier **hosts** avec le **Bloc-notes**.
- Apportez les modifications suivantes et enregistrez le fichier.

```
# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
192.200.0.1 GW
```

- Puis dans une *Invite de commandes* tapez la commande **ping gw**.

```
C:\Users\Administrateur>ping gw

Envoi d'une requête 'ping' sur GW [192.200.0.1] avec 32 octets de données :
```

Il s'agit d'une résolution **LOCALE**, ce fichier est connu uniquement sur votre machine.