



## ADMINISTRATION DES SYSTÈMES ET RÉSEAUX

# OUTILS DE BASE DE L'ADMINISTRATEUR DES RÉSEAUX

Auteur: Bernard GIACOMONI - Autoentreprise GIACOMONI Bernard

Version	Date	Objet
1.0	21/10/2019	Version initiale

## Table des matières

I. INTRODUCTION:	4
II. DIFFÉRENTS MOYENS D'ADMINISTRATION DES RÉSEAUX:	5
II.1. REMARQUE PRÉLIMINAIRE:	5
II.2. ADMINISTRATION DES POSTES DE TRAVAIL:	5
II.2.1. INTRODUCTION:	5
II.2.2. LES LOGICIELS ÉMULATEURS DE TERMINAUX:	5
II.2.3. PRINCIPAUX LOGICIELS ÉMULATEURS DE TERMINAUX:	6
II.2.3.1. TELNET:	6
II.2.3.2. RLOGIN:	7
II.2.3.3. SSH:	7
II.2.3.3.1. PRÉSENTATION:	7
II.2.3.3.2. UTILISATION:	7
II.2.3.4. PUTTY ET KITTY:	7
II.2.4. LES LOGICIEL DE PRISE DE CONTRÔLE A DISTANCE:	11
II.2.4.1. DÉFINITION:	11
II.2.4.2. UTILISATION:	11
II.2.4.2.1. PRINCIPAUX CAS D'UTILISATION:	11
II.2.4.2.2. CONDITIONS D'UTILISATION:	12
II.2.4.3. BUREAU A DISTANCE DE WINDOWS:	12
II.2.4.3.1. PRÉSENTATION:	12
II.2.4.3.2. AUTORISER LA CONNEXION SUR LE POSTE A CONTRÔLER:	12
II.2.4.3.3. PRENDRE LE CONTRÔLE A DISTANCE D'UN POSTE WINDOWS:	13
II.2.4.4. TEAMVIEWER:	16
II.2.4.4.1. PRÉSENTATION:	16
II.2.4.4.2. PRINCIPE DE FONCTIONNEMENT:	16
II.2.4.4.3. SÉCURITÉ:	17
II.2.4.4.4. UTILISATION POUR LE CONTRÔLE A DISTANCE:	17
II.2.4.5. LE LOGICIEL VCN:	19
II.2.4.5.1. PRÉSENTATION:	19
II.2.4.5.2. FONCTIONNEMENT:	19
II.2.4.5.3. UTILISATION EN MODE LISTENING VIEWER (ULTRA VNC):	20
II.3. ADMINISTRATION DES ROUTEURS:	23
II.3.1.1. RAPPELS:	23
II.3.1.2. CONNEXION AU SYSTÈME DE PARAMÉTRAGE D'UN ROUTEUR:	23
II.4. INSPECTION DES FLUX DE DONNÉES – LOGICIEL WIRESHARK:	25
II.4.1. PRÉSENTATION:	25
II.4.2. UTILISATION:	25
II.4.2.1. AVERTISSEMENTS:	25
II.4.2.2. DESCRIPTION DE LA PAGE D'ACCUEIL:	25
II.4.2.3. DÉMARRAGE D'UNE CAPTURE DE PAQUETS A PARTIR DE L'ACCUEIL:	27
II.4.2.4. REDÉMARRAGE D'UNE CAPTURE DE PAQUETS:	28
II.4.2.5. INSPECTION DES PAQUETS:	28
II.4.2.6. CRÉATION DE FILTRES ( À LA CAPTURE ET À L'ÉDITION):	29

III. COMMANDES D'ADMINISTRATION DES RÉSEAU:	30
III.1. INTRODUCTION:	30
III.2. PRINCIPALES TÂCHES D'ADMINISTRATION DES RÉSEAUX:	31
III.3. LES COMMANDES SYSTÈMES EN LIGNES DE COMMANDES:	32
III.3.1. INTRODUCTION:	32
III.3.2. RAPPEL:	32
III.3.2.1. SOUS LINUX/UNIX:	32
III.3.2.2. SOUS WINDOWS:	32
III.3.2.2.1. DROITS ASSOCIES AUX COMMANDES:	32
III.3.2.2.2. OUVERTURE EN MODE UTILISATEUR NON PRIVILÉGIÉ:	33
III.3.2.2.3. OUVERTURE EN MODE UTILISATEUR PRIVILÉGIÉ (ADMINISTRATEUR):	33
III.3.3. TEST DE LA CONNECTIVITÉ D'UNE MACHINE:	34
III.3.3.1. DÉFINITION:	34
III.3.3.2. COMMANDE PING (Windows et Unix/Linux):	34
III.3.4. DÉTERMINATION DE LA ROUTE D'UN PAQUET:	36
III.3.4.1. DÉFINITION:	36
III.3.4.2. UTILITÉ:	36
III.3.4.3. SOUS WINDOWS (Commande TRACERT):	36
III.3.4.4. SOUS LINUX/UNIX (Commande TRACEROUTE):	37
III.3.5. TEST DE L'ÉTAT DU RÉSEAU DANS UNE MACHINE:	38
III.3.5.1. DÉFINITION:	38
III.3.5.2. UTILITÉ:	38
III.3.5.3. COMMANDE NETSTAT:	39
III.3.6. GESTION ET VISUALISATION DES INTERFACES RÉSEAU:	41
III.3.6.1. DÉFINITIONS:	41
III.3.6.2. UTILITÉ:	42
III.3.6.3. IPCONFIG (window):	42
III.3.6.4. IFCONFIG (linux):	43
III.3.6.5. LA COMMANDE IP (linux):	43
III.3.6.5.1. PRÉSENTATION:	43
III.3.6.5.2. SYNTAXE GÉNÉRALE:	44
III.3.6.5.3. EXEMPLES:	44
III.3.7. FILTRER LES SORTIES D'UNE COMMANDES:	46
III.3.7.1. INTRODUCTION:	46
III.3.7.2. RAPPEL:	46
III.3.7.3. FILTRAGE PAR PIPELINES:	46
III.4. PRINCIPAUX FICHIERS DE CONFIGURATION DES RÉSEAUX:	48
III.4.1. FICHER /etc/hosts(Linux):	48
III.4.2. FICHER /etc/networks (Linux):	48
III.4.3. FICHER /etc/network/interfaces (Linux):	48
III.4.4. FICHER /etc/services (Linux):	49

## **I.INTRODUCTION:**

Parmi les missions qui lui sont confiées, l'administrateur de réseau est chargé plus particulièrement:

- De configurer et de paramétrer les logiciels de communication réseau installés sur les différents postes de travail et routeurs qui composent le réseau de l'entreprise ou de l'administration qui l'emploie (ce point inclue en particulier la gestion des droits d'accès des utilisateurs aux ressources);
- De surveiller le fonctionnement de ce réseau afin d'en détecter les dysfonctionnements et d'initier les actions correctives qui s'imposent;
- D'optimiser ce fonctionnement et de le sécuriser vis à vis des défaillances matérielles ou des actions malveillantes qui pourraient être menées par des agents extérieurs ou intérieurs à l'organisation utilisatrice du réseau.

Pour accomplir ces missions, l'administrateur a besoin:

- De surveiller et d'analyser les différents flux de données circulant dans le réseau (débits, contenus, etc.);
- D'intervenir sur les différents nœuds composant ce réseau (hôtes terminaux et routeurs) afin de les configurer, de les paramétrer ou d'en corriger les anomalies de fonctionnement.

Ces interventions doivent en général être effectuées à distance. En effet:

- Les interventions d'administration doivent perturber le moins possible l'activité des utilisateurs: de ce fait il est en général difficile d'utiliser l'IHM local (écran, clavier, souris) de la machine cible pour les réaliser;
- Beaucoup de nœuds d'un réseau (serveurs, routeurs, etc.) ne possèdent pas d'IHM d'exploitation local (par exemple, les routeurs). De ce fait, le seul moyen de s'y connecter est de le faire depuis un poste distant;
- Enfin, un réseau d'entreprise pouvant s'étendre sur plusieurs sites éloignés les uns des autres, l'administrateur peut difficilement effectuer les déplacements qu'impliquerait l'utilisation des IHM locaux.

De ce fait, l'administrateur intervient le plus souvent en se connectant à distance aux systèmes par l'intermédiaire de logiciels qui lui permettent:

- Soit de faire exécuter des "commandes en ligne" sur la machine cible par l'intermédiaire d'invites de commandes déportées;
- Soit de "prendre la main à distance" sur le système d'exploitation de cette machine;
- Soit encore d'inspecter, depuis un hôte du réseau, les flux de données circulant dans ce réseau.

## II.DIFFÉRENTS MOYENS D'ADMINISTRATION DES RÉSEAUX:

### II.1.REMARQUE PRÉLIMINAIRE:

A part les outils d'inspection des flux ("sniffers" de paquets), ces moyens ne sont pas spécifiques à l'administration des réseaux: on les emploie également pour l'administration des systèmes d'exploitation.

### II.2.ADMINISTRATION DES POSTES DE TRAVAIL:

#### II.2.1.INTRODUCTION:

Les postes de travail d'un réseau d'entreprise sont en général équipés de systèmes d'exploitation "généralistes": unix, linux, mac os, windows en version professionnelle, etc. Ils peuvent être administrés à l'aide de commandes systèmes ou de "script shells" à condition d'avoir accès à une "invite de commande" de leur système d'exploitation (fenêtre de type "console" sous windows ou "terminal" sous unix-linux. Nous avons vu que ces actions peuvent difficilement être effectuées à partir de l'IHM local de ces postes. De ce fait, il va falloir recourir à des émulateurs de terminaux ou à des logiciels permettant de prendre à distance le contrôle sur l'IHM local.

#### II.2.2.LES LOGICIELS ÉMULATEURS DE TERMINAUX:

Ces logiciels permettent d'ouvrir sur l'écran d'un poste de travail connecté au réseau une "invite de commande" (un "shell") agissant sur un hôte distant, conférant ainsi à ce poste de travail la fonction de TERMINAL DÉPORTÉ de l'hôte distant.

Ces logiciels présentent une architecture de type "client-serveur": le CLIENT, situé sur le poste local de l'administrateur, se connecte au SERVEUR situé sur le poste distant que l'on veut administrer :

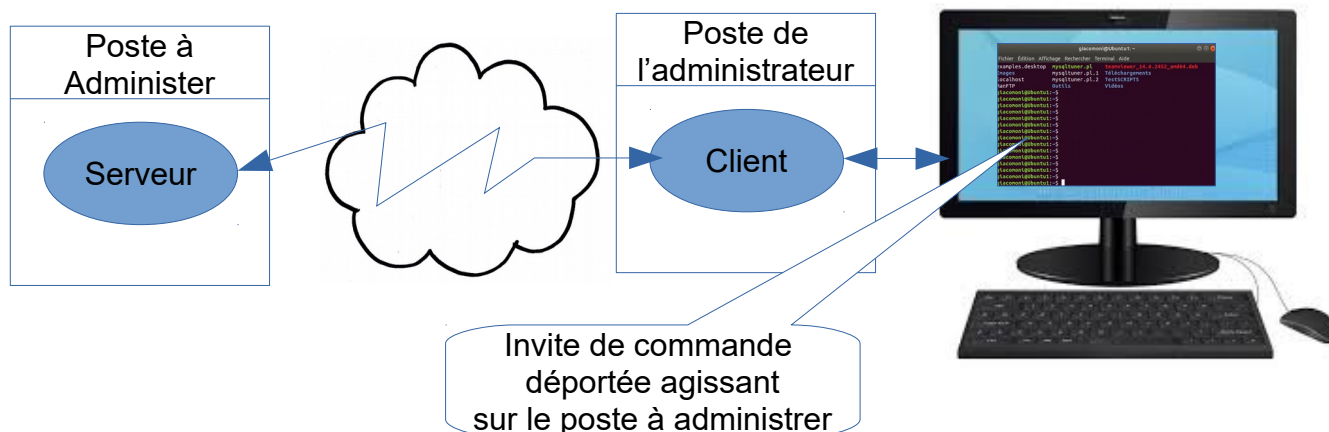


Figure II.2 .2 : Terminal déporté et invite de commande

Ceci implique:

- **Que le CLIENT soit INSTALLÉ sur la machine utilisée par l'administrateur.** La plupart des clients de ces logiciels sont installés automatiquement dans les versions de base des systèmes d'exploitation . Dans le cas contraire, il faudra les installer manuellement;
- **Que le SERVEUR soit INSTALLÉ et DÉMARRÉ sur la machine distante.** Ces serveurs, restant à l'écoute en permanence, consomment beaucoup de la puissance des processeurs. De ce fait, ils ne sont généralement pas installés dans les versions de base des O.S: il faudra donc les installer avec option de démarrage automatique au lancement du système d'exploitation de la machine.

### ***II.2.3.PRINCIPAUX LOGICIELS ÉMULATEURS DE TERMINAUX:***

#### ***II.2.3.1.TELNET:***

##### **PRÉSENTATION:**

Telnet (Terminal Network) est un protocole de communication de niveau application. Il permet de communiquer en mode TEXTE avec un serveur distant (serveur TELNET), dans un terminal déporté ouvert sur l'écran du poste de l'administrateur. Le protocole de transport est TCP et le port par défaut 23.

Telnet demande une authentification par nom d'utilisateur et mot de passe. En revanche, les échanges se font en clair (sans cryptage): les informations échangées par TELNET ne sont donc pas sécurisées. Ceci explique que TELNET est de plus en plus abandonné au profit de SSH pour l'administration des réseaux.

Malgré ce défaut, TELNET est encore utilisé car un serveur TELNET est très souvent présent "de base" sur les équipements réseaux (postes UNIX, LINUX et WINDOWS), contrairement à SSH.

##### **UTILISATION:**

La commande de lancement de TELNET sous linux s'écrit:

```
> telnet <adresse de la machine distante> [ <numéro de port> ] [ -l <nom de l'utilisateur> ]
```

Telnet demande alors une authentification de l'utilisateur par identificateur et mot de passe (l'utilisateur doit être déclaré sur la machine distante). Après authentification, les commandes qui sont saisies sont exécutées dans la machine distante. La commande logout permet de terminer la session sur la machine distante et de revenir à l'invite de commande locale.

TELNET, du fait de sa rusticité, peut également être utilisé pour tester l'activité de nombreux types de serveurs: en effet, avec un client TELNET, il est possible de dialoguer avec des serveurs comme SMTP, HTTP, POP ou IMAP.

**EXEMPLE:** interrogation d'un serveur HTTP APACHE avec TELNET:

La commande linux:

```
> telnet 182.168.1.12 80
```

donne la réponses suivante:

```
trying 192.168.1.12..  
connected to 192.168.1.12..  
escape character is '^]'
```

Cette réponse permet de s'assurer que le serveur HTTP 192.168.1.12 est bien actif.

On peut alors tenter d'envoyer une requête HTTP en la saisissant directement. Par exemple:

GET / HTTP/1.1 doit provoquer l'envoi par le serveur du code HTML de la page web par défaut du serveur.

### **II.2.3.2.RLOGIN:**

rlogin (Remote Login) est une commande Unix/Linux qui permet d'ouvrir une session à distance sur une autre machine de type Unix/Linux. Le protocole d'échange utilisé est TCP. Le port par défaut est 513. Comme TELNET, rlogin demande une authentification de l'utilisateur. Les échanges se font également sans cryptage.

### **II.2.3.3.SSH:**

#### **II.2.3.3.1.PRÉSENTATION:**

Le protocole SSH (en anglais Secure SHell), désigne à la fois des logiciels et un ensemble de protocoles permettant de se connecter sur une machine distante de façon sécurisée. Il repose sur les mécanisme d'authentification et de cryptage offerts par le protocole SSL/TSL.

#### **II.2.3.3.2.UTILISATION:**

Le protocole SSH (Securized Shell) est utilisé dans le cadre de l'administration système pour ouvrir des TERMINAUX SÉCURISÉS A DISTANCE sur les postes qu'ils doivent administrer. Ces terminaux permettent comme Rlogin et Telnet de lancer des commandes d'administration systèmes sur ces postes. Les avantages de SSH sur ces protocoles sont:

- Une procédure d'authentification renforcée;
- Un cryptage des données par une clef symétrique partagée au départ par un échange crypté en asymétrique.

### **II.2.3.4.PUTTY ET KITTY:**

Ce sont des logiciels munis d'une interface graphique qui supportent les fonctions de CLIENTS pour plusieurs protocoles de communication réseau (SSH, Telnet, rlogin, raw).

Ils gèrent également la connexion aux équipements par des liaisons séries RS232, ce qui les rend très utiles pour l'administration de certains routeurs.

Comme telnet, rlogin ou ssh, ils permettent d'ouvrir une "invite de commande" (un "shell") agissant sur l'hôte distant que l'on veut administrer. Ils peuvent être démarré immédiatement en cliquant sur une icône du bureau plutôt que d'utiliser une fenêtre système. De plus, l'interface graphique permet de paramétrer beaucoup plus finement la connexion:

- Choix du protocole (telnet, rlogin, ssh, raw, etc);
- Utilisation d'un "tunnel SSH";
- Nature de la liaison (réseau, RS232);
- Aspect de l'écran, utilisation des clefs du clavier;
- Enregistrement et nommage des sessions.
- Etc.

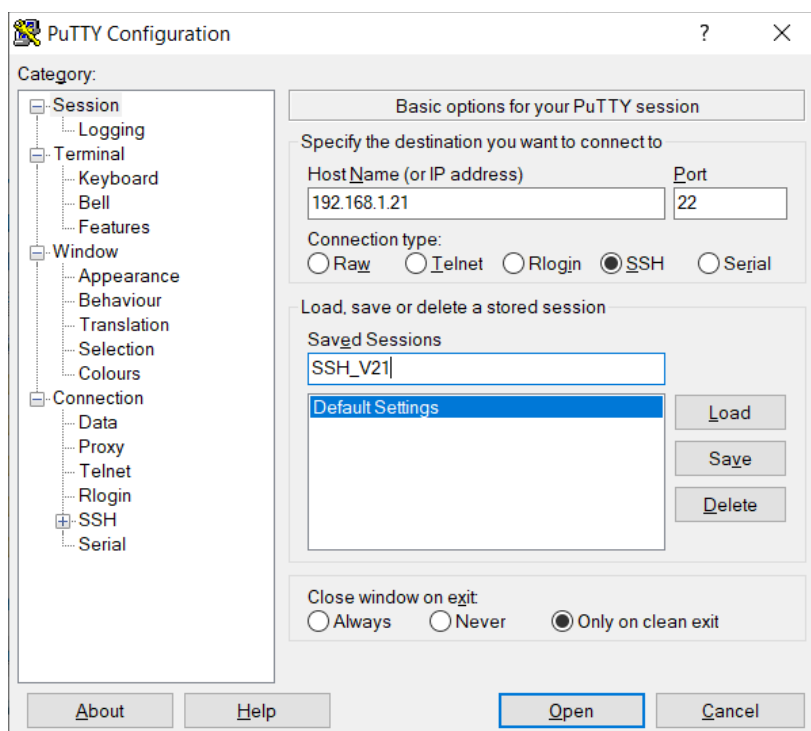
Le logiciel PUTTY peut être installé sous Windows et sur diverses plates-formes Unix (mais pas toutes). Le logiciel KITTY est une évolution de PUTTY.

**EXEMPLE:** ouverture avec PUTTY d'une invite de commande sur le poste distant 192.168.1.21 (hostname: ubuntu1):

La partie droite de l'écran permet de choisir le protocole de connexion, d'identifier le poste distant ( nom d'hôte ou adresse IP) et de donner un nom à la connexion.

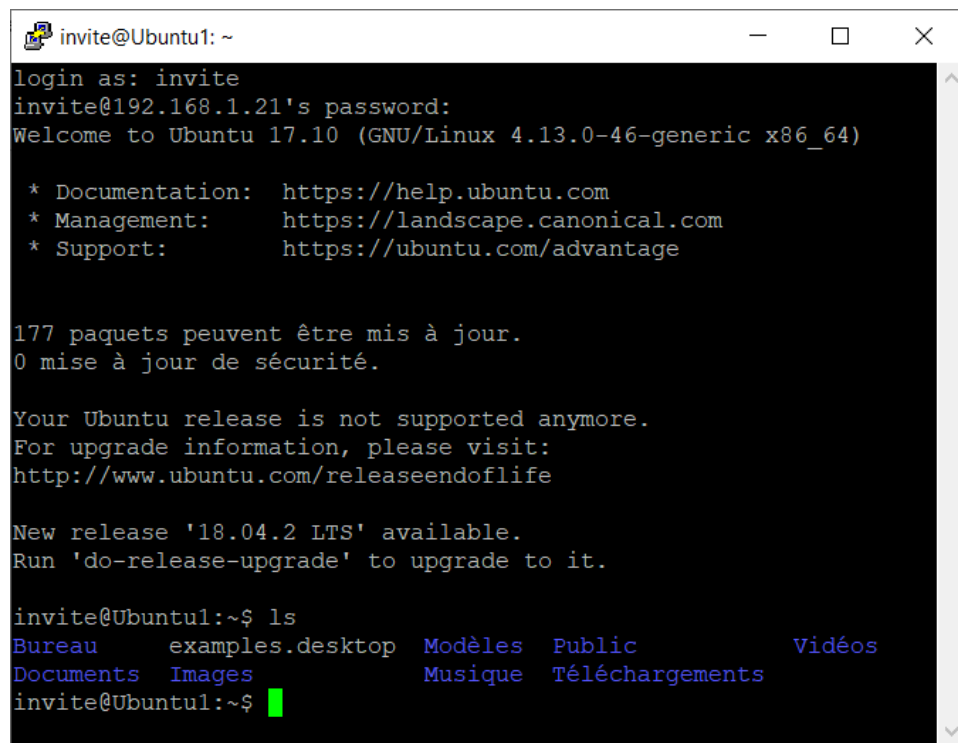
La partie gauche permet d'effectuer divers paramétrages concernant la session, le terminal à ouvrir, la fenêtre d'affichage, la connexion en elle-même.

En particulier, le sous-menu SSH permet d'agir sur les algorithmes, les clefs de cryptage et la tunnellation des échanges.



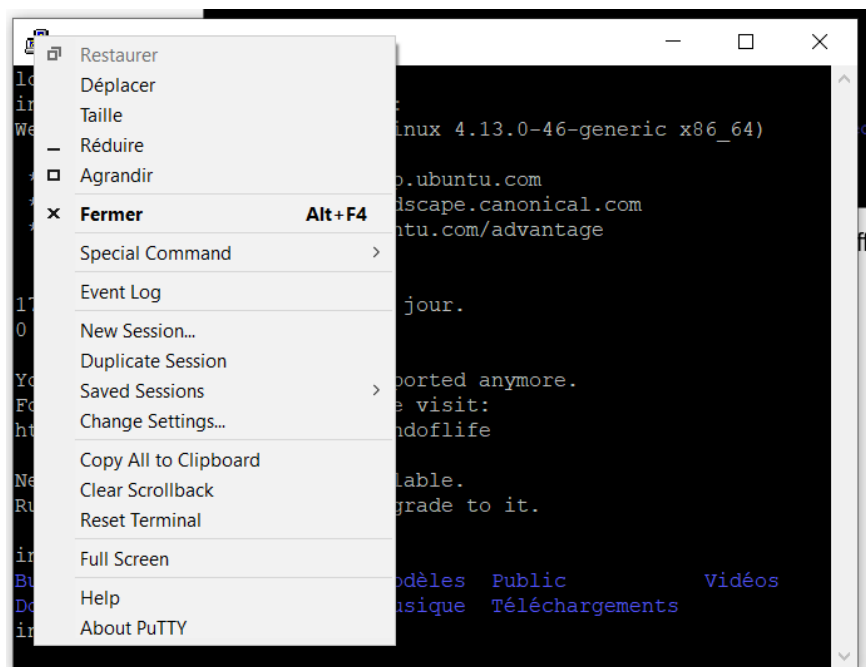
L'activation du bouton OPEN ferme cette fenêtre et ouvre l'invite de commande SSH agissant sur le poste distant ubuntu1 (192.168.1.12). Après authentification (ici, en tant qu'utilisateur "invite"), il est possible de saisir des commandes dans le langage de shell du poste distant (ici, il s'agit de commandes LINUX):



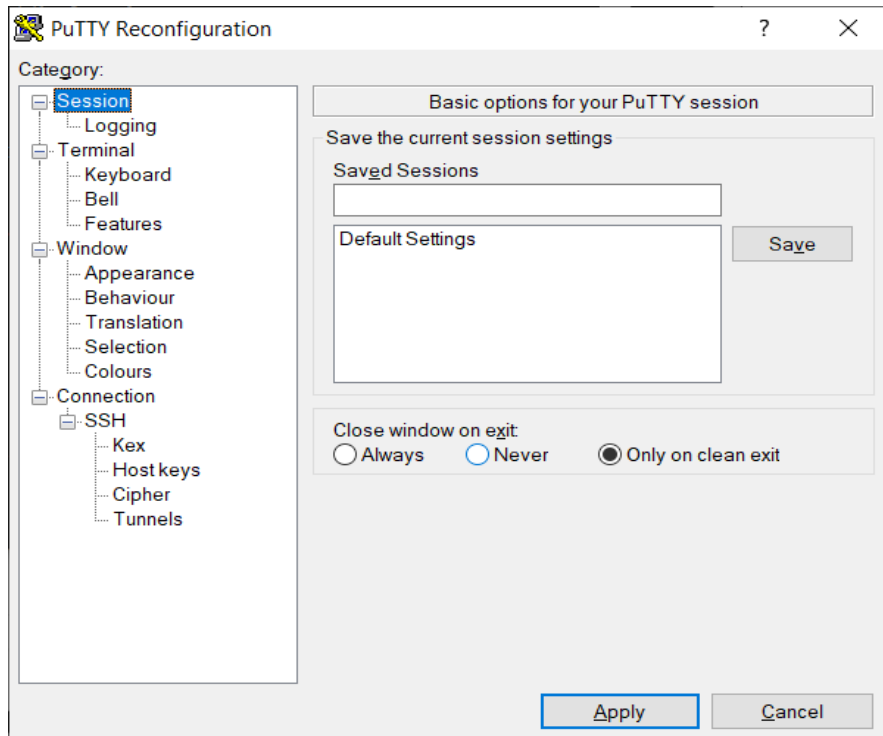


```
invite@Ubuntu1: ~  
login as: invite  
invite@192.168.1.21's password:  
Welcome to Ubuntu 17.10 (GNU/Linux 4.13.0-46-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/advantage  
  
177 paquets peuvent être mis à jour.  
0 mise à jour de sécurité.  
  
Your Ubuntu release is not supported anymore.  
For upgrade information, please visit:  
http://www.ubuntu.com/releaseendoflife  
  
New release '18.04.2 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
invite@Ubuntu1:~$ ls  
Bureau      exemples.desktop  Modèles  Public  Vidéos  
Documents  Images            Musique  Téléchargements  
invite@Ubuntu1:~$
```

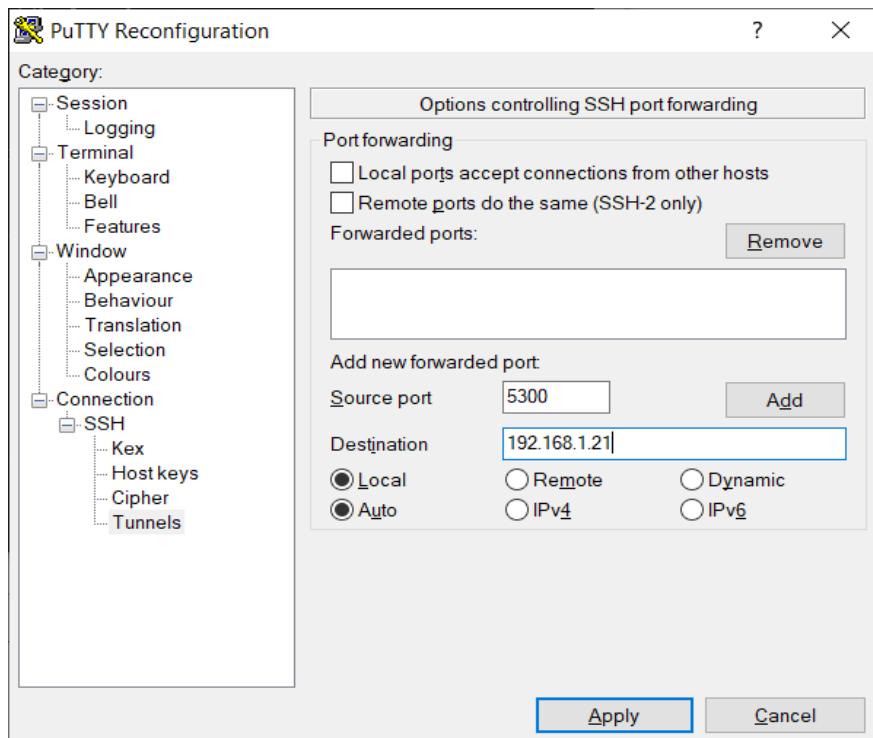
Un clic droit sur l'icône en haut et à gauche de cette fenêtre permet d'afficher diverses options de paramétrage :



En particulier, l'option "Change settings" permet de ré-afficher le menu initial pour reprendre le paramétrage, créer un tunnel SSH, etc.



**EXEMPLE:** Menu de création d'un tunnel SSH par la redirection du port 5300 de 192.168.1.21 vers le port 80 de la machine locale (faire Add pour valider la création).



## **II.2.4.LES LOGICIEL DE PRISE DE CONTRÔLE A DISTANCE:**

### **II.2.4.1.DÉFINITION:**

En informatique, la PRISE DE CONTRÔLE A DISTANCE d'un ordinateur est une méthode qui consiste à prendre le contrôle de l'IHM d'un ordinateur A depuis un ordinateur distant B de telle manière que l'on puisse effectuer les mêmes opérations que si l'on travaillait directement avec l'IHM local de l'ordinateur A (clavier, souris, écran).

Ceci implique:

- Que l'écran d'affichage de l'ordinateur contrôlé s'affiche dans une fenêtre de l'ordinateur distant;
- Que le curseur graphique sur l'écran de l'ordinateur contrôlé puisse être manipulé avec l'organe de pointage de l'ordinateur distant (déplacements, boutons de clics, boutons de défilement, etc.) ;
- Que les saisies sur le clavier de l'ordinateur distant soient transmises à l'ordinateur contrôlé et traitées par celui-ci comme si elles provenaient de son clavier local.

**REMARQUE:** en général, les logiciels de contrôle à distance supportent d'autres fonctionnalités comme le transfert de fichiers entre les deux postes ou le support de téléconférences .

### **II.2.4.2.UTILISATION:**

#### **II.2.4.2.1.PRINCIPAUX CAS D'UTILISATION:**

- Le CONTRÔLE A DISTANCE est utilisé essentiellement pour le DÉPANNAGE et l'ADMINISTRATION des postes de travail ou des serveurs. Dans ce cadre, Il permet de limiter les déplacements des personnels aux seuls cas où leur présence physique est indispensable (interventions sur le matériel, par exemple). Il permet également de raccourcir les délais d'intervention (pas de délais d'intervention dû au déplacement) ;
- Grâce au contrôle à distance, l'administrateur ou le technicien de maintenance peuvent, pour investiguer ou intervenir sur le paramétrage du système d'exploitation, utiliser les outils et menus graphiques du système d'exploitation de l'ordinateur contrôlé, ce qui très souvent permet d'améliorer la rapidité d'intervention et demande moins de "technicité" que l'utilisation de commandes en ligne ;
- Le contrôle à distance peut également permettre à un agent en déplacement de prendre la main à distance sur son ordinateur personnel (à condition que celui-ci reste accessible sur le web);

- Le contrôle à distance est également utilisé dans un BUT PÉDAGOGIQUE (enseignement à distance): l'apprenant peut, par ce moyen, "vivre en direct" sur son propre écran la manipulation que lui montre son tuteur comme si celui-ci était à côté de lui.

#### **II.2.4.2.2.CONDITIONS D'UTILISATION:**

- Le débit entre les deux postes doit être suffisant pour assurer un bon rafraîchissement de la fenêtre ouverte sur le poste de travail distant;
- Les deux postes de travail doivent être équipés des logiciels adéquats;
- La prise de contrôle à distance suppose toujours une phase d'authentification réciproque des deux machines. En général :
  - Le poste de travail distant fait une demande de connexion au poste à contrôler (en lui envoyant des informations d'authentification);
  - Le poste à contrôler examine ces informations et autorise ou non la connexion.

#### **II.2.4.3.BUREAU A DISTANCE DE WINDOWS:**

##### **II.2.4.3.1.PRÉSENTATION:**

Ce logiciel propriétaire de MicroSoft permet à un poste de travail muni du système d'exploitation WINDOWS de prendre le contrôle à distance sur un autre ordinateur muni d'une version PROFESSIONNELLE d'un système d'exploitation WINDOWS.

En effet, ce mécanisme suppose que le système à contrôler abrite un SERVEUR de contrôle à distance, tandis que le système contrôleur doit abriter un CLIENT de cette application. Or, si tous les systèmes windows sont équipé du CLIENT, les SERVEURS ne sont présents que sur les versions professionnelle.

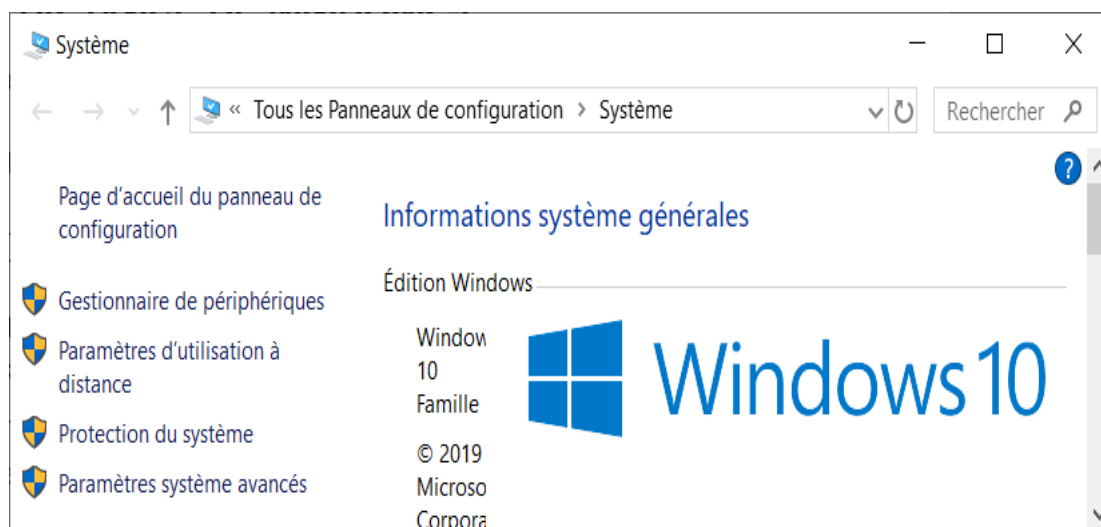
**EXEMPLE:** depuis un système windows en version "famille", il est possible de prendre le contrôle d'un système windows en version professionnelle. L'inverse n'est pas vrai.

Les deux paragraphes suivants décrivent les manipulations nécessaires.

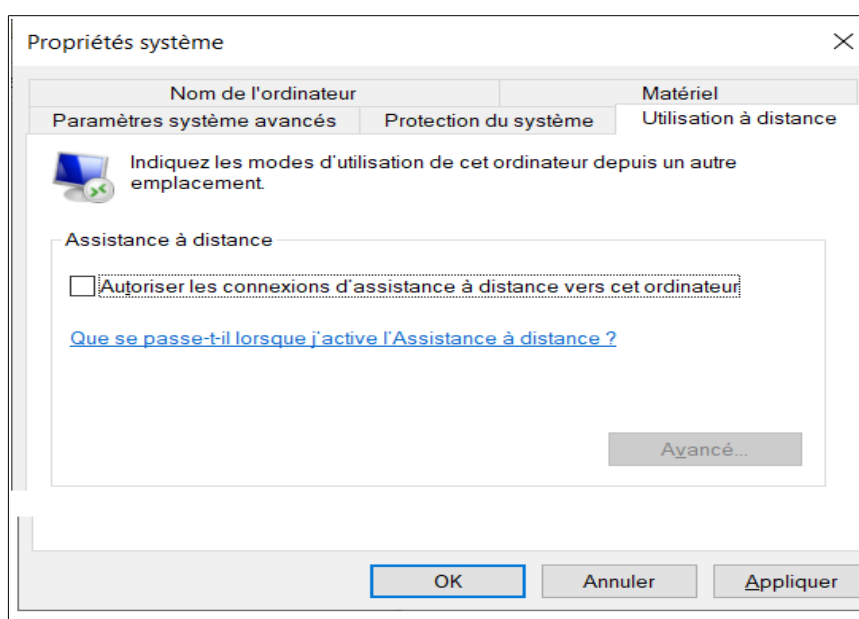
##### **II.2.4.3.2.AUTORISER LA CONNEXION SUR LE POSTE A CONTRÔLER:**

**RAPPEL:** Cette opération ne peut être effectuée que sur un ordinateur muni d'une version professionnelle de windows.

Sous WINDOWS 10 : sur le poste à contrôler, activer les touches clavier [windows]+ [Pause]. La fenêtre suivante s'affiche:



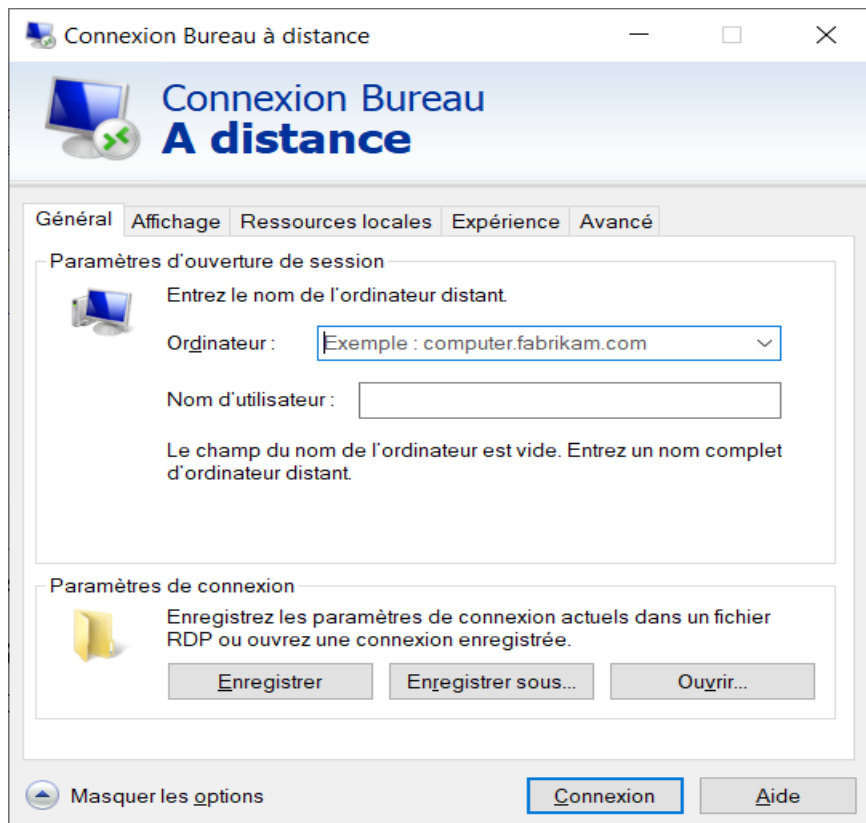
Activer alors "Paramètres d'utilisation à distance". La fenêtre suivante s'ouvre:



Cette fenêtre permet d'autoriser les postes distant à se connecter au poste local en cliquant sur le bouton "Autoriser les connexions à distance ...".

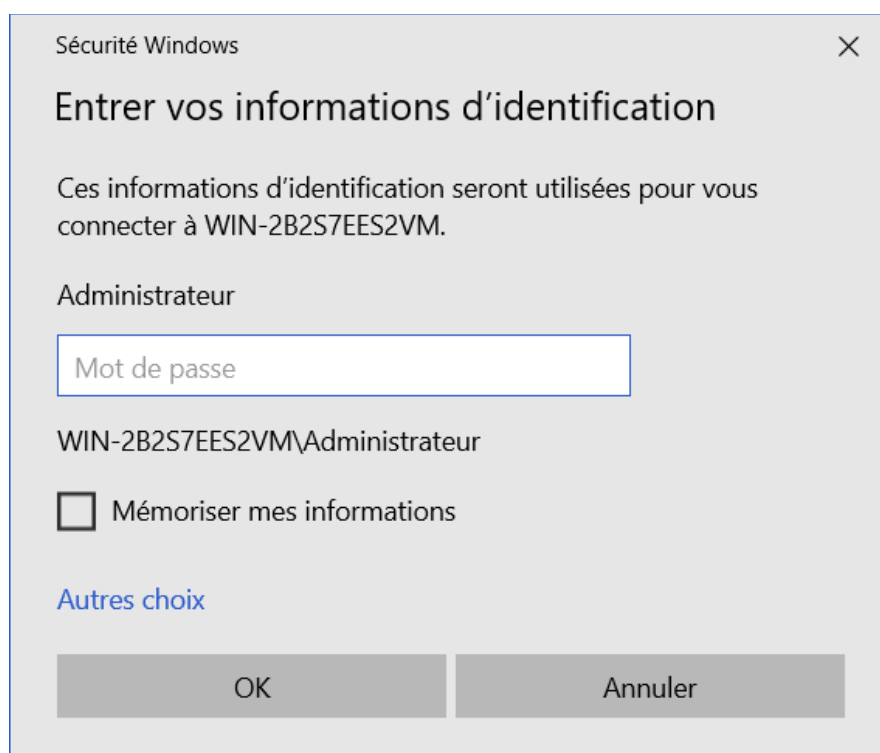
### **II.2.4.3.3.PRENDRE LE CONTRÔLE A DISTANCE D'UN POSTE WINDOWS:**

Sous Windows 10: Rechercher "Connexion Bureau à distance". Le menu suivant s'affiche:



**NOTA:** pour utiliser ce menu, il faut décocher "Masquer les options", si nécessaire.

Saisir alors le nom de l'ordinateur (par exemple, WIN-2B2S7EES2VM) et le nom d'utilisateur (par exemple: "Administrateur"), puis activer "Connexion". Le menu de connexion suivant s'affiche:



Saisir alors le mot de passe de l'utilisateur du système distant et valider (ok). La fenêtre de contrôle s'affiche alors sur l'écran: elle visualise le bureau de l'ordinateur contrôlé. Lorsque le curseur de la souris se trouve dans cette fenêtre, les informations en provenance du clavier et de la souris de l'ordinateur local sont envoyées à l'ordinateur contrôlé et traitées comme si elle provenaient de son clavier ou de sa souris.

## II.2.4.4. TEAMVIEWER

### II.2.4.4.1. PRÉSENTATION:

TeamViewer permet de contrôler un PC à distance via internet. C'est un logiciel propriétaire payant (environ 500 euros), mais qui est distribué gratuitement si l'acquéreur s'engage à l'utiliser dans un but non commercial.

**Attention, cette condition est effectivement contrôlée par la société éditrice car l'utilisation de TeamViewer nécessite la connexion à un de ses serveurs: en cas d'utilisation "illicite", l'éditeur peut vous interdire l'utilisation, à moins d'acheter la licence.**

Le principal avantage de TeamViewer est qu'il ne nécessite pas d'installer un serveur sur les postes: de ce fait, il peut fonctionner derrière un NAT sans redirection de port.

**REMARQUE :** TeamViewer offre aux utilisateurs trois fonctionnalités principales:

- Prise de contrôle à distance d'un ordinateur connecté au web ("bureau" à distance);
- Transfert de fichiers entre deux ordinateurs connectés au web;
- Support pour des téléconférences.

### II.2.4.4.2. PRINCIPE DE FONCTIONNEMENT:

La transaction entre les postes participants s'effectue par l'intermédiaire un SERVEUR de la société éditrice. Ce serveur assure:

- L'identification des postes connectés par un identificateur UNIQUE sur le web, associé à un mot de passe ( TeamViewer ID ).;
- Le transfert des données entre les postes connectés.

Au lancement de TeamViewer sur un ordinateur client, le logiciel se connecte au serveur TeamViewer, qui attribut à l'ordinateur concerné sa "TeamViewer ID" unique. Les connexions sont de type TCP:

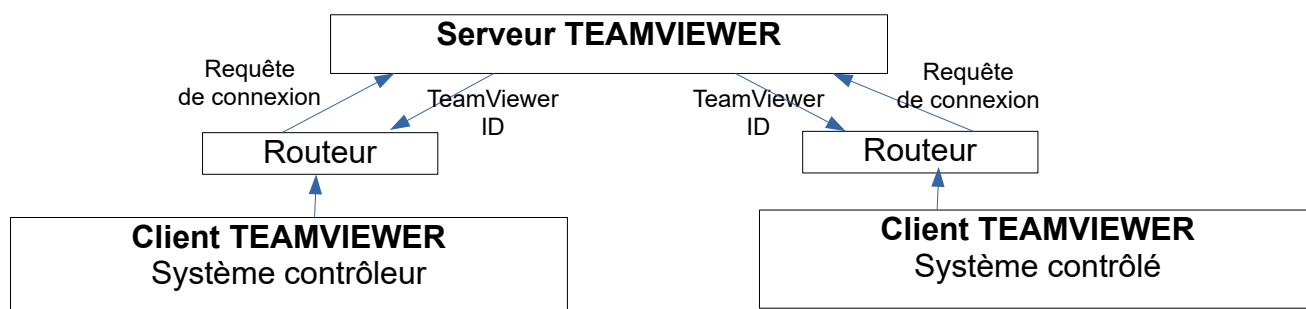


Figure II.2 .4.4.2: Architecture de communication Teamviewer

De ce fait, Teamviewer n'a pas besoin de faire une redirection de port pour atteindre des adresses au-delà du routeur, car on n'utilise que des connexions TCP sortantes. Cette technique s'appelle: **reverse connexion**. En général, la connexion TCP se fait sur le port



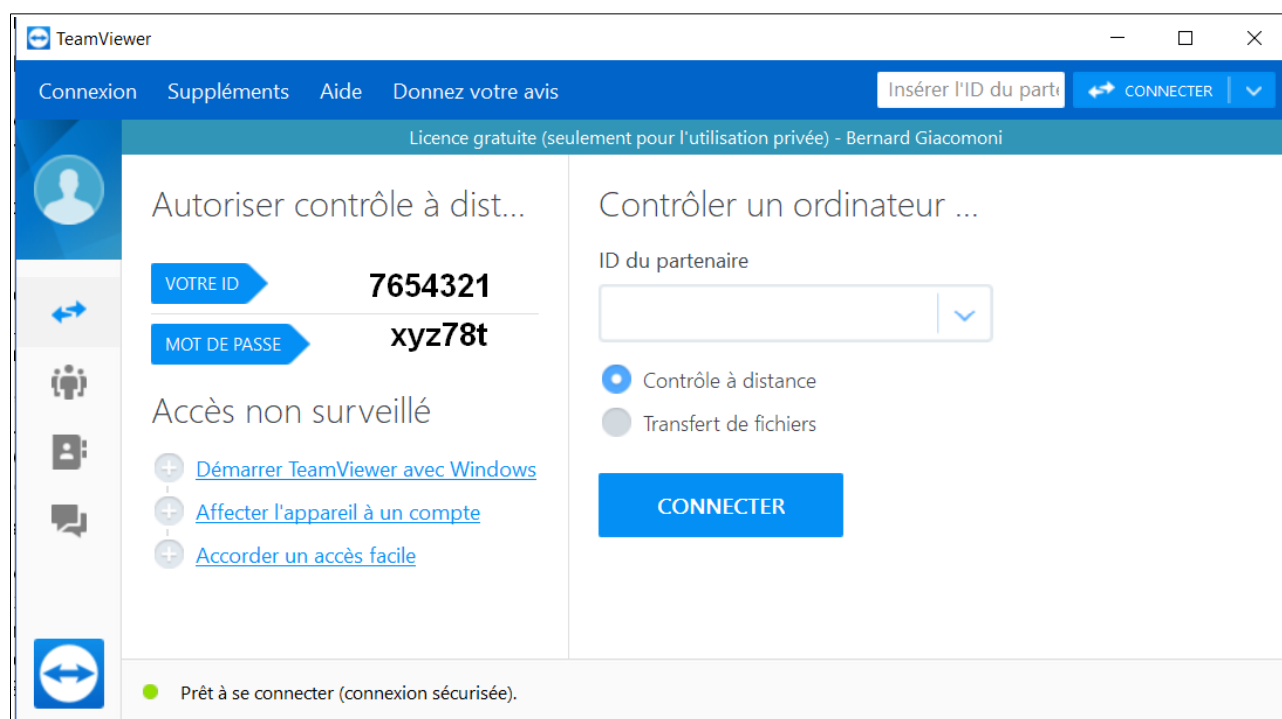
80 (utilisé par les serveurs web) car ce port, utilisé par le web, n'est jamais bloqué par les pare-feux.

### **II.2.4.4.3.SÉCURITÉ:**

TeamViewer utilise pour les transmissions de données un cryptage par clé symétrique de 256 bits; L'échange de cette clef est crypté par une paire de clés asymétrique RSA de 2048 bits. La sécurité est donc comparable à celle d'une transmission SSH.

### **II.2.4.4.4.UTILISATION POUR LE CONTRÔLE A DISTANCE:**

Au lancement de TeamViewer, quelle que soit l'utilisation que l'on veut en faire (contrôleur ou contrôlé), la fenêtre suivante s'affiche sur l'écran:



### **COMMENTAIRES:**

- Le champ qui apparaît à droite du label «VOTRE ID» est la «TeamViewer ID» attribuée à la machine par le serveur TeamViewer.
- A droite du label «MOT DE PASSE» apparaît le mot de passe correspondant à cette ID.
- Le champ situé en dessous du label "ID du partenaire" vous permet de saisir l'ID de la machine que vous voulez contrôler.

Pour prendre le contrôle d'un ordinateur à distance, il suffit donc:

- De lancer teamViewer sur votre machine en sélectionnant «Contrôle à distance» dans l'IHM;

- De demander au responsable de l'ordinateur à contrôler de lancer TeamViewer sur cet ordinateur (si ce n'est pas déjà fait), puis de vous communiquer l'ID de cet ordinateur (par téléphone, par mail, oralement, etc.);
- De saisir cette ID dans le champ labellisé «ID du partenaire» et d'activer le bouton de connexion.

Le TeamViewer du PC contrôleur demande alors au serveur Teamviewer de l'autoriser à prendre le contrôle de la machine correspondant à l'ID saisie dans le champ "ID du partenaire". Comme le logiciel TeamViewer est aussi lancé sur la machine à contrôler, celle-ci est également connectée au serveur Teamviewer. Le serveur peut alors faire transiter les données et commandes entre les deux machines par son intermédiaire. Ces deux machines ne communiquant physiquement qu'avec le serveur, il n'est nul besoin de faire une redirection de port.

## II.2.4.5.LE LOGICIEL VCN:

### II.2.4.5.1.PRÉSENTATION:

Comme TeamViewer, VCN est un logiciel dont la principale fonction est la prise de contrôle à distance d'un poste informatique. En revanche, VCN est un logiciel GRATUIT et OPEN SOURCE.

Tout comme Teamviewer, VCN est principalement utilisé pour la télémaintenance et la téléadministration des systèmes informatiques ainsi que pour la téléformation. il fonctionne sur les plateformes Windows, Mac et Linux.

### II.2.4.5.2.FONCTIONNEMENT:

Le VNC "de base" est composé de 2 applications communicant entre elles:

- Le SERVEUR VNC, exécuté sur la machine contrôlée à distance (le port VNC par défaut est 5900);
- Le CLIENT VNC (ou VIEWER), qui tourne sur la machine contrôleur à distance. Le viewer affiche la fenêtre de contrôle sur l'ordinateur distant et gère le clavier, la souris et le presse-papier.

Il supporte deux modes de fonctionnement:

**Dans le premier mode ("mode normal")**, le CLIENT se connecte au SERVEUR. De ce fait, le port utilisé par VNC doit être redirigé vers la machine commandée, pour qu'on puisse s'y connecter depuis internet. Ceci implique d'avoir accès à la configuration du routeur.

**Dans le second mode de fonctionnement (mode "listening viewer")**, la connexion s'établit en sens inverse: c'est le SERVEUR qui sollicite le client. Le CLIENT attend donc les sollicitations du serveur ("Listening Viewer"). De ce fait, ce mode permet de contrôler un ordinateur derrière un NAT ou un firewall même si on ne peut pas créer de redirection de port (par exemple, si on n'a pas accès à la configuration du routeur).

Le second mode correspond au logiciel Ultra VNC dont nous allons aborder l'utilisation :

### II.2.4.5.3.UTILISATION EN MODE LISTENING VIEWER (ULTRA VNC):

#### **INTRODUCTION:**

UltraVNC est une évolution du logiciel libre VNC suivant les principes de l'OPEN SOURCE. Il en exploite l'option LISTENING VIEWER. De ce fait, aucune redirection de port n'est nécessaire.

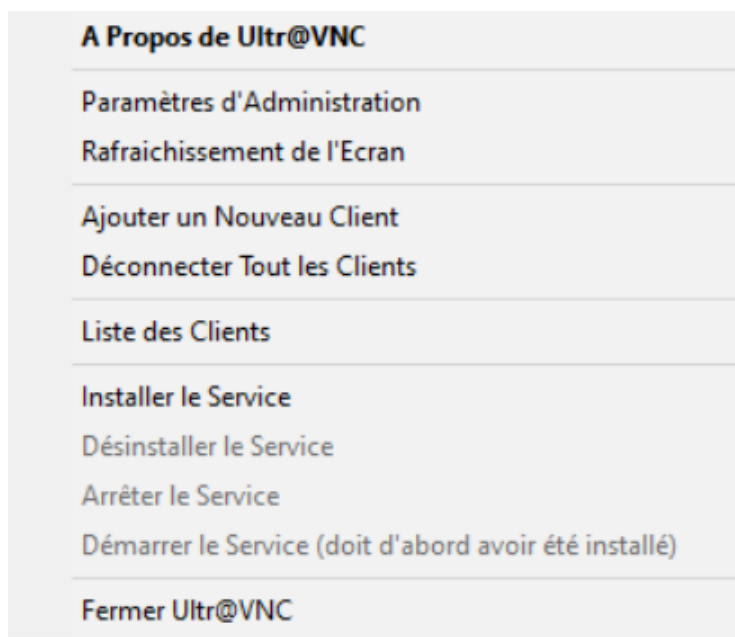
Le logiciel UltraVNC se compose d'un SERVEUR, installé sur le système à contrôler et d'un CLIENT qui permet de se connecter au serveur et d'afficher le bureau du système contrôlé dans une fenêtre.

#### **LANCEMENT DU SERVEUR SUR LA MACHINE A CONTRÔLER:**

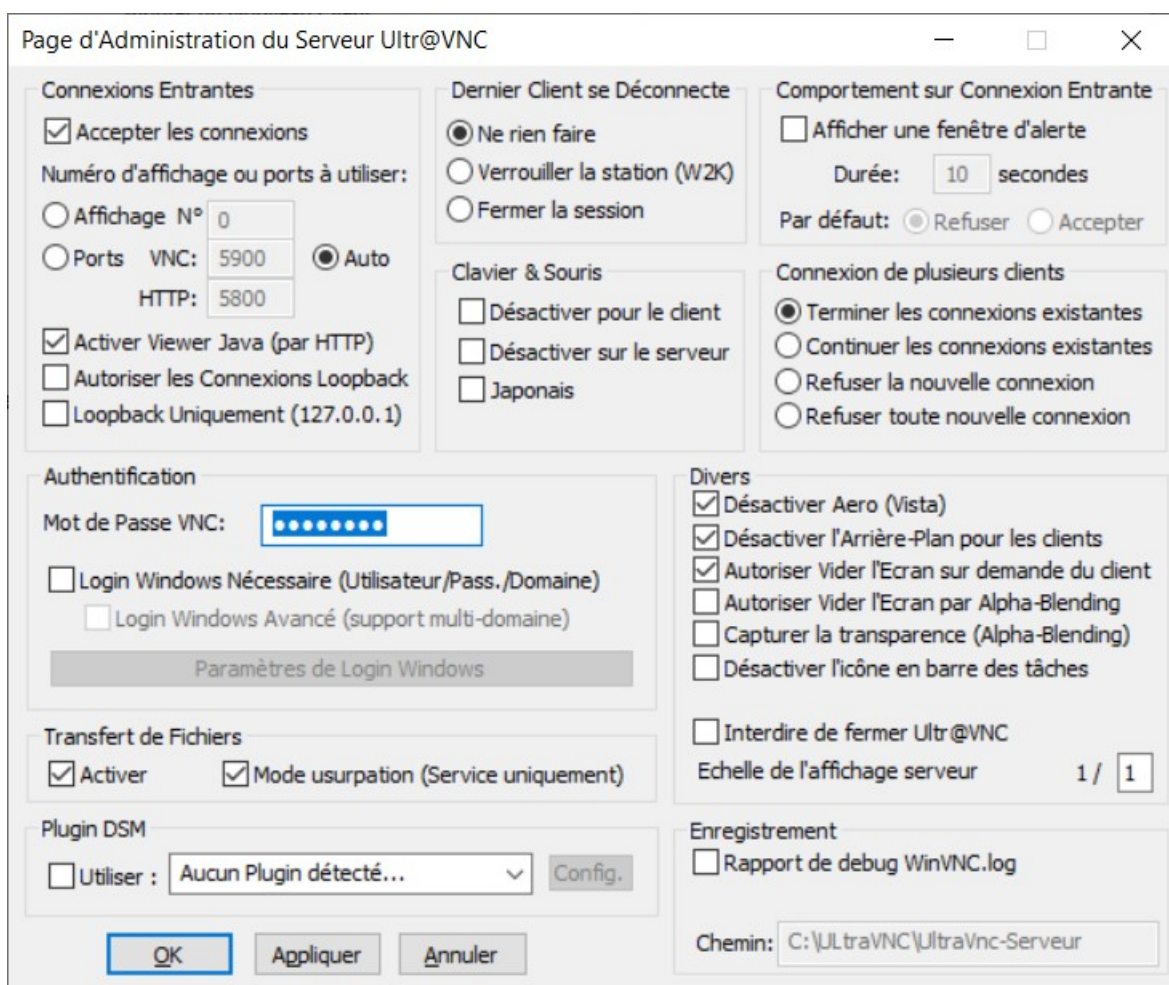
Sous WINDOWS: L'activation du lien d'exécution du logiciel VNC Server déclenche l'apparition dans la barre des tâches de l'icône:



Un clic droit sur cette icône permet d'afficher le menu contextuel suivant:



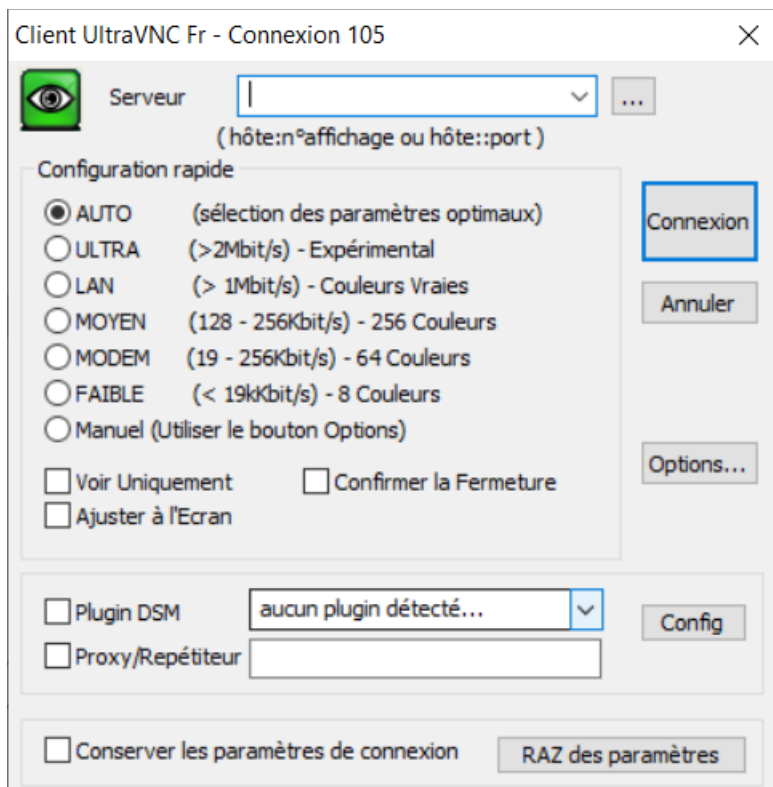
L'activation de "Paramètres d'administration" ouvre un menu de configuration du serveur:



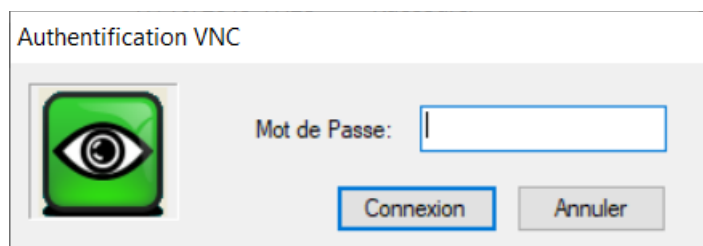
Ce menu d'administration permet en particulier de définir un "Mot de passe VNC" qui permettra aux clients (systèmes désirant contrôler l'ordinateur local) de se connecter.

**LANCEMENT DU CLIENT SUR LA MACHINE DU CONTRÔLEUR:**

Sous WINDOWS: L'activation du lien d'exécution du logiciel VNC Client déclenche l'ouverture du menu suivant:



Saisir alors le nom d'hôte ou l'adresse IP de la machine à contrôler (éventuellement accompagné du numéro de port, si le port par défaut n'est pas utilisé). L'activation de "Connexion" entraînera l'affichage d'un menu de connexion au serveur:



La saisie du mot de passe SERVEUR et l'activation de "Connexion" entraîne la connexion au serveur et l'affichage du bureau de la machine distante dans une fenêtre de l'écran local.

## II.3.ADMINISTRATION DES ROUTEURS:

### II.3.1.1.RAPPELS:

La plupart des routeurs intégrés dans un réseau se présentent comme des boîtiers "fermés" (non munis d'un IHM local). Ces boîtiers sont équipés:

- D'une carte mère supportant un microprocesseur, des mémoires ROM et RAM et les équipements matériels nécessaires au traitement d'au moins deux interfaces réseaux (sinon, on ne peut pas router);
- D'un certain nombre de "ports de connexion" de différentes technologies (ethernet RJ45, ethernet BNC (câble coaxial), spot de connexion wifi, liaisons séries point à point, etc ;
- D'un système d'alimentation sécurisé.

Un routeur se présente donc comme un "ordinateur minimal" spécialisé du point de vue du matériel et du logiciel dans la transmission d'informations entre des réseaux dont les technologie de liaison et de routage peuvent être différentes. La fonction de routage minimale suppose que le routeur sont équipé au moins des couches liaisons et routage de l'ISO (les couches ethernet et IP pour TCP/IP). En fait, certaines fonctionnalités d'un routeur moderne (PAT, port forwarding, etc.) exigent une couche TRANSPORT (TCP pour TCP/IP).

### REMARQUES:

- Le système d'exploitation d'un routeur est souvent spécifique de son constructeur, mais il peut aussi s'agir d'une version "allégée" de Linux;
- N'importe quel ordinateur doté d'un système d'exploitation unix/linus ou windows et d'au moins deux interfaces réseaux "physiques" peut être configuré en routeur: les systèmes Linux intègrent "de base" une fonction de routage minimale, sinon des logiciels de routage plus sophistiqués peuvent être implémentés. Un ordinateur généraliste supportant le routage est souvent appelé "PASSERELLE".

### II.3.1.2.CONNEXION AU SYSTÈME DE PARAMÉTRAGE D'UN ROUTEUR:

Les routeurs ne possédant pas d'IHM local, le seul moyen d'accéder à leur logiciel d'administration est d'utiliser un poste de travail déporté et de se connecter à distance. Les procédures de connexion varient suivant le type du routeur:

- Les routeurs destinés au grand public (comme les BOX des différents F.A.I) sont en général équipés d'un serveur HTTP qui permet à un poste d'administration déporté d'accéder à un certain nombre de menus de configuration (pages web). Ces menus permettent de configurer et paramétrer la fonction de routage proprement dite, mais aussi les autres fonctions habituellement supportées par les routeurs modernes: NAT/PAT, DHCP, Port Forwarding, constitution de VLANs, etc;

- Les routeurs destinés à des environnements plus professionnels sont souvent (au moins pour leur configuration initiale), accessibles uniquement par une liaison série, ce qui exige de connecter physiquement au routeur, par un CÂBLE SÉRIE, un ordinateur muni d'un CLIENT SPÉCIFIQUE. Une fois la connexion établie, il est parfois possible (si le système d'exploitation du serveur est un LINUX) d'ouvrir une FENÊTRE TERMINAL et de configurer le routeur en ligne. Si le système d'exploitation est spécifique (cas des routeurs SISCO, par exemple), la configuration se fait grâce à un langage de commande spécifique;
- Une fois cette configuration initiale effectuée grâce à une liaison série, il est parfois possible de lancer sur le routeur un service SSH qui permettra d'effectuer la configuration depuis un poste réseau muni d'un client SSH (avec PUTTY, par exemple).

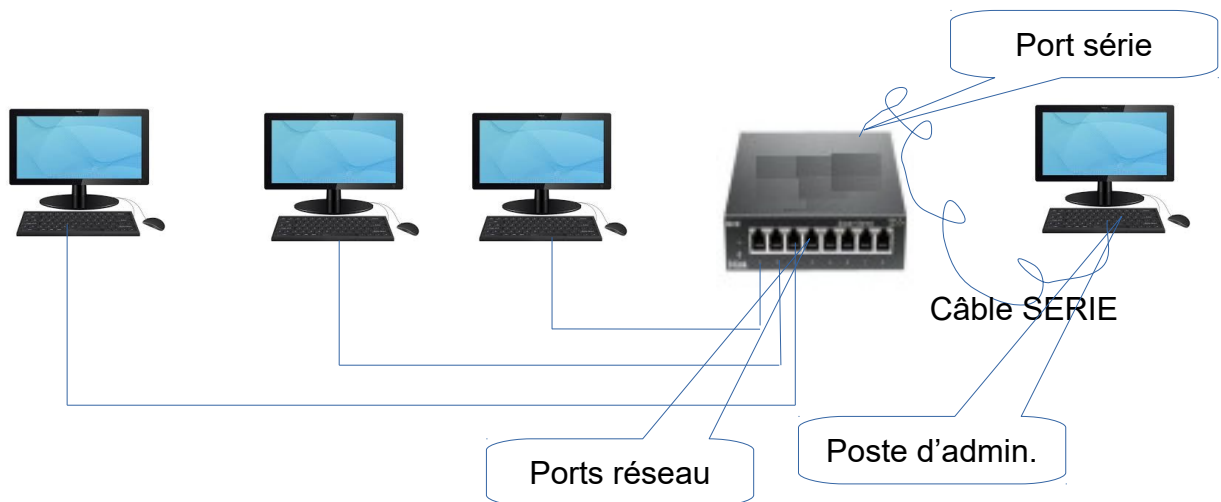


Figure II.3.1.2 : Administration d'un routeur par câble série



## **II.4.INSPECTION DES FLUX DE DONNÉES – LOGICIEL WIRESHARK:**

### **II.4.1.PRÉSENTATION:**

WIRESHARK est un logiciel qui permet d'analyser les PAQUETS de données circulant sur un réseau TCP/IP et de visualiser leur contenu. C'est un logiciel libre et gratuit. Ses fonctionnalités principales sont:

- La CAPTURE DE PAQUETS circulant dans le réseau auquel le système supportant WireSharh est connecté:
  - Le mode "promiscuous" activé autorise la capture de tous les paquets;
  - Le mode "promiscuous" désactivé n'autorise que la capture des paquets adressés à ce système ou émis par lui.
  - D'autre part, les paquets à capturer peuvent être sélectionnés à l'aide de FILTRES définissables par les utilisateurs;
- L'AFFICHAGE EN TEMPS RÉEL ou en temps différé des paquets capturés;
- L'ENREGISTREMENT des paquets capturés dans des fichiers pour les exploiter en temps différé.
- L'INSPECTION DES PAQUETS capturés au niveau de leur contenu binaire (informations utiles et couches de protocoles).

### **II.4.2.UTILISATION:**

#### **II.4.2.1.AVERTISSEMENTS:**

- WireShark est un outil extrêmement puissant, offrant des dizaines de fonctionnalités différentes. Il n'est pas question ici d'écrire un manuel d'utilisation. On se contentera de présenter quelques manipulations de base;
- De par ses fonctionnalités, Wireshark peut être utilisé pour des activités de "hacking" (capture d'identifiants de connexion, espionnage de contenus, etc.). Pour cette raison, l'installation et l'utilisation de Wireshark dans un réseau professionnel est la plupart du temps soumise à autorisation.

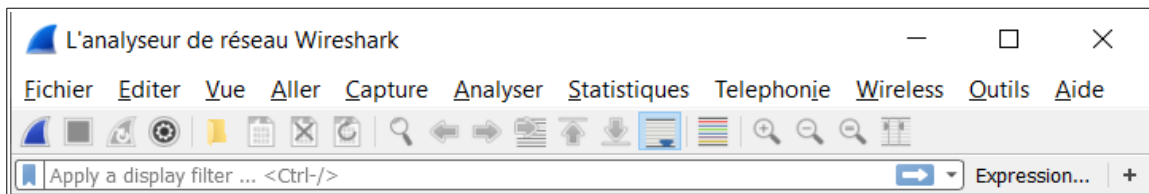
#### **II.4.2.2.DESCRPTION DE LA PAGE D'ACCUEIL:**

Au lancement du logiciel WireShark, un menu d'accueil s'affiche. Ce menu est constitué:

**A-D'une partie supérieure commune à tous les menus et comprenant:**

- Le nom du logiciel (analyseur réseau Wireshark)
- Une barre de menus donnant accès à divers sous-menus (Fichier, Éditer, Vue, Aller, paramétrer et commander une capture, etc);
- Une barre d'outils permettant de démarrer et d'arrêter une capture de paquets, de définir les options de captures (filtres, etc.) et de faire diverses opérations sur les données capturées ;

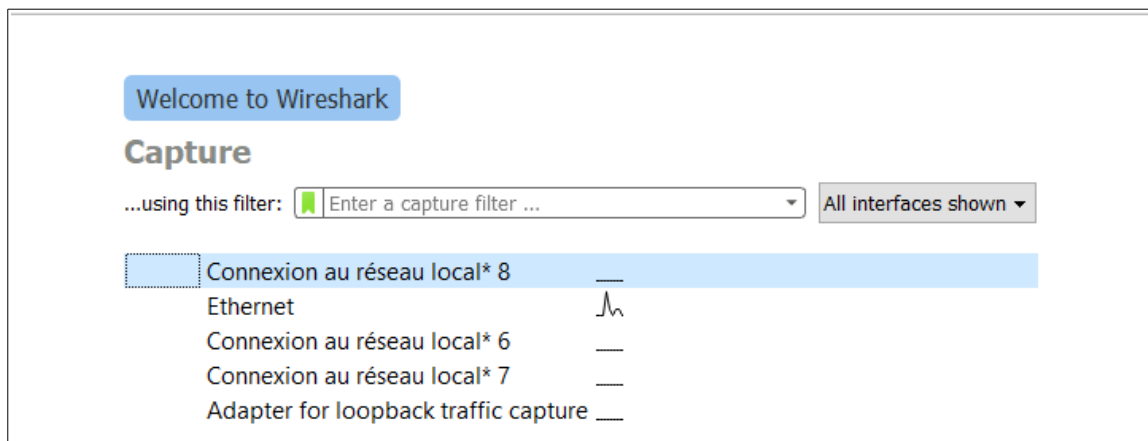
- Un champ permettant de définir des "expressions de filtrage" permettant de sélectionner les paquets lors de l'analyse d'une capture **en temps différé**:



**B-D'une partie centrale permettant d'initialiser une capture:**

Sous le label Capture nous trouvons:

- Le champ de définition d'un filtre de capture ("...using this filter:"). Celui-ci permet de définir un filtre applicable aux paquets à capturer ou d'en choisir un existant: les paquets peuvent être sélectionnés en fonction de leurs adresses IP, de leurs ports d'origine ou de destination, du protocole utilisé (tcp, udp, icmp, etc.), de leur mode (unicast, multicast, etc.). Un filtre est une expression littérale exprimant une condition logique de capture (ex: "tcp.port == 5000 and ip.addr=192.168.1.1" sélectionne les paquets adressés au port 5000 et à l'adresse IP V4) ;
- Une liste de choix possibles pour la connexion réseau à traiter (en cliquant sur la liste des connexions).



**REMARQUE:** Ces différentes actions peuvent également être effectuées à l'aide des menus de la première partie de la page.

**C-D'une partie pied de page qui est surtout informative:**

**Learn**

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

You are running Wireshark 3.0.5 (v3.0.5-0-g752a55954770). You receive automatic updates.

---

Prêt pour charger ou capturer || 
 Pas de paquets || 
 Profile: Default

**II.4.2.3.DÉMARRAGE D'UNE CAPTURE DE PAQUETS A PARTIR DE L'ACCUEIL:**

Il suffit pour cela, après avoir choisi ou saisi éventuellement le filtre à utiliser (champ en dessous du label "Capture"), de double-cliquer sur la connexion que l'on veut surveiller (un des élément de la liste des connexions : par exemple "Ethernet"). La partie centrale de la page est alors remplacée par trois zones: la première visualise les paquets capturés, ligne après ligne. La seconde affiche le contenu des couches de protocole. La troisième affiche le contenu du paquet (en hexadécimal ou en binaire). Chaque ligne de la première partie affiche un numéro de paquet, la date de réception, l'IP source, l'IP destination, le protocole, la longueur en octets et les ports émetteur et destinataires.

**EXEMPLE:** Capture des paquets adressés au port 80 (Filtre "port 80"):

No.	Time	Source	Destination	Protocol	Length	Info
16	0.023730	93.184.220.29	192.168.1.12	OCSP	841	Response
17	0.029066	93.184.220.29	192.168.1.12	TCP	60	80 → 54166 [ACK]...
18	0.029294	93.184.220.29	192.168.1.12	OCSP	841	Response
19	0.061776	192.168.1.12	93.184.220.29	TCP	54	54164 → 80 [ACK]...
20	0.066588	192.168.1.12	93.184.220.29	TCP	54	54165 → 80 [ACK]...
21	0.069160	192.168.1.12	93.184.220.29	TCP	54	54166 → 80 [ACK]...

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 52

0010	00 34 9c a7 40 00 80 06 00 00 c0 a8 01 0c 5d b8	.4..@... ..]
0020	dc 1d d3 94 00 50 b3 3b 62 a7 00 00 00 00 80 02	....P.; b.....
0030	fa f0 fb b0 00 00 02 04 05 b4 01 03 03 08 01 01	.....
0040	04 02	..

Identification (ip.id), 2 bytes || Paquets: 21 · Affichés: 21 (100.0%) || Profile: Default

**REMARQUE :** un clic droit sur la troisième zone permet de passer de l'affichage en hexadécimal à l'affichage en binaire et inversement.

Pour arrêter la capture, il suffit de cliquer sur le bouton rouge dans la barre des tâches.

Pour revenir à la page d'accueil, faire: Fichier → Close.

#### II.4.2.4. REDÉMARRAGE D'UNE CAPTURE DE PAQUETS:

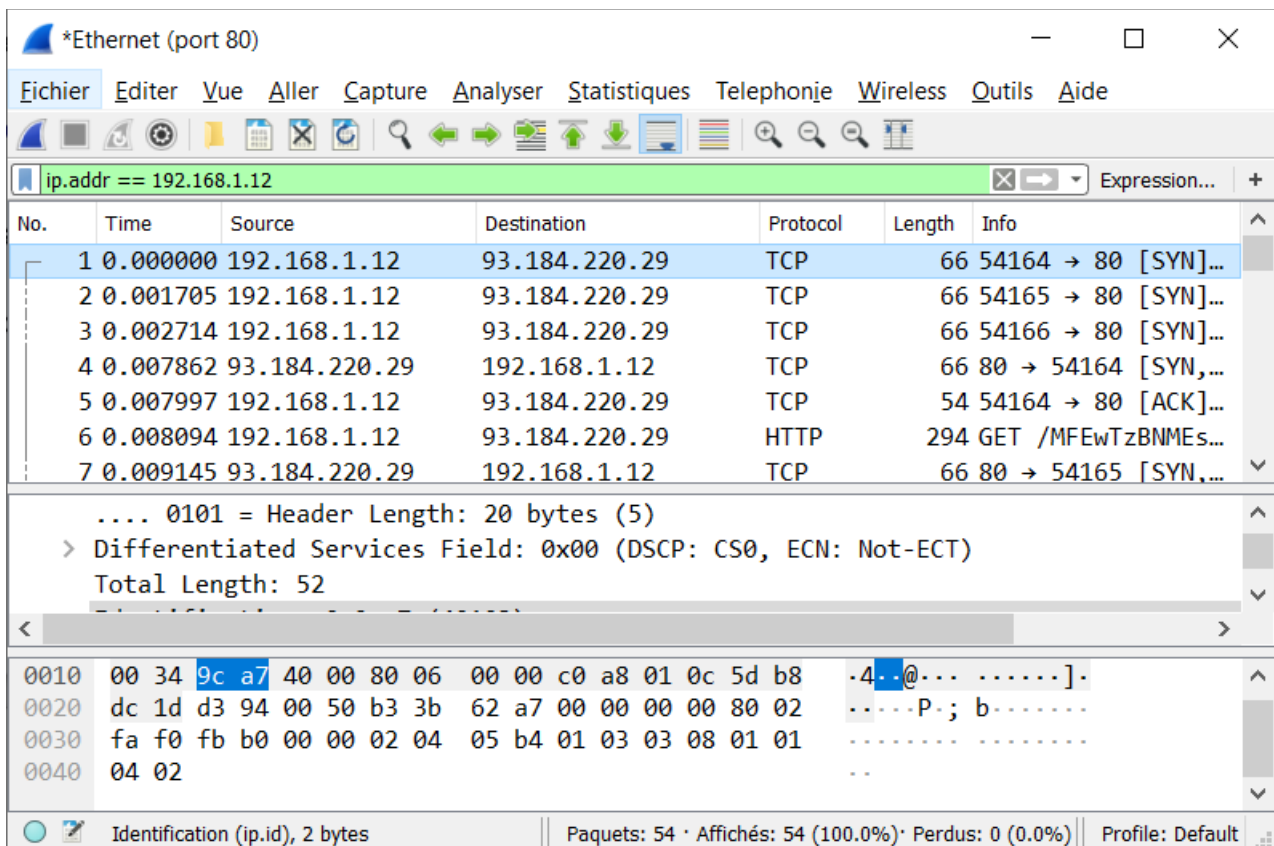
Pour redémarrer une capture, activer le bouton: 

#### II.4.2.5. INSPECTION DES PAQUETS:

Wireshark permet d'inspecter le contenu binaire des paquets (contenu utile et couches de protocole) grâce à des fonctions de sélection ou de mise en évidence (coloration en fonction du type d'information ou d'un motif binaire, etc.).

Il suffit de cliquer sur une des lignes capturées pour afficher dans les zones 2 et 3 les contenus des couches de protocole et du message global. Diverses fonctions d'édition permettent d'inspecter ce code. Le champ "Apply a display filter" permet de n'afficher que certains des paquets capturés en saisissant un filtre.

**EXEMPLE:** appliquons à la précédente capture le filtre "ip.addr == 192.168.1.12" (sélection des paquets contenant l'adresse IP 192.168.1.12):



The screenshot shows the Wireshark interface with the following details:

- Window title: \*Ethernet (port 80)
- Menu bar: Fichier, Editer, Vue, Aller, Capture, Analyser, Statistiques, Telephonje, Wireless, Outils, Aide
- Filter bar: ip.addr == 192.168.1.12
- Packet list table:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.12	93.184.220.29	TCP	66	54164 → 80 [SYN]...
2	0.001705	192.168.1.12	93.184.220.29	TCP	66	54165 → 80 [SYN]...
3	0.002714	192.168.1.12	93.184.220.29	TCP	66	54166 → 80 [SYN]...
4	0.007862	93.184.220.29	192.168.1.12	TCP	66	80 → 54164 [SYN,...
5	0.007997	192.168.1.12	93.184.220.29	TCP	54	54164 → 80 [ACK]...
6	0.008094	192.168.1.12	93.184.220.29	HTTP	294	GET /MFEwTzBNMEs...
7	0.009145	93.184.220.29	192.168.1.12	TCP	66	80 → 54165 [SYN,...

Below the table, the packet details pane shows:

- .... 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 52

The packet bytes pane shows hex and ASCII data:

```

0010  00 34 9c a7 40 00 80 06 00 00 c0 a8 01 0c 5d b8  -4. .@... ..]
0020  dc 1d d3 94 00 50 b3 3b 62 a7 00 00 00 80 02  -...P.; b-...
0030  fa f0 fb b0 00 00 02 04 05 b4 01 03 03 08 01 01  -.....
0040  04 02  ..
    
```

At the bottom, the status bar shows: Identification (ip.id), 2 bytes | Paquets: 54 · Affichés: 54 (100.0%) · Perdus: 0 (0.0%) | Profile: Default

#### **II.4.2.6. CRÉATION DE FILTRES ( À LA CAPTURE ET À L'ÉDITION):**

Wireshark offre des fonctions de filtrage puissantes qui permettent de sélectionner les paquets que l'on veut traiter en fonction des protocoles, des adresses IP (V4 et V6), des numéros de ports utilisés par ces paquets, etc. Il est possible de combiner ces différents critères dans des expressions logiques qui peuvent ensuite être nommées et enregistrées pour une utilisation ultérieure.

**Exemple:** l'expression "tcp.port == 5000 and ip.addr == 192.168.1.1" définit un filtre qui sélectionne uniquement les paquets TCP émis de ou vers l'adresse 192.168.1.1 et du ou vers le port 5000.

## III.COMMANDES D'ADMINISTRATION DES RÉSEAU:

### III.1.INTRODUCTION:

Les systèmes d'exploitation de type WINDOWS et UNIX/LINUX possèdent dans leurs jeux de commandes en ligne, de nombreuses primitives qui permettent, depuis une machine donnée:

- De surveiller les échanges d'informations dans les réseaux connectés à cette machine;
- De paramétrer le fonctionnement des différentes entités logicielles qui participent à la communication réseau dans cette machine (contrôleurs, pilotes de périphériques, tables et fichiers de configuration réseaux, etc.);
- D'agir sur l'état de ces entités (démarrer, arrêter, redémarrer leur fonctionnement).

Ces commandes doivent être saisies dans des "invites de commande" (ou "shells") accessibles par des fenêtres de type TERMINAL (ou CONSOLE) en mode "texte".

Il peut s'agir soit de terminaux déportés (ouverts par des logiciels de type Rlogin, TelNet, SSH ou Putty), soit de terminaux locaux manipulés par l'IHM local ou par un logiciel de prise de contrôle à distance (TemViewer, VCN, etc.).

Bien que les menus graphiques d'administration réseau offerts par les systèmes d'exploitation soient souvent plus rapides et plus sûrs pour des manipulateurs novices que les commandes en ligne et demandent beaucoup moins d'apprentissage, beaucoup d'administrateurs systèmes privilégient tout de même ces commandes en ligne comme outils d'administration: en effet, elles offrent souvent des options plus nombreuses et surtout elles peuvent être combinées en procédures d'administration (scripts shells) qui ont l'avantage d'être réutilisables.

### III.2.PRINCIPALES TÂCHES D'ADMINISTRATION DES RÉSEAUX:

Le tableau suivant énumère les principales tâches d'administration réseau sur un poste de travail et indique pour chacune les principales commandes disponibles et les fichiers de configuration concernés;

TÂCHE	FICHIERS DE CONFIGURATION	OUTILS (commandes)
Déclarer, supprimer un utilisateur, modifier les droits d'un utilisateur.	<b>Linux:</b> - /etc/passwd - /etc/group	<b>Linux:</b> - adduser, addgroup - deluser, delgroup - who, whoami <b>Windows:</b> - Ligne de cde: net user - Menus: Comptes ....
Afficher la table de résolution des adresses IP en adresses MAC pour une connexion (masque ARP).		arp
Gérer la Table de Routage IP d'un poste (visualiser, supprimer, ajouter, modifier des routes)		route
Visualiser la liste des ports ouverts		netstat
Créer, supprimer, visualiser les interfaces réseaux, tester leur état		<b>Windows:</b> - ipconfig <b>Linux/Unix:</b> - ifconfig, ip
Démarrer, arrêter un interface réseau	/etc/network/interfaces	<b>Windows:</b> <b>Linux:</b> - ifup, ifdown
Créer, supprimer un tunnel IP.		Ip tunnel add ....
Déterminer la route suivie par un paquet émis.		<b>Linux:</b> - traceroute <b>Windows:</b> - tracert
Tester la connectivité sur une interface		ping
Démarrer, arrêter, redémarrer le processus gérant le réseau.	Le répertoire /etc/init.d renferme des scripts de lancement des services (networking pour le service "réseau")	<b>Linux:</b> /etc/init.d/networking [start/stop/restart] <b>Windows:</b>

## III.3.LES COMMANDES SYSTÈMES EN LIGNES DE COMMANDES:

### III.3.1.INTRODUCTION:

Ce sous-chapitre n'est pas un manuel de référence de ces commandes. Son objectif est de les présenter sommairement en insistant sur l'emploi que l'on peut en faire pour l'administration des réseaux. Pour plus de détail, consulter les manuels correspondants ou les ressources en ligne telles que "man" et "help".

### III.3.2.RAPPEL:

Les commandes systèmes doivent être saisies dans des invites de commandes ouvertes dans des fenêtres de type "TERMINAL EN LIGNE DE COMMANDE". Suivant le système d'exploitation utilisé, l'ouverture d'un terminal s'obtient de différentes façons:

#### III.3.2.1.SOUS LINUX/UNIX:

- Dans un environnement graphique (tel que gnome), il suffit de faire un "click-droit" sur le fond du bureau pour faire apparaître un menu contextuel offrant l'option "ouvrir un terminal". Le choix de cette option provoque l'affichage de la fenêtre de ce nouveau terminal;
- En ligne de commande (dans un environnement non graphique ou dans un terminal en ligne de commande ouvert dans un environnement graphique): suivant le système d'exploitation utilisé, les commandes de type "terminal", "gnome-terminal", "konsole", etc. permettent d'ouvrir une fenêtre de terminal (pour ubuntu avec bureau graphique, c'est "gnome-terminal").

**REMARQUE:** droits associés aux commandes saisies dans un terminal:

Sous Unix/Linux, comme sous windows, certaines commandes ne peuvent être exécutées que par l'utilisateur "ADMINISTRATEUR". De ce fait, pour exécuter des commandes nécessitant de l'utilisateur les privilèges d'administrateur, il faudra:

- Soit (sous debian/ubuntu) utiliser la commande "sudo" (substitute user) en préfixe de ces commandes (exemple: > sudo netstat -b ). sudo permet d'exécuter la commande qui suit en mode "root" (administrateur);
- Soit la commande "su" qui permet de changer d'utilisateur d'une manière durable, quand cette commande est acceptée par l'implémentation de linux.

#### III.3.2.2.SOUS WINDOWS:

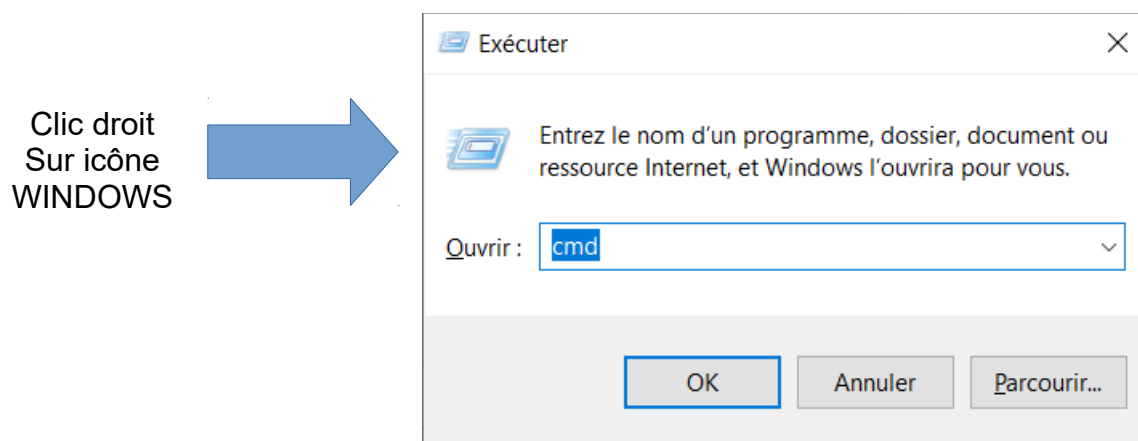
##### III.3.2.2.1.DROITS ASSOCIES AUX COMMANDES:

Sous WINDOWS comme sous Unix/Linux, certaines commandes ne peuvent être exécutées qu'en mode "ADMINISTRATEUR". Comme il est difficile, sous windows, de changer d'utilisateur entre deux commandes, le seul moyen pratique d'exécuter des commandes en mode administrateur est d'ouvrir un terminal doté de ces privilèges:



### III.3.2.2. OUVERTURE EN MODE UTILISATEUR NON PRIVILÉGIÉ:

Faire un "clic droit" sur le menu de démarrage (icône windows, coin bas-gauche), puis choisir "exécuter". Dans la fenêtre "exécuter" saisir "cmd" (logiciel exécuteur de commandes) dans le champ "ouvrir", puis valider (bouton "OK"). Le terminal s'ouvre alors dans une fenêtre.



### III.3.2.2.3. OUVERTURE EN MODE UTILISATEUR PRIVILÉGIÉ (ADMINISTRATEUR):

Pour ouvrir une console en mode administrateur:

- Faire un clic droit sur le menu de démarrage (icône windows, coin bas-gauche), puis choisir "exécuter". Saisir "cmd" (logiciel exécuteur de commandes) dans le champ "ouvrir", puis valider (bouton "OK") **tout en appuyant simultanément sur [ctrl] et [shift]**. Le terminal s'ouvre alors dans une fenêtre avec les droits "administrateur";
- Sinon, faire un clic droit sur le menu de démarrage (icône windows, coin bas-gauche), puis choisir "exécuter en mode administrateur".

### III.3.3. TEST DE LA CONNECTIVITÉ D'UNE MACHINE:

#### III.3.3.1. DÉFINITION:

La CONNECTIVITÉ d'une machine reliée physiquement à un réseau est sa capacité de communiquer effectivement par cette liaison avec d'autres machines du réseau. Sur un réseau ethernet TCP/IP, on utilise la fonction PING qui permet de vérifier la connexion entre la machine locale et une machine distante. Ping utilise le protocole ICMP. La commande ping existe sous Unix/Linux et Windows ainsi que sous la plupart des autres O.S.

#### III.3.3.2. COMMANDE PING (Windows et Unix/Linux):

##### FORME DE BASE:

La commande PING existe sous Windows et Unix/Linux. Sa forme la plus simple est:

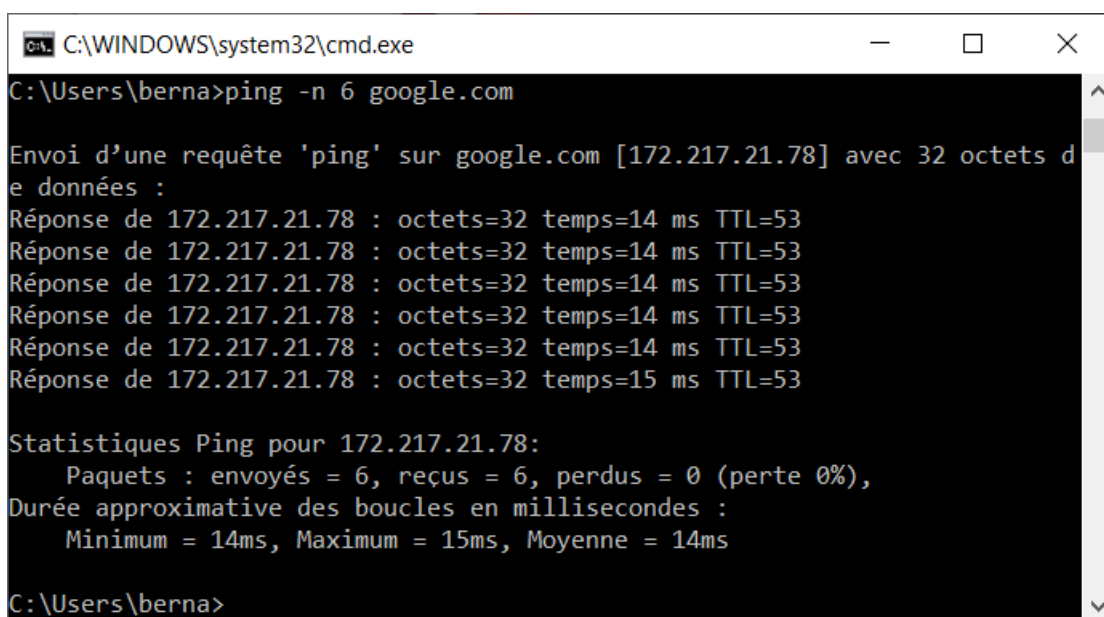
```
> ping [<@IP machine distante> / <URL machine distante> ]
```

Tester la connectivité avec la machine d'adresse IP 192.168.1.1: > *ping 192.168.1.1*

Tester la connectivité avec le serveur web dont l'URL est "google.com":> *ping google.com*

**REMARQUE:** Sous Windows et Linux, la commande supporte sensiblement les mêmes options. Cependant, les syntaxes ne sont pas les mêmes (consulter les manuels pour approfondir).

**EXEMPLE:** tester la connexion avec le serveur google.com (sous widows)



```
C:\WINDOWS\system32\cmd.exe
C:\Users\berna>ping -n 6 google.com

Envoi d'une requête 'ping' sur google.com [172.217.21.78] avec 32 octets de données :
Réponse de 172.217.21.78 : octets=32 temps=14 ms TTL=53
Réponse de 172.217.21.78 : octets=32 temps=14 ms TTL=53
Réponse de 172.217.21.78 : octets=32 temps=14 ms TTL=53
Réponse de 172.217.21.78 : octets=32 temps=14 ms TTL=53
Réponse de 172.217.21.78 : octets=32 temps=14 ms TTL=53
Réponse de 172.217.21.78 : octets=32 temps=15 ms TTL=53

Statistiques Ping pour 172.217.21.78:
    Paquets : envoyés = 6, reçus = 6, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 14ms, Maximum = 15ms, Moyenne = 14ms

C:\Users\berna>
```

**Remarques:**

- La commande "ping -n 6 google.com" envoie 6 messages ICMP vers la cible (l'option -n <count> permet de définir le nombre de messages à expédier). Sous Linux, la commande s'écrirait "ping -c 6 google.com".
- La présentation de la réponse varie entre Windows et Unix/Linux.

### III.3.4.DÉTERMINATION DE LA ROUTE D'UN PAQUET:

#### III.3.4.1.DÉFINITION:

La ROUTE suivie par un paquet est une information constituée par:

- La liste des nœud intermédiaires (routeurs, passerelles) utilisés par ce paquet pour se rendre d'un nœud à un autre du réseau,
- Les durées des trajet entre chacun des nœuds successifs constituant cette liste.

#### III.3.4.2.UTILITÉ:

Visualiser la route suivie par les paquets IP pour aller du poste local à un poste éloigné, permet à l'administrateur en charge de la gestion d'un réseau complexe de surveiller les délais de routage sur les différentes routes possibles.

L'administrateur peut ainsi ajuster le contenu des tables de routages de façon à équilibrer les trafics sur les différentes routes possibles et optimiser ainsi l'utilisation du réseau et les temps de réponse.

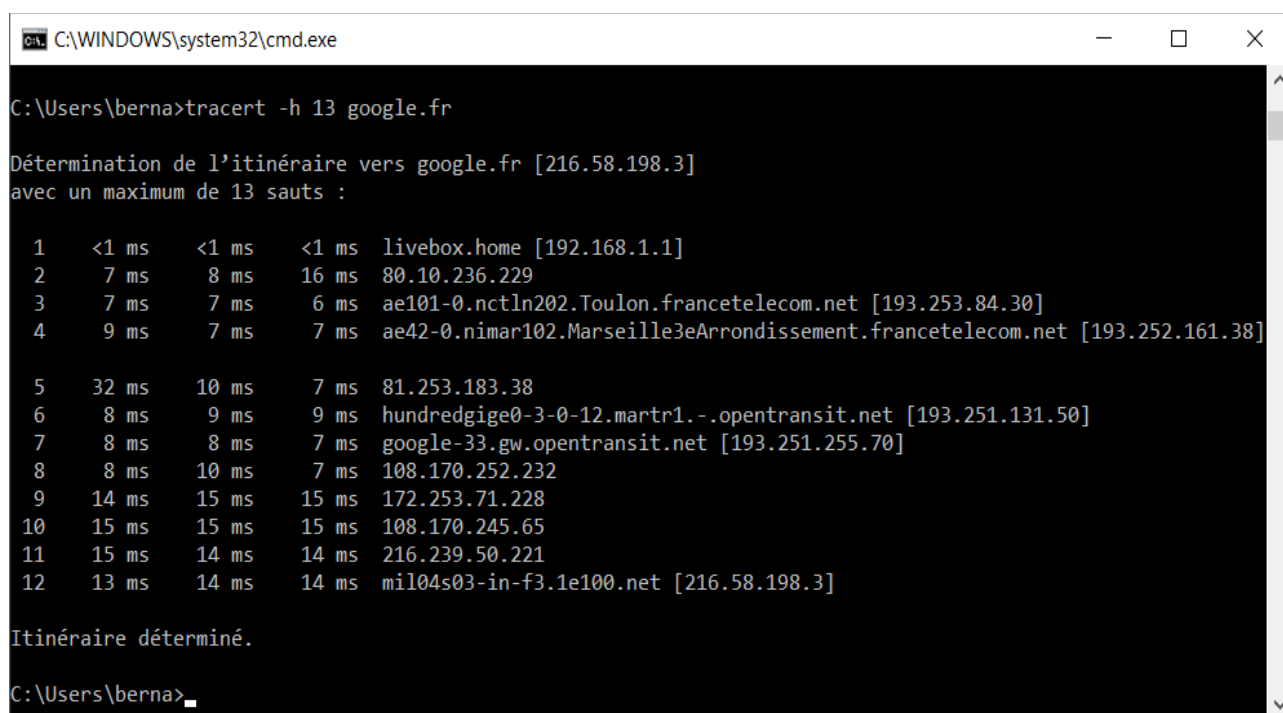
#### III.3.4.3.SOUS WINDOWS (Commande TRACERT)

Sous windows, la syntaxe de base de la commande est "tracert":

> **tracert** -h <TTL> [<@IP système distant> / [<URL serveur distant>]

**REMARQUE:** TTL est le Time To Live, c'est à dire le nombre maximum de nœuds du réseau que l'on peut parcourir avant que la recherche prenne fin.

**EXEMPLE:** (avec un ttl de 13)



```
C:\WINDOWS\system32\cmd.exe
C:\Users\berna>tracert -h 13 google.fr
Détermination de l'itinéraire vers google.fr [216.58.198.3]
avec un maximum de 13 sauts :

 1  <1 ms  <1 ms  <1 ms  livebox.home [192.168.1.1]
 2  7 ms   8 ms   16 ms  80.10.236.229
 3  7 ms   7 ms   6 ms   ae101-0.nctln202.Toulon.francetelecom.net [193.253.84.30]
 4  9 ms   7 ms   7 ms   ae42-0.nimar102.Marseille3eArrondissement.francetelecom.net [193.252.161.38]

 5  32 ms  10 ms   7 ms   81.253.183.38
 6  8 ms   9 ms   9 ms   hundredgige0-3-0-12.martr1.-.opentransit.net [193.251.131.50]
 7  8 ms   8 ms   7 ms   google-33.gw.opentransit.net [193.251.255.70]
 8  8 ms   10 ms  7 ms   108.170.252.232
 9  14 ms  15 ms  15 ms  172.253.71.228
10  15 ms  15 ms  15 ms  108.170.245.65
11  15 ms  14 ms  14 ms  216.239.50.221
12  13 ms  14 ms  14 ms  mil04s03-in-f3.1e100.net [216.58.198.3]

Itinéraire déterminé.
C:\Users\berna>
```

Chaque ligne correspond à un nœud parcouru par les paquets.

### **III.3.4.4.SOUS LINUX/UNIX (Commande TRACEROUTE):**

Sous linux/unix, la syntaxe de base de la commande est "traceroute":

> **traceroute** -m <TTL> [<@IP système distant> / [<URL serveur distant>]

#### **EXEMPLE:**

> traceroute -m 50 Lycos.com

Permet de déterminer la route d'un paquet depuis la machine locale jusqu'au serveur Lycos.com avec un nombre de nœuds maximum traversés de 50.

#### **Résultat:**

```
traceroute to lycos.com (209.202.254.90), 20 hops max, 60 byte packets
 1 livebox.home (192.168.1.1)  1.955 ms  1.835 ms  1.720 ms
 2 80.10.236.229 (80.10.236.229)  8.384 ms  9.036 ms  9.830 ms
 3 ae101-0.nctln202.Toulon.francetelecom.net (193.253.84.30)  9.704 ms  10.388
   ms  11.260 ms
 4 ae42-0.nimar102.Marseille3eArrondissement.francetelecom.net (193.252.161.38)
 11.966 ms  12.533 ms  13.878 ms
 5 193.252.137.54 (193.252.137.54)  23.786 ms  24.007 ms  24.155 ms
 6 193.251.132.154 (193.251.132.154)  25.885 ms  193.251.242.96 (193.251.242.96)
 22.620 ms  193.251.242.92 (193.251.242.92)  23.534 ms
 7 193.251.128.183 (193.251.128.183)  99.130 ms  193.251.240.202
   (193.251.240.202)  98.046 ms  193.251.243.241 (193.251.243.241)  94.845 ms
 8 comcast-3.gw.opentransit.net (193.251.249.40)  90.652 ms  92.135 ms  91.990
   ms
 9 be-10381-cr02.newyork.ny.ibone.comcast.net (68.86.86.249)  95.038 ms  95.335
   ms  95.025 ms
10 be-7922-ar01.needham.ma.boston.comcast.net (68.86.90.218)  100.049 ms
   104.137 ms  101.490 ms
11 96.108.71.46 (96.108.71.46)  103.186 ms  103.138 ms  105.344 ms
12 162.151.190.26 (162.151.190.26)  103.702 ms  111.268 ms  96.652 ms
13 50.224.253.194 (50.224.253.194)  98.431 ms  97.143 ms  96.863 ms
```

### III.3.5.TEST DE L'ÉTAT DU RÉSEAU DANS UNE MACHINE:

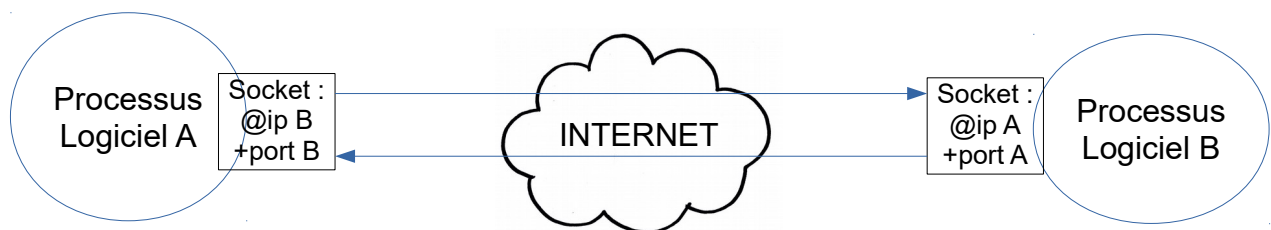
#### III.3.5.1.DÉFINITION:

A l'intérieur d'une machine donnée, l'ETAT RÉSEAU est représenté par l'ensemble des états des différentes "connexions logicielles" établies entre les applications réseau locales et des applications réseau distantes (on parle bien ici de "connexions logicielles" et non d'interfaces physiques).

Le standard TCP/IP utilise pour établir des connexions entre deux processus logiciels la notion de SOCKET. Un socket est représenté par une adresse IP associée à un numéro de port:

SOCKET == @ IP de la machine destinataire + N° de port du logiciel destinataire

Deux applications communicant sur INTERNET utilisent chacune un SOCKET:



Plusieurs types de SOCKETS existent. Ils dépendent du protocole de communication utilisé: TCP, UDP ou RAW (RAW permet de communiquer directement en protocoles ICMP, IP ou RIP).

D'autre part, à un instant donné, un SOCKET peut avoir plusieurs états. Par exemple

- LISTEN: en écoute de demande de connexion
- ESTABLISHED: connexion établie;
- SYN\_SENT: en attente de connexion;
- TIME\_WAIT: en attente de fin de transmission
- CLOSE: connexion fermée
- etc..

Ces différentes caractéristiques constituent les états des sockets existant à un moment donné dans la machine hôte.

#### III.3.5.2.UTILITÉ:

Pour l'administrateur réseau, l'inspection de l'état des sockets et des connexions permet:

- D'inspecter le fonctionnement de la communication entre processus logiciels et de diagnostiquer d'éventuels dysfonctionnements;
- De repérer d'éventuelles connexions inutiles ou indésirables.

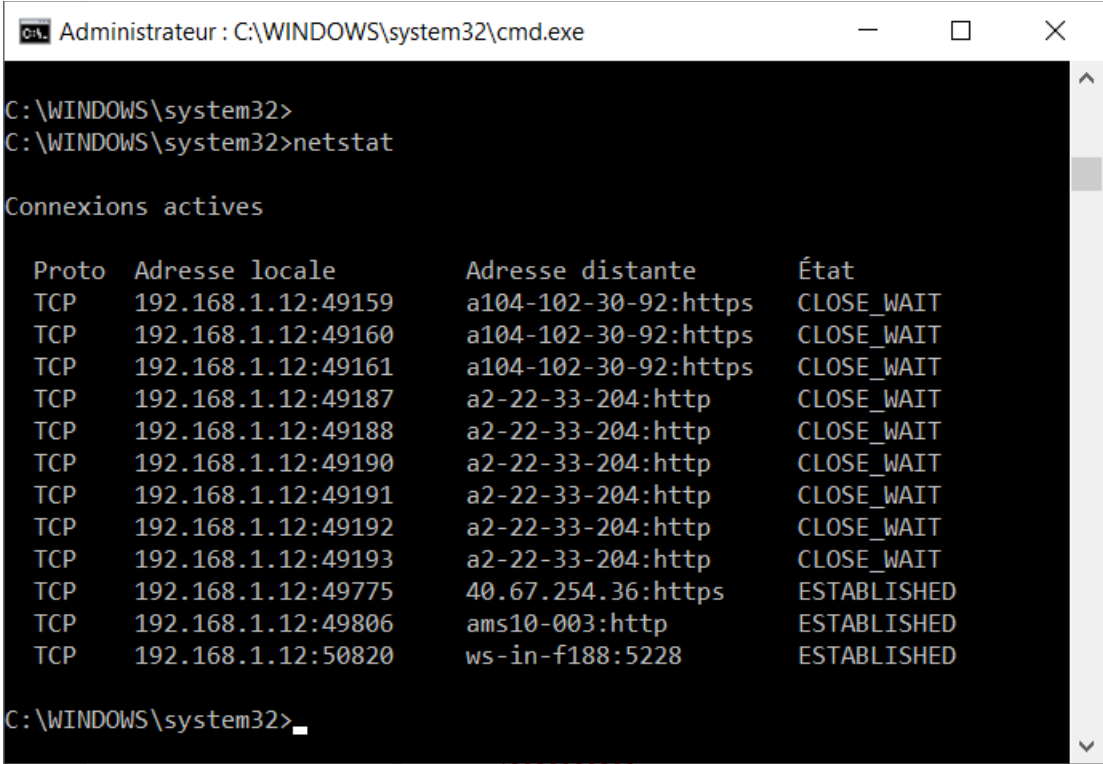
### III.3.5.3.COMMANDE NETSTAT

La commande **NETSTAT** permet de tester la configuration du réseau, visualiser l'état des connexions, visualiser les routes, établir des statistiques, notamment pour surveiller les serveurs. Sa syntaxe de base est:

> netstat

Cette commande existe pour Linux/Unix et Windows. Dans sa forme de base, elle permet d'afficher l'état des connexions réseau en cours d'utilisation.

**EXEMPLE:** Sous windows, netstat sans option permet d'afficher toutes les connexions logicielles (sockets) existantes à un instant donné réseau **ACTIVES** avec le protocole utilisé, le socket local utilisé (@IP et n° de port), le socket distant et l'état de la connexion.



```
C:\WINDOWS\system32>
C:\WINDOWS\system32>netstat

Connexions actives

Proto  Adresse locale          Adresse distante        État
TCP    192.168.1.12:49159      a104-102-30-92:https    CLOSE_WAIT
TCP    192.168.1.12:49160      a104-102-30-92:https    CLOSE_WAIT
TCP    192.168.1.12:49161      a104-102-30-92:https    CLOSE_WAIT
TCP    192.168.1.12:49187      a2-22-33-204:http       CLOSE_WAIT
TCP    192.168.1.12:49188      a2-22-33-204:http       CLOSE_WAIT
TCP    192.168.1.12:49190      a2-22-33-204:http       CLOSE_WAIT
TCP    192.168.1.12:49191      a2-22-33-204:http       CLOSE_WAIT
TCP    192.168.1.12:49192      a2-22-33-204:http       CLOSE_WAIT
TCP    192.168.1.12:49193      a2-22-33-204:http       CLOSE_WAIT
TCP    192.168.1.12:49775      40.67.254.36:https      ESTABLISHED
TCP    192.168.1.12:49806      ams10-003:http          ESTABLISHED
TCP    192.168.1.12:50820      ws-in-f188:5228         ESTABLISHED

C:\WINDOWS\system32>
```

Des options sont disponibles pour afficher d'autres informations, comme:

- a pour afficher toutes les connexions (actives ou non);
- p <protocole> pour sélectionner les connexions d'un protocole donné;
- b pour afficher les exécutable liés à chaque connexion;
- r pour afficher la table de routage;
- etc.

La syntaxe et la présentation varient selon que l'on opère depuis Linux ou Windows:

**EXEMPLE:** Commande netstat -a sous linux:

Connexions Internet actives (serveurs et établies)

25507 @/tmp/dbus-TUXImbTP

```
-----  
-----  
unix 2      [ ACC ]    STREAM    LISTENING    18486  
/run/NetworkManager/private-dhcp  
unix 2      [ ACC ]    STREAM    LISTENING    31083    @/tmp/dbus-lSY9FLma  
unix 2      [ ACC ]    STREAM    LISTENING    14311    /run/acpid.socket  
unix 2      [ ACC ]    STREAM    LISTENING    20636    @/tmp/dbus-pDqFUvGt  
unix 2      [ ACC ]    STREAM    LISTENING    19601  
/var/run/mysqld/mysqld.sock  
unix 2      [ ACC ]    STREAM    LISTENING    19656    @/tmp/.ICE-unix/832  
unix 2      [ ACC ]    STREAM    LISTENING    18398    @/tmp/dbus-9Ijybj17  
unix 2      [ ACC ]    STREAM    LISTENING    23787    /run/cups/cups.sock  
unix 2      [ ACC ]    STREAM    LISTENING    14360    /run/uidd/request  
unix 2      [ ACC ]    STREAM    LISTENING    14363  
/var/run/dbus/system_bus_socket
```

**REMARQUES:** Sous linux ou windows:

- Sous linux ou windows, > netstat -r affiche la table de routage;
- Sous Linux, > netstat -i affiche des statistiques sur chaque connexion;
- Sous Windows, > netstat -s affiche à peu près les mêmes statistiques.

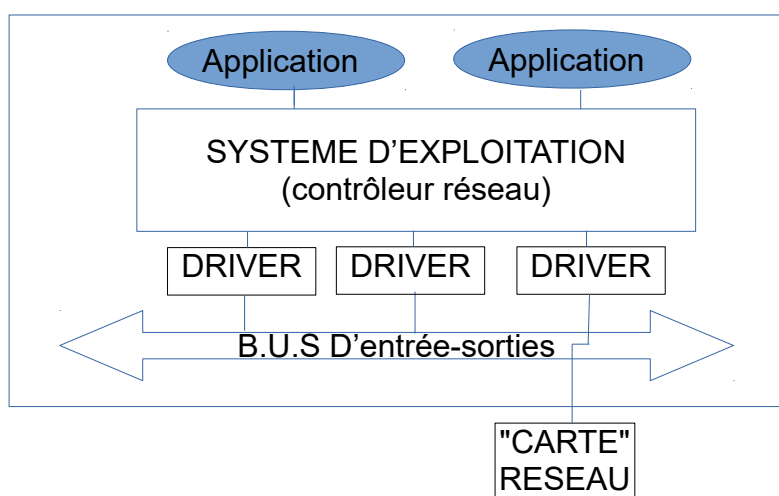


### III.3.6.GESTION ET VISUALISATION DES INTERFACES RÉSEAU:

#### III.3.6.1.DÉFINITIONS:

##### **INTERFACE PHYSIQUE:**

Dans son acception principale, un interface réseau fait référence à un équipement PHYSIQUE de liaison au réseau ("carte" réseau). A chacun de ces équipements est attaché un logiciel pilote de périphérique (DRIVER) chargé d'assurer la communication avec la périphérie de la machine d'une part et le système d'exploitation d'autre part.



##### **INTERFACE LOGIQUE:**

Cependant, les systèmes d'exploitation de type Unix/Linux définissent également au moins une interface "logique" qui est le "loopback": la boucle réseau interne (adresse ip 127.0.0.1) qui permet à une machine d'émettre vers elle-même.

##### **INTERFACE "VIRTUEL":**

De plus, dans le cas d'une machine virtuelle, celle-ci possède une interface "virtuelle" qui correspond à une des interfaces physiques de la machine physique support.

##### **ALIAS D'UNE INTERFACE:**

Enfin, à une interface physique donnée peuvent être associées plusieurs adresses IP (V4 ou V6). L'ajout de chaque adresses IP supplémentaire est effectué en créant un "alias" de l'interface physique qui apparaît dans la liste des interfaces de la machine (par exemple, dans linux, ajouter une adresse IP à l'interface eth0 revient à créer l'alias eth0:1, muni de la nouvelle adresse IP)

### III.3.6.2.UTILITÉ:

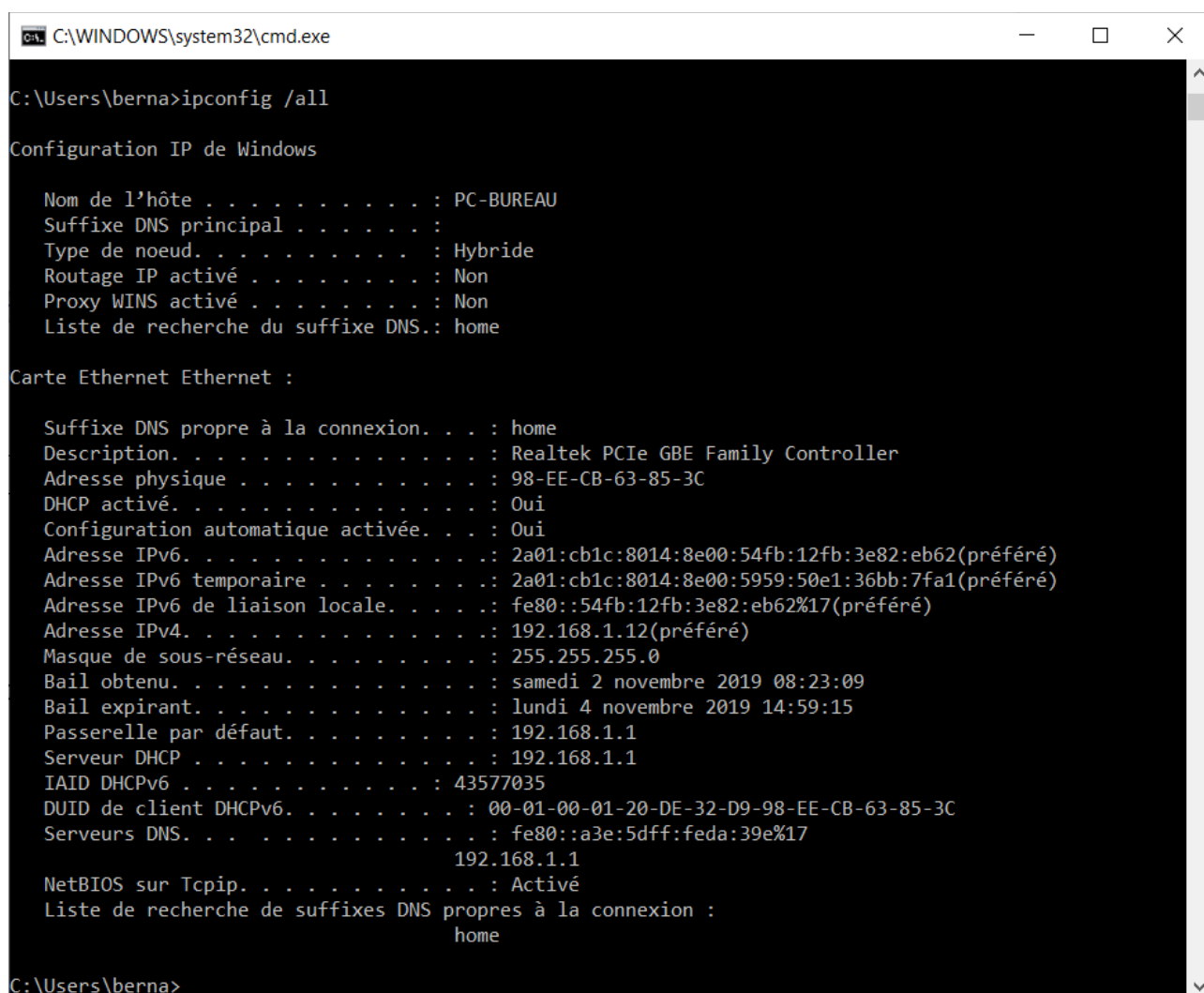
La surveillance des interfaces réseaux permet aux administrateurs de réseau d'évaluer les volumes de trafic transitant par ces interfaces et de repérer d'éventuels dysfonctionnements.

La gestion de ces interfaces permet, à partir des observations effectuées, d'optimiser le fonctionnement des entrées-sorties réseau.

### III.3.6.3.IPCONFIG (window):

Cette commande permet d'inspecter les cartes réseau physiques d'une machine windows:

**EXEMPLE:** ipconfig -all permet d'afficher toutes les informations relatives aux cartes réseau installées sur la machine:



```
C:\WINDOWS\system32\cmd.exe
C:\Users\berna>ipconfig /all

Configuration IP de Windows

Nom de l'hôte . . . . . : PC-BUREAU
Suffixe DNS principal . . . . . :
Type de noeud . . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
Liste de recherche du suffixe DNS.: home

Carte Ethernet Ethernet :

Suffixe DNS propre à la connexion. . . : home
Description. . . . . : Realtek PCIe GBE Family Controller
Adresse physique . . . . . : 98-EE-CB-63-85-3C
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6. . . . . : 2a01:cb1c:8014:8e00:54fb:12fb:3e82:eb62(préféré)
Adresse IPv6 temporaire . . . . . : 2a01:cb1c:8014:8e00:5959:50e1:36bb:7fa1(préféré)
Adresse IPv6 de liaison locale. . . . . : fe80::54fb:12fb:3e82:eb62%17(préféré)
Adresse IPv4. . . . . : 192.168.1.12(préféré)
Masque de sous-réseau. . . . . : 255.255.255.0
Bail obtenu. . . . . : samedi 2 novembre 2019 08:23:09
Bail expirant. . . . . : lundi 4 novembre 2019 14:59:15
Passerelle par défaut. . . . . : 192.168.1.1
Serveur DHCP . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 43577035
DUID de client DHCPv6. . . . . : 00-01-00-01-20-DE-32-D9-98-EE-CB-63-85-3C
Serveurs DNS. . . . . : fe80::a3e:5dff:feda:39e%17
                        192.168.1.1
NetBIOS sur Tcpip. . . . . : Activé
Liste de recherche de suffixes DNS propres à la connexion :
                        home

C:\Users\berna>
```

### III.3.6.4.IFCONFIG (linux):

**REMARQUE:** la commande IFCONFIG étant maintenant considérée comme obsolète, il est recommandé d'utiliser la commande IP en lieu et place de cette commande. Cependant, la commande ifconfig est encore largement utilisée à cause de sa moindre complexité.

La commande ifconfig de linux/unix permet:

- De configurer, paramétrer ou supprimer les interfaces d'une machine linux et d'obtenir des informations sur leurs états;
- D'activer ou désactiver ces interfaces;
- D'associer des adresses IP supplémentaires à une interface ("alias" d'interfaces);
- D'obtenir un certain nombre de données statistiques sur chaque interface;
- De configurer des tunnels IP;
- Etc.

**EXEMPLE:** la commande > ifconfig -a enp03 produit l'affichage suivant:

```
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.16 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::2b47:5ea9:1cd9:a36 prefixlen 64 scopeid 0x20<link>
    inet6 2a01:cb1c:8014:8e00:8af6:4a0c:4f7e:d995 prefixlen 64
    scopeid 0x0<global>
    inet6 2a01:cb1c:8014:8e00:bd33:3cd8:c1f7:bfa7 prefixlen 64
    scopeid 0x0<global>
    ether 08:00:27:aa:ba:4e txqueuelen 1000 (Ethernet)
    RX packets 8178 bytes 5549890 (5.5 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2800 bytes 211300 (211.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Nous voyons que les données de configuration de l'interface enp0s3 sont affichées, ainsi que des données statistiques concernant l'état de la connexion.

### III.3.6.5.LA COMMANDE IP (linux):

**REMARQUE:** la commande IFCONFIG étant maintenant considérée comme obsolète, il est recommandé d'utiliser la commande IP en lieu et place de cette commande.

#### III.3.6.5.1.PRÉSENTATION:

La commande IP permet d'obtenir tous les résultats fournis par la commande ifconfig:

- Configurer, paramétrer ou supprimer les interfaces d'une machine linux et d'obtenir des informations sur leurs états;
- Activer ou désactiver ces interfaces;
- Associer des adresses IP supplémentaires à une interface ("alias" d'interfaces);

- Obtenir un certain nombre de données statistiques sur chaque interface;
- Configurer des tunnels IP;

### III.3.6.5.2.SYNTAXE GÉNÉRALE:

Sa syntaxe générale est:

```
ip [ <options> ] <objet> { <commande>|help }
```

avec:

```
<options>:=: { -V[ersion] | -h[uman-readable] | -s[tatistics] | -d[etails] | -r[esolve] | -iec  
              | -f[amily] { inet | inet6 | ipx | dnet | link } | -4 | -6 | -l | -D | -B | -O  
              | -l[oops] { maximum-addr-flush-attempts } | -o[neline] | -rc[vbuf] [size]  
              | -t[imestamp] | -ts[hort] | -n[etns] name | -a[ll] | -c[olor] }
```

<objet>:=:

- link: Périphérique réseau;
- address: Adresse du protocole (v4, v6) sur un périphérique réseau;
- addrlabel: Étiquettes (*ou labels*) des protocoles de l'adresse sélectionné;
- route: Table de routage;
- rule: Règle de la sécurité de la table de routage;
- neighbour: Cache ARP;
- madresse: Adresse multicast;
- tunnel: tunnel IP.

Les commandes dépendent des objets manipulés: elles peuvent être: set, add, show, etc.

### III.3.6.5.3.EXEMPLES:

***Afficher la liste des interfaces réseaux de la machine, accompagnée de renseignements sur leur configuration:***

```
> ip a
```

Affichage obtenu:

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group  
   default qlen 1000  
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
   inet 127.0.0.1/8 scope host lo valid_lft forever preferred_lft forever  
   inet6 ::1/128 scope host valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP  
   group default qlen 1000  
   link/ether 08:00:27:aa:ba:4e brd ff:ff:ff:ff:ff:ff  
   inet 192.168.1.16/24 brd 192.168.1.255 scope global dynamic enp0s3  
   valid_lft 83105sec preferred_lft 83105sec  
   inet6 2a01:cb1c:8014:8e00:6c83:c3bc:1773:971c/64 scope global temporary  
   dynamic valid_lft 1759sec preferred_lft 559sec
```

```
inet6 2a01:cb1c:8014:8e00:8af6:4a0c:4f7e:d995/64 scope global mngtmpaddr  
noprefixroute dynamic valid_lft 1759sec preferred_lft 559sec  
inet6 fe80::2b47:5ea9:1cd9:a36/64 scope link valid_lft forever  
preferred_lft forever
```

**REMARQUE:** Il est possible de se restreindre aux adresses IP V4 ( > ip -4 a ) ou IP V6 ( > ip -6 a ) où à une interface ( > ip a show enp0s3 ).

**Ajouter une adresse à une interface:**

> sudo ip addr add 192.168.1.123/255.255.255.0 dev enp0s3

**Supprimer une adresse d'une interface:**

> sudo ip addr del 192.168.1.123/255.255.255.0 dev enp0s3

**Activer ou désactiver une interface :**

> sudo ip link set dev enp0s3 up

> sudo ip link set dev enp0s3 down

**Inspecter la table de routage:**

> ip r

**Ajouter ou supprimer une route:**

> sudo ip route add 192.168.1.21/24 via 192.168.1.16 dev enp0s3

> sudo ip route del 92.168.1.21/24

### **III.3.7.FILTRES LES SORTIES D'UNE COMMANDES:**

#### **III.3.7.1.INTRODUCTION:**

Très souvent, les commandes fournissent en retour de très nombreuses informations qu'il est difficile et fastidieux d'exploiter, surtout dans un contexte opérationnel. Les options attachées à chaque commande permettent de restreindre le volume des sorties des commandes en permettant de sélectionner un certain type de résultat.

Par exemple, la commande `> netstat -u` sous linux n'affichera que la liste des sockets udp.

Cependant, très souvent, il est nécessaire d'effectuer une sélection bien plus restreinte. C'est le cas, par exemple, lorsqu'on recherche des informations relatives à un numéro de port particulier ou à un logiciel particulier. Dans ce cas, les PIPELINES offrent des possibilités de filtrage beaucoup plus importantes.

#### **III.3.7.2.RAPPEL:**

Il est possible de rediriger le flux de sortie d'une commande vers le flux d'entrée d'une autre commande. L'opérateur "|" (appelé pipe-line ou tube) permet de réaliser cette opération:

`<commande 1> | <commande 2> | <commande 3> .....`

- La sortie de la commande n°1 est injectée dans l'entrée de la commande n° 2;
- La sortie de la commande n°2 est injectée dans l'entrée de la commande n°3;
- Et ainsi de suite.

D'autre part, les jeux de commandes linux et windows offrent la possibilité de filtrer l'affichage des lignes d'un fichier texte (par les commandes `grep` pour linux/unix et `find` pour windows).

#### **EXEMPLES:**

- Sur un système LINUX, la commande `> grep "192.168.1.12" /etc/hosts` n'affichera que les lignes du fichier `/etc/hosts` qui contiennent l'adresse IP `192.168.1.12`;
- Sur un système WINDOWS la commande `> find "127.0.0.1" c:/Windows/system32/drivers/etc/hosts` n'affichera que les lignes du fichier `/etc/hosts` qui contient l'adresse IP `127.0.0.1`;

#### **III.3.7.3.FILTRAGE PAR PIPELINES:**

Les pipelines permettent de filtrer la sortie d'une commande en redirigeant le flux vers une commande GREP (pour linux) ou FIND (pour windows).

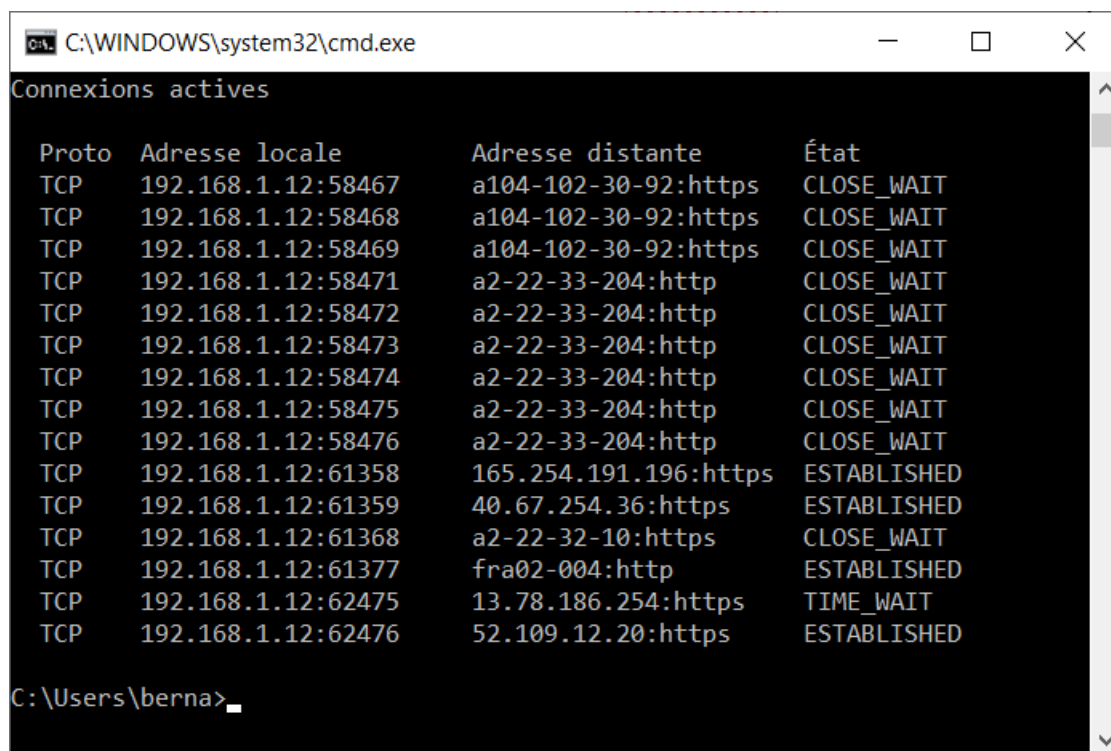
#### **EXEMPLE:**

## Doc: Administration Réseaux-Outils de base de l'administrateur des réseaux

Dans la sortie d'une commande NETSTAT, sélectionner uniquement les lignes qui concernent le port 61377:

- Pour LINUX: > netstat | grep "61377";
- Pour WINDOWS: > netstat | find "61377";

Sortie obtenue pour > netstat dans windows:




```
C:\WINDOWS\system32\cmd.exe
Connexions actives

Proto  Adresse locale      Adresse distante    État
TCP    192.168.1.12:58467  a104-102-30-92:https CLOSE_WAIT
TCP    192.168.1.12:58468  a104-102-30-92:https CLOSE_WAIT
TCP    192.168.1.12:58469  a104-102-30-92:https CLOSE_WAIT
TCP    192.168.1.12:58471  a2-22-33-204:http   CLOSE_WAIT
TCP    192.168.1.12:58472  a2-22-33-204:http   CLOSE_WAIT
TCP    192.168.1.12:58473  a2-22-33-204:http   CLOSE_WAIT
TCP    192.168.1.12:58474  a2-22-33-204:http   CLOSE_WAIT
TCP    192.168.1.12:58475  a2-22-33-204:http   CLOSE_WAIT
TCP    192.168.1.12:58476  a2-22-33-204:http   CLOSE_WAIT
TCP    192.168.1.12:61358  165.254.191.196:https ESTABLISHED
TCP    192.168.1.12:61359  40.67.254.36:https  ESTABLISHED
TCP    192.168.1.12:61368  a2-22-32-10:https   CLOSE_WAIT
TCP    192.168.1.12:61377  fra02-004:http      ESTABLISHED
TCP    192.168.1.12:62475  13.78.186.254:https TIME_WAIT
TCP    192.168.1.12:62476  52.109.12.20:https  ESTABLISHED

C:\Users\berna>
```

Sortie obtenue pour > netstat | find "61377" dans windows:



```
C:\WINDOWS\system32\cmd.exe
C:\Users\berna>netstat | find "61377"
TCP    192.168.1.12:61377  fra02-004:http      ESTABLISHED

C:\Users\berna>
```

## III.4.PRINCIPAUX FICHIERS DE CONFIGURATION DES RÉSEAUX:

### III.4.1.FICHIER /etc/hosts(Linux):

Le fichier hosts permet d'établir une correspondance entre une adresse IP et un NOM D'HÔTE. Ce nom pourra par la suite être substitué à l'adresse IP dans une commande.

**EXEMPLE: contenu de /etc/hosts:**

```
127.0.0.1 localhost ubuntu1
192.168.1.1 LiveBox4
192.168.1.12 PC-BUREAU
```

Avec ce contenu, il est possible d'envoyer un ping à la machine 192.168.1.12 avec la commande: > ping PC-BUREAU

### III.4.2.FICHIER /etc/networks (Linux):

Ce fichier permet de donner un NOM à un RÉSEAU.

**EXEMPLE: contenu de /etc/networks**

```
reseau_bureautique 192.168.1.0
reseau_interne 127.0.0.1
```

Ce contenu permet par exemple d'adresser le réseau local 192.168.1.\* dans une commande en employant le nom "reseau\_bureautique". Par exemple, pour définir une route dans la machine 192.168.1.12, la commande:

```
> route add -host reseau_bureautique gw 192.168.1.12
```

permet de router les paquets à envoyer vers le réseau 192.168.1.\* en employant la passerelle 192.168.1.12.

### III.4.3.FICHIER /etc/network/interfaces (Linux):

Le fichier /etc/network/interfaces contient les déclarations des interfaces réseau de la machine. La déclaration d'une interface obéit à la syntaxe suivante:

```
iface <nom_interface> inet [static] address <adresse ip>
netmask <masque_reseau> broadcast <adresse ip broadcast> ....
```

**EXEMPLE DE CONTENU:**

```
# interfaces files used by ufw(8) and ifdown(8)
auto lo
iface enp0s1 inet static address 192.168.1.12 netmask 255.255.255.0
broadcast 192.168.1.255
```



### **III.4.4.FICHER /etc/services (Linux):**

Le fichier "services" liste les services installés dans un système d'exploitation linux. Pour chacun de ces services, il affiche :

- Son nom (par exemple : ftp) ;
- Le numéro de port et le protocole utilisés (par exemple : 21/ftp) ;
- Des commentaires sur le service concerné.

Les ports dont le numéro est compris entre 1 à 1023 sont réservés aux services standards (21 pour ftp, 80 pour http , etc.)

#### **EXEMPLE DE CONTENU :**

```
cat /etc/services
# Network services, Internet style
#
# Note that it is presently the policy of IANA to assign a single well-known
# port number for both TCP and UDP; hence, officially ports have two entries
# even if the protocol doesn't support UDP operations.
#
# Updated from http://www.iana.org/assignments/port-numbers and other
# sources like http://www.freebsd.org/cgi/cvsweb.cgi/src/etc/services .
# New ports will be added on request if they have been officially assigned
# by IANA and used in the real-world or are needed by a debian package.
# If you need a huge list of used numbers please install the nmap package.

tcpmux      1/tcp                # TCP port service multiplexer
echo        7/tcp
echo        7/udp
discard     9/tcp          sink null
discard     9/udp          sink null
systat      11/tcp          users
daytime     13/tcp
daytime     13/udp
netstat     15/tcp
qotd        17/tcp          quote
msp         18/tcp                # message send protocol
msp         18/udp
chargen    19/tcp          ttytst source
chargen    19/udp          ttytst source
ftp-data    20/tcp
ftp         21/tcp
fsp         21/udp          fspd
ssh         22/tcp                # SSH Remote Login Protocol
telnet     23/tcp
smtp        25/tcp          mail
time       37/tcp          timserver
time       37/udp          timserver
```