Réseaux Applicatifs - Labos

Grégoire Roumache

Octobre 2019

Table des Matières

1 Attention !

- La partie **Wireshark** ne contient qu'une liste de filtres. Voir le labo sur Wireshark pour l'utilisation du logiciel.

2 Changer la configuration via la ligne de commande

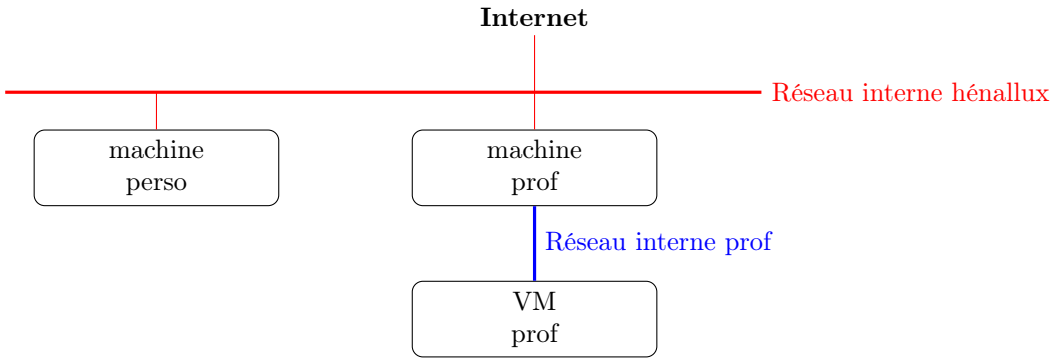
2.1 Windows

> Ouvrir l'invite de commande en tant qu'administrateur.

- Passer en mode statique:
  1. Noter les paramètres réseaux: `ipconfig /all`.
  2. Désactiver le DHCP (2 possibilités):
     `netsh interface ip add address "Ethernet" <adr_ip> <netmask> [<def_gateway>]`
     `netsh interface ip set address "Ethernet" static <adr_ip> <netmask> [<def_gateway>]`

Attention ! Si on veut tester la connexion à [1.1.1.1] avec ping, il faut avoir mis un default gateway.

- Passer en mode dynamique:
  1. Ré-activer le DHCP avec: `netsh interface ip set address "Ethernet" dhcp`.
  2. Vérifier si le DHCP est bien activé: `ipconfig /all`.
- Ping dans un réseau interne:



Imaginons qu'on ait la configuration suivante:

- machine prof = 10.101.101.189
- réseau interne prof = 172.16.10.0
- netmask = 255.255.255.0
- VM prof = 172.16.10.20

il faut utiliser la commande `route add` pour ajouter un default gateway:

route add	<network>	mask	<netmask>	<default_gateway>
route add	172.16.10.0	mask	255.255.255.0	10.101.101.189

Remarque: il faut avoir désactivé le firewall (voir configuration via GUI – section 4.3).

2.2 Linux

> Clavier belge: `setxkbmap be`.
> Super-utilisateur: `su - root`.

- Passer en mode statique:
  1. Noter les paramètres réseaux: `ip a`.
  2. Désactiver le DHCP: `ip addr flush dev <interface_réseau>`
  3. Ajouter une adresse IP: `ip addr add <adresse_ip>/<netmask> dev <interface>`
     > ex: `ip addr add 192.168.30.20/24 dev enp0s3`

  Remarque: impossible de ping [1.1.1.1] si on ne met pas /24 après l'ip.
- Passer en mode dynamique:
  1. Ré-activer le DHCP avec: `dhclient -v <interface>`.
  2. Afficher les process DHCP: `ps aux | grep dhclient`.
- Ping dans un réseau interne: dans la situation suivante,
  - machine prof = 10.101.101.189
  - réseau interne prof = 172.16.10.0
  - netmask = 255.255.255.0
  - VM prof = 172.16.10.20

  il faut utiliser la commande `ip route add` pour ajouter un default gateway:

ip route add	<réseau>	via	<default_gateway>	dev	<interface>
ip route add	172.16.10.0/24	via	10.101.101.189	dev	enp0s3

  Attention au /24.

3 Changer les paramètres via les fichiers de configuration

- On n'utilise les fichiers de configuration **que** dans les systèmes linux. Les options que l'on cherche à changer se trouvent dans le document: */etc/network/interfaces*. Commandes utiles:
  - `cat /etc/network/interfaces`: affiche le contenu du fichier.
  - `nano /etc/network/interfaces`: ouvre l'éditeur nano pour modifier le fichier.
  - `cp /etc/network/interfaces /etc/network/interfaces.sav`: copie le fichier (au cas où).
  - `man interfaces`: affiche la documentation relative à */etc/network/interfaces*.
- Configuration:

Configuration Dynamique	**Configuration Statique**

Dans *primary network interface*, mettre:
`auto <interface>`
`iface <interface> inet dhcp`
	Dans *primary network interface*, mettre:
	`auto <interface>`
	`iface <interface> inet static`
	`address <adresse_ip>`
	`gateway <default_gateway>`

Pour l'IPv6, 2 possibilités:
– `iface <interface> inet6 dhcp`
– `iface <interface> inet6 auto`
	Pour l'IPv6, mettre:
	`iface <interface> inet6 static`
	`address <adresse_ip>`
	`gateway <default_gateway>`

Remarques:

- souvent, <interface> = `eth0` ou `enp0s3`.
- le default gateway est optionnel.
- l'adresse IP est sous la forme: 192.68.2.7/24.

- Lorsque la configuration est terminée, utiliser la commande: `systemctl restart networking`, pour redémarrer le service réseau. Si il y a des erreurs, utiliser: `journalctl -xe`, pour obtenir plus d'informations.
- Au lieu d'utiliser la commande: `systemctl restart networking`, on peut utiliser la commande: `reboot`, qui sert à redémarrer le système. On peut également redémarrer uniquement une interface avec: `ifdown <interface>`, et: `ifup <interface>`. La commande: `ifquery <interface>`, sert alors à afficher les paramètres liés à cette interface.
- Dans l'idéal, il faut d'abord utiliser la commande: `systemctl restart networking`, pour redémarrer le service réseau pour ensuite redémarrer le système avec: `reboot`.

4 Configuration réseau via l'interface graphique

4.1 Linux Mint

- Vérifier/noter les paramètres réseau (*mint cinnamon*):
  1. dans le menu en bas à gauche, taper *network* dans la barre de recherche
  2. sélectionner *network* (**pas** *network connections*)

  > Si le clavier ne correspond pas, taper la commande: `setxkbmap be`, dans le terminal.

- Configuration statique:
  1. dans le menu en bas à gauche, taper *network* dans la barre de recherche
  2. sélectionner l'app *network connections*
  3. double-clicker sur *wired connection 1*
  4. sélectionner le menu *IPv4 settings* en haut à droite

4.2 Linux Kali

- Vérifier/noter les paramètres réseaux:
  1. Dans le menu de gauche (en bas), clicker sur le menu *Show Applications*.
  2. En haut, dans le barre de recherche, taper *Settings* et clicker sur cette application.
  3. Dans le menu de gauche, clicker sur *Network*.
  4. Dans la section *Wired*, clicker sur la roue dentée.
  5. Dans la nouvelle fenêtre qui vient de s'ouvrir, dans le menu du haut , clicker sur *Détails*.
- Configuration:
  1. Dans le menu de gauche (en bas), clicker sur le menu *Show Applications*.
  2. En haut, dans le barre de recherche, taper *Settings* et clicker sur cette application.
  3. Dans le menu de gauche, clicker sur *Network*.
  4. Dans la section *Wired*, clicker sur la roue dentée.
  5. Dans la nouvelle fenêtre qui vient de s'ouvrir, dans le menu du haut, clicker sur *IPv4* ou *IPv6*.

4.3 Windows

- Afficher les paramètres réseaux:
  1. taper la commande: `ncpa.cpl`
  2. double-clicker sur *Ethernet* puis sur *Détails*
- Configuration statique:
  1. taper la commande: `ncpa.cpl`
  2. double-clicker sur *Ethernet* puis *Propriétés*
  3. double-clicker sur *Protocole internet version 4 (TCP/IPv4)*
  4. **Attention !** Ne pas sélectionner *Valider les paramètres en quittant.*
- Désactiver le firewall:
  1. utiliser la commande: `firewall.cpl`
  2. clicker sur *Paramètres avancés*, puis *Règles de trafic entrant*
  3. trouver la règle telle que:
     - nom = *Partage de fichiers et d'imprimantes (Demande d'écho - Trafic entrant ICMPv4)*
     - profil = *Privé, Public*
  4. click-droit sur cette règle, puis clicker sur *Activer la règle*

5 Windows Server

Attention !

- Il faut configurer les paramètres réseaux du Windows Server en mode statique.
- Si on configure le serveur DHCP, il faut que ce soit dans un réseau interne.
- Le DNS du Windows Server est sa propre adresse IP.

5.1 Initialisation

- Pour déverrouiller Windows Server, on utilise `Ctrl+Alt+Delete`. Pour le faire, dans le menu en haut à gauche de la fenêtre, clicker sur *Entrée*, puis sur *Clavier*, puis *Envoyer Ctrl-Alt-Del*.
- Pour installer les rôles (webserveur, dns, dhcp), on va:
  1. dans la fenêtre *Server Manager*, en haut à droite, clicker sur *Manage*, puis sur *Add Roles and Features*
  2. dans *Installation Type* et *Server Selection*, laisser les paramètres par défaut
  3. dans *Server Roles*, ajouter les rôles:
     - DHCP Server
     - DNS Server
     - Web Server (IIS)
  4. pour le reste, garder les paramètres par défaut (clicker sur *Next*), puis clicker sur *Install*.
  5. une fois l'installation terminée, clicker sur le drapeau en haut à droite, puis sur *Complete DHCP configuration*.
- Quelle configuration pour le client ?
  - Si on a un serveur DHCP, on le laisse en DHCP.
  - Sinon, on peut choisir entre le mettre en DHCP ou en statique. **Attention !** Il faut configurer le serveur manuellement quand même.

5.2 Configuration DHCP

- Pour configurer le serveur DHCP:
  1. dans la fenêtre *Server Manager*, en haut à droite, clicker sur *Tools*, puis sur *DHCP*
  2. dans la fenêtre *DHCP*, dans le menu de gauche, click-droit sur *IPv4*
  3. clicker sur *New Scope*
  4. nom du *Scope* = pas important
  5. choisir le range d'adresses ip à distribuer, ainsi que les plages d'exclusions
  6. dans *Configure DHCP Options*, sélectionner *Yes, I want to configure these options now*
  7. donner l'adresse du serveur DNS (= adresse Windows Server).
- Pour réserver une adresse IP pour une MAC address particulière, il faut:
  1. dans la fenêtre *DHCP*, dans le menu de gauche, click-droit sur *IPv4/Scope/Reservations*
  2. clicker sur *New Reservation*.

5.3 Créer un 1er site web

- Configuration DNS:
  1. **Forward Lookup Zone**
     (a) dans la fenêtre *Server Manager*, en haut à droite, clicker sur *Tools*, puis sur *DNS*
     (b) dans le menu de gauche de la fenêtre *DNS Manager*, en dessous du nom du serveur (Win-DI...), click-gauche puis click-droit sur *Forward Lookup Zone*
     (c) clicker sur *New Zone*
     (d) sélectionner *Primary Zone*, puis mettre le nom de domaine (ex: `greg.labo`)
     (e) puis continuer avec les paramètres par défaut.
  2. **Reverse Lookup Zone**
     (a) Ensuite, dans *DNS Manager*, click-gauche puis click-droit sur *Reverse Lookup Zone*
     (b) clicker sur *New Zone*

(c) sélectionner *Primary Zone*, puis *IPv4 Reverse Lookup Zone*
(d) dans *Network ID*, mettre le réseau dans lequel le serveur opère
(e) puis continuer avec les paramètres par défaut.

3. **Création d'un enregistrement A** (`greg.labo` → `172.10.0.20`)
   (a) dans la fenêtre *DNS Manager*, dans le menu de gauche, click-droit sur le nom de votre site (ex: `greg.labo`) et clicker sur *New Host (A or AAAA)*.
   (b) dans *Name*, on peut mettre ce qu'on veut, voir rien du tout
   (c) dans *IP address*, mettre l'adresse du serveur
   (d) cocher la case *Create associated pointer (PTR) record.*
4. **Création d'un enregistrement CNAME** (`www.greg.labo` → `greg.labo`)
   (a) dans la fenêtre *DNS Manager*, dans le menu de gauche, click-droit sur le nom de domaine (ex: `greg.labo`)
   (b) clicker sur *New Alias (CNAME)*
   (c) utiliser *www* comme *Alias Name*
   (d) au lieu d'écrire dans *FQDN for target host*, clicker sur *Browse*
   (e) sélectionner l'enregistrement A que vous avez créé précédemment.
5. **Remarque**:
   on n'est pas obligé de créer un enregistrement CNAME, mais (apparemment) c'est une bonne pratique de créer un enregistrement: `www.greg.labo`, qui pointe vers: `greg.labo`, ou l'inverse en fonction de l'enregistrement A.

- Configuration WebServer (**IIS**):

1. dans la fenêtre *Server Manager*, en haut à droite, clicker sur *Tools*, puis sur *Internet Information Services (IIS) Manager*
2. dans cette nouvelle fenêtre, dans le menu de gauche, click-droit sur *Sites*, puis clicker sur *Add Website*
3. remplir le formulaire:
   – *Site name* – pas important
   – *Physical path* – créer un nouveau dossier dans: `C:\inetpub\wwwroot\`
   – *IP address* – adresse du serveur
   – *Host name* – `www.greg.labo`
4. à l'endroit indiqué dans *Physical path*, créer un document *index.html*, ce sera la première page du site web.

- On peut lier un **deuxième** nom de domaine au site en allant dans:
  – *IIS Manager*, dans le menu de gauche, click-droit sur le nom du site web
  – clicker sur *Edit Bindings*.

  C'est utile pour que: `www.greg.labo`, et: `greg.labo`, affichent le même site.

5.4 Créer un 2ème site

- Ajouter un enregistrement CNAME $\implies$ affiche le site par défaut.
- **Lier** un nouvel enregistrement CNAME $\implies$ affiche le premier site.
- Créer un nouveau site $\implies$ affiche le nouveau site.

> Pareil que créer le premier site, excepté pour la reverse zone, c-à-d:
>
> 1. créer une *forward lookup zone*
> 2. **ne pas** créer une *reverse lookup zone*
> 3. créer un *enregistrement A*

4. potentiellement, créer un *enregistrement CNAME*.

5.5 Connection HTTPS

- Ajouter une entrée DNS: créer un enregistrement CNAME pour: `secure.greg.labo`.
- Créer un certificat auto-signé:
  1. ouvrir la fenêtre *IIS Manager*
  2. dans le menu de gauche, clicker sur le nom du server (= Win-DI...)
  3. dans le menu central (dans la section IIS), click-droit sur *Server Certificates*
  4. clicker sur *Open Feature*
  5. dans le menu de droite, clicker sur *Create Self-Signed Certificate*
  6. choisir un nom et sélectionner *Web Hosting*
- Ajouter la liaison sécurisée:
  1. dans la fenêtre *IIS Manager*
  2. dans le menu de gauche, click-droit sur le site pour lequel vous voulez la liaison sécurisée
  3. clicker sur *Edit Bindings*, puis sur *Add*
  4. dans *Type*, mettre `https`, puis mettre l'IP du serveur
  5. dans *Host Name*, mettre `secure.greg.labo`
  6. sélectionner le certificat créé précédemment.
- **Attention !** Il faut absolument mettre **https** dans le navigateur (`https://secure.greg.labo`).

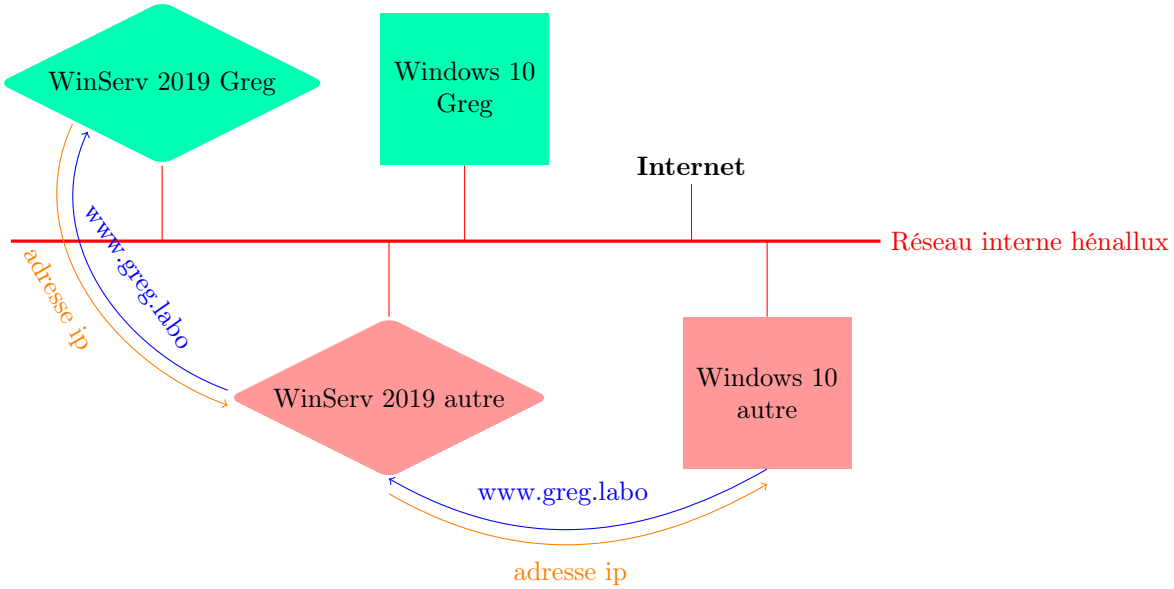
5.6 Serveur FTP

- Pour mettre en place un serveur FTP, il faut installer les rôles:
  - Web Server (IIS)
  - FTP Server
  - FTP Service
  - FTP Extensability

  Remarque: ils sont tous les uns en dessous des autres dans *Server Roles*.
- Créer un site FTP:
  1. ouvrir la fenêtre *IIS Manager*
  2. dans le menu de gauche, click-droit sur *site FTP*
  3. clicker sur *Add FTP Site*, puis mettre le nom du serveur
  4. créer un répertoire pour le site web (ex: `C:\inetpub\wwwroot\FTP-Folder`)
  5. indiquer l'adresse IP du serveur et désactiver le SSL
  6. mettre: *Authentification* = *Basic*, *Authorization* = *All users*
  7. cocher les cases *Read* et *Write*.
- Pour accéder au site FTP depuis le client, il faut:
  1. désactiver le firewall du serveur
  2. dans un navigateur ou un explorateur de fichiers, mettre: `ftp://<ip_serveur>/`, dans la barre de recherche
  3. se connecter avec:
     - login: `Administrator`
     - mdp: `Tigrou007`

5.7 Forwarder & Conditional Forwarder

- Topologie:



- **Attention !** Vu qu'on est connecté sur le réseau du laboratoire, il faut désactiver la fonction *serveur dhcp* des serveurs windows.
- Ajouter un *Forwarder* pour la connexion à internet:
  1. dans la fenêtre *Server Manager*, en haut à droite, clicker sur *Tools*, puis sur *DNS*
  2. dans la fenêtre, *DNS Manager*, dans le menu de gauche, clicker sur *Win-DI...* (= nom du serveur)
  3. click-droit sur *Forwarder*, puis clicker sur *Properties*
  4. clicker sur *Edit* et ajouter les adresses des serveurs DNS de l'école: 10.101.210.{8,9}.
- Connexion à un site web (`www.greg.labo`) hébergé sur le réseau interne avec un *Conditional Forwarder*:
  1. dans la fenêtre *Server Manager*, en haut à droite, clicker sur *Tools*, puis sur *DNS*
  2. dans la fenêtre, *DNS Manager*, dans le menu de gauche, click-gauche puis click-droit sur *Conditional Forwarders*
  3. clicker sur *New Conditional Forwarder*
  4. dans *DNS Domain*, mettre le nom de domaine auquel on veut accéder (ex: `greg.labo`)
  5. dans *IP addresses of the master servers*, ajouter l'adresse ip du serveur dns qui sait résoudre le nom de domaine (ici, l'ip de: WinServ 2019 Greg).

6 Wireshark

> Remarque: login kali = `root`, password kali = `toor`.

- Modifier les options: dans le menu en haut à gauche, clicker sur *Capture*, puis sur *Options*, puis sur *Options*. Décocher *Resolve MAC addresses* et cocher *Show capture information during live capture*.
- Filtrer des packets:
  - `arp`: pour ne capturer que des messages ARP.
  - `arp or icmp`: n'affiche que les messages ARP et les PING.
  - `udp.srcport == 68 or udp.srcport == 67`: messages DHCP.

- `dns`: pour les résolutions de nom de domaines.
- `ip.addr eq <adress_ip>`: uniquement les messages concernant cette IP.
- `ip.addr eq <Votre_IP> or ip.addr eq <IP_du_site>) and (tcp or dns)`: analyse session http (??)
- `http`: analyse session http.
- `tcp.port eq 443`: analyse session https.
- `tcp.port eq 80`: suivi de flux TCP (port 80 = http).
- `telnet`: limite l'affichage à la session telnet.
- `ssh`: limite l'affichage à la session ssh.

Remarque: il faut mettre les filtres en haut à gauche, où il est écrit: *Apply a display filter.*

7 SSH

7.1 Linux

- Pour le serveur ssh (= machine dont on prend le contrôle):
  1. Si nécessaire, installer le service ssh : `apt-get update && apt-get install ssh`.
  2. Démarrer le service ssh : `service ssh start`.
  3. Vérifier avec : `service ssh status`.
  4. **Attention !**
     - Si il n'y a pas d'autre utilisateur que `root`, il faut en créer un : `adduser <username>`.
     - Vérifier les comptes utilisateurs existants : `getent passwd {1000..60000}`.
- Pour se connecter au serveur ssh:
  1. Si nécessaire, installer nmap : `apt-get install nmap`.
  2. Vérifier que le serveur écoute bien sur le port 22 : `nmap -p 22 <ip_serveur>`.
  3. Pour se connecter, on utilise : `ssh <username>@<ip_serveur>`.

     > **Attention !** On ne peut pas se connecter en **root**.

7.2 Windows

- **Attention !** On ne peut pas se connecter en **root** directement avec ssh.
- Pour se connecter à un serveur ssh àpd la ligne de commande utiliser : `ssh <username>@<ip_serveur>`.
- Pour se connecter à un serveur ssh avec Putty:
  1. Ouvrir l'application *Putty*.
  2. Dans *Host Name (or IP address)*, mettre l'adresse du serveur.
  3. Dans *Port*, mettre: 22 (= port SSH).
  4. Clicker sur *Open*.

A Notation ligne de commande

Une commande est composée de 3 parties, la commande elle-même, les options et les arguments. Par exemple, pour ping l'adresse 8.8.8.8, on utilise la commande:

<commande>	[<options>]	<adresse_ip>	
ping		8.8.8.8	ping correctement
ping	-a	8.8.8.8	ping & résoud le hostname (dns.google)
ping	-6	<adresse_IPv6>	ping une adresse IPv6
ping	-6 -a	<adresse_IPv6>	ping une IPv6 & résoud le hostname

Notation utilisée pour la syntaxe de la ligne de commande:

Convention	**Description**
Texte sans chevrons/crochets/accolades	Éléments à recopier tel quel
< Texte à l'intérieur des chevrons >	Espace pour lequel il faut donner une valeur
[Texte à l'intérieur des crochets]	Éléments facultatifs
{ Texte à l'intérieur des accolades }	Choisir un des éléments

Remarque: quand on a lancé un programme par la ligne de commande, on peut utiliser: Ctrl+C, pour l'arrêter.

B Commandes réseaux

B.1 Linux

- Afficher des informations:
  - `ip a`: affiche les cartes réseaux & leurs protocoles.
  - `ip a show <interface>`: affiche le protocole configuré sur cette interface réseau.
  - `ip link show`: affiche des informations sur les interfaces réseaux.
  - `nslookup <nom_de_domaine>`: donne l'adresse IP du nom de domaine (ex: dns.google $\implies$ 8.8.8.8).
  - `nslookup <adresse_IP>`: résoud le nom de domaine (ex: 8.8.8.8 $\implies$ dns.google).
  - `ping <adresse_ip>`: vérifie la connection à une adresse ip.
  - `ifquery <interface>`: affiche des infos sur l'interface réseau.
  - `ps aux | grep dhclient`: affiche les process clients DHCP.
- Changement de la configuration réseau:
  - `ifup <interface>`: active l'interface réseau.
  - `ifdown <interface>`: désactive l'interface réseau.
  - `systemctl restart networking`: redémarre le service réseau.
  - `journalctl -xe`: affiche le détail des erreurs (à utiliser si le redémarrage du service réseau plante).
  - `ip addr flush dev <interface>`: supprime toutes les adresses ip de l'interface réseau.
  - `ip addr add <adresse_ip> dev <interface>`: ajoute une adresse ip à l'interface réseau.
  - `ip addr del <adresse_ip> dev <interface>`: supprime l'adresse ip de l'interface.
  - `ip route`: affiche le default gateway.
  - `ip route del default`: supprime le default gateway.
  - `ip route add default via <adresse_ip>`: ajoute le default gateway.

- `ip route add <network> via <default_gateway>`: crée une route statique.
- `ip route add <network> via <default_gateway> dev <interface>`: idem.
- `ip route del <network>`: supprime la route statique.
- `ip link set <interface> up`: active l'interface réseau.
- `ip link set <interface> down`: désactive l'interface réseau.
- `ip link set dev <interface> address <new_MAC_address>`: change la MAC address.
- `dhclient -v <interface>`: démarre un process client DHCP sur cette interface réseau.
- `pkill dhclient`: termine tous les process dhclient.

Remarque: ajouter: **-6**, aux commandes pour que ça s'applique à des adresses IPv6 aux lieu des IPv4.

- Commandes des 2 derniers labos:
  - `ip neigh show`: affiche la table ARP (= correspondance entre IP et MAC).
  - `ip neigh flush all`: efface la table ARP.
  - `dhclient -r -v eth0`: le serveur DHCP libère l'adresse IP (`-v` = affiche les logs).
  - `dhclient -v eth0`: le serveur DHCP renouvelle le bail.
  - `service ssh start`: démarre le service ssh.
  - `ssh <adresse_ip>`: établi une connexion ssh vers `<adresse_ip>`.
  - `service ssh stop`: arrête le service ssh.
  - `apt-get install telnetd`: installe le serveur Telnet.
  - `nmap -p 23 <ip_serveur>`: vérifie si le serveur écoute sur le port 23 (= port Telnet).
  - `telnet <ip_serveur>`: connection au serveur avec le protocole Telnet.
  - `cat /etc/shadow`: affiche les hash stockés sur la machine.
  - `ssh <ip_serveur>`: connection au serveur avec le protocole SSH[1].
    Remarque: impossible de se connecter en root.
  - `ssh <username>@<ip_serveur>`: connexion en `<username>` sur le serveur.
  - `adduser <username>`: ajoute un utilisateur.
  - `nc -nlvp <port>`: serveur de "chat" sur le port précisé.
  - `nc -nv <adresse_ip> <port>`: se connecte à l'autre machine pour le "chat".
  - `ncat`: comme `nc` mais plus moderne, possibilité de chiffrement.
  - `ssh -L 1234 :<ip_serveur_telnet> :23 remoteuser@<ip_serveur_ssh> -N`: créé un tunel ssh pour se connecter à un serveur telnet.
  - `telnet localhost 1234`: connection au serveur telnet (voir commande précédente).

B.2 Windows

- Afficher des informations:
  - `ipconfig [/all]`: affiche la configuration TCP/IP complète pour tous les adaptateurs.
  - `ping <adresse_ip>`: vérifie la connexion à une adresse ip.
  - `route print`: affiche la table de routage.
  - `neth interface show interface`: affiche les noms et statuts des interfaces réseaux.
- Changement de la configuration réseau:
  - `netsh interface ip set address "Ethernet" static <adresse_IP> <netmask> [<default_gateway>]`: passe en configuration statique et change les paramètres.

[1] SSH essaie de se connecter avec le même `username` que celui qui est utilisé sur la machine.
Exemple: machine.username = greg, commande = `ssh <ip_serveur>`, commande équivalent = `ssh greg@<ip_serveur>`

- `netsh interface ip add address "Ethernet" <adresse_ip> <netmask>`: ajoute une adresse ip supplémentaire.
- `netsh interface ip delete address "Ethernet" <adresse_ip>`: supprime l'adresse ip.
- `netsh interface ip set dns "Ethernet" static <adresse_ip>`: change le dns.
- `netsh interface set interface "Ethernet" enable`: active l'interface réseau.
- `netsh interface set interface "Ethernet" disable`: désactive l'interface réseau.
- `route add [-p] <network> mask <netmask> <default_gateway>`: ajoute un default gateway vers un réseau (= ajouter une porte d'entrée vers un réseau).
- `route delete <network>`: suppression de la route (default gateway) vers ce réseau.
- `netsh interface ip set address "Ethernet" dhcp`: active le DHCP.
- `netsh interface ip set dns "Ethernet" dhcp`: active le DHCP pour le DNS.

- Pour les adresses IPv6:
  - `netsh interface ipv6 set address "Ethernet" <adresse_ipv6>`: modifie l'adresse ipv6.
  - `netsh interface ipv6 add address "Ethernet" <adresse_ipv6>`: ajoute une adresse supplémentaire.
  - `netsh interface ipv6 delete address "Ethernet" <adresse_ipv6>`: supprime l'adresse ipv6.
  - `ping -6 <adresse_ipv6>`: teste la connexion à l'adresse ipv6.
- On ne reçoit pas d'adresse IPv6 du serveur DHCP de l'école. Si on veut en utiliser une, on doit utiliser l'adresse suivante:

  `2001:DB8:ACAD::X/64`

  où: **X**, est remplacé par le numéro sur l'étiquette du PC.

C Théorie - Configuration réseau

C.1 Machines virtuelles - configuration réseau

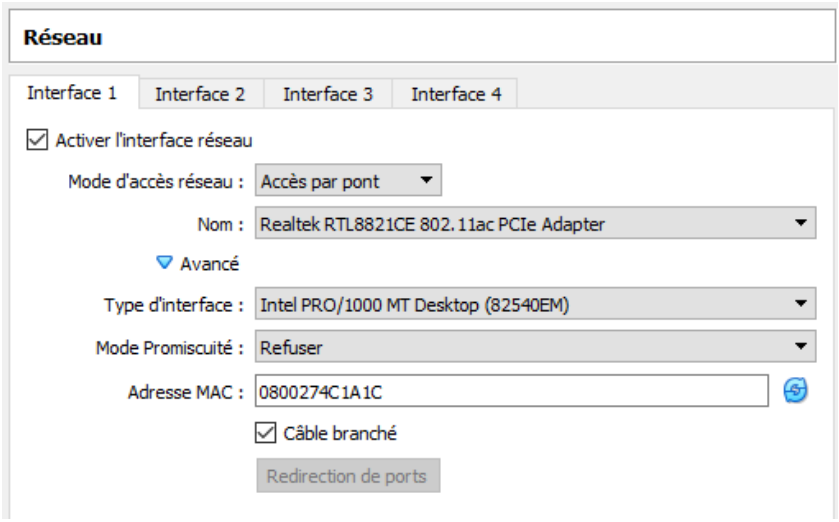
Les différents paramètres de configuration de la carte réseau de VirtualBox sont:

- **NAT** (Network Address Translation): l'accès au réseau se fait à partir de l'adresse IP de la machine hôte.

  > Remarque: quand *un réseau* fonctionne en NAT, chaque machine dans le réseau privé possède une adresse privée. Le routeur est le seul à avoir une adresse publique qu'il utilise pour communiquer sur le réseau public (internet).

- **Accès par pont** (bridge): la machine virtuelle "invitée" (dans VirtualBox) passe par dessus la machine virtuelle "hôte" pour se connecter directement à la carte réseau de l'ordinateur et ainsi obtenir sa propre adresse IP.
- **Réseau interne**: réseau virtuel isolé sur lequel les machines virtuelles communiquent entre elles. Les VM ne peuvent pas se connecter ni réseau extérieur, ni à l'hôte.
- **Réseau privé hôte**: réseau interne dans lequel les machines virtuelles peuvent communiquer entre elles et avec la machine hôte mais pas avec l'extérieur.

Quelle configuration faut-il pour être **joignable de l'extérieur** ? *Accès par pont.*
Quelle configuration utiliser pour **connecter 2 VM** exécutées sur le même ordinateur ? *Réseau interne (?)*
Expliquer les **options de configuration** ci-dessous:



- **Nom**: carte réseau.
- **Type d'interface**: pilote informatique (driver) - programme permettant la communication entre l'OS et un périphérique (ici, la carte réseau).
- **Mode Promiscuité**: configuration de la carte réseau, qui permet à celle-ci d'accepter tous les paquets qu'elle reçoit, même si ceux-ci ne lui sont pas adressés.
- **Adresse MAC**: aussi appelée *adresse physique*, est un identifiant physique unique au monde stocké dans une carte réseau.
- **Câble branché**: utile pour simuler qu'aucun câble n'est branché à cette interface. Si la case est décochée, la VM ne sera plus joignable.
- **Redirection de ports**: idk.

C.2 Paramètres d'un réseau hôte

- **Adresse IP statique**: adresse logique IP (V4) fixe, répartie sur 4 octets.
- **Masque de sous réseau**: masque distinguant les bits d'une adresse IPv4 utilisés pour identifier le sous-réseau de ceux utilisés pour identifier l'hôte.

  > Exemple:
  >
  > – adresse réseau: 192.57.194.0
  > – adresse hôte: 192.57.194.12
  > – masque de sous-réseau: 255.255.255.0

- **Adresse IP dynamique**: adresse IP reçue dynamiquement via un serveur extérieur et renouvelée à intervalles réguliers.
- **Adresses IP supplémentaires**: adresses IP utilisées en plus de celle de base.
- **Serveur DNS**: serveur qui permet de faire le lien entre adresse IP et FQDN (Fully Qualified Domain Name).

  > Exemple:
  >
  > – Domaine du site internet: google.com
  > – Adresse IP du domaine: 216.58.204.110

- **Host Name**: nom d'hôte Local d'une machine et/ou nom d'hôte DNS.
- **Passerelle par défaut**: adresse de l'élément qui va permettre la discussion entre deux hôtes, par exemple un routeur, serveur ou une boxe internet. Équivalent d'un panneau "toutes directions", vers lequel sont dirigés les paquets dont le chemin vers la destination est inconnu.
- **Passerelles supplémentaires**: passerelles correspondant au chemin vers des réseaux connus.
- **Firewall**: dispositif qui autorise/interdit le trafic réseau sur base de certains critères.
- **Carte réseau**: périphérique permettant de connecter son ordinateur à un réseau.
  Propriétés:
  - **Mac Address**: adresse matérielle d'une interface Ethernet. Sur 48 bits, notée en hexadécimal. La première partie correspond au constructeur.
  - **Duplex**: canal de communication qui transporte l'information dans les deux sens (bidirectionnel). Un canal qui transporte l'information dans un seul sens est appelé simplex (monodirectionnel).
    * **Full-duplex**: l'information peut être transportée simultanément dans les deux sens.
    * **Half-duplex**: l'information est transportée dans un sens à la fois (comme des talkie-walkies).
  - **Débit**: nombre maximal de b/secondes qui peuvent circuler par une interface.

  Remarque: b/seconde = bits/seconde, alors que: B/seconde = bytes/seconde (byte = octet).

C.3 Liste d'enregistrements DNS

Enregistrement	Signification du nom	Fonction
A	Adresse IPv4	nom de domaine $\Longrightarrow$ IPv4
AAAA	Adresse IPv6 (4× la taille d'une IPv4)	nom de domaine $\Longrightarrow$ IPv6
CNAME	Nom Canonique	nom de domaine $\Longrightarrow$ nom de domaine
MX	Mail Exchanger	nom de domaine $\Longrightarrow$ liste de serveurs (= hôtes)

Exemples:

- Type A: `www.example.com` → `192.168.1.32`
- Type AAAA: `www.example.com` → `2a02:a03f:417b:3300:3c88:a5ee:451b:82ca`
- Type CNAME: `www.hotmail.com` → `www.outlook.com`
- Type MX:
  - mail: `greg@example.com`
  - nom de domaine: `example.com`
  - hôtes: `server1.example.com`, `serveur2.example.com`, etc.

Remarque: les hôtes dans les enregistrements de types MX *doivent* aussi avoir un enregistrement de type A (ou AAAA) sur le même serveur DNS (pas de CNAME).

C.4 Serveur FTP/TFTP

- **Serveur FTP** (File Transfer Protocol):
  Protocole de partage de fichiers *en clair*, sur un réseau TCP/IP. L'authentification est requise mais peut aussi être anonyme (si le serveur l'autorise). On utilise FTPS pour une transmission sécurisée.
- **Serveur TFTP** (Trivial File Transfer Protocol):
  Protocole *simplifié* de transfert de fichiers, fonctionne en UDP. Il est souvent utilisé dans les systèmes de démarrage PXE), les configurations d'équipement de réseau, d'importation/exportation, etc.

D Examen blanc

Durée de l'examen : 2h
Machines : WinServ (192.168.0.1), Kali (192.168.0.10), Windows (client DHCP) — masque = 255.255.255.0

D.1 Windows Server

Mettre en place les services suivants:

- Serveur DNS : domaine = `domaine[VotreNom].be`.
- Serveur WEB : site = www.
- Serveur DHCP.

1. Configurer les paramètres réseaux en mode statique (section 4.3).
2. Installation des rôles (section 5.1).
3. Configuration serveur DHCP (section 5.2).
4. Configuration serveur DNS + serveur WEB (section 5.3).

D.2 Windows + Kali

Windows et Kali doivent pouvoir accéder au site.

1. Configurer les paramètres réseaux de Windows (section 4.3).
2. Configurer les paramètres réseaux de Kali (section 2.2 ou section 4.2).

D.3 Serveur SSH

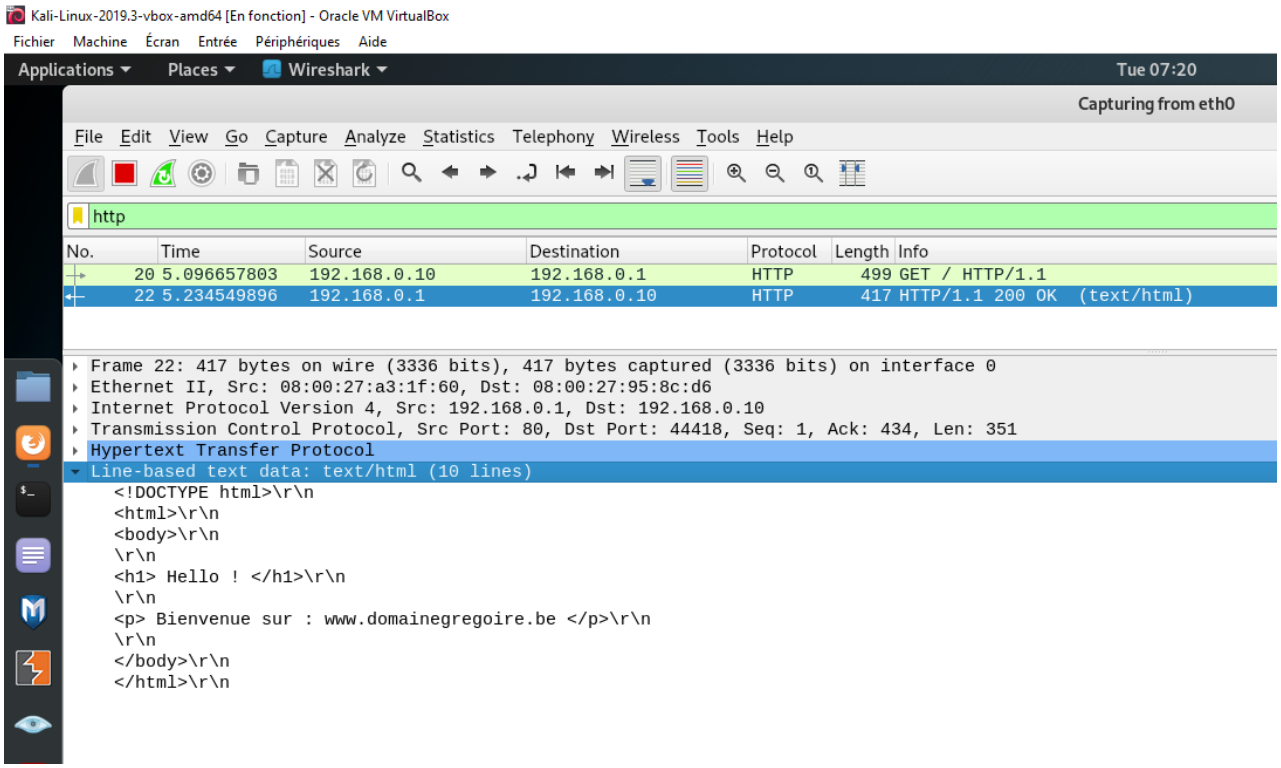
Kali = serveur SSH. S'y connecter avec Windows.

1. Activer le serveur SSH (section 7.1).
2. S'y connecter avec Windows (section 7.2).

D.4 Wireshark HTTP

Analyser le trafic entre Kali et le site, identifier les requêtes HTTP.

1. **Attention !** La partie Wireshark ne contient que les filtres. Voir le labo correspondant pour l'utilisation du logiciel.


Kali-Linux-2019.3-vbox-amd64 [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Applications Places Wireshark Tue 07:20
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
20 5.096657803 192.168.0.10 192.168.0.1 HTTP 499 GET / HTTP/1.1
22 5.234549896 192.168.0.1 192.168.0.10 HTTP 417 HTTP/1.1 200 OK (text/html)
Frame 22: 417 bytes on wire (3336 bits), 417 bytes captured (3336 bits) on interface 0
Ethernet II, Src: 08:00:27:a3:1f:60, Dst: 08:00:27:95:8c:d6
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.10
Transmission Control Protocol, Src Port: 80, Dst Port: 44418, Seq: 1, Ack: 434, Len: 351
Hypertext Transfer Protocol
Line-based text data: text/html (10 lines)
<!DOCTYPE html>\r\n
<html>\r\n
<body>\r\n
\r\n
<h1> Hello ! </h1>\r\n
\r\n
 Bienvenue sur : www.domainegregoire.be \r\n
\r\n
</body>\r\n
</html>\r\n