Réseau informatique 1 – Synthèse

Table des matières

Les différents paramètres réseaux d'un hôte :

- Adresse IP statique

Une adresse logique IP (V4) qui est fixe. Peut être fournie par un FAI éventuellement. Répartie sur 4 octets

- Masque de sous réseau

Masque binaire pour une adresse IP permettant de séparer la partie réseau de la partie hôte

- Adresse IP dynamique

Adresse IP reçue dynamiquement via un serveur extérieur et renouvelée à intervalles réguliers

- Adresses IP supplémentaires

Adresse IP qu'une interface utilise en plus de celle de base

- Serveur DNS

Adresse IP Serveur qui permet de faire le lien entre adresse IP et FQDN, nom de domaines via le protocole DNS

- Host Name

Nom d'hôte Local d'une machine et/ou nom d'hôte DNS

- Passerelle par défaut

Passerelle / routeur vers laquelle seront dirigés les paquets dont le chemin vers la destination est inconnu. L'équivalent d'un panneau "toute directions"

- 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 :
  - Mac Address

Adresse matérielle d'une interface Ethernet. Sur 48bits. La première partie correspond au constructeur. Se note en hexadécimal

  - Duplex :

Half : donnée circulent sur une paire de fils en UP/DOWN -> 100Mb total
Full : une paire de fils pour les données en UP, une autre pour en DOWN -> 100Mb / direction

  - Débit :

Nbre maximal de b/secondes qui peuvent circuler par une interface

Les différents modes réseaux :

1. Mode réseau NAT (Network Address Translation) :

Utilisation : Si vous avez une seule machine virtuelle (VM) et que vous voulez télécharger des applications, effectuer des mises à jour et naviguer sur Internet depuis cette VM.

2. Accès par pont (Bridge Mode) :

Utilisation : Si vous souhaitez que votre VM agisse comme un serveur web, apparaissant sur le réseau avec sa propre adresse IP distincte et étant accessible depuis l'extérieur.

3. Réseau interne (Internal Network) :

Utilisation : Utilisation de plusieurs VM pour simuler des réseaux privés qui ne sont pas accessibles depuis l'extérieur ni depuis la machine hôte. Cela crée un environnement isolé pour les machines virtuelles.

4. Réseau NAT (Network Address Translation) étendu :

Utilisation : Semblable au mode NAT, mais avec la possibilité pour plusieurs VM de communiquer entre elles, ce qui n'est pas possible avec le mode NAT classique. Utile si vous avez plusieurs VM qui ont besoin de s'entendre.

5. Réseau privé d'hôte (Host-only Network) :

Utilisation : Similaire au réseau interne, mais permet également à la VM de communiquer avec la machine hôte. Cela crée un réseau isolé entre la machine hôte et les machines virtuelles, sans accès direct à l'extérieur.

Commandes configuration réseaux sous Windows :

Tour ce qui est en bleu sera la couleur des commandes.

Tout ce qui est en rouge peut être différents en fonction de chaque utilisateur.

Tout ce qui est en vert est optionnel.

Tout ce qui est en orange est un bouton ou une utilisation dans une fenêtre graphique.

Sous Windows en interface graphique, si on recherche ncpa.cpl on peut trouver dans la connexion réseau les différentes méthodes de connexion réseau, si on clic droit sur un des méthodes on peut aller dans propriétés ensuite on peut voir différents types de connexion dont le IPv4, si on clic dessus et qu'ensuite on clic sur propriétés on peut configurer si on veut avoir un IP statique ou dynamique (DHCP).

On peut aussi accéder au firewall avec la recherche firewall.cpl par la suite on doit cliquez sur paramètre avancé où on pourrait trouver les réglés qui n'interdisent où pas qu'une connexion réseau se fassent.

Voir la configurations réseaux :

- Ipconfig
- ipconfig /all
- ipconfig / ?
- route print
- ipconfig /release = libère l'adresse ip actuelle.
- ipconfig /renew = demande une nouvelle adresse IP au serveur DHCP.

Configuration des paramètres réseaux :

Configurer une adresse statique sur une interface :

- netsh interface show interface = on peut voir le nom et le statut de notre interface.
- netsh interface ip set address « Ethernet » static IPv4_address netmask default_gateway = cette commande sert à définire une adresse ipv4 statique pour l'interface Ethernet (si dans la commande on change le ip par ipv6 cela changerait l'adresse ipv6).
- netsh interface ip add address « Ethernet » IPv4_address netmask default_gateway = pour modifier l'adresse IP.
- netsh interface ip delete address « Ethernet » IPv4_address = cette commande sert à effacer une adresse ip.

Configuration dynamique :

- netsh interface ip set address «Ethernet » dhcp = cette commande permet de se mettre ne mode adresse dynamique (elle est généralement suivi de la commande ipconfig /release et la commande ipconfig /renew).

Serveur DNS :

- netsh interface ip set dns « Ethernet » static IPV4_address = cette commande permet de changer l'adresse IPv4 d'un serveur DNS en statique.
- netsh interface ip add dns « Ethernet » 8.8.8.8 = cette commande permet d'ajouter un serveur DNS.
- netsh interface ip set dns « Ethernet » dhcp = cette commande permet de configurer en mode DHCP l'adresse IPv4 d'un serveur DNS.
- netsh interface delete interface « Ethernet » = supprime l'interface (de préférence désactiver l'interface avant de la supprimer !).

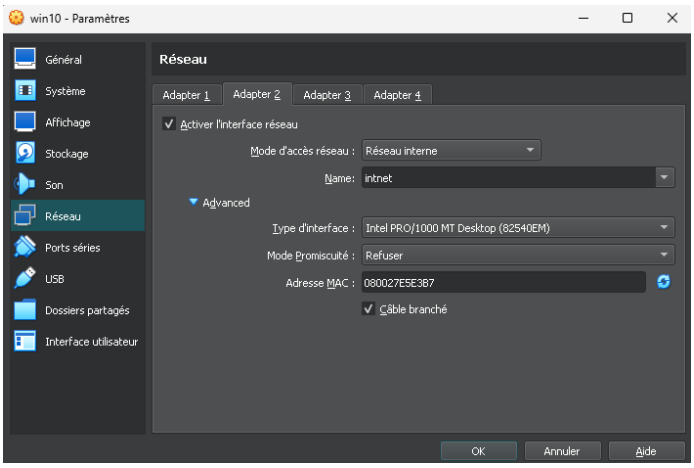
- Activer / désactiver une carte réseau :
- netsh interface set interface « Ehternet » enable
- netsh interface set interface « Ehternet » disable

supprimer/configurer le default gateway en IPv4 :

- route add -p 0.0.0.0 mask 0.0.0.0 192.168.1.1 = ajouter un nouveau gateway IPv4 (la commande route print sert à vérifier le gateway et le -p c'est pour dire si c'est une route persistante ou pas).
- route delete 0.0.0.0 = supprimer un gateway IPv4.

Ajouter une deuxième interface réseau sur une VM :

On peut ajouter une deuxième interface réseau en lui ajoutant une adresse MAC et en lui disant quel mode d'accès réseau être :



On peut voir si notre interface réseau est connecté avec la commande ipconfig /all qui nous montre les différents interface réseau dont celle qu'on vient de brancher, on peut aussi remarquer qu'elle est sur DHCP :

```
Physical Address. . . . . . . . . : 08-00-27-9E-B3-AB → carte sur le réseau interne

DHCP Enabled. . . . . . . . . . . : Yes → vérifiez que votre carte est bien en DHCP
```

Commandes configuration réseaux sous Linux :

Sous Linux en interface graphique, on peut aussi trouver dans une application qui s'appelle Network Configuration ou configuration réseau, une configuration statique ou dynamique pour notre connexion réseau.

Pour le firewall sou linux on recherche configuration du pare feu (Firewall Configuration).

Commandes basiques :

- apt-get update = installer des mis à jour (il est conseillé de l(utiliser pour la commande suivante).
- apt-get install resolvconf = permet d'installer le paquet resolvconf (qui nous servira pour les commandes réseaux).
- apt-get install network-manager = permet d'installer Network Manger qui gère les interfaces et leurs configurations (en rajoutant la commande systemctl enable NetworkManager on peut le laisser tout le temps active, même au redémarrage).
- su - = se mettre en mode super utilisateur (mode root).
- dpkg-reconfigure keyboard-configuration ou setxkbmap be = mettre le clavier en clavier Belge.

Commandes configuration réseaux :

- ip addr show = cette commande nous permet de voir les cartes de notre serveur et également les adresses IP (ip -6 addr show pour l'IPv6).
- ip link show = vous montre votre adresse MAC et tout le niveau deux de votre carte.
- ip route show = vous montre les route configurer sur le serveur et donc aussi celui du default geteway.
- cat /etc/resolv.conf = vous permet de voir le contenu du fichier resolv.conf qui ce trouve dans le dossier etc, et qui sert à vous montrer le serveur DNS que vous utilisez et le domaine de recherche.

Configuration des paramètres réseau via les fichiers de configuration :

Dans le fichier avec la racine /etc/network/interfaces, on peut faire en sorte que la configuration soit persistante c'est-à-dire qui reste après le reboot d'un serveur, comme se fichier est important et qu'il ne faut pas le modifier à la légère, il est préférable d'exécuter la commande cp /etc/network/interfaces /etc/network/interfaces.serv pour pouvoir copier le contenu du fichier et modifier le fichier sans prendre de risque.

Si on utilise la commande nano /etc/network/interfaces on peut ouvrir le fichier et le modifier.

L'auto devant chaque nom d'interface veut dire que l'interface est fonctionnelle, si on veut désactivé l'une des interfaces on peut tout simplement les mettre en commentaire en placent un # devant.

Exemple d'utilisation en adresse statique et dynamique (ne pas oublier d'effectuer un reboot ou le redémarrage de votre machine, un init 0 l'arrêtera, ou alors un systemctl restart networking qui redémarrera que le réseau) :

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static
        address 192.168.1.2
        netmask 255.255.255.0
        gateway 192.168.1.1
        dns-nameserver 8.8.8.8 8.8.4.4_
```

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet dhcp
```

Avec la commande journalctl -xe on peut voir la liste des actions qu'à fait nos interfaces.

La désactivation/activation/affichage d'une interface :

- ifdown enp0s3 = vous permet de désactiver l'interface souhaitez (dans ce cas-là l'interface enp0s3).
- Ifup enp0s3 = vous permet d'activer une interface.
- Ifquery enp0s3 = vous permet de voir la configuration de l'interface enp0s3(cette commande est liée au fichier /etc/network/interfaces et donc ne peut-être utiliser sans se système).

Changement de hostnme :

Dans le fichier /etc/hostname on peut trouver notre hostname (nom d'utilisateur) actuelle et le changer en mode statique.

On peut aussi le changer à chaud (ça veut dire non-persistant) avec la commande hostnamectl set hostname nomDUtilisateur.

Pour voir si ça à fonctionner on peut taper hostnamectl qui nous montre d'autres informations dont le nom d'utilisateur actuelle, il y de forte chance qu'il n'a pas changer il faut donc utiliser la commande hostname nomDUtilisateur (il faut utiliser le nouveau nom d'utilisateur).

Configuration des paramètres réseaux en ligne de commande :

Les commandes non persistantes :

Ajout/suppression d'adresse IP :

- ip addr flush dev enp0s3 = permet de supprimer toutes les configurations d'adresse IPv4 sur l'interface (pour l'IPv6 on utilise la commande ip -6 addr flush dev enp0s3).
- ip addr add 192.168.30.20/24 dev enp0s3 = permet d'ajouter une adresse supplémentaire (un alias).
- ip addr del 192.168.30.20/24 dev enp0s3 = permet de supprimer une adresse IP.

Commandes DHCP :

- dhclient -v enp0s3 = mets l'interface en mode DHCP (à exécuter après la commande ip addr flush dev enp0s3).
- ps aux | grep dhclient = permet de rechercher et afficher les processus en cours d'exécution et qui sont liés à DHCP.
- pkill dhclient = permet de (tuer) d''arrête tous les processus en cours d'exécution associés au programme dhclient.

Commandes Hostname :

- hostname NouveauHostname = la commande hostname avant le nom d'un utilisiateur permet d'avoir un hostname temporaire.

Commandes Default Gateway :

- ip route del default = supprime le default gateway (si on ajoute un -6 après l'ip ça sera pour l'IPv6).
- ip route add default via 172.16.10.1 = permet d'ajouter un default gateway(un -6 après l'ip = IPv6).

Tous Gateway (pas forcément le default):

- ip route add 192.168.1.0/24 via 172.16.10.40 dev enp0s3 = ajout d'une adresse et spécifications de la passerelle par la quelle doivent passer les paquets destiné à 192.168.1.0.
- ip route del 192.168.1.0/24 = supprimer la passerelle (pas forcément celle par défaut)
- ip link set enp0s3 up = permet d'activer l'interface enp0s3 (ip link set enp0s3 down permet de désactivé l'interface enp0s3).
- ip link set dev enp0s3 address aa:bb:cc:aa:bb:cc = permet de changer le MAC adresse sur une interface.

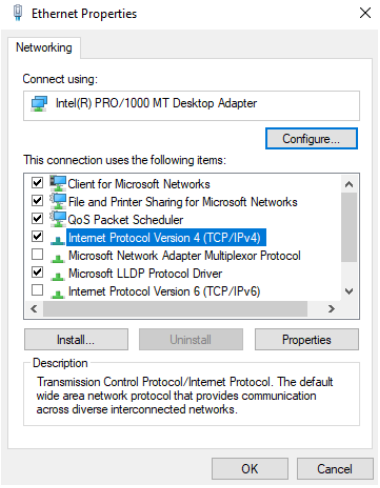
Commande DNS :

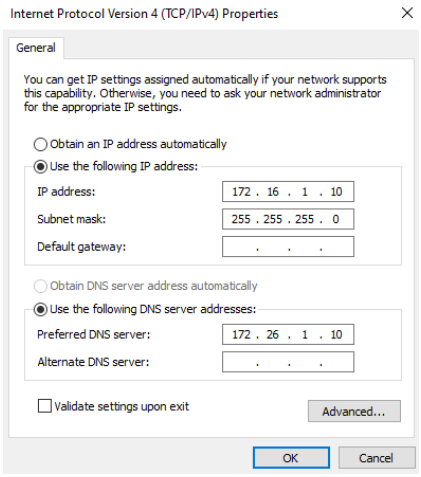
nslookup = permet de voir les l'adresse DNS et les domaines qui y sont liés (il faut installer dnsutils avec la commande apt-get install dnsutils pour pouvoir l'utiliser).

Configuration DNS, DHCP et web serveur (IIS) sur Windows serveur :

Dans la manipulation 5 on à installer Windows serveur 22 pour faire des services DNS, DHCP et web serveur (IIS) (**Ne pas oublier de mettre les VM en réseau interne**).

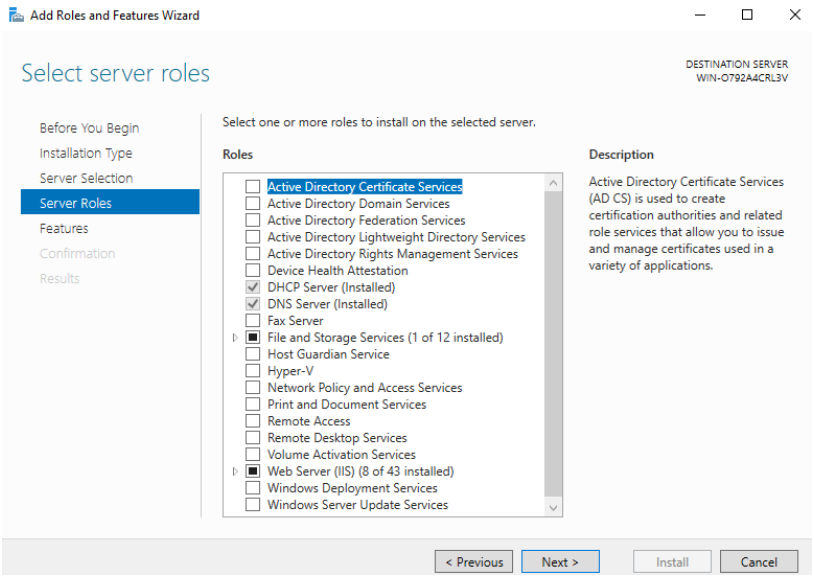
Pour ce faire on doit tout d'abord changer l'adresse IP du serveur dans ncpa.cpl aller dans les propriétés de l'interface (en général c'est Ethernet) on désactive l'IPv6 car on n'en a pas besoin et on clic sur l'IPv4 pour pouvoir changer l'adresse IP.





On peut changer les IP comme on le souhaite mais pour la manip on à dû changer l'adresse IP, le masque de sous-réseau et l'adresse DNS comme dans les consignes.

Par la suite on à installer un serveur DHCP,DNS et IIS en appuyant sur Manage -> Add Roles and Features, esuite on à une fenêtre où on peut passer directement (donc sans changer d'autre paramètres entre temps) à l'étape dû Server Roles où on à sélectionner les serveurs qui nous intéressent (DHCP Server,DNS Server,Web Server (IIS)) :



Après avoir fini de sélectionner, on passe aussi tous les étapes d'après jusqu'à appuyer sur install où on aura un téléchargement de quelques minutes, après avoir fini le téléchargement il y a juste le DHCP où on doit finaliser le téléchargement en appuyant sur le drapeau en haut à droite, même chose vous passer tout et vous terminer par Commit.

Configuration DNS :

Si on ouvre DNS dans Tools en haut à droite et qu'on clic sur le serveur puis sur le Forward Lookup Zones, on pourra créer une « zone » Forward c'est donc quand on « traduit » un nom de domaine en adresse IP, à l'inverse si on crée une zone dans le Reverse Lookup Zones on traduirait les adresses IP en nom de domaine.

Donc cela veut dire que les deux étapes sont importantes, pour commencer avec le Forward Lookup Zones on clic droit dessus puis on crée une nouvelle zone avec New Zone, ensuite on garde les paramètres déjà mise et on appuye sur Next jusqu'à arriver à l'endroit où on va choisir le nom de notre zone dans mon cas j'ai mis student.labo.

On ajoute aussi une nouvelle zone dans la Reverse Lookup Zones de la même manière que la Forward, et un moment on va nous demander de mettre notre sous-réseau dans mon cas c'était 172.16.1 (il y a un chiffre qui maque car c'est un sous-réseau en classe C masque de sous-réseau 255.255.255.0).

Ensuite il faut ajouter un Host dans le student.labo (donc clic droit New Host(A or AAA)) puis vous aurait une fenêtre où on vous demande le nom de domaine et l'adresse IP, on doit d'abord mettre le nom de domaine de notre serveur (moi c'était winserver) et l'adresse IP du serveur (pour moi c'était 172.16.1.10) et ensuite on coche Create associated pointer.

Maintenant on peut ajouter notre hôte linux en refaisant la même chose donc ajouter un Host et donner un nom de domaine (Dans mon cas linux) et l'adresse IP (l'adresse IP n'est pas encore attribuer à l'hôte donc vous pouvez mettre une adresse IP que vous allez remettre sur le linux, moi c'était 172.16.1.20) et on coche le PTR.

Avec la commande nslookup linux.student.labo (sachant qu'en rouge c'est le nom de domaine de mon hôte) on peut voir si notre serveur DNS est fonctionnel, la première partie du résultat est notre serveur qui recherche et la deuxième partie est le nom de domaine et l'adresse IP qu'on cherche.

Après avoir fait tout ça on peut commencer à démarrer notre hôte (pour ma part c'est une mint) et on lui configure l'adresse 172.16.1.20 et le DNS de notre server qui est 172.16.1.10 (on n'oublie pas de désactiver le IPv6 ou de le mettre en ignorer) et on peut de préférence faire un nslookup.

Maintenant on veut créer un Alias ou un CNAME qui « traduit » comme avec le nom de domaine avec l'adresse IP mais cette fois en dirigeants de l'alias (donc une façon plus courte de définir un nom) au nom de domaine.

Pour se faire on doit retourner dans le DNS et on fait comme quand on voulait créer notre Host, mais cette fois on crée un Alias.

On choisir d'abord le nom de l'alias pour mon cas c'est www ensuite on appuye sur Browse pour aller chercher le nom de domaine vers le quelle vas se dirige notre alias (winserver).

Il est préférable d'utiliser nslookup après chaque modification du DNS sur le serveur mais aussi sur le client.

Configuration DHCP :

La configuration DHCP commence également dans Tools puis dans DHCP, on trouve le serveur en cliquant dessus on trouve l'IPv4 et l'IPv6, vue qu'on travaille avec du IPv4 on doit faire un clic droit dessus et faire un New Scope.

Un Scope c'est une plage d'adresse dont va piocher le serveur DHCP pour distribuer les adresses aux hôtes.

Après avoir cliquer dessus on doit d'abord donner un nom à notre scope qui pour mon cas va se nommer MonScope, ensuite on va pouvoir noter la plage d'adresse de distribution pour mon cas c'est la plage (Start IP address : 172.16.1.15) à l'adresse (End IP address : 172.16.1.150) ensuite on n'oublie pas de mettre le masque de sous-réseau.

Pour ce qui est de l'étape d'après on peut choisir une plage qui se trouve dans la plage qu'on vient de citer et qui n'est pas à distribuer, dans mon cas j'ai mis la plage 172.16.1.100 à 172.16.1.120 et aussi la plage 172.16.1.130 à 172.16.1.140.

Pour l'étape suivant c'est le bail de nos plages d'adresses qu'on vient de citer donc c'est la durée pendant la quelle on peut garder ces plages-là, pour ma part j'ai laissé par défaut (donc à 8 jours).

Ensuite on nous demande si on veut configurer le Scope qu'on vient de faire maintenant, la réponse c'est Yes donc on laisse comme ça et on Next.

On peut dans cette étape choisir de mettre la passerelle par défaut, dans mon cas je n'en ai pas besoin mais j'ai quand même mis le 172.16.1.1.

Pour la suite on mets le nom de domaine de notre serveur DNS pour mon cas c'est le student.labo, et on peut voir qu'il y a déjà l'adresse IP de notre serveur DNS (172.16.1.10).

L'étape d'après on peut la passer, mais sachez que les serveurs WINS ressemble fortement au serveur DNS mais les serveurs WINS sont moins courants.

Ensuite on termine par activer le Scope en laissant sur Yes.

On doit maintenant ajouter notre client linux mint dans notre DHCP, pour se faire on doit d'abord aller voir la MAC adresse qui après une commande ip a se trouve après link/ether et qui est avant le brd (broadcast).

Ensuite on va dans notre scope et on va dans Reservation pour faire un clic droit dessus et faire une nouvelle réservation.

On donne un nom à notre réservation (dans mon cas c'est linux mint), on note l'IP adresse de notre client, on note le MAC de notre client (on ne doit pas mettre les :) et on ne touche pas au Supported types (on le laisse sur Both).

On redémarre notre client et il est sensé être automatiquement sur DHCP et avec l'adresse qu'on lui a attribué.

Il est aussi possible de voir son fonctionnement avec Address Leases qui se trouve au même niveau que Reservations et qui contient les baux du DHCP.

Configuration d'un Serveur Web (IIS) :

On commence par ouvrir Internet Information Services (IIS) Manger qui se trouve dans Tools.

On déplie les dossiers et on peut voir qu'on à un site par défaut on en à pas besoin donc on ne le touche pas, et on clic droit sur Sites pour faire un Add Website.

Pour le nom du site on peut le choisir dans mon cas c'est MonSite, ensuite on doit choisir l'endroit où on va mettre notre site mais de préférence on le met dans C:\inetpub\wwwroot qui est l'endroit par défaut (ne pas oublier de créer un dossier qui peut importe comment il s'appelle pour mon cas c'est site1 et il se trouve dans le dossier wwwroot et donc le chemin final c'est C:\inetpub\wwwroot\site1).

On laisse le type du site en http et on utilise l'adresse IP de notre serveur (172.16.1.10), on laisse le même port (80) et l'Host name correspond au domaine de notre site mais on peut mettre l'alias qui est plus court et plus simple (www.student.labo) et on appuye sur OK.

Maintenant que notre site est fait on peut mettre dans notre dossier site1 un fichier HTML qui va donne une structure à la page web (dans mon cas c'est un fichier au nom de index.html).

On peut vérifier si le site fonctionne avec le raccourci qui se trouve sur Windows serveur où en tapant le nom de domaine du site sur un navigateur (www.student.labo).

On peut également faire un clic droit sur notre site puis un Edit Blindings donc une Modification de liaison ensuite on pourra faire Add et ajouter un nouveau URL qui sera dans mon cas autre.student.labo et qui va me permettre d'accéder au même site.

Dans la manip 6 on à dû refaire un nouveau site pour les profs où on à dû dans IIS crée le site et donc lui donner un nouveau fichier index.html qui cette fois se trouvait dans le dossier prof au même niveau que site1.

On à donc dû configurer aussi le DNS en fonction de notre nouveau site, où on à dû crée une nouvelle zone dans le Forward Lookup Zone avec le Host de notre serveur qui est winserver et aussi un CNAME avec le www (donc ne pas oublier de faire tout ceci dans la nouvelle zone teacher.labo).

Configuration d'un site en HTTPS :

Pour faire un site en https on doit tout d'abord faire un certificat dans le IIS, on double clique sur notre local serveur donc qui est en dessous du Start Page et qui commence en général par WIN.

Ensuite on regarde la partie centrale de la fenêtre et on cherche Server Certificates, pour double cliquez dessus.

On peut voir qu'il est vide donc on à pas de certificat on peut en crée un dans la partie droite de notre fenêtre en appuyant sur Create Self-Signed Certificate, où on peut voir qu'on peut donner un nom à notre certificat(dans mon cas c'est student) et on peut choisir si il est Personnel ou si c'est dû Web Hosting, pour la manip j'ai choisi le Web Hosting (notez que le certificat web hosting pourrai faire référence à un certificat spécifique pour l'hébergement web, alors qu'un certificat personnel est auto-signé et est utiliser pour un usage interne).

Ensuite on doit revenir sur notre site (dans mon cas c'est le site student), où clic droit dessus pour faire une liaison avec Edit Blindings puis Add, et ensuite je peux choisir https, mettre la bonne adresse (172 .16.1.10) et mettre un Host name qui peut-être le même que www.student.labo par exemple mais dans mon cas j'ai mis secure.student.labo, on doit laisser le port par défaut (443) et on peut ensuite choisir notre certificat dans SSL certificate (dans mon cas c'est student) puis on appuye sur OK(sans rien cocher).

On doit ensuite ne pas oublier de faire comme tous les alias qu'on a fait on doit renseigner dans mon cas c'est le secure dans le CNAME avec le nom de domaine comme FQDN.

On peut maintenant taper notre site (secure.student.labo) dans le navigateur, et il nous dira que ce n'est pas un site sécurisé mais on peut l'ignorer et accédez au site(Évidemment les sites sécurité n'utilise pas un certificat auto-signer mais un certificat officiel d'une autorité qui va gérer les accès aux sites).

Configuration d'un serveur FTP :

Pour l'installation du serveur FTP on doit retourner dans Manager on met Add Roles and Features puis on passe tout jusqu'au Server Roles où on cherche FTP Server qui se trouve dans Web Server (IIS) (il faut déplier l'IIS) on le coche, et on doit aussi cocher dans le FTP Server (donc on déplie FTP server si ce n'est pas déjà fait) le FTP Extensibility (c'est donc les extensions de FTP).

Sachant que FTP est une fonctionnalité de IIS il va falloir travailler avec, mais on doit d'abord refrech l'IIS en appuyant dessus dans Server Manager -> IIS (Server Manager c'est le « menu principale » de votre Gestionnaire de Serveur) puis on refrech notre serveur local (qui commence par WIN) avec un clic droit puis refrech.

On peut commencer par ouvrir l'IIS ensuite on clic droit sur le dossier qui contient nos deux sites normalement (MonSite et SiteTeacher) et qui s'appelle Sites, puis on appuye sur la nouvelle fonctionnalité qui est Add FTP Site.

Une fois qu'on à la fenêtre on peut déjà donner un nom au serveur FTP (dans mon cas c'est MonSiteFTP) puis on peut choisir l'endroit où on va mettre les dossier (on peut choisir n'importe quel endroit mais pour mon cas c'est dans Documents) et on appuye sur Next.

Pour l'étape d'après on mets l'adresse IP de notre serveur, on laisse le même port (21) et on choisit de ne pas mettre de SSL (donc un chemin sécurité depuis notre client à notre serveur FTP) puis on met Next.

L'étape d'après on peut cocher l'authentification Basic et on autorise tous les utilisateurs à accéder au serveur FTP en sélectionnant All users et pour les permissions on coche Read (lire) et Write (écrire) comme ça tous ceux qui ont accès à notre serveur ils peuvent le consulter et le modifier.

Maintenant qu'on à fini notre serveur FTP on peut le consulter en tapent ftp://172.16.1.10 dans le navigateur.

Pour l'instant notre espace serveur FTP est vide donc c'est normal qu'on ait une page presque blanche, il faut donc mettre des fichiers dans Documents pour voir ces fichiers/dossier dans le navigateur.

Règle FireWall :

Maintenant on veut pouvoir accéder au serveur FTP mais depuis un client, pour se faire on doit d'abord, ou désactivé le firewall de notre Windows Server, ou alors on crée une règle qui nous permet de communiquer avec le serveur par le port 21 qui est le port FTP.

Pour ça on doit taper firewall.cpl dans la barre de recherche en appuyant dessus on peut appuyer sur Advanced setting (paramètres avancée) par la suite, on choisit le Inbound Rules et on appuye sur New Rules qui se trouve du côté droit de la fenêtre.

A ce moment là on peut voir une fenêtre qui apparaît et qui nous demande quel sera le type de notre règle, on choisit Port et on appuie sur Next. Ensuite on laisse sur TCP et on spécifie le numéro de port qui est 21, puis on appuie sur Next.

On laisse sur Allow the connection et on appuie sur Next.

On laisse les trois carré (Domain, Private et Public) cochers et on appuie sur Next.

On donne un nom à notre règle (pour ma part j'ai mis FTP port21) et on appuie sur Finish.

Accès au FTP par le client :

On peut comme on l'a vue à présent accéder à notre serveur FTP par le navigateur (mais attention sur certain navigateur récent ceci ne fonctionne pas).

Mais on peut également le faire avec ligne de commande sur que ça soit sur Windows ou Linux, mais il faut noter que sur Linux ce n'est pas toujours installer donc il faut l'installer avec la commande :

- apt-get update = mettre à jour les paquet.
- apt-get install ftp = installer le paquet ftp.

Si vous avez le paquet FTP l'accès est semblable dans les deux OS c'est-à-dire ftp 172.16.1.10 vous devez mettre le nom d'utilisateur et le mot de passe dur serveur Windows pour ma part c'est Administrator et le mot de passe c'est Tigrou007 (une fois connecter taper ? pour voir les commandes possibles).

Utilisation WireShark sur Kali Linux :

Utilisation de Network Manager :

Si on à pas Network Manager on utilise les commandes apt-get update pour mettre à jour les paquets, puis apt-get install network-manager et enfin systemctl enable NetworkManager pour que sont activation soit persistante.

On utilise Network Manager avec la commande nmcli qui nous permet de configurer/supprimer/ajouter des interfaces et des connexions réseaux.

- nmcli = si on utilise juste la commande nmcli on va voir tous les interfaces et les connexions réseaux mais plus en détails que si on utilisait la commande nmcli c (c = connection).
- nmcli general status = cette commande sert à voir le statuts du Network Manager.
- nmcli c mod Nom_de_la_connexion ipv4.address 192.168.1.2/24 ipv4.gateway 192.168.1.1 ipv4.dns 192.168.1.1 ipv4.method « manual »
  = cette commande sert à modifier à l'aide de mod (=modify) l'adresse ip, le dns, la passerelle et la méthode de connexion au réseau (il faut savoir que qu'on n'est pas obligé de les mettre tous (sauf la method qui sert à connaître si on veut le modifier en auto(dhcp) ou en manual (static)) et on peut les mettre dans l'ordre voulu cela ne changera rien (**il ne faut pas oublier de préciser le nom de la connexion ou le UUID**)).
- nmcli c up Nom_de_la_connexion = cette commande on l'utilise après la commande précédente et on le fait pour activer la connexion.
- nmcli c down Nom_de_la_connexion = cette commande fait l'inverse de sa précédente, elle désactive la connexion citer.
- nmcli c add con-name NouvelleConnexion ifname eth0 type ethernet ipv4.address 192.168.2.2/24 ipv4.gateway 192.168.1.1 ipv4.dns "192.168.1.1" ipv4.method « manual » = avec cette commande on peut ajouter une nouvelle connexion où on l'associe à une interface avec ifname et on lui donne un type de connexion avec type (on peut donc mettre d'autre type comme le wifi, vpn, bridge, vlan et bond par exemple).
- nmcli c mod Nom_de_la_connexion ipv4.method auto = cette commande modifie la connexion pour qu'elle soit en dhcp.

Commandes pour le ARP :

La commande ip neigh show permet de voir l'adresse IP et l'adresse MAC des hôtes qui se trouvent dans le même sous-réseau que l'utilisateur.

Le résultat sera de gauche à droite, l'adresse ipv4 ou ipv6 d'un hôte l'interface qui utilise cette adresse ensuite l'adresse MAC de l'hôte et en fin l'état de la connexion avec cet hôte.

Elle peut être REACHABLE pour dire qu'elle est correcte ou STALE pour dire qu'elle est obsolète ou instable, si on trouve avant l'un de ces deux états le mot route cela voudrait dire que cette connexion appartient au routeur.

La commande ip neigh flush all sert à vider toute la table pour pouvoir reprendre une sorte de capture des adresses IP et MAC des autres hôtes (le all n'est pas obligatoire il peut être remplacé par une adresse précise à enlever de la capture).

On peut envoyer des signaux à un autre hôte sans passer par le routeur en étant dans le même réseau, si on veut ping un appareil précis on indique son adresse IP et on peut le trouver par la suite dans la liste des ARP/NDP (la commande fping -g 192.168.1.0/24, peut envoyer un ping à tous les appareils qui se trouve dans la plage 192.168.1.0 - 192.168.1.255).

Sur Wireshark on peut donc utiliser le filtre arp pour voir comment nos appareils communiques entre elles en demandant à tous les autres appareils à qui appartient l'adresse IP en question pour pouvoir communiquer avec elle.

On peut aussi voir comment elles « rencontres » un serveur DHCP, en utilisant les quatre étapes qu'on à vue en théorie :

Discover (c'est quand notre ordinateur cherche un serveur DHCP pour demander un IP, il envoie son signale sur l'adresse de Broadcast qui est le 255.255.255.255).

Offer (c'est quand le serveur DHCP propose une adresse IP et un bail).

Request (c'est quand notre ordinateur répond à la proposition du serveur DHCP, il l'envoie à tous les autres appareils également pour dire que cette adresse est réservée).

ACK (c'est pour confirmer que le serveur il à reçu la réponse et qu'il va lui donner une adresse IP).

En utilisant le filtre udp.srcport == 68 or udp.srcport == 67 on peut voir les quatre étapes car la communication ce fait avec un protocole udp et avec les ports 67 et 68.

Comportement DNS :

Si on observe sur Wireshark la réaction d'un serveur DNS après lui avoir demander de nous fournir l'adresse IP d'un nom de domaine (Avec la commande nslookup www.nomdedomain.com), on peut observer que notre ordinateur envoie la demande pour dire à qu'elle adresse IP appartient se nom de domaine, ceux quoi notre serveur DNS répond avec l'adresse IP.

Et dans Wireshark on peut aussi observer directement dans le paquet de question l'indication vers un autre paquet qui est le paquet de réponse.

Connexion SSH :

Avec Putty sur notre pc physique on peut se connecter avec un autre ordinateur, et on peut observer sur Wireshark la connexion en mettant ip.addr == adressePcPhysique, et on peut observer la demande de synchronisation [SYN] de notre ordinateur physique, ensuite le renvoie de la Kali de la demande de synchronisation et l'Accusé de réception [SYN, ACK] et en fin le renvoie de l'Accusé de réception de notre pc physique à la Kali pour confirmer la réception [ACK].

Connexion http :

Si on se connecter sur un site http, on peut utiliser Wireshark pour voir tout ce qui contient le site, il suffit d'utiliser le filtre http dans la barre de recherche.

Ceci prouve les précautions qu'il faut prendre si on y va sur un site http.

Connexion par telnet :

Si on essaye d'installer telnet avec la commande apt-get install telnetd et qu'on établit une connexion avec la commande telnet 192.168.1.60, on peut suivre le moindre appuye sur le clavier de la synchronisation.

C'est pour cela que telnet à était délaissé pour être remplacé par le ssh qui lui chiffre les donné.

L'écoute avec Netcat :

Avec la commande netcat ou nc on peut écouter ou se connecter à un port ou une adresse IP pour par exemple communiquer, il suffit d'installer Netcat avec la commande apt-get install netcat.

Une fois que c'est fait on à qu'à se connecter d'un côté avec la commande nc -nlvp 4444 (le dernier numéro est le numéro de port et tant qu'il est non utilisé on peut communiquer avec) et de l'autre côté on doit mettre la commande nc -nv 192.168.1.60 4444, tant qu'on reste dans le canal on peut voir et écrire des messages avec l'autre hôte.

Ceci dit Netcat tout seule n'est pas sécurité, comme sur telnet on peut suivre la conversation avec Wireshark, pour chiffrer notre conversation on peut utiliser un certificat SSL, pour cela on doit juste ajouter --ssl à la fin des deux commande pour se connecter.

On peut également utiliser Cryptcat qui nous permet de crypter la conversation sans certificat SSL, pour se faire on doit installer Cryptcat avec la commande apt-get install cryptcat ensuite on a qu'à remplacer le nc dans nos deux commandes par cryptcat :

- cryptcat -nlvp 4444
- cryptcat -nv 192.168.1.60 4444

Mise en place du routage sous Linux :

Configuration et préparation des machines :

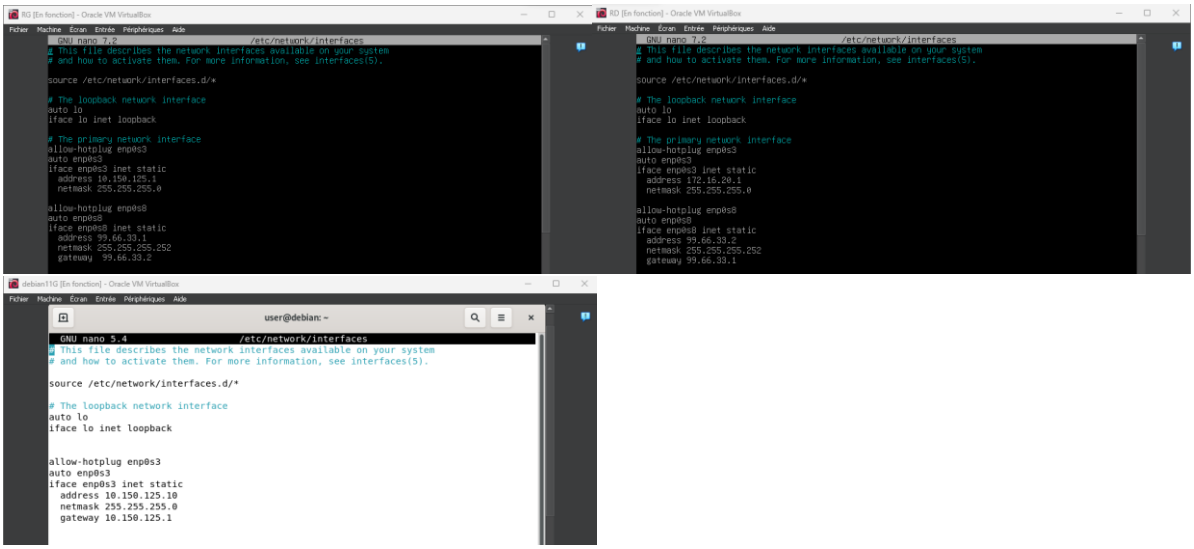
Tout d'abord je dois configurer mes machines pour qu'elle soit dans les même réseaux.

Je vais suivre cette configuration :

Réseau	Appareil	Cartes	Adresse IP	Masque	Passerelle
LanG	LinuxClient	Enp0s3	10.150.125.10	255.255.255.0	10.150.125.1
LanG	RouteurG	Enp0s3	10.150.125.1	255.255.255.0	
Routeur_link	RouteurG	Enp0s8	99.66.33.1	255.255.255.252	99.66.33.2
Routeur_link	RouteurD	Enp0s8	99.66.33.2	255.255.255.252	99.66.33.1
LanD	RouteurD	Enp0s3	172.16.20.1	255.255.255.0	
LanD	Windows10Client	Ethernet	172.16.20.10	255.255.255.0	172.16.20.1

Pour ce faire je dois créer deux interfaces pour les deux routeur (Pour voir comment faire pour ajouter des interfaces réseau c'est à la page 6 de cette synthèse).

Pour voir comment on configure un réseau sous Linux c'est à la page 7, à part ça voici le résultat :



Pour la Windows j'ai utilisé la commande netsh interface ip set « NAT » address static 172.16.20.10 255.255.255.0 99.66.33.2.

Configuration des routeurs :

Sur Linux on a la possibilité de faire une configuration pour mettre notre linux en routeur, pour cela on doit ouvrir le fichier /etc/sysctl.conf avec nano et on doit décommenté la ligne net.ipv4.ip_forward=1 ensuite on sauvegarde le fichier et on le quitte pour taper cette commande-là sysctl -p /etc/sysctl.conf.

Maintenant on aimerait que nos clients passent par des routes et non pas des routes par défaut (sachant que les routes par défaut on y passe quand on ne sait pas où envoyer le paquet).

Pour se faire on va aller dans le fichier /etc/network/interfaces (dans le routeur de gauche), on enlève le default gateway et en dessous des interfaces on ajoute up ip route add 172.16.20.0/24 via 99.66.33.2.

On fait la même chose avec le routeur de droite, up ip route add 10.150.125.0/24 via 99.66.33.1 (ne pas oublier d'utiliser la commande systemctl restart networking et/ou de reboot le système).