Leçon 5 : services réseaux de base

5.1 Introduction

Dans cette leçon, nous allons étudier les services réseaux de base que sont le service DNS, le service DHCP et leur gestion. Avant d'entrer dans les détails de configuration de ces services, nous commencerons par un rappel succinct des éléments importants sous-jacent à chaque service étudié.

Nous aborderons dès lors les thèmes suivants :

- Rappel réseau IPv4 et IPv6
- Rappel concernant le service DNS
- Rappel concernant le service DHCP
- Installation et configuration du service DNS
- Installation et configuration du service DHCP

5.2 Rappels IP

Le protocole réseau utilisé est le protocole IP (Internet Protocol). Les deux versions principales de ce protocole sont IPv4 et IPv6. Il y a de grandes similitudes dans le fonctionnement de ces deux protocoles mais également de grandes différences.

En **IPv4**, les adresses sont codées sur 32 bits et représentées sous la forme *décimale pointée*. Ainsi, on groupe l'adresse par blocs de 8 bits qu'on transforme en décimal afin de pouvoir lire cette adresse facilement. IPv4 réserve des adresses spécifiques à des usages donnés. Ainsi :

Adresses	Usage
`127.0.0.1`	Adresse qui désigne toujours la machine courante. Cette adresse porte le nom de *localhost*. Elle permet de contacter un service qui s'exécute sur la même machine que le programme client

`10.0.0.0/8`
`172.16.0.0/12`
`192.168/16`
	Ces adresses IP sont *locales* et réservées pour des réseaux internes. Elles sont utilisées par les utilisateurs pour connecter ensemble toutes les machines d'un réseau privé.

`224.0.0.0 à` `239.255.255.255`	Adresses réservées au multicast. Ces adresses sont utilisées pour atteindre *un groupe de machines*. La même information arrive à l'ensemble des machines du groupe.

En **IPv6**, les adresses sont codées sur 128 bits et représentées sous une forme *hexadécimale* dans laquelle on sépare chaque groupe de 16 bits par le symbole « : ». Elles sont nettement moins lisibles que des adresses IPv4. Certaines adresses ont une signification particulière :

Adresses	Usage
`::1`	Adresse qui désigne la machine courante en IPv6. Elle porte également le nom de *localhost*
`fe80::/10`	Adresses locale-lien. Ces adresses sont attachées à une interface donnée. Elles ont une portée limitée au LAN (ne traverse pas les routeurs). Elles sont souvent configurées automatiquement.
`fc00::/7`	Adresses locale-unique. Ces adresses sont des adresses privées qui ne peuvent pas être routées sur l'internet.

`2000::/3`	Adresses globale-unique. Ce sont les adresses publiques que l'on retrouve sur l'internet. Elles sont uniques et attribuées par un ISP.
`ff00::/8`	Adresses multicast. Ces adresses sont utilisées dans bien des cas (déterminer l'adresse physique correspondant à une adresse IP déterminée, …) quand il faut adresser une information à un groupe de machines.

En **IPv4**, le protocole **ARP** (Address Resolution Protocol) est utilisé pour trouver l'adresse physique correspondant à une adresse IP donnée (envoi d'une trame en broadcast sur le réseau en demandant : « Qui est le propriétaire de 192.168.190.2 »).

En **IPv6**, le protocole **NDP** (Neighbour Discovery Protocol) est utilisé pour découvrir ses voisins, construire une adresse IPv6 unique et connaître l'adresse physique d'une machine en fonction de son adresse IPv6 (envoi d'un message en multicast sur une adresse déterminée et reprenant les 24 derniers bits de l'adresse IPv6).

5.3 Rappels concernant le service DNS

Le service DNS est un des services critiques sur l'Internet. Il s'agit du service permettant de convertir un nom réseau en adresse IP et inversement. Sans ce service, nous serions obligés de mémoriser des adresses IP directement, ce qui ne serait guère pratique. Le service DNS est donc une base de données *décentralisée* capable de répondre *localement* à une demande du style « Qui est `www.swila.be` ». Pour rappel, le système hiérarchique assure qu'un nom sur l'Internet est unique car les propriétaires d'un domaine (`swila.be` par exemple) sont responsables de la gestion des noms et adresses de son domaine uniquement. Quand une requête ne concerne pas son domaine, le service DNS renvoie la requête à un serveur racine pour que celle-ci soit résolue.

Le système de noms fait donc correspondre des informations précises (adresses, …) à des noms configurés. Ainsi, pour l'enregistrement de `www.swila.be`, nous avons une entrée de type A qui mentionne son adresse IPv4 (`195.154.39.227`) et une entrée de type AAAA qui mentionne son adresse IPv6 (`2001:bc8:38eb:fe10::11`). Plusieurs types d'entrées sont possibles en fonction de l'information que l'on souhaite annoncer.

Il faut être prudent avec le système DNS car si les entrées qu'il contient ne sont pas valides, on peut tromper l'utilisateur sur les sites qu'il croit visiter. Enfin, les systèmes Microsoft utilisent le service DNS pour localiser l'annuaire Active Directory. Dès lors, dès qu'on installe Active Directory, des entrées particulières sont ajoutées dans le serveur DNS.

Enfin, mentionnons que pour des raisons de sécurité, il est possible de configurer un serveur DNS *secondaire* capable de répondre à toutes les requêtes (en fonction de sa configuration) lorsque le serveur principal est indisponible. La synchronisation entre les deux serveurs est automatique.

5.4 Rappels concernant le service DHCP

Le service DHCP est un autre service intéressant pour les administrateurs systèmes et réseaux. En effet, ce service est responsable de la distribution des adresses IP dans un réseau. L'intérêt est que le service envoie au client tous les éléments de configuration réseau afin que ce dernier soit configuré directement et sans intervention de l'utilisateur. Grâce à ce système, un ordinateur peut être connecté

sur le réseau et recevoir sa configuration depuis celui-ci. Ce mécanisme est particulièrement adapté aux périphériques nomades. Peu importe où ils se trouvent, le réseau leur donne la configuration à appliquer.

Cependant, si cela facilite la vie de l'administrateur, qui ne doit plus passer sur chaque ordinateur pour le configurer manuellement, cela ne facilite pas le contrôle. En effet, une adresse IP est attribuée à un périphérique durant un temps déterminé (= durée du bail). Une fois ce délai écoulé, le client doit faire une nouvelle demande au serveur. Dès lors, contrôler les utilisateurs devient plus difficile car une même adresse peut être attribuée à plusieurs personnes successivement.

Cependant, l'administrateur peut *réserver* des adresses à des utilisateurs. Cela revient à attribuer une adresse donnée à un client déterminé. On procède alors à une *réservation*. L'administrateur peut, de cette manière *réserver* les adresses pour l'ensemble des postes à connecter. Ainsi, les clients ne doivent rien configurer localement et l'administrateur garde la main mise sur toute la configuration réseau.

Il n'y a pas que les éléments réseaux qui peuvent être envoyés au client mais bon nombre d'options. Le service DHCP permet ainsi une configuration PXE (démarrage d'un ordinateur par le réseau), donner l'imprimante à utiliser, …

Le service DHCP existe à la fois pour les adresses IPv4 et IPv6. Cependant, en IPv6 la règle est plutôt de construire son adresse IP en utilisant le protocole NDP en fonction des informations reçues par le réseau (comme le préfixe à utiliser, …).

5.5 Installation et configuration du service DNS

Pour **installer** le service DNS, il faut d'abord vérifier que votre serveur dispose bien d'une adresse IP statique (fixe, non attribuée par le DHCP). Ensuite, il faut démarrer le **Server Manager > Manage > Add Roles and Features**. Dans la liste des rôles, il faut sélectionner *DNS Server*.

Une fois le rôle ajouté, il apparaît dans la liste des rôles disponibles sur le serveur. Pour la configuration, il faut donc se rendre dans **Server Manager > Tools > DNS** puis déployer **DNS > WIN16-1** (ou quelque soit le nom de votre serveur). On voit apparaître la fenêtre suivante :

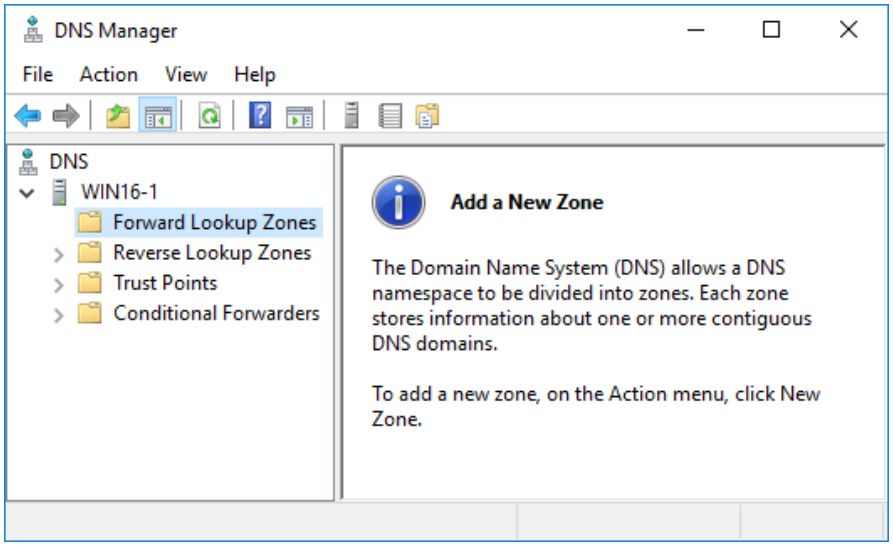

Figure 5.1 : tableau de configuration du service DNS

Dans la figure 5.1, nous remarquons les éléments suivants :

- *Forward Lookup Zones* : Ce sont les zones configurées pour faire les résolutions d'un nom vers l'adresse IP
- *Reverse Lookup Zones* : Ce sont les zones configurées pour faire les résolutions inverses d'une adresse IP vers le nom.
- *Trust Points* : Permet de configurer les éléments cryptographiques compatible avec DNSSEC qui permet de signer toutes les entrées d'une zone.
- *Conditional Forwarders :* ce sont les autres serveurs DNS à interroger suivant certaines conditions rencontrées. Un redirecteur est un serveur DNS vers lequel il est possible de rediriger une requête pour obtenir la résolution du nom.

Le **redirecteur** conditionnel ou non est un élément facultatif de la configuration du serveur DNS. En effet, tous les serveurs DNS disposent de la liste des serveurs racines qui servent à démarrer la recherche d'un nom donné. Cependant, dans certains cas, il est possible de rediriger une requête vers un autre serveur DNS configuré dans le redirecteur : par exemple si le nom à atteindre est local mais est servi par un autre serveur. De plus, à l'intérieur de certains réseaux, les requêtes DNS émises par d'autres serveurs que ceux autorisés peuvent être bloquées.

5.5.1 Propriétés du serveur DNS

Pour atteindre **la configuration générale** du service DNS, il faut faire un **clic-droit** sur le nom du serveur (`WIN16-1` sur la figure 5.1) et choisir l'option **Properties**. La fenêtre qui apparaît contient plusieurs onglets et plusieurs options :

- *Interfaces :* cet onglet permet de configurer les interfaces (et donc les adresses IP) sur lesquelles le service DNS écoute.
- *Forwarders :* cet onglet permet d'ajouter des redirecteurs *globaux* (non conditionnel). Ces redirecteurs reçoivent alors les requêtes DNS que le serveur ne sait pas résoudre et sont chargés de fournir la réponse au serveur. Sur le campus, on pourrait configurer un redirecteur vers l'adresse IP `192.168.128.2` afin de relayer toutes les requêtes vers lui.
- *Advanced :* précise des options avancées comme *désactiver la récursivité* (le serveur ne tente plus de résoudre des requêtes pour lesquelles il n'a pas de réponse), …
- *Root Hints :* cet onglet mentionne tous les serveurs racines connus par le serveur DNS. On trouve donc les 13 serveurs racines et leurs adresses IP.
- *Debug Logging, Event Logging et Monitoring :* ces onglets présentent les options d'analyse afin de trouver les dysfonctionnements du serveur DNS.

5.5.2 Ajout d'une nouvelle zone directe (Forward Lookup Zones)

Pour **ajouter une nouvelle zone** de recherche (nom DNS géré par ce serveur), il y a 2 possibilités. La première est de passer par l'*assistant d'ajout d'une zone* en faisant un **clic-droit** sur le nom du serveur (`WIN16-1` sur la figure 5.1) et en choisissant l'option *Configure a DNS Server Wizard*. La seconde méthode est d'aller sur l'élément **DNS > WIN16-1 > Forward Lookup Zones** et de choisir l'option *new zone* (soit par un *clic-droit*, soit en passant par le menu *autres actions*).

Lors de l'ajout d'une nouvelle zone, le serveur propose 3 types de zone :

- *Primary Zone :* ce serveur connaît et maintient les informations de conversion des noms vers les adresses IP
- *Secondary Zone* : le serveur est un backup d'un autre serveur DNS. Il synchronise automatiquement les informations avec l'autre serveur DNS (celui qui a cette zone en zone principale).
- *Stub Zone* : le serveur DNS stocke les informations concernant les serveurs pouvant résoudre cette zone particulière. Ce mécanisme plutôt étrange, ne sera pas abordé ici.

Si l'utilisateur ajoute *une zone principale* (**Primary Zone**)*,* il doit mentionner le nom de la zone pour laquelle il fait *autorité* (il a acheté cette zone et en est donc responsable). Si le suffixe de la zone est *.local* (au lieu de *.be* ou *.com)*, cette zone est considérée comme privée et ne se retrouve pas sur l'internet. Les zones locales peuvent donc être ajoutées sans risque. Ensuite, le système vous demande s'il faut utiliser un nouveau fichier ou un fichier existant (la plupart du temps, un nouveau fichier est l'option qu'il faut choisir). Ensuite, le système vous demande s'il faut *autoriser les mises à jour dynamiques* des zones. Pour des raisons de sécurité, nous choisirons l'option *Do not allow dynamic updates*. Enfin, un écran récapitulatif nous permet de contrôler si toutes les informations sont bien correctes. Si c'est le cas, il faut cliquer sur **Finish**.

La zone configurée apparaît alors dans la liste des *Forward Lookup Zones* (zone de recherche directe). Une fois la zone créée, il est possible d'ajouter des entrées :

Type d'entrée	Explication
A ou AAAA	Permet de faire correspondre un nom à une adresse. Le nom donné sera complété du suffixe DNS choisi. Ensuite, il faut mentionner l'adresse IPv4 ou IPv6 correspondant à cette entrée. On peut faire correspondre plusieurs adresses IP à une entrée. Normalement, une adresse IP est référencée dans une seule entrée de type A ou AAAA. Si plusieurs noms arrivent sur la même adresse, il faut créer des alias (CNAME)
CNAME	Permet d'ajouter un alias. L'alias est un élément inscrit dans le DNS servant à faire pointer un nom vers une entrée de type A ou AAAA (il est donc interdit de faire pointer un CNAME vers un autre CNAME).
MX	Permet de mentionner le serveur mail qui est chargé de traiter les mails pour ce domaine.
NS	Permet de mentionner le serveur DNS responsable d'un nom de domaine. Cette entrée **permet** également **de renseigner une délégation de zone**. Ainsi, un sous-domaine pourrait être géré par un autre serveur DNS.

Il est également possible de créer un **sous-domaine** qui est géré par le serveur actuel en utilisant l'option *new domain*. Une fois tous les hôtes configurés, la zone DNS est prête à être utilisée.

Si l'utilisateur ajoute **une zone secondaire**, il doit mentionner le nom de domaine concerné et puis le ou les serveurs principaux auprès desquels il faut se synchroniser. Une fois la synchronisation démarrée, le serveur secondaire est à même de répondre aux requêtes concernant cette zone.

5.5.3 Ajout d'une zone de recherche inversée (Reverse Lookup Zones)

La *Reverse Lookup Zones* permet de réaliser la conversion dans l'autre sens : d'une adresse IP vers un nom. Il est nécessaire d'ajouter une zone de recherche inversée par sous-réseau /24. Ainsi, si l'on dispose du sous-réseau suivant : `192.168.128.0/20` et qu'on souhaite avoir une zone inverse pour

l'ensemble, il faut créer 16 zones différentes : `192.168.128`, `192.168.129`, `192.168.130`, …, `192.168.143`.

Le nom de la zone inverse est un peu étrange car il reprend, par convention, chaque nombre décimal de l'adresse IP mais inversé. Ceux-ci sont ensuite suffixés par `.in-addr.arpa`. Ainsi, un nom valide de zone inverse pourrait être `128.168.192.in-addr.arpa`.

Une fois la zone crée, elle est prête pour accueillir des entrées. Les entrées possibles sont :

Type d'entrée	Explication
PTR	Permet de faire pointer une adresse vers un nom. Normalement, seul le dernier octet de l'adresse doit être complété.
CNAME	Permet de créer un alias

5.5.4 Configuration du client DNS

Le serveur Windows doit être configuré pour disposer d'un nom dans le domaine DNS configuré et, de plus, il doit être configuré pour utiliser le service DNS installé. Pour ce faire, il faut :

- Créer une entrée correspondant au serveur DNS courant et faire correspondre l'adresse IP
- Modifier le nom de l'ordinateur comme suit : **clic-droit** sur **This PC**, **Properties**. Choisir **Advanced system settings**, onglet **Computer Name** ensuite bouton **Change** puis le bouton **More** pour ajouter, comme suffixe DNS principal, le nom de la zone DNS configuré. Comme le nom est modifié, il sera nécessaire de redémarrer le serveur.
- Configurer le réseau pour utiliser le serveur DNS. Pour ce faire, il faut **modifier** les **paramètres de la carte réseau**. En effet, il faut modifier **le serveur DNS préféré** pour le remplacer par `127.0.0.1` (localhost) puisque le service DNS s'exécute sur notre serveur.

5.5.5 Scripting

Il est possible de configurer les entrées DNS au moyen **de la ligne de commande** en utilisant l'outil `dnscmd`. Cette commande permet d'ajouter des zones mais également d'ajouter les enregistrements de tous types à l'intérieur de celles-ci. L'aide en ligne est disponible par la commande **`dnscmd /?`**.

Par exemple, les commandes suivantes sont valides (si notre serveur s'appelle `DC`) :

```
C:\> dnscmd DC /RecordAdd 128.168.192.in-addr.arpa 3 PTR
                                                  data.cg.local
```

Cette commande ajoute, sur le serveur DC, dans la zone inverse (Reverse Lookup) l'enregistrement `192.168.128.3`[20] qui pointe vers le nom `data.cg.local`.

```
C:\> dnscmd DC /RecordAdd cg.local data.cg.local.  A 192.168.128.3
```

*Cette commande ajoute, sur le serveur DC, dans la zone directe (Forward Lookup) `cg.local` l'enregistrement `data.cg.local` qui a, comme adresse IP, l'adresse `192.168.128.3`. Il faut **absolument mentionner le point à la fin de l'enregistrement** afin de mentionner que le nom est complètement qualifié.*

[20] Pour rappel, une zone inverse (*Reverse Lookup Zones*) nécessite d'inverser tous les octets de l'adresse

On pourrait également écrire cette dernière commande comme suit :
`C:\> dnscmd DC /RecordAdd cg.local data A 192.168.128.3`
Dans cette dernière commande, nous avons uniquement mentionné le nom `data`, qui, puisque ce dernier ne se termine pas par un « . », est interprété comme `data.cg.local.` (et donc le nom mentionné est complété par celui de la zone).

En **Powershell**, en utilisant **l'exécution directe de commandes**, il est simple d'ajouter des enregistrements DNS :

```
$resultat = &"dnscmd" "DC" "/RecordAdd" "cg.local" "data"
        "A" "192.168.128.3"
```

5.6 Installation et configuration du service DHCP

Pour installer ce service, il faut démarrer le **Server Manager > Manage** puis choisir **Add Roles and Features**. Dans la liste proposée, il faut sélectionner *DHCP Server*. Une fois installé, une notification est ajoutée *Complete DHCP Configuration*. Il faut cliquer sur le lien et appuyer sur **Commit**.

Pour démarrer la configuration du service DHCP, il faut démarrer le **Server Manager > Tools > DHCP**.

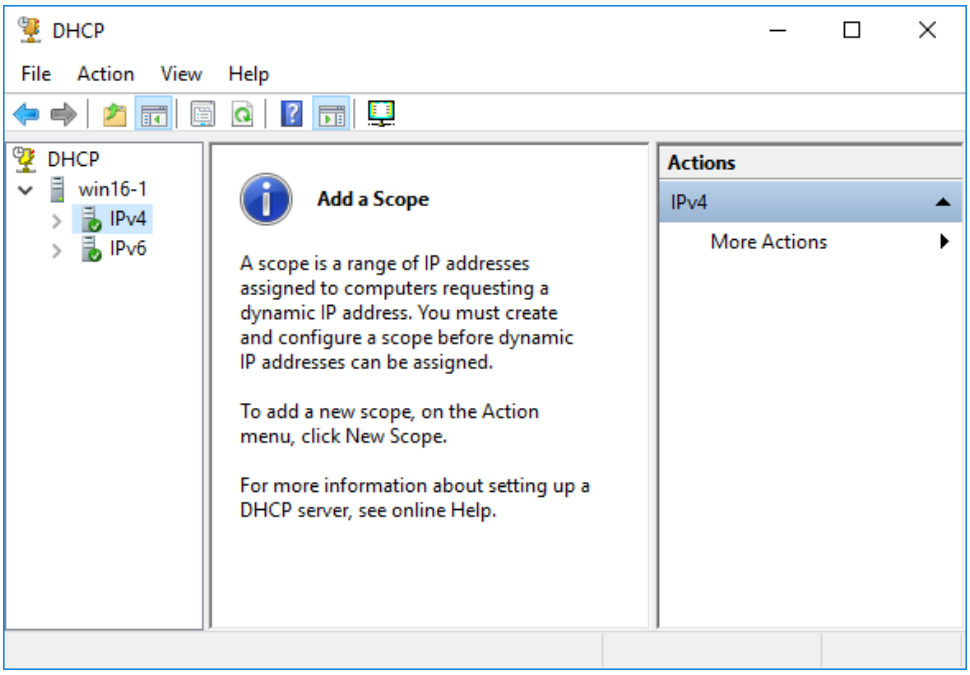

Figure 5.2 : Configuration du service DHCP

Il faut commencer par *ajouter une étendue* en faisant un **clic-droit** sur **IPv4** et en choisissant l'option *New Scope*. On doit donner un nom à l'étendue (dans *Name*) qui doit être univoque. Ensuite, il faut mentionner les adresses IP de départ et de fin qui pourront être distribuées aux clients. Le masque est ensuite renseigné, veillez à ce que celui-ci soit conforme au sous-réseau concerné.

Le *wizard* propose ensuite d'exclure une plage IP, cette configuration est facultative, elle permet d'empêcher l'attribution de certaines adresses IP.

Ensuite, il faut mentionner la durée du bail (*Lease duration*) qui indique le nombre de jours, d'heures et de minutes de validité de l'adresse IP. Si les utilisateurs sont nombreux et nomades (comme dans une école), une durée de bail courte (4 heures) est plus appropriée.

Enfin, le *wizard* vous propose de configurer certaines options :

- *Router (Default Gateway)* : mentionne l'adresse IP du routeur qui sera utilisé par les machines clientes pour sortir du réseau et atteindre Internet.
- *Domain Name and DNS Server* : mentionne les informations DNS qui seront distribuées aux machines clientes comme le *parent domain* (ou le domaine DNS utilisé) et les adresses IP (IP Address) des serveurs DNS à fournir. Veillez à donner l'adresse IP réelle de votre serveur et pas l'adresse *localhost* `127.0.0.1`.
- *WINS Servers :* cette fonctionnalité n'est pas nécessaire dans notre installation
- *Activate Scope :* une fois l'étendue active, le serveur DHCP sera actif.

Attention ! Il est toujours imprudent d'avoir plus d'un serveur DHCP actif sur le même sous-réseau. Ainsi lorsque vous activez un serveur DHCP, veillez bien à vous assurez qu'aucun autre serveur n'est actif sur ce même réseau[21].

Une fois le *wizard* fermé, en déployant les éléments à gauche, on voit apparaître les options configurées (comme l'étendue visible dans l'option *Address Pool*).

5.6.1 Les réservations DHCP (Reservations)

Une option intéressante du service DHCP est *la réservation*. Celle-ci consiste à associer une adresse physique à une adresse IP donnée. Ainsi, la machine concernée reçoit toujours la même adresse IP. En plus, si l'administrateur souhaite modifier la configuration réseau, il doit juste mettre à jour les données du serveur et redémarrer les machines.

Lors de l'encodage d'une réservation, il faut mentionner :

- *Reservation name :* Le nom de la réservation
- *IP address :* L'adresse IP réservée
- *MAC address :* L'adresse MAC sans aucun séparateur. Par exemple : 000C29DFBF93
- *Description :* Une description
- *Supported types :* Type pris en charge, dans notre cas, DHCP

Pour assurer que le service DHCP n'entre jamais en conflit avec une réservation réalisée, il est possible d'exclure l'adresse (ou la plage d'adresses) reprenant les réservations encodées. Les plages d'exclusion peuvent être configurées dans l'élément *Address Pool* via l'option *New Exclusion Range*.

5.6.2 Scripting

Il est possible d'ajouter des réservations DHCP directement **via la ligne de commande** en utilisant le programme `netsh`. Il s'agit d'un outil générique agissant sur la configuration réseau. Ainsi, pour obtenir l'aide concernant les entrées dans le DHCP, il faut entrer :

```
C:\> netsh dhcp server 127.0.0.1 list
```

Cette commande affiche l'aide et l'ensemble des commandes possibles. Pour chacune, il est possible d'obtenir l'aide en suffixant celle-ci par un « /? » .

[21] Si plus d'un serveur DHCP est actif, les clients pourraient recevoir des adresses de l'un ou l'autre serveur. Cela perturberait fortement le fonctionnement du réseau. **Vérifiez la configuration de pfSense !**

```
C:\> netsh dhcp server 127.0.0.1 scope 192.168.128.0 /?
```

Cette commande les commandes applicables à une étendue donnée (une plage configurée dans le DHCP). L'étendue est précisée par l'option `scope`*.*

```
C:\> netsh dhcp server 127.0.0.1 scope 192.168.128.0 add reservedip
       192.168.128.3 000C3A5BCDB9 data DHCP
```

Cette commande ajoute une réservation (`add reservedip`*) au serveur DHCP courant (*`server 127.0.0.1`*) pour l'étendue 192.168.128.0 (*`scope 192.168.128.0`*). L'entrée ajoutée a pour nom* `data`*, pour adresse IP réservée* `192.168.128.3` *associée à l'adresse MAC* `00-0C-3A-5B-CD-B9` *avec comme type pris en charge :* `DHCP`*.*

En **Powershell**, par l'**exécution directe de commandes**, il est facile d'ajouter des entrées dans le DHCP. Ainsi, la commande précédente prendrait la forme suivante :

```
$resultat = &"netsh" "dhcp" "server" "127.0.0.1" "scope" "192.168.128.0"
    "add" "reservedip" "192.168.128.3" "000C3A5BCDB9" "data" "DHCP"
```

5.7 Exercices

1. Installer le **service DNS** comme suit :
    a. Le nom de domaine correspondra à *votre nom de famille* suffixé par « *.local* ». Par exemple `swinnen.local`
    b. Ajouter les entrées suivantes :
        i. `fw` qui pointera vers l'adresse IP du firewall
        ii. `win16-01` qui pointera vers l'adresse IP de votre serveur
        iii. `host` qui pointera vers l'adresse IP de la machine hôte `192.168.190.1`
        iv. créer la zone inverse pour le sous-réseau `192.168.190.0` et ajoutez les entrées PTR pour `fw`, `host` et `win16-01`
    c. Configurer le redirecteur pour qu'il pointe vers le serveur DNS `192.168.128.2`

2. Configurer votre serveur Windows pour qu'**il soit client du serveur DNS configuré**.

3. Installer le **service DHCP** comme suit :
    a. Désactiver le serveur DHCP présent dans pfSense (**Services > DHCP Server**)
    b. Configurer une nouvelle étendue DHCP entre les adresses `192.168.190.150-200`
    c. Précisez toutes les options nécessaires (DNS, …)

4. Créer **un script Powershell** qui va créer des entrées dans le serveur DNS pour chaque adresse comprise dans la plage DHCP (entre `192.168.190.150` et `192.168.190.200`). Chaque entrée comprendra un enregistrement dans la zone directe et dans la zone de recherche inversée. Par exemple, voici un nom configuré : `ip-192-168-190-200.<votre-nom>.local` qui pointera vers l'adresse `192.168.190.200`, et ainsi de suite pour toutes les autres adresses.

5. Installer une nouvelle machine **Windows 10**[22] (mot de passe : `rootroot`)
    a. Configurée en mode DHCP
    b. Vérifiez la configuration réseau reçue et assurez-vous qu'elle a bien accès à Internet

6. A l'aide de **la ligne de commande** :
    a. Ajouter une réservation DHCP pour cette machine avec l'adresse `192.168.190.155` (assurez-vous que le serveur ne distribue plus cette adresse)
    b. Ajouter un alias DNS (`CNAME`) pour faire pointer le nom suivant : `vm10.<votre-nom>.local` vers le nom `ip-192-168-190-155.<votre-nom>.local.`

[22] Une machine virtuelle proposant la version d'évaluation de 90 jours de windows 10 est fournie dans le dossier `c:\admsys`