

# Administration Windows – TP1

Louis Lapointe

**L3 STRI - UPSSITECH**

25 octobre 2023  
Cr   par : louis lapointe

Louis Lapointe

Page 1-2 : Avant-propos :

Page 2-3 : Powershell

Page 3-9 : Mise en place d'un active directory

Page 10 : Convaincre

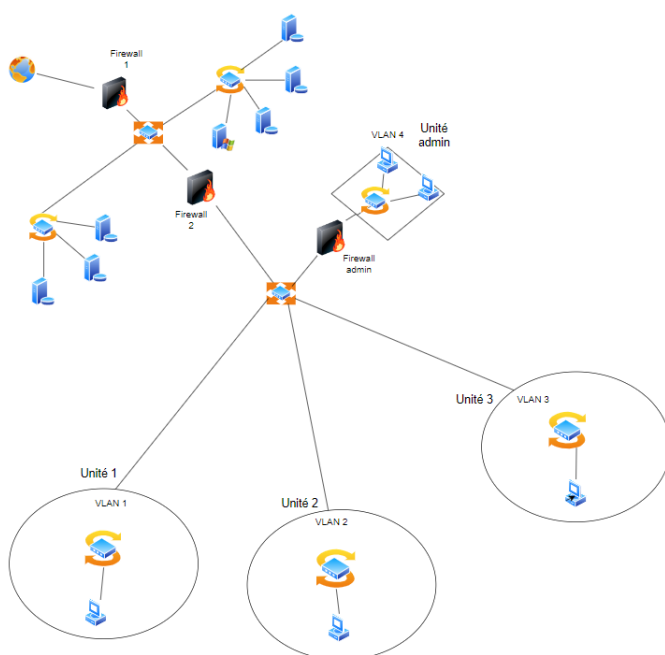
Page 11 : Adressage automatique

Page 12 : Un peu d'imagination

### Avant-propos :

La mise en place d'un Active Directory (AD) est un élément crucial pour les entreprises qui souhaitent centraliser la gestion de leurs utilisateurs, machines et services au sein d'un environnement Windows. L'AD offre non seulement une plateforme unifiée pour l'authentification et l'autorisation, mais il sert également de pierre angulaire pour d'autres services essentiels tels que DNS et DHCP.

### 1 – Schéma Infrastructure :



**Firewall** : Ici nous avons la présence de 3 firewalls au total, le premier (1) est présent pour sécuriser le réseau entrant par sa présence entre les salles de serveurs et le branchement à internet, il peut aussi permettre la sécurisation du réseau sortant. Le second firewall (2) quant à lui permet de sécuriser les serveurs des utilisateurs du réseau de l'entreprise. Enfin le firewall admin sert à isoler les admins du reste des utilisateurs afin d'éviter une attaque interne provenant de l'unité admin ou d'une des 3 unités.

**Routeur** : L'utilisation de routeurs

FIGURE 1 : SCHEMA D'INFRASTRUCTURE RESEAU POSSIBLE

centraux ont un rôle diviseur, afin de dissocier/diviser les différentes unités en sous réseaux. Cela permet d'isoler le trafic.

**Switch** : Utilisation pour augmenter les performances en comparaison de l'utilisation d'un routeur et moins coûteux, et permet surtout déplacement rapide d'informations dans leurs sous réseau

**Vlan** : Ici nous retrouvons 4 Vlan, 3 utilisateurs et 1 administrateur afin d'isoler les admins du reste des utilisateurs pour une meilleure sécurisation du réseau, du fait de l'utilisation d'un routeur central nous pouvons isoler ou non chaque Vlan indépendamment et ainsi avoir une meilleure gestion.

**Serveur** : Ici nous avons deux salles de serveurs isolable l'une de l'autre grâce au routeur central. L'intérêt d'une telle architecture serait d'attribuer une redondance entre les deux salles DNS, Active Directory, Data base etc... Ici je n'ai mis qu'un AD mais nous pouvons en ajouter un autre dans la seconde salle afin d'avoir une redondance et en cas d'attaque isoler une salle des serveurs.

## **2 – Powershell :**

### **L'utilisation d'un script à plusieurs points positif :**

L'automatisation des tâches, un script permet une exécution rapide tâches du fait qu'il exécute automatiquement une série d'instructions.

Une fois un script écrit il peut être portable et réutilisable, il permet aussi une modification plus rapide car nous ne devons chaque fois pas tout recommencer.

Ici nous pouvons déployer un petit script afin d'installer l'Active directory.

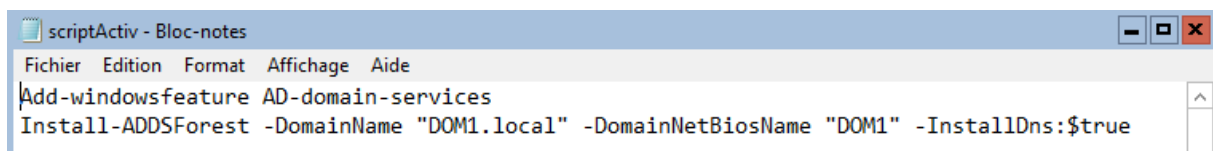


FIGURE 2 : SCRIPT INSTALLATION AD

« **Add-WindowsFeature AD-domain-services** » Ajoute le service Active directory à une instance de Windows.

« **DomainName** » est une option afin de donner un nom au domaine ici DOM1.local

« **DomainNetBiosName** "DOM1" », permet de définir le nom NetBIOS d'un domaine ici il porte un nom raccourci de celui du domaine

« **InstallDns:\$true** » Cette option indique que le DNS doit être installé en même temps que le contrôleur de domaine.

Nous pouvons aussi utiliser un script pour ajouter un contrôleur de domaine dans l'AD existante.

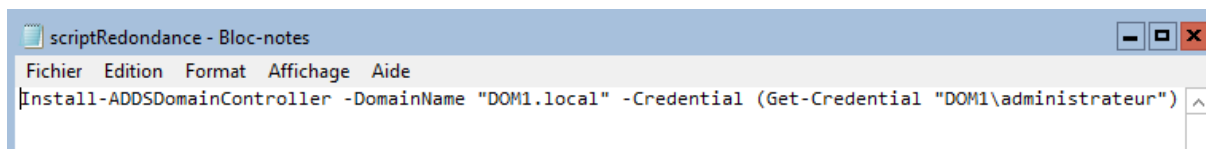


FIGURE 3: SCRIPT AJOUT D'UN CONTROLEUR DE DOMAINE

Et nous pouvons donc faire la totalité des instructions PowerShell d'un projet en script, l'intérêt reste de pouvoir réutiliser et exécuter plus rapidement les commandes, il faut donc sélectionner les scripts construits.

### 3 – Mise en place d'un active directory

#### Préparation de l'installation d'un active directory :

Après l'installation d'un VM sur ma machine je monte un ISO de Windows Server 2019, afin de travailler dessus.

Plusieurs étapes clés sont essentielles avant de commencer, premièrement sur les options de notre image ISO montée nous devons définir le « network » comme « internal » car par la suite nous allons faire communiquer plusieurs postes afin d'imager l'utilisation d'un AD.

Nous pouvons par la suite lancer l'iso que j'appellerai « windows10 ».

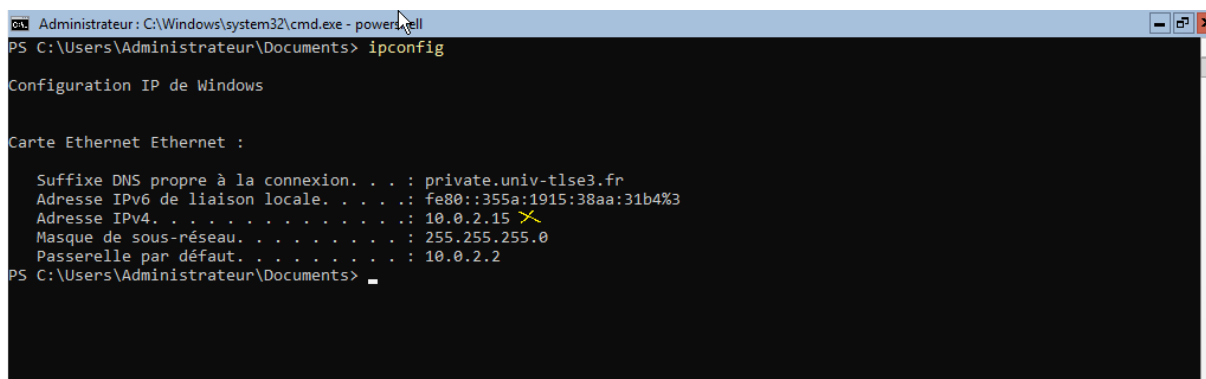


FIGURE 4: IPCONFIG VERIFICATIONS D'INFORMATIONS

A l'aide de la commande « ipconfig » nous pouvons vérifier que l'adresse IP n'est pas conforme aux demandes car nous voulons une adresse IP en 192.168.XXX.XXX par convention dans les petites entreprises. Or ici nous avons une adresse en 10.0.XXX.XXX. Nous devons donc la changer.

```
PS C:\Users\Administrateur\Documents> gip

InterfaceAlias      : Ethernet
InterfaceIndex      : 3
InterfaceDescription : Intel(R) PRO/1000 MT Desktop Adapter
NetProfile.Name     : Réseau
IPv4Address         : 10.0.2.15
IPv6DefaultGateway  :
IPv4DefaultGateway  : 10.0.2.2
DNSServer           : 130.120.124.102
                   : 195.220.43.67
```

FIGURE 5 GIP

Avant toutes choses vérifions avec GIT l'interface Alias qui nous servira au changement de l'IP ici il nous indique une interface Alias en « Ethernet ».

```
Administrateur : C:\Windows\system32\cmd.exe - powershell
PS C:\Users\Administrateur> Set-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 192.168.0.1 -PrefixLength 24
```

FIGURE 6: CHANGEMENT D'IP ET DE MASQUE

Avec ces informations nous pouvons enfin changer d'adresse IP avec « Set-NetIPAddress » (Set communément utilisé pour attribuer et Get pour donner/afficher) avec pour option l'interface alias vérifié avec GIP, la nouvelle adresse IP ici ce sera le poste 1 de notre réseau donc 192.168.0.1 et « prefixLength » servira à changer le masque en 255.255.255.0 essentiel afin de faire communiquer nos futurs VM.

### Installation de l'Active Directory :

Active Directory (AD) est un service d'annuaire développé par Microsoft pour les environnements Windows Server. Il fournit une variété de fonctions de réseau, notamment :

La gestion centralisée des utilisateurs et des ordinateurs : AD permet aux administrateurs de créer, de gérer et de supprimer des comptes utilisateurs et ordinateurs à partir d'un emplacement centralisé.

Authentification et autorisation : Active Directory utilise la technologie Kerberos pour authentifier les utilisateurs et les ordinateurs dans un réseau. Une fois authentifié, AD gère également les autorisations des utilisateurs, c'est-à-dire ce qu'ils sont autorisés à faire ou à accéder sur le réseau.

Gestion des politiques de groupe (GPO) : AD permet aux administrateurs de définir des politiques pour des ordinateurs ou des utilisateurs spécifiques. Ces politiques peuvent déterminer des aspects tels que les paramètres de sécurité, les installations de logiciels ou les paramètres de configuration.

Il existe de nombreuses autres utilisations mais que nous n'aborderons pas dans ce TP.

```
Administrateur: C:\Windows\system32\cmd.exe - powershell
PS C:\Users\Administrateur\Documents> ls

Répertoire : C:\Users\Administrateur\Documents

Mode                LastWriteTime         Length Name
----                -
-a----          17/10/2023   18:52             131 scriptActiv.ps1

PS C:\Users\Administrateur\Documents> cat .\scriptActiv.ps1
Add-windowsfeature AD-domain-services
Install-ADDSForest -DomainName "DOM1.local" -DomainNetBiosName "DOM1" -InstallDns:$true
PS C:\Users\Administrateur\Documents> .\scriptActiv.ps1
```

FIGURE 7: EXECUTION DU SCRIPT D'INSTALLATION DE L'AD

Nous allons donc exécuter le script construit plus tôt (cf. Figure 2) afin d'installer l'Active directory sur cette machine.

Ici la commande « Cat » n'a que pour intérêt d'afficher le contenu du script afin de savoir de quoi nous parlons.

### Mise en place de la redondance :

La redondance, en informatique et dans de nombreux autres domaines, désigne la duplication de composants ou de fonctions pour fournir une sauvegarde en cas de défaillance d'un élément. Elle vise à augmenter la fiabilité d'un réseau en assurant son fonctionnement continu même en présence de pannes. Voici l'intérêt général de la redondance, puis l'intérêt spécifique de la redondance d'un Active Directory (AD) :

### **Intérêt de la Redondance en informatique :**

- Disponibilité accrue : La redondance garantit que si un composant tombe en panne, le réseau continue de fonctionner grâce au composant redondant.
- Tolérance aux pannes : Dans un réseau redondant, les pannes peuvent être gérées sans interruption de service, car un autre composant peut prendre le relais.
- Maintenance simplifiée : Les composants peuvent être remplacés ou mis à niveau sans arrêter le réseau entier.
- Performance : Dans certaines configurations, la redondance peut aussi augmenter les performances. Par exemple, en utilisant plusieurs serveurs pour répartir la charge de travail.

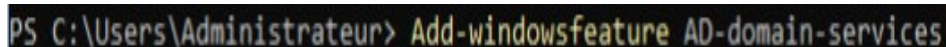
## Intérêt de la Redondance d'un Active Directory :

- Disponibilité continue des services d'annuaire : Si un contrôleur de domaine (DC) tombe en panne, les autres DC peuvent continuer à fournir des services d'authentification et d'annuaire à l'organisation.
- Équilibrage de charge : Dans les grandes entreprises, un seul DC peut ne pas être en mesure de gérer toutes les demandes d'authentification. Avoir plusieurs DC permet de répartir la charge.
- Réduction des temps d'arrêt lors des maintenances : Si un DC nécessite une maintenance, les services d'annuaire ne sont pas interrompus car les autres DC sont toujours actifs.
- Réplication et intégrité des données : La réplication entre les DC assure que toutes les modifications apportées à l'annuaire sont synchronisées. Cela garantit la cohérence et l'intégrité des données d'annuaire.
- Optimisation des performances pour les utilisateurs distants : Dans les organisations réparties géographiquement, la présence de DC dans différents emplacements peut réduire les temps de latence pour les utilisateurs distants, car ils peuvent se connecter au DC le plus proche.

Donc, la redondance d'AD est essentielle pour assurer la disponibilité, la performance et la résistance dans le temps des services d'annuaire dans une entreprise. Sans redondance, une défaillance d'un contrôleur de domaine pourrait entraîner des perturbations majeures voir un arrêt total du service. Son utilisation est donc primordiale.

Pour intégrer une redondance nous devons tout d'abord intégrer une nouvelle machine afin de l'utiliser comme redondance de l'active directory.

Nous allons donc procéder aux étapes de préparations déjà expliqué de la figure 4 à la figure 6 (changement d'IP et masque)



```
PS C:\Users\Administrateur> Add-windowsfeature AD-domain-services
```

FIGURE 8: FONCTIONNALITE ACTIVE DIRECTORY DOMAIN SERVICES (AD DS)

« Add-WindowsFeature » est une commande pour ajouter un rôle ou des fonctionnalités à un ordinateur, dans ce cas précis « Ad-domain-services » spécifie la fonctionnalité du service Active Directory.

```

C:\Windows\system32\cmd.exe - powershell
PS C:\Users\Administrateur> Get-NetNeighbor

ifIndex IPAddress LinkLayerAddress State PolicyStore
-----
6 ff02::1:fffc:2203 33-33-FF-FC-22-03 Permanent ActiveStore
6 ff02::1:3 33-33-00-01-00-03 Permanent ActiveStore
6 ff02::1:2 33-33-00-01-00-02 Permanent ActiveStore
6 ff02::fb 33-33-00-00-00-FB Permanent ActiveStore
6 ff02::16 33-33-00-00-00-16 Permanent ActiveStore
6 ff02::2 33-33-00-00-00-02 Permanent ActiveStore
6 ff02::1 33-33-00-00-00-01 Permanent ActiveStore
1 ff02::1:2 Permanent ActiveStore
1 ff02::16 Permanent ActiveStore
6 224.0.0.252 01-00-5E-00-00-FC Permanent ActiveStore
6 224.0.0.251 01-00-5E-00-00-FB Permanent ActiveStore
6 224.0.0.22 01-00-5E-00-00-16 Permanent ActiveStore
6 192.168.0.1 00-00-00-00-00-00 Unreachable ActiveStore
1 224.0.0.22 Permanent ActiveStore

```

FIGURE 9 VERIFICATION DU NUMERO D'INDEX

Le numéro d’index, fait référence à l’index de l’interface réseau sur le réseau. C’est un identifiant unique attribué à chaque interface réseau de l’ordinateur. Il permet de distinguer et d’identifier de manière unique chaque interface, surtout si plusieurs interfaces réseau sont présentes sur le réseau.

Dans ce cas nous pouvons retenir le numéro d’index utile pour la configuration de l’adresse DNS

```

C:\Windows\system32\cmd.exe - powershell
PS C:\Users\Administrateur.DOM1> Set-DnsClientServerAddress -InterfaceIndex 6 -ServerAddresses 192.168.0.1
PS C:\Users\Administrateur.DOM1>

```

FIGURE 10: ATTRIBUTION ADRESSE DNS

Nous attribuons l’adresse DNS à l’adresse 192.168.0.1 ici notre machine 1 (notre AD) à notre machine 2.

Ainsi, cette commande configure l’interface réseau avec l’index 6 pour utiliser 192.168.0.1 comme son serveur DNS.

```

PS C:\Users\Administrateur> Install-ADDSDomain -DomainName "DOM1.local" -Credential (get-Credential "DOM1\administrat

```

FIGURE 11 INSTALLATION REDONDANCE DOM1.LOCAL

Nous pouvons donc installer la redondance sur la machine 2 de la machine 1 « DOM1 » comme indiqué dans le script (cf. Figure 2).



### Test de la redondance :

Pour tester de la redondance nous allons donc devoir intégrer une nouvelle machine sur le réseau, car nous allons l'une à la suite de l'autre mettre hors service les deux AD afin de vérifier que l'un prend le relais de l'autre en l'occurrence ici le serveur 2 qui prend le relais sur le serveur 1.

Nous allons donc commencer en faisant le test pour un service non modifié donc aucun serveur n'est interrompu.

NB : L'arrêt d'un serveur se fera en stoppant simplement sa VM.

```
Sélection Administrateur : C:\Windows\system32\cmd.exe - powershell
PS C:\Users\Administrateur> tracert DOM1.local

Détermination de l'itinéraire vers DOM1.local [192.168.0.1]
avec un maximum de 30 sauts :

  1      1 ms    <1 ms    <1 ms    WIN-GBJ531G1RU8 [192.168.0.1]

Itinéraire déterminé.
```

FIGURE 12: AUCUN SERVEUR A L'ARRET

La commande tracert est utilisée pour afficher la route suivie par les paquets pour atteindre une destination réseau et indiquer le temps pris pour atteindre chaque saut le long de cette route.

Ici nous pouvons voir que cette commande affiche bien notre AD en fonctionnement 192.168.0.1, le serveur 1.

```
PS C:\Users\Administrateur> tracert DOM1.local

Détermination de l'itinéraire vers DOM1.local [192.168.0.2]
avec un maximum de 30 sauts :

  1      1 ms    <1 ms    <1 ms    WIN-3B9V4A41MK0 [192.168.0.2]

Itinéraire déterminé.
PS C:\Users\Administrateur>
```

FIGURE 13: ARRET SERVEUR 1

Suite à l'arrêt du serveur AD de la machine 1, nous pouvons donc constater que la commande tracert vers DOM1.local nous conduit bien sur le serveur 2, 192.168.0.2.

Nous pouvons donc conclure que la redondance marche car le serveur 2 a bien prit le relais suite à l'arrêt du 1.

```
Administrateur : C:\Windows\system32\cmd.exe - powershell
PS C:\Users\Administrateur> tracert DOM1.local

Détermination de l'itinéraire vers DOM1.local [192.168.0.1]
avec un maximum de 30 sauts :

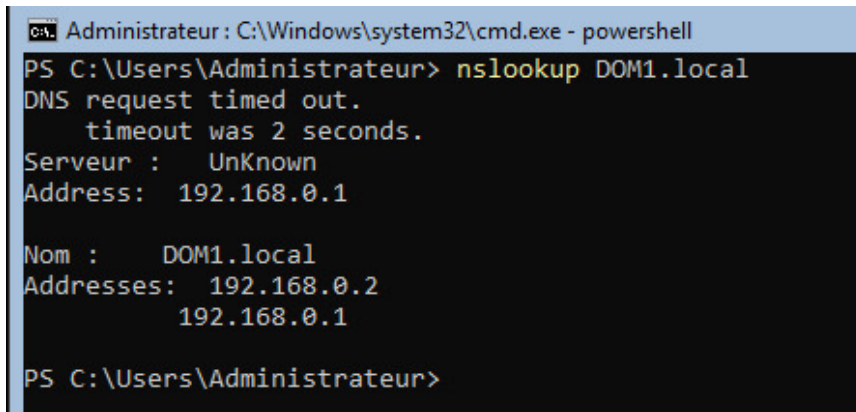
  1      <1 ms    <1 ms    <1 ms    WIN-GBJ531G1RU8 [192.168.0.1]

Itinéraire déterminé.
PS C:\Users\Administrateur>
```

Ici nous avons stoppé le serveur 2 pour bien vérifier que la serveur 1 joue encore son rôle d'AD

FIGURE 14: ARRET SERVEUR 2

Nous pouvons vérifier ces demandes avec une commande « nslookup » ainsi :



```
Administrateur : C:\Windows\system32\cmd.exe - powershell
PS C:\Users\Administrateur> nslookup DOM1.local
DNS request timed out.
    timeout was 2 seconds.
Serveur : UnKnown
Address: 192.168.0.1

Nom :      DOM1.local
Addresses: 192.168.0.2
           192.168.0.1

PS C:\Users\Administrateur>
```

FIGURE 15 VERIFICATION DE REDONDANCE

Cette commande permet de vérifier la redondance sans mise en situation, ici elle indique à la machine 3 qui demande le DOM1.local (l'AD), que l'AD est intégré au serveur 1 et 2.

Nous pouvons donc affirmer par double vérification que notre redondance marche.

#### 4 – Convaincre :

Au départ, il est essentiel d'évaluer la pertinence d'accorder des droits administrateurs au directeur sur l'Active Directory. Nous disposons au moins d'un employé qualifié (moi-même) pour gérer l'administration réseaux. Par conséquent, il n'est pas judicieux d'exposer inutilement le réseau à des risques en octroyant des droits administrateurs au directeur.

Les enjeux de sécurité sont primordiaux. Une erreur, telle que l'octroi de droits à une personne non autorisée, pourrait donner accès à des informations sensibles. De plus, toute maladresse pourrait entraîner une perte de données, nécessitant une restauration à partir d'un serveur redondant, et engendrant ainsi une instabilité du réseau.

Le risque d'une éventuelle intrusion externe, offrant un accès à des tiers aux informations critique de l'entreprise, est également à prendre en compte. Il est crucial de se rappeler qu'aucun réseau de sécurité n'est infaillible ; minimiser les points de vulnérabilité est donc primordial pour réduire les incidents de sécurités.

Nous pouvons donc proposer au directeur de passer un formation/certification adéquate afin de pouvoir gérer comme il se doit son réseau.

Si en revanche le directeur nous oblige à lui donner les droits nous lui rédigerons un document indiquant que nous nous déchargeons de tout problèmes causés par sa personne dans le cadre de l'administration réseau de cette entreprise.

## 5 – Adressage automatique :

Un serveur DHCP attribue automatiquement des adresses IP aux dispositifs d'un réseau, facilitant ainsi leur configuration et gestion. Nous pouvons donc suite à ça un réseau avec des entrant et des sortants beaucoup plus simple de gestion comme dans le cas d'une faculté par exemple

Ici nous initialiserons un serveur 4 comme au paravent, jouant le rôle de DHCP

```
PS C:\Users\Administrateur> Install-WindowsFeature DHCP

Success Restart Needed Exit Code      Feature Result
-----
True      No                Success      {Serveur DHCP}
```

FIGURE 16: INSTALLATION DU ROLE DE DHCP

Après l'installation du DHCP nous lui donnerons une portée afin de l'initialiser avant fonctionnement.

```
CA. Administrateur : C:\Windows\system32\cmd.exe - powershell
PS C:\Users\Administrateur> Add-DhcpServer4Scope -Name "Scope1" -StartRange 192.168.0.5 -EndRange 192.168.0.55
-SubnetMask 255.255.255.0
```

FIGURE 17: INITIALISATION DHCP

Ici nous initialisons une portée au DHCP afin de lui donner une contenance maximum d'utilisateurs, ici nous lui donnerons la possibilité d'avoir 50 utilisateurs ce qui permettrait de ne pas trop solliciter le réseau afin de permettre sa stabilité.

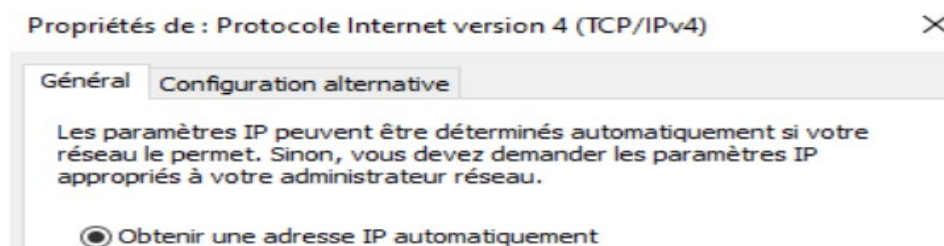


FIGURE 18: OBTENTION D'ADRESSAGE AUTOMATIQUE D'UN DHCP

En accédant aux menus propriétés de : Protocole Internet V4 nous pouvons sélectionner l'option d'attribution automatique d'IP par le DHCP

```
Adresse IPv4. . . . . : 192.168.0.5
Masque de sous-réseau. . . . . : 255.255.255.0
```

FIGURE 19: TEST D'ATTRIBUTION D'IP

Suite à la configuration d'une nouvelle machine du réseau le DHCP joue correctement son rôle en attribuant une IP au nouvel arrivant. Il peut faire ça dans la capacité de 50 nouveaux arrivant. Le DHCP est donc fonctionnel

## 6 – Un peu d'imagination :

Pour sécuriser l'accès aux serveurs de l'AD, je mettrai en place :

- Un Firewall son rôle permettra de sécuriser les données à l'entrée et à la sortie afin de ne pas compromettre de données directement dans les serveurs.
- Réduire au minimum le nombre de service, car dans le cas d'une surcharge de service permettrai une intrusion plus facile car la maintenance sera plus complexe.
- Isolation du réseau, comme vu dans le schéma du réseau (cf. Figure 1) une isolation du reste du réseau permettra d'interrompre, d'isoler, d'interrompre en cas de problème majeur, et de sécurisé physiquement les serveurs.
- Une équipe de surveillance permettant une régulation des mises à jour de sécurité, une bonne maintenance et une veille technologique sur les nouvelles failles rencontrées.

Il existe de nombreux protocoles de sécurisation d'un réseau mais beaucoup de critères rentrent en compte tel que le prix, le temps de déploiement, la maintenance disponible etc... c'est donc pourquoi un audit doit être fait dans ce contexte.