

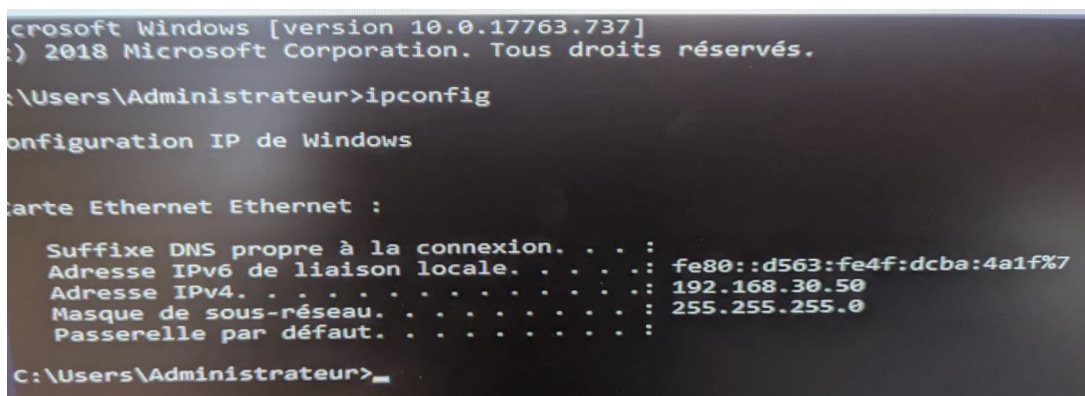
1.Introduction

Ce Rapport a pour objectif de mettre en place un serveur DHCP sur Windows Server 2019, avec un client Windows 10. Pour cela, nous utilisons deux ordinateurs avec une machine virtuel sur chacun des ordinateurs, un switch, un câble console, d'alimentation et deux câbles Ethernets.

2.Architecture

Windows Server 2019

- Rôle : serveur DHCP.
- Adresse IP statique : 192.168.30.50/24
- Réseau : Accès par pont



```
Microsoft Windows [version 10.0.17763.737]
(c) 2018 Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>ipconfig

Configuration IP de Windows

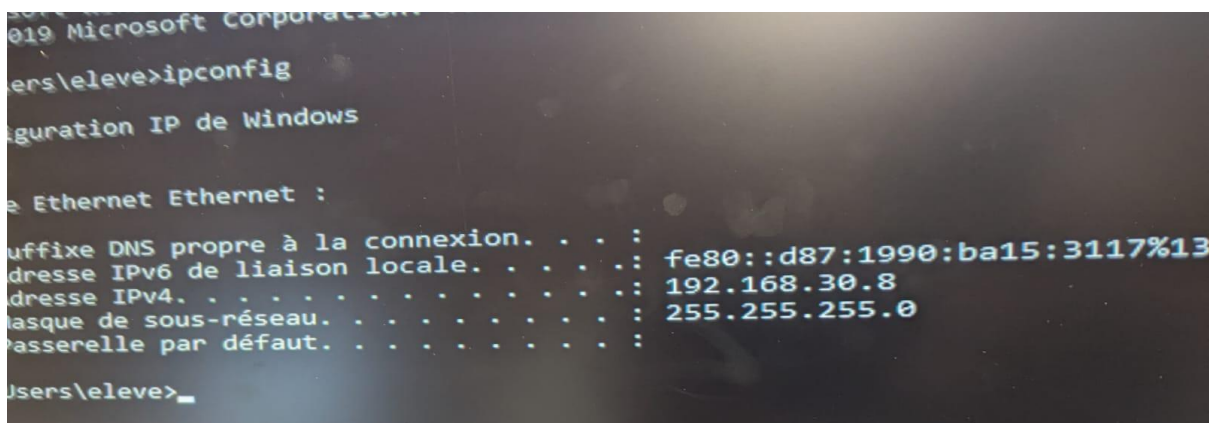
Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . . : 
    Adresse IPv6 de liaison locale. . . . . : fe80::d563:fe4f:dcba:4a1f%7
    Adresse IPv4. . . . . : 192.168.30.50
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 

C:\Users\Administrateur>
```

Windows 10

- Rôle : client DHCP.
- Adresse Ip statique : 192.168.30.8/24
- Réseau : Accès par pont



```
Microsoft Windows [version 10.0.17763.737]
(c) 2018 Microsoft Corporation. Tous droits réservés.

C:\Users\eleve>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . . : 
    Adresse IPv6 de liaison locale. . . . . : fe80::d87:1990:ba15:3117%13
    Adresse IPv4. . . . . : 192.168.30.8
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 

C:\Users\eleve>
```

3. Réinitialisation du Commutateur

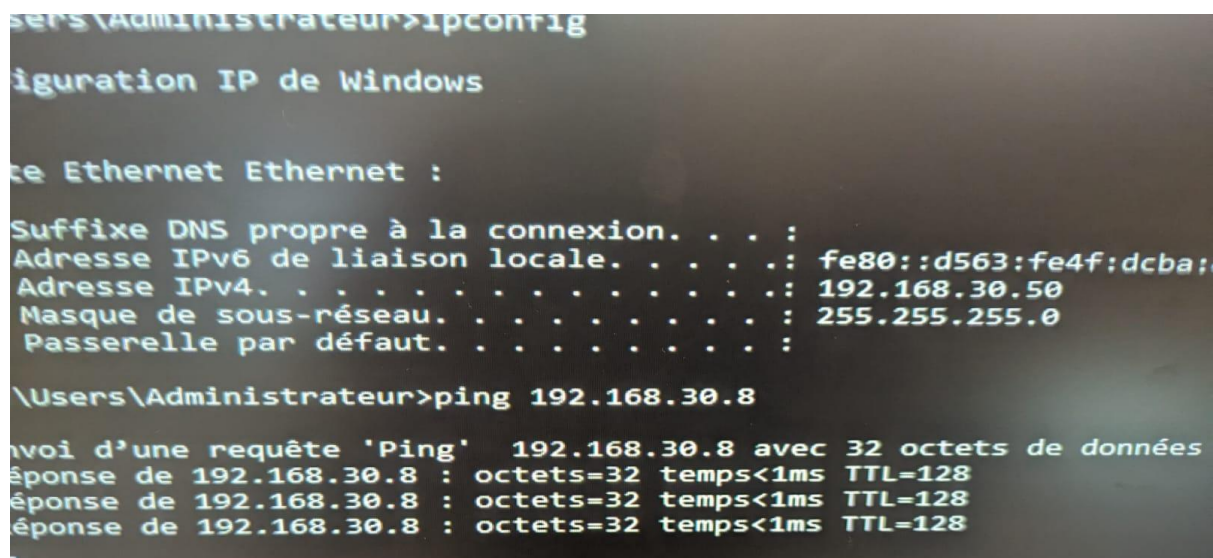
ACCEDER AU BOOT LOADER

- Connectez le câble console entre votre PC et le port console du commutateur.
- Maintenez le bouton MODE enfoncé, puis branchez le câble d'alimentation tout en continuant d'appuyer sur le bouton MODE.
- Relâchez le bouton MODE lorsque :
 - La LED supérieure (SYST) clignote en orange, puis devient verte en continu,
 - Le message "The password-recovery mechanism is enabled" apparaît dans le terminal.

REINITIALISER LE SWITCH

- flash_init : pour initialiser la mémoire Flash
- dir flash: pour afficher le contenu
- del flash:config.text pour supprimer la configuration
- boot pour relancer le commutateur

4. Test de Connectivité



```
Users\Administrateur>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet :

Suffixe DNS propre à la connexion. . . . :
Adresse IPv6 de liaison locale. . . . .: fe80::d563:fe4f:dcba:
Adresse IPv4. . . . .: 192.168.30.50
Masque de sous-réseau. . . . .: 255.255.255.0
Passerelle par défaut. . . . .:

Users\Administrateur>ping 192.168.30.8

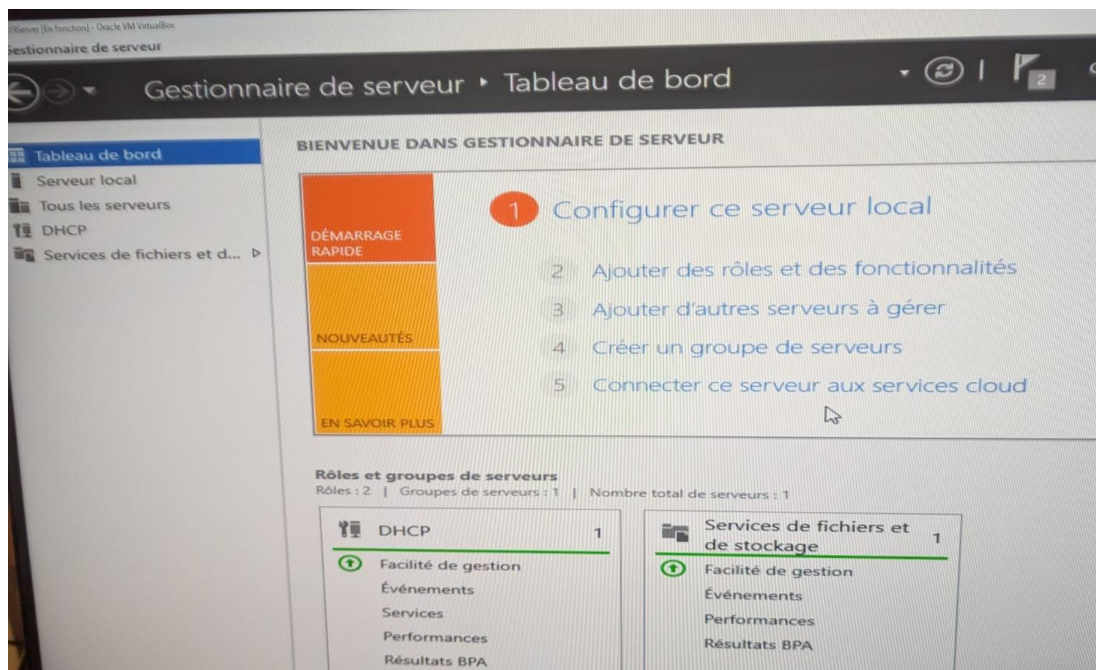
Envoi d'une requête 'Ping' 192.168.30.8 avec 32 octets de données
Réponse de 192.168.30.8 : octets=32 temps<1ms TTL=128
Réponse de 192.168.30.8 : octets=32 temps<1ms TTL=128
Réponse de 192.168.30.8 : octets=32 temps<1ms TTL=128
```

Envoi d'un ping depuis le serveur Windows Server 2019 vers l'adresse le client Windows 10. On peut voir que les deux machines peuvent bien communiquer entre elle, cela signifie que le switch fonctionne bien et que les adresses sont correctement configurées.

5. Installation du Rôle DHCP

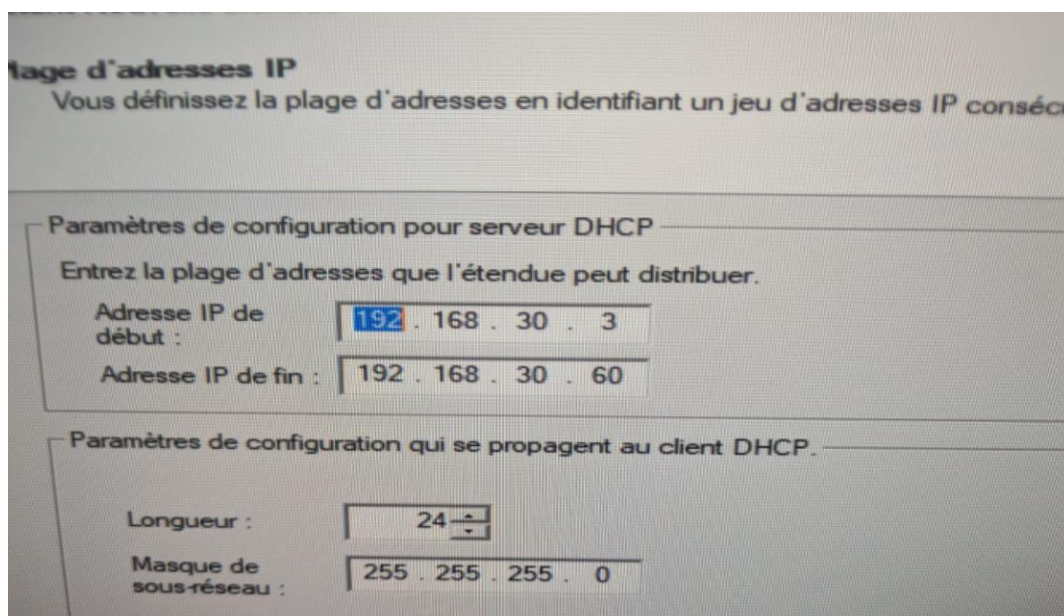
- Tout d'abord vous devez ouvrir le gestionnaire de serveur, ensuite cliquer sur Gérer, puis choisir Ajouter des rôles et des fonctionnalités.
- Dans "Selection Server " choisir Windows Server 2019
- Dans "Rôles Server" choisir serveur DHCP
- Enfin, cliquez sur Installer.

Une fois l'installation terminée, vous devriez voir une fenêtre avec DHCP d'actif comme ci-dessous



6. Configuration d'une Étendue DHCP

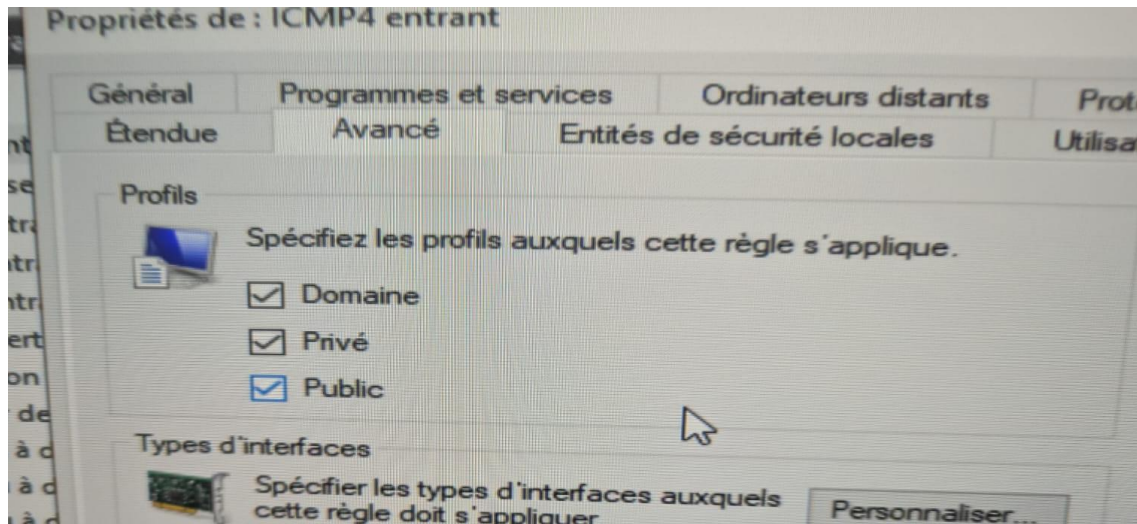
Développez IPv4, clic droit → Nouvelle étendue



7. Configuration du Pare-feu pour ICMP

Avant de vérifier que notre serveur DHCP distribue correctement une adresse IP, nous devons régler le profil du pare-feu en "Public" pour autoriser les requêtes ICMP

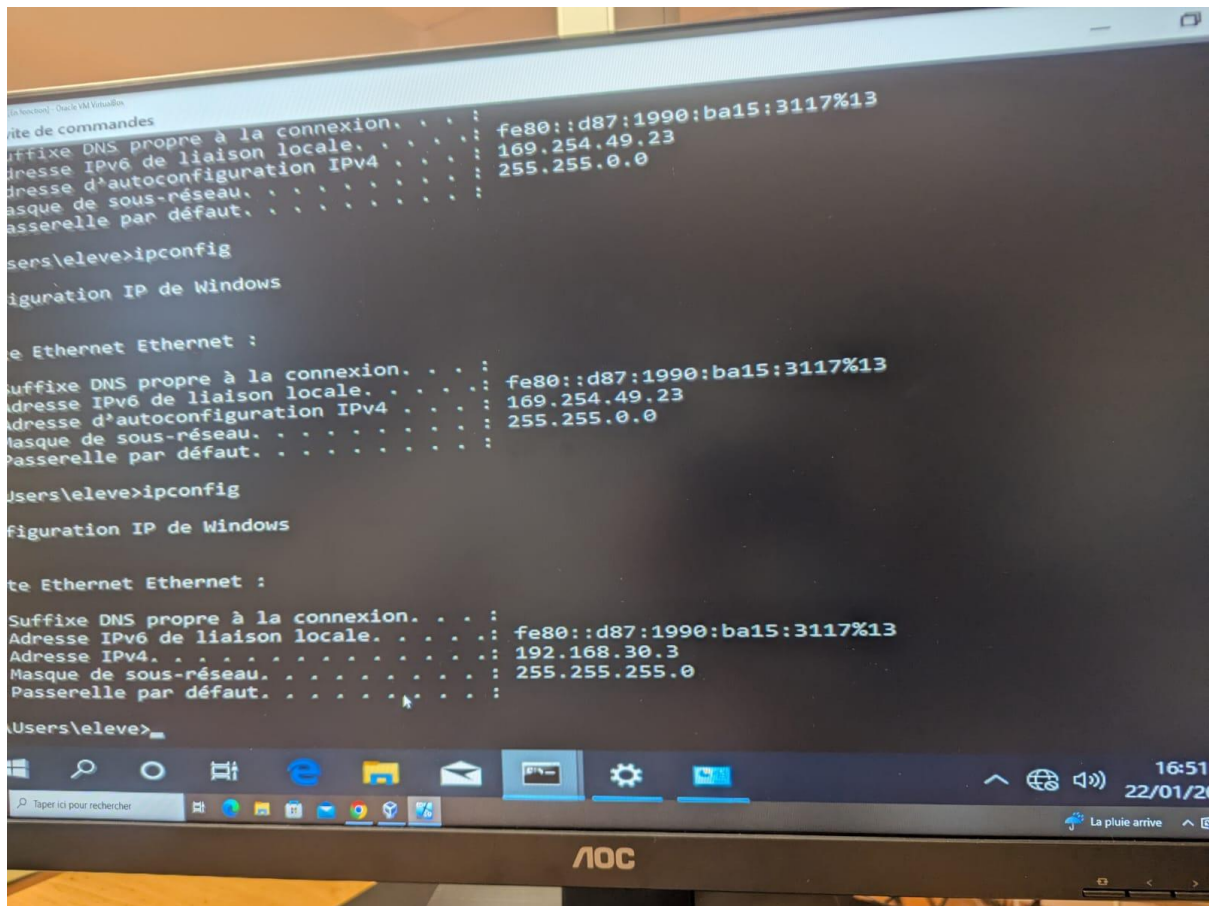
Gestionnaire de serveur → Outils → Pare-feu Windows avec fonctions avancées



Nous avons choisi de créer manuellement une règle temporaire de de pare-feu pour autoriser le trafic ICMP entrant et sortant sur le serveur, plutôt que d'activer la fonctionnalité de "File and Printer Sharing

- Dans Pare-feu Windows avec fonctions avancées, allez dans Règles de trafic entrant puis cliquez sur Nouvelle règle...
- Choisissez Personnalisée → Protocole ICMPv4 → Autoriser la connexion → Sélectionnez les profils → Donnez un nom à la règle
- Validez.

Après validation, vous verrez apparaître, dans la liste des règles de trafic entrant et sortant, ICMP4 entrant et ICMP4 sortant.



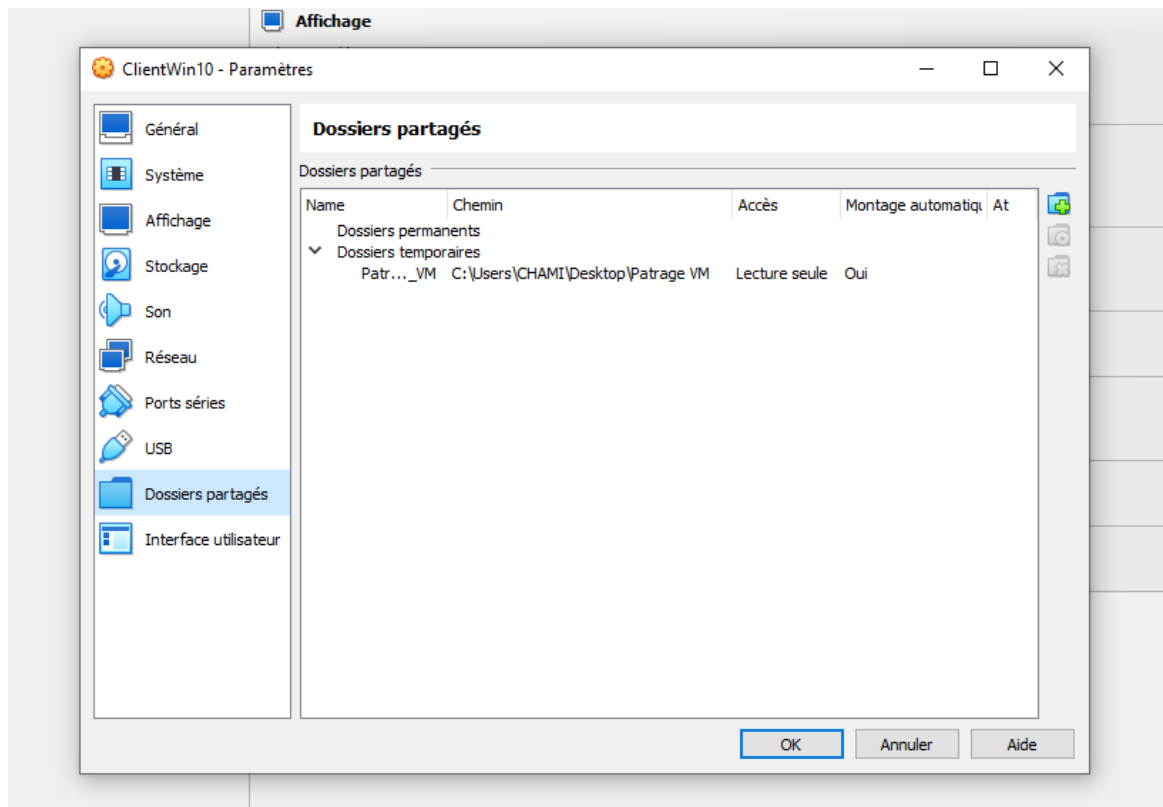
Lorsque nous passons la configuration réseau du poste client en IP dynamique, puis que nous vérifions l'adresse IP, nous constatons qu'elle a été mise à jour : le DHCP lui a attribué la première adresse disponible dans la plage (de 192.168.30.3 à 192.168.30.60).

Il est important de faire attention aux conflits d'adresses, car le serveur utilise une IP statique qui est 192.168.30.50 qui se situerait dans la même plage.

Dans notre cas, nous n'avons pas de problème car nous n'avons besoin que d'une seule adresse dynamique.

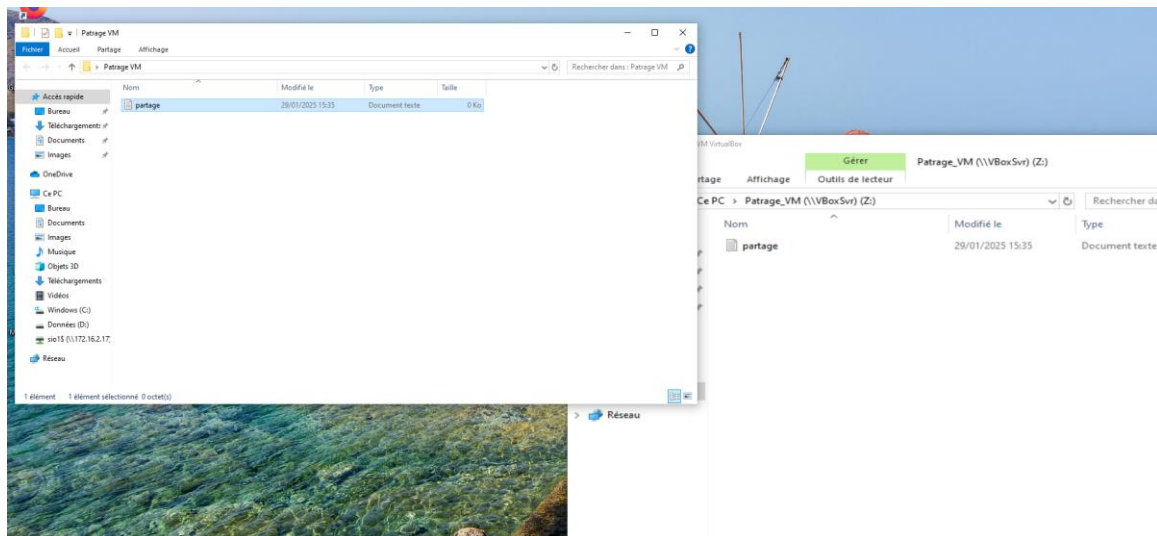
8.Installation de Wireshark pour l'Analyse Réseau

Maintenant nous devons installer WireShark sur le client afin de capturer des trames, pour cela nous devons faire un dossier partagé entre notre machine virtuel et machine physique afin de déplacer Wireshark dans ce dossier. Nous devons utiliser cette méthode car nous n'avons pas d'accès à internet sur la machine virtuel.



- Cliquez sur l'icône “+”
- Parcourez votre ordinateur hôte et sélectionnez le dossier
- Donnez un nom de partage
- Coché sur montage automatique et lecture seul

Résultat attendu



Maintenant que nous avons installé Wireshark, nous avons décidé de capturer le trafic réseau pour analyser les échanges ICMP entre le serveur et le client.

No.	Time	Source	Destination	Protocol	Length	Info
17	26.063985	Cisco_3e:2c:13	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/1/50:1c:bf:3
18	26.589556	192.168.30.50	192.168.30.3	ICMP	74	Echo (ping) request id=0x0001,
19	26.589636	192.168.30.3	192.168.30.50	ICMP	74	Echo (ping) reply id=0x0001,
20	27.607414	192.168.30.50	192.168.30.3	ICMP	74	Echo (ping) request id=0x0001,
21	27.607487	192.168.30.3	192.168.30.50	ICMP	74	Echo (ping) reply id=0x0001,
22	28.068490	Cisco_3e:2c:13	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/1/50:1c:bf:3
23	28.622630	192.168.30.50	192.168.30.3	ICMP	74	Echo (ping) request id=0x0001,
24	28.622724	192.168.30.3	192.168.30.50	ICMP	74	Echo (ping) reply id=0x0001,
25	29.637753	192.168.30.50	192.168.30.3	ICMP	74	Echo (ping) request id=0x0001,
26	29.637825	192.168.30.3	192.168.30.50	ICMP	74	Echo (ping) reply id=0x0001,

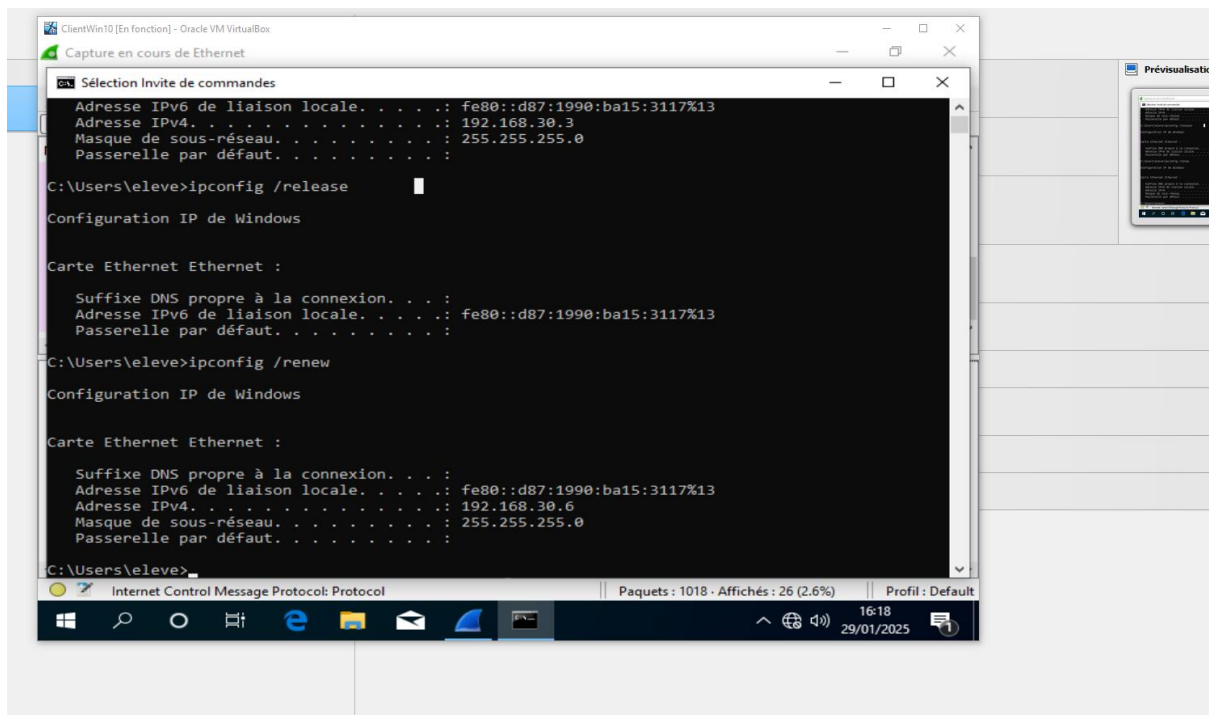
Dans la capture ci-dessus, on observe précisément les trames ICMP

Capture du trafic DHCP via Wireshark

Afin d'observer le processus d'attribution d'adresse IP entre le client et le serveur, nous allons forcer la libération puis la demande d'une nouvelle adresse via les commandes suivantes :

ipconfig /release : cette commande libère l'adresse IP actuelle du poste

ipconfig /renew : cette commande redemande une adresse IP au serveur DHCP



Nous pouvons observer dans Wireshark les quatre étapes :

DHCP Discover, DHCP Offer , IDHCP Request et DHCP Ack

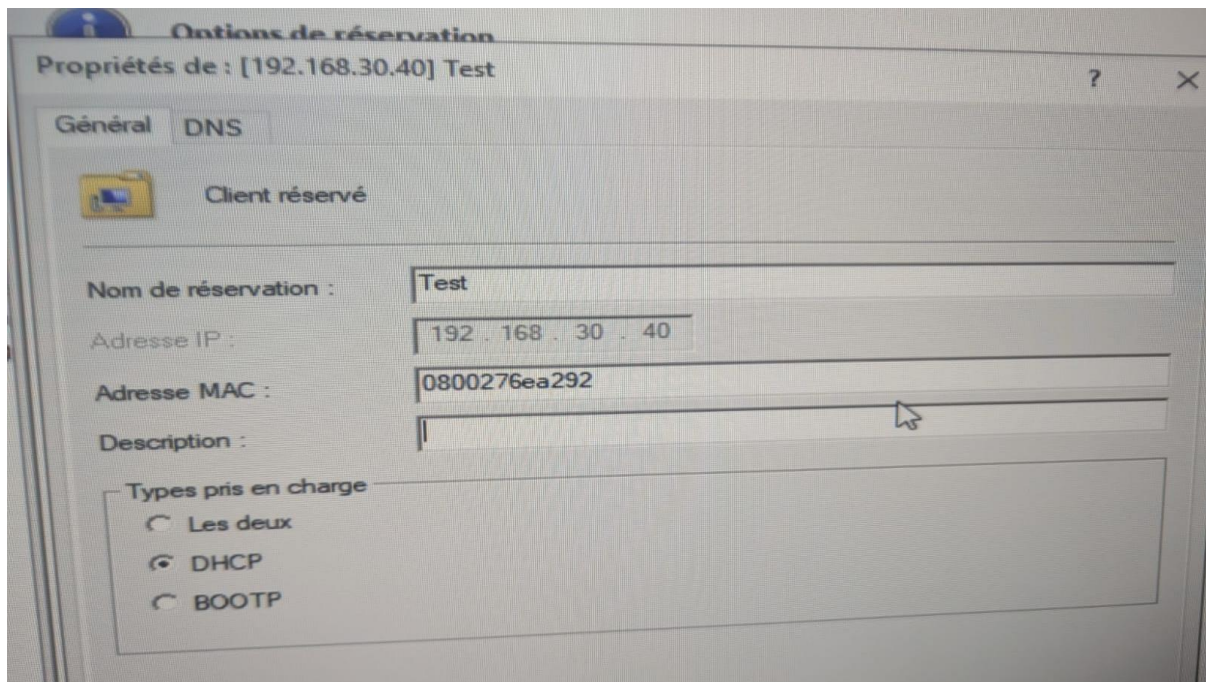
The screenshot shows a Wireshark packet capture of DHCP traffic. The filter is set to "dhcp". The following table represents the data shown in the packet list:

No.	Time	Source	Destination	Protocol	Length	Info
370	403.174432	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe1
371	403.177688	192.168.30.50	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xe1
372	403.178183	0.0.0.0	255.255.255.255	DHCP	368	DHCP Request - Transaction ID 0xe1
373	403.178956	192.168.30.50	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xe1

9. Mise en place d'une réservation d'adresse DHCP

Dans l'objectif de fournir toujours la même adresse IP à un client précis, nous pouvons configurer une réservation d'adresse dans la console DHCP.

1. Ouvrir la console DHCP (dans le Gestionnaire de serveur → Outils → DHCP).
2. Développer IPv4 → Clic droit sur Réservations → Nouvelle réservation.
3. Indiquer le Nom de réservation, l'Adresse IP, et l'Adresse MAC.
4. Choisir le DHCP en pris en charge
5. Valider en cliquant sur OK.



Nous pouvons voir que le DHCP a bien fournit au client l'adresse 192.168.30.40

```

Fichier  Éditer  Vue  Aller  Capture  Analyser  Statistiques  Téléphonie  Wireless  Outils  Aide
C:\Users\eleve>ipconfig /release

Configuration IP de Windows

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . . : 
    Adresse IPv6 de liaison locale. . . . . : fe80::d87:1990:ba15:3117%13
    Passerelle par défaut. . . . . : 

C:\Users\eleve>ipconfig /renew

Configuration IP de Windows

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . . : 
    Adresse IPv6 de liaison locale. . . . . : fe80::d87:1990:ba15:3117%13
    Adresse IPv4. . . . . : 192.168.30.40
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 

```