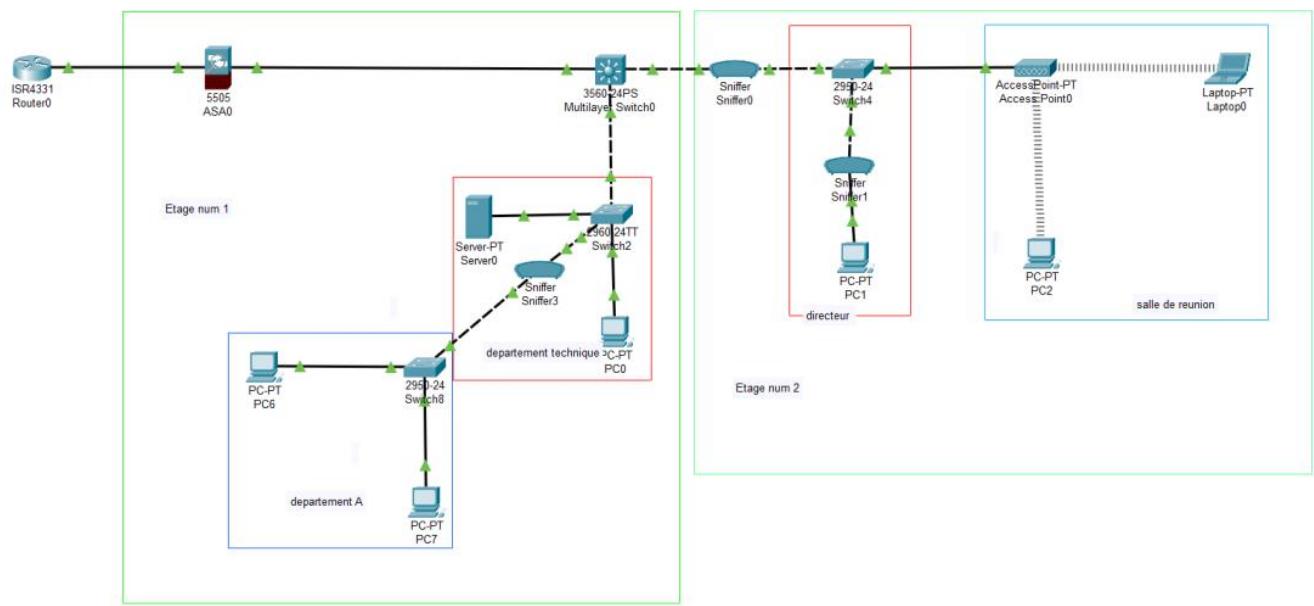
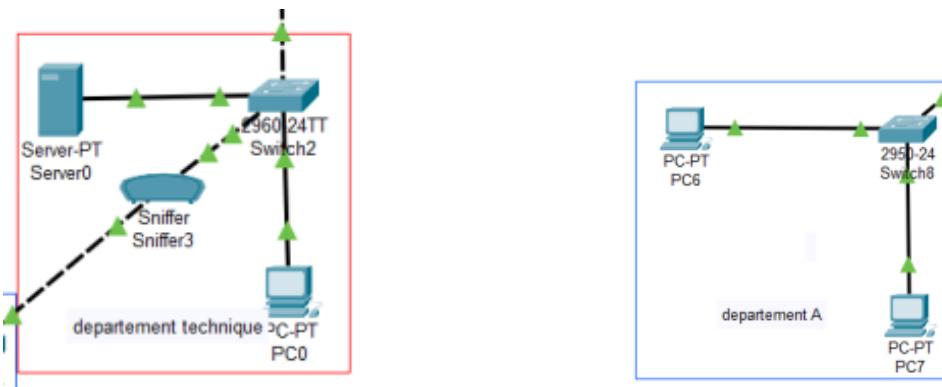


## 1. La réalisation :

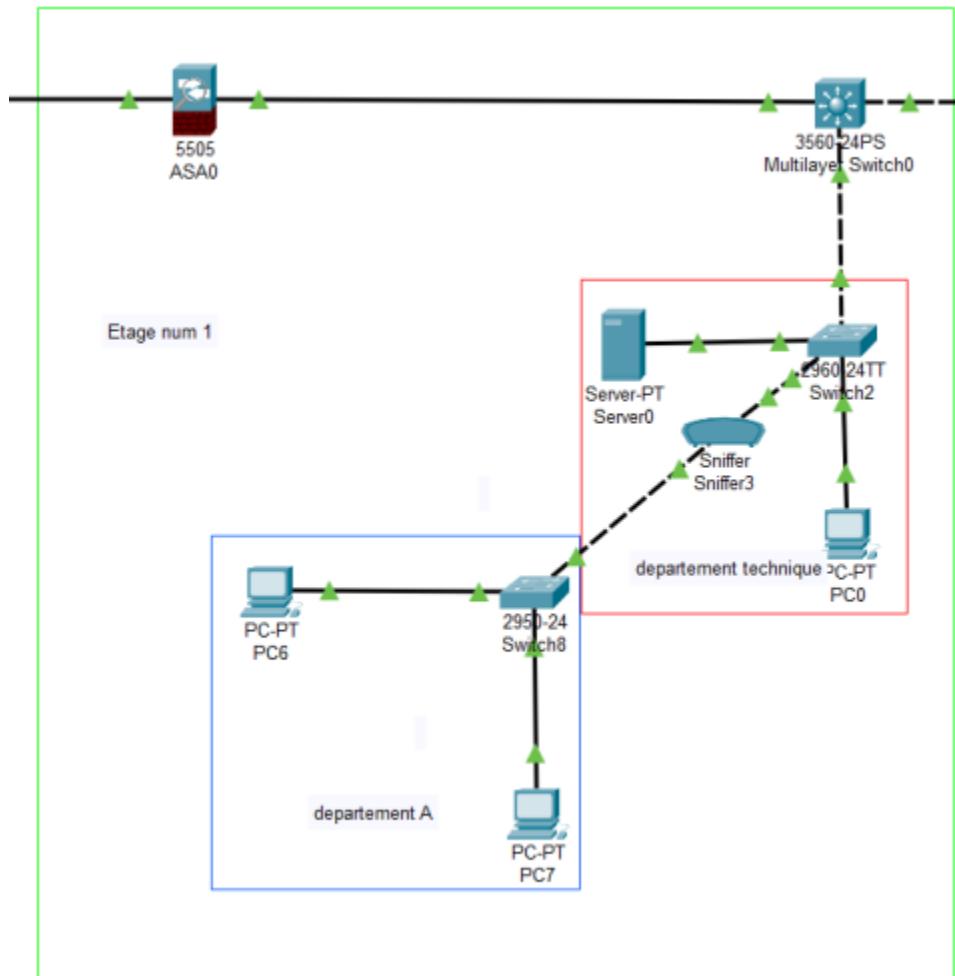
Un réseau Lan et très important pour une organisation pour cela il faut toujours être sûr qu'il fonctionne proprement pour cela on a réalisé une cartographie logique et même physique grâce au logiciel fameux **Packet Tracer** qui est un logiciel développer par **Cisco Systems** et qui permet aux utilisateurs de concevoir et tester des réseaux informatiques dans des simulation comme on a fait maintenant dans notre simulation d'un réseau d'une organisation



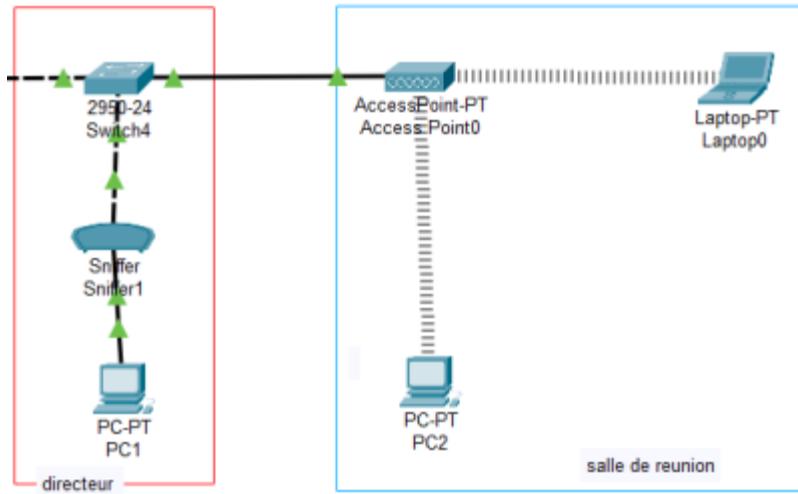
Notre organisation et diviser en deux partie comme vous pouver voir dans la figure precedante, la premiere partie appeler etage numero 1 et encore une fois diviser en deux, la premiere partie et concue au departement technique et la deuxieme et concue a un deparetement appeler departement A :



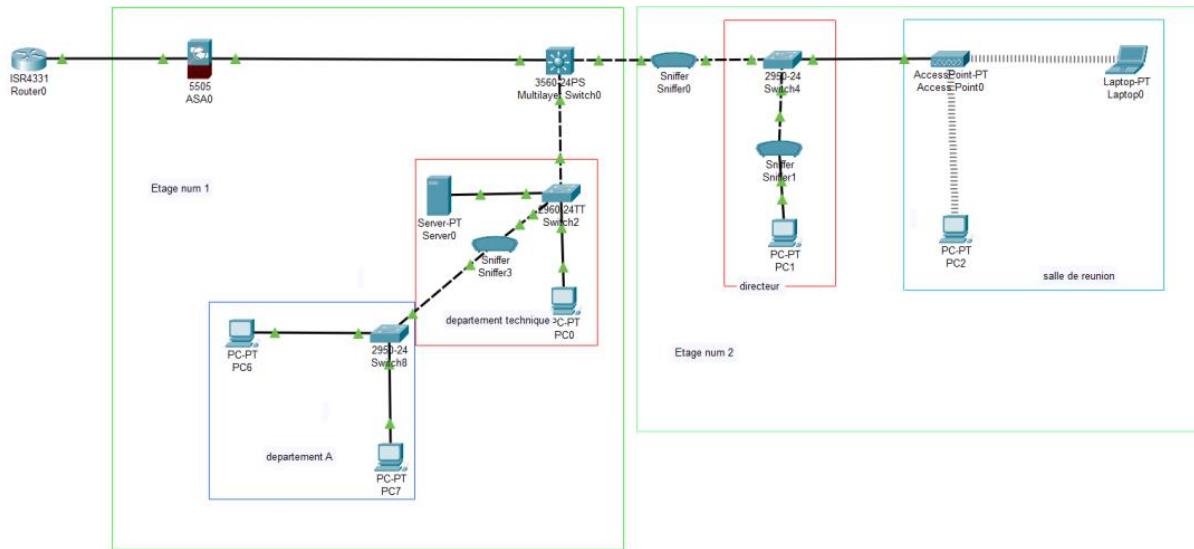
Les deux départements sont encore liés entre eux et représente tout l'étage numéro 1



Dans l'autre coter on a l'étage numéro 2 qui est de même constituer de bureaux de la direction et une salle de réunion :

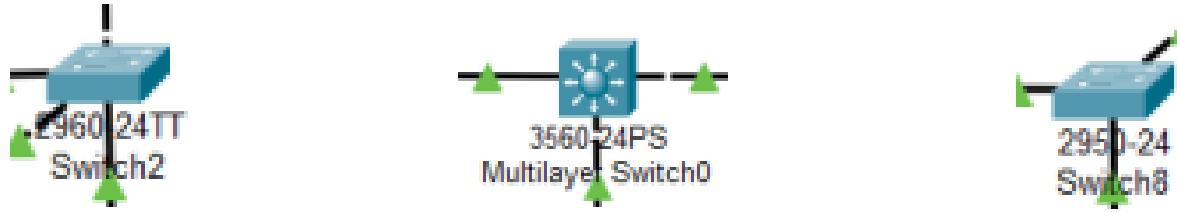


Et en gros on trouve notre cartographie comme dans la première figure.



## 2. Présentation des équipements :

Pour réaliser ce schéma on a fait appel à des différents switch ou on a trouvé plusieurs types et chaque type a sa propre caractéristique mais le choix a été fait sur **le switch 2960-24TT** et **le switch 2950-24** puisqu'ils sont des switches conçus pour les petites entreprises et prennent en charge les fonctionnalités de base telles que la gestion de la qualité de service (QoS), la sécurité des réseaux et la gestion de la bande passante. En résumé **le switch 2960-24TT** et **le switch 2950-24** sont des commutateurs abordables et fiables pour les petits réseaux qui nécessitent des fonctionnalités de base de gestion et de sécurité.

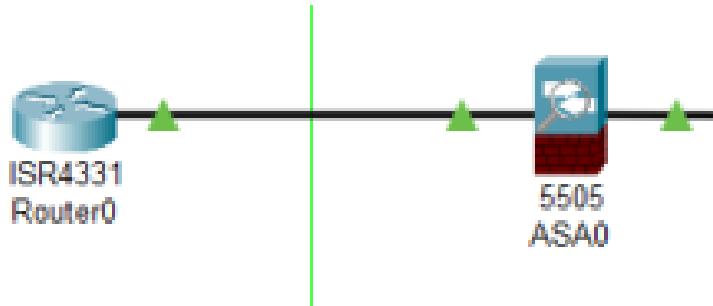


Et en même lieu on a encore choisi le **switch 3560-24PS** puisqu'il est conçu pour les petites entreprises et les départements d'entreprise qui ont besoin de fonctionnalités de gestion et de sécurité avancées, ainsi que de la possibilité d'alimenter des périphériques via le réseau Ethernet. On a encore fait appeler à serveur afin de faire fonctionner des différent service et les simuler dans notre réseau et un point d'accès pour établir une connexion sans fil dans l'environnement et bien sûr a des périphériques hôte sou forme d'ordinateurs.



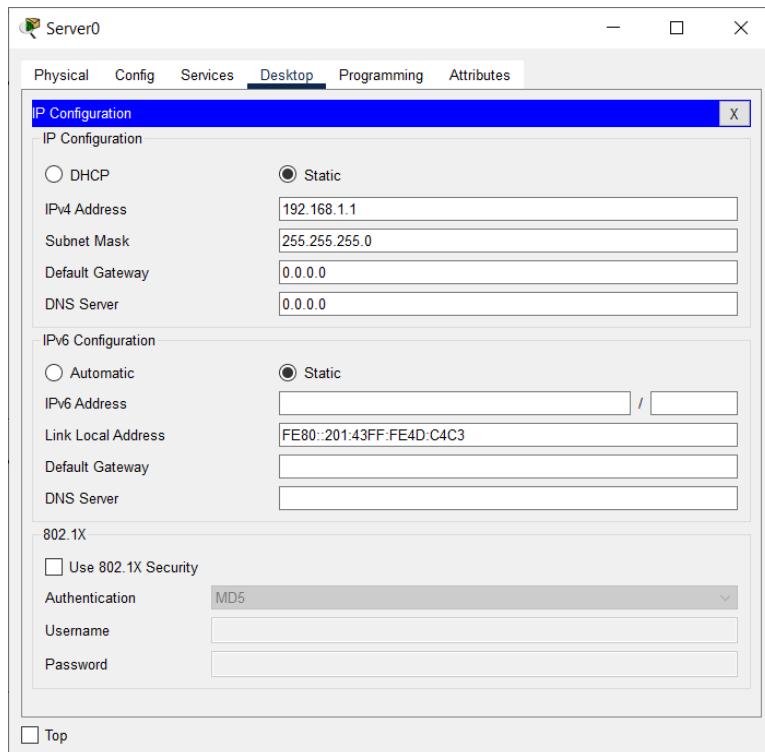
Et pour finir on doit inclure un par feu à notre réseau afin d'assurer une protection contre les connections non autoriser dans notre réseau qui pénètre généralement du routeur on a choisi le **ISR 4331** puisqu'il est un routeur robuste et fiable pour les petites et moyennes entreprises qui cherchent à connecter leurs réseaux locaux à Internet et à d'autres réseaux distants.

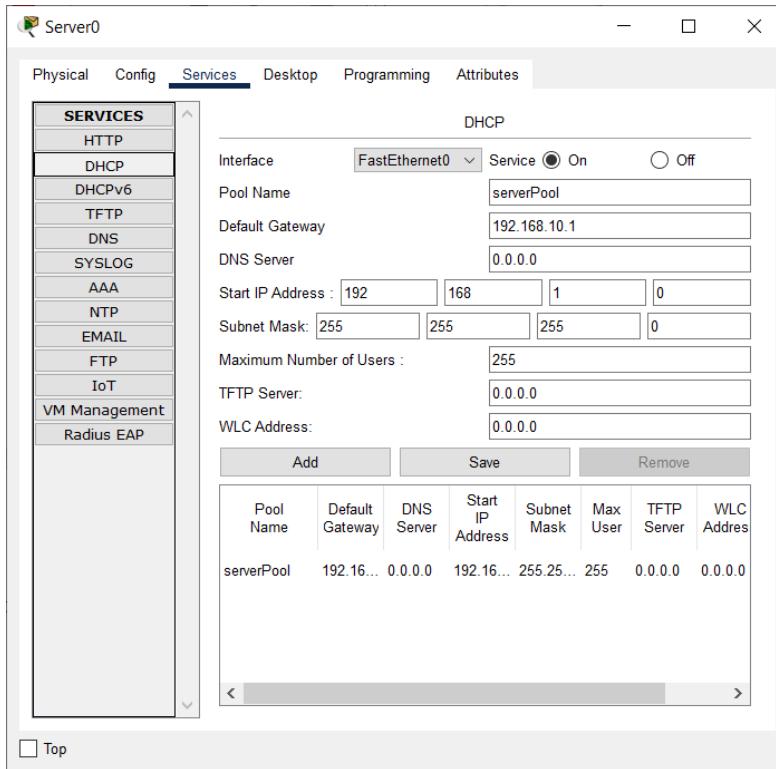
Et le pare-feu **5505ASA0** car Il est conçu pour les petites entreprises et les filiales de grandes entreprises qui cherchent à protéger leur réseau contre les attaques en ligne et à contrôler le trafic réseau entrant et sortant.



### 3. L'installation des services de réseau :

Comme dans les figures précédentes on a mis en place un serveur qui vas fournir d'abord à tous les périphériques hôtes connecter au réseaux un service **DHCP** et un service **MAIL** pour faire ceci il faut d'abord donner au serveur une adresse IP statique comme dans la figure suivante :

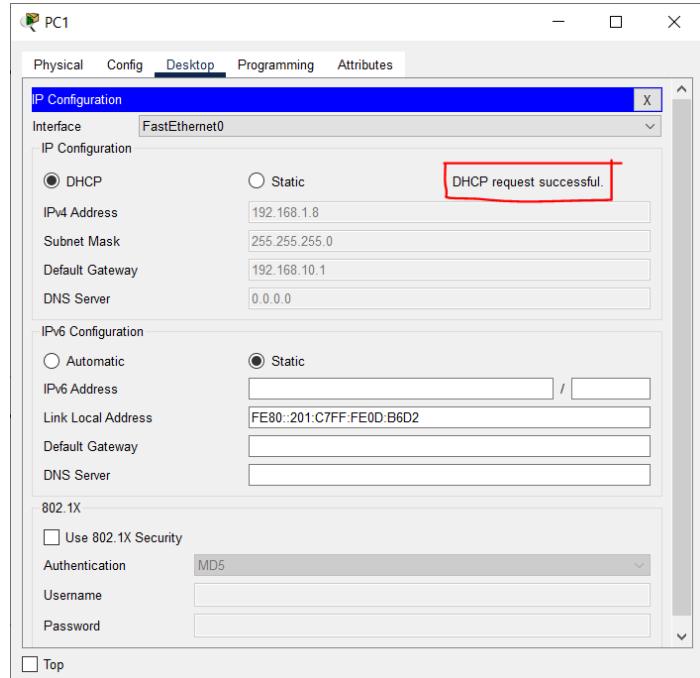




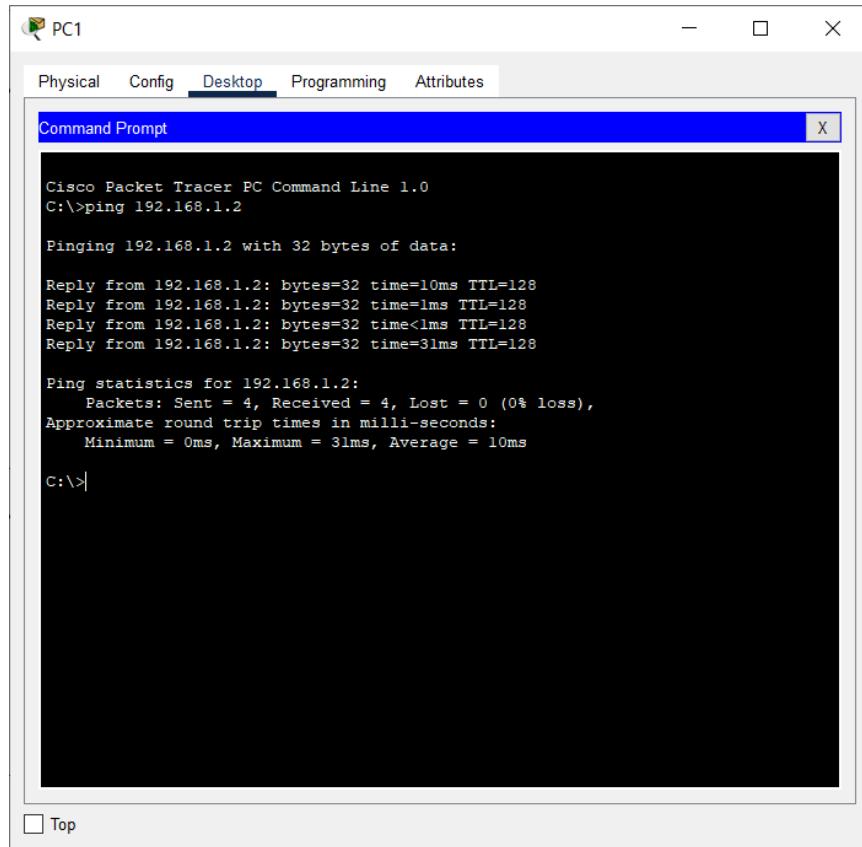
Et après cliquer sur service et activer le service **DHCP** et saisir l'adresse **IP** de début comme **192.168.1.0** et les nombres maximaux des utilisateurs et enregistrer. La configuration comme dans la fenêtre à gauche on a activé le service et on a donné un nom server Pool avec le nombre d'utilisateur une passerelle ou Gateway et on l'ajouter a notre service du serveur on clique sur Save ou enregistrer maintenant tous les ordinateurs et les

périphériques connecter au réseau vont avoir une adressé **IP** issue de notre serveur **DHCP** qu'on vient de le paramétrer donnant l'exemple par le pc qui existe dans la direction ou on va trouver comme si dessous :

Avec le message **DHCP** requête **successful** et on peut voir l'adresse **IP** fourni par le service **DHCP** a ce pc la qui a la forme de **192.168.1.8** et on demande une attribution des adresse **IP** automatiques tous les périphériques hauts vont être connecter entre eux et on peut tester cette connexion soit avec l'instruction ping suivit par l'adresse **IP** du périphérique destinataire ou par une simulation de paquet dans paquet tracer



Testons par exemple la connexion entre le **PC1** de la direction qui a comme adresse **IP 192.168.1.8** avec le **PC0** qui est dans le services technique qui a comme adresse **IP 192.168.1.2**



The screenshot shows a window titled "PC1" with a tab bar containing "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is selected. Inside the window, there is a "Command Prompt" window with the following text:

```
Cisco Packet Tracer PC Command Line 1.0
C:>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=10ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=31ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 31ms, Average = 10ms

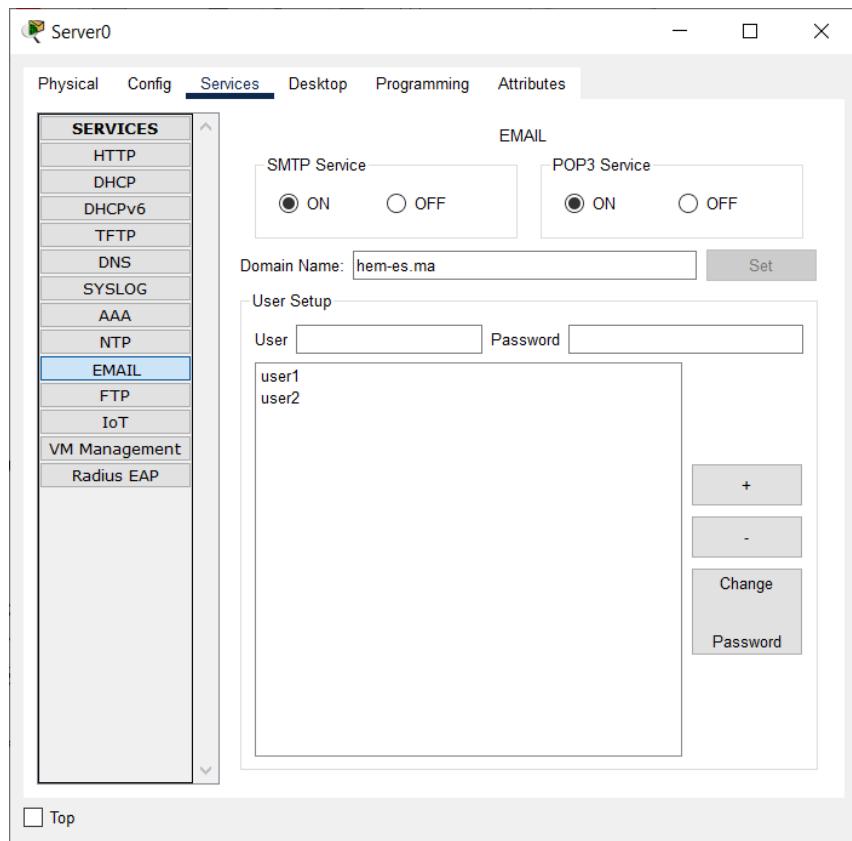
C:>|
```

At the bottom left of the Command Prompt window, there is a small checkbox labeled "Top".

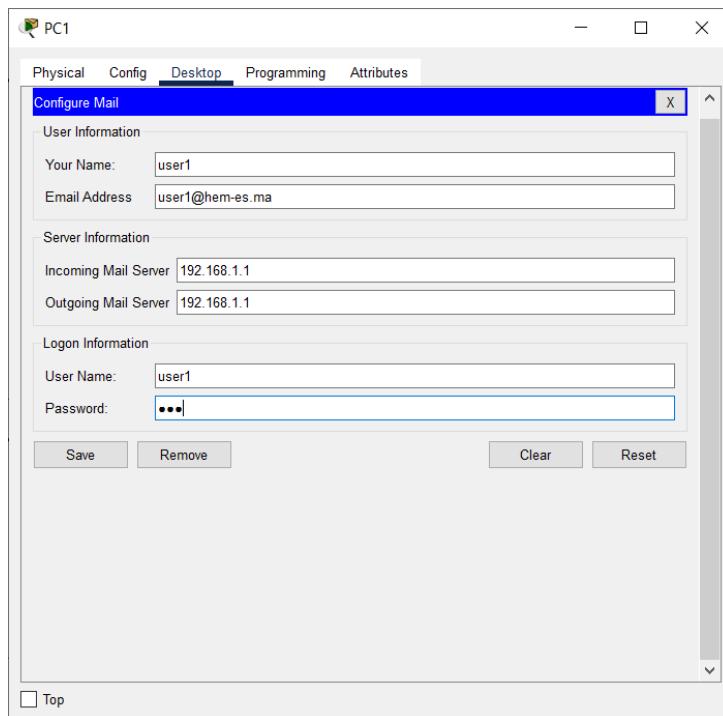
Ou on peut la tester avec la simulation des paquets

Fire	Last Status	Source	Destination	Type	Color	Time(sec)
	Successful	PC1	PC0	ICMP		0.000

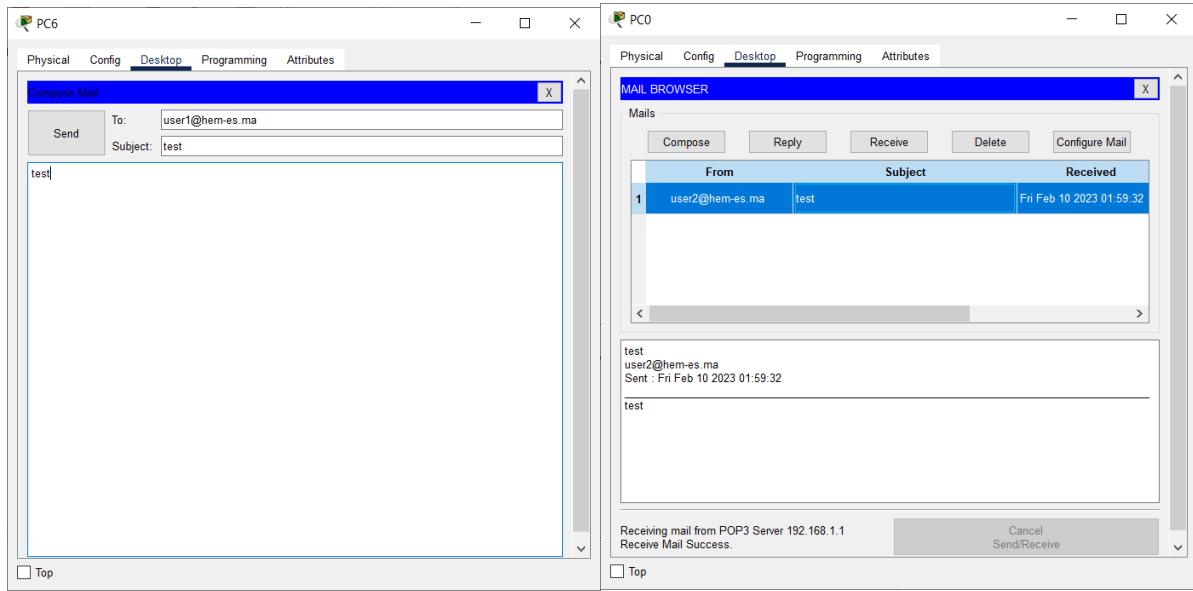
Comme ça on est assuré que la connexion qu'on a fait entre les différents hôtes grâce au switch et les autres composants est dans un bon état et que tous les périphériques sont connectés entre eux maintenant. On peut encore activer un service mail dans notre réseau en ajoutant le nom du domaine et les utilisateurs avec leurs mots de passe comme dans la figure suivante.



On peut tester le service mail tout simplement en se connecter à notre boite mail en entrant l'information fournit et l'adresse **IP** du serveur



Et en cliquant sur Save et on fait les mêmes étapes sauf cette fois pour un autre ordinateur dans notre réseau et en utilisant l'identifiant de **user2** et on va envoyer message test entre les deux



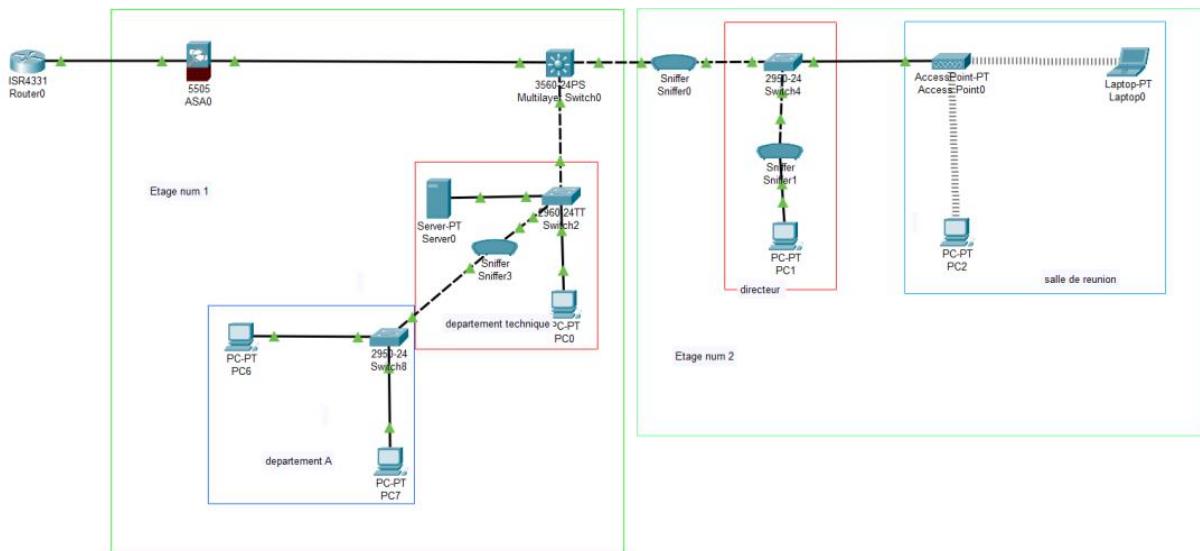
Et comme ça on a pu configurer un serveur mail et un serveur **DHCP** dans notre réseau.

#### 4. Le sniffer :

Un **sniffer** est un outil qui permet de capturer et d'analyser les paquets de données qui transitent sur un réseau. Il vous permet de voir les informations détaillées sur les paquets, telles que l'adresse source, la destination, le protocole utilisé, les informations de la couche liaison de données, etc. et il peut être utilisé pour déboguer les problèmes réseau, évaluer les performances et la sécurité du réseau.



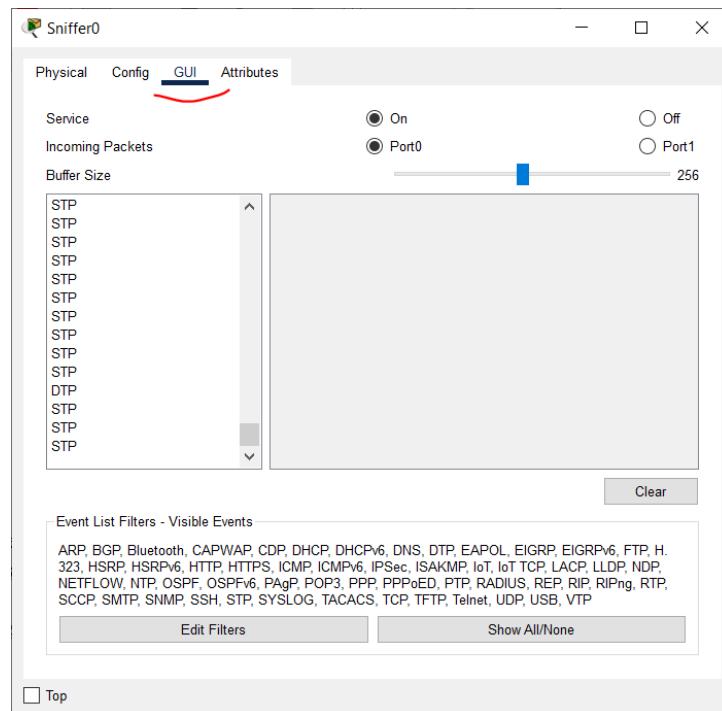
Dans notre schéma on a utilisé 3 sniffer afin d'analyser les paquets et mieux analyser le trafic, la charge et les performances dans notre réseaux



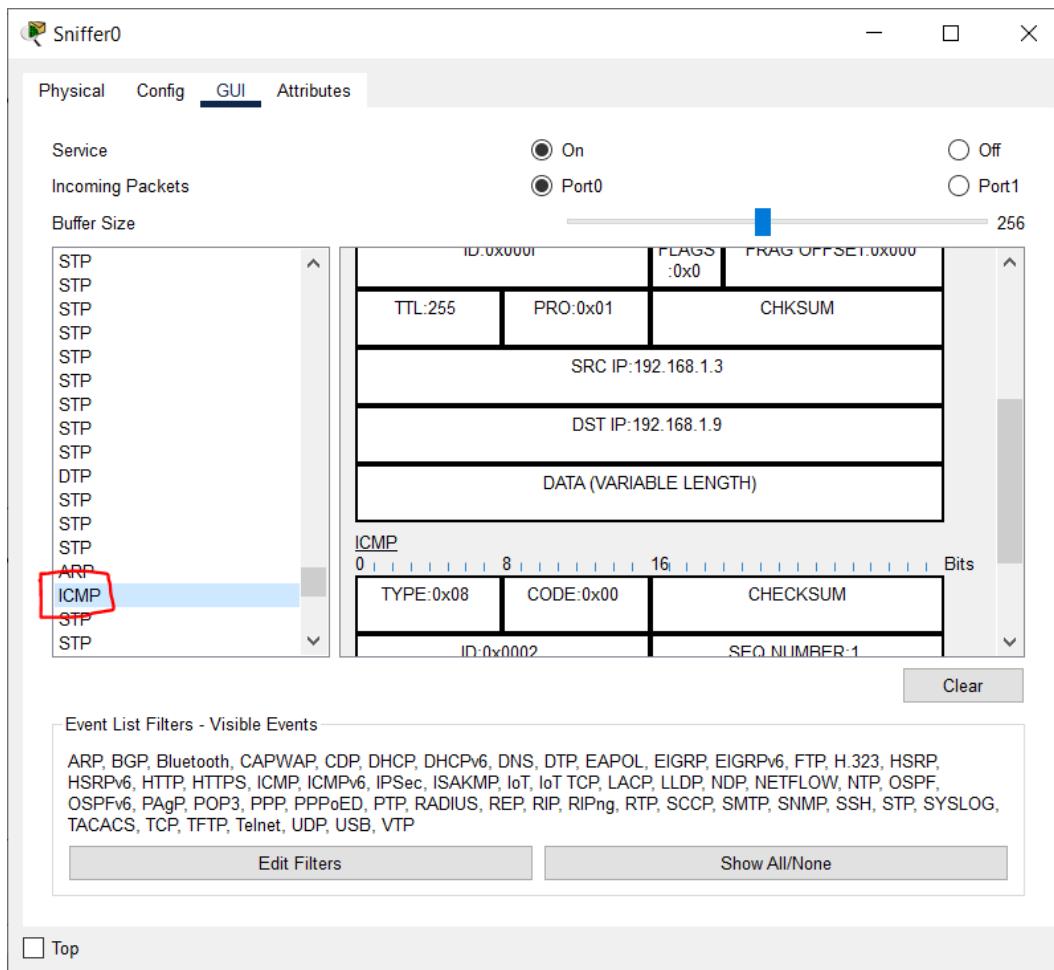
Le premier sniffer appeler sniffer0 analyse tous les paquets qui vont entrer vers étage numéro 2 et le sinfffer1 pour analyser précisément l'ordinateur de la direction et le dernier sniffer pour analyser les donner entrent est sortant vers le département A.

#### 4.1 analyser avec un sniffer :

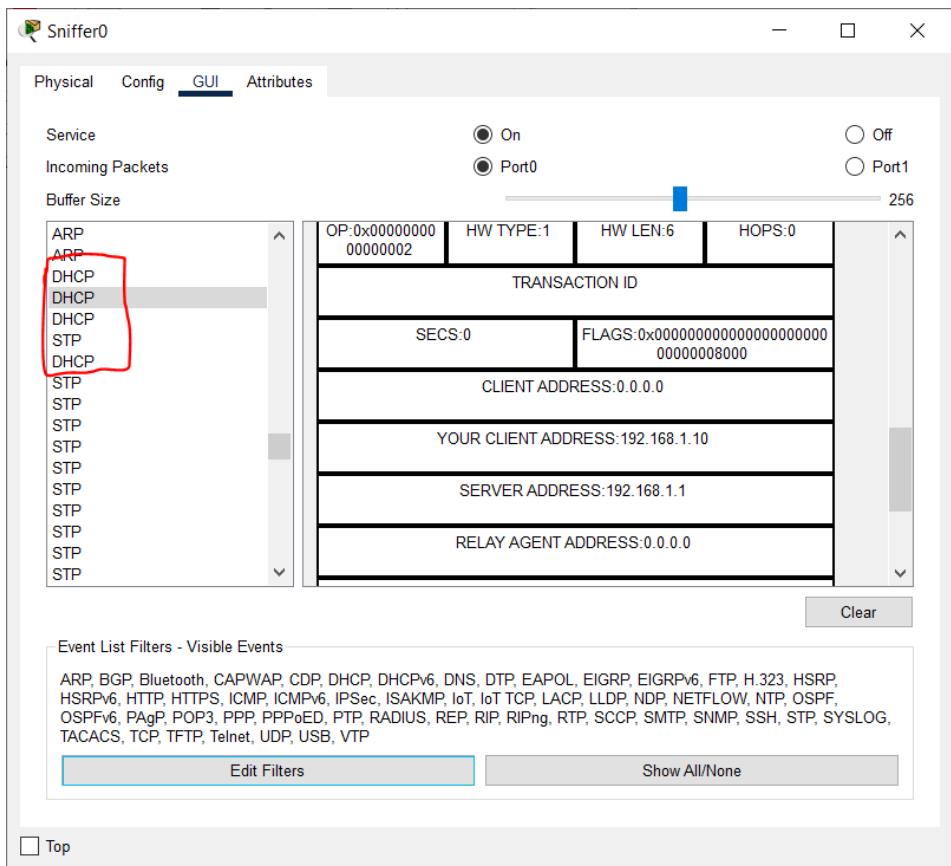
L’interface **GUI** (graphical user interface) du sniffer nous montre les différent protocole qui passe de ce dernier comme suit



On peut trouver juste **STP** comme protocole qui est un protocole utilisé pour contrôler les boucles dans un réseau étendu. Ou **DTP** qui est un protocole réseau utilisé pour négocier l'état du lien tronc entre les commutateurs mais après avoir faire un test de ping entre deux ordinateurs ou il y a un sniffer entre eux en remarque l'ajout de protocole **ICMP** qui est utiliser pour envoyer des messages d'erreurs ou de contrôles



Est quand on clique eu dessus on trouve les différentes informations de ce message tels que la source la destination et le type de la variable envoyer pour tester le réseau, puisqu'on a un serveur mail et un serveur **DHCP** donc lors de l'utilisation d'un de ces services on va remarquer qu'il y a des nouveaux protocoles comme **POP3** pour mail ou **DHCP** pour la demande d'une adresse IP.

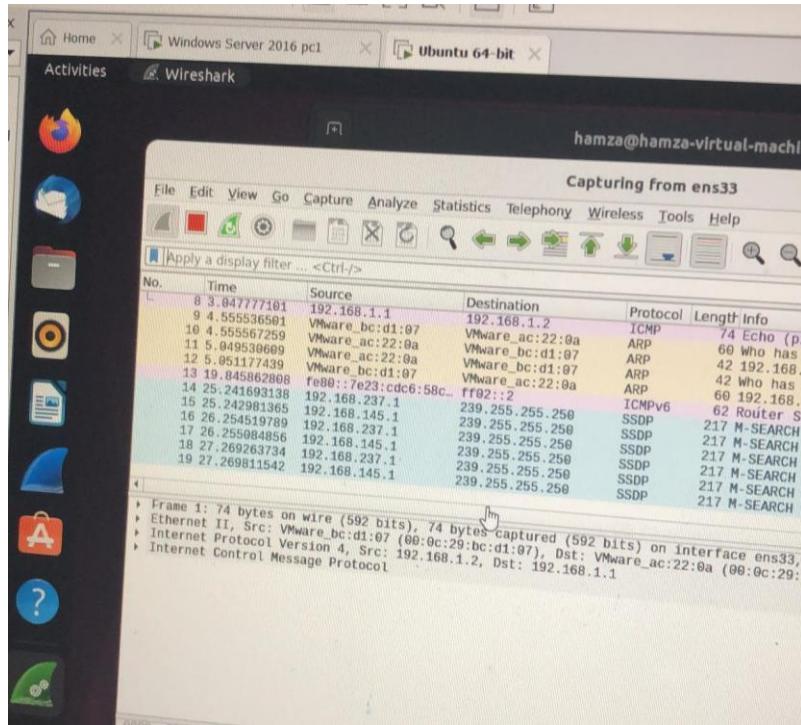


## 5. Utilisation des Analyseurs :

Dans notre simulation sur **Packet Tracer** on a pas un grand choix afin d'utiliser des analyseur sauf les Sniffer mais pas des logiciels open sources qu'on peut les utiliser dans notre boite à outils afin d'analyser le trafic et mieux comprendre la source du problème si jamais il y a un, il existe plusieurs analyseur qui peuvent analyser parfaitement le trafic comme : **Wire Shark**, **tcp dump**, **ngrep**... mais malheureusement il ne sont pas compatible avec la forme .pkt de **packet tracer** et c'est plutôt impossible de convertir de .pkt vers .pcap ou .pcapng des format qui sont lisible de l'appart des ana analyseurs comme **WireShark**.

### 5.1. Wireshark :

**Wireshark** est un analyseur de paquets réseau populaire et open source. Il permet à l'utilisateur de capturer et d'analyser les paquets réseau en temps réel, ce qui peut être très utile pour diagnostiquer les problèmes de réseau ou pour comprendre comment les différents protocoles réseau fonctionnent.



Cette image montre l'interface de **Wire Shark** avec les différentes informations des paquets reçu ou transmis de notre PC lors d'une simulation de connexion entre une machine virtuel Ubuntu avec une autre machine.

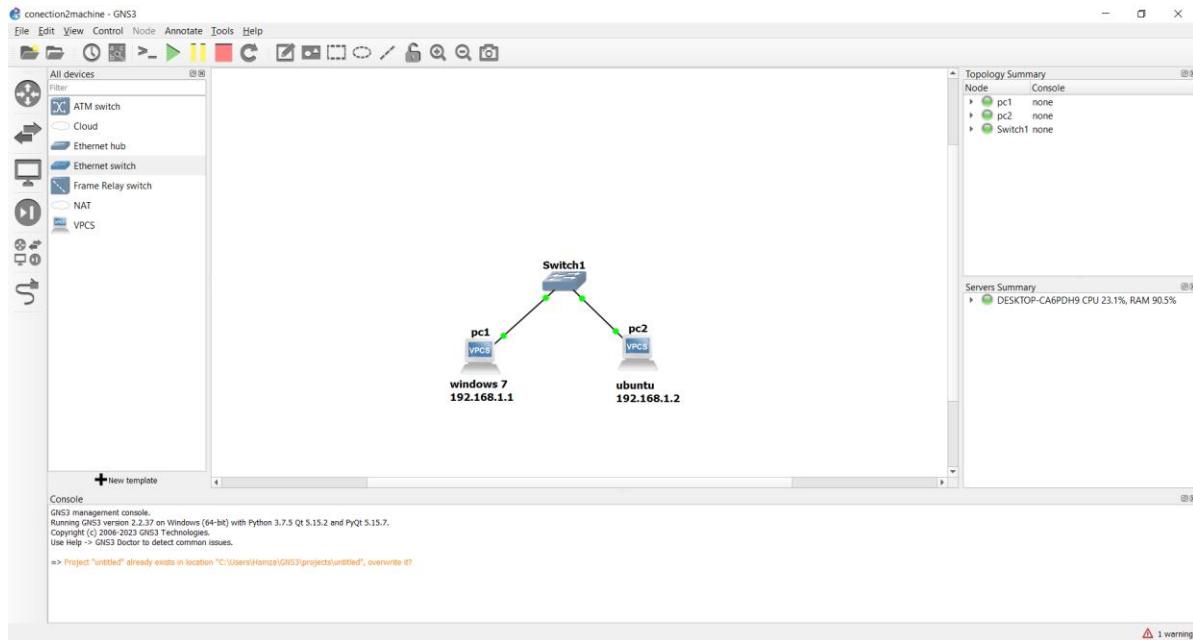
## 5.2 utilisation de Wire Shark dans notre réseau

Alors il est sur maintenant qu'on ne peut pas utiliser des analyseurs comme **Wire Shark** sur paquet tracer pour cela on va utiliser **GNS3**.

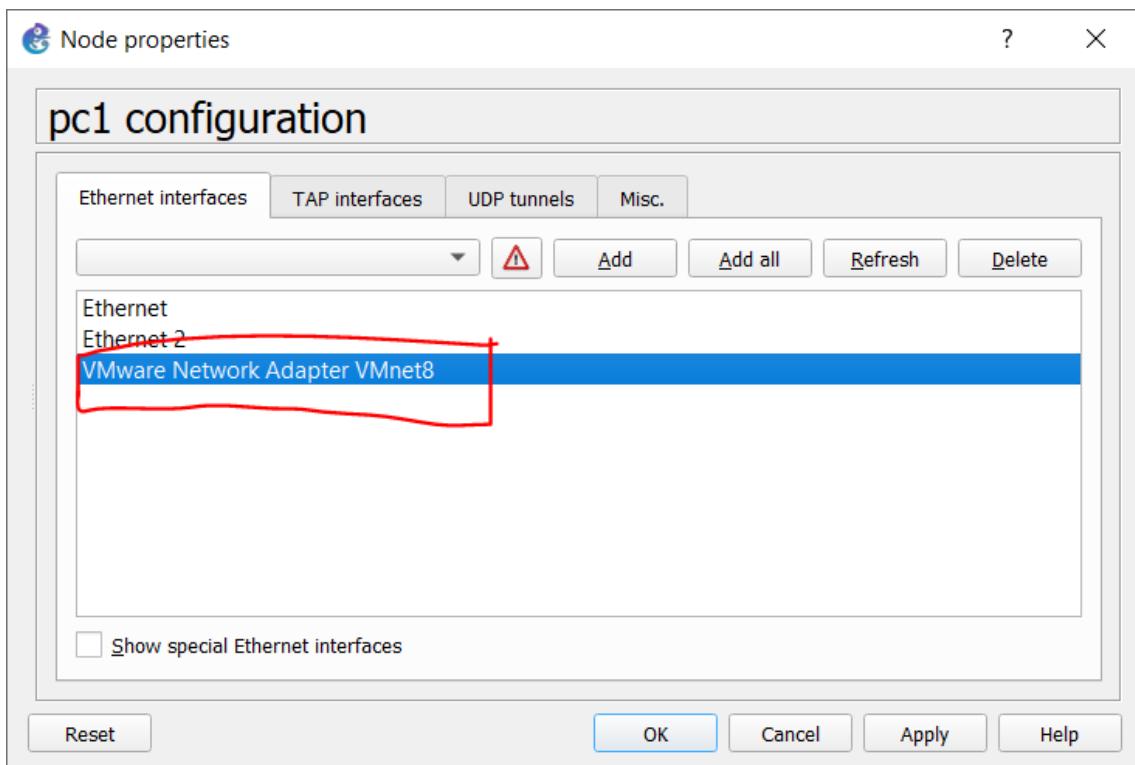
**GNS3** est un outil de simulation de réseau qui permet aux utilisateurs de concevoir et de simuler des topologies de réseau complexes, et il est open source et permet l'intégration des différent application d'analyse, pare-feu ou de virtualisation... et il va nous aider à mieux analyser notre réseau et détectera les différent problèmes qui peuvent nous parvenir.

## 6. Connecter et configurer des machines clients dans un réseau Windows ou linux :

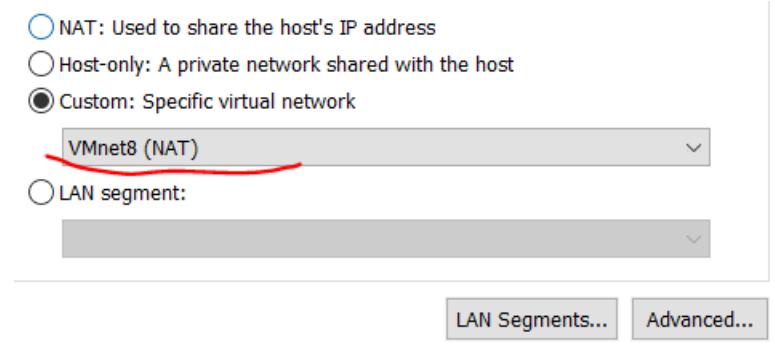
Pour connecter et configurer deux machines clientes en utilisant GNS3 on doit d'abord ouvrir le logiciel et crée un nouveau projet. Et on va nommer les deux machines à connecter par PC1 et PC2 et les liées par **switch1**.



Lors de la liaison il faut faire attention au port de réseau à connecter qu'il soit le même avec celui de la machine virtuel

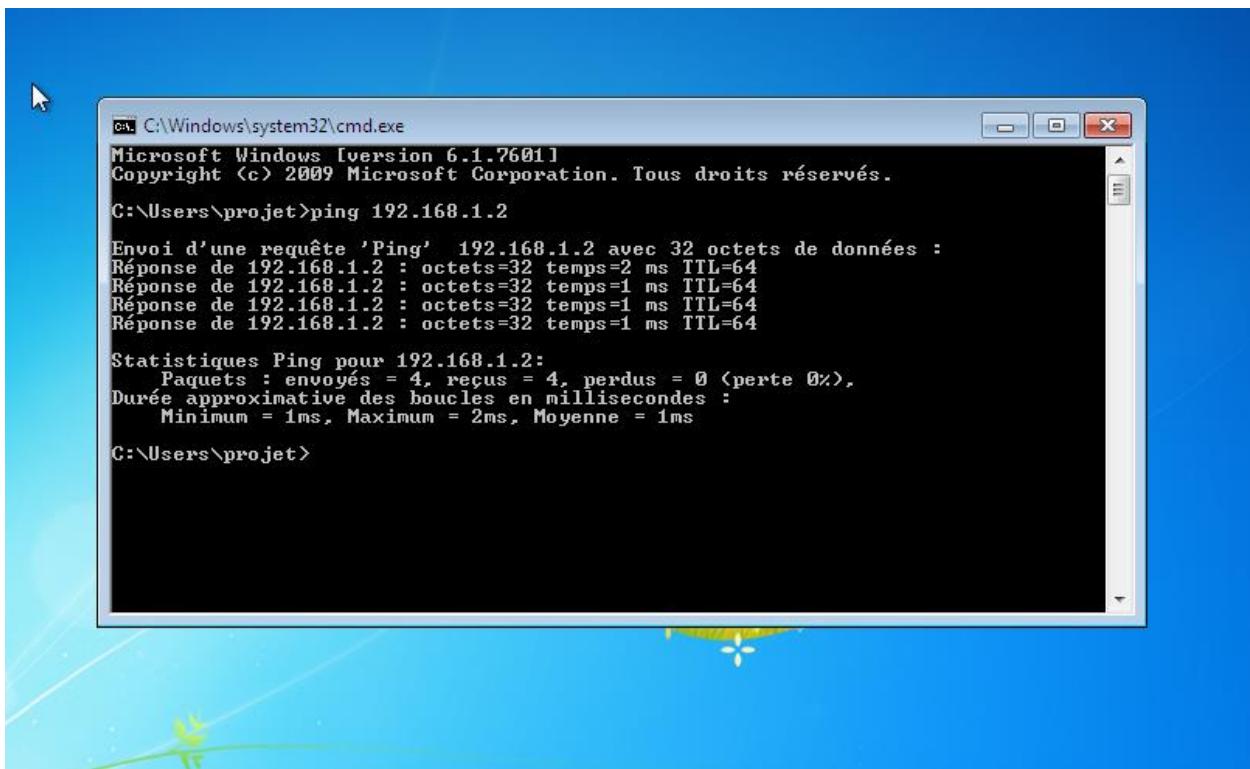


Ici on va connecter le port **VMnet8** avec le switch alors il faut qu'il soit le même sélectionner dans la machine virtuel

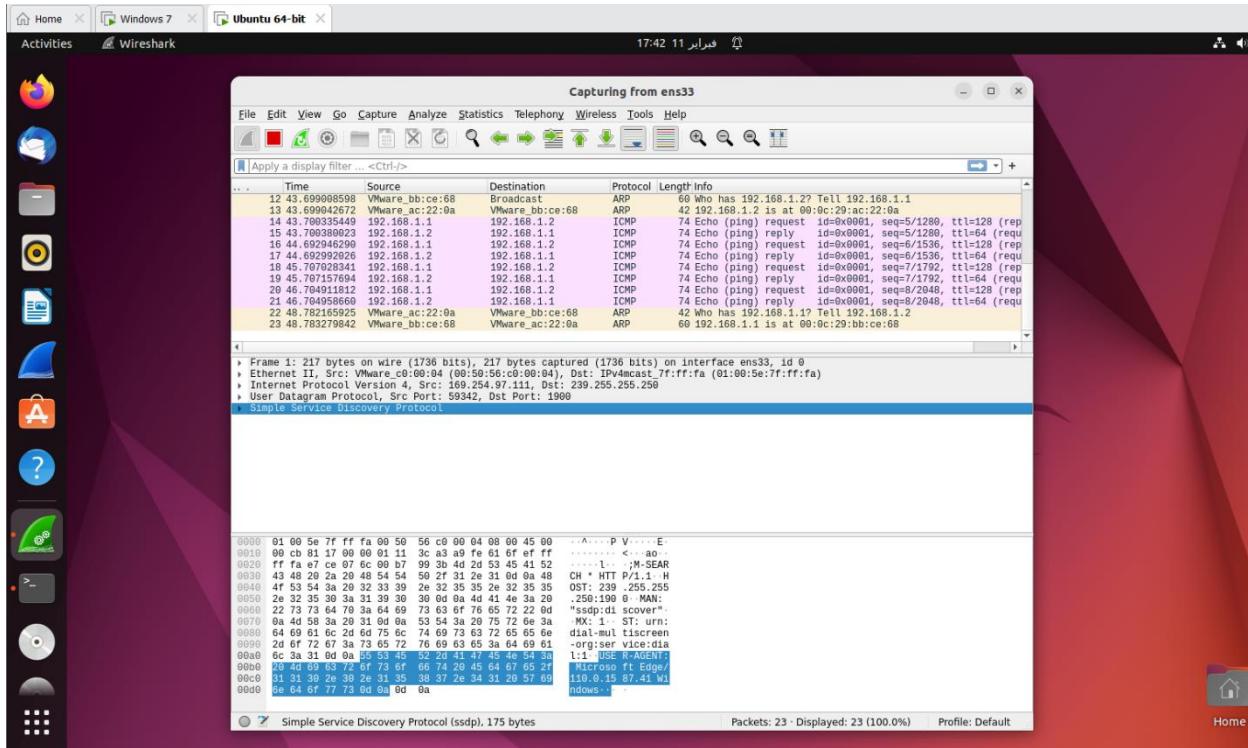


Maintenant notre première interface et prête pour lier le port **VMnet8** avec le switch, et il faut faire la même chose pour la deuxième machine.

On doit tout d'abord donner une adresse IP au PC1 et au PC2 comme exemple **192.168.1.1** et **192.168.1.2**. Comme ça notre connexion est prête il suffit de la tester avec la commande **ping**, testons la connexion du pc1 vers pc2 :



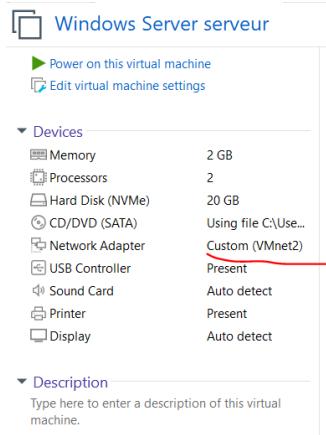
Comme vous voyez la connexion c'est rétabli. Exécutant **Wire Shark** dans le deuxième ordinateur et on remarque ce qui se passe.



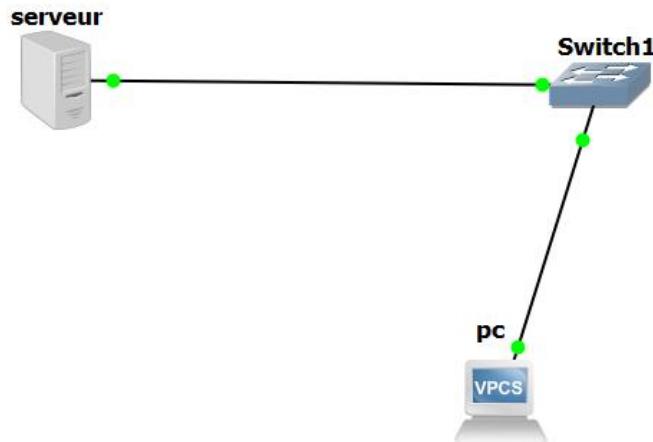
Wireshark a analysé notre connexion par succès et nous a montrer le temps la source et les informations nécessaires de ce dernier test on remarque la bande passante et les messages reçu avec les réponses.

## 7. Installation des serveurs linux ou Windows virtuels :

Pour installer et configurer des serveurs virtuels il faut tout d'abord télécharger le fichier .iso de système d'exploitation de serveur comme exemple Windows server 2016 avec le quelle on vas configurer le serveur et le connecter a des périphériques hôtes et il faut crée une machine virtuelle qui vas exécuter le fichier .iso d'os.

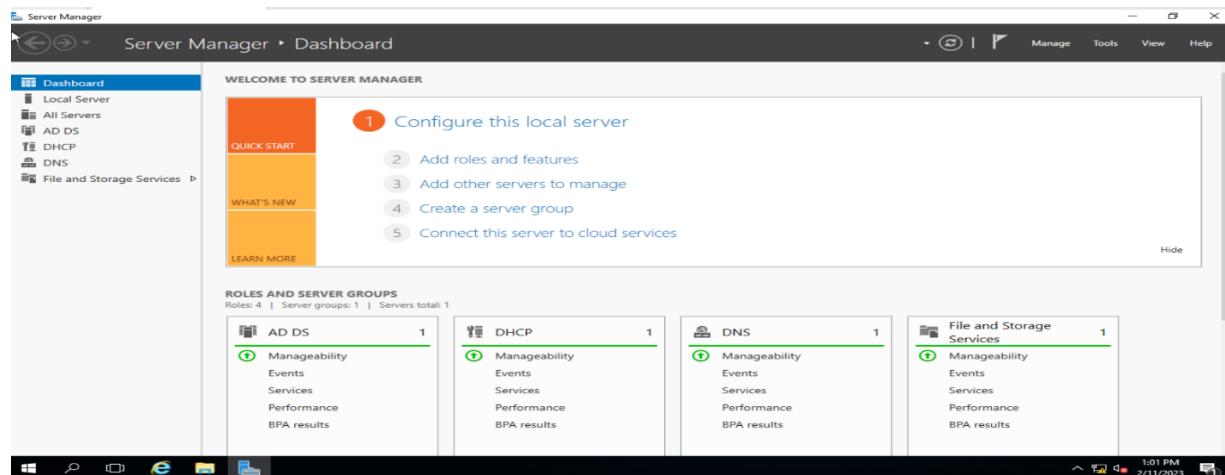


Après avoir fait la création de notre machine virtuelle et installation de notre système Windows Server 2016 il faut faire encore une fois attention au port Ethernet fourni à la machine pour bien la connecter dans **GNS3** avec la machine cliente comme ci-dessous.



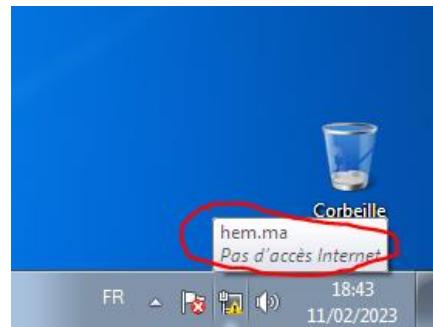
L'interface de Windows Server 2016 est une interface simple similaire à celle de Windows 10. On va essayer de configurer 3 serveurs : un serveur DHCP, DNS et un serveur AD (Active Directory) pour configurer c'est serveur. Il faut tout d'abord accéder à Windows Service Manager et les ajouter et les configurer après.

Voici l'interface après avoir fini tout ça :



Comme vous remarquer l'ajout des serveurs **DHCP**, **DNS** et **AD** s'est faite maintenant on peut tester le fonctionnement des serveurs.

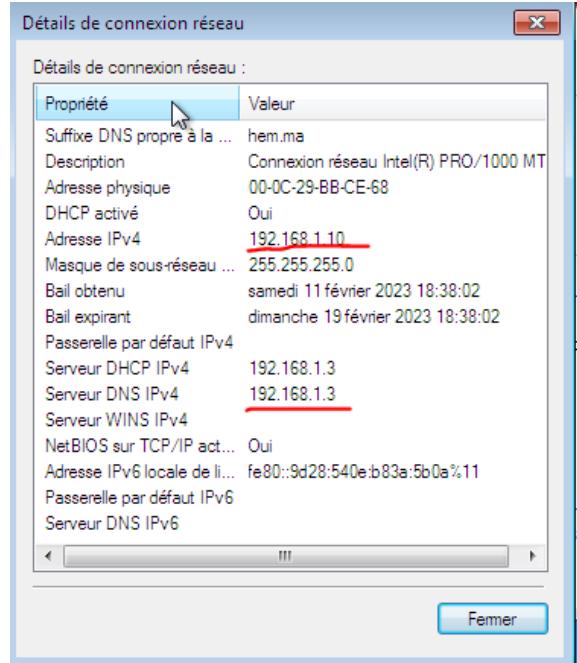
Débutant par le serveur DHCP ce dernier a comme début de plage d'adresse **192.168.1.10** dans sa première étendue alors il doit fournir au périphériques hôtes des adresses de **192.168.1.10** et plus, on allume l'ordinateur connecter avec le serveur on peut remarquer qu'il est connecté directement au serveur juste par remarquons le nom fournit au serveur **DNS**



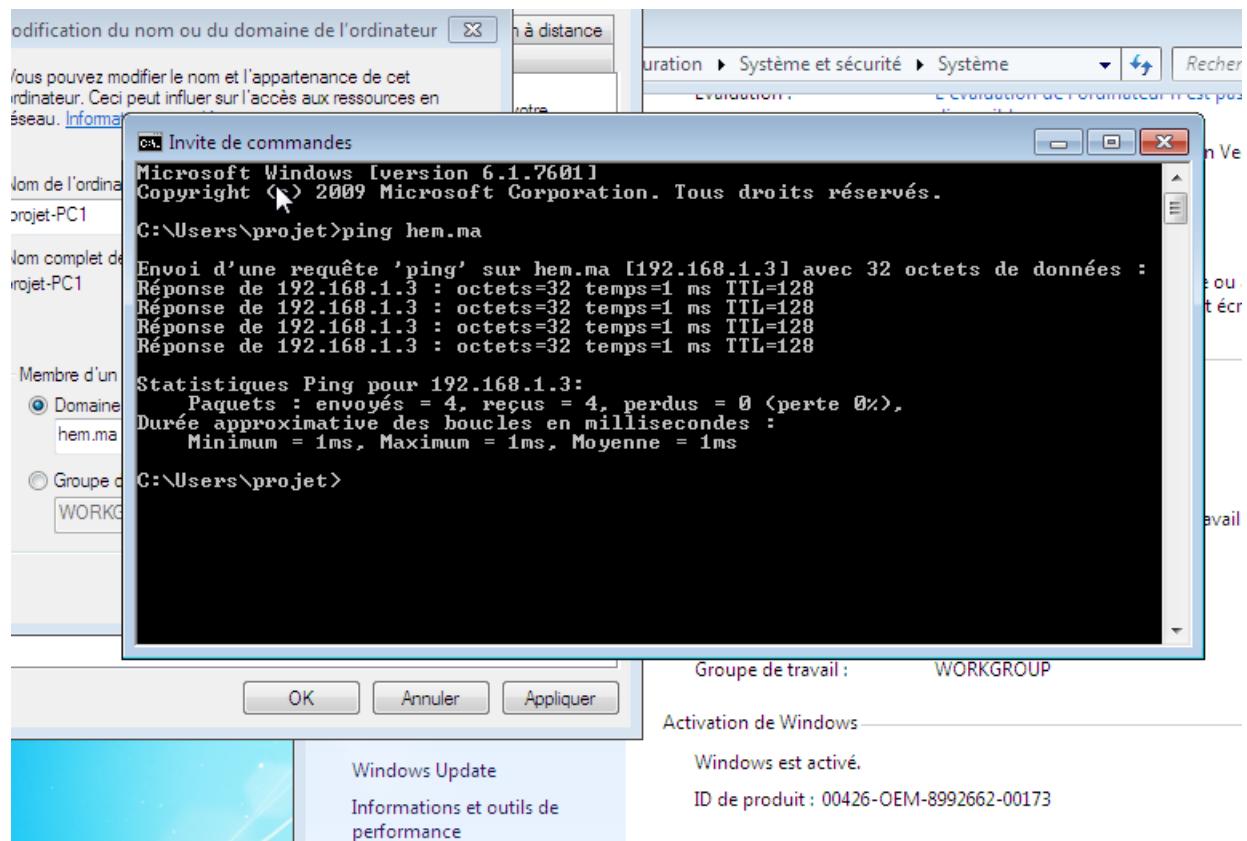
On cherche dans notre serveurs la liste de réservations des adresse **IP** on peut y trouver le nom de notre pc et l'adresse **IP** attribuer par notre serveur **DHCP**

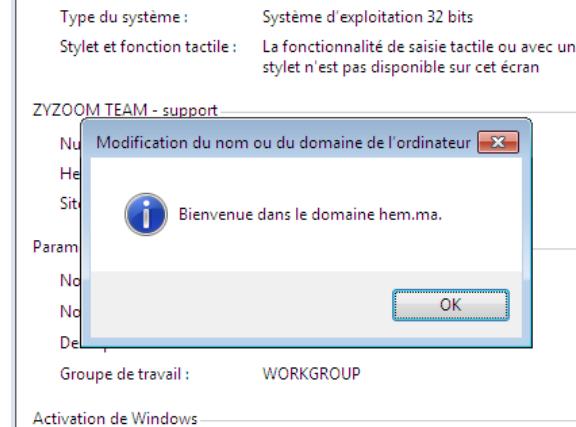
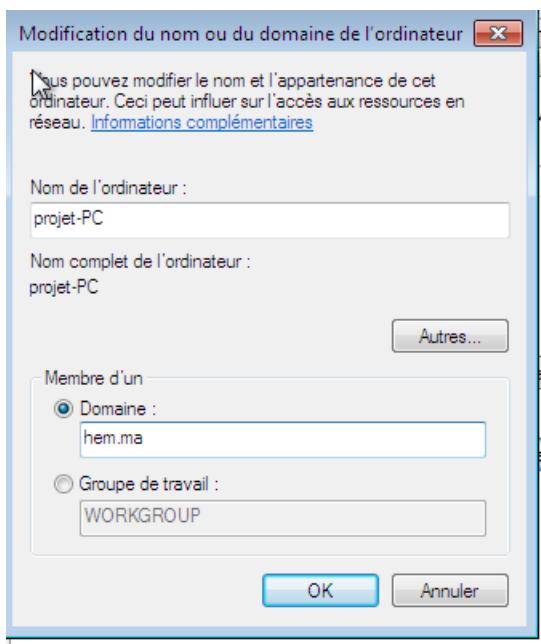
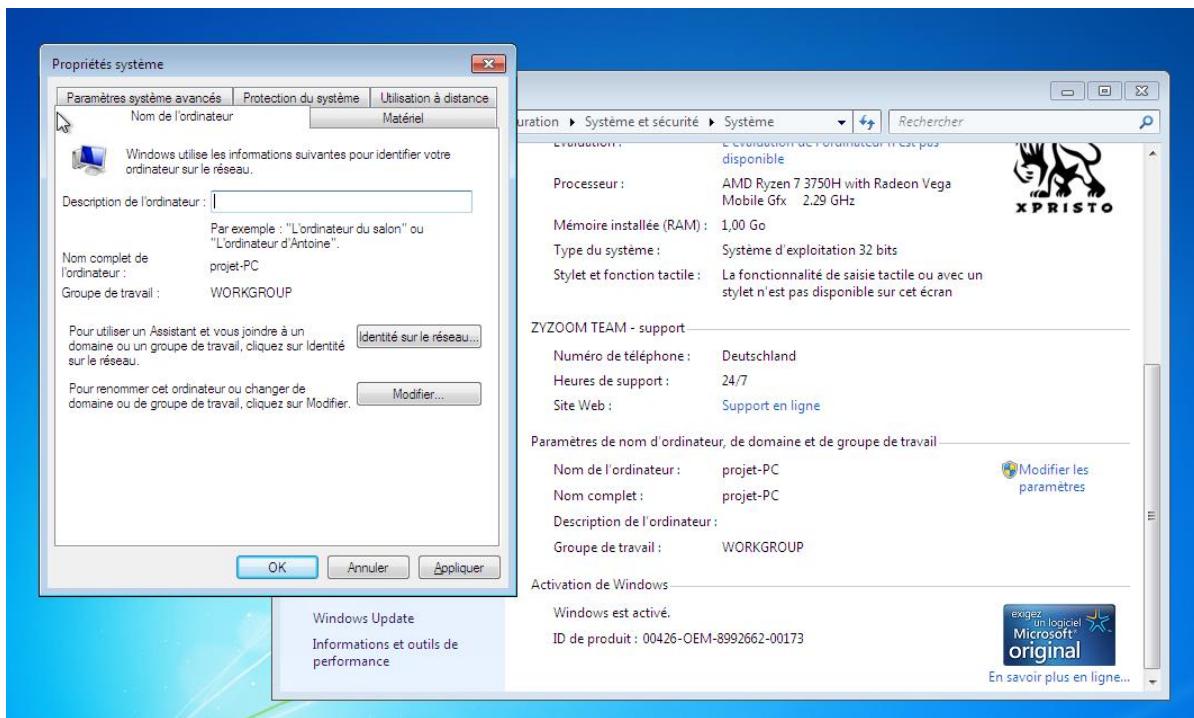
A screenshot of the Windows Server 2012 DHCP Management console. The left pane shows the DHCP tree structure under "Windows Server serveur". The right pane displays a table of reserved IP addresses. The table has columns: Client IP Address, Name, Lease Expiration, Type, Unique ID, Description, Network Access Protection, and IP. Two entries are listed: one for "projet-PC.hem.ma" with IP 192.168.1.10 and another for "DESKTOP-CA6PDH..." with IP 192.168.1.12. The "Name" column is highlighted with a red box.

Et même juste par vérifions les paramètre réseaux de notre ordinateur on vas trouver encore une fois l'adresse **IP** de notre serveur **DHCP** et l'adresse **IP** fournit par se dernière

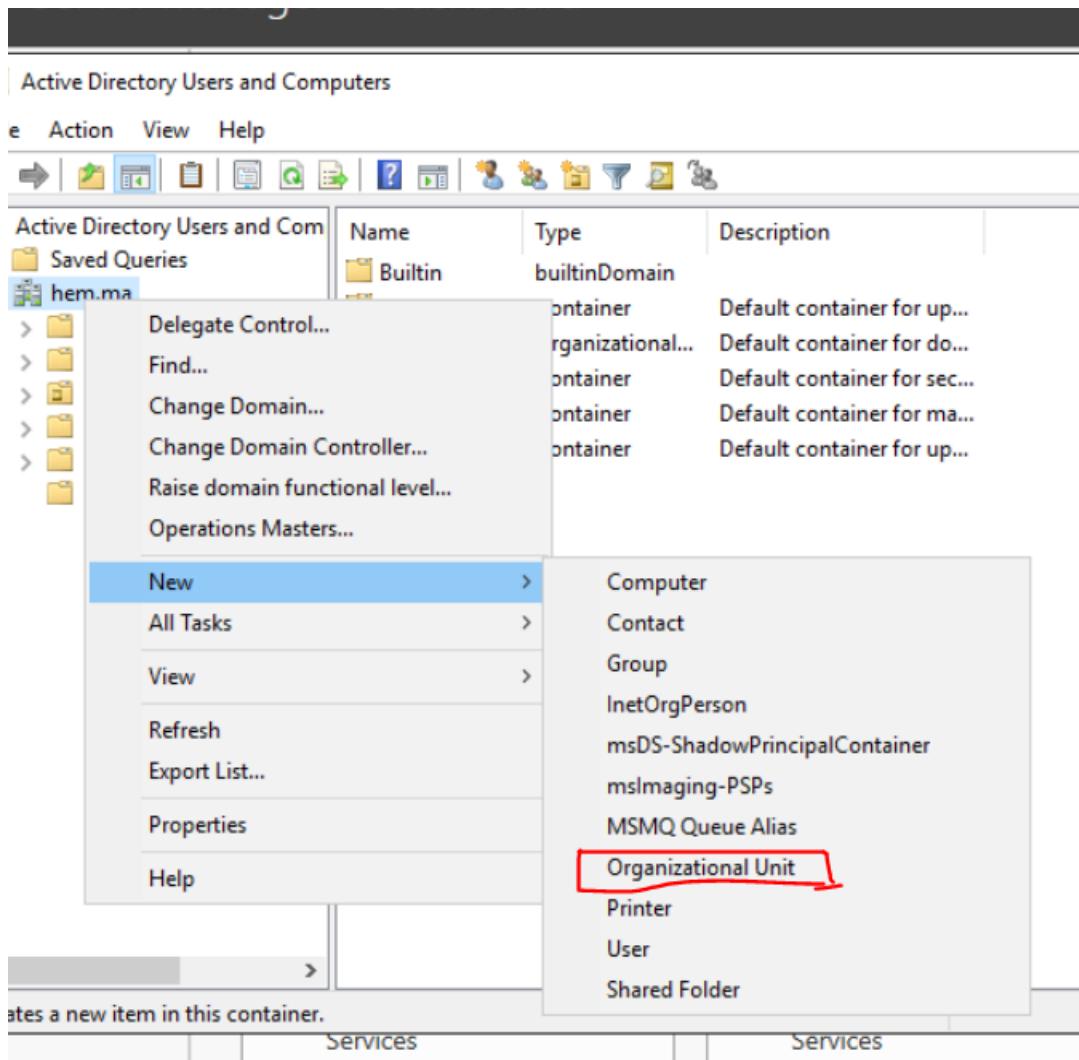


Maintenant analysons le fonctionnement des serveurs **DNS** et **AD** en rejoignons le domaine tout d'abord en utilisons ping pour voir si tout est bien connecter

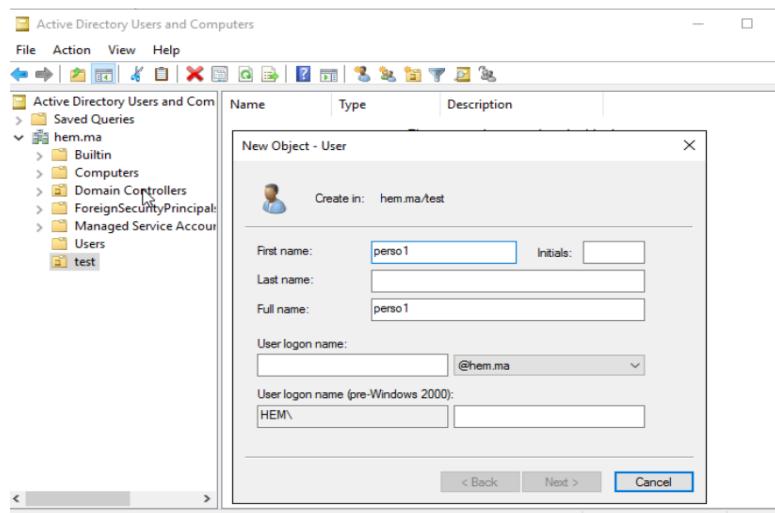


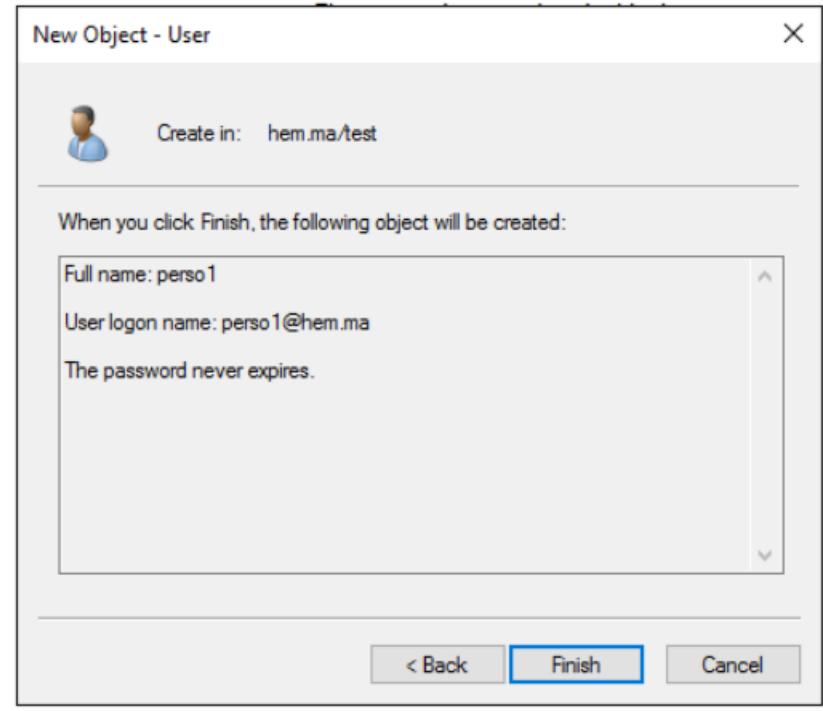


Maintenant on peut analyser le profil d'utilisateurs et donner l'accès au personne voulus et arrêter l'accès aux personnes plus autoriser grâce au serveur **AD** on simplement les ajouter dans une unité d'organisation au sein de notre serveur **AD** comme dans la figure suivante

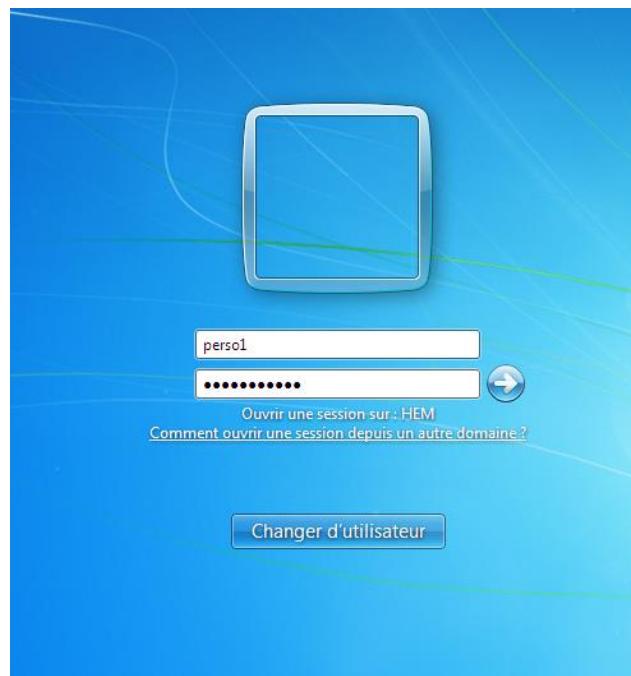


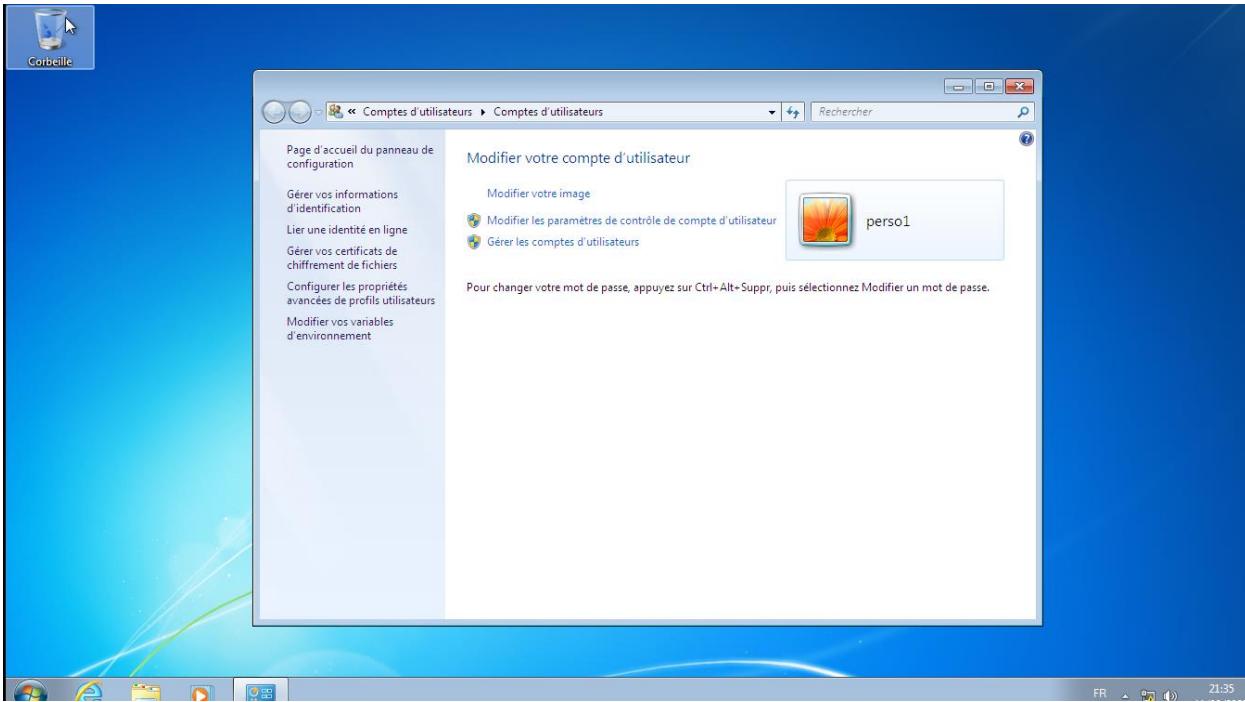
Apres avoir créer cette unité d'organisation on peut ajouter a créé des utilisateurs on lui donnant des mots de passe unique et des login unique





On peut tester si l'ajout de notre profil est valide juste on connecte notre ordinateur connecter au serveur et essayer de se connecter dans une nouvelle session :

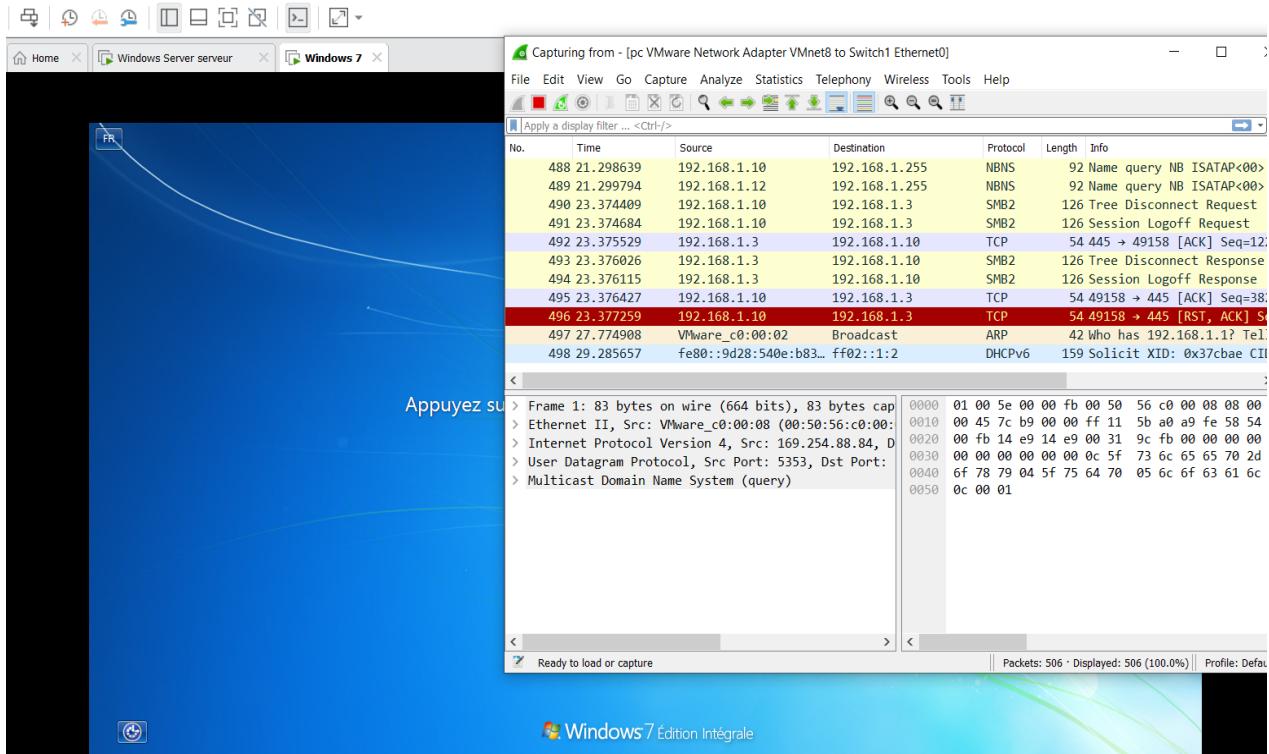




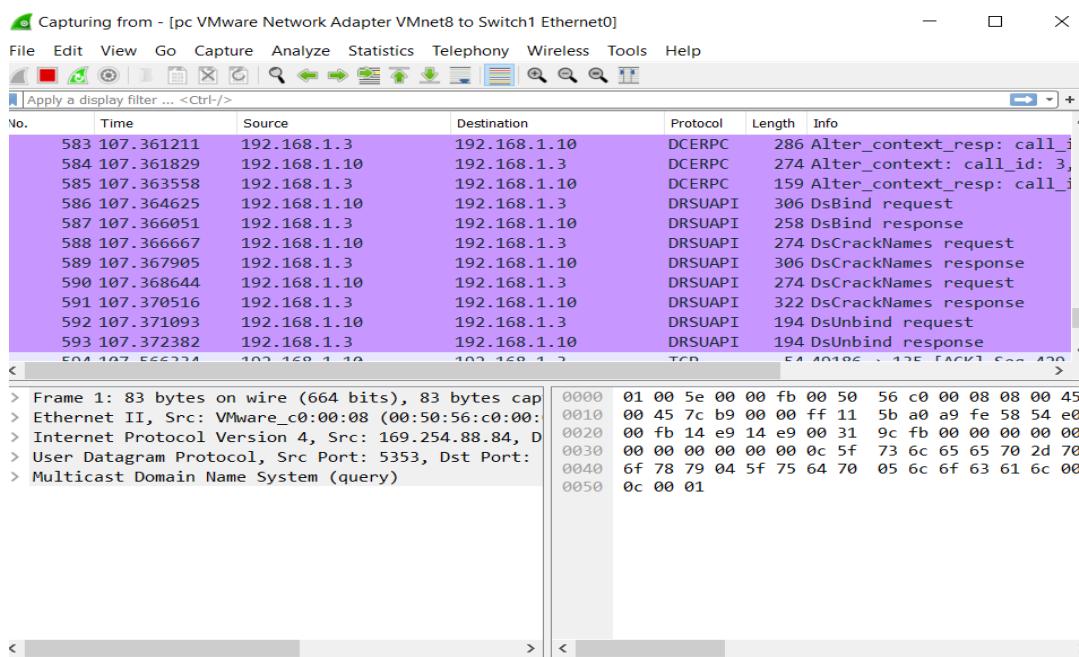
Et comme ça on a pu se connecter à notre session créée de la part de notre serveur **AD** avec notre mot de passe unique est comme ça on va y pouvoir analyser le profils des tout les utilisateurs dans notre réseau.

## 8. Analyse des paquets :

Pour analyser les paquets il suffit de faire une clique droit sur le fil de connexion dans GNS3 et choisir analyse des paquets cela va automatiquement ouvrir la fenêtre de **Wire Shark** et va commencer à analyser les différents paquets comme dans les dernières simulations après avoir analysé les paquets à l'instant où on allume l'ordinateur on trouve des différentes requêtes, demande et réponse entre l'ordinateur et le serveur afin de se connecter correctement au serveur et à toute cette fonctionnalité grâce à des protocoles qui assure la connexion entre clients et serveurs comme **SMB2**:

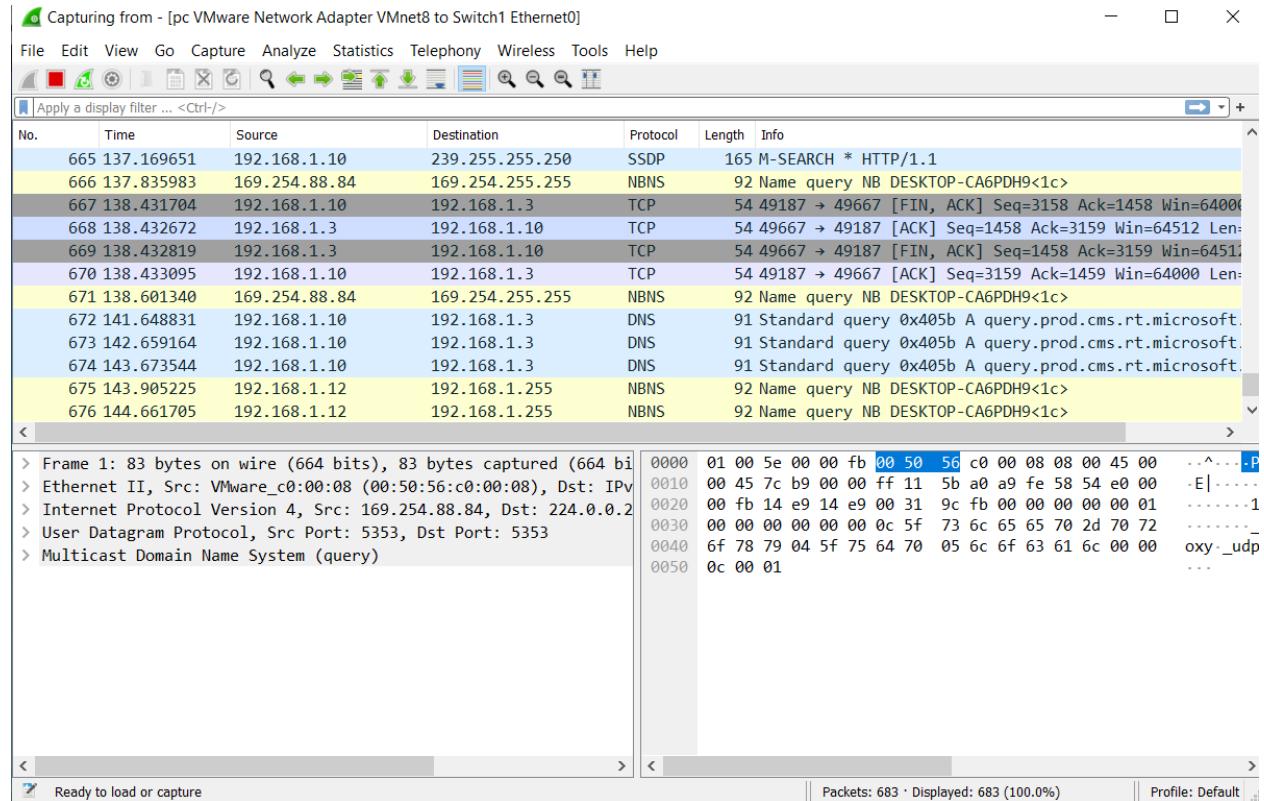


La figure suivante va présenter lors de la connexion à la session qu'on a créé par le serveur AD :



Comme on peut remarquer la présence du protocole **DRSUAPI** qui est un protocole utilisé par **AD** pour accéder et manipuler les données stockées dans les

bases de données d'**Active Directory**. Et à la fin de la connexion et quand finalement on rejoint la session on trouve encore dans notre analyseur



NBNS ou la version précédente du **DNS** qui traduit le nom des hôtes en adresse IP.

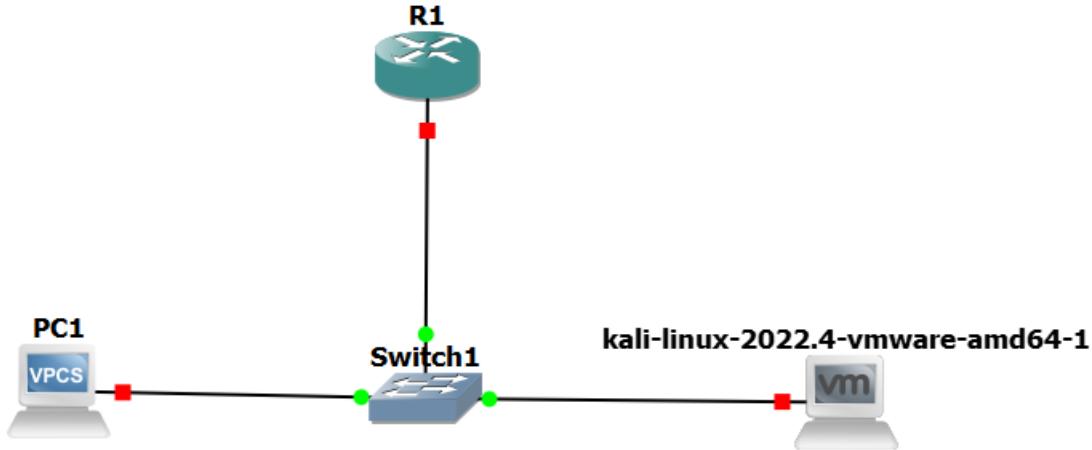
## 9. L'identification des stations qui génèrent un trafic important :

Il est devenu clair maintenant après avoir analyser les échanges entre pc et pc et pc et serveur que les stations qui génèrent un trafic important dans notre réseaux Lan sont des stations comme des serveurs dans leurs connexion avec les ordinateurs et les périphériques car grâce au différent serveur on peut assurer une connexion ou transfère de fichier et des donnés entre les différents périphériques hôtes

## 10. Simulation d'une attaque avec Yersinia :

Alors pour tester et analyser le système de sécurité on va simuler une attaque avec **Yersinia** à l'aide de **Kali Linux**. **Yersinia** est un outil de pénétration testing qui peut être utilisé pour simuler différentes attaques de réseau. Il est souvent utilisé pour tester la sécurité d'un réseau et identifier les vulnérabilités qui pourraient être

exploit es par des attaquants. On va essayer d'attaquer maintenant un serveur DHCP avec cet outil dans GNS3.



Ici le routeur R1 vas jouer le rôle de serveur **DHCP** mais avant ca il faut le configurer avec les commandes suivantes :

```
*Mar 1 00:00:02.235: %SW_VLAN-4-IFS_FAILURE: VLAN manager encountered file operation error: call = ifs_open/read / code =  
    / bytes transferred = 0  
*Mar 1 00:00:02.251: %LINEPROTO-5-UPDOWN: Line protocol on Interface VoIP-Null0, changed state to up  
*Mar 1 00:00:02.359: %SYS-5-CONFIG_I: Configured from memory by console  
*Mar 1 00:00:02.467: %SYS-5-RESTART: System restarted --  
Cisco IOS Software, 2600 Software (C2691-ENTSERVICESK9-M), Version 12.4(13b), RELEASE SOFTWARE (fc3)  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2007 by Cisco Systems, Inc.  
Compiled Tue 24-Apr-07 15:33 by prod_rel_team  
*Mar 1 00:00:02.475: %SNMP-5-COLDSTART: SNMP agent on host R1 is undergoing a cold start  
*Mar 1 00:00:03.211: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down  
*Mar 1 00:00:03.239: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down  
*Mar 1 00:00:04.211: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down  
*Mar 1 00:00:04.239: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down  
R1#  
R1#  
R1#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
R1(config)#int f0/0  
R1(config-if)#ip address 10.0.0.1 255.0.0.0  
R1(config-if)#no shutdown  
R1(config-if)#  
*Mar 1 00:02:36.379: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up  
*Mar 1 00:02:37.379: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up  
R1(config-if)#
```

Est passer maintenant a la configuration du serveur **DHCP** qui est configurer lui aussi dans la figure suivante.

```

Compiled Tue 24-Apr-07 15:33 by prod_rel_team
*Mar 1 00:00:02.475: %SNMP-5-COLDSTART: SNMP agent on host R1 is undergoing a cold start
*Mar 1 00:00:03.211: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down
*Mar 1 00:00:03.239: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
*Mar 1 00:00:04.211: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down
*Mar 1 00:00:04.239: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
R1#
R1#
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int f0/0
R1(config-if)#ip address 10.0.0.1 255.0.0.0
R1(config-if)#no shutdown
R1(config-if)#
*Mar 1 00:02:36.379: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 00:02:37.379: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config-if)#exit
R1(config)#service dhcp
R1(config)#ip dhcp pool hem
R1(dhcp-config)#network 10.0.0.0
R1(dhcp-config)#default-router 10.0.0.1
R1(dhcp-config)#lease 5
R1(dhcp-config)#exit
R1(config)#ip dhcp excluded-address 10.0.0.1
R1(config)#

```



Solar-PuTTY *free tool*

© 2019 SolarWinds Worldwide, LLC. All rights reserved.

Apres avoir fini la configuration du routeur et du serveur DHCP on vas tester maintenant si notre machine c'est bien connecter au service :

```

PC1> ?
?                                     Print help
! _COMMAND [ARG ...]      Invoke an OS _COMMAND with optional ARG(s)
arp                                     Shortcut for: show arp. Show arp table
clear ARG                            Clear IPv4/IPv6, arp/neighbor cache, command history
dhcp [OPTION]                         Shortcut for: ip dhcp. Get IPv4 address via DHCP
disconnect                           Exit the telnet session (daemon mode)
echo TEXT                             Display TEXT in output. See also set echo ?
help                                   Print help
history                               Shortcut for: show history. List the command history
ip ARG ... [OPTION]                  Configure the current VPC's IP settings. See ip ?
load [FILENAME]                      Load the configuration/script from the file FILENAME
ping HOST [OPTION ...]               Ping HOST with ICMP (default) or TCP/UDP. See ping ?
quit                                  Quit program
relay ARG ...                        Configure packet relay between UDP ports. See relay ?
rlogin [ip] port                     Telnet to port on host at ip (relative to host PC)
save [FILENAME]                      Save the configuration to the file FILENAME
set ARG ...                           Set VPC name and other options. Try set ?
show [ARG ...]                       Print the information of VPCs (default). See show ?
sleep [seconds] [TEXT]                Print TEXT and pause running script for seconds
trace HOST [OPTION ...]              Print the path packets take to network HOST
version                               Shortcut for: show version

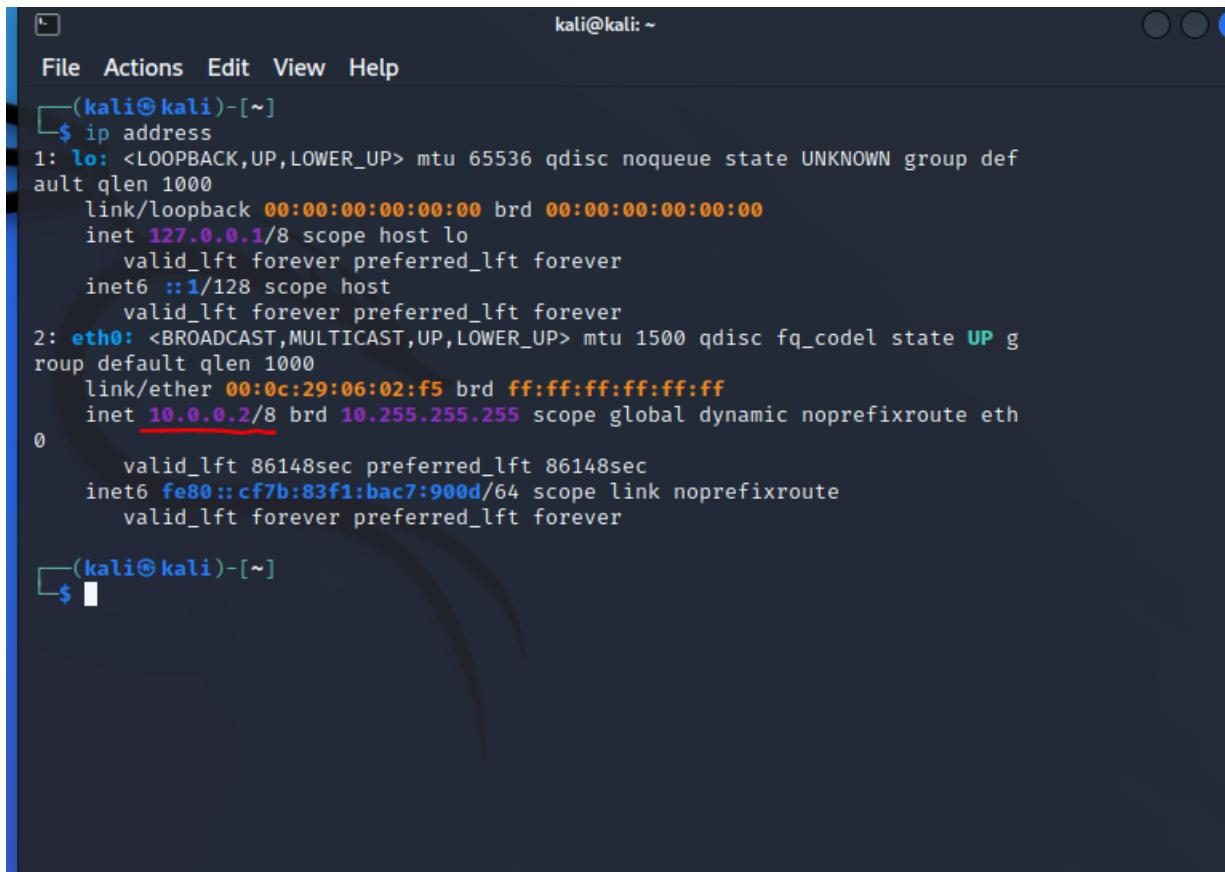
To get command syntax help, please enter '?' as an argument of the command.

PC1> dhcp
DDORA IP 10.0.0.4/8 GW 10.0.0.1

PC1> show ip
NAME       : PC1[1]
IP/MASK   : 10.0.0.4/8
GATEWAY   : 10.0.0.1
DNS        :
DHCP SERVER : 10.0.0.1
DHCP LEASE  : 431994, 432000/216000/378000
MAC        : 00:50:79:66:68:00
LPORT      : 10012
RHOST:PORT : 127.0.0.1:10013
MTU:       : 1500

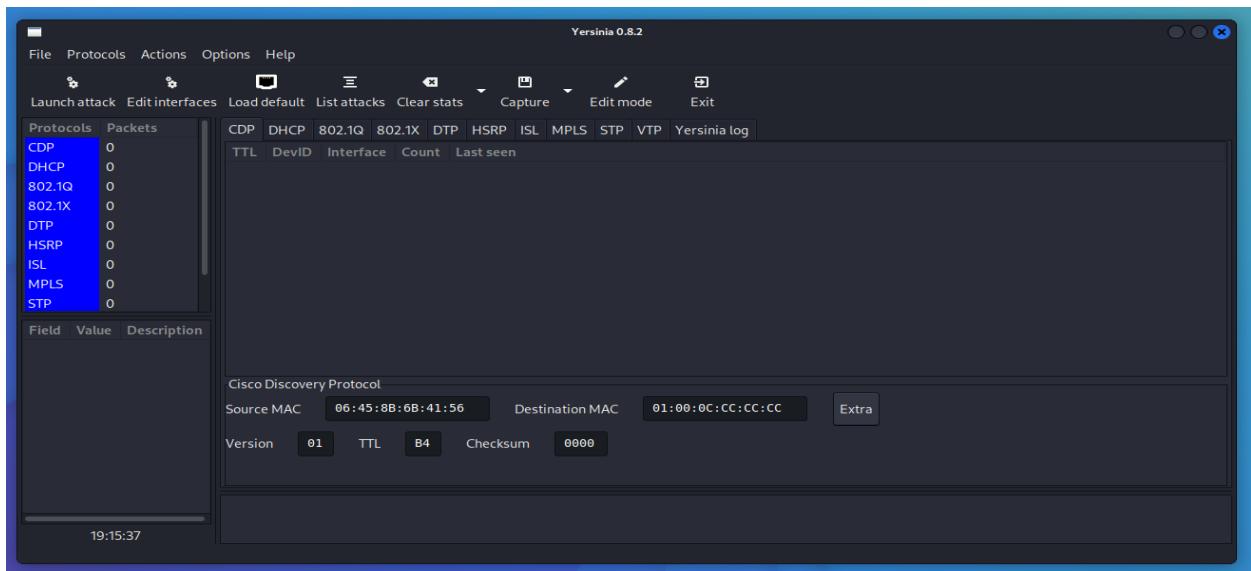
```

Grace à la commande **show IP** et **DHCP** on peut vérifier que le service marche parfaitement même dans notre deuxième machine **kali linux**

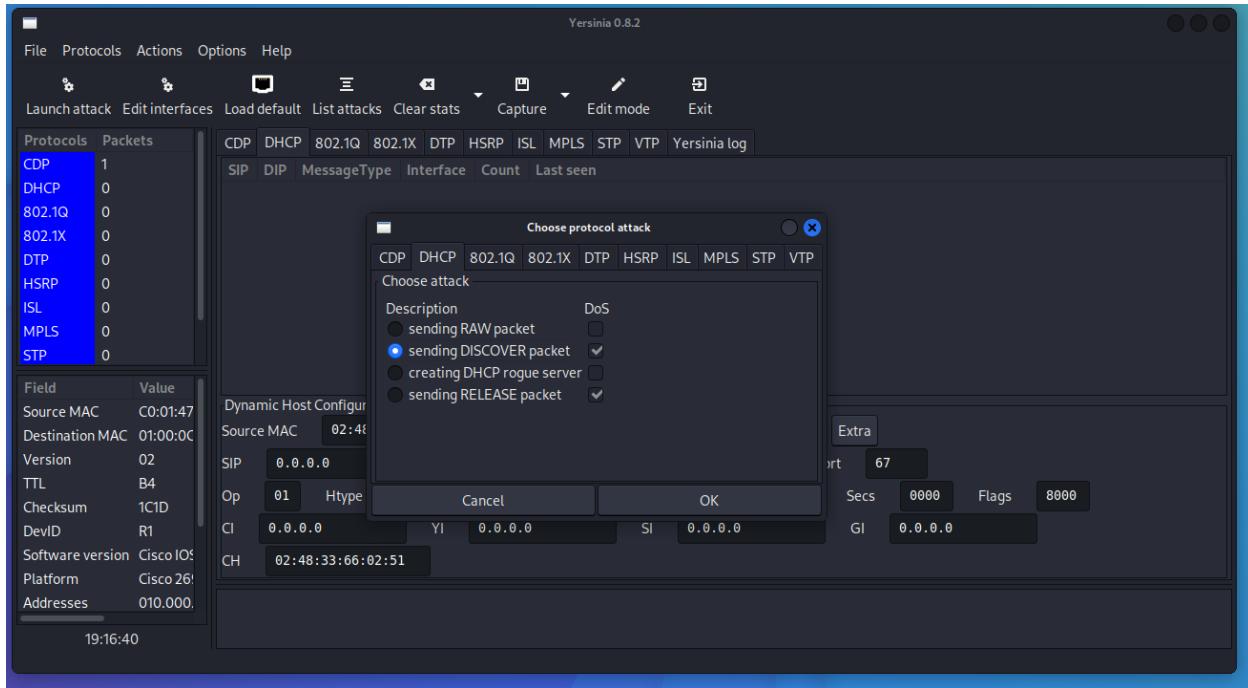


```
kali@kali: ~
File Actions Edit View Help
[(kali㉿kali)-[~]
$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:06:02:f5 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.2/8 brd 10.255.255.255 scope global dynamic noprefixroute eth0
        valid_lft 86148sec preferred_lft 86148sec
    inet6 fe80::cf7b:83f1:bac7:900d/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[(kali㉿kali)-[~]
$ ]
```

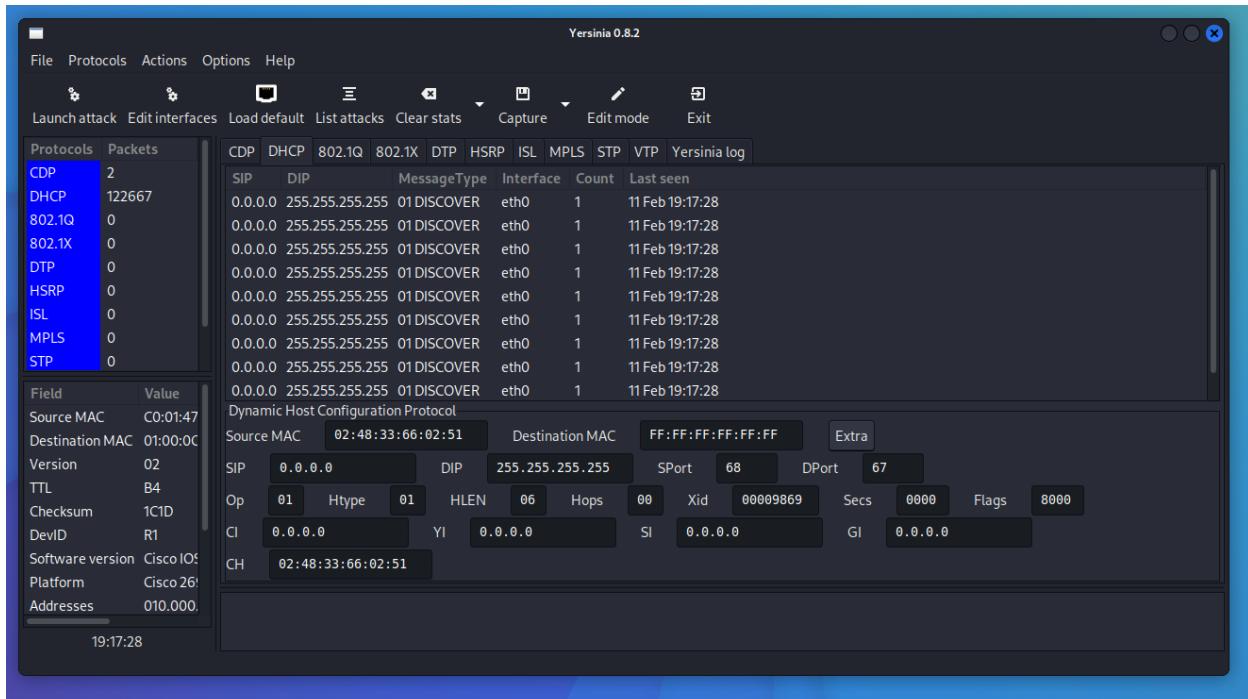
Comme dans la figure précédente notre machine a comme IP l'adresse fournit par le **DHCP**. Maintenant on lance Yersinia qui a une interface graphique comme ça



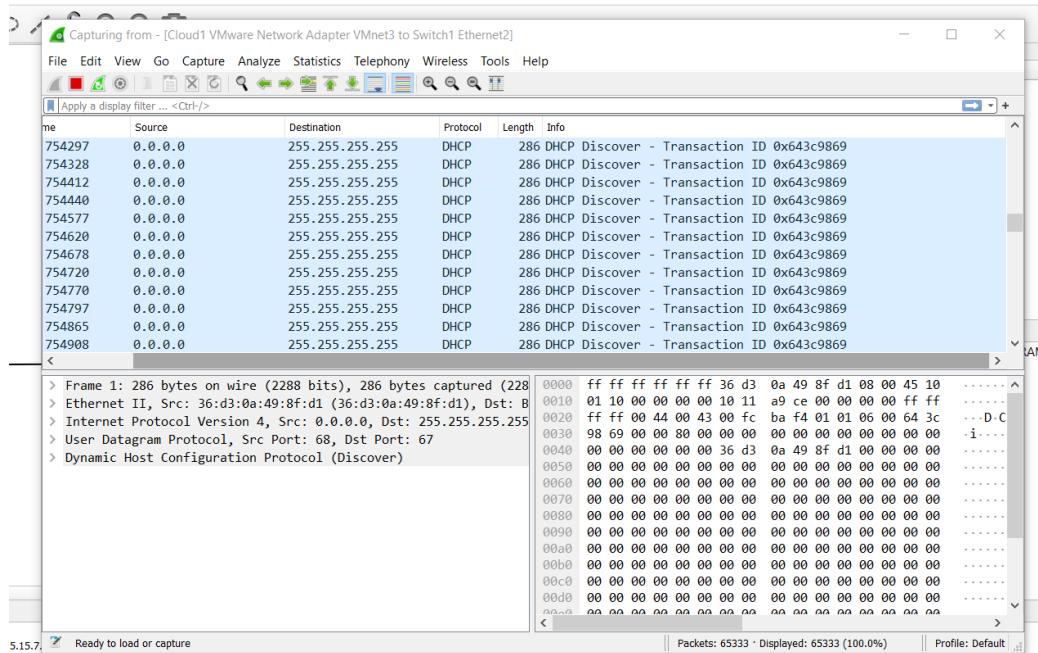
Et on débute l'attaque on clique sur launch attaque :



L'attaque a commencer :



Analysons les paquets avec **Wire Shark** on va voir comment l'attaque fonctionne :



Maintenant le service **DHCP** ne va plus fonctionner dans notre machine :

```

PC1> show ip
NAME      : PC1[1]
IP/MASK   : 10.0.0.3/8
GATEWAY   : 10.0.0.1
DNS       :
DHCP SERVER : 10.0.0.1
DHCP LEASE  : 86393, 86400/43200/75600
MAC        : 00:50:79:66:68:00
LPORT      : 10006
RHOST:PORT : 127.0.0.1:10007
MTU:       : 1500

PC1> renew ip
Bad command: "renew ip". Use ? for help.

PC1> dhcp
DDD
Can't find dhcp server
PC1>

```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

Maintenant si on arrête l'attaque et on demande encore une fois une adresse IP le service **DHCP** vas fonctionner normalement :

```
PC1> dhcp
DDD
Can't find dhcp server

PC1> dhcp
DORA IP 10.0.0.3/8 GW 10.0.0.1
```

Est comme ça on va pouvoir simuler une attaque sur notre réseau ou peu conclure que la présence d'un firewall physique ou parfois software est importante pour protéger notre système des connexions non autoriser qui peuvent créer des problèmes et des fails

## 11. Concevoir un plan d'action :

Pour concevoir un plan d'action à fin d'optimiser le fonctionnement de notre réseau, nous avons conçu les étapes suivantes :

- **Evaluation du réseau :** grâce à l'utile **Wire Shark** ou d'autre outils open source on peut évaluer la performance actuelle du réseau en utilisant des outils de surveillance et de diagnostic pour identifier les problèmes tels que la latence, les erreurs de paquet...
- **Identification de problème :** On analyse tous les données collectées par notre analyseur on peut y comprendre la nature de notre problème et concevoir un plan d'action pour le traiter.
- **Mise en évaluation :** avec notre plan d'action on commence à évaluer les différentes solutions possibles et tester encore une fois jusqu'à ce qu'il marche.
- La prise des notes des tâches réalisées.

## 12. Le guide de maintenance :

Afin d'élaborer notre guide de maintenance d'après les simulations précédentes nous allons avoir besoin d'une boîte à outils avec des logiciels open source afin de nous aider à mieux gérer la maintenance de notre réseau Lan,

### 12.1. La boîte à outils :

1. **GNS-3**, **GNS-3** est un simulateur de réseau open source qui permet de simuler et de tester des réseaux informatiques complexes. Il permet aux utilisateurs de concevoir et de tester leur réseau sans avoir à acheter des équipements coûteux.

**GNS-3** peut être utilisé pour simuler des réseaux basés sur des équipements tels que des routeurs, des commutateurs et des ordinateurs. Les utilisateurs peuvent également utiliser **GNS-3** pour simuler des réseaux en utilisant des images de logiciels pour des équipements réels.

2. **Wire Shark**, **Wireshark** est un analyseur de paquets réseau open source. Il permet aux utilisateurs de capturer, de visualiser et d'analyser les données réseau en temps réel, il est utilisé pour déboguer les problèmes de réseau, surveiller les performances du réseau et garantir la sécurité des données réseau.

3. **Linux**, Linux est un système d'exploitation open source populaire qui peut être utilisé pour de nombreuses tâches différentes. Il peut-être comme un serveur ou une station de travaille chose qui aide lors de la simulation du réseau.

Grace a ces outils on peut élaborer un guide de maintenance qui commence par :

- Installation de GNS3 et simuler les différent composant et les dispositifs présent dans le réseau comme routeur, switch....
- Utiliser Linux pour configurer et installer les différent service dans le réseau comme le serveur et les ordinateurs.
- Mise en place de Wire Shark pour que ce derniers analyse les paquets réseau et surveiller les performances du réseau a fin de détecter la source du problème
- Utilisation des informations reçu de Wire Shark pour debugger le problème et le résoudre dans notre simulation grâce à GNS-3 et Linux.
- Enregistrer les données et les étapes effectuer.