Base

AP2 - MISSION 2 : DÉCOUPAGE DU RÉSEAU AMÉLIORE

ALEXANDRE ALSINA **Plan TCP/IP optimisé / Une notice technique sur les solutions possibles de logiciels de scan réseau et votre choix puis sur la mise en place de la distribution automatique des IP par réservation dans les différents VLANs.**

ENZO AZALBERT **Répartition humaine et temporelle / Une notice technique sur les solutions possibles de logiciels de prise en main à distance et votre choix / Plan TCP/IP optimisé**

FÉLICIEN LANTOINE **Un plan du réseau détaillé sous Visio et un plan de nommage des équipements / Une notice technique sur la création des VLANs et la communication entre ces VLANs / Plan TCP/IP optimisé**

Réunions :

Jour 1 : **Réunion Jour 1 (début) - Google Docs**

Jour 2 : **Réunion Jour-2 - Google Docs**

Jour 3 : **Réunion Jour-3 - Google Docs**

Jour 4 : **Réunion Jour-4 - Google Docs**

🧑‍💻 logiciels de prise en main à distance

Notice Technique : Solutions de Logiciels de Prise en Main à Distance

1. Introduction

Les logiciels de prise en main à distance permettent d'accéder et de contrôler un ordinateur distant via un réseau. Ils sont utilisés pour l'assistance technique, l'administration informatique et le télétravail. Cette notice présente plusieurs solutions disponibles ainsi qu'une recommandation finale.

2. Solutions Disponibles

2.1. TeamViewer

- **Avantages :**
  - **Interface intuitive et facile à utiliser.**
  - **Fonctionnalités avancées (transfert de fichiers, chat, gestion multi-écrans).**
  - **Sécurisé avec un chiffrement de bout en bout.**
  - **Disponible sur Windows, macOS, Linux, Android et iOS.**
- **Inconvénients :**
  - **Version gratuite limitée à un usage personnel.**
  - **Coût élevé pour les entreprises.**

2.2. AnyDesk

- **Avantages :**
  - **Léger et rapide, avec faible latence.**
  - **Sécurité renforcée avec chiffrement AES 256 bits.**
  - **Compatible avec plusieurs plateformes.**
  - **Offre une version gratuite pour un usage personnel.**
- **Inconvénients :**
  - **Moins de fonctionnalités collaboratives que TeamViewer.**
  - **Version gratuite avec limitations.**

2.3. Chrome Remote Desktop

- **Avantages :**
  - **Gratuit et intégré à Google Chrome.**
  - **Facile à installer et utiliser.**
  - **Disponible sur diverses plateformes (Windows, macOS, Linux).**
- **Inconvénients :**
  - **Fonctionnalités limitées (pas de transfert de fichiers natif, pas de chat).**
  - **Dépendance à Google Chrome.**

2.4. Microsoft Remote Desktop (RDP)

- **Avantages :**
  - **Intégré à Windows, donc pas de coût supplémentaire.**
  - **Bonne performance sur un réseau local.**
  - **Sécurité renforcée avec authentification réseau.**
- **Inconvénients :**
  - **Moins efficace sur Internet que d'autres solutions.**
  - **Nécessite une configuration avancée et un accès réseau direct.**

2.5. VNC (Virtual Network Computing)

- **Avantages :**
  - **Open source et configurable.**
  - **Fonctionne sur plusieurs systèmes d'exploitation.**
  - **Adapté aux environnements d'entreprise.**
- **Inconvénients :**
  - **Configuration technique plus complexe.**
  - **Moins performant sur des connexions lentes.**

3. Recommandation

Le choix du logiciel dépend des besoins spécifiques :

- **Pour une utilisation personnelle et gratuite : Chrome Remote Desktop ou AnyDesk.**
- **Pour une entreprise avec des besoins avancés : TeamViewer pour ses fonctionnalités complètes.**
- **Pour un usage en réseau local : Microsoft Remote Desktop.**
- **Pour une solution open source et flexible : VNC.**

Si un bon équilibre entre performances, fonctionnalités et coût est recherché, AnyDesk est un excellent compromis grâce à sa rapidité et son coût raisonnable pour les entreprises.

4. Conclusion

Chaque solution présente des avantages et des inconvénients selon l'usage prévu. Il est recommandé de tester plusieurs solutions avant de choisir celle qui correspond le mieux aux besoins spécifiques de l'entreprise ou de l'utilisateur.

Dans notre cas, nous utiliserons TeamViewer. Voici une notice d'utilisation de ce logiciel.

NOTICE D'UTILISATION DE TEAMVIEWER

1. Présentation de TeamViewer

TeamViewer est un logiciel permettant la prise en main à distance d'un ordinateur, le partage d'écran, le transfert de fichiers et la collaboration en ligne. Il est utilisé pour l'assistance technique, le travail à distance et les réunions en ligne.

---

2. Installation de TeamViewer

1. **Téléchargement**
   - **Rendez-vous sur le site officiel : https://www.teamviewer.com**
   - **Téléchargez la version adaptée à votre système d'exploitation (Windows, macOS, Linux).**
2. **Installation**
   - **Lancez le fichier d'installation.**
   - **Choisissez "Installation par défaut" et cliquez sur "Suivant".**
   - **Acceptez les conditions d'utilisation et terminez l'installation.**
3. **Pour l'installation sous debian, la manipulation est différente car nous n'avons pas d'interface graphique.**
   - **wget https://download.teamviewer.com/download/linux/teamviewer-host_amd64.deb**
   - **dpkg -i teamviewer-host_amd64.deb**
   - **apt --fix-broken install**

   Puis configurer le logiciel :

   → teamviewer setup

---

3. Connexion et Configuration

1. **Lancer TeamViewer**
   - **Ouvrez l'application après l'installation.**
   - **Une fenêtre affiche "Votre ID" et "Votre mot de passe", nécessaires pour la connexion à distance.**
2. **Créer un compte (optionnel)**
   - **Cliquez sur "S'inscrire" pour créer un compte TeamViewer.**
   - **Se connecter permet d'accéder à des fonctionnalités avancées (gestion des appareils, liste de contacts).**

---

4. Prise en main à distance

1. **Contrôler un ordinateur distant**
    - **Demandez à l'utilisateur distant de vous fournir son ID et son mot de passe TeamViewer.**
    - **Entrez l'ID dans la section "Contrôler un ordinateur à distance", puis cliquez sur "Connexion".**
    - **Saisissez le mot de passe fourni et prenez le contrôle de l'appareil.**
2. **Autoriser un accès à distance**
    - **Donnez votre ID et mot de passe à la personne qui souhaite se connecter.**
    - **Une fois la connexion établie, l'utilisateur distant pourra contrôler votre PC.**

Sous debian il suffit d'utiliser la commande pour récupérer l'ID :

→ teamviewer info

---

5. Fonctions Principales

- **Transfert de fichiers :**
    - **Dans la barre supérieure, cliquez sur "Fichier et extras" → "Ouvrir le gestionnaire de transfert de fichiers".**
    - **Sélectionnez les fichiers à envoyer ou à recevoir.**
- **Chat et communication :**
    - **Utilisez la messagerie instantanée ou l'appel audio/vidéo intégrés pendant la session.**
- **Accès non surveillé (sans intervention de l'utilisateur distant) :**
    - **Activez l'option "Accès non surveillé" dans "Options" > "Sécurité".**
    - **Configurez un mot de passe personnel pour éviter de demander un nouveau code à chaque connexion.**

---

6. Sécurité et Bonnes Pratiques

→ Ne communiquez votre ID et votre mot de passe qu'à des personnes de confiance.
→ Activez la double authentification pour une sécurité renforcée.
→ Gardez votre TeamViewer à jour pour bénéficier des dernières améliorations et corrections de sécurité.

DHCP Debian

DHCP Debian

PC-2 (client de TEST)
Adresse MAC : 08:00:27:bc:d6:46
IP 172.16.70.6

Toutes les étapes se feront en root
Lorsque je dirais de sauvegarder cela signifie de faire “ctrl+x” ensuite “o” puis entrer.
Les IP dans cette documentation sont là pour donner un exemple.

Pour configurer un serveur DHCP sous debian nous allons suivre différentes étapes:

1- Mises à jour / installation des différents logiciels pour scanner, agent relais DHCP.
2- Configuration des différents fichiers du DHCP / agent relais DHCP.
2bis- Assigner la même ip à la même machine avec l’adresse MAC
3- Commandes pour scanner le réseau.
4- Test du serveur DHCP avec une autre machine virtuelle en debian.

1- Installation des différents logiciels

En commençant par arp scan qui permet de récupérer les adresses MAC des machines du réseau.
apt install arp scan

Pour ce qui est des Vlans, il faut installer l’extension.
apt install vlan

et les activer avec
modprobe 8021q

Pour l’agent relais DHCP
Commençons par l’installer.
apt install isc-dhcp-relay

2- Configuration des différents fichiers du DHCP

Pour ce qui est des fichiers du DHCP avec les vlans, nous devons dans un premier temps ajouter les interfaces vlans.
nano /etc/network/interfaces

et obtenir un fichier similaire à celui là avec nos vlans.

```
# The primary network interface
allow-hotplug enp0s3
#iface enp0s3 inet manual
#iface enp0s3 inet dhcp
iface enp0s3 inet static
        address 172.16.2.1
        netmask 255.255.255.128



# Vlan 60 - Wifi_Public
auto enp0s3.60
iface enp0s3.60 inet static
        address 172.16.20.1
        netmask 255.255.255.128
        vlan-raw-device enp0s3

# Vlan 70 - Filaire_Public
auto enp0s3.70
iface enp0s3.70 inet static
        address 172.16.21.1
        netmask 255.255.255.128
        vlan-raw-device enp0s3
```

Puis il faut redémarrer le fichier de configurations pour prendre en compte les modifications.
systemctl restart networking

puis modifier le fichier de configuration du DHCP
nano /etc/dhcp/dhcpd.conf

```
subnet 172.16.2.0 netmask 255.255.255.128 {
  range 172.16.2.2 172.16.2.126;
  option routers 172.16.2.1;
}

# Vlan 60 - Wifi_Public
subnet 172.16.20.0 netmask 255.255.255.128 {
        range 172.16.20.2 172.16.20.126;
        option routers 172.16.20.1;
}

# Vlan 70 - Filaire_Public
subnet 172.16.21.0 netmask 255.255.255.128 {
        range 172.16.21.2 172.16.21.126;
        option routers 172.16.21.1;
}
```

ne pas oublier de les ajouter dans isc.

nano /etc/default/isc-dhcp-server

avec cette ligne là qui correspond au différents vlans.

```
INTERFACESv4="enp0s3 enp0s3.60 enp0s3.70 enp0s3.80 enp0s3.90 enp0s3.100 enp0s3.110 enp0s3.120"
```

Voici les différentes commandes à mettre dans un switch cisco.

```
interface Vlan10
 ip helper-address 192.168.10.1

interface Vlan20
 ip helper-address 192.168.20.1
```

Puis redémarrer le service DHCP.

```
systemctl restart isc-dhcp-server
```

Pour l'agent relais DHCP,
nous devons ouvrir le fichier

```
nano /etc/default/isc-dhcp-relay
```

Puis configurer les lignes INTERFACES et SERVERS comme la capture d'écran en dessous.

```
# sourced by /etc/init.d/isc-dhcp-relay
# installed at /etc/default/isc-dhcp-relay by the maintainer scripts

#
# This is a POSIX shell fragment
#

# What servers should the DHCP relay forward requests to?
SERVERS="172.16.2.1"

# On what interfaces should the DHCP relay (dhrelay) serve DHCP requests?
INTERFACES="enp0s3.60 enp0s3.70 enp0s3.80 enp0s3.90 enp0s3.100 enp0s3.110 enp0s3.120 "

# Additional options that are passed to the DHCP relay daemon?
OPTIONS=""
```

Nous avons donc dans SERVERS l'IP de notre serveur DHCP. et dans INTERFACES les différentes interfaces virtuelles en fonction des vlans que nous avons configurés.

Puis il ne reste plus que faire :

```
systemctl restart isc-dhcp-relay
```

2bis- Configuration supplémentaire pour le serveur DHCP fasse en sorte qu'il assigne toujours la même configuration IP à un poste donné

Éditer la configuration du serveur DHCP

Éditer la configuration du serveur DHCP qui se trouve généralement à :

```
nano /etc/dhcp/dhcpd.conf
```

Ajouter une section comme celle-ci pour réserver une IP spécifique à l'adresse MAC du poste :

```
host PC-2 {
        hardware ethernet 08:00:27:bc:d6:46;          # Adresse MAC de la machine
        fixed-address 172.16.2.6;       # IP à assigner
}
```

Redémarrer le serveur DHCP

Après avoir sauvegardé les modifications, redémarre le service DHCP :

```
systemctl restart isc-dhcp-server
```

3- Commandes pour scanner le réseau

Nous avons vu précédemment comment installer arp nous allons maintenant voir comment l'utiliser.

Tout d'abord la commande pour scanner le réseau afin d'obtenir les adresses MAC des machines du réseau est :

```
ip neigh show
```

4- Test du serveur DHCP avec une autre machine virtuelle en debian.

Pour tester notre serveur DHCP,

→ Pour cela il faut la machine debian configurer avec le serveur DHCP ainsi qu'une machine avec un Windows 10 qui servira de client.

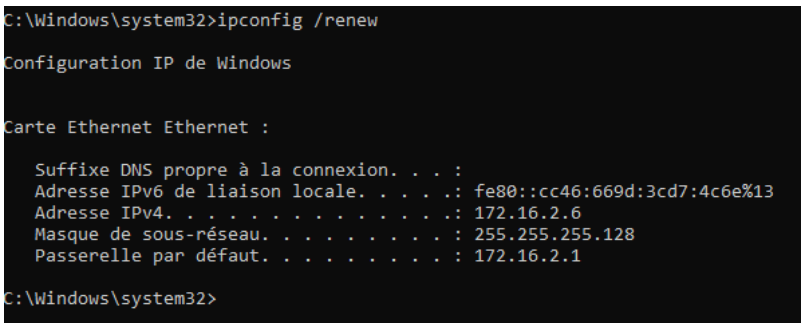
→ Dans la configuration des 2 machines virtualbox :

- Aller dans l'onglet réseau.
- Puis sélectionner le mode d'accès réseau : Réseau interne.
- Name : intnet.

Une fois celà effectué, il faut se rendre sur la machine virtuelle qui sert de client.
Ouvrir un CMD en tant qu'administrateur.
Il ne reste plus que faire la commande suivante :

```
ipconfig /renew
```

nous pouvons nous apercevoir que si les configurations précédentes ont bien été effectué la machine recevra l'ip que nous lui avons attribué et elle sera toujours la même.



Toutes les étapes se feront en root
Lorsque je dirais de sauvegarder cela signifie de faire “ctrl+x” ensuite “o” puis entrer.
Les IP dans cette documentation sont là pour donner un exemple.

Pour configurer un serveur DHCP sous debian nous allons suivre différentes étapes:

1- Mises à jour / installation du DHCP.
2- Configuration des différents fichiers du DHCP.
3- Test du serveur DHCP avec une autre machine virtuelle en debian.
4- Changer le nom de l’hôte sous debian.
5- Installation et configuration de TFTP.
6- Test de TFTP avec une autre machine virtuelle en debian

1- Mises à jour / installation du DHCP

apt update Mise à jour du debian.

apt install isc-dhcp-server Permet d’installer les fichiers de configuration du server DHCP

2- Configuration des différents fichiers du DHCP

ip a Pour récupérer l’interface juste après le “2:” normalement il s’agit de enp0s3

nano /etc/default/isc-dhcp-server Pour accéder au fichier texte du dhcp server et le modifier

→ Les lignes à modifier sont : DHCPv4_CONF à dé-commenter et spécifier l'interface dans INTERFACESv4.Puis sauvegarder.

```
  GNU nano 5.4                          /etc/default/isc-dhcp-server
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
#       Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="enp0s3"
#INTERFACESv6=""
```

nano /etc/network/interfaces Pour configurer le réseau du serveur.

→ il faudra commenter la ligne iface enp0s3 inet dhcp
puis ajouter en dessous:

iface enp0s3 inet static
address 172.16.2.1
netmask 255.255.255.128

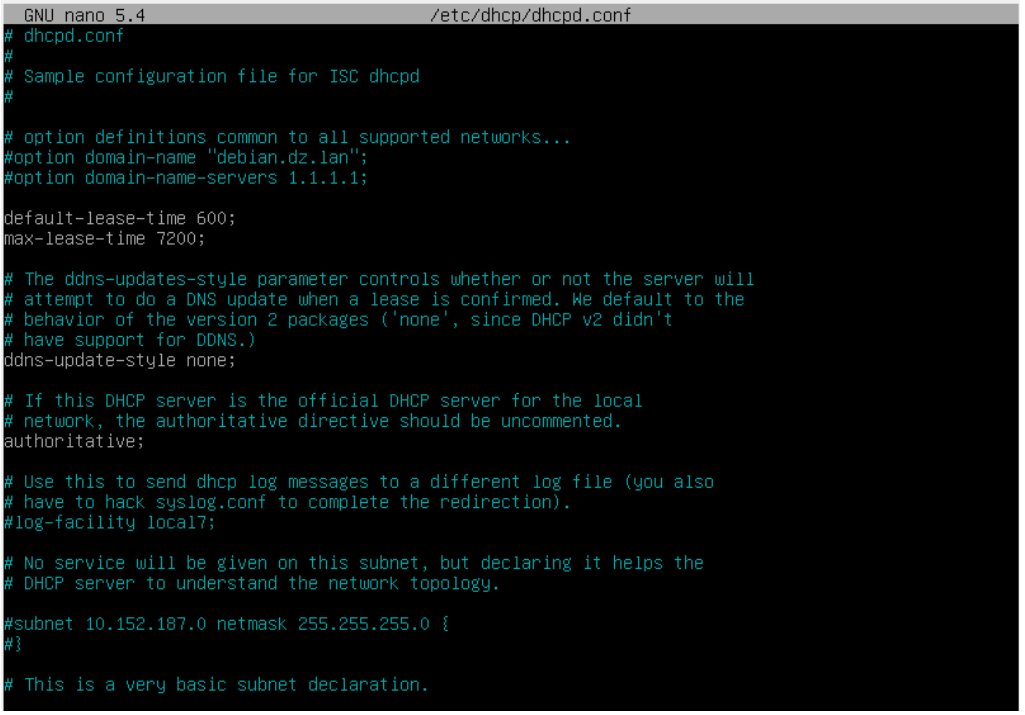
```
  GNU nano 5.4                                  /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
#iface enp0s3 inet dhcp
iface enp0s3 inet static
        address 172.16.2.1
        netmask 255.255.255.128
```

Puis enregistrer

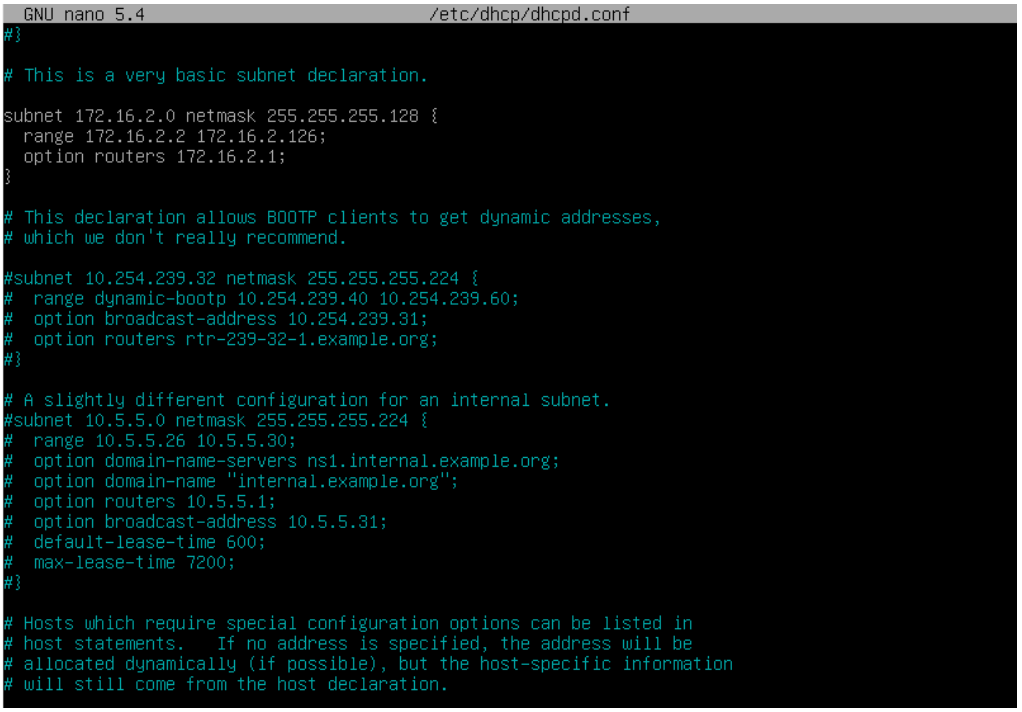
Le reste de la configuration se passera dans un seul est même fichier qui est :

nano /etc/dhcp/dhcpd.conf

→ il suffit de compléter, dé-commenter ou commenter certaines lignes de façon à obtenir un fichier de configuration similaire à la capture d'écran.



```
  GNU nano 5.4                              /etc/dhcp/dhcpd.conf
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#

# option definitions common to all supported networks...
#option domain-name "debian.dz.lan";
#option domain-name-servers 1.1.1.1;

default-lease-time 600;
max-lease-time 7200;

# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
ddns-update-style none;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
#log-facility local7;

# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.

#subnet 10.152.187.0 netmask 255.255.255.0 {
#}

# This is a very basic subnet declaration.
```



```
  GNU nano 5.4                              /etc/dhcp/dhcpd.conf
#}

# This is a very basic subnet declaration.

subnet 172.16.2.0 netmask 255.255.255.128 {
  range 172.16.2.2 172.16.2.126;
  option routers 172.16.2.1;
}

# This declaration allows BOOTP clients to get dynamic addresses,
# which we don't really recommend.

#subnet 10.254.239.32 netmask 255.255.255.224 {
#  range dynamic-bootp 10.254.239.40 10.254.239.60;
#  option broadcast-address 10.254.239.31;
#  option routers rtr-239-32-1.example.org;
#}

# A slightly different configuration for an internal subnet.
#subnet 10.5.5.0 netmask 255.255.255.224 {
#  range 10.5.5.26 10.5.5.30;
#  option domain-name-servers ns1.internal.example.org;
#  option domain-name "internal.example.org";
#  option routers 10.5.5.1;
#  option broadcast-address 10.5.5.31;
#  default-lease-time 600;
#  max-lease-time 7200;
#}

# Hosts which require special configuration options can be listed in
# host statements.   If no address is specified, the address will be
# allocated dynamically (if possible), but the host-specific information
# will still come from the host declaration.
```

Puis enregistrer

il ne reste plus qu'à rallumer le DHCP :
systemctl restart isc-dhcp-server

3- Test du serveur DHCP avec une autre machine virtuelle en debian.

→ Pour cela il faut la machine debian configurer avec le serveur DHCP ainsi qu'une machine avec un debian qui servira de client.

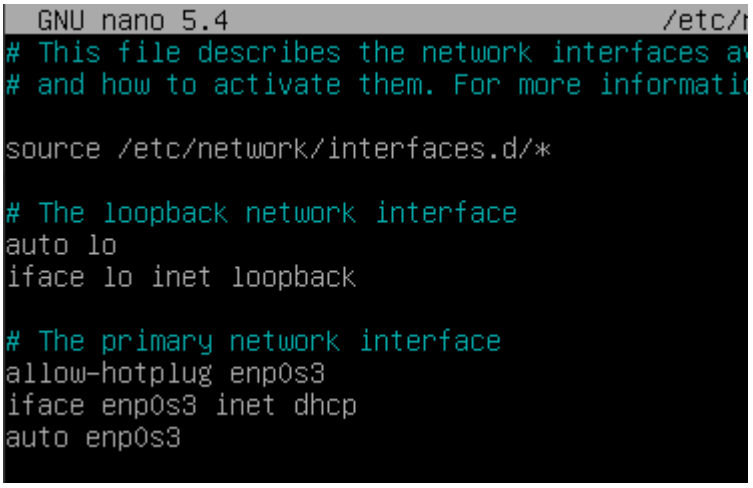
→ Dans la configuration des 2 machines virtualbox :

- Aller dans l'onglet réseau.
- Puis sélectionner le mode d'accès réseau : Réseau interne.
- Name : intnet.

Une fois celà effectué, il faut se rendre sur la machine virtuelle qui sert de client.

nano /etc/network/interfaces Permet d'ouvrir le fichier qui contient l'interface de réseau de la machine.

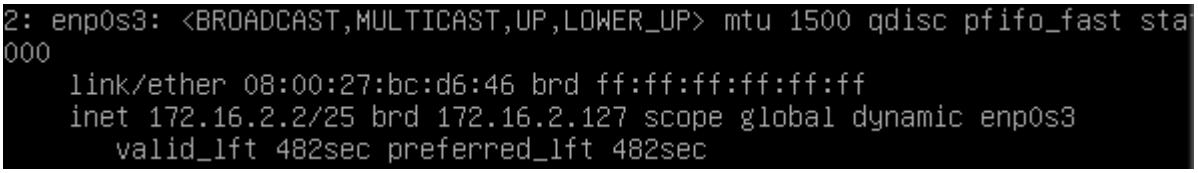
→ ajouter les lignes manquantes pour que le fichier ressemble à celui là:



Puis enregistrer

systemctl restart networking

ip a Vérifier que l'ip obtenu sur la machine client correspond à la plage donner au serveur DHCP



4- Changer le nom de l'hôte sous debian.

Pour changer le nom de l'hôte, il suffit d'effectuer la commande suivante :

→ hostnamectl set-hostname "new_hostname"

Exemple : hostnamectl set-hostname "LOLEsport"

NOMENCLATURE

Nomenclature par SWITCH :

- SW_Ligue_Basket
- SW_Ligue_Volley
- SW_Ligue_Football
- SW_Ligue_Curling
- SW_Ligue_LOL
- SW_DMZ
- SW_Ecrans_Affichage
- SW_Serveur_Switch
- SW_Service_Informatique
- SW_Administration

Règles de nommage des appareils :

- **Préfixe :** `PC-`
- **Nom de la ligue ou fonction :** `Basket`, `Volley`, `Foot`, `LoL`, etc.…
- **Numéro d'identifiant unique :** `01`, `02`, `03`, …

Nomenclature par VLAN / ligue :

VLAN	Nom VLAN	Sous-réseau	Nomenclature des PC
10	Ligue_Basket	172.16.10.0/26	PC-BASKET01 à PC-BASKET62
20	Ligue_Volley	172.16.10.64/26	PC-VOLLEY01 à PC-VOLLEY62
30	Ligue_Football	172.16.10.128/26	PC-FOOT01 à PC-FOOT62
40	Ligue_Curling	172.16.10.192/26	PC-CURLING01 à PC-CURLING62
50	Ligue_LoL	172.16.11.0/26	PC-LOL01 à PC-LOL62
60	WiFi_Public	172.16.20.0/25	PC-WIFI01 à PC-WIFI126
70	Filaire_Public	172.16.21.0/25	PC-FILAIRE01 à PC-FILAIRE126
80	Admin	172.16.30.0/25	PC-ADMIN01 à PC-ADMIN126
90	Écrans_Affichage	172.16.40.0/28	PC-ECRAN01 à PC-ECRAN14
100	DMZ	172.16.50.0/27	SRV-DMZ01 à SRV-DMZ30
110	Serveur_Switch	172.16.60.0/28	SRV-SW01 à SRV-SW14
120	Service_Info	172.16.70.0/28	PC-INFO01 à PC-INFO14

PLAN TCP/IP

PLAN TCP/IP OPTIMISÉ (Trié par Nombre de Postes) :

1️⃣ Réseaux avec 126 utilisateurs/postes :

- **Wi-Fi Public**
  - **Adresse réseau : 172.16.20.0**
  - **Masque : 255.255.255.128 (/25)**
  - **Plage d'IP utilisables : 172.16.20.1 - 172.16.20.126**
  - **Passerelle : 172.16.20.1**
  - **Adresse de diffusion : 172.16.20.127**

- **Filaire Public (salles ressources)**
  - **Adresse réseau : 172.16.21.0**
  - **Masque : 255.255.255.128 (/25)**
  - **Plage d'IP utilisables : 172.16.21.1 - 172.16.21.126**
  - **Passerelle : 172.16.21.1**
  - **Adresse de diffusion : 172.16.21.127**

- **Bureaux Administratifs, Reprographie, Multimédia**
  - **Adresse réseau : 172.16.30.0**
  - **Masque : 255.255.255.128 (/25)**
  - **Plage d'IP utilisables : 172.16.30.1 - 172.16.30.126**
  - **Passerelle : 172.16.30.1**
  - **Adresse de diffusion : 172.16.30.127**

2️⃣ Réseaux avec 62 postes :

- **Ligue Basket**
  - **Adresse réseau : 172.16.10.0**
  - **Masque : 255.255.255.192 (/26)**
  - **Plage d'IP utilisables : 172.16.10.1 - 172.16.10.62**
  - **Passerelle : 172.16.10.1**
  - **Adresse de diffusion : 172.16.10.63**

- **Ligue Volley-Ball**
  - **Adresse réseau : 172.16.10.64**
  - **Masque : 255.255.255.192 (/26)**
  - **Plage d'IP utilisables : 172.16.10.65 - 172.16.10.126**
  - **Passerelle : 172.16.10.65**
  - **Adresse de diffusion : 172.16.10.127**

- **Ligue Football**
  - **Adresse réseau : 172.16.10.128**
  - **Masque : 255.255.255.192 (/26)**

    - **Plage d'IP utilisables : 172.16.10.129 - 172.16.10.190**
    - **Passerelle : 172.16.10.129**
    - **Adresse de diffusion : 172.16.10.191**

- **Ligue Curling**
    - **Adresse réseau : 172.16.10.192**
    - **Masque : 255.255.255.192 (/26)**
    - **Plage d'IP utilisables : 172.16.10.193 - 172.16.10.254**
    - **Passerelle : 172.16.10.193**
    - **Adresse de diffusion : 172.16.10.255**

    -
- **Ligue LoL**
    - **Adresse réseau : 172.16.11.0**
    - **Masque : 255.255.255.192 (/26)**
    - **Plage d'IP utilisables : 172.16.11.1 - 172.16.11.62**
    - **Passerelle : 172.16.11.1**
    - **Adresse de diffusion : 172.16.11.63**
      128

3️⃣ Réseau avec 30 serveurs :

- **DMZ (serveurs accessibles)**
    - **Adresse réseau : 172.16.50.0**
    - **Masque : 255.255.255.224 (/27)**
    - **Plage d'IP utilisables : 172.16.50.1 - 172.16.50.30**
    - **Passerelle : 172.16.50.1**
    - **Adresse de diffusion : 172.16.50.31**

4️⃣ Réseaux avec 14 équipements/postes :

- **Écrans d'affichage**
    - **Adresse réseau : 172.16.40.0**
    - **Masque : 255.255.255.240 (/28)**
    - **Plage d'IP utilisables : 172.16.40.1 - 172.16.40.14**
    - **Passerelle : 172.16.40.1**
    - **Adresse de diffusion : 172.16.40.15**

- **Réseau Serveurs & Switches**
    - **Adresse réseau : 172.16.60.0**
    - **Masque : 255.255.255.240 (/28)**
    - **Plage d'IP utilisables : 172.16.60.1 - 172.16.60.14**
    - **Passerelle : 172.16.60.1**
    - **Adresse de diffusion : 172.16.60.15**

- **Réseau Service Informatique**
  - **Adresse réseau : 172.16.70.0**
  - **Masque : 255.255.255.240 (/28)**
  - **Plage d’IP utilisables : 172.16.70.1 - 172.16.70.14**
  - **Passerelle : 172.16.70.1**
  - **Adresse de diffusion : 172.16.70.15**

PLAN VLANS

Plan des VLANs sur le Switch Principal

Nous devons d’abord **créer tous les VLANs** sur le **switch principal et les autres switch**.

```
enable
configure terminal
vlan 10
name Ligue_Basket
vlan 20
name Ligue_Volley
vlan 30
name Ligue_Football
vlan 40
name Ligue_Curling
vlan 50
name Ligue_LoL
vlan 60
name WiFi_Public
vlan 70
name Filaire_Public
vlan 80
name Admin
vlan 90
name Ecrans_Affichage
vlan 100
name DMZ
vlan 110
name Serveur_Switch
vlan 120
name Service_Informatique
```

```
enable
configure terminal
interface range FastEthernet 0/1 - FastEthernet 0/6
switchport mode trunk
switchport trunk allowed vlan 110
exit
interface range FastEthernet 0/7 - FastEthernet 0/12
switchport mode trunk
switchport trunk allowed vlan 120
exit
interface range FastEthernet 0/13 - FastEthernet 0/18
switchport mode trunk
switchport trunk allowed vlan 130
exit
interface range FastEthernet 0/19 - FastEthernet 0/20
switchport mode trunk
switchport trunk allowed vlan 1
exit
```

```
enable
configure terminal
interface range FastEthernet 0/1 - FastEthernet 0/6
switchport mode access
switchport access vlan 110
exit
interface range FastEthernet 0/7 - FastEthernet 0/12
switchport mode access
switchport access vlan 120
exit
interface range FastEthernet 0/13 - FastEthernet 0/18
switchport mode access
switchport access vlan 130
exit
interface range FastEthernet 0/19 - FastEthernet 0/20
switchport mode access
switchport access vlan 1
exit
```

```
enable
configure terminal
vtp domain TEST
```

```
enable
configure terminal
vlan 110
name ADMINISTRATIF
vlan 120
name DEVELOPPEMENT
vlan 130
name COMMERCIAL
```

```
interface GigabitEthernet 0/0.110
encapsulation dot1Q 110
ip address 192.168.110.1 255.255.255.0
no shutdown
exit
interface GigabitEthernet 0/0.120
encapsulation dot1Q 120
ip address 192.168.120.1 255.255.255.0
no shutdown
exit
interface GigabitEthernet 0/0.130
encapsulation dot1Q 130
ip address 192.168.130.1 255.255.255.0
no shutdown
exit
```

PLAN SSH

PLAN SSH :

Nom Switch :

- Switch-LigueBasket
- Switch-LigueVolley
- Switch-LigueFootball
- Switch-LigueCurling
- Switch-LigueLoL
- Switch-LigueWifiPublic
- Switch-LigueFilairePublic
- Switch-LigueAdmin
- Switch-LigueEcransAffichage
- Switch-LigueDMZ
- Switch-LigueServeurSwitch
- Switch-LigueServiceInformatique

Switch ServicesInfo :

hostname SW_Service_Info / 172.16.70.2
username AdminServiceInfo privilege 15 secret 2JN5J26N289FNEF
enable secret Enable52JNJN24

SSH ROUTEUR :

username adminR privilege 15 secret 123456789

Switch ServeurSwitch :

hostname SW_Gestion
username AdminGestion privilege 15 secret KNFN32J5B2P225
enable secret EnableK2K5N2K15

NOTICE SSH

📌 Configuration du Protocole SSH sur le Switch et le Routeur

L'ajout du **protocole SSH** permet une **connexion sécurisée** à ton switch et à ton routeur, au lieu d'utiliser Telnet (qui n'est pas sécurisé).

1️⃣ Pourquoi Activer SSH ?

✅ **Sécurise l'accès au switch et au routeur** (au lieu de Telnet).
✅ **Chiffre les connexions à distance** pour éviter l'espionnage des mots de passe.
✅ **Obligatoire pour une bonne sécurité réseau**.

2️⃣ Étape 1 - Configuration de SSH sur le Switch

1️⃣ Choisir un Nom d'Hôte et un Domaine

Sur le **switch (Basket par exemple)**, entre ces commandes :

```
enable
configure terminal
hostname Switch-LigueBasket
ip domain-name m2l.local
```

📌 **Le nom d'hôte et le domaine sont obligatoires pour générer la clé SSH.**

2️⃣ Générer une Clé Cryptographique pour SSH

```
crypto key generate rsa
```

📌 **Si demandé, choisis une taille de clé d'au moins 1024 bits pour une bonne sécurité.** Exemple :

```
How many bits in the modulus [512]: 1024
```

3️⃣ Configurer un Nom d'Utilisateur et un Mot de Passe

Crée un utilisateur pour l'accès SSH :

```
username admin privilege 15 secret M2Lpass123
```

📌 **Remplace `M2Lpass123` par ton propre mot de passe sécurisé.**

4️⃣ Activer SSH sur la Ligne VTY

Applique la configuration aux sessions distantes (lignes VTY) :

```
line vty 0 4
transport input ssh
login local
exit
```

📌 **Cela empêche Telnet et force l'authentification SSH uniquement.**

5️⃣ Activer SSH en Version 2 (Sécurisé)

```
ip ssh version 2
```

📌 **SSH Version 2 est plus sécurisé que la version 1.**

3️⃣ Étape 2 - Configuration de SSH sur le Routeur

La configuration est **similaire au switch**, entre ces commandes sur le **routeur** :

```
enable
configure terminal
hostname Routeur-M2L
ip domain-name m2l.local
crypto key generate rsa
username admin privilege 15 secret M2Lpass123
line vty 0 4
transport input ssh
login local
exit
ip ssh version 2
```

4️⃣ Étape 3 - Test de la Connexion SSH

Sur un **PC connecté au VLAN 10**, ouvre le **"Command Prompt"** et tape :

```
ssh -l admin 192.168.10.1
```

📌 **Cela tente une connexion SSH au routeur (`192.168.10.1`).**

Si tu veux te connecter au **switch**, remplace `172.16.10.1` par son adresse IP.

Il te demandera le mot de passe (`M2Lpass123`).
Si la connexion fonctionne, **SSH est bien activé** !

📢 Conclusion

✅ **SSH sécurisé activé sur le switch et le routeur**.
✅ **Seuls les utilisateurs authentifiés peuvent se connecter**.
✅ **Test réussi avec la commande `ssh -l admin 172.16.10.1`**.

🔐 CONFIGURATION SSH POUR LE SWITCH EN VLAN 120 (Service_Informatique)

```
enable
configure terminal

! 🧾 Nom d'hôte et domaine requis pour SSH
hostname SW_Info
ip domain-name m2l.local

! 👤 Création d’un utilisateur avec privilèges élevés
username admin privilege 15 secret MonMotDePasseFort123

! 🔑 Génération de la clé RSA (obligatoire pour SSH)
crypto key generate rsa
2048

! ⚙️ Activer SSH version 2
ip ssh version 2

! 🛡️ Sécuriser les lignes VTY
line vty 0 4
 transport input ssh
 login local
 exec-timeout 5 0
exit

! 🔐 Mot de passe enable (si accès en console par ex)
enable secret EnableFort123

! 🌐 Interface VLAN 120 (SVI) avec IP de gestion
interface vlan 120
 ip address 172.16.70.2 255.255.255.240
 no shutdown

! 🚪 Passerelle par défaut pour la gestion distante
ip default-gateway 172.16.70.1

end
write memory
```

🧪 TEST DEPUIS UN AUTRE PC DANS VLAN 120 OU VLAN 110

```
ssh -l admin 172.16.70.2
```

🔐 OPTIONNEL : Limiter l'accès SSH à un ou plusieurs VLANs précis (ACL)

Tu peux, comme pour le switch du VLAN 110, créer une ACL pour **limiter les connexions SSH entrantes** (par ex : n'autoriser que certains admins depuis VLAN 110) :

```
ip access-list standard SSH_FROM_GESTION
 permit 172.16.60.0 0.0.0.15      ! VLAN 110
 permit 172.16.70.0 0.0.0.15      ! VLAN 120
 deny any

line vty 0 4
 access-class SSH_FROM_GESTION in
```

🧭 Étapes pour tester SSH avec l’interface "SSH Client" (autre solution)

📌 1. Clique sur ton PC (dans VLAN 120 par exemple)

> Ce PC doit avoir une IP correcte dans son VLAN (ex : `172.16.70.3` pour VLAN 120)

📁 2. Onglet "Desktop" → Choisis "SSH"

(illustration si tu veux visualiser l’emplacement)

🧑‍💻 3. Renseigne les champs comme suit :

Champ	Valeur
Host	`172.16.70.2` (IP du switch cible)
Port	`22` (par défaut pour SSH)
Username	`admin` (ou le nom de ton utilisateur)
Password	Ton mot de passe SSH (`MonMotDePasseFort123`)
Transport	SSH

✅ 4. Clique sur "Connect"

- Si tout est bien configuré (clé RSA, VTY, IP, VLAN, ACL), une session SSH va s’ouvrir juste en dessous avec un prompt :

```
Welcome to SW_Info
SW_Info>
```

🎯 CONFIGURATION COMPLÈTE SSH SUR LE ROUTEUR (avec filtrage VLAN 120 uniquement)

```
enable
configure terminal

! 🔧 Nom et domaine requis pour SSH
hostname R_Core
ip domain-name m2l.local

! 👤 Création de l'utilisateur local
username admin privilege 15 secret MotDePasseFort123

! 🔑 Génération des clés RSA pour SSH
crypto key generate rsa
2048

! ⚙️ Activer SSH version 2 uniquement
ip ssh version 2

! 🔐 Sécuriser les lignes VTY : SSH uniquement, login local
line vty 0 4
 transport input ssh
 login local
 exec-timeout 5 0
 exit

! 🔒 ACL pour n'autoriser SSH que depuis VLAN 120 (172.16.70.0/28)
ip access-list standard SSH_ONLY_FROM_VLAN120
 permit 172.16.70.0 0.0.0.15
 deny any

line vty 0 4
 access-class SSH_ONLY_FROM_VLAN120 in
exit
```

🌐 CONFIGURATION DE L'INTERFACE POUR VLAN 120 (si ce n'est pas déjà fait)

```
interface g0/0.120
 encapsulation dot1Q 120
 ip address 172.16.70.1 255.255.255.240
 no shutdown
```

✅ TEST SSH DEPUIS UN PC DU VLAN 120

- IP du PC : `172.16.70.3`
- Passerelle : `172.16.70.1`

Depuis le PC (onglet Desktop > Terminal ou SSH client) :

```
ssh -l admin 172.16.70.1
```

🔐 Résultat attendu

Test	Résultat
SSH depuis VLAN 120 (autorisé)	✅ Connexion OK
SSH depuis VLAN 10 à 110 (ligues)	❌ Refusé
SSH depuis VLAN 40, 100, etc.	❌ Refusé

NOTICE CONFIG ROUTEUR

📌 Configuration Complète du Routeur avec Tous les VLANs

Nous allons configurer **le routeur** pour gérer **tous les VLANs**, y compris le **VLAN 90** que tu avais mentionné.
Le **routeur assurera le routage inter-VLAN** en utilisant la technique **Router-on-a-Stick**.

1️⃣ Création des Sous-Interfaces VLAN sur le Routeur

Nous devons créer **une sous-interface pour chaque VLAN** avec la bonne adresse IP et le bon masque.

🔹 Accéder au Routeur

Sur le **routeur**, entre en mode configuration :

```
enable
configure terminal
interface GigabitEthernet 0/0
no shutdown
```

🔹 Création des Sous-Interfaces pour Chaque VLAN

Ajoute les **sous-interfaces VLAN** et attribue une adresse IP et un masque correct.

1️⃣ Réseaux avec 126 utilisateurs/postes

```
interface GigabitEthernet 0/0.60
encapsulation dot1Q 60
ip address 172.16.20.1 255.255.255.128
no shutdown

interface GigabitEthernet 0/0.70
encapsulation dot1Q 70
ip address 172.16.21.1 255.255.255.128
no shutdown

interface GigabitEthernet 0/0.80
encapsulation dot1Q 80
ip address 172.16.30.1 255.255.255.128
no shutdown
```

2️⃣ Réseaux avec 62 postes

```
interface GigabitEthernet 0/0.10
encapsulation dot1Q 10
ip address 172.16.10.1 255.255.255.192
no shutdown

interface GigabitEthernet 0/0.20
encapsulation dot1Q 20
ip address 172.16.10.65 255.255.255.192
no shutdown

interface GigabitEthernet 0/0.30
encapsulation dot1Q 30
ip address 172.16.10.129 255.255.255.192
no shutdown

interface GigabitEthernet 0/0.40
encapsulation dot1Q 40
ip address 172.16.10.193 255.255.255.192
no shutdown

interface GigabitEthernet 0/0.50
encapsulation dot1Q 50
ip address 172.16.11.1 255.255.255.192
no shutdown
```

3️⃣ Réseau avec 30 serveurs (DMZ)

```
interface GigabitEthernet 0/0.100
encapsulation dot1Q 100
ip address 172.16.50.1 255.255.255.224
no shutdown
```

4️⃣ Réseaux avec 14 équipements/postes

```
interface GigabitEthernet 0/0.90
encapsulation dot1Q 90
```

```
ip address 172.16.40.1 255.255.255.240
no shutdown

interface GigabitEthernet 0/0.110
encapsulation dot1Q 110
ip address 172.16.60.1 255.255.255.240
no shutdown

interface GigabitEthernet 0/0.120
encapsulation dot1Q 120
ip address 172.16.70.1 255.255.255.240
no shutdown
```

📌 **Tous les VLANs ont maintenant une interface configurée sur le routeur.**

2️⃣ Activation du Routage Inter-VLAN

Pour permettre aux **différents VLANs de communiquer entre eux**, active le **routage inter-VLAN** :

```
ip routing
```

📌 **Cette commande permet aux VLANs de s'envoyer des paquets via le routeur.**

3️⃣ Ajout du Relai DHCP (Si Un Serveur DHCP Externe Existe)

Si le serveur DHCP se trouve **dans un VLAN spécifique** (ex: VLAN 110 - Réseau Serveurs & Switches), on doit **ajouter un relais DHCP**.

Ajoute cette commande sur **chaque VLAN** qui doit recevoir une IP en DHCP :

```
ip helper-address 172.16.60.2
```

📌 **Remplace `172.16.60.2` par l'adresse IP de ton serveur DHCP.**

Exemple pour **VLAN 10 - Ligue Basket** :

```
interface GigabitEthernet 0/0.10
encapsulation dot1Q 10
ip address 172.16.10.1 255.255.255.192
ip helper-address 172.16.60.2
no shutdown
```

📌 **Ajoute cette ligne dans chaque VLAN où le DHCP doit être activé.**

4️⃣ Vérifications et Tests

1️⃣ Vérifier que les Interfaces VLAN sont Actives

Sur le routeur, utilise la commande :

```
show ip interface brief
```

📌 **Toutes les sous-interfaces doivent être "up".**

2️⃣ Vérifier la Connectivité entre VLANs

Depuis un **PC d'un VLAN**, fais un **ping vers un PC d'un autre VLAN**.

Exemple : **Depuis un PC du VLAN 10 (172.16.10.20), essaye de pinger un PC du VLAN 20 (172.16.10.70)**

```
ping 172.16.10.70
```

📌 **Si le ping fonctionne, le routage inter-VLAN est actif.**

3️⃣ Vérifier l'Attribution DHCP

Si un **PC est configuré en mode DHCP**, ouvre le **Command Prompt** et tape :

```
ipconfig /all
```

📌 **Le PC doit obtenir une IP correcte du serveur DHCP avec la bonne passerelle.**

📢 Conclusion

✅ **Le routeur est configuré pour gérer tous les VLANs (y compris VLAN 90).**
✅ **Chaque VLAN a sa propre passerelle et peut communiquer via le routage inter-VLAN.**
✅ **Le serveur DHCP peut être utilisé pour attribuer automatiquement des adresses IP.**
✅ **Les tests de ping permettent de vérifier que les VLANs peuvent communiquer entre eux.**

NOTICE DHCP PT

📌 Configuration Complète du Relai DHCP pour Tous les VLANs

Le **serveur DHCP est externe** (dans un VLAN spécifique), il faut activer le **relai DHCP (DHCP Helper Address)** pour que les PC des autres VLANs puissent obtenir leurs adresses IP.

1️⃣ Pourquoi le Relai DHCP est Nécessaire ?

📌 **Le DHCP fonctionne avec des requêtes en broadcast.**

- Par défaut, un **routeur bloque les requêtes broadcast** entre VLANs.
- Le **serveur DHCP ne voit donc pas les requêtes venant des autres VLANs**.
- Le **relai DHCP permet au routeur de transmettre ces requêtes** au serveur DHCP.

✅ **Solution : On configure `ip helper-address` sur chaque VLAN pour rediriger les requêtes vers le serveur DHCP.**

2️⃣ Définir le VLAN où se Trouve le Serveur DHCP

- Le **serveur DHCP** est dans le **VLAN 110 - Réseau Serveurs & Switches**.
- Son adresse IP est **`172.16.60.2`**.

📌 **Toutes les requêtes DHCP des autres VLANs seront envoyées vers `172.16.60.2`.**

3️⃣ Configuration du Relai DHCP pour Tous les VLANs

Tu dois ajouter **l'option `ip helper-address`** sur **chaque sous-interface VLAN** du routeur.

🔹 1️⃣ Réseaux avec 126 utilisateurs/postes

```
interface GigabitEthernet 0/0.60
encapsulation dot1Q 60
ip address 172.16.20.1 255.255.255.128
ip helper-address 172.16.60.2
no shutdown
```

```
interface GigabitEthernet 0/0.70
encapsulation dot1Q 70
ip address 172.16.21.1 255.255.255.128
ip helper-address 172.16.60.2
no shutdown

interface GigabitEthernet 0/0.80
encapsulation dot1Q 80
ip address 172.16.30.1 255.255.255.128
ip helper-address 172.16.60.2
no shutdown
```

🔹 2️⃣ Réseaux avec 62 postes

```
interface GigabitEthernet 0/0.10
encapsulation dot1Q 10
ip address 172.16.10.1 255.255.255.192
ip helper-address 172.16.60.2
no shutdown

interface GigabitEthernet 0/0.20
encapsulation dot1Q 20
ip address 172.16.10.65 255.255.255.192
ip helper-address 172.16.60.2
no shutdown

interface GigabitEthernet 0/0.30
encapsulation dot1Q 30
ip address 172.16.10.129 255.255.255.192
ip helper-address 172.16.60.2
no shutdown

interface GigabitEthernet 0/0.40
encapsulation dot1Q 40
ip address 172.16.10.193 255.255.255.192
ip helper-address 172.16.60.2
no shutdown

interface GigabitEthernet 0/0.50
encapsulation dot1Q 50
```

```
ip address 172.16.11.1 255.255.255.192
ip helper-address 172.16.60.2
no shutdown
```

🔹 3️⃣ Réseau avec 30 serveurs (DMZ)

```
interface GigabitEthernet 0/0.100
encapsulation dot1Q 100
ip address 172.16.50.1 255.255.255.224
ip helper-address 172.16.60.2
no shutdown
```

🔹 4️⃣ Réseaux avec 14 équipements/postes

```
interface GigabitEthernet 0/0.90
encapsulation dot1Q 90
ip address 172.16.40.1 255.255.255.240
ip helper-address 172.16.60.2
no shutdown

interface GigabitEthernet 0/0.110
encapsulation dot1Q 110
ip address 172.16.60.1 255.255.255.240
ip helper-address 172.16.60.2
no shutdown

interface GigabitEthernet 0/0.120
encapsulation dot1Q 120
ip address 172.16.70.1 255.255.255.240
ip helper-address 172.16.60.2
no shutdown
```

📌 **Chaque VLAN envoie maintenant ses requêtes DHCP au serveur situé en `172.16.60.2`.**

4️⃣ Vérifications et Tests

1️⃣ Vérifier que `ip helper-address` est bien appliqué

Sur le **routeur**, utilise la commande suivante :

```
show running-config | include helper-address
```

📌 **Cela doit afficher toutes les lignes `ip helper-address 172.16.60.2` sur les interfaces VLANs.**

2️⃣ Tester l'Attribution DHCP sur un PC

1️⃣ **Sur un PC client**, va dans **IP Configuration**.
2️⃣ **Sélectionne "DHCP"** au lieu de "Static".
3️⃣ **Attends quelques secondes**, puis vérifie que le PC a bien une IP correcte.

📌 **Si le PC obtient une adresse IP correspondant à son VLAN, le relai DHCP fonctionne !**

3️⃣ Vérifier le DHCP sur le Serveur

1️⃣ Ouvre le **serveur DHCP** dans **Packet Tracer**.
2️⃣ Va dans **Services > DHCP** et vérifie les **IP distribuées**.

📌 **Chaque VLAN doit recevoir des IPs de sa propre plage d'adresses.**

📢 Conclusion

✅ **Le routeur envoie maintenant toutes les requêtes DHCP au serveur externe (`172.16.60.2`).**
✅ **Chaque VLAN reçoit ses IPs dynamiquement via DHCP.**
✅ **Le test avec `ipconfig /all` permet de vérifier l'attribution automatique des IPs.**
✅ **La commande `show running-config | include helper-address` permet de confirmer la configuration.**

📌 Plans d’Adressage à Configurer dans le Serveur DHCP

Tu vas **configurer ton serveur DHCP** pour qu'il attribue **des adresses IP différentes pour chaque VLAN** en fonction de ton plan TCP/IP.

1️⃣ Récapitulatif du Plan d’Adressage à Configurer

Chaque VLAN doit avoir un **pool DHCP spécifique** avec :
✅ **Son adresse réseau**
✅ **Son masque de sous-réseau**
✅ **Sa passerelle (routeur)**
✅ **Un DNS (ex: 8.8.8.8 ou ton propre serveur DNS)**

🔹 Réseaux avec 126 utilisateurs/postes

VLAN	Nom	Adresse Réseau	Passerelle (Gateway)	Masque	Plage d’IP	Diffusion
60	Wi-Fi Public	172.16.20.0	172.16.20.1	255.255.255.128 (/25)	172.16.20.2 - 172.16.20.126	172.16.20.127
70	Filaire Public (Salles Ressources)	172.16.21.0	172.16.21.1	255.255.255.128 (/25)	172.16.21.2 - 172.16.21.126	172.16.21.127
80	Bureaux Administratifs, Reprographie, Multimédia	172.16.30.0	172.16.30.1	255.255.255.128 (/25)	172.16.30.2 - 172.16.30.126	172.16.30.127

🔹 Réseaux avec 62 postes

VLAN	Nom	Adresse Réseau	Passerelle (Gateway)	Masque	Plage d’IP	Diffusion
10	Ligue Basket	172.16.10.0	172.16.10.1	255.255.255.192 (/26)	172.16.10.2 - 172.16.10.62	172.16.10.63
20	Ligue Volley-Ball	172.16.10.64	172.16.10.65	255.255.255.192 (/26)	172.16.10.66 - 172.16.10.126	172.16.10.127
30	Ligue Football	172.16.10.128	172.16.10.129	255.255.255.192 (/26)	172.16.10.130 - 172.16.10.190	172.16.10.191
40	Ligue Curling	172.16.10.192	172.16.10.193	255.255.255.192 (/26)	172.16.10.194 - 172.16.10.254	172.16.10.255
50	Ligue LoL	172.16.11.0	172.16.11.1	255.255.255.192 (/26)	172.16.11.2 - 172.16.11.62	172.16.11.63

🔹 Réseau avec 30 serveurs (DMZ)

VLAN	Nom	Adresse Réseau	Passerelle (Gateway)	Masque	Plage d'IP	Diffusion
100	DMZ (Serveurs Accessibles)	172.16.50.0	172.16.50.1	255.255.255.224 (/27)	172.16.50.2 - 172.16.50.30	172.16.50.31

🔹 Réseaux avec 14 équipements/postes

VLAN	Nom	Adresse Réseau	Passerelle (Gateway)	Masque	Plage d'IP	Diffusion
90	Écrans d'Affichage	172.16.40.0	172.16.40.1	255.255.255.240 (/28)	172.16.40.2 - 172.16.40.14	172.16.40.15
110	Réseau Serveurs & Switches	172.16.60.0	172.16.60.1	255.255.255.240 (/28)	172.16.60.2 - 172.16.60.14	172.16.60.15
120	Réseau Service Informatique	172.16.70.0	172.16.70.1	255.255.255.240 (/28)	172.16.70.2 - 172.16.70.14	172.16.70.15

2️⃣ Configuration des Pools DHCP sur le Serveur

Si ton serveur DHCP est un **serveur Cisco (Packet Tracer)** ou **un serveur Windows/Linux**, voici comment entrer ces données.

📡 Configuration du Serveur DHCP dans Packet Tracer

1. **Ouvre le Serveur DHCP**
2. **Va dans Services > DHCP**
3. **Ajoute un Pool DHCP pour chaque VLAN**
   - Pool Name: **Ligue_Basket**
   - Default Gateway: **172.16.10.1**
   - Network Address: **172.16.10.0**
   - Subnet Mask: **255.255.255.192**
   - DNS Server: **8.8.8.8**
   - Start IP Address: **172.16.10.2**
   - Maximum Number of Users: **61**
4. **Clique sur "Add"** et répète l'opération pour chaque VLAN.

3️⃣ Vérifications et Tests

✅ **Tester DHCP sur un PC :**

1. **Mets un PC en mode DHCP** dans "IP Configuration".
2. **Vérifie qu'il obtient une adresse correcte avec `ipconfig /all`.**
3. **Teste un ping vers la passerelle (`ping 172.16.10.1`).**

✅ **Vérifier les IPs attribuées sur le serveur DHCP :**

- **Ouvre le serveur DHCP dans Packet Tracer.**
- **Regarde dans "DHCP > Clients" pour voir les adresses IP attribuées.**

📢 Conclusion

🎯 Le serveur DHCP est maintenant prêt à attribuer automatiquement des adresses IP pour tous les VLANs !
🚀 Chaque VLAN a son propre pool DHCP et les PC reçoivent bien leurs adresses IP dynamiques.

DHCP Windows

Documentation Windows Serveur

Machine Virtuelle Windows Serveur:
NOM: **AP_WS**
IPV4: **172.16.10.2**

Critères:

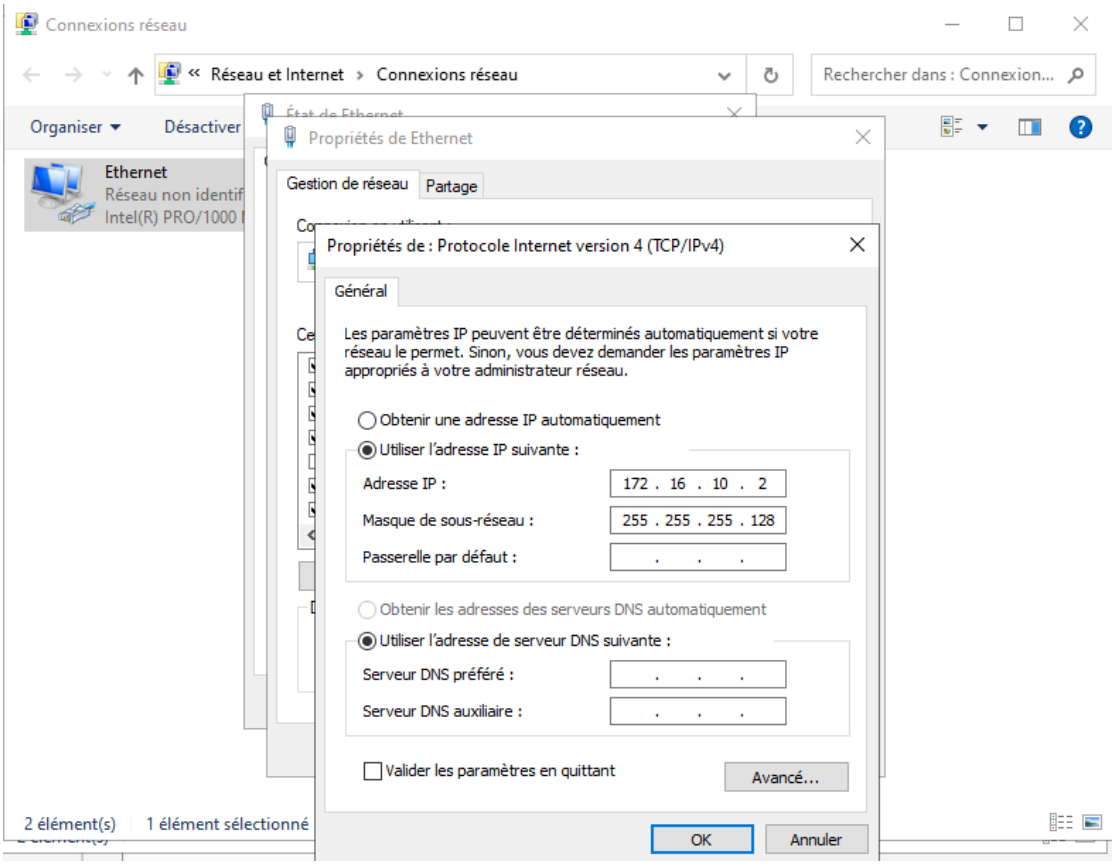
- Adressage IPv4 fixe
- Etendue DHCP par vlan géré
- DHCP fonctionnel
- Réservation IP via Adresse MAC
- Agent Relais DHCP
- Logiciel de scan réseau pour récup MAC

Adressage IPv4 fixe:

Aller dans les Paramètres → État du réseau → Modifier les options d'adaptateur

Cliquer sur la carte Ethernet → Propriétés → Protocole Internet version 4

Donner une IP fixe:



Étendue DHCP par vlan géré:

Ajouter le rôle DHCP:

Se rendre dans le Gestionnaire de serveur → Ajouter des rôles et des fonctionnalités

→ Suivant → Sélectionner Installation basée sur un rôle ou une fonctionnalité →

Choisir le serveur et cliquer sur Suivant → Cochez Serveur DHCP → Cliquez sur

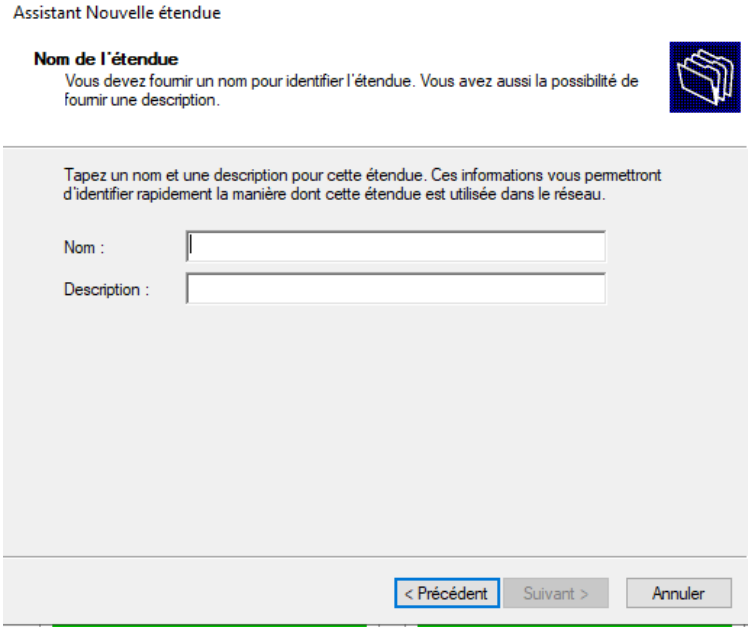
Suivant jusqu'à pouvoir l'installer→

Créer les étendues:

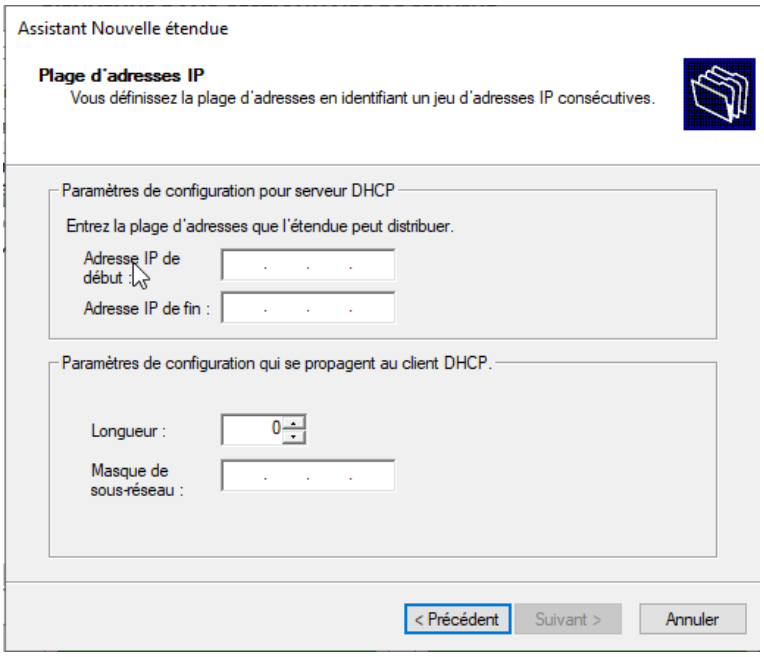
Se rendre dans le Gestionnaire de serveur → Outils (En haut à droite) → DHCP

→ Dérouler le serveur → Clique droit sur IPv4 → Nouvelle étendue… → Suivant

→ Donner un Nom à votre étendu puis Suivant

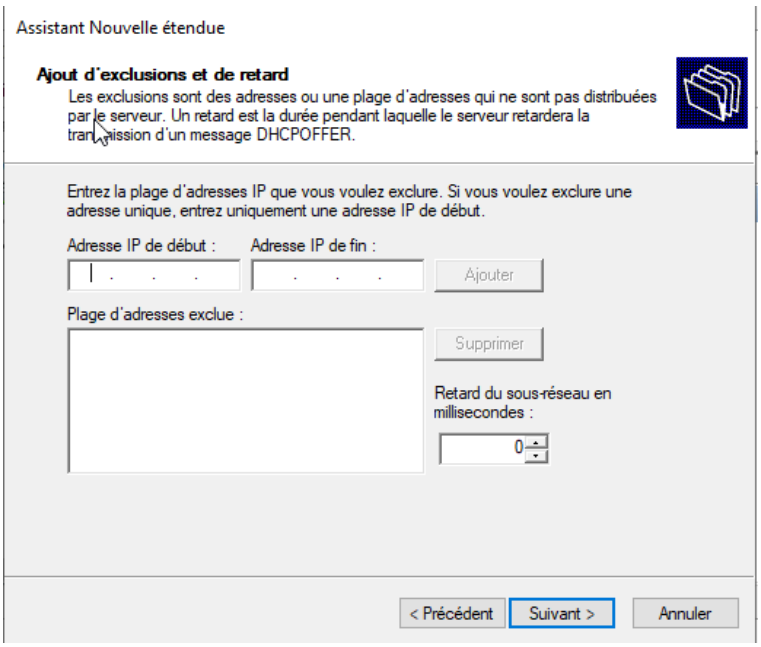


→ **Remplir votre plage d'adresses avec le masque puis Suivant**



→ **Définir le bail puis Suivant**

→ **Sélectionner Oui, je veux configurer ces options maintenant**



→ **Ajouter l'adresse routeur puis cliquer sur Suivant jusqu'à pouvoir activer l'étendu**

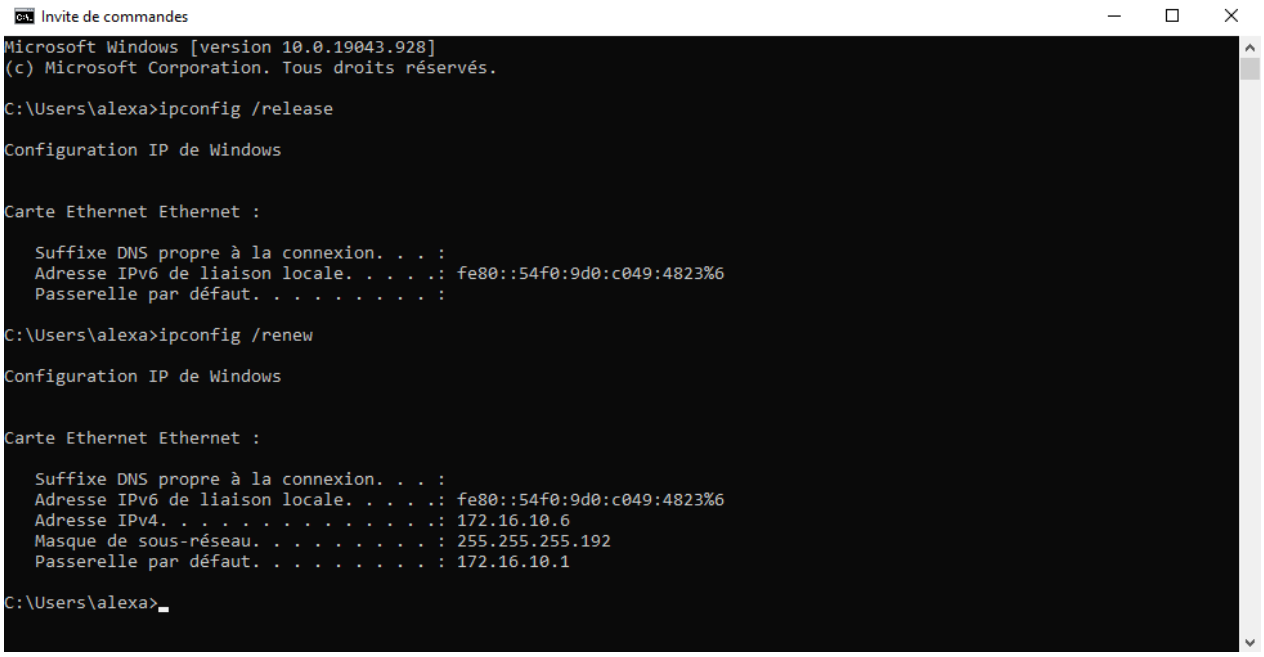
→ **Terminer**

Test DHCP:

Pour tester que le DHCP fonctionne correctement, il faut utiliser un PC client sur machine virtuelle sous Windows 10.

Passer les deux machines virtuelles dans le même réseau interne. (Sur VirtualBox: Configuration → Réseau)

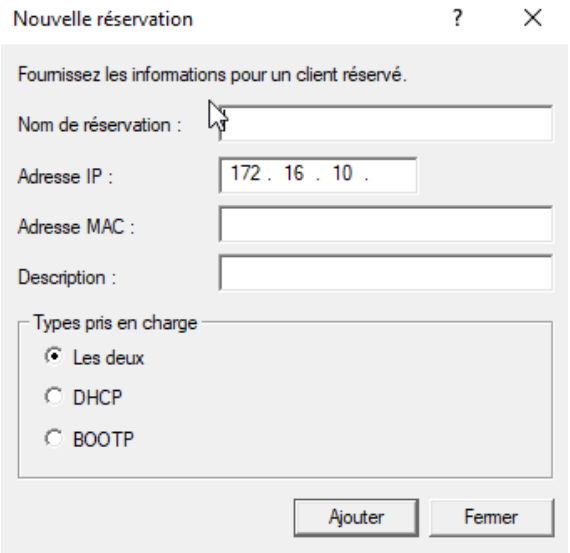
Allez dans l'invite de commande sur votre PC client tapez la commande ipconfig /release puis ipconfig /renew



DHCP Fonctionnel !

Réservation IP via Adresse MAC:

Se rendre dans le Gestionnaire de serveur
→ Outils (En haut à droite)
→ DHCP
→ Dérouler le serveur et IPv4
→ Dérouler une de vos étendues
→ Clique droit sur Réservation
→ Nouvelles réservation…
→ Donner une IP à l'adresse MAC de votre choix et Ajouter



Agent Relais DHCP:

Se rendre dans le Gestionnaire de serveur → Ajouter des rôles et des fonctionnalités

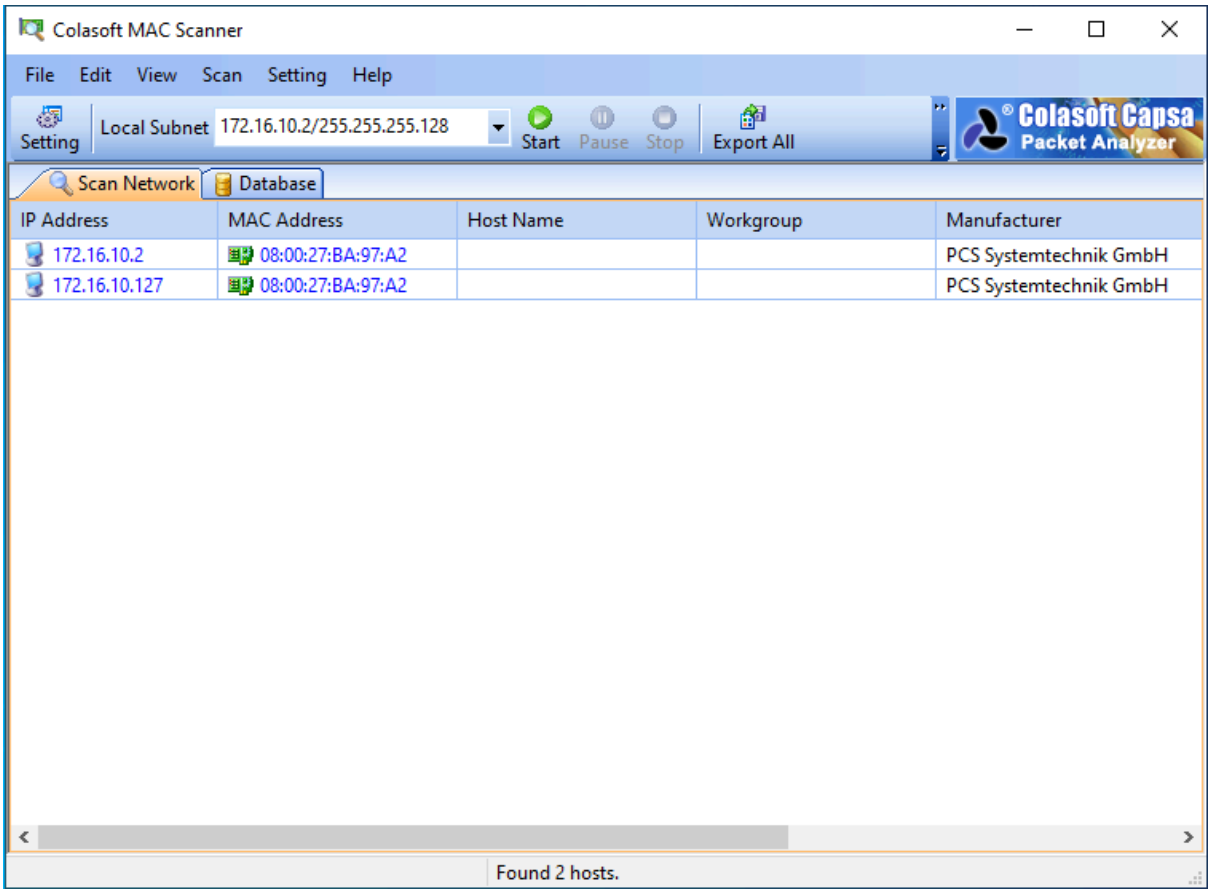
→ Suivant → Sélectionner Installation basée sur un rôle ou une fonctionnalité →

Choisir le serveur et cliquer sur Suivant → Cocher Accès à distance → Suivre les instructions jusqu'à l'installation

Logiciel de scan réseau pour récup MAC:

Se rendre sur le site : MAC Scanner, Free MAC Address Scanner - Colasoft et télécharger le logiciel.

Lancer le logiciel et lancer un scan sur votre réseau.



Les adresses MAC sont récupérées !