

RESTRUSTURATION DE RESEAU

PAR VLAN





SOMMAIRE

- 1 – Prérequis.....
- 2 – Création des VLAN.....
- 3 – Configuration des VLAN.....
- 4 – Configuration du routage et des ports.....
- 5 – Configuration des Services.....
- 6 – Test des accès et services.....
- 7 – Conclusion.....

1 – Prérequis :

- Posséder un switch de niveau 3 (Toutes les commandes s'appliquent à ce switch)
- Posséder une VM sous Debian
- Installer le terminal PUTTY pour configurer le switch niveau 3

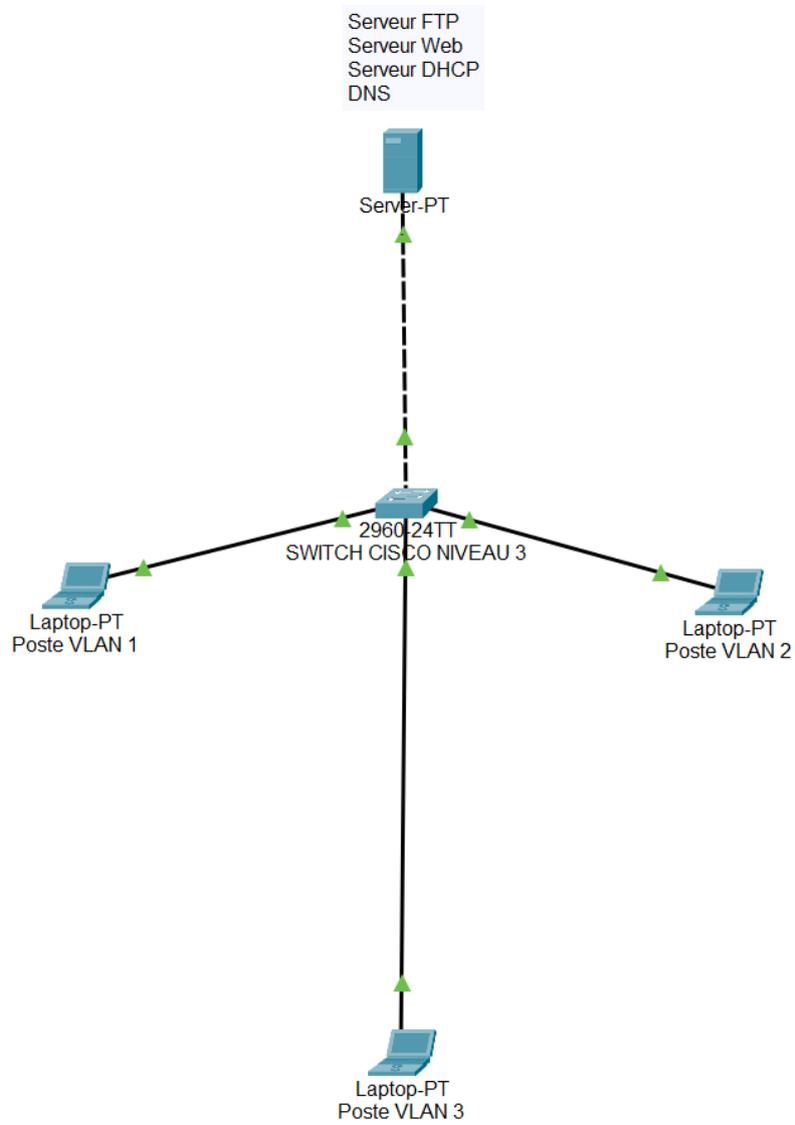
Nous devons configurer un Serveur FTP / WEB et un serveur DHCP.

- Le serveur DHCP devra distribuer des IP correspondantes à l'IP de chaque VLAN. - Nous devons avoir 3 VLAN.
- -Le serveur Web doit être accessible depuis tous les VLAN.
- Et le port 21 ne doit pas pouvoir accéder au FTP.
- Il faut aussi tester le routage inter VLAN.

Le switch utilisé est un cisco business 350 series de niveau 3 les commandes sont donc spécifiques à ce switch.

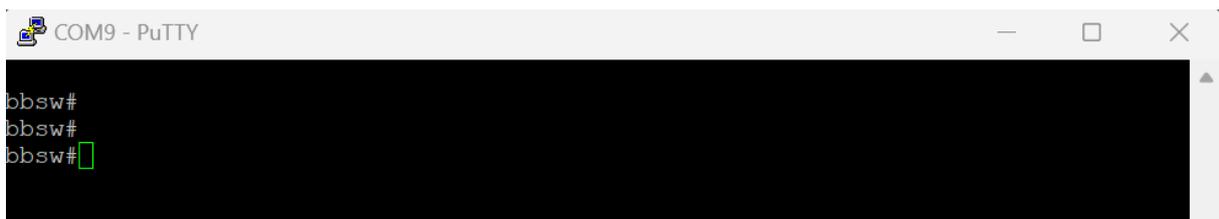
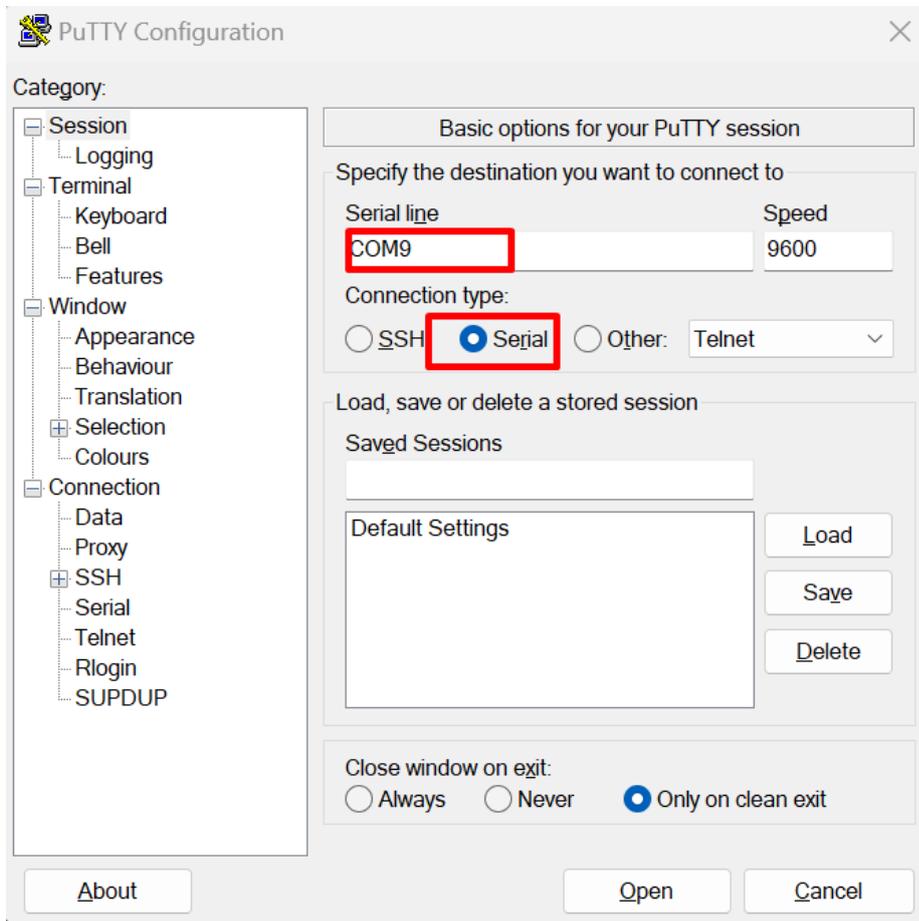


Architecture réseau de notre travail :



2 – Création des VLAN

Se connecter à Putty :



3 - Configuration des Vlan :

Ajout d'une IP sur le VLAN 1 :

- Interface VLAN1
- Ip address
- 192.168.1.1 255.255.255.0

La commande pour nommer les VLAN :

- Interface VLAN X
- Hostname X



Commande pour ajouter les ports dans les VLANs :

- Interface VLAN X
- Switchport mode access
- Switchport access VLAN X

Vlan 1

192.168.1.1 255.255.255.0

Interfaces : 1, 9, 10

Vlan 10 interfaces 2/3

Formation

192.168.10.254 255.255.255.0

Interfaces 2, 3

Vlan 20 interfaces 4/5

Personnel

192.168.20.254 255.255.255.0

Interfaces : 4, 5

Vlan 30 interfaces 6/7

Serveur

168.168.30.254. 255.255.255.0

Interfaces : 6, 7

Domaine :

Esicad.lan

4 - CONFIGURATION DU ROUTAGE ET DES PORTS

Configuration d'un accès SSH :

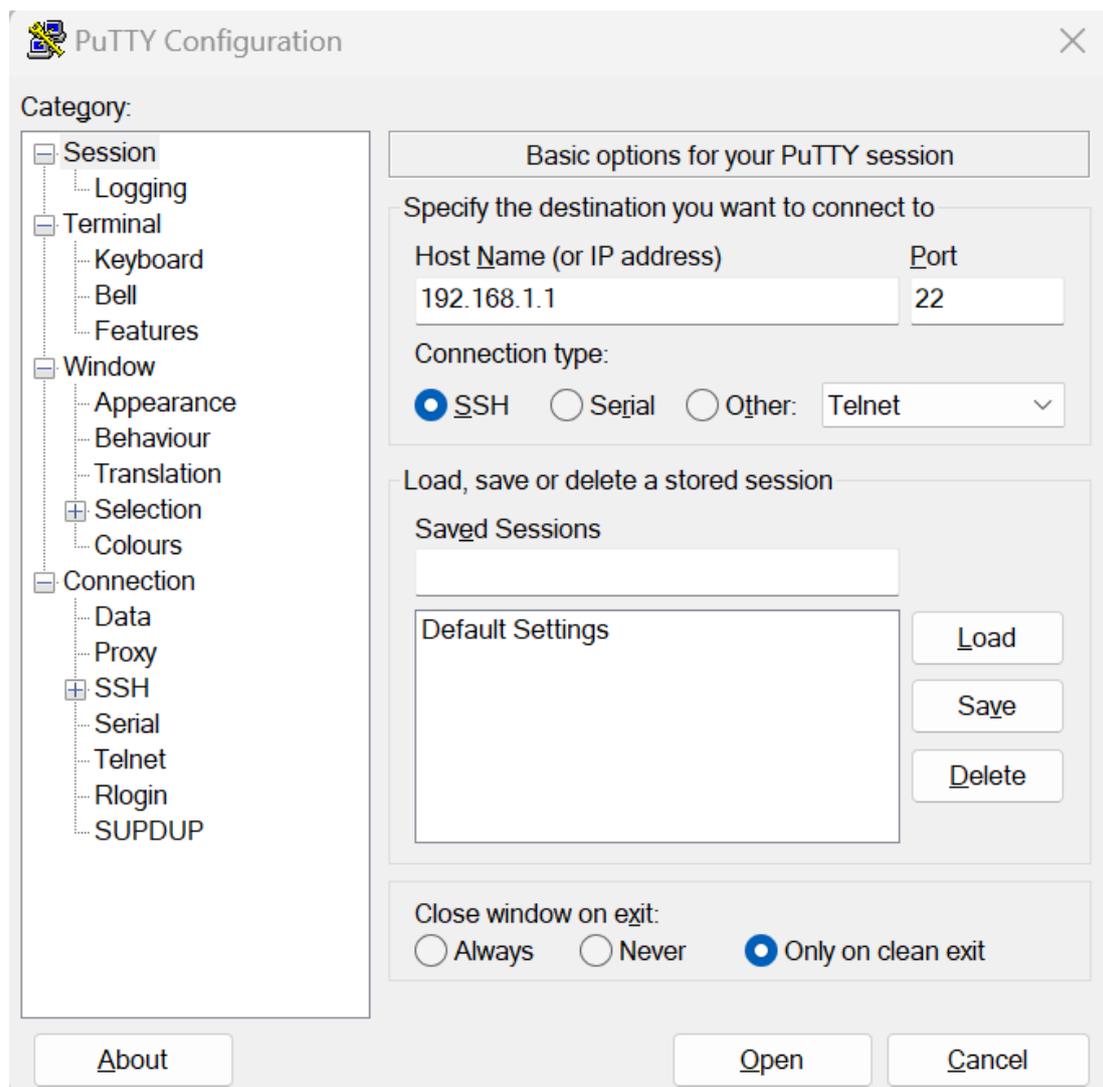
Via la commande

- Interface VLAN 1
- Ip ssh
- Ip ssh password – auth

Activation du routage :

- Ip routing

Test de l'accès SSH :





Ensuite cliquer sur Open :

```
?
Detected speed: 9600

User Name:
User Name:
authentication failed

press ENTER key to retry authentication

User Name:█
```

L'accès SSH fonctionne donc correctement.

Il faut maintenant vérifier que le routage inter VLAN fonctionne en faisant des tests de ping depuis des VLAN différents :

Ping d'un poste du VLAN 10 au VLAN 20 :

```
C:\Users\carcr>ping 192.168.20.10

Envoi d'une requête 'Ping' 192.168.20.10 avec 32 octets de données :
Réponse de 192.168.20.10 : octets=32 temps=99 ms TTL=127
Réponse de 192.168.20.10 : octets=32 temps=4 ms TTL=127
Réponse de 192.168.20.10 : octets=32 temps=5 ms TTL=127

Statistiques Ping pour 192.168.20.10:
    Paquets : envoyés = 3, reçus = 3, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 4ms, Maximum = 99ms, Moyenne = 36ms
```

Ping d'un poste du VLAN 20 au VLAN 10 :

```
C:\Users\carcr>ping 192.168.10.10

Envoi d'une requête 'Ping' 192.168.10.10 avec 32 octets de données :
Réponse de 192.168.10.10 : octets=32 temps=4 ms TTL=127
Réponse de 192.168.10.10 : octets=32 temps=4 ms TTL=127
Réponse de 192.168.10.10 : octets=32 temps=4 ms TTL=127
Réponse de 192.168.10.10 : octets=32 temps=5 ms TTL=127

Statistiques Ping pour 192.168.10.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 4ms, Maximum = 5ms, Moyenne = 4ms
```

On observe que les VLAN communiquent correctement entre eux ce qui prouve que notre routage est effectif et correctement configuré.

5 - CONFIGURATION DES DIFFERENTS SERVICES SOUS LINUX :

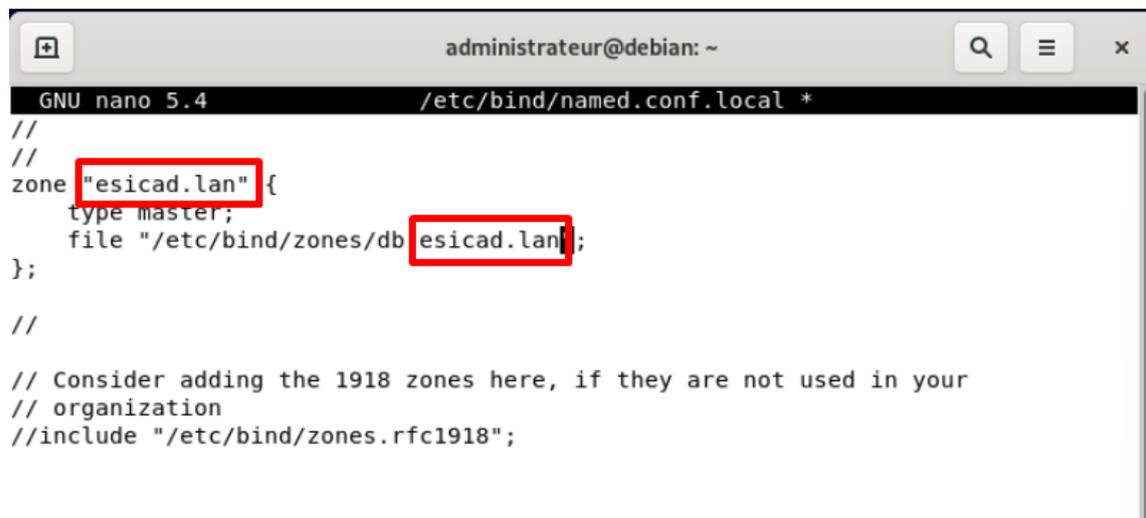
Configuration du DNS :

Ces commandes nous permettrons d'installer les différents services de bind9 qui nous permettrons de faire fonctionner notre DNS.

```
root@debian:/home/administrateur# sudo apt-get update
Atteint :1 http://security.debian.org/debian-security bullseye-security InRelease
Atteint :2 http://deb.debian.org/debian bullseye InRelease
Atteint :3 http://deb.debian.org/debian bullseye-updates InRelease
Lecture des listes de paquets... Fait
root@debian:/home/administrateur# sudo apt-get install bind9
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
bind9 est déjà la version la plus récente (1:9.16.44-1~deb11u1).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 10 non mis à jour.
root@debian:/home/administrateur#
```

Configuration des fichiers de zone :

Nano /etc/bind/named.conf.local



```
administrateur@debian: ~
GNU nano 5.4 /etc/bind/named.conf.local *
//
//
zone "esicad.lan" {
    type master;
    file "/etc/bind/zones/db.esicad.lan";
};
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
```

Configuration des enregistrements DNS :

Création du répertoire db.esicad.lan

```
root@debian:/home/administrateur# nano /etc/bind/zones/db.esicad.lan
root@debian:/home/administrateur# mkdir -p /etc/bind/zones
root@debian:/home/administrateur# touch /etc/bind/zones/db.esicad.lan
root@debian:/home/administrateur# sudo systemctl restart bind9
```

Nano /etc/bind/zones/db.esicad.lan

```

GNU nano 5.4 /etc/bind/zones/db.esicad.lan
$TTL 604800
@      IN      SOA      ns1.example.com. admin.example.com. (
                          2023103101 ; Serial
                          604800    ; Refresh
                          86400     ; Retry
                          2419200   ; Expire
                          604800 ) ; Negative Cache TTL
;
@      IN      NS       ns1.example.com.
@      IN      A        192.168.30.254
www    IN      CNAME    192.168.94.151

```

Passerelle et serveur

[Lecture de 11 lignes]

^G Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter ^C Emplacement
 ^X Quitter ^R Lire fich. ^\ Remplacer ^U Coller ^J Justifier ^_ Aller ligne

Notre DNS a donc été changé en db.esicad.lan ce qui permet aux utilisateurs d'accéder aux différents service en tapant ce nom plutôt que l'IP.

Configuration du serveur WEB :

Nous aurons besoin d'installer Apache.

```

root@debian:/home/administrateur# sudo apt update
Atteint :1 http://security.debian.org/debian-security bullseye-security InRelease
Atteint :2 http://deb.debian.org/debian bullseye InRelease
Atteint :3 http://deb.debian.org/debian bullseye-updates InRelease
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
10 paquets peuvent être mis à jour. Exécutez « apt list --upgradable » pour les voir.
root@debian:/home/administrateur#

```

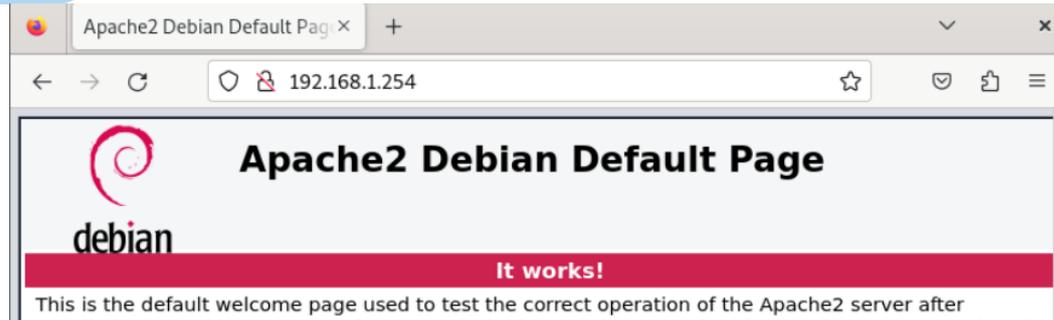
Installation d'apache :

```

root@debian:/home/administrateur# apt install apache2
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
apache2 est déjà la version la plus récente (2.4.56-1~deb11u2).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 10 non mis à jour.
root@debian:/home/administrateur#

```

Test d'accès à Apache 2



Configuration d'apache :

Ici on modifie le fichier `/var/www/html/index.html` afin d'avoir un site fonctionnel plutôt que l'interface de configuration d'apache.

```
GNU nano 5.4 /var/www/html/index.html
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/1999/xhtml"
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Debian Default Page: It works</title>
    <style type="text/css" media="screen">
  * {
    margin: 0px 0px 0px 0px;
    padding: 0px 0px 0px 0px;
  }

  body, html {
    padding: 3px 3px 3px 3px;

    background-color: #D8DBE2;

    font-family: Verdana, sans-serif;
    font-size: 11pt;
    text-align: center;
  }
  </style>
  </head>
  <body>
  </body>
</html>
```

Test d'accès au site après modification on peut voir que notre modification a bien été prise en compte par apache.



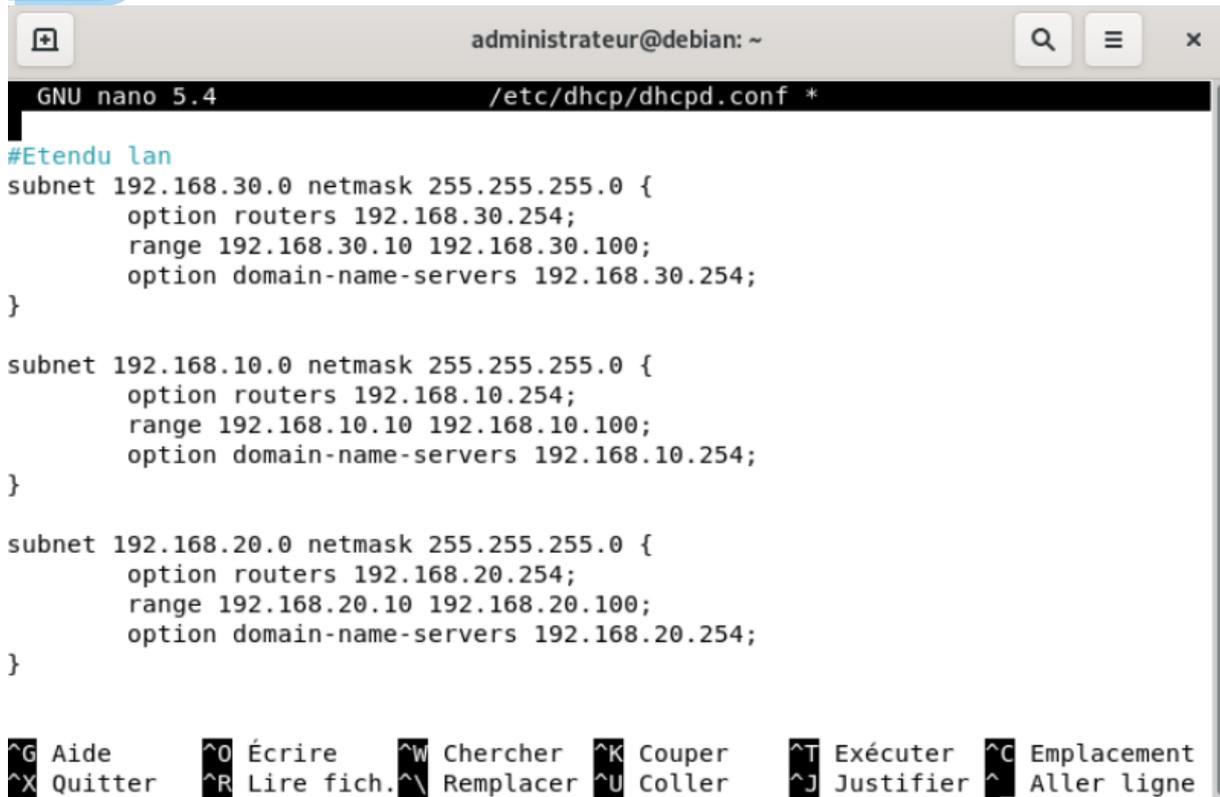
Configuration du serveur DHCP :

```
administrateur@debian: ~  
administrateur@debian:~$ su root  
Mot de passe :  
root@debian:/home/administrateur# sudo apt update  
Atteint :1 http://security.debian.org/debian-security bullseye-security InRelease  
Atteint :2 http://deb.debian.org/debian bullseye InRelease  
Réception de :3 http://deb.debian.org/debian bullseye-updates InRelease [44,1 kB  
]  
44,1 ko réceptionnés en 1s (81,0 ko/s)  
Lecture des listes de paquets... Fait  
Construction de l'arbre des dépendances... Fait  
Lecture des informations d'état... Fait  
10 paquets peuvent être mis à jour. Exécutez « apt list --upgradable » pour les  
voir.  
root@debian:/home/administrateur# sudo apt install isc-dhcp-server  
Lecture des listes de paquets... Fait  
Construction de l'arbre des dépendances... Fait  
Lecture des informations d'état... Fait  
isc-dhcp-server est déjà la version la plus récente (4.4.1-2.3+deb11u2).  
0 mis à jour, 0 nouvellement installés, 0 à enlever et 10 non mis à jour.  
root@debian:/home/administrateur#
```

Configuration du serveur DHCP et ajout de la range IP à distribuer.

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

On cherche à faire en sorte que le DHCP distribue des IP correspondantes à chaque VLAN, donc on modifie la plage IP distribués par le DHCP pour chaque VLAN, voici la configuration.



```
administrateur@debian: ~
GNU nano 5.4 /etc/dhcp/dhcpd.conf *
#Etendu lan
subnet 192.168.30.0 netmask 255.255.255.0 {
    option routers 192.168.30.254;
    range 192.168.30.10 192.168.30.100;
    option domain-name-servers 192.168.30.254;
}

subnet 192.168.10.0 netmask 255.255.255.0 {
    option routers 192.168.10.254;
    range 192.168.10.10 192.168.10.100;
    option domain-name-servers 192.168.10.254;
}

subnet 192.168.20.0 netmask 255.255.255.0 {
    option routers 192.168.20.254;
    range 192.168.20.10 192.168.20.100;
    option domain-name-servers 192.168.20.254;
}

^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich.^_ Remplacer  ^U Coller    ^J Justifier ^_ Aller ligne
```

Configuration de l'interface réseau :

- nano /etc/default/isc-dhcp-server
- interface v4 « ens33 »

Redémarrage des services :

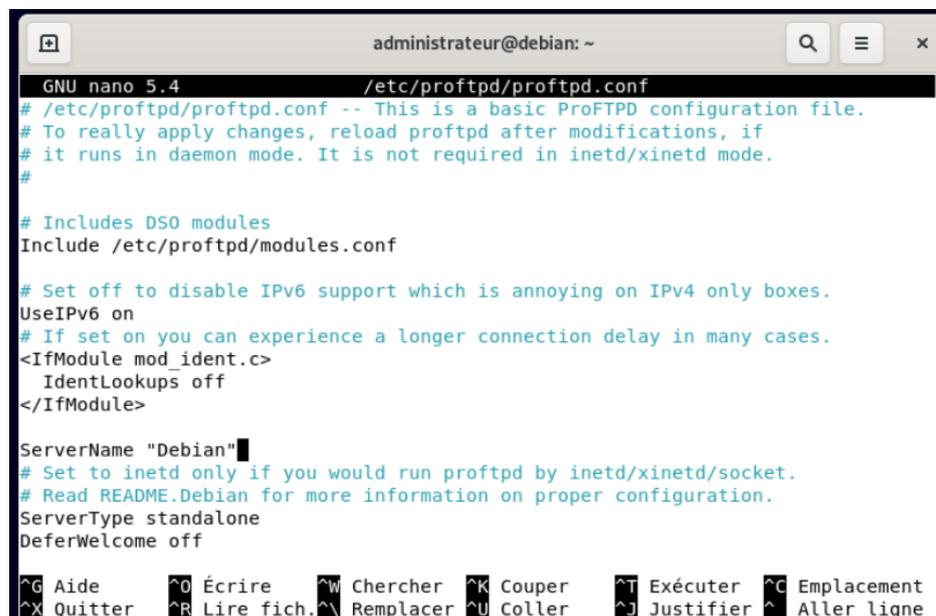
- systemctl restart isc-dhcp-serv

Installation du Serveur FTP:

```
~
Atteint :3 http://deb.debian.org/debian bullseye-updates InRelease
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
10 paquets peuvent être mis à jour. Exécutez « apt list --upgradable » pour les
voir.
root@debian:/home/administrateur# apt install proftpd
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Note : sélection de « proftpd-core » au lieu de « proftpd »
Les paquets supplémentaires suivants seront installés :
  libhiredis0.14 libmemcached11 libmemcachedutil2 proftpd-doc
Paquets suggérés :
  openbsd-inetd | inet-superserver proftpd-mod-ldap proftpd-mod-mysql
  proftpd-mod-odbc proftpd-mod-pgsql proftpd-mod-sqlite proftpd-mod-geoip
  proftpd-mod-snmp proftpd-mod-crypto proftpd-mod-wrap
Les NOUVEAUX paquets suivants seront installés :
  libhiredis0.14 libmemcached11 libmemcachedutil2 proftpd-core proftpd-doc
0 mis à jour, 5 nouvellement installés, 0 à enlever et 10 non mis à jour.
Il est nécessaire de prendre 4 425 ko dans les archives.
Après cette opération, 9 214 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [0/n]
```

Configuration de Pro FTPD :

- sudo nano /etc/proftpd/proftpd.conf



```
administrateur@debian: ~
GNU nano 5.4 /etc/proftpd/proftpd.conf
# /etc/proftpd/proftpd.conf -- This is a basic ProFTPD configuration file.
# To really apply changes, reload proftpd after modifications, if
# it runs in daemon mode. It is not required in inetd/xinetd mode.
#
# Includes DSO modules
Include /etc/proftpd/modules.conf
# Set off to disable IPv6 support which is annoying on IPv4 only boxes.
UseIPv6 on
# If set on you can experience a longer connection delay in many cases.
<IfModule mod_ident.c>
  IdentLookups off
</IfModule>
ServerName "Debian"
# Set to inetd only if you would run proftpd by inetd/xinetd/socket.
# Read README.Debian for more information on proper configuration.
ServerType standalone
DeferWelcome off
^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich. ^\ Remplacer  ^U Coller   ^J Justifier ^_ Aller ligne
```

Configuration des ACL afin de bloquer le port 21 :

- sudo iptables -L
- sudo iptables -A INPUT -p tcp --dport 21 -j DROP

(DROP) est en fait le rejet des paquets entrants et sortants sur ce port



Afin de sauvegarder cette règle on utilise la commande :

- `sudo iptables-save > /etc/iptables/rules.v4`

Pour activer le routage il faut utiliser la commande :

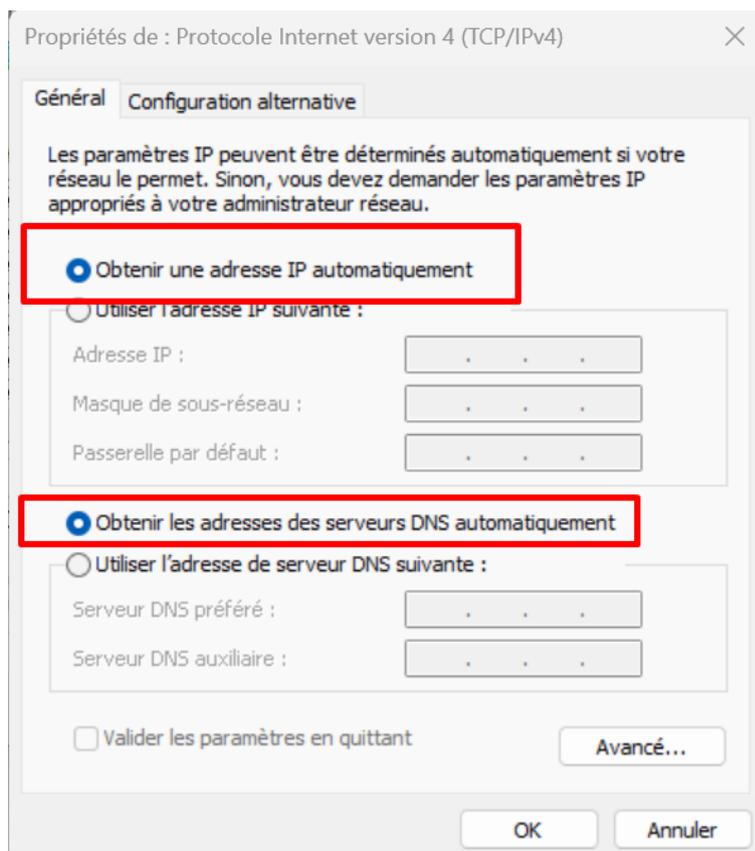
- `ip helper`

Test d'attribution d'ip via le serveur DHCP :

- Afin de pouvoir vérifier que nos VLAN distribuent correctement les adresses IP donné par le serveur DHCP nous allons effectuer différents Test :

Attribution d'ip du VLAN 10 sur le poste test :

Il faut d'abord passer notre carte réseau Ethernet en DHCP :



Ensuite ouvrir une invite de commande via Window + R / CMD

- Taper IPCONFIG et vérifier que l'adresse IP est correcte :

Carte Ethernet Ethernet 3 :

```
Suffixe DNS propre à la connexion. . . . :
Adresse IPv6 de liaison locale. . . . . : fe80::2267:e259:4165:77d4%13
Adresse IPv4. . . . . : 192.168.10.10
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . :
```

Test sur le VLAN 20 :

Carte Ethernet Ethernet 3 :

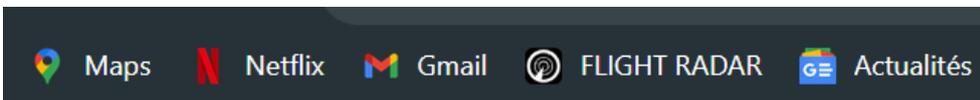
```
Suffixe DNS propre à la connexion. . . . :
Adresse IPv6 de liaison locale. . . . . : fe80::2267:e259:4165:77d4%13
Adresse IPv4. . . . . : 192.168.20.8
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . :
```

Les adresses distribuées par le DHCP sont correctes on peut voir que les adresses distribuées par le DHCP correspondent bien à chaque VLAN.

Test d'accès au serveur web :

Pour rappel tous les VLAN doivent accéder au service WEB depuis leur poste :

<https://db.esicad.lan>



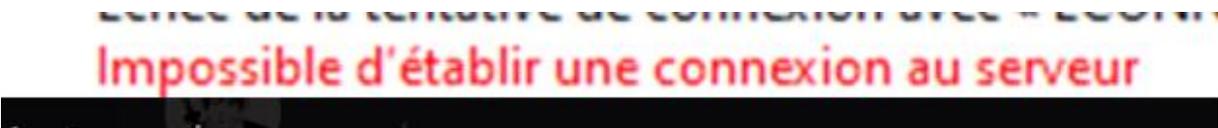
Bienvenue sur Esicad

On observe que j'accède bien au serveur web depuis mon poste étant donné que je n'ai pas configuré de règle l'empêchant d'y accéder depuis un VLAN différent, tous les VLAN y ont accès.

Test de l'accès au serveur FTP :

```
tatut : Connexion établie, attente du message d'accueil...
tatut : Serveur non sécurisé, celui-ci ne prend pas en charge FTP sur TLS.
tatut : Connecté
tatut : Récupération du contenu du dossier...
tatut : Contenu du dossier « /home/romain » affiché avec succès
```

L'accès au serveur FTP ne doit pas fonctionner depuis le port 21 :



Impossible d'établir une connexion au serveur

Voici le résultat lors du test d'accès au serveur FTP.

Pour conclure les différents test effectués nous ont montrés que le routage inter vlan était fonctionnel via des test de ping, on observe aussi que tous les VLAN ont accès au serveur web et que le port 21 n'a pas accès au FTP.