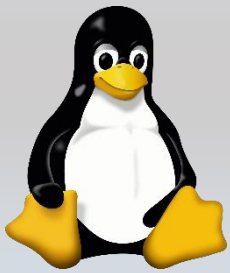
Travail Bloc 1 / TP 2

SWITCH / ROUTEUR

Dans ce document, vous découvrirez comment configurer un commutateur et un routeur Cisco. De plus, vous apprendrez à mettre en place un port mirroring, des règles iptables, le routage inter-VLAN, la configuration du service Telnet, ainsi que la mise en place d'un service IIS.



CISCO

Microsoft IIS

Saint Paul Bourdon Blanc

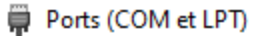
Table des matières

OBJECTIF : Cette section de la procédure vise à détailler la connexion à un switch

MODE OPÉRATOIRE :

1 – Première étape : Vérifier la connexion au port du switch

Pour vérifier que le switch est bien connecté sur le pc aller dans le gestionnaire des périphériques. Puis cliquer



, vérifié que le switch est bien branché sur le COM1.

2 – Deuxième étape : Lancer Tera Terme

Pour pouvoir communiquer avec le switch nous allons installer l'outil Tera Term :

https://github.com/TeraTermProject/teraterm/releases

Une fois que vous avez télécharger Tera Term vous pouvez alors sélectionner, l'options « série » :

3 – Troisième étape : Connexion au switch

Après avoir fini de configurer la connexion. Appuyez sur le bouton Mode et maintenez-le enfoncé. Après environ 3 secondes, les DELs du commutateur commencent à clignoter. Continuez de maintenir le bouton Mode enfoncé. Les DELs arrêtent de clignoter après 7 secondes supplémentaires et le commutateur redémarre ensuite.

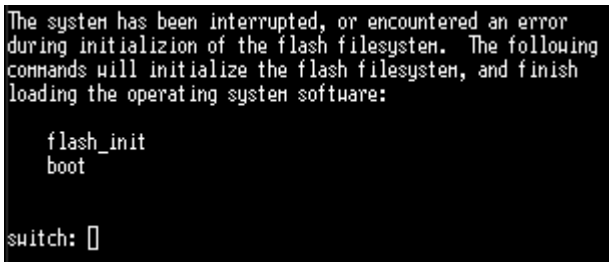
OBJECTIF : Cette section de la procédure vise à détailler la restauration d'un switch.

MODE OPÉRATOIRE :

1 – Première étape : Pour restaurer le switch

Pour restaurer un switch, commencez par saisir la commande :

➔ switch : flash_init



1 – Première étape : Pour restaurer le switch

Une fois cette commande réalisée, saisissez la commande :

➔ switch : dir flash

Cette commande permet de visualiser les fichiers que contient le switch.

1 – Première étape : Pour restaurer le switch

Nous constatons que notre switch contient plusieurs fichiers. Pour le réinitialiser, nous allons supprimer le fichier intitulé "config.text" avec la commande :

➔ switch : del flash:config.text

Nous pouvons aussi supprimer les fichiers contenant les vlan avec la même commande.

1 – Première étape : Pour restaurer le switch

Enfin vous pouvez taper la commande pour réinitialiser le switch :

➔ switch : boot

OBJECTIF : Cette section de la procédure vise à détailler la configuration d'un serveur tftp.

MODE OPÉRATOIRE :

1 – Première étape : Installé un TFTP

Une fois les étapes précédentes réalisées, pour pouvoir effectuer des sauvegardes, nous allons installer un serveur TFTP (TFTP32) :

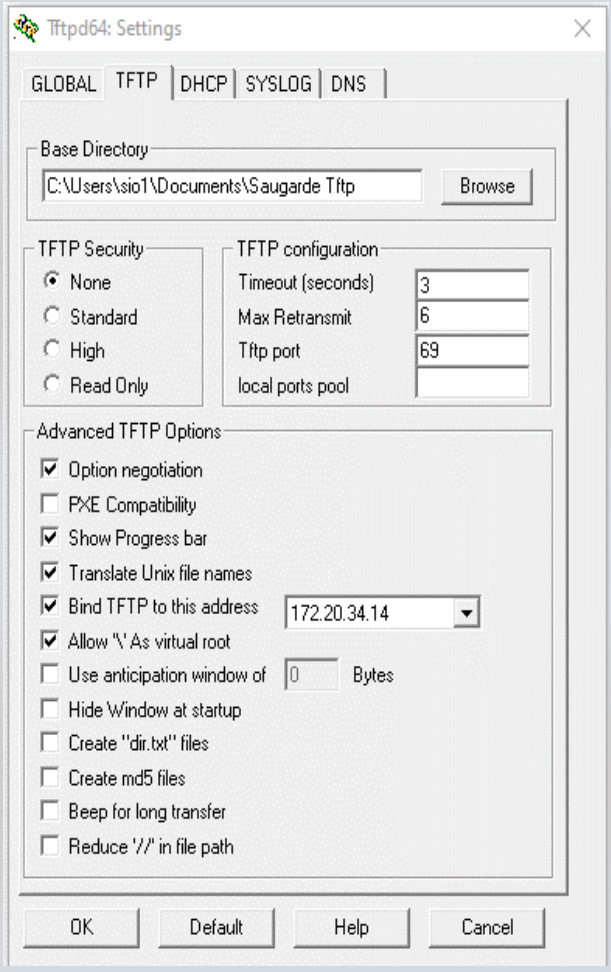
https://pjo2.github.io/tftpd64/

Une fois TFTP32 installé et lancé, allez dans les paramètres, puis configurez de la même manière :

- "Base Directory" permet de définir où la sauvegarde sera stockée.

- "TFTP Security" pour spécifier le niveau de sécurité que nous appliquons au switch.

Veillez à n'activer que le client et le serveur TFTP.



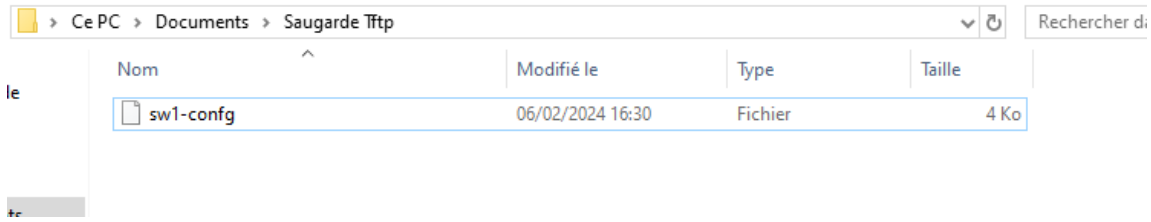
2 – Deuxième étape : Sauvegarder le switch

Pour effectuer une copie de votre configuration en cours d'exécution (running-config) sur le switch, il vous suffit de saisir la commande :

➔ copy running-config tfp

```
SW1#copy running-config tftp:
Address or name of remote host []? 172.20.34.14
Destination filename [sw1-confg]?
!!
3382 bytes copied in 1.115 secs (3033 bytes/sec)
SW1#
```

Vous pouvez alors voir dans le fichier de configuration situé dans le dossier que vous avez sélectionné via le TFTP :



3 –Troisième étape : Restaurer le switch

Une fois cela fait, vous pouvez restaurer votre configuration en tapant la commande

➔ copy tftp: running-config

```
copy ftp: running-config

Address or name of remote host [10.66.64.10]?
Source filename [backup_cfg_for_router]?
Destination filename [running-config]?
Accessing ftp://10.66.64.10/backup_cfg_for_router...
Loading backup_cfg_for_router !
[OK - 1030/4096 bytes]
1030 bytes copied in 13.213 secs (78 bytes/sec)
CE_2#
```

4 – Quatrième étape : Configurer la restauration sur le switch

Pour configurer le TFTP sur votre switch, vous devez d'abord lui attribuer un VLAN :

1. Utilisez la commande `interface vlan 1` pour accéder à l'interface du VLAN.

2. Définissez une adresse IP correspondant à votre réseau à l'aide de la commande `ip address <adresse_IP> <masque_de_sous_reseau>`.

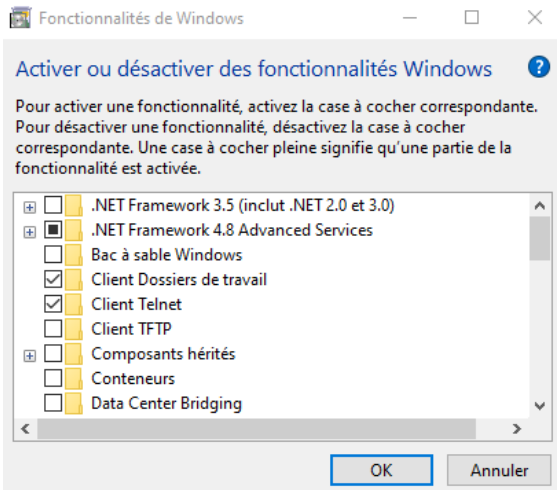
Ensuite, créez un utilisateur avec son mot de passe :

3. Utilisez la commande `username <nom_d'utilisateur> password <mot_de_passe>` pour créer un nouvel utilisateur avec le mot de passe spécifié.

Enfin, configurez votre ligne VTY pour l'accès à distance :

4. Accédez à la configuration de la ligne VTY en utilisant la commande `line vty 0 4`.

Enfin, il faut activer le Telenet sur le pc Windows.



Une fois cela fait, vous pouvez restaurer votre configuration en tapant la commande :copy tftp: running-config

OBJECTIF : Cette section de la procédure vise à détailler la configuration la création d'un serveur tftp.

MODE OPÉRATOIRE :

1 – Première étape : Faire la configuration de base

Pour configurer votre machine, suivez les étapes suivantes :

1. Commencez par modifier le nom de votre machine en utilisant la commande :

   ➔ nano /etc/hostname
   ➔ nano /etc/hosts

2. Mettez à jour votre système en exécutant les commandes : apt update et apt upgrade .

3. Enfin, installez le paquet ntp en utilisant la commande apt install ntpsec, puis vérifiez la date avec la commande : date .

(Maitre la VM en Accès pas pont)

2 – Deuxième étape : Installer le serveur tftp

Pour pouvoir installer le sereur tftp taper la commande :

➔ apt install tftpd-hpa

```
root@serveurTFTP:/home/sio# apt-get install tftpd-hpa
```

3 – Troisième étape : Configuration du serveur TFTP

Une fois installé, vous devez configurer le serveur TFTP. Les principales configurations se trouvent dans le fichier :

➔ nano /etc/default/tftpd-hpa.

```
# /etc/default/tftpd-hpa

TFTP_USERNAME="tftp"
TFTP_DIRECTORY="/srv/tftp"
TFTP_ADDRESS=":69"
TFTP_OPTIONS="--secure"
```

TFTP_USERNAME :

Nom de l'utilisateur sous lequel le serveur TFTP s'exécute.

TFTP_DIRECTORY :

Répertoire racine pour le serveur TFTP.

TFTP_ADDRESS :

Adresse IP et port sur lesquels le serveur écoute les connexions.

TFTP_OPTIONS :

Options supplémentaires pour le serveur TFTP.

Dans cet exemple, l'option --secure est utilisée pour empêcher les transferts de fichiers en dehors du répertoire spécifié.

4 – Quatrième étape : On crée un répertoire TFTP

Vous devez créer le répertoire que vous avez spécifié comme **`TFTP_DIRECTORY`** dans la configuration, pour se faire taper la commande :

➔ Mkdir -p /serv/tftp

5 – Cinquième étape : On redémarre le service

Après avoir effectué les configurations, redémarrez le service pour appliquer les changements, avec la commande :

➔ systemctl restart tftpd-hpa

```
root@serveurTFTP:/home/sio# systemctl restart tftpd-hpa
```

6 – Sixième étape : Vérification du fonctionnement

Vous pouvez vérifier si le serveur TFTP fonctionne correctement en utilisant la commande « ss » pour vérifier s'il écoute sur le port 69 :

➔ ss -tuln | grep 69

```
root@serveurTFTP:/home/sio# ss -tuln | grep 69
udp   UNCONN 0      0                                   0.0.0.0:69          0.0.0.0:*
udp   UNCONN 0      0                                      [::]:69             [::]:*
udp   UNCONN 0      0      [fe80::a00:27ff:fee9:869d]%enp0s3:123             [::]:*
root@serveurTFTP:/home/sio#
```

OBJECTIF : Cette section de la procédure vise à détailler la configuration du port.

MODE OPÉRATOIRE :

1 – Première étape : Configurer le port miroir

Pour pouvoir configurer le port source du miroir on se rend sur le port du miroir :

- ➔ Interface GigabiEthernet 0/10
- ➔ Switchport mode access

```
SW1(config)#interface GigabitEthernet 0/10
SW1(config-if)#suit
SW1(config-if)#switchport nod acc
SW1(config-if)#switchport nod
SW1(config-if)#switchport mode acc
SW1(config-if)#switchport mode access
```

2 – Deuxième étape : Configurer le port source

On configure le port source du mirroing :

- ➔ Monitor session 1 destination interface FastEthernet0/10 encapsulation replicate

```
SW1(config)#$tination interface GigabitEthernet 0/10 encapsulation replicate
SW1(config)#
```

3 – Troisième étape : Configurer le port destination

On configure le port source du mirroing :

- ➔ Monitor session 1 source interface GigabiEthernet 0/1

```
SW1(config)#monitor session 1 source interface GigabitEthernet 0/1
```

OBJECTIF : Cette section de la procédure vise à détailler la configuration de Telnet.

MODE OPÉRATOIRE :

1 – Première étape : Configure le switch

Les commande pour configurer le switch :

- conf t
- username ExempleNom password VotreMotDePasse
- interface vlan 1
- ip address 172.20.34.100 255.255.0.0 (On donne une ip en report avec notre réseau)
- exit
- line vty 0 4
- login local
- exit
- transport input telnet (pas forcément obligatoire)

2 – Deuxième étape : Se connecter à Telnet

Une fois que vous avez configurer corectement telnet, il vous suffit de vous rendre dans le cmd, et de taper la commande :

- telnet Address de l'interface

```
C:\WINDOWS\system32>telnet 172.20.34.100
```

On vous demande alors les identifiant que vous avez sur le switch pour vous y connecter :

```
Username: tom
Password:
```

OBJECTIF : Cette section de la procédure vise à détailler la configuration la récupération de mot de passe Telnet avec le port mirroring.

MODE OPÉRATOIRE :

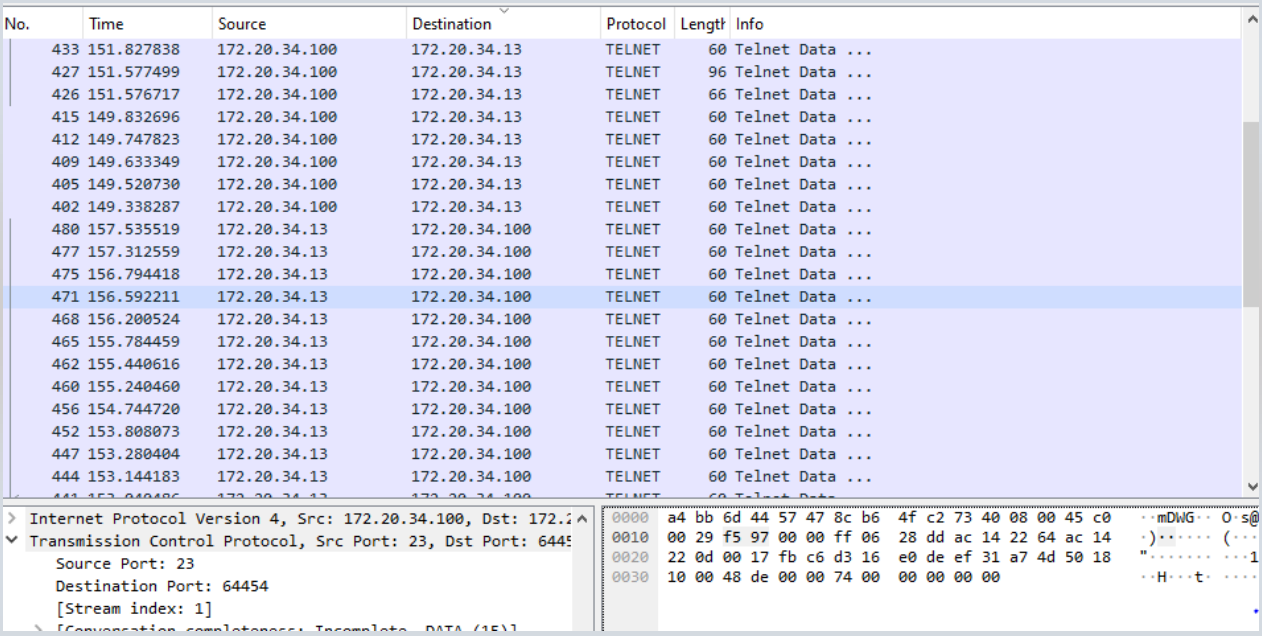
Exercice pour récupérer le mot de passe telnet

Pour récupérer le mot de passe telnet en claire nous allons analyser les trames avec l'outil wireshark.

Pour se faire nous allons connecter un pc sur le port 10 que nous avons mis en mirrore avec le port 1.

Nous devrions alors voire quand on lance se connecter au telnet avec le pc sur le port 1 le mot de passe telnet sur le wireshark pc sur le port 10.

Nous pouvons remarquer que le pc à bien récupérer les tram telnet et donc le mot de passe.



No.	Time	Source	Destination	Protocol	Length	Info
433	151.827838	172.20.34.100	172.20.34.13	TELNET	60	Telnet Data ...
427	151.577499	172.20.34.100	172.20.34.13	TELNET	96	Telnet Data ...
426	151.576717	172.20.34.100	172.20.34.13	TELNET	66	Telnet Data ...
415	149.832696	172.20.34.100	172.20.34.13	TELNET	60	Telnet Data ...
412	149.747823	172.20.34.100	172.20.34.13	TELNET	60	Telnet Data ...
409	149.633349	172.20.34.100	172.20.34.13	TELNET	60	Telnet Data ...
405	149.520730	172.20.34.100	172.20.34.13	TELNET	60	Telnet Data ...
402	149.338287	172.20.34.100	172.20.34.13	TELNET	60	Telnet Data ...
480	157.535519	172.20.34.13	172.20.34.100	TELNET	60	Telnet Data ...
477	157.312559	172.20.34.13	172.20.34.100	TELNET	60	Telnet Data ...
475	156.794418	172.20.34.13	172.20.34.100	TELNET	60	Telnet Data ...
471	156.592211	172.20.34.13	172.20.34.100	TELNET	60	Telnet Data ...
468	156.200524	172.20.34.13	172.20.34.100	TELNET	60	Telnet Data ...
465	155.784459	172.20.34.13	172.20.34.100	TELNET	60	Telnet Data ...
462	155.440616	172.20.34.13	172.20.34.100	TELNET	60	Telnet Data ...
460	155.240460	172.20.34.13	172.20.34.100	TELNET	60	Telnet Data ...
456	154.744720	172.20.34.13	172.20.34.100	TELNET	60	Telnet Data ...
452	153.808073	172.20.34.13	172.20.34.100	TELNET	60	Telnet Data ...
447	153.280404	172.20.34.13	172.20.34.100	TELNET	60	Telnet Data ...
444	153.144183	172.20.34.13	172.20.34.100	TELNET	60	Telnet Data ...

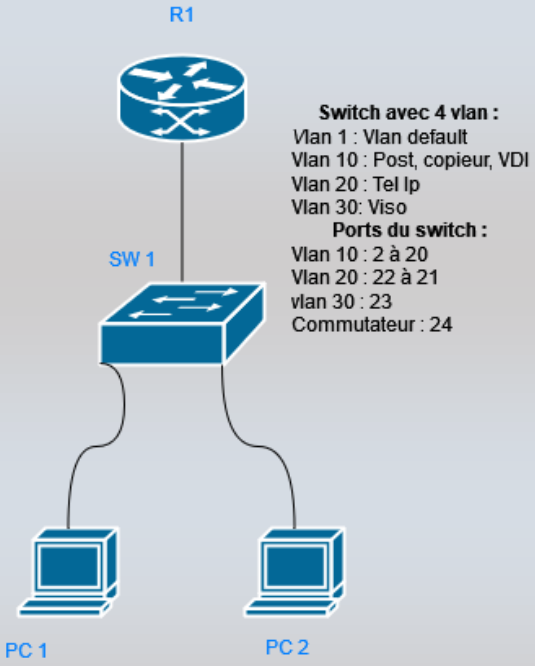
```
> Internet Protocol Version 4, Src: 172.20.34.100, Dst: 172.2
v Transmission Control Protocol, Src Port: 23, Dst Port: 6445
    Source Port: 23
    Destination Port: 64454
    [Stream index: 1]
```

```
0000  a4 bb 6d 44 57 47 8c b6  4f c2 73 40 08 00 45 c0   ··mDWG·· O·s@··E·
0010  00 29 f5 97 00 00 ff 06  28 dd ac 14 22 64 ac 14   ·)······ (···"d··
0020  22 0d 00 17 fb c6 d3 16  e0 de ef 31 a7 4d 50 18   "·····1 ·MP·
0030  10 00 48 de 00 00 74 00  00 00 00 00               ··H···t· ····
```

OBJECTIF : Cette section de la procédure vise à détailler la configuration du routage inter-Vlan sur switch et routeur CISCO.

Prérequis – Routage inter

Shéma :



Comme exemple d'adressage ip, nous allons prendre :

172.21.254.254/16 pour l'interface Vlan 10

172.22.254.254/16 pour l'interface Vlan 20

172.30.254.254/16 pour l'interface Vlan 30

De plus nos pc aurons comme ip : 172.21.1.1/16 pour le pc 1 dans le lan 10 et 172.22.2.2/16 pour le pc 2 dans le lan 20.

1 – Première étape : Crée-les vlan

Pour pouvoir crée nos 3 vlan nous allons taper une fois sur le switch en mode configuration de terminal, les commandes suivantes :

- vlan 10
- name VLAN10
- exit
- vlan 20
- name VLAN20
- exit
- vlan 30
- name VLAN30
- exit

```
SW1(config-vlan)#exit
SW1(config)#vlan 20
SW1(config-vlan)#nam
SW1(config-vlan)#name VLAN20
SW1(config-vlan)#
```

2 – Deuxième étape : Assigne des ports au VLAN

Pour pouvoir donner des ports au vlan il faut taper les commandes :

- interface range GigabitEthernet 0/2-20
- switchport mode access
- switchport access vlan 10
- exit
- interface range GigabitEthernet 0/21-22
- switchport mode access
- switchport access vlan 20
- exit
- interface range GigabitEthernet 0/23
- switchport mode access
- switchport access vlan 30
- exit

```
SW1(config)#interface range GigabitEthernet 0/2-20
SW1(config-if-range)#suitc
SW1(config-if-range)#switchport mode acc
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switch
SW1(config-if-range)#switchport acc
SW1(config-if-range)#switchport access vla
SW1(config-if-range)#switchport access vlan 10
SW1(config-if-range)#exit
```

3 – Troisième étape : Mode Trunk

On configure le mode trunk sur le port 24 du switch, avec les commandes :

- interface GigabiEthernet 24
- switchport mode trunk
- switchport trunk allowed vlan 10,20,30
- no shutdown
- exit

4 – Troisième étape : Configuration du Routeur

Pour pouvoir configurer le routeur correctement nous allons créer des interfaces virtuelles :

- enabel
- conf t
- interface FastEthernet 0/0
- no shutdown
- exit
- interface FastEthernet 0/0.10
- encapsulation dot1Q 10
- ip address 172.21.254.254 255.255.0.0
- no shotdown
- exit
- interface FastEthernet 0/0.20
- encapsulation dot1Q 20
- ip address 172.22.254.254 255.255.0.0
- no shotdown
- exit
- interface FastEthernet 0/0.30
- encapsulation dot1Q 30
- ip address 172.30.254.254 255.255.0.0
- no shotdown

5 – Cinquième étape : Activer le routage

Une fois que vous avez correctement activée les interfaces virtuelles, avec la commande :

➔ ip routing

```
R1(config)#ip routing
R1(config)#
```

A ce stade les deux pc devrait pourvoir ping entre les différents VLAN. (Penser à mettre comme passerelle l'ip des sous interface sans mettre d'ip à l'interface principale).

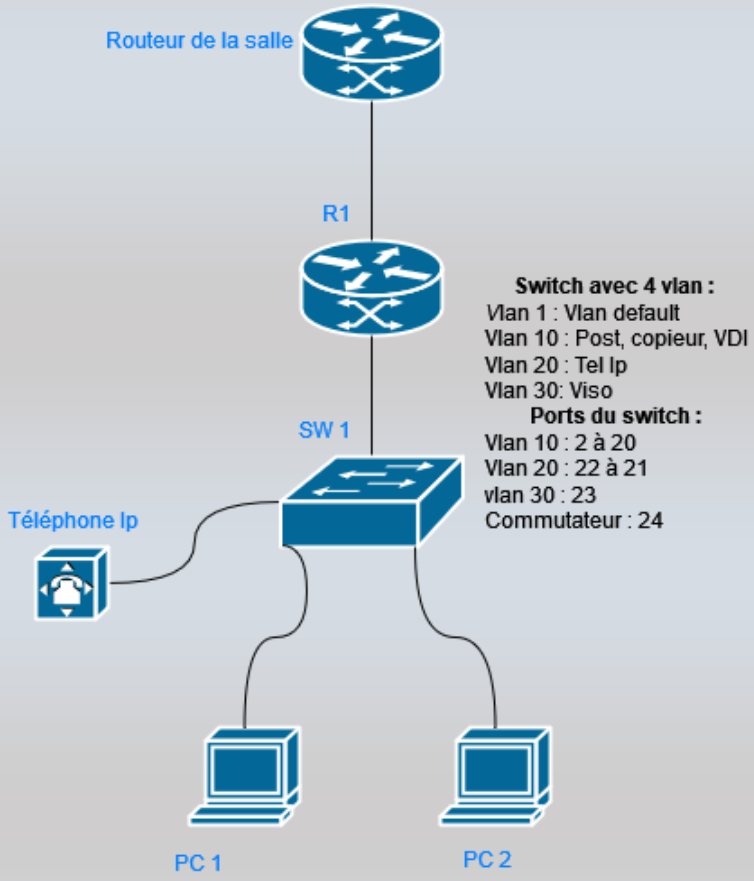
```
C:\Users\sio1>ping 172.22.1.1

Envoi d'une requête 'Ping'  172.22.1.1 avec 32 octets de données :
Réponse de 172.22.1.1 : octets=32 temps=1 ms TTL=127
Réponse de 172.22.1.1 : octets=32 temps=1 ms TTL=127
Réponse de 172.22.1.1 : octets=32 temps=1 ms TTL=127
Réponse de 172.22.1.1 : octets=32 temps=1 ms TTL=127

Statistiques Ping pour 172.22.1.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
```

OBJECTIF : Cette section de la procédure vise à détailler la configuration du routage inter-Vlan sur switch et routeur CISCO.

MODE OPÉRATOIRE :

Prérequis – Routage LINUX

Schéma :



Pour ce schéma nous allons reprendre les même ip que le schéma précédent cependant nous rajoutons un téléphone ip qui obtiendra sont ip à partir d'un serveur DHCP qui tourne sur le routeur R1 (Plage d'ip : 172.30.1.1 à 172.30.1.2).

De plus nous remplaçons le routeur Cisco par un routeur sous linux qui donnera l'internet au pc en passent par le routeur de la salle.

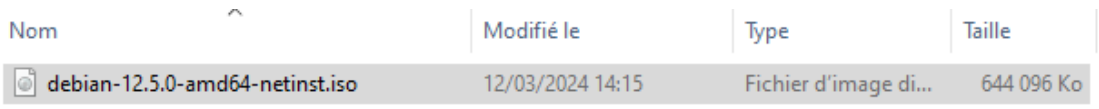
1 – Première étape : Installer Linux

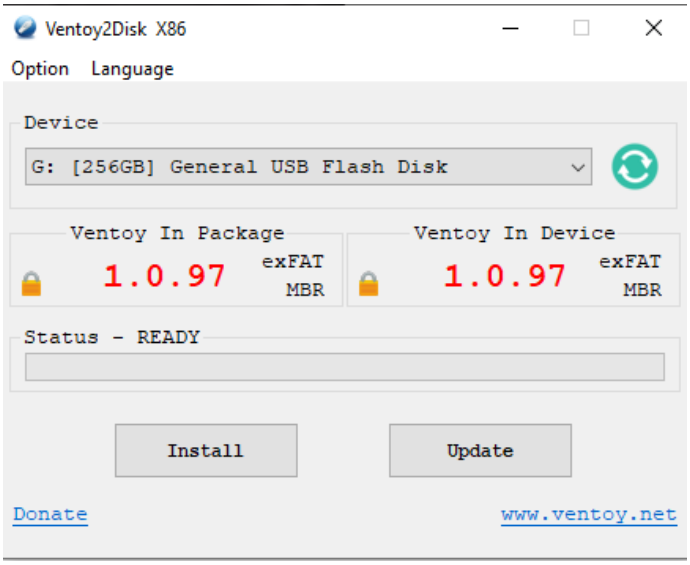
Pour pouvoir installé linux il vous faudra installer ventoye puis formater la clé. Une fois cela fais trouver un iso de de debian 12 avec l'interafce gnomme.

On se rend sur le site ventoy au lien : https://www.ventoy.net/en/download.html

On télécharge l'iso debain 12 en netinstall : https://www.debian.org/download

On formate la clé en FAT32 la clé et install Ventoy dessus :





Une fois que vous avez boot sur la clé sur penser à désactiver l'ip v6 et à arrêter le chargement sur le DHCP.

2 – Deuxième étape : Configurer le routeur LINUX

Sur notre pc nous avons actuellement 3 cartes réseau :

- enp4s0
- enp4s2
- enp0s25

Notre carte réseau enp0s25 sera celle qui fera la liaison entre le routeur de la salle puis notre carte réseau enp4s0 sera pour les interfaces de nos vlan

Dans le fichier :

➔ nano etc/network/interfaces

Nous rentrons les commandes suivantes :

##########Configuration de la carte réseau enp0s25##########

auto enp0s25

iface enp0s25 inet static

address 172.20.34.106

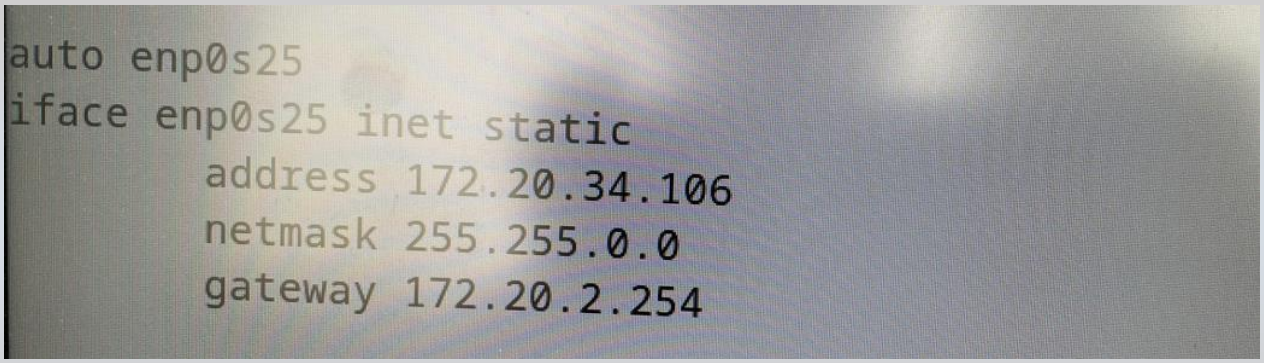
netmask 255.255.0.0

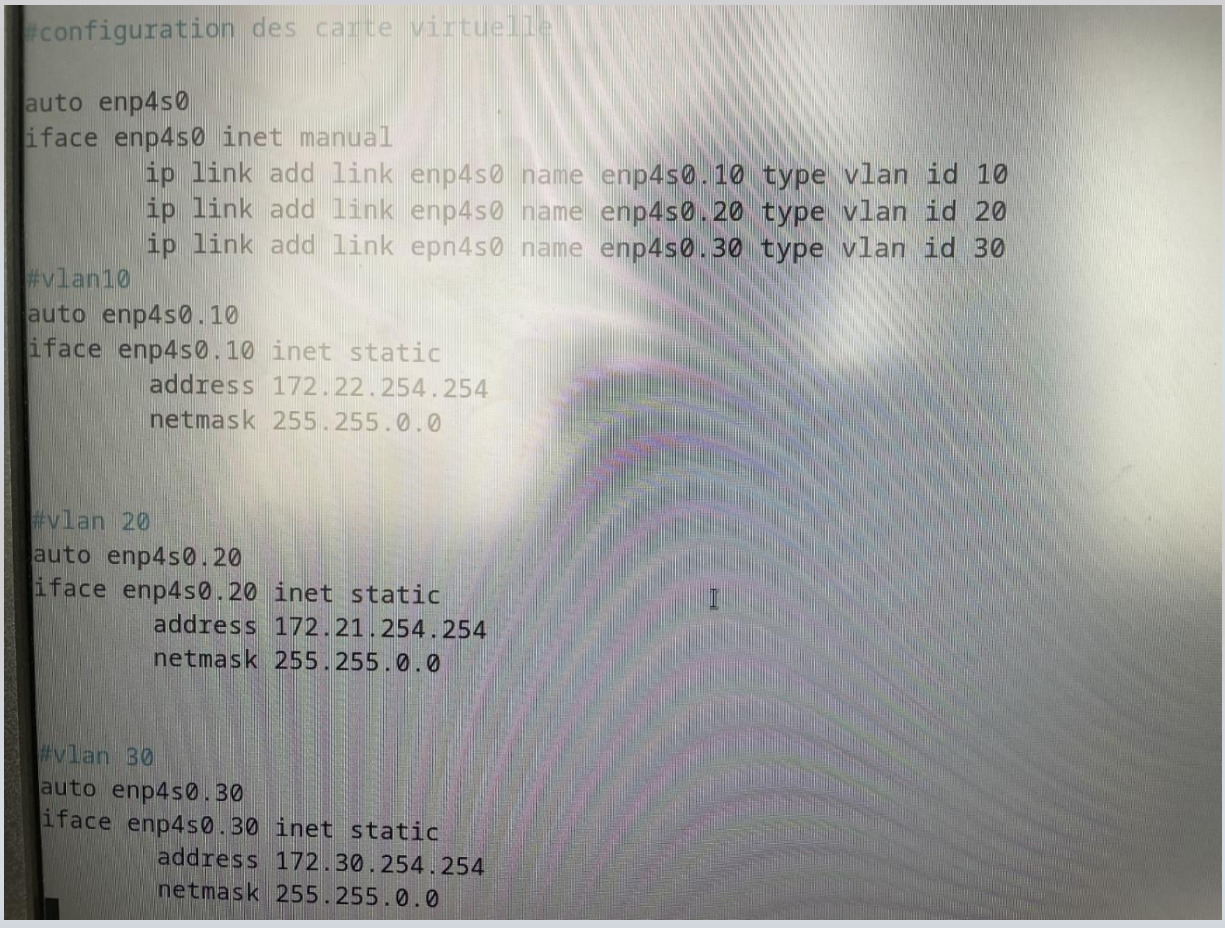
gateway 172.20.2.254

2 – Deuxième étape : Configurer le routeur LINUX

```
##########Configuration des interface virtuelle##########
auto enp4s0
iface enp4s0 inet manual
        ip link add enp4s0 name enp4s0.10 type vlan id 10
        ip link add enp4s0 name enp4s0.20 type vlan id 20
        ip link add enp4s0 name enp4s0.30 type vlan id 30
auto enp4s0.10
iface enp4s0.10 inet static
        address 172.21.254.254
        netmask 255.255.0.0
iface enp4s0.20 inet static
        address 172.22.254.254
        netmask 255.255.0.0
iface enp4s0.30 inet static
        address 172.30.254.254
        netmask 255.255.0.0
```

2 – Deuxième étape : Configurer le routeur LINUX



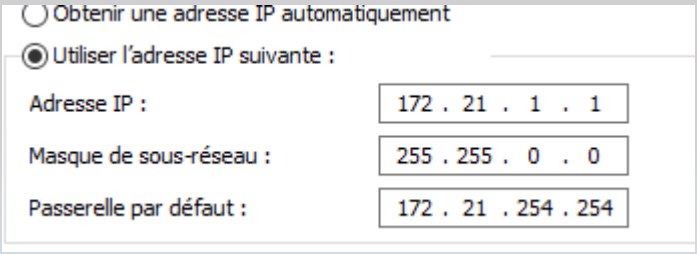


3 – Troisième étape : Donne une ip

A ce stade vous avez configurer le routeur linux et le switch Cisco sur votre infrastructure.

Il ne vous reste plus cas tester les pings entre les pcs. Pour ce faire nous allons comme dit précédemment donner l'ip 172.21.1.1 au pc et 172.22.1.1 au pc 2.

Exemple de configuration :



Les deux doivent normalement ping entre eux :

```
Envoi d'une requête 'Ping'  172.22.1.1 avec 32 octets de données :
Réponse de 172.22.1.1 : octets=32 temps=1 ms TTL=127
Réponse de 172.22.1.1 : octets=32 temps=1 ms TTL=127
Réponse de 172.22.1.1 : octets=32 temps=1 ms TTL=127
Réponse de 172.22.1.1 : octets=32 temps=1 ms TTL=127

Statistiques Ping pour 172.22.1.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
```

4 – Quatrième étape : Activer le Nat

Pour accéder à Internet, il est nécessaire de substituer votre adresse IP privée par une adresse IP publique. Pour réaliser cette opération, vous devez utiliser la commande suivante :

➔

```
root@RTRLNXLTREE:/home/r6# sudo iptables -t nat -A POSTROUTING -o enp0s25 -j MASQUERADE
```

5 – Cinquième étape : Activer le routage

Veuillez également entrer la commande suivante :

➔ Ip routing

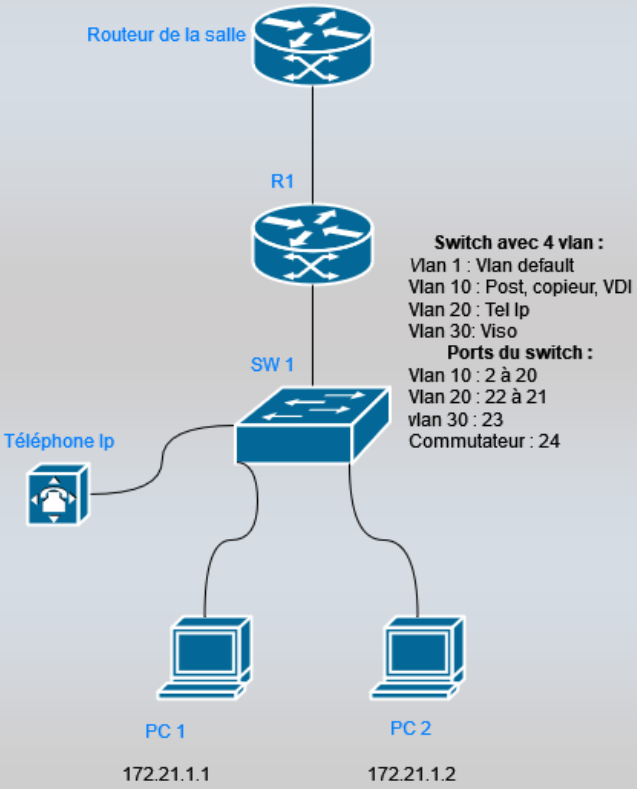
De plus activer le forwarding :

➔ Syctl -w net. ipv4.ip_forward = 1

OBJECTIF : Cette section de la procédure vise à détailler la connexion au switch

MODE OPÉRATOIRE :

Prérequis – Règle de filtrage



Dans notre infrastructure, nous souhaitons que seul notre PC1 ait accès au SSH du routeur, et non les autres postes.

De plus on veut que notre pc puisse sortir sur internet, mais qu'il ne soit pas possible de rentrer dans le réseau.

Exemple : Notre routeur en 172.20.34.106 peux ping le 172.20.34.12 mais le 172.20.34.12 ne doit pas pouvoir ping le 172.20.34.106

1 – Première étape : Filtrage du SSH

Pour désactiver l'accès SSH, commencez par exécuter la commande suivante :

Autoriser les connexions SSH entrantes de l'adresse IP 172.21.1.1

➔ sudo iptables -A INPUT -p tcp --dport 22 -s 172.21.1.1/32 -j ACCEPT

Par défaut, refuser toutes les autres connexions SSH entrantes

➔ sudo iptables -A INPUT -p tcp --dport 22 -j REJECT

Si vous voulez supprimer les règles existantes :

➔ sudo iptables -F

➔

```
root@RTRLNXLTREE:/home/r6# sudo iptables -F
root@RTRLNXLTREE:/home/r6# sudo iptables -A INPUT -p tcp --dport 22 -s 172.21.1.1/32 -j ACCEPT
root@RTRLNXLTREE:/home/r6# sudo iptables -A INPUT -p tcp --dport 22 -j REJECT
root@RTRLNXLTREE:/home/r6#
```

```
C:\Users\sio1>ssh r6@172.21.254.254
r6@172.21.254.254's password:
```

Il est observé que l'ordinateur avec l'adresse IP 172.21.1.1 conserve l'accès SSH, tandis que celui avec l'adresse IP 172.22.1.1 ne peut plus se connecter.

2 – Deux étape : Sauvegarde des règles

Pour sauvegarder les règles de filtrage, vous devez exécuter la commande suivante :

➔ sudo iptables-save > regles.txt

```
# Generated by iptables-save v1.8.9 (nf_tables) on Tue Mar 26 16:28:00 2024
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -s 172.21.1.1/32 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j REJECT --reject-with icmp-port-unreachable
COMMIT
# Completed on Tue Mar 26 16:28:00 2024
# Generated by iptables-save v1.8.9 (nf_tables) on Tue Mar 26 16:28:00 2024
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
-A POSTROUTING -o enp0s25 -j MASQUERADE
COMMIT
# Completed on Tue Mar 26 16:28:00 2024
```

3 – Troisième étape : Filtrage Internet

Pour bloquer l'accès à Internet, vous devez entrer les règles suivantes :

Autoriser le trafic sortant vers Internet pour les réseaux locaux (vlan 10, 20, 30)

sudo iptables -A FORWARD -s 172.21.0.0/16 -o enp0s25 -m state --state NEW,ESTABLISHED -j ACCEPT

sudo iptables -A FORWARD -s 172.22.0.0/16 -o enp0s25 -m state --state NEW,ESTABLISHED -j ACCEPT

sudo iptables -A FORWARD -s 172.30.0.0/16 -o enp0s25 -m state --state NEW,ESTABLISHED -j ACCEPT

Autoriser les réponses d'Internet vers les réseaux locaux (vlan 10, 20, 30)

sudo iptables -A FORWARD -d 172.21.0.0/16 -i enp0s25 -m state --state RELATED,ESTABLISHED -j ACCEPT

sudo iptables -A FORWARD -d 172.22.0.0/16 -i enp0s25 -m state --state RELATED,ESTABLISHED -j ACCEPT

sudo iptables -A FORWARD -d 172.30.0.0/16 -i enp0s25 -m state --state RELATED,ESTABLISHED -j ACCEPT

Bloquer tout le trafic entrant directement de Internet vers le routeur

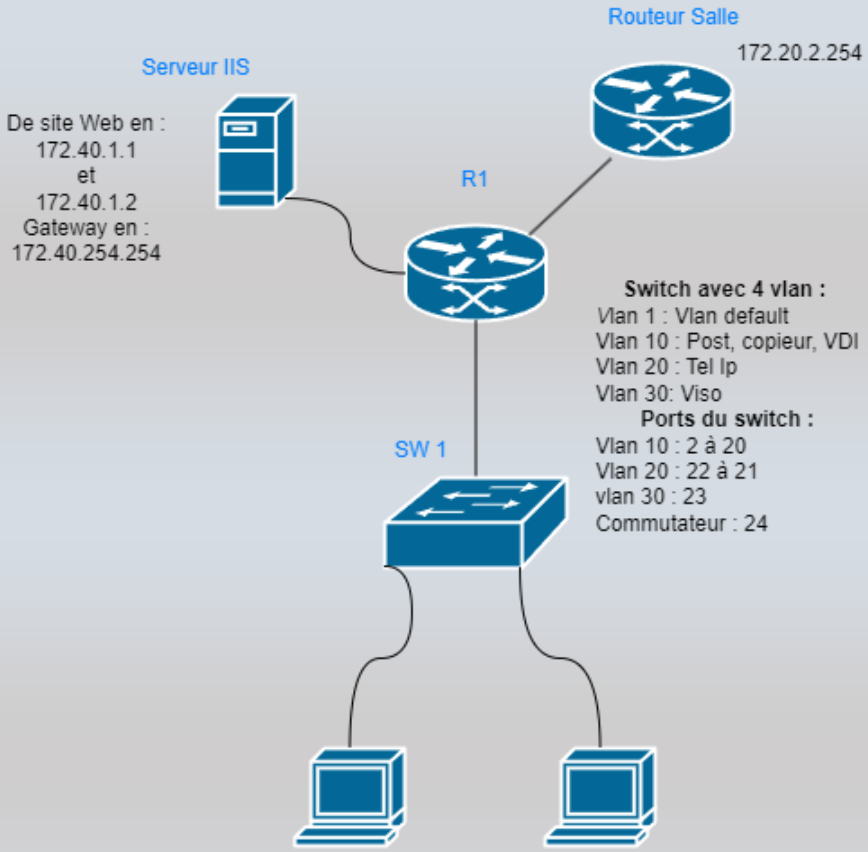
```
sudo iptables -A INPUT -j REJECT
```

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -s 172.21.1.1/32 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j REJECT --reject-with icmp-port-unreachable
-A INPUT -j REJECT --reject-with icmp-port-unreachable
-A FORWARD -s 172.21.0.0/16 -o enp0s25 -m state --state NEW,ESTABLISHED -j ACCEPT
-A FORWARD -s 172.22.0.0/16 -o enp0s25 -m state --state NEW,ESTABLISHED -j ACCEPT
-A FORWARD -s 172.30.0.0/16 -o enp0s25 -m state --state NEW,ESTABLISHED -j ACCEPT
-A FORWARD -d 172.21.0.0/16 -i enp0s25 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -d 172.22.0.0/16 -i enp0s25 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -d 172.30.0.0/16 -i enp0s25 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -d 172.30.0.0/16 -i enp0s25 -m state --state RELATED,ESTABLISHED -j ACCEPT
COMMIT
```

OBJECTIF : Cette section de la procédure vise à détailler la configuration du DMZ et du service IIS.

MODE OPÉRATOIRE :

Prérequis – DMZ



Pour ce schéma nous allons reprendre les même ip que le schéma précédent cependant nous rajoutons une DMZ, qui aura deux serveurs web IIS. Les ip seront 172.40.1.1 et 172.40.1.2 avec une Gateway sur le routeur en 172.40.254.254.

1 – Première étape : Ajouter le service

Une fois que vous êtes connecté avec votre nouveau compte utilisateur, allez dans :

➔ Gérer

➔ Ajouter des rôles et fonctionnalités

Dans « Rôles de serveurs » ajouter le serveur web (IIS) :

➔ Rôles de serveurs

➔ ☑ Serveur Web (IIS)

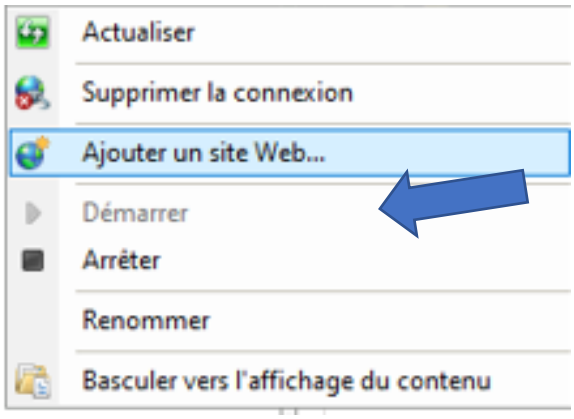
Puis dans « Rôle Web server (IIS) ajouter :

➔ ☐ Serveur FTP
☐ Service FTP

2 – Deuxième étape : Configurer le service

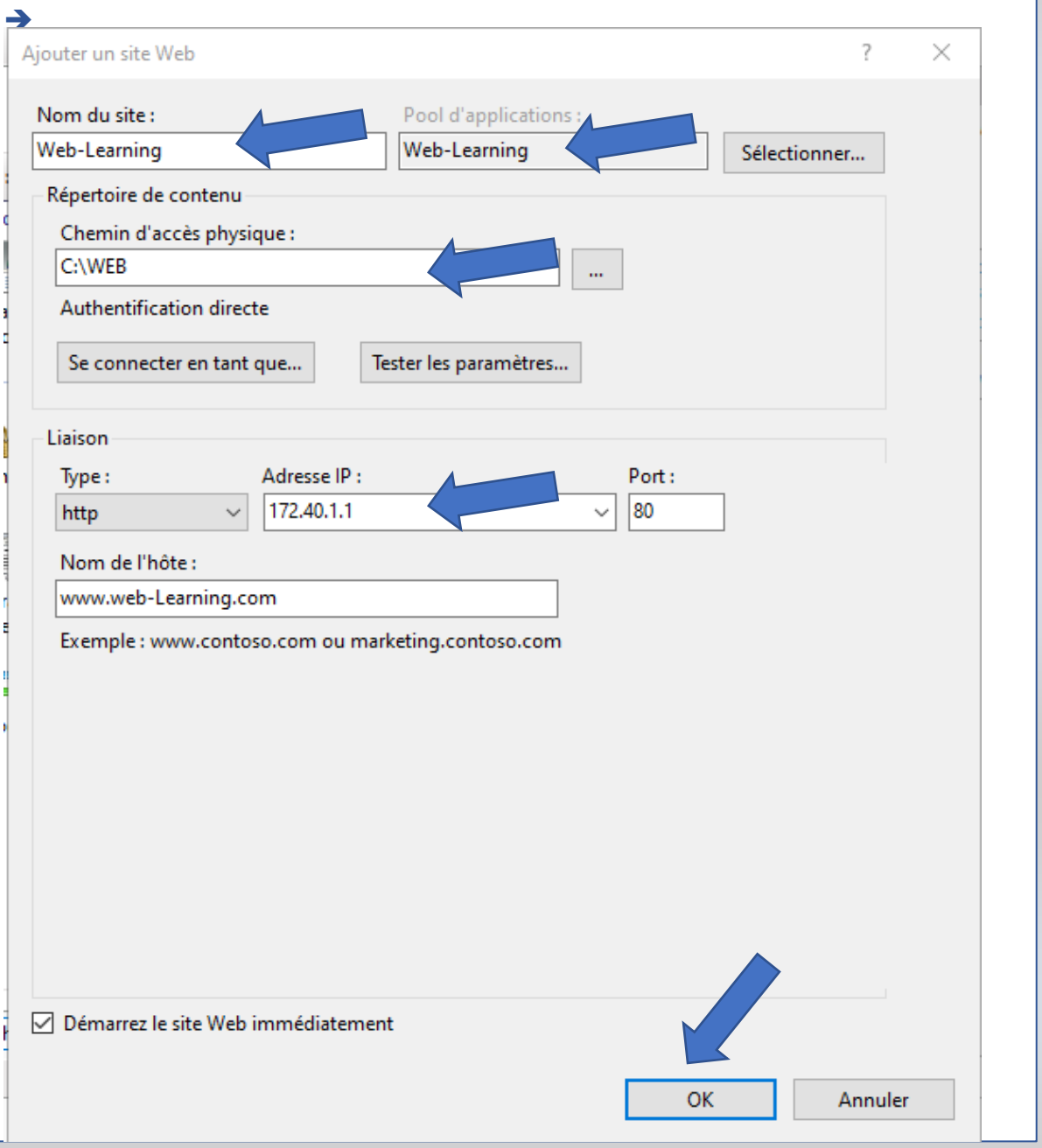
Pour pouvoir configurer le serveur aller cliquer sur le service IIS, puis :

➔



2 – Deuxième étape : Configurer le service

Puis configurer votre site :

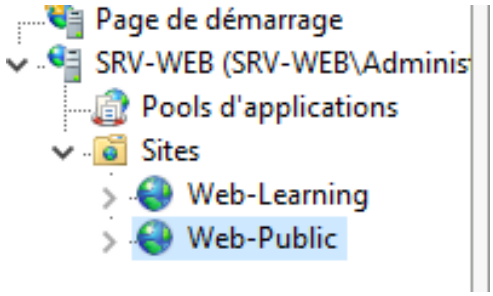


2 – Deuxième étape : Configurer le service

Vous pouvez alors constater qu'il y a deux site web, un site web Web-Learning et Web-Public.

L'ip du web Learning sera en 172.40.1.1 et de Web-Public en 172.40.1.2.

➔

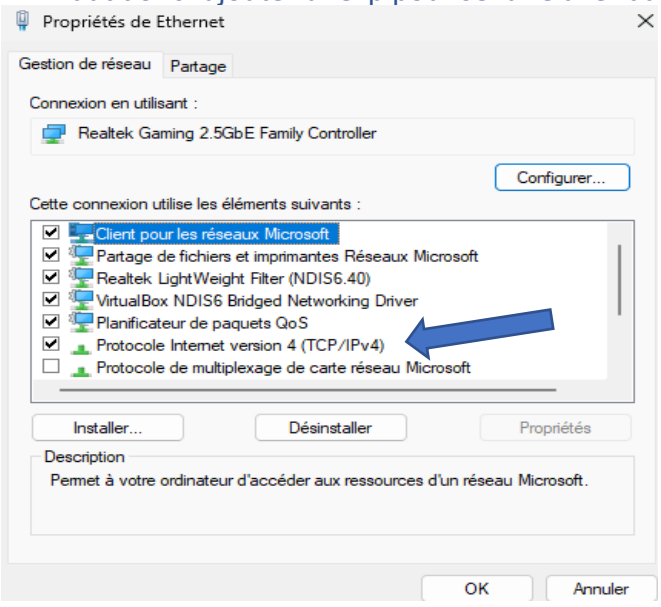


2 – Troisième étape : Configurer le service

Une fois que vous avez crée vos deux serveur web, vous pouvez alors vous connecter dessus avec leur ip. Cependant penser à rajouter une deuxième ip pour votre deuxième serveur web.

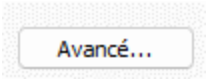
Je m'explique vous avez votre premier serveur web qui est en 172.40.1.1 cependant le deuxième est en 172.40.1.2. il faut donc rajouter une ip pour se faire aller dans :

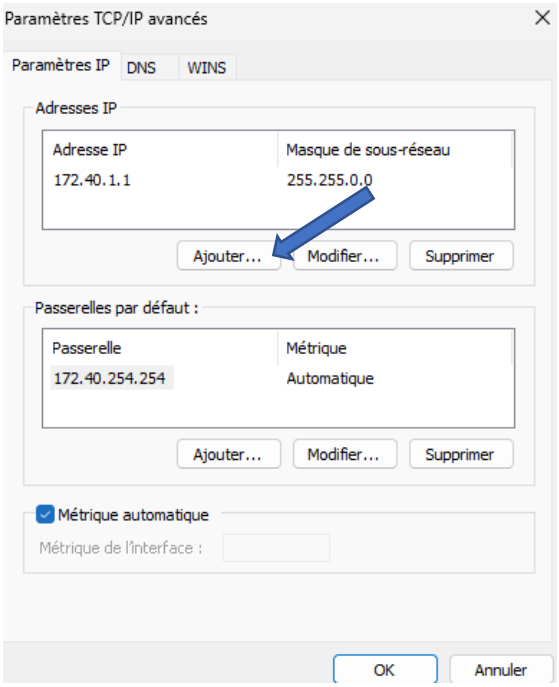
➔

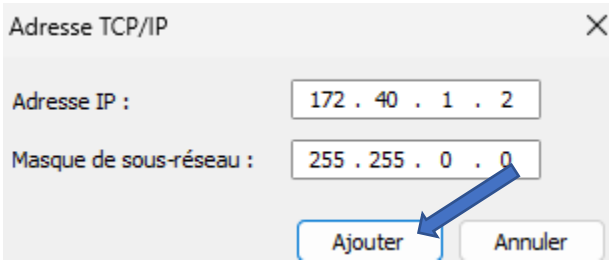


2 – Deuxième étape : Configurer le service

Une fois dans IPv4, aller dans :







3 – Troisième étape : Accéder à votre site web

Pour pouvoir avoir accès à votre site web aller dans, sur un navigateur et taper l'IP de votre machine :

➔ **LEARNING WEB**

4 – Quatrième étape : Crée une zone DNS

Pour crée une zone DNS, allez dans :

➔ Gérer

➔ Ajouter des rôles et fonctionnalités

Dans Rôles de serveurs ajouter le serveur DNS :

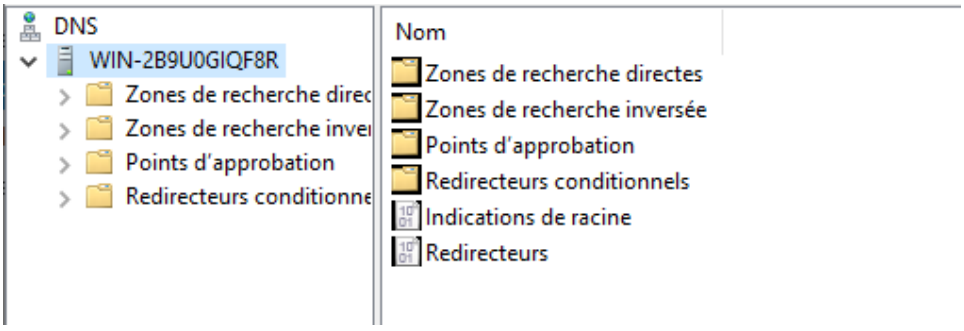
➔ Rôles de serveurs

➔ ☐ Serveur DNS

Une fois le service DNS installé, vous pouvez alors effectuer un clic droit sur votre serveur DNS et sélectionner :

➔ Gestionnaire DNS

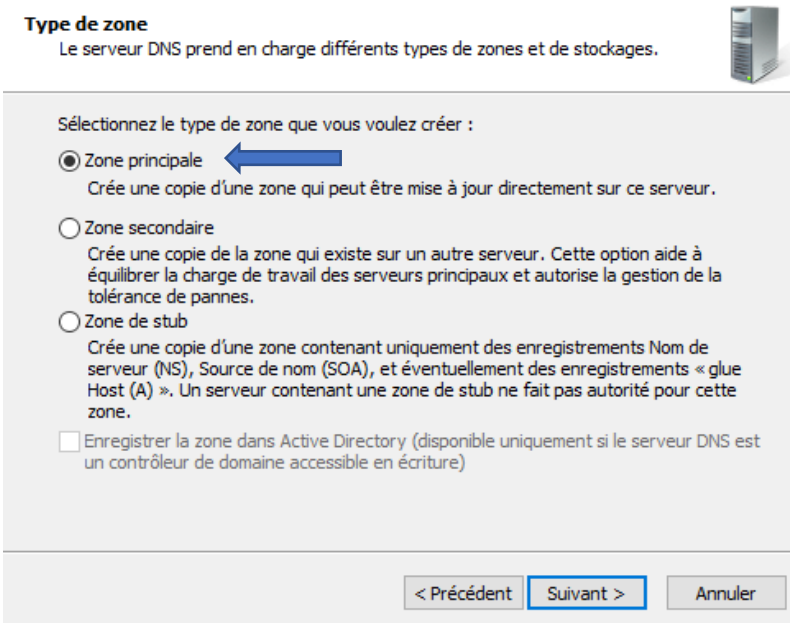
Vous accédez alors au panneau de configuration du DNS :



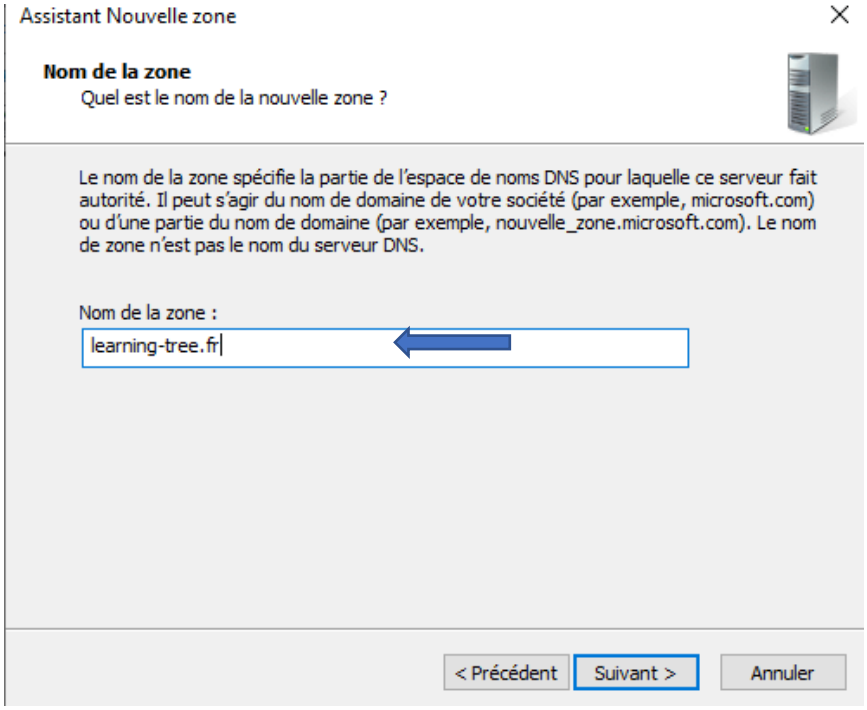
4 – Quatrième étape : Crée une zone DNS

Puis :

➔



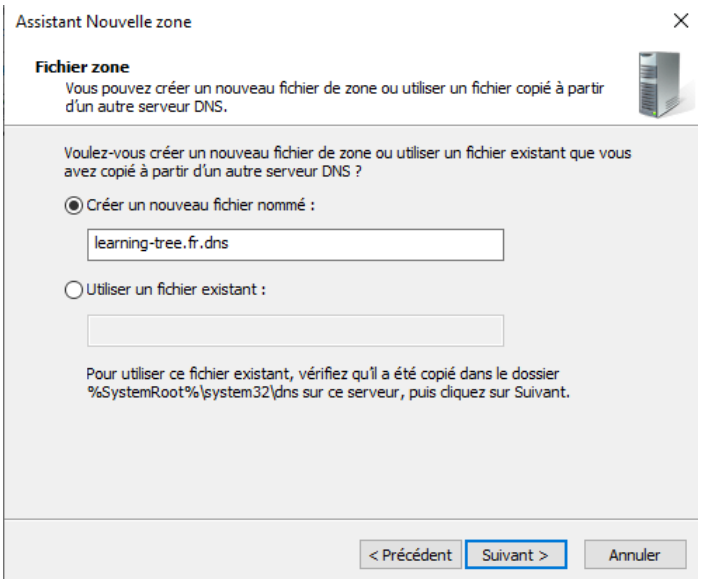
➔



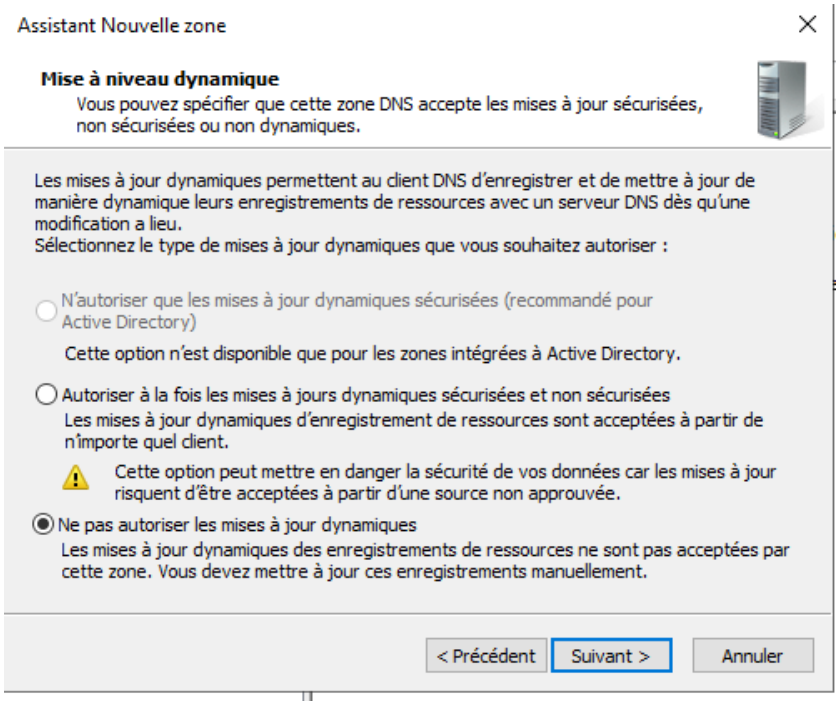
4 – Quatrième étape : Crée une zone DNS

Puis, le système vous offre le choix entre deux options. Si vous possédez déjà un fichier DNS que vous souhaitez réutiliser, vous pouvez cocher la deuxième option ; sinon, vous pouvez conserver la première :

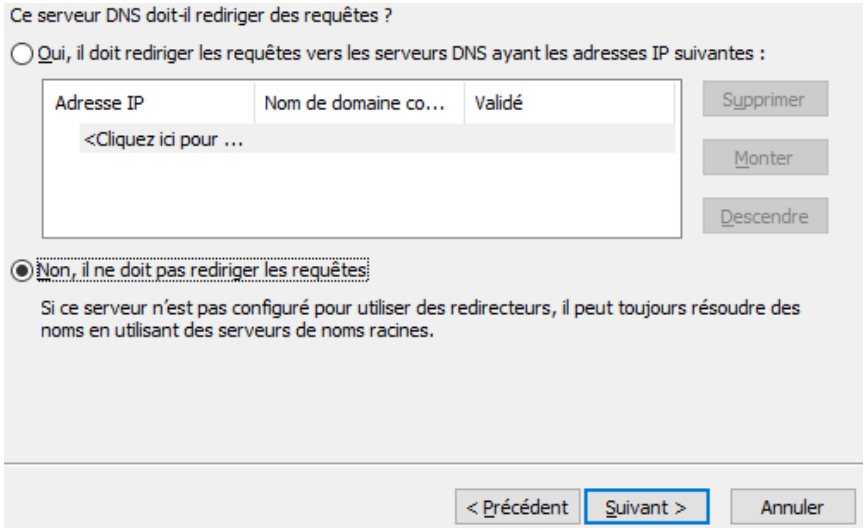
➔



➔

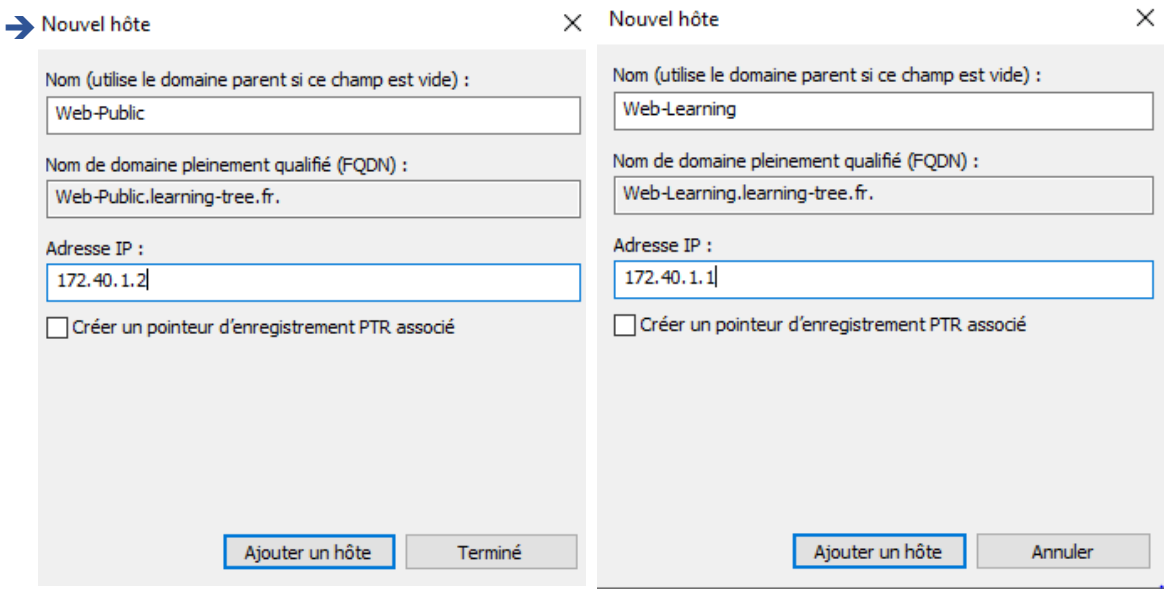


4 – Quatrième étape : Crée une zone DNS



4 – Quatrième étape : Crée une zone DNS

Enfin on ajoute nos nouveaux hôtes :



Vous devez donc avoir :

➔ F

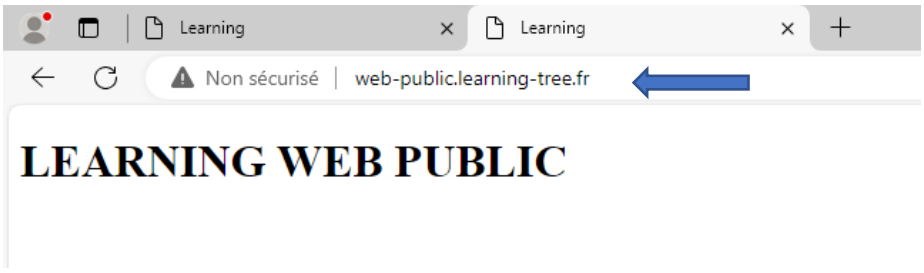
Nom	Type	Données
(identique au dossier parent)	Source de nom (SOA)	[1], srv-web., hostmaster.
(identique au dossier parent)	Serveur de noms (NS)	srv-web.
Web-Learning	Hôte (A)	172.40.1.1
Web-Public	Hôte (A)	172.40.1.2

(De plus votre machine penser à mettre comme DNS par défaut l'IP de votre serveur.)

5 – Cinquième étape : Tester la résolution de nom DNS

Sur votre machine avec le serveur iis, tenter de vous rendre sur votre site avec la résolution de nom :

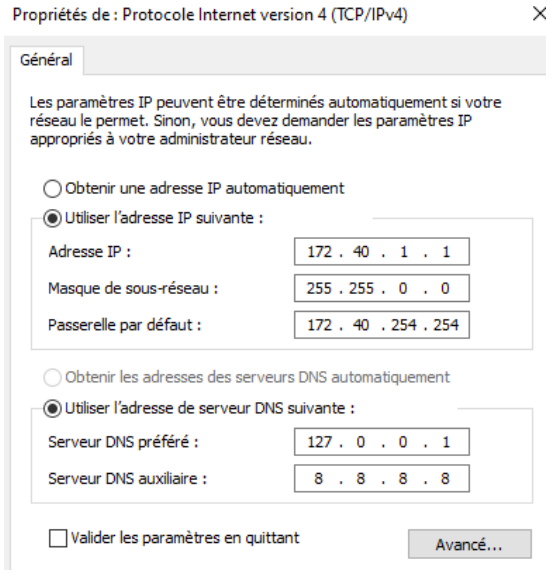
➔



À ce stade, vous pouvez accéder à l'un de vos deux sites web, cependant vous n'avez pas accès à votre site depuis internet.

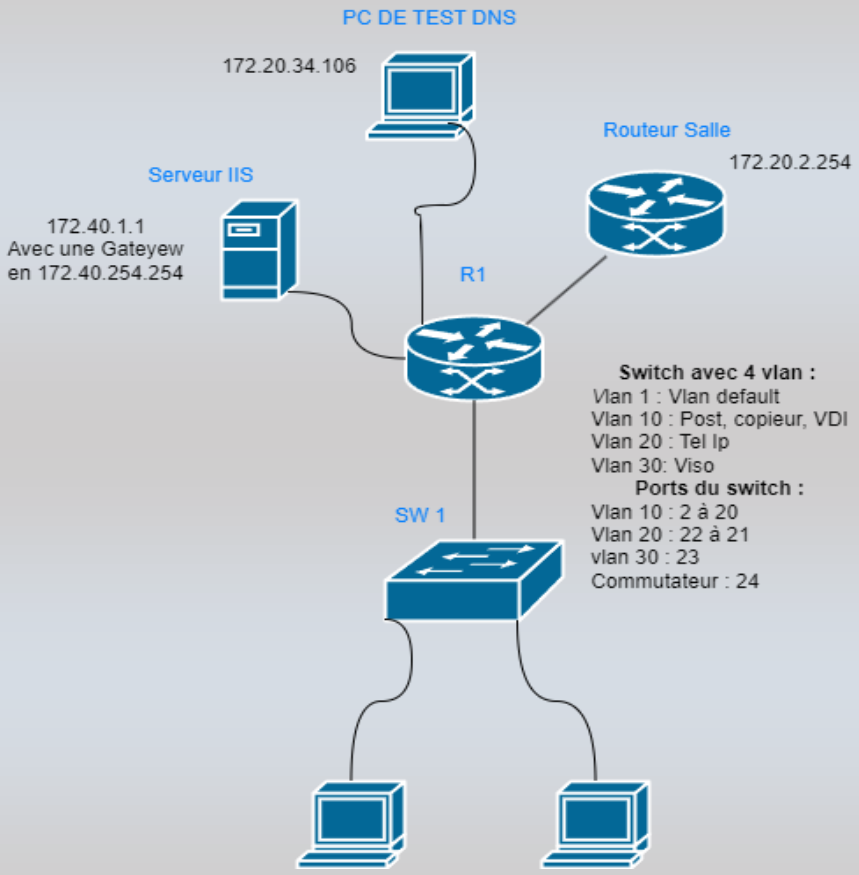
DNS IIS :

➔



6 – Sixième étape : Tester la résolution de nom sur un poste client

Schéma :

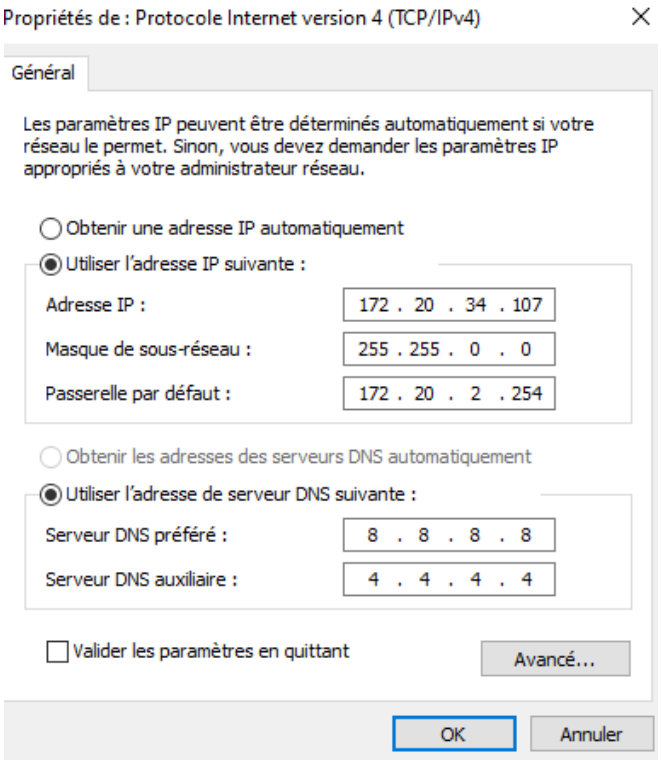


Dans l'infrastructure nous avons rajouter un PC « PC DE TEST DNS », en 172.20.34.107 il va nous permettre de tester la résolution de nom. Cependant nous passerons par la passerelle du routeur pour aller sur les sites web donc penser à mettre dans vos DNS, l'ip de du serveur iis.

6 – Sixième étape : Tester la résolution de nom sur un poste client

Pour pouvoir tester notre infrastructure nous allons mettre notre « PC DE TEST DNS », en 172.20.34.107 :

➔



Ensuite vous devez faire des règles iptables pour faire des redirections :

➔ sudo iptables -t nat -A POSTROUTING -p tcp –dport 8081 -i enp0s25 -j DNAT --to 172.40.1.1 :80

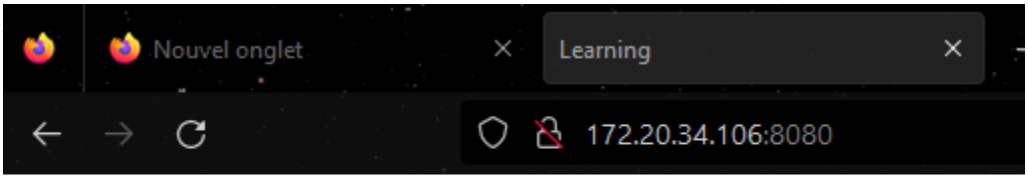
➔ sudo iptables -t nat -A POSTROUTING -p tcp –dport 8081 -i enp0s25 -j DNAT --to 172.40.1.2 :80

6 – Sixième étape : Tester la résolution de nom sur un poste client

Enfin vous pouvez tenter de vous connecter avec l'ip de votre routeur linux, donc :

- http://172.20.34.16:8080
- http://172.20.34.16:8081

Exemple :



LEARNING WEB

Actuellement pouvez-vous connecter à votre site avec l'ip 172.20.34.106 et les ports 8080 et 8081, cependant nous voulons pouvoir y accéder avec le nom de nos sites pour ce faire aller dans :

- `C:\Windows\System32\drivers\etc`

Une fois dans le dossier aller dans le fichier « hosts » et ajouter vos deux sites :

```
#
127.0.0.1 localhost
::1 localhost
172.20.34.106 web-learning.learning-tree.fr:8080
172.20.34.106 web-public.learning-tree.fr:8081
```

Editée par	Tom COELHO, Mathis BOUCHET	
Révisée par :	Tom COELHO, Mathis BOUCHET	
Suivie par :	Tom COELHO, Mathis BOUCHET	
Validée par :	Tom COELHO, Mathis BOUCHET	
Date : 03 / 01 / 2023	Saint Paul Bourdon Blanc	Version : 1