Amaury Chasline

BTS SIO1

Projet Learning Tree

Sommaire :

La mission :

- Learning Tree organisme international de formation a décidé de s'implanter à orléans en 2025 dans de nouveaux locaux sités Saint jean de Braye.

Le cabinet d'architectes SBEG a été désigné maître d'oeuvre pour la partie construction du bâtiment. Le plan des bâtiments est publié et confié à votre société de service sous forme de fichier autocad.

Elle fait appel à votre société de services pour la partie câblage, pour la configuration des éléments actifs (switch et routeur).

Le batiments vient juste d'être construit.

A savoir que Learning Tree s'est installé au rez-de-chaussée d'un batiments de 5 étages.

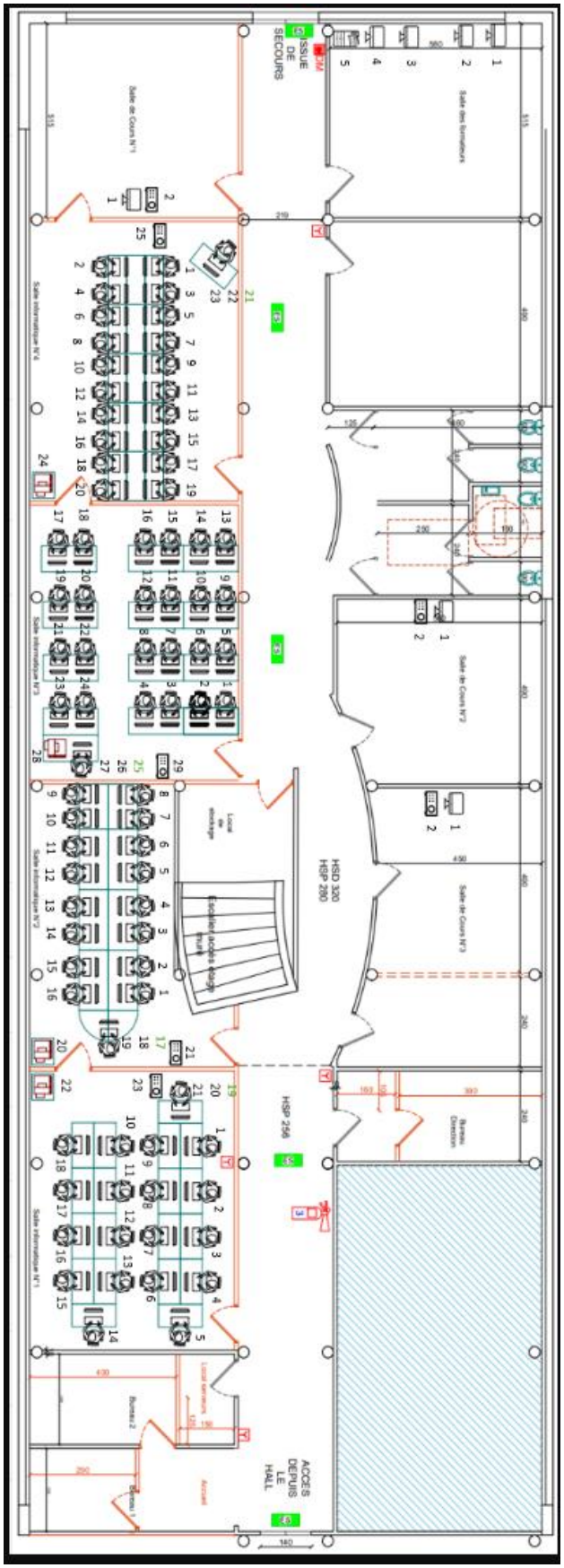
Sur les quatre autres étages, des entreprises ont installé leurs sièges.

Ces cinq entreprises se partagent donc un accès internet par fibre (1 gbit/s) afin de minimiser les coûts.

On fera d'autres missions:
- création de d'un câble
- Plan de réseau (adresse IP,nommage, etc ...)
- Sécuriter mise en place
- Réponse des question de cours !
- Installation et Configuration du commutateur CISCO 2960
-Configuration d'une machine Linux sous Debian
- Règle de filtrage

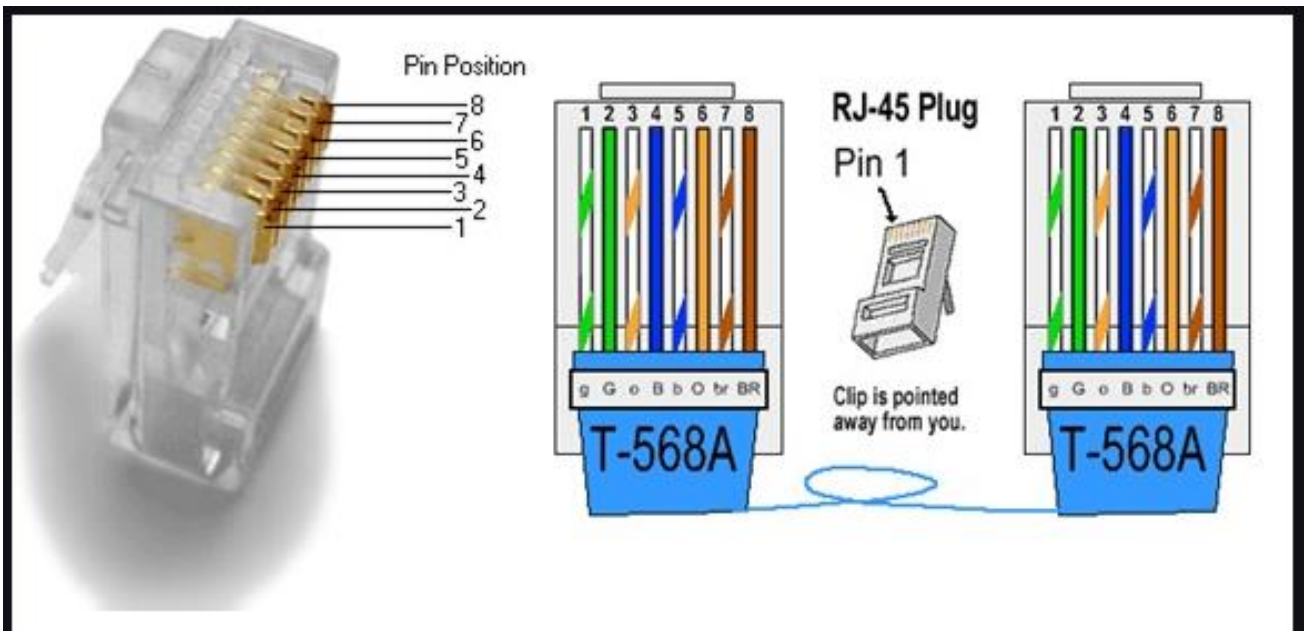
Voici le Plan de l’étage :

On peut voir dans ce schéma tous les port, PC, vidéo-projecteur, prise murale,



Création d’un câble de Brassage de catégorie EIA 568

Voici le schéma de câblage à réaliser + question de cours de 1-3 à 1-6 :



Le résultat afficher au micro scanner est :

1 2 3 4 5 6 7 8
| | | | | | | |
1 2 3 4 5 6 7 8

C’est un câble utilisé dans les réseaux informatiques pour connecter différents équipements actifs tels que des commutateurs, des routeurs, des serveurs et des panneaux de brassage. Son rôle principal est de relier ces équipements de manière à assurer la connectivité au sein du réseau.

Voici un exemple de prise murale à installer

Plan des adresses IP et nommage :

Plan D'adressage IP				
Salle	Matériel	Adresse Ip de début	Adresse Ip de fin	Explication plan d'adressage
Salle informatique n°1	Poste	172.21.1.1/16	172.21.1.20/16	PC= 172.21.X.Y (X= numéro de salle et Y= numéro de poste) ; vidéo projecteur (Y = 100) ; copieur (Y=101)
	Video Projecteur	172.21.1.100		
	Copieur	172.21.1.101		
Salle informatique n°2	Poste	172.21.2.1	172.21.2.18	PC= 172.21.X.Y (X= numéro de salle et Y= numéro de poste) ; vidéo projecteur (Y = 100) ; copieur (Y=101)
	Video Projecteur	172.21.2.100		
	Copieur	172.21.2.101		
Salle informatique n°3	Poste	172.21.3.1	172.21.3.26	PC= 172.21.X.Y (X= numéro de salle et Y= numéro de poste) ; vidéo projecteur (Y = 100) ; copieur (Y=101)
	Video Projecteur	172.21.3.100		
	Copieur	172.21.3.101		
Salle informatique n°4	Poste	172.21.4.1	172.21.4.22	PC= 172.21.X.Y (X= numéro de salle et Y= numéro de poste) ; vidéo projecteur (Y = 100) ; copieur (Y=101)
	Video Projecteur	172.21.4.100		
	Copieur	172.21.4.101		
Salle de Cour n°1	Poste	172.21.11.1		PC=172.21.X.Y(X = numéro de salle + 10 et Y = numéro de poste) ; vidéo projecteur (Y= 100)
	Video Projecteur	172.21.11.100		
Salle de Cour n°2	Poste	172.21.12.1		PC=172.21.X.Y(X = numéro de salle + 10 et Y = numéro de poste) ; vidéo projecteur (Y= 100)
	Video Projecteur	172.21.12.100		
Salle de Cour n°3	Poste	172.21.13.1		PC=172.21.X.Y(X = numéro de salle + 10 et Y = numéro de poste) ; vidéo projecteur (Y= 100)
	Video Projecteur	172.21.13.100		
Salle de Cour n°4	Poste	172.21.14.1		PC=172.21.X.Y(X = numéro de salle + 10 et Y = numéro de poste) ; vidéo projecteur (Y= 100)
	Video Projecteur	172.21.14.100		
Salle des Formateurs	Poste	172.21.20.1	172.21.20.5	PC=172.21.X.Y(X = numéro de alle formateur +20 et Y= numéro de Poste) ; Copieur(Y = 101)
	Copieur	172.21.14.101		

Plan De Nommage				
Salle	Matériel	Premier	Dernier	Explication plan de nommage
Salle informatique n°1	Poste	SI01PC01	SI01PC20	SI.X.Y.Z (SI = salle informatique ; X = Numéro de salle ; Y = type d'équipement ; Z = numéro d'équipement)
	Video Projecteur	SI01VP01		
	Copieur	SI01CP01		
Salle informatique n°2	Poste	SI02PC01	SI02PC18	SI.X.Y.Z (SI = salle informatique ; X = Numéro de salle ; Y = type d'équipement ; Z = numéro d'équipement)
	Video Projecteur	SI02VP01		
	Copieur	SI02CP01		
Salle informatique n°3	Poste	SI03PC01	SI03PC26	SI.X.Y.Z (SI = salle informatique ; X = Numéro de salle ; Y = type d'équipement ; Z = numéro d'équipement)
	Video Projecteur	SI03VP01		
	Copieur	SI03CP01		
Salle informatique n°4	Poste	SI04PC01	SI04PC22	SI.X.Y.Z (SI = salle informatique ; X = Numéro de salle ; Y = type d'équipement ; Z = numéro d'équipement)
	Video Projecteur	SI04VP01		
	Copieur	SI04CP01		
Salle de Cour n°1	Poste	SC01PC01		SC.X.Y.Z (SC = Salle de cour ; X = numéro de salle , Y = type d'équipement ; Z = numéro d'équipement)
	Video Projecteur	SC01VP01		
Salle de Cour n°2	Poste	SC02PC01		SC.X.Y.Z (SC = Salle de cour ; X = numéro de salle , Y = type d'équipement ; Z = numéro d'équipement)
	Video Projecteur	SC02PC01		
Salle de Cour n°3	Poste	SC02PC01		SC.X.Y.Z (SC = Salle de cour ; X = numéro de salle , Y = type d'équipement ; Z = numéro d'équipement)
	Video Projecteur	SC02VP01		
Salle de Cour n°4	Poste	SC03PC01		SC.X.Y.Z (SC = Salle de cour ; X = numéro de salle , Y = type d'équipement ; Z = numéro d'équipement)
	Video Projecteur	SC03VP01		
Salle des Formateurs	Poste	SF01PC01	SF01PC05	SF.X.Y.Z (SF = Salle Formateur ; X = numéro de salle ; Y= type d'équipement ; Z = numéro d'équipement
	Copieur	SF01CP01		

Réponse au questions de cours

Question de cours 1-1 ?

Total Câble

	M de câble par salle	Total
salle des formateurs	292,7	
salle cours N°1	172	
salle cours N°2	109	
salle cours N°3	106	
salle cours info N°1	389	
salle cours info N°2	640	
salle cours info N°3	864	
salle cours info N°4	906	
		3479 m

Question de cours 1-2 ?

- cable de brassage
- baie de brassage de 24U

Question de cours 1-3 ?

La norme à respecter est celle TIA/EIA-568 et ISO/IEC 11801.

Question de cours 2-1 ?

Nom hôte du commutateur : COM1 Mot de passe Telnet : LearningTREE
Adresse IP : 172.20.0.0
Masque de sous-réseau : /16
Mot de passe Administrateur : LearningTREE

Question de cours 2-2 ?
(Le switch étant neuf et n'ayant aucune adresse IP par défaut, proposer un type de liaison et une application à s'installer sur votre poste de travail pour le configurer)

Type de liaison : Série

Application installée : Tera Term

Question de cours 2-3 ?
Voir PAGE 18 pour routage -intervlan

Question de cours 2-4 ?
(Quelle norme doit respecter le commutateur cisco 2960 afin de véhiculer des trames taggées sur le port 24 ?)

Norme attendue : IEEE 802.1aq

Nombres de VLANS : 3

Nom des vlans :	Numéro :
- vlan 10	- 10
- vlan 20	- 20
- vlan 30	- 30

Question de cours 2-5 ?

Plan de Nomage pour salle informatique 4

Numéro de Port	Numéro du Vlan	NOM du Vlan	Débit du port	Sécurité ?	Particularité
1	1	MANAGEMENT			prof
2	10	Vlan 10	1Gitb/s		Élève
3	10	Vlan 10	1Gitb/s		Élève
4	10	Vlan 10	1Gitb/s		Élève
5	10	Vlan 10	1Gitb/s		Élève
6	10	Vlan 10	1Gitb/s		Élève
7	10	Vlan 10	1Gitb/s		Élève
8	10	Vlan 10	1Gitb/s		Élève
9	10	Vlan 10	1Gitb/s		Élève
10	10	Vlan 10	1Gitb/s		Élève
11	10	Vlan 10	1Gitb/s		Élève
12	10	Vlan 10	1Gitb/s		Élève
13	10	Vlan 10	1Gitb/s		Élève
14	10	Vlan 10	1Gitb/s		Élève
15	10	Vlan 10	1Gitb/s		Élève
16	10	Vlan 10	1Gitb/s		Élève
17	10	Vlan 10	1Gitb/s		Élève
18	10	Vlan 10	1Gitb/s		Élève
19	10	Vlan 10	1Gitb/s		Élève
20	10	Vlan 10	1Gitb/s		Élève
21	20	Vlan 20	1Gitb/s		TEL IP
22	20	Vlan 20	1Gitb/s		TEL IP
23	20	Vlan 20	1Gitb/s		TEL IP
24			10 Gbit/s		LIAISON

Les ports 1, 21, 22, 23 et 24, ont des types particuliers de fonctionnement.
Le port 1 est réservé au management du switch isolé dans un vlan nommé «MANAGEMENT».
Les ports 2 à 20 sont réservé aux PC, imprimantes et vidéo-projecteur.
Les ports 21, 22, 23 sont réservé au téléphones IP.
Le port 24 est utilisé pour la liaison avec le commutateur HP (cœur du réseau).

Question de cours 2-6 ?
PAGE 11 à 17
Question de cours 2-7 ?

- Test 1 : test de bande passante
- Test 2 :

Question de cours 2-8 ?

(Sauvegarde la configuration du switch sur un serveur tftp que vous aurez téléchargeé et paramétré sur votre poste de travail)

Question de cours 2-9 ?

Rappeler la définition de tftp : Trivial Transfer Protocol

Quelle est l'adresse ip du serveur tftp ?

Le port d'écoute : 10

La nature du port (tcp ou udp) : UDP

Quel est l'hôte qui est considéré comme client ?PC

Quel est l'hôte qui est considéré comme serveur ?

Est-ce une opération type «upload» ou «download» ? justifier

Quelle est la taille du fichier de sauvegarde en octets ou kilo octets : 3,50 Ko (3 584 octets)

Connexion et Restauration du switch 2960

Connexion :

La première étape consiste à se connecter au switch avec un câble console puis brancher le bout RJ45 au ports et le VGA au PC.

Voici à quoi ressemble un câble console :

Pour vérifier que le PC détecte bien le commutateurs, il faut aller dans le «gestionnaire des périphériques».

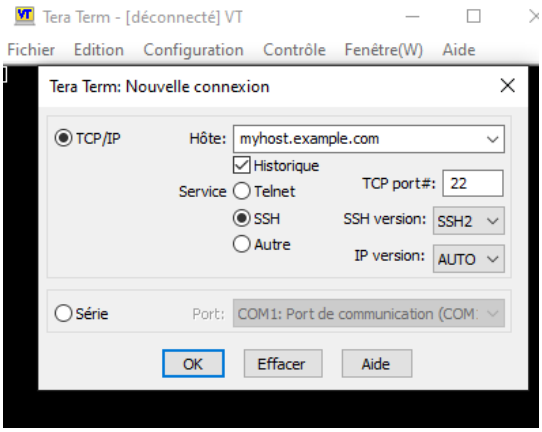
Normalement cette image doit apparaître.

Ports (COM et LPT)

La deuxième étape est le lancement d'application pour paramétré le commutateurs. Nous allons utiliser applications Tera Term.

Le lien de téléchargement : https://github.com/TeraTermProject/teraterm/releases

Après avoir lancer applications et que le câblage soit réussit cet image doit apparaittre

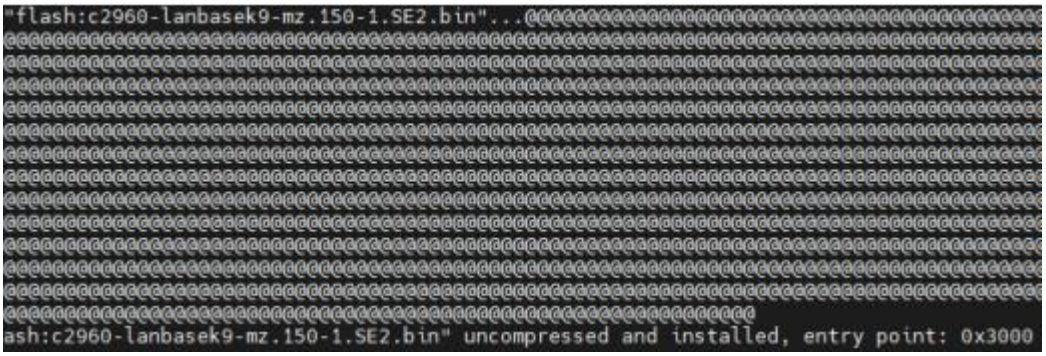


Pour réussir notre connexion, on va cliquer sur le mode «série».

La troisième étape consiste à avoir un affichage du commutateur à l'écran.
Après la configuration de connexion, vous devez appuyer sur le bouton « MODE » sur la façade avant, maintenir la pression enfoncée. Des DELS de lumière devraient s'allumer à clignoter, on maintient toujours la pression jusqu'a une interaction se passe à l'écran. (Temps générale environ 10 ou 15 seconde)

Voici le bouton à appuyer.

Si il se passe cet image, cela montre que le switch est en train de se réinitialiser.



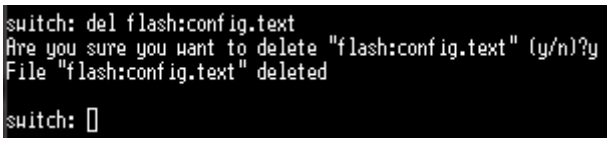
La quatrième étape va consister à la configuration à faire lorsqu'on a un nouveau équipement cisco.
Connexion faites alors taper les commandes **«write erase»** qui permet de supprimer la configuration d'avant.
La commande **«delete flash:vlan.dat»** est utilisée sur les équipements Cisco pour supprimer le fichier de configuration des VLAN enregistré dans la mémoire flash du périphérique.
Commande pour redémarrer le switch **«reload»**.

Restauration :

La première étape consiste à utiliser la commande «flash_init» c'est utilisée pour initialiser et préparer la mémoire flash.

La deuxième étape est d'afficher les fichiers du switch à utiliser et à paramétré.
Commande «dir flash» :

La troisième étape est de supprimer les dossier **«config.text»** et **«vlan.dat»**, nous avons aussi vue comment les supprimer avant vers la page 11 mais je présente une nouvel solutions !
Commande de suppression :
«del flash:config.tex» «delete flash:vlan.dat»



La quatrième étape parle de rédémarer le système.
Commande «BOOT»

Création d'un serveur TFTP pour la sauvegarde de configuration et port mirroning/Telnet

Configuration sauvegarde :

La première étape consista à la configuration.

Lien de téléchargement pour le serveur TFTP : https://bitbucket.org/phjounin/tftpd64/downloads/

Quand le téléchargement est fini, lancer l'application.

Logo à cliquer :

Plusieurs paramètres doit s'afficher devant à l'écran.

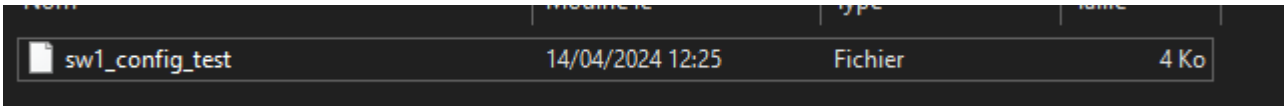
Le **«Base Directory»** va permettre de définir l'endroit ou on va sauvegarder la configuration.

{C:\Users\amaury\Documents\ProjetMouchard\sauvegarde tftp }

Le **«TFTP security»** montre le niveau de sécuriter à appliquer au switch.

La deuxième étape concerne son utilisation de sa sauvegarde avec des test !

Pour faire une sauvegarde il faut de configuration taper la commande **«copy running-config tftp»**.



La troisième étape consiste à tester notre sauvegarde.

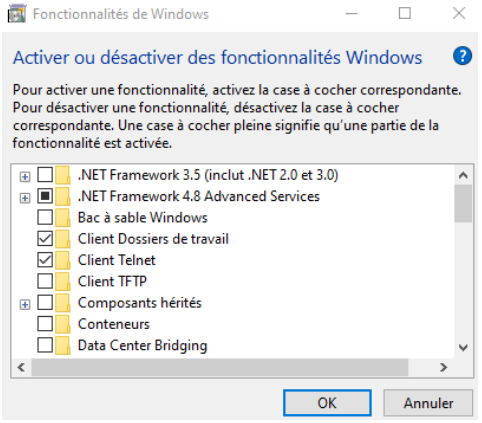
Taper la commande : **«copy tftp: runing-config»**

Aller dans le dossier config et faire des test pour savoir si la sauvegarde marche.

Normalement NON car il manque quelque config à faire !!

La quatrième étape consiste à faire d'autres configuration sur TFTP pour le switch.

- L'attribution d'un Vlan des (l'interface vlan 1)
- Définir une configuration IP qui correspond au réseau avec la commande : **«ip address <adresse-IP> <masque-de-sous-réseaux»**
- Création d'un utilisateurs avec la commande : **«username <nom-utilisateur> password <mot-de-passe>»**
- Configuration de la ligne VTY avec la commande : **«line vty 0 4»**
- activation du Telenet sur le PC windows (hosts) (image pour config du telnet sur windows)



Tester de nouveaux la sauvegarde avec des testes !!!

Création du serveur TFTP :

La configuration de base d'un serveur comme cela est installation de paquets, changement de noms et mettre à l'heure la machine.

La première étape consiste à changer le nom de la machine, cela se passe dans 2 fichiers de configuration (hostname et hosts).
Commande pour accéder au fichier :
« nano /etc/hostname»
« nano /etc/hosts»

La deuxième étape est l'installation de mise à jour du systèmes avec les commandes : **« apt upgrade & apt update»**.

La troisième étape consiste à mettre sa machine à l'heure ce qui est très importants pour la suite !!!
Installation du paquet NTP avec la commande : **«apt install ntpsec»**.

La quatrième étape parle d'installation du serveur tftp.
La commande est : **«apt-get install tftpd-hpa»**

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

La cinquième étape explique la configuration du serveur tftp.
Les principales configuration se passe dans dossier accessible avec la commande : **«nano /etc/default/tftpd-hpa»**.

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

```
TFTP_USERNAME="
TFTP_DIRECTORY
TFTP_ADDRESS="
TFTP_OPTIONS="
```

TFTP_USERNAME : exprime le nom de l'utilisateur avec lequel le serveur tftp s'exécute.
TFTP_DIRECTORY : répertoire racine pour le serveur TFTP.
TFTP_ADDRESS : adresse IP et le ports sur lequels le serveur écoute les connexions.
TFTP_OPTIONS : permet de mettre des options supplémentaires pour le serveur TFTP (ex : --secure).

La sixième étape consiste à créer un répertoire TFTP.
On va créer un répertoire pour spécifié comme (TFTP_DIRECTORY) la configuration.
Commande : **«mkdir -p /serv/tftp»**

La septième étape consiste à redémarrer le service après avoir apporter les modifications.
Commande : «systemctl restart tftpd-hpa»

```
:/home/sio# systemctl restart tftpd-hpa
```

Port Mirroring :

C’est quoi le port mirroring ?
Ce port mirroring est une fonctionnalité essentielle des commutateurs réseau qui permet de surveiller et d'analyser le trafic réseau à des fins de diagnostic, de sécurité et de gestion du réseau.

La première étape est la configuration du port.
Commande pour affectation à un port :
«interface GigabitEthernet 0/10»
«switchport mode access»
«exit»

La deuxième étape parle du port destination.
On configure le port source du mirroing. Monitor session 1 destination interface FastEthernet0/10 encapsulation replicate.

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

La troisième étape consiste à la vérification du ports source du mirroring qui doit être de GIG0/1.
Commande : «monitor session 1 sources interfaces gigabitethernet 0/1»

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

Telnet :

C’est quoi le telnet ?
Telnet est un protocole de communication utilisé pour établir des sessions interactives à distance sur un réseau informatique, mais il est considéré comme étant non sécurisé en raison de la transmission de données en texte clair.

La première étape consiste à le configurer le switch avec un utilisateurs.
Listes des commandes de configuration.

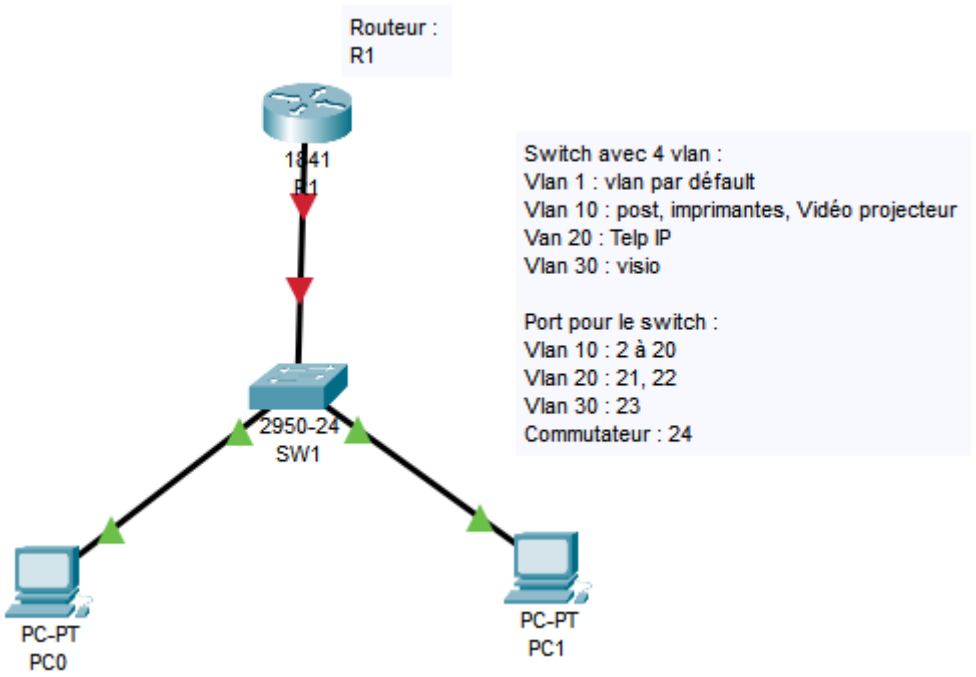
«conf t»
«username <noms> password <mot de passe>»
«interface vlan 1»
«ip address 172.20.37.100 255.255.0.0» (donner une adresse IP en rapport avec votre réseau)
«exit»
«line vty 0 4»
«login local»
«exit»

La deuxième étape parle d’une connexion au service telnet.
La configuration terminé, on va aller dans le «CMD» du PC pour taper la commande : «telnet <ip addresse de l’interface>»+ identifiants créer, tous cela permettra la connexion.

Pour récupérer le mot de passe, on utilise un outil qui s’appelle (Wireshark).
Nous allons connecter un autre PC au port 10 (port qu’on a mis en mirroring) avec le port 1.
On va pouvoir analyser se qu’il se passe lorsqu’on se connecte au telnet avec le PC sur le port 1, le mot de passe telnet du pc sur le port 10, on va pouvoir le voir.

Routage inter-vlan

Schéma :



C'est quoi ?
Le routage inter-VLAN est essentiel pour les réseaux d'entreprise où la segmentation du trafic est nécessaire pour des raisons de sécurité, de gestion du trafic et de performance du réseau.

La première étape était de faire un schéma simple et compréhensible !

La deuxième étape consiste à dire quel adresse IP qu'on va utiliser.
«172.21.254.254 /16» pour les interfaces du vlan 10
«172.22.254.254 /16» pour les interfaces du vlan 20
«172.30.254.254 /16» pour les interfaces du vlan 30
Exemple le PC1 aura 172.21.1.1 /16 dans le vlan 10 !

La troisième étape, c'est de créer les vlan dans le switch.
Voici le commandes à taper :

«vlan 10»
«name vlan10»
«exit»
«vlan 20»
«name vlan20»
«exit»
«vlan 30»
«name vlan30»
«exit»

La quatrième étape, c'est d'assigner des ports au vlan.
Voici le commandes à taper :

```
«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»
```

La cinquième étape, c'est de mettre des lien trunk.
C'est quoi ?
Un lien trunk est une connexion réseau qui transporte le trafic de plusieurs VLANs sur un seul lien physique, permettant ainsi une meilleure utilisation de la bande passante et une segmentation efficace du trafic réseau.
On configure le mode trunk sur le port 24 du switch car celui qui s'occupe des liaison entre réseaux.
Voici le commandes à taper :

```
«interface GigabiEthernet 24»
«switchport mode trunk»
«switchport trunk allowed vlan 10,20,30
«no shutdown»
«exit»
```

La sixième étape consiste à configurer le routeur, pour cela on devra créer des interfaces.
C'est utilisée pour configurer l'encapsulation IEEE 802.1Q sur une sous-interface d'un routeur ou d'un commutateur multilayer Cisco, afin de router le trafic entre le VLAN spécifié et les autres VLANs du réseau.

«enabe»l
«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»

La septième étape est d'activer le routage.
Après avoir faits les interfaces virtuelles, utiliser la commande «ip routing» pour activer le routage.
Les PC devraient pouvoir ping entre les différents Vlan.

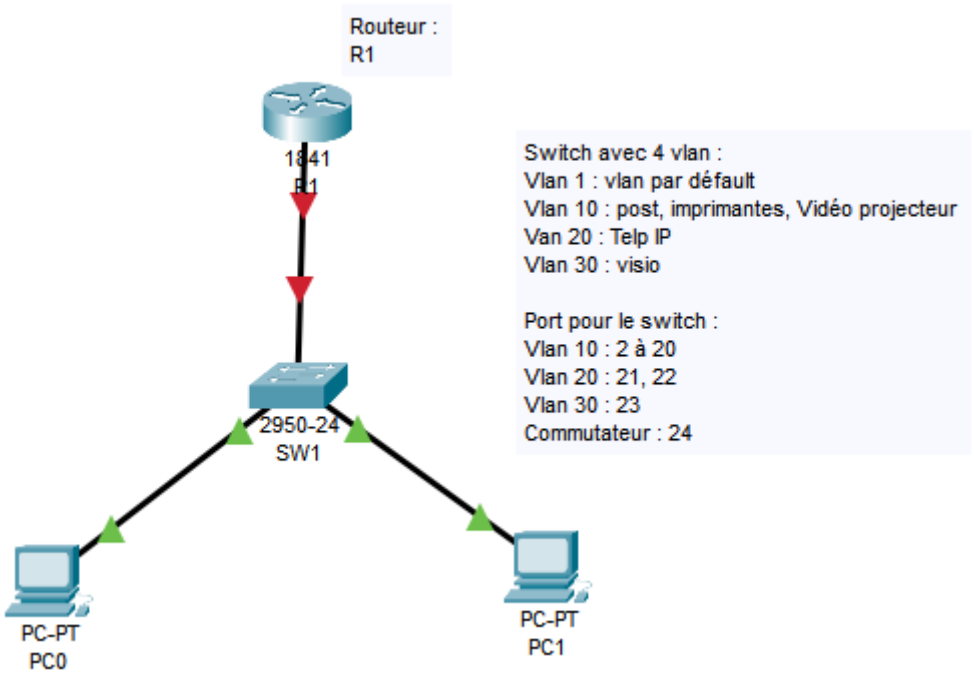
```
C:\Users\sio1>ping 172.22.1.1

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
```

Routeur sous linux

Routeur avec une machine linux :



On reprends le même schéma réseau et les mêmes adresses IP sauf qu'on rajoute une plage IP pour un téléphone.
Plage (172.30.1.1 à 172.30.1.2)
On remplace le routeur CISCO par un routeur sous linux qui donnera l'internet au PC en passant par le routeur de la salle.

La première étape est d'installé linux, il faudra installer VENTOY sur clé USB puis la formater après trouver un ISO de debian 12 avec l'interface gnome.
Téléchargement VENTOY : https://www.ventoy.net/en/download.html
Téléchargement iso debian 12: https://www.debian.org/download

Voici à quoi devrait ressembler DEBIAN dans la clé USB.

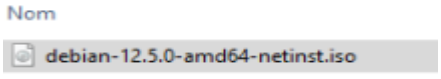
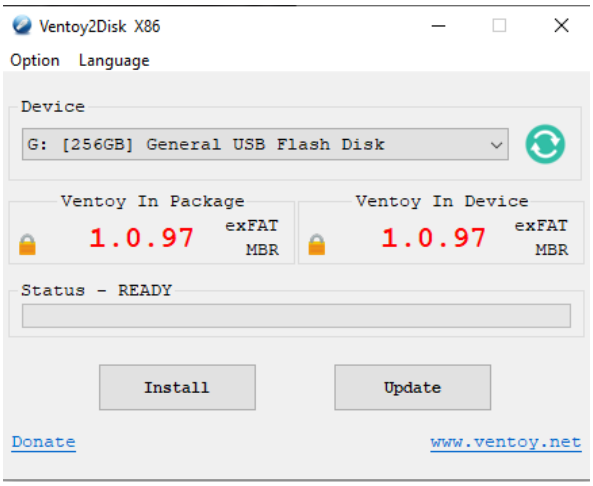


Image du téléchargement :



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

La deuxième étape, c'est de configurer les 3 cartes réseaux du serveur :

--> enp0s3

--> enp0s8

--> enp0s25

La carte réseau enp0s3 sera pour les interfaces des vlan et la carte réseau enp0s25 sera celle qui fera les liaison entre le routeur de la salle à notre carte réseaux enp0s3.

Aller dans le fichier «nano /etc/network/interfaces»

Ce fichier permet de configurer l'identiter réseaux du PC sous linux.

```
#Configuration de la carte réseau enp0s25
auto enp0s25
iface enp0s25 inet static
        address 172.20.37.100
        netmask 255.255.0.0
        gateway 172.20.2.254
```

Configuration IP pour les vlan.

```
#Configuration des interface virtuelle
auto enp0s3
iface enp0s3 inet manual
        ip link add enp0s3 name enp0s3.10 type vlan id 10
        ip link add enp0s3 name enp0s3.20 type vlan id 20
        ip link add enp0s3 name enp0s3.30 type vlan id 30
auto enp0s3.10
#vlan 10
iface enp0s3.10 inet static
        address 172.21.254.254
        netmask 255.255.0.0
#vlan 20
iface enp0s3.20 inet static
        address 172.22.254.254
        netmask 255.255.0.0
#vlan 30
iface enp0s3.30 inet static
        address 172.30.254.254
        netmask 255.255.0.0
```

Faire des ping entre PC pour voir si la connexion entre les deux postes est possibles.

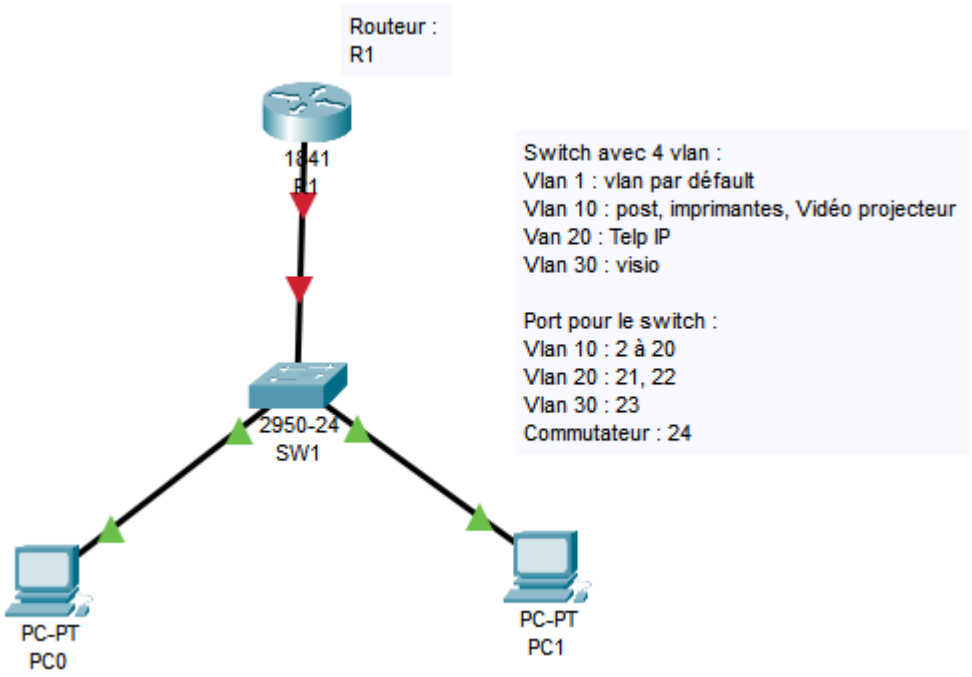
La troisième étape, consiste à activer le NAT.
C'est quoi le NAT ?
C'est une technique importante utilisée dans les réseaux informatiques pour permettre à plusieurs dispositifs de partager une seule adresse IP publique ou pour masquer les adresses IP privées derrière une adresse IP publique lors de la communication sur Internet.
La commande à taper sur linux :
« sudo iptables -t nat -A POSTROUTING -o enp0s25 -j MASQUERADE»

La quatrième étape est d'activer le routage.
Commande à taper :
«ip routing»

Et activer le forwarding :
C'est quoi ?
C'est le processus par lequel les périphériques réseau transfèrent les paquets de données d'une interface réseau vers une autre en fonction de l'adresse de destination des paquets.
Commande à taper :
«systl -w net. ipv4.ip_forward = 1»

On utilise ça pour un système Linux en changeant la valeur de (net.ipv4.ip_forwar net.ipv4.ip_forward) à 1, permettant ainsi au système de router les paquets IP entre différentes interfaces réseau.

Règle de filtrage



Dans notre infrastructure, nous souhaitons que seul notre PC1 ait accès au SSH du routeur, et non les autres postes.
On veut que notre PC sort sur internet, mais qu'il ne soit pas possible de rentrer dans le réseau.
Exemple : Notre routeur en 172.20.37.107 peux ping le 172.20.37.13 mais le 172.20.37.13 ne doit pas pouvoir ping le 172.20.37.107

La première étape consiste à faire du filtrage au niveau du SSH.
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»
```

La deuxième étape explique la sauvegarde des règles iptables.

Commande : «sudo iptables-save > regles.txt»

La troisième étape parle du filtrage à faire sur internet.
Commande à taper :

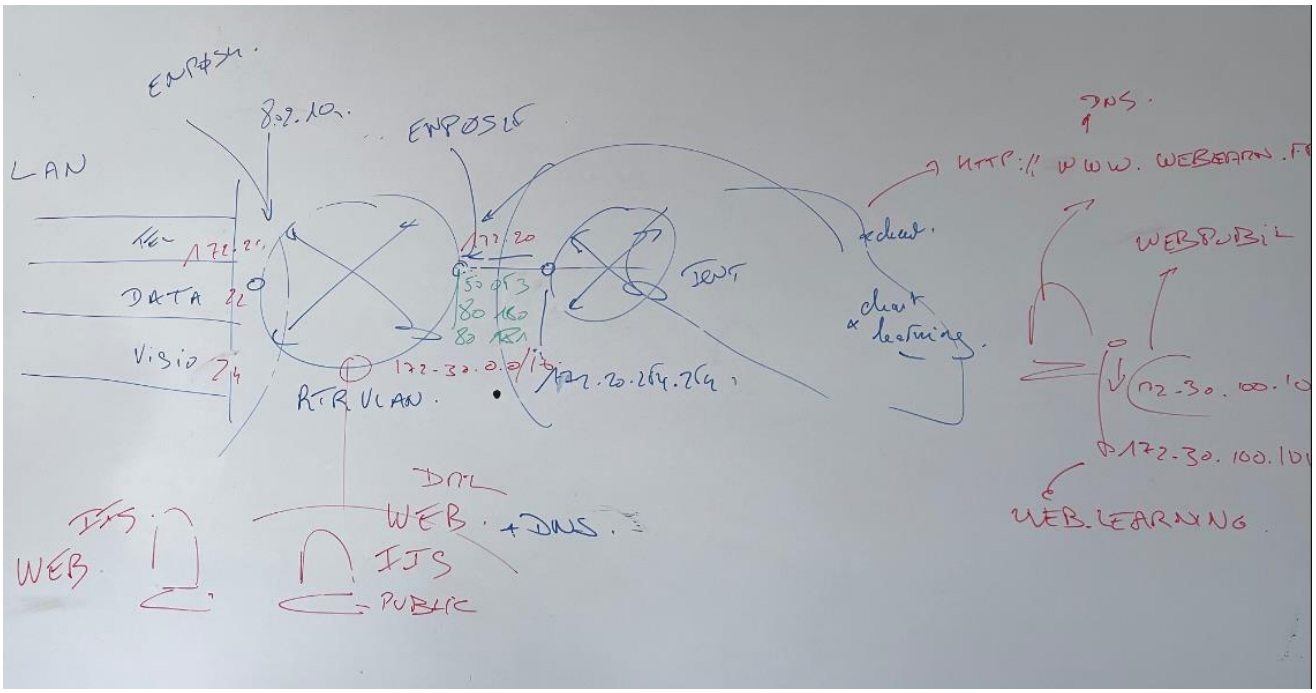
```
# Autorise le trafic réseaux vers Internet pour les VLAN (vlan 10, 20, 30)
sudo iptables -A FORWARD -s 172.21.0.0/16 -o enp0s25 -m state --state NEW,ESTABLISHED -j ACCEPT
sudo iptables -A FORWARD -s 172.22.0.0/16 -o enp0s25 -m state --state NEW,ESTABLISHED -j ACCEPT
sudo iptables -A FORWARD -s 172.30.0.0/16 -o enp0s25 -m state --state NEW,ESTABLISHED -j ACCEPT

# Autorise les réponses d'Internet vers les VLAN (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
```

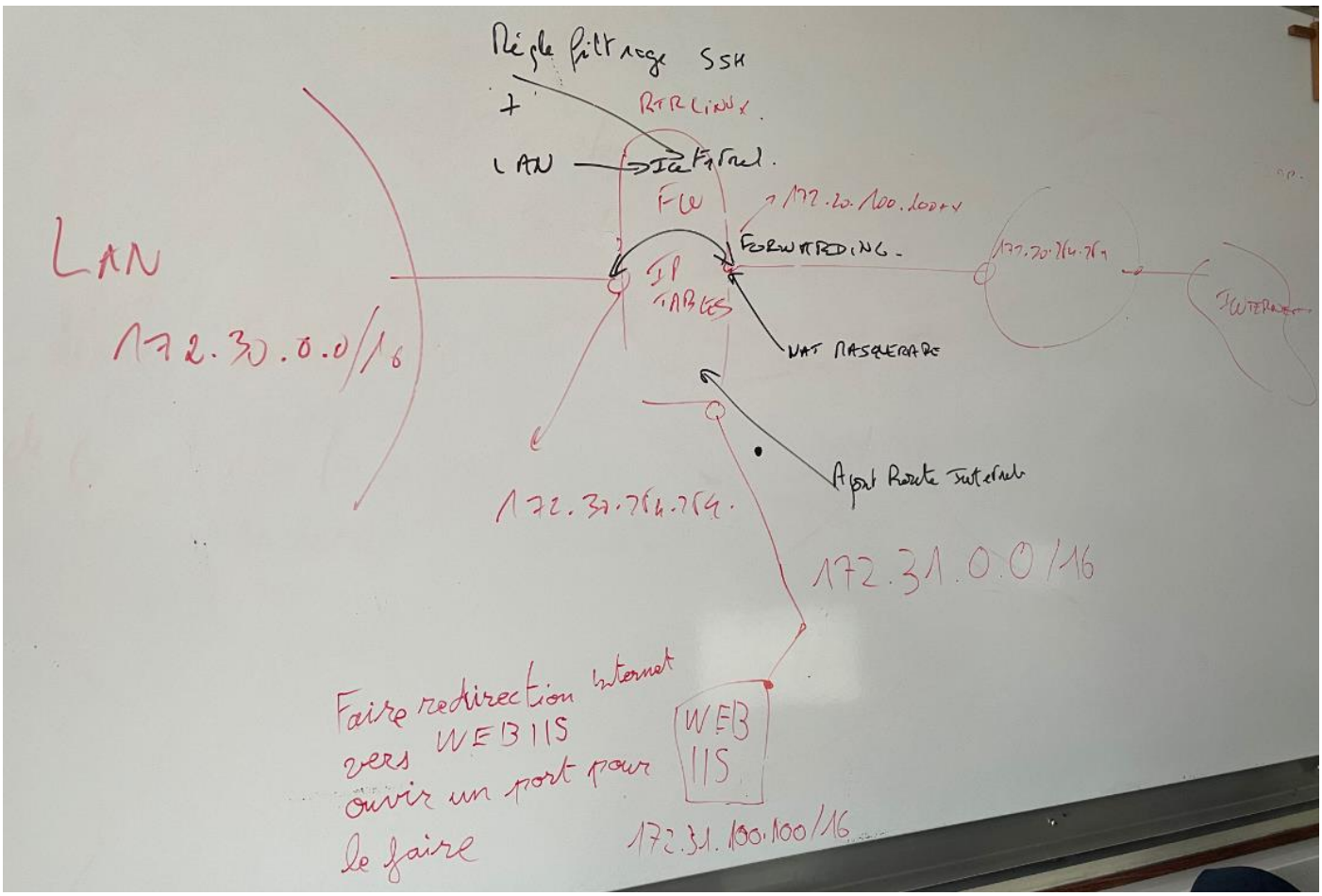
Annexes

Routeur utiliser pour le TP :

Switch utiliser pour le TP :



Règles de filtrages :



Filtrages Réseau :

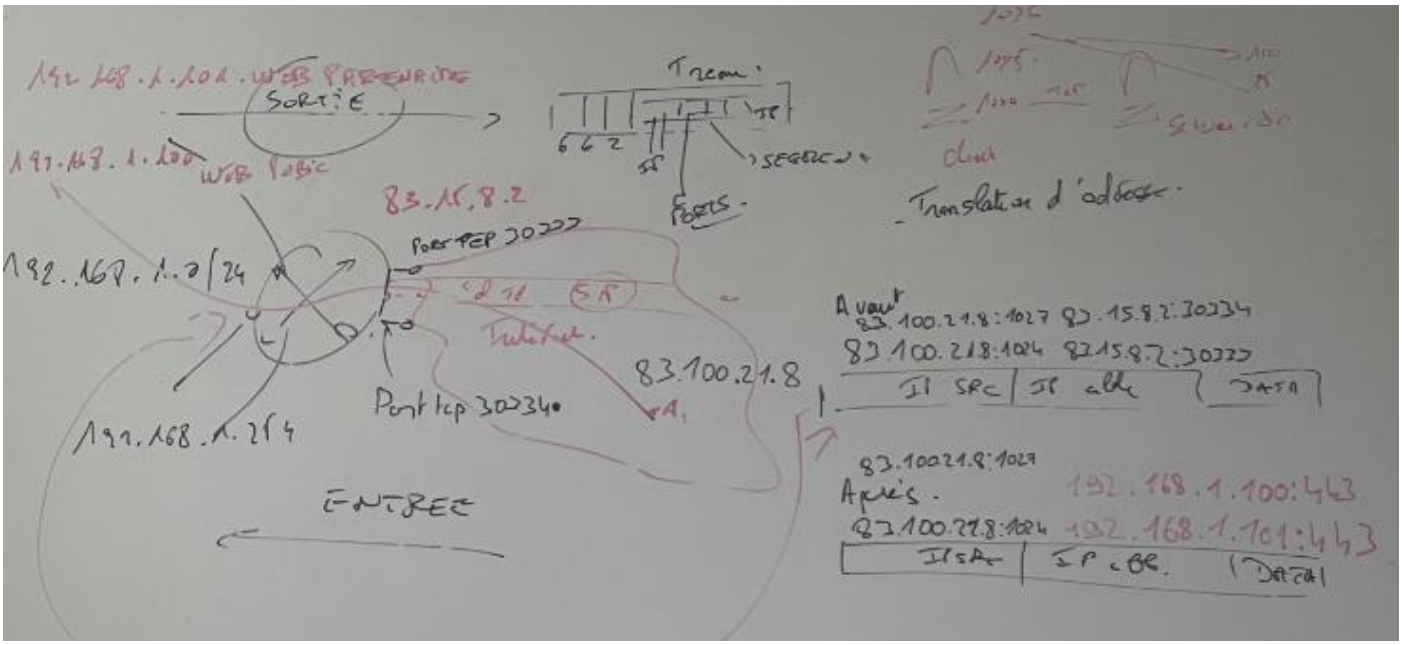
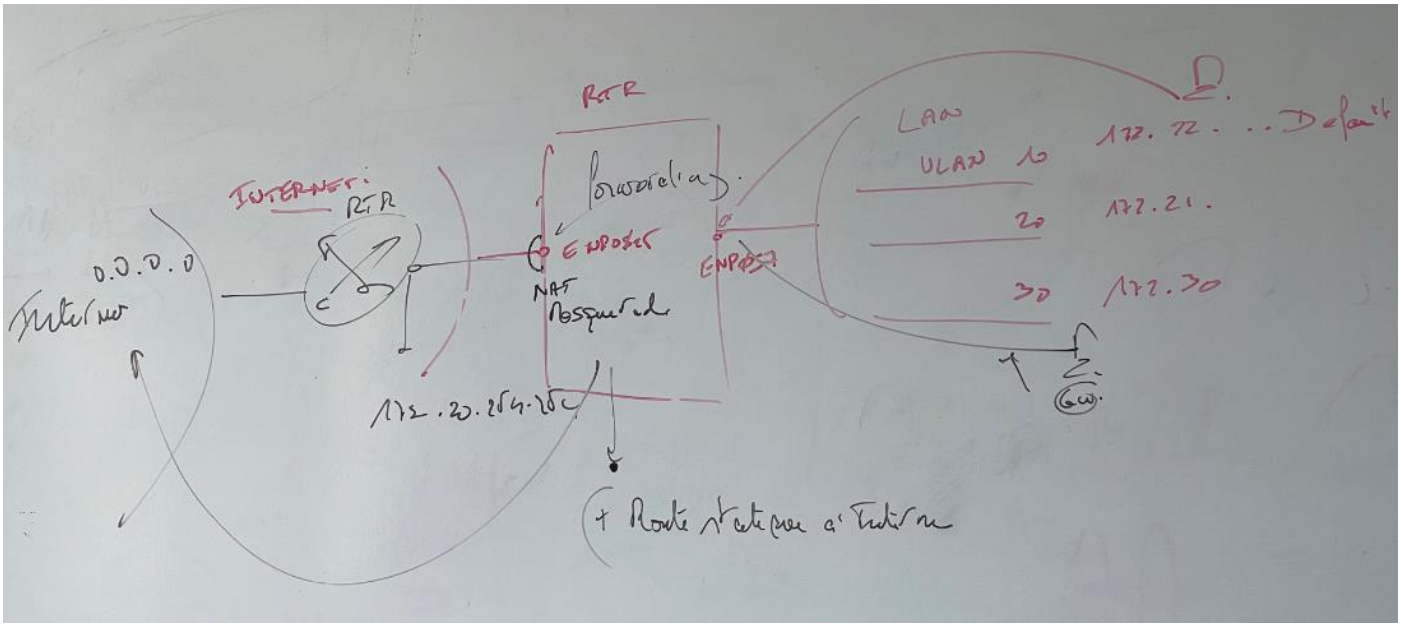
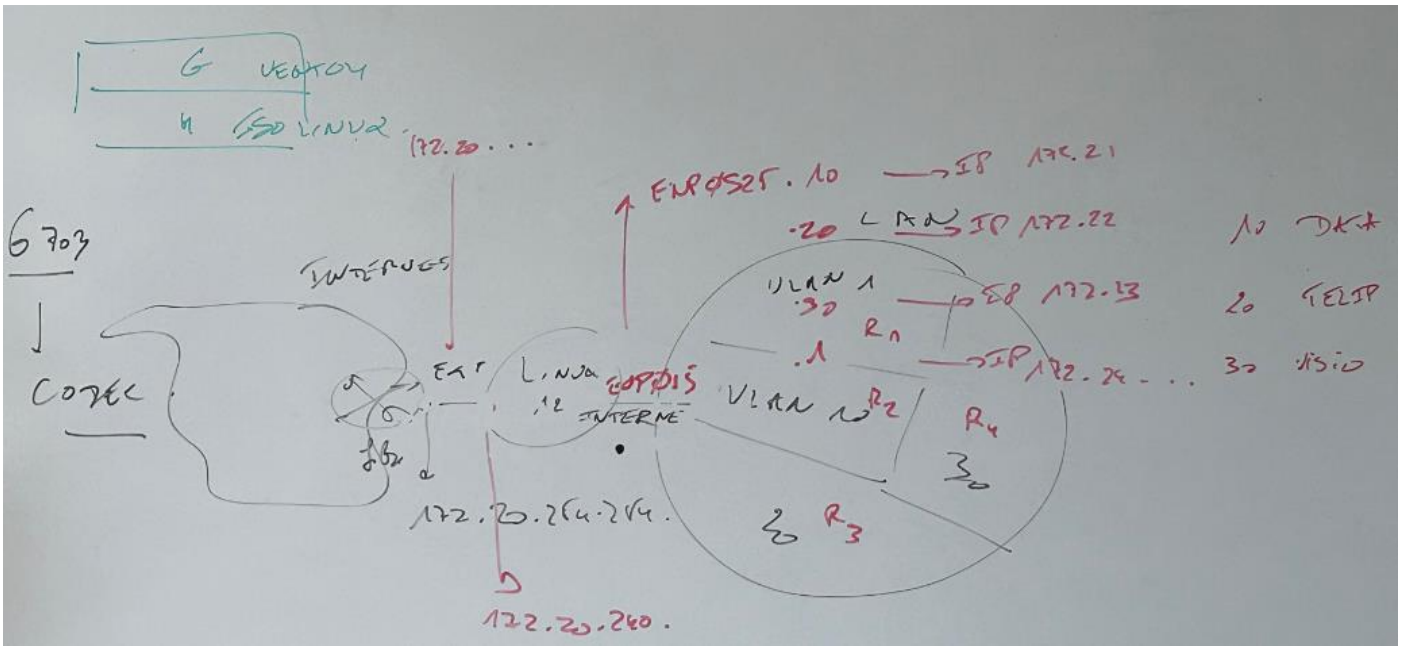


Schéma réseau :





FIN