

# Compte Rendu SAE 12

## • Analyse de la Trame Ethernet

Trame 33 analyse :

4 3.494191 Cisco\_78:e7:81 CDP/VTP/DTP/PagP/UD... CDP 456 Device ID: S2.reseau.local Port ID: FastEthernet0/1

0000	01 00 0c cc cc cc 00 19 aa 78 e7 81 01 ba aa aa	.....x.....
0010	03 00 00 0c 20 00 02 b4 b4 d9 00 01 00 13 53 32	.....S2
0020	2e 72 65 73 65 61 75 2e 6c 6f 63 61 6c 00 05 00	.reseau. local...
0030	f8 43 69 73 63 6f 20 49 4f 53 20 53 6f 66 74 77	.Cisco I OS Softw
0040	61 72 65 2c 20 43 32 39 36 30 20 53 6f 66 74 77	are, C29 60 Softw
0050	61 72 65 20 28 43 32 39 36 30 2d 4c 41 4e 42 41	are (C29 60-LANBA
0060	53 45 4b 39 2d 4d 29 2c 20 56 65 72 73 69 6f 6e	SEK9-M), Version
0070	20 31 32 2e 32 28 35 38 29 53 45 32 2c 20 52 45	12.2(58 )SE2, RE
0080	4c 45 41 53 45 20 53 4f 46 54 57 41 52 45 20 28	LEASE SO FTWARE (
0090	66 63 31 29 0a 54 65 63 68 6e 69 63 61 6c 20 53	fc1) Tec hnical S
00a0	75 70 70 6f 72 74 3a 20 68 74 74 70 3a 2f 2f 77	upport: http://w
00b0	77 77 2e 63 69 73 63 6f 2e 63 6f 6d 2f 74 65 63	ww.cisco .com/tec
00c0	68 73 75 70 70 6f 72 74 0a 43 6f 70 79 72 69 67	hsupport Copyrig
00d0	68 74 20 28 63 29 20 31 39 38 36 2d 32 30 31 31	ht (c) 1 986-2011
00e0	20 62 79 20 43 69 73 63 6f 20 53 79 73 74 65 6d	by Cisc o System
00f0	73 2c 20 49 6e 63 2e 0a 43 6f 6d 70 69 6c 65 64	s, Inc.. Compiled
0100	20 54 68 75 20 32 31 2d 4a 75 6c 2d 31 31 20 30	Thu 21- Jul-11 0
0110	32 3a 31 33 20 62 79 20 70 72 6f 64 5f 72 65 6c	2:13 by prod_rel
0120	5f 74 65 61 6d 00 06 00 19 63 69 73 63 6f 20 57	_team... -cisco W
0130	53 2d 43 32 39 36 30 2d 32 34 54 54 2d 4c 00 02	S-C2960- 24TT-L..
0140	00 11 00 00 00 01 01 01 cc 00 04 c0 a8 0a fe 00	.....
0150	03 00 13 46 61 73 74 45 74 68 65 72 6e 65 74 30	...FastE thernet0
0160	2f 31 00 04 00 08 00 00 00 28 00 08 00 24 00 00	/1.....-(...\$..
0170	0c 01 12 00 00 00 00 ff ff ff ff 01 02 21 ff 00	.....!..
0180	00 00 00 00 00 00 19 aa 78 e7 80 ff 00 00 00 09	.....x.....
0190	00 04 00 0a 00 06 00 02 00 0b 00 05 01 00 12 00	.....
01a0	05 00 00 13 00 05 00 00 16 00 11 00 00 00 01 01	.....
01b0	01 cc 00 04 c0 a8 0a fe 00 1a 00 10 00 00 00 01	.....
01c0	00 00 00 00 ff ff ff ff	.....

→ nom du réseau local : S2.reseau.local

→ port ID : FA0/1

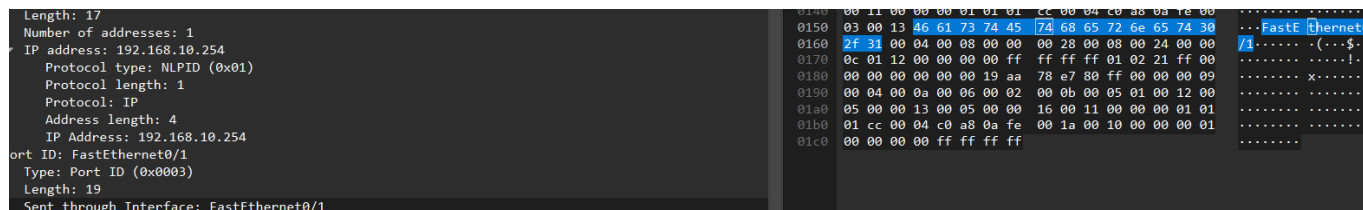
→ Vlan native : 2

Le nom du réseau local :

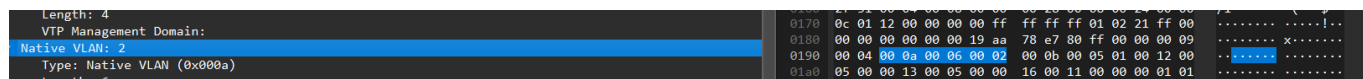
Checksum Status: Good]	0010 03 00 00 0c 20 00 02 b4 b4 d9 00 01 00 13 53 32	.....S2
Device ID: S2.reseau.local	0020 2e 72 65 73 65 61 75 2e 6c 6f 63 61 6c 00 05 00	.reseau. local...
Type: Device ID (0x0001)	0030 f8 43 69 73 63 6f 20 49 4f 53 20 53 6f 66 74 77	.Cisco I OS Softw
Length: 19	0040 61 72 65 2c 20 43 32 39 36 30 20 53 6f 66 74 77	are, C29 60 Softw
Device ID: S2.reseau.local	0050 61 72 65 20 28 43 32 39 36 30 2d 4c 41 4e 42 41	are (C29 60-LANBA
	0060 53 45 4b 39 2d 4d 29 2c 20 56 65 72 73 69 6f 6e	SEK9-M), Version

# IZAK ALI

Le port ID :



Vlan native :



Voici ma démarche pour avoir trouvé toutes ces informations.

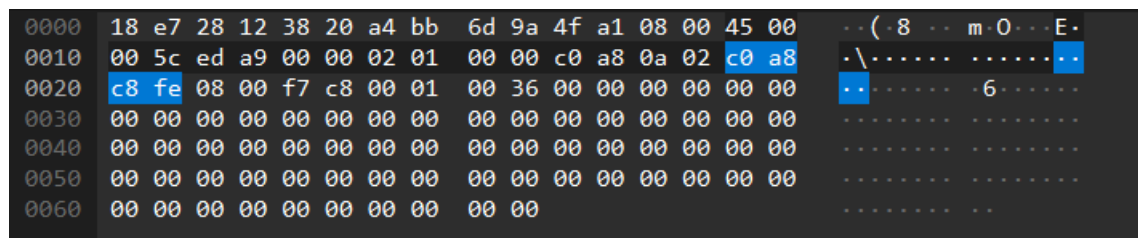
Chez Wireshark nous remarquons les points suivants :

- Le paquet va d'abord de la source 192.168.10.2 au premier routeur 192.168.10.1 ayant un paquet de demande d'écho ICMP avec TTL=1
- Le routeur supprimera ce paquet et enverra un message d'erreur ICMP Time Exceeded à la source.
- Tout cela se produit 3 fois avant que la machine source n'envoie le paquet suivant en ajoutant la valeur TTL de 1, c'est-à-dire TTL=2.
- On a aussi l'adresse IP du switch qui est : 192.168.10.254

17	18.199240	192.168.10.2	192.168.200.254	ICMP	106 Echo (ping) request id=0x0001, seq=51/13056, ttl=1 (no response found!)
18	18.199853	192.168.10.1	192.168.10.2	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
19	18.200242	192.168.10.2	192.168.200.254	ICMP	106 Echo (ping) request id=0x0001, seq=52/13312, ttl=1 (no response found!)
20	18.200891	192.168.10.1	192.168.10.2	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
21	18.201834	192.168.10.2	192.168.200.254	ICMP	106 Echo (ping) request id=0x0001, seq=53/13568, ttl=1 (no response found!)
22	18.202256	192.168.10.1	192.168.10.2	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)

À partir de cette image, nous pouvons observer que le message de réponse d'écho ICMP est envoyé de 192.168.200.254 (destination) à 192.168.10.2 (source) pour TTL 2

37	23.757887	192.168.10.2	192.168.200.254	ICMP	106 Echo (ping) request id=0x0001, seq=54/13824, ttl=2 (reply in 38)
38	23.758698	192.168.200.254	192.168.10.2	ICMP	106 Echo (ping) reply id=0x0001, seq=54/13824, ttl=127 (request in 37)
39	23.760086	192.168.10.2	192.168.200.254	ICMP	106 Echo (ping) request id=0x0001, seq=55/14080, ttl=2 (reply in 40)
40	23.760834	192.168.200.254	192.168.10.2	ICMP	106 Echo (ping) reply id=0x0001, seq=55/14080, ttl=127 (request in 39)
41	23.761465	192.168.10.2	192.168.200.254	ICMP	106 Echo (ping) request id=0x0001, seq=56/14336, ttl=2 (reply in 42)
42	23.762274	192.168.200.254	192.168.10.2	ICMP	106 Echo (ping) reply id=0x0001, seq=56/14336, ttl=127 (request in 41)



c0 a8 c8 fe → Adresse IP (192.168.200.254)

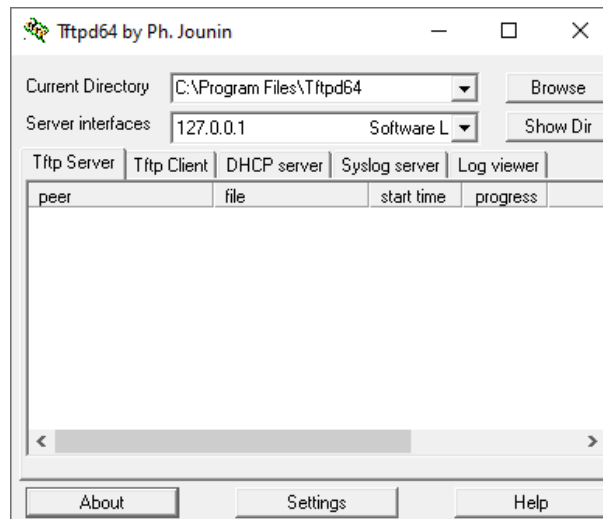
Pour conclure concernant cette analyse de trame nous avons dû pu trouver quelques informations importantes :

- Nous savons qu'il faut se connecter sur le Switch et le port 1 lors de la connexion
- L'adresse IP où nous avons la configuration est 192.168.200.254 et qu'elle est sur le Vlan native 2

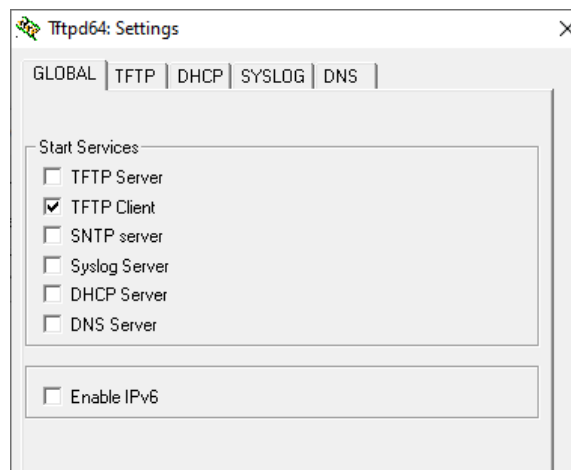
# IZAK ALI

## TUTO RECUPERATION CONF TFTPD :

### Comment récup le fichier de conf sur TFTPD :



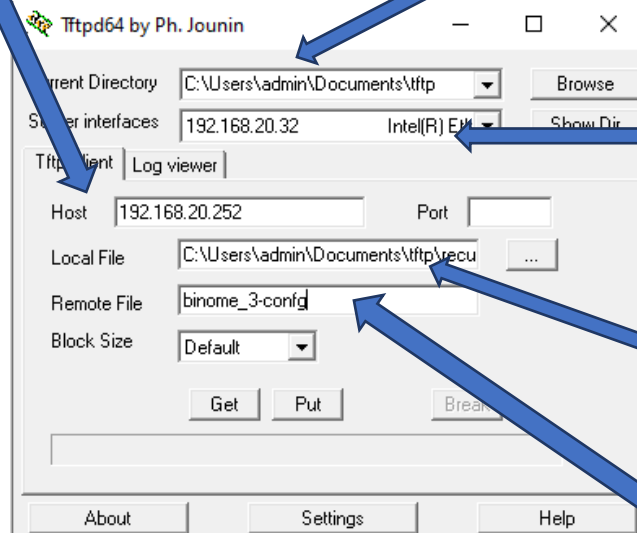
Dans un 1<sup>er</sup> temps il faut tout d'abord faire le paramétrage donc on clique sur "Settings"



Une fois ici on doit seulement avoir l'option "TFTP client" de sélectionner puis on valide

On doit mettre l'adresse IP du serveur tftp

Ici on met le chemin de redirection au quelle on veut stocker le fichier

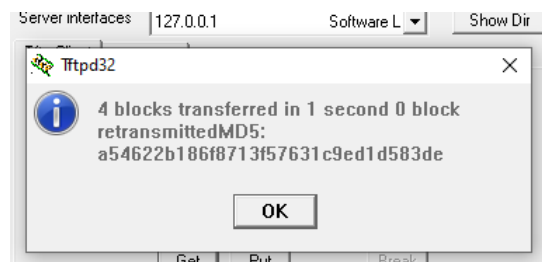


Ici on doit absolument mettre l'adresse IP du pc mais qui doit correspondre à l'adresse réseau du serveur tftp

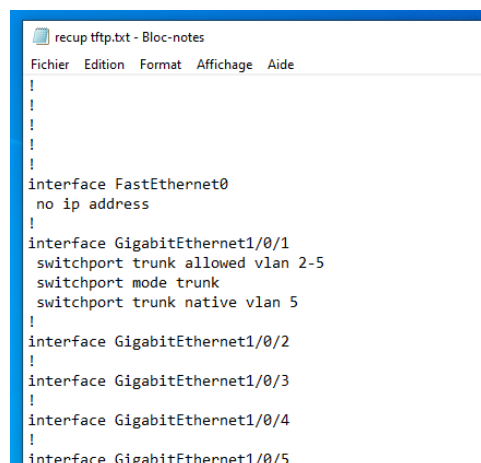
Ici on met le chemin de redirection au quelle on veut stocker le fichier (de préférence créer un fichier .txt vide)

Dans cette zone on met le nom exact du fichier auquel on veut récupérer

Une fois que tout cela est fait on appuie sur "Get" et normalement vous devriez avoir ceci :



Un message qui dit que le fichier a été bien restaurer

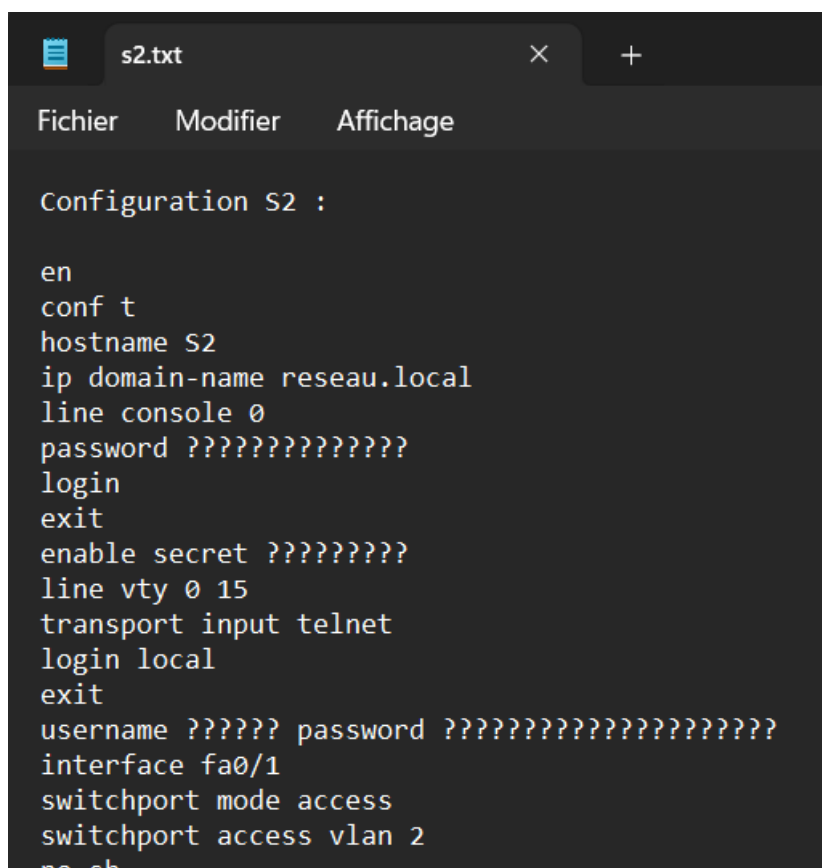


Ici on a bel et bien le fichier qui a été récupérer avec succès

J'ai ici une vidéo qui met en pratique le tuto → [Démonstration en vidéo](#)

# IZAK ALI

## CONFIG DE LA RECUP TFTP :



```
s2.txt
Fichier  Modifier  Affichage

Configuration S2 :

en
conf t
hostname S2
ip domain-name reseau.local
line console 0
password ??????????????
login
exit
enable secret ??????????
line vty 0 15
transport input telnet
login local
exit
username ?????? password ??????????????????????
interface fa0/1
switchport mode access
switchport access vlan 2
no sh
```

De plus j'ai aussi pu essayer de récupérer la config via d'autres moyens que tftpd. En faisant mes petites recherches j'ai aussi vu qu'on pouvait le faire aussi avec l'invite de commande windows :

```
C:\Users\IZAK LE GOAT>tftp -i 192.168.200.254 GET configS2.txt
Transfert réussi : 2699 octets en 1 seconde(s), 2699 octets/s
```

Après cette manipulation avec cette commande j'ai pu apercevoir que le service tftp sur windows n'est pas autorisé avec le pare-feu, c'est pour cela que j'ai eu du mal à récupérer la config. Par exemple au début sans n'avoir pas désactivé le pare-feu j'ai ceci comme message d'erreur :

```
C:\Users\IZAK LE GOAT>tftp -i 192.168.200.254 GET configS2.txt
Échec lors de la demande de connexion
```

## IZAK ALI

Je ne me suis pas directement dit que c'était le pare-feu et j'ai directement ouvert wireshark pour essayer de visualiser s'il y avait de la communication :

144	22.191719	192.168.200.254	192.168.10.2	TFTP	68 Error Code, Code: Not defined, Message: Undefined error code
145	22.191848	192.168.10.2	192.168.200.254	TFTP	63 Read Request, File: config52.txt, Transfer type: octet
146	22.195478	192.168.200.254	192.168.10.2	TFTP	558 Data Packet, Block: 1
147	22.201709	192.168.200.254	192.168.10.2	TFTP	558 Data Packet, Block: 1
154	23.191885	192.168.200.254	192.168.10.2	TFTP	68 Error Code, Code: Not defined, Message: Undefined error code
155	23.191885	192.168.200.254	192.168.10.2	TFTP	558 Data Packet, Block: 1
156	23.221971	192.168.200.254	192.168.10.2	TFTP	558 Data Packet, Block: 1
166	25.202091	192.168.200.254	192.168.10.2	TFTP	558 Data Packet, Block: 1
167	25.202091	192.168.200.254	192.168.10.2	TFTP	68 Error Code, Code: Not defined, Message: Undefined error code
170	26.232019	192.168.200.254	192.168.10.2	TFTP	558 Data Packet, Block: 1
184	28.201990	192.168.200.254	192.168.10.2	TFTP	558 Data Packet, Block: 1
190	29.232136	192.168.200.254	192.168.10.2	TFTP	68 Error Code, Code: Not defined, Message: Undefined error code
198	30.206847	192.168.10.2	192.168.200.254	TFTP	63 Read Request, File: config52.txt, Transfer type: octet

Sur la capture, on peut voir que le serveur TFTP essaye de me transmettre le fichier config52.txt. La première requête est une requête de lecture du fichier, avec le nom du fichier et le type de transfert (octet). La deuxième et troisième requêtes sont des paquets de données contenant le contenu du fichier.

Cependant, la quatrième requête est une erreur indiquant que le transfert a échoué. L'erreur est non définie, ce qui signifie que le serveur TFTP ne sait pas pourquoi le transfert a échoué. La cause la plus probable de l'échec du transfert est le pare-feu. Le pare-feu peut bloquer le trafic TFTP, où il peut limiter le trafic TFTP aux ports et aux adresses IP spécifiques.

# IZAK ALI

## Cisco Packet Tracer

Avant d'aller sur Cisco packet Tracer nous avons dû relever, s'intéresser aux différentes contraintes qu'il pourrait avoir (@IP, masque, Vlan, nombres de postes...)

J'ai donc relevé plusieurs choses comme :

Les contraintes pour les Vlan : Le Vlan 150 ne peut être pour l'administration du réseau mais il ne pourra pas être utilisé pour un des nouveaux sous-réseaux ci-dessus.

Le nombre de postes est de 19

1 LAN d'au moins 10 postes PC pour la nouvelle unité de production

1 LAN d'au moins 5 postes PC pour les nouveaux commerciaux

1 LAN d'au moins 4 postes PC pour RH

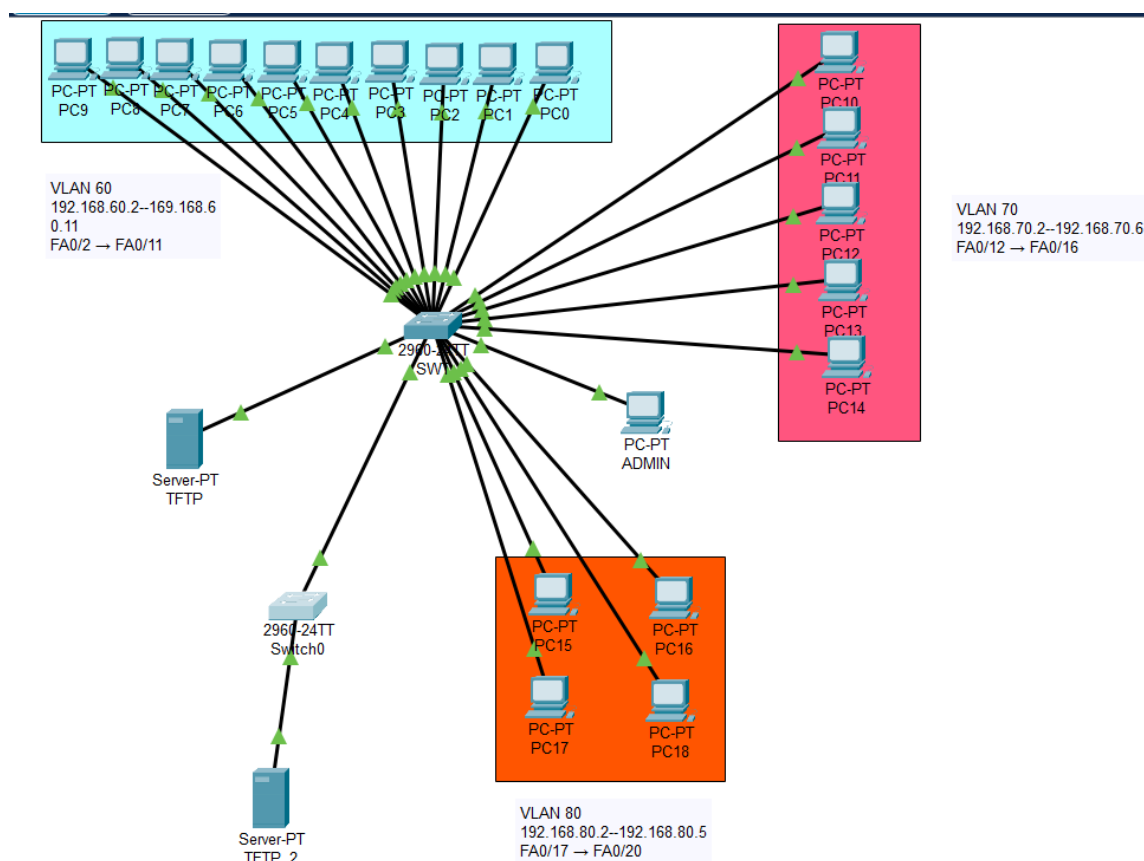
Suites à cela j'ai donc pu réaliser la topologie sur le logiciel Cisco packet tracer

Voici donc ma topologie sur Cisco packet tracer qui comporte bien les 3 LAN :

- Unité de production
- RH
- Nouveaux commerciaux

Pour ma part ici j'ai dû ajouter un autre serveur TFTP

# IZAK ALI



Pour ma part j'ai du crée un LAN comme ceci avec 2 server TFTP. J'ai mis en place le DHCP en ligne de commande directement dans le switch (SWT) :

```
ip dhcp excluded-address 192.168.60.1
ip dhcp excluded-address 192.168.70.1
ip dhcp excluded-address 192.168.80.1
!
ip dhcp pool vlan60
 network 192.168.60.0 255.255.255.0
 default-router 192.168.60.1
ip dhcp pool vlan70
 network 192.168.70.0 255.255.255.0
 default-router 192.168.70.1
ip dhcp pool vlan80
 network 192.168.80.0 255.255.255.0
 default-router 192.168.80.1
```

On peut y voir ici que j'ai du crée 3 pools pour chaque vlan en excluant l'adresse @IP de chaque passerelle

J'ai utilisé les vlans 60, 70 et 80

Voici en plus claire ce que cela donne sur l'un des pc du vlan 60 :

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

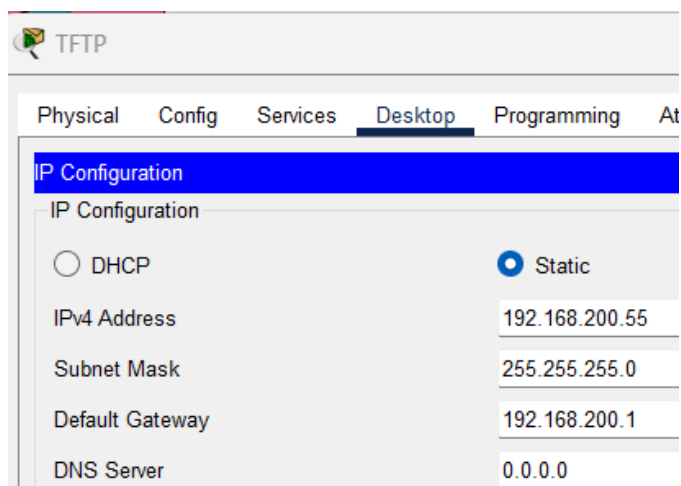
Connection-specific DNS Suffix.:
Physical Address.: 0007.EC7D.B3DB
Link-local IPv6 Address.: FE80::207:ECFF:FE7D:B3DB
IPv6 Address.: ::
IPv4 Address.: 192.168.60.3
Subnet Mask.: 255.255.255.0
Default Gateway.: ::
                  192.168.60.1
DHCP Servers.: 192.168.60.1
DHCPv6 IAID.:
DHCPv6 Client DUID.: 00-01-00-01-BE-B4-3A-52-00
DNS Servers.: ::
                0.0.0.0
```

On peut remarquer ici que le pc a bien une adresse @IP via DHCP



# IZAK ALI

Le switch (SWT) comprend aussi un server TFTP fonctionnel configurer avec un vlan a part le vlan 200 attribuer uniquement au port au quel le TFTP est connecté :



Voici la config du server TFTP connecté au switch (SWT)

D'une part on a aussi une connectivité entre le switch et le TFTP :

```
SWT#ping 192.168.200.55
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.55,
!!!!!
Success rate is 80 percent (4/5), round-trip min/

SWT#copy runni
SWT#copy running-config tftp:
Address or name of remote host []? 192.168.200.55
Destination filename [SWT-config]?

Writing running-config...!!
[OK - 2568 bytes]

2568 bytes copied in 0 secs
```

J'en ai aussi profité pour sauvegarder cette config dans le server

Service

SWT-config  
asa842-k8.bin  
asa923-k8.bin  
c1841-adviservicesk9-mz.124-15.T1  
c1841-ipssec-mz.122-14.T7.bin

# IZAK ALI

Passons maintenant à la configuration du SSH :

```
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 90
ip domain-name swt.com
!
username admin secret 5 $l$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
```

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

La configuration du service SSH sur notre switch implique la définition d'un nom de domaine via "ip domain-name" et l'activation de SSH avec "ip ssh version 2". La génération de la paire de clés RSA via "crypto key generate rsa" est cruciale, intégrant le nom de domaine pour renforcer l'identification. Des mesures de sécurité, telles que "ip ssh time-out 90" et "ip ssh authentication-retries 5", sont ajoutées. Sur les lignes vty de 0 à 4, "login local" est spécifié pour l'authentification locale, et "transport input ssh" restreint l'accès aux connexions SSH, renforçant la sécurité des connexions distantes.

J'ai dû aussi mettre un vlan uniquement pour le pc administration le vlan 666 :

```
!
interface Vlan666
 ip address 192.168.1.2 255.255.255.0
!
```

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::209:7CFF
    IPv6 Address . . . . .: ::
    IPv4 Address. . . . .: 192.168.1.3
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                192.168.1.2
```

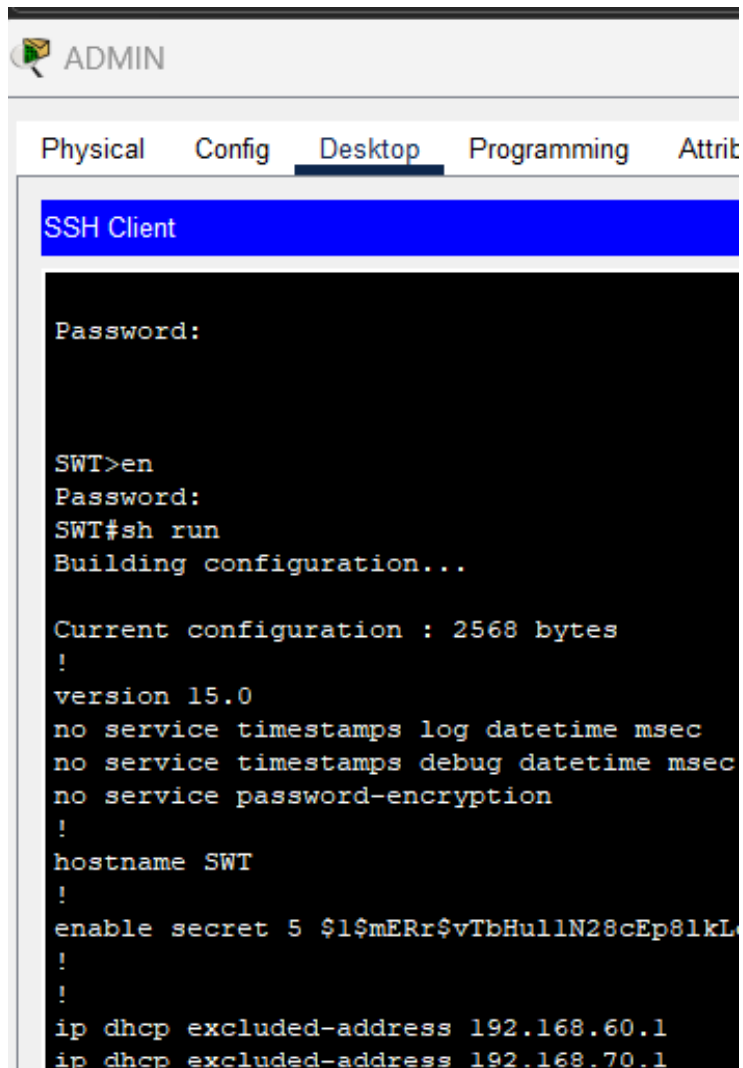
Ensuite avec toute ces configurations la on peut se connecter en SSH via le pc administration :

Telnet / SSH Client	
Session Options	
Connection Type	SSH
Host Name or (IP address)	192.168.1.2
Username	

Ici on spécifie l'adresse @IP de la passerelle soit l'IP du vlan 666

# IZAK ALI

Et nous voici en mode SSH sur le switch (SWT) :



```
ADMIN

Physical  Config  Desktop  Programming  Attrit

SSH Client

Password:

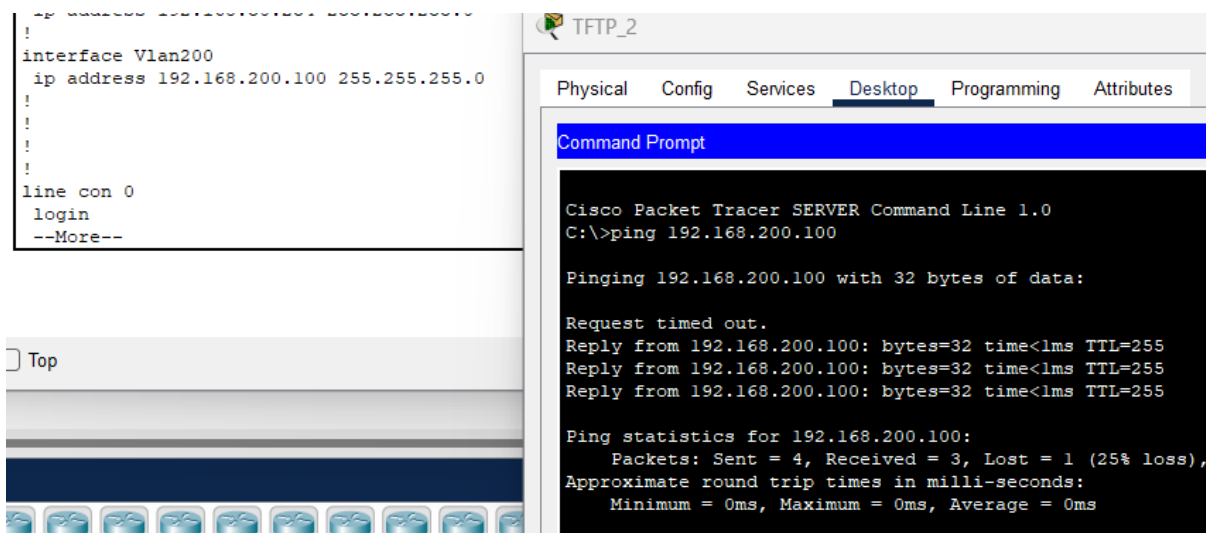
SWT>en
Password:
SWT#sh run
Building configuration...

Current configuration : 2568 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SWT
!
enable secret 5 $l$mERr$vTbHull1N28cEp8lkL
!
!
ip dhcp excluded-address 192.168.60.1
ip dhcp excluded-address 192.168.70.1
```

## IZAK ALI

Ensuite en ce qui concerne le switch (S2) j'ai copié collé la config sur le TFTP de la salle directement dans mon switch (S2) et j'ai aussi intégré un server TFTP du même principe et même fonctionnement du LAN avec le switch (SWT) à noter que les 2 switches sont liés avec des ports configurés en mode trunk

Juste une petite connectivité entre les 2 appareils :



Petite remarque sur ma config packet tracer ; mes 3 vlans ne pouvant pas communiquer extérieurement avec le 2<sup>ème</sup> TFTP en absence de routeur pour pouvoir faire les sous interfaces.

Mon packet tracer en lien [ici](#)

# IZAK ALI

## CONTENU DU DS TP SAÉ12

Durant la réalisation de notre TP on a du se basé sur ma configuration récupérer précédemment dans le server TFTP c'est-à-dire la config du switch 2 (S2). Pour la réalisation de notre LAN on a remarqué que dans la config (S2) y'avait une possibilité de plusieurs vlans :

```
no sh
interface vlan 2
ip add 192.168.10.254 255.255.255.0
no sh
interface vlan 3
ip add 192.168.20.254 255.255.255.0
no sh
interface vlan 4
ip add 192.168.30.254 255.255.255.0
no sh
interface vlan 5
ip add 192.168.40.254 255.255.255.0
no sh
interface vlan 6
ip add 192.168.50.254 255.255.255.0
no sh
```

Dans notre cas a nous, nous avons pris 3 vlans pour notre LAN

Les vlans 2,3 et 4

Alors pourquoi nous avons pris ces vlans là et pas d'autre ? Parce que tout simplement on a dû remarquer que l'un des ports du switch (S2) était en mode trunk et aussi qu'il pouvait faire sortir les vlans allant de 1 jusqu'à 150 :


```
interface fa0/24
switchport mode trunk
switchport trunk allowed vlan 1-150
switchport trunk native vlan 150
```

Ce port-là nous indique clairement peu faire un lien depuis notre LAN jusqu'au server TFTP

# IZAK ALI


Une fois qu'on a tout ce qu'il nous faut il était tant qu'on passe à la configuration de notre switch :

```
interface GigabitEthernet1/0/1
!
interface GigabitEthernet1/0/2
  switchport access vlan 2
  switchport mode access
!
interface GigabitEthernet1/0/3
!
interface GigabitEthernet1/0/4
!
interface GigabitEthernet1/0/5
  switchport access vlan 3
  switchport mode access
!
interface GigabitEthernet1/0/6
!
interface GigabitEthernet1/0/7
  switchport access vlan 4
  switchport mode access
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
  switchport trunk native vlan 150
  switchport trunk allowed vlan 1-150
  switchport mode trunk
```



On peut voir ici qu'on a attribuer le port 2 au vlan 2, le port 5 au vlan 5, le port 7 au vlan 4 et le port 13 en copie du port 24 du switch S2. Ayant fait une copie du port 24 du switch S2 c'est pour notamment faire un lien direct de notre LAN au server TFTP

Et voici les adresses IP de chaque vlan de notre LAN. On a dû prendre différentes adresses IP que celui du switch S2 pour éviter justement des conflits entre switch et switch



```
!
interface Vlan2
  ip address 192.168.10.2 255.255.255.0
!
interface Vlan3
  ip address 192.168.20.2 255.255.255.0
!
interface Vlan4
  ip address 192.168.30.2 255.255.255.0
!
```

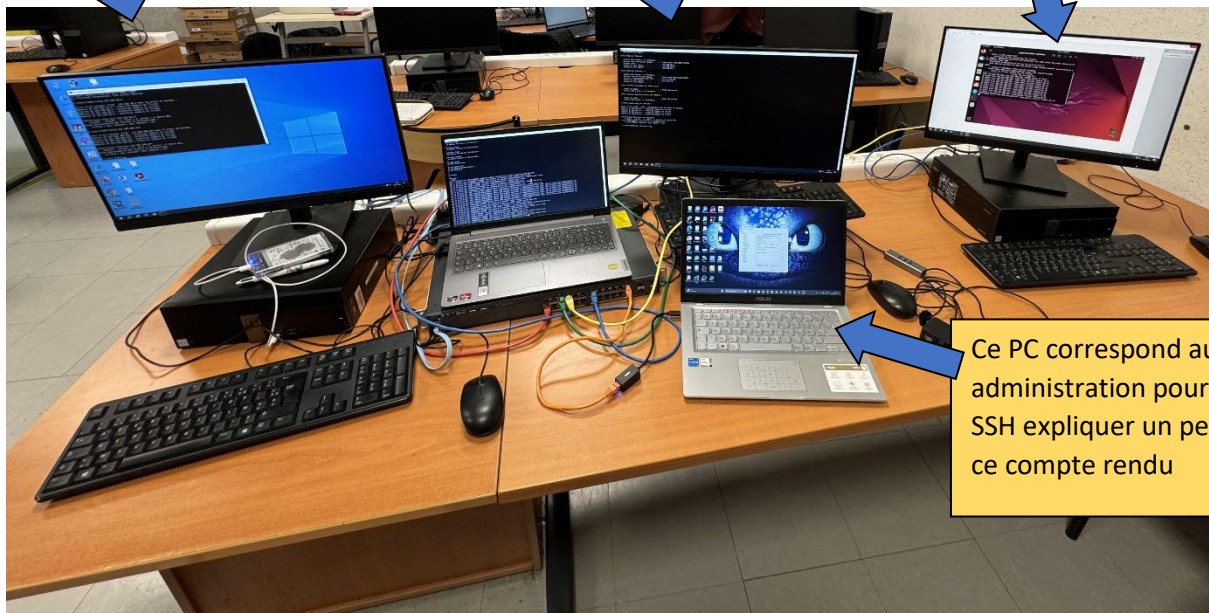
# IZAK ALI

Voici a quoi correspond notre LAN :

Le pc\_1 la brancher au port 2 du switch lié au vlan 2

Le pc\_2 la brancher au port 5 du switch lié au vlan 3

Le pc\_3 la brancher au port 7 du switch lié au vlan 4 fonctionnant sous Ubuntu (linux)



Ce PC correspond au pc administration pour la connexion en SSH expliquer un peu plus tard dans ce compte rendu

Pour notre situation, on n'a pas eu besoin d'entrer manuellement les adresses IP puisque dans notre configuration de notre switch on a inclus le service DHCP :

```
ip dhcp excluded-address 192.168.10.1
ip dhcp excluded-address 192.168.20.1
ip dhcp excluded-address 192.168.30.1
!
ip dhcp pool vlan2
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
!
ip dhcp pool vlan3
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
!
ip dhcp pool vlan4
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
!
```

Ces lignes indiquent les adresses IP qui doivent être exclues de la plage d'adresses attribuées par le serveur DHCP. En l'occurrence, les adresses 192.168.10.1, 192.168.20.1 et 192.168.30.1 ne seront pas attribuées dynamiquement par le serveur DHCP. Ces adresses IP correspondent aux sous interfaces du routeur

Le premier pool est configuré pour le VLAN 2, avec une plage d'adresses de 192.168.10.0 à 192.168.10.255 et une passerelle par défaut (default-router) de 192.168.10.1.

De manière similaire, le deuxième pool est configuré pour le VLAN 3 avec une plage d'adresses de 192.168.20.0 à 192.168.20.255 et une passerelle par défaut de 192.168.20.1.

Enfin, le troisième pool est pour le VLAN 4 avec une plage d'adresses de 192.168.30.0 à 192.168.30.255 et une passerelle par défaut de 192.168.30.1.



## IZAK ALI

Une fois qu'on a mis en place le DHCP, on s'est aussi mis à mettre en place le SSH :

Déjà pour une connexion en SSH, on a du créer un autre vlan qui est hors des vlans prédéfinis :

```
interface GigabitEthernet1/0/23
 switchport access vlan 666
 switchport mode access
```

Ce vlan correspondre au vlan administration pour la connexion en SSH. On n'a pas pris le vlan 150 qui était déjà défini pour justement à cette connexion en SSH parce qu'on n'avait pas envie de créer des conflits avec les autres camarades

```
interface Vlan666
 ip address 192.168.1.2 255.255.255.0
```

Dans un premier temps, on a dû mettre un nom de domaine sur notre switch en utilisant la commande "ip domain-name". La configuration de ce nom de domaine est essentielle avant d'activer le service SSH. Le nom de domaine est utilisé lors de la génération des clés RSA, ajoutant ainsi un élément d'identification unique à la paire de clés.

En activant le service SSH, il est recommandé de spécifier la version 2 du protocole avec la commande "ip ssh version 2". Cette préférence pour la version 2 est due à ses améliorations en matière de sécurité par rapport à la version 1, offrant des algorithmes cryptographiques plus forts et des fonctionnalités avancées.

Une fois le nom de domaine configuré et la version 2 de SSH activée, l'étape suivante consiste à générer la paire de clés RSA. Cette paire de clés est cruciale pour l'authentification sécurisée lors des connexions SSH. La commande "crypto key generate rsa" est utilisée à cette fin, générant une clé privée et une clé publique. Le nom de domaine configuré précédemment est intégré dans la clé publique, renforçant ainsi l'association entre la clé et l'appareil spécifique.

On a dû aussi mettre quelques paramètres en plus, tels que "ip ssh time-out 90" et "ip ssh authentication-retries 5", pour configurer des mesures de sécurité supplémentaires lors de l'accès via SSH. Ces paramètres définissent un délai d'inactivité de 90 secondes avant la déconnexion automatique et limitent à 5 le nombre de tentatives d'authentification, renforçant ainsi la sécurité du service SSH.



## IZAK ALI

De plus, pour les lignes vty de 0 à 4, on a spécifié "login local" afin d'utiliser une méthode d'authentification locale, ce qui signifie que les utilisateurs doivent entrer leurs identifiants locaux pour accéder à l'appareil. La commande "transport input ssh" a également été configurée pour restreindre l'accès uniquement aux utilisateurs qui se connectent via SSH, renforçant ainsi la sécurité des connexions distantes sur les lignes virtuelles de terminal.

Ma config SWT du DS TP [ICI](#)

Maintenant que tout a été bien configurer passons au test de connectivité :

Vidéos :

- [SSH](#)
- [PC 1 VERS PC 2 ET PC 1 VERS TFTP](#)
- [PC 3 \(LINUX\) VERS TFTP](#)