# Cours : Réseau complexe

FICHIER PACKETTRACER :

https://drive.proton.me/urls/4TWT9B473C#8eZI6l0G5kiP

## Sommaire

I. Une administration avec plusieurs services ..... 3
II. Ajout d'un point d'accès sans fil ..... 7
III. Les commutateurs de couche 2 ..... 8
IV. Configuration des commutateurs de couche 2 ..... 12
V. Accès sécurisé aux commutateurs ..... 16
VI. Configuration des routeurs ..... 20
1) On veut relier le site principal à un site distant en passant par Internet. Pour sécuriser la connexion, on utilise un tunnel VPN entre 2 routeurs ..... 20
2) Configuration sécurisée du routeur ..... 20
3) Configuration des interfaces ..... 22
4) Configuration du routage ..... 23
5) Vérification ..... 25
VII. Configuration des VLAN ..... 29
1) Identifier les domaines de collision et de diffusion ..... 29
2) Utiliser les VLANs pour réduire les domaines de diffusion ..... 30
3) Paramétrage des VLANs ..... 31
VIII. Ajout de la téléphonie IP ..... 32
1) Ajout des téléphones ..... 32
2) Configuration ..... 32
3) Vérifications ..... 33
4) Trunk de VLAN ..... 35
5) Routage inter VLAN ..... 35
IX. Sauvegarde des configurations ..... 39
1) Exemple avec le switch Info ..... 40

# I. Une administration avec plusieurs services

Chaque service dispose pour l'instant de 2 PC et une imprimante.

Il y a 2 services par étage (6 services, 3 étages).

Au sous-sol, une salle informatique (PC + imprimante), 3 serveurs et un routeur, et le cœur de réseau.

Comment choisir les commutateurs ? quel débits ?

Dans les services, FastEthernet 100 gbps avec 1 port GigabitEthernet -> Cisco 2960




Un routeur GigabitEthernet -> Cisco 1941




Cœur de réseau GigabitEthernet -> Cisco 2960 Pas compatible, il faut prendre un Cisco 3650




Nom des ports :

Routeur : g0/0 à g0/1

Commutateur : f0/1 à f0/24

Cœur : g1/0/1 = g1/0/24

⚠ Numérotation

Les routeurs commencent à partir de 0

Les commutateurs à partir de 1

On décide d'utiliser les ports suivants :

PC1 : Première interface disponible

PC2 : Seconde interface disponible

Imprimante : Troisième interface disponible

1er étage

| Interface | Connecté à |
|---|---|
| **fo0/1** | PC1 - Dir |
| **fo0/2** | PC2 - Dir |
| **fo0/3** | Impr - Dir |
| **fo0/4** | PC1 - Exam |
| **fo0/5** | PC2 - Exam |
| **fo0/6** | Impr - Exam |

2ème étage

| Interface | Connecté à |
|---|---|
| **fo0/1** | PC1 - Paie |
| **fo0/2** | PC2 - Paie |
| **fo0/3** | Impr - Paie |
| **fo0/4** | PC1 - Emploi |
| **fo0/5** | PC2 - Emploi |
| **fo0/6** | Impr - Emploi |

3ème étage

| Interface | Connecté à |
|---|---|
| **fo0/1** | PC1 - Med |
| **fo0/2** | PC2 - Med |
| **fo0/3** | Impr - Med |
| **fo0/4** | PC1 - Assur |

| | |
|---|---|
| **fo0/5** | PC2 - Assur |
| **fo0/6** | Impr - Assur |

Plan d'adressage :

| **Groupes** | **@Réseau** | **1er @ disponible** | **Dernière @ disponible** | **Passerelle** |
|---|---|---|---|---|
| **Direction** | 192.168.20.0/24 | 192.168.20.1/24 | 192.168.20.253/24 | 192.168.20.254/24 |
| **Examen** | 192.168.21.0/24 | 192.168.21.1/24 | 192.168.21.253/24 | 192.168.21.254/24 |
| **Paie** | 192.168.22.0/24 | 192.168.22.1/24 | 192.168.22.253/24 | 192.168.22.254/24 |
| **Emploi** | 192.168.23.0/24 | 192.168.23.1/24 | 192.168.23.253/24 | 192.168.23.254/24 |
| **Med** | 192.168.24.0/24 | 192.168.24.1/24 | 192.168.24.253/24 | 192.168.24.254/24 |
| **Assur** | 192.168.25.0/24 | 192.168.25.1/24 | 192.168.25.253/24 | 192.168.25.254/24 |
| **Info** | 192.168.27.0/24 | 192.168.27.1/24 | 192.168.27.253/24 | 192.168.27.254/24 |
| **Serveurs** | 192.168.30.0/24 | 192.168.30.1/24 | 192.168.30.253/24 | 192.168.30.254/24 |
| **Impression** | 192.168.40.0/24 | 192.168.40.1/24 | 192.168.40.253/24 | 192.168.40.254/24 |

Adressage des PC :

| Groupes | PC1 | PC2 | Passerelle |
|---|---|---|---|
| **Direction** | 192.168.20.1/24 | 192.168.20.2/24 | 192.168.20.254/24 |
| **Exam** | 192.168.21.1/24 | 192.168.21.2/24 | 192.168.21.254/24 |
| **Paie** | 192.168.22.1/24 | 192.168.22.2/24 | 192.168.22.254/24 |
| **Emploi** | 192.168.23.1/24 | 192.168.23.2/24 | 192.168.23.254/24 |
| **Med** | 192.168.24.1/24 | 192.168.24.2/24 | 192.168.24.254/24 |
| **Assur** | 192.168.25.1/24 | 192.168.25.2/24 | 192.168.25.254/24 |
| **Info** | 192.168.27.1/24 | 192.168.27.2/24 | 192.168.27.254/24 |

Adressage des imprimantes :

| Impr - Dir | Impr - Exam | Impr - Paie | Impr - Exam | Impr - Med | Impr - Assur | Impr - Info |
|---|---|---|---|---|---|---|
| 192.168.40.1 | 192.168.40.2 | 192.168.40.3 | 192.168.40.4 | 192.168.40.5 | 192.168.40.6 | 192.168.40.7 |

Adressage serveurs :

| Serveur - AD | Serveur - Appli | Serveur - Fichiers | Passerelle |
|---|---|---|---|
| 192.168.30.1 | 192.168.30.2 | 192.168.30.3 | 192.168.30.254 |

## II. Ajout d'un point d'accès sans fil

Le réseau sera 192.168.60.0/24 :

- Ajouter une borne AP-PT sur le commutateur central
- Ajout des périphériques finaux : Laptop, tablette, smartphone, TV
- Ajouter une webcam

| SSID | Sécurité | Mot de passe |
|---|---|---|
| Metropole | WPA2-PSK | 1234-Metropole:1234 |

| Laptop | TV | Tablette | Smartphone | Caméra IP | Passerelle |
|---|---|---|---|---|---|
| **G** | - | 60.2 | 60.3 | 60.4 | 192.168.60.254 |

## III. Les commutateurs de couche 2

Ils maintiennent un tableau dont chaque ligne contient le numéro de port et l'adresse MAC du destinataire.

Une trame Ethernet avec une adresse de destination sortira toujours par le même port, quel que soit son port d'entrée. Elle ne sera jamais transmise sur son port d'entrée.

L'adresse MAC est l'identifiant unique physique de chaque carte réseau : elle est composée de 12 caractères hexadécimaux.

Exemple : B4-6D-83-DD-CE-49 (3 premiers : marque ; 3 derniers : identifiant de la carte réseau).

La table d'adresse MAC est stockée dans la mémoire de contenu (CAM : Content Adressable Memory)

Afficher la table CAM du commutateur Dir-Exam en utilisant la commande : show mac-adress-table

```
Switch>show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

Switch>
```

Sur cette capture d'écran, on observe que la table des adresse MAC est vide, cela est normal état donné que l'on a effectué aucune requête sur notre réseau.

Lancer un ping entre PC1-Dir et PC2-Dir et redemander la table

```
Switch>show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    00d0.582d.7081    DYNAMIC     Fa0/1
   1    00e0.8f7a.3b69    DYNAMIC     Fa0/2
Switch>
```

Après le ping, on remarque que la table d'adresse MAC contient maintenant l'adresse MAC du PC1, ainsi que le port sur lequel il est connecté sur le Switch, ainsi que celle du PC de destination sur le port Fa0/2

| | **PC1 - Dir** | **PC2 - Dir** |
|---|---|---|
| **Adresse MAC** | 00:D0:58:2D:70:81 | 00:E0:8F:7A:3B:69 |
| **Port** | Fa0/1 | Fa0/2 |

⚠ Attention, un port peut avoir plusieurs adresses de destination, par exemple s'il est relié à un autre commutateur

**Méthode Switch learn and forward**

- Processus en 2 étapes effectué par le switch pour chaque trame entrante

Étape 1 : mode découverte - Examen de l'adresse source

- Si l'adresse source n'est pas dans la table, alors elle est ajoutée avec le numéro de port entrant.
- Si l'adresse existe déjà, le commutateur réinitialise le compteur d'obsolescence. (5 min)
- Si l'adresse existe déjà mais pas sur le bon port, elle est traitée comme nouvelle avec le bon port.

⚠ Un seul port possible par adresse MAC

Etape 2 : Transfert-examen de l'adresse de destination

- Si l'adresse est une adresse de non-diffusion, le commutateur la recherche dans sa table.
- Si elle est dans la table, il lit le numéro de port et transfert la trame par ce port.
- Si elle n'est pas dans la table, le commutateur transfère la trame sur tous les ports, sauf le port d'entrée. C'est une micro-diffusion inconnue.
- Si l'adresse est une diffusion, la trame est aussi envoyée sur tous les ports sauf le port entrant.

**Interface CLI (Interface en ligne de commande) :**

Par sécurité, 2 modes

- Utilisateur (view only) : L'invite se termine par >
- Priviligié (actif) pour les commandes de configuration :
- L'invite se termine par #.

Pour accéder à la configuration, il faut accéder au mode de configuration globale : (config) #

Exemple :

- Switch (config-line)# → accès à distance SSH

- Switch (config-if)# → accès par l'interface

Commandes :

- Pour passer du mode utilisateur au mode privilégié : enable

- Pour revoir : disable

- Pour passer en mode de configuration globale : configure terminal

- Pour revenir : exit

Exercice :

Dans cet exercice, nous allons effectuer plusieurs commandes sur notre Switch (étant sur Dir et Exam).

Switch> enable (en)

Pour passer en mode privilégié, nous devons utiliser la commande enable :

```
Switch>enable
Switch#
```

Ici, on peut voir que notre prompt a changé, il est passe de « Switch> » a « Switch# ». Cela signifie bien que l'on est passé en privilégié

Switch# configure terminal (conf t)

Pour passer en mode configuration, nous devons utiliser la commande configure terminal :

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/
Switch(config)#
```

Ici, on peut voir que notre prompt a changé, il est passe de « Switch# » a « Switch(config)# ». Cela signifie bien que l'on est passé en privilégié

Switch (config)# line console 0 (line c 0)

Switch(config-line)# exit

Switch(config)# interface FastEthernet0/1 (int F0/1)

Switch(config-if)# exit

Switch(config)# exit

Switch#

## IV. Configuration des commutateurs de couche 2

L'interface SVI :

Pour configurer un commutateur de couche 2, je peux utiliser un câble console, mais il faut que je sois physiquement à côté. Une interface SVI va permettre d'y accéder à distance par le réseau IP. Cette interface logicielle se trouve par défaut dans le VLAN 1 (réseau virtuel 1). Tous les ports sont par défaut dans le VLAN 1.

Commande : show vlan brief

```
Switch#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

Pour des raisons de sécurité, on utilise un autre VLAN pour la gestion :

| Groupes | VLAN ID | @ réseau | 1ere adresse | Dernière | Passerelle |
|---|---|---|---|---|---|
| **Périphérique réseau** | 10 | 192.168.10.0/24 | 192.168.10.1 | 192.168.10.253 | 192.168.10.254 |
| **Administrateur** | 100 | 192.168.100.0/24 | 192.168.100.1 | 192.168.100.253 | 192.168.100.254 |

| VLAN 100 | @IPv4 | @IPv6 |
|---|---|---|
| **Cœur de réseau Cisco 3650** | 192.168.100.1 | 2001:DB8 :ACAD:100::1/64 |
| **Dir – Exam Cisco 2960** | 192.168.100.2 | 2001:DB8 :ACAD:100::2/64 |
| **Paie – Emploi** | 192.168.100.3 | 2001:DB8 :ACAD:100::3/64 |
| **Med – Assur** | 192.168.100.4 | 2001:DB8 :ACAD:100::4/64 |
| **Info** | 192.168.100.5 | 2001:DB8 :ACAD:100::5/64 |
| **Passerelle** | 192.168.100.254 | 2001:DB8 :ACAD:100::254/64 |

Exemple pour Dir-Exam :

- Switch(config)# hostname Dir-Exam
- Dir-Exam(config)# interface vlan 100

- Dir-Exam(config-if)# ip address 192.168.100.2 255.255.255.0
  ipv6 address 2001:DB8:ACAD:100::2/64
  no shutdown

Remarque :

- Le SVI pour le VLAN 100 ne sera pas activé (up) tant qu'un appareil n'est pas connecté.
- La configuration IPv6 n'est pas activée par défaut sur les Cisco 2960 :

- En configuration globale : sdm prefer dual-ipv4-and-ipv6 default
- En configuration privilégié : reload

Passerelle :

Dir-Exam(config)# ip default-gateway 192.168.100.254

Vérifier

- show ip interface brief

```
Vlan100                192.168.100.2   YES manual down                  down
```

- show ipv6 interface brief

```
Vlan100                    [down/down]
    FE80::206:2AFF:FECC:3701
    2001:DB8:ACAD:100::2
```

Mettre les ports dans le VLAN en mode access.

Pour mettre un port physique en mode access, il suffit de se rendre dans une interface physique en mode configuration privilégié (configuration terminal), puis il faut ce

rendre dans cette interface grâce à la commande « interface FastEthernet0/15 » étant l'interface choisi pour ce test.

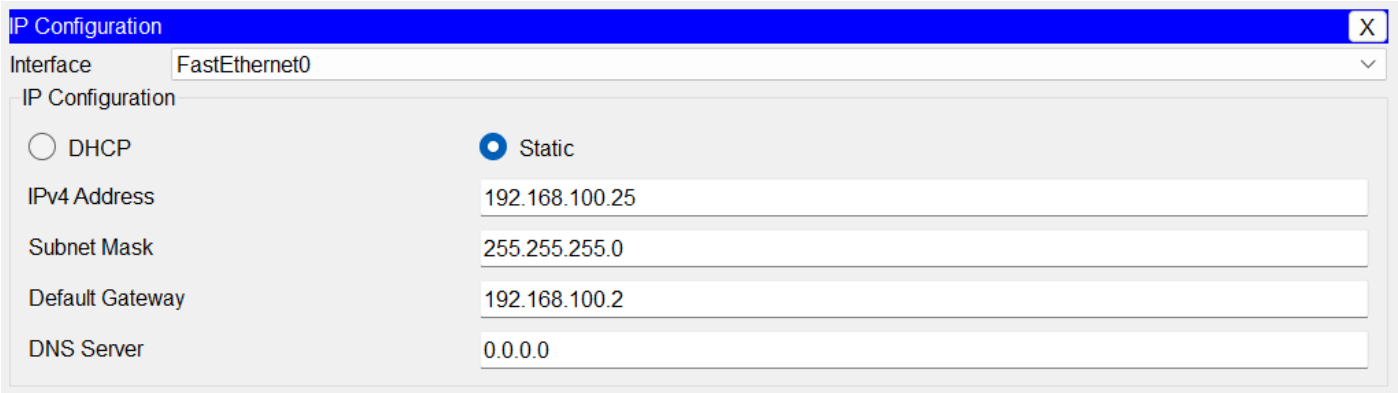
Une fois dans cette dernière, nous allons utiliser la commande « **switchport access vlan 100** » pour que cette interface soit liée à ce VLAN :

Rajouter provisoirement un PC en 192.168.100.25 pour faire des pings sur le VLAN 100.

Le PC a bien été ajouté avec une IP en 192.168.100.25 sur le port FastEthernet0/15




⚠ Il est important que le PC sois connecté sur le port FastEthernet0/15 du Switch étant donné que le VLAN est en mode access sur cette interface.




Si l'on essaie de faire un ping vers le Switch, on remarque que l'on peut communiquer avec étant donné que le port physique lié à la machine est dans le bon réseau.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.100.2

Pinging 192.168.100.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.100.2: bytes=32 time<1ms TTL=255
Reply from 192.168.100.2: bytes=32 time<1ms TTL=255
Reply from 192.168.100.2: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.100.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.100.2
```

Activer le VLAN 100 :

Dir-Exam(config)# vlan 100

Dans notre exemple, nous avons déjà mis le vlan sur un port, par conséquent il a automatiquement été activé

```
Enter configuration commands, one per line.  End with CNTL/Z.
Dir-Exam(config)#vlan 100
Dir-Exam(config-vlan)#
```

Dans l'interface graphique, mettre le bon port dans le VLAN 100.

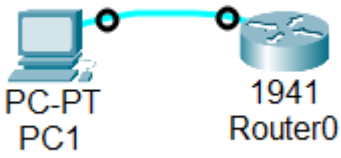
Nous l'avons fait en ligne de commande, mais si on vérifie l'interface graphique, et que l'on se rend dans l'interface FastEthernet0/15

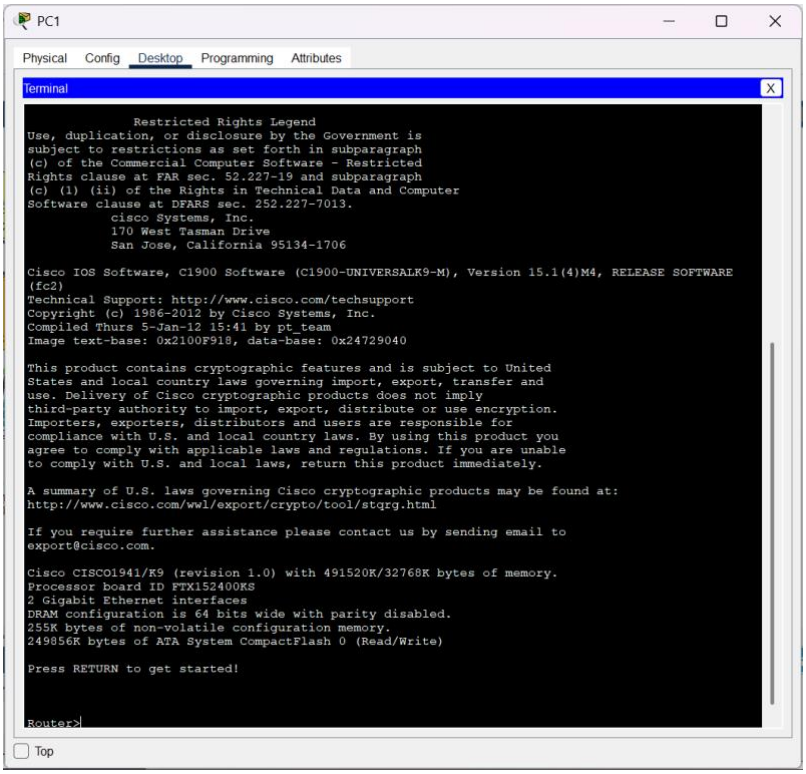
## V. Accès sécurisé aux commutateurs

- Accès en port console

  Port COM, port série, RS232

Faisable avec PT : brancher un PC sur le port console

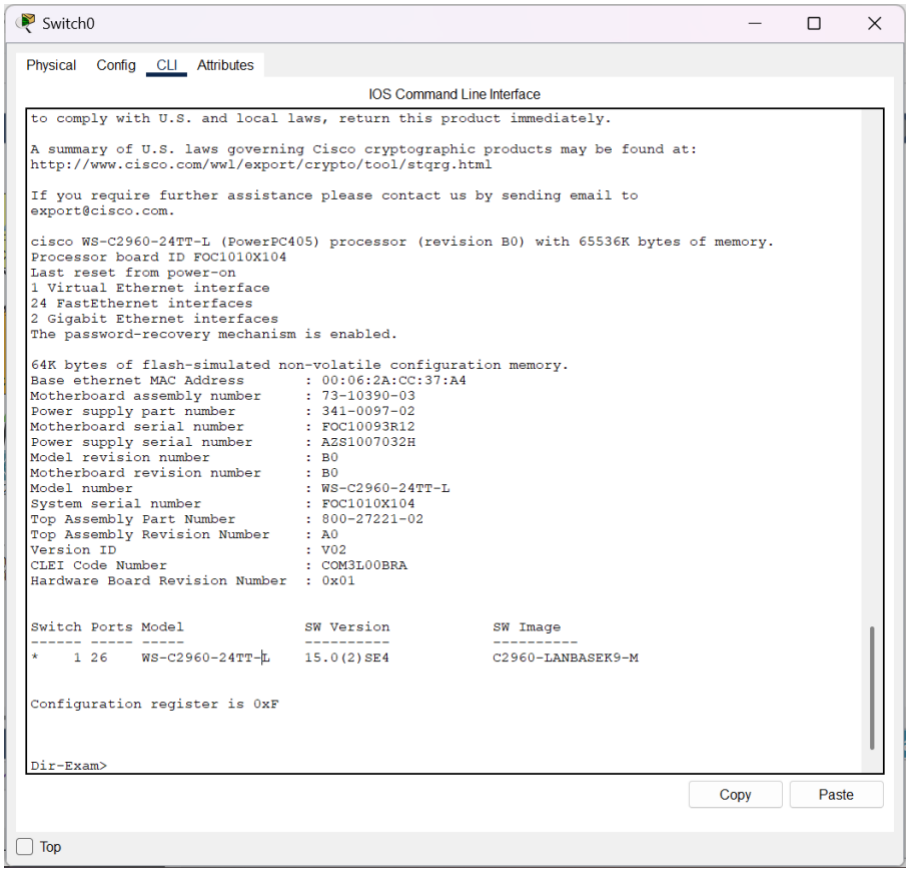



- Accès en SSH

Pour vérifier que le switch est compatible SSH, il faut que vérifier que sa version IOS contient « K9 » :

Dir-Exam# show version




Configuration de la connexion SSH :

Dir-Exam# show ip ssh

configure terminal

Dir-Exam (config)# enable secret 1234-MetroPole:1234

ip domain-name metropole.com

crypto key generate rsa

ip ssh version 2

username admin secret 1234-MetroPole:1234

line vty 0 15

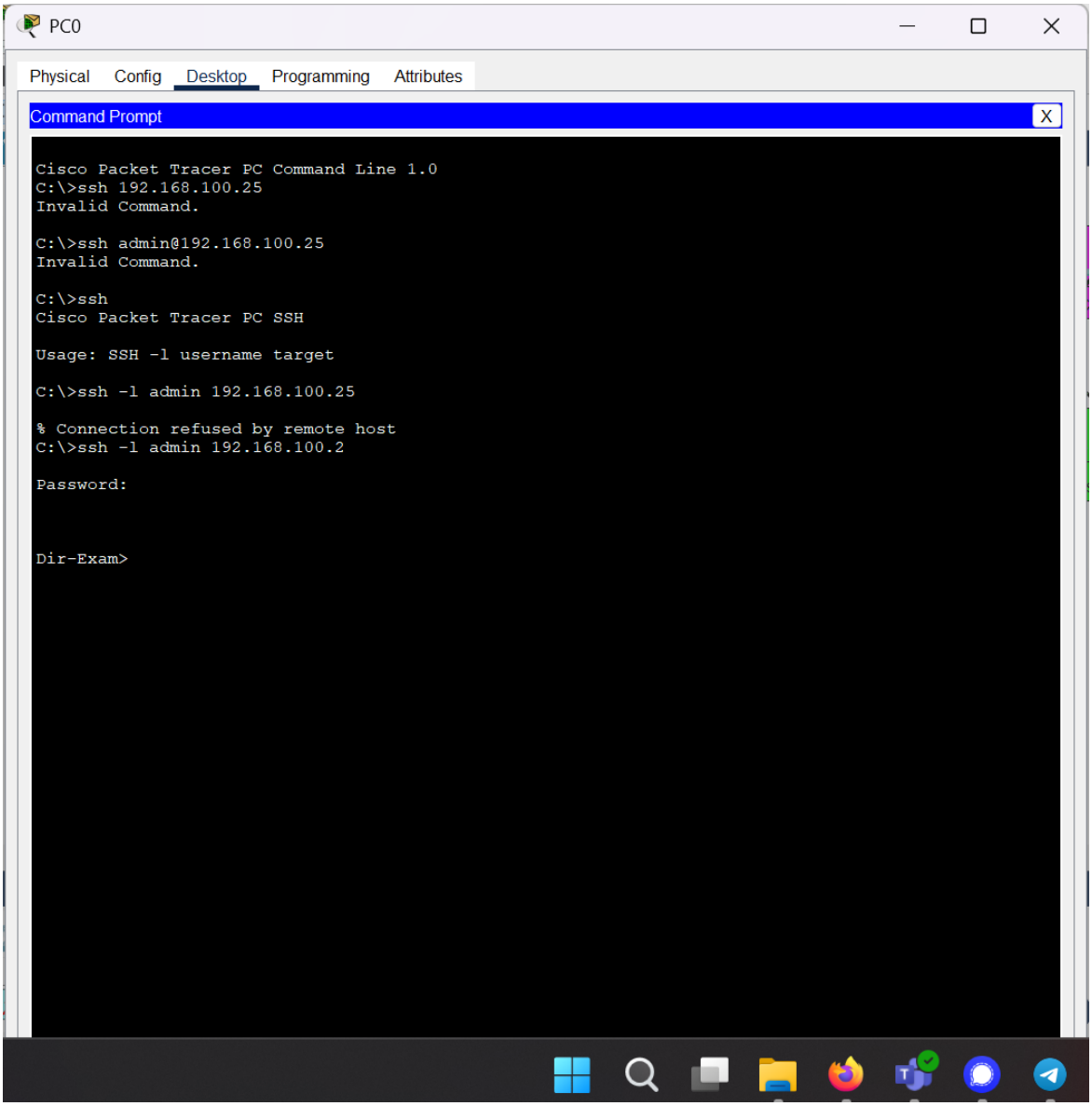
Dir-Exam(config-line)# transport input ssh

login local

exit

Connexion depuis un PC :

ssh user@ip ou ssh -l user IP



# VI. Configuration des routeurs

## 1) On veut relier le site principal à un site distant en passant par Internet. Pour sécuriser la connexion, on utilise un tunnel VPN entre 2 routeurs

- Gérer le site distant avec 2 PC, 1 imprimante, reliés à un commutateur 2960, lui-même relié en GigabitEthernet à un routeur 1941.
- Relier les 2 routeurs pour une liaison série. Pour cela il faut ajouter à chaque routeur une carte HWIC-2T

Remarques :

- L'éclair représente une connexion WAN longue distance.
- Pour relier les 2 routeurs, on utilise en réel des câbles bleus DCE/DTE.

Configuration du site distant :

| PC1 - VPN | PC2 - VPN | Imp - VPN | Passerelle |
|---|---|---|---|
| 192.168.110.1/24 | 192.168.110.2/24 | 192.168.110.3/24 | 192.168.110.254/24 |

## 2) Configuration sécurisée du routeur

- Nom d'hôte
- Mot de passe du mode privilégié
- Configuration SSH
- Mot de passe console
- Mot de passe ligne VTY
- Cryptage
- Bannière d'accès
- Sauvegarde

```
Router> enable

Router# conf t

Router(config)# hostname RouterVPN

RouterVPN(config)# enable secret 1234-MetroPole:1234
                   ip domain-name metropole.com
                   username admin secret 1234-MetroPole:1234
                   crypto key generate rsa (1024)
                   ip ssh version 2
                   line console 0

RouterVPN(config-line)# password 1234-MetroPole:1234
                        login
                        exit

RouterVPN(config)# line vty 0 15
RouterVPN(config-line)# transport input ssh
                        login local
                        exit

RouterVPN(config)# service password-encryption
                     banner motd # Acces aux personnes autorisées seulement #
                     exit
```

RouterVPN# copy running-config startup-config

### 3) Configuration des interfaces

RouterVPN(config)# interface GigabitEthernet0/0

RouterVPN(config-if) ip address 192.168.110.254 255.255.255.0

ipv6 address 2001:db8:acad:110::254/64

description Lien Sous-réseau VPN

no shutdown

exit

RouterVPN(config)# interface Serial0/1/0

RouterVPN(config-if)# ip address 10.0.0.2 255.255.255.0

ipv6 address 2001:db8:acad:1001::2/64

description Lien RouteurVPN-RouteurMetro

no shutdown

exit

Configuration de l'adresse de bouclage :

RouterVPN(config)# interface loopback 0

RouterVPN(config-if)# ip address 192.168.200.2 255.255.255.0

exit

## 4) Configuration du routage

Un routeur a au minimum deux interfaces pour relier au moins deux (sous-)réseaux. Quand il reçoit un paquet, il détermine vers quelle interface le transférer. L'interface peut être la destination finale du paquet (routeur d'extrémité) ou bien un passage par un routeur intermédiaire. Pour cela, il consulte sa table de routage.

Exemple : le routeur doit atteindre l'hôte 172.16.0.10 à partir de cette table. Quelle route va-t-il choisie ?

| Route | Préfixe | Adresse binaire |
|---|---|---|
| **1** | 172.16.0.0/12 | 10101100.0001\|0000.00000000.00001010 |
| **2** | 172.16.0.0/18 | 10101100.00010000.00\|000000.00001010 |
| **3** | 172.16.0.0/26 | 10101100.00010000.00000000.00\|001010 |

Le routeur choisit la meilleure route : celle qui a le plus long préfixe correspondant au destinataire. Donc la route 3.

Les tables de routage se remplissent de plusieurs manières :

- Un réseau directement connecté est ajouté si l'interface est configurée (@IP/Masque) et activée (up).

- Les réseaux distants ne sont pas directement connectés donc le routeur va apprendre de deux manières différentes :
  - Par une route statique ajoutée manuellement
  - Par un protocole de routage dynamique (OSPF)

- La route par défaut spécifie le routeur intermédiaire suivant lorsqu'il n'y a pas de solution dans la table.

Configuration de nos 3 routeurs (avec le switch cœur de réseau) :

Table de routage de RouteurMetro :

| Destination | Masque | Passerelle |
|---|---|---|
| 0.0.0.0 | 0.0.0.0 | 10.0.0.1 |

RouterVPN(config)# ip route 0.0.0.0 0.0.0.0 10.0.0.1

ipv6 unicast-routing

ipv6 route ::/0 2001:DB8:ACAD:1001::1

Table de routage de RouteurMetro :

| Destination | Masque | Passerelle | |
|---|---|---|---|
| 0.0.0.0 | 0.0.0.0 | 192.168.10.2 | Cœur de réseau |
| 192.168.110.0 | 255.255.255.0 | 10.0.0.2 | Routeur VPN |

RouteurMetro(config)# ip route 192.168.110.0 255.255.255.0 10.0.0.2

ip route 0.0.0.0 0.0.0.0 192.168.10.2

ipv6 unicast-routing

ipv6 route 2001:DB8:ACAD:110::0/64

2001:DB8:ACAD:1001::2

ipv6 route ::/0 2001:DB8:ACAD:10::2

Table de routage :

| **Destination** | **Masque** | **Passerelle** |
|---|---|---|
| 0.0.0.0 | 0.0.0.0 | 192.168.10.1 |

```
Switch(config)# hostname SwitchL3
SwitchL3(config)# interface g1/0/1
SwitchL3(config-if)# no switchport
                     ip address 192.168.10.2 255.255.255.0
                     ipv6 address 2001:DB8:ACAD:10::2/64
                     exit

SwitchL3(config)# ip routing
                   ip route 0.0.0.0 0.0.0.0 192.168.10.1
                   ipv6 unicast-routing
                   ipv6 route ::/0 2001:DB8:ACAD:10::1
```

## 5) Vérification

- show ip interface brief

```
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1/0/1   192.168.10.2    YES manual up                    up
```

- show ipv6 interface brief

```
SwitchL3#show ipv6 interface brief
GigabitEthernet1/0/1       [up/up]
    FE80::203:E4FF:FEBB:D501
    2001:DB8:ACAD:10::2
```

- show ip route

```
SwitchL3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.10.1 to network 0.0.0.0

C    192.168.10.0/24 is directly connected, GigabitEthernet1/0/1
```

On remarque que notre route a bien été défini sur l'interface GigabitEthernet1/0/1 pour le réseau 192.168.10.0/24. Le « C » signifie que cette route est connectée.

- show ipv6 route

```
SwitchL3#show ipv6 route
IPv6 Routing Table - 26 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
S   ::/0 [1/0]
     via 2001:DB8:ACAD:10::1
C   2001:DB8:ACAD:10::/64 [0/0]
     via ::, GigabitEthernet1/0/1
L   2001:DB8:ACAD:10::2/128 [0/0]
     via ::, GigabitEthernet1/0/1
```

Quelques tests à partir de RouteurVPN :

- ping 192.168.10.1

```
C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time=24ms TTL=254
Reply from 192.168.10.1: bytes=32 time=20ms TTL=254
Reply from 192.168.10.1: bytes=32 time=24ms TTL=254
Reply from 192.168.10.1: bytes=32 time=14ms TTL=254

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 24ms, Average = 20ms

C:\>
```

- ping 192.168.110.254

```
C:\>ping 192.168.110.254

Pinging 192.168.110.254 with 32 bytes of data:

Reply from 192.168.110.254: bytes=32 time<1ms TTL=255
Reply from 192.168.110.254: bytes=32 time<1ms TTL=255
Reply from 192.168.110.254: bytes=32 time<1ms TTL=255
Reply from 192.168.110.254: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.110.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

- ping 10.0.0.2

```
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time<1ms TTL=255
Reply from 10.0.0.2: bytes=32 time=1ms TTL=255
Reply from 10.0.0.2: bytes=32 time=1ms TTL=255
Reply from 10.0.0.2: bytes=32 time=1ms TTL=255

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

- ping 10.0.0.1

```
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time=42ms TTL=254
Reply from 10.0.0.1: bytes=32 time=27ms TTL=254
Reply from 10.0.0.1: bytes=32 time=1ms TTL=254
Reply from 10.0.0.1: bytes=32 time=30ms TTL=254

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 42ms, Average = 25ms

C:\>
```

- ping 192.168.10.2

```
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time=1ms TTL=253
Reply from 192.168.10.2: bytes=32 time=1ms TTL=253
Reply from 192.168.10.2: bytes=32 time=1ms TTL=253
Reply from 192.168.10.2: bytes=32 time=1ms TTL=253

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>
```

Exemples d'utilisation de filtres :

- show running-config | section GigabitEthernet0/1
- show ip interface brief | include up
- show ip interface brief

Pensez à utilizer les flèches, le show history…

- terminal history size 200

# VII. Configuration des VLAN

## 1) Identifier les domaines de collision et de diffusion

Collision : C'est quand 2 paquets sont émis en même temps.

La congestion du réseau arrive quand le réseau est ralenti.

Switch <-> PC

Domaine de collision

Plus le domaine de collision est petit, meilleur est le réseau.

- Un ensemble de commutateurs connectés forme un domaine de diffusion.

Les routeurs sont utilisés pour segmenter les domaines de diffusion.

Switch <-> RouteurVPN <-> RouteurMetro <-> Switch

Plan segmenté en 3 domaines de diffusions.

Le problème, c'est que le réseau principal Métropole est trop gros donc trop lent : c'est un seul réseau de diffusion.

## 2) Utiliser les VLANs pour réduire les domaines de diffusion

On pourrait mettre des routeurs pour chaque service, mais c'est trop cher ! Les VLANs permettent une segmentation logique en cohérence avec les services.

Plan d'adressage simplifié :

| GROUPES | VLAN | @ | PREMIER @ | DERNIER @ | PASSERELLE |
|---|---|---|---|---|---|
| **DIRECTION** | 20 | 192.168.20.0 | 192.168.20.1 | 192.168.20.253 | 192.168.20.254 |
| **EXAMEN / CONCOURS** | 21 | 192.168.21.0 | 192.168.21.1 | 192.168.21.253 | 192.168.21.254 |
| **PAIE / DRH** | 22 | 192.168.22.0 | 192.168.22.1 | 192.168.22.253 | 192.168.22.254 |
| **EMPLOI** | 23 | 192.168.23.0 | 192.168.23.1 | 192.168.23.253 | 192.168.23.254 |
| **MEDECINE** | 24 | 192.168.24.0 | 192.168.24.1 | 192.168.24.253 | 192.168.24.254 |
| **ASSURANCE** | 25 | 192.168.25.0 | 192.168.25.1 | 192.168.25.253 | 192.168.25.254 |
| **INFO / RGPD** | 27 | 192.168.27.0 | 192.168.27.1 | 192.168.27.253 | 192.168.27.254 |
| **SERVEURS** | 30 | 192.168.30.0 | 192.168.30.1 | 192.168.30.253 | 192.168.30.254 |
| **IMPRESSION** | 40 | 192.168.40.0 | 192.168.40.1 | 192.168.40.253 | 192.168.40.254 |
| **TELEPHONES** | 50 | 192.168.50.0 | 192.168.50.1 | 192.168.50.253 | 192.168.50.254 |
| **WIFI** | 60 | 192.168.60.0 | 192.168.60.1 | 192.168.60.253 | 192.168.60.254 |

| | | | | | |
|---|---|---|---|---|---|
| **ADMINISTRATION** | 100 | 192.168.100.0 | 192.168.100.1 | 192.168.100.253 | 192.168.100.254 |

Avantages des VLANs :

- Domaines de diffusion réduits : moins de machines/
- Sécurité optimisée : seuls les utilisateurs d'un même VLAN peuvent communiquer.
- Meilleure efficacité : regroupement des utilisateurs par VLAN.
- Coût réduit : moins de mise à niveau matérielles du réseau et meilleure utilisation de la bande passante.
- Meilleure performances : réduction du trafic inutile.
- Gestion simplifiée des projets et applications.

## 3) Paramétrage des VLANs

| VLAN | Nom |
|---|---|
| 20 | Direction |
| 21 | Examens/Concours |
| 40 | Impression |
| 50 | Téléphonie |
| 100 | Administration |

Dir-Exam(config)# vlan 20

Dir-Exam(config-vlan)# name direction

end

Dir-Exam(config)# int fa0/1

Dir-Exam(config-if)# switchport mode access

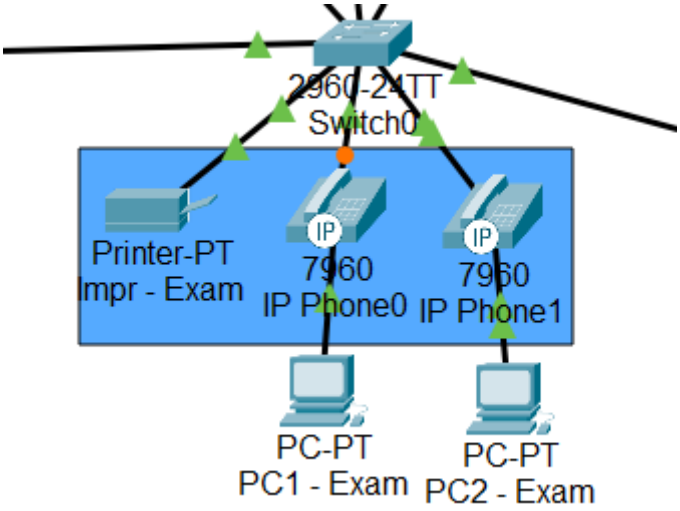
```
switchport access vlan 20

exit
```

# VIII. Ajout de la téléphonie IP

## 1) Ajout des téléphones

Direction 192.168.20.0 Examen 192.168.21.0




## 2) Configuration

Il faut configurer les commutateurs pour indiquer le VLAN voix sur les ports reliés à un téléphone

Rappel : un seul VLAN par port sauf si on ajoute :

- Un VLAN voix
- Ou un port TRUNK

Nous avons déjà créé le VLAN voix, donc :

- On active la qualité de service (QoS) sur les interfaces
- Et on ajoute le VLAN voix.

Exemple pour Dir-Exam :

Dir-Exam(config)# int f0/4

Dir-Exam(config-if)# mls qos trust cos

# switchport voice vlan 50

# exit

Dir-Exam(config)# int f0/2

Dir-Exam(config-if)# mls qos trust cos

# switchport voice vlan 50

# exit

Ou bien int range f0/1-2 pour faire les 2 en même temps !

## 3) Vérifications

show vlan brief

```
Dir-Exam#sh vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gig0/1, Gig0/2
20   direction                         active    Fa0/1, Fa0/2
21   Examen                            active    Fa0/4, Fa0/5
40   impression                        active    Fa0/3, Fa0/6
50   voix                              active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
100  VLAN0100                          active    Fa0/15
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Dir-Exam#
```

show interfaces f0/1 switchport

```
Dir-Exam#show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 20 (direction)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: 50
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none


Dir-Exam#
```

Pour modifier l'appartenance d'un port à un VLAN :

switchport access vlan nouvel_id

Pour supprimer l'appartenance d'un port à un VLAN :

no switchport access vlan

Pour supprimer un vlan (seulement si tous les ports ont été supprimés) :

no vlan vlan_id

Pour revenir au paramétrage d'usine des VLANs :

delete vlan.dat (et redémarrer le switch !)

Pour revenir au paramétrage d'usine du commutateur :

- Débrancher tous les câbles sauf l'alim et la console
- Entrer les commandes : erase startup-config
  delete vlan.dat

## 4) Trunk de VLAN

Un Trunk de VLAN est un lien de couche 2 entre deux commutateurs qui achemine le trafic pour tous les VLANs.

Dir-Exam(config)# interface g0/1

Dir-Exam(config-if)# switchport mode trunk

switchport trunk native vlan 100

switchport trunk allowed vlan 20,21,40,50,100

De même pour les commutateurs Paie-Emploi, Med-Ass et Info.

Vérification : show interface g0/1 switchport

Pour réinitialiser en cas d'erreur :

- no switchport allowed vlan
- no switchport trunk native vlan

## 5) Routage inter VLAN

Configuration VLAN du Cœur de réseau :

- Créer les VLANs,
- Affecter les VLANs dans les interfaces
- Créer les trunks et autoriser les VLANs

```
SwitchL3(config)# vlan 20

SwitchL3(config-if)# name Direction

                     exit

                     vlan 21

                     name Examen

                     exit

                     vlan 22

                     name Paie

                     vlan 23

                     name Emploi

                     exit

                     vlan 24

                     name Medecine

                     exit

                     vlan 25

                     name Assurance

                     exit

                     vlan 27

                     name Informatique

                     exit

                     vlan 30

                     name Serveurs
```

exit

vlan 40

name Impression

exit

vlan 50

name Telephonie

exit

vlan 60

name WiFi

exit

vlan 100

name Administration

exit

Création des différents trunks sur chaque port (excepté le pour le point d'accès WiFi qui sera en access 60).

interface g1/0/2

~~switchport trunk encapsulation dot1q~~ (Norme 802.1Q)

switchport mode trunk

switchport trunk native vlan 100

switchport trunk allowed vlan 20,21,40,50,100

exit

```
interface g1/0/3
  …
  switchport mode allowed vlan 22,23,40,50,100
  …

interface g1/0/4
  …
  switchport mode allowed vlan 24,25,40,50,100
  …

interface g1/0/5
… vlan 27,40,50,100

interface range g1/0/6-8
  switchport mode access
  switchport access vlan 30
  exit
int g1/0/9
  switchport mode access
  switchport access vlan 60
  exit
```

Il reste à créer les passerelles avec des interfaces virtuelles SVI (Switch Virtual Interface) :

```
SwitchL3(config)# interface vlan 20
SwitchL3(config-if)# description Passerelle SVI Direction
                    ip address 192.168.20.254 255.255.255.0
                    ipv6 address 2001:db8:acad:20::254/64
                    no shutdown
                    exit
```

## IX. Sauvegarde des configurations

Objectifs : Résister à un crash de switch, une erreur humaine, un acte de malveillance ou tout simplement dupliquer une configuration sur un autre switch.

Accès au système de fichiers CISCO (IOS File Systems) :

```
show file systems
dir
```

Attention : La mémoire flash est volatile (comme la RAM), par contre la NVRAM est non volatile (comme la ROM).

Le fichier startup-config contient la configuration de démarrage.

Le fichier running-config contient la configuration en cours.

Pour sauvegarder nos modifications :

```
copy running-config startup-config
```

Dans PacketTracer, l'onglet config permet de faire les sauvegardes graphiquement.

Export possible vers un serveur TFTP.

copy running-config tftp

1) Exemple avec le switch Info

Pour copier la configuration sur un serveur TFTP, nous allons devoir mettre une IP sur l'interface SVI Vlan30 pour que notre Switch puisse communiquer avec les serveurs (dans notre test, nous définissons le Vlan30)

```
Info-Serveurs#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Info-Serveurs(config)#int vlan30
Info-Serveurs(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

Info-Serveurs(config-if)#ip address 192.168.30.25 255.255.255.0
Info-Serveurs(config-if)#end
```

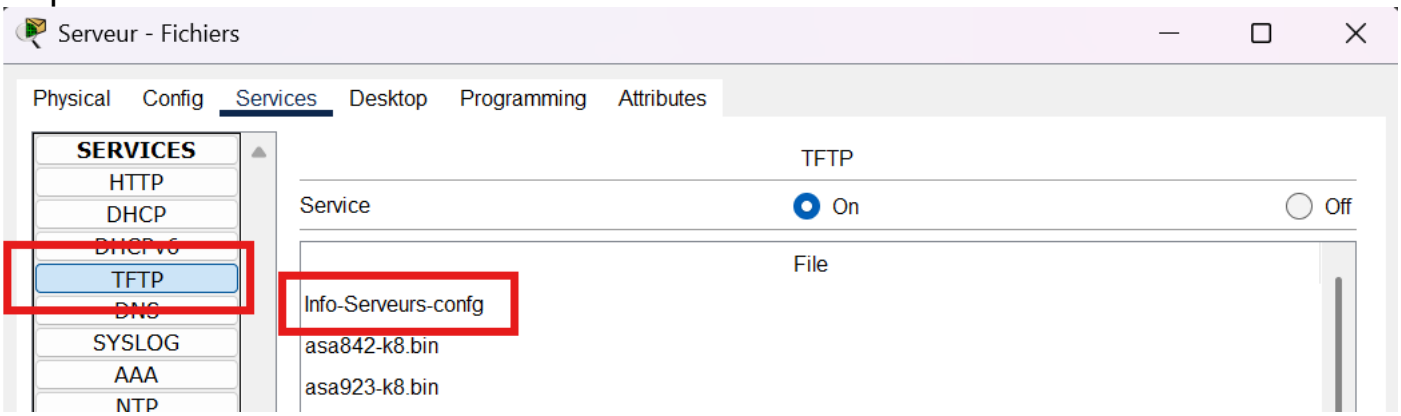
Une fois cette adresse défini, nous allons pouvoir démarrer la commande suivante : copy running-config tftp qui va nous permettre de copier cette configuration sur un serveur TFTP. Une fois la commande exécuté, il suffit d'y entrer l'adresse IP du serveur ainsi du nom de fichier que l'on souhaite obtenir sur ce dernier :

```
Info-Serveurs#copy running-config tftp
Address or name of remote host []? 192.168.30.3
Destination filename [Info-Serveurs-confg]?

Writing running-config....!!
[OK - 1502 bytes]

1502 bytes copied in 3.002 secs (500 bytes/sec)
Info-Serveurs#
```

Une fois ceci fait, on peut vérifier le service TFTP sur le serveur Fichiers pour y voir si notre configuration y est bien présente :




Faire des tests de fonctionnement

Rendre le TP :

- Compte-rendu
- Fichier TP
- Fichiers startup-config