

Réseau complexe



Sommaire

I. Réseau d'une administration avec plusieurs services	3
II. Ajout d'un point d'accès sans fil.....	6
III. Commutateurs de niveau 2.....	7
IV. Configuration des commutateurs	8
V. Accès à distance sécurisé à un commutateur	11
VI. Configuration des routeurs	13
VII. Configuration des VLANs	16
VIII. Ajout de la téléphonie IP.....	22
1) Ajout des téléphones	22
2) Configuration	22
3) Vérifications	23
4) <i>Trunk de VLAN</i>	23
5) Réalisez le routage inter-vlan.....	25
IX. Sauvegarde des configurations	27
1) Système de fichiers des routeurs et switches L3.....	27
2) Sauvegarde en mémoire non volatile(NVRAM)	28
3) Sauvegarde graphique dans PT.....	28

I. Réseau d'une administration avec plusieurs services

- Chaque service dispose de 2 PC et d'une imprimante ;
- 2 services par étage, 3 étages donc 6 services
- Au sous-sol, le service informatique avec 1 PC et 1 imprimante, 3 serveurs, 1 routeur et 1 switch cœur de réseau.

Comment choisir les commutateurs ? Quels débits sur les commutateur et routeur ?

- Dans les services, commutateurs en FastEthernet avec une entrée en GigabitEthernet. Est-ce que le Cisco Catalyst 2950 convient ? OUI



- Le routeur est en GigabitEthernet. Cisco 1941 ? OUI



- Le cœur de réseau est en GigabitEthernet. Cisco Catalyst 2960 ? NON FastEthernet



- Le cœur de réseau est en GigabitEthernet. Cisco Catalyst 3650 ? OUI



Comment s'appellent les ports du routeur ? g0/0 et g0/1

----- commutateur cœur de réseau ? g1/0/1 à g1/0/4-- g1/1/1 g1/1/4

----- des commutateur de services ? f0/1 à f0/24 et g0/1 et g0/2

Que comprenez-vous de la numérotation des ports ? La numérotation démarre à 0 sur les routeurs, à 1 sur les commutateurs.

Affichage des ports sur PT : options/Préférences/Always show ports labels.

Dans les services, on décide de mettre toujours PC 1 sur le 1^{er} port, PC2 sur le 2^{ème} et Imp sur le 3^{ème}.

Exemple 1^{er} étage :

Interface	Connecté à
F0/1	PC1-Dir
F0/2	PC2-Dir
F0/3	Imp-Dir
F0/4	PC1-Exam
F0/5	PC2-Exam
F0/6	Imp-Exam

2^{ème} étage

Interface	Connecté à
F0/1	PC1-DRH
F0/2	PC2-DRH
F0/3	Imp-DRH
F0/4	PC1-Emploi
F0/5	PC2-Emploi
F0/6	Imp-Emploi

3^{ème} étage

Interface	Connecté à
F0/1	PC1-Med
F0/2	PC2-Med
F0/3	Imp-Med
F0/4	PC1-Ass
F0/5	PC2-Ass
F0/6	Imp-Ass

Sous-sol

Interface	Connecté à
F0/1	PC1-Dir
F0/2	PC2-Dir
F0/3	Imp-Dir
F0/4	PC1-Exam

F0/5	PC2-Exam
F0/6	Imp-Exam

Plan d'adressage :

Groupes	Adresse IP	1 ^{ère} adresse	Dernière adresse	Passerelle
Direction	192.168.20.0/24	192.168.20.1	192.168.20.253	192.168.20.254
Examen	192.168.21.0/24	192.168.21.1	192.168.21.253	192.168.21.254
Paie-DRH	192.168.22.0/24	192.168.22.1	192.168.22.253	192.168.22.254
Emploi	192.168.23.0/24	192.168.23.1	192.168.23.253	192.168.23.254
Médecine	192.168.24.0/24	192.168.24.1	192.168.24.253	192.168.24.254
Assurance	192.168.25.0/24	192.168.25.1	192.168.25.253	192.168.25.254
Info/RGPD	192.168.27.0/24	192.168.27.1	192.168.27.253	192.168.27.254
Serveurs	192.168.30.0/24	192.168.30.1	192.168.30.253	192.168.30.254
Impression	192.168.40.0/24	192.168.40.1	192.168.40.253	192.168.40.254

Adressage des PC :

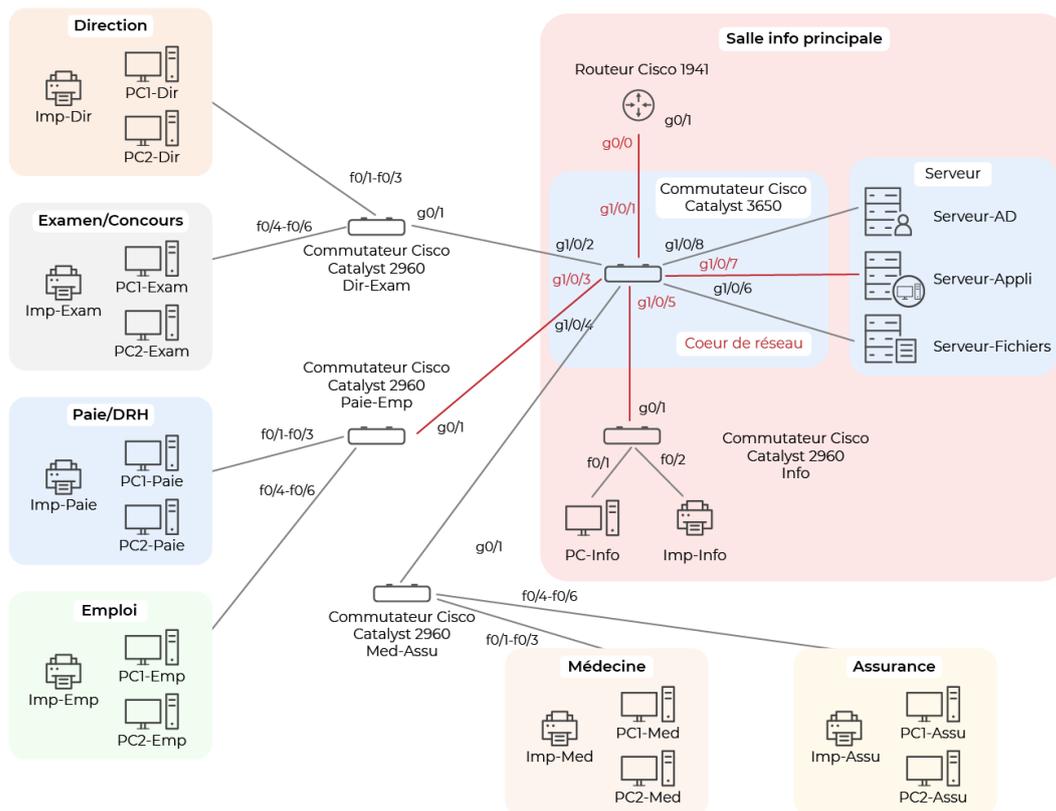
Groupes	PC1	PC2	Passerelle
Direction	192.168.20.1/24	192.168.20.2/24	192.168.20.254/24
Examen	192.168.21.1/24	192.168.21.2/24	192.168.21.254/24
Paie	192.168.22.1/24	192.168.22.2/24	192.168.22.254/24
Emploi	192.168.23.1/24	192.168.23.2/24	192.168.23.254/24
Médecine	192.168.24.1/24	192.168.24.2/24	192.168.24.254/24
Assurance	192.168.25.1/24	192.168.25.2/24	192.168.25.254/24
Info	192.168.27.1/24		192.168.27.254/24

Imprimantes :

Imp-Dir	Imp-Exam	Imp-Paie	Imp-Emp	Imp-Med	Imp-Assu	Imp-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

Serveur :

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 réseaux WIFI sera en 192.168.60.0/24 :

- Ajouter un point d'accès AP-PT sur le commutateur central,
- Ajouter des périphériques : laptop, TV, tablette, smartphone,
- Ajouter une webcam (menu Home)

Configuration :

SSID	Sécurité	MDP
Métropole	WPA-PSK	1234-Metropole :1234

Pas d'IP pour les point d'accès : couche 2 du modèle OSI

Plan d'adressage :

Laptop	TV	Tablette	Smartphone	Caméra IP	Passerelle
192.168.60.1	192.168.60.2	192.168.60.3	192.168.60.4	192.168.60.5	192.168.60.254

III. Commutateurs de niveau 2

Un switch de niveau 2 maintient un tableau dont chaque ligne contient le numéro du port et l'adresse MAC du destination sort par le même port de sorte quel soit le port d'entrée. Une trame n'est jamais renvoyée par le port d'entrée.

Rappel : adresse MAC = identifiant physique unique d'une carte réseau, composé de 12 caractères hexadécimaux.

B4-6D-83		DD-CE-49
Identification du constructeur		Identification de la carte réseaux

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

Afficher la table CAM du commutateur dir-Exam

Commande : `show mac-address-table`

(Normalement, elle est vide !)

Lancez un ping entre PC1-Dir et PC2-Dir.

(Normalement, la table se remplit.)

Méthode « Switch Learn and forward » : processus en 2 étapes effectué sur chaque trame.

- Etape 1 : découverte, examen de la source
 - o Si l'adresse MAC de la source n'existe pas dans la table, elle est rajoutée.
 - o Si elle existe, compteur d'obsolescence est réinitialisé (5 minutes).
 - o Si elle existe sur un autre port, la table est actualisée.
 - ➔ **Un port peut être associé à plusieurs adresse MAC , mais une adresse MAC ne peut pas être associée à plusieurs ports.**

- Etape 2 : Transfert, examen de la destination
 - o Si l'adresse MAC du destinataire est une adresse de monodiffusion, le commutateur cherche le port destinataire dans sa table MAC
 - o Si l'adresse est dans la table, transfert de la trame vers le port destinataire.
 - o Si l'adresse n'est pas dans la table, le commutateur transfère sur tous les ports (sauf celui d'entrée).
 - o Si l'adresse MAC est une adresse de multidiffusion, la trame est aussi envoyée sur tous les ports (sauf celui d'entrée).

Interface en ligne de commande (CLI)

Deux modes de commande :

- Mode d'exécution utilisateur (view only)
 - o Commandes de surveillance uniquement, pas de configurateur.
 - o Invite >
- Mode d'exécution privilégié (actif)
 - o Commandes de configuration
 - o Invite #
 - o Permet d'accéder au mode de configuration globale Switch(config)#
 - o Commandes enable / Disable

Exemple :

```
switch > enable
switch # configure terminal
switch (config) # Line console 0
switch (config-line)# exit
switch(config)# interface FastEthernet 0/1
switch (config-if)# exit
switch (config)# exit
switch #
```

IV. Configuration des commutateurs

Les commutateurs étant de niveau 2, ils n'ont pas d'adresse IP. Donc pour pouvoir se connecter à distance, on a inventé une interface virtuelle SVI (Switch Virtual Interface), Dans le VLAN1 (par défaut).

Commande : [Show vlan brief](#)

Pour des raisons de sécurité, on évite de laisser des ports dans le VLAN1. Nous allons utiliser 2 VLAN :

Groupes	VLAN ID	@ Réseaux	1 ^{ère} adresse	Dernière @	Passerelle
Périphérique	10	192.168.10.0/24	192.168.10.1	192.168.10.253	192.168.10.254
Administration	100	192.168.100.0/24	192.168.100.1	192.168.100.253	192.168.100.254

VLAN 100	@ IPv4	@I
Cœur de réseau Catalyst 3650	192.168.100.1/24	2001:DB8:ACAD:100::1/64
Dir-Exam	192.168.100.2	2001:DB8:ACAD:100::2/64
Paie-Empl	192.168.100.3	2001:DB8:ACAD:100::3/64
Med-Assu	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 Dir-Exam :

```
Switch(config)# hostname Dir-Exam
```

```
Dir-Exam(config)# interface VLAN100
Dir-Exam(config-if)# IP address 192.168.100.2 255.255.255.0
IPv6 address 2001:DB8:ACAD:100::2/64
no shutdown
```

Remarques :

- L'interface svi n'apparaît pas comme « up » tant que le VLAN100 n'est pas créé et q'un appareil n'est pas connecté.
- La commandes IPv6 n'est pas activée par défaut sur les Cisco 2960

Mode de configuration globale :

```
Dir-Exam# sdm prefer ipv4-and-ipv6 default
```

Mode de configuration privilégié :

```
Dir-Exam(config)#reload
```

- Pour la passerelle :

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

Pour le test, rajouter un PC en 192.168.100.25 pour faire des ping pour activer le VLAN 100 :

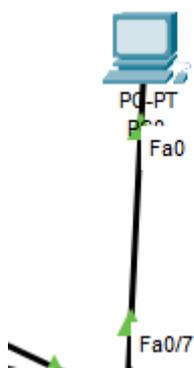
```
Dir-Exam(config)#VLAN100
```

Pour tester :

```
Show ip interface brief
```

```
Show ipv6 interface brief
```

Tout d'abords on ajoute un pc de test et on le brache au switch configurer



Puis dans le pc on vient lui mettre une @IP un masque et une passerelle.

IP Configuration	
<input type="radio"/> DHCP	
<input checked="" type="radio"/> Static	
IPv4 Address	192.168.100.25
Subnet Mask	255.255.255.0

Gateway/DNS IPv4	
<input type="radio"/> DHCP	
<input checked="" type="radio"/> Static	
Default Gateway	192.168.100.254
DNS Server	

Puis dans le switch on va dans la configuration du port qui est relia au pc de tester et on lui met le VLAN que l'on vient de créer.

FastEthernet0/7	
Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input type="radio"/> 100 Mbps <input type="radio"/> 10 Mbps <input checked="" type="checkbox"/> Auto
Duplex	<input type="radio"/> Half Duplex <input type="radio"/> Full Duplex <input checked="" type="checkbox"/> Auto
Access	VLAN
Tx Ring Limit	10

Le test de ping entre le nouveau PC et le switch en VLAN100

```
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=2ms TTL=255
Reply from 192.168.100.2: bytes=32 time=2ms TTL=255
Reply from 192.168.100.2: bytes=32 time=2ms TTL=255

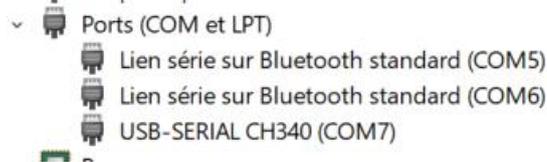
Ping statistics for 192.168.100.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

V. Accès à distance sécurisé à un commutateur

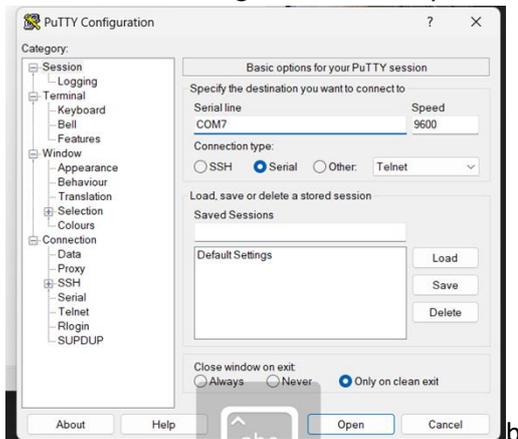
- Câble console RJ45/USB
 - o Anciennement COM ou série ou console
- Branchement du switch sur le port console



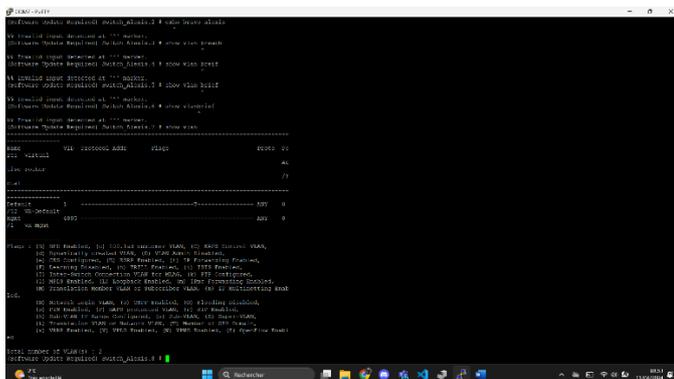
- Recherche du port détecté dans le gestionnaire de périphérique



- Installation et configuration de Putty



- Connexion



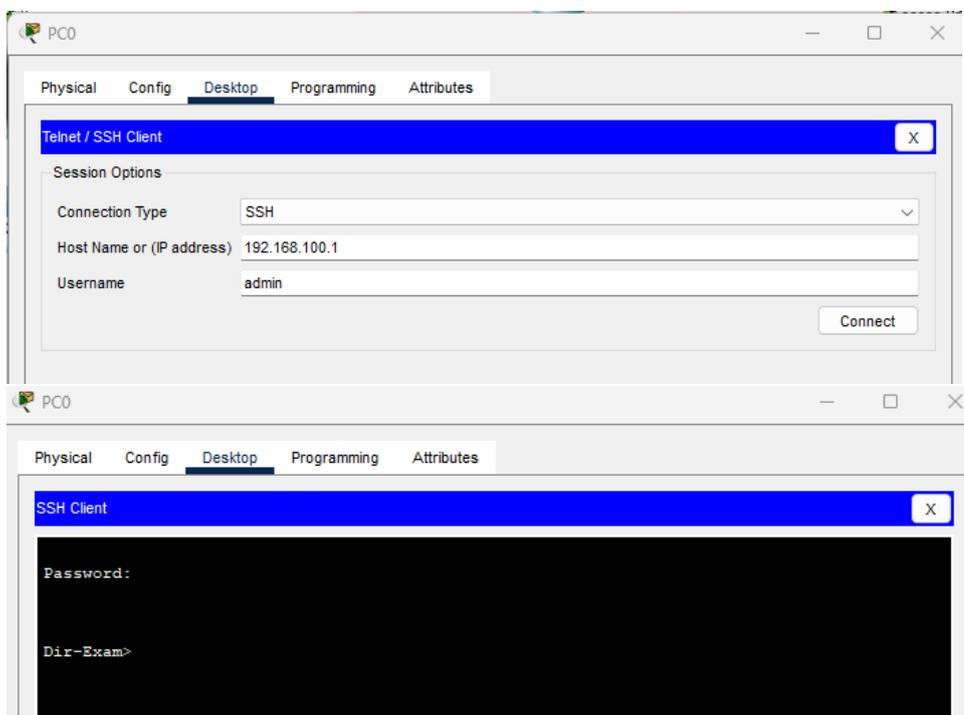
Procédure lourde qui implique d'être physiquement à côté du switch ...
Ne jamais utiliser Telnet (pas sécurisé)

Accès SSH : Sur les Catalyst 2960

```
Dir-Exam# show version
  Show ip ssh
  Enable
  Configure terminal
  Enable secret 1234-Metropole:1234
  Ip domain-name metropole.fr
  Crypto key generate rsa
    1024
  Ip ssh version 2
  Username admin secret 1234-Metropole :1234
  Line vty 0 15
Dir-Exam(config-line)#transport input ssh
  Login local
  Exit
```

Vérifier l'accès à distance avec putty en ssh (plus de port COM) :

```
Ssh utilisateur@ip
Ssh -l admin 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 va utiliser un tunnel VPN entre les 2 routeurs.

Plan d'adressage site distant :

PC1-VPN	PC2-VPN	Imp-VPN	Passerelle
192.168.110.1	192.168.110.2	192.168.110.3	192.168.110.254

- 2) Configurer le routeur pour le sécuriser

Objectif sécurité !

- Configurer :
1. Le nom de l'hôte.
 2. Un mot de passe pour le mode privilégié
 3. La configuration SSHv2, avec un utilisateur admin, la création d'une clé SSH et d'un nom de domaine.
 4. Un mot de passe pour l'accès console.
 5. Un mot de passe pour les ligne VTY pour l'accès
 6. Le cryptage des mot de passe
 7. L'affichage d'une bannière légale d'accès non autorisée.
 8. La copie de la configuration en mémoire non volatile.

```
Router > enable
```

```
Router# configure terminal
```

```
Router(config)# host secret 1234-Metropole :1234
```

```
ip domain-name metropole.fr
```

```
username admin secret 1234-Metropole :1234
```

```
crypto key generate RSA
```

```
1024
```

```
ip ssh version 2
```

```
line console 0
```

```
RouteurVPN(config-line)# password 1234-Metropole :1234
```

```
RouteurVPN(config-line)# login
```

```
Exit
```

```
RouteurVPN(config)#line vty 0 15
```

```
RouteurVPN(config-line)# transport input ssh
```

```
    Login local
```

```
    Exit
```

```
RouteurVPN(config)# service password-encryption
```

```
    Banner motd #Accès autorisé seulement.#
```

```
    Exit
```

```
RouteurVPN# copy running-config startup-config
```

Même configuration sur RouteurMetro.

3) Configuration des interfaces routeurs

Pour être disponible, une interface doit :

- Être configuration avec au moins une adresse IP (commandes `IP address` et `ipv6 address`),
- Être activé car elle ne l'est pas par défaut (commande `no shutdown`) et l'interface doit être connectée à un autre périphérique,
- Avoir une description (optionnel, max 240 caractères).

Sur le routeur VPN :

```
RouteurVPN(config)#interface GigabitEthernet0/0
```

```
RouteurVPN(config-if)#ip address 192.168.110.254 10.1 255.255.255.0
```

```
    ipv6 address 2001 :db8 :acad :110 ::254 10 :: 1 /64
```

```
    No shutdown
```

```
    Description lien sous-reseau VPN
```

```
    Exit
```

```
RouteurVPN(config)#interface Serial 0/1/1 0
```

```
RouteurVPN(config-if)#ip address 10.0.0.2 1 255.255.255.0
```

```
    ipv6 address 2001 :db8 : acad : 1001 :: 2 1 /64
```

```
    No shutdown
```

```
    Description Lien routeurVPN - RouteurMetro
```

```
    Exit
```

Même config sur Routeur Metro

Configuration de l'adresse de bouclage :

Une interface de bouclage est une interface logique interne au routeur. Elle n'est pas attribuée à un port physique et ne peut pas être connectée à un périphérique. Elle est automatiquement « up » tant que le routeur fonctionne.

```
RouteurVPN(config)# interface loopback 0
RouteurVPN(config-if)#ip address 192.168.200.2 255.255.255.0
exit
```

Même config sur RouteurMetro.

4) Configuration du routage

Lorsqu'un routeur reçoit un paquet sur une interface, il détermine sur quelle interface le renvoyer en consultant sa table de routage. Elle est remplie de différentes façons :

- Réseaux directement connectés : lorsqu'une interface est configurée avec une IP et un masque.
- Réseaux distant, non directement connectés.
 - ➔ Route statique, définie manuellement avec une passerelle
 - ➔ Route dynamique par les protocoles OSPF et EIGRP
- Route par défaut 0.0.0.0

Sur routeurVPN :

```
RouteurVPN(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.1
```

Sur routeurMetro :

```
RouteurVPN(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 10.0.0.1
```

Sur le cœur de réseaux :

- Donner un nom
- Configurer les interfaces
- Configurer les routes

```
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
Exit
SwitchL3(config)#ip routing
Ip route 0.0.0.0 0.0.0.0 192.168.10.1
```

5) Vérification

Commandes : `show ip interface brief`
----- ipv6 -----

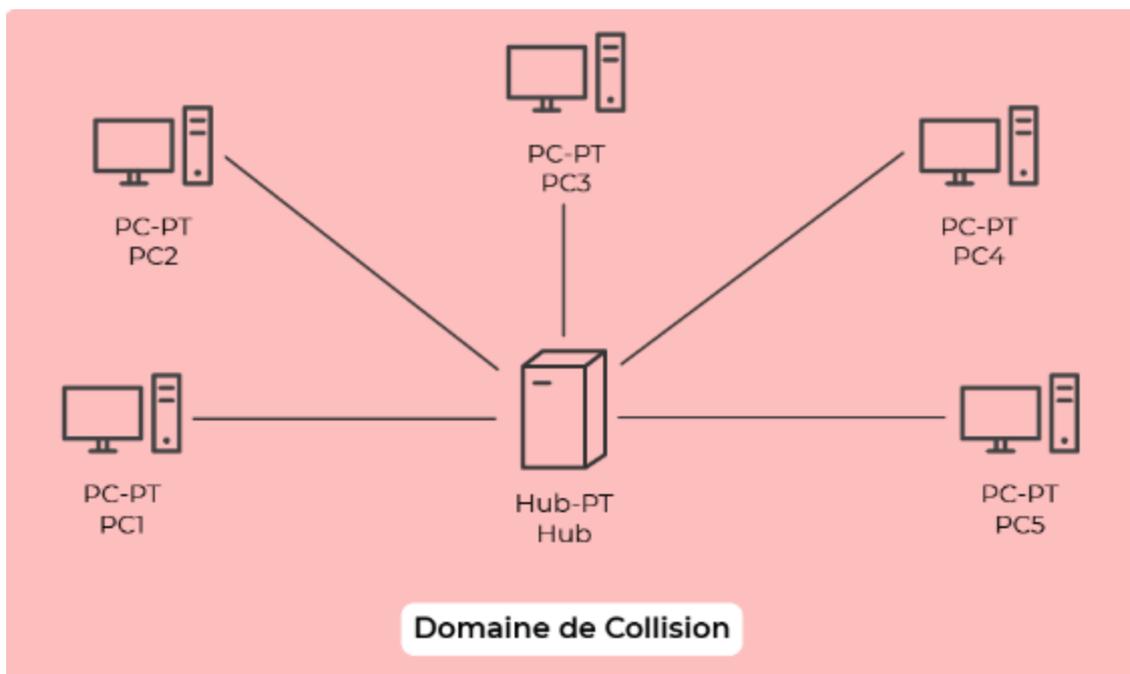
VII. Configuration des VLANs

1) Identifier les domaines de collision et de diffusion

Collision : quand 2 paquets sont émis en même temps sur le réseaux

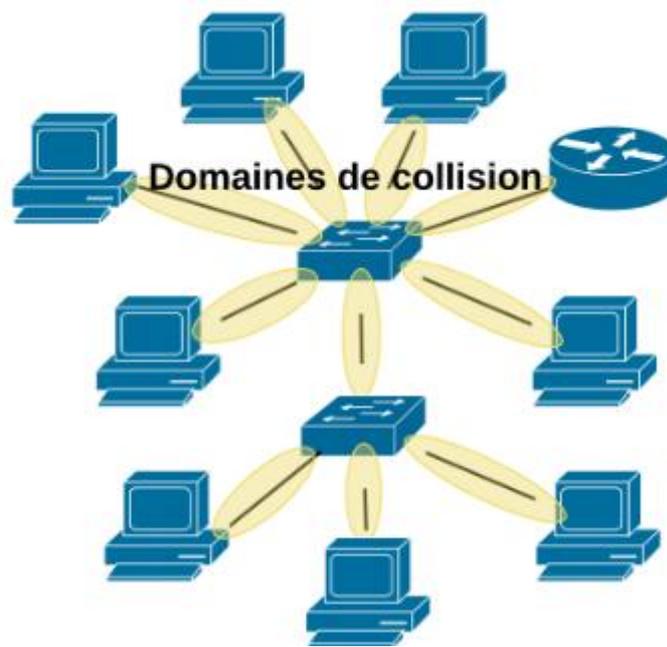
Congestion : Quand l'augmentation du trafic ralentit le réseaux.

Domaine de collision avec un concentrateur (hub).

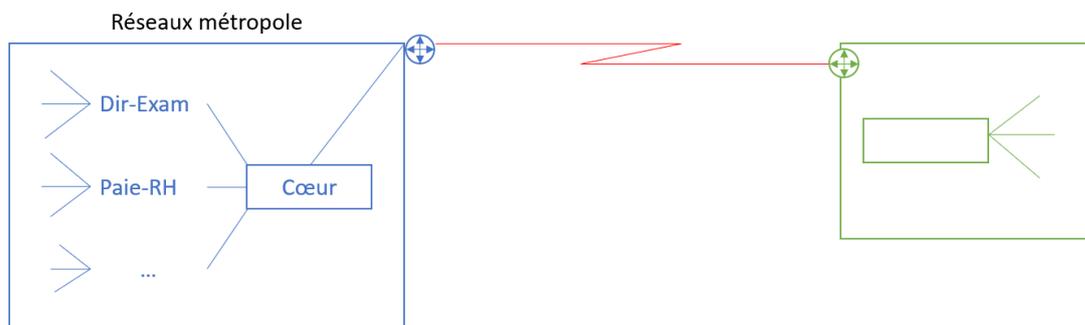


Domaine de collision avec un commutateur (switch) :

- Chaque segment est dans son propre domaine de collision,
- Plus les domaines de collision sont petits et meilleur est le réseau.



Domaine de diffusion : ensemble de commutateur connectés. Seul un routeur peut réduire le domaine de diffusion (et de collision).



3 domaines de diffusion seulement. Le domaine de diffusion du réseau Métropole est très grand : ce n'est pas BON ! Risques de congestion, car tous les commutateurs renvoient les trames de diffusion à l'ensemble des machines connectées (sauf l'émetteur). Pour éviter d'acheter des routeurs supplémentaires, on crée des VLANS !!!

2) Utilisation des VLANs

Les Vlan permettent à un administrateur réseaux de segmenter son réseau en fonction des services, équipes logiciels de l'entreprise, **d'où l'importance de connaître les métiers de ses clients.**

Chaque VLAN est considéré comme un réseau logique indépendant, même s'il partage la même infrastructure (switch). Les autres VLANs ne sont pas impactés par les trames de diffusion.

Exemple dans le réseaux Métropole, on ne peut mettre toutes les imprimantes dans le même VLAN. Cela a des conséquences sur le plan d'adressage :

Groupes	VLAN ID	Adresse réseau	Première adresse	Dernière adresse	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	192.168.22.253
Emploi	23	192.168.23.0	192.168.23.1	192.168.23.253	192.168.23.254
Médecine	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	192.168.24.254
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
Téléphones	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

Avantage de la conception d'un réseaux avec des VLANs :

- Domaines de diffusion plus petit : moins de périphérique dans le domaine de diffusion.
- Sécurité optimisée : seuls les utilisateur d'un même VLANs peuvent communiquer ensemble.
- Amélioration de l'efficacité des ressources IT : les utilisateur ayant des besoin similaires sont sur le même VLAN qui peut être nommé.
- Coût Réduit : réduction du trafic inutile.
- Gestion simplifiée : regroupement des utilisateurs, périphériques ...

Les types de VLAN :

a) VLAN par défaut

- VLAN 1, tous les ports sont dedans
- C'est aussi le VLAN natif
- C'est aussi le VLAN de gestion
- Il ne peut pas être renommé ou supprimé

Commande : `show vlan brief`

b) VLAN de données

Pour séparer le trafic en groupes d'utilisateurs ou périphériques.

c) VLAN natif

Les ports de TRUNK sont utilisés entre les commutateurs pour agglomérer les transmissions de plusieurs VLAN. En général, on va dédier un VLAN natif différent de 1 pour mettre tous les ports TRUNK.

d) VLAN de gestion

Configuré spécialement pour les administrateurs : SSH, HTTPS, SNMP.

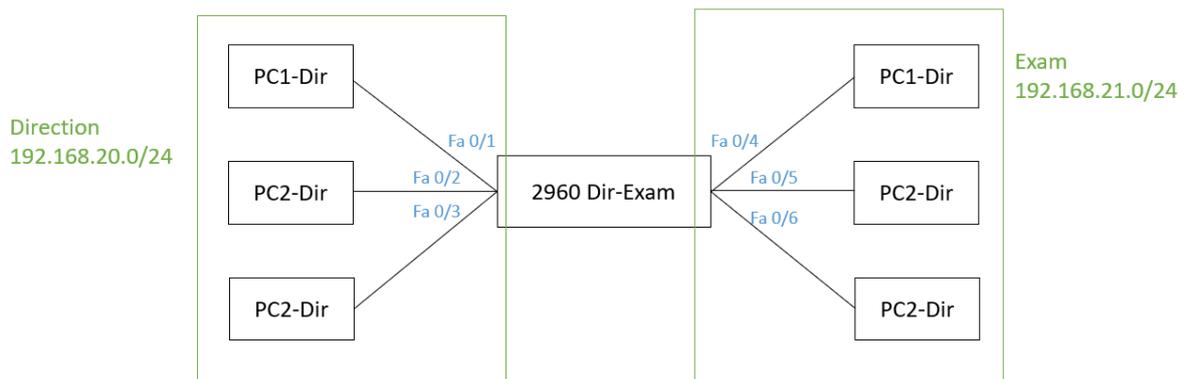
e) VLAN voix

Pour prendre en charge la VOIP.

- Bande passante consolidée pour la qualité de la voix
- Priorité de transmission sur les autres VLANs
- Possibilité de routage multiple
- Délai de ping < 150 ms

3) Paramétrer les VLANs

Exemple pour le commutateur Dir-Exam :



Création de 5 VLANs :

ID	Nom
20	Direction
21	Exam
40	Impression
50	Téléphonie
100	Administration

```

Dir-Exam# configure terminal
Dir-Exam(config)#VLAN 20
Dir-Exam(config-vlan)#name Direction
Exit

```

Paie-Emploi :

ID	Nom
22	Paie-DRH
23	Emploi
40	Impression
50	Téléphonie
100	Administration

Med-Assu :

ID	Nom
24	Médecine
25	Assurance
40	Impression
50	Téléphonie
100	Administration

Info :

ID	Nom
27	Informatique
30	Serveurs
40	Impression
50	Téléphonie
100	Administration

Pour PC1 :

```

Dir-Exam(config)#int fa 0/1
Dir-Exam(config-if)#Switchport mode access
Switchport access VLAN 20
Exit

```

Pour PC2, VLAN 20 aussi.

Pour Imp, VLAN 40 ! Show VLAN brief

```
Dir-Exam#show VLAN brief
```

VLAN Name	Status	Ports
1 default	active	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
20 Direction	active	Fa0/1, Fa0/2, Fa0/7
21 Exam	active	Fa0/4, Fa0/5
40 Impression	active	Fa0/3, Fa0/6
50 telephonie	active	
100 Administration	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

```
Dir-Exam#
```

```
Paie-Empl#show VLAN b
```

VLAN Name	Status	Ports
1 default	active	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
22 Paie-DRH	active	Fa0/1, Fa0/2
23 Emploi	active	Fa0/4, Fa0/5
40 Impression	active	Fa0/3, Fa0/6
50 Telephonie	active	
100 Administration	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

```
Paie-Empl#
```

```
Med-Assu#show vlan b
```

VLAN Name	Status	Ports
1 default	active	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
24 Medecine	active	Fa0/1, Fa0/2
25 Assurance	active	Fa0/4, Fa0/5
40 Impression	active	Fa0/3, Fa0/6
50 Telephonie	active	
100 Administration	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

```
Med-Assu#
```

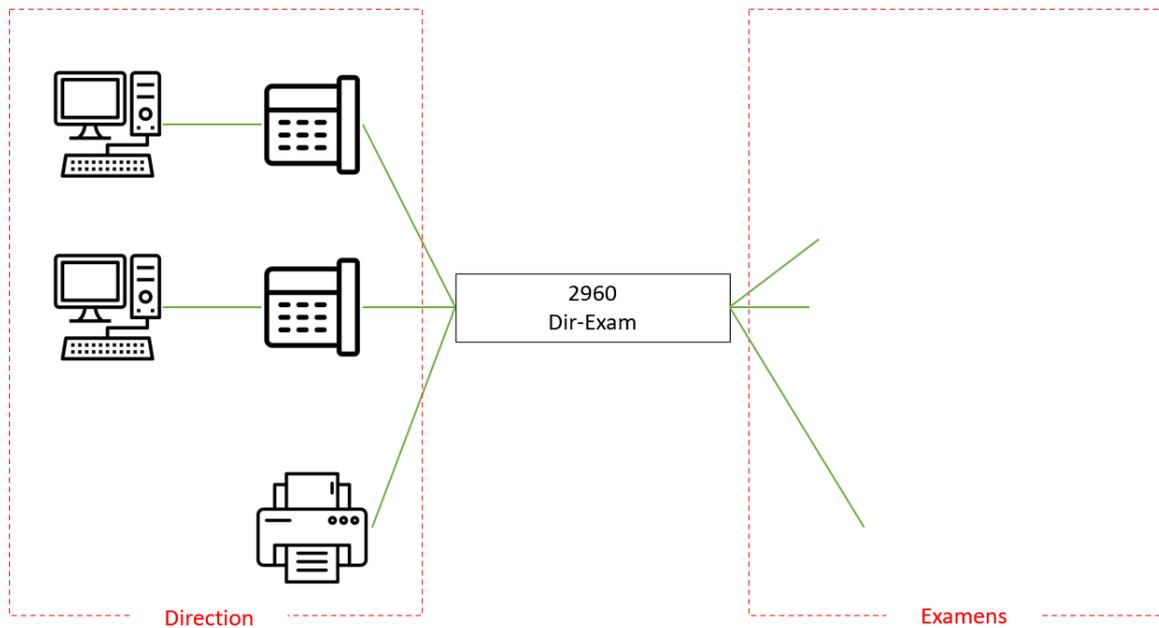
```
show vlan br
```

VLAN Name	Status	Ports
1 default	active	Fa0/2, 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
27 Informatique	active	Fa0/1
30 Serveurs	active	
40 Impression	active	Fa0/3
50 Telephonie	active	
100 Administration	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

```
info#
```

VIII. Ajout de la téléphonie IP

1) Ajout des téléphones



A faire dans tous les services.

Ne pas oublier d'allumer les téléphones.

2) Configuration

Il faut configurer le commutateur pour rajouter le VLAN voix sur les ports connectés aux téléphones.

Rappel : un seul VLAN par interface sauf pour les VLAN voix et les TRUNK.

Pour la téléphonie, il faut aussi activer la qualité de service (QoS).

Exemple Dir-Exam :

```
Dir-Exam(config)# int f0/1
Dir-Exam(config-if)# mls qos trust cos
Switchport voice vlan 50
Exit
```

Refaire avec f0/2

Ou bien int f0/1-2 pour faire les 2 en même temps. Refaire avec f0/4 et f0/5 et les autres services ;

3) Vérifications

Show vlan (brief)

Show interfaces fa0/1 switchport

Pour modifier le VLAN d'un port : `switchport access vlan nouvel-ID`

----- supprimer ----- : `no switchport access vlan`

-----un VLAN : `no vlan vlan-ID`

Pour revenir à la configuration d'usine on supprime le

fichier de configuration : `delete vlan.dat` (et redémarrer !)

Pour rétablir la configuration d'usine :

- Débrancher tous les câbles réseaux (sauf console)
- `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 VLAN (à moins que la liste des VLAN autorisés ne soit restreinte manuellement ou dynamiquement).

Pour activer la liaison Trunk du commutateur Dir-Exam, configurez le port d'interconnexion avec l'ensemble des commandes de configuration d'interface indiquées dans ce tableau :

Tâche	Commande IOS
Passer en mode de configuration globale	Dir-Exam# configure terminal
Passer en mode de configuration d'interface	Dir-Exam(config)# interface g0/1
Régler le port en mode de trunking permanent	Dir-Exam(config-if)# switchport mode trunk
Choisir un VLAN natif autre que le VLAN 1	Dir-Exam(config-if)# switchport trunk native vlan 100

Indiquer la liste des VLAN autorisés sur la liaison Trunk	Dir-Exam(config-if)# switchport trunk allowed vlan 20,21,40,50,100
Repasser en mode d'exécution privilégié	Dir-Exam(config-vlan)# end

Il faut que vous fassiez de même sur le lien Trunk des commutateurs Paie-Emp, Med-Assu et Info.

Pour vérifier que le lien Trunk est bien configuré, utilisez la commande show interfaces vue précédemment, mais cette fois-ci sur l'interface où est configuré le Trunk :

```
Dir-Exam# show interface g0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 100 (Administration)
Voice VLAN: none
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: 20-21,40,100
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 réinitialiser le port Trunk à l'état par défaut, utilisez les commandes no switchport allowed vlan et no switchport trunk native vlan pour supprimer les VLAN autorisés et réinitialiser le VLAN natif du Trunk.

Lorsqu'il est remis à l'état par défaut, le Trunk autorise tous les VLAN, et utilise le VLAN 1 comme VLAN natif.

5) Réalisez le routage inter-vlan

La configuration de notre cœur de réseau (commutateur de niveau 3) diffère très peu de la configuration d'un commutateur de niveau 2 :

- *Créer les VLAN dans le commutateur de niveau 3.*
- *Affecter les VLAN dans les différentes interfaces.*
- *Créer les liaisons Trunks et autoriser les VLAN sur ces liaisons Trunks.*

```
SwitchL3(config)# vlan 20
SwitchL3(config-vlan)# name Direction
SwitchL3(config-vlan)# exit
SwitchL3(config)# vlan 21
SwitchL3(config-vlan)# name Examen/Concours
SwitchL3(config-vlan)# exit
SwitchL3(config)# vlan 22
SwitchL3(config-vlan)# name Paie/DRH
SwitchL3(config-vlan)# exit
SwitchL3(config)# vlan 23
SwitchL3(config-vlan)# name Emploi
SwitchL3(config-vlan)# exit
SwitchL3(config)# vlan 24
SwitchL3(config-vlan)# name Medecine
SwitchL3(config-vlan)# exit
SwitchL3(config)# vlan 25
SwitchL3(config-vlan)# name Assurance
SwitchL3(config-vlan)# exit
SwitchL3(config)# vlan 27
SwitchL3(config-vlan)# name Info/RGPD
SwitchL3(config-vlan)# exit
SwitchL3(config)# vlan 30
SwitchL3(config-vlan)# name Serveurs
SwitchL3(config-vlan)# exit
SwitchL3(config)# vlan 40
SwitchL3(config-vlan)# name Impression
SwitchL3(config-vlan)# exit
SwitchL3(config)# vlan 50
SwitchL3(config-vlan)# name Telephonie
SwitchL3(config-vlan)# exit
SwitchL3(config)# vlan 60
SwitchL3(config-vlan)# name Wifi
SwitchL3(config-vlan)# exit
SwitchL3(config)# vlan 100
SwitchL3(config-vlan)# name Administration
SwitchL3(config-vlan)# exit
SwitchL3(config)# interface g1/0/2
SwitchL3(config-if)# switchport trunk encapsulation dot1q
SwitchL3(config-if)# switchport mode trunk
SwitchL3(config-if)# switchport trunk native vlan 100
SwitchL3(config-if)# switchport trunk allowed vlan 20,21,40,50,100
SwitchL3(config-if)# exit
SwitchL3(config)# interface g1/0/3
SwitchL3(config-if)# switchport trunk encapsulation dot1q
```

```

SwitchL3(config-if)# switchport mode trunk
SwitchL3(config-if)# switchport trunk native vlan 100
SwitchL3(config-if)# switchport trunk allowed vlan 22,23,40,50,100
SwitchL3(config-if)# exit
SwitchL3(config)# interface g1/0/4
SwitchL3(config-if)# switchport trunk encapsulation dot1q
SwitchL3(config-if)# switchport mode trunk
SwitchL3(config-if)# switchport trunk native vlan 100
SwitchL3(config-if)# switchport trunk allowed vlan 24,25,40,50,100
SwitchL3(config-if)# exit
SwitchL3(config)# int g1/0/5
SwitchL3(config-if)# (switchport trunk encapsulation dot1q) déjà par défaut !
SwitchL3(config-if)# switchport mode trunk
SwitchL3(config-if)# switchport trunk native vlan 100
SwitchL3(config-if)# switchport trunk allowed vlan 27,40,50,100
SwitchL3(config-if)# exit
SwitchL3(config)# int g1/0/6
SwitchL3(config-if)# switchport mode access
SwitchL3(config-if)# switchport access vlan 30
SwitchL3(config-if)# exit
SwitchL3(config)# int g1/0/7
SwitchL3(config-if)# switchport mode access
SwitchL3(config-if)# switchport access vlan 30
SwitchL3(config-if)# exit
SwitchL3(config)# int g1/0/8
SwitchL3(config-if)# switchport mode access
SwitchL3(config-if)# switchport access vlan 30
SwitchL3(config-if)# exit
SwitchL3(config)# int g1/0/9
SwitchL3(config-if)# switchport mode access
SwitchL3(config-if)# switchport access vlan 60
SwitchL3(config-if)# exit

```

Il faut bien spécifier l'utilisation des trames en dot1q sur les liaisons Trunks sur un commutateur de niveau 3 en utilisant la commande switchport trunk encapsulation dot1q.

Non, dépend de Cisco / norme 802.1

La capacité d'un commutateur de niveau 3, c'est de faire du routage. Il reste donc à créer une passerelle de routage pour que tous les VLANs puissent communiquer.

- Création des virtuelles (SVI : Switch Virtual interfaces)

```

SwitchL3(config)# interface vlan 20
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

```

Faire de même pour les autres VLANs : 21,22,23,24,25,27,30,40,50,60,100

```
C:\>ping 192.168.22.2

Pinging 192.168.22.2 with 32 bytes of data:

Reply from 192.168.22.2: bytes=32 time=1ms TTL=127
Reply from 192.168.22.2: bytes=32 time=1ms TTL=127
Reply from 192.168.22.2: bytes=32 time=1ms TTL=127
Reply from 192.168.22.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.22.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Ici en faisant un ping du pc1-Dir on obtient une réponse cela veut dire que notre réseaux communique

IX. Sauvegarde des configurations

1) Système de fichiers des routeurs et switches L3

La commande show file systems affiche les diques disponibles : mémoire totale et libre, type de FS, autorisation.

* : Système actuel par défaut

: Disque amorsable

Dir : contenu de FS par défaut

Repérer le `.bin` du système.

```
SwitchL3#show file systems
File Systems:

      Size(b)      Free(b)      Type  Flags  Prefixes
*  1539575808  1034041683  flash  rw  flash:
      29688      23590      nvram  rw  nvram:

SwitchL3#dir
Directory of flash:/

 3  -rw-   505532849      <no date>  cat3k_caa-universalk9.16.03.02.SPA.bin
 4  -rw-     1276      <no date>  vlan.dat

1539575808 bytes total (1034041683 bytes free)
SwitchL3#
```

2) Sauvegarde en mémoire non volatile(NVRAM)

Commandes utiles : `cd` , `pwd` , `dir`

Repérer le fichier de configuration de démarrage : `startup-config`

Sauvegarde de la configuration en cours :

`Copy running-config startup-config`

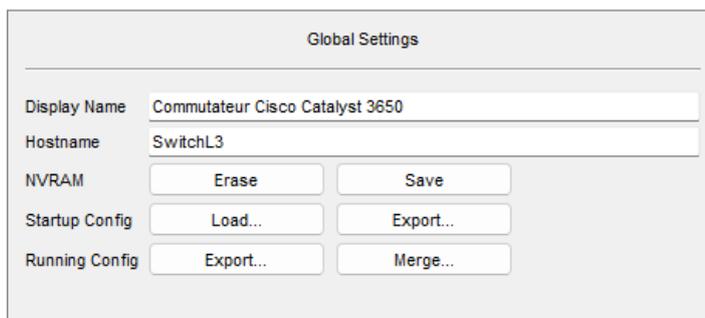
```
SwitchL3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SwitchL3#
```

Quelle commande pour revenir à la configuration de démarrage sans redémarrer ?

`Copy startup-config running-config`

3) Sauvegarde graphique dans PT

→ Menu `Config`



Possibilité aussi de sauvegarde sur un serveur externe en TFTP.

→ Menu `Services`