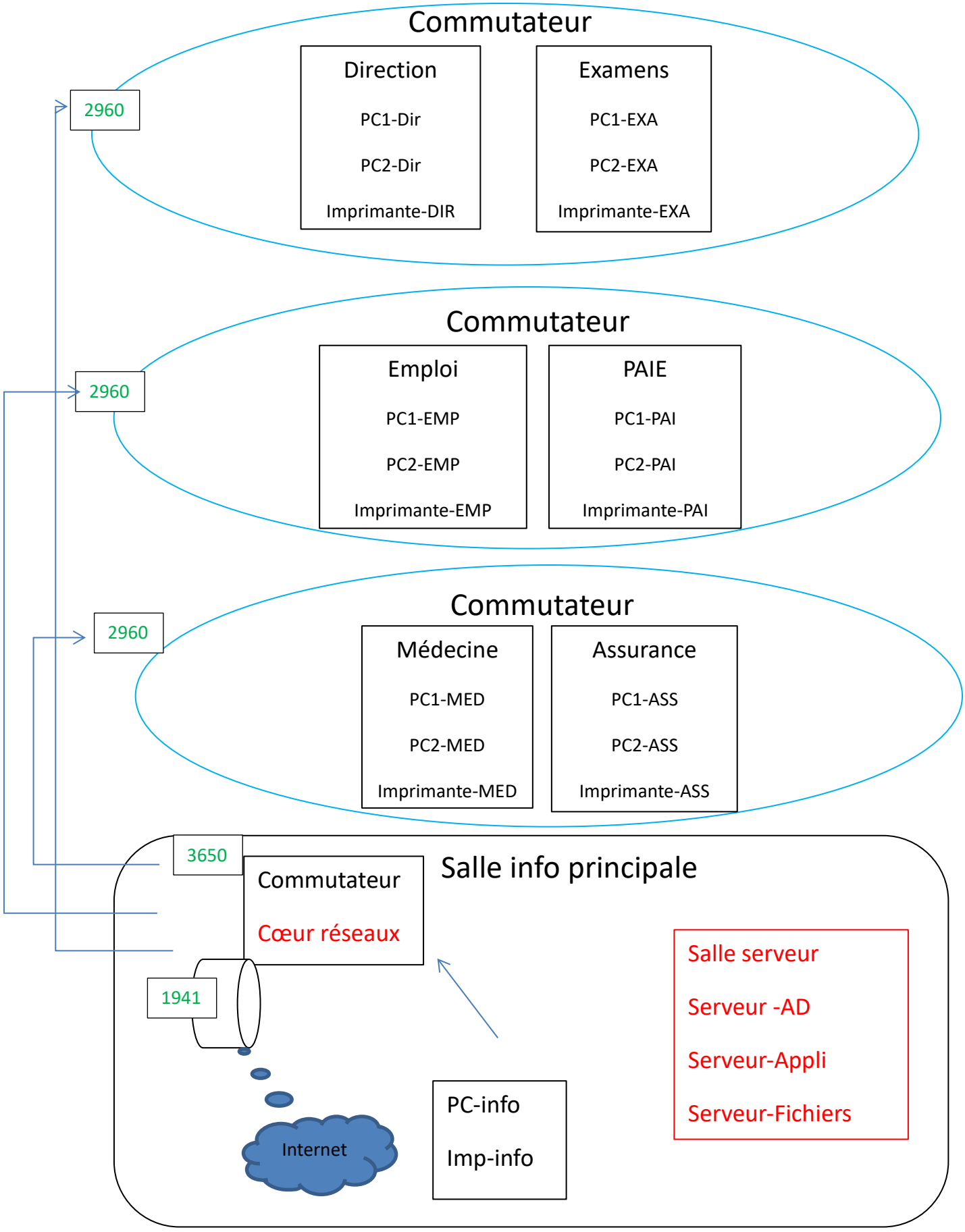
Réseaux complexe

Sommaire

1

I. Réseaux complexe

1/réseaux administratif



BERNARD ARDISSON CISCO Réseau complexe SIO24

Comment choisir les commutateurs et routeur ? quel débit ?

-dans les réseaux, les commutateurs doivent être en Fast Ethernet (100 Mb/s) avec une entrée de 1Gb/s. Cisco Catalyst ?

-Cœur de réseaux en Gb/s donc Cisco Catalyst ?

-routeur Gigabit Ethernet Cisco ?

-comment s'appellent les ports routeurs ?

Les ports routeurs s'appellent g0/0 et g0/1

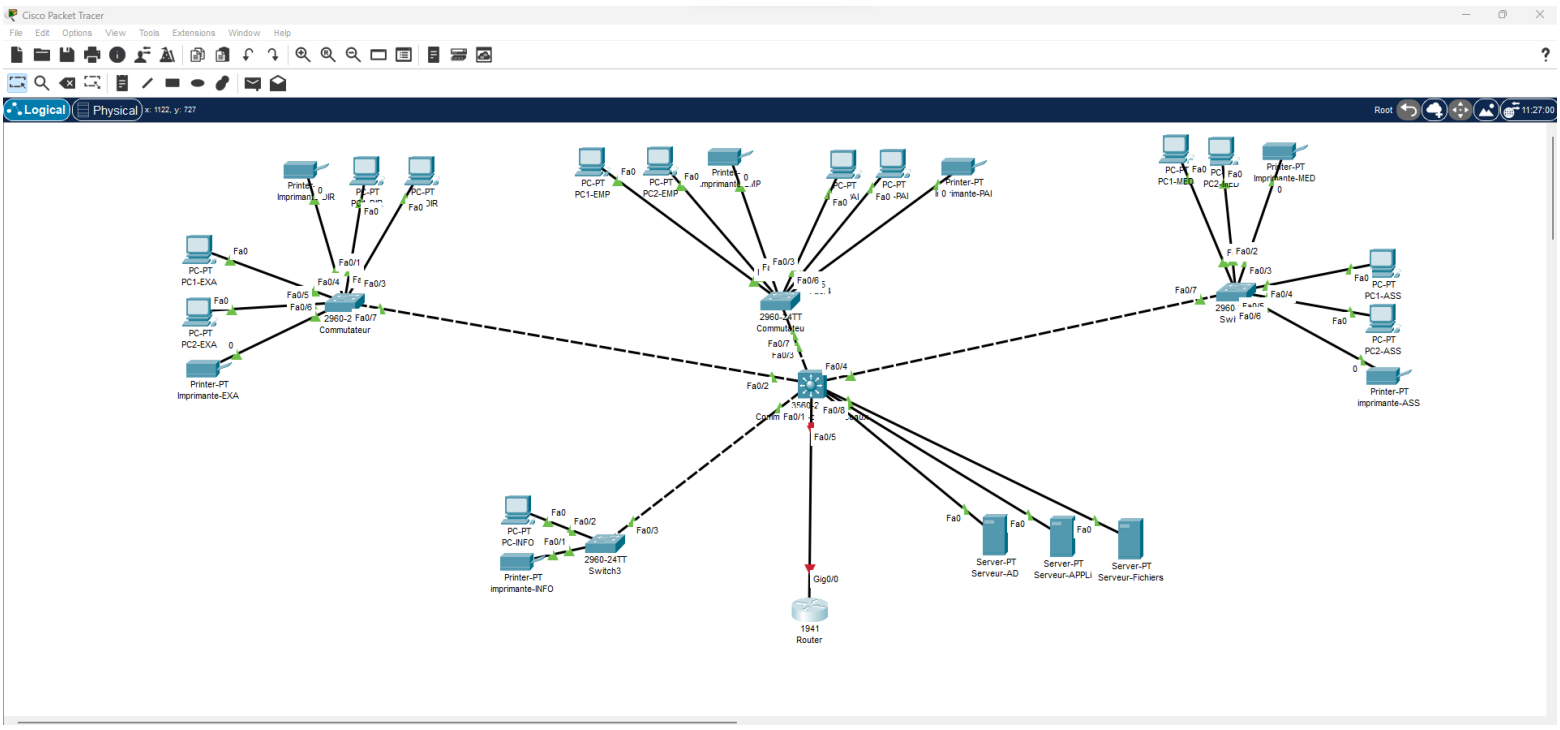
- ..... des commutateurs ?

Les port routeurs s'appellent f0/1 a f0/24, g0/1 et g0/2

-..... du cœur de réseaux ?

Les ports du cœur de réseaux s'appellent g1/0/1 a g1/0/24, g1/1/1 a 1/1/4

Schéma packet tracert :



ATTENTION Les routeurs démarrent leur numérotation a 0, et les commutateurs a 1.

Le cœur de réseaux est de niveau 3 (programmable)

PC1 sur la 1er interface disponible	f0/1	Pc1-DIR
PC2 ……..2èmme ……..	f0/2	PC2-DIR
Imp……..3èmme ……..	f0/3	Imp-DIR
PC1……4èmme ……	f0/4	PC1-Exa
PC2……5èmme……..	f0/5	PC2-Exa
Imp…….6èmme……..	f0/6	Imp-Exa

Dans le Modèle OSI (pour afficher les ports : option /préférences : Always show ports labels)

Plan d'adressage

Groupe	Adresse réseau	1er adresse disponible	Dernière adresse disponible	Passerelle réseau
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	192.16.21.253	192.168.21.254

PAIE : 22

Emploi : 23

Médecine : 24

Assurance : 25

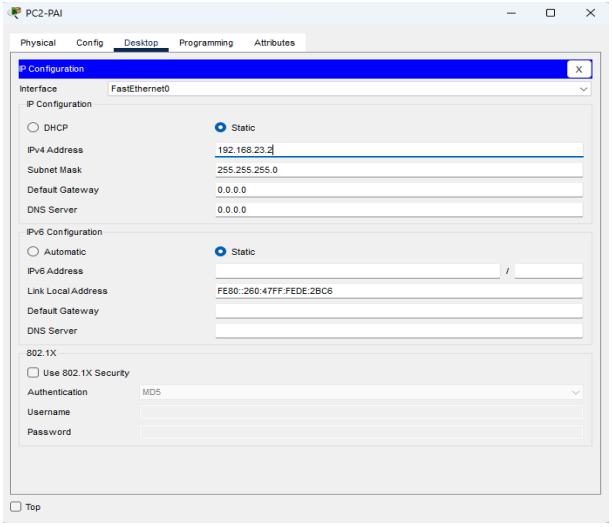
Info : 27

Serveurs : 30

Imprimantes : 40

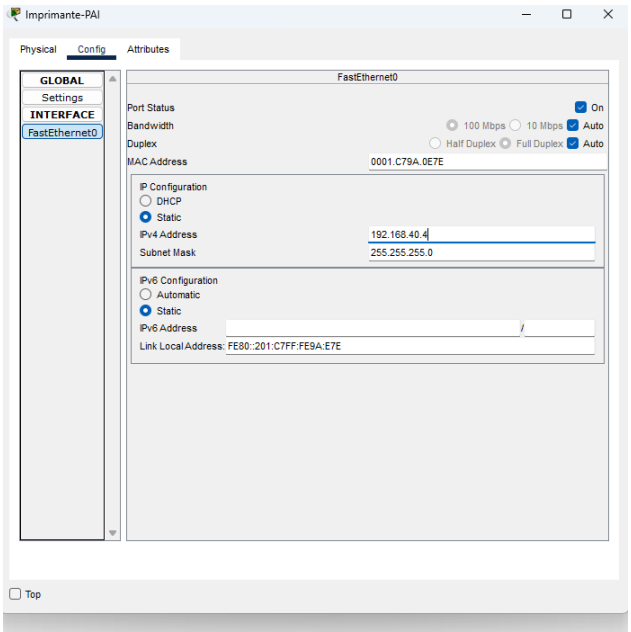
Plan d’adressage des PC :

Groupes	PC 1	PC2	Passerelle
Direction	192.168.20.1	192.168.20.2	192.168.20.254
Examen	192.168.21.1	192.168.21.2	192.16.21.254
Emploi	192.168.22.1	192.168.22.2	192.168.22.254
Paie	192.168.23.1	192.168.23.2	192.168.23.254
Médecine	192.168.24.1	192.168.24.2	192.168.24.254
Assurance	192.168.25.1	192.168.25.2	192.168.25.254
INFO	192.168.27.1		192.168.27.254



Plan d’adressage des imprimantes :

Imp-DIR	Imp-EXA	Imp-PAI	Imp-EMP	Imp-MED	Imp-ASS	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



Plan d'adressage des serveurs :

SRV-AD	SRV-Appli	SRV-Fichiers	Passerelle
192.168.30.1	192.168.30.2	192.168.30.3	192.168.30.254

2/Ajout d'un point d'accès sans fils

Le réseau WIFI sera en 192.168.60.0/24 :

-ajouter un point d'accès AP-PT sur le commutateur central

-ajouter les périphériques : laptop, TV, tablette, smartphone

-ajouter une webcam (menu home)

Configuration :

Nom SSID	Sécurité sans fil	Mot de passe
Métropole	WPA2-PSK	1234-Metropole :1234

En théorie, impossible d'attribuer un IP au point d'accès (couche 2 OSI)

Plan d'adressage :

Laptop	TV	Tablette	Smartphone	Caméra	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

II. Commutateur de couche 2

Les commutateurs maintiennent un tableau dont chaque ligne contient le numéro du port et l'adresse MAC du destinataire. Par conséquent une trame Ethernet avec une adresse de destination sort toujours par le même port, quel que soit son port d'entrée. Une trame Ethernet ne sera jamais transférée sur son port d'entrée.

Rappel : adresse MAC = identifiant unique pour chaque carte réseau composée de 12caractères hexadécimaux :

B4-6D-83 – DD-CE-49

ID : constructeur -> ID :carte réseau

La table d'adresses MAC du commutateur est stockée dans la mémoire de contenu (CAM : content Adressage Memory)

Afficher la table CAM du commutateur Dir-Exam :

Show mac-adresse-table :

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

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

   1    00d0.ff5a.3e02    DYNAMIC     Fa0/7
```

Normalement elle est vide.

Lancez un ping de Pc1-Dir sur Pc2-Dir et redemander la table.

Un port du commutateur est associé à une adresse MAC ou plusieurs par exemple si le commutateur est relié à un autre.

Méthode « switch learn and forward »

Etape 1 : Mode découverte, examen de l'adresse source le commutateur vérifie si de nouvelles informations sont disponibles sur la trame entrante.

-Si l'adresse MAC source n'est pas dans sa table, il ajoute.

-Si l'adresse MAC existe dans la table, il met à jour le computeur d'obsolescence de cette ligne. En général, les entées sont conservées 5 minutes dans la table.

-Si l'adresse MAC existe, mais sur autre port, il doit mettre à jour sur la table …

Un port ------>plusieurs adresses MAC

Une adresse MAC = un seul port

Etapes 2 : Mode transfert, examen de l'adresse de destination.
-Si l'adresse MAC de destination est une adresse de monodiffusion, le commutateur cherche une correspondance dans sa table pour trouver le port de destination.

-Si l'adresse MAC existe, le commutateur transfère la trame.

-Si l'adresse MAC n'existe pas, le commutateur transfère la trame
Sur tous les ports sauf le port d'entrée (monodiffusion inconnue)

-Si l'adresse MAC de destination est une diffusion ou multidiffusion, la trame est également envoyée sur tous les ports sauf le port d'entrée.

Les décisions de transfert de trames dans les commutateurs sont très rapides grâce à des circuits intégrés spécifiques aux applications (ASIC). Deux méthodes sont utilisées :

-Commutation de stockage et de retransmission (Store and forward). Vérification d'erreurs sur la trame avec des algorithmes de contrôle de redondance cyclique (CRC) -> Cisco

- Commutation par coupure (Cut through), plus rapide mais sans vérification

Interface CLI

Certains équipements d'interconnexion ont une interface graphique, mais tous ont une interface CLI (Commande Line Interface) plus complète.
Dans Packet Tracer, deux méthodes modes de commande :

-Utilisateur (view-only) : fonctionnalités limitées, pour les opérations de base.
Invite se termine par >

-Privilégié (mode actif) : pour les commandes de configuration
Invite de commande se termine par #

Pour configurer, l'utilisateur doit passer en mode de configuration globale : l'invité se termine (config) # après le nom de l'appareil.
Deux sous-modes sont régulièrement utilisés :
-le mode de configuration de ligne, pour SSH par exemple : invite se termine par Switch(config-ligne) #
-le mode de configuration d'interface, pour configurer un port par exemple : invite se termine par switch (config-if) #

Commande :
-Pour passer du mode utilisateur ou mode privilégié : enable
-pour l'inverse : disable
-pour passer en mode configuration globale : configure terminal
-pour revenir en mode d'exécution privilégié : exit
-sous-modede configuration de ligne : line
- « « « « « « « « « « « « d'interface : interface
-pour revenir en mode configuration globale : exit
Pour passer d'un sous-mode au mode d'exécution privilégié : end ou CTRL + Z

Exemple :

```
Switch > enable
Switch # configure terminal
Switch(config) # line console 0
```

Simplifié

```
en
conf t
line c 0
exit
int F0/1
exit
```

Switch(config-line) # exit
Switch(config) # interface FastEthernet 0/1
Switch(config-if) # exit
Switch(config)

PENSEZ à l'autocomplétions « ? » pour l'aide

Pensez à afficher la table (en mode utilisateur)

III. Configuration de commutateurs de niveau 2

Interface SVI

Les commutateurs de niveau 2 n'ont pas d'adresse IP mais sont équipés de ports physiques pour se connecter par câble.
Dans Packet Tracert, on utilise les SVI (Switch Virtual Interface) : interface logicielle. Chaque commutateur dispose d'une SVI dans le VLAN1 par défaut. Par défaut, tous les ports sont dans le VLAN1.
Dans le mode d'exécution privilégié, pour afficher les VLAN : show vlan brief
Pour des raisons de sécurité, on utilise des VLAN différents de VLAN1. Nous utiliserons VLAN10 pour les connexions entre commutateurs et VLAN 100 pour les équipements réseau.

Groupes	VLAN ID	Adressse réseau	Première adresse disponible	Derrière adresse	Passerelle
Périphériques Réseaux	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

Pour le VLAN 100 :

VLAN 100	Adresse IPV4	Adresse IPV6

Commutateur Cisco Catalyst 3650	192.168.100.1	2001 :db8 :acad :100 ::1 /64
Commutateur Dir-EXAM	12.168.100.2 /24	----------2 /64
PAIE-Emp	----------.3 /24	
MED-ASSU	----------.4	
INFO	----------.5	
Passerelle	192.168.100.254 /24	

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
Dir-Exam (config -if) # ipv6 address 2001 :db8 :acad :100 ::2 /64
Dir-Exam (config -if) # no shutdown

Remarques :

- Le SVI du VLAN100 n'apparaîtra pas comme « up » jusqu'à ce que VLAN 100 soit créé et qu'un appareil soir connecté.

- La configuration n'est pas activée par défaut : il faut l'activer dans le mode de configuration globale

  sdm prefer dual-ipv4-and-ipv6 default

  Et retourner dans le mode de configuration privilégié pour

  Unreload

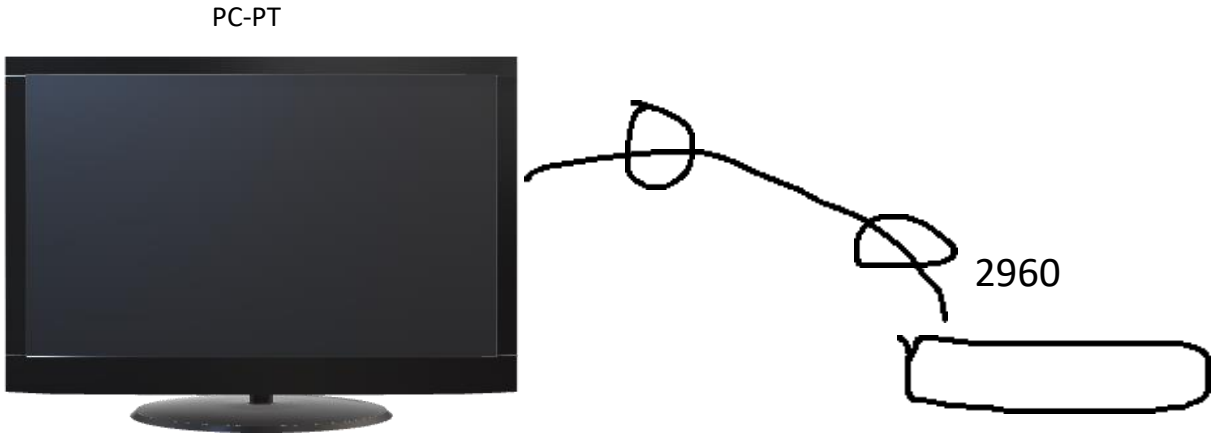
Le SVI du VLAN100 m'apparaitra pas comme "up" jusqu'à ce que VLAN100 soit créé et qu'un appareil soit connecté.

La configuration n'est pas activée par défaut : il faut l'activer dans le mode de configuration globale :
et retourner dans le mode de configuration privilégié pour : reload
Pour configurer la passerelle :
Dire-Exam(config)#ip default-gateway 192.168.100.254
Pour vérifier : show ip interface brief
show ipv6 interface brief

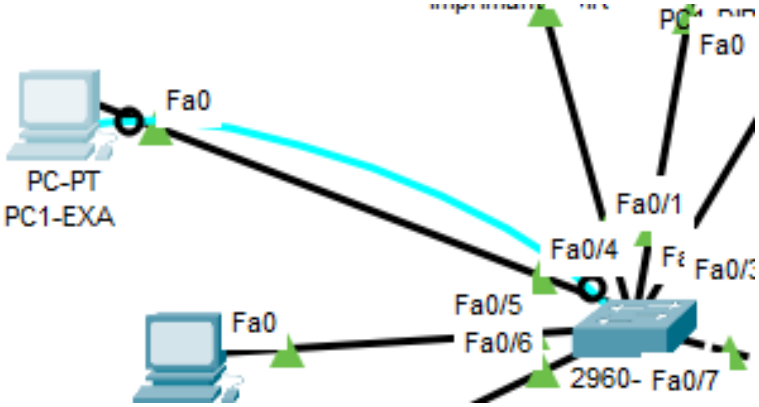
IV. Accès à distance sécurisé d'un commutateur

Accès en port console (RJ45) du switch et à un port COM (série, RS232) d'un PC

Simulation sur Packet Tracer :



Les ports COM et console sont en train de disparaitre, remplacés par de l'USB. C'est une méthode peu pratique car il faut se déplacer



Accès en SSH :

Il ne faut plus utiliser telnet qui n'est pas sécurisé !

Comme toutes les données d'un réseau transitent par les commutateurs, il faut absolument les sécuriser.

Les catalyses prennent en charge SSH à partir des versions d'ios qui contiennent K9 dans leur nom.

DIR-EXA# show ip ssh

DIR-EXA# configure terminal

DIR-EXA (config)# enable secret 1234-MetroPole :1234

DIR-EXA(config)# ip domain-name metropole.com

DIR-EXA (config)# ip ssh version 2

DIR-EXA (config)# crypto key generate rsa

1024

DIR-EXA (config)# username admin secret 1234-MetroPole :1234

DIR-EXA (config)# line vty 0 15

DIR-EXA (config)# transport input ssh

DIR-EXA (config)# login local

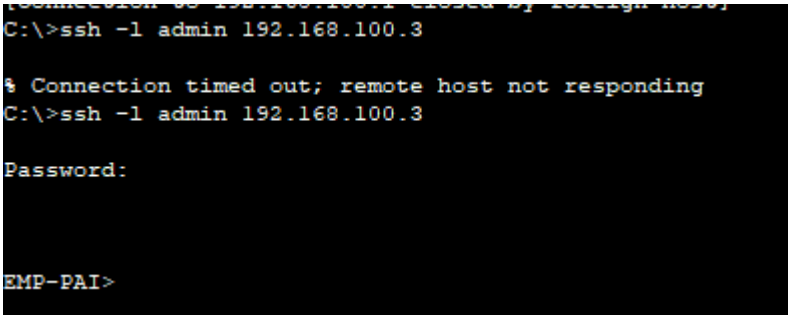
DIR-EXA (config)# exit

VTY correspond aux interfaces virtuelles pour l'accès à distance. Le fait de limiter les connexions sur les terminaux 0 à 15 permet d'empêcher les connexions non SSH (comme telnet)

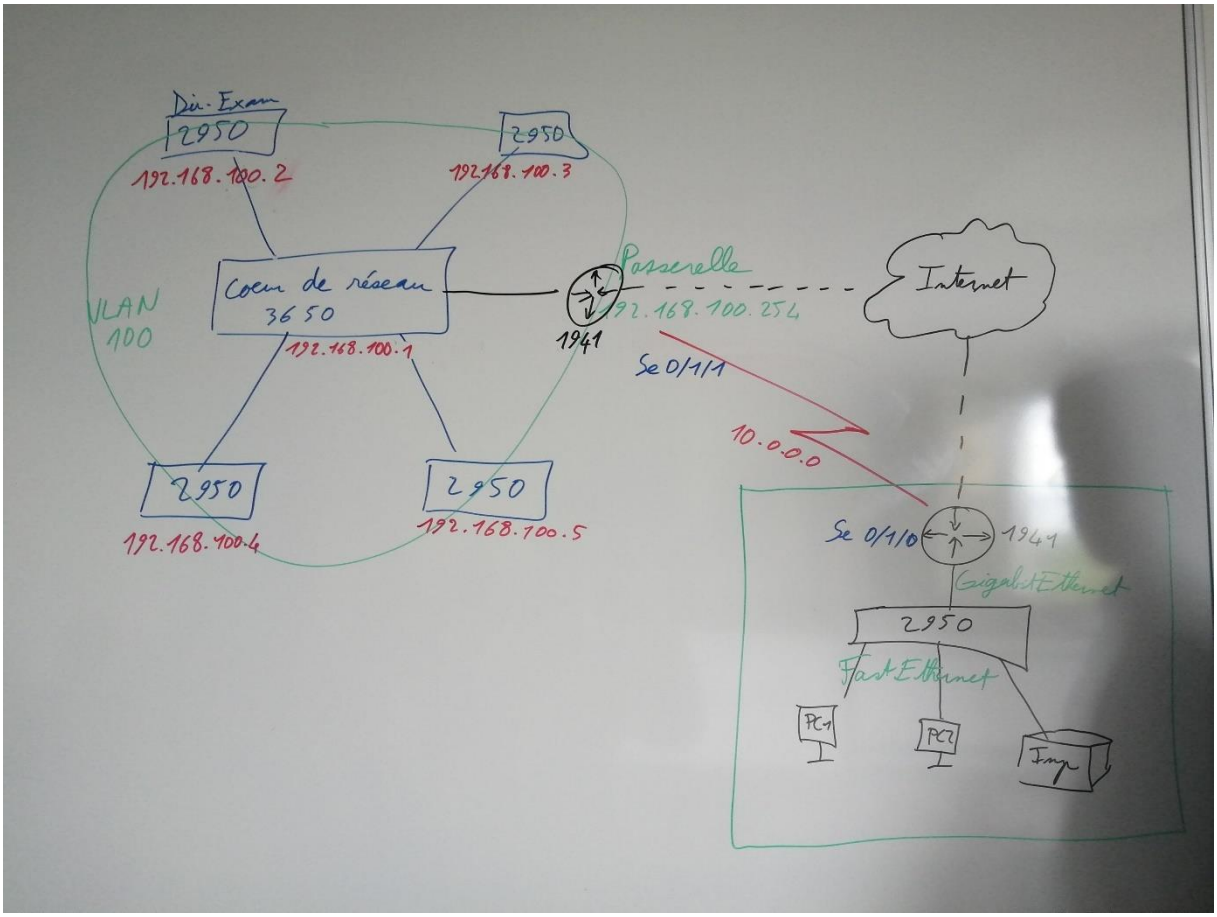
Pour vérifier l'accès SSH : lancer une invite de commandes sous Windows (ou Putty), ou un terminal utilisateur sous linux .

Ssh utilisateur@ip

Sous Packet Tracer, utiliser Command Prompt dans le Desktop du PC.



V. Configuration des routeurs



1) On veut relier e site principale à un site distant en passant par Internet. Pour sécuriser la connexion, on utilise un tunnel VPN entre deux routeurs
   La liaison VPN est représentée par un câble série ↯ . Pour cela, il faut ajouter une carte HWIC-2T aux 2 routeurs..
   Le câble série représente en fait une liaison WAN, câble DTE/DCE

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) Configurer le routeur pour le sécuriser

   -Nom de l'hôte
   -Mot de passe du mode privilégié
   -Configuration SSH v2, utilisateur admin, clé RSA 1024, nom de domaine

-Mot de passe port console
-Mot de passe lignes VTY pour SSH
-Cryptage
-Affichage d'une bannière
-Copie de la configuration en mémoire non volatile

Sur le routeur distant :

Routeur> enable
Routeur#configure terminal
Routeur(config)#hostname RouteurVPN
RouteurVPN(config)# enable secret 123-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
routeurVPN(config-line)# password 1234-MetroPole :1234
_____#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 aux personnes autorisées seulement !#
_____ exit

Faire la même configuration sur le routeur du site principal RouteurCG

3) Configurationdes interfaces sur les routeurs

Pour être disnponible, une interface doit :

--être configurée avec au moins une adresse IP
Ip adress AdressIP/Masque
Ipv6 adress AdressIP/Préfixe
--être activée car elles ne le sont pas par default
No shutdown

Cela revient à mettre l'interface sous tension .il faut aussi qu'elle soit connectée à un autre périphérique pour que la couche physique fonctionne.

--Avoir une description (facultative) : 240 caractères maximum.
Exemple sur RouteurVPN :

```
RouteurVPN(config)# interface GigabitEthernet 0/0
RouteurVPN(config-if)#ip adress 192.168.110.254 255.255.255.0
RouteurVPN(config-if)#ipv6 adress 2001 :db8 :acad :110 ::254/64
_____description Lien sous-Réseau  VPN
_____No shutdown
_____exit
RouteurVPN(config)#interface serial 0/1/1
RouteurVPN(config-if)#ip adress 10.0.0.2 255.255.255.0
_____ ipv6 adress 2001 :db8 :acad :1001 ::2/64
_____description Lien RouteurVPN-RouteurCG
_____no shutdown
_____ exit

Faire aussi le routeurCG
Serial 0/1/0n10.0.0.1/24    2001 :db8 :acad
```

Adresse de bouclage du routeur :

L'interface de bouclage est une interface logique interne au routeur. Elle n'est pas attribuw cwée à un pont physique et ne peut être connectée à un autre appareil. Elle est automatique-ment placée en « up » (active) quand le routeur est allumé. Elle est utile pour les tests et la gestion du routeur, car elle garantit qu'au moins une interface est toujours disponible.

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

Et pour le RouteurCG : 192.168.200.1/24

4) Configurer le routage du routeur

Un routeur a au moins 2interfaces disponibles pour relier 2 réseaux différents. Lorsqu'un un routeur reçoit un paquet, il détermine quelle inteface il doit utiliser pour le transférer. Sa fonction est donc de calculer le plus court chemin en fonction de sa table de routage.

Exemple : Le meilleur chemin pour atteindre la machine 172.16.0.10 sera la correspondance la plus longue dans la table.

Route	Réseau	Adresse binaire
1	172.16.0.0/12	10101100.00010000.00000000.00001010
2	192.16.0.0/18	10101100.00010000.00000000.00001010
3	172.16.0.0/26	10101100.00010000.00000000.00001010

La correspondance la plus longue est la route 3

Les tables de routage se remplissent de plusieurs manières :

-Les réseaux directement connectés sont configurés sur les interfaces du routeur et ajoutés automatiquement à la table de routage dès qu'elles sont actives.

-Les réseaux distants ne sont pas connectés directement donc :

. On peut définir une route statique manuellement ;

. Utiliser les protocoles de routage dynamique qui apprennent Dynamiquement des paquets qui transitent. OSPF (open shortest routing path first) et EIGRP (enchanced Interior Gateway routing protocol)……

-une route par defaut specifie le routeur suivent lorsqu'il n'y a pas de correspondance dans la table. Elle est définie statiquement ou dynamiquement.

Nous avons 3 routeurs à configurer (avec le switch de niveau 3) :

-Table de routage de réseauVPN :

Destination	Masque	Passerelle
0.0.0.0	0.0.0.0	10.0.0.1

On configure une roue par défaut car c'est un routeur d'extrémité. Donc pour aller ailleurs que sur votre sous-réseau 192.168.110.0/24, vous êtes obligé de passer par la passerelle 10.0.0.1

RouteurVPN(config)# ip route 0.0.0.0 0.0.0.0 10.0.0.1

Pas la peine de spécifier les interfaces sur les routeurs CISCO.

RouteurVPN(config)# ipv6 unicast-routing

_____ ipv6 route ::/0 2001 :db8 :acad :1001 ::1

-Table de routage de réseauCG :

Destination	Masque	Passerelle
192.168.110.0	255.255.255.0	10.0.0.2
0.0.0.0	0.0.0.0	192.168.10.2

RouteurCG(config)# ip route 192.168.110.0 255.255.255.255.0 10.0.0.2

_____ ip route 0.0.0.0 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

-Cœur de réseau

Respecter les 3 étapes :

1)donner un nom d'hôte

2)configurer les interfaces

3)configurer la table de routage

Destination	Masque	Passerelle
0.0.0.0	0.0.0.0	192.168.10.1

Switch(config)# hostname SwitchL3
SwhitchL3(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)Vérifications

Pour vérifier l'état des interfaces :

Show ip interface brief
Show ipv6 interface brief

Exemple :

RouteurVPN# show ip interface brief

Interface	IP adress	OK ?	Method	Status	Protocol
GigabitEthernet 0/0	192.168.110.254	YES	Manual	Up	Up
GigabitEthernet 0/1	Unasigned	YES	Unset	Down	Down
Serial 0/0/0	Unassigned	YES	Manual	Up	up
Serial 0/0/1	10.0.0.2	YES	Manual	Up	up
Vlan 1	Unassigned	YES	Unset	Down	Down

Pour vérifier les routes :

Show ip route
Show ipv6 route

```
RouteurVPN>en
Password:
RouteurVPN#Show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.110.254 YES manual up                    up
GigabitEthernet0/1     unassigned      YES NVRAM  administratively down down
Serial0/1/0            unassigned      YES unset  down                  down
Serial0/1/1            10.0.0.1        YES manual down                  down
Loopback0              192.168.200.2   YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

Quelque tests a partir de routeur VPN du site distant :

Ping 192.168.110.1
Ping 192.168.110.254
Ping 10.0.0.2
Ping 192.168.10.1
Ping 192.168.10.2

Quatre paramètres de filtrage possibles.

Exemples :

Show running-config | section GigabitEthernet 0/1
Show interface brief | include up
Show interface brief | exclude unassigned
Show ip route |begin Gateway

Tester avec ou sans les pipes

Rappel : utiliser les flèches pour l'historique des commandes.

Show history affiche par defaut les 10 dernières commandes :

```
EMP-PAI>show history
  show running-config
  show running-config|section GigabitEthernet 0/1
  show hystory
  show history
```

Terminal history size 50 pour changer le nombre de commande :

```
EMP-PAI>Terminal history size 50
EMP-PAI>
```

L'historique est vidé si on se déconnecte.

VI.Configuration des VLAN

1. Identifiez les domaines de collision et de diffusion

Une collision arrive quand deux paquets sont émis en même temps sur un segment de réseau. La congestion du réseau arrive quand le réseau est très fortement ralenti. Dans les anciens segments Ethernet basés sur des concentrateurs (hub), les périphériques réseau était en concurrence sur le support partagé, formant des domaines de collision et congestionnent le réseau.

Avec les commutateurs, on a le mode bidirectionnel et chaque segment est dans son propre domaine de collision.
domaines de collision avec un switch

Plus les domaines de collisions sont petits, plus le réseau est performant
Un ensemble de commutateurs interconnectés constitue un unique domaines de diffusion. Seul un routeur peut séparer en deux ou plusieurs domaines de diffusion. Donc les routeurs sont utilisés pour segmenter les domaines de diffusion, et aussi les domaines de collision.

domaines de diffusion

Le domaine de diffusion constitué par le site principal est trop gros, ce n'est pas bon signe. Lorsqu'un commutateur reçoit une trame de diffusion, il la transmet à tous les ports sauf le port d'entrée. Donc chaque périphérique connecté reçoit la trame et la traitre. Les diffusions réduisent l'efficacité du réseau.

2. Utiliser des VLAN pour réduire les domaines de diffusion

Trop cher et trop complexe d'utiliser des routeurs, donc on utilise des VLAN qui reposent sur des connecteurs logiques et plus physiques.
Les VLAN sont crées en fonction des services dans l'entreprise.
Site principal avec des VLAN

Les domaines de diffusion sont devenus plus petits, mais plus nombreuses. Les administrateurs réseau peuvent mettre en œuvre des politiques d'accès et de sécurité en fonction des groupes d'utilisateurs. Chaque port de communicateur peut être attribué à un seul VLAN sauf pour les téléphones IP et vers un autre commutateur.

Groupe	VLAN	Adresse réseau	1*ère*adresse	Dernière adresse	Passerelle
Direction	20	192.168.20.0/24	192.168.20.1/24	192.168.20.253/24	192.168.20.254/24
Examen/concours	21	192.168.21.0/24	192.168.21.1/24	192.168.21.253/24	192.168.21.254/24
Paie/DRH	22	192.168.22.0/24	192.168.22.1/24	192.168.22.253/24	192.168.22.254/24
Emploi	23	192.168.23.0/24	192.168.23.1/24	192.168.23.253/24	192.168.23.254/24
Médecine	24	192.168.24.0/24	192.168.24.1/24	192.168.24.253/24	192.168.24.254/24
Assurance	25	192.168.25.0/24	192.168.25.1/24	192.168.25.253/24	192.168.25.254/24
Info/RGPD	27	192.168.27.0/24	192.168.27.1/24	192.168.27.253/24	192.168.27.254/24
Serveurs	30	192.168.30.0/24	192.168.30.1/24	192.168.30.253/24	192.168.30.254/24
Impression	40	192.168.40.0/24	192.168.40.1/24	192.168.40.253/24	192.168.40.254/24
Téléphone	50	192.168.50.0/24	192.168.50.1/24	192.168.50.253/24	192.168.50.254/24
Wifi	60	192.168.60.0/24	192.168.60.1/24	192.168.60.253/24	192.168.60.254/24
Administration	100	192.168.100.0/24	192.168.100.1/24	192.168.100.253/24	192.168.100.254/24

Avantages des VLAN :
- Domaines de diffusion plus petits : nombre de périphériques réduit.
- Sécurité optimisée : seuls les utilisateurs d'un même VLAN peuvent communiquer.
- Amélioration de l'efficacité des ressources : simplification de la gestion des utilisateurs et de l'identification (nommages des VLAN).

- Coût réduit : utilisation plus efficace de la largeur de bande (100 Mb/s, 1Gb/s…), moins besoin de changer les switch et routeurs.
- Meilleurs performances : réduction du trafic inutile.
- Gestion simplifié des projets et des applications : exemple logiciel de comptabilité.

Différents types de VLAN :

- VLAN par défaut : VLAN1
  Tous les ports sont attribués au VLAN1 par défaut.
  Le VLAN1 est le VLAN natif
  Le VLAN1 est le VLAN de gestion par défaut
  Le VLAN1 ne peut être renommer ou supprimé
  Show VLAN brief
- VLAN de données
  crées pour séparer le trafic des utilisateurs.
  Exemple : VLAN21 examens concours
- VLAN natif
  Le trafic utilisateur est marqué par son ID VLAN lorsqu'il est envoyé à un commutateur. Ce sont les ports de Trunk transmettent cette information entre commutateurs. En général, ou définit un VLAN natif différent de VLAN1 et inutilisé pour tous les ports Trunkes du domaine.
- VLAN de gestion
  C'est un VLAN de données réservé au trafic de gestion : ssh, SNMP, HTTPS. Exemple : VLAN100
- VLAN voix
  Spécifique à la voix sur IP (VoIP)
  - Bande passante consolidée pour garantir la qualité de la voix
  - Priorité de transmission
  - Possibilité de routage autour des Zones encombrées
  - Délai (ping) inférieur à 150 ans sur tout le réseau.

3.Paramétrage

- Pour le commutateur Dir-Exam, créer 5 VLAN :

	NOM
20	Direction
21	Examen/Concours
40	Impression
50	Téléphone
100	Administration

```
Dir-Exam# conf t
Dir-Exam(config)# vlan 20
```

Dir-Exam(config-vlan)# name Direction
Dir-Exam(config-vlan)# end Mettre sur chaque commutateur

Pour attribuer un Vlan a une interface :

Dir-Exam #config terminal

Dir-Exam # int fa0/1

Dir-Exam# switchport mode access

‘’’’’’’’’’’’’# switchport access vlan 20

‘’’’’’’’’’’’’# exit

Faire les vlan sur chaque commutateur

VII. Ajout de la téléphonie IP

1)ajout des téléphones

IMAGE

Penser à allumer les téléphones !

2)configuration

Rappel : impossible de configurer plusieurs VLAN sur une interface, sauf si on ajoute un VLAN voix ou ports TRUNK.

Sur le VLAN Telephonie , il faut activer la qualité du service (QoS) et mettre le vlan sur chaque interface :

Dir-Exam (config)# int fa0/1

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

Même chose sur fa0/2

Int range fa0/1-2 : les 2 même temps

3) Vérification

Show vlan (brief)

Show interfaces fa0/1 switchport

Pour modifier un vlan : switchport access vlan nouveau_id

Pour supprimer un vlan sur un port : no switchport acces vlan

Pour supprimer un vlan : no vlan vlan_id <- Penser à basculer avant tout ses ports sur un autre vlan.

Pour revenir au parametrage d'usine des VLAN :

Delete vlan.dat

Et redémarrer le commutateur !

Pour revenir au paramétrage d'usine :

-débrancher tous les câbles (sauf l'alimentation et la console)

-erase startup-config

-Delete vlan.dat

4)Trunk de VLAN

C'est un lien de console 2 entre deux commutateurs qui achemine le trafic pour tous les VLANs.

Tâche	Commande
Passer en configuration globale	Dir-Exam# configure terminal
Passer en configuration d'interface	Dir-Exam(config)# interface g0/1
Regage en mode de trunking permanant	Dir-Exam (config-if)# switchport mode trunk
Choisir le VLAN (différent de 1)	Dir-Exam (config-if)# switchport trunk native vlan 100
Liste des vlans autorisés	Dir-exam (config-if)# switchport trunk allowed vlan 20,21,40,50,100
Repasser en configuration privilégié	Dir-Exam (config-if) end

Faire le lien sur tous les commutateurs 2960.

Verification : Dir-Exam# show interface g0/1 switchport

Pour réinitialiser : no switchport allowed vlan

No switchport trunk native vlan

5)routage inter-VLAN

-créer les VLANs sur le commutateur de niveau 3

switchL3(config)# vlan 20

switchL3(config-vlan)# name Direction

exit

Faire de même pour :

21	Exam/concours
22	Paie/DRH
23	Emploi

24	Medecine
25	Assurance
27	Info /RGPD
30	Serveurs
40	Impression
50	Telephonie
100	Administration

Affecter le VLANs aux interfaces :

switchL3(config)# interface g1/0/2

-création des passerelles de routage inter-vlan

On crée des interfaces virtuelles (SVI-Switch virtual interface) pour que les VLAN puissent communiquer ensemble.

switchL3(config)# interface vlan 20

switchL3(config-if)# description Passerelle SVI Direction

ip adress 192.168.20.254 255.255.255.0

ipv6 address 2001 :db8 :acab :20 ::254/64

no shutdown

exit

De même pour le vlan 21,22,23,24,25,27,30,40,50,60,100

VIII. sauvegarde des configurations

- système de fichiers des switchs/routeurs :

Show file système TEST /commentaires

➔ Mémoire totale,libre,FS, droits
#si amorçable

→Commande : dir,cd,pwd,copy

- Sauvegarde de la configuration

  Copy running-config startup-config

- Restauration de la configuration de démarrage :

  Copy startup-config running-config

➔ Existe aussi en version graphique