

Cours Réseaux Complexe Noah SANDIER SIO25 :

Cours Réseaux Complexe Noah SANDIER SIO25 :	1
1. Architecture physique d'un reseau :.....	2
2. Simulateur :.....	3
3. Connecter vos machines et vos réseaux :.....	4
4. Modèles en couches :.....	11
Réseau complexe	15
5. Configuration des commutateurs	24
6. Accès à distance sécurisé à un commutateur :.....	26
7. Configuration des routeurs :.....	30
8. Configuration des VLANs :.....	32
9. Sauvegarde des configurations :	43

1. Architecture physique d'un reseau :

1) Notions

Comment fonctionne Internet utilisé tous les jours ?

Envoi d'un mail : requête sur un serveur distant, câbles, équipements divers.

Un réseau permet d'interconnecter une multitude de machine. Pour transmettre des informations.

C'est mieux que la disquette !

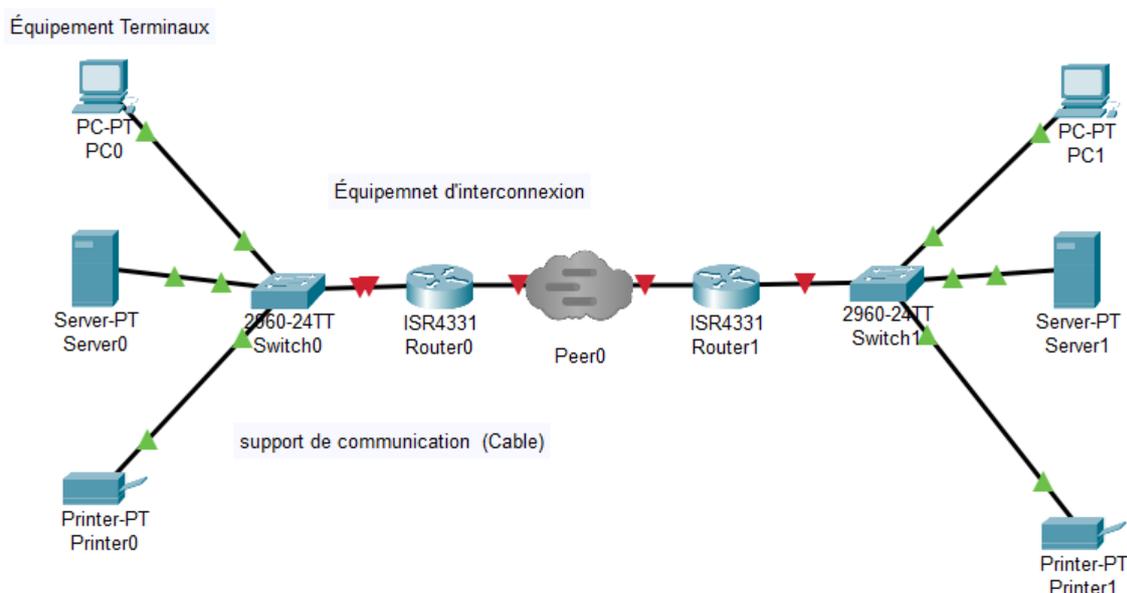
Différents types de réseaux :

- LAN (Local Area Network) : échelle locale, réseaux domestique, entreprise.
- MAN (Metropolitan Area Network) : échelle d'une ville, université, plusieurs LAN interconnecté.
- WAN (Wide Area Network) : echelle Mondiale, Internet

2) Eléments physiques

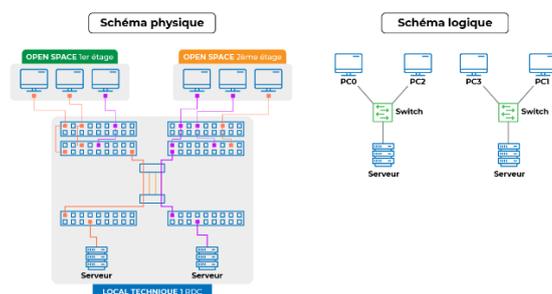
Architecture complète d'un réseau :

Schéma logique



1. Schéma logique et schéma physique

- Logique : pour concevoir, modéliser, configurer
- Physique : pour déployer, installer, câbler



2. Simulateur :

1) Concevoir réaliser une maquette

- À la main (papier, crayon)
- Grâce à un outil de simulation (plus qu'un logiciel de dessin, il permet aussi de simuler le comportement d'un équipement).

Exemple de simulateurs : Packet tracer (Propriété CISCO, gratuit), GNS3 (libre et complet)

2) Installation de Packet Tracer

Sur le site de cours en ligne de cisco, www.netacad.com :

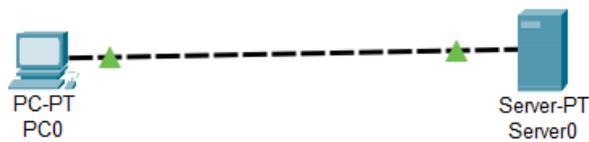
- Sign up today
- S'inscrire au cours Introduction to PT
- Télécharger PT dans ressources

3) Première Mission

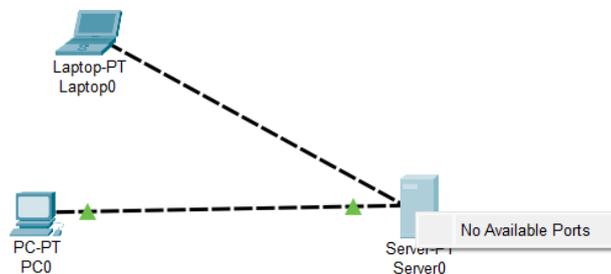
Vous venez d'arriver dans une ESN (Entreprise de service du numérique) spécialisée dans la conception de réseau. Votre manager vous demande de travailler pour un nouveau client : L'auto école TACOT.

Pour le moment, un seul utilisateur, le dirigeant M. FALMAN.

Votre mission est de connecter son PC à un serveur de stockage de manière sécurisée. Commencez par réaliser le schéma réseau.

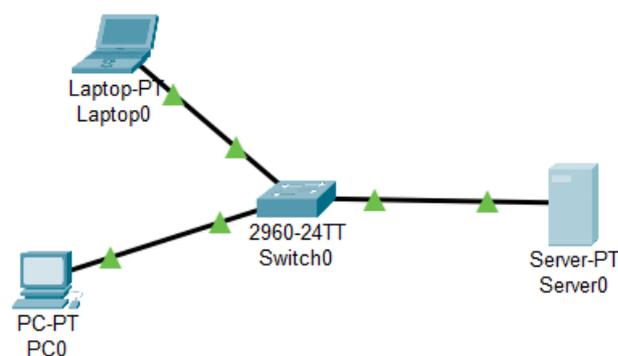


Quelques jours plus tard, le client vous rappelle : il vient d'accueillir son 1^{er} employé et vous devez relier son PC portable au serveur de stockage. Mais PT vous indique qu'il y a pas de port disponible :



En effet, il n'y a qu'une seule carte réseau sous le serveur. Deux solutions :

- Ajouter une carte réseau, mais s'il y a un 2^e salarié...
- Ajouter un équipement d'interconnexion (Commutateur).



3. Connecter vos machines et vos réseaux :

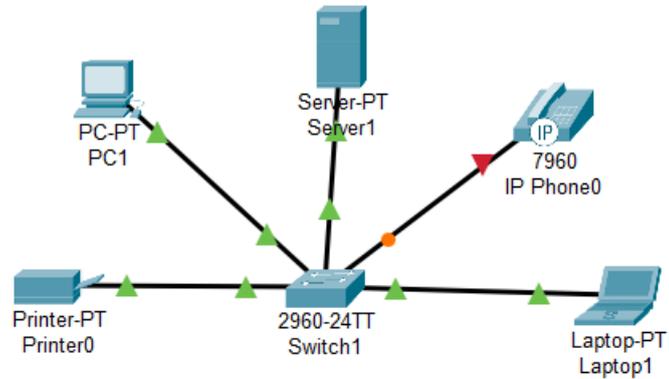
1) Distinguer les équipements d'interconnexion

Deux types : les commutateurs et les routeurs

Commutateurs : //rond-point ou aiguillage

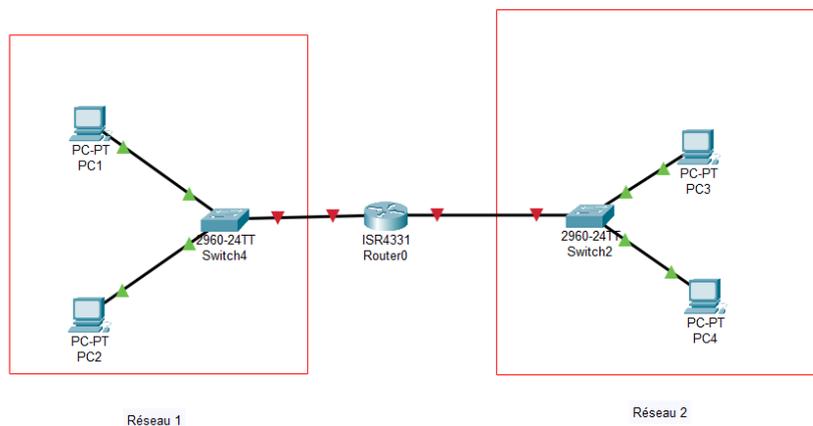
- Nombre de port (4 a 96)
- Types de ports : RJ45, SFP

- Débits possible : 10/100/1000 Mbps en RJ45
1 / 10 / 100 Gbps en SFP
- Fonctionnalités : interface de configuration, compatibilité



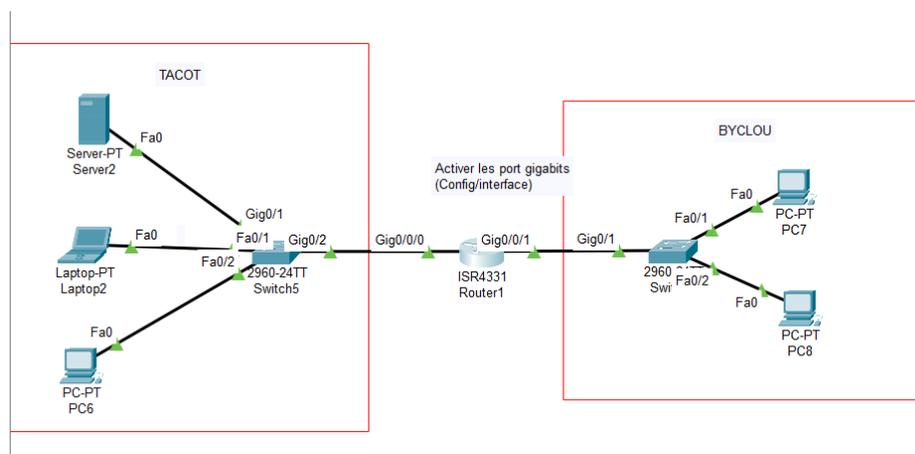
Routeur : // pont, passerelle

- Sépare 2 réseaux
- Décide ce qui passe ou pas
- Aiguille dans la bonne direction



2) Deuxième mission

Un an plus tard, les locaux de l'entreprise TACOT sont partagés avec l'entreprise BYCLOU. Elles collaborent en échangeant des fichiers. Il faut interconnecter les 2 réseaux.



3) Déterminer le bon support de communication

Pour aller de Paris a Grenoble, on peut utiliser la route (voiture), le rail (TGV), l'air (avion).

	Cable cuivre	Fibre Optique	Sans-fil
Portée	100m	60KM	50m
Mobilité	Moyenne	Mauvaise	Bonne
Résistance/perturbation	Moyenne	Très bonne	Mauvais
Débit	Bon	Très bon	Moyens
Compatibilité	Très bon	Moyen	Très bon
Sécurité	Très bon	Très bonne	Mauvais
Contexte	Domicile entreprise	Domicile entreprise	Domicile entreprise

4) Utiliser la bonne carte réseau

- Cuivre,optique,sans-fil

5) Réseau local sans-fils

- Wireless Local Area Network : WLAN (WIFI)
- Chiffrement WPA 2

2. Configuration d'un reseau

Dans toute communication, il faut identifier la source (qui parle ?), le destinataire (à qui ?) et le message (pour dire quoi ?).

1) Identifier l'adresse MAC

L'adresse MAC (Media Access Control) ou adresse physique est l'identifiant unique d'une carte réseau, composé de 6 octets écrits en hexadécimal. Les 3 premiers identifient le constructeur.

Quel est mon adresse MAC ?

D8-F8-83-08-09-44

Quel est le constructeur ?

Result for: [D8-F8-83-08-09-44](#)

Address Prefix	D8:F8:83
Vendor / Company	Intel Corporate
Start Address	D8F883000000
End Address	D8F883FFFFFF
Company Address	Lot 8, Jalan Hi-Tech 2/3 Kulim Kedah 09000 My

Sur PT, simulation entre 2 machine.



2) Troisième mission

Tester le réseau local privé de TACOT :

- Serveur 0 : 192.168.0.1
- PC0 : 192.168.0.2
- Portable : 192.168.0.3

Vérifier que vous m'accédez a BYCLOU.

- PC1 : 192.168.100.1
- PC2 : 192.168.100.2

Tester la communication avec Serveur 0.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

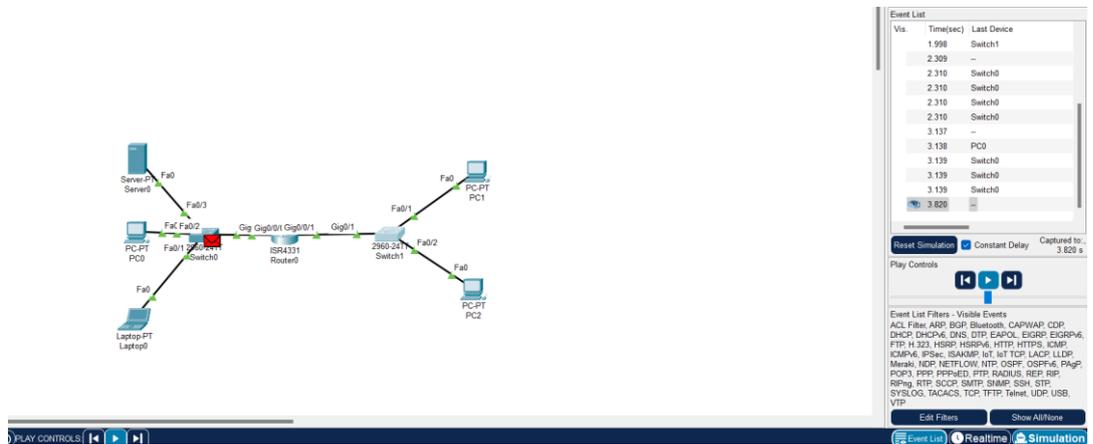
Request timed out.
Request timed out.
```

3) Routage

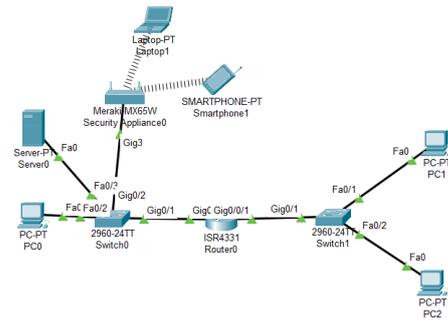
Une table de routage est un tableau qui indique au routeur vers quel réseau envoyer un paquet en fonction de sa destination.

- Activer les deux cartes réseau du routeur.
- Affecter a chaque carte l'IP 254 dans chaque réseau.
- Indiquer a chaque terminal la passerelle de son réseau dans Global/Settings

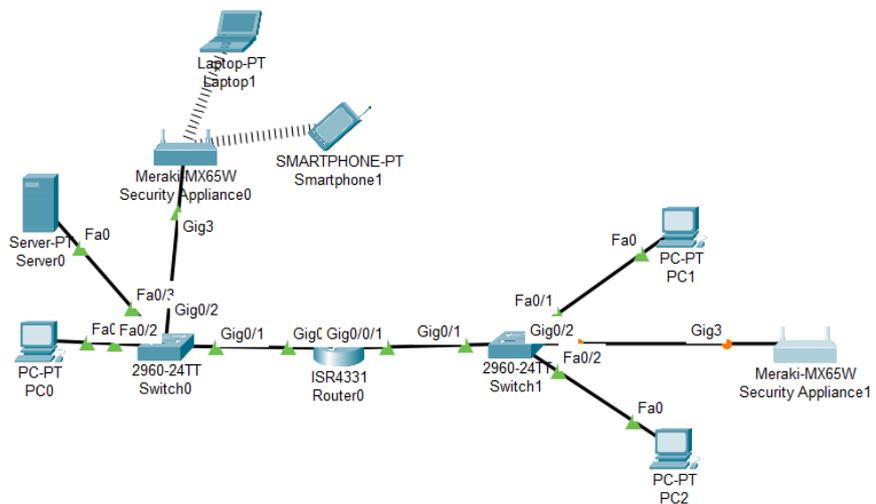
Tester la connexion :



- Rajouter une borne WIFI chez TACOT et mettre le portable dessus.



- Rajouter une borne WIFI chez BYCLOU



Remarque : Pas de configuration sur les switchs

4. Modèles en couches :

Pour communiquer, ils vont mieux parler le même langage.

Il y a 2 catégories de règles dans les réseaux :

- Les règles matérielles (normes)
- Les règles logiciels (protocoles)

Les modèles permettent de classer ces règles en couches réseaux

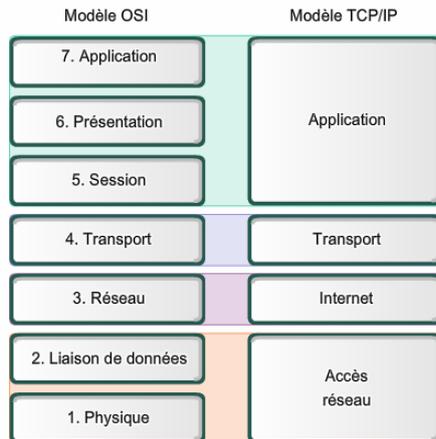
1) Le modèle OSI (Open System Interconnexion) en 7 couches

	TCP/IP	Modèle OSI	
	PDU (protocole data unit)	Couche	Rôle
Couches hautes	Donnée	7-Application	Point d'accès aux services réseau
		6-Présentation	Gère le chiffrement et le déchiffrement des données, convertit les données machine en données exploitables par n'importe quelle autre machine
		5-Session	Communication Interhost, gère les sessions entre les différentes applications
	Segment	4-Transport	Connexion de bout en bout, connectabilité et contrôle de flux ; notion de port (TCP et UDP)
Couches matérielles	Paquet	3-Réseau	Détermine le parcours des données et l'adressage logique (adresse IP)
	Trame (frame)	2-Liaison (link)	Adressage physique (adresse MAC)
	Bit	1-physique	Transmission des signaux sous forme numérique ou analogique

A peine serré, Tu rends le portefeuille. (Sens descendant)

Pour le réseau, tout se passe ainsi. (Sens ascendant)

2) Le modèle TCP/IP



3. Automatiser l'attribution d'adresses IP

1) Serveur DHCP

Chaque machine doit avoir une adresse IP unique sur le réseau, configuration en fixe (manuellement) ou automatique (dynamiquement).

DHCP : Dynamic Host Configuration Protocol

- Service centralisé pour connaître les adresses utilisées et éviter les doublons.



Une adresse IP est allouée juste le temps du bail. Le client doit demande le renouvellement.

Quelle est votre adresse IP automatique ? L'IP du serveur et la plage ?

```

Connection-specific DNS Suffix . . . : 
Description . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
Physical Address. . . . . : D8-F8-83-08-09-44
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-Local IPv6 Address . . . . . : fe80::170d:83a5:785:b175%14(Preferred)
IPv4 Address. . . . . : 192.168.0.65(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 07 March 2024 08:39:44
Lease Expires . . . . . : 08 March 2024 15:16:48
Default Gateway . . . . . : 192.168.0.254
DHCP Server . . . . . : 192.168.0.254
DHCPv6 IAID . . . . . : 64551043
DHCPv6 Client DUID. . . . . : 00-01-00-01-29-9F-43-01-D8-F8-83-08-09-44
DNS Servers . . . . . : 8.8.8.8
                        8.8.4.4
NetBIOS over Tcpi. . . . . : Enabled

```

2) Quatrième mission

Deux commerciaux itinérants arrive chez BYCLOU : ils auront des ordinateurs portables.

- Rajouter un serveur DHCP sur le réseau BYCLOU
- Server 1 en IP fixe 192.168.100.250/24
- Activer le service
- Configurer la plage (pool) d'adresses de 192.168.100.10 à 50.
- Profitez-en aussi pour définir la passerelle
- Rajoutez les 2 portables et testez

1) Serveur DNS

La résolution de nom permet d'associer une adresse IP à un nom de domaine et vice-versa, ce qui est beaucoup plus pratique a retenir. Pour cela, un serveur DNS (Domain Name System) tient a jour un annuaire, sachant que plusieurs noms de domaines peuvent êtres hébergé sur la même machine. Généralement, l'adresse du serveur DNS est fournis par le serveur DHCP.

2) Cinquième mission

L'entreprise Byclou envisage de créer un site internet interne pour répertorier toutes ses pieces détachés. Pour que les salarié puissent utiliser un nom de domaine plutôt qu'une adresse IP, rajoutez un serveur DNS au serveur 1 de Byclou, avec l'annuaire suivant.

Nom	Adresse IP
PC1	192.168.100.1
PC2	192.168.100.2
Serveur 1	192.168.100.250
Intranet.byclou.fr	192.168.100.250

Rajouter l'IP du DNS sur PC1 et PC2

Gateway/DNS IPv4

DHCP

Static

Default Gateway

DNS Server

Rajouter l'IP du DNS dans le serveur DHCP pour qu'elle se répercute sur les portables

DHCP

Interface Service On Off

Pool Name

Default Gateway

DNS Server

Start IP Address :

Subnet Mask:

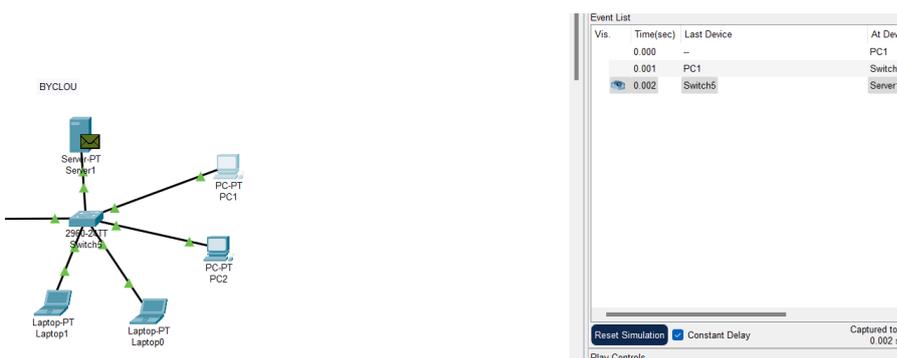
Tester avec des pings

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.100.250

Pinging 192.168.100.250 with 32 bytes of data:

Reply from 192.168.100.250: bytes=32 time<1ms TTL=128
Reply from 192.168.100.250: bytes=32 time<1ms TTL=128
Reply from 192.168.100.250: bytes=32 time<1ms TTL=128
```

Tester en mode simulation et repérer les échanges DNS avant le ping (protocole ICMP)



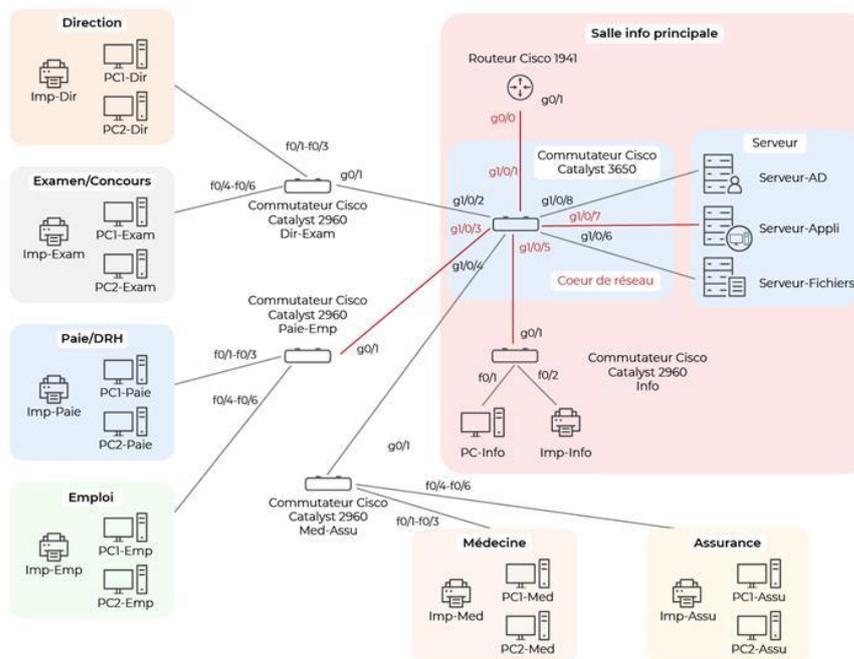
Démarrer le serveur Web sur serveur 1

Le serveur Web est démarré lorsqu'on configure intranet.byclou.fr sur le DNS

Tester avec un navigation web depuis un PC.



Proposer une offre commerciale avec avec devis pour installer le réseau complet de Tacot et Biclou, avec option NAS.



Réseau complexe

1. 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 1PC et 1 imprimante, 3 serveur, 1 routeur et 1 switch cœur de réseau.

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

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

Oui elle convient car il y a 2 port Gigabit et les rest en FastEthernet



- Le routeur est en Gigabit. Cisco 1941 ?

Le Cisco 1941 a un port Gigabit alors elle convient



Spécifications du produit

Tableau 7. Spécifications produit des routeurs ISR Cisco 1941

	Cisco1941, Cisco1941W
Services et densité des slots	
Accélération matérielle intégrée des fonctions de chiffrement (IPSec + SSL)	Oui
Nombre de ports WAN 10/100/1000 intégrés	2
Ports RJ-45	2
Ports SFP	0
Slots SM (Service Module)	(0
Slots SM-D (Service Module double largeur)	0
Slots EHWIC	2
Slots EHWIC de double largeur (l'utilisation d'un slot EHWIC de double largeur occupera deux slots EHWIC)	1

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

Il ne convient car il est en FastEthernet (10/100)



Switch Model	Description	Uplinks
Catalyst 2960-S Switches with 1 Gigabit Uplinks and 10/100/1000 Ethernet Connectivity		
Cisco Catalyst 2960S-48TS-S	48 Ethernet 10/100/1000	2 1 GbE ports
Cisco Catalyst 2960S-24TS-S	24 Ethernet 10/100/1000	2 1 GbE SFP ports
Catalyst 2960 Switches with 1 Gigabit Uplinks and 10/100 Ethernet Connectivity		
Cisco Catalyst 2960-48PST-S	48 Ethernet 10/100 PoE ports (370W capacity)	2 fixed 10/100/1000 ports and 2 SFP ports
Cisco Catalyst 2960-24PC-S	24 Ethernet 10/100 PoE ports (370W capacity)	2 dual-purpose ports (10/100/1000 or SFP)
Cisco Catalyst 2960-24LC-S	24 Ethernet 10/100 and 8 10/100 PoE ports (123W capacity)	2 dual-purpose ports (10/100/1000 or SFP)
Cisco Catalyst 2960-48TC-S	48 Ethernet 10/100	2 dual-purpose ports (10/100/1000 or SFP)
Cisco Catalyst 2960-48TT-S	48 Ethernet 10/100	2 fixed 10/100/1000 ports
Cisco Catalyst 2960-24TC-S	24 Ethernet 10/100	2 dual-purpose ports (10/100/1000 or SFP)
Cisco Catalyst 2960-24-S	24 Ethernet 10/100	None
Compact Switches		
Cisco Catalyst 2960-8TC-S	8 Ethernet 10/100 compact size with no fan	1 dual-purpose port (10/100/1000 or SFP)

3650 ?

Étape 7 Connectez un câble Ethernet de catégorie 5 à :

- N'importe quel port Ethernet 10/100/1000 ou 10/100/1000 PoE+ situé sur la façade avant du commutateur.

Comment s'appellent les ports du routeur ?

INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1

Comment s'appellent les ports du commutateurs cœur de réseau ?

g/1/0/1 -> g1/0/24

g/1/1/1 -> g1/1/4

Comment s'appellent les ports du commutateurs de services ?

f0/1 -> f0/24

g0/1 et g0/2

Que comprenez-vous de la numérotation des ports ?

La numérotation démarre a 0 sur les routeurs, a 1 les

commutateurs

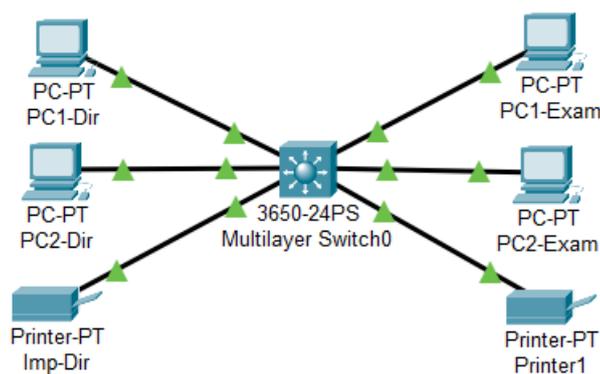
Affichage des ports sur PT : Option/Préférence/Always show port

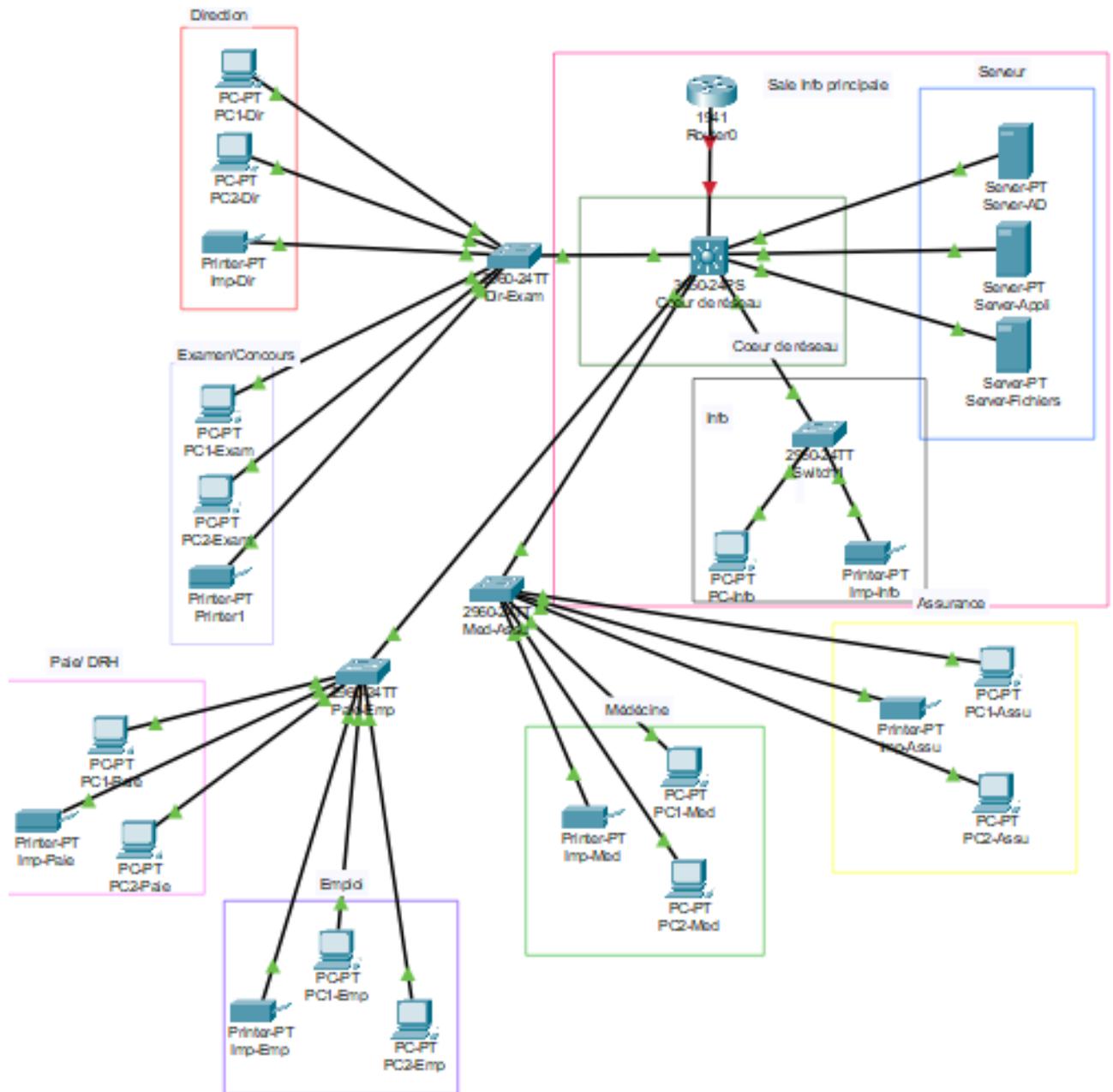
labels

Dans les services, on décide de mettre toujours PC1 sur le 1^{er}, PC2 sur le 2^e et Imp sur le 3^e

sur le 2^e e

Exemple 1^{er} étage :





Plan d'adressage :

Groupes	Adresse IP	1er Adresse	Derniere Adresse	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			
Paie-DRH	192.168.22.0/ 24			

Emploi	192.168.23.0/ 24
Médecin e	192.168.24.0/ 24
Assuranc e	192.168.25.0/ 24
Info/RGP D	192.168.27.0/ 24
Serveurs	192.168.30.0/ 24
Impressi on	192.168.40.0/ 24

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-I
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.

Serveurs :

Serveur-AD	Serveur Appli	Serveur 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

Le reseau WIFI sera en 192.168.60.0/24 :

- Ajouter un point d'accès AP-PT sur le commutateur central,
- Ajouter des périphérique : laptop,TV,Tablette,smartphone,
- Ajouter une Webcam (Menu Home).

Configuration :

SSID	Sécurité	Mot de passe
Metropole	WPA-PSK	1234-MetroPole:1234

Pas d'IP pour le point d'accès : couche 2 du modele OSI.

Plan d'adressage :

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

3. Commutateurs de niveau 2

Un switch de niveau 2 maintient un tableau dont chaque ligne contient le numéro de port et l'adresse MAC de destination. Donc une trame Ethernet qui arrive avec une adresse

destination. Sort par le même port de sortie quel que soit le port d'entrée. Une trame n'est jamais renvoyée par le port d'entrée.

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

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

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

Afficher la table CAM du commutateur DIR EXAM Commande : show mac-address-table

```
Switch>show mac-address-table
      Mac Address Table
-----
Vlan    Mac Address      Type        Ports
----    -
1       0002.4a0d.ec88   DYNAMIC    Gig0/1
1       0003.e441.b701   DYNAMIC    Gig0/1
Switch>
```

Lancez un ping entre PC1 – dir et pc2 DIR

```
C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.20.2: bytes=32 time<lms TTL=128
```

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

- Etape 1 : découverte, examen de la source
 - Si l'adresse MAC de la source n'existe pas dans la table, elle est rajouter
 - Si elle existe, le compteur d'arboresence est réinitialiser
 - Si elle existe sur un autre port, la table est actualisé
- Un port peut être associé a plusieurs adresses MAC, mais une adresse MAC ne peut être associé a plusieurs ports
- Etape 2 : transfert, examen de la destination

- Si l'adresse MAC de destination est une adresse de mono-diffusion, le commutateur cherche le port destinataire dans sa table MAC.
- Si l'adresse est dans la table, transfert de la trame vers le port destinataire.
- Si l'adresse n'est pas dans la table, le commutateur transfère sur tous les ports (sauf celui d'entrée).
- 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 commandes :

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

Exemple :

Switch > enable

Switch # configure terminal

Switch (config)# line console 0

Switch (config-line)# exit

Switch (config)# interface Fa 0/1

Switch (config-if)# exit

Switch (config)# exit

Switch #

Tester, utilisateur la complétion automatique ? pour l'aide dans chaque mode

Commandes raccourcies

En

Conf t

Int F0/1

Tester, utiliser la complétion automatique ? pour l'aider dans chaque mode.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#line console 0
Switch(config-line)#exit
Switch(config)#interface Fa 0/1
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG I: Configured from console by console

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int F0/1
Switch(config-if)#
```

5. 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 VLAN 1. Nous allons utiliser 2 VLAN :

Groupes	VLAN ID	Réseau	1ere adresse	Dernière adresse	Passerelle
Périphérique	10	192.168.10.0 /24	192.168.1.0.1	192.168.10.253	192.168.10.254
Administration	100	192.168.100.0 /24	192.168.100.0.1	192.168.100.253	192.168.100.254

VLAN 100	@IPv4	@IPv6
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
Paie-Emploi	192.168.100.3	2001 :DB8 : ACAD : 100 ::3
Med-Assu	192.168.100.4	2001 :DB8 : ACAD : 100 ::4
Info	192.168.100.5	2001 :DB8 : ACAD : 100 ::5
Passerelle	192.168.100.254	2001 :DB8 : ACAD : 100 ::254

Exemple 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
```

Remarques :

- L'interface SVI n'apparaît pas comme up tant que le VLAN 100 n'est pas créé et qu'un appareil n'est pas connecté.
- La commande IPv6 n'est pas activée par défaut sur les Cisco 2960.

Mode de configuration :

```
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)# vlan 100

Pour tester :

Show IP interface brief

```
Dir-Exam#show ip interface brief
Interface          IP-Address      OK? Method Status  Protocol
FastEthernet0/1    unassigned      YES manual up       up
FastEthernet0/2    unassigned      YES manual up       up
FastEthernet0/3    unassigned      YES manual up       up
FastEthernet0/4    unassigned      YES manual up       up
FastEthernet0/5    unassigned      YES manual up       up
FastEthernet0/6    unassigned      YES manual up       up
FastEthernet0/7    unassigned      YES manual down   down
FastEthernet0/8    unassigned      YES manual down   down
FastEthernet0/9    unassigned      YES manual down   down
FastEthernet0/10   unassigned      YES manual down   down
FastEthernet0/11   unassigned      YES manual down   down
FastEthernet0/12   unassigned      YES manual down   down
FastEthernet0/13   unassigned      YES manual down   down
FastEthernet0/14   unassigned      YES manual down   down
FastEthernet0/15   unassigned      YES manual down   down
FastEthernet0/16   unassigned      YES manual down   down
FastEthernet0/17   unassigned      YES manual down   down
FastEthernet0/18   unassigned      YES manual down   down
FastEthernet0/19   unassigned      YES manual down   down
FastEthernet0/20   unassigned      YES manual down   down
FastEthernet0/21   unassigned      YES manual down   down
FastEthernet0/22   unassigned      YES manual down   down
FastEthernet0/23   unassigned      YES manual down   down
FastEthernet0/24   unassigned      YES manual down   down
GigabitEthernet0/1 unassigned      YES manual up       up
GigabitEthernet0/2 unassigned      YES manual down   down
Vlan1               unassigned      YES manual administratively down down
Vlan100             192.168.100.2  YES manual down   down
```

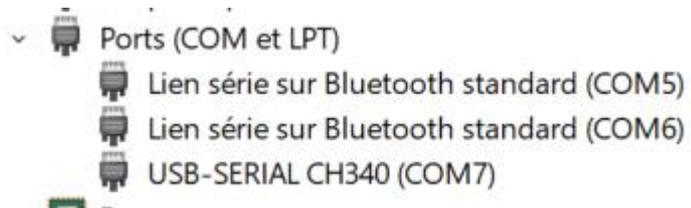
Show ipv6 interface brief

6. Accès à distance sécurisé à un commutateur :

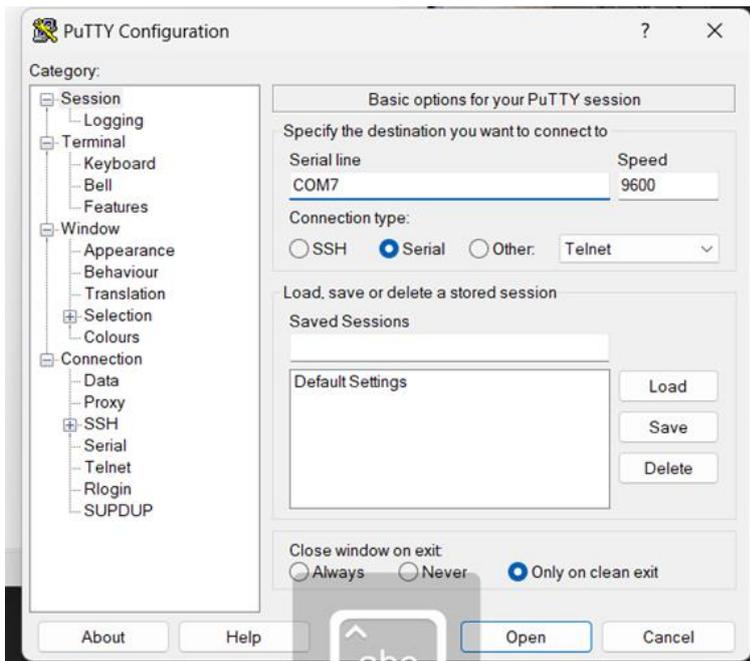
- Câble console RJ45/USB, anciennement COM ou Série ou RS232



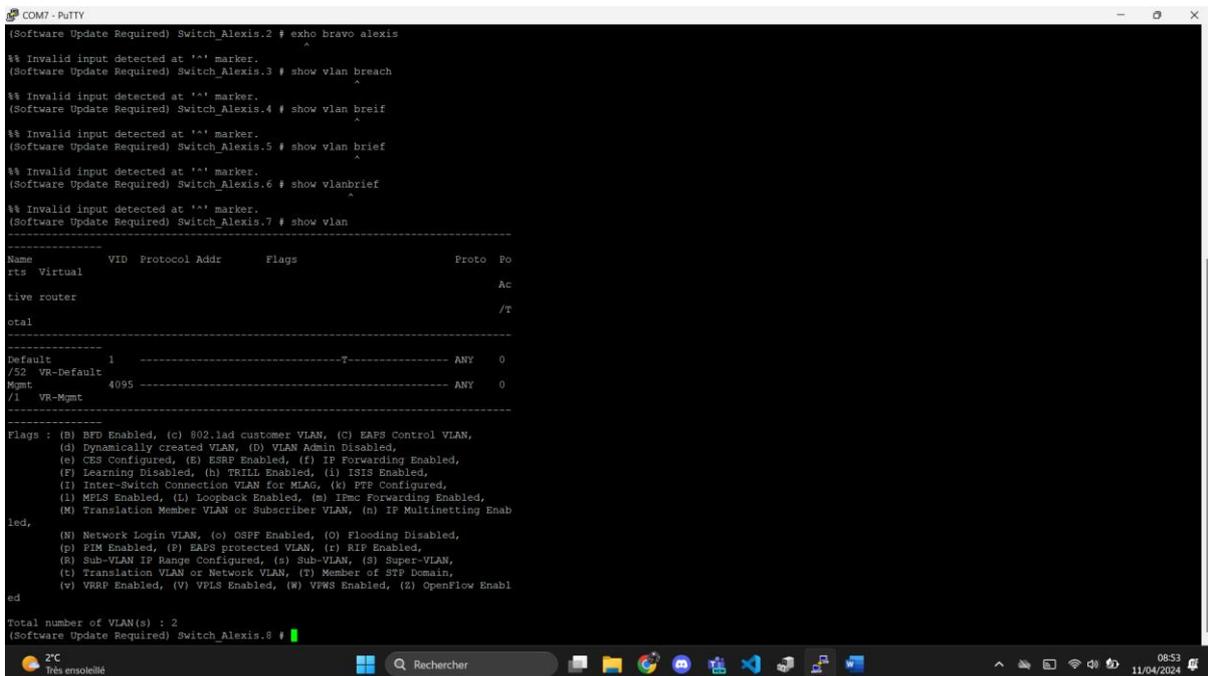
- Branchement du switch sur le port console (voir la première photo)
- Recherche du port détecté dans le gestionnaire de périphérique :



- Installation et configuration de PuTTY :



- Connexion :

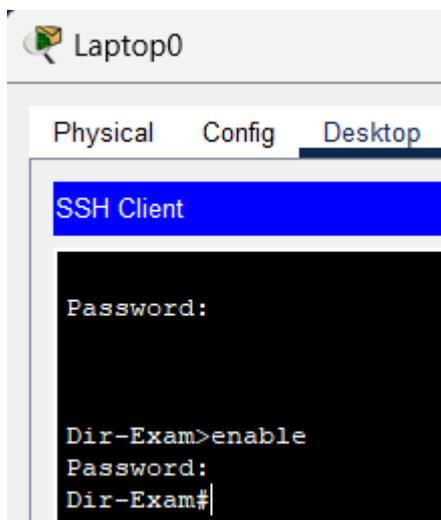
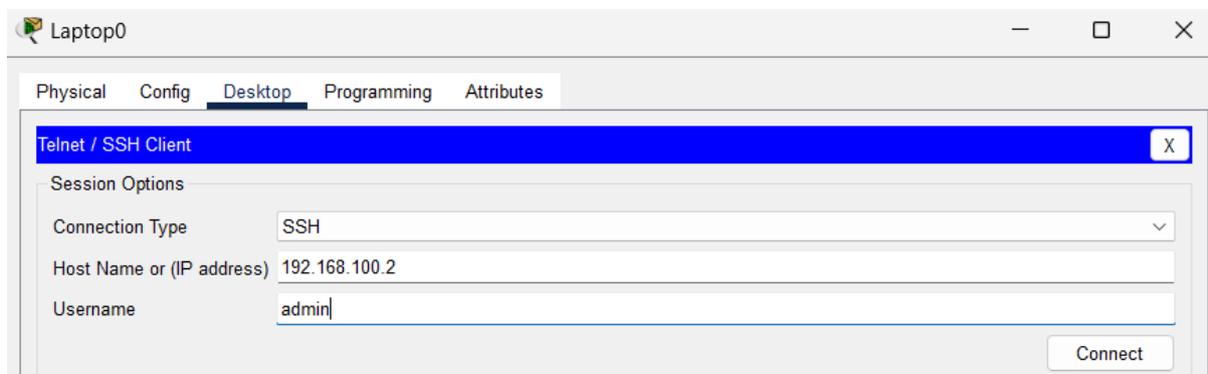


Procédure lourde qui implique d'être physiquement à côté du switch...
Ne jamais utiliser Telnet (pas sécurisé)

Accès SSH : sur les Catalyst 2960

Dir-Exam show version

```
show ip ssh
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
Dir-Exam(config-live)#
login local
exit
```



7. 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 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 d'hôte.

2. Un mot de passe

3. La configuration ssh v2, 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 lignes VTY pour l'accès SSH.

6. Le cryptage des mots de passe.

7. L'affichage d'une bannière légale d'accès non autorisé.

8. La copie de la configuration en mémoire non volatile.

```
Router > enable
```

```
Router# configure terminal
```

```
Router (config)# hostname RouteurVPN
```

```
RouteurVPN(config)#enable secret 1234-Metropole:1234
```

```
ip domaine-name metropole.fr
```

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

```
crypto key generate RSA
```

```
1024
```

```
ip ssh version 2
```

```
live console 0
```

```
Routeur VPN(config-live)#password 1234-Metropole;1234
```

```
login
```

```
exit
```

```
Routeur VPN (config)#live vty 0 15
```

```
Routeur VPN(config-live) #transport import ssh
```

```
login local
```

```
exit
```

```
Routeur VPN(config)#service password-encryption
```

```
banner motd #Accès autorisé seulement #
```

```
exit
```

Routeur VPN#copy running-config startup-config

Même configuration sur RouteurMetro

3) Configuration des interfaces routeurs

Pour être disponible, une interface doit :

- être configurée avec au moins une adresse IP (commandes ip address et ipv6 address),
- être activée car elle ne l'est pas par défaut (command no shutdown) et l'interface doit être connectée à un autre périphérique
- avoir une description (optionnel, max 240 caractères).

Sur le secteur VPN :

```
RouteurVPN(config)#interface GigabitEthernet 0/0
RouteurVPN(config-if)# ip address 192.168.110.254 255.255.255.0
                        ipv6 address 2001:db8:acad:110::254/64
                        no shutdown
                        description Lien sous-réseau VPN
                        exit
RouteurVPN(config)# ip address 10.0.0.2 255.255.255.0
                        ipv6 address 2001:db8:acad:1001::2/64
                        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 pont 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
```

Même config sur Routeur Metro

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 distants, non directement connectés.
 - o route statique, définie manuellement avec une passerelle.
 - o route dynamique par les protocoles OSPF et EIGRP
- Route par défaut 0.0.0.0

Sur routeur VPN :

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

```
RouteurVPN(config)# ip route 192.168.110.0 255.255.255.0 10.0.0.2
ip route 0.0.0.0 0.0.0.0 192.168.10.2
```

Sur le Coeur de réseau :

- 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) Vérifications :

Commandes : `show ip interface brief`
`ipv6`
`show ip route`
`ipv6`
`show historyh è-m0`

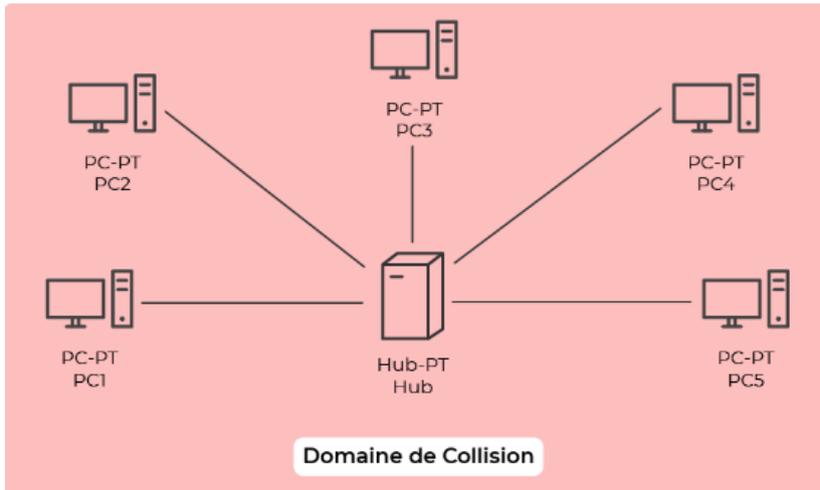
8. Configuration des VLANs :

1) Identifier les domaines de collision et de diffusion

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

Congestion : quand l'augmentation du trafic ralentit le réseau.

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

Le switch permet de régler tous ces problèmes.

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

Si on prend l'exemple avec le réseau Métropole, 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 émetteur).

Pour éviter d'acheter des routeurs supplémentaires, on crée des VLANs !

2) Utilisation des VLANs

Les VLANs permettent à un administrateur réseau 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 réseau Métropole, on 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/ 24	192.168.2 0.1	192.168.20.2 53	192.16 8.20.25 4
Examen/ Concours	21	192.168.21.0/ 24	192.168.2 1.1	192.168.21.2 53	192.16 8.21.25 4
Paie/DRH	22	192.168.22.0/ 24	192.168.2 2.1	192.168.22.2 53	192.16 8.22.25 4
Emploi	23	192.168.23.0/ 24	192.168.2 3.1	192.168.23.2 53	192.16 8.23.25 4
Médecine	24	192.168.24.0/ 24	192.168.2 4.1	192.168.24.2 53	192.16 8.24.25 4
Assurance	25	192.168.25.0/ 24	192.168.2 5.1	192.168.25.2 53	192.16 8.25.25 4
Info/RGPD	27	192.168.27.0/ 24	192.168.2 7.1	192.168.27.2 53	192.16 8.27.25 4
Serveurs	30	192.168.30.0/ 24	192.168.3 0.1	192.168.30.2 53	192.16 8.30.25 4
Impression	40	192.168.40.0/ 24	192.168.4 0.1	192.168.40.2 53	192.16 8.40.25 4
Téléphones	50	192.168.50.0/ 24	192.168.5 0.1	192.168.50.2 53	192.16 8.50.25 4
Wifi	60	192.168.60.0/ 24	192.168.6 0.1	192.168.60.2 53	192.16 8.60.25 4
Administration	100	192.168.100/ 24	192.168.1 00.1	192.168.100. 253	192.16 8.100.2 54

Avantages de la conception d'un réseau avec des VLANs :

- Domaines de diffusion plus petits : moins de périphériques dans le domaine de diffusion.
- Sécurité optimisée : seuls les utilisateurs d'un même VLAN peuvent communiquer ensemble.
- Amélioration de l'efficacité des ressources IT : Les utilisateurs ayant des besoins similaires sont sur le même VLAN qui peut être nommé.
- Coût réduit : moins de routeurs et meilleure utilisation de la bande passante.
- Meilleures performances : 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 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 :

VLAN	Nom
20	Direction
21	Exam
40	Impression
50	Telephonie
100	Administration

```
Dir-Exam# configure terminal
Dir-Exam(config)# vlan 20
Dir-Exam(config-vlan)# name direction
end
```

Dir-Exam>Show 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 Fa0/15, 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
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	

Paie-Empl#show 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 Fa0/15, 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	

```
Med-Assu#show 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 Fa0/15, 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	

```
info#show vlan brief
```

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	

VIII – Ajout de la téléphonie IP

1) Ajout des téléphones

3) vérifications :

Show vlan (brief)

show interfaces fa0/1 switchport

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

Pour supprimer le VLAN d'un port : no switchport access vlan

Pour supprimer 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

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.

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

- Création des VLANs sur les interfaces
- Création des liaisons TRUNK

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 interfaces virtuelles (SVI : switch virtual interfaces)

```
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
```

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

Tester avec des ping inter-vlan :

```
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.27.1

Pinging 192.168.27.1 with 32 bytes of data:

Request timed out.
Reply from 192.168.27.1: bytes=32 time=10ms TTL=127
Reply from 192.168.27.1: bytes=32 time<1ms TTL=127
Reply from 192.168.27.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.27.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\>
```

Après avoir testé les pings entre les différents VLANs, on peut voir que sa communique bien. Que ce soit entre les imprimantes ou bien les ordinateurs.

9. Sauvegarde des configurations :

1) Système de fichiers des routeurs et switchs L3 :

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

* : système actuel par défaut

: disque amorçable

Dir : contenu du 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 :

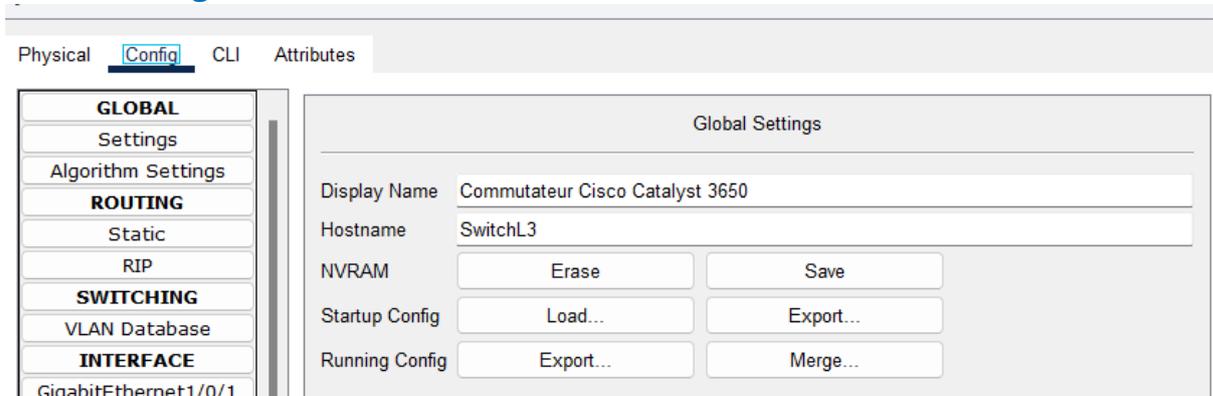
Copy running-config startup-config

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

On inverse les deux commandes.

3) Sauvegarde graphique sans PT :

-> Menu [config](#)



Possibilité aussi de sauvegarder sur un serveur externe en TFTP.

-> Menu [Services](#)

Dans packet tracer, le menu service n'existe pas sur la version actuelle.

Sur une machine en physique on peut le faire dans tous les cas.