

ACTIVITE 4

Utilisation et configuration de VLAN

L'objectif de cette activité est d'apprendre à configurer des VLAN, définir le mode d'accès, utiliser le VLAN de configuration, ...

Ce document est votre compte rendu

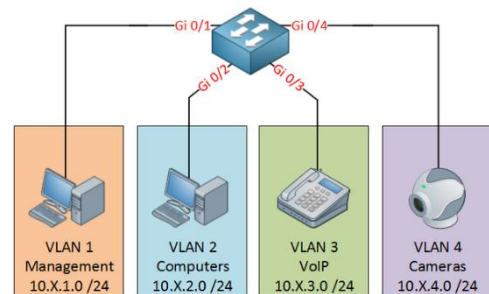
1 – Pourquoi utilise-t-on des VLAN ?

Un VLAN (**Virtual Local Area Network**) est un réseau local regroupant un ensemble de machines de façon logique. C'est-à-dire que l'on va regrouper des machines sur un réseau "virtuel" en fonction de leurs adresses IP ou MAC ou des protocoles utilisés ou des numéros de ports d'un switch.

Cela permet de réaliser des réseaux de façon indépendante **du système de câblage**. Par exemple, des machines situées dans une même pièce peuvent se retrouver sur des VLAN différents (des réseaux "virtuels" différents).

Avantages

- ☞ Ils améliorent la sécurité, en créant des règles de communication inter-VLAN.
- ☞ Ils optimisent la bande passante, en réalisant des réseaux disjoints. On peut aussi séparer les flux (Audio / vidéo / data) et diminuer les domaines de collision et de diffusion.



✍ 1 – Qu'est-ce qu'un domaine de collision ?

Un domaine de collision est une zone d'un réseau informatique où les paquets de données peuvent entrer en collision entre eux. Ce domaine est limité par la taille du réseau de l'entreprise, mais on peut le réduire si on le "découpe" en VLAN ou en Sous-Réseaux. Les domaines de collision ne peuvent pas traverser les routeurs.

✍ 2 – Qu'est-ce qu'un domaine de diffusion ?

Un domaine de diffusion est une partie d'un réseau informatique où n'importe quel ordinateur connecté au réseau peut directement transmettre à tous les autres ordinateurs du même domaine, sans devoir passer par un routeur.

Remarque : On confond quelques fois les VLAN avec la segmentation d'un réseau en sous réseaux. Les deux techniques sont différentes :

- Le VLAN est créé au niveau du commutateur (SWITCH).
- La segmentation réseau est effectuée au niveau du routeur. On le verra lors du prochain cours.

2 – Topologie des VLAN

Les commutateurs classiques du commerce (autour de 15 €) ne permettent pas la mise en œuvre de VLAN. Pour la technologie VLAN, on parle de "SWITCH Manageable" (quelques centaines d'euros). Il existe trois méthodes pour mettre en place une topologie de VLAN.

☞ - VLAN de niveau 1

Type : VLAN par port.

Chaque port du commutateur est associé à un VLAN. Par exemple, les ports 1,5 et 9 sont attribués au VLAN 1, les ports 2, 3, 4 et 8 au VLAN 2. Par sécurité, les ports non utilisés (6, 7, 10, 11 et 12) sont éteints (shutdown).

☞ - VLAN de niveau 2

Type : VLAN par adresse MAC.

Les VLAN sont définis en fonction des adresse MAC des hôtes connectés au commutateur.

Par exemple, le VLAN 1 est défini pour accepter les adresses MAC des postes 1, 2 et 4, le VLAN 2 est défini pour accepter les adresses MAC des postes 3, 5, 6 et 7.

Inconvénient de cette méthode : si on change la carte réseau d'un hôte, il faut reconfigurer le commutateur.

☞ - VLAN de niveau 3

Type : VLAN basé sur les protocoles ou les adresses IP.

VLAN par sous-réseau : on définit un VLAN en fonction des adresses IP des postes.

VLAN par protocole permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, AppleTalk, etc.), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même sous réseau.

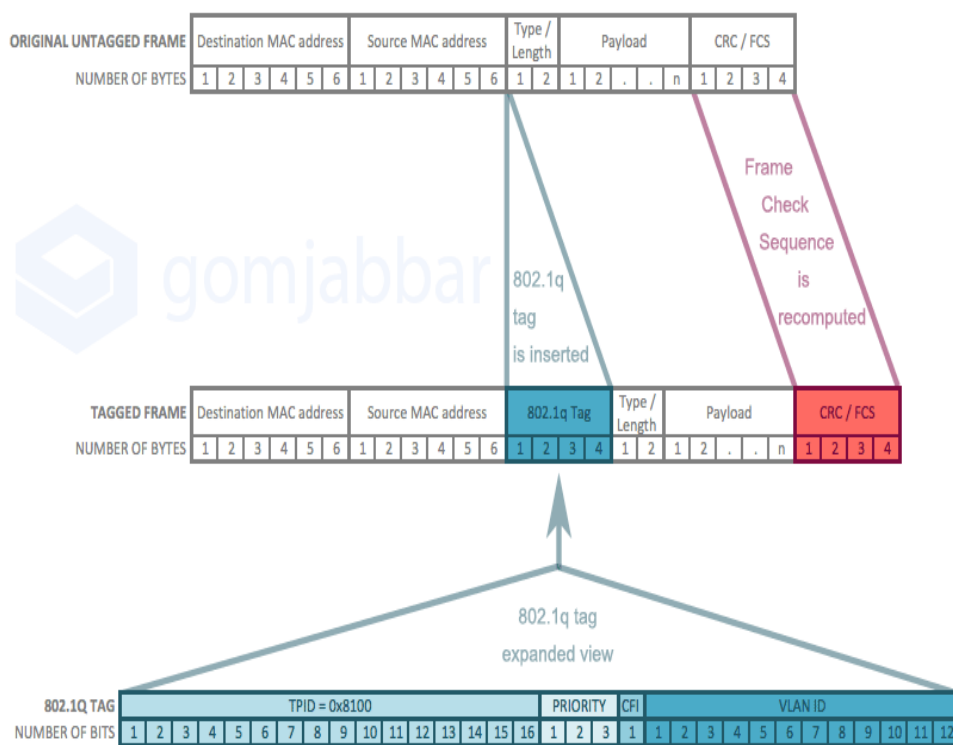
Remarque

Les VLAN de niveau 2 ou 3 permettent le déplacement des hôtes sur le réseau. Il n'est pas nécessaire de reconfigurer le commutateur.

3 - Comment identifier une trame sur un VLAN ?

On utilise des étiquettes VLAN pour indiquer l'appartenance d'une trame en circulation à un VLAN.

Un TAG de 4 octets (identification du VLAN) est ajouté à la trame Ethernet au moment où elle entre dans un port du commutateur. Le TAG est retiré lorsque la trame quitte un port configuré en mode "ACCESS".



TPID – Tag Protocol

Identifier (16 bits) :

identification du protocole véhiculé dans la trame (ici 8100 => IEEE 802.1Q).

Priority (3 bits) :

permet de coder le niveau de priorité d'un VLAN par rapport à un autre.

CFI - Canonical Format

Identifier (1 bit) :

précise si le système est compatible avec une architecture Token Ring. Par défaut le bit est à 0 (rarement utilisé).

VLAN ID (12 bits) :

permet d'identifier le VLAN (valeur comprise entre 0 et 4093)

4 - Quel mode choisir pour une interface : ACCESS ou TRUNK

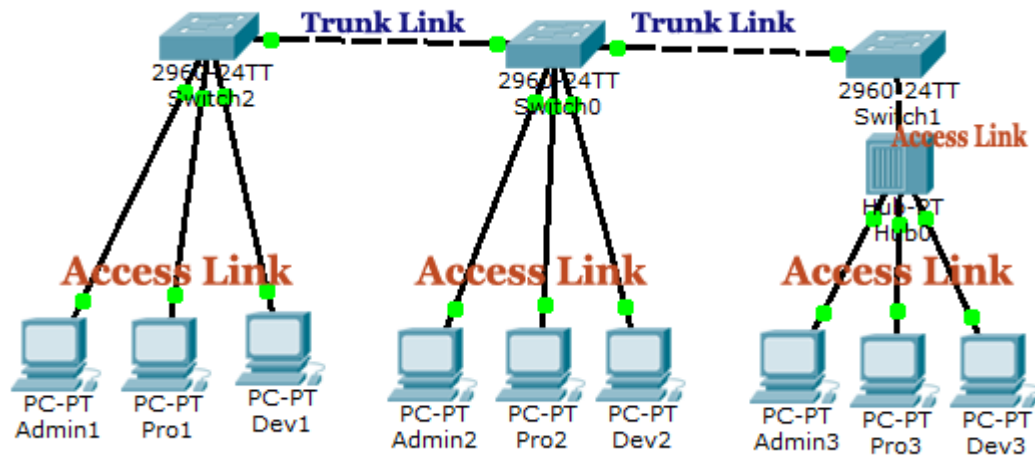
Mode TRUNK

Le mode TRUNK est utilisé dans le cas où plusieurs VLAN doivent circuler sur un même lien. Les trames sont taguées et cela est utilisé pour transporter plusieurs VLANs d'un switch à un autre. On trouve une liaison TRUNK entre :

- Deux commutateurs
- Un commutateur et un hôte (Attention à la sécurité de l'hôte car dans ce mode il peut accéder à tous les VLAN du réseau).
- Un commutateur et un routeur.

Mode ACCESS

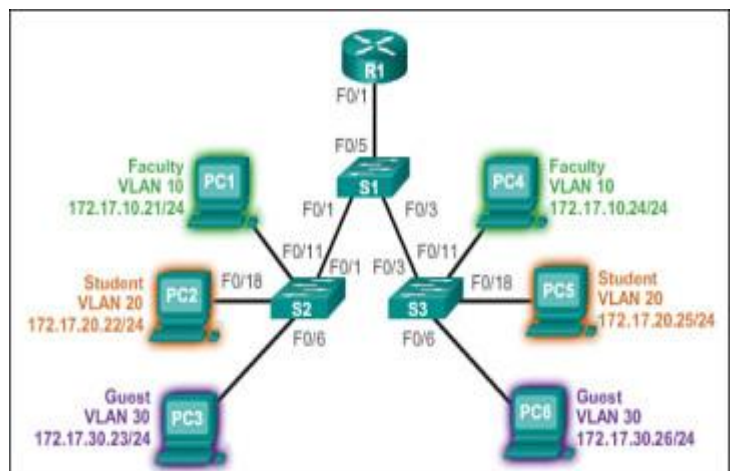
Le mode ACCESS est utilisé pour la connexion terminale d'un périphérique (pc, imprimante, serveur, ...) appartenant à un seul VLAN. Ajout d'un TAG dans la trame. Lorsque la trame quitte un port de type "ACCESS" alors il perd son TAG.



Exercice

Précisez le mode (access ou trunk) des ports des switch et du routeur.

Switch / routeur	Ports en mode access	Ports en mode trunk
S2	F0/6 – F0/11 – F0/18	F0/1
S3	F0/6 – F0/18 – F0/11	F0/3
S1	Rien	F0/1 – F0/3 – F0/5
R1	Rien	F0/1



5 - Cas particulier du VLAN de configuration

Le VLAN de configuration est un VLAN présent sur le commutateur et permettant la configuration du SWITCH à distance. Pour cela, il dispose d'une adresse IP pour être joignable à distance. Par défaut, il n'est pas activé et tous les ports lui sont attribués.

6 - Le routage inter-VLAN

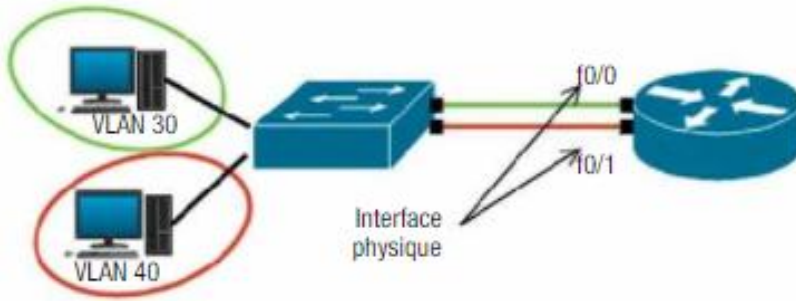
Un VLAN représente un domaine de diffusion unique. Dans ce cas, les périphériques situés sur des VLANs différents ne peuvent pas communiquer.

Si l'on souhaite établir une connectivité entre des utilisateurs situés sur des VLANs différents alors il faut mettre en place du routage inter-VLAN.

Trois solutions :

- Legacy inter-VLAN routing (couteux en port)
- Router on a stick (1 port mais plusieurs interfaces virtuelles)
- Multilayer switching (pas besoin de routeur mais d'un switch de niveau 3)

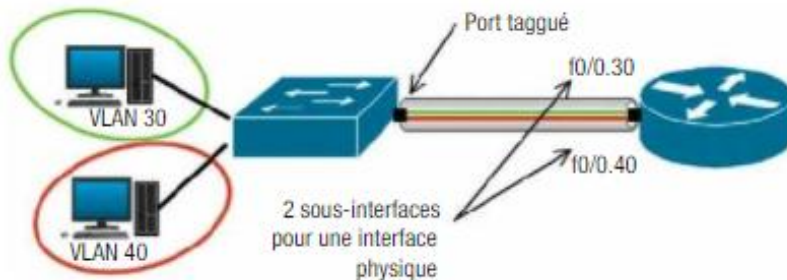
- SOLUTION 1 : Legacy inter-VLAN routing



Cette solution nécessite un routeur avec autant de ports qu'il y a de VLANs sur le Switch.

Solution inadaptée pour des réseaux avec beaucoup de VLANs.

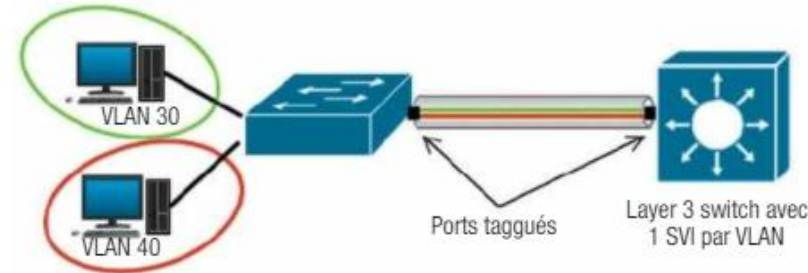
- SOLUTION 2 : Router on a stick



Cette solution utilise qu'une connexion entre le SWITCH et le Routeur, mais l'interface du routeur est divisée "**virtuellement**" en plusieurs sous interface (.10, .20, .30, ...).

Inconvénient : Tout le trafic passe par la même interface et cela peut provoquer un goulot d'étranglement.

- SOLUTION 3 : Multilayer switching



C'est la solution la plus utilisée.

Elle nécessite un SWITCH de niveau 3 capable d'effectuer du routage inter-VLAN
(Configuration hors programme du BTS).

Activité pratique

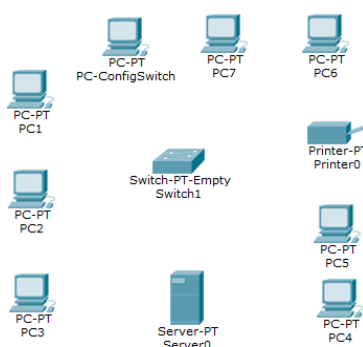
L'objectif de cette activité est de définir plusieurs VLANs en configurant les ports d'un switch. Vous utiliserez le logiciel Packet Tracer pour réaliser le schéma de câblage, effectuer la configuration du switch et simuler le réseau.

Remarque :

- ✍ Ce symbole signifie qu'il faut rédiger une réponse sur votre compte rendu.
- 🔧 Ce symbole signifie qu'il faut exécuter, manipuler, configurer un élément.

Pour paramétrer le switch, vous utiliserez la fiche "**Fiche SWITCH - Commandes CISCO.pdf**" qui propose une description des principales fonctions utilisées pour la configuration d'un switch.

👉 3 - Saisissez le schéma ci-dessous sous Packet tracer.



Modèle du switch utilisé : **switch-PT-Empty**.
Equipement : 10 modules "**PT-SWITCH-NM-1CGE**"

4 - Configurez les adresses IP des postes PC0 à PC6 en respectant les caractéristiques suivantes :

- Nom du réseau : 192.168.1.0

- Masque de sous réseau : 255.255.255.0

Attention : le **PC-ConfigSwitch** ne doit pas être connecté au switch à l'aide d'un câble Ethernet. Par mesure de sécurité, ce PC est isolé du réseau.

5 - Testez la configuration des postes (ping) et présentez les résultats dans un tableau. Il n'y a pas de VLAN pour le moment.

	Communique avec ...								
Hôte	PC1	PC2	PC3	PC4	PC5	PC6	PC7	Imprimante	Serveur
PC 1		x	x	x	x	x	x	x	x
PC 2	x		x	x	x	x	x	x	x
PC 3	x	x		x	x	x	x	x	x
PC 4	x	x	x		x	x	x	x	x
PC 5	x	x	x	x		x	x	x	x
PC 6	x	x	x	x	x		x	x	x
PC 7	x	x	x	x	x	x		x	x
Impr	x	x	x	x	x	x	x		x
Serv	x	x	x	x	x	x	x	x	

6 – Connectez-vous au switch avec l'outil terminal.

7 – Changez le nom du switch. Nouveau nom : "TP_Switch4"

Commande CISCO : **Switch(config)#hostname TP_Switch4**

8 – Définissez un mot de passe pour activer le mode privilège. (Mot de passe = **MdpPrivilege**)

Commande CISCO :

TP_Switch4(config)#enable password MdpPrivilege

9 – Définissez les noms des VLAN 2,3 et 4. Vous affecterez les ports aux VLAN à la question 13.

Nom VLAN 2 : Nom "administration" – PC4, PC5, le serveur et l'imprimante.

Nom VLAN 3 : Nom "atelier" – PC1, PC2, PC3.

Nom VLAN 4 : Nom "commercial" – PC6, PC7.

Commandes CISCO : (exemple pour le VLAN 2)

TP_Switch4(config)#vlan 2

TP_Switch4(config-vlan)#name administration

TP_Switch4(config-vlan)#exit

✍ 10 – Affichez la liste des VLAN disponibles sur le switch. Compléter le tableau suivant :

Commandes CISCO : **TP_Switch4#show vlan**

Numéro VLAN	Nom du VLAN	Etat du VLAN	Ports affectés
1	default	Actif	Gig0/1 – Gig1/1 – Gig2/1 – Gig3/1 Gig4/1 – Gig5/1 – Gig6/1 – Gig7/1 Gig8/1 – Gig9/1
2	administration	Actif	
3	atelier	Actif	
4	commercial	Actif	

✍ 11 – Que constate-t-on au niveau de l'affectation des ports ?

Tous les ports sont affectés par défaut au VLAN 1 qui est aussi le VLAN de configuration.

✍ 12 – Déterminer le mode "access" ou "trunk" pour les différentes interfaces du switch.

Hôtes	Nom de l'interface du switch	Mode access ou trunk	VLAN
PC 1	Gig0/1	access	vlan 3
PC 2	Gig1/1	access	vlan 3
PC 3	Gig2/1	access	vlan 3
PC 4	Gig3/1	access	vlan 2
PC 5	Gig4/1	access	vlan 2
PC 6	Gig5/1	access	vlan 4
PC 7	Gig6/1	access	vlan 4
Imprimante	Gig7/1	access	vlan 2
Serveur	Gig8/1	access	vlan 2

✍ 13 – Configurez les bons modes pour toutes les interfaces utilisées du switch.

Commandes CISCO pour la première interface :

TP_Switch4(config)#interface gigabitEthernet 0/1

TP_Switch4(config-if)#switchport mode access

TP_Switch4(config-if)#switchport access vlan 3

TP_Switch4(config-if)#exit

✍ 14 – Désactivez les interfaces non utilisées.

Commandes CISCO :

TP_Switch4(config)#interface gigabitEthernet 0/1

TP_Switch4(config-if)#shutdown

TP_Switch4(config-if)#exit

☞ 15 – Affichez la liste des VLAN et vérifier la conformité avec le cahier des charges.

✍ 16 – Testez la configuration des postes (ping) et présentez les résultats dans un tableau.

		Communique avec ...								
Hôte	Nom VLAN	PC1	PC2	PC3	PC4	PC5	PC6	PC7	Imprimante	Serveur
PC 1	atelier		X	X	échec	échec	échec	échec	échec	échec
PC 2	atelier	X		X	échec	échec	échec	échec	échec	échec
PC 3	atelier	X	X		échec	échec	échec	échec	échec	échec
PC 4	administration	échec	échec	échec		X	échec	échec	X	X
PC 5	administration	échec	échec	échec	X		échec	échec	X	X
PC 6	commercial	échec	échec	échec	échec	échec		X	échec	échec
PC 7	commercial	échec	échec	échec	échec	échec	X		échec	échec
Impr	administration	échec	échec	échec	X	X	échec	échec		X
Serv	administration	échec	échec	échec	X	X	échec	échec	X	

✍ 17 – Que peut-on en conclure pour les postes qui ne sont pas sur le même VLAN.

On constate que les postes qui sont sur le même VLAN peuvent communiquer, par contre, s'ils sont sur des VLAN différents, la communication est impossible.

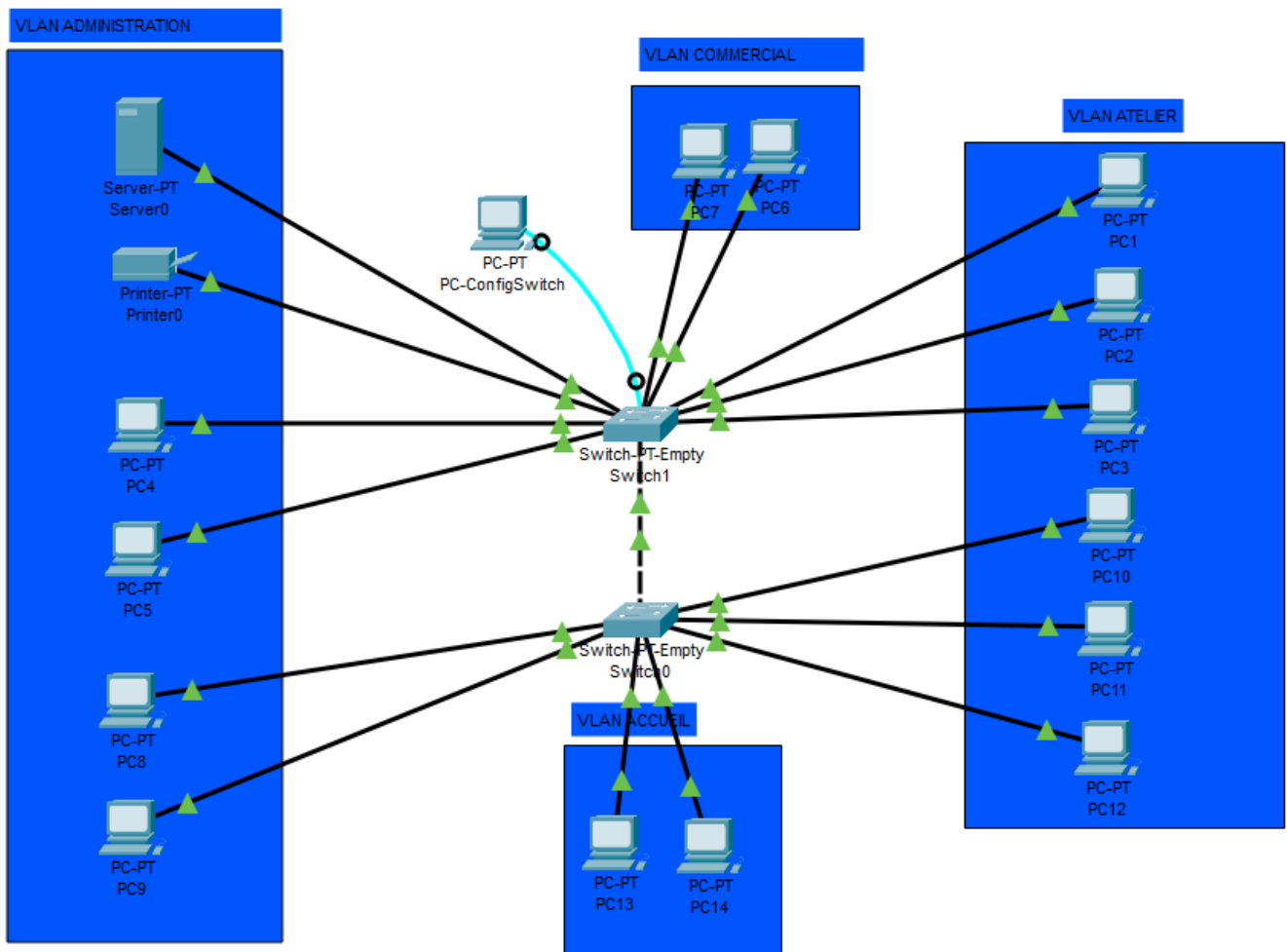
✍ 18 – Quelle solution pourrait-on proposer pour résoudre ce problème ? (Ne pas mettre en œuvre votre solution)

Il faut utiliser un routeur et faire du routage inter-VLAN. Il existe trois solutions (voir la partie cours page 4)

L'entreprise vient de construire un nouveau bâtiment. Il accueille de nouveaux bureaux et une extension de l'atelier.

- 2 bureaux équipés de 2 ordinateurs (PC 8 et PC 9). Ils appartiennent au VLAN administration.
- Extension atelier : 3 ordinateurs PC10, PC11 et PC12. Ils appartiennent au VLAN atelier.
- Hall d'accueil de l'entreprise : 2 ordinateurs PC13, PC14. Définir un nouveau VLAN "accueil" pour ces deux éléments.
- Tous les postes informatiques ont les mêmes caractéristiques : Full Duplex -1 Gbits/s

Ce bâtiment sera géré à partir d'un deuxième switch (identique au précédent). Il sera relié au premier.



✍ 19 – L'interface Gig9/1 du SWITCH 1 sera reliée à l'interface Gig9/1 du SWITCH 2. Quel mode utilise-t-on pour relier les deux switches ?

Il faudra utiliser le mode TRUNK pour permettre le passage de plusieurs VLAN par la même interface du SWITCH. Ne pas oublier de réactiver l'interface Gig9/1 du SWITCH1 et de la configurer en mode TRUNK aussi.

✍ 20 – Proposez les commandes CISCO pour configurer correctement ces deux interfaces.

```
Switch(config)#interface gigabitEthernet 9/1
Switch(config-if)#switchport mode TRUNK
Switch(config-if)#switchport trunk native vlan 2
Switch(config-if)#switchport trunk allowed vlan add 1 (OU ... allowed vlan add 1-5)
Switch(config-if)#switchport trunk allowed vlan add 2
Switch(config-if)#switchport trunk allowed vlan add 3
Switch(config-if)#switchport trunk allowed vlan add 4
Switch(config-if)#switchport trunk allowed vlan add 5
Switch(config-if)#exit
```

👉 21 – Configurez les autres interfaces du SWITCH 2.

✍ 22 – Testez ce nouveau réseau et concluez.

Fonctionnement correct