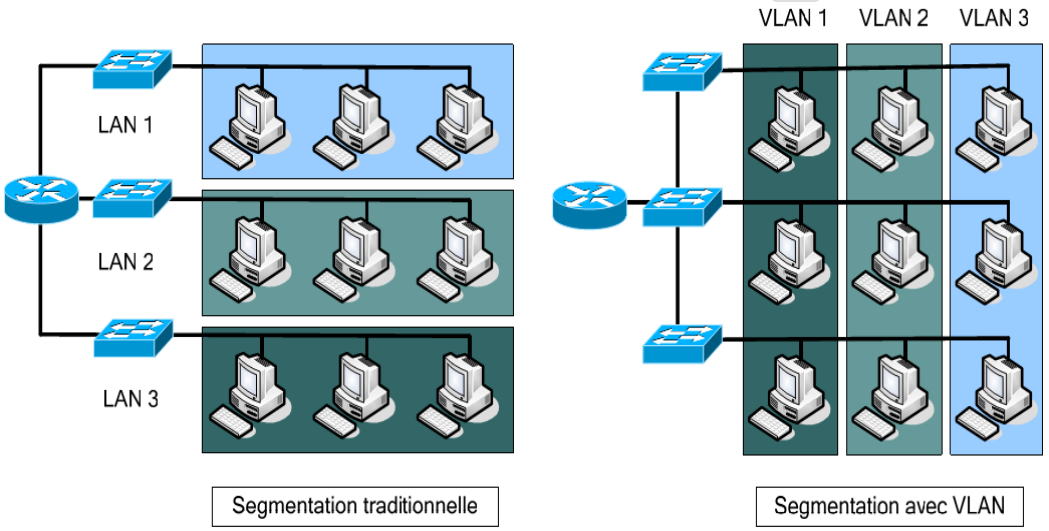
Chapitre 02	Mettre en œuvre les VLAN

1. Présentation des VLAN

1.1. VLAN, c'est quoi ?

- VLAN = Virtual LAN (anglais) = Réseau local virtuel (français)
- VLAN est un ensemble d'unités regroupées en domaine de diffusion quel que soit l'emplacement de leur segment physique.



- Les VLANs reposent sur des connexions logiques, et non des connexions physiques.
- Les VLANs permettent à un administrateur de segmenter les réseaux en fonction de facteurs (ex. fonction, équipe de projet…) quel que soit l'emplacement physique de l'utilisateur ou du périphérique.
- N'importe quel port de commutateur peut appartenir à un VLAN.
- Chaque VLAN est considéré comme un réseau logique distinct et les paquets destinés aux stations n'appartenant pas au VLAN doivent être transférés par un périphérique qui prend en charge le routage.
- Un VLAN crée un domaine de diffusion logique qui peut s'étendre sur plusieurs segments de réseau local physique.

1.2. Avantages de VLAN

Sécurité optimisée	Les groupes contenant des données sensibles sont séparés du reste du réseau, ce qui diminue les risques de violation de confidentialité.
Coûts réduits	Des économies sont réalisées grâce à une diminution des mises à niveau onéreuses du réseau et à l'utilisation plus efficace de la bande passante.

Meilleures performances	La division des réseaux linéaires de couche 2 en plusieurs groupes de travail logiques (domaines de diffusion) réduit la quantité de trafic inutile sur le réseau et augmente les performances.
Domaines de diffusion réduits	La division d'un réseau en VLAN réduit le nombre de périphériques dans le domaine de diffusion.
Gestion efficace	Les VLAN rassemblent des utilisateurs et des périphériques réseau pour prendre en charge des impératifs commerciaux ou géographiques.

1.3. Types de VLANs

VLAN de données	Un VLAN configuré pour transmettre le trafic généré par l'utilisateur.
VLAN par défaut	Tous les ports de commutateur font partie du VLAN par défaut après le démarrage initial d'un commutateur chargeant la configuration par défaut. Le VLAN par défaut pour les commutateurs Cisco est VLAN 1
VLAN natif	Un VLAN natif est affecté à un port trunk 802.1Q.
VLAN de gestion	Un VLAN configuré pour accéder aux fonctionnalités de gestion d'un commutateur. Le VLAN 1 est le VLAN de gestion par défaut.

2. Configuration des VLAN

2.1. Plages VLAN des commutateurs

- Le nombre de VLAN pris en charge est suffisamment élevé pour répondre aux besoins de la plupart des entreprises.
- Par exemple, sur les commutateurs Catalyst (gamme 2960 et 3560), les VLAN à plage normale sont numérotés de 1 à 1005 et les VLAN à plage étendue, de 1006 à 4094.

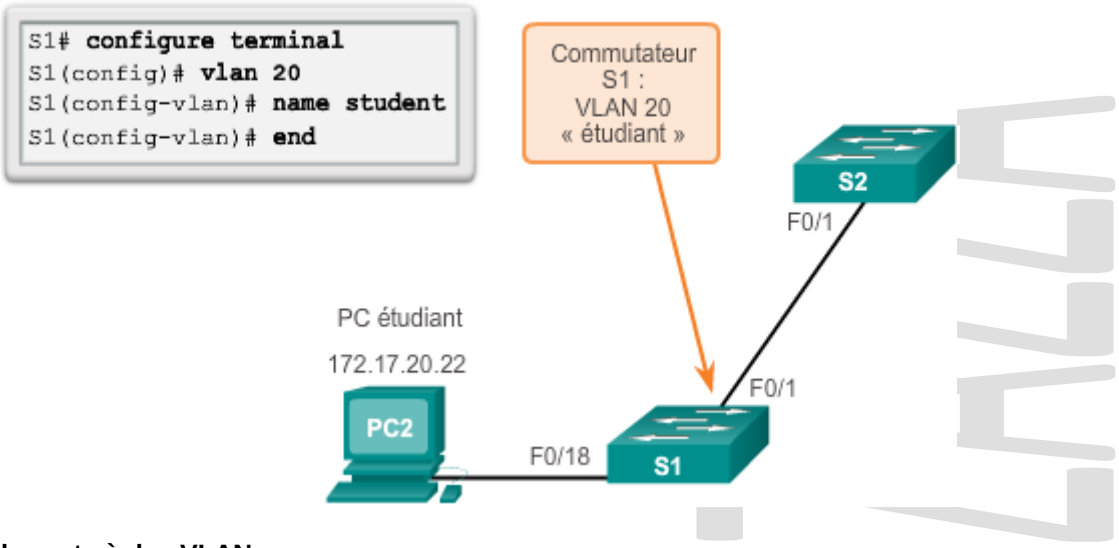
2.2. Création de VLAN

- Lors de la configuration de VLAN à plage normale, les détails de la configuration sont stockés dans la mémoire Flash du commutateur dans un fichier nommé **vlan.dat**.
- La mémoire Flash est permanente et ne requiert pas la commande **copy running-config startup-config**. Cependant, comme d'autres détails sont souvent configurés sur un commutateur Cisco au moment où ces VLAN sont créés, il est recommandé d'enregistrer les modifications de la configuration en cours dans la configuration initiale.
- Voici les commandes de création des VLAN :

Créer un VLAN avec un numéro d'identité valide.	S1(config)# **vlan** *id-vlan*

Indiquer un nom unique pour identifier le VLAN	S1(config-vlan)# **name** *nom-vlan*

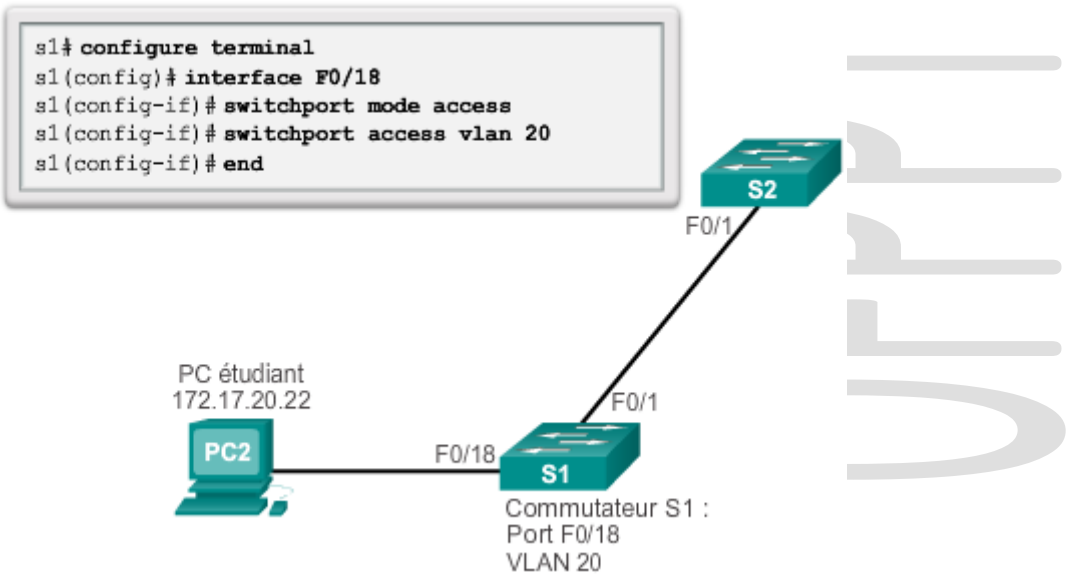
- Exemple :



2.3. Affectation de ports à des VLAN

Passer en mode de configuration d'interface pour SVI	S1(config)# **interface** *id-interface*
Définir le port en mode d'accès	S1(config)# **switchport mode access**
Affecter le port à un réseau local virtuel	S1(config-vlan)# **switchport access vlan** *id-vlan*

- Exemple :



- Remarque : la commande **interface range** permet de configurer simultanément plusieurs interfaces.
- Exemple :

```
S1 (config) # interface range  fa0/1 – 5
S1 (config-if-range) # switchport mode access
S1 (config-if-range) # switchport access vlan 20
```

2.4. Suppression de l'affectation de ports aux VLAN :

Passer en mode de configuration d'interface	S1 (config) # **interface** *interface_id*
Supprimer l'attribution VLAN du port	S1 (config-if) # **no switchport access vlan**

2.5. Suppression de VLAN

Supprimer un VLAN de la base de données VLAN	S1 (config) # **no vlan** *id-vlan*
Supprimer tous les VLAN (Rétablir les paramètres d'usine)	S1 (config) # **delete flash: vlan.dat**

- Attention : avant de supprimer un VLAN, il faut réattribuer tous les ports lui appartenant à un autre VLAN. Tous les ports qui ne sont pas déplacés vers un VLAN actif ne pourront plus communiquer avec d'autres hôtes une fois le VLAN supprimé et tant qu'ils ne seront pas attribués à un VLAN actif.
- Remarque : La commande **delete vlan.dat** peut être utilisée pour supprimer tous les VLAN si le fichier vlan.dat n'a pas été déplacé de son emplacement par défaut (flash).

2.6. Vérification des interfaces VLAN

show vlan [**brief** | **id** *vlan_id* | **name** *vlan_name* | **summary**]	
brief	Affiche une ligne pour chaque VLAN comportant le nom du VLAN, son état et ses ports.
id *vlan_id*	Affiche des informations sur un VLAN unique identifié par son numéro.
name *vlan_name*	Affiche des informations sur un VLAN unique identifié par son nom
summary	Affiche un résumé sur les VLAN.

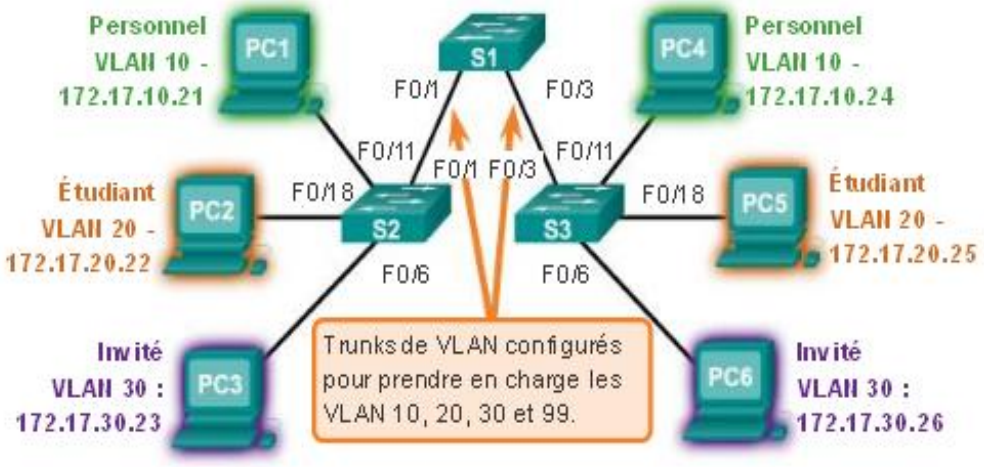
show interfaces [*interface_id* | **vlan** *vlan_id*] | **switchport**	
interface_id	Les interfaces autorisées comprennent les ports physiques (type, numéro de port, …) et les canaux de port (plage comprise entre 1 et 6).
vlan *vlan_id*	Identification du VLAN. La plage est comprise entre 1 et 4094.
switchport	Affiche l'état administratif et opérationnel d'un port de commutation, y compris les paramètres de blocage et de protection du port.

3. Trunk de VLAN

3.1. Définition du trunk de VLAN

- Un **Trunk de VLAN** est une liaison point à point entre deux commutateurs qui acheminent le trafic pour tous les VLAN.

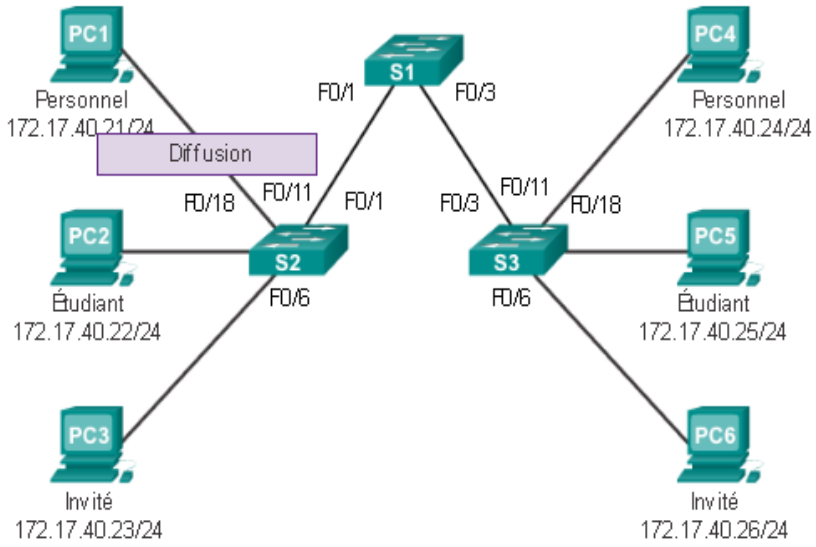
- Les trunks de VLAN permettent à tout le trafic VLAN de se propager entre les commutateurs, de sorte que les périphériques du même VLAN connectés à différents commutateurs puissent communiquer sans l'intervention d'un routeur.



- Un trunk de VLAN n'appartient pas à un VLAN spécifique, mais constitue plutôt un conduit pour plusieurs VLAN entre les commutateurs et les routeurs.
- Cisco prend en charge la norme IEEE 802.1Q pour la coordination des trunks sur les interfaces Fast Ethernet, Gigabit Ethernet et 10 Gigabit Ethernet.

3.2. Contrôle des domaines de diffusion à l'aide de VLAN

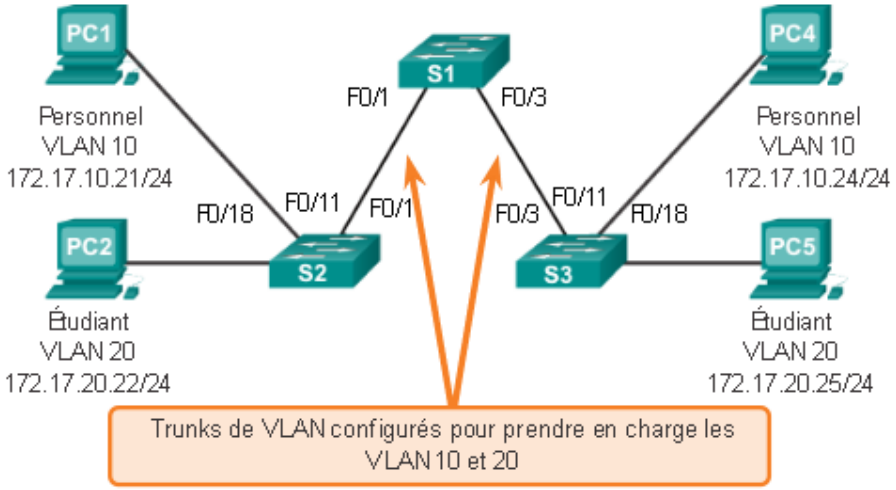
Réseau sans VLAN	Dans des circonstances normales, lorsqu'un commutateur reçoit une trame de diffusion sur l'un de ses ports, il la transfère par tous les autres ports, à l'exception du port de réception. Dans l'exemple suivant, PC1 envoie une diffusion de couche 2 locale. Les commutateurs transmettent la trame de diffusion par tous les ports disponibles. Par la suite, l'ensemble du réseau reçoit la diffusion, car il s'agit d'un seul domaine de diffusion.



Réseau avec VLAN

Le réseau a été segmenté en utilisant deux VLAN. Lorsqu'une trame de diffusion est envoyée de PC1 au commutateur S2, ce dernier transfère la trame de diffusion uniquement aux ports du commutateur configurés pour prendre en charge le VLAN 10.

Dans l'exemple suivant, PC1 envoie une diffusion de couche 2 locale. Les commutateurs transmettent la trame de diffusion uniquement par les ports configurés pour le VLAN 10.



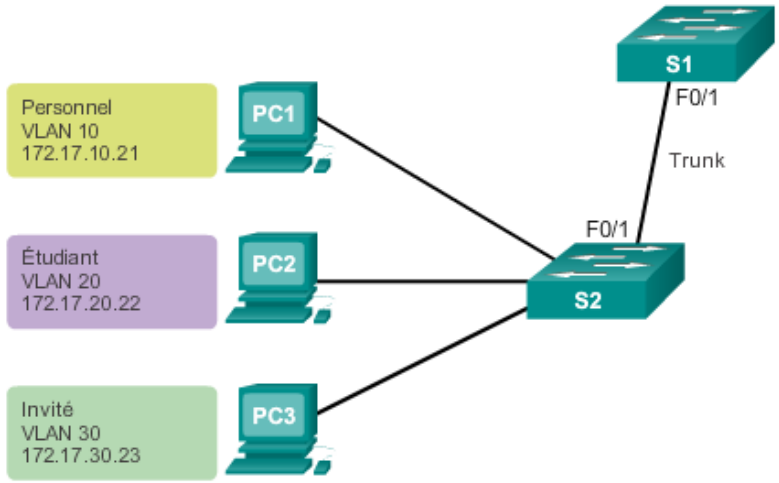
3.3. Configuration du trunk

Passer en mode de configuration d'interface	S1 (config) # **interface** *interface_id*
Forcer la liaison à devenir une liaison trunk	S1 (config-if) # **switchport mode trunk**
Indiquer un VLAN natif pour les trunks 802.1Q non étiquetés	S1 (config-if) # **switchport trunk native vlan** *vlan_id*
Indiquer la liste des VLAN autorisés sur la liaison trunk. Par défaut, tous les VLAN sont autorisés sur une liaison trunk.	S1 (config-if) # **switchport trunk allowed vlan** *vlan_list*

Vérification de la configuration de trunk sur une interface.	S1 # **show interfaces** *interface_id* **switchport**

- **Remarque** : Pour activer une liaison trunk, la configuration des ports sur chaque extrémité de la liaison physique doit être pareille.
- **Exemple :**

VLAN 10 : Personnel - 172.17.10.0/24
VLAN 20 : Etudiant - 172.17.20.0/24
VLAN 30 : Invité [172.17.30.0/24]
VLAN 99 : Native [172.17.99.0/24]



S1(config) # **interface FastEthernet0/1**
S1(config-if) # **switchport mode trunk**
S1(config-if) # **switchport trunk native vlan 99**
S1(config-if) # **switchport trunk allowed vlan 10, 20, 30, 99**

3.4. Pour réinitialiser le trunk à l'état par défaut

Passer en mode de configuration d'interface	S1 (config) # **interface** *interface_id*
Définir le trunk de sorte qu'il autorise tous les VLAN	S1 (config-if) # **no switchport trunk allowed vlan**
Redéfinir le VLAN natif sur les paramètres par défaut	S1 (config-if) # **no switchport trunk native vlan**

- **Remarque :** une fois réinitialisé sur l'état par défaut, le trunk autorise tous les VLAN et utilise le VLAN 1 comme VLAN natif.

4. Routage inter-VLAN

4.1. Pourquoi le routage inter-VLAN ?

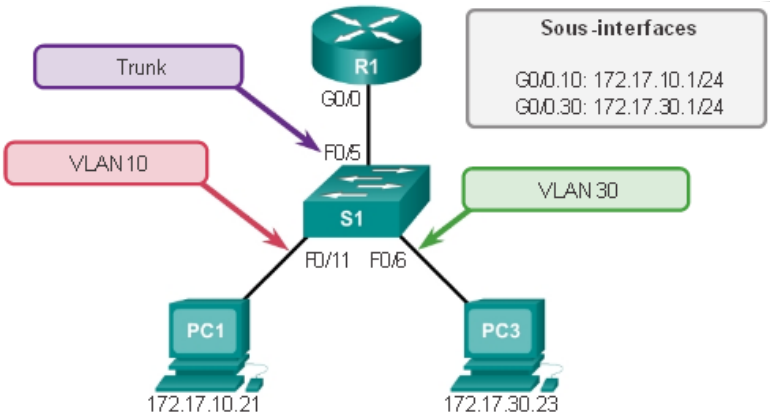
- Un VLAN est un **domaine de diffusion**, cela veut dire que les ordinateurs se trouvant sur des VLAN différents ne peuvent donc pas communiquer sans l'intervention d'un dispositif de routage (routeur ou commutateur multicouche).
- Le **routage inter-VLAN** est un processus de transfert du trafic réseau d'un VLAN à un autre.

4.2. Types de routage inter-VLAN

Routage inter-VLAN existant	Repose sur l'utilisation des routeurs où chaque interface devait être connectée à un réseau distinct et configurée pour un VLAN différent. Les différentes interfaces de routeur physiques sont connectées aux différents ports de commutateur physiques.
Routage inter-VLAN « router-on-a-stick »	Un type de configuration de routeur dans laquelle une seule interface physique achemine le trafic entre plusieurs VLAN d'un réseau.
Routage inter-VLAN commutateurs multicouches	Les commutateurs multicouches peuvent effectuer des fonctions de couche 2 et 3, ce qui évite aux routeurs dédiés d'effectuer du routage de base sur un réseau. Les commutateurs multicouches prennent en charge le routage dynamique et le routage inter-VLAN.

4.3. Configurer le routage inter-VLAN « router-on-a-stick »

- L'interface physique du routeur doit être connectée à une liaison trunk sur le commutateur adjacent.
- Sur le routeur, des sous-interfaces sont créées pour chaque VLAN unique sur le réseau.



Étape 1 : Activer le trunking sur le port du commutateur connecté au routeur	S1(config)# **interface f0/5** S1(config-if)# **switchport mode trunk**
Étape 2 : Configurer les sous-interfaces du routeur	R1(config)# **interface g0/0.10** R1(config-subif)# **encapsulation dot1q 10** R1(config-subif)# **ip address 172.17.10.1 255.255.255.0** R1(config-subif)# **exit** R1(config)# **interface g0/0.30** R1(config-subif)# **encapsulation dot1q 30** R1(config-subif)# **ip address 172.17.30.1 255.255.255.0** R1(config-subif)# **end**

	R1(config)# **interface g0/0** R1(config-if)# **no shutdown**
Étape 3 : Vérifier la configuration	PC1> **ping 172.17.30.23** PC1> **tracert 172.17.30.23**

4.4. Configuration du routage inter-VLAN « commutateurs multicouches »

- Le modèle router-on-a-stick est facile à mettre en œuvre, car les routeurs sont généralement disponibles dans chaque réseau.
- La plupart des réseaux d'entreprise utilisent des commutateurs multicouches pour atteindre des taux de traitement des paquets élevés via une commutation matérielle. Les commutateurs de couche 3 offrent généralement des débits de l'ordre de plusieurs millions de paquets par seconde, alors que les routeurs traditionnels assurent des commutations allant de 100 000 à plus de 1 million de paquets par seconde.
- Tous les commutateurs multicouches Catalyst prennent en charge les types d'interfaces de couche 3 suivants :
  - **Port routé** : interface de couche 3 pure similaire à une interface physique sur un routeur Cisco IOS.
  - **Interface virtuelle de commutateur (SVI)** : interface VLAN virtuelle pour le routage inter-VLAN. En d'autres termes, les interfaces SVI sont des interfaces VLAN virtuellement acheminées.
- Tous les commutateurs Cisco Catalyst de couche 3 prennent en charge les protocoles de routage, mais plusieurs modèles de commutateurs Catalyst nécessitent un logiciel optimisé pour des fonctions spécifiques de protocole de routage.

5. Protocole VTP

5.1. A quoi sert le protocole VTP

- **VTP** est l'abrégé de **VLAN Trunking Protocol**.
- Afin de ne pas redéfinir tous les VLANs existant sur chaque commutateur, Cisco a développé le protocole VTP permettant un héritage de VLANs entre commutateur.
- Le protocole VTP est basé sur la norme 802.1q et exploite une architecture client-serveur avec la possibilité d'instancier plusieurs serveurs.

5.2. Architecture de VTP

- Un commutateur doit alors être déclaré comme serveur, on lui attribue également un nom de domaine VTP. C'est sur ce commutateur que chaque nouveau VLAN devra être défini, modifié ou supprimé. Ainsi chaque

commutateur client présent dans le domaine héritera automatiquement des nouveaux VLANs crées sur le commutateur serveur.

- Le protocole VTP minimise donc l'administration dans le réseau commuté. Ceci réduit avantageusement le besoin de configurer les mêmes VLANs sur chaque commutateur individuellement.
- Les commutateurs de VTP peuvent être configurés pour fonctionner suivant les trois modes suivants :

Mode serveur	- L'information est stockée dans la NVRAM, - Il définit le nom de domaine VTP, - Il peut ajouter, modifier ou supprimer un Vlan, - Il stocke la liste des VLAN du domaine VTP.
Mode client	- Il possède un nom de domaine, - Il stocke une liste de Vlan non modifiable.
Mode transparent	- Il ne participe pas aux domaines VTP du réseau, - Il transmet les paquets VTP via ses lien trunk, - Il possède sa propre liste de Vlan qu'il est possible de modifier.

- **Remarque :** Si une des conditions suivantes n'est pas respectée, le domaine de VTP ne sera pas valide et l'information ne se propagera pas :
  - Il faut assigner le même nom de domaine de VTP à chaque commutateur
  - L'option trunk pour l'interconnexion des commutateurs doit être activée.

5.3. Commandes de configuration

Créer un domaine VTP	Switch(config)#**vtp domain TEST**
Configurer un mot de passe VTP	Switch(config)#**vtp password cisco123**
Activer la version 2 de VTP (à faire sur tous les switchs)	Switch(config)#**vtp version 2**
Configurer le mode server (client ou transparent)	Switch(config)#**vtp mode server**
Vérifier le mot de passe VTP configuré	Switch#**show vtp password**
Vérifier les compteurs des messages VTP envoyés et reçus	Switch#**show vtp counters**
Vérifier la configuration globale de VTP	Switch#**show vtp status**

6. Protocole DTP

6.1. Présentation du protocole DTP

- Une interface du commutateur peut être configurée pour le trunking ou le non-trunking, ou pour négocier un trunking avec l'interface voisine.
- La négociation de trunk est gérée par le protocole **DTP** (Dynamic Trunking Protocol).

- DTP fonctionne uniquement de point à point, entre les périphériques réseau.
- Remarque : DTP gère la négociation de trunk uniquement si le port du commutateur voisin est configuré dans un mode trunk qui prend en charge ce protocole.

6.2. Modes de ports selon DTP

`switchport mode access`	- Place le port d'accès en mode non-trunking permanent et négocie pour convertir le lien en liaison non-trunk. - Le port devient un port non-trunk, indépendamment du port voisin (trunk ou non).
`switchport mode dynamic auto`	- Rend le port capable de convertir le lien en liaison trunk. - Le port devient un port trunk si le port voisin est configuré en mode trunk inconditionnel ou souhaitable. - C'est le mode par défaut de tous les ports Ethernet de commutateur.
`switchport mode dynamic desirable`	- Le port tente activement de convertir le lien en liaison trunk. - Le port devient trunk si le port voisin est en mode trunk, desirable ou auto. - C'est le mode de port par défaut sur les anciens commutateurs.
`switchport mode trunk`	- Place le port en mode trunking permanent et négocie pour convertir la liaison en trunk. - Le port devient trunk même si le port voisin n'est pas un port trunk.
`switchport nonegotiate`	- Empêche le port de générer des trames DTP. - Utilisé uniquement lorsque le mode du port est access ou trunk. - Le port voisin doit manuellement être configurée en port trunk pour avoir une liaison trunk.

6.3. Modes d'interfaces négociés

	Dynamique automatique	Dynamique souhaitable	Trunk inconditionnel	Accès
Dynamique automatique	Accès	Trunk inconditionnel	Trunk inconditionnel	Accès
Dynamique souhaitable	Trunk inconditionnel	Trunk Inconditionnel	Trunk Inconditionnel	Accès
Trunk inconditionnel	Trunk inconditionnel	Trunk inconditionnel	Trunk inconditionnel	Connectivité limitée
Accès	Accès	Accès	Connectivité limitée	Accès

6.4. Exercice : Planification du comportement du protocole DTP

Quelles combinaisons du mode DTP entre deux commutateurs deviennent des liaisons de trunk et lesquelles des liaisons d'accès ?

TR = Trunk inconditionnel
AC = Accès
DA = Dynamique automatique
DD = Dynamique souhaitable