les vlans

Table des matières

[Introduction : 2](#_Toc192105338)

[Définition vlan : 2](#_Toc192105339)

[Mise en place de VLAN : 6](#_Toc192105340)

[Mise en place : 6](#_Toc192105341)

[Test : 7](#_Toc192105342)

[Mise en œuvre des VLANs et des trunking 8](#_Toc192105343)

[Définitions : 8](#_Toc192105344)

[Attribution des ports : 8](#_Toc192105345)

[Création des interfaces de gestion virtuelle (SVI) : 8](#_Toc192105346)

[Adressage des interfaces de gestion : 9](#_Toc192105347)

[Configuration des interfaces de gestion : 9](#_Toc192105348)

[Configuration du trunking statique et désactivation du protocole DTP  : 10](#_Toc192105349)

[Configurez le protocole DTP : 11](#_Toc192105350)

[Vérification : 13](#_Toc192105351)

[Test : 14](#_Toc192105352)

[Communication inter-vlan via IP : 14](#_Toc192105353)

[Configuration IP : 14](#_Toc192105354)

[Routeur : 16](#_Toc192105355)

[RIP : 16](#_Toc192105356)

[Adresses IP : 16](#_Toc192105357)

[PCs : 16](#_Toc192105358)

[Server 0 : 16](#_Toc192105359)

[Vérifications : 17](#_Toc192105360)

[Questions : 17](#_Toc192105361)

[Dépannage de routage inter-vlan : 19](#_Toc192105362)

[Détection et résolution des problèmes réseaux : 19](#_Toc192105363)

[Vérifications : 20](#_Toc192105364)

[Dépannage du routage inter-VLAN - Mode Physique : 21](#_Toc192105365)

[Evaluation du fonctionnement du réseau : 21](#_Toc192105366)

[Connection au routeur : 21](#_Toc192105367)

[Connection aux switchs : 22](#_Toc192105368)

[Autres vérifications : 25](#_Toc192105369)

[VLAN natif incorrect : 25](#_Toc192105370)

[VLANs autorisés incorrects sur les trunks : 26](#_Toc192105371)

[Mauvaise configuration sur fa0/5 : 26](#_Toc192105372)

[Mauvaise configuration du VLAN 13 : 27](#_Toc192105373)

[Sources : 29](#_Toc192105374)

# Introduction :

Dans ce TP, on va apprendre à utiliser des réseaux virtuels (VLAN) pour que plusieurs services d’une entreprise puissent accéder à un serveur de fichiers en commun, tout en restant bien séparés les uns des autres. Le but est de tester différentes manières de configurer le réseau pour que chaque service puisse utiliser la ressource partagée, mais sans pouvoir communiquer directement avec les autres services. Cela nous aidera à mieux comprendre comment organiser et sécuriser un réseau informatique.

# Définition vlan :

Un VLAN (Virtual Local Area Network) est une technologie qui permet de segmenter un réseau physique en plusieurs réseaux logiques indépendants, améliorant ainsi la sécurité, la gestion et les performances du réseau. Il permet de regrouper des utilisateurs ou des services selon leur fonction plutôt que leur emplacement physique, réduisant ainsi le trafic de broadcast et optimisant la bande passante. Les VLANs sont couramment utilisés pour séparer différents types de trafic, comme les données utilisateur, la téléphonie VoIP ou la gestion des équipements réseau. Chaque VLAN est identifié par un numéro et fonctionne comme un réseau distinct, nécessitant un routeur ou un pare-feu pour communiquer avec d’autres VLANs. Les ports des switches peuvent être configurés en mode access (associé à un seul VLAN) ou trunk (transportant plusieurs VLANs via un marquage 802.1Q). Grâce aux VLANs, les entreprises peuvent renforcer la sécurité en cloisonnant le trafic et en limitant l’accès aux ressources sensibles, tout en simplifiant l’administration et l’évolution de leur infrastructure réseau.

Une image contenant texte, capture d’écran, Police, conception

Le contenu généré par l’IA peut être incorrect.

Il existe trois modes de configuration des VLANs :

Le mode Access est utilisé pour connecter un appareil final (comme un PC, une imprimante ou un téléphone IP) à un switch. Un port en mode Access appartient à un seul VLAN et ne tague pas le trafic, ce qui signifie que les appareils connectés ne sont pas conscients de l'existence des VLANs. Ce mode est principalement utilisé pour segmenter le réseau et assurer que chaque appareil est isolé dans son VLAN spécifique.

Une image contenant texte, capture d’écran, conception

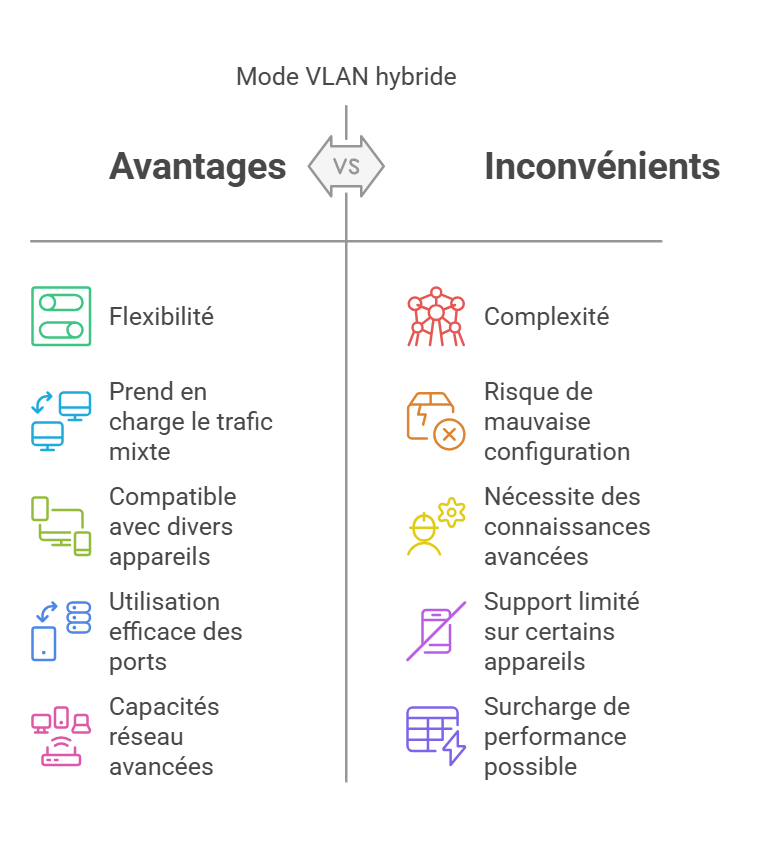
Le contenu généré par l’IA peut être incorrect.

Le mode Trunk, quant à lui, est utilisé pour transporter plusieurs VLANs sur un seul lien physique entre deux équipements réseau (switch-switch, switch-routeur, switch-firewall). Il utilise le protocole 802.1Q pour ajouter une balise (tag) VLAN à chaque trame Ethernet, permettant ainsi d’identifier à quel VLAN appartient chaque paquet. Le VLAN natif est utilisé pour gérer le trafic non tagué sur un trunk.

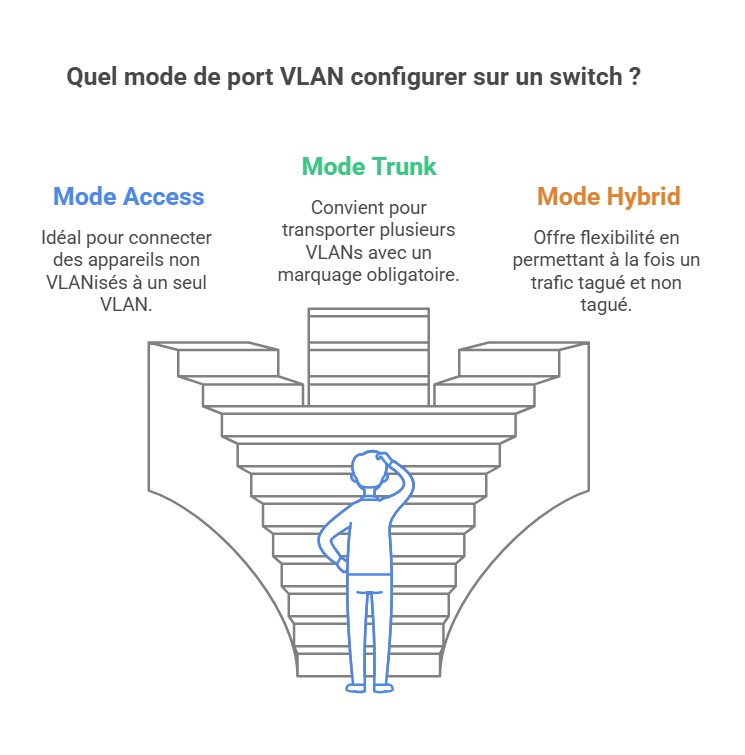
Une image contenant texte, capture d’écran, carte de visite, Police

Le contenu généré par l’IA peut être incorrect.

Le mode Hybrid VLAN est un mode de configuration des ports sur un switch qui permet de transporter à la fois du trafic VLAN tagué et non tagué, tout en offrant plus de flexibilité que les modes Access et Trunk. Il est souvent utilisé sur des équipements réseau avancés, notamment ceux des fabricants comme HPE, Huawei et certains modèles de Cisco, pour s'adapter à des environnements réseau mixtes.Contrairement au mode Trunk, qui transporte plusieurs VLANs mais exige que tous les VLANs (sauf le VLAN natif) soient tagués, le mode Hybrid permet de transmettre simultanément du trafic VLAN tagué et non tagué sur un même port, et ce, pour plusieurs VLANs différents. Cela le rend particulièrement utile dans des scénarios où un même port doit gérer des appareils qui ne comprennent pas le marquage VLAN (comme certains téléphones IP ou imprimantes) tout en autorisant d'autres VLANs tagués à passer.



Pour résumer les différences entre les différents modes :



# Mise en place de VLAN :

J'ai choisi d'utiliser des câbles Straight Through pour relier le matériel, car ils sont spécialement conçus pour connecter des équipements de types différents, comme un PC à un switch ou un switch à un routeur.

Les PC et le serveur admin seront connectés sur les interfaces fa0/0 et fa0/1, les PC et le serveur développement seront connecter sur les interfaces fa0/7 et fa0/8 et les PC et le serveur communication seront sur les interfaces fa0/13 et fa0/14. Les interfaces fa0/21 fa0/22 et fa0/23 sont reservés a l’interconnexion des switchs entre eux.

On met toujours les PC et serveurs sur les premières interfaces et les interconnections sur les dernières pour la lisibilité du réseau et sa maintenance pour réduire les risques d’erreurs de configuration.

## Mise en place :



Je créer des vlans, ici le 110, puis je le nomme. Cela me permet de segmenter le réseau en affectant un groupe spécifique d'appareils à ce VLAN. En nommant le VLAN, je rends la configuration plus lisible et plus facile à gérer, surtout lorsqu'il y a plusieurs VLANs sur le réseau.

Une image contenant texte, Police, capture d’écran, blanc

Le contenu généré par l’IA peut être incorrect.

Je configure l'interface fa0/7 en mode access et je l'associe au vlan 120. Cela signifie que tout appareil connecté à ce port appartiendra uniquement à ce VLAN. Cette configuration est utile pour connecter des postes de travail ou des équipements qui ne doivent pas être dans un mode de commutation dynamique.

Une image contenant texte, capture d’écran, Police, nombre

Le contenu généré par l’IA peut être incorrect.

J'applique une configuration en mode trunk sur une plage d'interfaces fa0/21 à 0/23. Cela permet à ces interfaces de transporter plusieurs vlans, facilitant ainsi la communication entre les switches ou entre un switch et un routeur. Les messages UPDOWN indiquent que les interfaces ont brièvement changé d’état, ce qui peut se produire lors de l’application de la configuration.

J’ai fait le choix de mettre que les interfaces qui ont besoin d’accéder au trunk pour se protéger du VLAN Hopping.

Le VLAN Hopping est une attaque réseau qui permet à un attaquant de s'échapper de son VLAN d'origine et d'accéder à d'autres VLANs. Il existe deux manières d’y arriver. Le Switch Spoofing, ou l’attaquant configure son appareil pour se faire passer pour un switch en utilisant le protocole Dynamic Trunking Protocol (DTP). Si le switch cible a DTP activé, il peut établir un trunk avec l’attaquant, lui permettant d’envoyer et de recevoir du trafic sur plusieurs VLANs. Et le Double Tagging (Double Encapsulation) ou l’attaquant envoie un paquet avec deux étiquettes VLAN (double tagging).Le premier switch enlève la première étiquette VLAN et envoie le paquet au VLAN cible en pensant qu’il est valide.Si le switch de destination ne vérifie pas correctement les balises VLAN, le paquet peut être redirigé vers un VLAN non autorisé.

## Test :

Une image contenant capture d’écran, texte, ligne, Police

Le contenu généré par l’IA peut être incorrect.

Les pings dans le vlan administration fonctionnent mais pas celui d’entre ADM11 et COM11 car ils ne sont pas dans le même vlan. Les vlans segmentent bien le réseau en empêchant les appareils de différents vlan de communiquer entre eux.

Une image contenant texte, capture d’écran, Police, ligne

Le contenu généré par l’IA peut être incorrect.

Les pings dans le vlan développement fonctionnent mais pas celui entre DEV21 et COM21 car ils ne sont pas dans le même vlan. Les vlans segmentent bien le réseau en empêchant les appareils de différents vlan de communiquer entre eux.

Une image contenant capture d’écran, texte, Police, ligne

Le contenu généré par l’IA peut être incorrect.

Les pings dans le vlan commercial fonctionnent mais pas celui d’entre COM31 et DEV31 car ils ne sont pas dans le même vlan. Les vlans segmentent bien le réseau en empêchant les appareils de différents vlan de communiquer entre eux.

# Mise en œuvre des VLANs et des trunking

## Définitions :

Nonegociate : Désactive l'envoi de trames DTP (Dynamic Trunking Protocol), empêchant ainsi l'interface de négocier dynamiquement son mode de fonctionnement (trunk ou access). Elle empêche une interface de basculer en mode trunk accidentellement et donc une meilleure sécurité. Utile lorsqu’on connecte un équipement qui ne supporte pas DTP, ça apporte aussi une meilleure compatibilité et évite l’envoi inutile de trames DTP, une réduction du trafic.

## Attribution des ports :

### Création des interfaces de gestion virtuelle (SVI) :



Je créer un vlan (le 10 ici) et je le renomme pour qu’on puisse l’identifier plus facilement.

### Adressage des interfaces de gestion :

|  |  |  |
| --- | --- | --- |
| Numéro | Noms | Ports |
| 10 | Admin | Fa0/1 ; fa0/4 |
| 20 | Comptes | Fa0/2 |
| 30 | Ressources\_humaines | Fa0/3 |
| 40 | Voix | Fa0/4 |
| 99 | Management | Gig0/2 |
| 100 | Natif | Gig0/1 |

J’attribue un vlan a un port pour segmenter le réseau et optimiser la gestion du trafic en fonction des besoins des utilisateurs et des équipements connectés. En attribuant un VLAN spécifique à un port, je m’assure que le trafic de cet appareil ne sera visible que par d’autres équipements du même VLAN. Cela limite les risques d’attaques comme l’interception de données (sniffing) et empêche la propagation de tempêtes de broadcast à l’ensemble du réseau. Sans VLANs, tous les appareils seraient sur un même domaine de broadcast, ce qui sature le réseau inutilement. Avec les VLANs, le trafic est mieux réparti, réduisant la congestion et améliorant la fluidité des échanges.

Une image contenant texte, Police, blanc, capture d’écran

Le contenu généré par l’IA peut être incorrect.

Je configure le port fa0/1 en mode access, puis je l’associe au VLAN 10. Cela signifie que tous les appareils connectés à ce port feront partie de ce VLAN. C'est une configuration classique pour segmenter le réseau en isolant des groupes d'appareils dans un VLAN spécifique.

PC7 :





Je configure l’interface fa0/4 en l’associant à deux VLANs :

* sw ac vlan 10 pour le trafic de données, ce qui permet aux appareils connectés à ce port de faire partie du VLAN 10.
* sw voice vlan 40 pour le trafic voix, ce qui est typiquement utilisé pour connecter des téléphones IP. Cela permet de prioriser le trafic vocal et de le séparer du trafic standard pour éviter les latences et pertes de qualité.

Il faut configurer les VLANs sur les trois switchs qui communiquent car si le switch reçoit une trame VLAN-tagged (IEEE 802.1Q) et que le VLAN indiqué n'existe pas sur le switch, alors la trame est immédiatement supprimée.

Une image contenant texte, Police, capture d’écran, ligne

Le contenu généré par l’IA peut être incorrect.

### Configuration des interfaces de gestion :



Je crée le VLAN 99 et je lui attribue une adresse IP (192.168.99.254/24). Ce type de configuration est souvent utilisé pour un VLAN de gestion, permettant aux administrateurs d’accéder au switch à distance via une interface réseau distincte.

J’ai aussi configuré le switch SWA pour que l’interface gig0/1 soit sur le même

Il faut aussi configurer le switch SWA car les paquets ICMP ne seront pas propagées correctement entre les switches car SWA agit comme un point de transit entre SWB et SWC.

Une image contenant capture d’écran, texte, ligne, Caractère coloré

Le contenu généré par l’IA peut être incorrect.

### Configuration du trunking statique et désactivation du protocole DTP  :

Une image contenant texte, capture d’écran, Police, nombre

Le contenu généré par l’IA peut être incorrect.

Je modifie les paramètres d'affichage dans *Cisco Packet Tracer* en accédant à Options > Preferences. Ensuite, j’active l’option Always Show Port Labels in Logical Workspace, ce qui permet d’afficher en permanence les noms des ports dans l’espace logique. Cela facilite l’identification des interfaces utilisées sur les équipements réseau et permet de voir les interfaces (pas accessibles sur le .pka).

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Le contenu généré par l’IA peut être incorrect.

Une image contenant texte, Police, capture d’écran, blanc

Le contenu généré par l’IA peut être incorrect.

Je configure l’interface en mode trunk (switchport mode trunk) et désactive la négociation DTP avec switchport nonegotiate. Cela empêche le switch d’envoyer des paquets DTP (Dynamic Trunking Protocol), rendant la configuration statique et évitant d’éventuels conflits avec d’autres équipements. Je le fais sur tous les switchs

Une image contenant texte, Police, ligne, capture d’écran

Le contenu généré par l’IA peut être incorrect.

Je définis le VLAN natif de l’interface gig0/1 sur VLAN 99 (switchport trunk native vlan 99). Cependant, une erreur apparaît : BPDU received with inconsistent VLAN ID, ce qui signifie que l’autre extrémité du lien trunk utilise un VLAN natif différent. Cette incohérence bloque le trafic sur le port concerné.Une image contenant texte, Police, ligne, capture d’écran

Le contenu généré par l’IA peut être incorrect.

Je configure l’interface gig 0/2 sur SA avec un VLAN natif 100 (switchport trunk native vlan 100). Une alerte CDP-4-NATIVE\_VLAN\_MISMATCH est générée, indiquant une différence entre les VLANs natifs sur les switches connectés (VLAN 100 sur SWA, VLAN 99 sur SWC). Cela peut causer des problèmes de communication entre les équipements sur les VLANs natifs.

Une image contenant texte, Police, capture d’écran, ligne

Le contenu généré par l’IA peut être incorrect.

Je reconfigure gig0/1 en mode trunk et désactive la négociation DTP (switchport nonegotiate). Cela empêche l’interface de changer automatiquement de mode, garantissant une configuration stable et cohérente avec l’autre extrémité du lien trunk.

## Configurez le protocole DTP :



J'essaie de configurer l'interface gig0/2 en mode dynamic desirable (switchport mode dynamic desirable), mais une erreur apparaît : "Conflict between 'nonegotiate' and 'dynamic' status". Cela signifie que la négociation DTP (Dynamic Trunking Protocol) est désactivée (switchport nonegotiate), empêchant ainsi l'interface de fonctionner en mode dynamique.

Une image contenant texte, capture d’écran, Police, ligne

Le contenu généré par l’IA peut être incorrect.

Je corrige l'erreur précédente en supprimant la négociation forcée (no switchport nonegotiate), puis je configure l'interface en mode dynamic desirable. Cette fois, la configuration est acceptée et l'interface gig0/2 passe en état up.

Une image contenant texte, capture d’écran, Police, ligne

Le contenu généré par l’IA peut être incorrect.

Je configure l'interface en mode dynamic auto (switchport mode dynamic auto). L'interface passe également en état up, indiquant qu'elle peut maintenant accepter des connexions trunk si l'autre extrémité le demande.

Une image contenant texte, capture d’écran, Police, nombre

Le contenu généré par l’IA peut être incorrect.

J'exécute la commande show cdp neighbors detail sur SWC pour voir les équipements connectés. Je remarque que SWA est connecté via le port gig0/2. Cela permet de confirmer la liaison et d'identifier d'éventuels problèmes de compatibilité.

Une image contenant texte, capture d’écran, Police, nombre

Le contenu généré par l’IA peut être incorrect.

Je vérifie la configuration des trunks avec show interfaces trunk. L'interface gig0/2 est bien en mode trunk avec l'encapsulation 802.1Q et a comme VLAN natif 100. Cependant, elle autorise plusieurs VLANs, y compris 1, 10, 20, 30, 40, 99, 100, ce qui pourrait causer des conflits si l'autre switch n'a pas la même configuration.

Une image contenant texte, capture d’écran, Police, algèbre

Le contenu généré par l’IA peut être incorrect.

Je modifie l'interface gig0/2 en mode accès (switchport mode access) et l'assigne au VLAN 99 (switchport access vlan 99). Cela transforme le port en un port d'accès normal au lieu d'un trunk, ce qui peut être utile si je veux connecter un équipement utilisateur plutôt qu'un autre switch. L'interface VLAN 99 passe en état up, confirmant que la configuration est correcte.

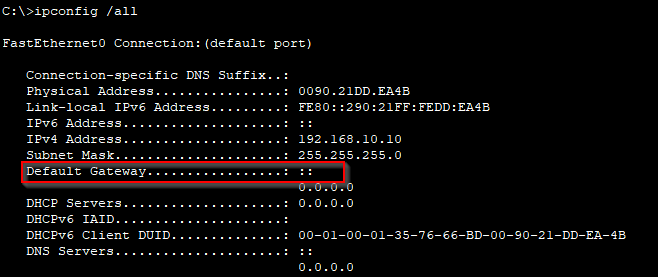
Il faut mettre gig0/1 en nonegotiate et gig0/2 en dynamique sur switch milieu J’ai choisi de configurer Gig0/1 en nonegotiate et Gig0/2 en mode dynamique sur le switch du milieu pour assurer une connectivité efficace tout en maintenant la sécurité et la flexibilité du réseau.

L’interface Gig0/1 est une interconnexion avec un autre switch et je veux qu’elle reste en trunk de manière forcée et sécurisée. En activant switchport nonegotiate, j’empêche le switch d’envoyer ou de répondre aux trames DTP, ce qui verrouille la configuration du trunk et empêche tout changement intempestif. Je m’assure que Gig0/1 restera en trunk quoi qu’il arrive, sans être influencé par un équipement mal configuré ou ne supportant pas DTP. L’interface Gig0/2, quant à elle, est configurée en mode dynamique pour offrir plus de flexibilité, notamment si je connecte un autre switch qui pourrait être configuré en dynamic auto ou dynamic desirable.

## Vérification :



Le ping entre deux postes du même vlan ne fonctionne pas.

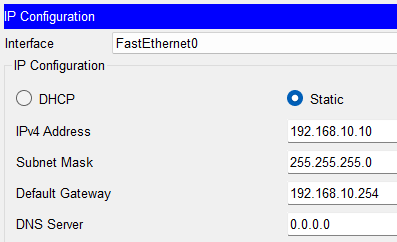


L’adresse de la passerelle par défaut n’est pas configurée sur PC1. Il ne peut donc pas communiquer avec l’exterieur.

Une image contenant texte, capture d’écran, Police, nombre

Le contenu généré par l’IA peut être incorrect.

PC5 n’as pas non plus de passerelle par défaut. Il ne pourra donc pas communiquer au-delà de son VLAN.



Je mets l’adresse IP du vlan, qui est configuré sur l’adresse IP du VLAN (sur le switch) dont l’appareil doit appartenait au VLAN.

## Test :

Une image contenant capture d’écran, texte, ligne, Police

Le contenu généré par l’IA peut être incorrect.

On voit que les pings du PC1 (vlan 10) vers le PC4 (vlan 10) et vers le PC7 (vlan 10) marchent, le routage inter-vlan marche bien. On voit aussi que le ping entre le PC1 (vlan 10) et le PC5 (vlan 20) ne marche pas, les VLANs segmentent donc bien le réseau.

Une image contenant capture d’écran, texte, ligne, Police

Le contenu généré par l’IA peut être incorrect.

On voit que le ping du PC2 (vlan 20) vers le PC5 (vlan 20) marche, le routage inter-vlan marche bien. On voit aussi que le ping entre le PC2 (vlan 20) et le PC6 (vlan 30) ne marche pas, les VLANs segmentent donc bien le réseau.

Une image contenant capture d’écran, ligne

Le contenu généré par l’IA peut être incorrect.

On voit que le ping du PC3 (vlan 30) vers le PC6 (vlan 30) marche, le routage inter-vlan marche bien. On voit aussi que le ping entre le PC3 (vlan 30) et le PC7 (vlan 10) ne marche pas, les VLANs segmentent donc bien le réseau.

# Communication inter-vlan via IP :

On utilise un routeur avec plusieurs interfaces physiques dédiées à un vlan. Chaque vlan a son propre port sur le routeur, ce qui simplifie la gestion et la sécurité et réduit la complexité du routage inter-VLAN. Chaque VLAN a une interface dédiée, ce qui évite la congestion sur un unique lien trunk, ce qui est idéal pour des infrastructures où les besoins en bande passante sont élevés. Il est plus aussi facile pour les administrateurs de comprendre et de dépanner la configuration. Si le réseau évolue et que de nouveaux VLANs sont nécessaires, il faudrait ajouter un routeur avec plus d’interfaces ou utiliser un switch de niveau 3. Une modification du plan de VLANs nécessiterait des changements physiques sur le routeur. Ca nécessite aussi que le routeur dispose du nombre exact de ports Gigabit correspondant aux VLANs.

## Configuration IP :

Une image contenant texte, Police, capture d’écran, ligne

Le contenu généré par l’IA peut être incorrect.

Le vlan 1 est celui par default, il ne peut pas changer car c’est le vlan natif par default.

Je vais changer le vlan natif pour plus de sécurité et pour modifier le vlan 1 comme étant le vlan commerciale :

Une image contenant texte, capture d’écran, Police, ligne

Le contenu généré par l’IA peut être incorrect.

Je crée un VLAN 99 et je le nomme Natif. Ensuite, je configure un ensemble de ports en mode trunk et je spécifie que le VLAN natif est le VLAN 99 avec la commande sw trunk native vlan 99. Le message d’erreur “Received BPDU with inconsistent peer vlan id” indique que le VLAN natif n’est pas cohérent entre deux commutateurs.

Il faut configurer les deux switches sur le même vlan natif car sinon le protocole Spanning Tree détecte un conflit de VLANs natifs. Il considère cela comme une anomalie réseau et bloque l’interface pour éviter des boucles et des incohérences de transmission.

Spanning Tree (STP) est un protocole réseau utilisé pour éviter les boucles dans les réseaux Ethernet commutés. Il permet de détecter et de désactiver les chemins redondants tout en assurant la redondance et la résilience du réseau. Il identifie un "Root Bridge", qui est le switch principal du réseau. Puis il analyse tous les chemins disponibles et désactive automatiquement les liens redondants qui pourraient provoquer des boucles. En cas de panne d’un lien principal, STP peut réactiver un chemin redondant pour assurer la continuité du réseau.



J’essaie de renommer le VLAN 1 en COMMERCIAL avec la commande name COMMERCIAL. Cependant, une erreur apparaît, indiquant que le VLAN 1 ne peut pas être renommé car il est utilisé en interne pour des protocoles de gestion (CDP, VTP, STP, etc.).

Je vais utiliser le vlan 4 pour le COMMERCIAL, à la suite du vlan 1, 2 et 3.



Je configure les interfaces fa0/3 et FastEthernet 0/4 en mode access et je les associe au VLAN. Cela permet aux appareils connectés sur ces ports de faire partie du VLAN 2 uniquement.

Une image contenant texte, capture d’écran, Police, ligne

Le contenu généré par l’IA peut être incorrect.

Je configure l’interface fa0/20 en mode trunk (switchport mode trunk) sur le switch. Ensuite, je limite les VLANs autorisés sur ce lien à 2, 3 et 4 (switchport trunk allowed vlan 2,3,4). Cela signifie que seuls ces VLANs peuvent traverser cette interface. Le message %LINEPROTO-5-UPDOWN indique que l’état de l’interface a changé, d’abord en down puis en up, ce qui indique l’activation de l’interface.

## Routeur :

### RIP :

Une image contenant texte, Police, capture d’écran, blanc

Le contenu généré par l’IA peut être incorrect.

Je configure un routeur avec le protocole RIP version 2 (router rip puis version 2). J’ajoute trois réseaux (network 10.1.0.0, network 172.16.0.0, network 192.168.1.0) pour qu’ils soient annoncés aux autres routeurs RIP. Enfin, la commande no auto-summary désactive le résumé automatique des routes, permettant d’annoncer les sous-réseaux spécifiques plutôt que les réseaux de classe par défaut.

### Adresses IP :

|  |  |  |
| --- | --- | --- |
| VLAN | Adresse IP | Passerelle par défaut |
| 2 | 10.1.0.0/24 | 10.1.0.254 |
| 3 | 172.16.0.0/24 | 172.16.0.254 |
| 4 | 192.168.1.0/24 | 192.168.1.254 |

Le dernier .254 de chaque sous-réseau est utilisé comme adresse de passerelle pour le routage inter-VLAN car c’est la dernière adresse disponible.



J’active l’interface fa0/6

Une image contenant texte, capture d’écran, Police, ligne

Le contenu généré par l’IA peut être incorrect.

Je configure une sous-interface sur fa6/0 pour gérer le trafic du VLAN 2 avec 802.1Q. int fa6/0.2 permet de créer la sous-interface pour le VLAN 2 sur fa6/0. encapsulation dot1Q 2 permet d’activer l’encapsulation 802.1Q pour associer cette sous-interface au VLAN 2. ip address 172.16.0.254 255.255.255.0 permet d’attribuer de l’adresse IP 172.16.0.254 avec un masque 255.255.0.0, qui sert de passerelle aux hôtes du VLAN 2.

## PCs :

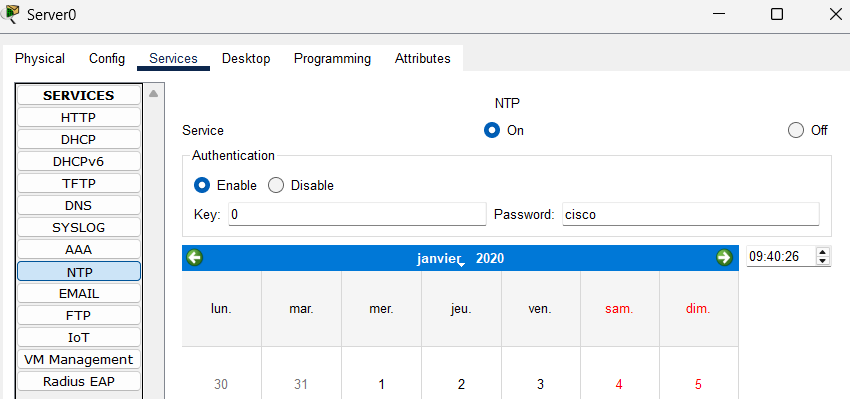
Une image contenant texte, capture d’écran, logiciel, nombre

Le contenu généré par l’IA peut être incorrect.

Dans cette capture, je configure l’adresse IP de PC0 en mode statique sur l’interface FastEthernet0. L’IP attribuée est 10.1.0.1 (a la suite des adresses disponibles dans la plage d’adresse du VLAN) avec un masque de sous-réseau 255.255.255.0. La passerelle par défaut est définie sur 10.1.0.254, ce qui permet au PC de communiquer avec des réseaux externes via le routeur correspondant. Enfin, le serveur DNS est défini sur 192.168.10.10, indiquant que les requêtes de résolution de noms seront envoyées à cette adresse. Cette configuration garantit une connectivité réseau stable sans dépendre d’un serveur DHCP.

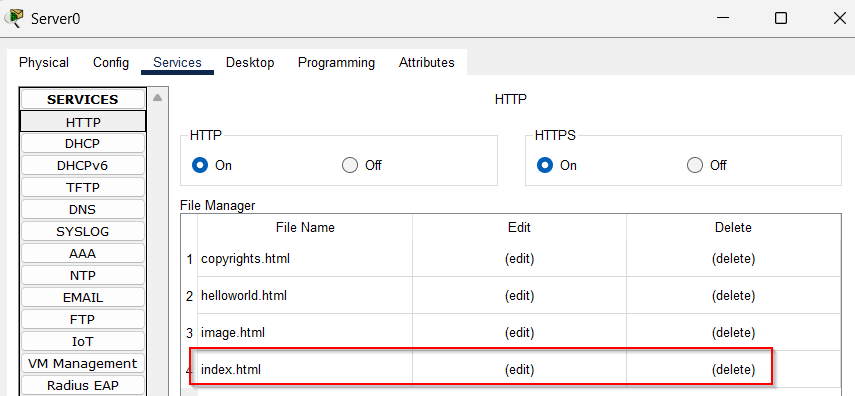
## Server 0 :

### NTP :



Je configure le service NTP sur Server0 en l'activant via l'option On. L'authentification est activée avec un mot de passe défini sur "cisco", ce qui permet de sécuriser la synchronisation horaire entre les périphériques du réseau. La date affichée est janvier 2020, et l'heure est 09:40:26, indiquant que le serveur agit comme une référence de temps pour les autres équipements du réseau.

### HTTP :



Je configure le service HTTP/HTTPS sur le même serveur. Les deux services sont activés, permettant l'hébergement et l'accès aux pages web. Un gestionnaire de fichiers est visible, répertoriant plusieurs fichiers HTML, dont index.html, qui est généralement la page d'accueil d'un site web. Je peux éditer ces fichiers en cliquant sur (edit) ou les supprimer avec (delete). Cette configuration est essentielle pour mettre en place un serveur web interne accessible aux clients du réseau. J’ajoute mon site web dans le fichier index.html pour y accéder en ligne.

### DNS :

Une image contenant texte, capture d’écran, nombre, Police

Le contenu généré par l’IA peut être incorrect.

Dans cette capture, le serveur DNS est activé sur Server0. Il contient deux enregistrements A, associant les noms de domaine vialette.com et vialette.fr à l’adresse IP 192.168.10.10. Cela signifie que tout appareil du réseau qui interroge ce serveur DNS pour ces domaines recevra cette adresse IP en réponse, facilitant ainsi la résolution de noms. Cette configuration est utile pour permettre aux machines du réseau d’accéder à des services hébergés sur 192.168.10.10 en utilisant des noms de domaine plutôt que des adresses IP.

## Vérifications :

Une image contenant texte, capture d’écran, Police, ligne

Le contenu généré par l’IA peut être incorrect.

On voit que le ping du PC0 (vlan 4) vers le PC5 (vlan 4) marche, le routage inter-vlan marche bien. On voit aussi que le ping entre le PC1 (vlan 4) et le PC6 (vlan 2) ne marche pas, les VLANs segmentent donc bien le réseau.

Une image contenant texte, capture d’écran, Police, ligne

Le contenu généré par l’IA peut être incorrect.

On voit que le ping du PC2 (vlan 2) vers le PC6 (vlan 2) marche, le routage inter-vlan marche bien. On voit aussi que le ping entre le PC2 (vlan 2) et le PC7 (vlan 3) ne marche pas, les VLANs segmentent donc bien le réseau.



On voit que le ping du PC4 (vlan 3) vers le PC7 (vlan 3) marche, le routage inter-vlan marche bien. On voit aussi que le ping entre le PC4 (vlan 3) et le PC5 (vlan 2) ne marche pas, les VLANs segmentent donc bien le réseau.

## Questions :

* Quelles sont les adresses IP des réseaux choisis ?

|  |  |  |
| --- | --- | --- |
| VLAN | Adresse IP | Passerelle par défaut |
| 2 | 10.1.0.0/24 | 10.1.0.254 |
| 3 | 172.16.0.0/24 | 172.16.0.254 |
| 4 | 192.168.1.0/24 | 192.168.1.254 |

Les adresses IP sont choisies selon les adresses privées définies par la RFC 1918. Chaque VLAN a un sous-réseau distinct, assurant une segmentation du réseau et améliorant la sécurité et la gestion.

* Quelles sont les adresses IP des cartes réseau du routeur ?

|  |  |
| --- | --- |
| Interface Routeur | Adresse IP |
| Fa6/0.1 | 10.1.0.254 |
| Fa6/0.2 | 172.16.0.254 |
| Fa6/0.3 | 192.168.1.254 |

Chaque VLAN a une sous-interface dédiée sur le routeur pour permettre le routage inter-VLAN. L’adresse .254 est utilisée car elle est facile à identifier comme passerelle pour les machines clientes.

|  |  |  |
| --- | --- | --- |
| FastEthernet6/0.1 | 10.1.0.254 | Passerelle VLAN 1 |

* Quelle est la passerelle par défaut des stations des vlan 1 et 2 et 3 ?

|  |  |
| --- | --- |
| VLAN | Passerelle par défaut |
| 4 (commercial) | 10.1.0.254 |
| 2 (comptabilité) | 172.16.0.254 |
| 3 (production) | 192.168.1.254 |

Les passerelles sont définies sur le routeur et permettent aux stations de communiquer avec d’autres VLANs. Chaque poste client doit être configuré avec la bonne passerelle pour accéder au réseau correctement.

* Quels sont les différents modes pour chacun des ports des switchs ?

|  |  |  |
| --- | --- | --- |
| Port | Mode | Description |
| Connectés aux PC | Access | Assigné à un VLAN spécifique |
| Connectés au routeur | Trunk | Transporte tous les VLANs entre le switch et le routeur |

Les ports en mode Access ne permettent qu’un seul VLAN et sont attribués aux postes utilisateurs. Le port en mode Trunk permet au routeur de gérer plusieurs VLANs sur une seule interface physique.

* Montrer la table MAC et la table ARP du switch :

### Switch1 :

Mac :

Une image contenant texte, capture d’écran, Police, nombre

Le contenu généré par l’IA peut être incorrect.

La commande show arp ne donnais rien malgré les pings effectués car les switches de niveau 2 (comme celui-la) ne conservent pas d’entrée ARP car ils ne routent pas de paquets IP.

ARP :

Une image contenant texte, capture d’écran, Police, nombre

Le contenu généré par l’IA peut être incorrect.

### Switch2 :

Mac :

Une image contenant texte, capture d’écran, Police, nombre

Le contenu généré par l’IA peut être incorrect.

ARP :

Une image contenant texte, capture d’écran, Police, nombre

Le contenu généré par l’IA peut être incorrect.

La commande show arp ne donnais rien malgré les pings effectués car les switches de niveau 2 (comme celui-la) ne conservent pas d’entrée ARP car ils ne routent pas de paquets IP.

# Dépannage de routage inter-vlan :

## Détection et résolution des problèmes réseaux :

Dans ce tableau , il y a une analyse des problèmes réseau et les solutions mises en place pour chaque problème.

|  |  |
| --- | --- |
| Problèmes : | Solutions : |
| Une image contenant texte, Police, blanc, capture d’écran  Le contenu généré par l’IA peut être incorrect.  La commande show interface trunk ne retourne rien, ce qui signifie qu'aucun port du switch n'est en mode trunk. Le switch ne transmet pas les VLANs au routeur, donc le routage inter-VLAN ne peut pas fonctionner. | J’ai configuré le mode trunk sur l’interface. Cela signifie que seuls ces VLANs peuvent traverser ce lien trunk, assurant ainsi la communication inter-VLAN via le routeur. |
| Une image contenant texte, capture d’écran, Police, ligne  Le contenu généré par l’IA peut être incorrect.  L’interface gig0/1.10, du vlan 10 n’est pas activée, ce qui empêche toute communication avec le VLAN 10. | J’ai activé l’interface gig0/1.10 pour permtre aux équipements connectés au VLAN 10 d’accéder au réseau via le routeur. |
| Une image contenant texte, capture d’écran, Police, nombre  Le contenu généré par l’IA peut être incorrect.  L’interface gig0/1.10, celle du VLAN 10 est encapsulée sur le VLAN 30 et non sur le VLAN 10. Ce qui empêche la communication correcte entre les VLANs. | J’ai encapsulé l’interface gig0/1.10 avec le VLAN 10. Ça n’a pas marché car les interfaces sont déjà assignées. Il faut donc les supprimer et les recréer. |
|  | J’ai supprimé les deux interfaces puis j’ai recréé l’interface gig0/1.10 et l’es affectée à l’encapsulation dotlQ 10 |
| Une image contenant texte, capture d’écran, Police, nombre  Le contenu généré par l’IA peut être incorrect.  L’interface gig0/1.30, celle du VLAN 10 est encapsulée sur le VLAN 10 et non sur le VLAN 30. Ce qui empêche la communication correcte entre les VLANs. | J’ai créé l’interface gig0/1.30 et est encapsulé l’interface gig0/1.30 avec le VLAN 30. |
| Les interfaces des VLANs (gig0/1.10 et gig0/1.30) n’ont pas d’adresse IP, le routeur ne peut donc pas communiquer avec les PC dans les VLANs 10 et 30. | J’assigne à l’interface gig0/1.10 l’adresse IP 172.17.10.1 avec le masque 255.255.255.0, permettant à ce routeur d’être la passerelle pour le VLAN 10. Ensuite, je configure gig0/1.30 avec l’adresse IP 172.17.30.1 pour le VLAN 30. Cette configuration permet aux appareils des VLANs 10 et 30 de communiquer via le routeur. |
| PC3 n’a pas la bonne passerelle par default. Elle a celle du VLAN 10 mais elle est sur le VLAN 30. Elle ne pourra donc pas communiquer. | J’ai changé l’adresse IP de la passerelle par defaut pour qu’elle corresponde au VLAN 30 du routeur. |

## Vérifications :

Une image contenant capture d’écran, ligne, Police, texte

Le contenu généré par l’IA peut être incorrect.

J’effectue un test de communication ICMP entre PC1 et R1 via un ping, et le test est réussi. Cela indique que la connectivité du VLAN 10 fonctionne.

Une image contenant capture d’écran, ligne, Police, texte

Le contenu généré par l’IA peut être incorrect.

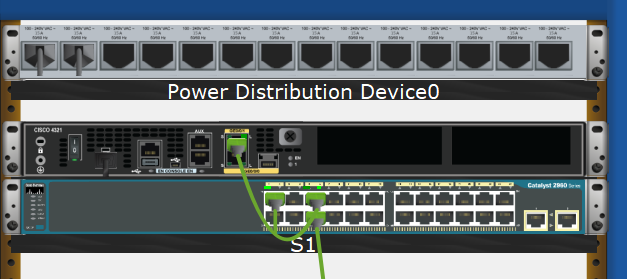
Un test ICMP est effectué entre R1 et PC3, et la communication est également réussie. Cela signifie que le routage du VLAN 30 est opérationnel.

 Un test ICMP est réalisé directement entre PC1 et PC3, et il est réussi. Cela confirme que la communication inter-VLAN est fonctionnelle.

# Dépannage du routage inter-VLAN - Mode Physique :

## Evaluation du fonctionnement du réseau :

### Connection au routeur :



Le routeur est ici car on voit cisco 4321, juste en dessus du switch 1.

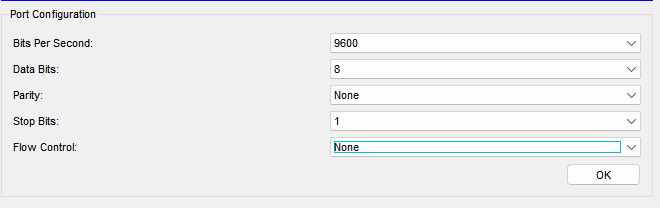


Je choisi un câble console (en bleu claire) car contrairement aux connexions SSH ou Telnet, qui nécessitent une connectivité réseau préalable, la connexion via un câble console permet d’accéder directement au routeur, même en cas de problème de configuration ou d’absence de connectivité. Il est utilisé pour connecter le pc portable au routeur que je connecte au port série (RS-232) et au port console du routeur :

Une image contenant Appareils électroniques, machine, capture d’écran, conception

Le contenu généré par l’IA peut être incorrect.

Ensuite, j’ouvre le terminal sur le PC portable et je configure les paramètres de connexion :



Puis je clique sur OK pour démarrer la session.

Une image contenant texte, capture d’écran, Police, conception

Le contenu généré par l’IA peut être incorrect.

Je tape le mot de passe « cisco » et me voici connectée sur l’interface du routeur R1

### Connection aux switchs :

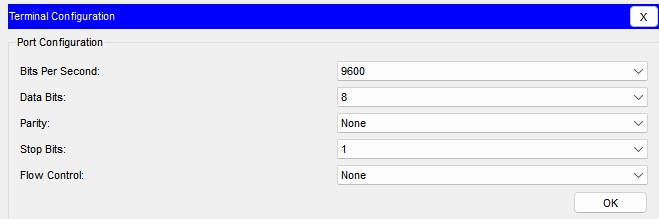
Pour aller sur les switches, il suffit de déplacer le câble console sur le port console du switch sauf que le port n’est pas visible, je vais donc regarder derrière lui.

Une image contenant texte, Police, capture d’écran

Le contenu généré par l’IA peut être incorrect.

Une image contenant capture d’écran, Bleu électrique, Rectangle, conception

Le contenu généré par l’IA peut être incorrect.

En effet, il y a bien le port console, je branche donc mon câble. 

Je configure les paramètres de connexion du terminal pour accéder à un équipement réseau via le port série. Les paramètres choisis sont :

* Bits Per Second : 9600 → C’est la vitesse de transmission standard pour la plupart des équipements réseau.
* Data Bits : 8 → Nombre de bits de données par trame, valeur classique.
* Parity : None → Pas de contrôle de parité, évitant ainsi les vérifications supplémentaires.
* Stop Bits : 1 → Indique la fin d’une trame de données, configuration standard.
* Flow Control : None → Désactive le contrôle de flux, évitant tout blocage du transfert de données.

Ils permettent d’interagir avec l’équipement en mode CLI (Command Line Interface).

Une image contenant texte, capture d’écran, Police, conception

Le contenu généré par l’IA peut être incorrect.

On me demande un mot de passe, je rentre cisco et me connecte sur l’interface du switch.

Ensuite je fais exactement les mêmes étapes pour connecter le switch 2.

| De | Pour | Résultats de la commande Ping |
| --- | --- | --- |
| R1 | S1 VLAN 3 (10.3.0.11) | Le ping vers 10.3.0.11 a échoué, avec un taux de réussite de 0% (0/5). Cela signifie que les paquets ICMP envoyés n’ont reçu aucune réponse. |
| R1 | S2 VLAN 3 (10.3.0.12) | Le ping vers 10.3.0.12 a échoué, avec un taux de réussite de 0% (0/5). Cela signifie que les paquets ICMP envoyés n’ont reçu aucune réponse. |
| R1 | PC-A (10.4.0.50) | Le ping vers 10.4.0.50 a échoué, avec un taux de réussite de 0% (0/5). Cela signifie que les paquets ICMP envoyés n’ont reçu aucune réponse**.** |
| R1 | PC-B (10.13.0.50) | Le ping vers 10.13.0.50 a échoué, avec un taux de réussite de 0% (0/5). Cela signifie que les paquets ICMP envoyés n’ont reçu aucune réponse. |
| S1 | S2 VLAN 3 (10.3.0.12) | Le ping vers 10.3.0.12 a échoué, avec un taux de réussite de 0% (0/5). Cela signifie que les paquets ICMP envoyés n’ont reçu aucune réponse. |
| S1 | PC-A (10.4.0.50) | Le ping vers 10.4.0.50 a échoué, avecun taux de réussite de 0% (0/5). Cela signifie que les paquets ICMP envoyés n’ont reçu aucune réponse. |
| S1 | PC-B (10.13.0.50) | Le ping vers 10.13.0.50 a échoué, avec un taux de réussite de 0% (0/5). Cela signifie que les paquets ICMP envoyés n’ont reçu aucune réponse. |
| S2 | PC-A (10.4.0.50) | Le ping vers 10.4.0.50 a échoué, avec un taux de réussite de 0% (0/5). Cela signifie que les paquets ICMP envoyés n’ont reçu aucune réponse. |
| S2 | PC-B (10.13.0.50) | Le ping vers 10.13.0.50 a échoué, avec un taux de réussite de 0% (0/5). Cela signifie que les paquets ICMP envoyés n’ont reçu aucune réponse. |

## Autres vérifications :

VLAN natif incorrect :

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

J'exécute show interfaces trunk pour voir la configuration des liens *trunk* sur le switch S1. L’interface Fa0/1 est en mode trunk avec l’encapsulation *802.1Q*. Le VLAN natif est configuré sur VLAN 1. Les VLANs autorisés sont 4, 8 et 13. Le VLAN actif en spanning-tree est VLAN 4, ce qui peut indiquer que les autres VLANs ne sont pas correctement propagés.

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Le contenu généré par l’IA peut être incorrect.

La configuration des liens trunk est presque la même. Il y a une incohérence de VLAN natif entre les trunks de S1 et S2. S1 utilise VLAN 1 comme VLAN natif et S2 utilise VLAN 8 comme VLAN natif.



J’exécute la commande switchport trunk native vlan 8 sur l’interface Fa0/1 de S1 pour changer le VLAN natif de 1 à 8.

### VLANs autorisés incorrects sur les trunks :

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Le contenu généré par l’IA peut être incorrect.Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Sur S2, la commande show interfaces trunk montre que l’interface Fa0/1 est en trunk avec un VLAN natif 8, le CDP (Cisco Discovery Protocol) détecte une erreur de mismatch VLAN natif. Cela signifie que S1 utilise VLAN 1 comme natif alors que S2 utilise VLAN 8.



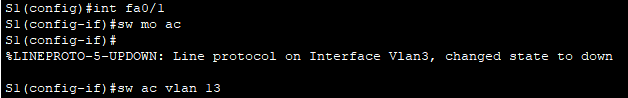
Je corrige la liste des VLANs autorisés sur le trunk de S1 et S2 en ajoutant VLAN 3. Cela assure que VLAN 3 est également propagé à travers le lien trunk.

### Mauvaise configuration sur fa0/5 :

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

J’exécute la commande show vlan brief pour afficher la configuration des VLANs sur S1. VLAN 3 (*Management*) est actif et configuré sur Fa0/5. VLAN 4 (*Operations*) est actif sur Fa0/6. VLAN 7 (*ParkingLot*) est actif sur plusieurs interfaces (Fa0/2, Fa0/3, Fa0/4, etc.). VLAN 8 (*Native*) est bien actif, ce qui correspond à une configuration précédente où on changeait le VLAN natif sur le trunk. Les VLANs 1002 à 1005 sont des VLANs par défaut.Il n'y a pas de VLAN 13, ce qui signifie qu’une interface attribuée à ce VLAN n’aura pas de connectivité.



Je modifie la configuration de l’interface Fa0/1 :

1. Je la mets en mode access (switchport mode access).
2. Le lien passe en état down → Cela signifie que l’interface était probablement en trunk avant cette modification.
3. J’attribue VLAN 13 à l’interface (switchport access vlan 13), mais VLAN 13 n'existe pas sur le switch, donc l’interface restera inactive.

### Mauvaise configuration du VLAN 13 :

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

J’affiche la table VLAN sur S1 avec show vlan brief. Je remarque que VLAN 13 n'existe pas sur ce switch. Seuls les VLANs 3, 4, 7 et 8 sont actifs.

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Je fais la même vérification sur S2 et cette fois, VLAN 13 est bien présent et actif. Cela signifie qu’il a été créé uniquement sur S2, mais pas sur S1, ce qui peut causer des problèmes de communication entre les équipements connectés aux deux switches.



Ici, j’ajoute VLAN 13 sur S2 et je le nomme Maintenance. Cela permet aux interfaces affectées à ce VLAN de fonctionner correctement sur S2, mais il manque encore sur S1.

## Interface trunk manquante sur R1 (routeur) :

Une image contenant texte, Police, capture d’écran, conception

Le contenu généré par l’IA peut être incorrect.

J’exécute show interface trunk sur R1, et il n’affiche rien. Cela signifie que R1 n’a aucune interface configurée en trunk, ce qui est problématique si je veux qu’il communique avec plusieurs VLANs via un switch.Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Je configure une sous-interface sur R1 avec dot1Q encapsulation. Cela définit VLAN 8 comme VLAN natif sur cette sous-interface.

## Changement de l’interface trunk de S1 :

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

S1 est sur le VLAN 1, qui n’est vraiment pas sécurisé. Je l’ai donc changé pour mettre le VLAN 8 à la place.

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Le contenu généré par l’IA peut être incorrect.

Sur S1, j’active le trunk sur l’interface FastEthernet0/5. Je configure VLAN 8 comme VLAN natif, ce qui correspond bien à la configuration de R1. J’autorise les VLANs 3, 4, 8 et 13 sur ce trunk.

## Mode trunk sur S1 :

Une image contenant texte, capture d’écran, Police

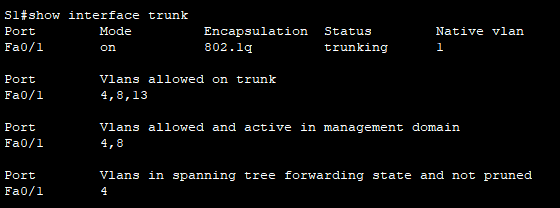
Le contenu généré par l’IA peut être incorrect.

L’interface fa0/5 n’est pas dans les ports trunk, il faut pourtant le mettre car fa0/5 relie deux équipements qui doivent transporter plusieurs VLANs.

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Le contenu généré par l’IA peut être incorrect.

Je passe l’interface fa0/5 en mode trunk grâce à la commande « switchport mode trunk ».



La configuration du trunk est incomplète et a une mauvaise affectation des ports aux VLANs. D’abord, les VLAN 8 et 13 n’étaient pas autorisés sur le port en mode trunk (FastEthernet0/1). De plus, le VLAN natif restait par défaut sur VLAN 1, alors qu’il devait être déplacé sur VLAN 8 pour correspondre à la configuration souhaitée. Enfin, certains ports d’accès n’étaient pas assignés au bon VLAN, empêchant les utilisateurs ou équipements de se connecter correctement au réseau.

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Le contenu généré par l’IA peut être incorrect.

Sur le switch S1, les interfaces FastEthernet0/1 et FastEthernet0/5 sont configurées en mode trunk, permettant le passage des VLANs 3, 4, 8 et 13. Le VLAN 8 est défini comme VLAN natif, garantissant que les trames non taguées transitent sur ce VLAN. Ensuite, l'interface Fa0/6 est configurée en mode accès et assignée au VLAN 4, ce qui signifie que tout appareil connecté à ce port sera directement intégré à ce VLAN. Une configuration groupée est ensuite appliquée à plusieurs interfaces via la commande interface range, incluant Fa0/2-4, Fa0/7-24 et GigabitEthernet0/1-2. Ces interfaces sont mises en mode accès et assignées au VLAN 7, mais elles sont immédiatement désactivées avec la commande shutdown, ce qui empêche toute communication sur ce VLAN. Pour corriger cela, il faudrait exécuter no shutdown sur ces interfaces si elles doivent être utilisées. Enfin, il est essentiel de vérifier la présence des VLANs 4 et 7 sur le switch avec show vlan brief, et de s’assurer que la configuration des trunks est bien synchronisée entre les switches avec show interfaces trunk.

## Vérifications :

| De | Pour | Résultats de la commande Ping |
| --- | --- | --- |
| R1 | S1 VLAN 3 (10.3.0.11) | Le ping vers 10.3.0.11 a réussi. |
| R1 | S2 VLAN 3 (10.3.0.12) | Le ping vers 10.3.0.12 a réussi. |
| R1 | PC-A (10.4.0.50) | Le ping vers 10.4.0.50 a réussi**.** |
| R1 | PC-B (10.13.0.50) | Le ping vers 10.13.0.50 a réussi. |
| S1 | S2 VLAN 3 (10.3.0.12) | Le ping vers 10.3.0.12 a réussi. |
| S1 | PC-A (10.4.0.50) | Le ping vers 10.4.0.50 a réussi. |
| S1 | PC-B (10.13.0.50) | Le ping vers 10.13.0.50 a réussi. |
| S2 | PC-A (10.4.0.50) | Le ping vers 10.4.0.50 a réussi. |
| S2 | PC-B (10.13.0.50) | Le ping vers 10.13.0.50 a réussi. |

Les pings ont été effectuer avec succès, les problèmes ont tous été résolus.

# Conclusion :

Ce TP sur la mise en place des VLANs a permis de comprendre et de maîtriser la segmentation d’un réseau en plusieurs sous-réseaux logiques afin d’améliorer la sécurité, la gestion et les performances globales du réseau. Grâce aux différentes étapes de configuration, nous avons pu observer comment les VLANs isolent les flux de communication tout en permettant un accès contrôlé aux ressources communes.

L’implémentation du trunking, l’attribution des ports et la gestion du routage inter-VLAN ont été des points clés pour assurer l’interconnexion des différents VLANs tout en respectant les règles de segmentation. De plus, les tests de connectivité ont mis en évidence l’importance d’une configuration rigoureuse, notamment en matière de gestion des VLANs natifs et des protocoles de routage.

Les différentes vérifications et résolutions de problèmes ont permis de renforcer la compréhension des erreurs possibles et des solutions à apporter, notamment en matière de configuration des trunks, des interfaces et des adresses IP.

En conclusion, ce TP a offert une approche pratique et concrète du fonctionnement des VLANs, démontrant leur utilité dans la structuration et la sécurisation des réseaux d’entreprise. La mise en œuvre réussie de cette segmentation renforce la résilience du réseau face aux menaces et facilite sa gestion et son évolution future.

# Sources :

<https://www.cisco.com/c/fr_ca/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb4986-vlan-configuration-via-cli-on-300-500-series-managed-switche.html>

<https://www.clemanet.com/switch-vlan-cisco.php>

<https://www.cisco.com/c/fr_ca/support/docs/lan-switching/private-vlans-pvlans-promiscuous-isolated-community/40781-194.html>