Installation, configuration et dépannage des réseaux

Dr. OTMANI Amina

Université Abu Bekr Belkaid TLEMCEN

Faculté de Technologie

Département Télécommunication

Email : *otmani1amina@gmail.com*

Table des matières

Introduction Générale

I

1. Fiche-Contact

Établissement :

- Université : Abou Baker Belkaïd Tlemcen
- Faculté : Technologie
- Département : Télécommunications

Unité d'Enseignement :

- Intitulé de Cours : Installation, Configuration et Dépannage des Réseaux
- Code : TOP941
- Crédit : 3
- Coefficient : 2

Horaire :

- Jour : Mercredi
- Heure : 11h30 - 13h00

Public Ciblé :

- Année : 2ème année Master
- Spécialité : Télécommunications
- Option : Optique

Durée :

- Total : 37 heures et 30 minutes

Enseignante :

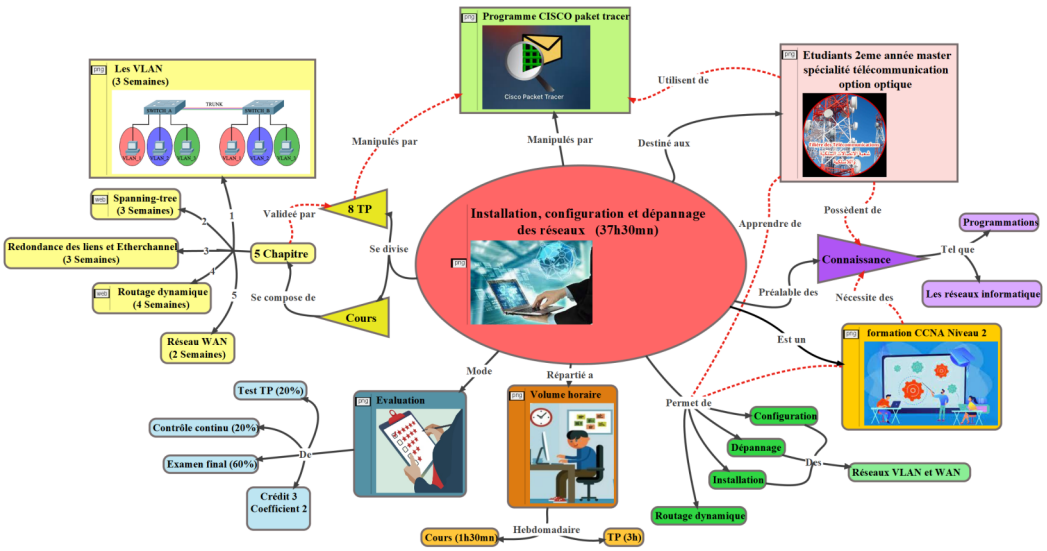
- Nom : Otmani Amina
- Contact par Mail : otmani1amina@gmail.com

Disponibilités :

- Lieu : Département des Télécommunications
- Jours : Dimanche, Mardi, Mercredi
- Heure : 11h30 - 13h00

2. Présentation du Cous

Bienvenue dans ce cours universitaire hybride sur les technologies avancées de mise en réseau. Ce cours est conçu pour vous offrir une compréhension complète des concepts essentiels et des pratiques modernes dans le domaine des réseaux informatiques. À travers ce parcours, vous développerez des compétences clés qui vous permettront de concevoir, configurer et optimiser des réseaux complexes.



Carte conceptuelle du cours TOP941

3. Objectifs du Cours

Ce cours vise à atteindre les objectifs suivants :

- **Décrire** les concepts fondamentaux des VLAN, du Spanning Tree Protocol (STP), de la redondance des liens, d'EtherChannel, du routage dynamique et des réseaux WAN.
- **Expliquer** comment chaque technologie contribue à l'optimisation et à la gestion efficace des réseaux.
- **Configurer** des VLAN, des protocoles STP, des solutions de redondance et d'EtherChannel, ainsi que de protocoles de routage dynamique sur des équipements réseau.
- **Analyser** les configurations réseau pour identifier les problèmes, les inefficacités et les opportunités d'amélioration.
- **Intégrer** les technologies étudiées dans des architectures réseau cohérentes pour répondre à des besoins particuliers en matière de performance, de résilience et de sécurité.
- **Évaluer** l'efficacité des configurations et des solutions mises en place, en utilisant des critères de performance, de sécurité et de résilience

4. Pré-requis / Connaissances préalables nécessaires

Pour suivre ce cours avec succès, il est essentiel d'avoir une compréhension solide des concepts de base des réseaux. Les apprenants doivent avoir assimilé les concepts fondamentaux et posséder les connaissances suivantes :

- Connaissances de Base en Réseautique (Modèles OSI et TCP/IP,des Adresses IP et MAC).

- Connaissances en Commutation (Fonctionnement, Connaissance des Hub et Switch).
- Configuration Réseau de Base.

5. Exercice : Test des pré-requis

Si vous avez rencontré des difficultés avec les questions de prérequis, nous vous encourageons à consulter la chaîne YouTube suivante pour réviser les concepts abordés : *Formip - Certification IT*

Exercice : 1

Quel est le rôle de la couche 3 du modèle OSI ?

- ○ Gérer les connexions physiques
- ○ Assurer la transmission de données entre les applications
- ○ Fournir les adresses logiques et acheminer les paquets
- ○ Contrôler l'accès au média de transmission

Exercice : 2

Qu'est-ce qu'une adresse IP et quel est son rôle dans un réseau?

- ○ Un identifiant unique pour chaque appareil sur un réseau.
- ○ Une adresse physique des appareils.
- ○ Une méthode de transfert de données sur le réseau.
- ○ Une technologie sans fil.

Exercice : 3

Quelle est la fonction principale d'une adresse MAC?

- ○ Identifier logiquement les appareils sur le réseau.
- ○ Faciliter le routage des paquets.
- ○ Assurer la livraison des paquets au bon appareil au niveau de la couche de liaison de données.
- ○ Gérer les sessions de communication entre les appareils.

Exercice : 4

- Un envoie les données uniquement au port du périphérique cible, ce qui améliore l'efficacité et la sécurité du réseau.
- Un diffuse les données à tous les ports, ce qui peut provoquer des collisions et une utilisation inefficace de la bande passante.

  Un connecte différents réseaux et gère le routage des paquets entre eux.

  Un connecte des appareils au sein d'un même réseau et gère la communication entre eux en utilisant des adresses MAC.

Exercice : 5

Qu'est-ce qu'un protocole de commutation ?

- O Un protocole utilisé pour la gestion des adresses IP
- O Un protocole permettant la communication entre différents réseaux
- O Un protocole gérant la transmission de données dans un réseau local
- O Un protocole de sécurité pour les réseaux sans fil

Exercice : 6

Quel est le problème potentiel lorsque plusieurs chemins sont actifs simultanément dans un réseau Ethernet ?

- O Collisions de données
- O Pertes de paquets
- O Boucles de commutation
- O Congestion du réseau

Exercice : 7

Quelle commande est utilisée pour configurer une adresse IP sur une interface d'un routeur Cisco ?

- O ip address
- O interface
- O config ip

Virtual Local Area Network

II

1. Objectifs

Le chapitre I vise à :

- **Définir** les concepts clés associés aux VLANs et leurs objectifs.
- **Expliquer** les étapes de configuration des VLANs sur des équipements réseau.
- **Comprendre** le concept de trunking et son rôle dans le transport de multiples VLANs.
- **Clarifier** le concept de VLAN Native et son importance.
- **Évaluer** les différentes approches de routage inter-VLAN.
- **Discuter** le fonctionnement du Virtual Trunking Protocol (VTP) et son utilisation pour la gestion des VLANs.

2. Des rappelles

2.1. Adresse MAC

Une adresseMAC* est également appelée adresse matérielle, adresse Ethernet ou adresse physique. C'est un identifiant unique et propre à la carte réseau de la machine. Elle est constituée de 48 bits (6 octets) et elle est généralement représentée sous la forme hexadécimale. Par exemple 5E:FF:56:A2:AF:15. [1]*

2.2. Adresse IP

Une adresseIP* (Internet Protocol) est un numéro d'identification unique attribué de façon permanente ou provisoire à chaque périphérique faisant partie d'un réseau.

Il existe deux grandes versions d'adresses IP : la version 4 (IPv4) codée sur 32 bits, et la version 6 (IPv6) codée sur 128 bits. La version 4 est actuellement la plus utilisée : elle est généralement représentée en notation décimale [2]*

2.3. Hub

Un hub, également connu sous le nom de concentrateur, est un appareil qui permet de connecter plusieurs appareils ensemble pour former un réseau. Il est souvent utilisé pour les petits réseaux domestiques et de petite entreprise. L'un des avantages d'un hub est qu'il est très facile à installer et à utiliser. Pour se connecter à un hub, il suffit de brancher un câble Ethernet dans un port disponible.

Le principe d'un hub est simple. Lorsqu'un appareil envoie des données à un hub, le hub transmet ces données à tous les autres appareils connectés. Cela signifie que tous les appareils connectés reçoivent une copie des données, même si elles ne sont pas destinées à eux. Cela peut entraîner des problèmes de congestion de réseau, en particulier si de nombreux appareils sont connectés à un hub.[3]*

Hub

2.4. Switch

Un switch, en revanche, est conçu pour résoudre ce problème de congestion de réseau.

Un commutateur (switch) conserve un registre des adresses MAC* (Media Access Control) de tous les appareils qui y sont connectés. Grâce à ces informations, un commutateur réseau peut identifier quel appareil se trouve sur chaque port. Ainsi, lorsqu'une trame est reçue, celui-ci sait exactement à quel port l'envoyer, sans augmenter les temps de réponse du réseau contrairement à un hub. Le rôle d'un switch est donc de gérer le trafic réseau de manière efficace.

Il est souvent utilisé dans les réseaux d'entreprise pour connecter plusieurs ordinateurs, serveurs et autres appareils réseau ensemble.[3]*

Switch

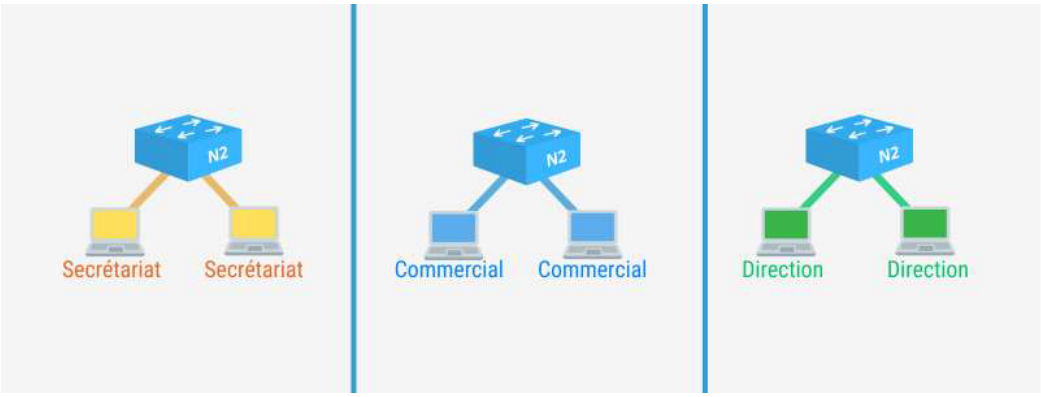
2.5. Requête ARP (Address Resolution Protocol)

Une requête ARP* est un message envoyé par un périphérique sur le réseau afin de trouver l'adresse MAC du destinataire. Elle est envoyée en broadcast afin que tous les équipements présents dans le réseau local reçoivent cette requête.

3. Problématique

Exemple : 01

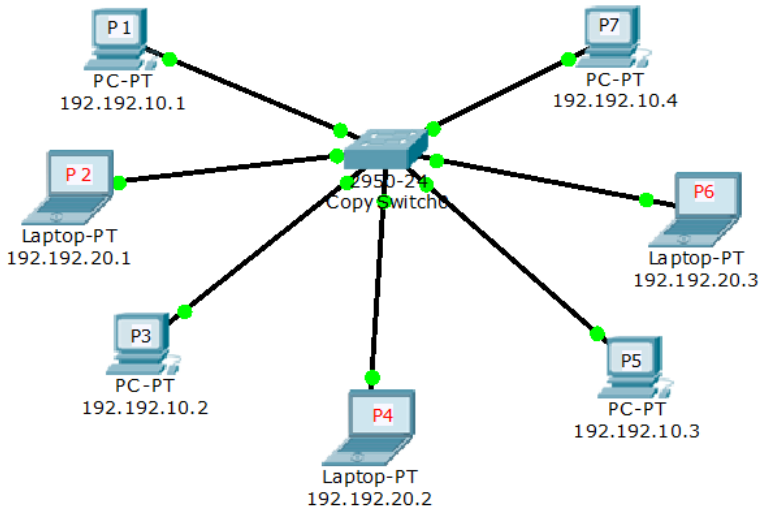
Imaginons une entreprise composée de trois départements : Secrétariat, Direction et Commercial. Dans un scénario traditionnel, pour isoler la communication de chaque groupe, l'administrateur aurait besoin de trois switchs distincts. Cette solution serait non seulement coûteuse, mais elle manquerait également de flexibilité.[4] *



une entreprise composée de trois départements

Exemple : 02

Nous prendrons ici en considération cette architecture : nous avons un switch, et des machines avec deux plages des adresses IP 192.192.10.0/24 (le réseau secrétaire) et 192.192.20.0/24 (le réseau patron).



Un réseau local

Avec les plages d'adressesIP*, nous avons segmenté notre réseau en deux mais si PC1 par exemple va envoyer un broadcast (broadcast de niveau 2 c'est FFFF), une requête ARP est transmise au switch. Ce dernier rediffuse cette requête à tous ses ports, ce qui signifie que la diffusion atteint tous les appareils connectés au switch, y compris PC2 qui n'est pas concerné par la requête car il n'appartient pas au même réseau.

Si le réseau compte 2000 machines et qu'il utilise des millions de plages d'adresses IP différentes, chaque machine recevra les diffusions de tous les autres périphériques, ce qui peut entraîner une utilisation inefficace de la bande passante.

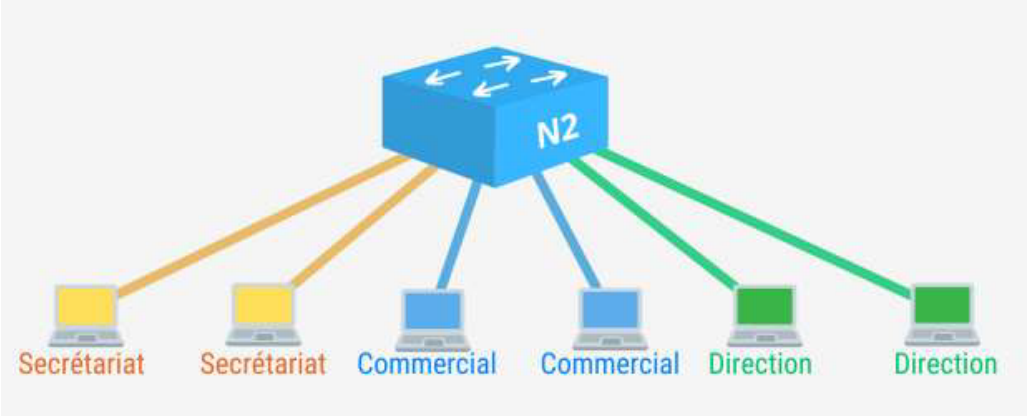
Méthode : les VLAN

C'est là qu'interviennent les VLAN*s (Virtual Local Area Networks). L'objectif principal des VLAN*s est de réduire le domaine de diffusion des broadcasts.

4. VLAN (Virtual Local Area)

Un VLAN* (Virtual Local Area Network ou Réseau Local Virtuel) est un réseau local regroupant un ensemble de machines de manière logique plutôt que physique. C'est une solution ingénieuse qui permet de subdiviser un réseau Ethernet physique en plusieurs sous-réseaux. Bien qu'ils utilisent la même infrastructure physique, ces sous-réseaux opèrent comme s'ils étaient complètement séparés.

Exemple : 01

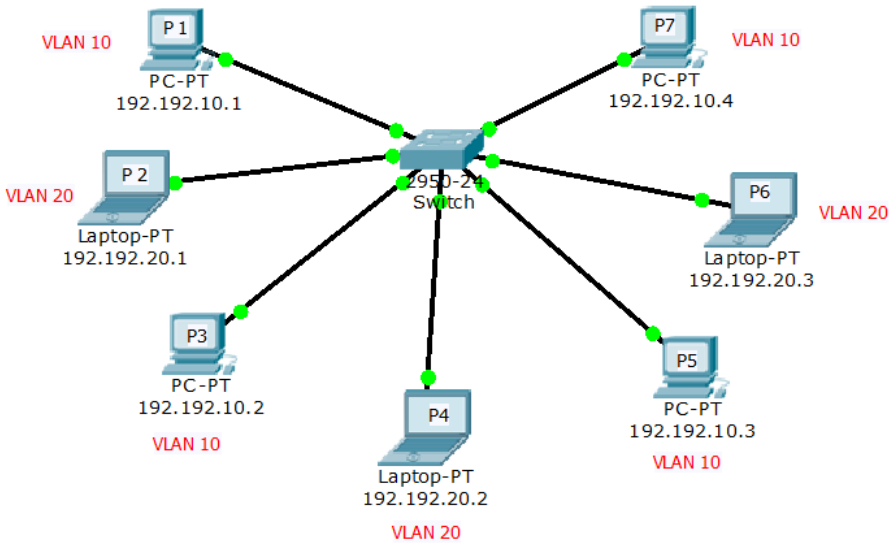


une entreprise composée de trois départements

Grâce à cette configuration, les membres de chaque groupe peuvent communiquer librement entre eux au sein de leur VLAN respectif. Ils restent cependant isolés des autres groupes, comme s'ils étaient connectés à des switches physiques séparés.[4]*

Exemple : 02

Le réseau est divisé sur deux réseaux virtuels VLAN 10 et VLAN 20. Lorsqu'une machine de VLAN 10 envoie un broadcast, la requête circulera uniquement dans ce réseau virtuel.



Le réseau divisé sur 2 VLAN

4.1. Les avantages

- Permet de déplacer les périphériques d'un VLAN à un autre sans avoir besoin de recâbler le réseau.
- Les VLANs aident les entreprises à surmonter les problèmes de congestion en réduisant le trafic de couche 2 (diminuer le domaine de broadcast).
- Renforce la sécurité en limitant l'accès aux périphériques autorisés dans un VLAN donné.
- Peut servir à isoler des groupes d'utilisateurs.

4.2. Table CAM

Un switch contient une table CAM* (Content-Addressable Memory) qui sert à faire la relation entre un port, une adresse Mac et la troisième colonne qui est du VLAN.

```
Switch# show mac-address-table
Mac Address Table
-------------------------------------------
Vlan Mac Address Type Ports
---- ----------- -------- -----
10 0002.1604.94c5 DYNAMIC Fa0/1
10 0050.0f58.58ca DYNAMIC Fa0/2
20 0006.2a77.6cb9 DYNAMIC Fa0/3
20 00d0.ff8c.2b36 DYNAMIC Fa0/4
30 0001.64ac.30ed DYNAMIC Fa0/5
30 0060.3e9b.26ae DYNAMIC Fa0/6
```

Table CAM

Chaque adresse MAC est en effet associée à un VLAN spécifique. Ainsi, pour que notre switch puisse acheminer efficacement une trame à son destinataire, il est crucial que l'expéditeur et le destinataire appartiennent au même VLAN. Cela garantit que la communication se fasse correctement au sein du groupe logique défini par le VLAN.[5]*

4.3. Identifiant VLAN (VLAN ID ou VLAN Taguing)

La numérotation VLAN est essentielle pour identifier et distinguer les différents VLANs au sein d'un réseau.

Chaque VLAN est identifié par un VLAN ID unique. Ce numéro est utilisé pour marquer le trafic Ethernet appartenant à un VLAN spécifique, surtout lorsqu'il traverse des liens qui transportent des informations pour plusieurs VLANs.

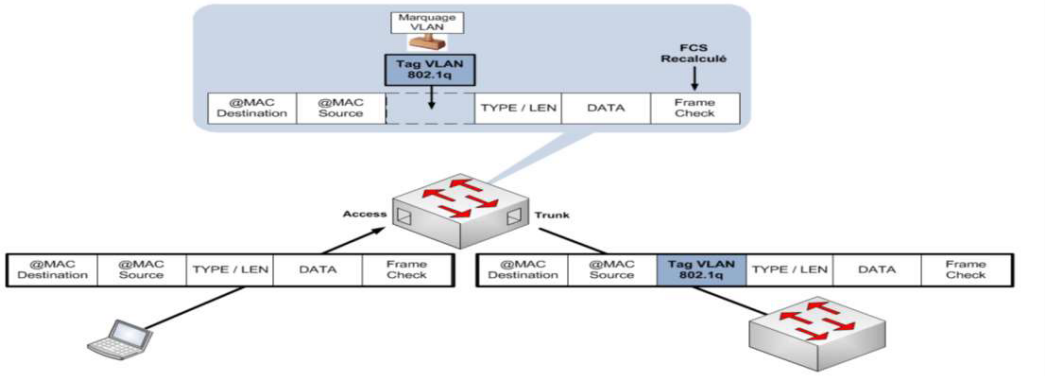
Lorsque VLAN Taguing est activé, un champ ID VLAN sera ajouté à la trame (dans l'état d'encapsulation de la trame) Ceci est possible en utilisant l'un des deux protocoles

4.3.1. Cisco ISL (Inter-Switch Link)

Il ajoute 30 octets (ancien protocole)

4.3.2. IEEE 802.1Q (dot1q)

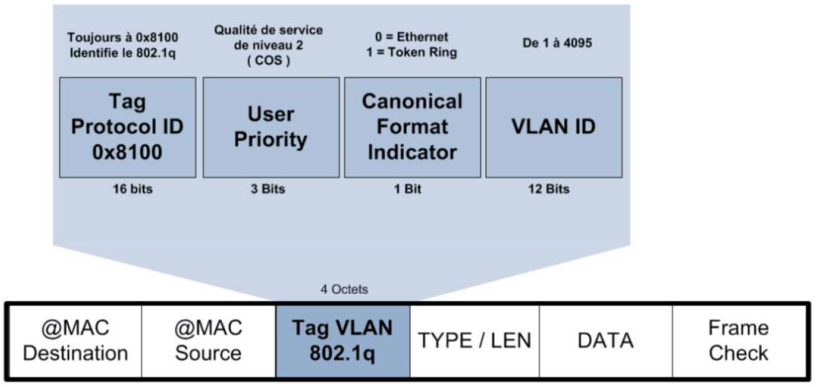
Ce protocole va ajouter un Tag 802.1Q juste après les adresses MAC destination et source de nos trames (4 octets).



Tag 802.1Q

Donc le champ réservé pour les IDs VLAN de 12 bits

$$Tag\ VLAN = 12\ bits = 2^{12} = 4096\ VLAN$$



Tag 802.1Q

Il existe trois types de VLANs :

- VLAN : 0 et 4095 sont réservés et ne sont pas utilisés pour le trafic utilisateur. VLAN 0 est parfois utilisé pour indiquer l'absence de VLAN.
- VLAN standard : 1 à 1001, ils sont considérés comme des VLANs “normaux” et peuvent être utilisés pou n'importe quel type de trafic Ethernet (tout nouveau commutateur de l'usine est livré avec le numéro de VLAN par défaut égal à 1).
- VLANs réservés : 1002 à 1005 sont réservés aux anciens protocoles et ne doivent pas être utilisés pour le trafic utilisateur dans les réseaux modernes.
- VLANs étendus : 1006 à 4094 Bien que cette distinction soit plus pertinente pour les anciens commutateurs Cisco, de nombreux commutateurs modernes traitent tous les VLANs de la même manière, quelle que soit leur numérotation.

Le protocole IEEE 802.1q ajoute un tag sur chaque trame sauf sur les trames appartenant au VLAN natif, Si un port trunks utilisant ce protocole normalisé reçoit une trame non taguée, il en déduit que cette trame fait partie du VLAN natif.[6]*

4.4. Affecter un VLAN

Il existe plusieurs méthodes pour affecter un VLAN à un port ou à un dispositif sur un commutateur.

- **Affectation statique :** L'administrateur attribue manuellement un port à un VLAN. C'est la méthode la plus basique et la plus utilisée.
- **Affectation dynamique :** avec un serveur (comme RADIUS* (Remote Authentication Dial-In User Service)).
- **Affectation basée sur le protocole :** avec un protocole (comme IP* ouIPX)*.
- **Affectation par Voix :** Pour les téléphones IP. Certains commutateurs séparent automatiquement le trafic vocal dans un VLAN dédié pour assurer une bonne qualité des appels.

L'affectation des VLANs est une composante fondamentale de la gestion d'un réseau commuté. Choisir la bonne méthode d'affectation dépend des besoins et de la taille du réseau, ainsi que des exigences de sécurité et de gestion.

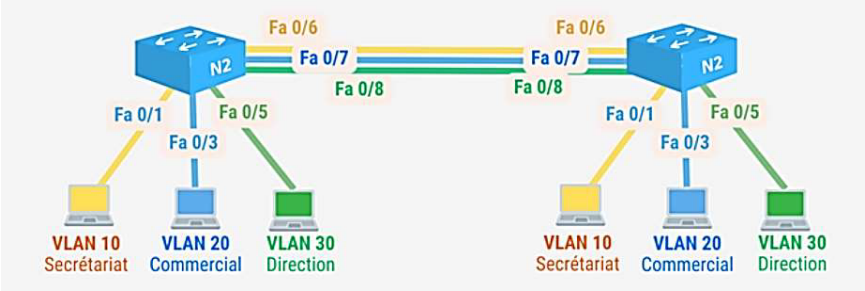
4.5. Compréhension du VLAN par les machines

Les PC ou autres dispositifs finaux (comme les imprimantes ou les serveurs) ne sont généralement pas au courant de leur appartenance à un VLAN. Pour eux, ils sont simplement connectés à un réseau. Le VLAN est transparent pour ces dispositifs et représente principalement une abstraction au niveau du switch, utilisée pour organiser et contrôler le trafic réseau.

5. Les liens Trunk (802.1q)

Pour établir les communications suivantes :

- Le VLAN 10 du S1 puisse discuter avec le VLAN 10 du S2.
- Le VLAN 20 du S1 puisse discuter avec le VLAN 20 du S2.
- Le VLAN 30 du S1 puisse discuter avec le VLAN 30 du S2.



Communications sans liaison TRUNK

Sans liaison TRUNK, il est impératif de suivre ces étapes :

- Créer un lien inter-switch pour le VLAN 10
- Créer un lien inter-switch pour le VLAN 20
- Créer un lien inter-switch pour le VLAN 30

Pour configurer un switch (Switch 1) afin de permettre la communication entre VLANs spécifiques sans utiliser de liaison TRUNK, voici les étapes générales

```
SWITCH_01(config)# interface FastEthernet 0/6
SWITCH_01(config-if)# description VERS_SWITCH_02_VLAN_10
SWITCH_01(config-if)# switchport mode access
SWITCH_01(config-if)# switchport access vlan 10
SWITCH_01(config)# interface FastEthernet 0/7
SWITCH_01(config-if)# description VERS_SWITCH_02_VLAN_20
SWITCH_01(config-if)# switchport mode access
SWITCH_01(config-if)# switchport access vlan 20
SWITCH_01(config)# interface FastEthernet 0/8
SWITCH_01(config-if)# description VERS_SWITCH_02_VLAN_30
SWITCH_01(config-if)# switchport mode access
SWITCH_01(config-if)# switchport access vlan 30
```

Configuration Switch 1

La configuration dans switch 2

```
SWITCH_02(config)# interface FastEthernet 0/6
SWITCH_02(config-if)# description VERS_SWITCH_01_VLAN_10
SWITCH_02(config-if)# switchport mode access
SWITCH_02(config-if)# switchport access vlan 10
SWITCH_02(config)# interface FastEthernet 0/7
SWITCH_02(config-if)# description VERS_SWITCH_01_VLAN_20
SWITCH_02(config-if)# switchport mode access
SWITCH_02(config-if)# switchport access vlan 20
SWITCH_02(config)# interface FastEthernet 0/8
SWITCH_02(config-if)# description VERS_SWITCH_01_VLAN_30
SWITCH_02(config-if)# switchport mode access
SWITCH_02(config-if)# switchport access vlan 30
```

Configuration Switch 2

Remarque

Si vous avez 1000 VLANs, cela signifierait qu'il vous faudrait 1000 liaisons inter-switch, ce qui n'est pas pratique du tout ! Heureusement, la solution est simple : il suffit de mettre en place une liaison TRUNK ! Les liaisons trunk, aussi appelées liens trunk, sont utilisées dans les réseaux commutés pour permettre le transit du trafic de plusieurs VLANs à travers un seul lien physique. Les trunks sont essentiels pour maintenir la séparation des données entre les VLANs tout en facilitant la communication entre eux via des routeurs ou des commutateurs de niveau 3.

Communications avec liaison TRUNK

Dans un monde où les liaisons TRUNK existent, il est possible de mettre en place une seule liaison inter-switch. Lorsqu'un commutateur reçoit une trame d'une machine, il lui attribue l'ID VLAN correspondant et la transmet sur le réseau. Lorsque le deuxième commutateur la reçoit, il vérifie l'ID VLAN et la transmet uniquement aux machines associées au même VLAN.[7]*

6. VLAN natif

La notion de VLAN natif n'intervient que lorsque l'on configure un port “Trunk”. Quand un port est configuré en tant que port Trunk, le commutateur insère une “étiquette” dans l'en-tête de la trame avec le numéro de VLAN approprié.

Toutes les trames passant par un “Trunk” sont ainsi étiquetées sauf les trames appartenant au VLAN natif. Donc, les trames du VLAN natif, par défaut le VLAN 1, ne sont pas étiquetées.

Le VLAN natif par défaut est le VLAN 1 on peut le changé par la configuration. Mais pourquoi l'IEEE a-t-il créé le VLAN natif ?

Il y a fort longtemps, l'utilisation d'un hub était courante. Ils pouvaient être placés sur une liaison trunk. Les utilisateurs finals connectés sur ces hubs recevaient des trames 802.1q et ne les comprenez pas...

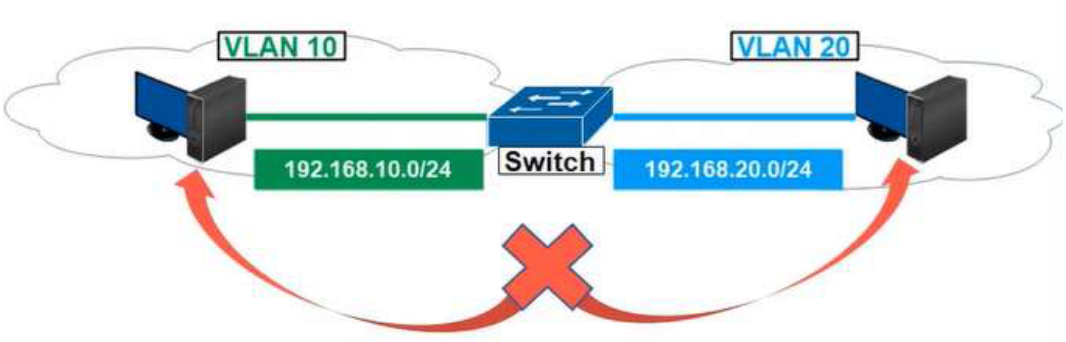
S'ils font partie du VLAN natif, la trame n'est pas taguée et devient compréhensible par les utilisateurs finals.

Depuis la sortie de Windows XP, les utilisateurs finals comprennent les trames 802.1q sans tenir compte du marquage VLAN. Le VLAN natif reste important vu que les trames non taguées reçues par un port trunk 802.1 q vont être placé dans le VLAN natif.

Ce type de VLAN existe pour assurer une inter-opérabilté avec du trafic ne supportant pas l'étiquetage. On recommandera de changer le numéro du VLAN natif.[8]*

7. Routage inter VLAN

Chaque VLAN constitue un domaine de broadcast distinct. Par défaut, les machines sur des VLANs séparés ne peuvent pas communiquer entre eux. Pour permettre la communication entre VLANs, il est nécessaire de mettre en place du routage inter-VLAN, effectué par un périphérique de couche 3 tel qu'un routeur. Il est important de noter que le switch est un périphérique de couche 2.

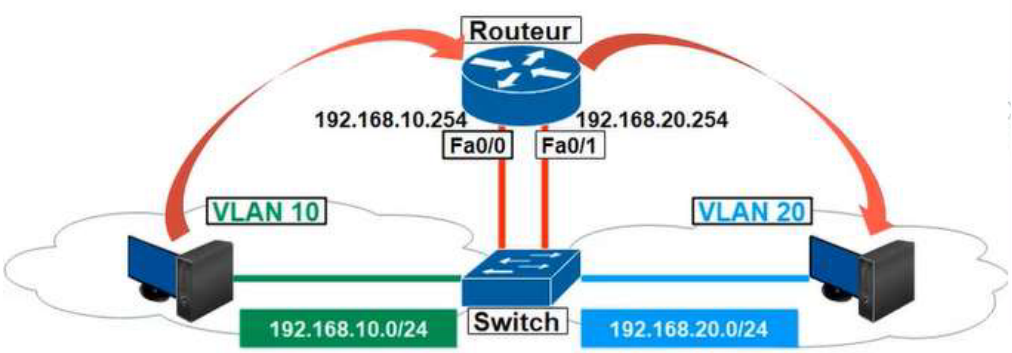


Réseau local avec périphérique de couche 2

Il y'a 3 manières différentes pour faire du routage inter-vlan.

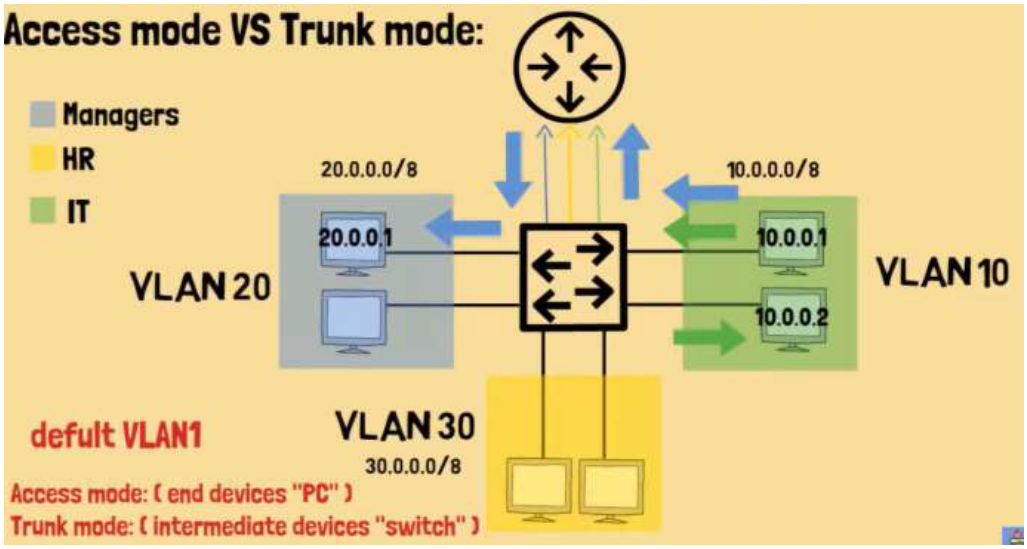
7.1. Routage inter-vlan traditionnel

Pour réaliser du routage inter-VLAN, on utilise un routeur doté d'interfaces distinctes pour chaque VLAN. Cette méthode traditionnelle de routage inter-VLAN requiert plusieurs interfaces physiques du côté du routeur et du côté du switch. Chaque VLAN est associé à un sous-réseau IP unique au sein du réseau. Cette configuration de sous-réseau simplifie le processus de routage dans un environnement multi-VLAN. Lorsque l'on utilise un routeur pour effectuer le routage entre les VLANs, les interfaces du routeur doivent être connectées à des VLANs distincts. Par exemple, les PC du VLAN 10 envoient leur trafic via le routeur pour atteindre le VLAN 20.



Routage inter-vlan traditionnel

Un inconvénient majeur de cette approche est qu'elle nécessite l'utilisation d'une interface distincte du routeur pour chaque VLAN. Plus le nombre de VLANs augmente, plus cela implique de bloquer des interfaces sur le routeur. À terme, cela peut conduire à une pénurie d'interfaces disponibles sur le routeur, rendant cette solution peu évolutive.



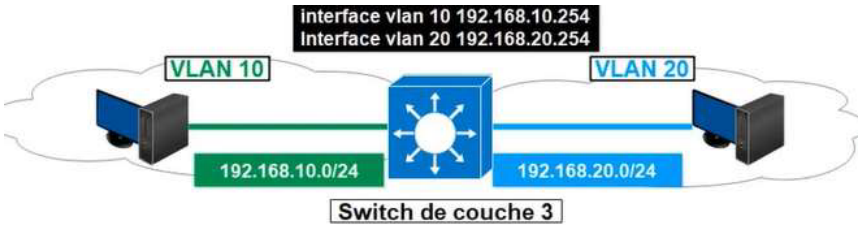
Echange des données dans un réseau a routage inter-vlan traditionnel

7.2. Switch de couche 3 (Switch Virtual Interface (SVI))

Certains switchs peuvent effectuer des fonctions de couche 3, ce qui permet de remplacer le routeur. Les switchs de couche 3 sont capables d'effectuer le routage inter-VLAN.

Traditionnellement, un switch examine l'entête de la couche 2 pour acheminer les paquets et le routeur examine la couche 3. Un switch de couche 3 combine la fonctionnalité d'un switch et d'un routeur dans un seul et même appareil.

Il commute le trafic lorsque la source et la destination sont dans le même VLAN, et achemine le trafic lorsqu'il est dans des VLAN différents (c'est-à-dire sur différents sous-réseaux IP*).

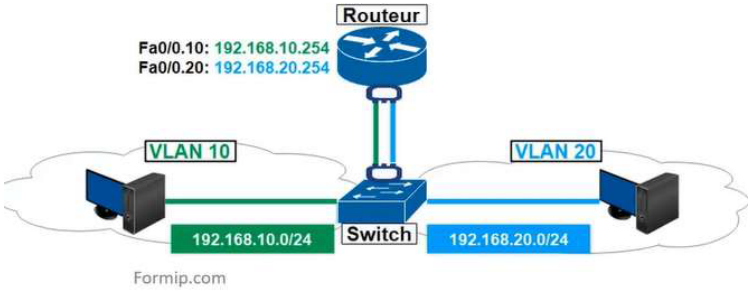


Réseau local avec périphérique de couche 3

Pour activer la fonction de routage sur un switch de couche 3, il faut lui configurer les interfaces VLAN en utilisant les adresses IP correspondant au sous réseau auquel le vlan est associé (Il est tout à fait possible de configurer des routes statiques, mais les protocoles de routage dynamique ne seront pas pris en charge).

7.3. le Router On a Stick (ROAS)

Certains logiciels de routeurs permettent de configurer plusieurs interfaces sur un seul et même lien Trunk (ce seront alors des sous-interfaces).



le Router On a Stick (ROAS)

La figure montre un routeur qui est attaché à un switch de couche 2. La configuration entre un routeur et un switch est appelée router on a stick.

C'est un type de configuration dans lequel une seule interface physique relie le trafic entre plusieurs VLAN sur un réseau.

Le routeur effectue le routage inter-VLAN à l'aide de ses sous-interfaces. Les sous-interfaces sont des interfaces virtuelles multiples associées à une interface physique. Pour effectuer les fonctions de routage inter-VLAN, le routeur doit savoir comment atteindre tous les VLAN interconnectés. Chaque vlan, dois avoir sa propre interface virtuelle.

Chacune de ses sous-interfaces est configurée indépendamment avec une adresse IP.

Les sous-interfaces sont configurées pour différents sous-réseaux correspondant à leur affectation VLAN (dans l'Exemple, Fa0/0.10 pour le vlan 10 et Fa0/0.20 pour le vlan 20).

Cela facilite la compréhension du routage logique par rapport au tag que recevra la trame pour être routée.[9]*

	3 Vlans	500 Vlans
Méthode Pré-historique	3 interfaces physique	500 interfaces physique
Méthode ROAS (Routeur)	1 interface physique 3 interfaces logique (subif)	1 interfaces physique 500 interfaces logique (subif)
Méthode SVI (Switch L3)	0 interface physique 3 interfaces logique (Vlan)	0 interface physique 500 interfaces logique (Vlan)

Comparaison des trois méthodes de routage

8. VLAN Voice

Dans les réseaux Ethernet basés sur IP, il est courant que les téléphones IP soient placés à côté des ordinateurs sur le même bureau.

Le Voice VLAN joue un rôle essentiel dans la transmission de haute qualité des données vocales. Un Voice VLAN est un VLAN spécifiquement dédié aux flux de données vocales des utilisateurs. Il garantit la qualité du trafic vocal en accordant une priorité de transmission élevée à ces flux lorsqu'ils sont transmis simultanément avec d'autres types de trafic comme les données ou la vidéo. Ainsi, même lorsque plusieurs services sont utilisés en même temps, le trafic vocal est priorisé pour assurer une transmission sans interruption.

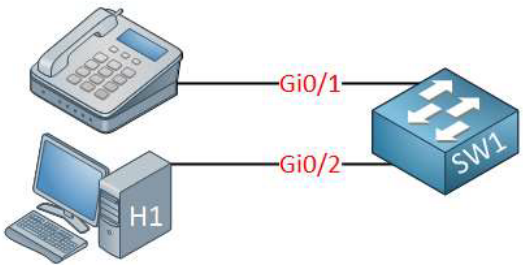
8.1. Application

Le voice Vlan est généralement utilisé dans les scénarios où il y a des téléphones IP, comme dans les grandes entreprises et les établissements financiers. Dans ces endroits, les bureaux sont largement distribués et le personnel est dispersé, ce qui augmente le besoin de téléphones IP pour maintenir une communication à plusieurs parties fréquentes.

Si nous voulons connecter les téléphone IP à un commutateur, nous avons deux options :

8.1.1. Connection direct

Vous pouvez connecter l'ordinateur et le téléphone IP à l'aide de deux câbles différents :



Connection direct

Cela fonctionnera mais cela présente quelques inconvénients :

- Vous devez installer un nouveau câble entre le switch et le téléphone IP.
- Vous perdrez un port de commutation pour le téléphone IP.

8.1.2. Voix et données utilisant un seul port

La majorité des téléphones VOIP* sont équipés de deux ports Ethernet : l'un destiné à faire face à la prise murale (par la suite au réseau local de l'entreprise c-à-d port de switch), l'autre destiné à faire face à un PC.

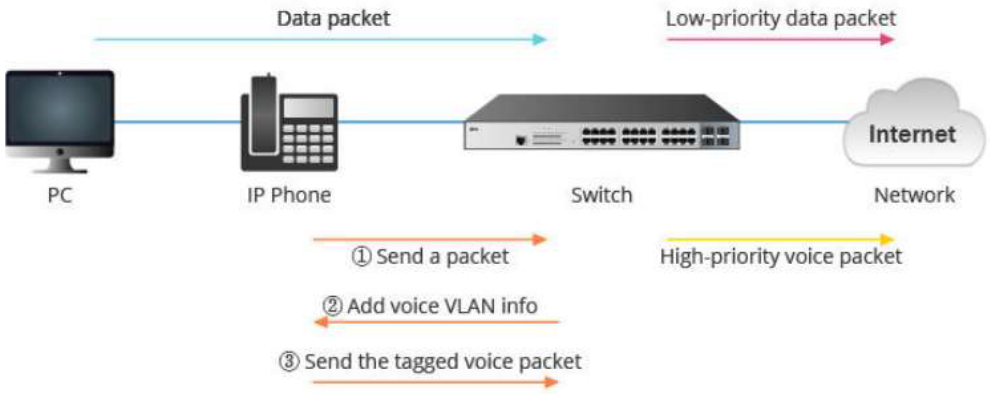
Téléphones VOIP

Grâce à ces deux ports, le PC peut être connecté au téléphone, et le téléphone peut ensuite être connecté au port de switch, Cela permet aux deux appareils de partager un seul port.

Pour expliquer le fonctionnement du Voice VLAN (VLAN Voix) et comment il permet la transmission simultanée de la voix et des données sur un seul port, voici les étapes clés :

- **Configuration du VLAN Voice :** Un VLAN Voice est configuré sur le commutateur réseau pour gérer le trafic VoIP (Voice over IP). Ce VLAN est dédié au transport des données vocales.
- **Tagging des trames :** Lorsqu'un téléphone IP envoie des données, le commutateur ajoute un tag VLAN à chaque type de trafic. Les données vocales sont marquées avec l'ID VLAN du VLAN Voice, tandis que les données informatiques sont marquées avec l'ID VLAN correspondant au VLAN de données.
- **Transport sur un seul port :** Les trames marquées avec différents VLANs sont transportées sur un seul port physique du commutateur, souvent configuré en mode TRUNK. Cela permet au téléphone IP de transmettre à la fois les données vocales et les données informatiques sur un même câble Ethernet vers le commutateur.
- **Gestion au niveau du commutateur :** À l'arrivée des trames sur le commutateur, ce dernier utilise les tags VLAN pour diriger chaque type de trafic vers les VLANs appropriés. Ainsi, les données vocales sont dirigées vers le VLAN Voice et les données informatiques vers le VLAN de données, bien que ces deux flux passent par le même port physique du téléphone IP.

En mode VLAN, un commutateur réseau détermine si le paquet de données est un paquet vocal en fonction de l'ID VLAN du paquet entrant dans l'interface. Comme le montre l'image suivante :



Échange de Paquets : Données et Voix

- Le téléphone IP envoie initialement des paquets de données à un commutateur réseau.
- Le commutateur reçoit ces paquets et ajoute les informations VLAN appropriées, notamment les tags VLAN pour les données vocales.
- Après avoir reçu les paquets contenant les tags VLAN pour les données vocales, le téléphone IP renvoie ces paquets vocaux avec les tags correspondants. Si le tag VLAN correspond au Voice VLAN configuré sur le commutateur, celui-ci traite le paquet en priorité.

De cette façon, le commutateur peut assurer la transmission prioritaire des paquets vocaux en cas de congestion du réseau.

8.2. Les avantages du voice Vlan

L'utilisation du voice Vlan présente trois avantages principaux.

- Il assure que les appareils VoIP* (Voice over IP) ne sont pas directement exposés à tout le trafic de diffusion et aux autres données du VLAN.
- Il garantit la qualité de service sur les réseaux IP, particulièrement lorsque plusieurs VLAN sont configurés et partagés sur des liaisons montantes utilisant 802.1Q sur un commutateur réseau.
- Le Voice VLAN peut être utilisé pour prioriser différents services vocaux, assurant ainsi une communication vocale fluide et fiable.

8.3. Configuration du Voice VLAN

Pour finaliser la configuration du Voice VLAN, voici les étapes à suivre :

- **Créer un VLAN :** Définissez un VLAN spécifique pour le trafic vocal.
- **Configurer les adresses OUI :** Configurez les adresses MAC OUI* (Organizational Unique Identifier) pour identifier les téléphones IP et autres périphériques VoIP. Cela permet au switch de reconnaître automatiquement les périphériques VoIP*.
- **Configurer le VLAN vocal globalement :** Activez le Voice VLAN sur l'ensemble du switch ou sur les interfaces pertinentes pour permettre la segmentation et la priorisation du trafic vocal.
- **Configurer le mode Voice VLAN sur les ports :** Sur les ports où sont connectés les téléphones IP, configurez le mode Voice VLAN pour que le switch identifie et traite correctement le trafic vocal, en lui attribuant le VLAN vocal approprié et en appliquant les règles de priorisation si nécessaire.[10]*

9. VTP (Vlan Trunk Protocol)

Imaginons que nous avons un réseau composé de 50 switches et que vous souhaitez créer un nouveau VLAN. Cela implique de configurer ce VLAN sur chacun des 50 équipements actifs pour l'ajouter à leur base de données VLAN (vlan.dat).

Méthode : VTP (VLAN Trunking Protocol)

Le protocole VTP* (VLAN Trunking Protocol) est un protocole de gestion des VLAN utilisé dans les réseaux informatiques. Son rôle principal est de propager les informations VLAN à tous les équipements du réseau, simplifiant ainsi la gestion des VLAN dans un environnement étendu.

Il permet aux administrateurs de configurer et de modifier les VLAN sur un seul commutateur, puis de diffuser ces informations à tous les autres commutateurs du réseau. Cela simplifie grandement la configuration des VLAN dans les réseaux de grande taille, permettant ainsi aux administrateurs de gagner du temps et de minimiser les erreurs de configuration.

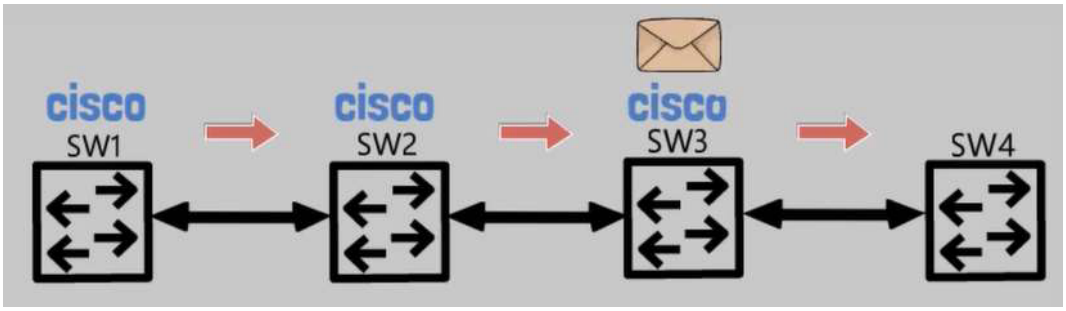
Pour que VTP fonctionne correctement, il y a trois conditions à respecter :

- Tous les commutateurs doivent être dans le même domaineVTP*.
- Toutes les liaisons entre les commutateurs doivent être configurées en mode trunk.
- Tous les commutateurs doivent exécuter la même version de VTP (1, 2, ou 3).

9.1. Un domaine VTP

Un domaine VTP est composé d'un ou plusieurs commutateurs partageant le même nom de domaine VTP et connectés entre eux par des liaisons Trunk. Le domaine de tous les commutateurs au début par défaut est nul, c'est-à-dire que chaque commutateur est isolé et n'appartient à aucun domaine VTP.

Lorsqu'un nom de domaine VTP est introduit dans un switch, ce dernier envoie une trame contenant ce nom à tous les switchs du même réseau qui portent le nom nul, puis ils le changent par le nouveau nom.

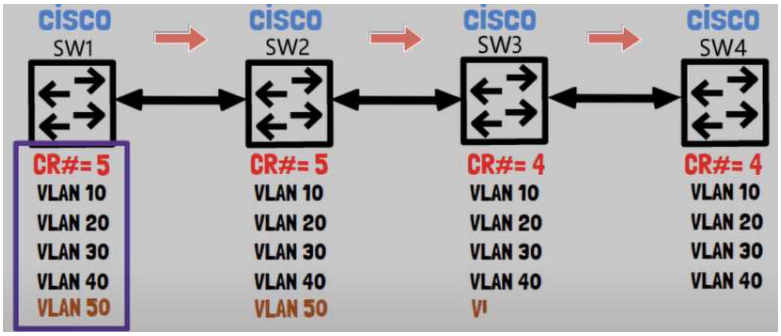


Un domaine VTP

9.2. Configuration Revision Number (CR ou RN)

A chaque création/suppression/modification de VLAN, une variable appelée RN* (Revision Number) s'incrémente (initialement 0 puis 1 puis 2 puis 3 et ainsi de suite). A chaque opération sur VLAN, le switch Server envoie un message VTP avec la nouvelle valeur du RN.

Les autres switchs compare le RN* reçu du switch Server avec le RN qu'ils stockent en local, si ce dernier est plus petit (logiquement) alors les switchs se synchronisent avec le Server et récupère la nouvelle base de données des VLANs.



la synchronisation de variables RN

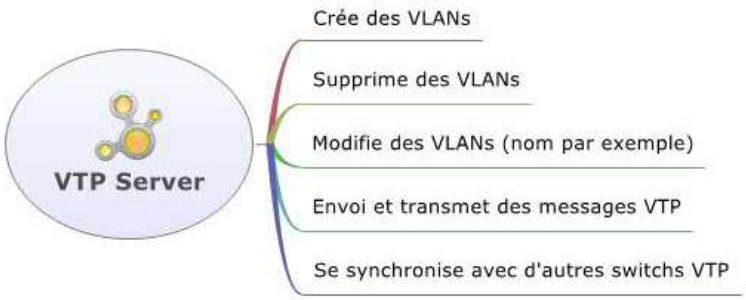
Par défaut, le RN* est envoyé automatiquement dès une création/suppression/modification de VLAN puis envoyé toutes les 5 minutes.

9.3. Architecture du VTP

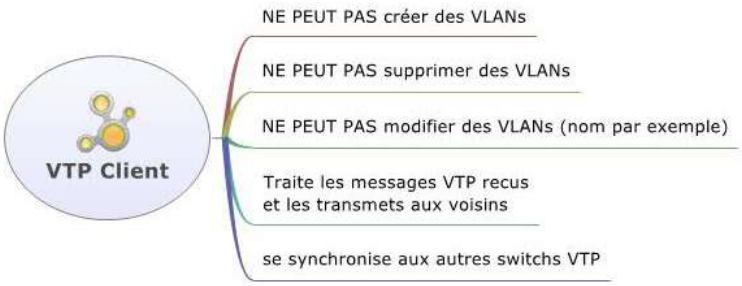
Au début tous les commutateurs sont en mode par défaut qui est serveur mais l'administrateur peut changer ce mode.

Le switch possède 3 modes VTP :

9.3.1. VTP Server :



a) VTP Client



9.3.2. VTP Transparent

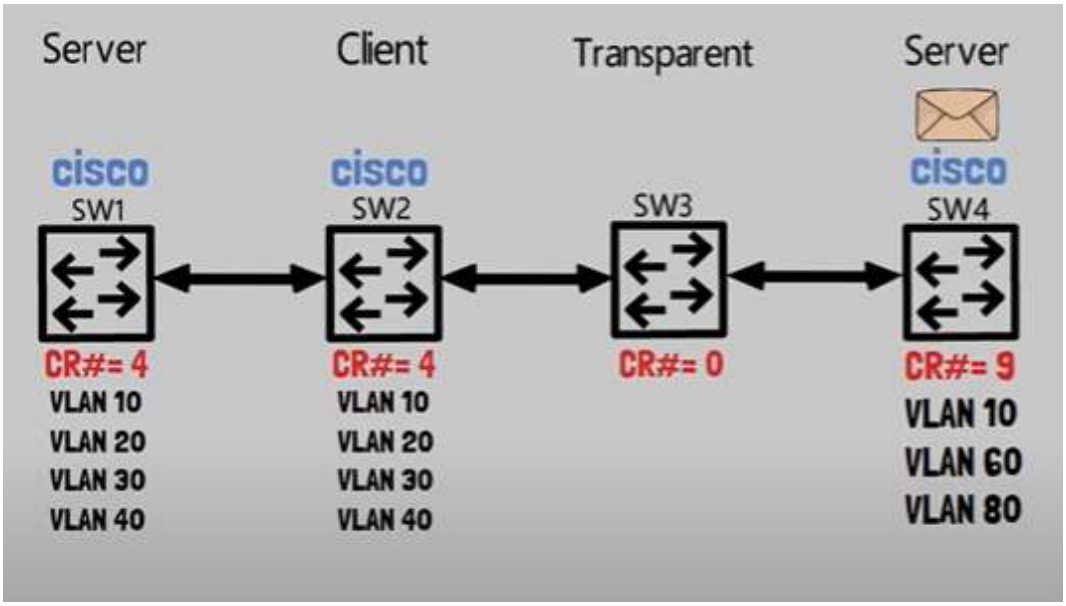
9.3.3. VTP OFF

Ignore complètement le VTP. Cela peut être utile dans des scénarios où le VTP n'est pas nécessaire ou s'il est désactivé pour des raisons de sécurité.

- Le switch ne propage pas les modifications de VLAN aux autres switches via VTP.
- Il ne reçoit pas les mises à jour de VLAN des autres switches via VTP.

Remarque

- Vous pouvez ajouter un mot de passe pour chaque domaine pour assurer une bonne sécurité.
- VTP ne gère que la plage de VLAN comprise entre 1 et 1005.
- Si un switch client possède un RN plus élevé que le switch Server (imaginons qu'il était dans un autre réseau puis branché au notre), contrairement à ce qu'on peut penser, le client ne va pas récupérer la base de données de VLAN du Server. Parce que quel que soit le mode du switch, Server ou Client, il se synchronise toujours sur celui qui a le RN le plus élevé. Dans notre cas, c'est le Server qui va se synchroniser et récupérer la base de données de VLAN du Client. Il est donc très important de remettre le RN à zéro. Pour cela, effectuer un simple basculement en mode Transparent puis en mode Client (exemple plus bas)



la synchronisation par VTP

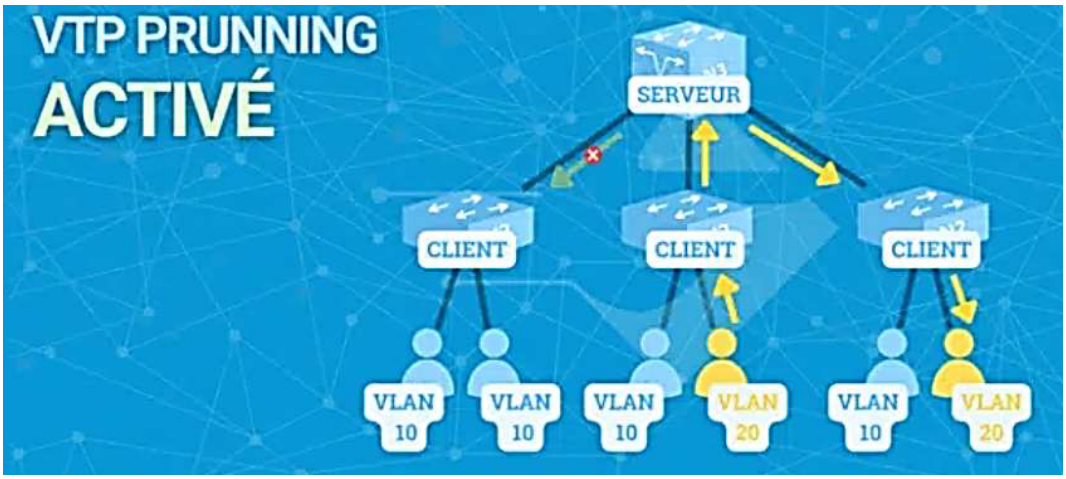
- Les messages VTP contiennent non seulement l'ID des VLANs mais aussi leur nom.
- Les messages VTP contiennent la liste des VLANs mais pas les ports associés à chaque VLAN.[11*,12]*

9.4. Le VTP pruning

Le VTP pruning est une commande facultative qui permet de rationaliser l'utilisation de la bande passante.

Lorsqu'un switch reçoit un message concernant un VLAN donné (par exemple VLAN 20) mais aucune de ses interfaces n'appartient à ce VLAN, il est inefficace que le switch voisin continue à lui envoyer du trafic pour ce VLAN.

En activant la fonction VTP pruning à partir du switch Server, on informe le switch voisin de ne pas lui envoyer de trafic pour ce VLAN, réduisant ainsi la consommation inutile de bande passante.[12]*



Le VTP pruning activé

10. Conclusion

Base de comparaison	Réseau local	VLAN
Acronyme	LAN - Réseau local	VLAN - Réseau Local Virtuel
Appareils couramment Utilisés	Hub, répéteurs, commutateurs, points d'accès sans fil, imprimantes et routeurs.	Commutateurs et ponts.
Contrôle de diffusion	Chaque appareil du réseau local reçoit une diffusion de la trame.	Seuls les appareils spécifiques de ce VLAN (domaine de diffusion) particulier reçoivent la diffusion de la trame.
Latence	La latence du LAN est généralement élevée par rapport au VLAN.	La latence du VLAN est généralement inférieure à celle du LAN.
Sécurité	Le LAN n'est pas suffisamment sécurisé et les mesures de sécurité ne sont mises en oeuvre qu'au niveau du routeur.	L'utilisation de VLAN augmente la sécurité en limitant les trames au domaine de diffusion spécifique.
Efficacité, flexibilité et Évolutivité	LAN filtre uniquement les trames et est moins évolutif que VLAN.	Plus flexible et évolutif, le VLAN spécifie le port et les protocoles utilisés pour identifier une trame.
Coût	Coût élevé car davantage d'appareils sont nécessaires pour séparer les utilisateurs.	Moins coûteux, un commutateur peut être virtuellement divisé en plusieurs VLAN.
Domaine de Défaillance	Si un commutateur desservant un groupe d'utilisateurs tombe en panne, ils ne peuvent pas être facilement transférés vers un autre commutateur. Cela rend le LAN moins efficace que le VLAN.	Si un commutateur desservant un groupe d'utilisateurs tombe en panne, celui-ci peut être déplacé vers un autre commutateur avec peu de configuration. Surclasse un réseau local en termes de performances et d'efficacité.
Composé de	Un LAN peut être composé de plusieurs VLAN.	Un VLAN peut s'étendre sur plusieurs LAN si nécessaire.
Physique vs Virtuel	Le réseau local est physique.	Un VLAN est virtuel

Comparaison des Réseaux Locaux avec et sans VLAN

Abréviations

ARP : Address Resolution Protocol

IP : Internet Protocol

IPX : Internetwork Packet Exchange

MAC : Media Access Control

OUI : Organizational Unique Identifier

RADIUS : Remote Authentication Dial-In User Service

RN : Revision Number

table CAM : table Content-Addressable Memory

VLAN : Virtual Local Area Network

VoIP : Voice over IP

VTP : VLAN Trunking Protocol

Bibliographie

N.Nicolas, et E.Jouffillon. "Adresse MAC _ tout ce que vous devez savoir ." FingerInTheNet. Electronically published April 1, 2023. https://www.fingerinthenet.com/adresse-mac/.

Howard." Voice VLAN Configuration Guidelines on Ethernet Switches. FS Community",29 September 2021, from https://community.fs.com/article/voice-vlan-configuration-guidelines-on-ethernet-switches.html

A. Afroz. "VLAN Trunking Protocol (VTP) - What is VTP in Networking?".Afroz Ahmad. 5 MARCH 2024. https://afrozahmad.com/blog/vlan-trunking-protocol-what-is-vtp-in-networking/

N.Nicolas, et E.Jouffillon. "VTP (VLAN Trunking Protocol) Configuration Guide". FingerInTheNet. https://www.fingerinthenet.com/vtp/

M.QARA "Le protocole STP [Français] - Introduction" Mohamed QARA. 15 août 2020. https://www.youtube.com/watch?v=G-jD5-kT8eE&t=1s

CCNA Réponses. "Notions de base sur la commutation, le routage et sans fil : modules 5 concepts du STP",8 April 2023 from https://ccnareponses.com/notions-de-base-sur-la-commutation-le-routage-et-sans-fil-modules-5-concepts-du-stp/

M.QARA "02 - Le protocole STP [Français] - Le pont racine" Mohamed QARA.15 août 2020. https://www.youtube.com/watch?v=WQXqaA_Nx1I&t=26s

M.QARA "03 - Le protocole STP [Français] - Les ports racines" Mohamed QARA.15 août 2020. https://www.youtube.com/watch?v=W3KMSBeyHew&list=TLPQMjgwNjIwMjRJv7v3JTyHdQ&index=2

M.QARA "04 - Le protocole STP [Français] - Les ports désignés et les ports non désignés" Mohamed QARA. 15 août 2020. https://www.youtube.com/watch?v=9q5-2Eao92g&list=TLPQMjgwNjIwMjRJv7v3JTyHdQ&index=3

M.Alaa "27. CCNA 200-301 (Port Fast & BPDU Guard) "mohab alaa. 16 sept 2021. https://www.youtube.com/watch?v=G6BldPwBGYk

M.Alaa "25. CCNA 200-301 (Rapid Spanning Tree protocol (RSTP)) "mohab alaa. 14 sept 2021. https://www.youtube.com/watch?v=aYIiq1JvZ2g

Cloudflare. "Qu'est-ce qu'un protocole Internet (IP) ?" Cloudflare. https://www.cloudflare.com/fr-fr/learning/network-layer/internet-protocol/.

Irving. "Do you know the differences between hubs, switches, and routers?" FS Community. Updated December 17, 2021. https://community.fs.com/article/do-you-know-the-differences-between-hubs-switches-and-routers.html.

Noel Nicolas "VLAN _ Maîtrisez les bases en 5 minutes" FingerInTheNet. 24 mars 2018 https://www.fingerinthenet.com/vlan/

Nicolas, Noël, et Eric Jouffillon. "Les liens Trunk : Présentation et configuration" FingerInTheNet. https://www.fingerinthenet.com/trunk/

FingerInTheNet. "Présentation des liens TRUNK" https://www.fingerinthenet.com/topics/presentation-des-liens-trunk/

Cisco. "VLAN Best Practices and Security Tips for Cisco Business Routers." 27 janvier 2020. https://www.cisco.com/c/fr_ca/support/docs/smb/routers/cisco-rv-series-small-business-routers/1778-tz-VLAN-Best-Practices-and-Security-Tips-for-Cisco-Business-Routers.html

SO, Damien. "Inter-VLAN Routing: Definition, Benefits, and Configuration." FormIP. Accessed June 28, 2024. https://formip.com/inter-vlan/

Webographie

"Comment fonctionne un SWITCH - La Table CAM"Finger In The Net. déc. 2019 https://www.youtube.com /watch?v=SiOkTKrcjwo