Chapitre 3

Prérequis

Le modèle OSI et notamment le rôle de la couche liaison de données et de la couche réseau sont à connaître, ainsi que la notion de trame, de protocole Ethernet et de protocole IP. Toutes ces notions sont abordées dans le livre "Cisco - Notions de base sur les réseaux" dans la collection Certifications aux Éditions ENI.

Les chapitres précédents sont également des prérequis.

Objectifs

À la fin de ce chapitre, vous serez en mesure de :

☒Expliquer la notion de VLAN et de trunk (agrégation).

☒Expliquer les meilleures pratiques et leurs conceptions.

☒Mettre en place des VLAN et des trunk.

☒Expliquer les types d'attaques et les méthodes de contre-mesures.

☒Dépanner les problèmes de VLAN et de trunk.

☒Dépanner les problèmes de configuration de base des VLAN.

Au regard du cahier des charges de la certification ICND1, vous serez capable de :

☒Reconnaître le but et les fonctionnalités de divers périphériques réseau (compétence transversale).

☒Sélectionner les composants requis pour rencontrer une spécification réseau donnée (compétence transversale).

☒Identifier les applications courantes et leurs impacts sur le réseau (compétence transversale).

☒Prédire le flux de données entre deux hôtes à travers le réseau (compétence transversale).

☒Dépanner et corriger les problèmes communs associés à l'adressage IP et à la configuration des hôtes (compétence transversale).

☒Configurer et vérifier les VLAN.

☒Configurer et vérifier l'agrégation des commutateurs Cisco, ce qui inclut :

- le protocole DTP ;
- l'auto-négociation.

☒Assigner des ports non utilisés dans un VLAN non utilisé.

☒Placer le VLAN natif dans un autre VLAN que le VLAN 1.

☒Dépanner et résoudre les problèmes d'agrégation (trunk) sur un commutateur Cisco.

- vérifier l'état d'une agrégation ;
- vérifier l'encapsulation d'une agrégation ;
- vérifier et corriger l'appartenance d'un VLAN à une agrégation (*VLAN allowed*).

A. Vue d'ensemble des VLAN

En IPv4, les réseaux locaux sont sensibles aux diffusions, en effet lors d'une diffusion (*broadcast*) toutes les machines du réseau (ou du sous-réseau) reçoivent l'information diffusée, même si cette information ne les concerne pas ! Seuls les routeurs bloquent le trafic de diffusion.

Réduire la taille d'un domaine de diffusion en découpant celui-ci en sous-domaines permet de réduire le nombre de périphériques impactés par la diffusion et d'augmenter les performances du réseau.

Les routeurs sont des appareils spécialisés dans le routage et le transfert de données à longue distance (pour les réseaux WAN) et leurs circuits intégrés gérant la commutation ne sont pas aussi performants que ceux des commutateurs. De plus, les routeurs ne disposent pas de suffisamment de cartes réseau pour autoriser le nombre de subdivisions nécessaires dans un réseau moderne.

L'accès au LAN est généralement géré par un commutateur d'accès L2 (couche 2) qui placera le périphérique dans le réseau virtuel (VLAN) adéquat.

Même si les VLAN sont principalement utilisés dans des réseaux locaux commutés, ils sont de plus en plus employés dans les réseaux étendus (WAN).

1. Définition

Les VLAN sont des regroupements logiques de périphériques au sein d'un même réseau physique, ils sont identifiés par un numéro. Un groupe de périphériques dans un VLAN communiquent comme s'ils étaient reliés au même câble. Des appareils partageant une même connexion physique, mais isolés logiquement dans des VLAN différents, se comporteront comme s'ils étaient sur des réseaux indépendants.

Les diffusions (*broadcast*) sont communiquées uniquement à des périphériques d'un même VLAN et les paquets destinés aux stations n'appartenant pas à ce VLAN doivent être transférés par un routeur (ou un appareil ayant des capacités de routage).

Un VLAN crée un domaine de diffusion logique qui peut s'étendre sur plusieurs segments de réseau local physique.

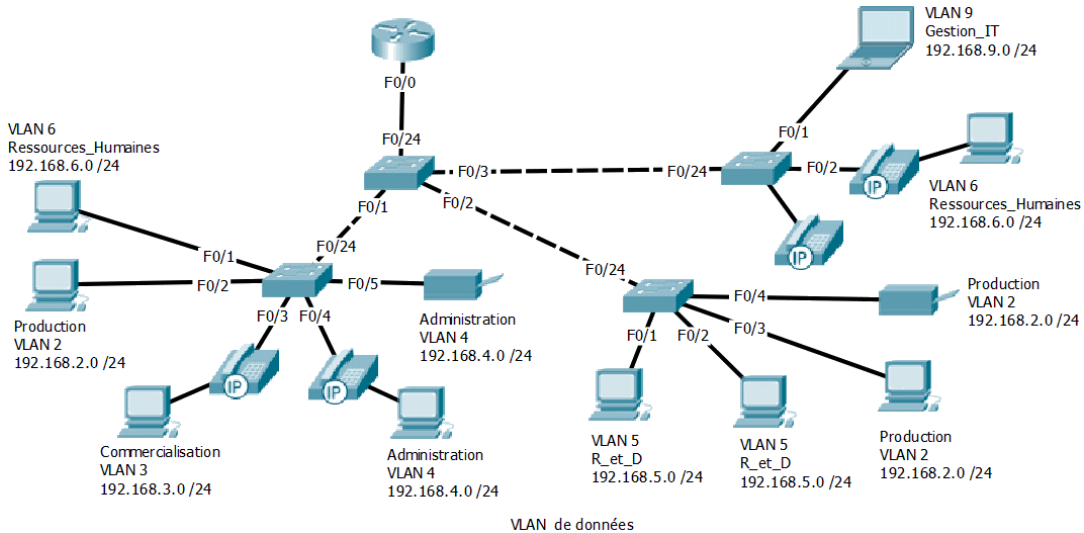
☞*Un VLAN est donc indépendant de sa structure physique et il permet de séparer logiquement des périphériques appartenant à un même réseau physique.*

Les avantages des VLAN sont les suivants :

- Sécurité (confidentialité) : il est possible de séparer logiquement les trames et ainsi de les acheminer uniquement aux destinataires voulus. Chaque port en mode accès d'un commutateur peut être attribué à un seul VLAN (à l'exception des ports connectés à un téléphone IP, à un autre commutateur ou à un point d'accès Wi-Fi). Dans le cas particulier des téléphones IP, le port appartient à deux VLAN.
- Réduction des coûts : l'utilisation d'un réseau convergé où les données informatiques, la téléphonie, la vidéo et les flux vidéo partagent un même média, réduit fortement les coûts d'infrastructure.
- Meilleures performances : la subdivision du réseau en sous-réseaux logiques permet de diminuer les diffusions au sein d'un domaine et diminue également l'impact lors d'incident comme une tempête de diffusion (*broadcast storm*).

- Gestion accrue : la mise en place de VLAN peut sembler dans un premier temps complexe mais en réalité elle simplifie la gestion du service informatique en regroupant les périphériques non pas en fonction de leur localisation mais plutôt en fonction de critères de fonctionnalité, de type de trafic (*class*), de besoins ou de sécurité. Étant donné que les VLAN peuvent être nommés (sauf le VLAN 1), ils sont plus facilement identifiables. Il est possible également de définir des politiques de sécurité et des accès différents par VLAN.

☞*Une tempête de diffusion se produit lorsque toute la bande passante disponible est consommée en raison du nombre trop élevé de trames de diffusion prises dans une boucle de couche 2 et provoque une panne du réseau.*



Exemple de VLAN dans un réseau local.

Chaque VLAN d'un réseau commuté correspond à un sous-réseau IP. L'adressage réseau appliqué aux segments réseau ou aux VLAN doit être réfléchi, cohérent. Il faut donc prendre en compte l'ensemble du réseau afin de clarifier et simplifier au maximum celui-ci !

La méthode d'implémentation des VLAN qui sera abordée est basée sur le port ou réseau local virtuel d'accès (*Access VLAN*).

2. Les types de VLAN

VLAN par défaut : le VLAN par défaut est le VLAN 1. Tous les ports deviennent membres du VLAN par défaut après le démarrage initial du commutateur. Le VLAN 1 ne peut pas être renommé ni supprimé.

```
Switch# show vlan brief
VLAN Name                 Status    Ports
---- -------------------- --------- -------------------------------
1    default              active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                    Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                    Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                    Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                    Gig0/1, Gig0/2
1002 fddi-default         active
1003 token-ring-default   active
1004 fddinet-default      active
1005 trnet-default        active
```

Tous les ports physiques du commutateur sont dans le VLAN 1 qui est le VLAN par défaut.

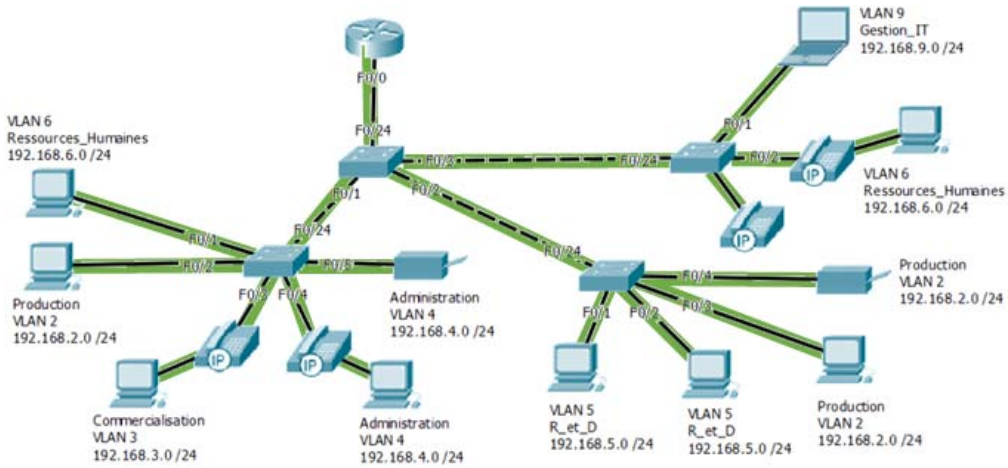
☞*Par défaut, le trafic de contrôle de couche 2, tel que le trafic des protocoles CDP et STP, est associé au VLAN 1. Pour des raisons de sécurité, il est conseillé de choisir un autre VLAN que le VLAN 1 en tant que VLAN par défaut ou en tant que VLAN natif.*

- VLAN natif : un VLAN natif est défini sur un port d'agrégation 802.1Q (*trunk*) afin de déterminer à quel VLAN appartient le trafic non étiqueté. Un port d'agrégation est un port par lequel peuvent passer plusieurs VLAN. Le VLAN natif par défaut est le VLAN 1.
- VLAN natif non étiqueté : il n'y a pas de modification de la trame. C'est le comportement standard d'un commutateur Cisco. Il est parfois nécessaire de recourir à cette technique lorsqu'il faut faire passer le trafic d'un protocole qui vérifie l'intégrité de ses trames.
- VLAN natif étiqueté : même le VLAN natif est marqué par une étiquette. Cette technique de plus en plus courante permet de se prémunir des attaques utilisant un double étiquetage (*double tagging attack*), le but de ces attaques étant de provoquer un saut de VLAN.

☞*Le protocole STP (Spanning Tree Protocol) garantit l'unicité du chemin logique entre toutes les destinations sur le réseau en procédant intentionnellement au blocage des chemins redondants susceptibles d'entraîner la formation d'une boucle.*

a. VLAN de données

Les VLAN de données ne transportent que le trafic généré par l'utilisateur. Il est d'usage de séparer le trafic de voix et de gestion du trafic de données car ils ne nécessitent pas le même traitement.

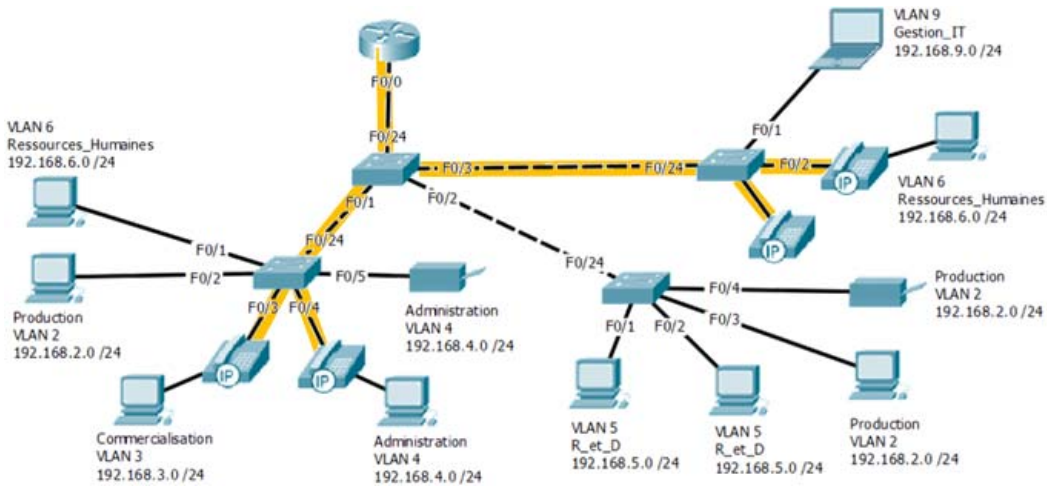


VLAN de données.

b. VLAN voix

Un VLAN spécifique est nécessaire pour prendre en charge la voix sur IP (VoIP) dont le trafic est très sensible. Ce VLAN a comme caractéristiques :

- Une bande passante consolidée pour garantir la qualité de la voix. Ce qui implique de prioriser le trafic en donnant une priorité absolue à ce VLAN.
- Un délai inférieur à 150 ms sur l'ensemble du réseau. Qu'il soit local, intersite ou VPN.



VLAN voix.