VLAN

Fonctionnement\*\* : Un VLAN permet de segmenter un réseau physique en plusieurs réseaux logiques au niveau de la couche 2 (liaison de données) de l'OSI. Cela permet de regrouper des périphériques qui peuvent être dispersés physiquement mais qui doivent

Utilisation\*\* : Les VLAN sont utilisés pour améliorer la performance et la sécurité du réseau en limitant les domaines de diffusion et en séparant logiquement les groupes d'utilisateurs ou de périphériques

Prenons un exemple concret avec des adresses IP pour illustrer l'utilisation des VLANs.

Supposons que nous ayons un réseau d'entreprise avec trois départements : Administration, Finance et Ressources Humaines. Chaque département doit être isolé des autres pour des raisons de sécurité et de gestion du trafic. Voici comment nous pouvons configurer les VLANs et les sous-réseaux :

### Configuration des VLANs et sous-réseaux

1. \*\*Administration\*\* :

- \*\*VLAN ID\*\* : 10

- \*\*Adresse IP du sous-réseau\*\* : 192.168.10.0/24

- \*\*Plage d'adresses IP\*\* : 192.168.10.1 à 192.168.10.254

2. \*\*Finance\*\* :

- \*\*VLAN ID\*\* : 20

- \*\*Adresse IP du sous-réseau\*\* : 192.168.20.0/24

- \*\*Plage d'adresses IP\*\* : 192.168.20.1 à 192.168.20.254

3. \*\*Ressources Humaines\*\* :

- \*\*VLAN ID\*\* : 30

- \*\*Adresse IP du sous-réseau\*\* : 192.168.30.0/24

- \*\*Plage d'adresses IP\*\* : 192.168.30.1 à 192.168.30.254

### Mise en place

Pour mettre en place cette configuration, nous devons configurer nos commutateurs réseau pour assigner les ports physiques aux VLANs respectifs. Par exemple :

- \*\*Port 1 à 10\*\* du commutateur pour les ordinateurs de l'administration seront assignés au VLAN 10.

- \*\*Port 11 à 20\*\* du commutateur pour les ordinateurs de la finance seront assignés au VLAN 20.

- \*\*Port 21 à 30\*\* du commutateur pour les ordinateurs des ressources humaines seront assignés au VLAN 30.

### Exemple d'utilisation

- Un ordinateur de l'administration avec l'adresse IP 192.168.10.10 pourra communiquer avec un autre ordinateur du même VLAN avec l'adresse IP 192.168.10.20, même s'ils sont physiquement connectés à différents commutateurs.

- Un ordinateur de la finance avec l'adresse IP 192.168.20.15 ne pourra pas directement communiquer avec un ordinateur des ressources humaines avec l'adresse IP 192.168.30.25 sans passer par un routeur configuré pour gérer le trafic inter-VLANs.

### Avantages

1. \*\*Isolation\*\* : Les VLANs isolent les différents départements, réduisant le risque de propagation de virus ou de malware entre eux.

2. \*\*Sécurité\*\* : Les données sensibles de chaque département sont protégées contre l'accès non autorisé des autres départements.

3. \*\*Gestion du trafic\*\* : En limitant les domaines de diffusion, les VLANs réduisent la quantité de trafic inutile sur le réseau, améliorant ainsi les performances globales.

Cette configuration montre comment les VLANs et les sous-réseaux peuvent être utilisés ensemble pour segmenter logiquement et sécuriser un réseau d'entreprise, tout en optimisant la gestion du trafic réseau.

une salle de réunion et une salle de laboratoire. Pour simplifier, nous pourrions configurer les VLAN comme suit :

Dans cette configuration, chaque salle forme un VLAN distinct avec un identifiant unique. Par exemple, les appareils connectés à des ports dans la salle de classe 1 communiqueraient uniquement avec d'autres appareils dans le même VLAN (VLAN 10). De même, les appareils dans la salle de classe 2 seraient dans un VLAN différent (VLAN 20) et ne pourraient pas communiquer directement avec les appareils dans la salle de classe 1 à moins que cela ne soit explicitement configuré pour le permettre.

- Salle de classe 1 : VLAN 1

- Salle de classe 2 : VLAN 2

- Salle de classe 3 : VLAN 3

- Salle de réunion : VLAN 4

- Salle de laboratoire : VLAN 5

- Salle de classe 1 : VLAN 6

- Salle de classe 2 : VLAN 7

- Salle de classe 3 : VLAN 8

- Salle de réunion : VLAN 9

- Salle de laboratoire : VLAN 10

- Salle de classe 1 : VLAN 11

- Salle de classe 2 : VLAN 12

- Salle de classe 3 : VLAN 12

- Salle de réunion : VLAN 14

- Salle de laboratoire : VLAN 15

- Salle de classe 1 : VLAN 16

- Salle de classe 2 : VLAN 17

- Salle de classe 3 : VLAN 18

- Salle de réunion : VLAN 19

- Salle de laboratoire : VLAN 20

1. Chaque salle forme un VLAN distinct , Chaque point d'accès forme son propre VLAN

Dans ce contexte, chaque salle et chaque point d'accès forme son propre VLAN distinct, ce qui signifie que chaque VLAN est isolé des autres. Voici un exemple illustratif :

Imaginons un bâtiment avec plusieurs salles de classe, chacune équipée d'un point d'accès Wi-Fi.

* Salle de classe 1 : VLAN 10
  + Le point d'accès de la salle de classe 1 forme également le VLAN 10 pour les appareils connectés à ce point d'accès.
* Salle de classe 2 : VLAN 20
  + Le point d'accès de la salle de classe 2 forme le VLAN 20 pour les appareils connectés à ce point d'accès.

Ainsi, les appareils dans la salle de classe 1 ne peuvent pas communiquer directement avec les appareils dans la salle de classe 2, car ils appartiennent à des VLAN différents. De même, les appareils connectés à chaque point d'accès ne peuvent pas communiquer avec les appareils des autres salles, car chaque point d'accès forme son propre VLAN isolé. Cette configuration offre une segmentation du réseau pour des raisons de sécurité et de gestion du trafic.

Top of Form

Pour configurer les VLANs dans un réseau, vous aurez besoin d'un équipement réseau tel que des commutateurs (switches) et des points d'accès Wi-Fi. Voici un exemple de configuration basique utilisant des commutateurs Cisco et des points d'accès Wi-Fi :

***Voir la configuration dans Configuration Terminal VLAN***