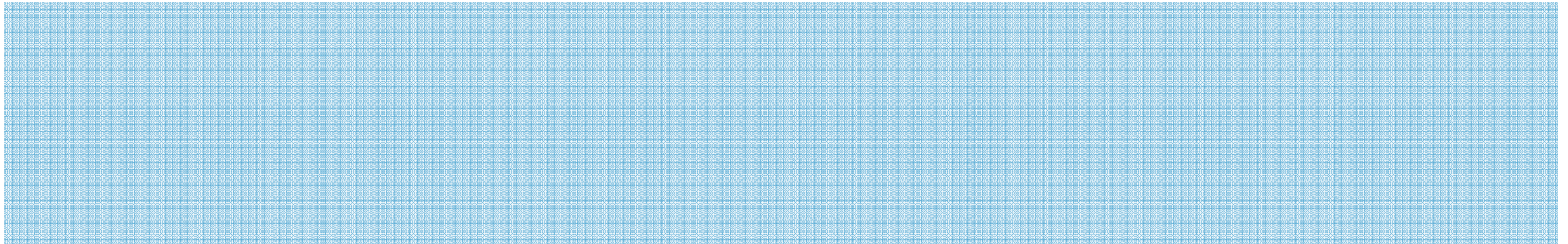


Cours : Administration réseaux et Qualité de service

Chapitre 4 : Technologies Commutation



LAN virtuel (VLAN)

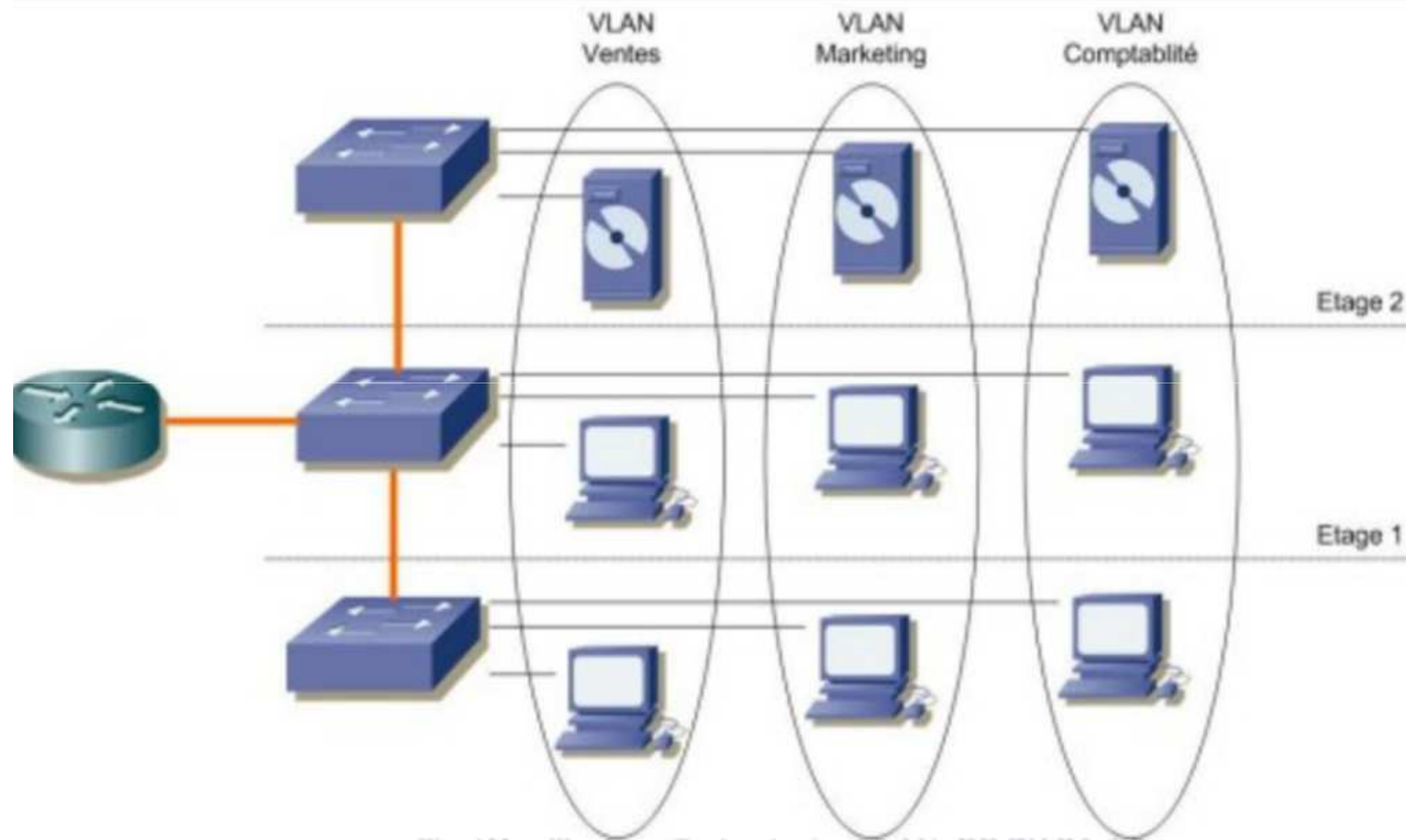
Définition

La virtualisation d'un LAN consiste à séparer l'infrastructure physique des services de transfert rapide fournis par les commutateurs.

L'objectif fondamental d'un VLAN est de rendre la fonction d'un LAN (tel que décrit plus haut) indépendante de l'infrastructure physique.

Soit une seule infrastructure physique supporte plusieurs LAN distincts (VLANs)

LAN virtuel (VLAN)



Les avantages du VLAN

Le VLAN offre les avantages suivants :

- Plus de souplesse pour l'administration et les modifications du réseau car toute l'architecture peut être modifiée par simple paramétrage des commutateurs.
- Gain en sécurité car les informations sont encapsulées dans un niveau supplémentaire et éventuellement analysées
- Réduction de la diffusion du trafic sur le réseau.

De plus, cette fonctionnalité peut être étendue sur des ports de commutateurs distants à travers toute l'infrastructure. Dans ce cas, les commutateurs devront transporter entre eux du trafic appartenant à plusieurs VLANs sur une ou plusieurs liaisons spécifiques .

Les niveaux de VLAN

Typologie de VLAN

Plusieurs types de VLAN sont définis, selon le critère de commutation et le niveau auquel il s'effectue :

Un **VLAN de niveau 1** (aussi appelés **VLAN par port**, en anglais Port-Based VLAN) définit un réseau virtuel en fonction des ports de raccordement sur le commutateur ;

Un **VLAN de niveau 2** (également appelé **VLAN MAC**, VLAN par adresse IEEE ou en anglais MAC Address-Based VLAN) consiste à définir un réseau virtuel en fonction des adresses MAC des stations.

Les niveaux de VLAN

Un **VLAN de niveau 3** : on distingue plusieurs types de VLAN de niveau 3 :

Le **VLAN par sous-réseau** (en anglais *Network Address-Based VLAN*) associe des sous-réseaux selon l'adresse IP source des datagrammes.

Le **VLAN par protocole** (en anglais *Protocol-Based VLAN*) permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, AppleTalk, etc.), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau.

Les types de VLAN

VLAN de données

Un VLAN de données est un réseau local virtuel qui est configuré pour ne transporter que le trafic généré par l'utilisateur.

VLAN par défaut

Tous les ports du commutateur deviennent membres du VLAN par défaut après le démarrage initial du commutateur.

VLAN natif

Un VLAN natif est affecté à un port d'agrégation 802.1Q.

Un port d'agrégation 802.1Q prend en charge le trafic provenant de nombreux VLAN (trafic étiqueté ou « tagged traffic »), ainsi que le trafic qui ne provient pas d'un VLAN (trafic non étiqueté ou « untagged traffic »). Le port d'agrégation 802.1Q place le trafic non étiqueté sur le VLAN natif.

Les types de VLAN

VLAN de gestion

Un VLAN de gestion est un réseau local virtuel que vous configurez pour accéder aux fonctionnalités de gestion d'un commutateur. C'est le VLAN 1 qui fait office de VLAN de gestion si vous ne définissez pas explicitement un VLAN distinct pour remplir cette fonction

VLAN voix

Il est facile de comprendre pourquoi un VLAN distinct est requis pour prendre en charge la voix sur IP (VoIP). Imaginez que vous recevez un appel d'urgence et que soudain, la qualité de la transmission se dégrade tellement que vous ne comprenez plus ce que dit votre interlocuteur.

Configuration des VLAN

Un port peut être configuré pour prendre en charge les types de VLAN suivants :

VLAN statique : les ports d'un commutateur sont affectés manuellement à un VLAN.

VLAN dynamique L'appartenance d'un port à un VLAN dynamique se configure à l'aide d'un serveur spécial appelé serveur VMPS (VLAN Membership Policy Server). Avec le serveur VMPS, vous affectez dynamiquement les ports de commutateur aux VLAN.

VLAN voix : un port est configuré en mode voix pour qu'il puisse prendre en charge un téléphone IP qui est connecté dessus.

Agrégation de VLAN

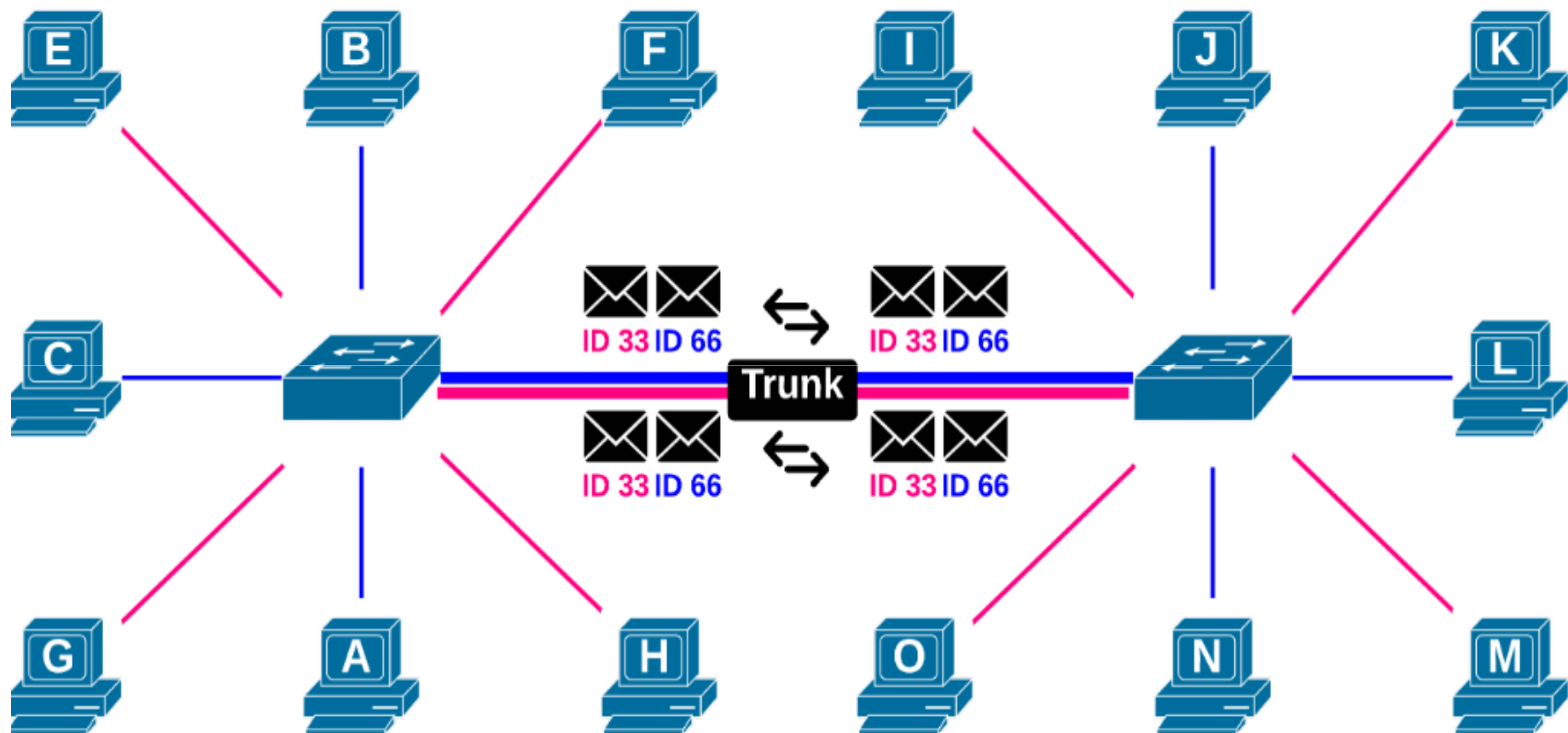
Définition

Une agrégation est une liaison point à point entre deux périphériques réseau qui porte plusieurs VLAN.

Une agrégation de VLAN vous permet d'étendre les VLAN à l'ensemble d'un réseau.

Une agrégation de VLAN n'appartient pas à un VLAN spécifique, mais constitue plutôt un conduit pour les VLAN entre les commutateurs et les routeurs.

Trunk ou Liaison d'agrégation



Les hôtes A, B, C, J, L, N appartiennent au VLAN 66. Les hôtes E, F, G, H, I, K, M O appartiennent au VLAN 33.

Les commutateurs isolent le trafic entre les VLANs distincts mais transfèrent le trafic d'un même VLAN sur une liaison Trunk en ajoutant une étiquette dans chaque trame.

Liaison d'agrégation (Trunk)

Liaison d'agrégation

Les ports d'une liaison qui agrègent le trafic de plusieurs VLANs s'appellent un "Trunk" chez le constructeur Cisco Systems et "liaison d'agrégation" chez d'autres.

Sur ce type de liaison, le commutateur ajoute des champs supplémentaires dans ou autour de la trame Ethernet.

Ils servent notamment à distinguer le trafic de VLANs différents car ils contiennent entre autres le numéro d'identification du VLAN.

Protocoles (Trunk)

On trouvera deux protocoles de “Trunk” ou de “liaison d’agrégation” VLAN qui permettent de distinguer le trafic de VLANs distincts.

Il agissent au niveau de la couche 2 “liaison de données” (L2). Ils opèrent sous les couches TCP/IP.

Inter-Switch Link (ISL) : protocole propriétaire Cisco qui encapsule la trame d’origine avec un en-tête spécifique qui contient entre autres le numéro de VLAN et un nouveau champ FCS.

Il est indépendant de la technologie sous-jacente. Il est de moins en moins rencontré au profit de IEEE 802.1q.

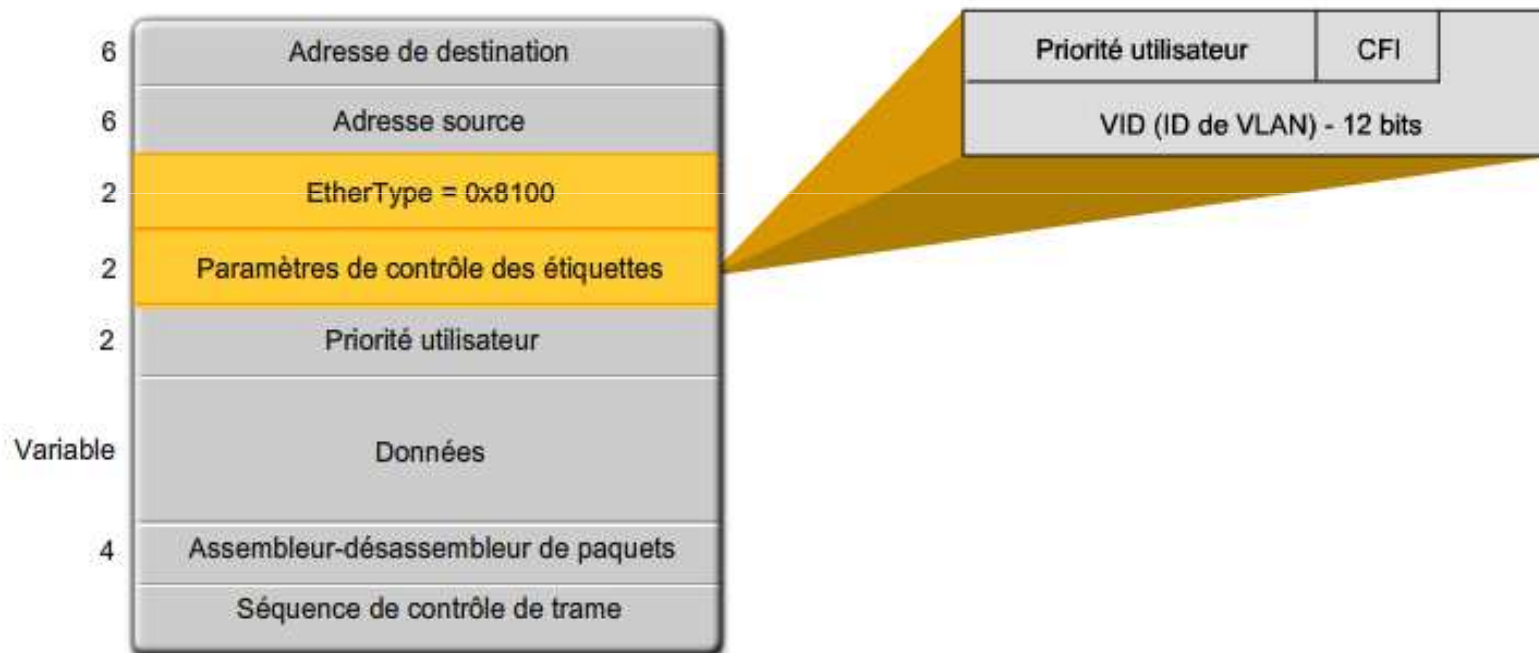
Protocoles (Trunk)

IEEE 802.1q : Standardisé et interopérable, il ajoute une étiquette dans l'en-tête de la trame (un ensemble de champs juste après le champ d'adresse MAC d'origine). Cette étiquette a une taille de 4 octets ou 32 bits dont 12 bits sont consacrés au numéro de VLAN.

Le standard supporte les technologies IEEE 802.3 (Ethernet), IEEE 802.11 (WIFI), IEEE 802.5 (Token-Ring), etc. en tant que protocole de "pontage" (bridging, IEEE 802.1). Vu que la trame sera modifiée, le commutateur recalculera la valeur du champ CRC/FCS.

Champ de l'étiquette VLAN

Détails du champ de l'étiquette VLAN



Format de l'étiquette VLAN

Le champ de l'étiquette VLAN se compose d'un champ EtherType, d'un champ d'informations de contrôle d'étiquette et du champ de la séquence de contrôle de trame.

Champ EtherType

défini sur la valeur hexadécimale 0x8100. Cette valeur s'appelle la valeur de l'ID de protocole d'étiquette (TPID).

Le champ EtherType étant défini sur la valeur du TPID, le commutateur qui reçoit la trame sait qu'il doit rechercher des informations dans le champ d'informations de contrôle d'étiquette.

Format de l'étiquette VLAN

Champ Paramètres de contrôle des étiquettes

Le champ Paramètres de contrôle des étiquettes contient :

3 bits de priorité utilisateur : utilisés par la norme 802.1p qui spécifie comment assurer la transmission prioritaire des trames de couche 2.

1 bit d'identificateur de format canonique (CFI) : permet aux trames Token Ring d'être facilement transportées sur des liens Ethernet.

12 bits d'ID de VLAN (VID) : numéros d'identification de VLAN ; prend en charge jusqu'à 4 096 ID de VLAN.

Format de l'étiquette VLAN

Champ de la séquence de contrôle de trame

Une fois que le commutateur a inséré le champ EtherType et le champ d'informations de contrôle d'étiquette, il recalcule les valeurs de la séquence de contrôle de trame et les insère dans la trame.

.

Référence

J-f .Pillou. F. Lemainque ,tout sur les réseaux et internet ,
Dunod. 2012.

<https://cisco.goffinet.org/ccna/vlans/concepts-vlan-cisco/>

<https://www.commentcamarche.net/contents/543-vlan-reseaux-virtuels>