Collection Formation Réseau Cisco CCNA

LAN SWITCHING

Technologies VLAN
(Cisco IOS)

François-Emmanuel Goffinet
Formateur IT
Version 15.10

Prérequis

- TCP/IP fondamental
- Technologie Ethernet et commutation
- Prise en main d'un commutateur Cisco©
- Routeurs et routage IPv4/IPv6 (notions)

Objectifs ICND1

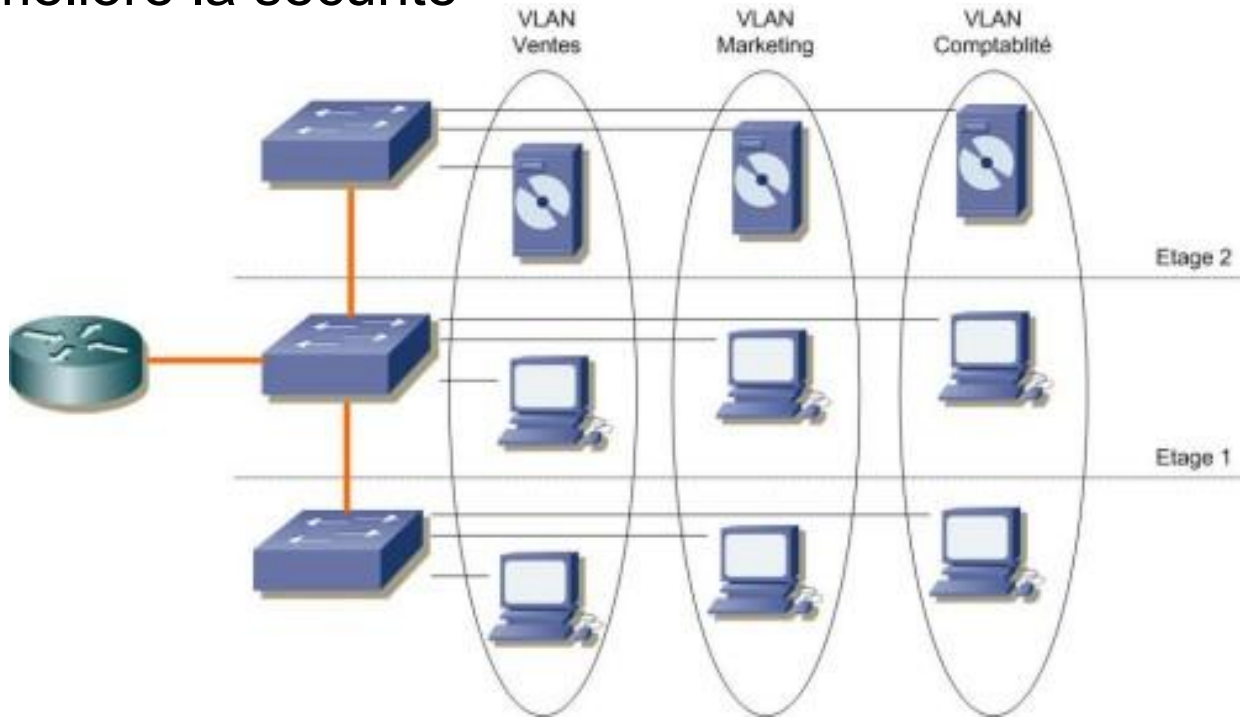
1. Définir et caractériser la notion de LAN et la comparer à celle de **VLAN** dans son fonctionnement
2. Définir la notion de **Trunking** VLAN, expliquer ses avantages et ses inconvénients, et analyser les protocoles associés
3. Expliquer la notion de routage des VLANs
4. Expliquer les différents modes sur les ports des commutateurs Cisco
5. Définir les différents types de VLANs
6. Configurer et dépanner des VLANs et des trunks sous Cisco IOS®
7. Caractériser et configurer le protocole DTP
8. Caractériser et configurer le protocole VTP
9. Appliquer les bonnes pratiques de configuration des VLANs

Sommaire

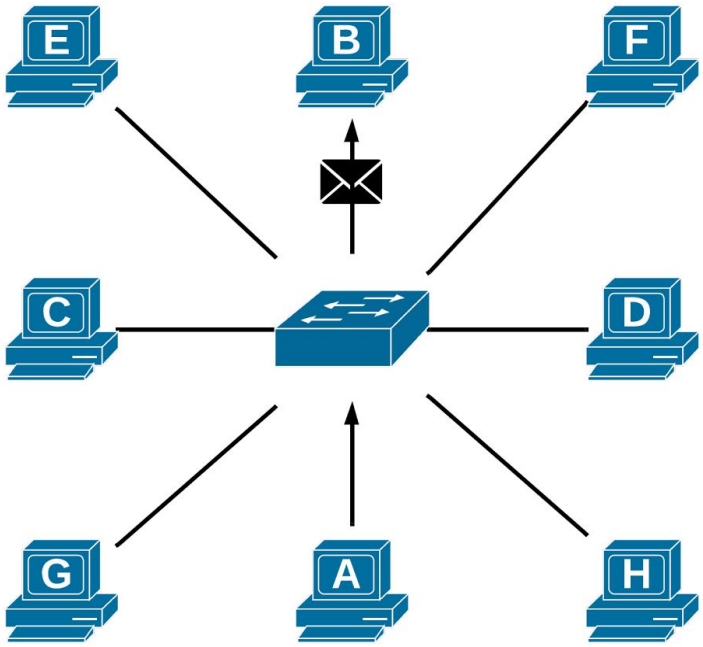
1. Notion de LAN virtuel (VLAN)

Avantages de la technologie VLANs

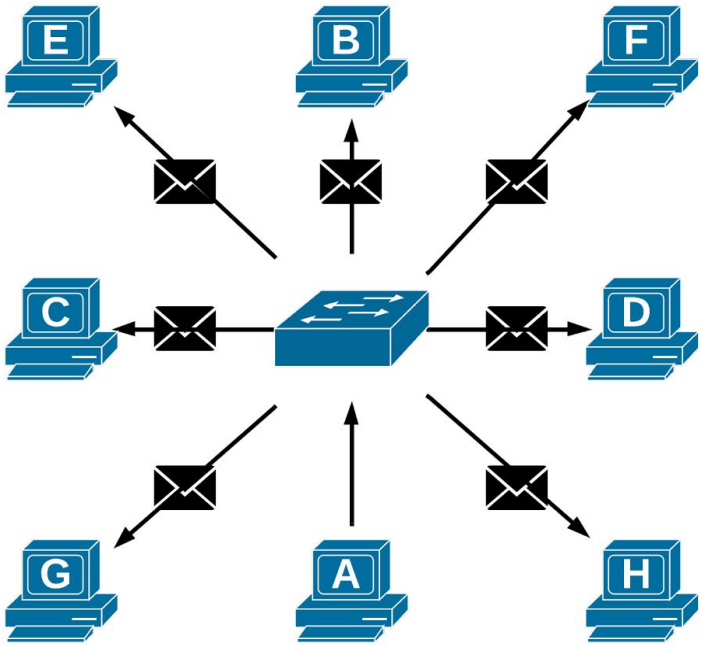
- Réduit la taille des domaines de *broadcast*/*multicast*
- Permet de classer le trafic
- Améliore la gestion
- Virtualise l'infrastructure en domaines IP
- Améliore la sécurité



Fonctionnement d'un LAN



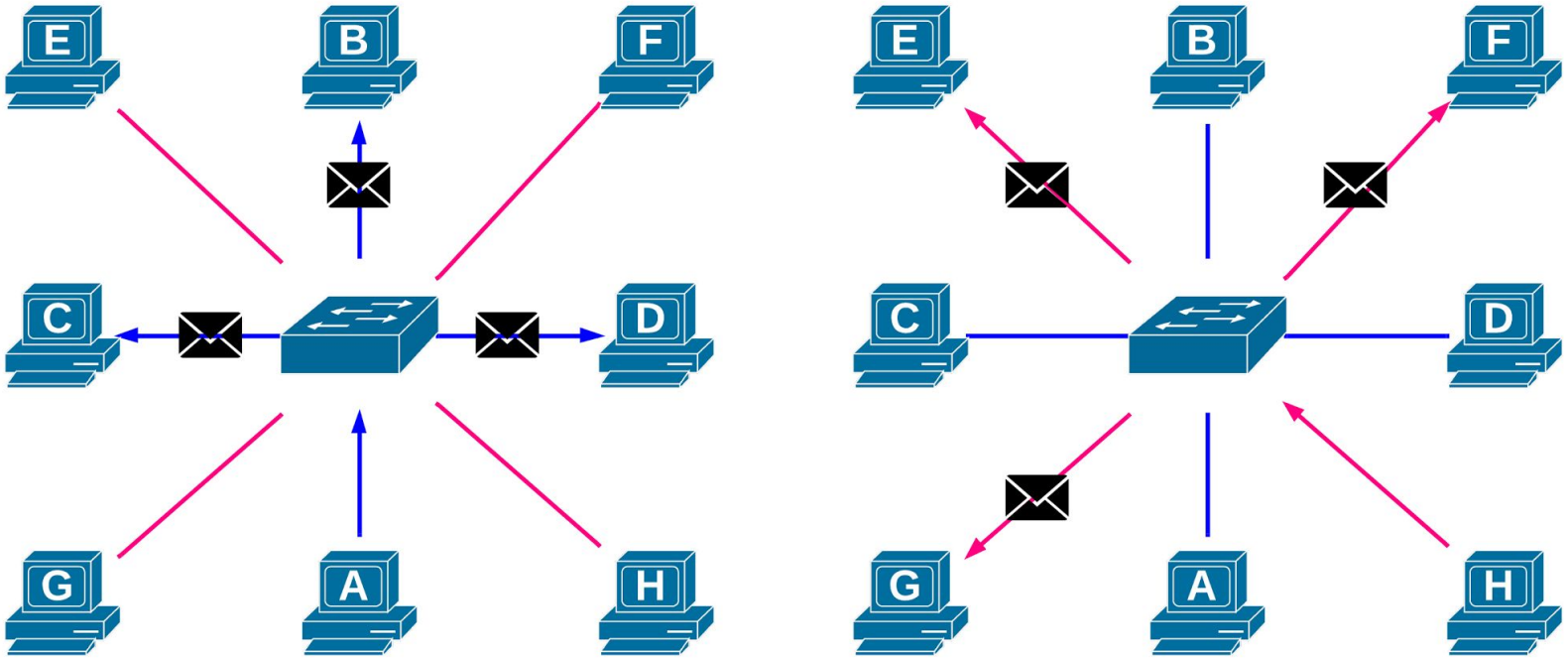
L'hôte A émet du trafic *unicast* à destination de B



L'hôte A émet du trafic *broadcast* ou *multicast*

Au sein d'un LAN défini comme une infrastructure commutée, soit un réseau composé de commutateurs, toutes les interfaces hôtes disposent d'une adresse unique : une adresse physique MAC du protocole IEEE 802. Un commutateur tient des tables de correspondance entre ses ports et les adresses des hôtes afin de transférer rapidement le trafic. Sur ces réseaux, on connaît du trafic *unicast* (à destination d'un seul hôte), du trafic de *broadcast* (diffusion, à destination de tous les hôtes) et du trafic *multicast* (à destination de certains hôtes). Un commutateur transfère le trafic de diffusion (*broadcast*) et *multicast* à travers tous ses ports sauf celui d'origine; un routeur « filtre » le trafic de diffusion en ne le transférant pas.

LAN Virtuel (VLAN)



Les hôtes A, B, C, D appartiennent au VLAN 66. Les hôtes E, F, G, H appartiennent au VLAN 33.
Les figures illustrent le trafic de *broadcast* émanant respectivement des hôtes A et H.

Un VLAN est un LAN logique fonctionnant sur une infrastructure LAN physique commutée. Une infrastructure physique commune peut supporter plusieurs VLANs. Chaque LAN virtuel fonctionnera comme n'importe quel LAN distinct. Concrètement, les ports du commutateur prennent un identifiant VLAN. Cet identifiant logique définit l'étendue du domaine de diffusion : le trafic de diffusion ne sera transféré que sur les ports ayant le même identifiant. Autrement dit, par exemple, le trafic de diffusion venant d'un port appartenant au VLAN 66 ne se sera transféré que sur les ports ayant pour attribution le VLAN 66. La séparation fonctionnelle entre deux ports ayant des identifiants VLAN différents correspond à une séparation physique. En quelque sorte, la technologie VLAN permet de diviser logiquement les ports du commutateur, soit l'infrastructure physique elle-même.

Définition

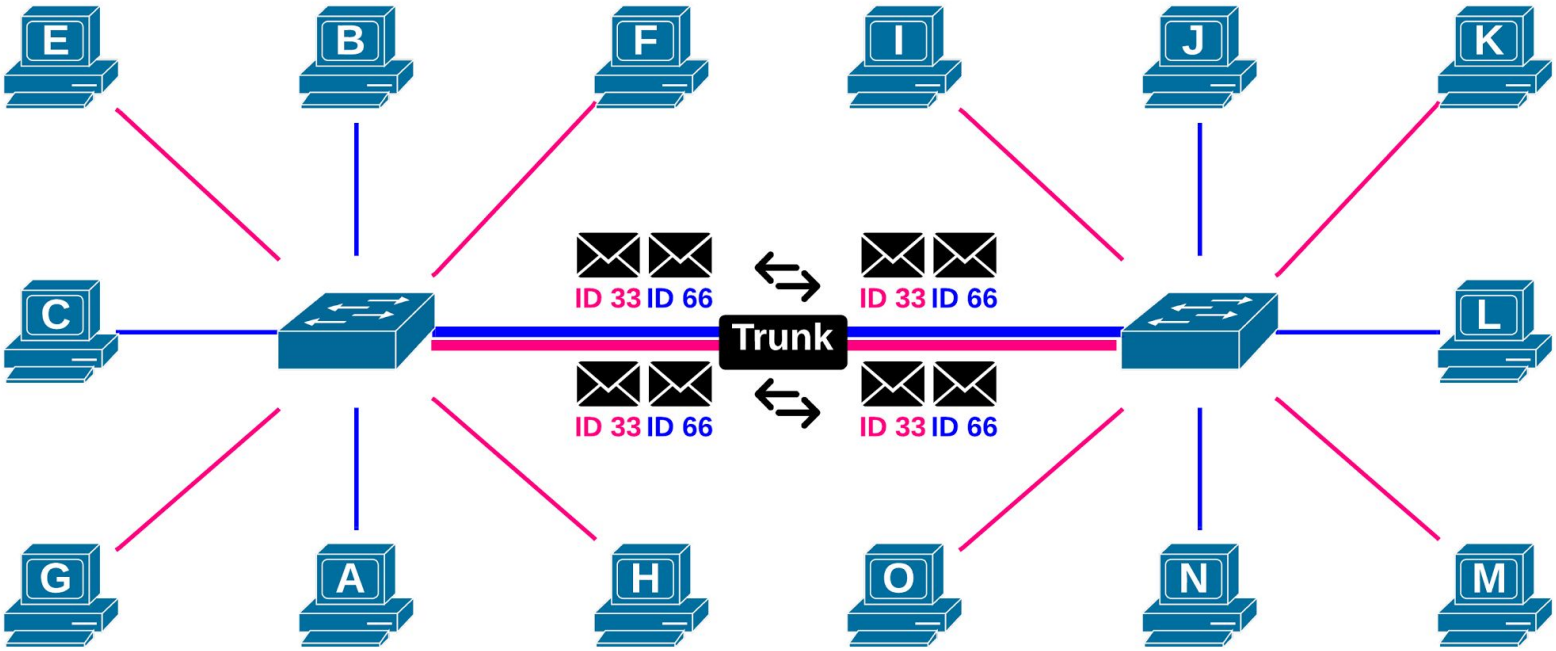
La virtualisation d'un LAN consiste en la séparation de l'infrastructure physique et des services de transfert rapide fournis par les commutateurs.

L'objectif fondamental d'un VLAN est de rendre la fonction d'un LAN (tel que décrit plus haut) indépendante de l'infrastructure physique. Cette technologie s'intègre pleinement dans les marchés des environnements virtualisés, des déploiements de réseaux sans fil, de la VoIP, des passerelles Internet d'entreprise et familiales.

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 ...**

2. Trunking

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.

... 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.

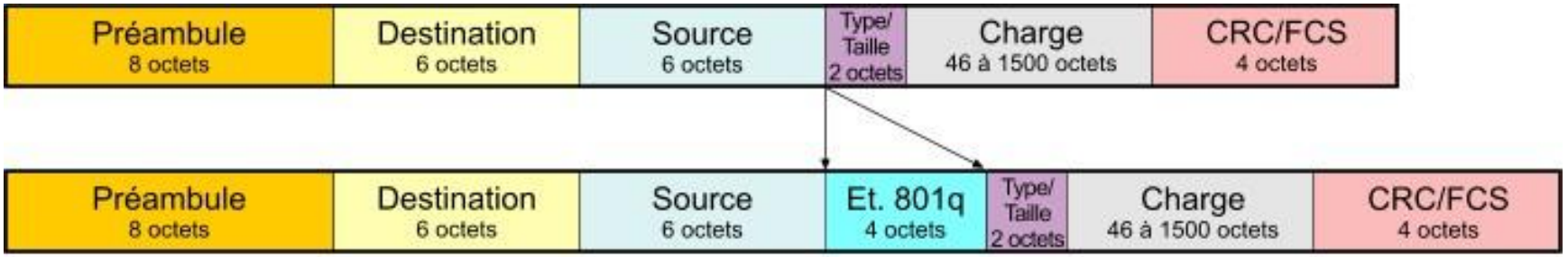
Protocoles “Trunk”

Deux protocoles de “Trunk” ou de “liaison d'agrégation” VLAN peuvent être rencontrés. Il agissent au niveau de la couche 2 “liaison de données”. 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.

- **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.

Etiquette 802.1q



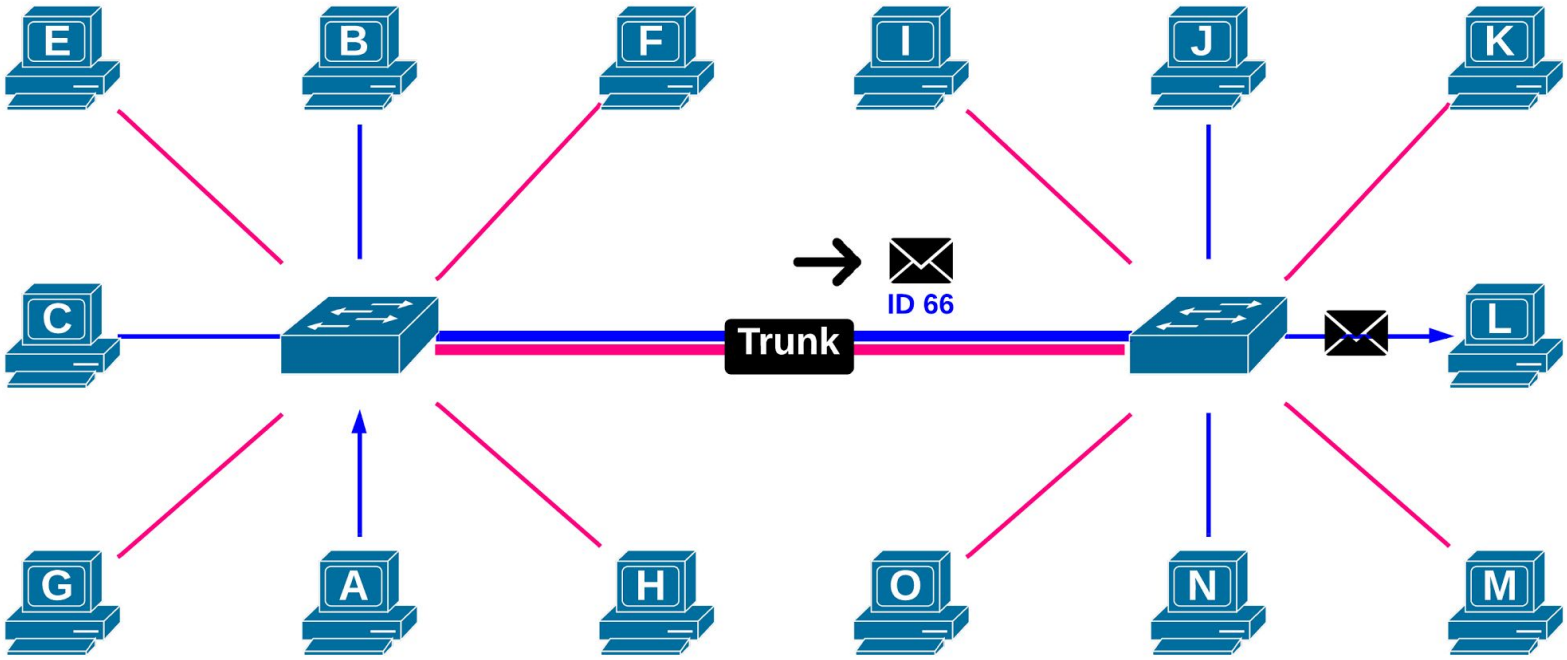
Où L'étiquette IEEE 802.1q est composée de :

- **TPID** *Tag Protocol Identifier* (16 bits) : 0x8100, valeur annonçant la charge IEEE 801.q
- **TCI** *Tag Control Identifier* (16 bits) :
  - **PCP** *Priority Code Point* (3 bits), priorité IEEE 802.1p
  - **CFI** *Canonical Format Indicator* (1bit), la valeur 0 correspond à une adresse MAC en format canonique
  - **VID** *VLAN Identifier* (12 bits), l'identifiant VLAN

- TPID (16 bits)
- TCI/PCP (3 bits)
- VID (12 bits)

```
Ethernet II, Src: Cisco_df:ae:18 (00:13:c3:df:ae:18), Dst: Cisco_1b:a4:d8 (00:1b:d4:1b:a4:d8)
 ▷ Destination: Cisco_1b:a4:d8 (00:1b:d4:1b:a4:d8)
 ▷ Source: Cisco_df:ae:18 (00:13:c3:df:ae:18)
   Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 118
   000. .... .... .... = Priority: Best Effort (default) (0)
   ...0 .... .... .... = CFI: Canonical (0)
   .... 0000 0111 0110 = ID: 118
   Type: 802.1Q Virtual LAN (0x8100)
```

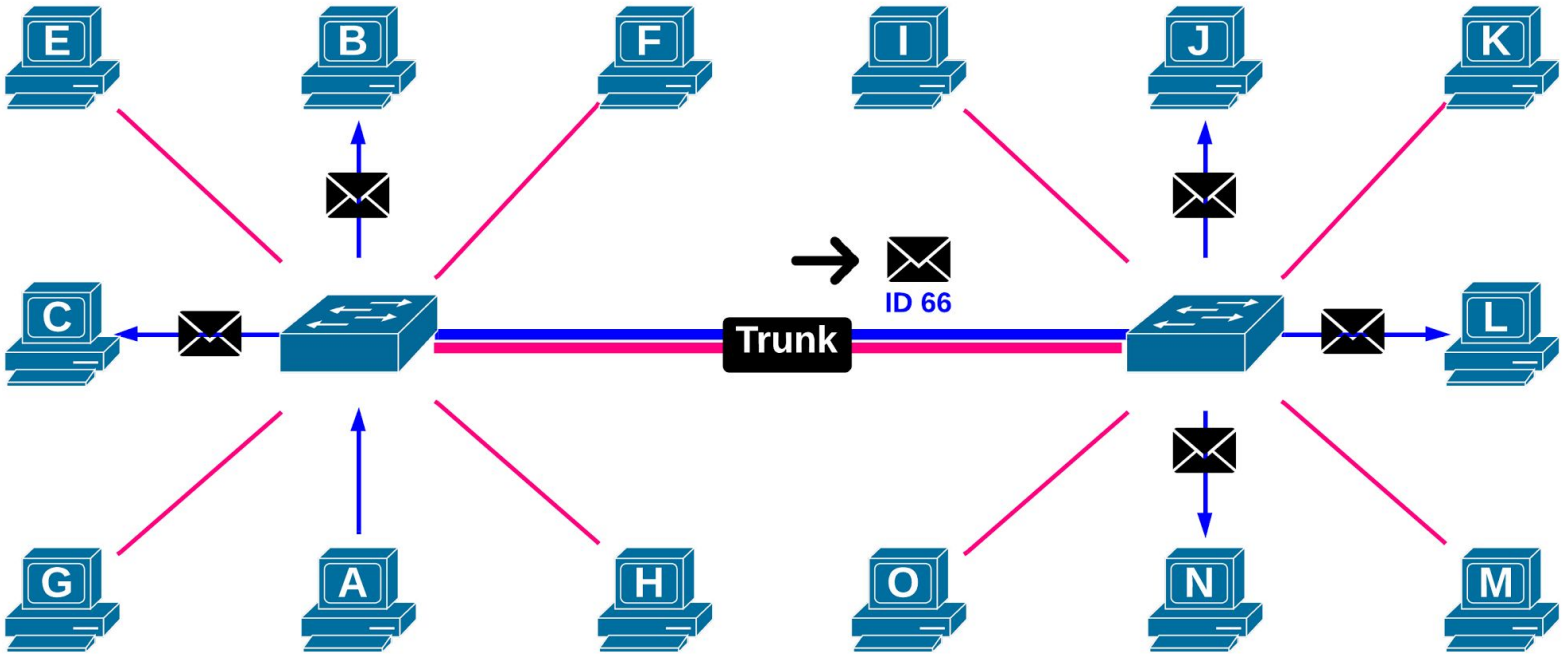
Encapsulation



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.
L'hôte A transmet du trafic à l'hôte L. La trame prend une étiquette sur la liaison Trunk. L'étiquette est retirée lors de la livraison locale.

Quand cette encapsulation IEEE 802.1q intervient-elle ? Un hôte A veut joindre un hôte L connecté à un commutateur distant. Les commutateurs sont interconnectés par une « liaison d'agrégation » ou *Trunk*. La trame sera étiquetée seulement si elle quitte le commutateur sur un port qui connecte une liaison d'agrégation. Lors de la livraison locale de la trame à la station destinataire, elle sort du port du commutateur sans étiquette.

Multicast/Diffusion



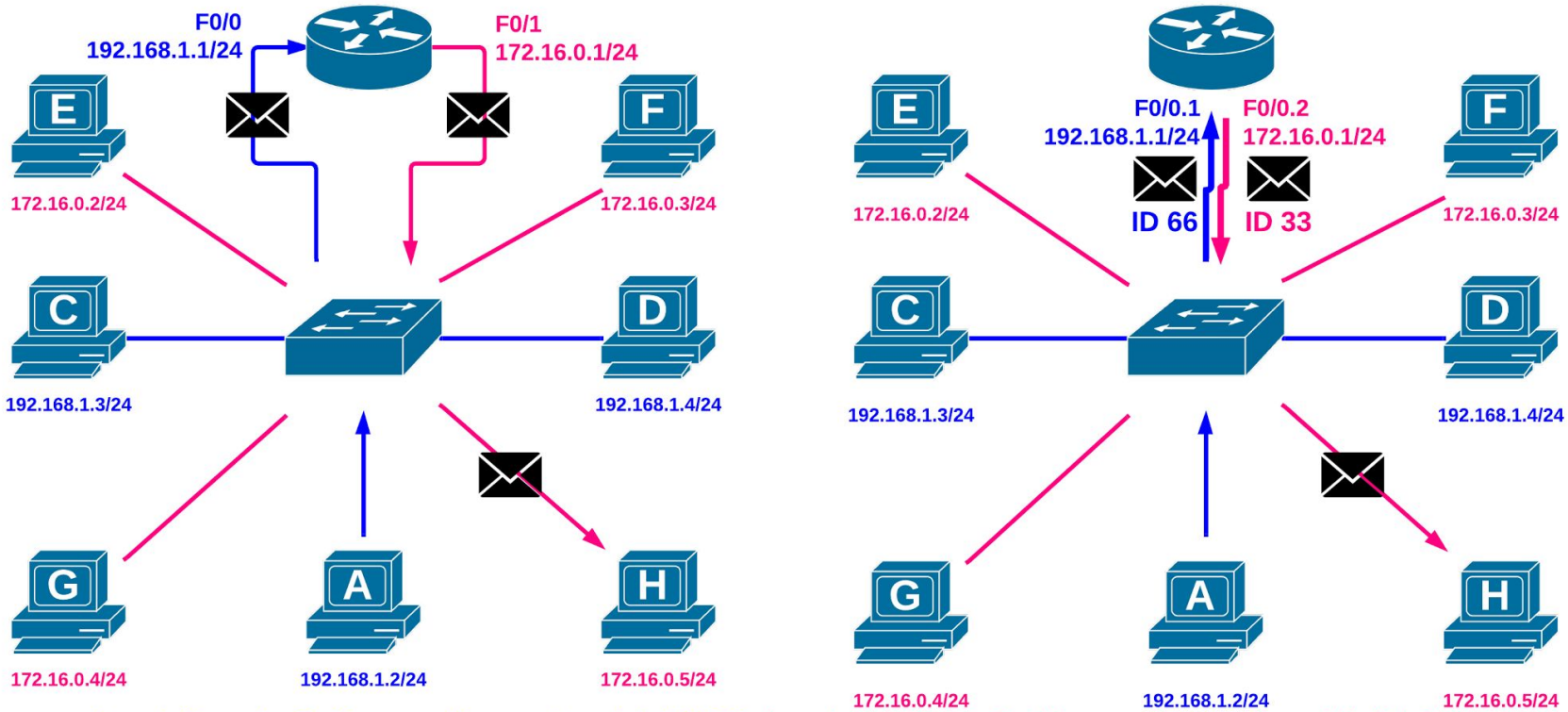
Les hôtes A, B, C, J, L, N appartiennent au VLAN 66. Les hôtes E, F, G, H, I, K, M O appartiennent au VLAN 33. L'hôte A transmet du trafic *broadcast*. Les commutateurs transfèrent le trafic uniquement sur les ports identifiés VLAN 66.

Le trafic de diffusion (*broadcast*) comme celui de *multicast* sera porté à la destination de tous les ports ayant le même identifiant VLAN, à travers des ports de « liaison d'agrégation ». Les hôtes connectés à un port d'un identifiant VLAN différent ne seront pas affectées par ce trafic. En ce sens, la taille des domaines de diffusion peut être contrôlée sur une infrastructure commutée à des fins de performance, d'administration du trafic, des machines et des utilisateurs.

Domaines IP

- Comme dans tout LAN, le réseau IP est homogène et correspond à un adressage marqué par un préfixe et un masque de réseau.
- Au sein d'un LAN, toutes les interfaces qui participent à IP partagent le même adressage.
- Un routeur constitue la limite d'un VLAN comme celle d'un LAN. En conséquence, pour que des VLANs communiquent ensembles, en tant que réseaux logiques différents, une fonction de routage est nécessaire. On parle dans la littérature de **routage inter-VLAN**.
- Cette fonction peut être remplie par des plate-formes d'entreprise comme les routeurs d'accès, des routeurs Linux/BSD ou des commutateurs LAN disposant d'un logiciel de routage (commutateurs L3). Les routeurs sont capables de transférer du trafic de VLANs différents à partir d'un seul port physique reconnu comme port d'agrégation VLAN.

Routage inter-VLAN

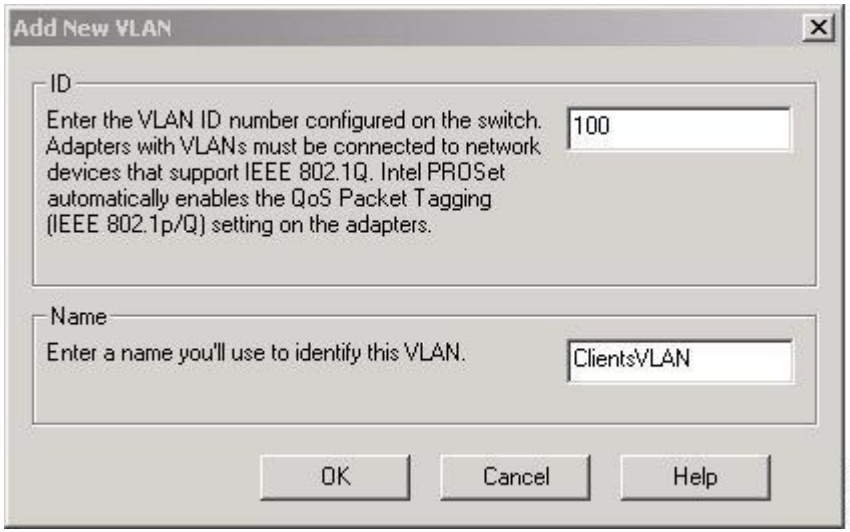


Les hôtes A, C, D appartiennent au VLAN 66. Les hôtes E, F, G, H appartiennent au VLAN 33.
Les figures illustrent le trafic de l'hôte A vers l'hôte H à travers un routeur IPv4 avec deux interfaces physiques distinctes (à gauche) ou sur une seule liaison *Trunk* (à droite).

Dans cet exemple, une seule interface du routeur est nécessaire. Elle sera configurée en mode trunk en créant pour chaque VLAN une sous-interface logique différente. Évidemment, l'interface physique ne prend pas d'adresse IP.

3. Implémentation de la technologie

Cartes 802.1q pour serveur Intel



Si le standard est largement disponible sur les commutateurs d'entreprise, les hôtes tels que les serveurs ou du matériel embarqué peuvent supporter la technologie VLAN en fonction des pilotes développés pour l'interface physique. Alors que les systèmes d'exploitation Linux/BSD supportent un grand nombre de cartes, les cartes Intel (ou Broadcom) sont bien supportées sous Microsoft Windows; elles sont proposées d'emblée par les grands assembleurs comme HP ou Dell.

Implémentation VLAN

On trouvera différents types d'implémentations, à savoir :

- Les **VLANs statiques** ou dits "port-based" ou "port-centric" : un port de commutateur apartient "statiquement" à un VLAN. Ce type de configuration nécessite un configuration manuelle de chaque port.
- Les **VLANS dynamiques** : où l'attribution d'un VLANs est effectuée dynamiquement sur base d'une adresse physique (MAC), logique (IP) ou de crédits quelconques (IEEE 802.1X). Ce type d'implémentation est la plus coûteuse … La dernière 802.1X étant un MUST.

Mode des ports “Access”

- Sur un commutateur Cisco, on distinguera les ports dits "access" des ports dits "trunk". Ce n’est pas le cas chez les autres constructeurs.
- **Un port "access" est un port qui ne transportera des informations que d'un seul VLAN.** A priori, ce type de port connectera une station.
- Un port “access” n’ajoute pas d’étiquette au trafic puisqu’il est destiné à une station de travail.

Mode des ports “trunk”

- **Un port "trunk" est un port qui transportera des informations de tous les VLANs.** On y connectera un autre commutateur, un routeur ou même la carte réseau 802.1q d'un serveur.
- Un port “trunk” ajoute des étiquettes au trafic puisqu’il est destiné à un autre commutateur.
- Autrement dit, un port "access" n'est pas un port "trunk" et inversément.
- Toutefois, sur les commutateurs Cisco on aura la possibilité de configurer le port en mode dynamique grâce au Dynamic Trunk Protocol (DTP, protocole point à point propriétaire Cisco).

4. Nomenclature des VLANs

VLAN 1

Le VLAN 1 est un VLAN spécial. Il est le VLAN par défaut de tous les ports, y compris l'interface de gestion (SVI). En plus, une série de protocoles de couche 2 comme CDP (Cisco Discovery Protocol), VTP (VLAN Trunk Protocol), PAgP (Port Aggregation Protocol) et DTP doivent impérativement transiter à travers ce VLAN spécifique. Pour ces deux raisons, le VLAN 1 ne peut jamais être supprimé, il existe d'office.

Types de VLANs (Cisco)

On trouvera quatre types de VLANs :

- VLAN par défaut (Default VLAN)
- VLANs utilisateur (User VLAN)
- VLAN de gestion (Management VLAN)
- VLAN natif (Native VLAN)

Vlan par défaut

Par défaut, le VLAN 1 est celui qui assigné à tous les ports d'un commutateur tant qu'ils n'ont pas été configurés autrement. Cela signifie que tous les autres types de VLANs (utilisateur, gestion et natif) sont membres du VLAN 1.

VLAN utilisateur

On dira que ce type de VLAN est un VLAN "normal" dans le sens où il est celui qui a été configuré pour rendre une segmentation logique du commutateur dans le cadre de l'utilité des VLAN. La numérotation des VLANs est disponible sur 12 bits. Ceci dit, chaque modèle de switch aura ses limites en nombre total à créer et à gérer.

VLAN de gestion

- Le VLAN de gestion est un VLAN spécifique attribué aux commutateurs pour qu'ils soient accessibles via une adresse IP (ICMP, Telnet, SNMP, HTTP).
- Qu'il existe ou non une interface physique appartenant au VLAN de gestion désigné, on joindra le commutateur en IP via une interface virtuelle (SVI) de type VLANx. Tous ports "access" associés à ce VLANx répondent en IP pour l'interface virtuelle VLANx.

Dans les bonnes pratiques de configuration, on le distinguera du VLAN par défaut d'un VLAN utilisateur ou du VLAN natif. Dans le cas d'une tempête de diffusion ou d'un souci de convergence avec Spanning-Tree, l'administrateur devrait toujours avoir accès au matériel pour résoudre les problèmes via ce VLAN. Aussi, une bonne raison de séparer le VLAN de management des autres tient au fait évident de séparer logiquement les périphériques "dignes de confiance" des autres. Il s'agit alors d'appliquer les règles de sécurité nécessaires afin d'éviter, par exemple, que des utilisateurs classiques accèdent au matériel.

VLAN natif

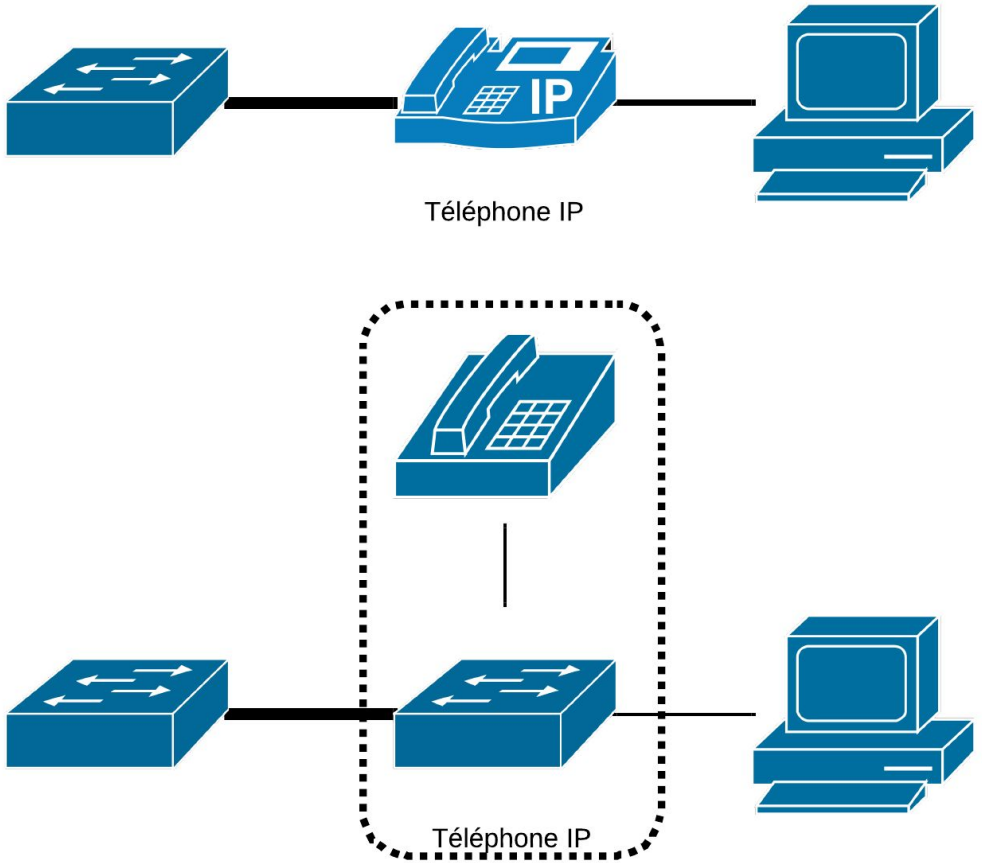
La notion de VLAN natif n'intervient que lorsque l'on configure un port *Trunk*. Quand un port est configuré en tant que tel, le commutateur "étiquette" la trame avec le numéro de VLAN approprié.

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. Ce type de VLAN existe pour assurer une inter-opérabilté avec du trafic ne supportant pas l'étiquetage (*tagging*).

Aussi, les protocoles de contrôles tels que CDP, VTP, PAgP et DTP sont toujours transmis par le VLAN natif. Si on change l'identifiant du VLAN natif, il faut le faire sur toutes les liaisons Trunk, voire sur toute la topologie.

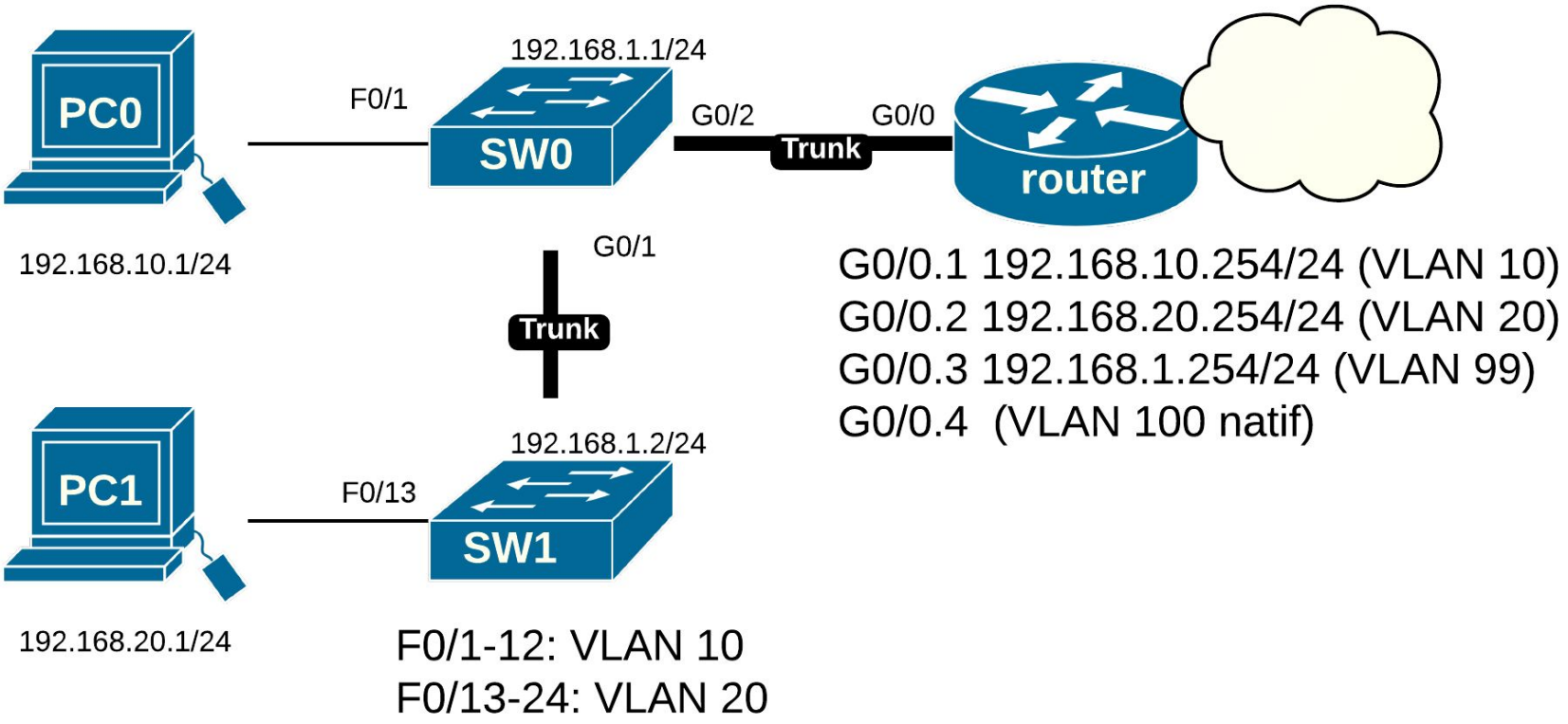
VLAN Voice

Pour assurer la Qualité de Service (QoS) des communications vocales, le VLAN Voice se configure sur un port Access et crée une sorte de mini-Trunk vers un téléphone IP.



5. Configuration des VLANs sous Cisco IOS®

Topologie de base



Création des VLANs

Les VLANs doivent d'abord être créés sur chaque commutateur. Par exemple, le VLAN 10 et pour chaque VLAN :

```
(config)#vlan 10
(config-vlan)#exit
```

Vérification

```
#show vlan
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
                                                Gig1/1, Gig1/2
10   VLAN0010                         active
                                --- Output omited ---
```

L'interface VLANx de gestion (SVI)

L'interface VLANx de gestion (SVI) correspond aux interfaces physique appartenant à ce VLAN (le numéro 10 dans l'exemple) pour le joindre en IPv4 à des fins de gestion (en Telnet, SSH, HTTP ou SNMP). Comme tout périphérique joignable sur le réseau, le commutateur doit posséder une adresse IPv4, un masque et une passerelle.

```
(config)#interface vlan 10
(config-if)#ip address 192.168.10.1 255.255.255.0
(config-if)#no shutdown
(config-if)#exit
(config)#ip default-gateway 192.168.10.254
```

Vérification

```
#show interface vlan 10
                              --- Output omited ---
```

ping vers une destination

Configuration des ports Access

Sous Cisco IOS un port Access est un port qui appartient à un seul VLAN. En option, on peut activer « spanning-tree portfast » qui fait passer le port directement à l'état STP « forwarding » vu qu'il connectera des périphériques de terminaison (qui ne créent pas de boucles)

```
(config)#interface range f0/1 - 20
(config-if-range)#switchport mode access
(config-if-range)#switchport access vlan 10
(config-if-range)#spanning-tree portfast
(config-if-range)#exit
```

Vérification des ports Access

Vérification

```
#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig1/1, Gig1/2
10   VLAN0010                         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
                                  --- Output omited ---
```

Configuration d'un port Trunk

Un port dit *Trunk* est un port qui transporte le trafic appartenant à plusieurs VLANs, tous par défaut sur du matériel Cisco.

```
(config)#int G0/1
(config-if)#switchport mode trunk
(config-if)#exit
```

Vérification

```
#show interfaces G0/1 switchport
                          --- Output omited ---
#show interfaces trunk
                          --- Output omited ---
```

Configuration d'un port Trunk

Commandes supplémentaires

Pour autoriser certains VLANs sur le port Trunk :

```
(config)#int G0/1
(config-if)#switchport trunk allowed vlan 10, 20
```

Pour ne pas placer d'étiquette 802.1q sur un VLAN (VLAN natif) :

```
(config-if)#switchport trunk native vlan 100
(config-if)#exit
```

Configuration du Trunk sur le routeur (Router-on-A-Stick)

Pour que différents VLANs communiquent entre eux, le routage est nécessaire. Le routage peut être assuré par un routeur ou un commutateur de niveau 3. Ici la configuration sur un routeur (configuration Router-on-A-Stick).

```
(config)#interface G0/0
(config-if)#no ip address
(config-if)#no shut
(config-if)#interface G0/0.1
(config-subif)#encapsulation dot1q 10
(config-subif)#ip address 192.168.10.254 255.255.255.0
(config-subif)#exit
(config)#...
(config)#interface G0/0.4
(config-subif)#encapsulation dot1q 100 native
(config-subif)#exit
```

Suppression d’un VLAN

```
(config)#no vlan 10
(config-vlan)#exit
```

Routage avec un commutateur L3

1. Vérifier que votre commutateur est capable de remplir des tâches de routage.
2. Activer le routage IPv4 :

   ```
   (config)#ip routing
   ```

3. Créer les VLANs et les ports Trunks vers les commutateurs d'accès.
4. Pour chaque VLAN à router, création d'une interface VLAN.
5. Éventuellement, activation d'un protocole de routage

6. Dynamic Trunking Protocol (DTP)

Dynamic Trunking Protocol (DTP)

Dynamic Trunking Protocol (DTP) est un protocole propriétaire Cisco (activé par défaut sur les C2960 et C3560) qui négocie aussi bien :

- le statut des ports “*trunk*”
- l'encapsulation des ports “*trunk*”

DTP gère la négociation *trunk* seulement si le port sur l'autre commutateur est configuré dans un *mode trunk* supporté par DTP.

DTP mode “on” et “dynamic auto”

- Par défaut, tous les ports du commutateur sont configurés en **switchport mode dynamic auto**; le commutateur local annonce qu'il est capable de se monter en trunk mais ne demande pas à son correspondant de passer en *mode trunk*. *Après la négociation DTP, le port local termine en mode trunk uniquement si le port correspondant est “on” (trunk) ou "désirable"*. Si le port correspondant est en "auto" ou "access", la négociation aboutit local en mode "access".
- Si le port du commutateur est configuré en **switchport mode trunk**, le port du commutateur envoie régulièrement des messages DTP selon lesquels il est inconditionnellement en *mode trunk*

DTP mode “auto desirable” et “nonegociate”

- Si le commutateur est configuré en **switchport dynamic desirable**, le commutateur local annonce qu'il est capable de se monter en trunk et demande à son correspondant de passer en mode trunk. *Après la négociation DTP, le port local termine en mode trunk si le port correspondant est “on” (trunk) ou "désirable" ou "auto".* Si le port correspondant est en "access", la négociation aboutit local en mode "access". Si le port distant est en non-negociate, le port local reste en mode "access".
- Si le commutateur est en **switchport mode trunk nonegociate**, le port local reste inconditionnellement en mode trunk. Il n'y a aucune négociation. On utilise cette commande pour intégrer au trunking des commutateurs d'autres constructeurs.

DTP tableau récapitulatif

	Dynamic auto	**Dynamic desirable**	**Trunk**	**Access**
Dynamic auto	Access	Trunk	Trunk	Access
Dynamic desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	-
Access	Access	Access	-	Access

7. Virtual Trunking Protocol (VTP)

Virtual Trunking Protocol

- **VTP** est un protocole propriétaire Cisco servant à maintenir la base de donnée de VLANs sur plusieurs commutateurs.
- Tout au plus VTP va-t-il ajouter ou supprimer des ID VLAN ...
- VTP ne permettra en aucun cas de configurer les ports de manière centralisée !

Domaine et rôles

Deux éléments sont nécessaires au bon fonctionnement de VTP :

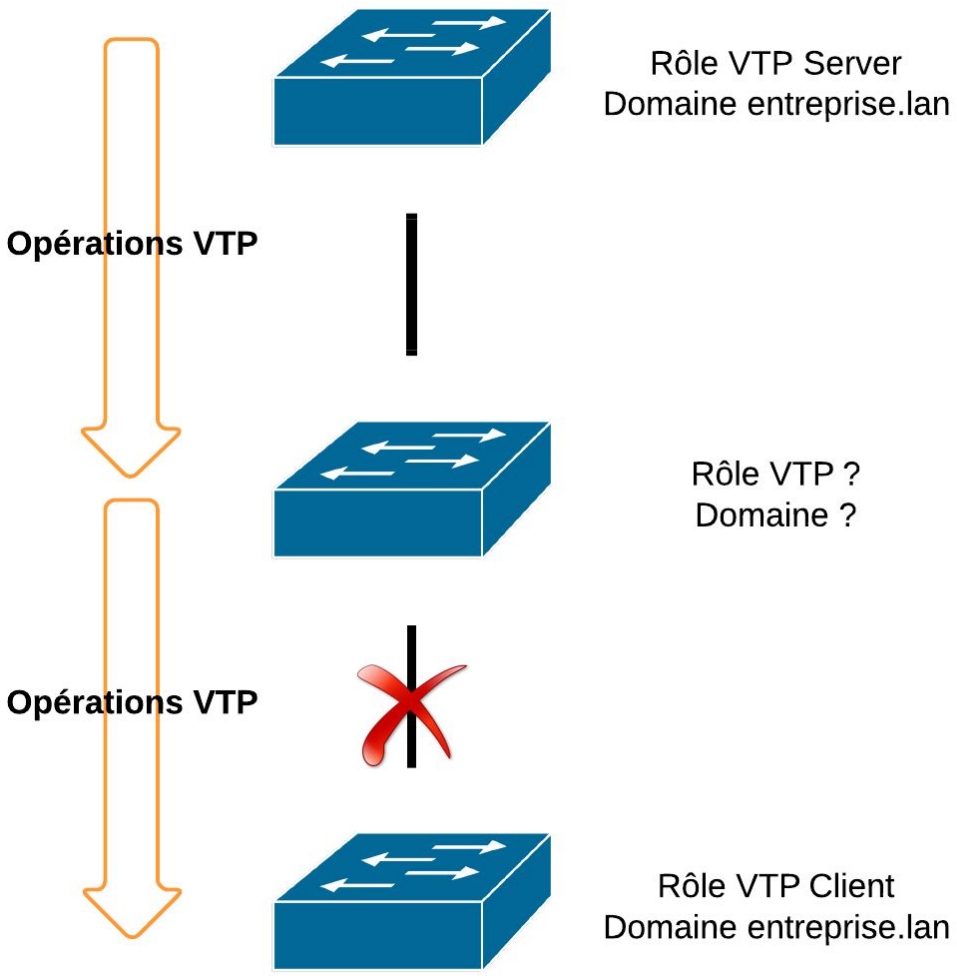
- **Définir un nom de domaine VTP** (appelé aussi domaine de gestion). Ne participent à cette gestion que les commutateurs qui appartiennent à un même domaine.
- Définir pour chaque commutateur un rôle :
  - soit *client*,
  - soit *transparent*,
  - soit, pour un seul d'entre eux, *server*.

Il ne peut y avoir qu'un seul commutateur *server* dans un domaine VTP.

Rôles VTP

Chaque opération à partir du *server* VTP sera répercutée sur les *clients* VTP.

Le mode *transparent* laissera le commutateur indifférent à toutes ces opérations. Mais à quoi sert-il de ce cas ? Simplement, il assure la connectivité VTP du *server* vers les *clients*.



Messages VTP
et numéros de révision

Les messages VTP sont appelés "VTP Advertisements". Ceux-ci ont sont identifiés par un numéro de révision de configuration.

Le numéro de révision le plus élevé sera celui qui modifiera la base de donnée VLAN.

Ce mécanisme maintient les informations VTP à jour dans un domaine.

Configuration de VTP

- Configurer le rôle VTP du commutateur :

  `(config)#`**`vtp {server | client | transparent}`**

- Définir le domaine VTP :

  `(config)#`**`vtp domain`** *`name`*

- Pour configurer un mot de passe (identique sur tous les commutateurs du domaine) :

  `(config)#`**`vtp password`** *`my_password`*

Avant d'intégrer un nouveau commutateurs dans un domaine, on prendra garde d'effacer sa base de donnée VLAN (flash:/vlan.dat) et de le redémarrer en mode *client*. Manipuler VTP dans un environnement en production est déconseillé !

Vérification de VTP (paramètre par défaut)

```
#show vtp status
VTP Version                     : 2
Configuration Revision          : 9
Maximum VLANs supported locally : 255
Number of existing VLANs        : 8
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x13 0xBC 0x6D 0xC9 0xF0 0xF1
0x46 0xC3
Configuration last modified by 0.0.0.0 at 3-1-93 01:03:40
Local updater ID is 192.168.1.1 on interface Vl30 (lowest numbered
VLAN interface found)
```

Mode transparent

Configuration en mode “transparent” :

```
(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
(config)#vtp domain mydomain
Changing VTP domain name from NULL to mydomain
```

Vérification :

```
#show vtp status
```

8. Bonnes pratiques

Meilleures pratiques VLAN

1. Déplacer tous les ports du VLAN 1 dans un autre VLAN.
2. Faire tomber tous les ports inutilisés.
3. Séparer le trafic de gestion de celui des utilisateurs.
4. Changer l'ID du VLAN de gestion dans un autre VLAN que le VLAN 1.
5. Changer l'ID du VLAN natif dans un autre VLAN que le VLAN 1.
6. S'assurer que seuls les périphériques du VLAN de gestion puissent se connecter aux commutateurs.
7. Connexion distante au commutateur uniquement en SSH.
8. Désactiver l'autonégociation sur les ports Trunk.
9. Ne pas utiliser les modes desirable ou auto sur les ports.
10. Désactiver VTP et CDP

Quelle serait la procédure pour appliquer ces principes ?

9. Topologie de lab

Topologie de lab

On vous demande de monter un prototype pour éprouver votre expérience des VLANs avec du matériel Cisco. Vous disposez de deux commutateurs C2960 et d'un routeur ou d'un commutateur multi-couche. Il s'agit d'un exercice portant sur la matière :

- Configuration des VLANs
- Routage inter-VLANs

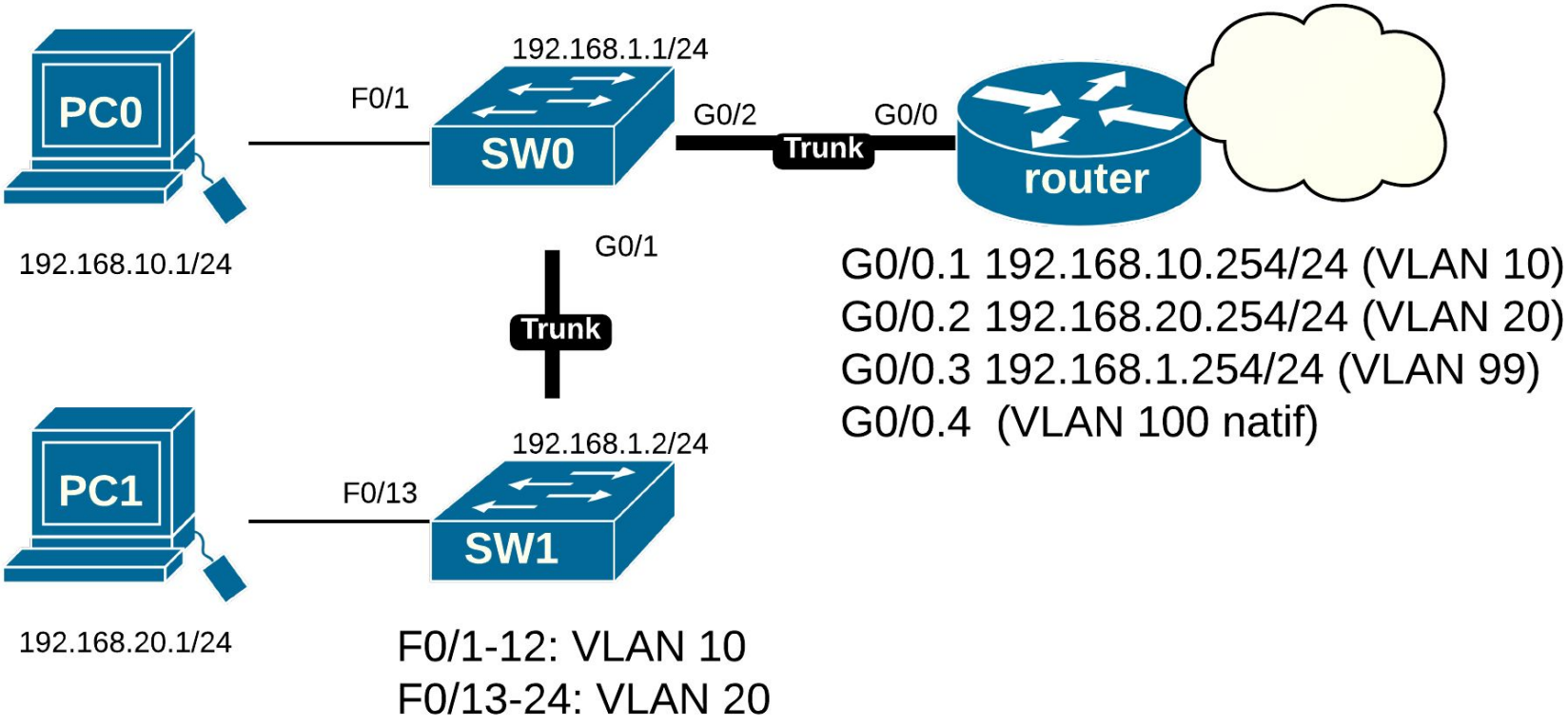
Cette topologie comporte quatre VLANs :

- Un premier VLAN pour la trafic de données dénommé "DATA", prenant l'ID 10.
- Un second VLAN pour le trafic de téléphonie IP dénommé "VOICE", prenant l'ID 20.
- Un Troisième VLAN pour la Gestion des périphériques dénommé "MANAGEMENT", prenant l'ID 99.
- Un dernier VLAN natif qui prend l'ID 100.

Il vous est demandé de configurer cette topologie et d'en faire le diagnostic.

Diagramme

[Le document de lab est disponible sous ce lien.]



Étapes de configuration

1. **Configuration des paramètres globaux**
   a. Configuration statique de l'interface de gestion
   b. Enregistrement
   c. Vérification de la Configuration courante
2. **Création des VLANs sur les commutateurs**
3. **Configuration des ports "access" et "trunk"**
   a. Ports “access” VLAN 10
   b. Ports “access” VLAN 20
   c. Vérification
   d. Ports “trunk”
   e. Vérification
4. **Activation du routage**
   a. Configuration du Trunk
   b. Vérification
   c. Configuration du service DHCP sur le routeur
   d. Configuration d'un commutateur multicouche
   e. Vérification
5. **Configuration des stations de travail**
6. **Diagnostic**
   a. Résumé des commandes diagnostic VLANs

Présentations ICND1/ICND2 sur la commutation LAN

- Technologie Ethernet et commutation
- Prise en main d'un commutateur Cisco©
- Technologies VLANs
- Lab VLANs
- Spanning-Tree et Etherchannel
- Labs VLANs+STP+Etherchannel
- Diagnostic sur le LAN
- Sécurités sur le LAN

Droits