CHAPITRE 4 : Filtrage Niveau 1 de TCP/IP: Segmentation des réseaux

Mohammed SABER

Département Électronique, Informatique et Télécommunications
École Nationale des Sciences Appliquées "ENSA"
Université Mohammed Premier OUJDA

Année Universitaire : 2017-2018

Plan de chapitre

Plan de chapitre

Introduction

- Le système d'information des entreprises contient un ensemble des données de nature différentes et appartient à des services différents.
- Les réseaux locaux permettent aux entreprises de partager localement des fichiers et des imprimantes de manière efficace et rendent possibles les communications internes.
- Les réseaux locaux gèrent les données, les communications locales et l'équipement informatique.
- Pour protéger ou sécuriser la circulation des informations dans le réseau local des entreprises, il faut premièrement segmenter le réseau local.
- Création des zones, pour chaque zone dépend un service.

Introduction

Principe
- Filtrage niveau 1 du modèle TCP/IP ;
- Filtrage niveau 1 et 2 du modèle OSI ;
- Déterminer de l'architecture réseau ;

But
- Réduire les domaines de collision ;
- Réduire les domaines de diffusion ;

Types
- Physique ;
- Logique ;

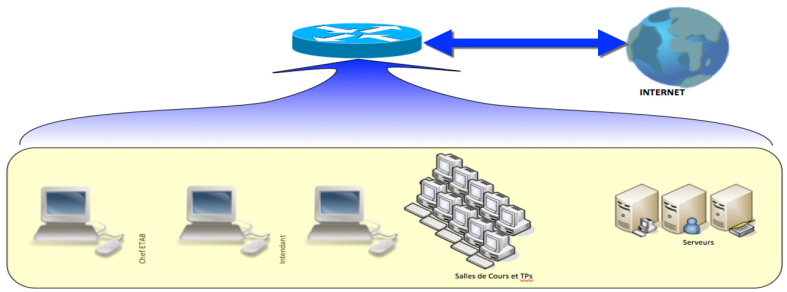
Équipements
- Commutateur (Switch) ;
- Routeur ;

Choix des zones
- Nombre et nature des utilisateurs ⇒ Groupes ;
- Topologie physique du réseau (plan de câblage, géographie, etc.) ;
- Trafic sur le réseau ;
- Ressources sollicités par type d'utilisateur, etc.

Plan de chapitre

La segmentation physique

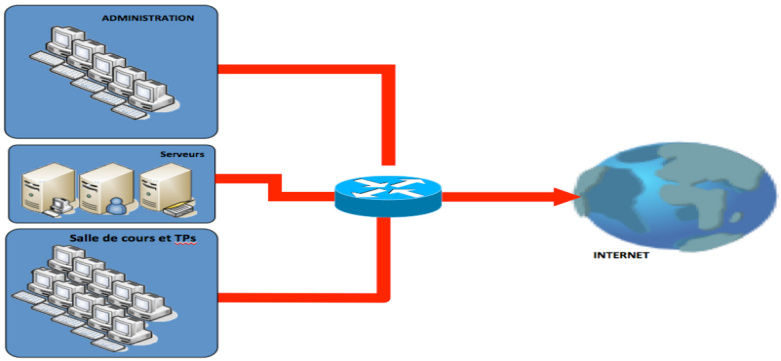
- Exemple d'architecture simple de réseau informatique d'un établissement.



- Mettre toutes les machines dans un même LAN pose plusieurs problèmes de sécurité.

La segmentation physique

- Exemple d'architecture de réseau segmenté.



- Amélioration des performances.
- Segmentation facilite le travail, la gestion et même facilite de mettre en œuvre un système de protection.

La segmentation physique
Création des zones

- La création des zones, nous regroupement les machines qui appartenant au même service ou qui partagent les mêmes données etc ... ;
- DMZ ;
- Les machines libre service ;
- Les services administratifs ;
- La production ;
- Le service commercial ;
- ... ;

Zone DMZ

- DMZ = Demilitarized Zone Area : zone démilitarisé ;
- DMZ = Zone de confinement ;
- Une zone DMZ est une zone moins sûre que le réseau interne ;
- Cette zone va accueillir les services visibles de l'extérieur du réseau : (Web : http, https ; ftp ; Mail ; DNS).
- Elle sera donc la plus vulnérable.
- Pour limiter les dégâts en cas de compression de la DMZ on limitera au maximum les services accessibles depuis la DMZ vers le réseau interne.

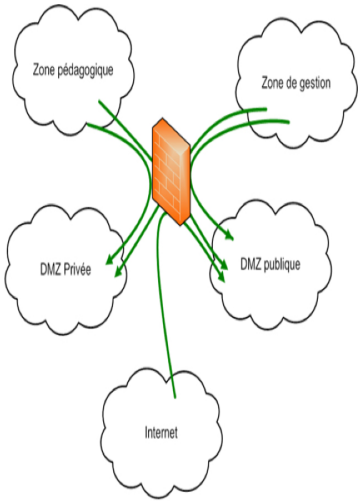
La segmentation physique
Zone DMZ

DMZ privée

- Zone accessible par la pédagogie et par l'administration ;
- **Risques** : malveillance interne ;

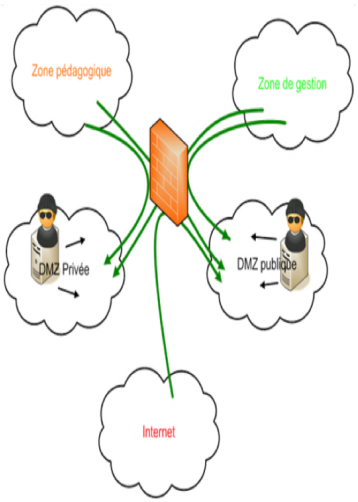
DMZ publique

- Zone accessible par la pédagogie, l'administration et tout internet ;
- **Risques :** malveillance interne et extérieure ;



La segmentation physique
Zone DMZ

- Le pirate risque difficilement atteindre les zones pédagogique et administrative.
- Il ne peut attaquer que les machines dans la DMZ où il a compromis la machine.



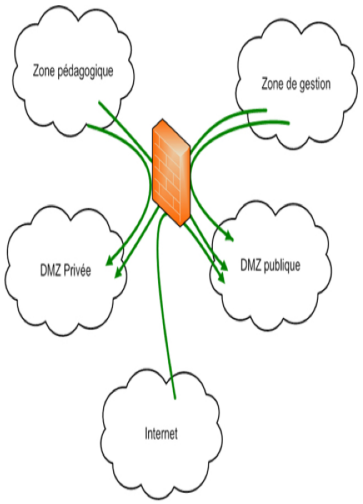
La segmentation physique
Zone DMZ

Zone de gestion

- Seule la gestion peut y accéder.
- Une attaque ne peut survenir que de la zone de gestion (malveillance interne, malwares).
- Exemple de serveur en gestion : horus.

Zone pédagogique

- Seule la pédagogie peut y accéder.
- Une attaque ne peut survenir de la zone pédagogique ou administrative (malveillance interne, malwares).



Plan de chapitre

Qu'est-ce qu'un VLAN ?

- Un réseau local virtuel (VLAN) est un réseau local (LAN) distribué sur des équipements de niveau 2(couche liaison) du modèle OSI (niveau 1 du modèle TCP/IP).
- Un LAN virtuel (ou VLAN) est un groupe de services réseau qui ne sont pas limités à un segment physique ou à un commutateur LAN.
- Les VLAN sont créés pour fournir des services de segmentation habituellement fournis par les routeurs physiques dans les configurations LAN.
- Les LAN virtuels segmentent logiquement le réseau en différents domaines de broadcast.
- Les VLAN segmentent les réseaux commutés de manière logique sur la base des fonctions, des équipes de projet ou des applications de l'entreprise, quel que soitl'emplacement physique ou les connexions au réseau.
- Consiste à créer des réseaux logiques indépendants dans un réseau physique existant :
  - Aucune modification du câblage n'est nécessaire.
  - La prise en charge s'effectue au niveau des switchs.

Qu'est-ce qu'un VLAN ?

- Les machines appartenant à un même VLAN se comportent comme si elles étaient connectées au même réseau physique :
  - Même si elles sont physiquement raccordées à un autre segment du réseau.
  - Ces machines peuvent changer de lieu géographique mais rester dans le même VLAN.
- Les VLAN répondent aux problèmes d'évolutivité, de sécurité et de gestion des réseaux.
- La définition de base étant posée, deux problèmes restent à résoudre :
  - Comment communiquer entre plusieurs réseaux locaux virtuels ?
    - Pour traiter le premier problème, il faut rappeler qu'il est absolument nécessaire de passer par un routeur (niveau réseau du modèle OSI) pour interconnecter plusieurs réseaux locaux.
  - Comment assurer la répartition de plusieurs réseaux locaux virtuels sur plusieurs équipements de niveau liaison ?
    - Pour traiter le premier et le second problème, il est donc nécessaire d'élaborer une technique de partage des réseaux locaux entre équipements.

Remarque

Les commutateurs ne peuvent pas acheminer de paquets entre des VLAN par le biais de ponts.

Les avantages des VLAN

- Segmentation du réseau local flexible :
  - Pouvoir facilement attribuer des autorisations différentes, en fonction des droits et rôles de chaque groupe de personnes.
  - Regrouper les utilisateurs / ressources qui communiquent le plus fréquemment indépendamment de leur emplacement.
- L'administrateur organise son réseau de manière logique et non physique :
  - Faciliter la gestion de la mobilité des postes.
  - Organisation virtuelle, gestion simple des ressources.
  - Modifications logiques ou géographiques facilitées et gérées via une console d'administration plutôt que changer des câbles dans une armoire de brassage.
  - Ajouter ou déplacer facilement les stations de travail (Aucune modification matérielle n'est nécessaire) ;
  - Modifier facilement la configuration du LAN (L'administrateur peut associer n'importe quel port du commutateur à un VLAN sans toucher au câblage) ;
- Sécurité du réseau améliorée :
  - Limiter l'effet des inondations de broadcasts.
  - Partage possible d'une même ressource par plusieurs VLAN.
  - Supprimer la possibilité de communication entre certaines parties du réseau, sécurisé des domaines.

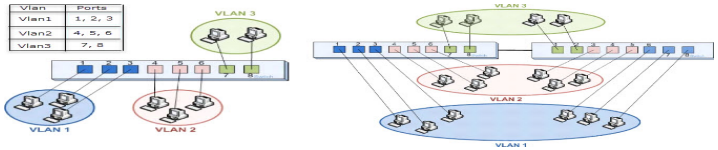
L'appartenance à un VLAN Comment est-elle définie ?

Trois méthodes sont généralement utilisées pour attribuer un équipement à un réseau VLAN :

- Les réseaux VLAN basés sur les ports :
  - VLAN de niveau 1.
  - Les ports d'un switch peuvent être associés à des Vlans différents.
- Les réseaux VLAN basés sur les adresses MAC :
  - VLAN de niveau 2.
  - Le switch lit l'adresse MAC de la machine et l'associe à son VLAN d'appartenance.
- Les réseaux VLAN basés sur les protocoles :
  - VLAN de niveau 3.
  - Le switch lit l'adresse IP de la machine et l'associe à son VLAN d'appartenance.

VLAN niveau 1 ou par port

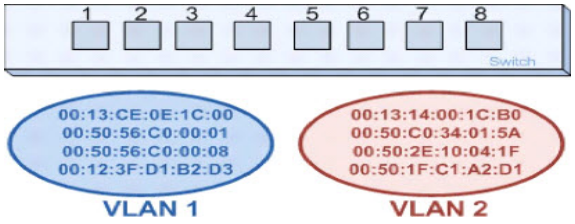
- Un VLAN de niveau 1 (aussi appelés VLAN par port, en anglais Port-Based VLAN) dénommé VLAN statique, est définit un réseau virtuel en fonction des ports de raccordement sur le switch ou commutateur.



- Dans le cadre des réseaux VLAN basés sur les ports, l'appartenance de chaque port du commutateur à tel ou tel réseau VLAN est configurée manuellement.
- L'un des problèmes que posent les réseaux VLAN basés sur les ports est que si le périphérique d'origine est retiré du port pour être remplacé par un autre périphérique, le nouveau périphérique appartiendra au même réseau VLAN que son prédécesseur.
- ***Problème :*** une station ne peut pas changer de VLAN ou appartenir à plusieurs VLAN. Le commutateur assure une isolation complète entre la station et le VLAN auquel il appartient.

VLAN niveau 2 ou par Adresse MAC

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



- Ce type de VLAN est beaucoup plus souple que le VLAN par port car le réseau est indépendant de la localisation de la station.
- Les réseaux VLAN basés sur les adresses MAC permettent de résoudre le problème de changement de port. En effet, dans ce cas, l'appartenance au réseau VLAN dépend de l'adresse MAC du périphérique et non du port de commutation physique. Lorsque le périphérique est retiré pour être connecté à un autre port, son appartenance au réseau VLAN le suit.

VLAN niveau 3 ou par Protocoles

- Un VLAN de niveau 3 (également appelé VLAN par protocoles)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.
- Avec les réseaux VLAN basés sur les protocoles, c'est le protocole de couche 3 transporté par la trame qui permet de déterminer l'appartenance aux réseaux VLAN.
- Cette méthode peut fonctionner dans un environnement où figurent plusieurs protocoles, mais n'est pas très pratique sur un réseau à prédominance IP.
- ***Le problème :*** Exclusion la possibilité d'utiliser DHCP.

Bilan sur les types de VLAN

Types de VLANs	Description
Basé sur le port	▪ Configuration la plus courante ▪ Ports affectés individuellement à un ou plusieurs VLANs ▪ Facile à mettre en place ▪ Couplé à DHCP, les VLAN par ports offrent une bonne flexibilité ▪ Les interfaces de gestion des switchs permettent une configuration facile
Basé sur l'adresse MAC	▪ Rarement utilisé ▪ L'adresse MAC détermine l'appartenance à un VLAN ▪ Les switchs s'échangent leurs tables d'adresses MAC ce qui peut ralentir les performances ▪ Difficile à administrer, à dépanner et à gérer
Basé sur le protocole	▪ Pas utilisé aujourd'hui à cause de la présence de DHCP ▪ L'adresse IP (sous-réseau) détermine l'appartenance à un VLAN

Gestion des VLANs

- La mise en place de VLANs nécessite de disposer d'équipements administrables : Commutateurs ou switch «manageable».
- La base de données des Vlans est la même sur tout le LAN.
- Soit configurée manuellement sur chaque commutateur : La maintenance peut être assez lourde si on souhaite faire évoluer le LAN.
- Soit configurée automatiquement via un protocole propriétaire qui dépend de la marque de l'équipement :
  - Cas du Vlan Trunking Protocol (VTP) de la marque CISCO (Voir plus loin).
  - Le protocole se charge de distribuer sur l'ensemble du LAN les informations sur les VLANs.

Affichage des informations sur les VLANs

- Il est fortement recommandé de vérifier la configuration VLAN à l'aide des commandes ***show vlan***, ***show vlan brief*** ou show ***vlan id id_vlan***.

```
SwitchA#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,
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Numéro de VLAN — Nom de VLAN — Etat de VLAN — Ports appartenant au VLAN

- Les faits suivants s'appliquent aux VLAN :
  - Un VLAN créé reste inutilisé jusqu'à ce qu'il soit associé à des ports de commutateur.
  - Tous les ports Ethernet sont situés sur le VLAN 1 par défaut.

Création des VLANs

- Ajouter un VLAN à la base des données des VLAN d'un commutateur :

```
Switch(config)# vlan vlan_number
Exemple
Switch(config)# vlan 50
```

- OU

```
Switch# vlan database
Switch(vlan)# vlan vlan_number
```

- Ajouter un nom pour le VLAN :

```
Switch(config)# vlan vlan_number
Switch(config-vlan)# name vlan_name
Exemple
Switch(config-name)# name computers
```

- OU

```
Switch# vlan database
Switch(vlan)# vlan vlan_number name vlan_name
```

Création des VLANs

- Afficher les informations sur les VLANs :

```
SwitchA#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,
                                Fa0/23, Fa0/24, Gi0/1, Gi0/2
50   Computers        active
```

VLAN 50 Computers

- Enlever un VLAN entièrement de la base des données des VLAN d'un commutateur :

Switch(config)# ***no vlan*** vlan_number

- OU

Switch# ***vlan database***
Switch(vlan)# ***no vlan*** vlan_number

Affectation des ports au VLAN

- Associer le port d'un switch à un VLAN, on utilisant la commande switch-port (En précisant le numéro de VLAN).

Switch(config)# ***interface Fastethernet*** interface_number
Switch(config-if)# ***switchport mode access***
Switch(config-if)# ***switchport access vlan*** vlan_number

- ***Exemple***

Switch(config)# ***interface*** fa0/1
Switch(config-if)# ***switchport mode access***
Switch(config-if)# ***switchport access vlan*** 50

- Afficher les informations sur les VLANs :

```
SwitchA#show vlan

VLAN Name             Status    Ports
---- ---------------- --------- -------------------------------
--
1    default          active    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,
                                Fa0/23, Fa0/24, Gi0/1, Gi0/2
50   Computers        active    Fa0/1, Fa0/2
```

Ports de VLAN 50

Affectation des ports au VLAN

- Afficher les informations sur un port de VLAN :

```
SwitchA#show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 50 (Computers)
Trunking Native Mode VLAN: 1 (default)
```

Etat de port
Méthode d'accès
VLAN d'appartenance

- Enlever un port d'un VLAN :

Switch(config)# ***interface Fastethernet*** interface_number
Switch(config-if)# ***no switchport access vlan*** vlan_number

Affectation des ports au VLAN

- Associer plusieurs ports de switch à un VLAN, on utilisant la commande :

Switch(config)# ***interface range Fastethernet*** interface_numberDébut - interface_numberFin
Switch(config-if)# ***switchport mode access***
Switch(config-if)# ***switchport access vlan*** vlan_number

- ***Exemple***

Switch(config)# ***interface*** fa0/1 - 15
Switch(config-if)# ***switchport mode access***
Switch(config-if)# ***switchport access vlan*** 50

- Afficher les informations sur les VLANs :

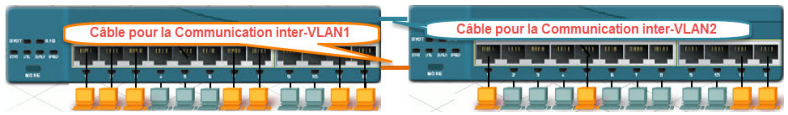
```
SwitchA#show vlan

VLAN Name             Status    Ports
---- ---------------- --------- -------------------------------
--
1    default          active    Fa0/23, Fa0/24, Gi0/1, Gi0/2
50   Computers        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,
```

Ports VLAN 50

Agrégation (Trunking)

- La plupart des VLAN étaient définis sur chaque commutateur, ce qui signifie que la création de VLAN sur un réseau étendu était une tâche complexe.
- Chaque fabricant de commutateur avait une conception différente de la mise en place des VLAN sur leurs commutateurs, ce qui compliquait davantage le processus.
- L'un des problèmes de la configuration "Campus" est qu'il faut transporter plusieurs VLAN à travers deux ou plus switches.

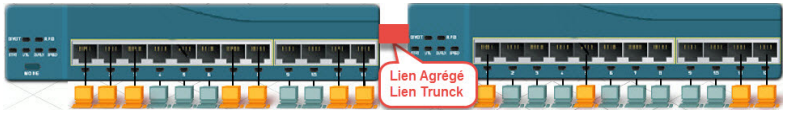
- Comment faire communiquer les hôtes de même VLAN dans les deux switch ?



- Comment faire dans le cas où-il y a plusieurs VLAN sur chaque switch ?

Agrégation (Trunking)

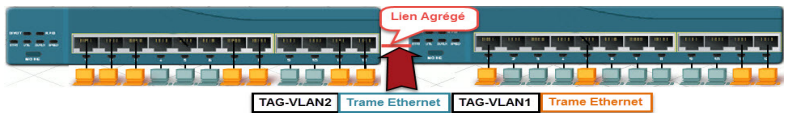
- Le concept d'**agrégation** de VLAN a été développé pour résoudre ces problèmes.



- Est-ce que les trames seront diffuser vers tous les VLANs d'un Switch ? (Non, vers un seul VLAN).
- Comment faire distinguer les trames d'un VLAN sur un lien trunk ?
- Le mécanisme d'agrégation de VLAN permet de définir de nombreux VLAN au sein d'une société en ajoutant des étiquettes spéciales aux trames pour identifier le VLAN auquel elles appartiennent.

Agrégation (Trunking)

- Il existe deux types de mécanismes d'agrégation :
  1. Le filtrage des trames.
  2. L'étiquetage des trames.
- L'étiquetage des trames a été adopté par l'IEEE comme mécanisme d'agrégation standard.
- Chaque trame envoyée sur la liaison est étiquetée afin d'identifier le VLAN auquel elle appartient.



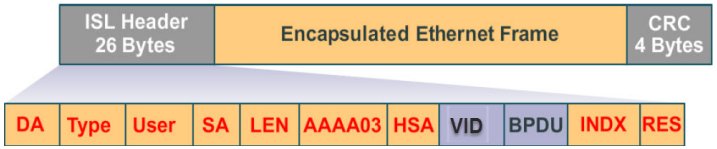
- Le VLAN Tagging est utilisé pour permettre le passage de plusieurs VLAN à travers un seul lien.
- Lien "Trunk" :lorsque les paquets sont reçus par le switch, il les attribue un identifiant unique qui correspond à son VLAN.
- Les paquets de plusieurs VLAN sont ainsi transmis sur le même lien.
- Le paquet est forwardé selon son tag et son adresse MAC.
- En arrivant au switch de destination, le tag est retiré et le paquet est envoyé au destinataire.

Configuration de l'agrégation (Trunking)

- Le VLAN Tagging est fait grâce à une modification de l'entête Ethernet.
- Les systèmes d'étiquetage les plus courants pour les segments Ethernet sont :
  - **ISL (Inter-Switch Link) :** Protocole propriétaire de Cisco
  - **IEEE 802.1Q :** Norme IEEE plus particulièrement traitée dans cette section

VLAN type Cisco Inter-Switch Link (ISL VLAN)

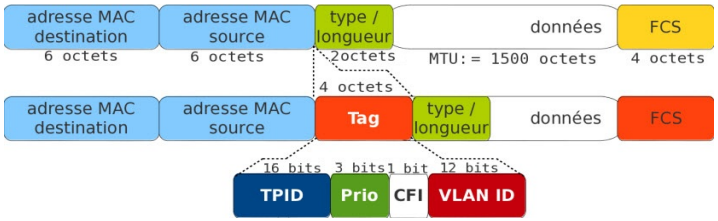
- Technique développée pour les équipements Cisco.
- La trame originale est complètement encapsulée dans des trames ISL :
  - Ajout d'une en-tête de 26 octets et d'une en-queue (CRC) de 4 octets.
  - Support de multiples protocoles de niveau 2 (Ethernet, Token Ring, ATM, FDDI.
  - Support de Spanning Tree (voir chapitre STP).
  - N'utilise pas de VLAN Natif.
- Technique non compatible avec les standards IEEE 802.1Q, il faut configurer le ***même protocole*** sur les ***extrémités*** d'un ***lien trunk***.



- VID : (15 bits) seulement les 10 derniers bit sont utilisés (donc 1024 VLANs)

VLAN IEEE 802.1Q (dot1q)

- Standard qui fournit un mécanisme très répandu, implanté dans de nombreux équipements de marques différentes
- Fonctionnalités de IEEE 802.1Q :
  - Support d'Ethernet et Token Ring.
  - Jusque 4096 VLANs.
  - Les protocoles de Spanning Tree sont supportés.
  - Support des trames non tagé, via le VLAN natif (C'est le VLAN associé au port trunk 802.1Q qui a la capacité de véhiculer les données marquées ou pas par un identifiant de VLAN).
  - Support de la QoS.
- L'en-tête de la trame est complétée par une balise de 4 octets.



Protocoles d'agrégation (Trunking)

- Définir un port d'un switch comme port trunk, on utilisant la commande :

Switch(config)# ***interface Fastethernet*** interface_number
Switch(config-if)# ***switchport mode trunk***
Switch(config-if)# ***switchport trunk encapsulation*** {dot1q ou isl}

- Afficher les informations sur les VLANs :

```
SwitchA#show interfaces fa0/14 switchport
Name: Fa0/14
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
```

Etat de port au niveau de switch A

```
SwitchB#show interfaces fa0/14 switchport
Name: Fa0/14
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
```

Etat de port au niveau de switch B

QUESTIONS ?