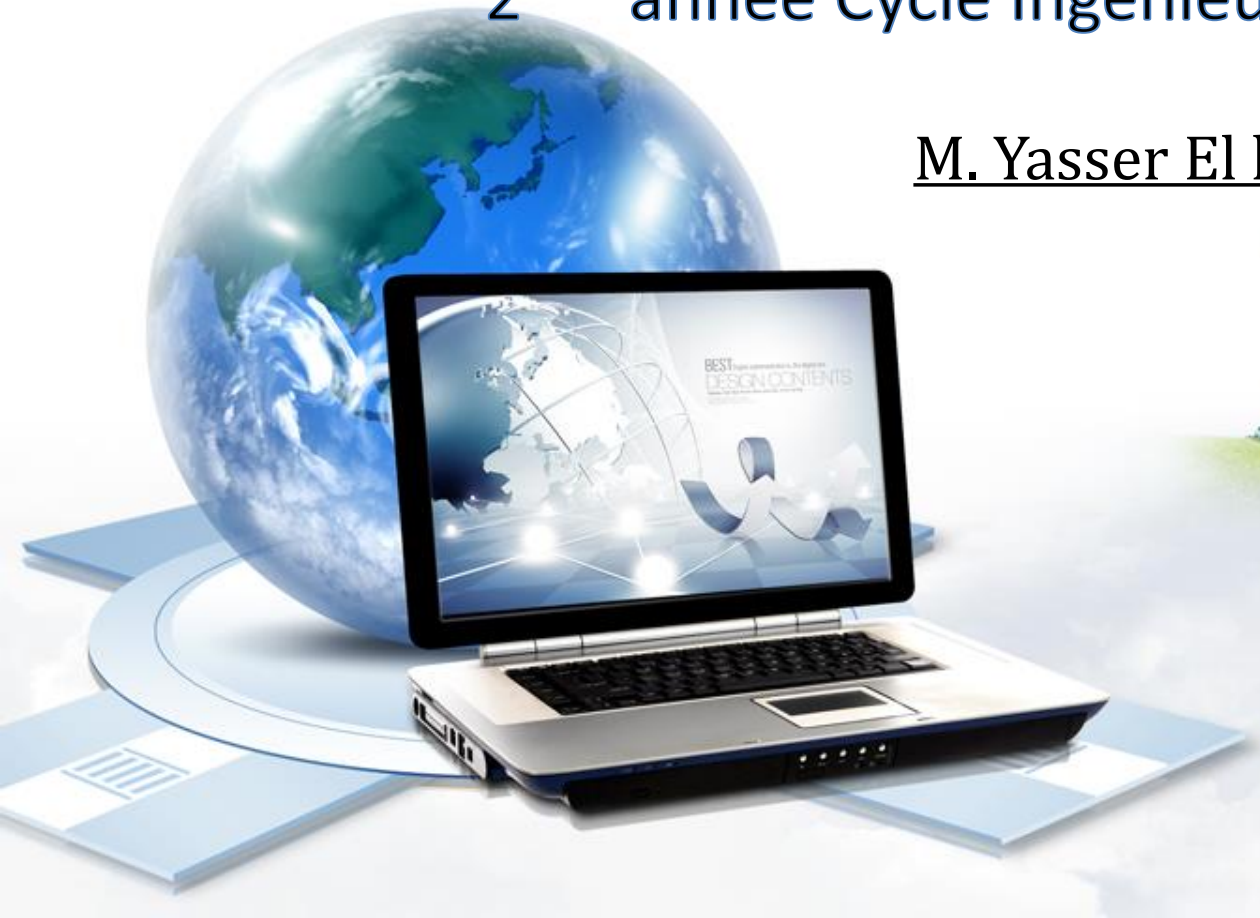
المدرسة الوطنية للعلوم التطبيقية بتطوان
École Nationale des Sciences Appliquées de Tétouan
جامعة عبد المالك السعدي
Université Abdelmalek Essadi

Réseaux informatiques 2

2ème année Cycle Ingénieur GSTR – *P5*

M. Yasser El khamlichi



ENSA Tétouan

VLAN

- Généralités
- Types de VLAN
- Coût d’administration
- L’interface virtuelle
- Communication entre VLAN
- Configuration des VLANs
- VTP
- STP

VLAN

Généralités

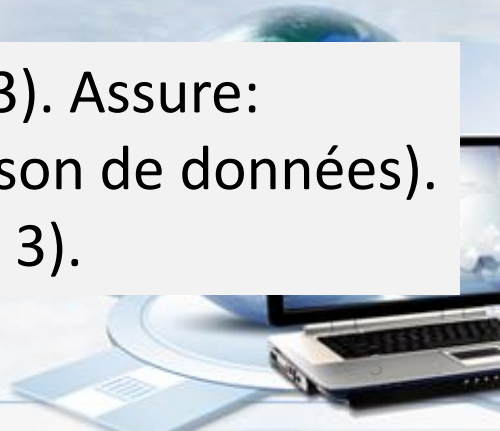
Réseau local virtuel (VLAN : Virtual Local Area Network) :

- Réseau local : technologie Ethernet (ou Wi-Fi).
- Virtuel : dissociation entre la structure matérielle du réseau et la définition logique de réseaux IP.
- Principe : diviser un réseau local (physique) en plusieurs réseaux logiques (IP) appelés VLAN.
- Équipement VLAN : le switch 2-3 ou commutateur-routeur.

Switch 2-3 (commutateur-routeur ou switch niveau 3). Assure:

–Une fonction de commutation Ethernet (niveau liaison de données).

–Une fonction de routage IP (niveau réseau = niveau 3).



VLAN

Généralités

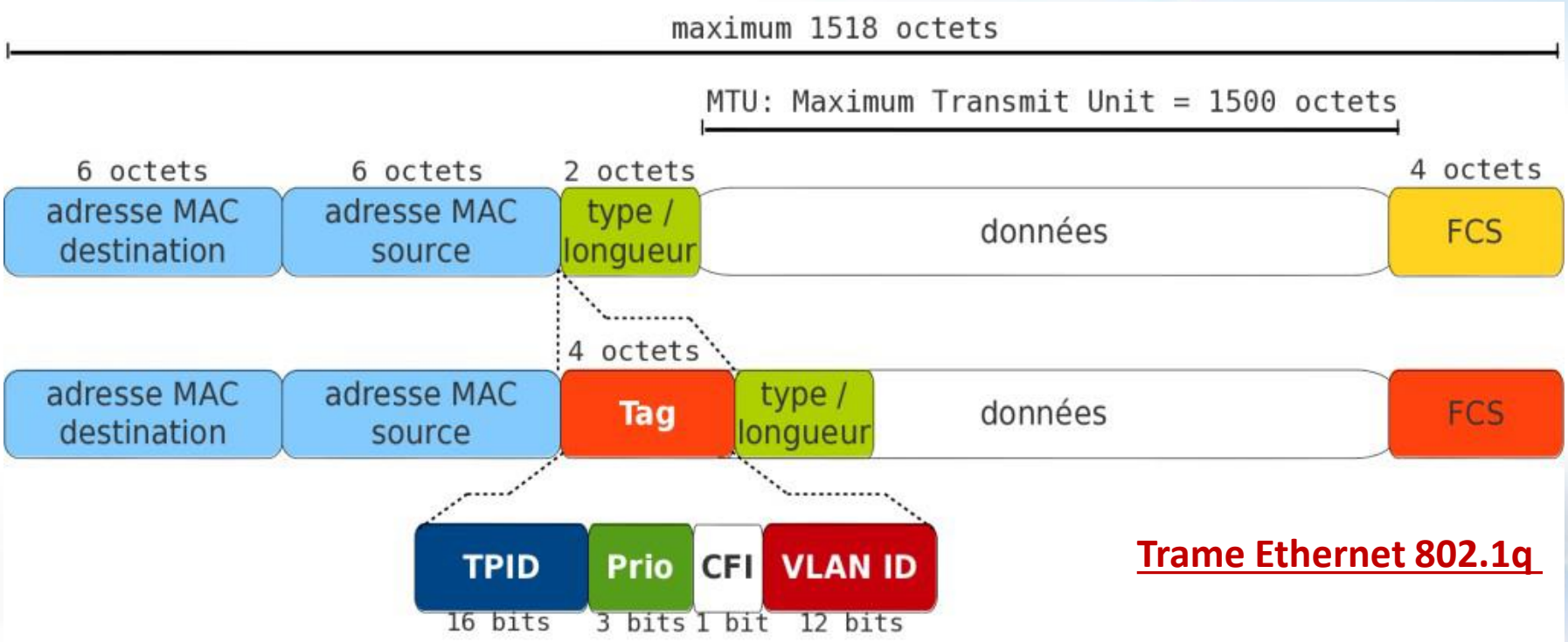
Les VLANS agissent au niveau 2 du modèle OSI et permettent la segmentation d'un support physique en segments logiques.
Ils apportent les avantages suivant:

- limite la diffusion des broadcastes ;
- Une flexibilité de la segmentation et évolutivité plus grande
- Administration centralisée des réseaux
- Une amélioration de la sécurité suite à l'isolation des traffics
- Priorisation des flux.

Un VLAN fonctionne comme un réseau local Ethernet : les stations d'un même VLAN font partie du même réseau Ethernet (et donc du même réseau IP).

VLAN

Généralités:



Trame Ethernet 802.1q

TPID : type de tag, 0x8100 pour 802.1q ; **CFI** : Ethernet ou Token-ring ;
Priorité : niveau de priorité définit par l'IEEE 802.1p ;
VID : Vlan identifier, on peut coder jusqu'à 4096 vlans.

VLAN

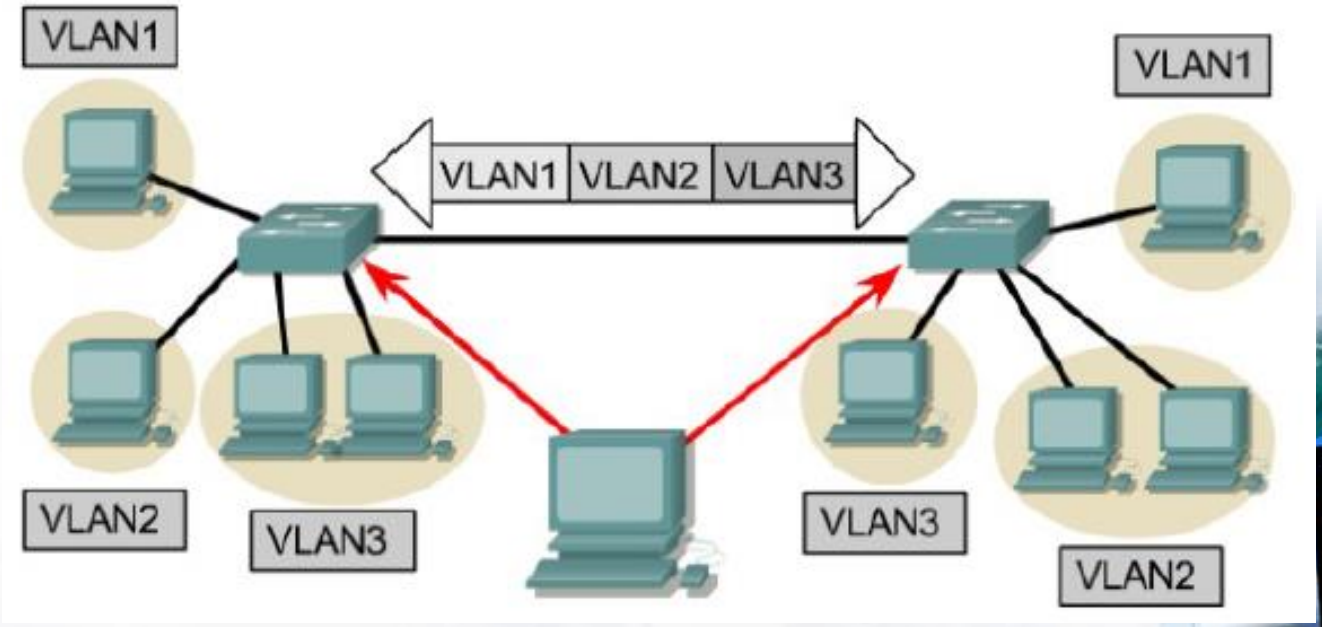
Généralités

- Il faut noter que le champ **FCS** est recalculé après l'insertion de la balise de VLAN.
- Tag protocol identifier, **TPID,** identifie le protocole véhiculé dans la trame. (0x8100 désigne une balise IEEE 802.1Q / 802.1P).
- **Priority** : On peut coder 8 niveaux de priorités de 0 à7. **La notion de priorité dans les VLANs est sans rapport avec les mécanismes de priorité IP au niveau réseau**. Elles sont utilisés pour fixer une priorité aux trames d'un VLAN relativement aux autres VLANs.
- **Canonical Format Identifier** : assure la compatibilité entre les adresses MAC Ethernet et Token Ring. Toujours fixée à 0. Si un port Ethernet reçoit 1, la trame ne sera pas propagée puisqu'elle est destinée à un port «sans balise» (untagged port).

VLAN

Types des VLAN

Il existe différents types de VLAN :
Par port ;Par adresse MAC ;Par adresse IP ;Par protocole de niveau 3.



VLAN

Types des VLAN

VLAN de niveau 1 : En fonction des ports des switch2-3 :

- Mise en place simple sauf si les VLANs sont sur plusieurs switchs (utiliser 802.1q).
- Très bonne sécurité.

VLAN de niveau 2 : Défini par la liste des @MAC des stations :

- Configuration centralisée entre switchs.
- Sécurité moyenne (usurpation d'@MAC)

VLAN de niveau 3 : Défini par son @IP de réseau :

- Appartenance automatique d'une station par son @IP.
- Sécurité faible (usurpation d'@IP) – Processus lent.

VLAN

Types des VLAN

Répartition statique de Vlan niv1 : Le port ne peut appartenir qu'a un seul VLAN défini à l'avance. Par défaut tous les ports sont assignés au VLAN 1 (statique) :

- Les stations d'un même port font toujours partie du même VLAN.
- Les trames échangées entre les stations d'un même VLAN sont des trames Ethernet standard.

Répartition dynamique de Vlan niv1 avec un **identifiant**, dans le cas d'un inter-réseau formé de plusieurs switch2-3 :

- Les ports des switch2-3 sont affectés chacun à un VLAN.
- Les stations d'un même VLAN sont librement réparties.
- Chaque VLAN est identifié par un VLAN ID (VID) sur 12 bits.
- Le protocole 802.1q est activé entre les switch2-3 pour que les trames échangées soient des « tagged frames » comprenant l'en-tête (VID) permettant aux switch2-3 de rediriger correctement les trames..

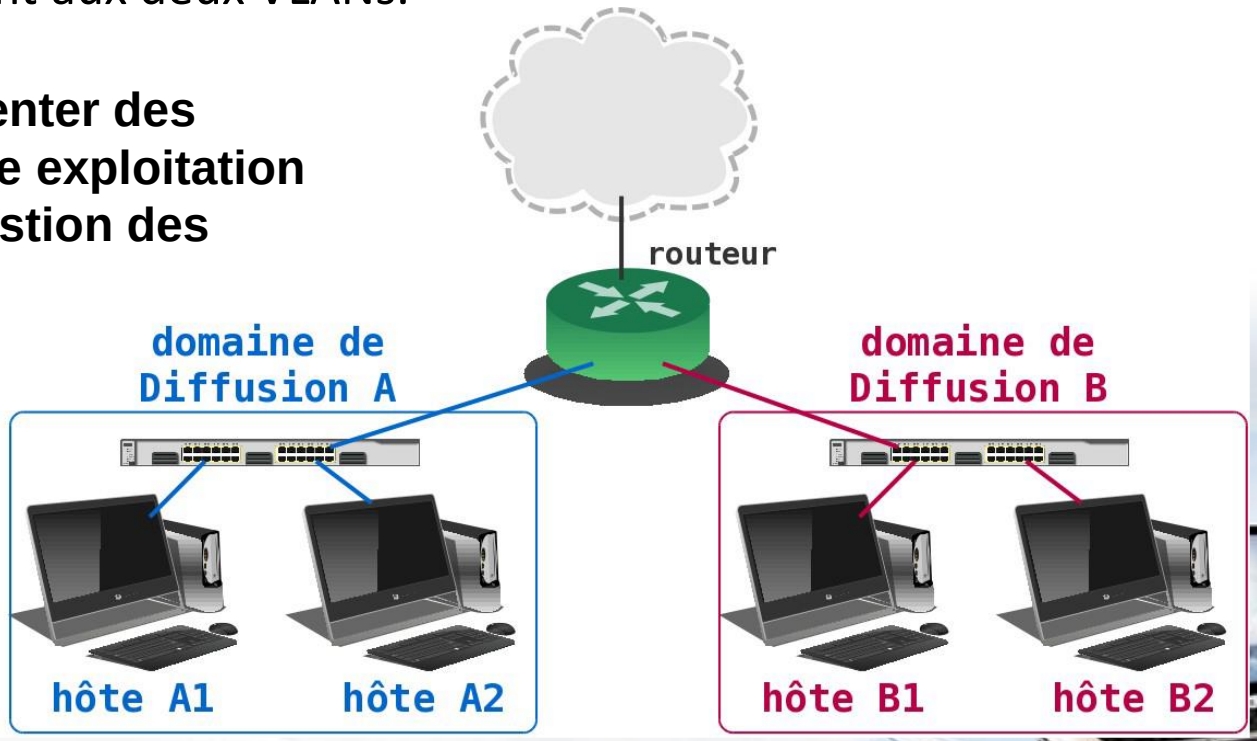
VLAN

Coût d'administration

- Si on programme le commutateur A avec 2 VLANs distincts pour chacun des PCs A1 et A2, alors toute communication entre A1 et A2 sera impossible.
- Ces deux PCs ne pourront communiquer avec d'autres réseaux que si l'interface du routeur RA appartient aux deux VLANs.

Cette situation peut présenter des avantages du point de vue exploitation mais elle dépend de la gestion des interfaces physiques

le coût d'administration devient très important dès que le nombre de réseaux augmente.



VLAN

Coût d'administration

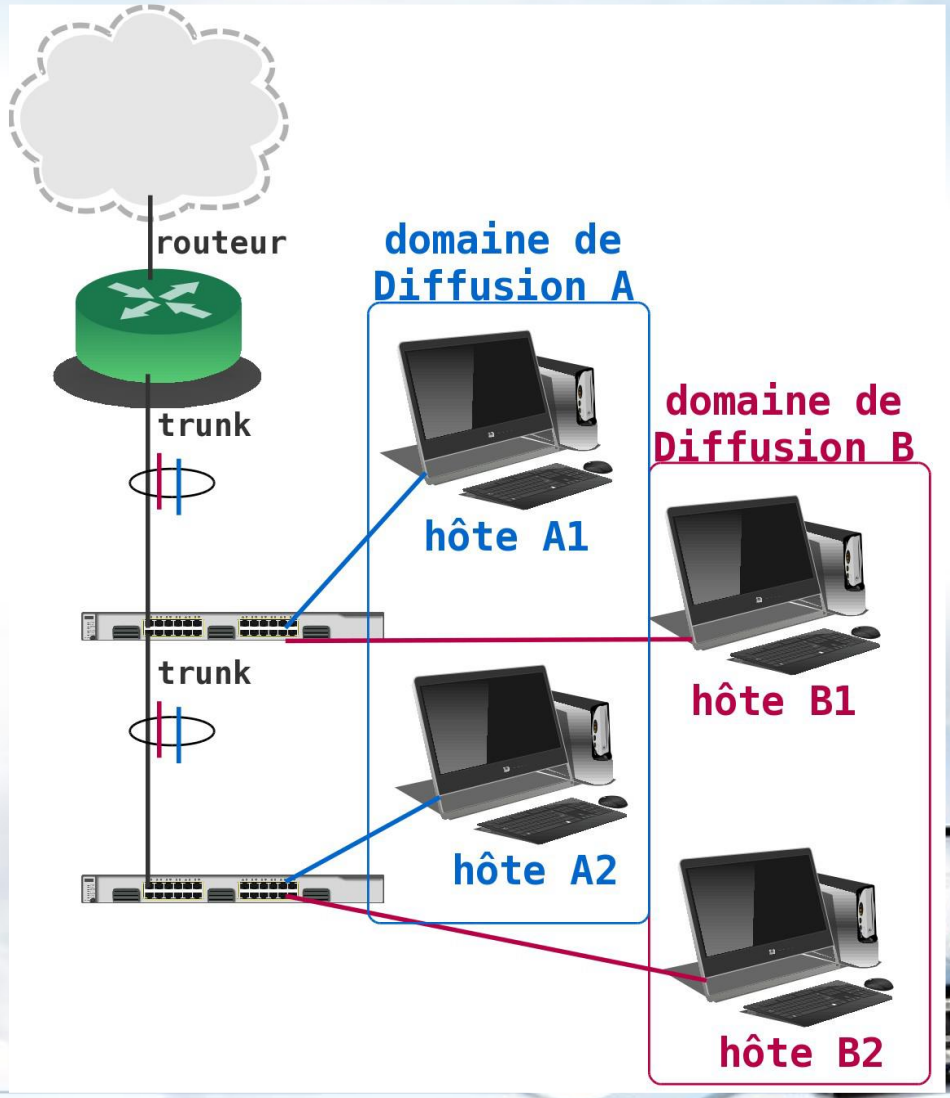
- Si l'utilisateur du PC A1 déménage dans un lieu ou seul le domaine de diffusion B est distribué, il est nécessaire d'étendre le domaine de diffusion A jusqu'à ce nouveau lieu.
- En conséquence, il faudra installer un nouveau commutateur et câbler de nouvelles prises entre le point de brassage principal du domaine A et ce lieu.
- Sur une même infrastructure, on se retrouve rapidement avec des commutateurs saturés pour lesquels tous les ports disponibles sont utilisés et d'autres commutateurs pour lesquels seuls quelques ports sont utilisés.

VLAN

L’ Interface «virtuelle»

On n'associe plus une interface physique à chaque domaine de diffusion mais une **interface «virtuelle»!**

Le contrôle d'accès sera centralisé au niveau du routeur.
On obtient de véritables réseaux locaux distribués sur la totalité de l'infrastructure



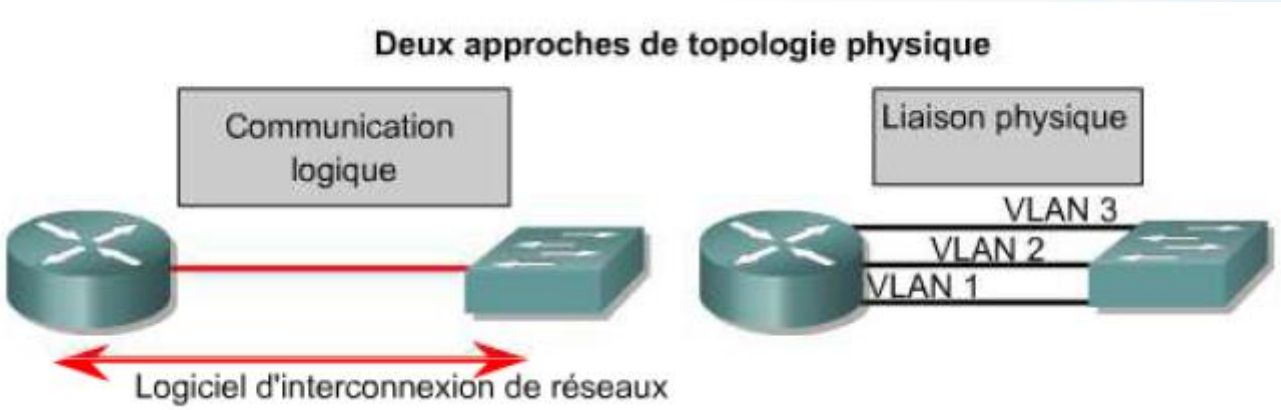
VLAN

L’ Interface «virtuelle»

- On peut noter sur le schéma précédent un nouveau type de lien, ***Trunk***. Ce type de lien peut être placer entre :
- deux commutateurs : c'est le mode de distribution des réseaux locaux le plus courant.
- un commutateur et un hôte : c'est le mode de fonctionnement à surveiller étroitement. Un hôte qui supporte le ***trunking*** a la possibilité d'analyser le trafic de tous les réseaux locaux virtuels.
- un commutateur et un routeur : c'est le mode fonctionnement qui permet d'accéder aux fonctions de routage, donc à l'interconnexion des réseaux virtuels par routage inter-VLAN.
- Les VLANs véhiculés dans le même ***trunk*** **partagent la bande passante** du média utilisé.

VLAN

Communication entre VLANS



La communication entres VLANS se fait au niveau 3 du modèle OSI

Le routage entre interfaces virtuelles ne peut être réalisé que par un routeur, seul apte à modifier le VID associé à une trame.

VLAN

Configuration des VLANS

1. Static access : un port statique peut etre assigné manuellement à un seul VLAN. Par defaut tous les ports sont afféctés au VLAN 1.

2. Multi-VLAN :Un port multi VLAN est configurable manellement et peut etre assigné à 250 VLANs. (ne peut pas etre appliqué avec le mode trunk du switch)

3. Trunk : (802.1q) un trunk est par defaut membre de tous les VLANs dans la base de données des VLANs.

```
config-if# switchport mode xxxxx (access, multi ou trunk)
```

VLAN

Configuration des VLANS

Pour ajouter un VLAN sur un commutateur, entrer les commandes:

Switch# vlan database

Switch(vlan)# vlan 3

Pour affecter un port au vlan crée, on utilise les commandes:

```
Enter configuration commands, one per line. End wi

SydneySwitch#configure terminal
SydneySwitch(config)#interface fastethernet 0/9
SydneySwitch(config-if)#switchport access vlan 300
SydneySwitch(config-if)#exit
SydneySwitch(config)#exit
```

VLAN

Configuration des VLANS

Pour changer l'adresse IP du VLAN par défaut (nommé "VLAN 1")

conf t # int VLAN 1

ip address 100.100.100.100 255.255.255.0

Pour utiliser le mode trunk il faut encapsuler les paquets TCP avec l'un des deux protocoles disponibles : ISL (propriétaire CISCO) ou 802.1q (standard).

#interface FastEthernet 0/4

Passer en mode trunk # switchport mode trunk

Passer en encapsulation 802.1q # switchport trunk encapsulation dot1q

OPTIONNEL :

Ajouter les VLAN 1,2,5 et 6 à la liste des VLAN supportés par le port trunké

switchport trunk allowed vlan add 1,2,5,6

VLAN

VTP

Lorsqu'il s'agit simplement d'un VLAN existant sur deux ou plusieurs switchs différents, on peut éviter de configurer le même VLAN sur tous les switchs, en distribuant la configuration des VLANs sur tous les switchs du domaine.

Le **VTP** (**VLAN Trunk Protocol**) est un protocole propriétaire de CISCO qui est disponible sur la plupart des produits de la famille Catalyst.

Le serveur VTP maintient une liste complète stockée dans NVRAM, de tous les VLAN. Le serveur **peut ajouter, enlever et renommer** les VLAN.

Le client VTP maintient la liste des VLAN reçue du serveur sans la stocker ni la modifier.

Le "transparent VTP" ne participe pas au VTP. Ainsi, il ne tiendra pas compte des messages broadcast VTP. Un VLAN dans ce cas n'est que local sur le switch et est enregistré dans la NVRAM.

VLAN

VTP

Le VTP fonctionne avec des messages multicast envoyés à une adresse MAC particulière (01-00-0C-CC-CC-CC). Ces messages ne circulent qu'à travers des ports trunkés. Ainsi, l'information VTP ne passe qu'à travers un port 802.1q, lorsque le trunk est up.
Les messages VTP ne sont transportés que vers le VLAN1.

Dans le menu *vlan database* :

```
# vtp [client | server | transparent]
# vtp domain 'name‘
```

Exemple, pour configurer un client VTP dans le domaine "test" :

```
# vlan database
# vtp client
# vtp domain test
```

VLAN

VTP

Pour voir les stats a propos du VTP : # sh vtp counters *ou* # sh vtp status

On peut attribuer un mot de passe au domaine VTP dans la "vlan database" :
vtp password mon_mot_de_passe
Ce mot de passe devra être identique sur tous les switchs du domaine VTP.

Les modes de configuration du switch ressemble à ceux du routeur
switch>enable → switch# → configure terminal → switch(conf)#
Pour changer le nom d'hote du Switch: # hostname NOM_SWITCH

Désactiver la recherche DNS
switch(conf)# No ip domain-lookup

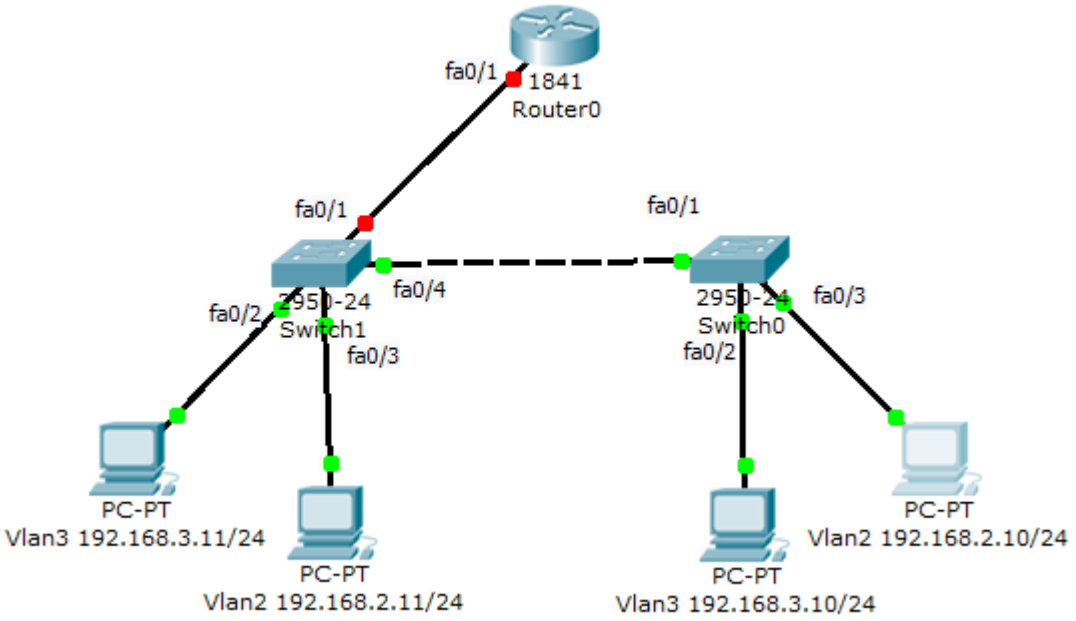
Désactiver le Spanning Tree STP
no spanning-tree vlan 1

Activer Telnet:
conf t
line vty 0 4
password MOTDEPASSE
end

VLAN

VTP

Switch(config)#vlan 10
Switch(config-vlan)#name vlan_10
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name vlan_20
Switch(config-vlan)#vlan 99
Switch(config-vlan)#name Native
Switch(config-vlan)#exit

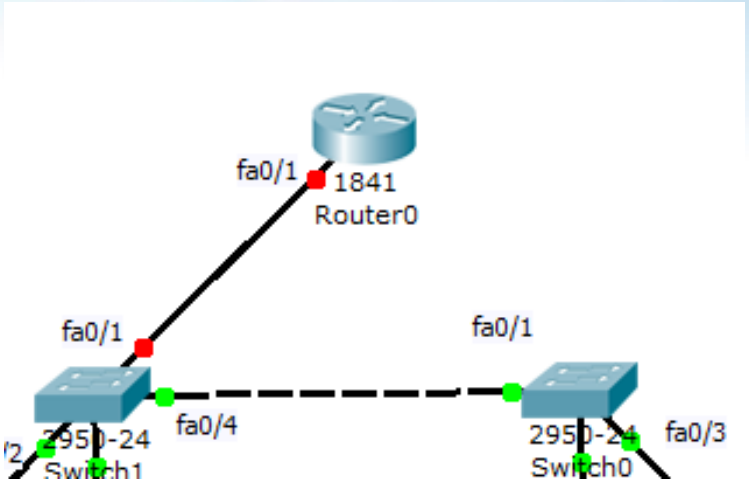


Switch(config)#interface fa0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 20,30,99
Switch(config-if)# switchport trunk native vlan 99
Switch(config-if)#no shutdown
Switch(config-if)#exit

Switch(config)#interface fa0/24

VLAN

VTP

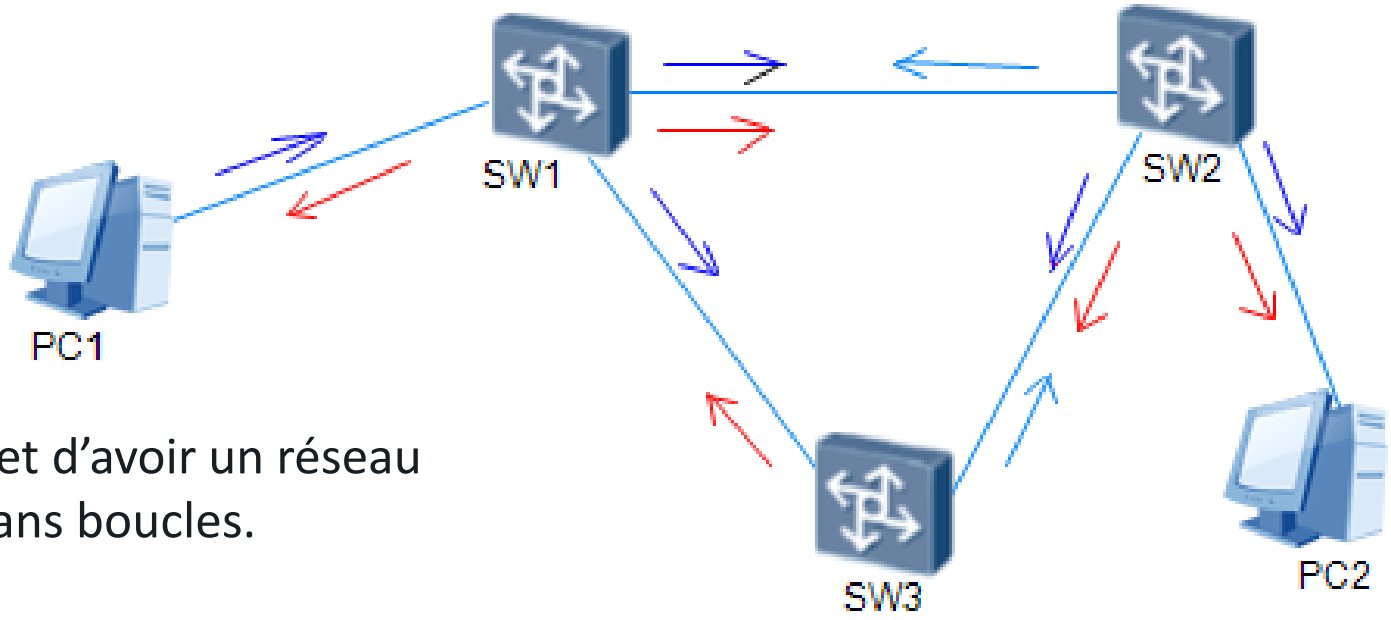



```
Router>enable
Router#configuration terminal
Router(config)#interface fa0/0
Router(config-if)#no shutdown
Router(config-if)#exit

Router(config)#interface fa0/0.2
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.30.254 255.255.255.0
Router(config-subif)#no shutdown
Router(config-subif)#exit

Router(config)#interface fa0/0.1
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.254 255.255.255.0
Router(config-subif)#no shutdown
Router(config-subif)#exit
```

VLAN

STP

Le STP (Spanning Tree Protocol) est un protocole réseau de couche 2. Il apporte une solution au problème posé par la présence de boucles dans les réseaux commutés de type Ethernet. la redondance dans ces réseaux crée des boucles qui génèrent des tempêtes de diffusion (broadcast storm) .Ces boucles saturent le réseau et finissent par le paralyser complètement.



STP nous permet d'avoir un réseau redondant et sans boucles.

VLAN

STP

Le protocole STP utilise des trames de données spéciales appelées BPDU (Bridge Protocol Data Units). Pour permettre aux switchs d'avoir une trace des changements sur le réseau, des BPDU sont échangées toutes les deux secondes sur l'adresse multicast 01:80:C2:00:00:00. Les informations contenues dans les BPDU sont utilisées pour activer ou désactiver les ports selon la topologie réseau requise. Lorsqu'un switch ou un pont est connecté au réseau, il commence par envoyer des BPDU pour déterminer la topologie du réseau, avant de pouvoir transférer des données. Les BPDU sont envoyés sur l'adresse multicast 01:80:C2:00:00:00.

On distingue trois types de BPDU :

CBPDU (Configuration BPDU) : pour le calcul du spanning tree.
TCN BPDU : pour annoncer les changements topologiques.
TCA BPDU : pour l'acquittement de changement de notification de la Topologie

VLAN

STP

Le protocole STP procède en quatre phases :

- Election du commutateur racine (Root Bridge ou RB)
- Détermination du port racine (Root Port ou RP) sur chaque switch
- Détermination du port désigné (Designated Port ou DP) sur chaque segment
- Blocage des autres ports

Etats des ports d'un switch où STP est actif sont :
Listening : le switch écoute les BPDU et détermine la topologie réseau.
Learning : le commutateur construit une table faisant correspondre les adresses MAC aux numéros des ports.
Forwarding : opération normale, le port reçoit et envoie des données,
Blocking : Aucune donnée n'est ni envoyée ni reçue mais le port peut passer en mode forwarding si un autre lien tombe.
Disabled : Le port est désactivé (l'administrateur réseau peut manuellement désactiver un port).

VLAN

STP

Election du commutateur racine (Root Bridge ou RB)

Le Root Bridge est choisi selon le Bridge identifier(BID).Le BID d'un switch est constitué de l'adresse MAC et de la priorité de ce switch. La priorité est un nombre codé sur 12bits (soit une valeur comprise entre 0 et 65535).La priorité est paramétrable par l'administrateur réseau. Par défaut, elle est égale à 32768 (ou 0x8000 en hexadécimal).

Le switch avec la priorité la plus basse est élu Root Bridge, et en cas d'égalité, c'est le switch dont l'adresse MAC est la plus basse qui est élu Root Bridge.

Remarque : Généralement, l'administrateur réseau fixe la priorité de telle sorte que le switch le plus près possible du coeur de réseau soit élu et qu'un autre switch devienne Root Switch en cas de défaillance du Root Bridge principal.

VLAN

STP

Détermination du port racine (Root Port ou RP) sur chaque commutateur
Chaqu'un des switchs restants détermine parmi ses ports actifs un Root Port. Le Root Port est celui qui possède la distance la plus courte (le coût ou cost le moins élevé) vers le Root Bridge. Le coût dépend de la bande passante de chaque lien. En cas d'égalité, c'est le port ayant le port ID le plus faible qui sera élu. Donc, l'élection d'un Root Port est effectuée en tenant compte des champs path cost et Port ID d'un paquet BPDU. En cas d'égalité, c'est le port ayant le port ID le plus faible qui sera élu.

Détermination du port désigné (Designated Port ou DP) sur chaque segment
Pour chaque segment réseau reliant des switchs, un DP (Designated Port) est ensuite déterminé. Le port désigné est le port relié au segment qui mène le plus directement à la racine (somme totale des coûts des différents segments traversés est la plus petite).

VLAN

STP

Blocage des autres ports
Les ports qui ne sont ni RP, ni DP sont bloqués (BP : Blocked Port). Un port bloqué peut recevoir des paquets BPDU mais ne peut pas en émettre.

Changements de topologie
Lorsqu'un lien est coupé ou qu'un switch est hors service, l'algorithme est exécuté à nouveau et une nouvelle topologie est mise en place.

Quand un périphérique est connecté au réseau, son port se mettra automatiquement d'abord en mode listening puis en mode learning et ensuite en mode forwarding.

Forward delay : est le délai de transition entre les modes listening vers learning et learning vers forwarding. Ce délai est fixé par le Root Bridge et vaut quinze secondes par défaut.