



جامعة عبد المالك السعدي  
Université Abdelmalek Essaadi

**Université Abdelmalek Essaadi**  
**Faculté des Sciences et Techniques de**  
**Tanger**



FST  
Tanger

## Administration Réseaux

### (services sous Linux)


Pr. Abdelhamid ZOUHAIR

Intitulé du module	Administration Réseaux
Etablissement dont relève le module	Faculté des Sciences et Techniques de Tanger
Filière	Cycle Ingénieur LSI
Semestre d'appartenance du module	<b>S 4</b>

A. U: 2024/2025

## Plan

- Serveur FTP, Telnet et SSH
- Serveur HTTP Apache
- VPN & OpenVPN
- **VLAN, VTP et STP**
- Configuration des ACLs
- Configuration SNMP
- Serveur NFS et Serveur de fichiers Samba
- Serveur DNS (BIND9)
- Serveur OpenLDAP (Annuaire, authentification et Centralisation des services)
- Serveur d'impression



# Les VLANs



## Les VLANs

### LAN : Problèmes à résoudre

- ❑ Un LAN est un réseau où tous les périphériques sont dans le même domaine de broadcast (adresse de diffusion vers tous les périphériques d'un réseau). Dans un LAN :
  - Chaque élément du réseau peut communiquer avec l'ensemble du réseau sans passer par un routeur.
  - Un switch considère toutes ses interfaces comme étant dans le même LAN et donc dans le même domaine de broadcast.
- ❑ Les Réseaux LAN sont sujets à divers problèmes affectant les performances du réseau, à savoir :
  - Les collisions ;
  - La latence des équipements Réseaux ;
  - La remise des données de type Broadcast ;
  - **Sécurité :**
    - Réseau diffusant.
    - N'importe qui peut '*sniffer*' les trames.





## LAN : Solutions

Afin d'optimiser les performances du réseau ..., la segmentation est nécessaire.

### Solution 1 : Routeurs entre LANs

- Bloquent les broadcasts
- Filtrant les paquets

#### Mais

- Coût élevé ;
- Latence importante (Délai de propagation des trames).

## Solution 2 : avec des réseaux virtuels

➔ Virtualiser le réseau avec des switches

5



## LAN : Solutions

### Solution : réseaux virtuels

➔ Virtualiser le réseau avec des switches

Il n'est pas nécessaire d'avoir des VLAN lorsque vous avez un petit réseau avec très peu de fonctionnalité.

6

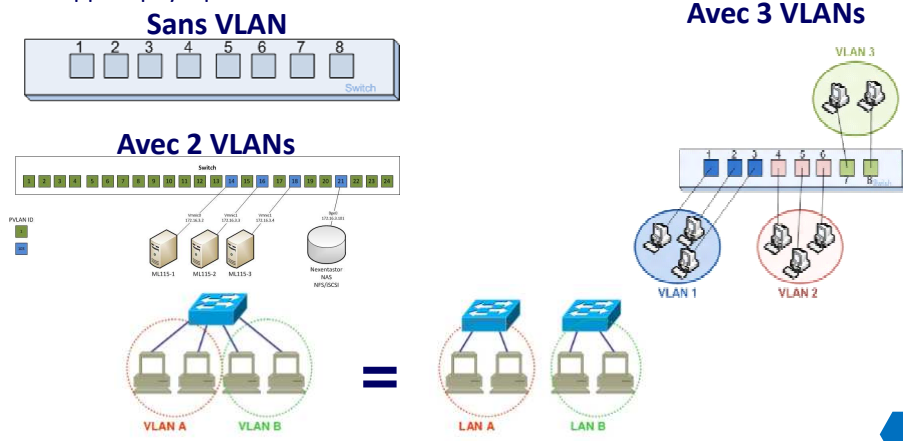
### VLAN = Virtual Local Area Network

- Un **réseau local virtuel**, communément appelé VLAN (pour Virtual LAN), est un réseau informatique logique indépendant.
- Un VLAN est un réseau local regroupant un ensemble de machines de façon logique et non physique.
  - Permettent de regrouper des machines de façon logique sans avoir à tenir compte de leur emplacement sur le réseau.
- Dans un réseau local, la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels (VLANs) il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage, ...) en définissant une segmentation logique basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.).
- Définis par les standards : ([https://fr.wikipedia.org/wiki/IEEE\\_802.1](https://fr.wikipedia.org/wiki/IEEE_802.1))
  - IEEE 802.1Q pour la notion de VLAN
  - IEEE 802.1p pour la qualité de service (QoS)
  - IEEE 802.1v pour la Classification by Protocol and Port

7

### VLAN = Virtual Local Area Network

Avec les VLANs, un switch peut mettre certaines de ses interfaces dans un domaine de broadcast et d'autres dans un autre domaine de broadcast. Un même switch a alors plusieurs domaines de broadcast. Soit plusieurs séparations logiques sur un même support physique.



8

### Les avantages d'un réseau local virtuel (VLAN)

#### ❑ Limiter les domaines de broadcast : Meilleures performances

Le fait de diviser des réseaux linéaires de couche 2 en plusieurs groupes de travail logiques (*domaines de diffusion*) réduit la quantité de trafic inutile sur le réseau et augmente les performances.



#### ❑ La sécurité

Les groupes contenant des données sensibles sont séparés du reste du *réseau*, ce qui diminue les risques de violation de confidentialité.

#### ❑ Réduction des coûts

Des économies sont réalisées grâce à l'utilisation plus efficace de *la bande passante* et des liaisons ascendantes existante.

#### ❑ Atténuation des tempêtes de diffusion

❑ Le fait de diviser un réseau en **plusieurs réseaux VLAN** réduit le nombre de périphériques susceptibles de participer à *une tempête de diffusion*.

#### ❑ Efficacité accrue du personnel informatique

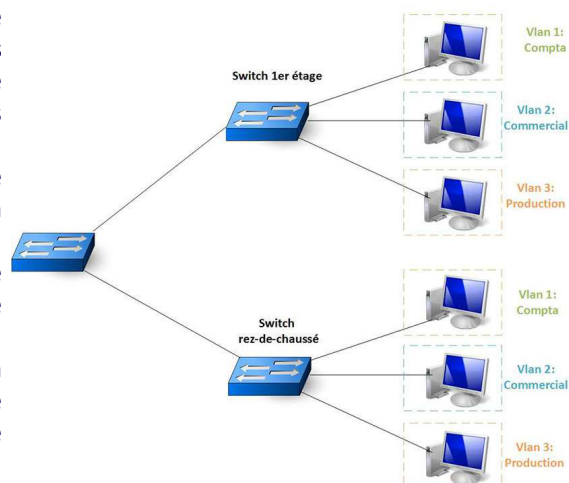
Les **VLAN** facilitent *la gestion du réseau*, car les utilisateurs ayant des besoins réseau similaires partagent le même VLAN.

#### ❑ Permettre la mobilité des utilisateurs

9

### Les avantages d'un réseau local virtuel (VLAN)

- Les VLANs vous permettent de séparer logiquement des départements ou des groupes de travail sans pour autant qu'ils soient séparés physiquement.
- Ainsi on pourra avoir le département comptabilité sur un Vlan, le département commercial sur un autre et de même pour le département production et le département direction.
- Evidemment ce n'est qu'un exemple, le réseau peut être divisé avec n'importe quelle logique voulue.



10

### Les avantages d'un réseau local virtuel (VLAN)

- Les VLANs entraînent un certain niveau de sécurité, particulièrement pour les attaques utilisant le broadcast (**ARP cache poisoning, DHCP spoofing, MAC table overflow...**).
- De plus, des règles de sécurité pourront être ajoutées sur les communications entre les VLANs permettant ainsi d'apporter une nouvelle couche de sécurité à la défense en profondeur de l'entreprise.
- La QoS (Quality of Service) est également simplifiée avec la création de VLANs. Par exemple, si tous les téléphones IP sont dans le même VLAN appelé VoIP, on pourra favoriser le flux venant de ce VLAN.
- Les VLANs sont des configurations essentielles dans un réseau d'entreprise. En effet les VLANs optimisent le réseau et permettent d'implémenter de la sécurité et de la QoS.

11

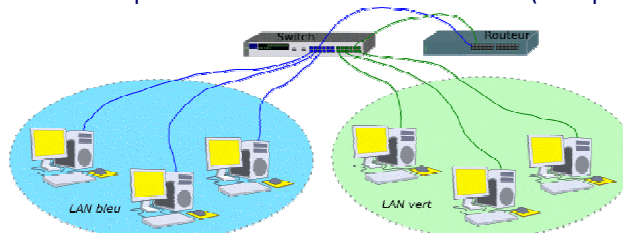
### VLAN: Principe

#### Où intervient le virtuel :

- Un SWITCH appartenait à un et un seul LAN. L'idée de base est de pouvoir assigner certains ports du SWITCH à un LAN, certains autres ports à un autre LAN.



- Sur un même SWITCH physique, nous allons pouvoir créer plusieurs LANS et assigner certains de ses ports aux divers LANS créés. Ici, nous avons un LAN bleu et un LAN vert.
- Comme si l'on avait découpé notre SWITCH en deux morceaux (sans pour autant le détruire).



- Le SWITCH a été virtuellement coupé en deux.

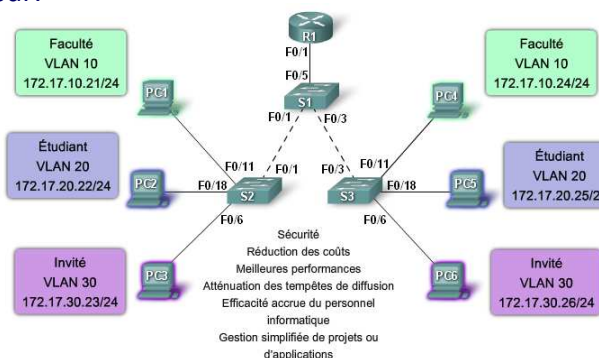
12

### VLAN: Principe (suite)

- Regrouper « logiquement » un groupe de stations dispersées géographiquement.
- Les Vlan permettent aux ordinateurs des différents groupes d'être séparés bien qu'ils partagent la même infrastructure.

Peuvent être regroupés par:

- **Fonction**
- **Services**
- **Application**

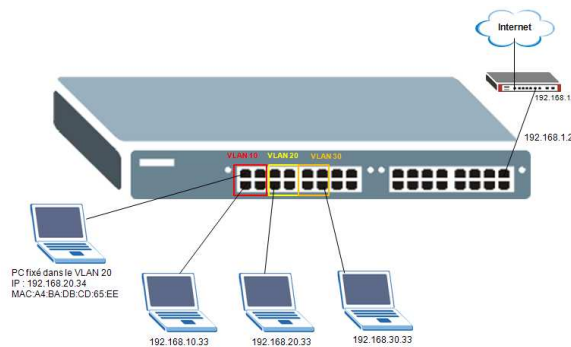


### Différents types de VLANs

- ☐ **Par ports de commutateur :** (Couche 1 : Port par Port)
  - Evolution : VLAN sur un seul Switch, puis VLAN inclus dans plusieurs switches
  - Contrainte : reconfigurer le VLAN en cas de changement de port pour un Hôte.
- ☐ **Par @ MAC :** (Couche 2 : Filtrage par @ MAC)
  - Identifie un VLAN en fonction de l'adresse MAC des postes ;
  - On indique directement les adresses MAC des cartes réseaux contenues dans les machines que l'on souhaite voir appartenir à un VLAN.
- ☐ **Par @IP : niveau 3** (Filtrage par protocole réseau)
- ☐ **Les VLAN de protocoles**
- ☐ **Les VLAN par règles**



### VLAN de niveau 1 (ou VLAN par port)



15

### VLANs par Port (niveau 1)

- ☐ VLAN par ports (Port Based VLAN).
- ☐ Consiste à affecter certains ports du commutateur à un numéro de VLAN.
- ☐ Simplicité de la mise en oeuvre :
  - Le VLAN peut être réparti sur plusieurs commutateurs grâce aux :
    - échanges d'informations entre commutateurs.
    - marquage des trames.
- ☐ Toutefois la configuration des switches est **statique**.
  - Elle doit être faite « à la main » switch par switch.
  - Tout déplacement d'un poste nécessite une reconfiguration des ports.

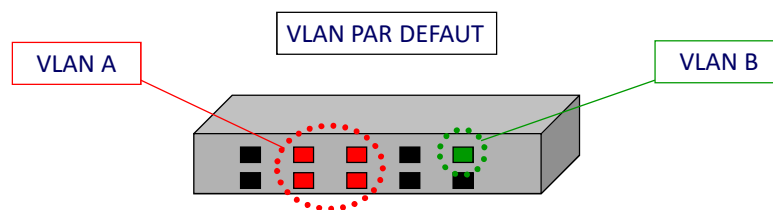
16



### VLANs par Port (niveau 1)

VLAN de niveau 1 ⇔ VLAN par port

- 1 port du switch dans 1 VLAN
- configurable au niveau de l'équipement
- 90% des VLAN sont des VLAN par port



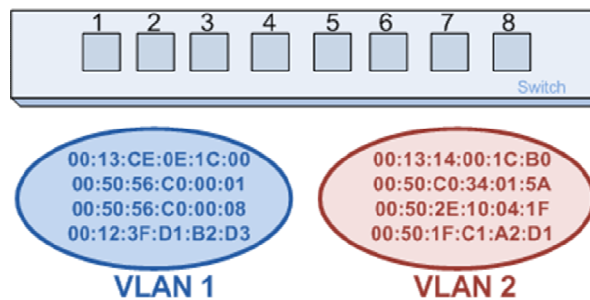
17

### VLANs par Port (niveau 1)

- Actuellement, 90% des VLAN sont des VLAN par port (ils sont configurés statiquement : en effet, nous affectons les ports du commutateur à des Vlan particuliers).
- Les utilisateurs ont accès à certaines ressources en fonction du Vlan auxquels ils appartiennent.
- L'**avantage** des Vlan statiques est qu'ils sont faciles à mettre en œuvre.
- L'**inconvénient** majeur des Vlan statique est que si l'utilisateur se connecte à un port du commutateur affecté à un autre Vlan, celui-ci appartient à un autre Vlan et par conséquent n'a pas accès aux mêmes ressources et n'a pas les mêmes droits.
- Les Vlan statiques sont de moins en moins appropriés aux utilisateurs d'aujourd'hui qui se déplacent au sein des locaux de leur entreprise, changent de bureau et souhaitent conserver les mêmes conditions de travail où qu'ils soient.

18

## VLAN de niveau 2 (ou VLAN MAC)



19

## VLANs par @ MAC : (niveau 2)

- ☐ VLAN d'adresses MAC (MAC Address Based VLAN).
- ☐ Associe des stations au moyen de leur adresse MAC (adresse IEEE) en regroupant ces adresses dans des tables d'adresses.

Principe : Comme l'adresse MAC d'une station ne change pas, on peut la déplacer, physiquement sans avoir à reconfigurer le VLAN.

- ☐ Bien adaptés à l'utilisation de stations portables.
- ☐ Configuration fastidieuse :
  - Impose de créer et maintenir la table des adresses MAC des stations participant au VLAN de manière statique (switch par switch).
  - Comme cette table doit être partagée par tous les commutateurs, cela crée un trafic supplémentaire sur le réseau : (overhead).

20

### VLANs par @ MAC (ou VLAN MAC)

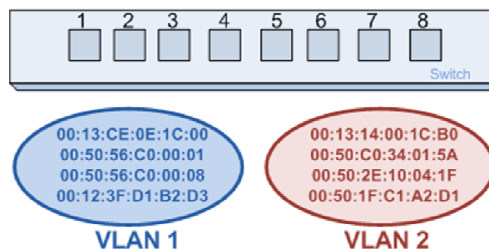
#### VLAN de niveau 2 ⇔ VLAN par adresse MAC

- L'appartenance d'une trame à un VLAN est déterminée par son adresse MAC.
- En fait il s'agit, à partir de l'association Mac/VLAN, d'affecter dynamiquement les ports des commutateurs à chacun des VLAN en fonction de l'adresse MAC de l'hôte qui émet sur ce port.
- L'intérêt principal de ce type de VLAN est l'indépendance vis-à-vis de la localisation géographique. Si une station est déplacée sur le réseau physique, son adresse physique ne changeant pas, elle continue d'appartenir au même VLAN (ce fonctionnement est bien adapté à l'utilisation de machines portables).
- Si on veut changer de Vlan il faut modifier l'association Mac / Vlan.

21

### VLANs par @ MAC (ou VLAN MAC)

- Les VLANs de niveau 2 ou VLAN MAC associent des stations par leurs adresses MAC selon les tables d'adresses introduites par l'administrateur.



- Ici l'on indique directement les adresses MAC des cartes réseaux contenues dans les machines que l'on souhaite voir appartenir à un VLAN, cette solution est plus souple que les VLAN de niveau 1, car peu importe le port sur lequel la machine sera connectée, cette dernière fera partie du VLAN dans lequel son adresse MAC sera configurée

22

### VLANs par @ MAC (ou VLAN MAC)

#### Les avantages du VLAN par adresse MAC:

- Filtrage requis: impact sur les performances
- Echange des tables d'adresses des VLANs entre les commutateurs..

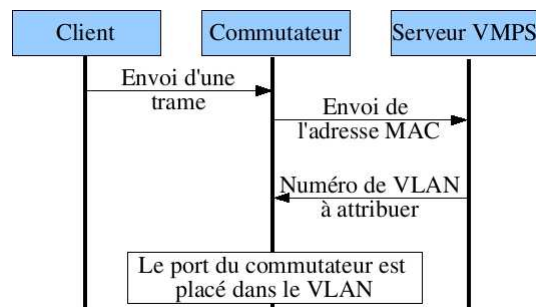
#### Les inconvénients:

- grosses difficultés d'administrations à l'échelle d'un campus.

23

### VLANs par @ MAC : Configuration

La gestion de Vlan est devenu fastidieuse sur grand site hétérogène, il a alors fallu trouver une solution pour automatiser cette gestion. Le **VMPS (Vlan Membership Policy Server)** est un service, crée par Cisco, chargé de faire correspondre un Vlan à une (ou plusieurs) adresse Mac et s'impose donc comme l'une des solutions.



Principe de fonctionnement du **VMPS**

24

### Marquage ou l'étiquetage de trames

- Un commutateur peut gérer plusieurs VLAN et un même VLAN peut être géré par plusieurs commutateurs. L'appartenance d'une trame circulant entre les différents commutateurs devra donc être déterminée pour savoir à quel VLAN elle appartient.
- **Le marquage (protocole 802.1q)**  
Pour savoir à quel VLAN appartient telle ou telle trame, il est nécessaire de les repérer. C'est le rôle du **marquage ou de l'étiquetage de trames** : il attribue à chaque trame un code d'identification de VLAN unique.
- Plusieurs protocoles de gestion des VLAN sont proposés par les constructeurs tels que : **VTP (Vlan Trunk Protocol)** de CISCO, **GARP (Generic Attribute Registration Protocol)**, ou **GVRP (Generic – ou GARP - Vlan Registration Protocol)**
- Ceci permet à une station de déclarer son appartenance à un VLAN et maintient sur les commutateurs une base de données des ports membres du VLAN.

25

### Marquage ou l'étiquetage de trames

**Le marquage peut être :**

- **Implicite (VLAN non taggé – *untagged VLAN*), dans le cas où l'appartenance à tel ou tel VLAN peut être déduite de l'origine de la trame (VLAN par port) ou des informations normalement contenues dans la trame (adresse MAC, adresse IP ou protocole) ;**
- **Explicite (VLAN taggé – *tagged VLAN*), dans le cas où un numéro de VLAN est inséré dans la trame.**

En effet, dès lors qu'il s'agit de faire circuler la trame à travers plusieurs commutateurs ou routeurs, on doit gérer son appartenance à tel ou tel VLAN. On utilise en effet la commutation à l'intérieur du VLAN, mais pour les interconnecter, on doit utiliser des routeurs ou des commutateurs supportant les fonctions de routage.

26

### Marquage ou l'étiquetage de trames

Tout dépend alors du niveau de VLAN :

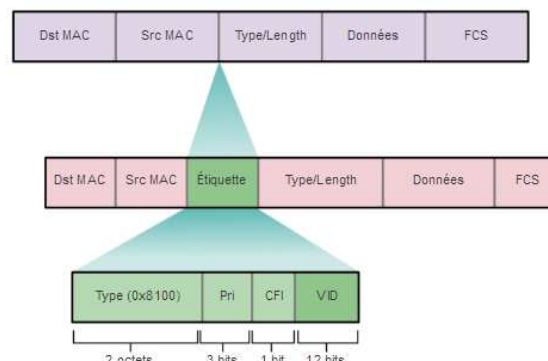
- dans le cas d'un **VLAN par port**, la trame ne conserve normalement pas, d'information sur son appartenance à tel VLAN. Il est donc nécessaire de mettre en oeuvre un marquage explicite des trames si on veut la faire circuler entre plusieurs commutateurs,
- dans le cas d'un **VLAN par adresse MAC**, on peut envisager de distribuer sur tous les commutateurs concernés la table de correspondance entre adresses MAC et numéros de VLAN.
- C'est une solution lourde à laquelle on peut préférer un marquage explicite,
- dans le cas d'un **VLAN de niveau 3** le marquage est implicite et il n'est donc pas nécessaire de marquer les trames qui transitent entre commutateurs.

Toutefois, l'analyse des trames dégradant les performances, il peut être, là encore, préférable de les marquer explicitement.

27

### Marquage ou l'étiquetage de trames

- L'en-tête 802.1Q inclut une étiquette de 4 octets insérée dans l'en-tête d'origine de la trame Ethernet, indiquant le VLAN auquel la trame appartient.
- Lorsque le commutateur reçoit une trame sur un port configuré en mode d'accès et associé à un VLAN, il insère une étiquette VLAN dans l'en-tête de trame, recalcule la séquence de contrôle de trame, puis envoie la trame étiquetée par un port trunk.



28

### Marquage ou l'étiquetage de trames

#### Détails du champ de l'étiquette VLAN

L'étiquette VLAN se compose d'un champ Type, d'un champ Priorité, d'un champ CFI (Canonical Format Identifier) et d'un champ d'ID de VLAN :

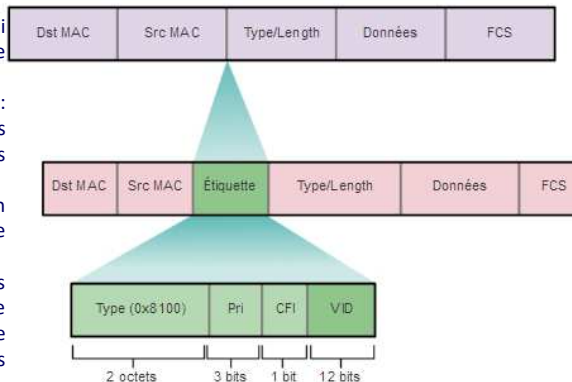
**Type** : valeur de 2 octets appelée ID de protocole d'étiquette (TPID). Pour Ethernet, elle est définie sur une valeur hexadécimale 0x8100.

**Priorité utilisateur** : valeur de 3 bits qui prend en charge l'implémentation de niveaux ou de services.

**CFI (Canonical Format Identifier)** : identificateur de 1 bit qui active les trames Token Ring à transmettre sur des liaisons Ethernet.

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

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

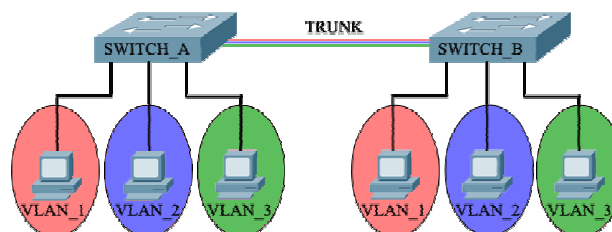


Champs d'une trame Ethernet 802.1Q

29

### Trunks de VLAN

- Dans le contexte de VLANs, un lien de réseau supportant des VLANs multiples entre 2 commutateurs ou entre un commutateur et un routeur est appelé « **trunk** ».
- Un trunk est une liaison point à point entre deux périphériques réseau qui transporte plusieurs VLAN. Un trunk de VLAN permet d'étendre les VLAN à l'ensemble d'un réseau. Cisco prend en charge la norme IEEE 802.1Q pour la coordination des trunks sur les interfaces Fast Ethernet, Gigabit Ethernet et 10 Gigabit Ethernet.
- Dans le cas où une trame Ethernet doit être transportée d'un commutateur à un autre, sur un lien « trunk », il est nécessaire de connaître le VLAN auquel elle appartient. C'est ce qu'on appelle le marquage des trames (tag en anglais). L'étiquetage permet de reconnaître le VLAN d'origine d'une trame.



30

### Trunks de VLAN

- Sans trunks de VLAN, les VLAN ne serviraient pas à grand-chose. Les trunks de VLAN permettent à tout le trafic VLAN de se propager entre les commutateurs, de sorte que les périphériques du même VLAN connectés à différents commutateurs puissent communiquer sans l'intervention d'un routeur.
- Un trunk de VLAN n'appartient pas à un VLAN spécifique, mais constitue plutôt un conduit pour plusieurs VLAN entre les commutateurs et les routeurs. Un trunk peut également être utilisée entre un périphérique réseau et un serveur ou un autre périphérique équipé d'une carte réseau 802.1Q appropriée.
- Par défaut, sur un commutateur Cisco Catalyst, tous les VLAN sont pris en charge sur un port trunk.
- La liaison physique unique (trunk) entre les deux commutateurs est capable de transporter le trafic pour n'importe quel VLAN. Pour cela, chaque trame envoyée sur la liaison est étiquetée afin d'identifier le VLAN auquel elle appartient.
- L'identificateur est interprété et examiné par chaque commutateur avant tout broadcast ou transmission à d'autres commutateurs, routeurs ou équipements de station d'extrémité.

31

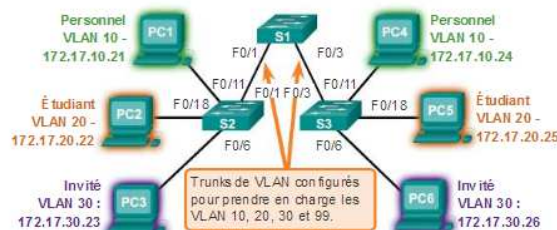
### Trunks de VLAN

#### Exemple 1 :

Dans la figure, les liaisons entre les commutateurs S1 et S2 ainsi que S1 et S3 sont configurés pour transmettre le trafic provenant des VLAN 10, 20, 30 et 99 sur l'ensemble du réseau. Ce réseau ne peut pas fonctionner sans trunks de VLAN.

VLAN 10 Personnel - 172.17.10.0/24  
VLAN 20 Étudiants - 172.17.20.0/24  
VLAN 30 Invité - 172.17.30.0/24  
VLAN 99 Gestion et natif - 172.17.99.0/24

F0/1-5 sont des interfaces de trunk 802.1Q avec le VLAN 99 comme VLAN natif.  
F0/11-17 se trouvent dans le VLAN 10.  
F0/18-24 se trouvent dans le VLAN 20.  
F0/6-10 se trouvent dans le VLAN 30.



32



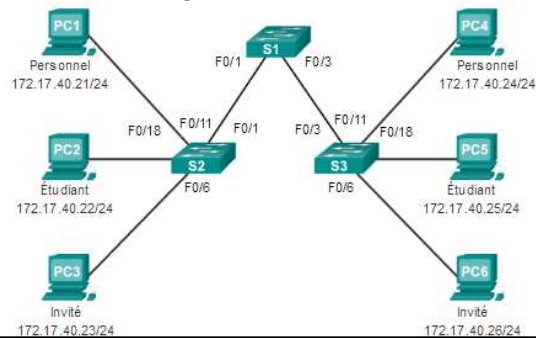
### Trunks de VLAN

#### Exemple 2 :

##### Réseau sans VLAN

- Dans des circonstances normales, lorsqu'un commutateur reçoit une trame de diffusion sur l'un de ses ports, il la transfère par tous les autres ports, à l'exception du port de réception. Dans la Figure, le réseau entier est configuré dans le même sous-réseau (172.17.40.0/24) et aucun VLAN n'est configuré. Par conséquent, lorsque l'ordinateur du personnel enseignant (PC1) envoie une trame de diffusion, le commutateur S2 l'envoie par tous ses ports. Par la suite, l'ensemble du réseau reçoit la diffusion, car il s'agit d'un seul domaine de diffusion.

Aucun segmentation VLAN



33

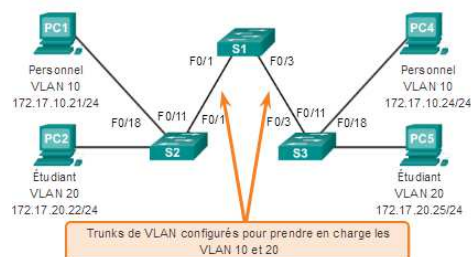
### Trunks de VLAN

#### Exemple 2 (suite):

##### Réseau avec VLAN

- Comme le montre l'animation de la Figure, le réseau a été segmenté en utilisant deux VLAN. Les périphériques du personnel enseignant sont affectés au VLAN 10 et les périphériques des étudiants au VLAN 20. Lorsqu'une trame de diffusion est envoyée de l'ordinateur du personnel enseignant (PC1) au commutateur S2, ce dernier transfère la trame de diffusion uniquement aux ports du commutateur configurés pour prendre en charge le VLAN 10.
- Les ports qui assurent la connexion entre les commutateurs S2 et S1 (ports F0/1) et entre les commutateurs S1 et S3 (ports F0/3) sont des trunks qui ont été configurés pour prendre en charge tous les VLAN du réseau.

Avec segmentation VLAN



34

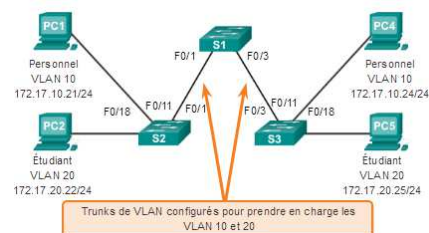
### Trunks de VLAN

#### Exemple 2 (suite)

##### Réseau avec VLAN

- Lorsque le commutateur S1 reçoit la trame de diffusion sur le port F0/1, il la transfère par le seul autre port configuré pour prendre en charge le VLAN 10, soit le port F0/3. Lorsque le commutateur S3 reçoit la trame de diffusion sur le port F0/3, il la transfère par le seul autre port configuré pour prendre en charge le VLAN 10, soit le port F0/11. La trame de diffusion parvient au seul autre ordinateur sur le réseau configuré dans le VLAN 10, soit l'ordinateur PC4 du personnel enseignant.
- Lorsque des VLAN sont implémentés sur un commutateur, la transmission du trafic monodiffusion, multidiffusion et diffusion à partir d'un hôte figurant sur un VLAN donné est limitée aux périphériques se trouvant sur ce VLAN.

Avec segmentation VLAN

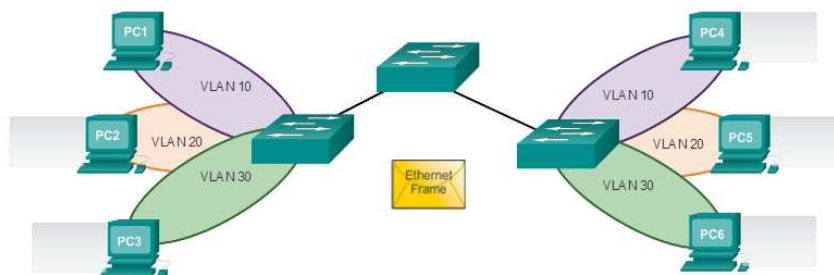


### Trunks de VLAN

#### Planification du comportement du commutateur

##### Scénario: Trunks de VLAN en action

PC1 envoie une diffusion « trames Ethernet (enveloppes en jaune) ». Quels PC recevoir une copie de la trame de diffusion ?



### Plages VLAN sur les commutateurs

#### Affectation de VLAN

- Divers commutateurs Cisco Catalyst prennent en charge des nombres de VLAN différents.
- Le nombre de VLAN pris en charge est suffisamment élevé pour répondre aux besoins de la plupart des entreprises.
- Par exemple, les commutateurs de la gamme Catalyst 2960 et 3560 sont compatibles avec plus de 4 000 VLAN. Sur ces commutateurs, les VLAN à plage normale sont numérotés de 1 à 1 005 et les VLAN à plage étendue, de 1 006 à 4 094.

#### 1. Réseaux locaux virtuels à plage normale

- Utilisés dans les réseaux de petites, moyennes et grandes entreprises.
- Identifiés par un ID de VLAN compris entre 1 et 1005.
- Les ID de 1002 à 1005 sont réservés aux VLAN Token Ring et aux VLAN à interface de données distribuées sur fibre (FDDI).
- Les ID 1 et 1002 à 1005 sont automatiquement créés et ne peuvent pas être supprimés.

37

### Plages VLAN sur les commutateurs

#### Affectation de VLAN

#### 1. Réseaux locaux virtuels à plage normale

- Les configurations sont stockées dans un fichier de base de données VLAN nommé vlan.dat. Le fichier vlan.dat se trouve dans la mémoire Flash du commutateur.
- Le protocole VTP (VLAN Trunking Protocol), qui permet de gérer les configurations VLAN entre les commutateurs, peut uniquement découvrir et stocker les VLAN à plage normale.

#### 2. VLAN à plage étendue

- Permettent aux fournisseurs de services d'étendre leur infrastructure à un plus grand nombre de clients. Certaines multinationales peuvent être suffisamment grandes pour avoir besoin d'une plage étendue d'ID de VLAN.
- Sont identifiés par un ID de VLAN compris entre 1006 et 4094.
- Les configurations ne sont pas écrites dans le fichier vlan.dat.
- Prennent en charge moins de fonctionnalités VLAN que les VLAN à plage normale.
- Sont par défaut enregistrés dans le fichier de configuration en cours.
- Le protocole VTP ne prend pas en compte les VLAN à plage étendue.

**Remarque :** 4096 est le nombre maximum de VLAN disponibles sur les commutateurs Catalyst, car il y a 12 bits dans le champ d'ID de VLAN de l'en-tête IEEE 802.1Q.

38

### Création d'un VLAN

#### Implémentations de VLAN : Affectation de VLAN

- Lors de la configuration de VLAN à plage normale, les détails de la configuration sont stockés dans la mémoire Flash du commutateur dans un fichier nommé `vlan.dat`. La mémoire Flash est permanente et ne requiert pas la commande **copy running-config startup-config**.
- Cependant, comme d'autres détails sont souvent configurés sur un commutateur Cisco au moment où ces VLAN sont créés, il est recommandé d'enregistrer les modifications de la configuration en cours dans la configuration initiale.
- La Figure ci-dessous présente la syntaxe des commandes Cisco utilisée pour ajouter un VLAN à un commutateur et le nommer. Il est recommandé de nommer chaque VLAN lors de la configuration du commutateur.

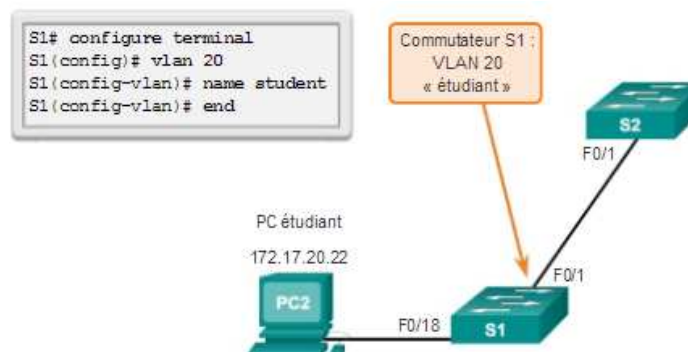
Passez en mode de configuration globale.	S1#configure terminal
Créez un VLAN avec un numéro d'identité valide.	S1(config)# vlan vlan-id
Indiquez un nom unique pour identifier le VLAN.	S1(config-vlan)# name vlan-name
Reprenez en mode d'exécution privilégié.	S1(config-vlan)# end

39

### Création d'un VLAN

#### Implémentations de VLAN : Affectation de VLAN

- La figure ci-dessous montre comment le VLAN « étudiant » (le VLAN 20) est configuré sur le commutateur S1.
- Dans l'exemple de topologie, l'ordinateur « étudiant » (PC2) n'a pas encore été associé à un VLAN, mais il possède l'adresse IP 172.17.20.22.



40

### Création d'un VLAN

#### Implémentations de VLAN : Affectation de VLAN

- La commande **show vlan brief** permet d'afficher le contenu du fichier vlan.dat.

```

Créer le VLAN 20 et attribuez-lui le nom Étudiant. Retournez directement au mode
d'exécution privilégié lorsque vous avez terminé.
S1# configure terminal
Entrez les commandes de configuration, une par ligne. Terminez
par CTRL/Z.
S1(config)# vlan 20
S1(config-vlan)# name Student
S1(config-vlan)# end
S1#
*Mar 31, 08:55:14.5555: %SYS-5-CONFIG_I: Configured from console
by console
S1#

Affichez les informations de brief VLAN.
S1# show vlan brief
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

```

41

### Affectation de ports à des VLAN

#### Implémentations de VLAN : Affectation de VLAN

- Après la création d'un VLAN, l'étape suivante consiste à lui attribuer des ports. Un port d'accès peut appartenir à un seul VLAN à la fois. La seule exception à cette règle consiste en un port connecté à un téléphone IP. Dans ce cas, deux VLAN sont associés au port : un pour la voix et l'autre pour les données.
- La Figure ci-dessous présente la syntaxe permettant de définir un port d'accès et de l'affecter à un VLAN. La commande **switchport mode access** est facultative, mais vivement recommandée comme meilleure pratique de sécurité. Avec cette commande, l'interface passe en mode d'accès permanent.
- Remarque** : utilisez la commande **interface range** pour configurer simultanément plusieurs interfaces.

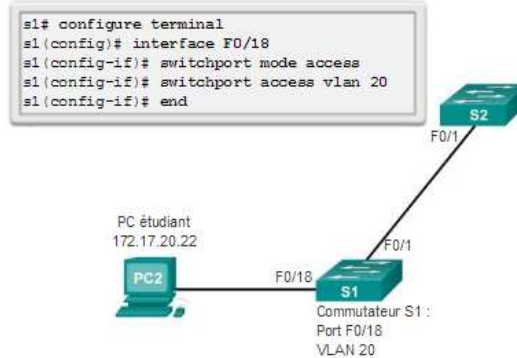
Passez en mode de configuration globale.	S1#configure terminal
Passez en mode de configuration d'interface pour SVI.	S1(config)# interface interface_id
Définissez le port en mode d'accès.	S1(config-if)# switchport mode access
Affectez le port à un réseau local virtuel.	S1(config-if)# switchport access vlan vlan_id
Repassez en mode d'exécution privilégié.	S1(config-if)# end

42

### Affectation de ports à des VLAN

#### Implémentations de VLAN : Affectation de VLAN

Dans l'exemple de la Figure ci-dessous, le VLAN 20 est affecté au port F0/18 du commutateur S1 ; par conséquent, l'ordinateur « étudiant » (PC2) se trouve dans le VLAN 20. Lorsque le VLAN 20 est configuré sur d'autres commutateurs, l'administrateur réseau sait qu'il doit configurer les autres ordinateurs des étudiants dans le même sous-réseau que le PC2 (172.17.20.0/24).



43

### Affectation de ports à des VLAN

#### Implémentations de VLAN : Affectation de VLAN

- Utilisez la commande **show vlan brief** pour afficher le contenu du fichier vlan.dat.
- La commande **switchport access vlan** force la création d'un VLAN s'il n'existe pas déjà sur le commutateur.
- Par exemple, le VLAN 30 n'est pas présent dans le résultat de la commande **show vlan brief** du commutateur. Si la commande **switchport access vlan 30** est saisie sur n'importe quelle interface sans configuration précédente, le commutateur affiche les éléments suivants :
- % Access VLAN does not exist. Creating vlan 30

```

Définissez F0/18 en mode d'accès et affectez le port au VLAN 20. Retournez
directement au mode d'exécution privilégié lorsque vous avez terminé.
S1# configure terminal
Entrez les commandes de configuration, une par ligne. Terminez
par CTRL/Z.
S1(config)# interface f0/18
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
S1#
*Mar 31, 09:34:24.3484: %SYS-5-CONFIG_I: Configured from console
by console
S1#
Affichez les informations de brief VLAN.
S1# show vlan brief
  
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4

### Modification de l'appartenance des ports aux VLAN

#### Implémentations de VLAN : Affectation de VLAN

- Il existe plusieurs façons de modifier l'appartenance des ports aux VLAN. La Figure ci-dessous illustre la syntaxe permettant de faire passer un port de commutateur en appartenance VLAN 1 à l'aide de la commande de mode de configuration d'interface **no switchport access vlan**.

Passez en mode de configuration globale.	S1#configure terminal
Supprimez l'attribution VLAN du port.	S1(config-if)# no switchport access vlan
Repassez en mode d'exécution privilégié.	S1(config-if)# end

L'interface F0/18 avait été précédemment attribuée au VLAN 20. Saisissez la commande **no switchport access vlan** pour l'interface F0/18. Examinez les informations affichées par la commande **show vlan brief** qui suit immédiatement, comme illustré en Figure. La commande **show vlan brief** affiche le type d'attribution de VLAN et d'appartenance de tous les ports du commutateur. La commande **show vlan brief** affiche une ligne pour chaque VLAN. Le résultat pour chaque VLAN inclut son nom, son état et ses ports du commutateur.

```
S1(config)# int f0/18
S1(config-if)# no switchport access vlan
S1(config-if)# end
S1# show vlan brief
```

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 Gi0/1, Gi0/2
20 student	active	
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

### Modification de l'appartenance des ports aux VLAN

#### Implémentations de VLAN : Affectation de VLAN

- Le VLAN 20 est toujours actif, même si aucun port ne lui est affecté. Dans la Figure ci-dessous, la commande **show interfaces f0/18 switchport** vérifie que le VLAN d'accès pour l'interface F0/18 a été réinitialisé sur le VLAN 1.

```
S1# sh interfaces f0/18 switchport
Name: F0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
<resultat omis>
```

- Il est très facile de modifier l'appartenance d'un port à un VLAN. Il n'est pas nécessaire de commencer par supprimer un port d'un VLAN pour modifier son appartenance à ce réseau. Lorsqu'un port d'accès est réaffecté à un autre VLAN existant, cette nouvelle appartenance remplace simplement la précédente.

### Modification de l'appartenance des ports aux VLAN

#### Implémentations de VLAN : Affectation de VLAN

Dans la Figure ci-dessous, le port F0/11 est affecté au VLAN 20.

```
S1# config t
S1(config)# int f0/11
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
S1#
S1# show vlan brief
```

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, Fa0/12, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gi0/2
20	student	active	F0/11
1002	fdi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdiinet-default	act/unsup	
1005	trinet-default	act/unsup	

47

### Suppression de VLAN

#### Implémentations de VLAN : Affectation de VLAN

- Dans la figure, la commande de mode de configuration globale **no vlan *vlan-id*** est utilisée pour supprimer le VLAN 20 du commutateur. Le commutateur S1 possède une configuration minimale avec tous les ports du VLAN 1 et un VLAN 20 non utilisé dans la base de données VLAN. La commande **show vlan brief** vérifie que le VLAN 20 n'est plus présent dans le fichier vlan.dat après utilisation de la commande **no vlan 20**.

```
S1# conf t
S1(config)# no vlan 20
S1(config)# end
S1#
S1# sh vlan brief
```

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, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gi0/1, Gi0/2
1002	fdi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdiinet-default	act/unsup	
1005	trinet-default	act/unsup	

48



### Suppression de VLAN

#### Implémentations de VLAN : Affectation de VLAN

- **Attention** : avant de supprimer un VLAN, réattribuez d'abord tous les ports lui appartenant à un autre VLAN. Tous les ports qui ne sont pas déplacés vers un VLAN actif ne pourront plus communiquer avec d'autres hôtes une fois le VLAN supprimé et tant qu'ils ne seront pas attribués à un VLAN actif.
- Le fichier `vlan.dat` peut aussi être entièrement supprimé à l'aide de la commande **`delete flash:vlan.dat`** en mode d'exécution privilégié. La version abrégée de la commande (**`delete vlan.dat`**) peut être utilisée si le fichier `vlan.dat` n'a pas été déplacé de son emplacement par défaut. Après l'exécution de cette commande et le redémarrage du commutateur, les VLAN précédemment configurés ne sont plus présents. Cette commande rétablit les paramètres d'usine par défaut du commutateur en ce qui concerne les configurations de VLAN.
- **Remarque** : pour un commutateur Catalyst, la commande **`erase startup-config`** doit accompagner la commande **`delete vlan.dat`** avant le redémarrage afin de rétablir les paramètres par défaut du commutateur.

## VTP (VLAN Trunking Protocol)

## Protocole VTP (VLAN Trunking Protocol)

### Introduction au VTP

#### Réseaux Lan sans VTP

- Dans un réseau avec plusieurs commutateurs, chaque VLAN doit être **créé manuellement** sur chaque switch.
- Risque d'**incohérences** (mauvais identifiants VLAN, erreurs humaines).
- **Configuration longue et fastidieuse**, surtout dans un grand réseau.

===== > **Protocole VTP (VLAN Trunking Protocol)**

- VTP est donc une **solution efficace** pour simplifier la gestion des VLAN, mais il doit être configuré avec précaution.
- Le **VTP (VLAN Trunking Protocol)** résout principalement le problème de la **gestion centralisée des VLAN** dans un réseau de commutateurs.

51

## Protocole VTP (VLAN Trunking Protocol)

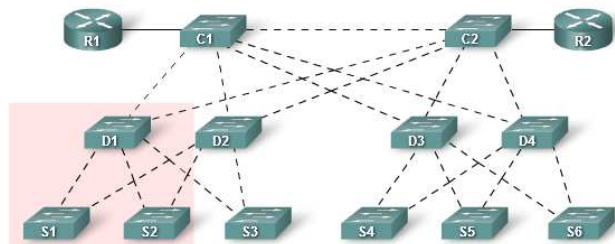
### Introduction au VTP

Gestion des VLANs : un défi

**Problème:** Gestion de plusieurs commutateurs

VLAN existants : 10, 20, 99

Tâche de gestion VLAN : ajout de VLAN 30



**Solution:** Le protocole VTP

52

## Protocole VTP (VLAN Trunking Protocol)

### Introduction au VTP

#### Qu'est-ce que VTP ?

- VTP (VLAN Trunking Protocol) est un protocole propriétaire de Cisco.
- Il permet la gestion centralisée des VLAN dans un réseau de commutateurs.
- Réduit la complexité de gestion des VLAN.
- VTP est un protocole qui utilise les trames d'agrégation de couche 2 pour gérer l'ajout, la suppression et l'attribution de nouveaux noms aux VLAN sur un domaine unique;
- VTP autorise les changements centralisés qui sont communiqués à tous les autres commutateurs du réseau.
- Le protocole VTP V1 et V2 détecte uniquement les réseaux locaux virtuels de plage normale (ID de VLAN de 1 à 1 005), par contre VTPv3 support des VLAN étendus (1006-4094), pour une meilleure sécurité, protection contre les suppressions accidentelles.
- Les réseaux locaux virtuels de plage étendue (ID supérieur à 1 005) ne sont donc pas pris en charge par le protocole VTP;
- Les messages VTP sont encapsulés dans des trames de protocole Cisco ISL (Inter-Switch Link) ou IEEE 802.1Q, puis transmis sur des liens multi-VLAN aux autres unités;

53

## Protocole VTP (VLAN Trunking Protocol)

### Fonctions et avantages de VTP

#### Fonctions :

- Synchronisation automatique des VLAN entre les commutateurs.
- Distribution des informations VLAN depuis un serveur VTP.
- Réduction des erreurs de configuration.

#### Avantages :

- Administration centralisée.
- Facilité de gestion des VLAN.
- Moins de risque d'incohérence dans la configuration des VLAN.
- **Le protocole VTP assure la cohérence de la configuration VLAN en gérant :**
  - L'ajout ;
  - La suppression ;
  - Le changement ;

**de nom des réseaux locaux virtuels sur plusieurs commutateurs**

54

## Protocole VTP (VLAN Trunking Protocol)

### Modes de fonctionnement de VTP

#### 1. Serveur (Server) :

Crée, modifie et supprime les VLAN.  
Envoie des mises à jour VTP.

#### 2. Client (Client) :

Reçoit et applique les mises à jour VTP.  
Ne peut pas créer, modifier ou supprimer des VLAN.

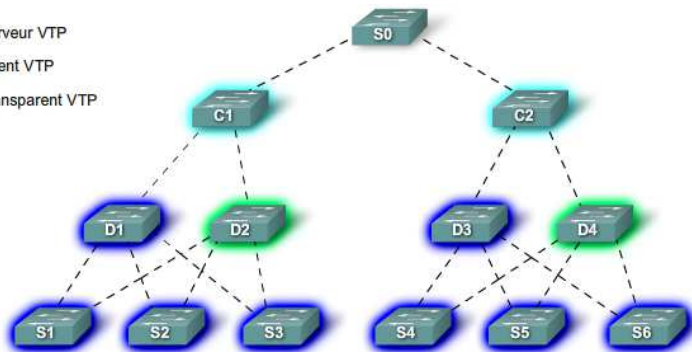
#### 3. Transparent (Transparent) :

Ne participe pas au processus VTP.  
Transmet simplement les mises à jour VTP aux autres commutateurs.  
Permet la gestion locale des VLAN.

55

## Protocole VTP (VLAN Trunking Protocol)

### Modes de fonctionnement de VTP



#### 1. Serveur (Server) :

Crée, modifie et supprime les VLAN.  
Envoie des mises à jour VTP.

#### 2. Client (Client) :

Reçoit et applique les mises à jour VTP.  
Ne peut pas créer, modifier ou supprimer des VLAN.

#### 3. Transparent (Transparent) :

Ne participe pas au processus VTP.  
Transmet simplement les mises à jour VTP aux autres commutateurs.  
Permet la gestion locale des VLAN.

56

## Protocole VTP (VLAN Trunking Protocol)

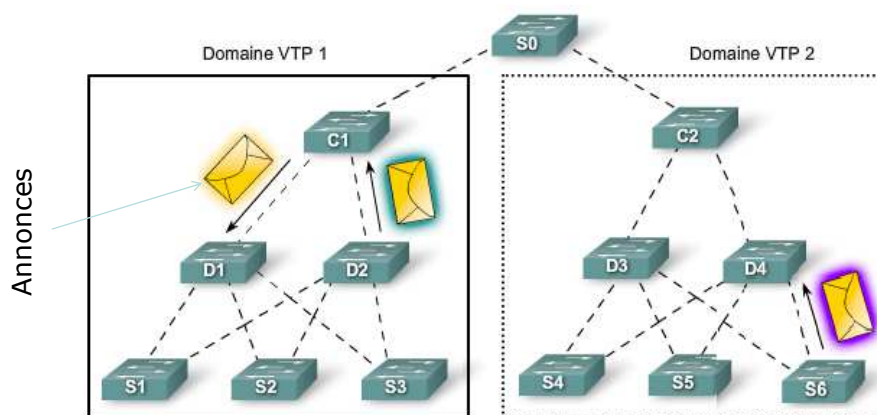
### Composants VTP

- **Domaine VTP** : composé d'un ou de plusieurs commutateurs interconnectés. Tous les commutateurs d'un domaine partagent les détails de configuration VLAN à l'aide d'annonces VTP;
- **Annonces VTP** : le protocole VTP utilise une hiérarchie d'annonces pour distribuer et synchroniser les configurations VLAN sur le réseau;
- **Modes VTP** : un commutateur peut être configuré dans un des trois modes : **serveur, client ou transparent**;
- **Serveur VTP** : les serveurs VTP annoncent les paramètres VLAN de domaine VTP aux autres commutateurs compatibles dans le même domaine VTP. Les serveurs VTP stockent les informations VLAN pour l'ensemble du domaine dans la mémoire vive non volatile. Le serveur est l'emplacement sur lequel vous pouvez créer, supprimer ou renommer des réseaux locaux virtuels pour le domaine;

57

## Protocole VTP (VLAN Trunking Protocol)

### Composants VTP

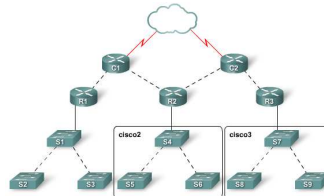


58

## Protocole VTP (VLAN Trunking Protocol)

### Composants VTP: Domaines VTP

- Un domaine VTP se compose d'un commutateur ou de plusieurs commutateurs interconnectés partageant le même nom de domaine VTP;
- Un commutateur peut être membre d'un seul domaine VTP à la fois;
- Tant que le nom de domaine VTP n'est pas spécifié, vous ne pouvez pas créer ni modifier de réseaux locaux virtuels sur un serveur VTP, et les informations VLAN ne sont pas propagées sur le réseau;



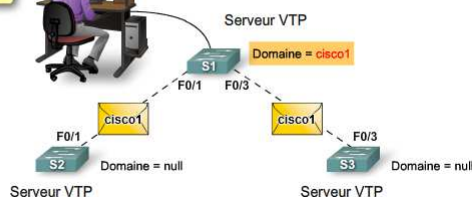
59

## Protocole VTP (VLAN Trunking Protocol)

### Propagation de nom de domaines VTP

- Au départ tous les commutateurs ont un nom de domaine VTP null;
- L'administrateur réseau configure le nom de domaine VTP **cisco1** sur le commutateur **serveur VTP S1**. Le serveur VTP envoie une annonce VTP incorporant le nouveau nom de domaine. Les commutateurs serveurs VTP **S2** et **S3** mettent à jour leur configuration VTP avec le nouveau nom de domaine.

Comm1 envoie le nouveau nom de domaine à Comm2 et Comm3.



60

## Protocole VTP (VLAN Trunking Protocol)

### Structure de la trame VTP

- **Trame VTP = En-tête VTP+ Message VTP ;**
- Les informations VTP sont insérées dans le champ de données d'une trame Ethernet;
- La trame Ethernet est ensuite encapsulée comme trame d'agrégation 802.1Q;
- Chaque commutateur du domaine envoie régulièrement des annonces de chaque port d'agrégation vers une adresse de multidiffusion réservée
- 01-00-0C-CC-CC-CC;
- Ces annonces sont reçues par les commutateurs voisins, qui mettent à jour leurs configurations VTP et VLAN selon les besoins;

61

## Protocole VTP (VLAN Trunking Protocol)

### Annonces VTP

- **Annonces de type résumé**
- L'annonce de type résumé contient le nom de domaine VTP, le numéro de révision actuel, ainsi que d'autres détails sur la configuration VTP.
- Les annonces de type résumé :
  - sont envoyées toutes les 5 minutes par un serveur VTP ;
  - informent les commutateurs compatibles VTP du numéro de révision de configuration VTP courant ;
  - sont envoyées immédiatement après une modification de configuration.
- **Annonces de type sous-ensemble**
- Modifications qui Sont déclenchées par:
  - Création ou suppression d'un réseau local virtuel
  - Arrêt ou activation d'un réseau local virtuel
  - Modification du nom d'un réseau local virtuel
  - Modification de la MTU d'un réseau local virtuel

62

## Protocole VTP (VLAN Trunking Protocol)

### Annonces VTP

- **Annonces de type requête**
- Lorsqu'une annonce de type requête est envoyée à un serveur VTP du même domaine VTP, le serveur VTP répond en envoyant une annonce de type résumé, puis une annonce de type sous-ensemble. Des annonces de type requête sont envoyées si :
  - le nom de domaine VTP a été changé ;
  - une annonce de type résumé arrive avec un numéro de révision de configuration supérieur ;
  - il manque un message d'annonce de type sous-ensemble ;
  - le commutateur a été réinitialisé.
- VTP en Pratique
- Vidéo 4.2.4.2

63

## Protocole VTP (VLAN Trunking Protocol)

### Structure de la trame VTP

Ou  
IEEE 802.1Q



L'en-tête VTP varie en fonction du type de message VTP, mais quatre éléments sont généralement inclus dans tous les messages VTP :

- ☐ **Version du protocole VTP**: version 1 ou 2;
- ☐ **Type de message VTP**: indique l'un des trois types;
- ☐ **Longueur du nom de domaine de gestion**: indique la taille du nom;
- ☐ **Nom du domaine de gestion**: nom configuré pour le domaine de gestion;

64



## Protocole VTP (VLAN Trunking Protocol)

### Structure de la trame VTP

- Les trames VTP contiennent les informations de **domaine globales** de longueur fixe suivantes :
  - Nom de domaine VTP;
  - Identité du commutateur envoyant le message, et heure à laquelle il a été envoyé;
  - Configuration VLAN d'algorithme MD5, comprenant la taille d'unité de transmission maximale (MTU: est la taille maximale d'un paquet pouvant être transmis en une seule fois (sans fragmentation) pour chaque réseau local virtuel);
  - Le protocole **VTP (VLAN Trunking Protocol)** utilise **MD5** pour sécuriser la synchronisation des bases de données VLAN entre les commutateurs.
  - Pour éviter les modifications non autorisées des VLAN, VTP utilise un **hachage MD5** afin de vérifier l'intégrité des mises à jour envoyées entre les commutateurs.
  - Lorsqu'un Serveur VTP envoie une mise à jour VTP, il génère une **empreinte MD5** basée sur : Le **nom du domaine VTP**; Le **numéro de révision** ; La **configuration VLAN**; La **clé secrète**
- **Remarque : VTP supporte-t-il d'autres algorithmes de hachage ?**
  - **Non** , Cisco ne propose pas d'autres algorithmes comme SHA-256 pour VTP. Il repose uniquement sur **MD5**, même dans les versions les plus récentes (VTPv3).

65

## Protocole VTP (VLAN Trunking Protocol)

### Numéro de révision

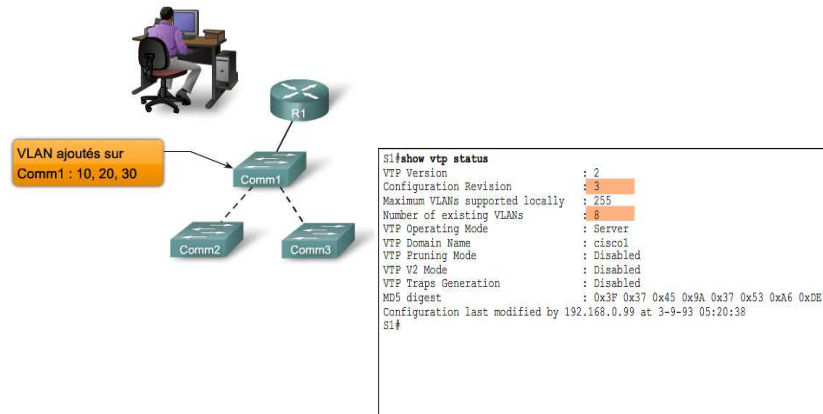
- Le numéro de révision de configuration est un nombre 32 bits qui indique le niveau de révision d'une trame VTP;
- Le numéro de configuration par défaut d'un commutateur est zéro,
- Chaque fois qu'un réseau local virtuel est ajouté ou supprimé, le numéro de révision de configuration est incrémenté;
- Chaque périphérique VTP effectue le suivi du numéro de révision de configuration VTP qui lui est attribué;
- Remarque: le changement de nom de domaine VTP n'incrémente pas le numéro de révision. Au contraire, il le remet à zéro;
- Le numéro de révision de configuration indique si les informations de configuration reçues d'un autre commutateur compatible VTP sont plus récentes que la version stockée sur le commutateur.

66

## Protocole VTP (VLAN Trunking Protocol)

### Numéro de révision

- La figure montre un administrateur réseau ajoutant trois réseaux locaux virtuels au commutateur Comm1,



67

## Protocole VTP (VLAN Trunking Protocol)

### Versions de VTP

Version	Fonctionnalités principales
VTPv1	Gestion de base des VLAN, modes Server/Client/Transparent
VTPv2	Support Token Ring VLAN, amélioration de la stabilité
VTPv3	Support des VLAN étendus (1006-4094), meilleure sécurité, protection contre les suppressions accidentelles

68

## Protocole VTP (VLAN Trunking Protocol)

### Sécurité et VTP

- VTP utilise **MD5** pour vérifier l'intégrité des mises à jour.
- Un mot de passe peut être configuré pour sécuriser les annonces VTP.
- **Risques :**
  - Un commutateur mal configuré peut supprimer tous les VLAN si son numéro de révision est plus élevé.
  - Nécessité d'un contrôle strict des mises à jour.

69

## Protocole VTP (VLAN Trunking Protocol)

### Configuration de VTP (Exemple en CLI)

#### 1. Configuration en mode serveur

```
Switch(config)# vtp domain LSI
Switch(config)# vtp mode server
Switch(config)# vtp password MonMotDePasse
```

#### 2. Configuration en mode client

```
Switch(config)# vtp domain LSI
Switch(config)# vtp mode client
Switch(config)# vtp password MonMotDePasse
```

#### 3. Configuration en mode transparent

```
Switch(config)# vtp mode transparent
```

70

## Protocole VTP (VLAN Trunking Protocol)

### Commandes de vérification

#### Vérification des informations VTP

Switch# show vtp status

#### Affichage des statistiques VTP

Switch# show vtp counters

71

## Protocole VTP (VLAN Trunking Protocol)

### Bonnes pratiques avec VTP

- Utiliser VTPv3 pour plus de sécurité.
- Toujours configurer un mot de passe VTP.
- Placer les commutateurs non essentiels en mode transparent.
- Vérifier le numéro de révision VTP avant d'ajouter un nouveau switch.
- Sauvegarder la configuration des VLAN régulièrement.

72

# STP (Spanning-Tree Protocole)

## STP (Spanning-Tree Protocole)

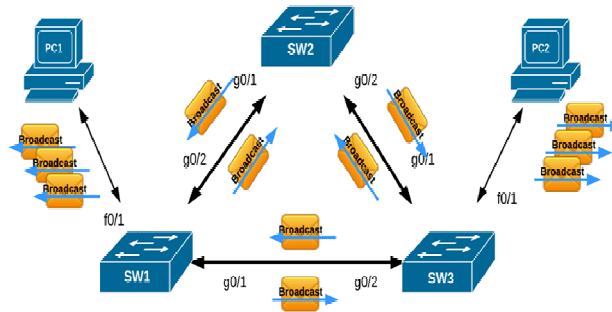
### Introduction

- Dans le domaine des réseaux, il existe un concept appelé redondance de réseau (**network redundancy**).
- En général, la redondance de réseau est obtenue par l'ajout de chemins de réseau alternatifs, et elle est considérée comme l'un des facteurs clés du maintien de la fiabilité du réseau.
- Nous utilisons des chemins de réseau redondants afin que le réseau continue de fonctionner si un lien ou un port tombe en panne. Cela nous permet également de partager la charge du trafic et d'augmenter la capacité et la vitesse.
- Mais cela peut causer des problèmes si des mesures appropriées ne sont pas prises comme les boucles de commutation (**Switching Loops**).

## STP (Spanning-Tree Protocole)

### Introduction

Par exemple, dans le cas illustré ici :

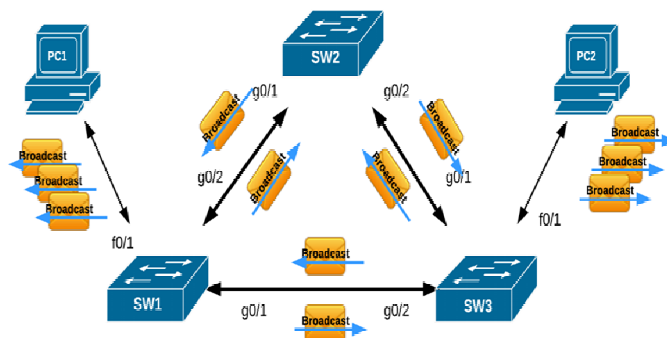


1. PC1 envoie une trame de diffusion
2. Les commutateurs SW1, SW2 et SW3 diffusent la trame de PC1 sur tous les ports.
3. Ce qui fait que les trames sont bouclées et multipliées à chaque fois qu'elles passent par un commutateur. Comme ces données de couche 2 n'ont pas de durée de vie (un Time to Live comme les paquets IP traités par les routeurs), elles tourneront indéfiniment entre les commutateurs.

75

## STP (Spanning-Tree Protocole)

### Introduction



- Ceci crée un phénomène appelé "**broadcast storm**", qui peut faire tomber tout le réseau en quelques secondes.
- La question est donc la suivante : **comment un réseau peut-il bloquer les liens qui peuvent provoquer des boucles tout en maintenant la redondance des liens ?**
- La réponse est d'utiliser le **protocole Spanning-Tree (STP)**

76

## STP (Spanning-Tree Protocole)

### Introduction

- STP permet de résoudre plusieurs problèmes critiques liés aux réseaux Ethernet redondants :
- **Boucles de commutation (Switching Loops)** : Lorsque plusieurs chemins existent entre des commutateurs, les trames peuvent circuler indéfiniment, provoquant des tempêtes de broadcast et une saturation du réseau.
- **Tempêtes de broadcast (Broadcast Storms)** : Une boucle réseau peut engendrer une propagation incontrôlée des trames de broadcast, consommant toute la bande passante disponible.
- **Incohérences dans la table MAC** : En présence de boucles, un switch peut recevoir la même trame sur plusieurs ports, rendant la table MAC instable et empêchant la bonne livraison des paquets.
- **Consommation excessive des ressources réseau** : Un trafic inutilement dupliqué dans le réseau entraîne une surcharge des switches et une baisse des performances globales.
- **Perte de connectivité et instabilité réseau** : Sans STP, une boucle peut rapidement entraîner une perte de connectivité pour l'ensemble du réseau, rendant le trafic inutilisable.

77

## STP (Spanning-Tree Protocole)

### STP (Spanning Tree Protocol)



- ❑ Le protocole STP (**Spanning Tree Protocol**) est un protocole réseau qui a été développé en 1995 pour éviter les boucles de réseau de couche 2 lorsque des ordinateurs échangent des données sur un réseau local avec des chemins redondants.
- ❑ Il est basé sur un algorithme inventé par Radia Perlman en 1985 et publié dans un article intitulé "**An Algorithm for Distributed Computation of a Spanning Tree in an Extended LAN**".
- ❑ Ce protocole est situé sur la couche 2 du modèle OSI et joue le rôle d'un protocole de gestion de liens.

78



## STP (Spanning-Tree Protocole)

### Variantes du protocole Spanning-Tree

Il existe plusieurs variétés de protocoles spanning-tree qui ont émergé depuis la version originale IEEE 802.1D. Ci-après une comparaison des variétés STP:

Les protocoles	Spanning Tree Protocol (STP)	PVST+	Rapid Spanning Tree (RSTP)	PVRST+
Standard	IEEE 802.1D	Cisco PTS	IEEE 802.1w	RSTP Cisco
Description	Il s'agit d'une norme de spanning tree développée par l'IEEE qui élit un seul commutateur racine par topologie entière.	C'est une norme spanning tree développée par Cisco pour ses matériels qui trouve le commutateur racine par VLAN.	Il s'agit d'une norme de spanning développée par l'IEEE qui offre une convergence plus rapide que le STP commun mais qui conserve la même idée de trouver un commutateur racine unique dans la topologie.	Cette norme Spanning Tree est développée par Cisco et permet une convergence plus rapide que PVST+.
Convergence	lent	lent	rapide	rapide
Ressources (CPU et mémoire)	Faible	Élevé	moyenne	très élevé



## Algorithme du Spanning-Tree (comment cela fonctionne?)



## STP (Spanning-Tree Protocole)

### Fonctionnement du STP

STP fonctionne en établissant une arborescence (« spanning tree ») dans le réseau. Voici les étapes principales :

#### 1. Élection du Root Bridge

- Le switch ayant l'identifiant de pont (Bridge ID) le plus bas devient le root bridge.
- Le Bridge ID est composé de la priorité du switch et de son adresse MAC.
- Chaque switch compare son Bridge ID avec les autres en envoyant des **BPDUs (Bridge Protocol Data Units)**.

#### 2. Sélection des ports

- **Root Port (RP)** : Le port sur chaque switch qui a le chemin le plus court vers le root bridge.
- **Designated Port (DP)** : Un port sur chaque segment qui a le meilleur chemin vers le root bridge et transmet les trames.
- **Blocked Port** : Ports non essentiels qui sont mis en veille pour éviter les boucles.

81

## STP (Spanning-Tree Protocole)

### Fonctionnement du STP (suite)

#### 3. État des ports STP

- **Blocking** : Ne transmet pas de trames de données, mais écoute les BPDUs.
- **Listening** : Attend les BPDUs pour déterminer la topologie sans apprendre les adresses MAC.
- **Learning** : Apprend les adresses MAC mais ne transmet toujours pas de trames.
- **Forwarding** : Envoie et reçoit activement des trames de données.
- **Disabled** : Port désactivé administrativement.

82

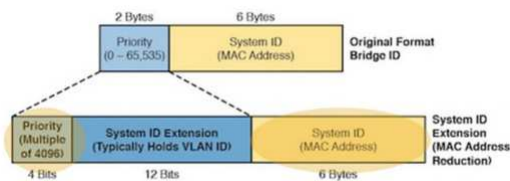
## STP (Spanning-Tree Protocole)

### Fonctionnement du STP

Étant donné que le **spanning-tree** est activé, les **switches** vont s'envoyer des trames **BPDU** (Bridge Protocol Data Unit). Les parties importantes à noter sont : le champ de l'**adresse MAC** et celui de la **priorité du bridge**. Ces deux champs identifient le **Bridge ID**.

**Bridge ID = priorité + adresse mac**

C'est l'information dont le **spanning-tree** a besoin pour effectuer ses calculs.



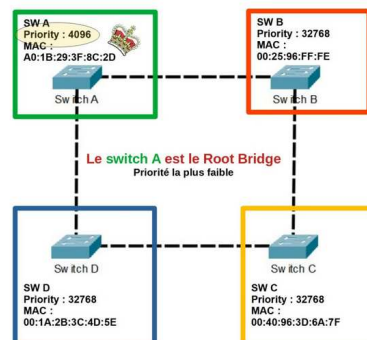
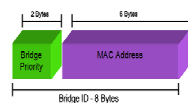
83

## STP (Spanning-Tree Protocole)

### Fonctionnement du STP

#### Élection du Root Bridge :

- Le protocole **STP** commence par l'élection d'un switch de référence, appelé **Root Bridge** (pont racine). Le switch qui a la plus petite priorité sera élu **Root Bridge**. Mais s'il y a égalité de priorité entre plusieurs **commutateurs**, **STP** sélectionnera le **commutateur** avec la plus petite **adresse MAC** (il n'est pas possible d'avoir plusieurs fois la même **adresse MAC**).
- Par défaut, les **switches** ont une **priorité** de 32 768. Le **Root Bridge** sert de point central pour la **topologie de l'arbre**.
- Exemple 1 : Dans un réseau avec quatre **switches** (A, B, C, D), si A a une priorité plus basse que les autres, il sera élu comme **Root Bridge**. Cela signifie que tous les autres **switches** calculeront leurs chemins en fonction de leur distance par rapport à A.



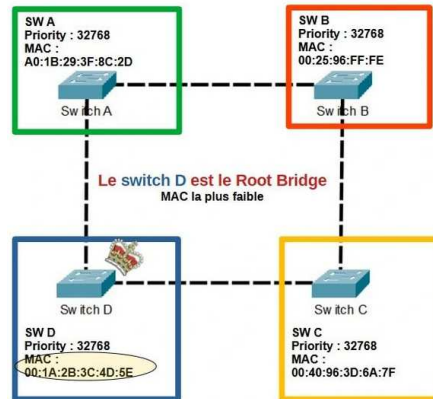
84

## STP (Spanning-Tree Protocole)

### Fonctionnement du STP

#### Élection du Root Bridge :

- 2<sup>e</sup> Exemple : Si maintenant tous les **switches** ont la même priorité, **STP** élit le **commutateur** qui a la plus petite **adresse MAC**. On peut voir ici que le **Root Bridge** n'est plus le **commutateur A**, mais le **D**, car l'**adresse MAC** commençant par 00.1A est plus petite que 00.1B.



85

## STP (Spanning-Tree Protocole)

### Fonctionnement du STP

#### Calcul du chemin le plus court :

- La seconde étape est que chaque **commutateur** du réseau détermine le chemin le plus rapide pour atteindre le **Root Bridge**. Ce calcul est basé sur un **coût** associé à chaque lien ;
- STP** préférera un lien de 1 **Gbps** à un de 100 **Mbps**.
- Un lien a un coût spécifique que le **spanning-tree** a défini par défaut.

Vitesse	Coût STP
10 Mbps	100
100 Mbps	19
1 Gbps	4
10 Gbps	2

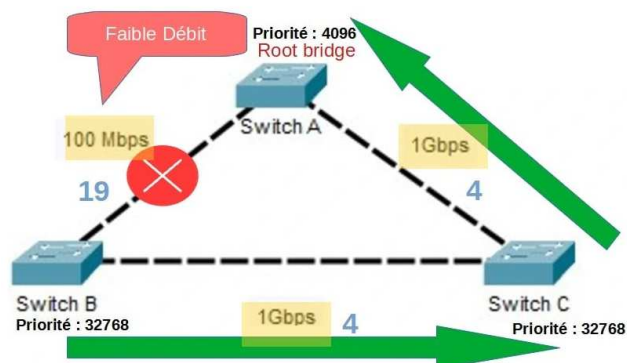
86

## STP (Spanning-Tree Protocole)

### Fonctionnement du STP

#### Calcul du chemin le plus court :

- Exemple : Si un **commutateur** B peut atteindre le **Root Bridge** A via deux chemins, un direct à 100 **Mbps** ou deux liens de 1 **Gbps** chacun passant par le **commutateur** C, il choisira le chemin via C, car le **coût** du lien de 8 (4+4) est inférieur à 19, garantissant une transmission plus rapide.



87

## STP (Spanning-Tree Protocole)

### Fonctionnement du STP

#### Désignation des ports :

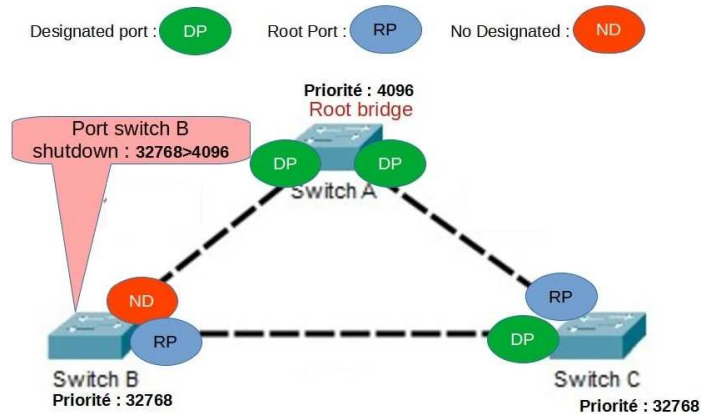
- Une fois les chemins calculés, chaque **commutateur** désigne un **Root Port (port racine)** pour la communication avec le **Root Bridge** et un **Designated Port ou Forwarding (port désigné)** pour les autres liaisons. Les ports restants, susceptibles de créer des **boucles**, sont mis en état de blocage **ND (non designated)**, qui seront bloqués.
- Pour qu'un lien soit bloqué, il faut qu'un des deux ports de ce lien soit bloqué. Mais lequel choisir ? **STP** utilise la même méthode que pour l'élection du **Root Bridge** : il regarde la **priorité** des deux **switches**, sinon leurs **adresses MAC** si nécessaire. Il bloquera ainsi le port du **commutateur** ayant la **priorité** la plus haute.
- Exemple : Reprenons l'exemple précédent. Ici, il y a une **boucle** et nous souhaitons l'éviter pour les raisons mentionnées plus haut. Dans ce cas, le lien entre le **commutateur** A et B sera celui à couper. Le port du **commutateur** B sera mis en état de « shutdown » car il a la **priorité** la plus élevée.

88

## STP (Spanning-Tree Protocole)

### Fonctionnement du STP

#### Désignation des ports :



**Remarque :** STP surveille en permanence le réseau. Si un lien tombe, comme celui entre les commutateurs B et C, STP réévalue la **topologie** et active un chemin bloqué pour rétablir la communication (on pourrait réactiver le lien entre A et B), tout en évitant la formation de **boucles**.

89

## STP (Spanning-Tree Protocole)

### Bonnes Pratiques pour l'Implémentation

#### Bonnes Pratiques pour l'Implémentation

- Définir manuellement un **Root Bridge** pour un meilleur contrôle de la topologie.
- Configurer les priorités STP pour optimiser les chemins de commutation.
- Activer **PortFast** sur les ports connectés à des hôtes pour accélérer la connexion.
- Utiliser **BPDU Guard** pour éviter les configurations indésirables.
- Mettre en place **Loop Guard** et **Root Guard** pour prévenir les modifications involontaires de la topologie STP.

90

## STP (Spanning-Tree Protocole)

### Les Commandes de Packet tracer

Pour vérifier la priorité d'un commutateur, on utilise la commande :

`show spanning-tree`

Pour influencer le processus d'élection:

`spanning-tree vlan ID root primary`

Pour configurer la valeur de la priorité du commutateur, on utilise la commande :

`spanning-tree vlan ID priority 24576`

Si un commutateur racine alternatif est souhaité en cas de panne du commutateur racine primaire, nous utilisons la commande:

`spanning-tree vlan ID root secondary`

Pour remplacer la valeur par défaut sur l'interface, nous utilisons la commande:

`spanning-tree cost VALUE`

Pour vérifier l'état actuel du port, nous utilisons la commande :

`show spanning-tree Interface ID`

`show running-config | include span`

pour désactiver STP sur une base par réseau local virtuel (VLAN) , nous utilisons la commande :

`no spanning-tree vlan vlan-id`

91

## Bibliographie

1. <https://cyberopti.com/spanning-tree-protocol-stp-guide-complet/>
2. <http://eventus-networks.blogspot.com/2013/11/les-topologies-physiques-et-logiques.html>
3. [https://fr.wikipedia.org/wiki/IEEE\\_802.3](https://fr.wikipedia.org/wiki/IEEE_802.3)
4. Hardware support : <http://www.cisco.com/public/support/tac/hardware.shtml>
5. <http://www.cisco.com/>
6. <http://standards.ieee.org/getieee802/download/802.1Q-1998.pdf>
7. <http://standards.ieee.org/getieee802/download/802.1Q-2003.pdf>
8. <http://standards.ieee.org/getieee802/download/802.1X-2004.pdf>
9. <http://www.cisco.com/univercd>
10. <http://www.cisco.com/warp/public/473/21.html>
11. <http://www.reseaucerta.org/docs/didactique/VLAN.pdf>

92