

LES VLAN

Hainaut Patrick 2017

But de cette présentation

- Vu la prolifération des ordinateurs, leur mise en réseau est non seulement indispensable mais doit être planifiée et organisée
- Bien souvent, on ne peut pas se contenter de tout mettre dans le même réseau local, mais il y a lieu de créer des réseaux différents sans pour autant multiplier le matériel physique
- C'est à ce niveau qu'interviennent les réseaux virtuels, dits vlan (prononcer vélane ;-))
- Les exemples de configuration seront donnés pour le matériel Cisco

Fonctionnement du commutateur

- Contrairement à un concentrateur (hub), un commutateur (switch) ne diffuse pas les trames
- Il met en relation les seuls postes concernés par l'échange



© Hainaut P. 2017 - www.coursonline.be

3

Fonctionnement du commutateur

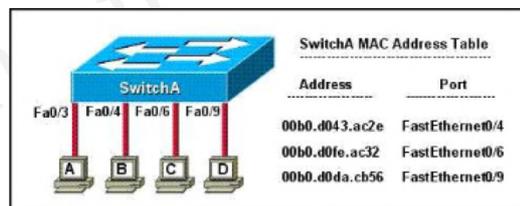
- A chaque fois qu'un message lui parvient, le commutateur associe le port par lequel arrive la trame à l'adresse matérielle (adresse MAC) de l'émetteur de la trame
- Ainsi après un certain nombre de trames, le commutateur connaît « l'emplacement » (c'est à dire le port de rattachement) des postes sur le réseau et peut les mettre en relation deux à deux

© Hainaut P. 2017 - www.coursonline.be

4

Fonctionnement du commutateur

- Cette association adresse MAC / port est gérée dans des tables d'association présentes dans chaque commutateur
- Cette table est construite progressivement par apprentissage



© Hainaut P. 2017 - www.coursonline.be

5

Fonctionnement du commutateur

- Si une trame contient une adresse de destination qui n'est pas présente dans la table, cette trame est transmise sur tous les ports du commutateur à l'exception du port émetteur de la trame
- C'est aussi ainsi que sont traités les trames de diffusion

© Hainaut P. 2017 - www.coursonline.be

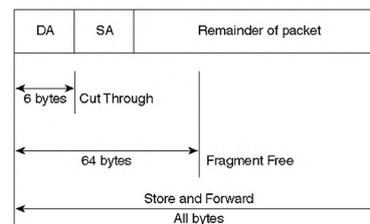
6

Fonctionnement du commutateur

- On distingue deux modes de fonctionnement du commutateur:
 - Store and forward :
 - il stocke les trames entièrement avant de les réémettre
 - Il ne réémet donc pas les trames erronées ou en collision
 - Par contre ces commutateurs sont plus lents et nécessitent des mémoires tampons importantes

Fonctionnement du commutateur

- On the fly (appelé aussi cut through chez CISCO) :
 - à la volée, les commutateurs réémettent immédiatement après lecture de l'adresse MAC destinataire
 - C'est plus rapide mais on propage les trames erronées
 - notamment les trames en collision et celles dont le CRC indique une erreur de transmission



Fonctionnement du commutateur

- Le commutateur permet de garantir la bande passante d'un réseau. La bande passante, c'est le débit d'un réseau
- Ainsi un commutateur 100 mb/s de 12 ports garantira 100 mb/s par port alors qu'un concentrateur 100 mb/s de 12 ports divisera cette bande passante entre tous ses ports

Ethernet commuté

- En utilisant uniquement des commutateurs, il n'y a plus de collision possible
- Chaque port forme un mini-segment composé du commutateur et d'une carte ou aucune collision ne peut se produire
- Dans ce cas, pendant l'émission d'une trame, la paire de réception n'est plus monopolisée par la détection de collision et on peut recevoir en même temps, c'est à dire travailler en mode bidirectionnel (full duplex)

Spanning tree

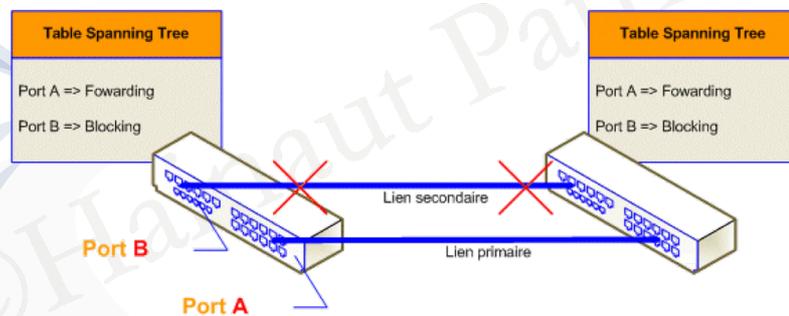
- Dans une architecture entièrement commutée, on met généralement en œuvre des interconnexions redondantes entre commutateurs pour garantir une plus grande tolérance aux pannes
- Les liaisons redondantes doivent être invalidées quand elles ne sont pas utiles et validées en cas de rupture d'une liaison
- Si les liaisons redondantes fonctionnent de pair, cela crée une boucle qui va générer des « tempêtes » de diffusion (broadcast storm) au sein des commutateurs -> saturation des liens et disfonctionnement

© Hainaut P. 2017 - www.coursonline.be

11

Spanning tree

- Cette gestion de la redondance est prise en charge par le protocole 802.1D (arbre de recouvrement, en anglais spanning tree protocol)



© Hainaut P. 2017 - www.coursonline.be

12

Spanning tree: définitions

- STP (Spanning tree protocol): c'est le protocole permettant d'obtenir un réseau sans boucles
- STA (Spanning tree algorithm): c'est l'algorithme utilisé par STP pour déterminer quels ports seront mis en état de blocage pour éviter des boucles sur le réseau
- Commutateur racine (root switch) ou pont racine (root bridge): c'est le commutateur utilisé comme point de référence pour le calcul de tous les chemins
- BPDU (Bridge Protocol Data Unit): trames échangées régulièrement entre commutateurs pour élire le commutateur racine et pour réagir à une éventuelle modification de topologie

Spanning tree: commutateur racine

- Tous les commutateurs associés au protocole STP échangent des trames BPDU pour identifier le commutateur doté de l'identificateur de pont (Bridge Identifier BID) le plus faible sur le réseau
- Celui-ci devient automatiquement le commutateur racine
- L'identificateur de pont contient une valeur de priorité, l'adresse MAC du commutateur émetteur et un ID système étendu facultatif. La valeur d'identificateur de pont la plus faible est déterminée par la combinaison de ces trois champs

Spanning tree: configuration automatique

- Le fait que tout se fasse automatiquement est très chouette, mais si on veut pouvoir choisir le commutateur racine à la place du système, c'est possible
- En général, ce n'est pas indispensable, le STP n'étant pas l'élément principal à configurer
- Cependant, si vous voulez maîtriser complètement tous les aspects du STP, vous pouvez utiliser les commandes des pages suivantes
- Attention que la plupart de ces commandes ne sont pas supportées par la version actuelle de Cisco Packet Tracer

© Hainaut P. 2017 - www.coursonline.be

15

Spanning tree: commutateur racine

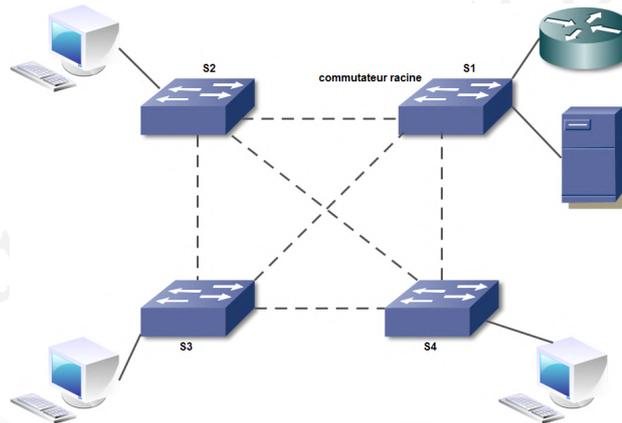
- Si on veut maîtriser tous les aspects du STP, il est judicieux de choisir, en premier lieu, un commutateur racine performant situé au milieu du réseau
- Si vous placez le commutateur racine au centre du réseau en le raccordant directement aux serveurs et aux routeurs, vous réduisez la distance moyenne qui sépare les clients des serveurs et des routeurs

© Hainaut P. 2017 - www.coursonline.be

16

Spanning tree: commutateur racine

- Dans le cas ci-dessous, on doit s'arranger pour que S1 soit le commutateur racine



© Hainaut P. 2017 - www.coursonline.be

17

Spanning tree: commutateur racine

- Pour désigner un commutateur comme commutateur racine:
 - Méthode 1:
`S1(config) # spanning-tree vlan 1 root primary`

remarque: *vlan 1* est le réseau virtuel par défaut dans lequel se trouvent tous les ports d'un commutateur

Si vous utilisez les VLAN, il faudra donc désigner un commutateur racine par VLAN (et remplacer le 1 par l'id du VLAN)

Pour configurer un commutateur racine secondaire prenant la place du premier en cas de défaillance:

```
S3(config) # spanning-tree vlan 1 root secondary
```

© Hainaut P. 2017 - www.coursonline.be

18

Spanning tree: commutateur racine

- Pour désigner un commutateur comme commutateur racine:
 - Méthode 2:
`S1(config) # spanning-tree vlan 1 root priority valeur`
où *valeur* est un nombre compris entre 0 et 65536 par pas de 4096
Par défaut, tous les commutateurs reçoivent la priorité 32768
Par défaut, l'utilisation de *primary* (méthode 1) impose 24576 comme priorité
Et l'utilisation de *secondary* impose 28672
- C'est la valeur la plus faible (on parle de coût) qui est retenue

Spanning tree: meilleur chemin

- Une fois que le pont racine a été déterminé, l'algorithme STA calcule le chemin le plus court vers le pont racine
- Chaque commutateur utilise l'algorithme STA pour identifier les ports devant être bloqués
- Pendant que l'algorithme STA détermine les meilleurs chemins vers le pont racine pour toutes les destinations du domaine de diffusion, aucune donnée ne peut être transmise sur le réseau (temps de convergence)

Spanning tree: meilleur chemin

- L'algorithme STA prend en compte les coûts de chemin et de port lors de la sélection du chemin qui ne doit pas être bloqué
- Le coût de la route est calculé à l'aide des valeurs de coût de port associées à la vitesse de port de chacun des ports des commutateurs sur un chemin donné
- La somme des valeurs des coûts de ports détermine le coût du chemin global vers le pont racine
- Si plusieurs chemins sont disponibles, l'algorithme STA choisit le chemin doté du coût de chemin le plus faible

© Hainaut P. 2017 - www.coursonline.be

21

Spanning tree: coût des ports

- Coût par défaut des ports:

Vitesse de liaison	Coût du port
10 Gbits/s	2
1 Gbits/s	4
100 Mbits/s	19
10 Mbits/s	100

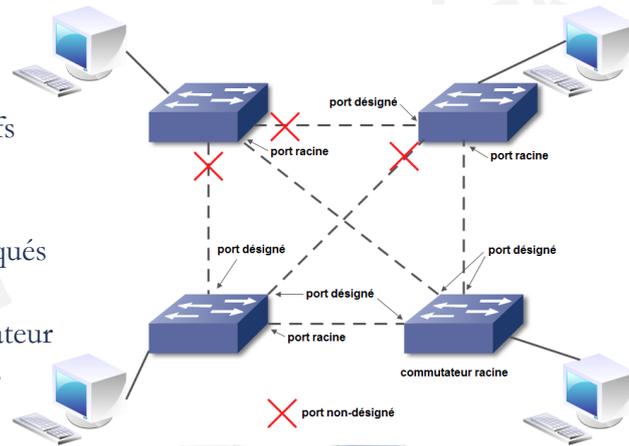
- Pour modifier ce coût par défaut (au niveau d'une interface):
`S2(config-if) # spanning-tree cost 25`
- Pour rétablir le coût par défaut:
`S2(config-if) # no spanning-tree cost`

© Hainaut P. 2017 - www.coursonline.be

22

Spanning tree: ports

- *Ports racine*: ports de commutateur connectés au commutateur racine
- *Ports désignés*: ports de commutateur actifs
- *Ports non désignés*: ports de commutateur bloqués
- *Ports désactivés*: ports de commutateur non opérationnels



© Hainaut P. 2017 - www.coursonline.be

23

Spanning-tree: priorité des ports

- Le système fixe une priorité de port par défaut égale à 128 à laquelle est associée l'id de port
- Ainsi le premier port aura une priorité par défaut de 128.1
- On peut modifier cette priorité par défaut:
S2(config-if) # spanning-tree vlan 1 port-priority 112

La plage va de 0 à 240 par pas de 16

- Comme pour la désignation du commutateur racine, c'est la valeur la plus faible qui sera retenue
- Cela permettra, par exemple, de forcer la sélection d'un port racine

© Hainaut P. 2017 - www.coursonline.be

24

Spanning tree: diagnostic (CISCO)

- Pour le diagnostic:
`switch# show spanning-tree (sb sp)`

Cette commande permet de voir le commutateur racine, le statut des ports connectés, leur coût, le coût des chemins, ...

Remarque: le spanning-tree n'est activé que si le commutateur est connecté à un autre élément du réseau

Spanning tree: diagnostic (CISCO)

```
Switch#sh sp
VLAN0001
Spanning tree enabled protocol ieee
Root ID    Priority    32769
           Address    0001.4382.0CD5
           This bridge is the root
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
           Address    0001.4382.0CD5
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Fa0/4    Desg FWD 19    128.4   P2p
Fa0/22   Desg FWD 19    128.22  P2p
Fa0/23   Desg FWD 19    128.23  P2p
Fa0/24   Desg FWD 19    128.24  P2p
```

← commutateur racine

```
Switch#sh sp
VLAN0001
Spanning tree enabled protocol ieee
Root ID    Priority    32769
           Address    0001.4382.0CD5
           Cost    19
           Port    22 (FastEthernet0/22)
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
           Address    0040.0BA9.3D80
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Fa0/22   Root FWD 19    128.22  P2p
Fa0/23   Altn BLK 19    128.23  P2p
Fa0/24   Altn BLK 19    128.24  P2p
Fa0/1    Desg FWD 19    128.1   P2p
```

← coût du chemin

↑ rôle, état et coût du port

© Hainaut P. 2017 - www.coursonline.be

Spanning tree: PortFast de CISCO

- Lorsqu'un port de commutateur configuré avec la technologie PortFast est défini comme port d'accès, ce port passe immédiatement de l'état de blocage à l'état activé, sans passer par les états traditionnels d'écoute et d'apprentissage STP
- Vous pouvez utiliser PortFast uniquement sur les ports d'accès (qui sont connectés à une station de travail ou à un serveur unique) pour permettre à ces périphériques de se connecter immédiatement au réseau au lieu d'attendre la convergence STP

Spanning tree: PortFast de CISCO

- Activation:
switch (config) # interface FastEthernet 0/8 (int f0/8)
switch (config-if) # spanning-tree portfast (span portf)
- Désactivation:
switch (config-if) # no spanning-tree portfast (no span portf)
- Vérification:
show running config (sh run)
...
interface FastEthernet 0/8
switchport mode access
spanning-tree portfast
...

Spanning tree: temps de convergence

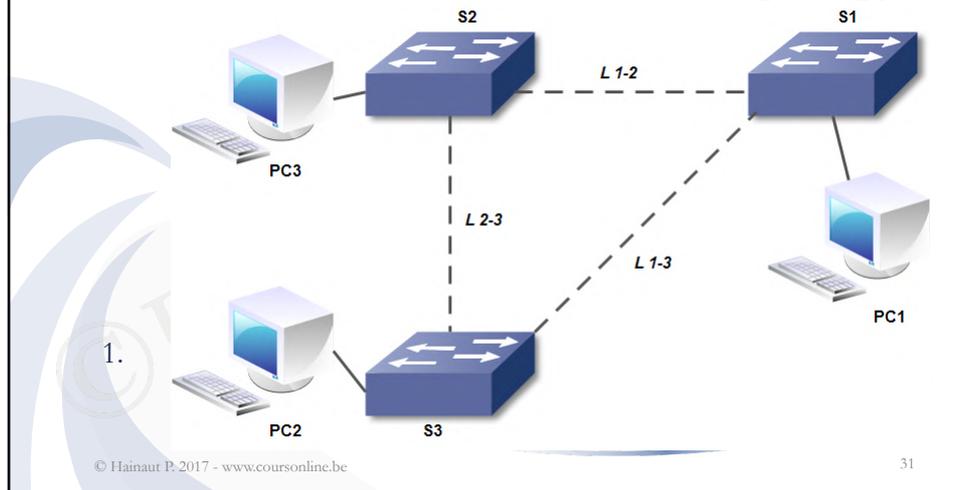
- Le temps de convergence dû à l'algorithme STP n'est pas négligeable (30 à 50 sec)
- En effet, celui-ci procède en 4 étapes:
 - Election du commutateur racine
 - Détermination du port racine de chaque commutateur
 - Détermination du port désigné sur chaque segment
 - Blocage des autres ports
- En cas de changement de topologie (coupure d'une liaison par exemple), le protocole est à nouveau exécuté

Spanning tree: RSTP

- Pour améliorer le temps de convergence, RSTP (Rapid STP) a été mis au point
- Ce temps de convergence passe à +/- 6 sec
- Rapid PVST+ est l'implémentation Cisco du RSTP
- Activation:
switch(config) # spanning-tree mode rapid-pvst

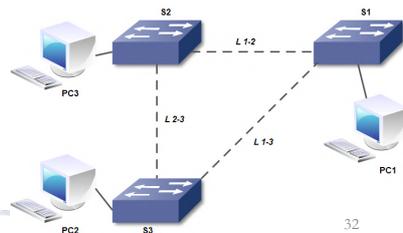
Spanning tree: Exercice

- Exercice: Reproduire la topologie suivante sans la liaison L 1-3



Spanning tree: Exercice

1. Configurez les PC pour qu'ils puissent se pinguer
2. Désactivez le spanning-tree sur les commutateurs (actif par défaut)
3. Ajoutez la liaison L 1-3
4. Retestez les ping
5. Consultez la table arp de chaque PC
6. Utilisez wireshark ou le mode simulation de Packet Tracer pour analyser le trafic
7. Tirez-en les conclusions
8. Activez STP
9. Tirez-en les conclusions
10. Retrouvez le commutateur racine, les ports racine, désignés et non-désignés
11. Changez la configuration pour assigner vous-même le commutateur racine (non réalisable sous Packet Tracer)
12. Remplacez STP par RSTP
13. Tirez-en les conclusions

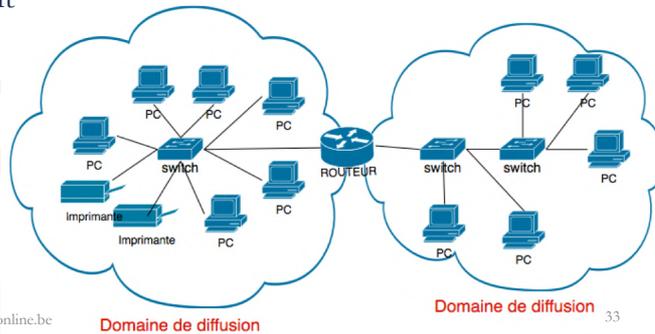


© Hainaut P. 2017 - www.coursonline.be

32

Domaines de diffusion

- Si le commutateur segmente les domaines de collision, il maintient cependant un seul domaine de diffusion
- Les trames de diffusion sont propagées sur tout le réseau, or ces trames sont nombreuses (ARP, DHCP, Netbios, etc)

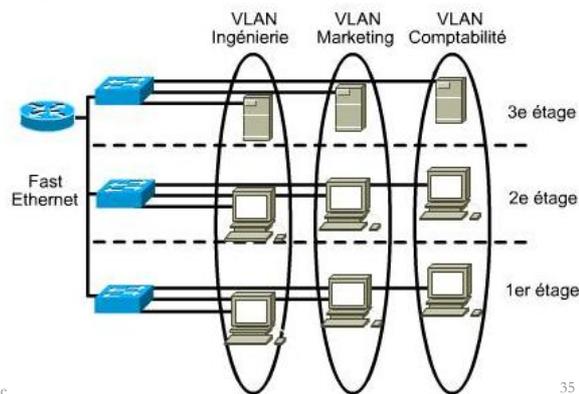


LAN - VLAN

- Un réseau local (LAN) est un réseau physique construit autour d'un commutateur ou de plusieurs en cascades
- Ce réseau local partage un espace d'adressage et un domaine de diffusion
- Un réseau local virtuel (VLAN) est un sous-réseau logique (virtuel) construit dans le réseau physique précédent et permettant de segmenter ce réseau
- Il y a aura autant de domaines de diffusion qu'il y a aura de VLAN mais pas forcément autant d'espaces d'adressage (voir les méthodes de construction des VLAN)

Domaines de diffusion

- Un VLAN permet donc de créer des domaines de diffusion (broadcast domains) gérés par les commutateurs indépendamment de l'emplacement où se situent les nœuds, ce sont des domaines de diffusion gérés logiquement
- Dans l'exemple ci-contre, il y a trois domaines de diffusion au lieu d'un



© Hainaut P. 2017 - www.coursonline.be

35

Avantages des VLAN

- La réduction des messages de diffusion (notamment les requêtes ARP) limités à l'intérieur d'un VLAN
- La création de groupes de travail indépendants de l'infrastructure physique ; possibilité de déplacer la station sans changer de réseau virtuel
- L'augmentation de la sécurité par le contrôle des échanges inter-VLAN utilisant des routeurs (filtrage possible du trafic échangé entre les VLAN)

© Hainaut P. 2017 - www.coursonline.be

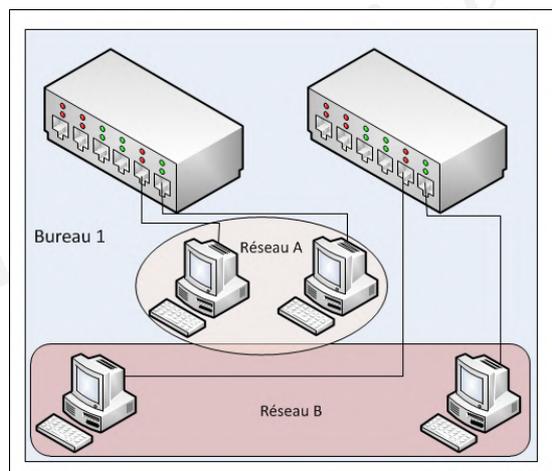
36

Exemples: cas n°1

- Soit un bureau où cohabite des architectes et des ingénieurs
- Ayant des besoins différents, ils sont dans deux réseaux différents
- les architectes seront dans le réseau A et les ingénieurs dans le réseau B

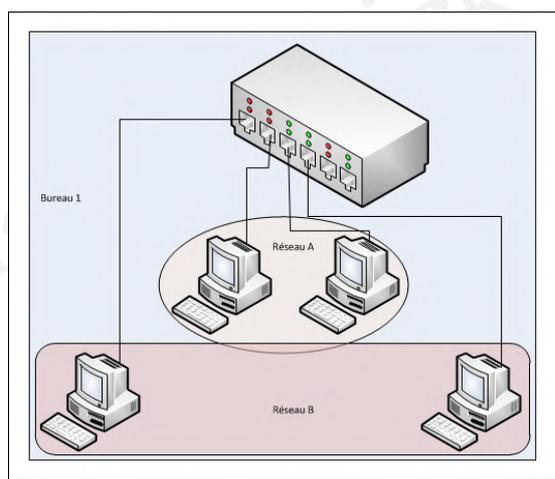
Cas n°1: sans VLAN

- 2 switches sont nécessaires



Cas n°1: avec VLAN

- Un seul switch (manageable) est nécessaire



© Hainaut P. 2017 - www.coursonline.be

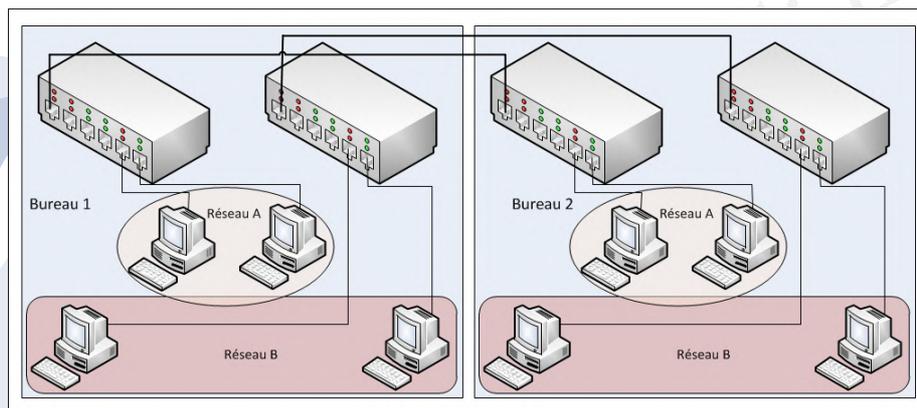
Exemples: cas n°2

- L'entreprise s'est agrandie et nous avons maintenant un ensemble de bureaux où cohabitent architectes et ingénieurs
- Ils sont répartis ensemble dans les différents bureaux pour les échanges d'idées mais ont besoin chacun d'un réseau spécifique
- Les architectes seront toujours dans le réseau A et les ingénieurs dans le réseau B

© Hainaut P. 2017 - www.coursonline.be

40

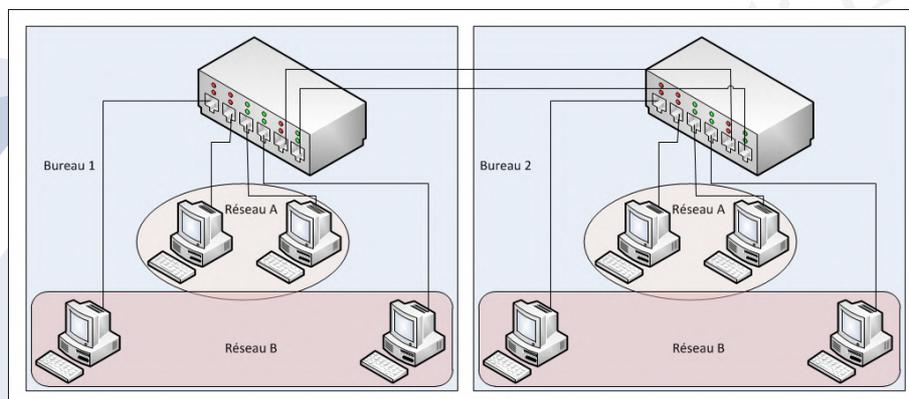
Cas n°2: sans VLAN



© Hainaut P. 2017 - www.coursonline.be

41

Cas n°2: avec VLAN



© Hainaut P. 2017 - www.coursonline.be

42

Types de VLAN

- *VLAN de données*: VLAN créés par l'utilisateur
- *VLAN par défaut*: Chez Cisco, c'est le VLAN 1 dont tous les ports du commutateur font partie par défaut, il ne peut être ni supprimé ni renommé (1 par commutateur)
- *VLAN natif*: il reçoit le trafic non-tagué (qui ne provient pas d'un VLAN). Il est recommandé d'utiliser un autre VLAN que le VLAN 1 (1 par commutateur)

Types de VLAN

- *VLAN de gestion (ou d'administration)*: permet d'accéder aux fonctions de gestion du commutateur et de prendre la main à distance (1 par commutateur)
On attribuera au VLAN de gestion une adresse IP et un masque de sous-réseau
VLAN 1 par défaut mais à changer pour des raisons de sécurité !
- *VLAN voix*: Vu le caractère temps réel de la VOIP, on différencie le trafic voix du trafic de données, il est donc normal de transporter la VOIP sur un VLAN distinct

Organisation des VLAN

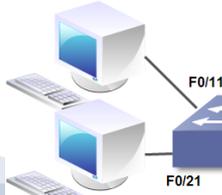
- L'indépendance entre infrastructure physique et groupe de travail implique qu'un commutateur puisse gérer plusieurs VLAN et qu'un même VLAN puisse être réparti sur plusieurs commutateurs
- En conséquence, une trame qui circule dans un commutateur et entre les commutateurs doit pouvoir être associée à un VLAN

Organisation des VLAN

- Pour répondre aux objectifs des VLAN, la règle suivante doit être impérativement respectée : une trame doit être associée à un VLAN et un seul et ne peut pas sortir du VLAN, sinon l'étanchéité du niveau 2 n'est plus respectée
- Il y aura donc deux types de communication:
 - Une communication intra-VLAN: deux hôtes appartenant au même VLAN communiquant ensemble
La communication se passe exclusivement au niveau de la couche 2
 - Une communication inter-VLAN: deux hôtes sur deux VLAN différents communiquant ensemble
La communication doit passer par la couche 3

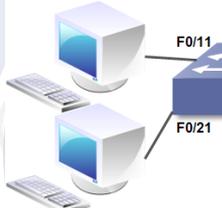
Organisation des VLAN: Exercice

PC1 - 192.168.30.11/24 - VLAN30
Passerelle: 192.168.30.1

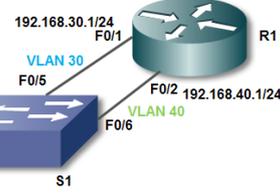


PC2 - 192.168.40.12/24 - VLAN40
Passerelle: 192.168.40.1

PC3 - 192.168.30.13/24 - VLAN30
Passerelle: 192.168.30.1



PC4 - 192.168.30.14/24 - VLAN40
Passerelle: 192.168.40.1



Détaillez toutes les étapes d'envoi d'un paquet de données de:

- PC1 à PC3
- PC1 à PC4

47

Agrégation de VLAN (Trunk)

- Si on regarde le schéma précédent, on voit qu'il faut une ligne par VLAN pour faire la liaison entre les commutateurs
- Si on a deux VLAN, ça va ... mais si on en a dix, ça devient problématique ...
- Il faut donc trouver une solution pour faire passer les VLAN dans une seule ligne -> ça s'appelle le trunk (ou l'agrégation de VLAN en français)

© Hainaut P. 2017 - www.coursonline.be

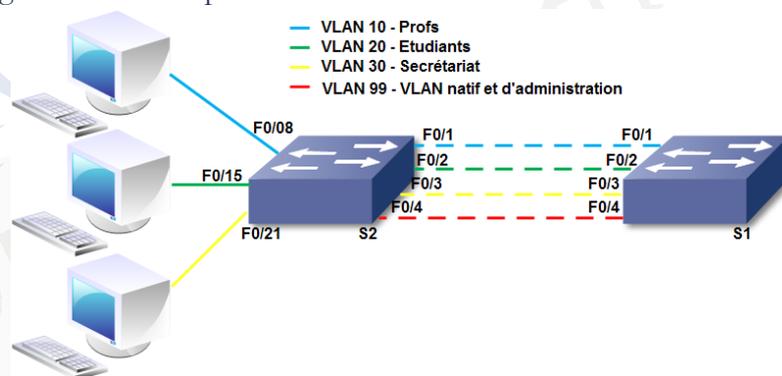
48

Agrégation de VLAN (Trunk)

- Une agrégation est une liaison point à point, entre deux périphériques réseau, qui porte plusieurs VLAN
- Une agrégation de VLAN vous permet d'étendre les VLAN à l'ensemble d'un réseau
- Une agrégation de VLAN n'appartient pas à un VLAN spécifique, mais constitue plutôt un conduit pour les VLAN entre les commutateurs et les routeurs

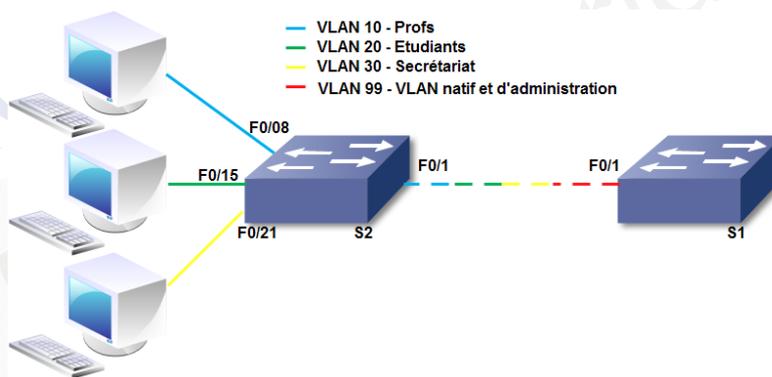
Agrégation de VLAN (Trunk)

- Sans trunk, on monopolise 4 liaisons pour transmettre le trafic des différents VLANS actifs ...
- Imaginez si on multiplie le nombre de VLAN actifs



Agrégation de VLAN (Trunk)

- Avec un trunk, une seule liaison est nécessaire quelque soit le nombre de VLAN actifs



© Hainaut P. 2017 - www.coursonline.be

51

Utilisation des trunks

- On utilisera généralement les trunks entre 2 commutateurs pour la communication intra-VLAN ou entre un commutateur et un routeur pour la communication inter-VLAN
- Si un hôte supporte le trunking (un PC sous Linux par exemple), il peut aussi être connecté à un port du commutateur en mode trunk
- Si pas, le port devra être configuré en mode accès statique

© Hainaut P. 2017 - www.coursonline.be

52

Méthodes de construction des VLAN

- Les méthodes de construction d'un VLAN doivent donc déterminer la façon dont le commutateur va associer la trame à un VLAN

Usuellement, on présente trois méthodes pour créer des VLAN :

- les VLAN par port (niveau 1)
- les VLAN par adresses MAC (niveau 2)
- les VLAN par adresses IP (niveau 3) ainsi que des méthodes dérivées

Les VLAN par port

- On affecte chaque port des commutateurs à un VLAN
- L'appartenance d'une trame à un VLAN est alors déterminée par la connexion de la carte réseau à un port du commutateur
- Les ports sont donc affectés statiquement à un VLAN
- Si on déplace physiquement une station, il faut désaffecter son port du VLAN puis affecter le nouveau port de connexion de la station au bon VLAN
- Si on déplace logiquement une station (on veut la changer de VLAN) il faut modifier l'affectation du port, et l'affecter au nouveau VLAN

Les VLAN par adresse MAC

- On affecte chaque adresse MAC à un VLAN
- L'appartenance d'une trame à un VLAN est déterminée par son adresse MAC
- On affecte dynamiquement les ports des commutateurs à chacun des VLAN en fonction de l'adresse MAC de l'hôte qui émet sur ce port
- 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

© Hainaut P. 2017 - www.coursonline.be

55

Les VLAN par adresse IP (par protocole)

- On affecte une adresse IP à un VLAN
- L'appartenance d'une trame à un VLAN est alors déterminée par l'adresse IP qu'elle contient (le commutateur doit donc accéder à ces informations)
- A partir de l'association IP/VLAN, on affecte dynamiquement les ports des commutateurs à chacun des VLAN
- Dans ce type de VLAN, les commutateurs apprennent automatiquement la configuration des VLAN en accédant aux informations de couche 3. Ceci est un fonctionnement moins rapide que le VLAN de niveau 2
- On parle souvent de VLAN par sous-réseau

© Hainaut P. 2017 - www.coursonline.be

56

Types de commutateurs

- Les commutateurs non-administrables (ce sont toujours des switches « layer 2 »): ne prennent pas en charge les VLAN
- Les commutateurs administrables (manageables) « layer 2 » (les plus courants) travaillant avec les adresses MAC et permettant une association n°de port/adresse MAC
- Ces commutateurs prennent en charge les VLAN par port et par adresse MAC et gèrent la communication intra-VLAN
Exemples chez CISCO: entre autre, séries 2950 et 2960



© Hainaut P. 2017 - www.coursonline.be

57

Types de commutateurs

- Les commutateurs administrables « layer 3 » permettent de construire des VLAN par port, par adresse MAC ou par adresse IP
 - par port => affectation statique des ports dans un VLAN
 - par adresse MAC => affectation dynamique sur base de l'adresse MAC (layer 2) de la station qui émet sur ce port
 - par adresse IP => affectation dynamique sur base de l'adresse IP (layer 3) de la station émettant sur ce port
- Exemples chez CISCO: entre autre, les séries 3750 et 4500



© Hainaut P. 2017 - www.coursonline.be

58

Types de commutateurs

- Au niveau de la commutation des paquets, un switch Layer 3 permet d'effectuer la transmission des paquets sur base des adresses layer 2 (adresses MAC) du destinataire = fonction du switch layer 2 (commutation intra-vlan)
- il permet également d'effectuer la transmission des paquets sur base des adresses layer 3 (adresses IP) du destinataire = fonction du switch layer 3 (commutation inter-vlan)



© Hainaut P. 2017 - www.coursonline.be

59

Types de commutateurs

- Il existe aussi des commutateurs « layer 7 » qui peuvent commuter en fonction des données de la couche application
- Exemple chez CISCO: entre autre, le CSS 11501



© Hainaut P. 2017 - www.coursonline.be

60

La norme 802.1Q

- Le standard IEEE 802.1Q fournit un mécanisme d'encapsulation implanté dans de nombreux équipements de marques différentes
- Son objet est de faire coexister plusieurs réseaux logiques de niveau 3 indépendants au sein d'un même réseau physique de niveau 2, par un mécanisme de virtualisation
- 802.1Q définit le contenu de la balise VLAN (VLAN tag) avec laquelle on complète l'en-tête de trame Ethernet (4 octets en plus)

Rappel: la trame Ethernet

- Deux modèles de trame Ethernet sont encore usitées:
 - La trame Ethernet II
 - La trame 802.3
- Elles peuvent coexister sur un même réseau grâce au champ long/type différent
- Il y a peu de différences entre les deux

Trame Ethernet II

Préambule	Délimiteur de début de trame	Adr. MAC dest.	Adr. MAC source	type	Données	Ctrl
7 octets	1 octet	6 octets	6 octets	2 octets	46-1500 octets	4 octets

Trame IEEE 802.3

Préambule	Délimiteur de début de trame	Adr. MAC dest.	Adr. MAC source	long	Entête LLC & données	Ctrl
7 octets	1 octet	6 octets	6 octets	2 octets	46-1500 octets	4 octets

Rappel: la trame Ethernet

- Le champ préambule permet d'acquérir la synchronisation des horloges de transmission (7x 0xAA)
- Le champ délimiteur de début de trame permet de valider le début de la trame (1x 0xAB)
- Ensuite, viennent les adresses MAC de destination et source, sur 6 octets

Trame Ethernet II

Préambule	Délimiteur de début de trame	Adr. MAC dest.	Adr. MAC source	type	Données	Ctrl
7 octets	1 octet	6 octets	6 octets	2 octets	46-1500 octets	4 octets

Trame IEEE 802.3

Préambule	Délimiteur de début de trame	Adr. MAC dest.	Adr. MAC source	long	Entête LLC & données	Ctrl
7 octets	1 octet	6 octets	6 octets	2 octets	46-1500 octets	4 octets

© Hainaut P. 2017 - www.coursonline.be

63

Rappel: la trame IEEE 802.3

- Le champ longueur indique la taille du champ de données
- Ce champ a une valeur inférieure ou égale à 0x5DC (1500 en décimal), ce qui est normal, le champ de données ayant une longueur maximum de 1500 octets
- Une trame valide ayant une longueur minimale de 64 octets, le champ de données doit faire 46 octets minimum
(64 – 12 (adresses) – 6 (lg+ctrl))

Préambule	Délimiteur de début de trame	Adr. MAC dest.	Adr. MAC source	long	Entête LLC & données	Ctrl
7 octets	1 octet	6 octets	6 octets	2 octets	46-1500 octets	4 octets

© Hainaut P. 2017 - www.coursonline.be

64

Rappel: la trame IEEE 802.3

- Quand ce n'est pas le cas, du bourrage (padding) sans signification est ajouté aux données pour atteindre les 64 octets
- Ce bourrage sera enlevé par la sous-couche de contrôle LLC (située entre la sous-couche MAC et la couche réseau)
- C'est transparent pour l'utilisateur

Préambule	Délimiteur de début de trame	Adr. MAC dest.	Adr. MAC source	long	Entête LLC & données	Ctrl
7 octets	1 octet	6 octets	6 octets	2 octets	46-1500 octets	4 octets

© Hainaut P. 2017 - www.coursonline.be

65

Rappel: la trame Ethernet II

- Le champ type indique le protocole de couche supérieure recevant les données
- Ce champ a une valeur supérieure ou égale à 0x0600, pour permettre une différenciation d'avec la trame 802.3

- Exemples: 0x0800 IPv4
0x86DD IPv6
0x0806 ARP
0x8035 RARP
0x8100 IEEE 802.1Q

Trame Ethernet II

Préambule	Délimiteur de début de trame	Adr. MAC dest.	Adr. MAC source	type	Données	Ctrl
7 octets	1 octet	6 octets	6 octets	2 octets	46-1500 octets	4 octets

© Hainaut P. 2017 - www.coursonline.be

66

Rappel: la trame Ethernet II

- La trame Ethernet II n'ayant de sous-couche LLC, le bourrage éventuel sera enlevé par la couche supérieure

Trame Ethernet II

Préambule	Délimiteur de début de trame	Adr. MAC dest.	Adr. MAC source	type	Données	Ctrl
7 octets	1 octet	6 octets	6 octets	2 octets	46-1500 octets	4 octets

Rappel: la trame Ethernet

- Le champ contrôle permet, grâce à un calcul polynomial de degré 32 (basé sur les adresses, le champ long/type et le champ de données), de vérifier que la trame est correcte
- Si le résultat des calculs à l'émission et à la réception sont les mêmes, la trame est considérée comme correcte

Trame Ethernet II

Préambule	Délimiteur de début de trame	Adr. MAC dest.	Adr. MAC source	type	Données	Ctrl
7 octets	1 octet	6 octets	6 octets	2 octets	46-1500 octets	4 octets

Trame IEEE 802.3

Préambule	Délimiteur de début de trame	Adr. MAC dest.	Adr. MAC source	long	Entête LLC & données	Ctrl
7 octets	1 octet	6 octets	6 octets	2 octets	46-1500 octets	4 octets

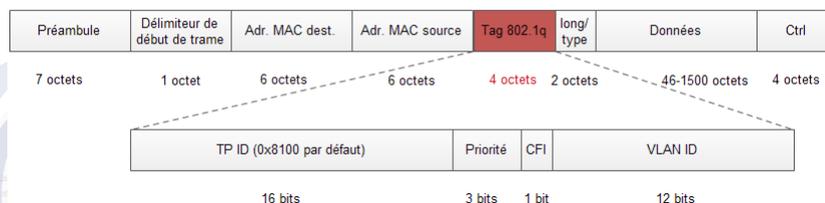
Rappel: la trame Ethernet

- Exercice: Au moyen de Wireshark, analysez le trafic réseau HTTP et déterminez le type de trames Ethernet circulant sur le réseau local

Trame Ethernet taguée

- Comme dit plus haut, la balise VLAN (VLAN Tag) complète l'entête de trame Ethernet par 4 octets

Trame taguée 802.1q



Trame Ethernet taguée

- TPID (Tag Protocol Identifier) est un champ qui permet d'identifier le protocole de la balise insérée, ici 0x8100 pour le 802.1Q
- Le champ priorité fait référence au protocole 802.1p qui permet d'introduire une priorité dans les VLAN (QoS niveau 2), indépendante de la priorité IP (QoS niveau 3)
8 niveaux de priorité sont ainsi définis permettant par exemple de transmettre en priorité les données « voix »

VLAN Tag



© Hainaut P. 2017 - www.coursonline.be

71

Trame Ethernet taguée

- CFI (Canonical Format Identifier) assure la compatibilité entre Ethernet et Token-Ring. Sera toujours à 0 dans un commutateur Ethernet
- VLAN ID permet d'identifier le VLAN auquel appartient la trame
- Permet de coder $2^{12} = 4096 - 2 = 4094$ VLAN
 - Les identifiants VLAN vont de 1 à 4094
 - 0 signifie pas de VLAN
 - 4095 est réservé
 - 1002 à 1005 sont réservés pour des VLAN FDDI et Token-Ring

VLAN Tag



© Hainaut P. 2017 - www.coursonline.be

72

Trame Ethernet taguée

- Les identifiants de 1 à 1024 font partie de la plage normale
- Les identifiants de 1025 à 4094 font partie de la plage étendue qui n'est pas supportée par tous les commutateurs
- Le nombre de VLAN supportés par un commutateur dépend du modèle
Exemple: Le CISCO Catalyst 2960 supporte 255 VLAN maximum
- Les VLAN 1, 1002 à 1005 sont créés par défaut et ne peuvent être supprimés

VLAN Tag

TP ID (0x8100 par défaut)	Priorité	CFI	VLAN ID
16 bits	3 bits	1 bit	12 bits

802.1Q: Activation sur CISCO

- Avant la norme 802.1Q, CISCO avait développé un protocole propriétaire ISL
- Celui-ci est maintenant obsolète
- La commande pour passer d'ISL à 802.1Q était:
switch (config-if) # switchport trunk encapsulation dot1q
- La configuration des VLAN est stockée en flash dans le fichier vlan.dat

Création d'un VLAN

- Pour créer un VLAN, il suffit de l'identifier:

```
S1(config) # vlan 99
```

- On peut éventuellement le nommer:

```
S1(config-vlan) # name vlan_natif
```

- Pour supprimer un VLAN:

```
S1(config) # no vlan 99
```

- Pour désactiver un VLAN:

```
S1(config) # shutdown vlan 99
```

Affectation d'un port à un VLAN

- Pour affecter un port unique à un VLAN:

```
S1 (config) # int f0/8
```

```
S1 (config-if) # switchport mode access
```

```
S1 (config-if) # switchport access vlan 10
```

- Pour affecter une série de ports à un VLAN:

```
S1 (config) # int range f0/8-13
```

```
S1 (config-if-range) # switchport mode access
```

```
S1 (config-if-range) # switchport access vlan 10
```

- Les ports sont ici d'abord configuré en mode accès statique (qui est le mode par défaut), pour être connectés à des hôtes

Affectation d'un port à un VLAN

- Pour supprimer la configuration, mettre no devant la commande :

```
S1 (config) # int f0/8
```

```
S1 (config-if) # no switchport access vlan 10
```

- Pour une série de ports:

```
S1 (config) # int range f0/8-13
```

```
S1 (config-if-range) # no switchport access vlan 10
```

Configuration d'un port en mode trunk

- Pour configurer un port en mode trunk:

```
switch (config) # int f0/1
```

```
switch (config-if) # switchport mode trunk (sw m tr)
```

- Pour indiquer quels VLAN peuvent passer par le trunk:

```
switch (config-if) # switchport trunk allowed vlan add 10, 20, 30
```

- Pour interdire un (ou des) VLAN à passer par le trunk:

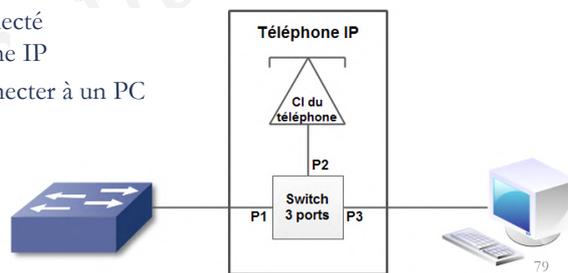
```
switch (config-if) # switchport trunk allowed vlan remove 20
```

- Pour supprimer le passage des VLAN par le trunk:

```
switch (config-if) # no switchport trunk allowed vlan
```

Configuration d'un port en mode voix

- Généralement, on configure un VLAN par port (hors trunk)
- La voix sur IP (VOIP) constitue un cas particulier, chez CISCO du moins
- En effet, les téléphones IP CISCO possèdent un commutateur interne à 3 ports
 - Un port pour se connecter au commutateur
 - Un port interne connecté au circuit du téléphone IP
 - Un port pour se connecter à un PC



Configuration d'un port en mode voix

- On doit donc avoir à la fois un VLAN voix et un VLAN données

```
S1(config) # vlan 60
S1(config-vlan) # name voix
S1(config-vlan) # exit
S1 (config) # int f0/22
S1 (config-if) # switchport mode access
S1 (config-if) # switchport access vlan 10
S1 (config-if) # switchport voice vlan 60
S1 (config-if) # exit
```

Vérification de la configuration des VLAN

- Pour vérifier la configuration des différents VLAN et l'affectation des ports:

```
S1 # show vlan
```

ou

```
S1 # show vlan brief
```

- Pour avoir des infos sur un VLAN en particulier:

```
S1 # show vlan id 10
```

ou

```
S1 # show vlan name profs
```

Configuration du VLAN natif

- Le VLAN natif prend en charge le trafic non-étiqueté et abandonne le trafic étiqueté (tagué) -> ne jamais envoyer du trafic étiqueté sur le VLAN natif
- Par défaut, le VLAN natif est le VLAN 1

- Pour changer cela:

```
switch (config) # int f0/1
```

```
switch (config-if) # switchport mode trunk (sw m tr)
```

```
switch (config-if) # switchport trunk native vlan 99 (sw tr n v 99)
```

Dans cet exemple, on configure le port 1 du commutateur en mode trunk et on configure le VLAN natif avec l'id 99

Configuration du VLAN natif

- Attention que tous les ports trunk doivent avoir le même VLAN natif (et par extension tous les commutateurs interconnectés), il faudra donc répéter la configuration précédente sur les autres ports trunk et commutateurs sous peine d'avoir un message du système:
« %CDP4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (99), with S2 FastEthernet0/1 (1). »
- Pour que le VLAN natif soit actif, il faut qu'il soit créé sinon il sera renseigné comme inactif

Configuration du VLAN natif

- Vérification de la configuration précédente (sur les ports trunk):
S1 # show interfaces f0/1 switchport (sh int f0/1 sw)
- Avant config.

```
Switch>en
Switch#show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
Switch#
```

Après config.

```
S1#sh int f0/1 sw
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (vlan_natif)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
S1#
```

Configuration du VLAN natif

- Pour revenir à la situation par défaut (VLAN 1 comme VLAN natif):

```
S1 (config-if) # no switchport trunk native vlan
```

Configuration du VLAN de gestion

- Il faut d'abord créer le VLAN de gestion

```
S1(config) # vlan 98
```

```
S1(config-vlan) # name vlan_gestion
```

```
S1(config-vlan) # exit
```

- Il faut ensuite affecter des paramètres IP à ce VLAN de gestion

```
S1(config) # interface vlan 98
```

```
S1(config-vlan) # ip address 192.168.0.254 255.255.255.0
```

```
S1(config-vlan) # exit
```

- Le VLAN de gestion peut être combiné avec le vlan natif pour ne former qu'un VLAN

Configuration du VLAN de gestion

- Pour pouvoir communiquer avec le switch, il faut encore indiquer la passerelle pour le vlan **98** présente sur le routeur
S1(config) # ip default-gateway 192.168.0.1 255.255.255.0
- Sur le routeur, pour le vlan **98**, on aura la configuration suivante:
Router(config)#interface f0/0
Router(config-if)#no ip address
Router(config-if)#no shut
Router(config-if)#interface f0/0.98
Router(config-subif)#encapsulation dot1q 98
Router(config-subif)#ip address 192.168.0.1 255.255.255.0
- A répéter (3 dernières lignes) pour tous les vlans passant par le trunk

© Hainaut P. 2017 - www.coursonline.be

87

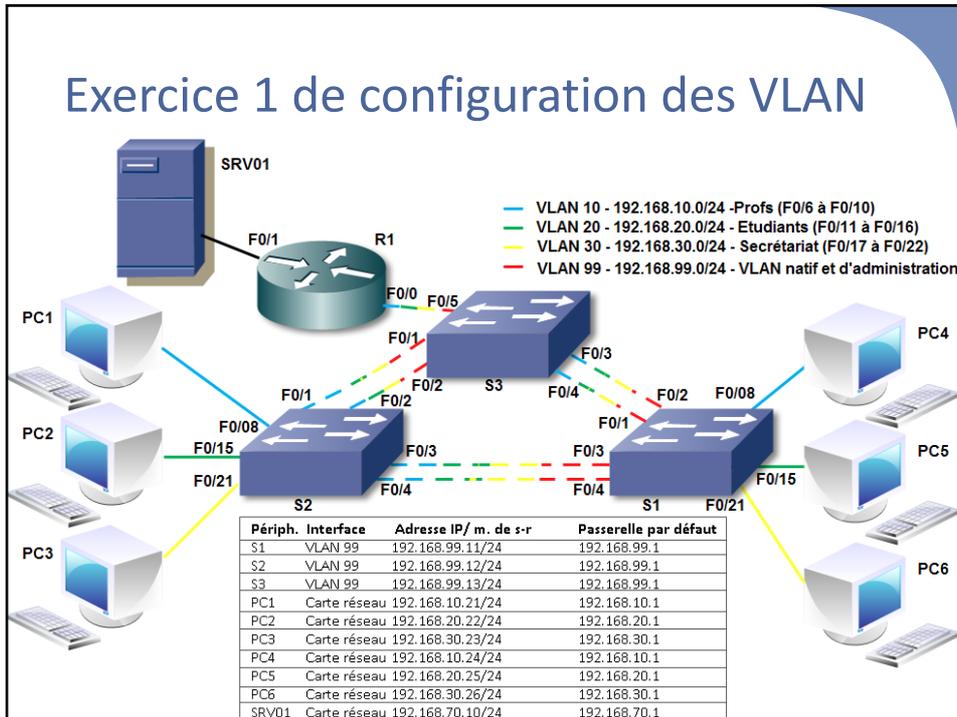
Exercice 1 de configuration des VLAN

- Je vous propose un premier exercice récapitulatif qui reprend ce qu'on a vu jusqu'à présent (VLAN par port)
- Nous allons procéder par étape et décomposer cet exercice
- Il nous permettra:
 - De configurer le spanning tree
 - De configurer des vlans et de les affecter à des ports
 - De tester la communication intra-vlan
 - De configurer un routeur de façon à gérer le trafic inter-vlan
 - De configurer un serveur Web linux pour communiquer avec les postes de travail

© Hainaut P. 2017 - www.coursonline.be

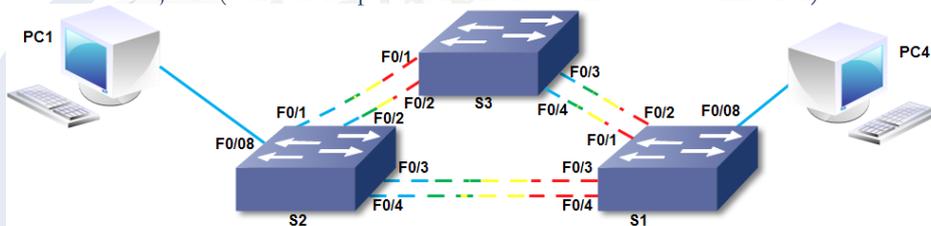
88

Exercice 1 de configuration des VLAN



Exercice 1 de configuration des VLAN

- Première étape: configuration du spanning-tree
 - S3 doit être le commutateur racine
 - F0/1 et F0/3 doivent être ports racines
 - Ces deux points sont non réalisables sous Packet Tracer -> si vous faites la manipulation sous PT, utilisez la configuration automatique du STP et passez simplement du stp au rstp
 - Supprimez les connexions entre S2 et S3 et vérifiez que le système fonctionne toujours (attribuez les paramètres IP nécessaire à cette vérification)

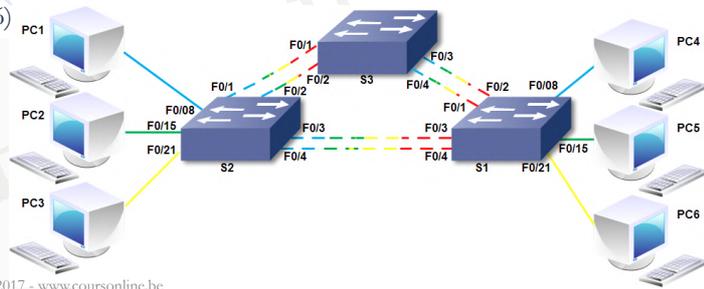


© Hainaut P. 2017 - www.coursonline.be

90

Exercice 1 de configuration des VLAN

- Deuxième étape: configuration et test des VLAN
 - Attribuez les paramètres IP aux différentes interfaces
 - Créez les différents vlan et affectez-y les ports désignés
 - Créez les trunks et désignez les vlans passant par eux
 - Donnez des paramètres IP au vlan d'administration
 - Testez la communication intra-vlan (PC1 -> PC4, PC2 -> PC5, PC3 -> PC6)

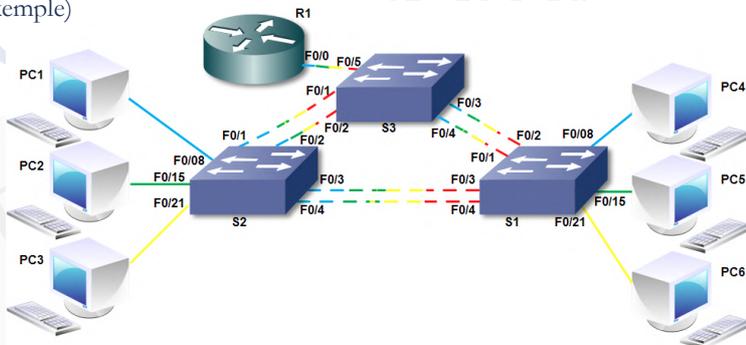


© Hainaut P. 2017 - www.coursonline.be

91

Exercice 1 de configuration des VLAN

- Troisième étape: communication inter-vlan
 - Configurez le routeur pour qu'il prenne en charge le trunk et les différents vlans (voir dia 87 et cherchez sur le net au besoin)
 - Configurez-le et testez la communication inter-vlan (PC1->PC5 par exemple)

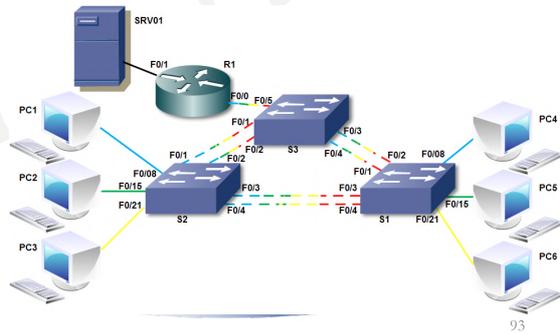


© Hainaut P. 2017 - www.coursonline.be

92

Exercice 1 de configuration des VLAN

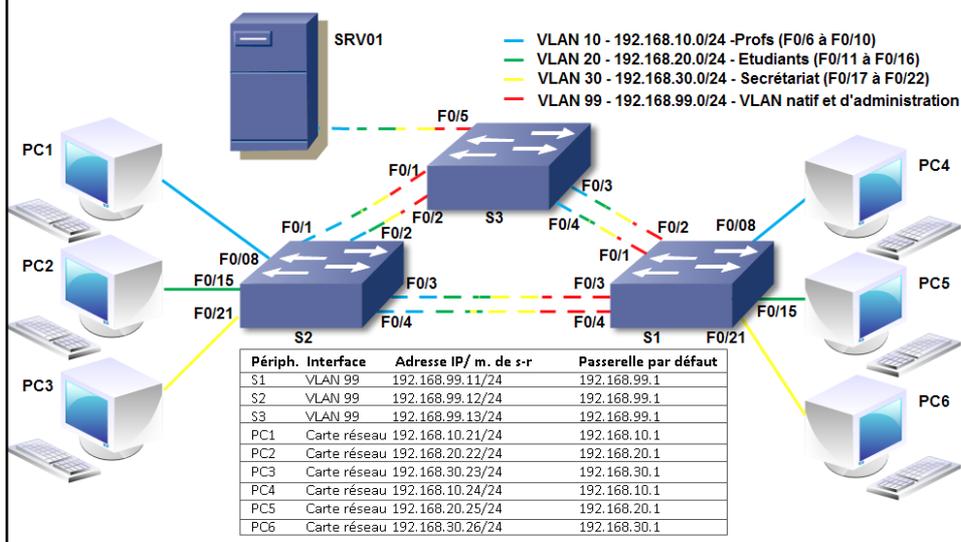
- Quatrième étape: configuration du serveur linux
 - Configurez un petit serveur web apache hébergeant un intranet (réalisable sous Packet Tracer)
 - Connectez ce serveur au routeur par une liaison point à point classique
 - Configurez le routeur pour que chaque VLAN ait accès au site intranet
 - Testez la disponibilité du site sur les différents PC



© Hainaut P. 2017 - www.coursonline.be

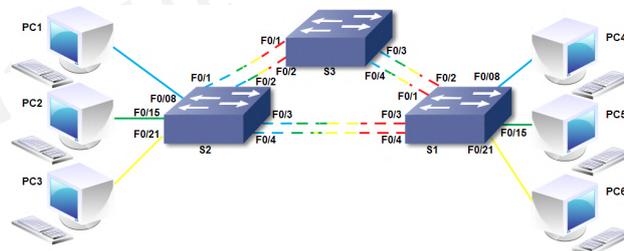
93

Exercice 2 de configuration des VLAN



Exercice 2 de configuration des VLAN

- Ce deuxième exercice est une variante du premier; le routeur est remplacé par le serveur Web qui devra donc gérer le trunk et le trafic inter-VLAN
- Les deux premières étapes sont les mêmes que dans l'exercice précédent (configuration du STP et de la communication intra-VLAN)

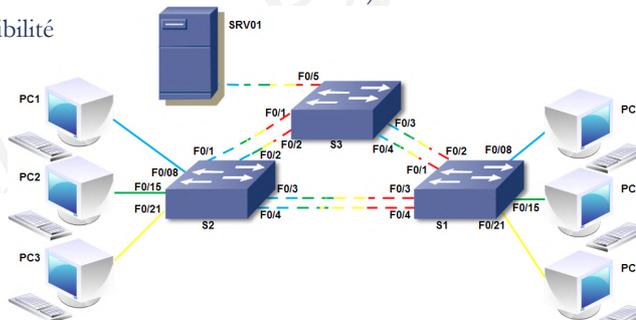


© Hainaut P. 2017 - www.coursonline.be

95

Exercice 2 de configuration des VLAN

- Troisième étape: configuration du serveur linux
 - Configurez un petit serveur web apache hébergeant un intranet
 - Recherchez comment configurer la carte réseau du serveur pour qu'elle fonctionne avec des interfaces virtuelles et qu'elle accepte le trafic VLAN en mode trunk (non réalisable sous Packet Tracer...)
 - Testez la disponibilité du site sur les différents PC



© Hainaut P. 2017 - www.coursonline.be

96

NOTIONS COMPLÉMENTAIRES

© Hainaut P. 2017 - www.coursonline.be

97

EtherChannel: Principes

- EtherChannel est une technologie d'agrégation de liens propriétaire Cisco
- Elle permet d'assembler plusieurs liens physiques Ethernet en un lien logique, comme si ces connections n'en formaient qu'une
- Le but est d'augmenter la vitesse et la tolérance aux pannes entre les commutateurs, les routeurs et les serveurs
- Un lien EtherChannel groupe de deux à huit liens actifs 100 Mbit/s, 1 Gbit/s et 10 Gbit/s, plus éventuellement un à huit liens inactifs en réserve qui deviennent actifs quand des liens actifs sont coupés

© Hainaut P. 2017 - www.coursonline.be

98

EtherChannel: Principes

- EtherChannel est principalement utilisé entre les switches du réseau local, mais on peut aussi l'utiliser pour connecter des serveurs et/ou des postes utilisateurs (en fonction de la compatibilité matérielle et logicielle)
- La technologie EtherChannel a été inventée par la société Kalpana au début des années 1990
- Cette société a ensuite été rachetée par Cisco en 1994
- En 2000, l'IEEE a publié le standard 802.3ad, qui est une version ouverte de EtherChannel

© Hainaut P. 2017 - www.coursonline.be

99

EtherChannel: Principes

- EtherChannel ne nécessite pas de câblage spécifique, il peut donc être utilisé avec des câbles UTP existants ou de la fibre
- Toutes les interfaces groupées doivent fonctionner à la même vitesse et travailler avec le même duplex (full ou half)
- Tous les liens participant à EtherChannel partagent la même adresse MAC
- Cela rend EtherChannel transparent aux protocoles réseau, aux applications et aux utilisateurs, car ils ne voient qu'une seule connexion logique et n'ont pas connaissance des différents liens physiques

© Hainaut P. 2017 - www.coursonline.be

100

EtherChannel: Principes

- EtherChannel répartit les paquets sur les différents ports actifs
- On obtient une répartition de charge équitable dans les configurations à 2, 4 ou 8 ports, tandis que les autres configurations mènent à une répartition inéquitable des échanges

EtherChannel: Principes

- Il existe 2 protocoles d'agrégation de liens
 - Port Aggregation Protocol (PAgP), propriétaire Cisco
 - Link Aggregation Protocol (LACP), normalisé IEEE 802.3ad
- Les protocoles EtherChannel et IEEE 802.3ad sont très semblables et accomplissent le même but. 802.3ad est maintenant le plus utilisé
- Les différences principales sont:
 - EtherChannel nécessite de configurer précisément le commutateur, alors que 802.3ad n'a besoin que d'une configuration initiale
 - EtherChannel prend en charge plusieurs modes de distribution de la charge sur les différents liens, alors que 802.3ad n'a qu'un mode standard
 - EtherChannel peut être configuré automatiquement à la fois par LACP et par PAgP, tandis que 802.3ad ne peut l'être que par LACP

EtherChannel: Configuration

- Activation du canal EtherChannel
S1(config) # interface port-channel 1
S1(config-if) # exit
- Définition des interfaces constituant l'EtherChannel (1^{ère} méthode en définissant un "range")
S1(config)# interface range fa0/23-24
S1(config-range-if)#
- Choix du protocole
S1(config-range-if) # channel-protocol lacp ou pagp

EtherChannel: Configuration

- Choix du mode (dépend du protocole choisi précédemment)
S1(config-range-if)# channel-group 1 mode mode

PAgP	LACP
auto: ce mode place l'interface dans un état passif dans lequel elle répond aux paquets PAgP qu'elle reçoit, mais ne déclenche pas la négociation PAgP. C'est le mode par défaut.	passive: ce mode place l'interface dans un état passif dans lequel elle répond aux paquets LACP qu'elle reçoit, mais ne déclenche pas la négociation LACP. C'est le mode par défaut.
desirable: ce mode place l'interface dans un état actif dans lequel elle initialise la négociation PAgP en envoyant des paquets PAgP.	active: ce mode place l'interface dans un état actif dans lequel elle initialise la négociation LACP en envoyant des paquets LACP.
on: ce mode force l'interface EtherChannel à ne pas utiliser les protocoles PAgP et LACP	on: ce mode force l'interface EtherChannel à ne pas utiliser les protocoles PAgP et LACP

EtherChannel: Configuration

- Combinaisons possibles:

Switch 1	switch2	Etherchannel OK ?	protocole
AUTO	AUTO	NON	PAgP
AUTO	DESIRABLE	OUI	PAgP
AUTO	ON	NON	
DESIRABLE	DESIRABLE	OUI	PAgP
DESIRABLE	ON	NON	
ON	ON	OUI	-
PASSIVE	PASSIVE	NON	LACP
PASSIVE	ACTIVE	OUI	LACP
PASSIVE	ON	NON	
ACTIVE	ACTIVE	OUI	LACP
ACTIVE	ON	NON	

EtherChannel: Configuration

- Choix du mode (exemple avec LACP)
 - S1(config-range-if)# channel-group 1 mode active*
 - S2(config-range-if)# channel-group 1 mode passive*
 - (pour ce qui précède S2 est configuré de manière identique à S1)
- Configuration du mode trunk (pas obligatoire mais essentiel si plusieurs VLAN sont utilisés)
 - switch1(config-range-if)# switchport mode trunk*
- Activation des interfaces du "range"
 - switch1(config-range-if)# no shutdown*

EtherChannel: Configuration

- Autre façon de configurer (par interfaces)

```
S1(config)# interface port-channel 1  
S1(config-if)# exit
```

```
S1(config)# interface fa0/2  
S1(config-if)# channel-group 1 mode on  
S1(config-if)# exit
```

```
S1(config)# interface fa0/3  
S1(config-if)# channel-group 1 mode on  
S1(config-if)# exit
```

```
S1(config)# interface port-channel 1  
S1(config-if)# switchport mode trunk
```

© Hainaut P. 2017 - www.coursonline.be

107

EtherChannel: Configuration

- Remarque: le mode **on** sera généralement utilisé lorsqu'on interface un switch et un autre périphérique avec une liaison EtherChannel, lorsque le périphérique ne supporte pas les protocoles PAgP et LACP

© Hainaut P. 2017 - www.coursonline.be

108

EtherChannel: VLAN natif

- Pour changer le VLAN natif véhiculé par l'EtherChannel:

```
S1(config)# interface port-channel 1
S1(config-if) # switchport trunk native vlan 99 (sw tr n v 99)
S1(config-if)# exit
```

EtherChannel: Vérification

- Il y a plusieurs façons de vérifier que notre lien EtherChannel fonctionne

- Via STP: les deux liens doivent maintenant être en fonction

- Par les commandes:

```
S1#show interfaces etherchannel
```

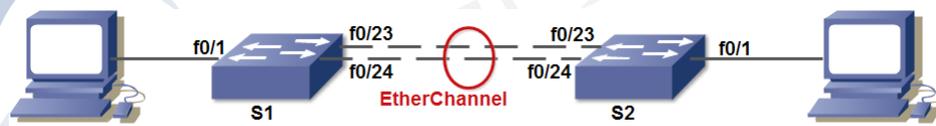
```
S1#show etherchannel summary
```

```
S1#show etherchannel port-channel
```

qui donnent différentes informations sur l'EtherChannel mis en place (s'il est actif, les ports utilisés, le protocole utilisé, ...)

EtherChannel: Vérification

- Pour vérifier le gain au niveau de la bande passante, on câblera le schéma suivant avec des machines physiques et on utilisera un outil comme *netperf*



© Hainaut P. 2017 - www.coursonline.be

111

Protocole VTP (propriétaire CISCO)

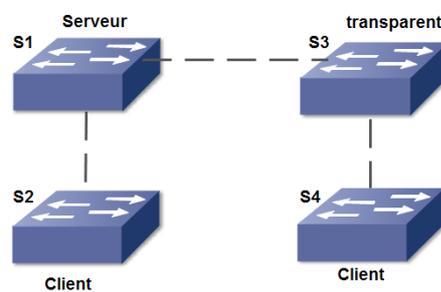
- Le protocole VTP (VLAN Trunking Protocol) permet de configurer un commutateur pour qu'il propage des configurations VLAN à d'autres commutateurs du réseau (au moyen d'annonces VTP)
- Le protocole VTP (protocole de messagerie de couche 2) assure la cohérence de la configuration VLAN en gérant l'ajout, la suppression et la modification des VLAN sur l'ensemble des commutateurs faisant partie d'un domaine VTP
- Le commutateur peut être configuré dans le rôle d'un serveur VTP, d'un client VTP ou d'un commutateur transparent

© Hainaut P. 2017 - www.coursonline.be

112

Protocole VTP

- les commutateurs transparents transmettent les annonces VTP aux clients et serveurs VTP mais ne participent pas au protocole VTP
- Les réseaux locaux virtuels créés, renommés ou supprimés sur un commutateur transparent sont uniquement associés à ce commutateur



© Hainaut P. 2017 - www.coursonline.be

113

Protocole VTP

- Le protocole VTP détecte uniquement les réseaux locaux virtuels de plage normale (ID de VLAN de 1 à 1005)
- Les réseaux locaux virtuels de plage étendue (ID supérieur à 1005) ne sont donc pas pris en charge par le protocole VTP

© Hainaut P. 2017 - www.coursonline.be

114

Protocole VTP: remarque

- Il est conseillé de configurer deux serveurs VTP pour des raisons de redondance
- Le protocole VTP mémorise les configurations VLAN dans la base de données VLAN appelée *vlan.dat*

Protocole VTP: configuration

- La configuration VTP par défaut est:
 - Version VTP = 1
 - Nom de domaine VTP = null
 - Mode VTP = Serveur
 - Révision config = 0
 - VLAN = 1
- Affichage de l'état VTP: *S1#show vtp status*
- Remarque: vous pouvez uniquement ajouter dans le domaine VTP, des commutateurs qui se présentent avec leur configuration VTP par défaut, sous peine de problèmes de cohérence du domaine VTP

Protocole VTP: configuration

- Avant de connecter tout commutateur, il faut d'abord vérifier qu'il soit en configuration par défaut, sinon il faut la rétablir
- Sur le serveur VTP, on configure le nom de domaine VTP, la version et les VLAN et trunk si ce n'est déjà fait
- Sur le client VTP, on active le mode client VTP

Configuration VTP: domaine

- Un domaine VTP se compose d'un ou 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.

Configuration VTP: serveur

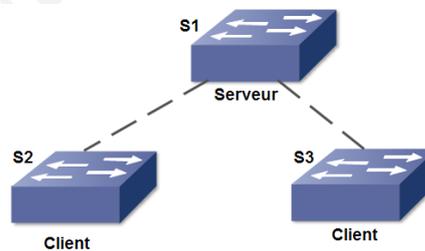
- Pour configurer le nom de domaine sur le serveur VTP:
S1(config)#vtp domain isat
- Pour sécuriser la configuration du serveur VTP, on peut assigner un mot de passe:
S1(config)#vtp password password
- VTP possède 3 versions. Les versions 1 et 2 sont supportées par la plupart des commutateurs, mais on peut utiliser une seule version par domaine
- Pour changer de version:
S1(config)#vtp version 1

Configuration VTP: client

- Configuration du mode (serveur par défaut):
S1(config)#vtp mode client
- Remarque: toutes les commandes précédentes peuvent être inversées par le commutateur *no*

Configuration VTP: vérification

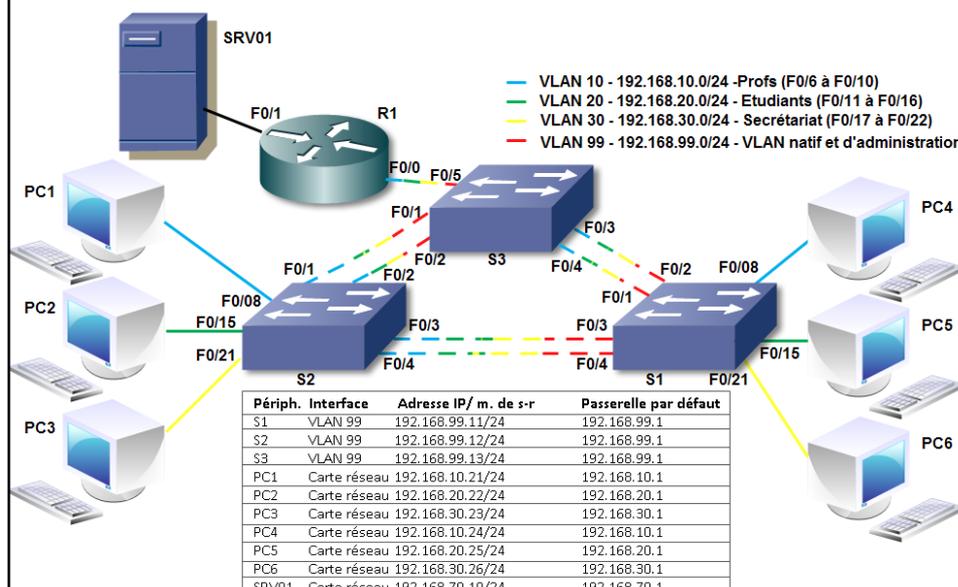
- Pour vérifier la configuration et l'état VTP, on retrouve la commande:
S1#show vtp status
- Une fois la configuration effectuée sur chacun des commutateurs, on peut les connecter ensemble et vérifier la propagation de la configuration VLAN sur les commutateurs clients VTP



© Hainaut P. 2017 - www.coursonline.be

121

Configuration VTP: Exercice



Configuration VTP: Exercice

- Reprenez l'exercice 1 des VLAN avec maintenant un EtherChannel entre les trois switches
- S3 sera serveur VTP
- S1 et S2 seront clients VTP
- Tirez les conclusions au niveau du VTP: qu'est-ce qui est diffusé ? Est-ce intéressant ou pas ?

Conclusion

- Voici une introduction au domaine des VLAN qui sont très utilisés dans les réseaux d'entreprise
- Merci de votre attention