C4 : VTP/STP
M1 – ARCHITECTURE DES RESEAUX

Sondes Kallel Khemiri
PRISM/HPC-NETS
sondes.kallel@prism.uvsq.fr

Organisation

- 9 heures de cours (6 cours)
  - 6 séances de 1h30 heures
    - 1,5 heures : Introduction : Réseaux Locaux (CSMA/CD) C1
    - 1,5 heures : Réseaux Locaux Méthodes d'accès C2
    - 1,5 heures : Les VLANs C3
    - 1,5 heures : VTP/STP C4
    - 1,5 heures : Interconnexion des LANs C5
    - 1,5 heures : Interconnexion des LANs C6
- 18 heures de travaux dirigés
  - 6 séances de TDs/TPs de 3 heures
  - Salles réseaux : découverte et configuration de matériels cisco
    - Séance 1 et 2 : 2 TDS sur les LAN et les méthodes d'accès
    - Séance 3 TP VLAN sur Packet Tracer
    - Séance 4 TP VTP/STP sur Packet Tracer
    - Séance 5 TP Configuration de base d'un périphérique Cisco
    - Séance 6 TP Configuration de base d'un périphérique Cisco
- 1 CC

Objectifs pédagogiques

- Acquérir une culture générale sur l'architecture des réseaux et une bonne connaissance des réseaux LAN
  - Architectures et topologies des réseaux
  - Les réseaux locaux LAN: techniques d'accès CSMA/CD, Token ring, Ethernet, VLAN
  - Interconnexion des réseaux Locaux
- Consolidation avec des travaux pratiques
  - Packet tracer : un simulateur de matériel réseau Cisco (routeurs, commutateurs)
    - Cartable numérique
  - Salles réseaux : découverte et configuration de matériels Cisco
    - http://e-campus2.uvsq.fr : vérifier votre accès (login + mdp)

Références

- Analyse structurée des réseaux, 2ème édition, James Kurose et Keith Ross, Traduction par Stéphane Pauquet, Pearson Education France 2003
- Andrew Tanenbaum, *«Réseaux »* Dunod 2002
- Guy Pujolle, *« Les Réseaux »,* Eyrolles, ed. 2005
- Khaldoun Alagha & Guy Pujolle & Guillaume Vivier, *« Réseaux sans fil et mobiles »*, octobre 2001
- Claude Servin, « *Réseaux et télécoms »,* Dunod 2003
- L. Toutain *« Réseaux Locaux et Internet »*
- Le web
- …

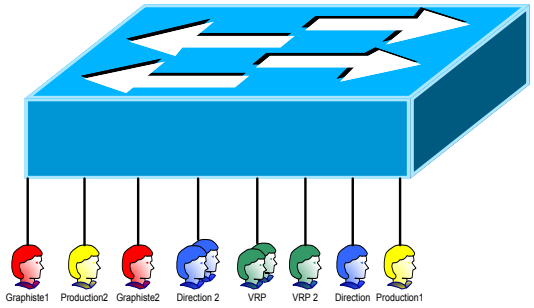
Plan

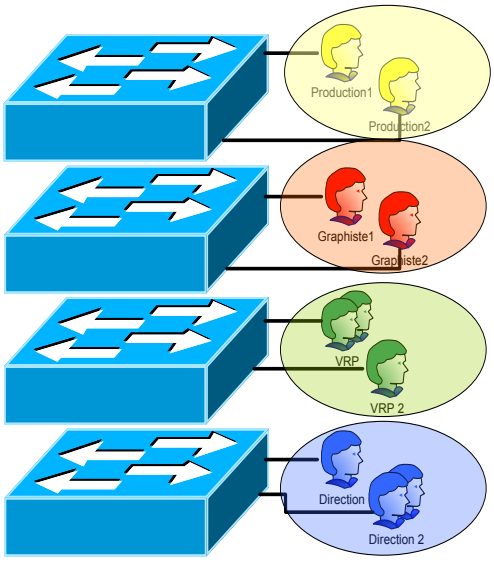
- Rappel VLAN
- La gestion des VLANs
  - VTP
- Le protocole STP

Rappel

- VLANS
  - Ensemble logique d'unités ou d'utilisateurs pouvant être regroupé quelque soit leur emplacement physique
  - Est utilisé pour segmenter les domaines de diffusion
  - Avantages des VLANs
    - Réduction du coût, securité, meilleure performance, meilleure gestion

Rappel





Peuvent être regroupés par :

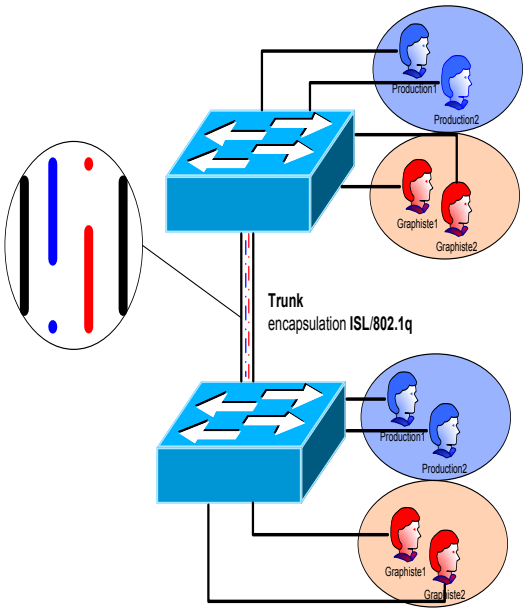
- Fonction (ex : même service dans l'entreprise)
- Application (ex : utilisation des même logiciels)
- Protocole (ex : protocoles de couches 3)
- Identifiant (ex : adresse MAC)
- etc.

Rappel

- Types de Trafic dans un VLAN
  - Données
  - Voix
  - Protocol de réseau
  - Gestion de réseau
- La communication entre différent VLANs requiert l'utilisation de
  - Routeurs

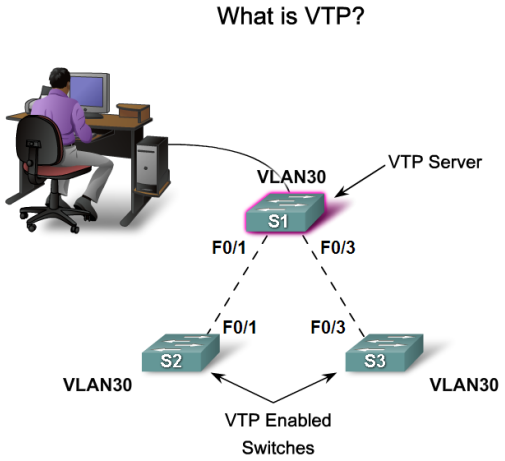
Rappel

- Les trunks
  - Un conduit commun utilisé par plusieurs VLANs pour une communication intra-VLAN
- IEEE 802.1Q
  - Le standard du protocole de trunking
  - Utilise le tagging des trames pour identifier le VLAN auquel appartient la trame



Problématique

- Pour ajouter un VLAN sur un réseau
  - L'administrateur doit l'ajouter sur chaque switch !
  - Necessite beaucoup de manipulation sur de grands réseaux
- Imaginons que nous avons un grand nombre de switch !!!
  - C'est pénible de faire la configuration sur tous les switchs un par un
    - Solution : administration des VLANs



Administration des VLAN ?

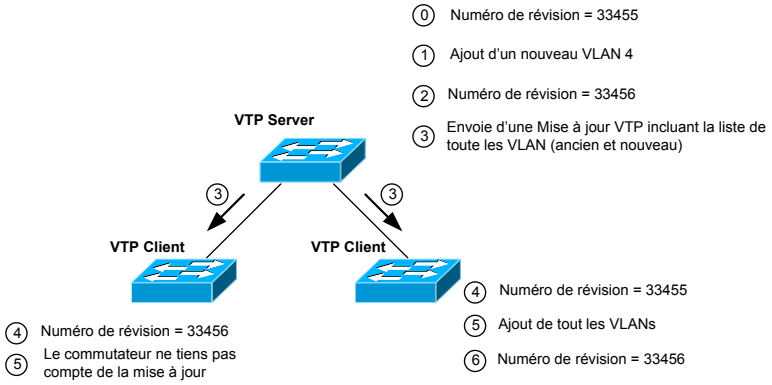
- Pour éviter cela, sur des switchs Cisco, la manipulation peut être faite sur un seul switch
  - La modification sera alors diffusée sur les autres via le protocole VTP : VLAN Trunking Protocol
  - Nous distinguons dans ce cas, des switchs VTP server et des VTP client
  - Le VTP server va diffuser la modification vers les autres switchs VTP client

VTP

- Le protocole VTP (VLAN Trunk Protocol) a pour but de diffuser la création des VLAN à travers les commutateurs
- Réduction de la charge administrative en ne créant les VLAN que sur les commutateurs « servers »
- 3 états VTP possibles pour un commutateur :
  - Server
  - Client
  - Transparent (autonome)

VTP: Fonctionnement du protocole

- Quand il y a changement dans la création des VLAN, une mise à jour est envoyée avec un numéro de révision par les « VTP servers »
- Si un VTP client reçoit une mise à jour avec un numéro de révision supérieur au sien, il l'applique.



Updates toutes les 5 minutes

- Contenu des messages VTP:
  - Un numéro de mise à jour incrémenté à chaque nouvelle diffusion
  - Les noms et numéro de VLANs
    - transmission du fichier « flash:vlan.dat »

Le vocabulaire VTP

- Le VTP domain
  - Tous les switchs appartenant au même VTP domain échangeront leurs informations sur les VLAN
- Les VTP Mode
  - Un switch peut être en mode server
    - il diffuse ses informations sur les VLAN à tous les autres switchs appartenant au même VTP domain
    - ces informations sont stockées en NVRAM et sur un tel switch, il est possible de créer, modifier ou détruire un VLAN du VTP domain
  - en mode client
    - Il stocke uniquement les informations sur les VLAN, transmises par le switch en mode VTP server sur le même domaine.
  - ou bien en mode transparent
    - Il transmet les informations VTP aux autres switchs mais ne les traitent pas. Ces switchs sont autonomes et ne participent pas aux VTP
- Le VTP Pruning
    - Supprime la propagation des messages de broadcast, multicast et autres messages inconnu unicast sur les liens trunks afin d'optimiser la bande passante

VTP: fonctions des modes

- Les modes VTP

Fonction	Mode Server	Mode Client	Mode Transparent
Envoie des MAJ VTP	OUI	NON	NON
Les instances reçoivent les MAJ et synchronise et se synchronise avec les autres Switch	OUI	OUI	NON
Fait suivre les MAJ VTP reçue par une liaison « trunk »	OUI	OUI	OUI
Sauvegarde la configuration des VLAN en NVRAM	OUI	NON	OUI
Peut créer, modifier ou supprimer des VLAN en utilisant les commandes de configurations	OUI	NON	OUI

Commandes Cisco

Commandes de création de domaine

- **vtp domain {nom} [password mdp | pruning | v2-mode]**
  - Donne un nom de domaine
- **vtp mode {server | client | transparent}**
  - Donne un mode VTP au switch

```
Switch>enable
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
Switch(config)# vtp domain LABO
Changing VTP domain from CISCO to LABO
Switch(config)# vtp mode transparent
Setting Device to VTP TRANSPARENT mode.
```


Commandes Cisco

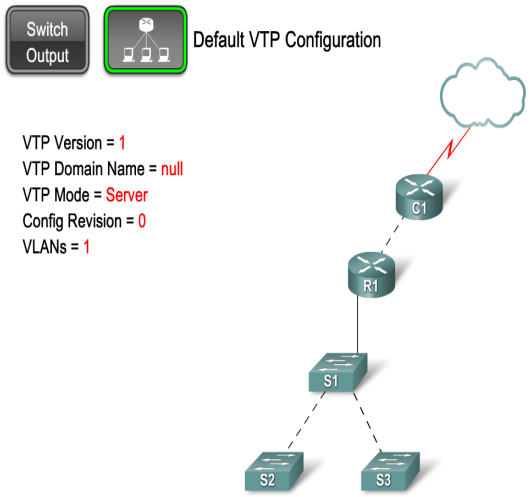
Commandes de visualisation de VLAN

- **show vlan [id {id} | name {nom de vlan}]**
  - Affiche des informations sur le VLAN

```
Switch#show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, 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
10   DRH                              active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10
30   Admin                            active    Fa0/1
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

La configuration par défaut

- Par défaut, un switch est en mode server
  - le VTP domain name = null
  - Tous les ports sont dans le VLAN 1
  - Le numéro de révision de la configuration VTP est 1
  - La version du protocole VTP est 1
    - Il existe 3 versions. Pour un VTP domain, tous les switchs doivent être dans la même version
- La commande show vtp status permet de visualiser la configuration d'un switch



Commandes Cisco

Commandes d'affichage d'état

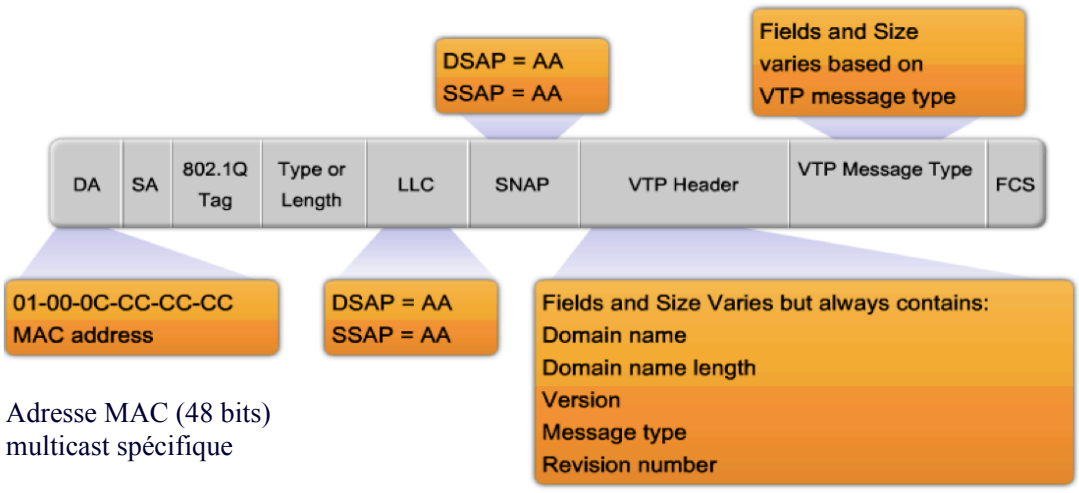
- **show vtp status**
  - Affiche la configuration VTP et le statut du processus

```
Switch#sh vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 250
Number of existing VLANs        : 7
VTP Operating Mode              : Server
VTP Domain Name                 : LABO
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x80 0x86 0x88 0xE7 0xB1 0x6E 0xBB 0xF8
Configuration last modified by 0.0.0.0 at 3-1-93 00:08:35
Local updater ID is 0.0.0.0 (no valid interface found)
Switch#
```

La propagation du domaine

- Les VTP Server propagent leur domaine VTP vers les autres switchs via des messages VTP advertisement
- Ces messages de type advertisement sont utilisés pour transporter
  - les informations sur les domaines VTP
  - les informations sur les modifications des VLAN
- Chaque message VTP est composé
  - d'un VTP header et
  - d'un VTP data field
- Chaque message VTP est inséré dans le champ de données des trames Ethernet qui sont elles-mêmes encapsulées dans une trame 802.1q trunk ou ISL(protocole propriétaire de Cisco).
- Chaque switch envoie périodiquement, par multicast, sur ses liens trunk des VTP advertisement.

Les VTP advertisement messages



Adresse MAC (48 bits) multicast spécifique

Rappel : LLC

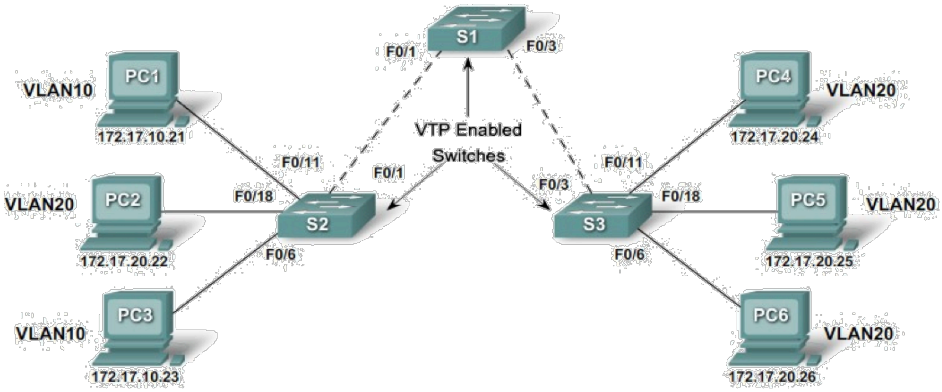
- La Trame LLC
  - Le champ DSAP (Destination Service Access Point) (8bits), adresse destination,
  - Le champ SSAP (Source Service Access Point) (8bits), adresse source
  - le champ contrôle (8 bits LLC1 ou 16 bits LLC2), permet dans LLC2 le contrôle d'erreur et de séquencement.

Les VTP revision number

- Codé sur 32 bit
  - Par défaut, c'est la valeur 0
- A chaque ajout ou suppresion d'un VLAN, ce nombre est incrémenté de 1 par le switch VTP server
- Au changement du nom du VTP domain, ce nombre est mis à 0
- Permet de connaître le message VTP le plus récent

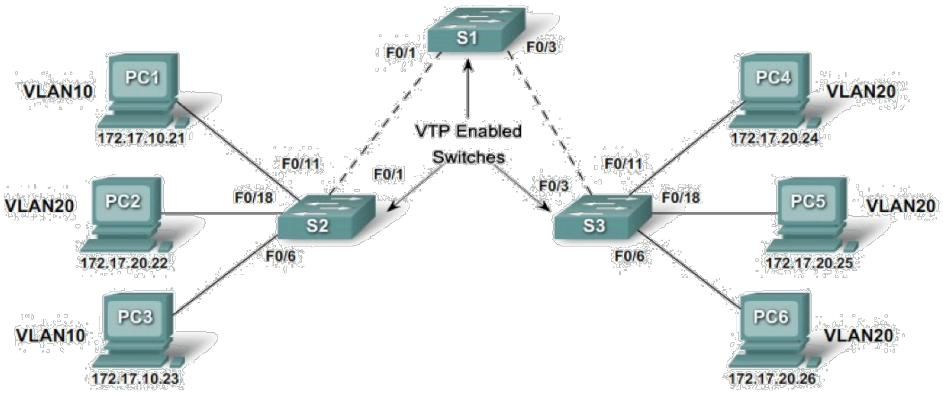
VTP Pruning

- Les messages echangés sont diffusés, dans certain cas, il est inutile de propager les informations vers tous les switchs



- Dans cet exemple : Il est inutile de propager vers le switch S1 les informations du VLAN 10

VTP Pruning



- Le VTP Pruning Supprime la propagation des messages de broadcast, multicast et autres messages inconnu unicast sur les liens trunks afin d'optimiser la bande passante

Les informations d'un message advertisement

VTP advertisements send this global domain information:

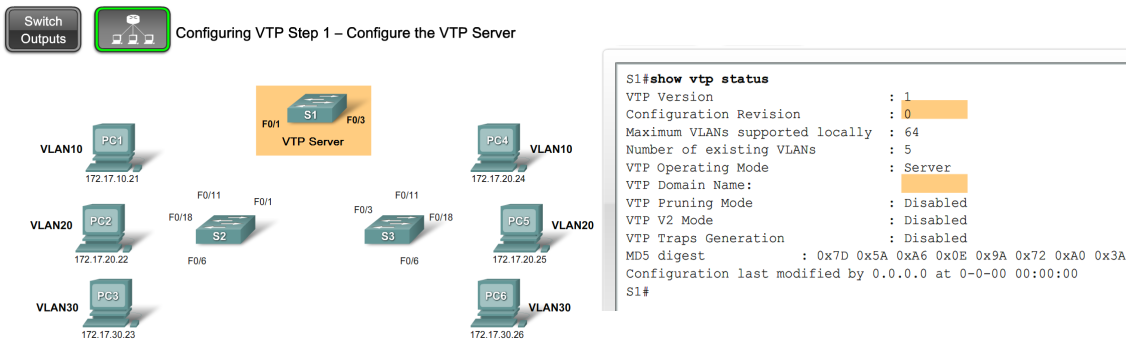
- VTP domain name
- Updater identity and update timestamp
- MD5 digest
- Frame format

VTP advertisements send this VLAN information:

- VLAN ID
- VLAN name
- VLAN type
- VLAN state

Configurer VTP dans les commutateurs

- Configurer VTP dans le switch
  - Il faut un serveur et des clients



Configurer VTP dans les commutateurs

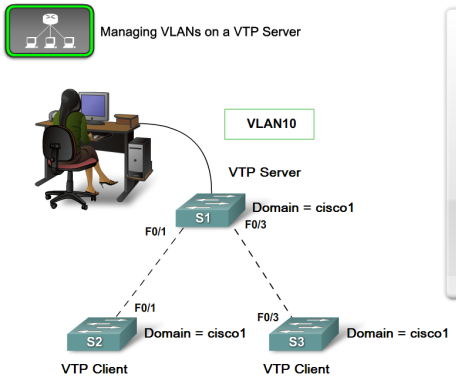
- Identifier les problèmes rencontrés dans la configuration

Common VTP Configuration Issues

- Incompatible VTP Versions
- VTP Password Issues
- Incorrect VTP Mode Name
- All Switches set to VTP Client Mode

Configurer VTP dans les commutateurs

- Gérer les VLANs dans un réseau implémentant VTP




```
S1>enable
Password:
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#vlan 10
S1(config-vlan)#name faculty
S1(config-vlan)#exit
S1(config)#interface FastEthernet 0/11
S1(config-if)#switchport access vlan 10
S1(config-if)#exit
S1(config)#exit
S1#
```

Annexe

Types de messages

Les types de message advertisement

- Summary Advertisement
  - Message utilisé dans la plupart des cas

Summary Advertisement			
Version	Code	Followers	MgmtD Len
Management Domain Name (Zero-Padded to 32 Bytes)			
Configuration Revision Number			
Updater Identity			
Update Timestamp (12 Bytes)			
MD5 Digest (16 Bytes)			

Followers - The Followers field indicates that this packet is followed by a Subset Advertisement packet.

MgmtD Len – Indicated the length of the management domain name.

Updater Indentity - The Updater Identity is the IP address of the switch that is the last to have incremented the configuration revision.

Les types de message advertisement

- Subset Advertisement
  - Contient le détail de chaque VLAN

Advertisements Details

Subset Advertisements			
Version	Code	Seq-Number	Domain Name Length
Management Domain Name (zero-padded to 32 bytes)			
Configuration Revision Number			
VLAN-info Field 1			
:			
VLAN-info Field N			

The VLAN-info field contains information for each VLAN and is formatted as follows:

VLAN-Info			
Info Length	Status	VLAN-Type	VLAN-name Len
ISL VLAN-id		MTU Size	
802.10 Index			
VLAN-name (Padded with 0s to Multiples of 4 bytes)			

Les types de message advertisement

- Request advertisement
  - Utilisé quand un switch n'a pas reçu les informations sur tous les VLAN
  - Quand il est en mode client et démarre par exemple

Advertisement Request			
Version	Code	Rvsd	MgmtD Len
Management Domain Name (zero-padded to 32 bytes)			
Start Value			

StartValue – This field is used when there are several subset advertisements. If the first (n) subset advertisement has been received and the subsequent one (n+1) has not been received, the VTP enabled switch only requests advertisements from the (n+1)th one.

Les commandes

- Changer le mode VTP
  - `Switch(config)# vtp mode { client | server | transparent }`
- Changer la version de VTP
  - `Switch(config)# vtp version { 1 | 2 }`
  - Sur les switchs Cisco 2960, seules les versions 1 et 2 sont disponibles
- Changer le VTP domain
  - `Switch(config)# vtp domain` *`le-domaine`*
- Définir un mot de passe
  - `Switch(config)# vtp password mot-de-passe`
- Reset du Revision Number
  - Il faut effectuer un changement de nom du VTP domaine
- Pour voir les informations sur le protocole VTP
  - `Switch# show vtp status`
- `Pour visualiser les liaisons trunk`
  - `Switch# show interfaces trunk`

Le SPT

Conception d'un bon réseau

- Besoin de fiabilité, tolérance de pannes
  - Établissement de chemins redondants

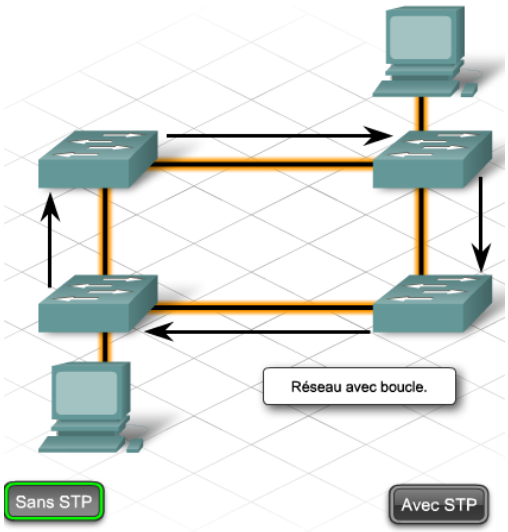
- Conséquences
  - Boucles de commutations
  - Tempêtes de broadcast
  - Bande passante réduite
  - Congestion

Boucle de commutation

- Un bon réseau doit pouvoir proposer un chemin alternatif en cas de panne d'une liaison ou d'un commutateur. Le protocole Spanning-tree garantit un chemin unique entre deux nœuds du réseau.

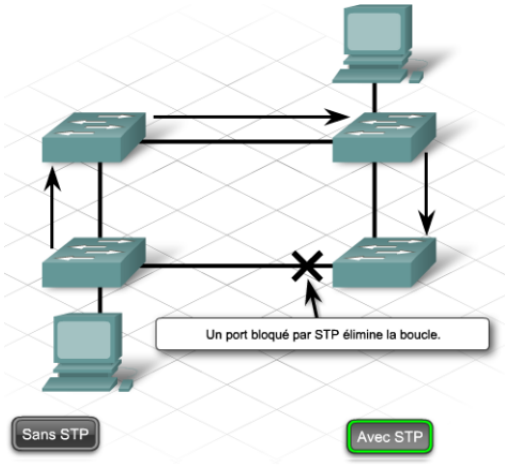
Boucle de commutation

- Bouclage dans un réseau maillé
- L'envoi d'une trame broadcast qui tourne indéfiniment. (tempête de broadcast)
  - Peut causr crash de l'ordinateur

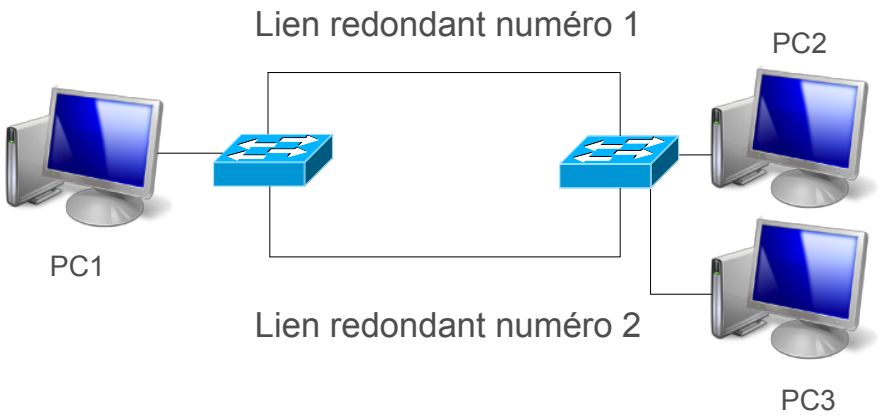


Boucle de commutation : Solution

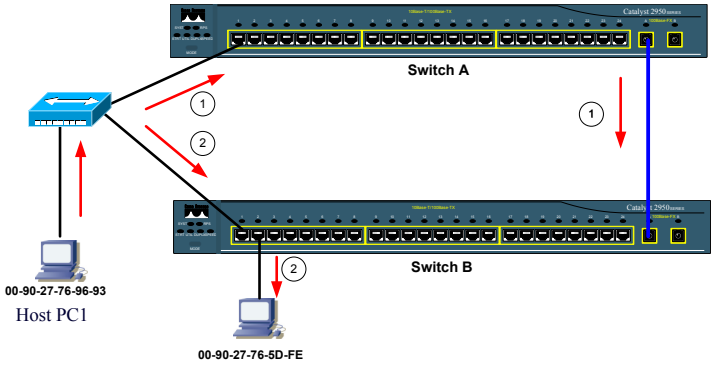
- Un bon réseau doit pouvoir proposer un chemin alternatif en cas de panne d'une liaison ou d'un commutateur.
- Le protocole **Spanning-tree** garantit un chemin unique entre deux nœuds du réseau.



Lien redondant

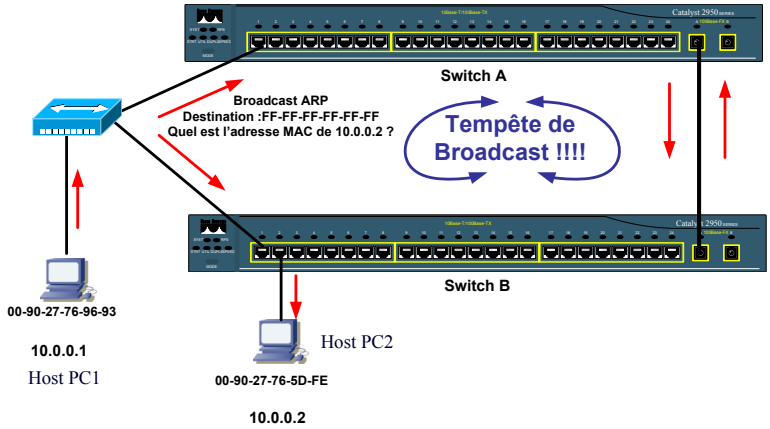


Topologie redondante



- PC1 peut joindre PC2 via 2 chemins
- Si le lien entre le hub et le switch B casse il reste une alternative

Topologie redondante



- Si PC1 envoie un broadcast ARP pour obtenir l'adresse MAC de PC2
- La trame est diffusé par PC1, et tous les ports des switchs A et B
  - Tempête de broadcast

Spanning Tree

- But de STP
  - Éviter les boucles de commutations
  - Garder une tolérance de pannes
- Moyens utilisés
  - Établir un arbre unique de chemins
  - Supprimer les boucles de commutation
  - Garder des liens redondants (backup)

SPT

- Augmente la fiabilité avec un lien de secours.
- Si un lien est défaillant, un lien redondant prend la relève.
- Coût supplémentaire :
  - Est ce que la fiabilité ajouté au réseau compense le coût de matériel ?

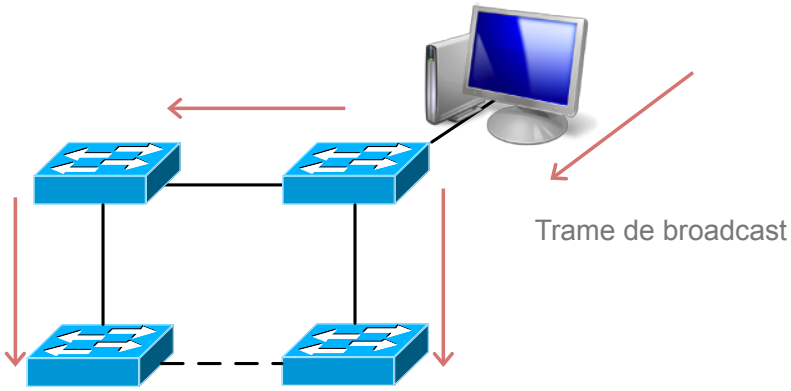
Spanning Tree

- Etats des ports
  - Établissement de l'arbre
    - Attribution d'un état à chaque port des commutateurs

Blocage	**BPDU entendus**
Ecoute	**Ecoute des trames**
Apprentissage	**Apprentissage des adresses**
Acheminement	**Trames acheminés**
Désactivation	**Aucune trames acheminés ni BPDU**

Spanning Tree

- Exemple d'implémentation



Le protocole SPT

- Standard IEEE 802.1D
- Échange de BPDU*
- Par défaut les liaisons ont des coûts :

Default Port Costs According to IEEE

Speed of Ethernet	Original IEEE Cost	Revised IEEE Cost
10 Mbps	100	100
100 Mbps	10	19
1 Gbps	1	4
10 Gbps	1	2

*** Bridge Protocol Data Unit**

Le protocole SPT

- But de STP
  - Éviter les boucles de commutations
  - Garder une tolérance de pannes

- Moyens utilisés
  - Établir un arbre unique de chemins
  - Supprimer les boucles de commutation
  - Garder des liens redondants (backup)

Le protocole SPT

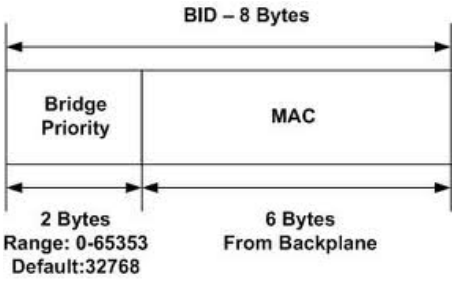
- Élection du pont racine → **root bridge**
  - fondé sur la priorité de pont et sur l'adresse MAC (Bridge ID)
  - priorité la plus faible est élu
  - sinon, adresse MAC la plus faible

- Chaque commutateur calcule le coût vers le root bridge, élection du port racine → **root port**
  - coût le plus faible est élu
  - coût basé sur la bande passante

- Élections de ports désignés ou les ports bloqués → **designated port et blocked port**

Identification de commutateur

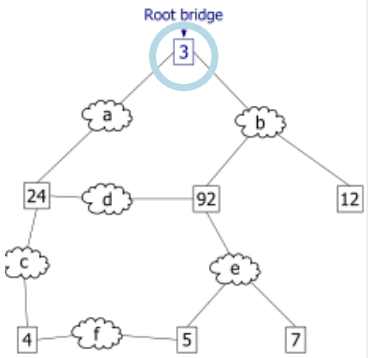
Bridge ID (BID)
Priorité
+
Adresse MAC

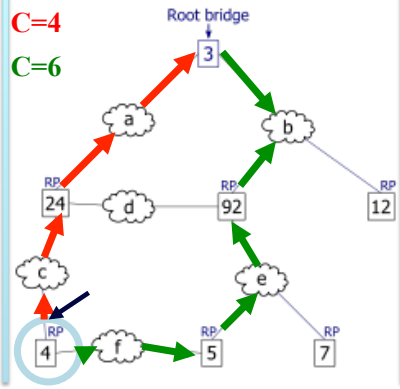


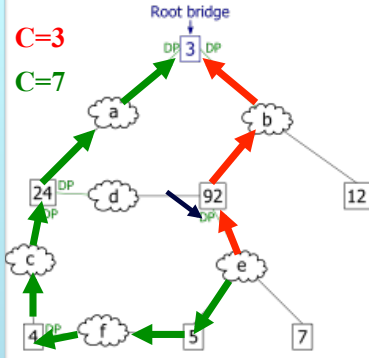
Commutateur A

- Par défaut la priorité du pont = 32 768
- Si @ MAC d'un switch = AA-11-BB-22-CC-33 => BID = 32768: AA-11-BB-22-CC-33

Fonctionnement du SPT (1)







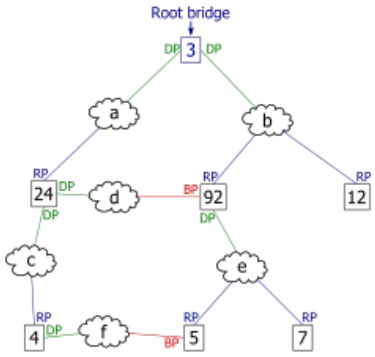
Pont racine :
Le plus petit *bridge ID* vaut 3. Par conséquent, le commutateur 3 devient le commutateur racine.

Port racine (RP)
En supposant que le coût de traversée de chaque segment réseau est 1, le chemin de moindre coût du commutateur 4 au com racine passe par le segment réseau c. Par conséquent, le port racine pour le com 4 est celui qui mène au segment réseau c.
Du switch x au switch racine

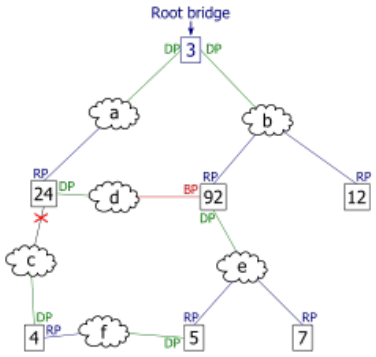
Port désignés (DP):
Le chemin de moindre coût depuis le segment réseau e passe par le com 92. Par conséquent, le port désigné pour le segment réseau e est le port qui le connecte au commutateur 92.
Du segment au switch racine

a,b,c,d,e et f : segment de réseau / 3,24,92,4,5,7,12 : switch

Fonctionnement du SPT (2)



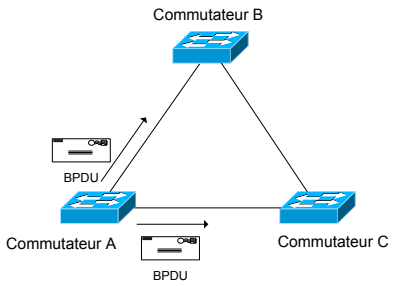
Port bloqué :
Tout port qui n'est ni racine ni désigné devient un port bloqué.



Après la chute d'un lien (marquée par une croix), un nouvel arbre de moindre coût est calculé.

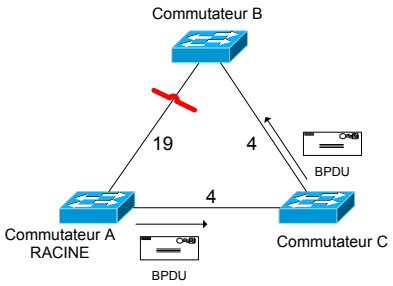
Élection du Root Bridge

- Une topologie sans boucle ressemble à un arbre et à la base de chaque arbre, on trouve ses racines (*roots*).
- Le commutateur avec la priorité la plus basse l'emporte, et en cas d'égalité, c'est l'adresse MAC la plus basse qui l'emporte.



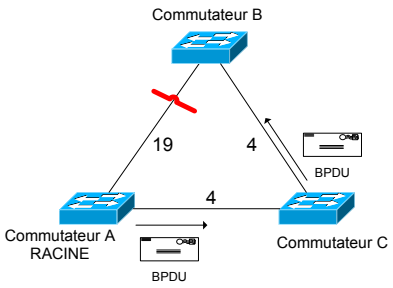
Désignation des ports

- Les autres commutateurs du réseau vont alors déterminer quel est le port qui possède la « distance » la plus courte vers le commutateur racine.
- Pour cela, ils utilisent le « coût » de chaque lien traversé, ce coût dépendant de la bande passante du lien.
- Chaque commutateur doit avoir un seul *root port*.
- L'élection d'un *root port* est effectuée d'après les champs *path cost* et *port ID* d'un paquet BPDU.
- En cas d'égalité, c'est le port ayant le *port ID* le plus faible qui sera élu.



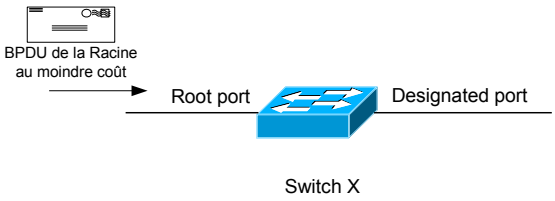
Désignation des ports

- Les autres commutateurs du réseau vont alors déterminer quel est le port qui possède la « distance » la plus courte vers le commutateur racine.
- Pour cela, ils utilisent le « coût » de chaque lien traversé, ce coût dépendant de la bande passante du lien.



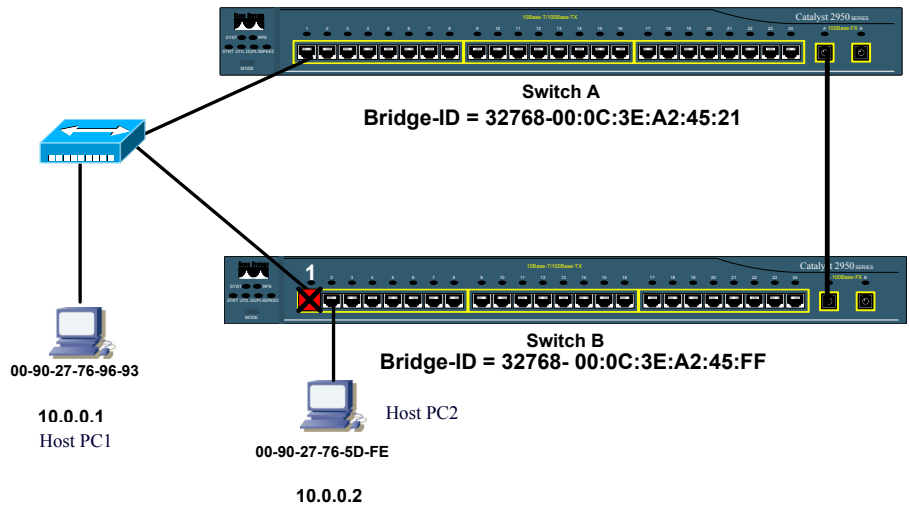
Désignation des ports

- Chaque commutateur doit avoir un seul *root port*.
- L'élection d'un *root port* est effectuée d'après les champs *path cost* et *port ID* d'un paquet BPDU.
- En cas d'égalité, c'est le port ayant le *port ID* le plus faible qui sera élu.



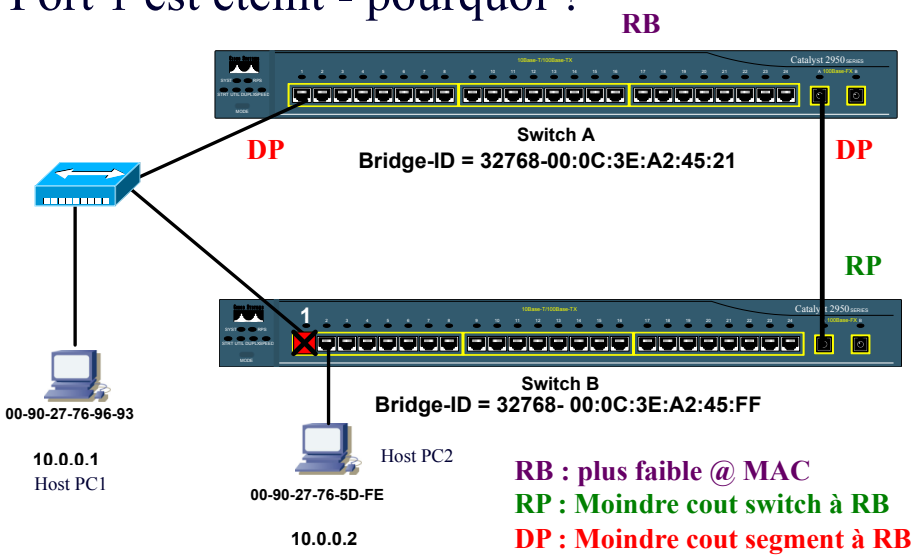
Exemple

- Port 1 est éteint - pourquoi ?



Exemple

- Port 1 est éteint - pourquoi ?



Les différents états STP

- **Blocking :** Aucune trames transmises, unités BPDU reçue
- **Listening :** Aucune trames transmises, écoute de trames
- **Learning :** aucune trames transmises, acquisition des informations
- **Forwarding :** trames transmises, acquisition des informations
- **Disabled :** aucune émission, aucune écoute de trames BPDU

Convergence STP

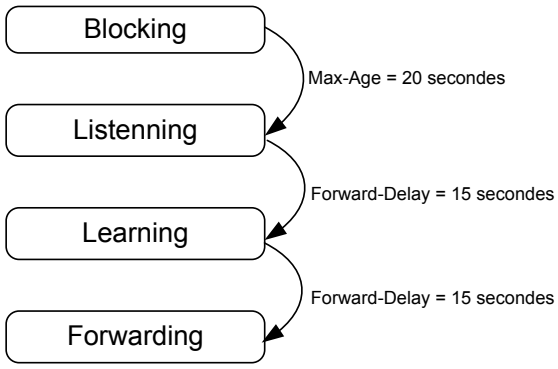
- Afin de communiquer, STP utilise des BPDU
- Les BPDU Hello sont transmise toute les 2 secondes

- Protocole STP:
  - Branchement d'un nouveau switch
  - Le port s'active, le protocole STP se met en marche
  - Max age (20 secondes) Temps de sécurité à attendre en cas de changement topologique
  - Listenning (15 secondes) Temps pour que le commutateur écoute les trames qu'il peut recevoir, sans émettre
  - Learning (15 secondes) Temps pour apprendre les informations de la topologie STP

- Le port met donc 50 secondes à s'initialiser

Convergence STP

- Temps de convergence = 50s :



- Lorsqu'une modification topologique est détectée :
  - Arbre STP recalculé
  - Trafic stoppé

Mise en marche d'un port

- Une solution possible pour les utilisateurs finaux (end-users)
  - Possibilité d'activer le « port-fast », le port passe alors directement à la connexion physique en forwarding
  - A utiliser avec précaution, ne jamais brancher d'autres commutateurs ou autres périphériques STP sur ce type de port.

RSTP

- Rapid Spanning Tree Protocol **(802.1w)**
- 3 états :
  - Discarding (blocking, listenning, disabled)
  - Learning
  - Forwarding
- Plus rapide car :
  - Lien invalide quand 3 HELLO ne sont plus reçus (par défaut 6 secondes au lieu du max age 20 secondes)
  - Plus de listenning
  - Learning amélioré (1 à 2 secondes au lieu de 15)

Commandes Cisco

Modification de la priorité d'un port :

- **Switch_A>enable**
- **Switch_A#configure terminal**
- **Switch_A(config)#interface Ethernet N°_d'interface**
- **Switch_A(config-if)#spanning-tree cost (0 -> 65535)**

  - Par défaut : le « cost » est calculé en fonction de la bande passante du lien.

Commandes Cisco

Modification de la priorité d'un commutateur :

- **Switch_A>enable**
- **Switch_A#configure terminal**
- **Switch_A(config)#spanning-tree priority (0 -> 65535)**

  - Par défaut : priority = 32768

Commandes Cisco

Information de Root ID, Brigde ID et interface :

- Switch_A>enable
- Switch_A#show spanning-tree

Information sur le coût de la liaison d'une interface sur un commutateur :

- Switch_A>enable
- Switch_A#show spanning-tree interface fastEthernet 0/1

Commandes Cisco

Information en temps réel :

- Switch_A>enable
- Switch_A#debug spanning-tree

Pour stopper :

- Switch_A#u all (undebug all)