# Les réseaux locaux virtuels (VLANs) et protocole du Spanning Tree

T. BEJAOUI

http://sites.google.com/site/tarekbejaoui

# Rappel sur l'évolution des réseaux locaux

# Evolution des applications

***Avant :***

Applications basées sur du texte

***Aujourd'hui :***

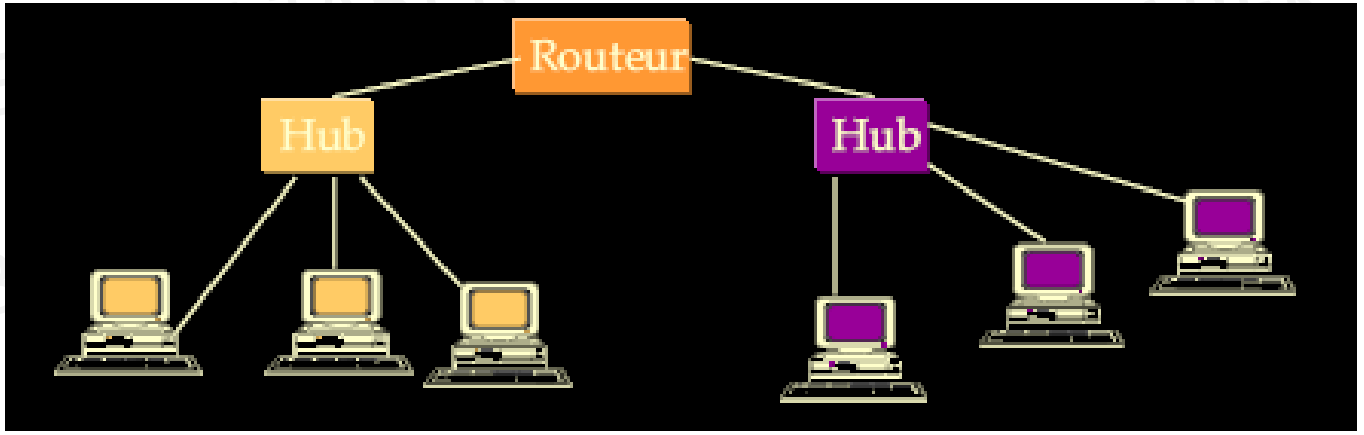
incluant la voix, les images et la vidéo

→ de nouvelles exigences en terme de QoS

# Evolution des réseaux partagés (1)

***Les contraintes :***

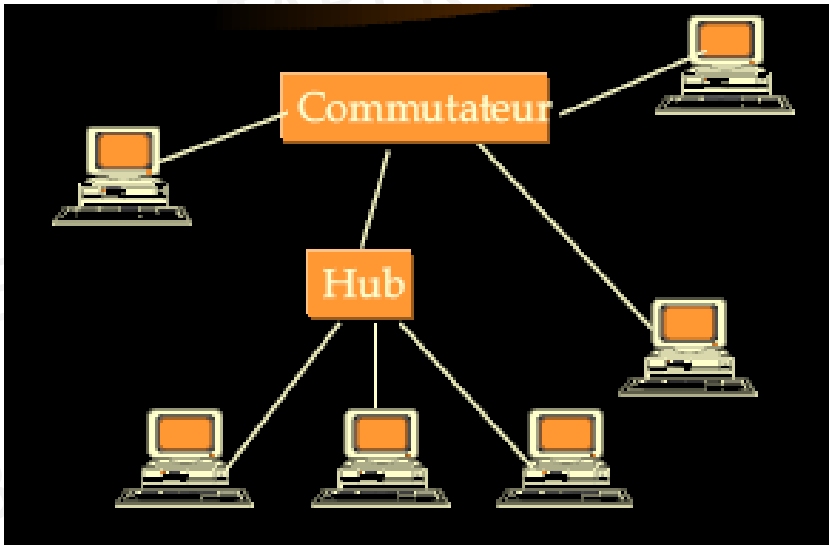
- Les sous-réseaux sont liés aux hubs
- Les utilisateurs sont groupés géographiquement
- Pas de sécurité sur un segment
- Plan d'adressage difficile
- La mobilité entraîne un changement d'adresse



# Evolution des réseaux partagés (2)

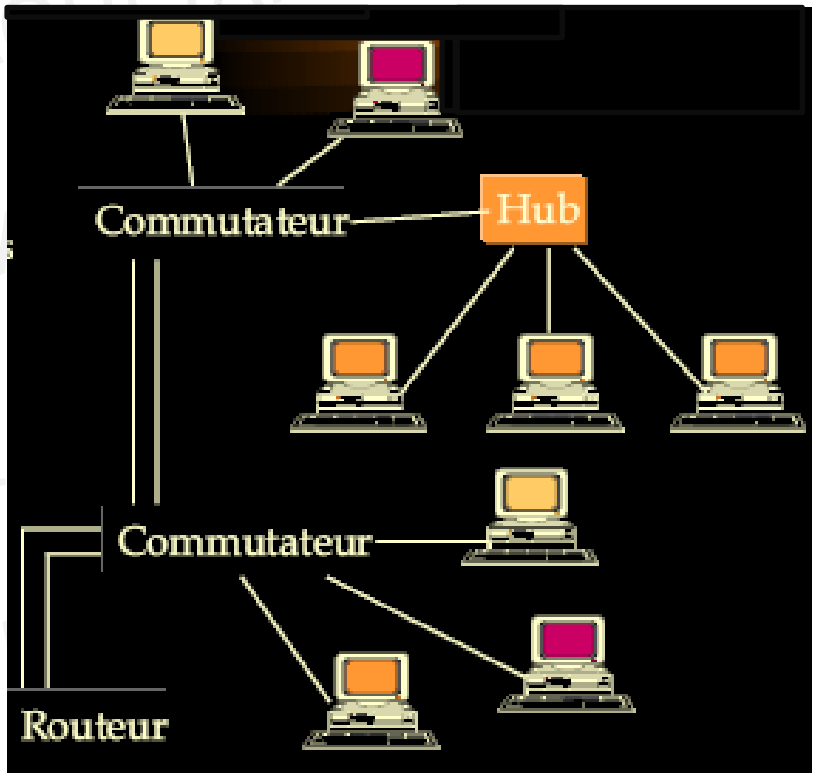
***La commutation :***

- Meilleur accès au média
  - Bande passante dédiée,
  - Moins de conflits d'accès
  - Collisions réduites
- Le trafic est dirigé vers la station spécifiée
- Les « broadcast » sont diffusés plus vite
- L'évolutivité reste un problème



# Le réseau local commuté

- Domaines de collisions réduits
- Intelligence dans le port du commutateur
- les frontières physiques disparaissent
- Regroupement logique des utilisateurs
- Meilleur contrôle de la BP et des changements dans le réseau
- Centralisation de l'administration
- Routeur pour la communication inter-réseau



# Technologies commutées

- Ethernet commuté 10/100 Mbps
- Gigabit Ethernet
- Token Ring commuté 4/16 Mbps
- FDDI/CDDI commuté 100 Mbps

  Caractéristiques communes
  - Modes Half-Duplex et Full-Duplex
  - Cut-Through et Store and Forward
  - Commutateur = Pont multi-ports
- ATM (155 Mbps, 622 Mbps, 2.4 Gbps), circuit virtuel
- MPLS

# Les réseaux locaux virtuels

# Qu’est ce qu’un réseau virtuel?

- Un réseau virtuel (VLAN) est un réseau informatique logique indépendant.
- Trois nécessités pour introduire le concept

  - Limiter les domaines de broadcast
  - Garantir la sécurité
  - Permettre la mobilité des utilisateurs

  *Une nouvelle manière d’exploiter la technique de la commutation pour donner plus de flexibilité aux réseaux locaux;*
  ***C’est un réseau logique***

- De nombreux VLANs peuvent coexister sur un même commutateur réseau.

# Qu’est ce qu’un réseau virtuel?

- Réseau dans le cadre duquel la segmentation des groupes ou domaines n’est pas contrainte par des éléments physiques ou géographiques mais par une configuration logique avec l’aide de matériel et logiciel spécifiquement conçu pour le VLAN

# Principe du VLAN (1)

- Indépendamment de la localisation géographique sur le réseau, les stations peuvent communiquer comme si elle étaient sur le même segment
- Un VLAN est assimilable à un domaine de diffusion (Broadcast Domain) → les messages de diffusion émis par une station d'un VLAN ne sont reçus que par les stations de ce VLAN.

# Principe du VLAN (2)

VLANS devenus réalisables après apparition des commutateurs.

***Avant :*** Pour constituer des domaines de diffusion → nécessité de créer des réseaux physiques, reliés entre eux par des routeurs → obligation liée à la localisation géographique des stations, contraignante pour l'administrateur

***Aujourd'hui :*** Les VLAN ont révolutionné le concept de segmentation des réseaux → permettent de constituer autant de réseaux logiques (de même caractéristiques que les réseaux physiques) que l'on désire sur une seule infrastructure physique

# Les avantages du VLAN (1)

***Segmentation:***

- Réduction de la diffusion du trafic
- Création de groupes de travail sans remise en cause de l'infrastructure physique
- Contrôle des échanges entre les différentes VLAN
- Les messages de broadcast sont limités à l'intérieur de chaque VLAN. Les broadcasts d'un serveur peuvent être limités aux clients de ce serveur.
- Le membre d'un groupe peut se déplacer sans changer de réseau virtuel
- Les échanges inter-VLAN se réalisent tout comme pour tous les échanges inter-réseau, à travers des routeurs.

# Les avantages du VLAN (2)

- ***Flexibilité*** : Possibilité de travailler au ***niveau 2*** (Adresse ***MAC***) ou au ***niveau 3 (IP)***. Les VLANs fonctionnent au niveau de la couche 2 du ***modèle OSI***. Toutefois, un VLAN est souvent configuré pour se connecter directement à un réseau IP, ce qui donne l'impression de travailler plutôt au niveau de la couche 3. Les VLAN'S peuvent aussi se baser sur les ports physiques des commutateurs (attention à ne pas confondre les ***ports "physiques"*** avec les ***ports "logiques"*** du protocole) (en anglais : "port-based" ) ce qui correspond au niveau 1 du modèle OSI et non au numéro de port du ***niveau 4*** (par exemple : le port 80 en ***TCP*** qui "pointe" vers le service ***HTTP***).

# Les avantages du VLAN (3)

Le réseau virtuel :

- permet la gestion dynamique de la mobilité
- Permet à des utilisateurs géographiquement dispersés de partager des données
- Maintient la sécurité
- Conserve les domaines de broadcast traditionnels des LANs
- Requiert une couche 3 pour la communication entre VLANs

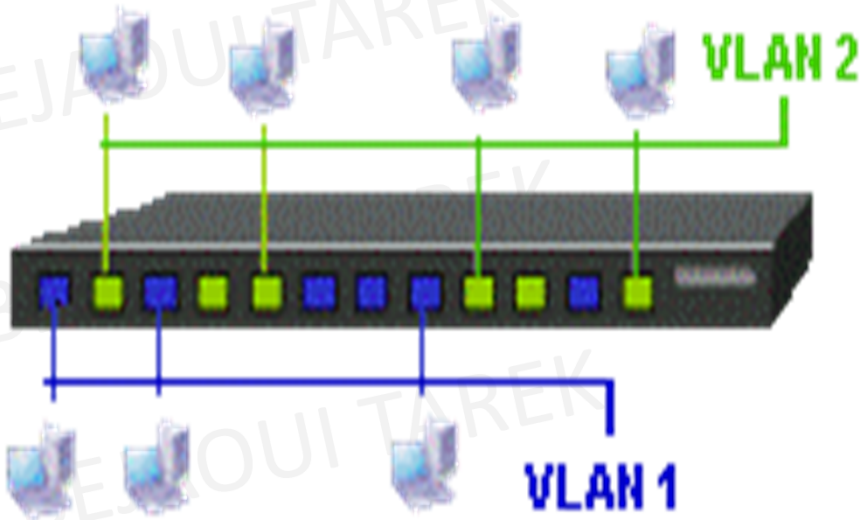
# Construction de VLANs

Plusieurs méthodes existent:

- Par port (niveau 1)
- Par adresse IEEE ou MAC (niveau 2)
- Par protocole (niveau 3)
- Par sous-réseau (niveau 3)

# VLAN par port (1)

- Obtenu en associant chaque port du commutateur à un VLAN particulier.
- Les premiers VLAN ne permettaient pas de créer un même réseau sur plusieurs commutateurs
- Une nouvelle génération de commutateurs permet de le réaliser grâce à l'échange d'information entres les commutateurs et au marquage des trames.



# VLAN par port (2)

- ***Le marquage*** permet de reconnaître les trames. L'appartenance à tel ou tel VLAN peut être déduite des informations contenues dans la trame (@ MAC protocole…)ou insérée dans cette trame.
- Plusieurs solutions constructeurs ont été proposées, toutes incompatibles entre elles.

  → l'IEEE a défini une norme VLAN sous la référence 802.1Q.

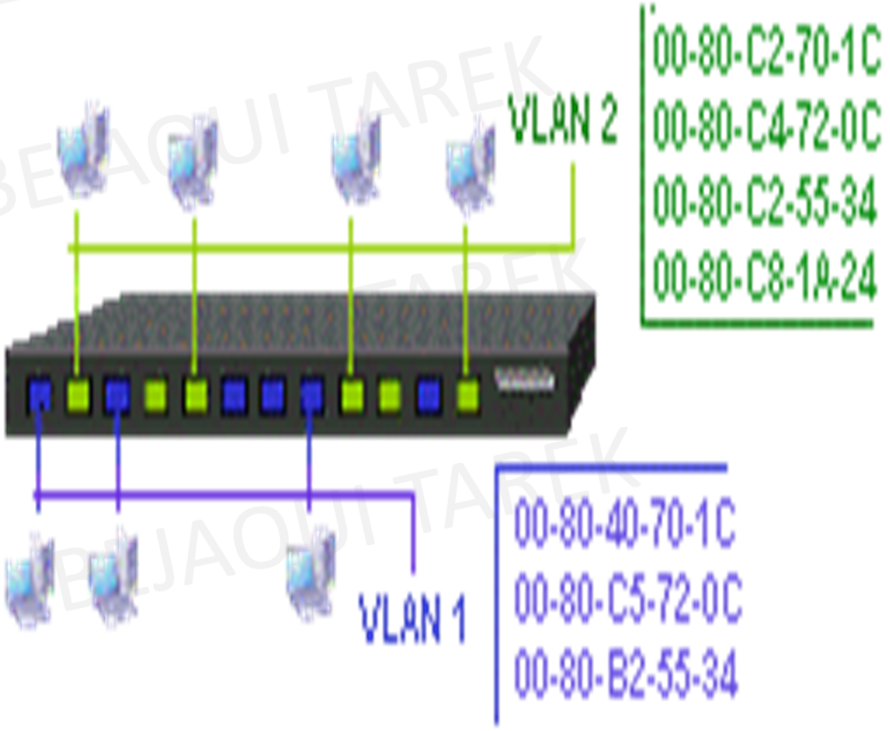
# VLAN par port (3)

Les faiblesses:

- Manque de souplesse
- Tout déplacement d'une station nécessite une reconfiguration des ports.
- Les stations reliées sur un port par l'intermédiaire d'un même concentrateur, appartiennent au même VLAN
- Nécessité de rechercher les adresses
- Pas de filtrage des broadcasts sur les segments partagés
- Beaucoup d'administration

# VLAN par adresse MAC (1)

- Constitué en associant les adresses MAC des stations à chaque VLAN.
- Intérêt : indépendance de la localisation → station peut être déplacée, son @ physique ne changeant pas, il est inutile de reconfigurer le VLAN
- VLAN configurables avec l'@ MAC sont bien adaptés à l'utilisation de stations portables



# VLAN par adresse MAC (2)

Les faiblesses :

- Configuration fastidieuse car elle nécessite de renseigner une table de correspondance avec toutes les adresses MAC et elle doit être partagée par tous les commutateurs → Echange des tables d'adresses des VLANs entre les commutateurs -> Overhead dû à l'administration
- Filtrage requis -> impact sur les performances

# VLAN par protocole

- Obtenu en associant un réseau virtuel par type de protocole du réseau → possibilité de constituer un réseau virtuel pour les stations communiquant avec le protocole TCP/IP et un autre pour les stations communiquant avec le protocole IPX…
- Les commutateurs s'adaptent à la configuration
- Solution moins performante car les commutateurs doivent analyser des informations

# VLAN par sous-réseau

- Il utilise les adresses IP. Un réseau virtuel est associé à chaque sous-réseau IP → les commutateurs apprennent la configuration et il est possible de changer une station de place sans reconfigurer le VLAN.
- Pas d'administration manuelle des VLANs
- Uniquement avec les protocoles routables
- L'une des plus intéressantes solutions malgré une petite dégradation des performances de la commutation due à l'analyse des informations.

# Bilan

- Simplicité des VLANs par port (statique)
- Facilité d'administration des VLANs par port (dynamique)
- Intérêt des VLANs par sous-réseau pour les protocoles routables et des VLANs par adresse MAC pour les protocoles non routables
- Administration cenralisée

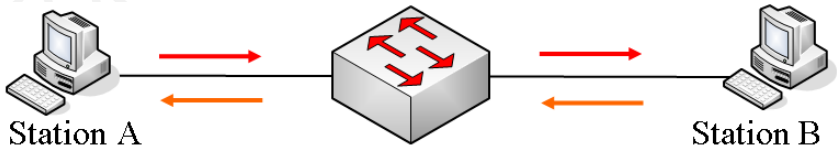
# Utilisation des VLANs aujourd'hui

- Gestion du trafic broadcast et multicast
- Centralisation des serveurs
  - administration, sécurité
- Isolement de certaines applications
  - Protection du backbone
- Administration centralisée
  - Groupes logiques d'utilisateurs
  - Contrôle de chaque utilisateur, chaque port, chaque commutateur

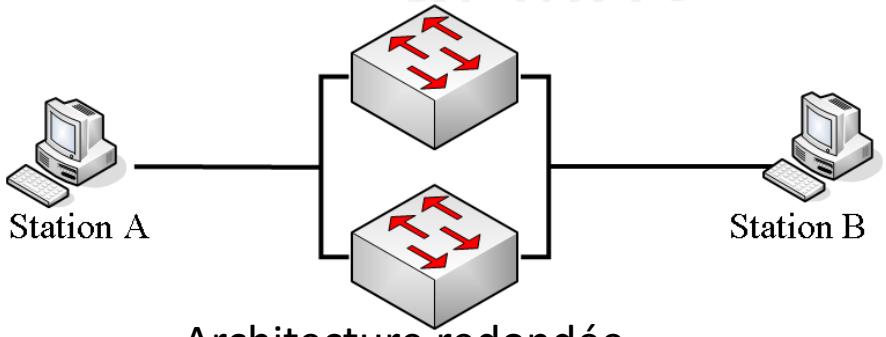
# Protocole du Spanning Tree

# Objectif

- Le protocole Spanning-tree est actif par défaut sur les commutateurs
- Augmenter la fiabilité d'un réseau → dupliquer les équipements physiques → redondance ou résilience




Architecture non redondée



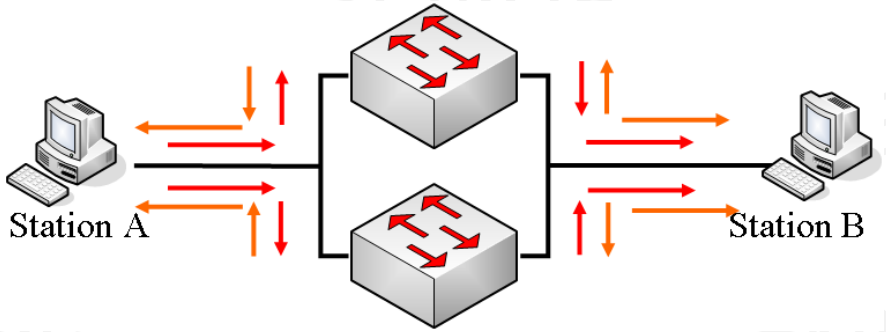

Architecture redondée

# Problèmes dus à la redondance

- Une redondance physique dans un LAN commuté  crée 3 problèmes :
- Tempête de broadcast
- Duplication de trame
- Instabilité de la table MAC

# Tempête de broadcast

- imaginons que A envoi un message de broadcast (trame niveau 2 avec comme adresse MAC de destination FFFF.FFFF.FFFF)




• Le switch du haut reçoit la trame sur son port, **extrait l'adresse MAC** de destination (FFFF.FFFF.FFFF) et **la duplique sur tous ses ports** car c'est une adresse de broadcast. La trame sort donc du switch du haut et se dirige vers le switch du bas

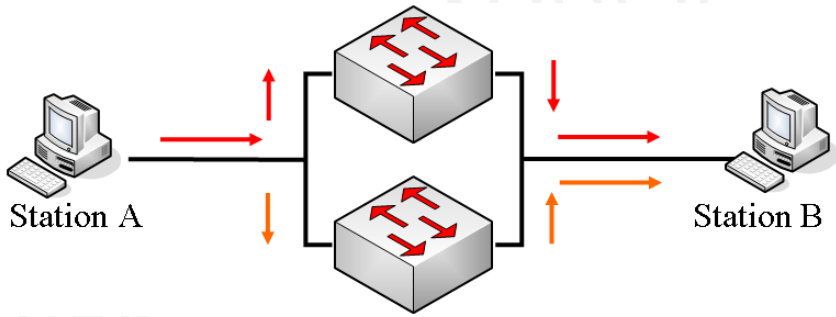
• idem pour le switch du bas; il reçoit la trame sur son port, **extrait l'adresse MAC** de destination (FFFF.FFFF.FFFF) et **la duplique sur tous ses ports** car c'est une adresse de broadcast. La trame sort donc du switch du bas et se dirige vers le switch du haut

• et ces trames **tournent sans arrêt** entre les 2 switchs, faisant monter leur CPU à 100% et les font plus ou moins planter (souvent un reboot est nécessaire)

Ce phénomène s'appelle la **tempête de diffusion**, ou **broadcast storm** en anglais.

# Duplication de trame

- imaginons que la station A envoi une trame vers la station B, donc la trame sera forgée avec les informations suivantes:
  - adresse MAC source: A
  - adresse MAC destination: B

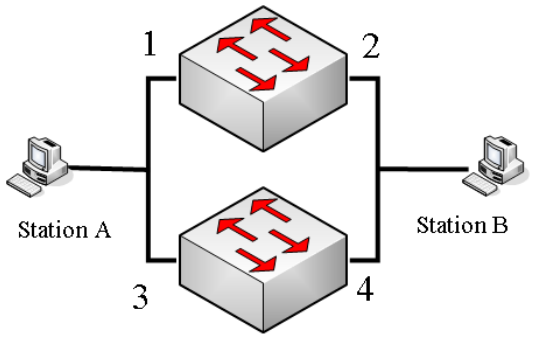



• Le switch du haut reçoit la trame sur son port (flèche rouge), **extrait l'adresse MAC** de destination (B) et la commute sur le port de droite. La station B reçoit bien la trame de la station A

• Mais le switch du bas reçoit aussi la trame sur son port (flèche orange), **extrait l'adresse MAC** de destination (B) et la commute sur le port de droite. La station B reçoit donc pour une deuxième fois la trame de la station A

Ce phénomène s'appelle la **duplication de trame**

# Instabilité de la table MAC (1)




| Port | @ MAC |
|---|---|
| 1 | ? |
| 2 | ? |

| Port | @ MAC |
|---|---|
| 3 | ? |
| 4 | ? |

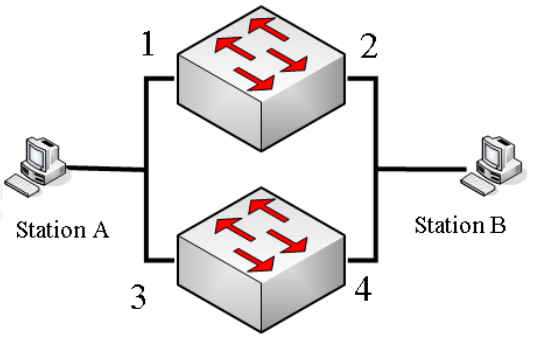
la trame précédente (message de A vers B):

- la trame arrive sur le port 1 du switch du haut. Le switch **extrait l'adresse MAC source** et **l'insère dans sa table MAC** [port 1 = adresse MAC A]
- la trame arrive aussi sur le port 3 du switch du bas. Le switch **extrait l'adresse MAC source** et **l'insère dans sa table MAC** [port 3 = adresse MAC A]
- Maintenant que chaque switch a extrait l'adresse MAC source pour l'insérer dans sa table, chacun **extrait l'adresse MAC de destination** (B) et **la compare à sa table**. Comme aucune entrée n'est trouvée, chaque switch va dupliquer la trame sur tous ses ports:

  le switch du haut envoi la trame sur son port 2

  le switch du bas envoi la trame sur son port 4

# Instabilité de la table CAM

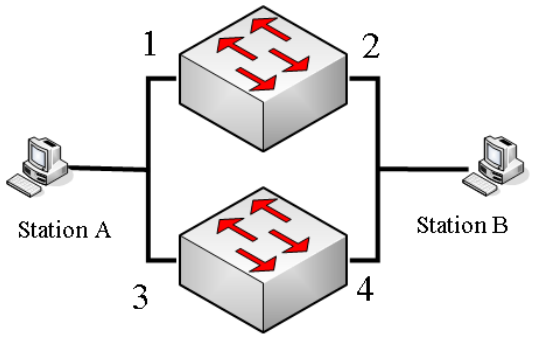



| Port | @ MAC |
|---|---|
| 1 | ? |
| 2 | ? |

| Port | @ MAC |
|---|---|
| 3 | ? |
| 4 | ? |

- La table **CAM – Content Addressable Memory**, est une table dans laquelle le switch garde une correspondance du type « Adresse MAC A -> derrière port 1 »
- C'est grâce à cette table que le switch saura sur quel port transmettre les trames qu'il reçoit.
- Dans l'exemple ci-contre : PC1 envoie un message à PC 2.
- Le message va jusqu'aux switchs S1 et S2.
- Ceux-ci vont alors envoyer la trame vers PC2.
- Sauf que le message arrivera aussi au deuxième switch.
- Par exemple, S2 transmet la trame vers PC2, et celle-ci arrive aussi sur S1 – port 2.
- 
- A ce moment-là, S1 va noter dans sa table CAM, que PC1 (son adresse MAC), se trouve derrière le port 2 (et non plus derrière le port 1).
- Les tables CAM de S1 et S2 seront alors faussées.

# Instabilité de la table MAC (2)




| Port | @ MAC |
|---|---|
| 1 | ? |
| 2 | ? |

| Port | @ MAC |
|---|---|
| 3 | ? |
| 4 | ? |

chaque switch recoit la trame de l'autre switch…

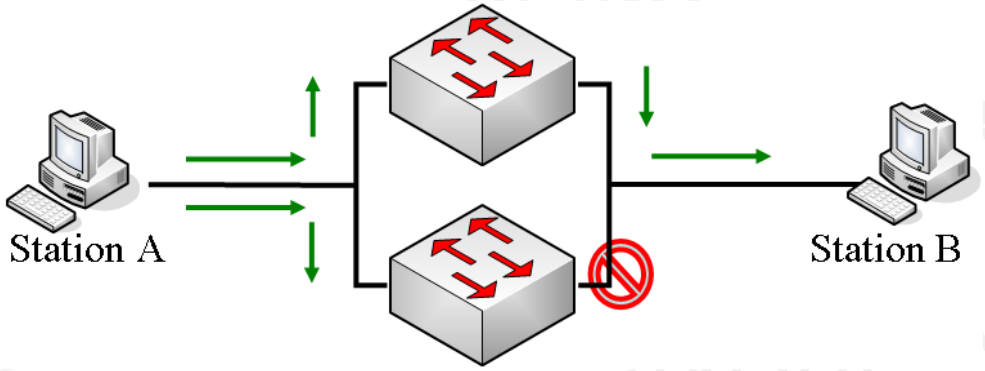
- le switch du haut reçoit sur son port 2 la trame du switch du bas
  - le switch **extrait l'adresse MAC source** et **l'insère dans sa table MAC** [port 2 = adresse MAC A]. Pour cela, **il supprime l'entrée précédente** qui était [port 1 = adresse MAC A]
- le switch du bas reçoit sur son port 4 la trame du switch du haut
  - le switch **extrait l'adresse MAC source** et **l'insère dans sa table MAC** [port 4 = adresse MAC A]. Pour cela, **il supprime l'entrée précédente** qui était [port 3 = adresse MAC A]

On voit ici que les switchs mettent à jour leur table MAC à chaque fois qu'ils reçoivent une trame.

Ce phénomène s'appelle l'**instabilité de la table MAC**.

# Résolution des 3 problèmes

- Protocole de Spanning-tree pour éviter les problèmes de : tempête de broadcast, duplication de trame et instabilité de table MAC
- Spanning-tree permet d'identifier une boucle physique et de la bloquer « logiciellement »




- Dans cet exemple, tout le trafic passera par le switch du haut pour joindre la station B, le chemin du bas étant bloqué au niveau du port du switch du bas.
- Si le switch du haut tombe en panne, le protocole spanning-tree va le détecter et va débloquer le port du bas. A ce moment, tout le trafic passera pour le switch du bas.

# Le Protocole Spanning Tree (STP) (arbre couvrant)

- C'est un protocole réseau de couche 2 conçu pour les commutateurs et les ponts.
- Permet une topologie réseau sans boucle dans un contexte de liaisons redondantes entre des matériels de couche 2.
- STP détecte et désactive des boucles et fournit un mécanisme de liens de backup.
- Permet de faire en sorte que des matériels compatibles avec le standard ne fournissent qu'un seul chemin entre 2 stations d'extrémité.
- Défini dans la norme IEEE 802.1D

# Mode de fonctionnement

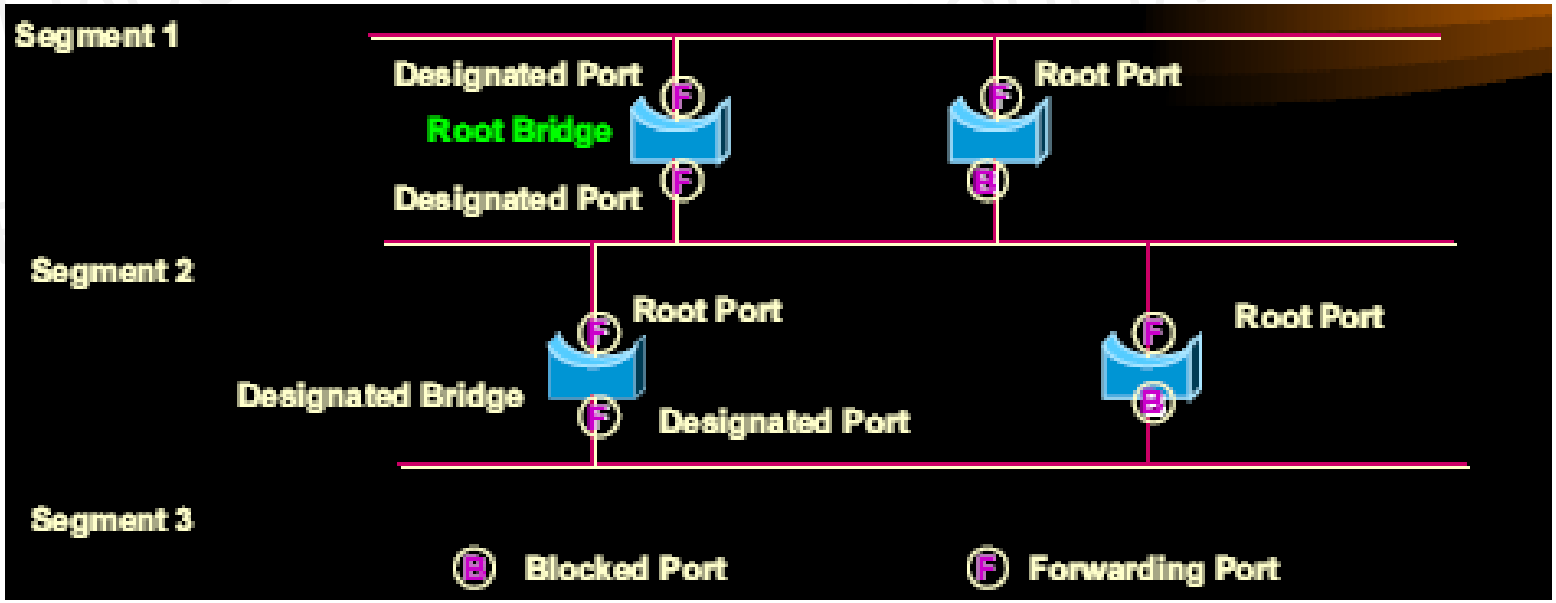
- Topologie sans boucle : les réseaux doivent avoir un unique chemin entre 2 points
- STP crée un chemin sans boucle basé sur le chemin le plus court → chemin établi en fonction de la somme des coûts de liens entes les switchs, basés sur la vitesse d'un port.
- Un chemin sans boucle suppose que certains ports soient bloqués et pas d'autres.
- STP échange régulièrement des informations appelées **BPDU –Bridge Protocol Data unit,** afin qu'une éventuelle modification de topologie puisse être adaptée sans boucle.
- STP garantit l'unicité du chemin entre 2 points du réseau en affectant un port dédié (***root port***), celui qui a le chemin le plus court vers le **root bridge**, à chaque segment du LAN (domaine de collision).
- La présence de boucle génère des tempêtes de diffusion (Broadcast storm) qui paralysent le réseau
- Un bon réseau doit inclure une redondance des matériels pour fournir un chemin alternatif en cas de panne

# Bridge Protocol Data Units (BPDU)

- Les Identificateurs de ponts (BID) et autres informations du protocole *spanning tree* sont transportés dans des unités de trames de données spéciales nommées **BPDU** (*Bridge Protocol Data Units*).
- Les BPDU sont échangées régulièrement (toutes les deux secondes) et permettent aux commutateurs de garder une trace des changements sur le réseau afin d'activer ou de désactiver les ports requis.
- Quand un ***commutateur*** ou un ***pont*** est raccordé au réseau, il commence par envoyer des BPDU afin de déterminer la topologie du réseau, avant de pouvoir commencer à transférer des données.

# Election d'un « root bridge » (ou switch root) (1)

- Une topologie sans boucle ressemble à un arbre et à la base de chaque arbre, on trouve ses racines (*roots*).
- Le switch root (ou le *root bridge- commutateur maître-*) sera le point central de l'arbre STP. Il est automatiquement choisi par l'algorithme du *spanning tree*.



# Election d'un « root bridge » (ou switch root) (2)

- Chaque commutateur a une **adresse MAC** (6 oct) et un numéro de priorité paramétrable (2 oct) égale par défaut à 32768 (0x8000 par défaut) dans 802.1d, multiples de 4096 sur 16 bits. Ces deux nombres constituant l'identification du *bridge* (nommée BID).
- Le switch qui aura le BID le plus faible c'est celui qui sera élu « Root».

**exemple**: un commutateur avec une priorité par défaut de 32768 (8000 Hex) et une adresse MAC 00:A0:C5:12:34:56

son BID est : 8000:00A0:C512:3456

# Election d'un « root bridge » (ou switch root) (3)

- On peut changer la priorité d'un switch avec la commande :

  (config)#**spanning-tree [vlan** *vlan-id*] **priority** *priority*

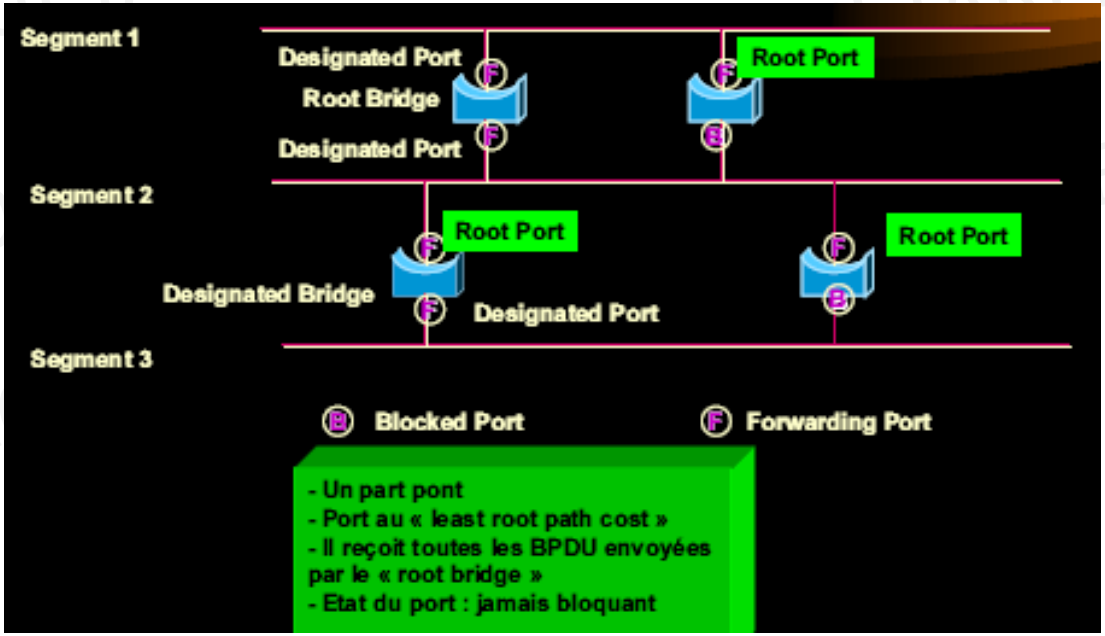
- Le BID est utilisé pour élire le *root bridge* en fonction des numéros de priorité. En cas d'égalité, l'adresse MAC la plus basse l'emporte, et comme toutes les adresses MAC sont uniques, un commutateur pourra toujours être élu comme *root bridge*.

# Election d'un « root bridge » (ou switch root) (4)

- Les autres commutateurs du réseau vont alors calculer la distance la plus courte vers le *root bridge* en utilisant le « coût » de bande passante le plus faible.
- Le numéro de priorité est normalement laissé par défaut, mais l'administrateur du réseau peut s'il le souhaite modifier ce numéro pour faire élire un commutateur particulier ; dans le cas contraire, tout le processus est automatique.
- Sur un root bridge, **tous les ports sont des ports désignés**, autrement dit, ils sont en état « forwarding », ils envoient et reçoivent le trafic.

# Election des « root ports » (1)

- Un « *port racine* » est un port qui sera utilisé pour transmettre les données (par opposition à un port bloqué). Chaque commutateur doit avoir un seul « *port racine* ».
- Chaque « commutateur non-racine » va sélectionner un « port racine » qui aura le chemin le plus court vers le « commutateur racine ».

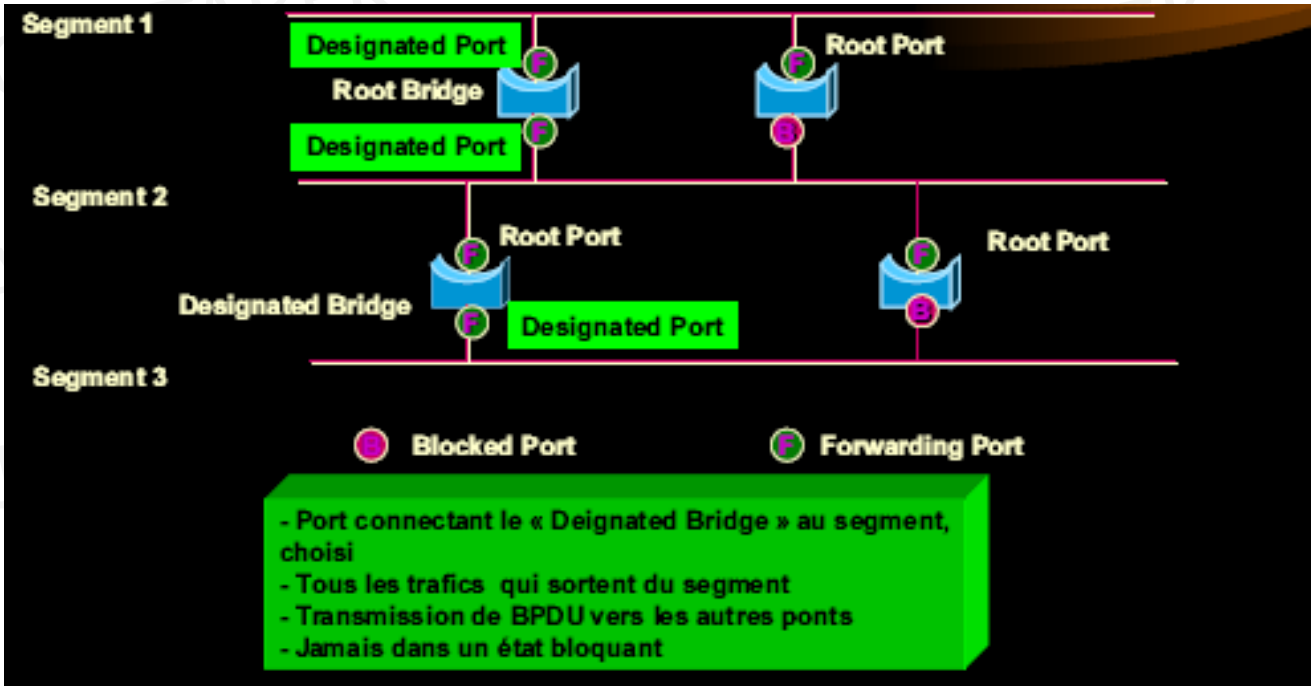


# Election des « root ports » (2)

- La sélection d'un « *port racine* » est effectuée d'après les champs **path cost** (coût du lien) 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.
- Un port bloqué ne peut émettre et recevoir des paquets BPDU (Bridge Protocol Data Units). Les autres ports d'un commutateur sont des « d*esignated ports »*, ce sont eux qui transmettent les paquets BPDU.

# Election d'un port désigné (Designated port) pour chaque segment (1)

- Pour chaque segment d'un LAN (domaine de collision), il y a un port désigné.
- Le port désigné est celui qui a le chemin le plus court vers le « pont racine ».



# Election d'un port désigné (Designated port) pour chaque segment (2)

- Les ports désignés sont normalement en état « forwarding », autrement dit, envoient et reçoivent du trafic de données.
- Si plus d'un port sur un même segment a le même coût vers le switch Root, le port du switch qui l'ID la plus faible est choisi. Tous les autres sont des ports non-désignés en état « blocking ».

# Récapitulation

- **1 switch Root par réseau dont tous les ports sont désignés**
- **1 port Root par switch non-root**
- **1 port désigné par domaine de collision**
- **Tous les autres ports sont non-désignés**

# Exemple

Soit un pont d'ID=92 qui a reçu un ensemble de BPDU de configuration conformément au tableau ci-après :

| | ID racine | coût | ID pont émetteur |
|---|---|---|---|
| Port 1 | 11 | 90 | 50 |
| Port 2 | 11 | 83 | 41 |
| Port 3 | 81 | 0 | 81 |
| Port 4 | 17 | 32 | 26 |

**ID racine** : Identification du pont supposé être la racine

**ID pont émetteur** : Identification du pont émettant le message de configuration

**Coût** : coût du meilleur trajet depuis le pont émetteur jusqu'à la racine

**ID port**: adresse physique d'un port

# Exemple (suite)

L'ID racine le plus petit est 11; le coût le plus faible parmi les messages ayant 11 comme ID racine est 83, donc le port 2 est le port racine.

Le pont détermine ensuite sa distance au pont racine qui est 83. La BPDU de configuration que peut émettre notre pont vaut : 11.83.92.

Ce message est meilleur que celui qu'il a reçu sur les ports 1, 3 et 4. Le pont 92 est par conséquent « pont désigné » sur ces trois ports, sur lesquels il envoie sa BPDU de configuration.

# Mode des ports sur les commutateurs en STP (1)

Cinq états de ports peuvent être rencontrés sur un port STP, qui sont :

- **Listening** : le commutateur « écoute » les BPDU et détermine la topologie réseau.
- **Learning** : le commutateur construit une table faisant correspondre les adresses MAC aux numéros des ports.
- **Forwarding** : un port reçoit et envoie des données, opération normale.
- **Blocking** : un port provoquant une boucle, aucune donnée n'est envoyée ou reçue mais le port peut passer en mode *forwarding* si un autre lien tombe.
- **Disabled** : désactivé, un administrateur peut manuellement désactiver un port s'il le souhaite

# Mode des ports sur les commutateurs en STP (2)

- Quand un client tel qu'un ordinateur, une imprimante ou un serveur est connecté au réseau, son port se mettra automatiquement d'abord en mode *listening* puis en mode *learning*, avant de se mettre en mode *forwarding*. Le délai entre le mode *listening* et *forwarding* est d'environ 50 secondes.
- Pour raccourcir le délai de 50 secondes inhérent à la connexion d'un nouveau périphérique, le **Rapid STP** a été développé et standardisé par la norme IEEE ***802.1w*** qui permet à un port de commutateur de passer directement en mode *forwarding*.

# Différents états STP (1)

- Cinq états de ports peuvent être rencontrés sur un port STP. Chaque état comporte un délai.
- Propriétés : L'âge maximal de 20 secondes par défaut est le temps maximal pour que STP effectue de nouveaux calculs quand une interface ne reçoit plus de BPDUs.
- Le temps de forwarding de 15 secondes par défaut est le temps de passage d'un état "listening" à "learning" et de "learning" à "forwarding". Aussi, la fréquence d'envoi de BPDUs Hello est de 2 secondes par défaut.

# Différents états STP (2)

**Etat « Listening »** :

- le commutateur « écoute » les BPDU et détermine la topologie réseau.
- Rejette toutes les trames de données venant du segment attaché
- Rejette toutes les trames de données venant d'un autre port de transfert
- N'intègre aucun emplacement de station dans sa table MAC (il n'y pas d'apprentissage)
- Reçoit les BPDUs et les transmet à son système
- Envoie les BPDUs reçus de son système
- Répond à SNMP

# Différents états STP (3)

**Etat « Learning »**

- Rejette toutes les trames de données venant du segment attaché
- Rejette toutes les trames de données venant d'un autre port de transfert
- Intègre les emplacements de station dans sa MAC table (apprentissage)
- Reçoit les BPDUs et les transmet à son système
- Envoie les BPDUs reçus de son système
- Répond à SNMP

# Différents états STP (4)

**Etat « Forwarding »**

- Commute toutes les trames de données venant du segment attaché
- Commute toutes les trames de données venant d'un autre port de transfert
- Intègre les emplacements de station dans sa MAC table (apprentissage)
- Reçoit les BPDUs et les transmet à son système
- Envoie les BPDUs reçus de son système
- Répond à SNMP

# Différents états STP (5)

**Etat « Blocking »**

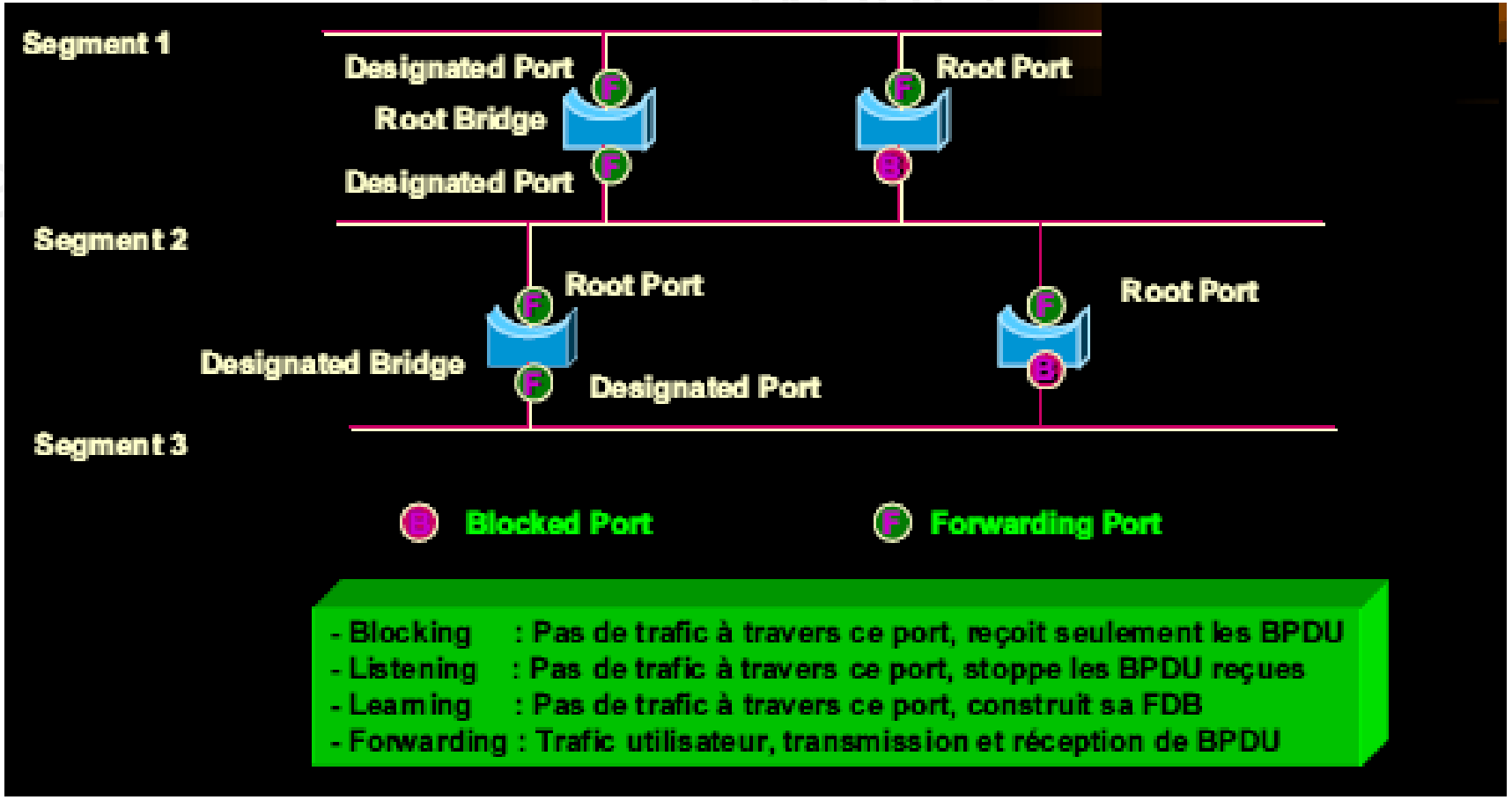
- Rejette toutes les trames de données venant du segment attaché
- Rejette toutes les trames de données venant d'un autre port de transfert
- N'intègre aucune emplacement de station dans sa MAC table (il n'y pas d'apprentissage)
- Reçoit les BPDUs et les transmet à son système
- N'envoie pas de BPDUs reçus de son système
- Répond à SNMP

# Différents états STP (6)

**Etat « Disabled »**

- Cet état est similaire à l'état « blocking » sauf que le port est considéré physiquement non opérationnel (*shut down ou problème physique*).

# Récapitulatif sur l'états des ports



# Paramètres de configuration



- Paramètres réseau
  - –Hello interval
    - •Fréquence à laquelle un « designated port » envoie des BPDU, 2 s par défault.
  - –Forward delay
    - •Passage de l 'état « listening, learning » à l 'état « forwarding », 15 s par défault
  - –Max age
    - •Pseudo TTL pour les BPDU
  - –Bridge priority (per bridge)
    - •Intervalle 1-32768, valeur par défaut 32768
- Paramètres liés au port
  - –Port cost
    - •Coût de transmission d 'une trame sur un segment
    - •Path cost
      - – coût total vers le « root bridge »
      - – lors de l 'envoi d 'une BPDU, le « port cost » du port précédent qui a reçu la BPDU est ajouté
    - •Par défaut : 1000/Débit en Mbps
      - •10 Base T = 100, 100 Base FX, FDDI = 10, ATM = 6
  - –Port priority

# Simulation du fonctionnement de STP

Visitez le site :

http://www.cisco.com/warp/public/473/spanning_tree1.swf

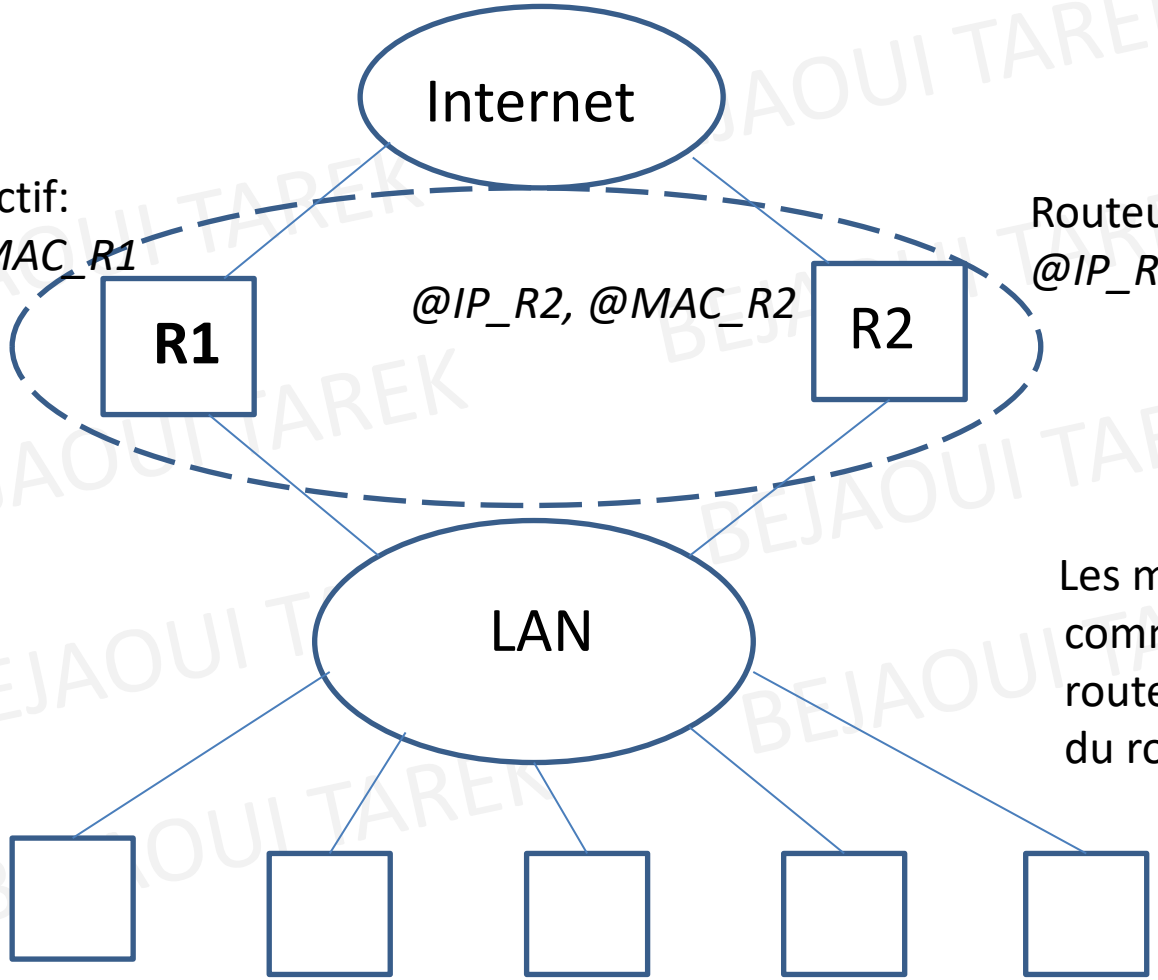
# Protocole VRRP (Virtual Router Redundancy Protocol)

- VRRP : un standard Internet proposant une solution permettant à un réseau de ne pas être complètement isolé lorsqu'un équipement d'interconnexion (routeur, commutateur-routeur) tombe en panne
- VRRP décrit comment installer plusieurs équipements de secours qui prennent la relève de l'équipement défaillant

# Protocole VRRP (Virtual Router Redundancy Protocol) - suite

- Deux routeurs ou plus se partagent une adresse IP et une adresse MAC virtuelles
- Un seul routeur est actif (Master router) à l'instant t
- En cas de panne du routeur actif, le changement de routeur est transparent pour les utilisateurs

# Protocole VRRP (Virtual Router Redundancy Protocol) - suite




R1 routeur actif:
*@IP_R1, @MAC_R1*

Routeur virtuel RV :
*@IP_RV, @MAC_RV*

Les machines du réseau ont comme seule adresse de routeur par défaut l'adresse du routeur virtuel: @IP_RV

# Protocole VRRP (Virtual Router Redundancy Protocol) - suite

Les routeurs VRRP utilisent l'adresse MAC virtuelle : 00-00-5E-00-01-Id du routeur VRRP (cet identifiant est codé sur 6 octets).

L'adresse IP virtuelle et les adresses IP réelles des routeurs sont déterminées par l'administrateur, en fonction de la structure du réseau.

# Protocole VRRP (Virtual Router Redundancy Protocol) - suite

Les routeurs VRRP se trouvent dans l'un des 3 états suivants:

- Initialize : le routeur attend un événement qui le fera basculer dans l'un des deux autres états
- Backup : sert à vérifier que le routeur actif est bien dans l'état Master et qu'il est en fonctionnement
- Master : dans cet état, le routeur actif informe les routeurs de secours (Backup routers) à intervalles réguliers qu'il peut toujours assurer le routage vers l'extérieur du réseau

# Réferences


- J.P Gautier, UREC - CNRS
- François Goffinet, Networking Academy, Cisco Systems, http://cisco.goffinet.org/s3/spanning_tree
- http://fr.wikipedia.org/wiki/Spanning_tree_protocol