







La commutation dans les LAN








Principe de la commutation
Matrices de commutation
Problème de congestion
Techniques et modes de commutation

Commutation dans les LAN

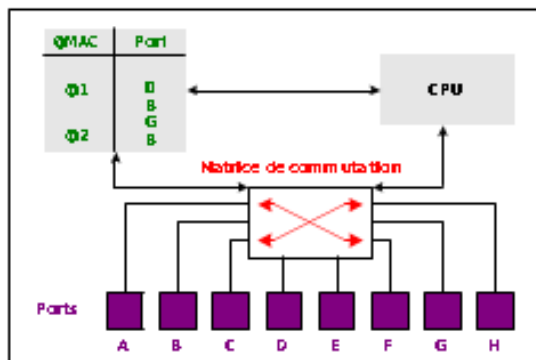
-  Issue de la téléphonie (RTC) et des réseaux grande distance (WAN)
-  Apparition dans Ethernet (Switched Ethernet)
-  garantit une certaine bande passante
-  évite les problèmes d'effondrement dans le cas des réseaux CSMA/CD chargés
-  permet des communications full-duplex
-  Aujourd'hui, les commutateurs sont largement utilisés dans les réseaux Ethernet

Principe de la commutation

Commutation = mise en relation directe d'un port d'entrée avec un port de sortie

-  établissement d'une liaison point à point
-  avant chaque communication par un protocole de signalisation spécifique (circuit virtuel)
-  dynamiquement (réseaux locaux) en fonction d'une table d'acheminement (FDB : Forwarding Data Base)
-  plus de problème d'accès multiples au support (évite les collisions)
-  Comment établir cette mise en relation ?
-  plus ou moins complexe, plus ou moins coûteux
-  nécessite de l'intelligence dans l'équipement

- Table construite par analyse du trafic entrant (@MAC source)
 - Les trames à destination d'une @ non présente dans la table sont répétées sur tous les ports sauf le port d'entrée
 - Plusieurs trames peuvent être traitées simultanément
 - Mémoire limitée dans le commutateur
 - Les entrées les plus anciennes sont effacées
 - Un timer est associé à chaque entrée de la table
- Il est réinitialisé lors de la réception d'une trame de cette provenance



L'algorithme de commutation



Matrices de commutation

Comment mettre en relation N ports d'entrée avec N ports de sortie ?

cross-bar complet : N^2 transistors passants ou bloqués, complexe, efficace, coûteux

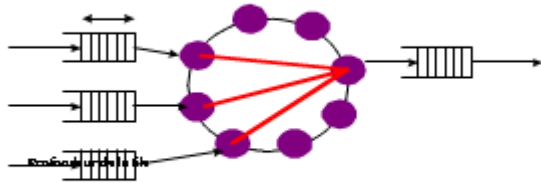
commutation type Banyan : $N \cdot \log N$ points de connexion (traversée de plusieurs étages, pas adapté à la diffusion)

architectures à bus interne ou à mémoire partagée avec gestion des accès multiples simultanés

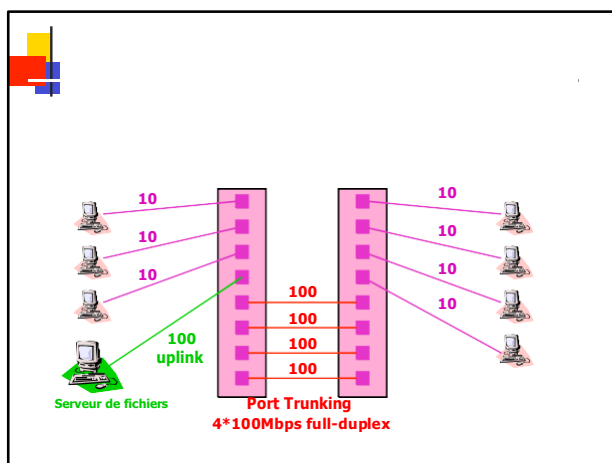
Problème de congestion

Plusieurs ports d'entrée peuvent simultanément être dirigés vers un même port de sortie

✎ saturation des files d'attente (perte de trames)



Solution partielle : attribuer plus de bande passante aux liens qui risquent d'être saturés



Contrôle de flux "back pressure" dans certains commutateurs

✎ émission de données vers les liens qui consomment trop de ressources du commutateur

-> provoque l'arrêt des émissions (collisions)

en CSMA/CD (ne fonctionne que pour du half-duplex)

✎ en full-duplex, émission d'une trame particulière indiquant un délai pendant lequel l'équipement ne doit plus émettre de trames

Techniques de commutation

"Cut through" - commutation rapide à la volée

- ✎ dès que le port de destination est connu (premier champ de la trame Ethernet), les données sont recopiées directement vers le port de sortie
- ✎ rapide mais pas appropriée si un port est relié à un hub standard (transmission des trames de collision erronées)

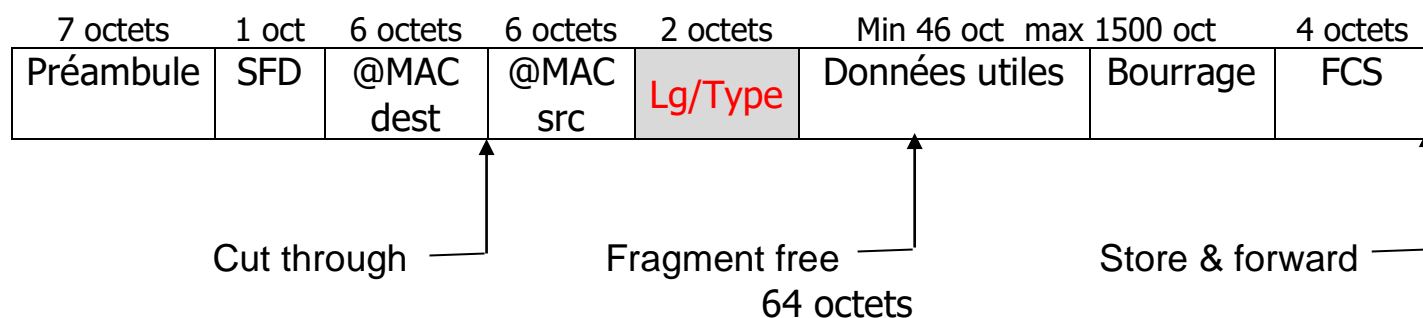
✎ "Store & Forward" - stockage avant retransmission

- ✎ une trame est entièrement mémorisée avant retransmission
- ✎ permet vérification du CRC, des longueurs minimales et maximales des trames, détection des trames de collision
- ✎ mais : mémoire sur le commutateur, délai supplémentaire

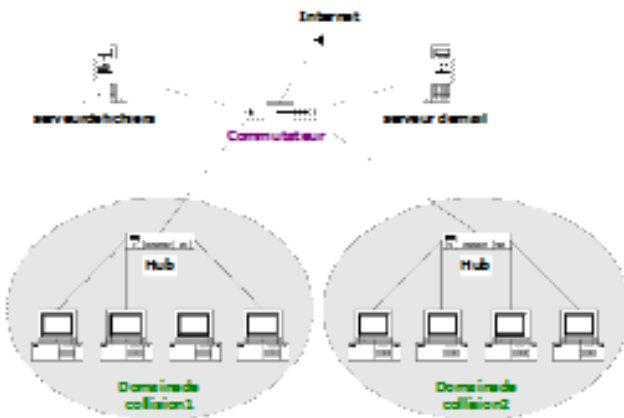
✎ Le commutateur fait du CSMA/CD sur un port relié à un hub
-> mémorisation obligatoire (retransmissions)

✎ Variantes

- ✎ méthode "fragment-free" : équivalent au "cut-through" mais supprime les trames trop courtes (collisions)
- ✎ méthode au choix de l'administrateur du commutateur : la méthode est fixée par une commande
- ✎ méthode adaptative :
 - démarrage en mode "cut-through"
 - passage en "store & forward" au delà d'un certain seuil de taux d'erreurs calculé par vérification des CRC (paramétrable ou non)
 - retour en mode "cut-through" en dessous du seuil



Séparation des domaines de collision



Un port du commutateur = un domaine de collision










Critères de choix du commutateur

- ✎ Quelle est la bande passante globale ?
- ✎ Commutateur de segments ou de stations ?
- ✎ Quelles performances ?
 - ✎ Temps de latence
 - ✎ cut-through : 1er bit entré - 1er bit sorti
 - ✎ store & forward : dernier bit entré - 1er bit sorti
- ✎ Le coût par port dépend
 - ✎ architecture (matrice de commutation)
 - ✎ nombre d'adresses MAC gérées par port
 - ✎ taille des buffers en entrée/sortie pour chaque port
 - ✎ présence de ports 10/100/1000

Ethernet full-duplex

- ✎ Ethernet full-duplex impossible sur un support partagé avec accès CSMA/CD
- ✎ Ethernet full-duplex nécessite une liaison point à point, utilisable dans les deux sens de communication, sans méthode d'accès
- ✎ Fast Ethernet et Gigabit Ethernet utilisent des commutateurs qui émulent des liaisons point à point full-duplex pour
 - ✎ garantir la bande passante (elle n'est plus partagée)
 - ✎ diminuer les problèmes de limitation de distance
 - ✎ nécessite des cartes d'interface full-duplex sur les stations

Conclusions sur la commutation

-  Meilleur accès au média
 -  meilleur contrôle de la bande passante : le trafic est dirigé vers la station spécifiée uniquement
 -  la charge du réseau est mieux répartie (segmentation du trafic)
 -  moins de conflits d'accès, collisions réduites
-  Les trames de diffusion sont répétées sur tous les ports
-  Intelligence dans le port du commutateur
 -  analyse des trames, mémorisation, prises de décision
 -  temps de traversée de l'équipement plus élevé
-  Deux techniques : "store & forward" et "cut through"

Réseaux Locaux Virtuels (VLAN)

Principe des VLAN

Intérêts

Appartenance à un VLAN

Etiquetage des trames (802.1p/Q)

Pourquoi les VLANs ?

- ✎ Dans les réseaux locaux partagés
 - ✎ les sous-réseaux sont liés aux hubs
 - ✎ les utilisateurs sont groupés géographiquement
 - ✎ pas de sécurité sur un segment : n'importe quelle station du segment peut capturer l'ensemble du trafic réseau
 - ✎ la mobilité entraîne un changement d'adresse et/ou un re-câblage
 - ✎ les broadcasts interrompent tous les matériels réseau avec traitement au niveau du CPU

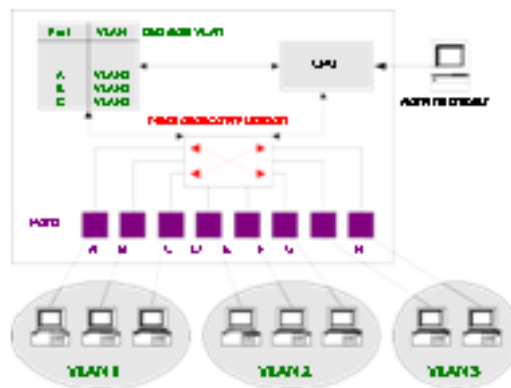


- ✎ Trois nécessités auxquelles un LAN commuté ne répond pas
 - ✎ Limitation des domaines de diffusion
 - ✎ Garantir la sécurité par isolement de certains trafics
 - ✎ Permettre la mobilité des utilisateurs
- ✎ Les VLANs : une nouvelle manière d'exploiter la technique de la commutation en donnant plus de flexibilité aux réseaux locaux
 - ✎ -> segmentation du réseau un peu à la manière de la commutation mais de façon logique (indépendamment du câblage physique)

Principe des VLANs

Créer des réseaux logiques indépendants les uns des autres

Une diffusion provenant d'une station du VLAN2 ne sera répercutée que sur les ports D, E, F



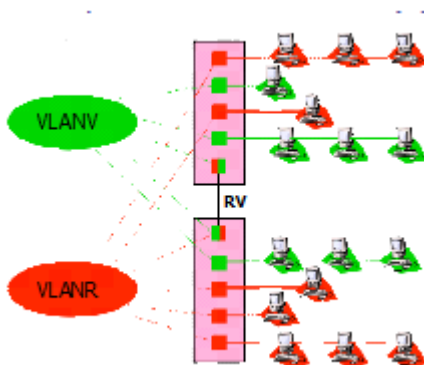
- ✎ L'administrateur configure statiquement la table des VLAN
- ✎ Les communications inter-VLAN ne sont possibles qu'à travers un routeur
- ✎ L'appartenance à un VLAN est indépendante de la localisation géographique - un VLAN peut s'étendre sur plusieurs commutateurs
- ✎ Un segment Ethernet est un domaine de collision
- ✎ Un VLAN est **un domaine de diffusion**

Intérêts des VLAN

- ✎ Confidentialité et sécurité
 - ✎ le trafic entre les réseaux virtuels est isolé
 - ✎ permet de limiter l'accès à certains équipements ou services (VLAN des machines en libre service, VLAN des accès à Internet, ...)
- ✎ Performance
 - ✎ limite la portée des broadcast (ARP)
 - ✎ répartition de la charge du réseau
- ✎ Facilité de mise en œuvre et souplesse
 - ✎ logiciel d'administration du commutateur
 - ✎ on peut retirer ou donner l'accès à un VLAN sans modifier le câblage dans les armoires de brassage, voire sans déplacer la station
 - ✎ une station peut appartenir à plusieurs VLANs

Appartenance à un VLAN

- ✎ définie par le port physique du commutateur
 - ✎ chaque port est associé à 1 ou plusieurs VLAN
 - ✎ configuration statique fixée par l'administrateur
 - ✎ inconvénient : le déplacement d'une machine nécessite la reconfiguration du port du commutateur
 - ✎ sécurisé : un utilisateur ne peut pas changer de VLAN
- ✎ définie par l'adresse MAC
 - ✎ plus souple : permet la mobilité des machines sans reconfigurer les VLAN
 - ✎ l'administrateur doit connaître les @ MAC...
 - ✎ deux stations du même segment Ethernet peuvent appartenir à des VLAN distincts
 - ✎ moins sécurisé : un utilisateur peut changer son @ MAC
- ✎ définie par les adresses de niveau 3 (IP)
 - ✎ très souple : association d'un préfixe IP (@ de sous-réseau ou plages d'@) et d'un numéro de VLAN
 - ✎ un routeur permet de passer d'un VLAN à l'autre
 - ✎ perte de performance : il faut analyser les trames au niveau 3 pour déterminer l'appartenance à un VLAN
 - ✎ ne respecte pas l'indépendance des couches...
 - ✎ non sécurisé : l'utilisateur peut facilement changer son @ IP
- ✎ définie par protocoles de niveau 3 (permet d'isoler le trafic de chaque protocole)
- ✎ définie par numéro de port TCP (permet d'isoler le trafic de chaque type d'applications)



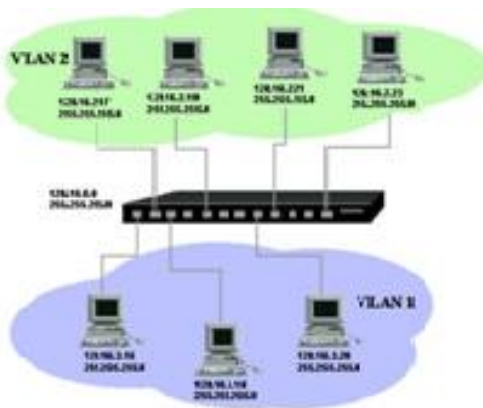
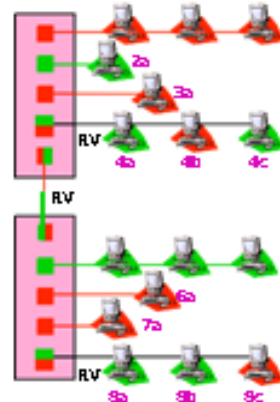
Pas de filtrage des broadcasts sur un même segment

VLAN de niveau 1 (par port ou segment)

Pas d'analyse de la trame pour déterminer l'appartenance à un VLAN

VLAN de niveau 2 ou 3





- ✎ Une adresse MAC ne peut appartenir qu'à un seul VLAN
- ✎ Plusieurs VLAN par port autorisés
- ✎ Nécessite une analyse de chaque trame
- ✎ Echange des tables de correspondances @MAC/VLAN entre les commutateurs ou étiquetage des trames nécessaires



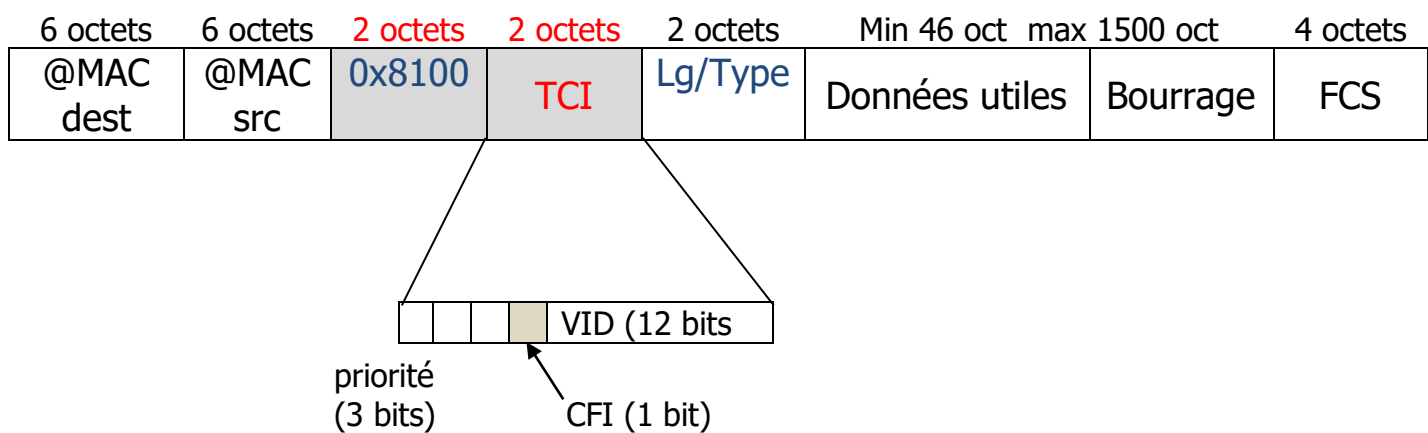
VLAN sur plusieurs commutateurs

- ✎ Il faut transporter l'information d'appartenance à un VLAN (chaque commutateur doit connaître le VLAN associé à la source et au destinataire)
- ✎ Deux possibilités
 - ✎ chargement des tables de VLAN dans tous les équipements (problème de facteur d'échelle)
 - ✎ ajout d'une étiquette aux trames transportées entre les commutateurs uniquement (côté émetteur)
 - ✎ l'étiquette identifie le VLAN de la station source
 - ✎ norme IEEE 802.1p/Q : format des étiquettes indépendant du constructeur de l'équipement

 Modification transparente de l'en-tête MAC (compatibilité avec les anciens équipements)

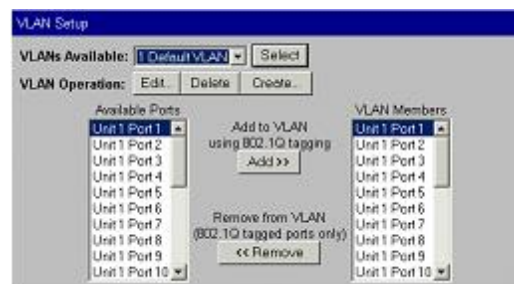
-  un niveau d'encapsulation 802.1p/Q identifié par 0x8100
-  la trame 802.3 est allongée de 4 octets (nécessite de recalculer le FCS)
-  champ priorité sur 3 bits : files d'attente plus ou moins prioritaires dans les commutateurs (QoS - voix par ex.)
-  bit CFI pour le routage par la source

Trame IEEE 802.1p/Q

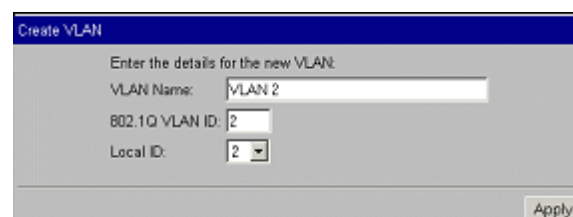


Administration des VLANs

- Création/suppression d'un VLAN
- Ports supportants l'étiquetage 802.1Q des trames



- Paramétrage d'un VLAN



- Configuration d'un port








Port 7 Setup

Port:	7	Media Type:	10 BASE-T/100 BASE-TX
Link State:	Disabled	Port Speed:	10Mbps FD
Auto negotiation:	Enabled	Port State:	Enabled
Speed/Duplex:	Auto	Security:	Disabled
FD Flow Control:	Auto	PACE:	Stack Default
HD Flow Control:	Enabled	VLT Tagging:	Disabled
802.1p Multicast Learning:	Stack Default	802.1Q VLAN Learning:	Stack Default
Untagged VLAN:	2 VLAN 2		
Fwd Unknown VLAN Tags:	Auto		

Apply

Règles de design des VLAN

Les questions qu'il faut se poser

-  nombre d'utilisateurs du réseau ?
-  plan du campus et plan de câblage ?
-  partitions des utilisateurs partageant des données ou des services ?
-  les utilisateurs qui partagent des données sont-ils géographiquement proches ?
-  la mobilité se fait-elle par département ou par éléments isolés ?
-  répartition du trafic sur le réseau ?
-  ressources centralisées ou distribuées ?