Chapitre2:
Les Réseaux commutés

Enseignante: Soumaya Dahi

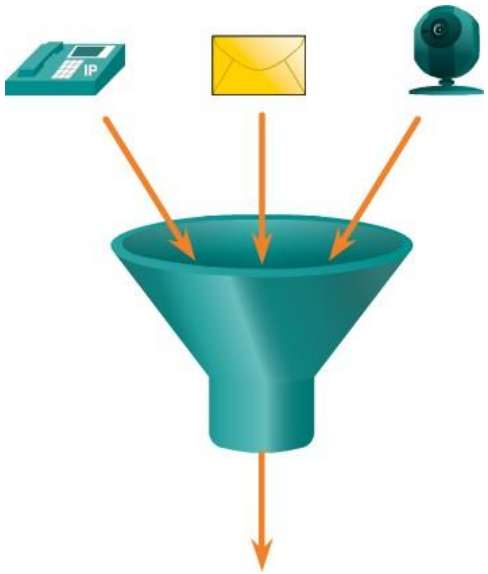
Réseaux convergents

Complexité croissante des réseaux

- Le monde numérique change
  - Les informations doivent être accessibles où que l'on se trouve dans le monde
  - Les réseaux doivent être sécurisés, fiables et extrêmement disponibles

Éléments d'un réseau convergent

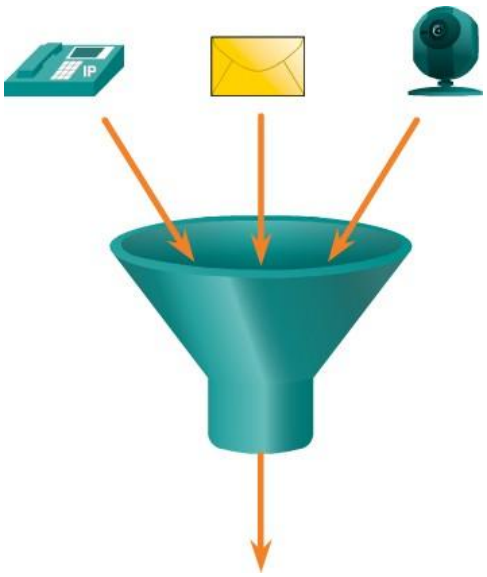
- La collaboration est une exigence
  - Pour prendre en charge la collaboration, les réseaux utilisent les solutions convergentes
  - Services de données tels que les systèmes vocaux, les téléphones IP, les passerelles voix, la prise en charge de la vidéo et les vidéoconférences
  - Le contrôle des appels, la messagerie vocale, la mobilité et le standard automatisé sont d'autres fonctions courantes



RÉSEAUX CONVERGENTS

Avantages des réseaux convergents :

- Plusieurs types de trafic, un seul réseau à gérer
- Des économies considérables sur l'installation et la gestion des différents réseaux (voix, vidéo, données)
- Gestion informatique intégrée



Rôle des réseaux commutés

- Le rôle des réseaux commutés a évolué
  - Un réseau local (LAN) commuté accroît la flexibilité et permet la gestion du trafic
  - Il prend également en charge des fonctionnalités telles que la qualité de service, la sécurité renforcée, la prise en charge de la technologie sans fil et de la téléphonie IP, et les services de mobilité

ÉQUIPEMENTS D'INTERCONNEXION

- Les équipements d'interconnexion de réseaux permettent :
  - de **relier des réseaux hétérogènes** (couches et protocoles différents)
  - d'**organiser au mieux le réseau** pour une exploitation optimale (adressage des réseaux et sous-réseaux,...)
  - de **contourner les limites techniques** des architectures des réseaux (augmentation des distances des segments physiques, changement de support physique, ...)

ÉQUIPEMENTS D'INTERCONNEXION

- Le répéteur (transceiver):
- C' est un équipement d'interconnexion de niveau 1
- Il reçoit des informations et les retransmets en régénérant un signal afin de compenser l'affaiblissement .
- Un répéteur permet de connecter 2 segments Ethernet dans un LAN et d'augmenter ainsi la distance d'un segment physique

ÉQUIPEMENTS D'INTERCONNEXION

Le concentrateur (*hub*)

- est aussi un équipement d'interconnexion de niveau 1
- Le *hub* se comporte comme un **répéteur multi-ports**.
- Un Hub récupère les trames Ethernet en provenance d'un port et les renvoie vers tous les autres ports.
- Avantage: on est 'sûr' que le destinataire recevra l'information.
- ***Inconvénients : toutes les interfaces pour lesquelles la trame n'est pas destinée la recevront également.***
  - ***Cela génère beaucoup de trafic inutile sur le réseau, il y a risque de saturation.***
- En *Ethernet* avec un *hub* 100Mbps, on obtient un débit partagé de 100Mbps pour l'ensemble des équipements raccordés.
- La trame n'est jamais modifiée lors de la traversée d'un répéteur ou d'un concentrateur (*hub*)

ÉQUIPEMENTS D'INTERCONNEXION

- **Le Pont/Bridge:**
- a 2 ports physiques
- Le Switch peut avoir de 4 à plusieurs **centaines** de ports physiques
- Le fonctionnement interne est quasiment le même entre ces 2 équipements
- L'avantage du Bridge par rapport au Hub est qu'il lit la couche 2 du modele OSI, appelée **liaison de données**, donc il connait toutes les adresses MAC du réseau sur ses deux ports physiques.

- Lorsqu'une trame arrive sur un port du Bridge, ce dernier lit dans l'entête Ethernet le champ **adresse MAC destination** et vérifie sur quel port cette adresse MAC a été vue:
  - si l'adresse MAC de destination se trouve **sur le même port de réception** alors le Bridge **supprime la trame** car la trame n'a pas besoin de traverser le Bridge pour joindre sa destination
  - si l'adresse MAC de destination se trouve **sur l'autre port** alors le bridge **commute** la trame vers ce port pour transmettre l'information vers l'autre coté (dans mon exemple, l'autre bâtiment)
- Avec ce comportement, le Bridge "coupe" le réseau en **deux domaines de collision**

ÉQUIPEMENTS D'INTERCONNEXION

Switch

- équipement d'interconnexion de niveau 2 qui relie des équipements appartenant à un même réseau physique (LAN).
- Alors que les Hubs ne font que transférer, de façon aveugle, les trames à travers le réseau, les switchs sont capables de connaître la destination en consultant dans chaque trame l'adresse MAC de l'expéditeur et du destinataire.
- un switch est capable de transférer exactement la trame sur le port où est raccordé le destinataire (sauf les trames de Broadcasts).
- En Ethernet avec un switch 100Mbps, on obtient un débit dédié de 100Mbps par port.
- Un réseau Ethernet constitué d'un switch suit une topologie physique et logique en étoile.

ÉQUIPEMENTS D'INTERCONNEXION

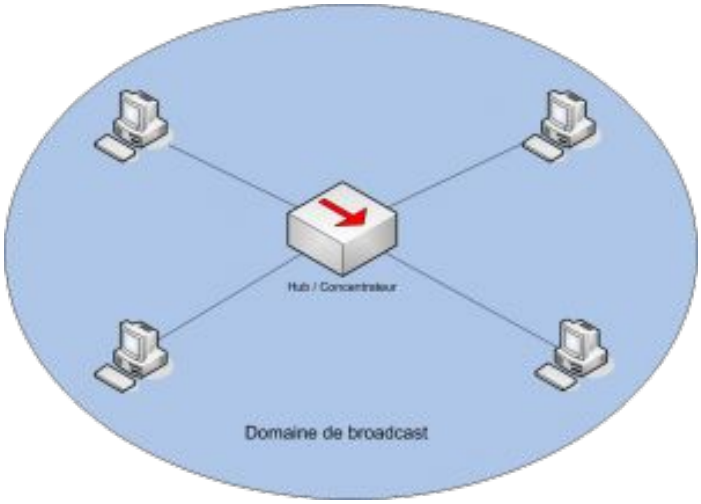
- **Routeur**
- C'est une passerelle entre le LAN (réseau local) et un autre réseau (Internet par exemple).
- Ils sont employés pour relier 2 réseaux ensemble et diriger le trafic des réseaux basés sur les adresses IP.
- Le routeur contient une base de données appelée « Routing Table » qui détient des chemins d'accès aux différents réseaux.
- Ils sont parfois associés à des fonctions de sécurité de type pare-feu « (Firewall) » pour filtrer les accès distants.
- Un routeur doit être configuré pour pouvoir connaître où router les messages.
- Les mécanismes de routage sont basés sur l'adresse IP.

LES DOMAINES DE DIFFUSION

- Un **domaine de diffusion (broadcast domain)** est une aire logique d'un réseau informatique où n'importe quel ordinateur connecté au réseau peut directement transmettre à tous les autres ordinateurs du même domaine, sans devoir passer par un routeur.
- c'est une zone du réseau informatique composée de tous les ordinateurs et équipements de communication qui peuvent être contactés en envoyant une trame à l'adresse de diffusion de la couche liaison de données (L2).
- Généralement, les concentrateurs et commutateurs conservent le même domaine de diffusion, alors que les routeurs les divisent.
- L'utilisation de réseaux virtuels permet cependant de séparer virtuellement un commutateur en plusieurs domaines de diffusion.
- Le routeur est un élément indispensable à la communication de deux domaines de diffusions.

LES DOMAINES DE DIFFUSION

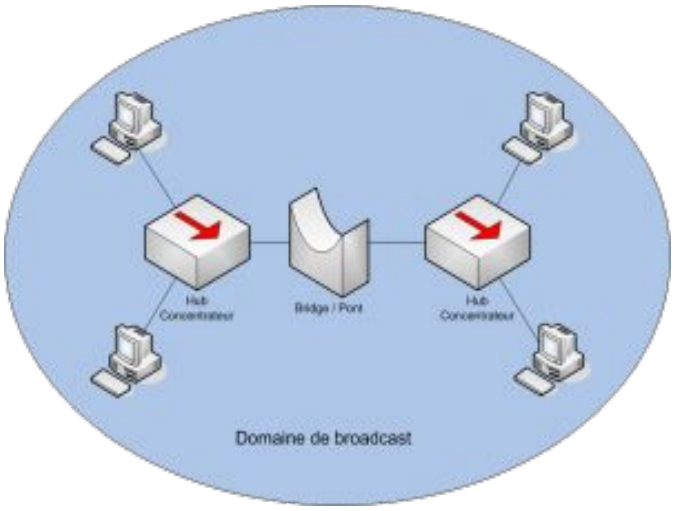
- Domaine de broadcast du Hub/Concentrateur



Un hub **ne lit pas** le niveau 2 donc il transmet la donnée sur tous ses ports

LES DOMAINES DE DIFFUSION

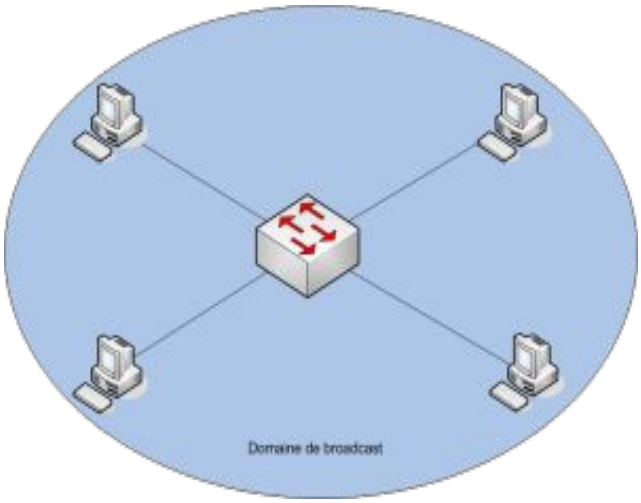
- Domaine de broadcast avec le Bridge/Pont



Un bridge **lit le niveau 2** et comprend que la donnée est a destination de tout le monde (adresse MAC destination = **ffff.ffff.ffff**) donc elle transmet cette donnée sur son second port

LES DOMAINES DE DIFFUSION

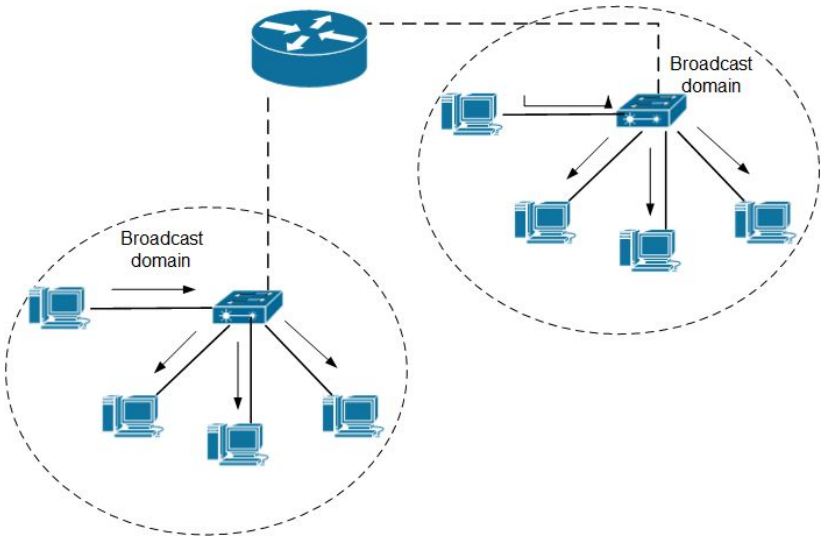
- Domaine de broadcast avec le Switch/Commutateur



Un Switch **lit aussi le niveau 2** et comprend que la donnée est a destination de tout le monde (adresse MAC destination = **ffff.ffff.ffff**) donc elle transmet cette donnée sur tous ses ports

LES DOMAINES DE DIFFUSION

- Domaine de broadcast avec le Routeur



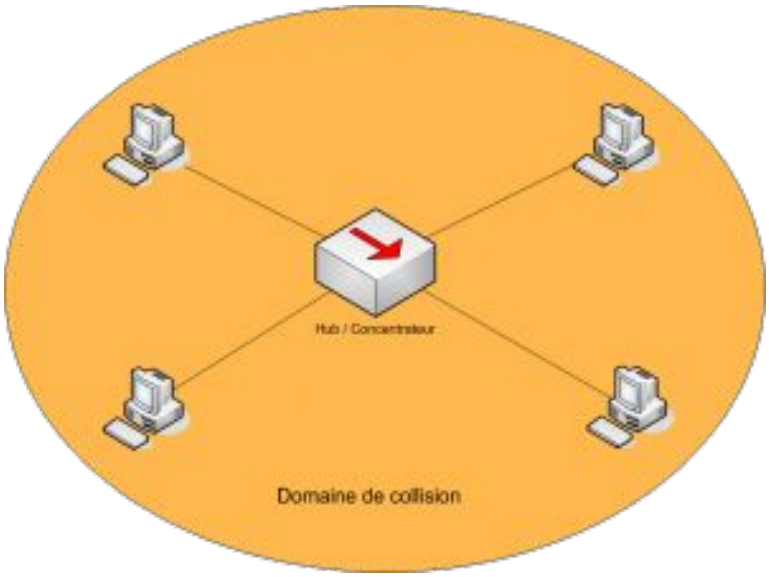
avec la **présence d'un routeur**, la notion de domaine de broadcast **explose** et on a un domaine de broadcast par interface du routeur.

LES DOMAINES DE COLLISION

- Un domaine de collision est une région du réseau au sein de laquelle les hôtes partagent l'accès au média
- Un **domaine de collision** est une zone logique d'un réseau informatique où les paquets de données peuvent entrer en **collision** entre eux.
- si deux entités sont dans le même **domaine de collision** et envoient des données à un instant T alors il y a **corruption** des données et il faut **retransmettre** les données.

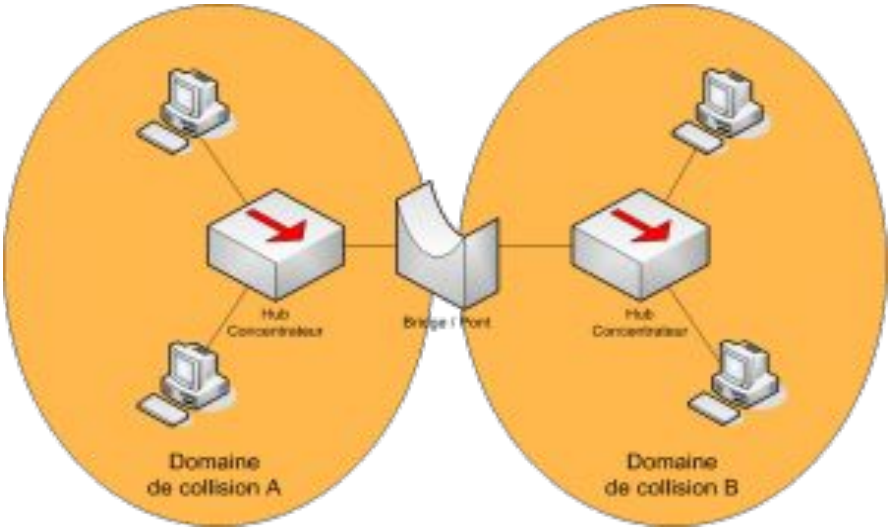
LES DOMAINES DE COLLISION

- Domaine de collision avec le Hub/Concentrateur



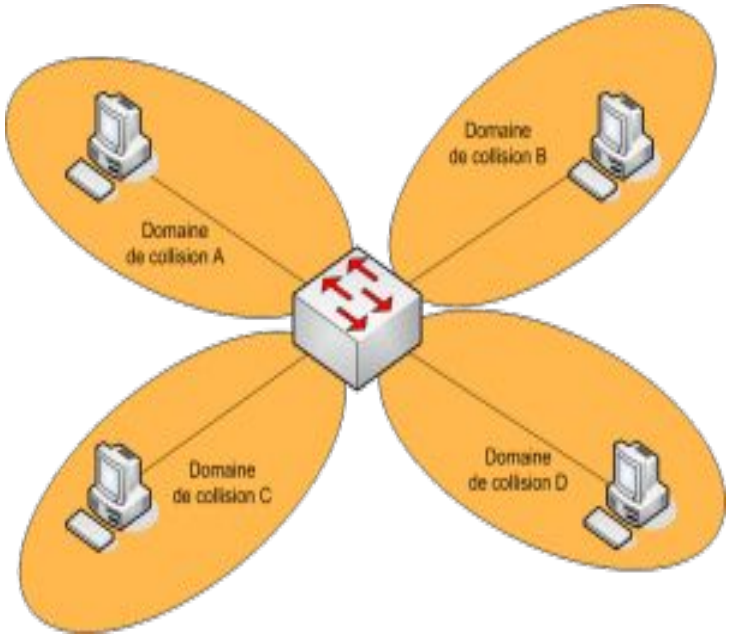
LES DOMAINES DE COLLISION

- Domaine de collision avec le Bridge/Pont



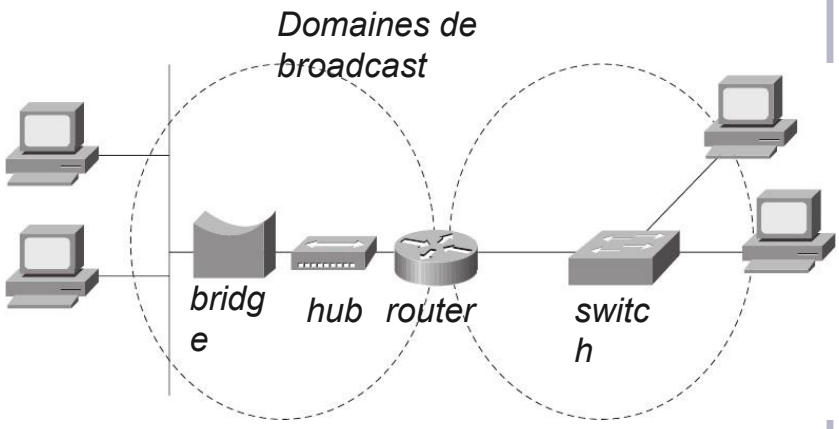
LES DOMAINES DE COLLISION

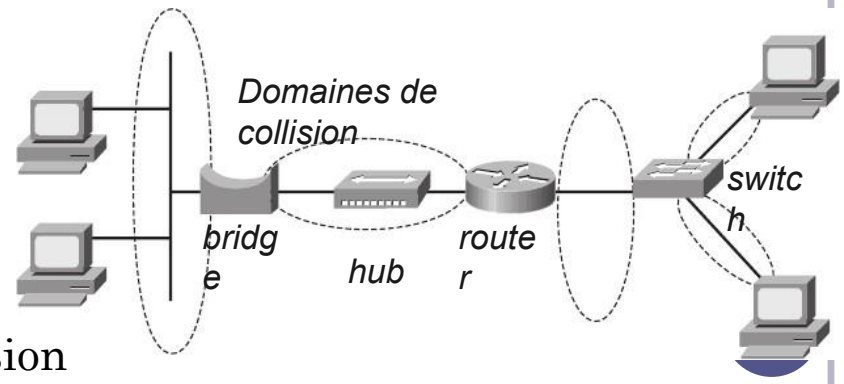
- Domaine de collision avec le Switch/Commutateur



Domaines de broadcast *versus* collision

- Répéteurs (*hub*) étendent les domaines de collision
- Ponts (*bridge*) et commutateurs (*switch*) étendent les domaines de broadcast
- Routeurs délimitent les domaines de broadcast
- Chaque port d'un commutateur/pont délimite un domaine de collision

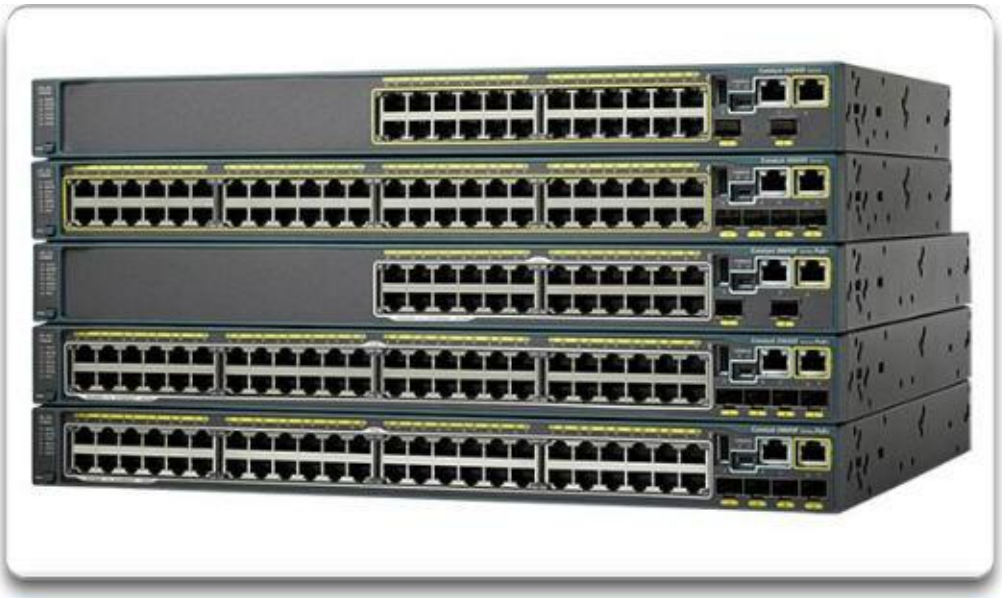




- LES COMMUTATEURS

Facteur de forme

- Fixe



Les fonctions et les options sont limitées à celles fournies à l'origine avec le commutateur.

Facteur de forme

- Modulaire

Le châssis accepte les cartes d'interface qui contiennent les ports.

Facteur de forme

- Empilable

Les commutateurs empilables, connectés à l'aide d'un câble spécial, fonctionnent comme un seul commutateur de grande taille.

La commutation comme concept général

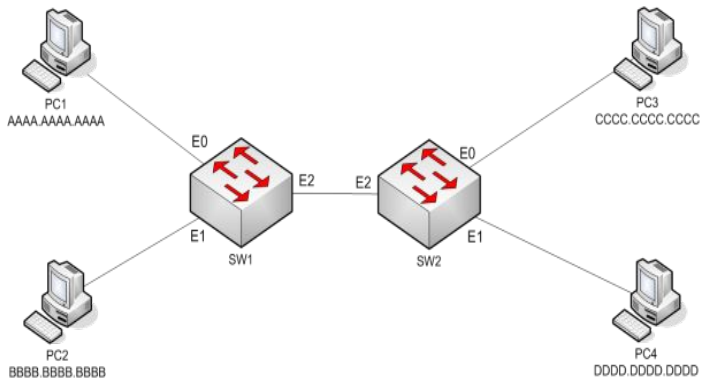
- Un commutateur prend une décision en fonction du port d'entrée et de destination
- Un commutateur LAN gère une table qu'il utilise pour déterminer comment acheminer le trafic
- Les commutateurs LAN transmettent des trames Ethernet basées sur l'adresse MAC de destination des trames.

Remplissage dynamique de la table d'adresses MAC d'un commutateur

- Un commutateur doit d'abord savoir quels équipements figurent sur chaque port avant de pouvoir transmettre une trame
- Il crée une table appelée table d'adresses MAC, ou table de mémoire associative (CAM)
- Le port de mappage de périphériques est stocké dans la table CAM
- Les informations de la table d'adresses MAC sont utilisées pour transmettre les trames
- Lorsqu'un commutateur reçoit une trame entrante dont l'adresse MAC ne figure pas dans la table CAM, il l'envoie à tous les ports, sauf à celui qui l'a reçue.

Remplissage dynamique de la table d'adresses MAC d'un commutateur

- Exemple:quatre PC sont branchés physiquement sur les switchs SW1 et SW2



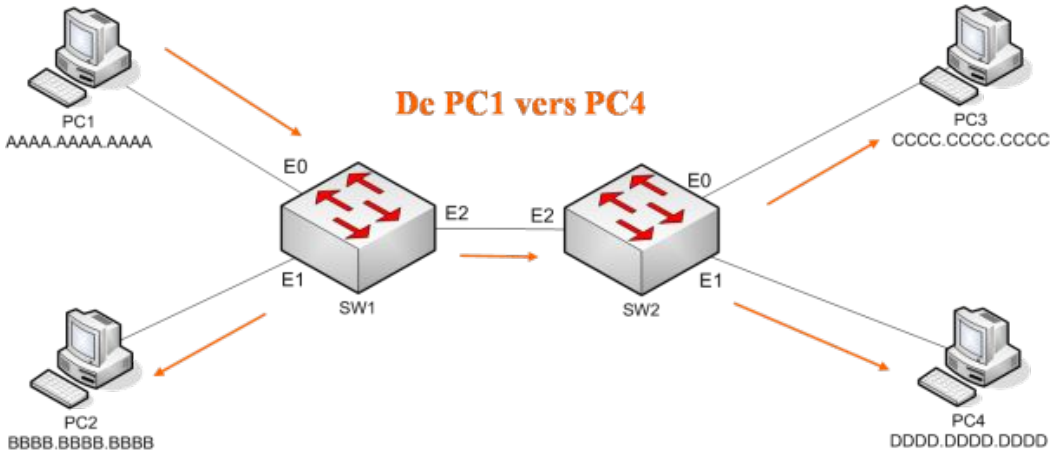
Interface	MAC
E0	
E1	
E2	

Interface	MAC
E0	
E1	
E2	

- Dans chaque switch se trouve une base de données appelée “table MAC” pour **Medium-Access-Control** ou “table CAM” pour **Content-Addressable-Memory**.
- Cette table fait le lien entre les ports physiques du switch (E0, E1, E2) et les adresses MAC sources qui arrivent sur ces ports.
- Lorsqu’on démarre un switch, ce dernier ne peut pas savoir quel PC est connecté sur tel ou tel port, la table est donc logiquement vide.

Remplissage dynamique de la table d'adresses MAC d'un commutateur

- Trame initiée par PC1 à destination de PC4



Interface	MAC
E0	AAAA.AAAA.AAAA
E1	
E2	

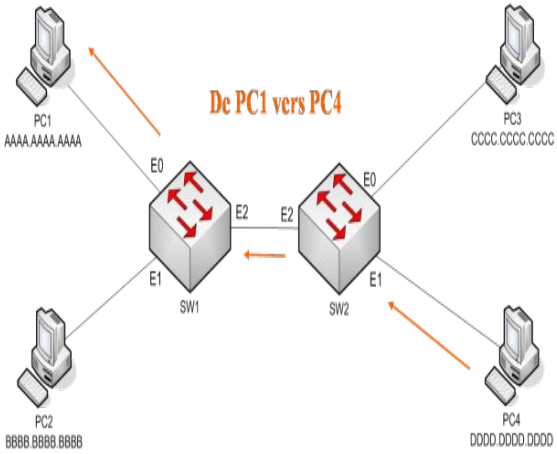
Interface	MAC
E0	
E1	
E2	AAAA.AAAA.AAAA

Remplissage dynamique de la table d'adresses MAC d'un commutateur

- 1. la trame sort de la carte réseau de PC1 avec:
  - adresse MAC source = AAAA.AAAA.AAAA
  - adresse MAC destination = DDDD.DDDD.DDDD
- 2. la trame arrive sur le port E0 du switch SW1
  - le switch extrait l'adresse MAC source et l'insère dans sa table (cf schéma). Maintenant le switch sait que pour joindre cette adresse MAC (AAAA.AAAA.AAAA), il doit commuter les trames vers le port E0. Cette information lui servira donc pour le retour de la trame.
  - puis le switch extrait l'adresse MAC destination (DDDD.DDDD.DDDD) et la compare à sa table: aucune entrée trouvée donc ne sachant pas où envoyer la trame, il la diffuse sur tous les ports excpetés le port de réception E0.
- 3. la trame arrive sur le port E2 du switch SW2
  - le switch extrait l'adresse MAC source et l'insère dans sa table (cf schéma). Maintenant le switch sait que pour joindre cette adresse MAC (AAAA.AAAA.AAAA), il doit commuter les trames vers le port E2. Cette information lui servira donc pour le retour de la trame.
  - puis le switch extrait l'adresse MAC destination (DDDD.DDDD.DDDD) et la compare à sa table: aucune entrée trouvée donc ne sachant pas où envoyer la trame, il la diffuse sur tous les ports excpetés le port de réception E2.
- 4. la trame arrive sur la carte réseau du PC4: gagné pour la trame aller!

Remplissage dynamique de la table d'adresses MAC d'un commutateur

- Trame réponse envoyée par PC4 à destination de PC1



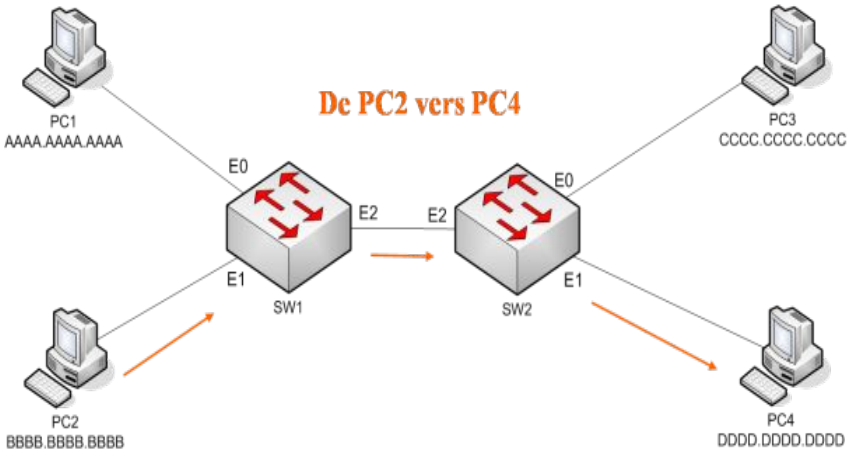
Interface	MAC
E0	AAAA.AAAA.AAAA
E1	
E2	DDDD.DDDD.DDDD

Interface	MAC
E0	
E1	DDDD.DDDD.DDDD
E2	AAAA.AAAA.AAAA

- la trame arrive sur les switchs, ils insèrent l'adresse MAC source DDDD.DDDD.DDDD dans leur table.
- Puis ils extraient l'adresse MAC destination (AAAA.AAAA.AAAA) et la comparent à leurs table et là ils savent où se situe cette adresse MAC; port E2 pour le switch SW2 et port E0 pour le switch SW1.
- Ils n'ont plus qu'à commuter la trame **UNIQUEMENT** sur le port en question.

Remplissage dynamique de la table d'adresses MAC d'un commutateur

- Trames envoyées par les différents PC



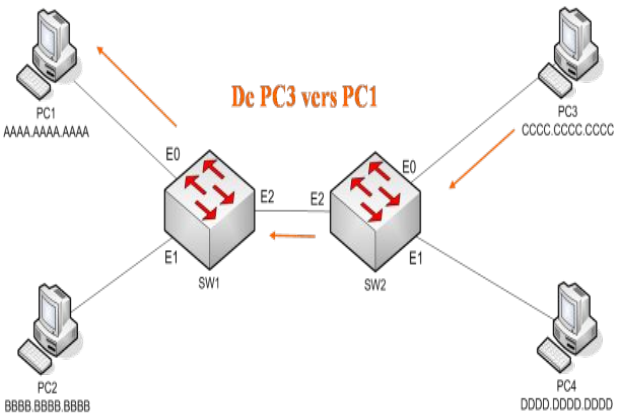
Interface	MAC
E0	AAAA.AAAA.AAAA
E1	BBBB.BBBB.BBBB
E2	DDDD.DDDD.DDDD

Interface	MAC
E0	
E1	DDDD.DDDD.DDDD
E2	AAAA.AAAA.AAAA BBBB.BBBB.BBBB

En générant petit à petit du trafic entre les différents PC, les tables MAC des switchs sont se remplir.

L'objectif est de ne plus diffuser les trames vers tous les ports mais uniquement vers un seul port, celui où se situe le PC de destination.

Remplissage dynamique de la table d'adresses MAC d'un commutateur



Interface	MAC
E0	AAAA.AAAA.AAAA
E1	BBBB.BBBB.BBBB
E2	DDDD.DDDD.DDDD CCCC.CCCC.CCCC

Interface	MAC
E0	CCCC.CCCC.CCCC
E1	DDDD.DDDD.DDDD
E2	AAAA.AAAA.AAAA BBBB.BBBB.BBBB

Pour visualiser le contenu de la table sur un switch Cisco:

```
Switch# show mac-address-table
```

- On dit que le switch a convergé quand sa table MAC contient toutes les adresses MAC se trouvant dans le réseau (des PC, des imprimantes, des bornes Widi, des serveurs,…).
- Les adresses des 4 PC sont bien dans chacune des tables de SW1 et SW2.
- Au final, lorsqu'une trame arrive sur SW1 ou SW2, ils sauront exactement où commuter cette trame.
- **Remarques importantes:**
- la table MAC est effacée à chaque reboot du switch
- la table MAC a une taille finie. Par exemple, sur un Cisco 2950, c'est 8000 entrées.
- ce fonctionnement d'apprentissage des adresses MAC est vulnérable à certaines attaques comme par exemple la saturation de table MAC.

Attaques Ethernet: inondation de la table CAM

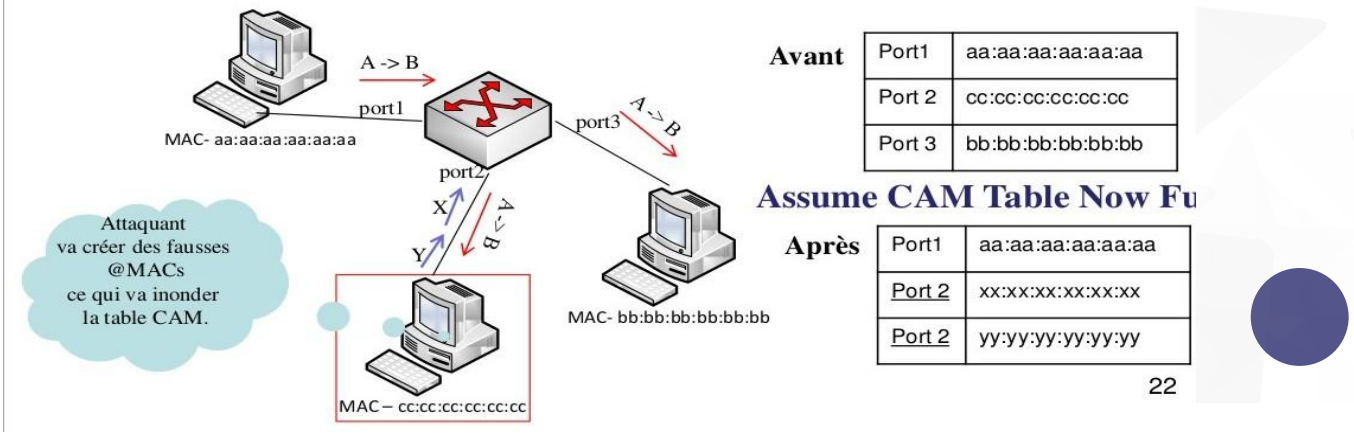
Vulnérabilités:

Lorsque la table est pleine, des entrées existantes sont enlevées.

Lorsqu'une adresse MAC ne se retrouve pas dans la table CAM, le commutateur diffuse la trame sur tous les ports.

Attaque: L'attaquant inonde le commutateur avec de fausses trames ==> **le commutateur se transforme en HUB**

Risque: Divulgation d'informations sensibles (p.ex. mots de passe) qui ne devraient pas être envoyées sur un port



Attaques Ethernet: inondation de la table CAM

Parades

- Limiter le nombre d'@ MAC permises sur un port donné.
- Limiter la durée qu'une @ MAC reste assignée à un port:
  - Une fois pleine de fausses entrées, la table se videra d'elle-même.
- Assigner des @ MACs statiques à des ports.
  - Ces @ ne seraient jamais enlevées si la table devenait pleine.
  - Les @ des serveurs ou des équipements importants sont ainsi configurées dans le commutateur.
- Authentification 802.1X
  - L'accès à un port n'est permis qu'après une authentification.

Domaines de collision

- Le domaine de collision est le segment sur lequel les périphériques sont en concurrence les uns avec les autres pour communiquer
- Tous les ports d'un concentrateur appartiennent au même domaine de collision
- Chaque port d'un commutateur constitue un domaine de collision
- Le commutateur décompose le segment en domaines de collision plus petits.

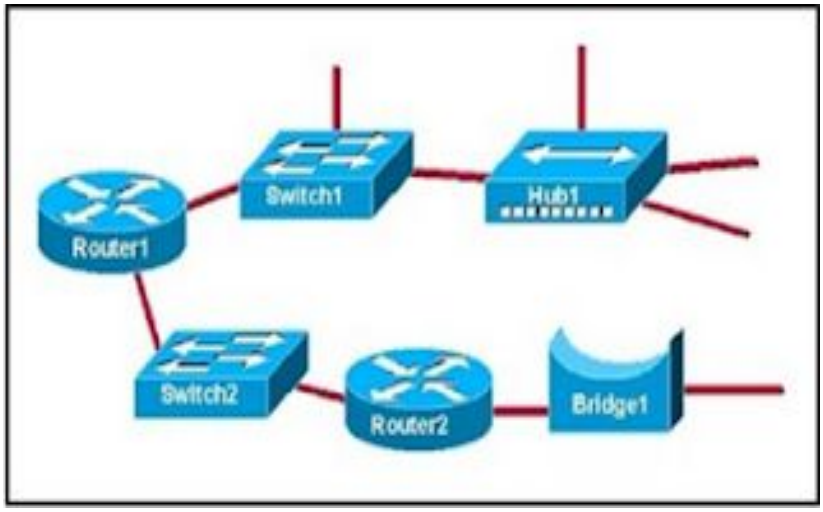
Domaines de diffusion

- Le domaine de diffusion représente l'étendue du réseau dans laquelle une trame de diffusion peut être « entendue ».
- Les commutateurs envoient les trames de diffusion à tous les ports. C'est pourquoi ils ne segmentent pas les domaines de diffusion.
- Tous les ports d'un commutateur (avec la configuration par défaut) appartiennent au même domaine de diffusion
- Si deux commutateurs ou plus sont connectés, les diffusions sont envoyées vers tous les ports de tous les commutateurs (à l'exception de celui qui les a initialement reçues)

Réduction de l'encombrement du réseau

- Les commutateurs contribuent à réduire l'encombrement du réseau :
  - Ils facilitent la segmentation d'un LAN en domaines de collision séparés
  - Ils assurent une communication bidirectionnelle simultanée entre les périphériques
- Ils tirent profit de leur densité de ports la plus élevée
- Ils utilisent les ports haut débit
- Ils exploitent leur méthode rapide de commutation interne
- Ils représentent un faible coût par port

- **Combien de domaines de broadcast y a-t-il dans le schéma ?**



- **Combien de domaines de collision y a-t-il dans le schéma ?**