

Réseaux locaux

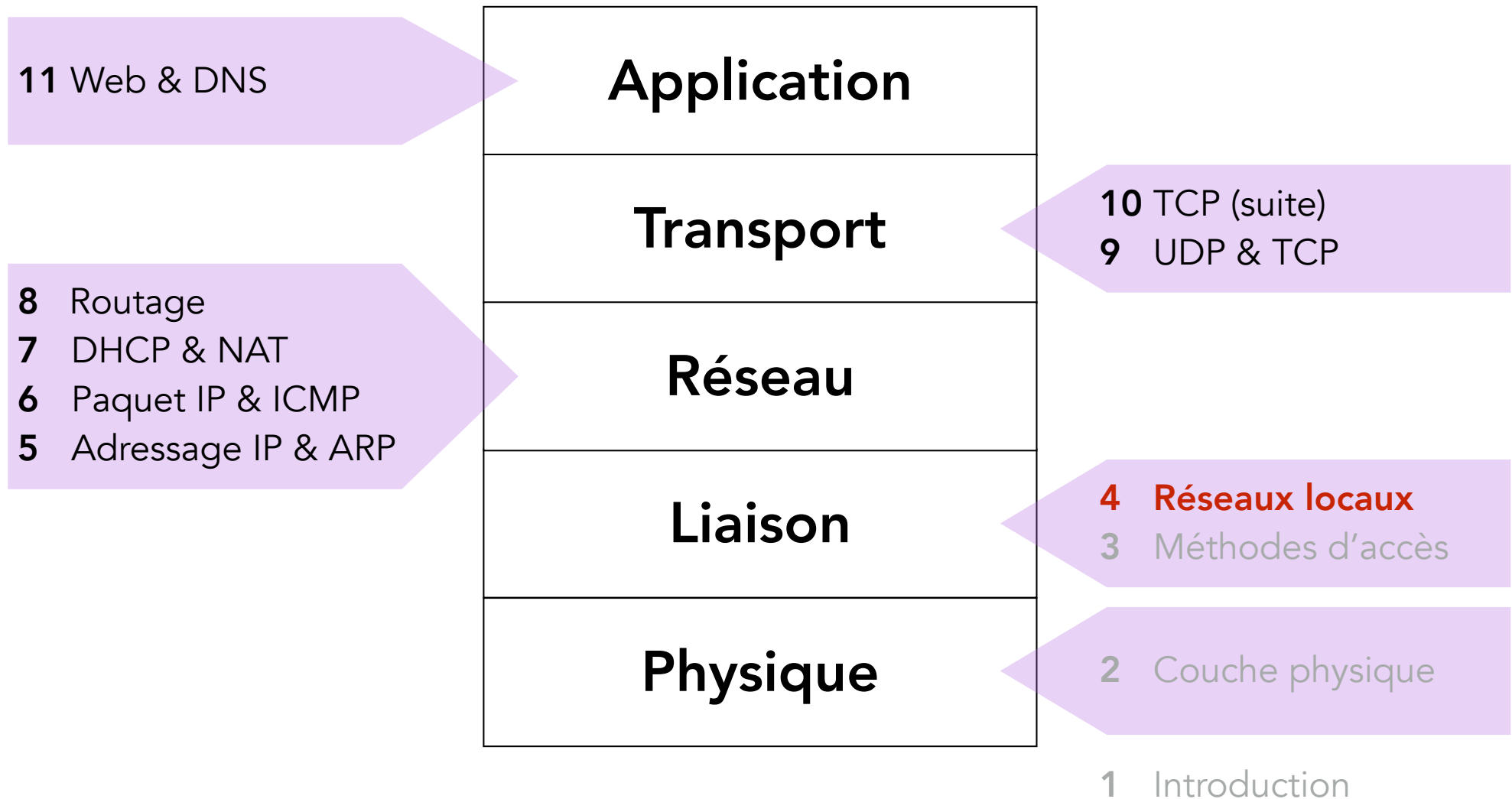
UE LU3IN033 Réseaux
2023-2024

Bruno Baynat

Bruno.Baynat@sorbonne-universite.fr



Programme de l'UE LU3IN033



Plan du cours

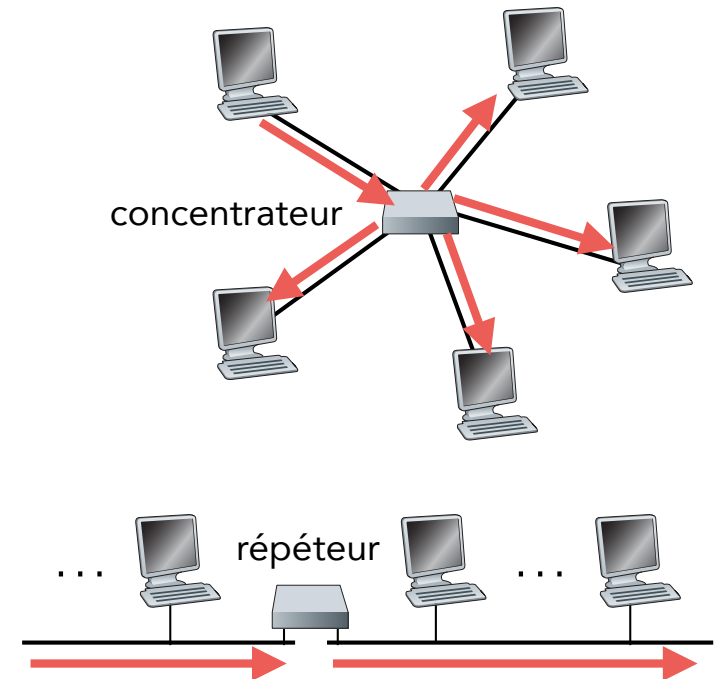
- Domaine de collision vs domaine de diffusion
- Concentrateurs vs commutateurs
- Techniques et protocoles propres aux commutateurs
 - Auto-apprentissage
 - STP (construction d'un arbre couvrant)
 - Cut-through switching
 - VLAN
- VLAN

LAN

- Un **LAN** (*Local Area Network*) est un **réseau local** constitué d'un ensemble d'ordinateurs (et de périphériques) connectés au moyen de liaisons physiques (filaires ou sans fil) et utilisant des protocoles de communication communs
- 3 types d'équipements permettent d'interconnecter des stations dans les LANs
 - Les **concentrateurs** (*hubs*)
 - agissent au niveau de la couche physique (1)
 - Les **commutateurs** (*switches*)
 - agissent au niveau de la couche liaison (2)
 - Les **routeurs** (*routers*)
 - agissent au niveau de la couche réseau (3)

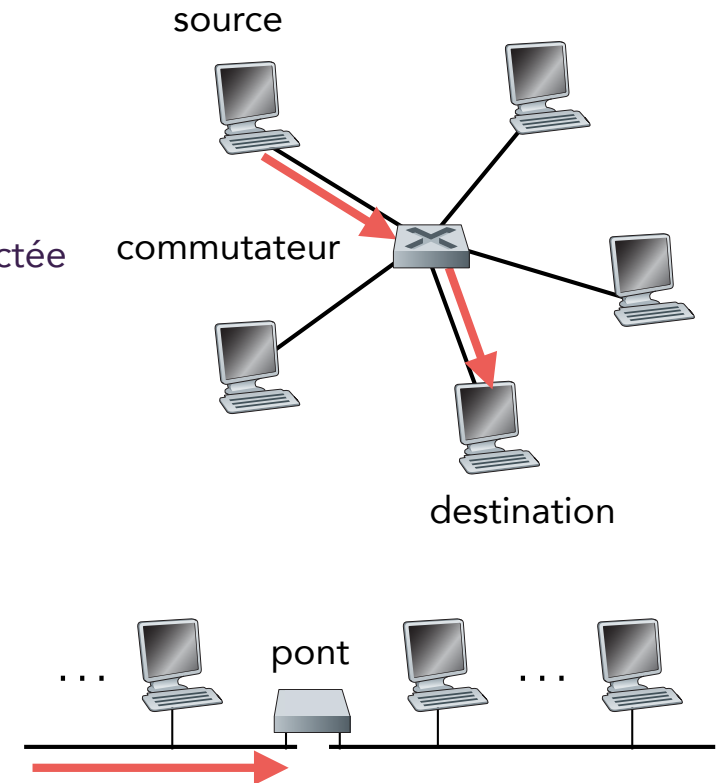
Concentrateurs

- Les **concentrateurs** (*hubs*)
 - agissent au niveau de la couche physique (1)
 - lorsqu'une trame est reçue sur un des ports, elle est recopiée sur tous les autres ports
- Les **répéteurs** (*repeaters*)
 - concentrateurs à 2 ports permettant de relier 2 segments internet (bus)
- Concentrateurs et répéteurs étendent le domaine de collision
- Inconvénients
 - Facteur d'échelle
 - augmentation du nombre de stations connectées et de la portée du réseau
 - la bande passante est partagée par toutes les stations
 - Délai et retard
 - les collisions augmentent avec le nombre de stations
 - les collisions successives retardent les transmissions (*exponential backoff*)
 - Pannes
 - une station défectueuse peut affecter tout le réseau



Commutateurs

- Les **commutateurs** (*switches*)
 - agissent au niveau de la couche liaison (2)
 - lorsqu'une trame est reçue sur un des ports, le commutateur la renvoie uniquement sur le port sur lequel la destination est connectée
 - phase d'apprentissage nécessaire
- Fonctionnalités
 - **CSMA/CD**
 - **auto-apprentissage**
 - **arbre couvrant STP** (*Spanning Tree Protocol*)
 - **store & forward** ou **cut-through switching**
- Transparents
 - les stations n'ont pas connaissance de leur existence
- Plug and play
 - ne nécessitent aucune configuration
- Les **ponts** (*bridges*) connectent des bus
 - Commutateur à 2 ports permettant de relier 2 segments internet (bus)



Domaine de collision vs diffusion

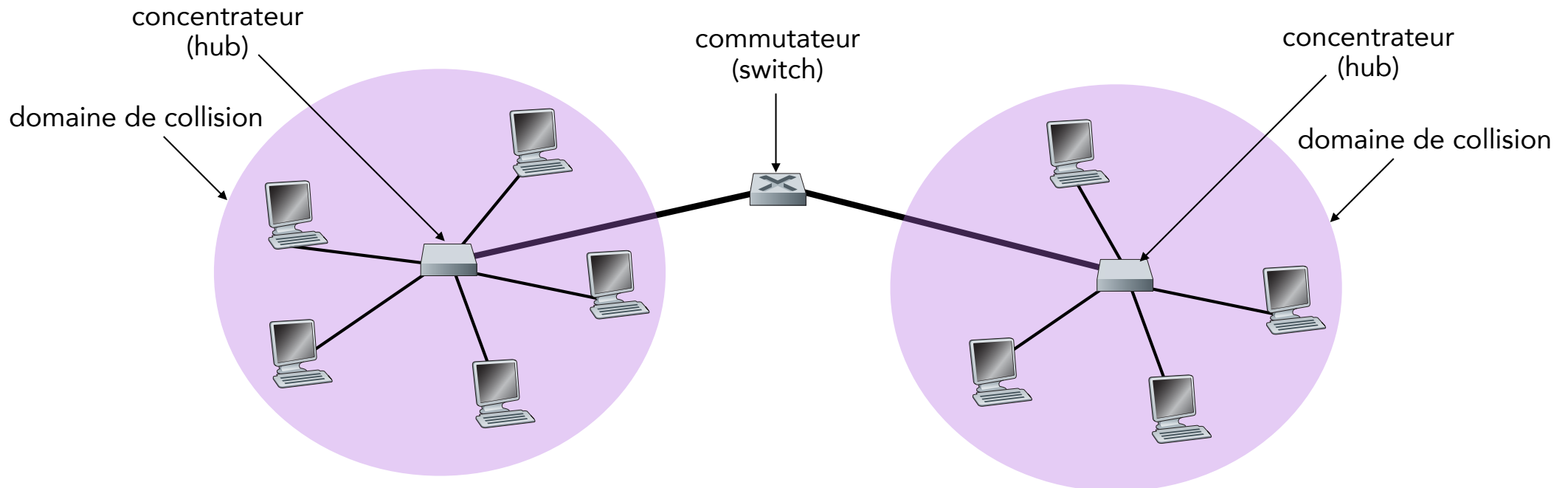
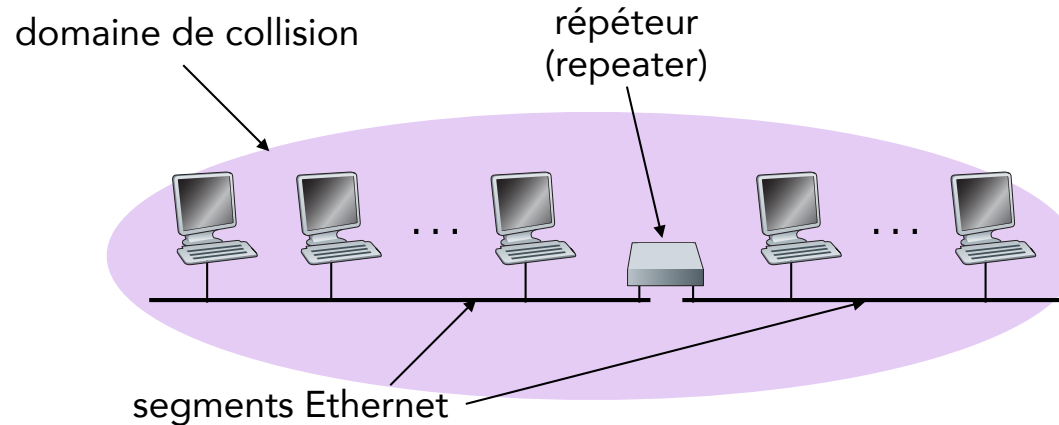
- Domaine de collision

- Zone logique au sein de laquelle des transmissions simultanées se télescopent : collisions
 - Bus : segments Ethernet interconnectés par des **répéteurs** (*repeaters*)
 - Etoile : stations connectées par des **concentrateurs** (*hubs*)
- Les **commutateurs** (*switches*) et les routeurs (*routers*) divisent un réseau en plusieurs domaines de collision

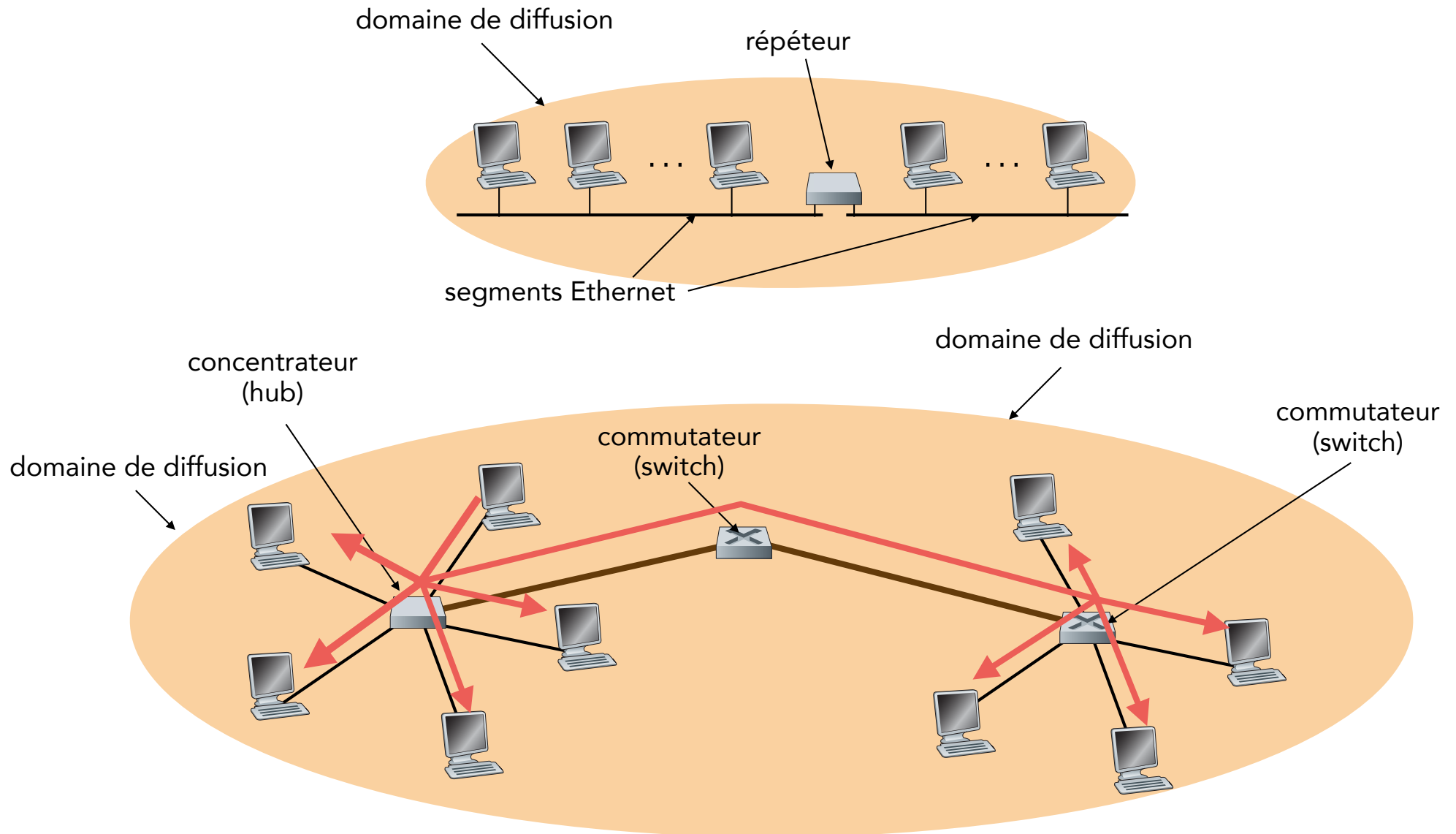
- Domaine de diffusion

- Zone logique au sein de laquelle une même trame peut être diffusée (« broadcastée ») à toutes les stations de la zone
 - Les **routeurs** divisent un réseau en plusieurs domaines de diffusion
 - Les **VLANs** font de même

Domaine de collision



Domaine de diffusion



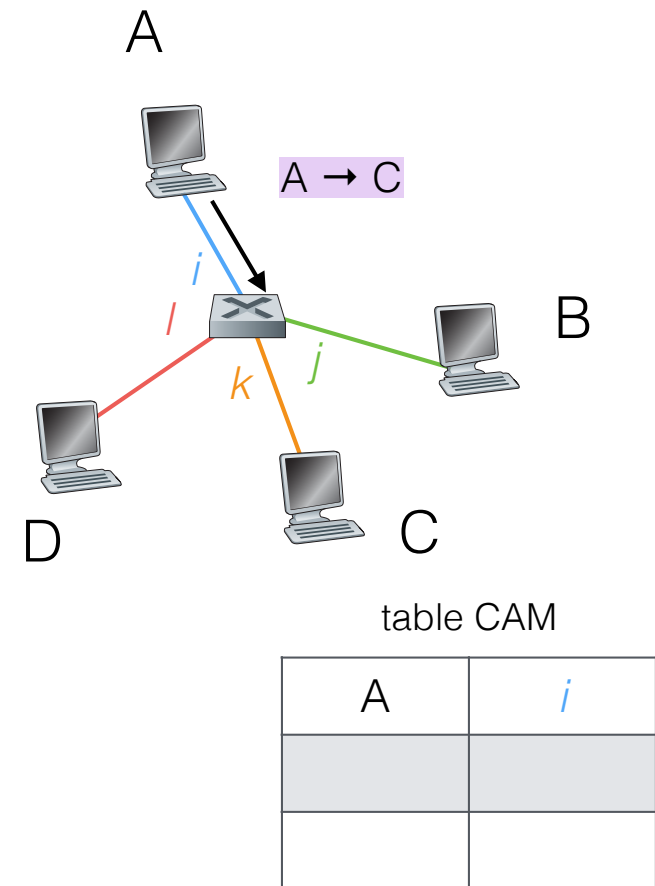
Commutateurs



Auto-apprentissage

Peuplement de la table CAM

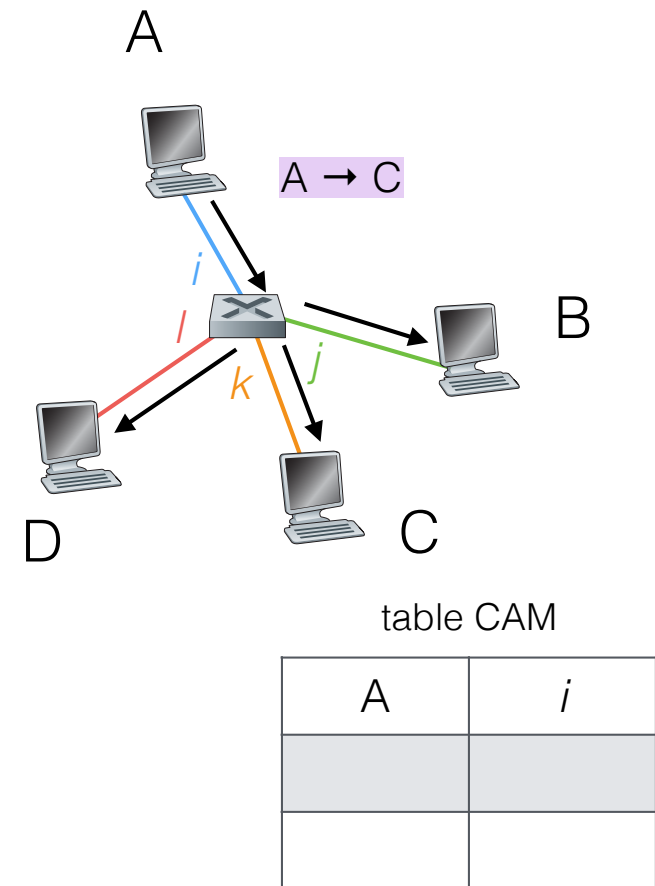
- Lorsqu'une trame arrive sur le port d'entrée d'un commutateur
 - inspecter l'adresse MAC source
 - associer cette adresse au port d'entrée de la trame
 - créer une entrée dans la **table CAM** (Content Addressable Memory) ou **table MAC**
 - associer un TTL (*aging time*) à cette entrée permettant
 - de maintenir la taille de la table CAM petite
 - de prendre en compte
 - les changements de topologie
 - les stations qui bougent ou qui deviennent inactives



Auto-apprentissage

Destinations inconnues

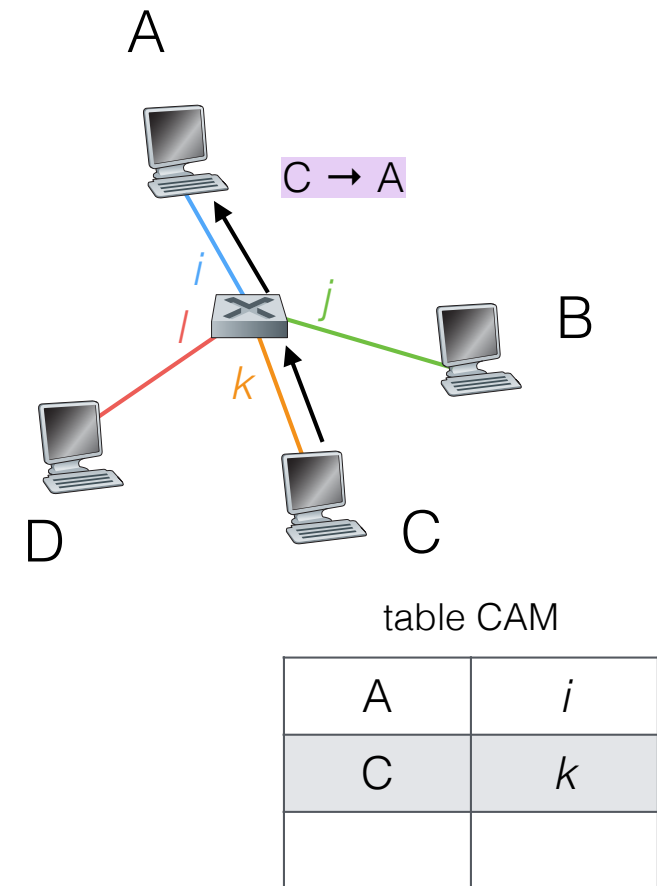
- Si la destination n'est pas connue (n'est pas présente dans sa table CAM)
 - envoyer la trame sur tous les ports à l'exception du port d'entrée : **inondation**



Auto-apprentissage

Destination connue

- Si la destination est connue (est présente dans sa table CAM)
 - envoyer la trame uniquement sur le port indiqué pour cette destination par la table CAM (si différent du port d'entrée)



Peuplement des tables CAM

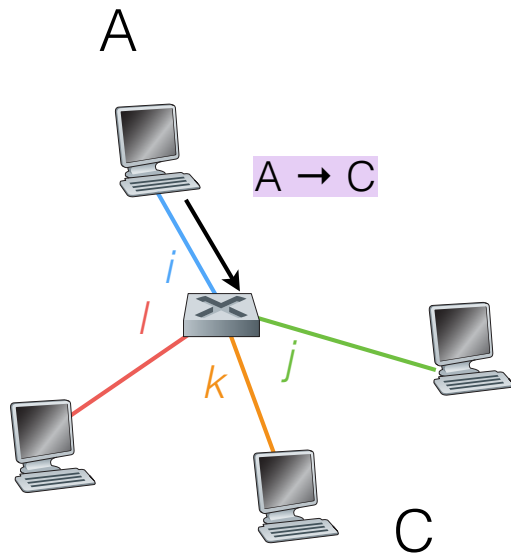


table CAM

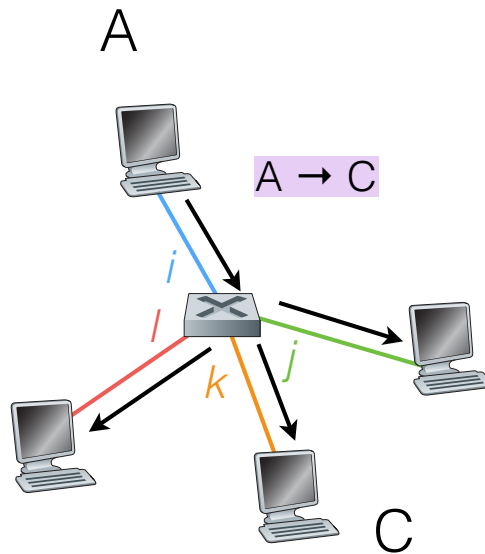


table CAM

A	<i>i</i>

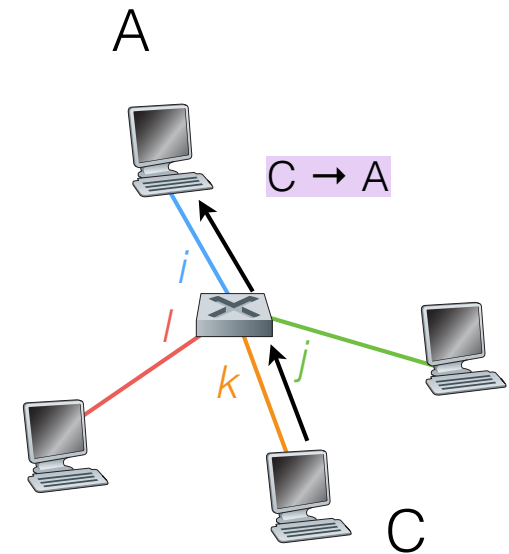


table CAM

A	<i>i</i>
C	<i>k</i>

Algorithme

Acheminement/Filtrage

- Sur réception d'une trame

chercher l'adresse destination dans la table CAM

si une entrée est trouvée alors

si le port indiqué par l'entrée est identique au port d'entrée de la trame alors

supprimer la trame

sinon

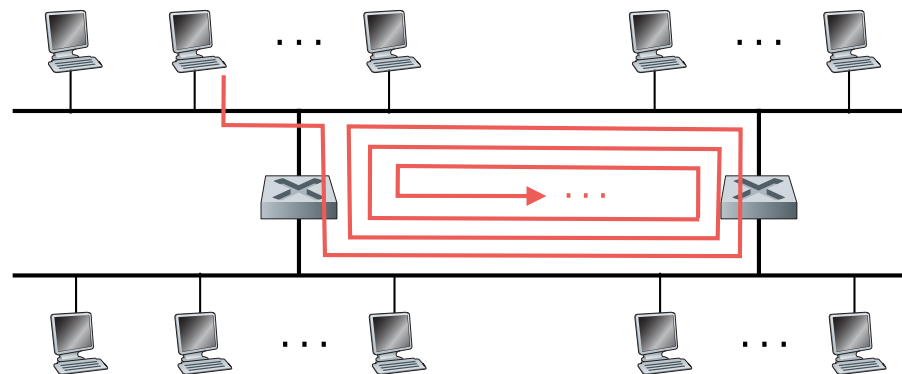
envoyer la trame sur le port indiqué par l'entrée de la table CAM

sinon

inonder

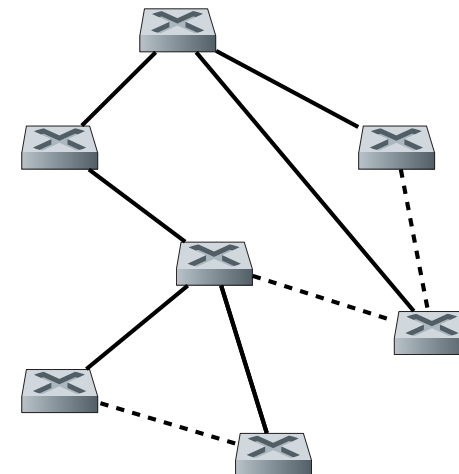
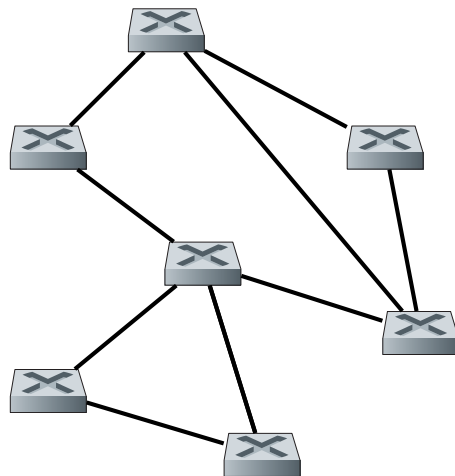
Inondation et boucles

- Les commutateurs ont parfois besoin d'inonder
 - les trames à destination d'adresses inconnues (non présentes dans la table CAM)
 - les trames à destination de l'adresse de **broadcast** (FF:FF:FF:FF:FF:FF)
- L'inondation des trames peut entraîner des **tempêtes de broadcasts**
 - le réseau peut contenir des boucles
 - involontaires : erreurs de câblage
 - volontaires : redondance pour résister aux pannes
 - l'entête des trames Ethernet ne contient pas de champ TTL



Arbre couvrant

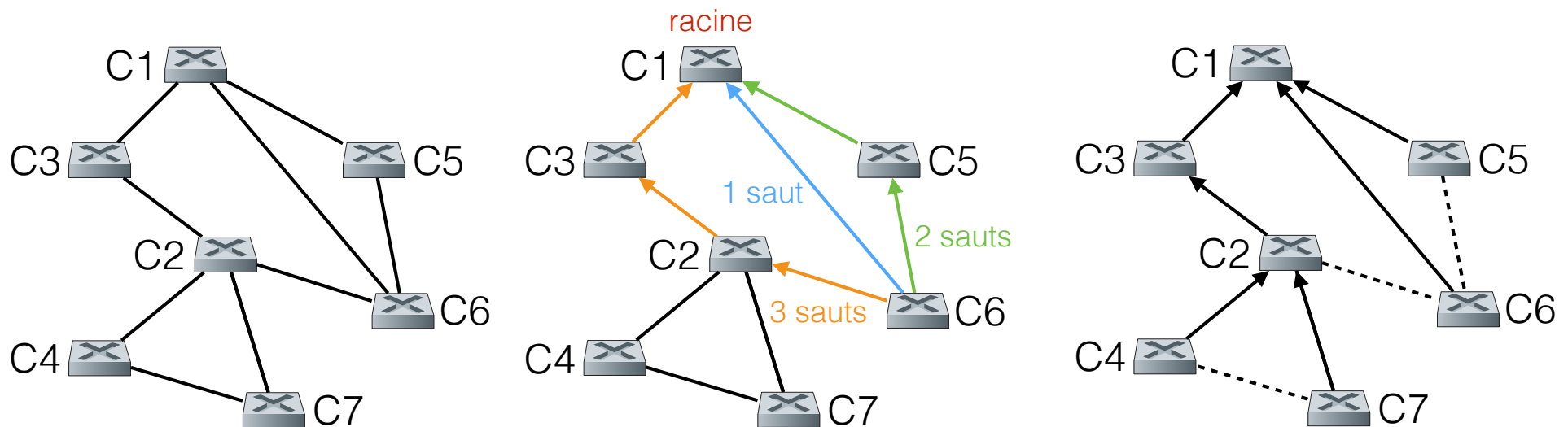
- Objectif : interdire les boucles d'acheminement
 - en évitant certains liens
 - sans rendre aucune destination inaccessible
- Solution : construire sur la topologie du réseau un **arbre couvrant**
 - en choisissant certains liens et en désactivant les autres
 - afin d'avoir un chemin unique entre toute paire de noeuds



Construction de l'arbre couvrant

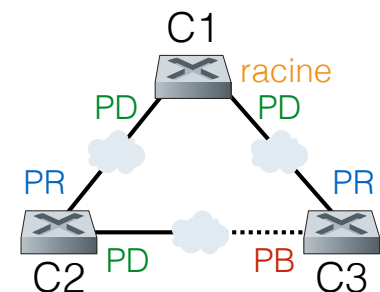
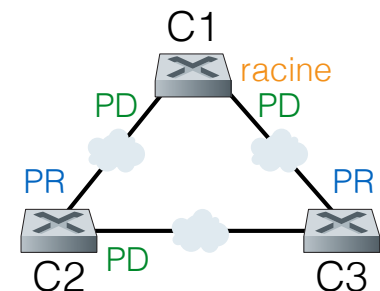
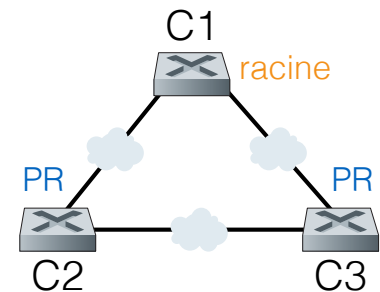
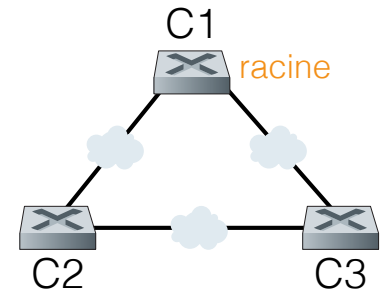
- Choix d'une racine
 - basé sur les identifiants des commutateurs
- Identification des liens actifs
 - chaque commutateur identifie le lien auquel il est connecté qui lui permet de joindre la racine le long du « plus court chemin »
- Désactivation des autres liens
 - les liens qui n'ont pas été choisis sont désactivés

débit	coût
10 Mbit/s	100
100 Mbit/s	19
1 Gbit/s	4
10 Gbit/s	2
100 Gbit/s	1



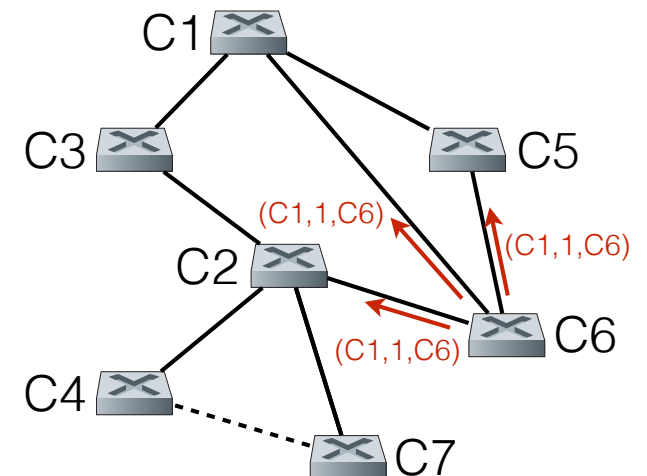
Etapes du protocole STP

- *Spanning Tree Protocol*
- 4 étapes
 - Election du commutateur racine
 - commutateur ayant le plus petit identifiant
 - identifiant = adresse mac (unique) + priorité (réglable)
 - Détermination des ports racines
 - chaque commutateur identifie le port « racine » qui lui permet de joindre la racine le long du plus court chemin
 - en cas d'égalité choisir le chemin passant par le voisin ayant le plus petit identifiant
 - Détermination des ports désignés
 - pour chaque segment reliant plusieurs commutateurs, le port « désigné » est celui qui le mène à la racine le long du plus court chemin
 - Blocage des autres ports
 - tous les ports qui ne sont ni racines ni désignés sont bloqués
 - aucun message de données ne sera retransmis sur un port bloqué



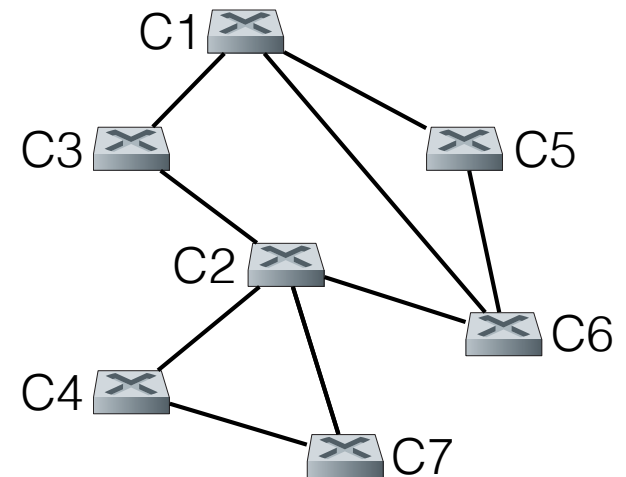
Algorithme STP

- Les commutateurs s'échangent périodiquement des messages BPDU (*Bridge Protocol Data Unit*)
 - encapsulés dans des trames IEEE 802.3
 - envoyées à l'adresse MAC multicast 01:80:C2:00:00:00
 - 3 types
 - BPDU de configuration (CBPDU)
 - BPDU de notification de changement de topologie (TCN)
 - BPDU d'acquittement de changement de topologie (TCA)
- Message CBPDU : X envoie (Y, d, X)
 - sur tous ses ports (y compris ceux désactivés)
 - X pense que Y est la racine
 - et que d est la distance qui le sépare de Y
- Les ports d'un commutateur qui s'allume passent par 3 phases
 - Listening (15 secondes par défaut)
 - Learning (15 secondes par défaut)
 - Forwarding / Blocking



Exemple

- Les commutateurs C4 et C7 s'allument et considèrent tous les deux être la racine
 - C7 envoie (C7, 0, C7) sur tous ses ports
 - C4 envoie (C4, 0, C4) sur tous ses ports
- C7 reçoit le message (C4, 0, C4) de C4
 - commence à considérer C4 comme étant la racine (car $\text{id } C4 < \text{id } C7$)
 - calcule la distance du chemin vers C4 : $d = 1$
 - marque son port vers C4 comme port racine
 - C7 envoie (C4, 1, C7) sur tous ses ports
- C7 reçoit le message (C1, 2, C2) de C2
 - considère C1 comme la racine
 - calcule la distance du chemin vers C1 : $d = 3$
 - marque son port vers C2 comme port racine



Algorithme STP

- L'algorithme doit réagir aux pannes ou aux changement de configuration
 - panne du commutateur racine
 - élection d'une nouvelle racine
 - panne des autres commutateurs ou des liens, ou changement de configuration
 - recalcul de l'arbre couvrant
- Les commutateurs envoient périodiquement leurs messages BPDU
 - la racine continue à s'annoncer comme étant la racine
 - les autres commutateurs continuent
 - à calculer la distance qui les séparent de la racine
 - à envoyer leurs messages BPDU (toutes les 2 secondes par défaut)
- Détection des pannes sur expiration de TTL
 - l'état des ports d'un commutateur est associé à une durée « *max age* » (20 secondes par défaut)
 - l'absence de réception de messages BPDU pendant cette durée provoque le recalcul de l'arbre couvrant

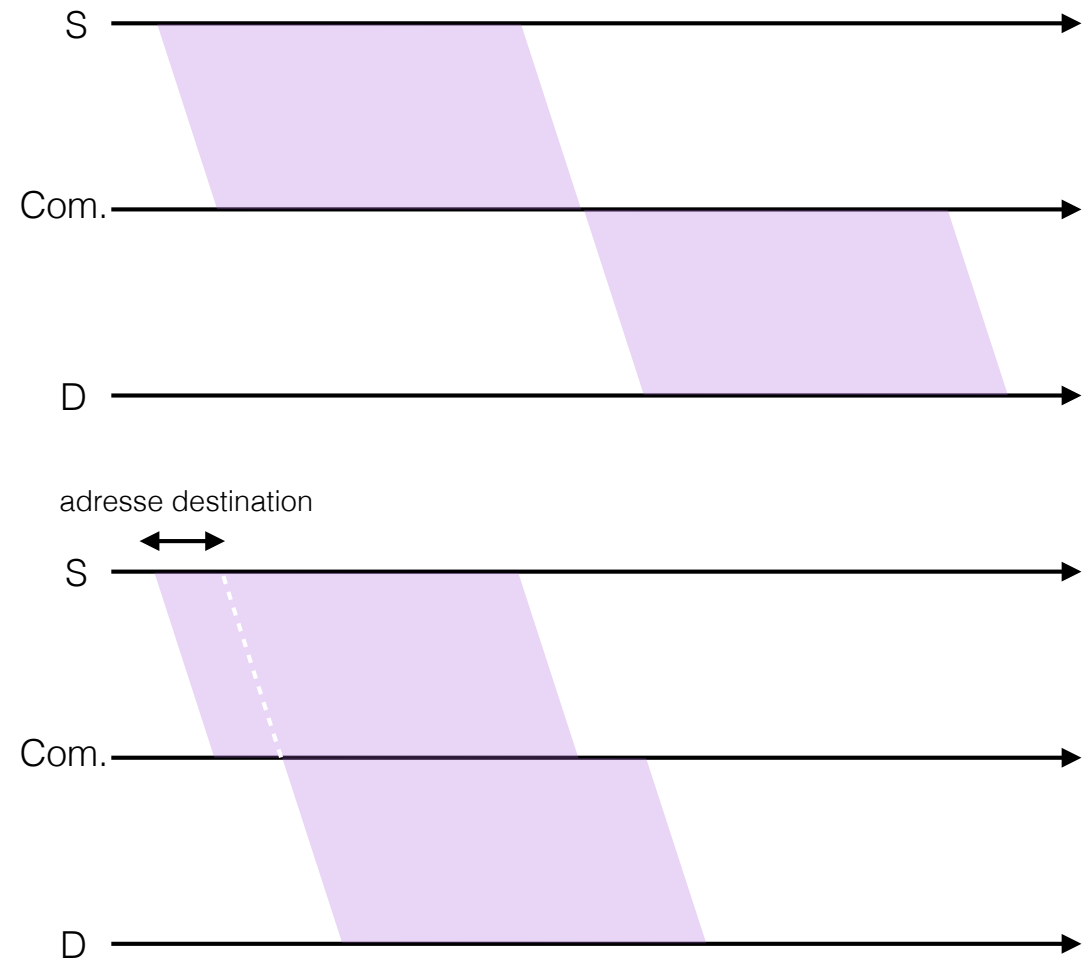
Store & Forward vs Cut-Through

- *Store & forward switching*

- retransmission lorsque la trame est intégralement reçue et vérifiée
- coûteux en termes de temps et de mémoire

- *Cut-through switching*

- retransmission de la trame aussitôt que possible
 - inspecter la table CAM dès que l'adresse destination est reçue
 - retransmettre la trame sur le port de sortie (si le support est libre) sans attendre de l'avoir entièrement reçue
- inconvénient : propagation des erreurs



Commutateurs vs Concentrateurs

Avantages

- Plug-and-play
 - configuration automatique
- Réduction du nombre de collisions
 - augmentation de la portée du réseau
- Filtrage du trafic
 - réduction du trafic inutile
 - préservation de la bande passante
 - meilleure confidentialité
- Elimination des boucles d'acheminement
 - évite les surcharges liées à des trames qui bouclent indéfiniment

Inconvénients

- CSMA/CD
 - mémoires pour stocker les trames
 - solution : liens full duplex
- *Store & forward switching*
 - retard dans le traitement des trames
 - solution : *cut-through switching*
- Construction des tables CAM
 - taille des tables
 - solution : TTL pour limiter leur taille
- Délai de convergence de l'algorithme STP
 - plusieurs dizaines de secondes
 - solution : Rapid STP (RSTP)

VLAN



VLAN : LAN Virtuels

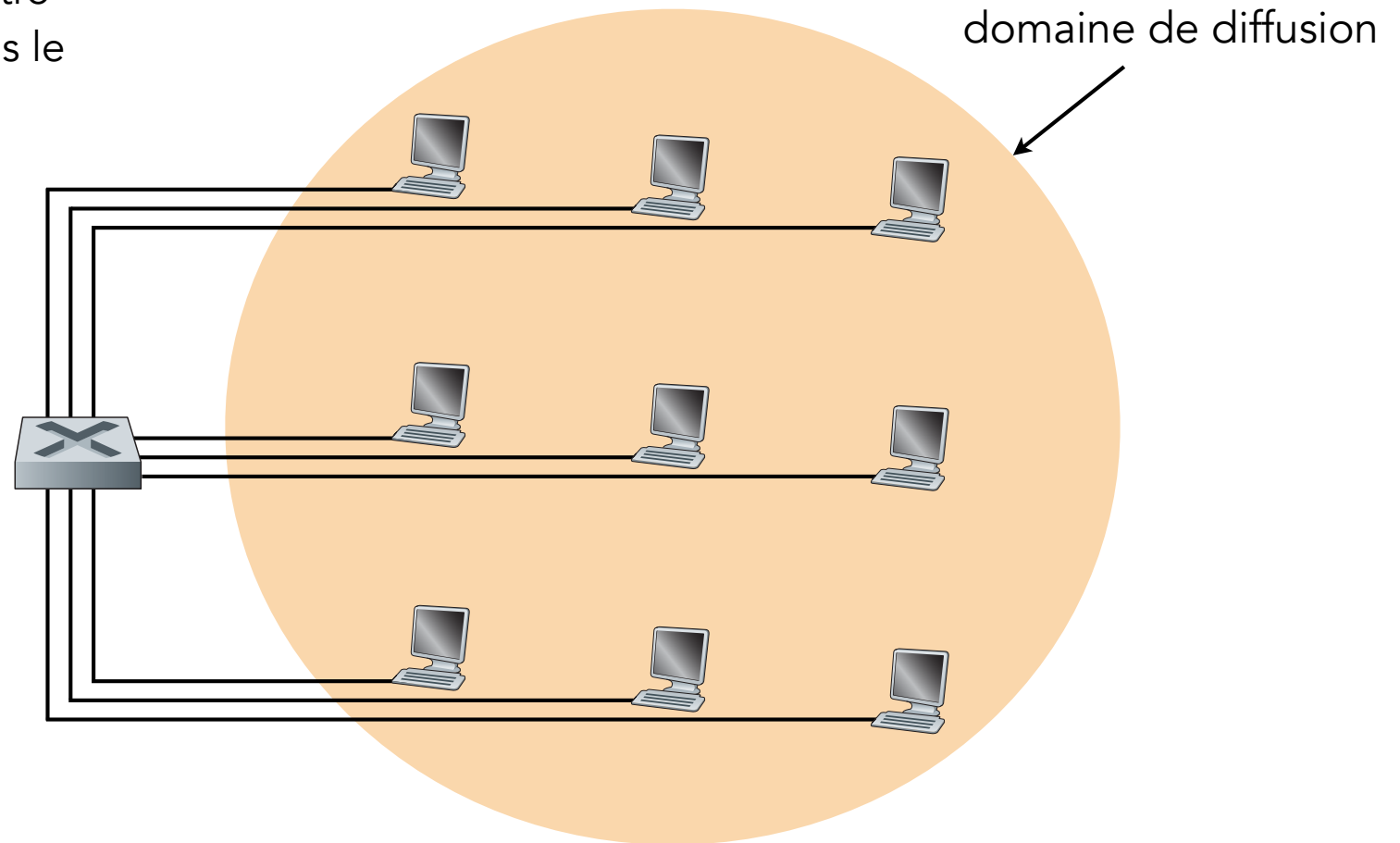
- Les commutateurs Ethernet
 - divisent le réseau en plusieurs sous-domaines de collision
 - étendent le réseau en un seul domaine de diffusion
 - une trame inondée est reçue de tous
- Charge
 - Les trames inondées circulent dans tout le réseau et en augmentent la charge
 - Isoler les trafics permet de préserver la bande passante
- Sécurité
 - Les stations du réseau local appartiennent toutes au même domaine de diffusion
 - elles voient toutes passer tout le trafic
 - Isoler les trafics permet d'améliorer la confidentialité
- Les VLANs permettent de découper le réseau en plusieurs sous-domaines de diffusion (un par VLAN)
 - Isoler les trafics au sein de chaque sous-domaine de diffusion

Réorganisation logique du réseau

- Découpage du réseau en sous-domaines de diffusion
 - limiter la portée des trames inondées
 - préservation de la bande passante
 - sécurisation par isolement des trafics
 - réduire la taille des tables CAM
 - limiter la complexité du STP
- Réorganisation logique des stations (utilisateurs)
 - en tenant compte des relations organisationnelles / fonctionnelles des utilisateurs au sein de l'entreprise
 - regroupement des stations selon leur appartenance au même service / département
 - indépendamment de leur position physique
 - sans recâblage

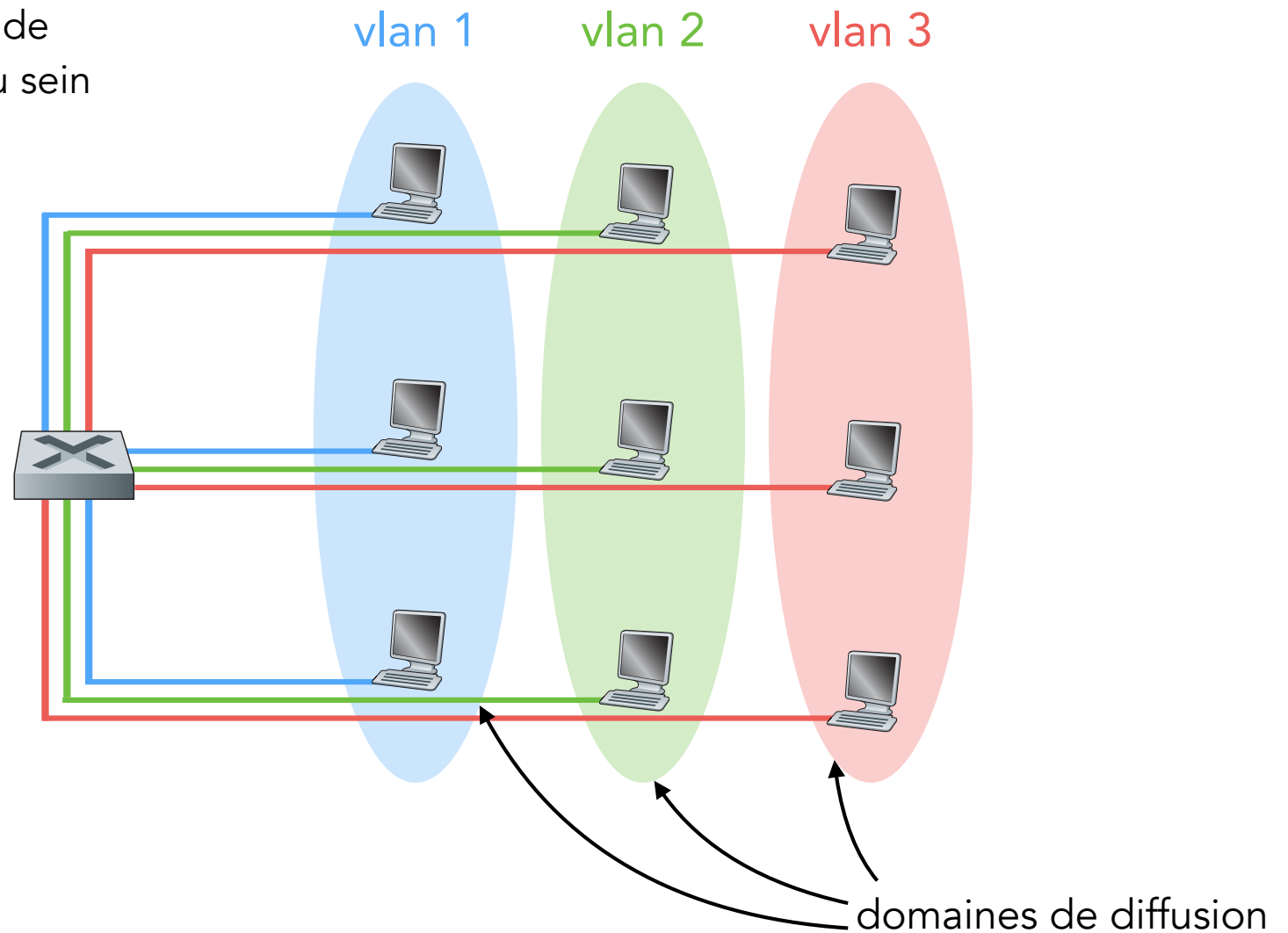
Domaine de diffusion

Les trames peuvent être inondées partout dans le réseau



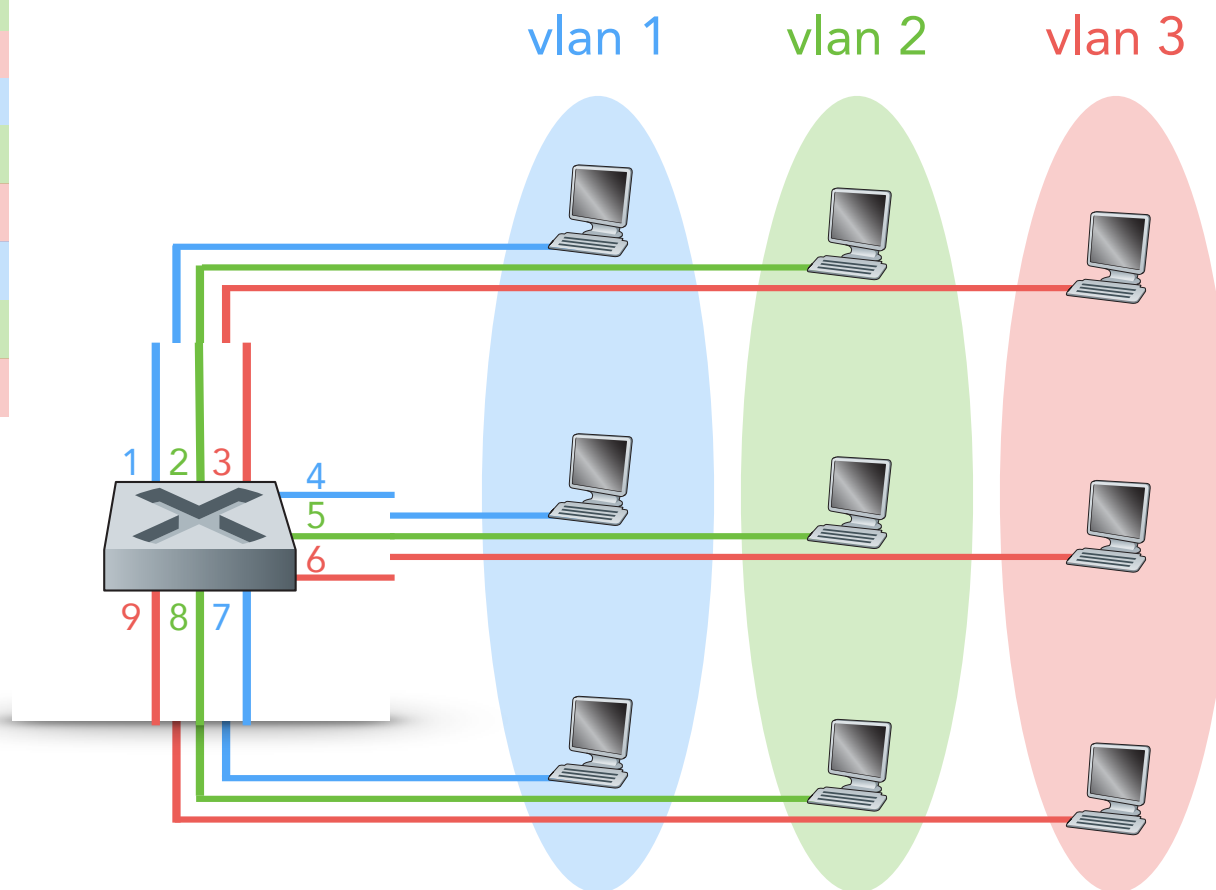
Virtual LANs

Les trames y compris de broadcast circulent au sein d'un seul VLAN



Virtual LANs

Port	VLAN
1	1
2	2
3	3
4	1
5	2
6	3
7	1
8	2
9	3



Les trames reçues sur le port 1 sont transmises uniquement sur les ports 4 et 7

Appartenance aux VLANS

- Les commutateurs sont configurés avec une table de VLAN
 - indiquant à quel VLAN appartient une trame
- Appartenance des trames aux VLAN
 - Statique
 - définie par le port du commutateur
 - Dynamique
 - définie par l'adresse MAC source des trames
 - définie par le champ Type des trames
 - définie par l'adresse IP source du paquet encapsulé
 - définie par l'application véhiculée dans le paquet encapsulé

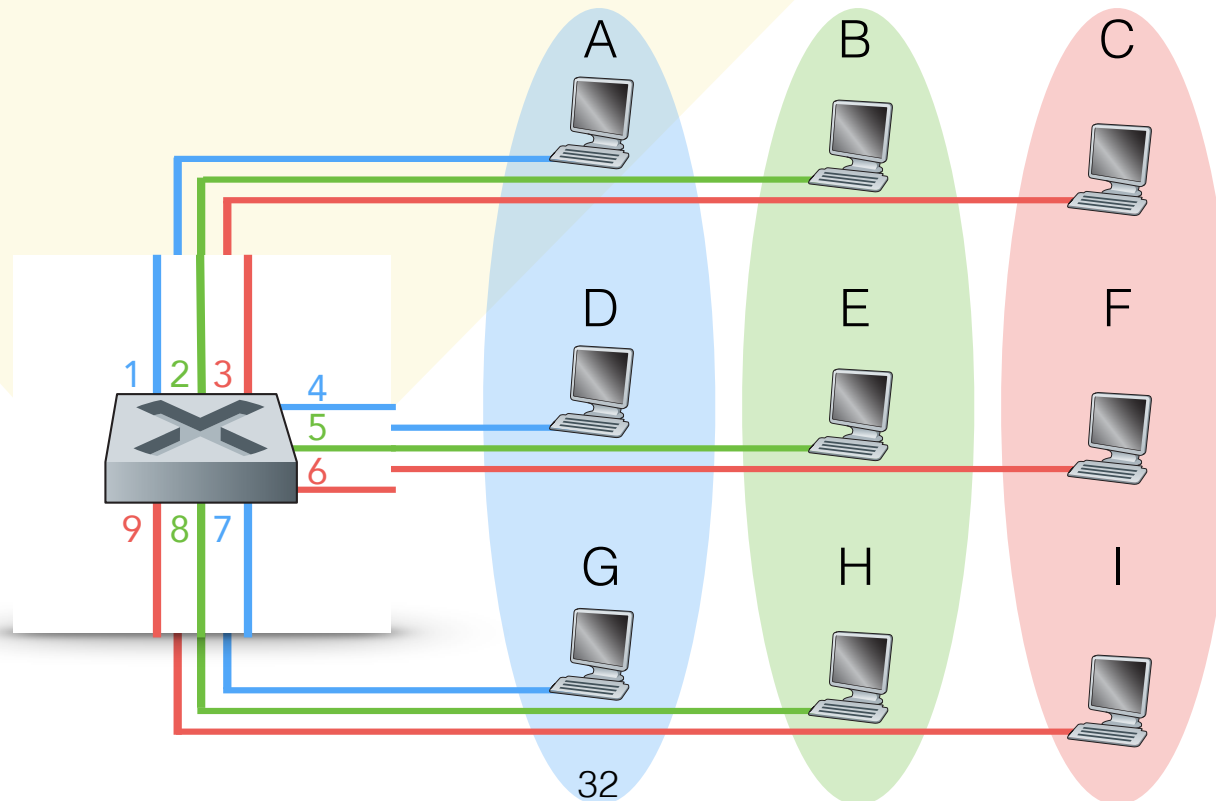
table statique construite
manuellement par l'administrateur

VLAN 1	VLAN 2	VLAN 3
MAC A	MAC B	MAC C
MAC D	MAC E	MAC F
MAC G	MAC H	MAC I

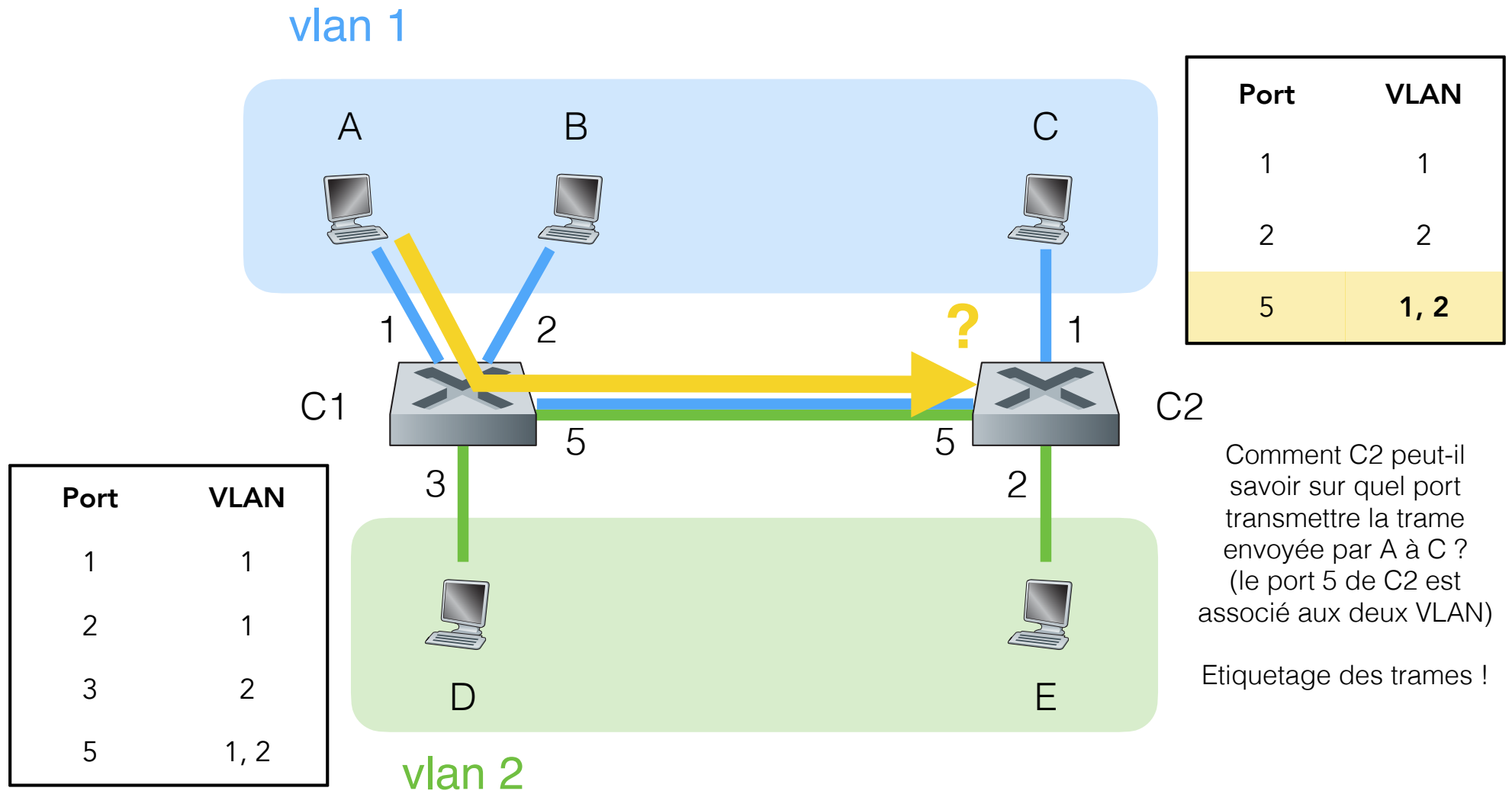
table dynamique construite
par le commutateur

Port	VLAN
1	1
2	2
3	3
4	1
5	2
6	3
7	1
8	2
9	3

L'association des ports
aux VLAN se fait sur
réception des
premières trames



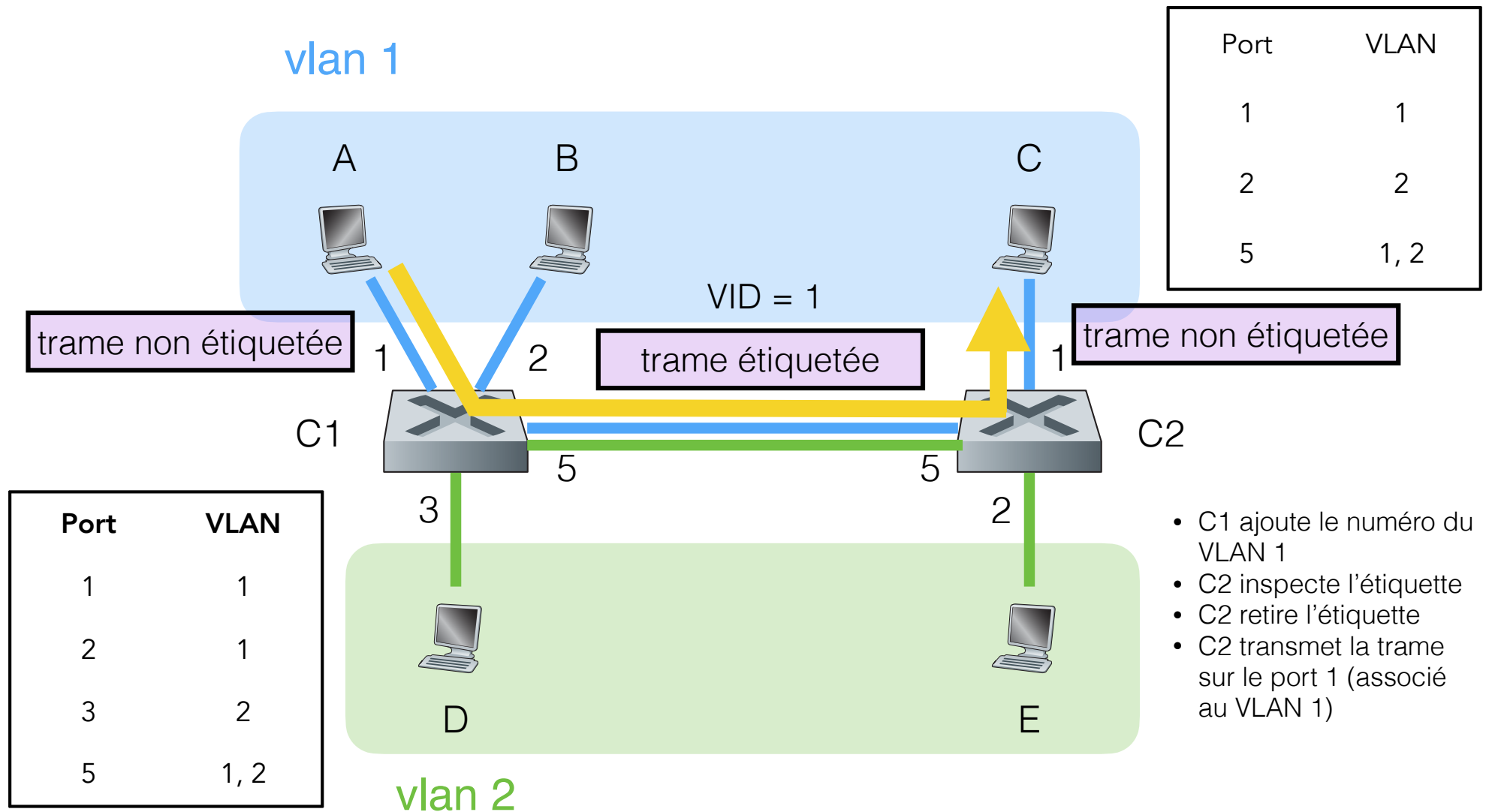
Interconnexion de commutateurs



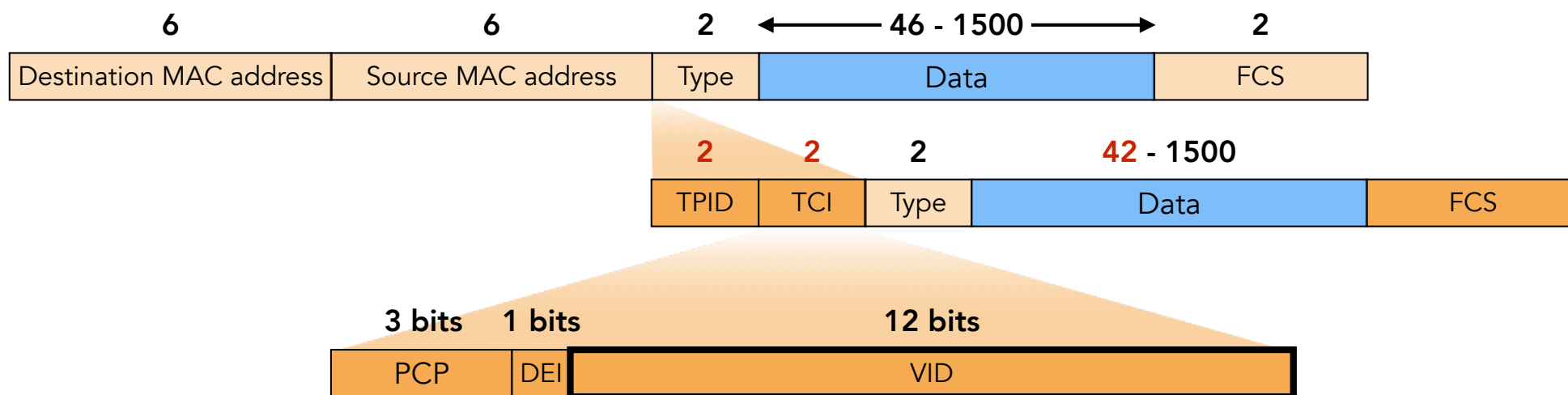
Transfert des trames entre deux commutateurs

- Ajouter deux liaisons physiques entre les deux commutateurs
 - une liaison par VLAN
 - coûteux
- Ajouter l'association (Adresse MAC, VLAN) dans les commutateurs
 - chaque commutateur doit gérer des 2 types de tables de VLAN
 - configuration laborieuse et fastidieuse
- Ajouter le numéro de VLAN dans l'entête des trames
 - 802.3Q : format des trames VLAN-"étiquetées" (tagged)

Interconnexion de commutateurs



Trames 802.1Q



- Tag protocol identifier (TPID)
 - 0x8100 pour les trames IEEE 802.1Q
- Tag control information (TCO)
 - Priority code point (PCP)
 - IEEE 802.1p class of service
 - Drop eligible indicator (DEI)
 - indiquent des trames qu'il est possible de supprimer en cas de congestion
 - VLAN identifier (VID)
 - indique le numéro de VLAN auquel la trame appartient

Conclusions

- Interconnecter des segments Ethernet
 - Concentrateurs (*hubs*) / Répéteurs (*repeaters*)
 - Commutateurs (*switches*) / Ponts (*bridges*)
- Domaine de collision vs domaine de diffusion
 - Commutateurs et Ponts limitent le domaine de collision...
 - ... mais étendent le domaine de diffusion
- Concepts propres aux commutateurs
 - Auto-apprentissage (table CAM)
 - Arbres couvrants (protocole STP)
 - *Cut-through switching*
 - LANs virtuels (VLANs)
- Les VLANs découpent logiquement le réseau en sous-domaines de diffusion

A faire

- Cours 4
 - à relire attentivement
- Devoir 4 sur Moodle
 - date de rendu : dimanche 1er octobre