TELECOM Paris

IP PARIS

RES 101

Technologies des réseaux

- Réseaux câbles
- Réseaux sans fils

Agenda

- Couche physique
- Couche liaison de données
- Ethernet: IEEE 802.3
- WiFi: IEEE 802.11

The Ethernet standard

- L'évolution des standards Ethernet et les premières versions :

⇒1975 : Projet de recherche des laboratoires Xerox Parc. « Ethernet expérimental » à 2.94 Mbps sur câble coaxial.

⇒1980 : Ethernet Version I, proposé par DEC et INTEL à 10 Mbps.

⇒1982 : DEC, INTEL et Xerox (DIX) proposent Ethernet version II

⇒1984 : Standards 802.2+802.3 proposés par l'IEEE (compatible avec DIX v2) : thick Ethernet 10 Base 5 (10Mbps)

⇒1985 : 802.3a (thin Ethernet 10 Base 2)

⇒1990 : 802.3i (10 Base T)

⇒1993 : 10 Base F

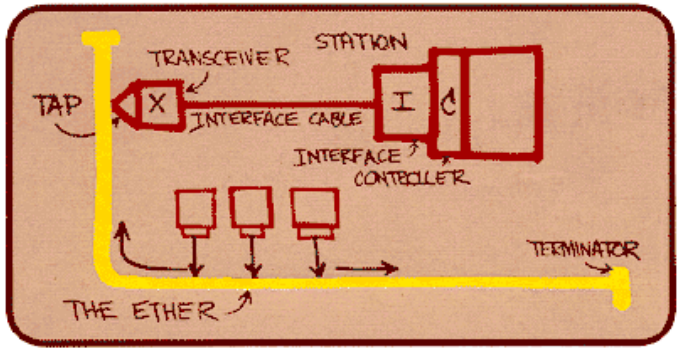
⇒1995 : Fast Ethernet 100 Mbps

⇒1997 : Mode Full duplex

⇒1998 : Gigabit Ethernet 1 Gbps

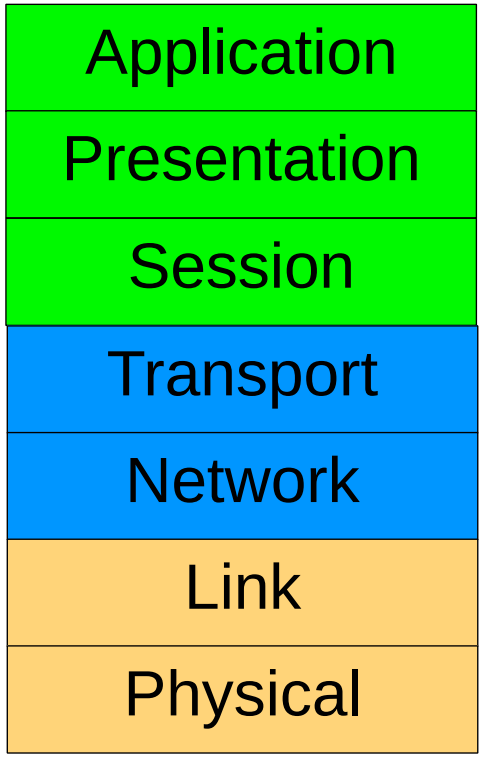
⇒2003 : Gigabit Ethernet 10 Gbps

⇒2015 : 100 Gbps Ethernet



Dessin initial de Robert Metcalfe

Le Role du « Physical Layer »



Physical Layer:

*La **couche physique** est responsable de la transmission de bits à travers un moyen physique* (e.g. signaux électriques, radio, optiques, etc).

NIC : Network Interface Card (Carte de ligne)

Les bits sont transportés comme signaux électriques à travers des câbles.

Routeur WiFi

Les bits sont transportés comme ondes électromagnétiques

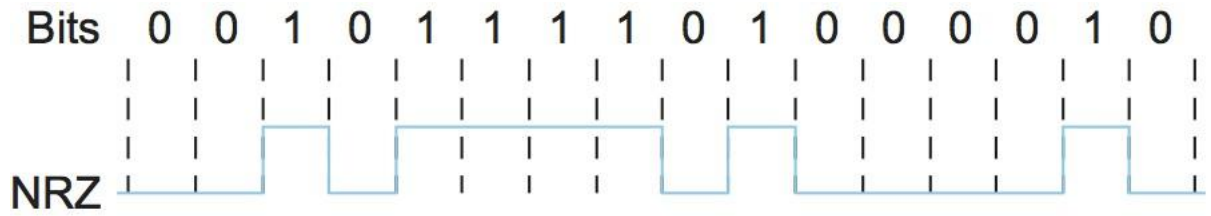
Images depuis Wikipedia

Codage en ligne

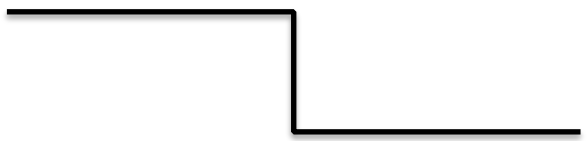
Codage: représentation du signal numérique pour être transmis sur des canaux de communication par des signaux analogiques.

Par exemple : 0 = 0V and 1 = +5V

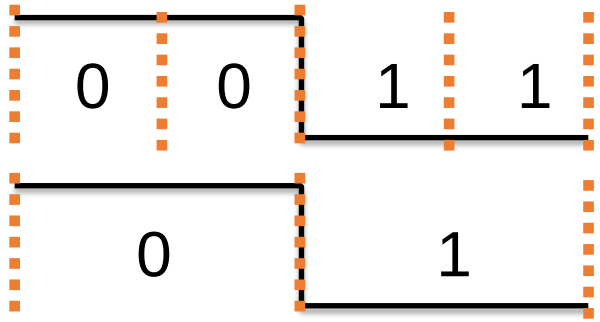
Non-Return to Zero (NRZ)



Problème : ambiguïté dans les systèmes synchronisation d'horloge



Doit on considerer "0 0 1 1" ou "0 1" ?

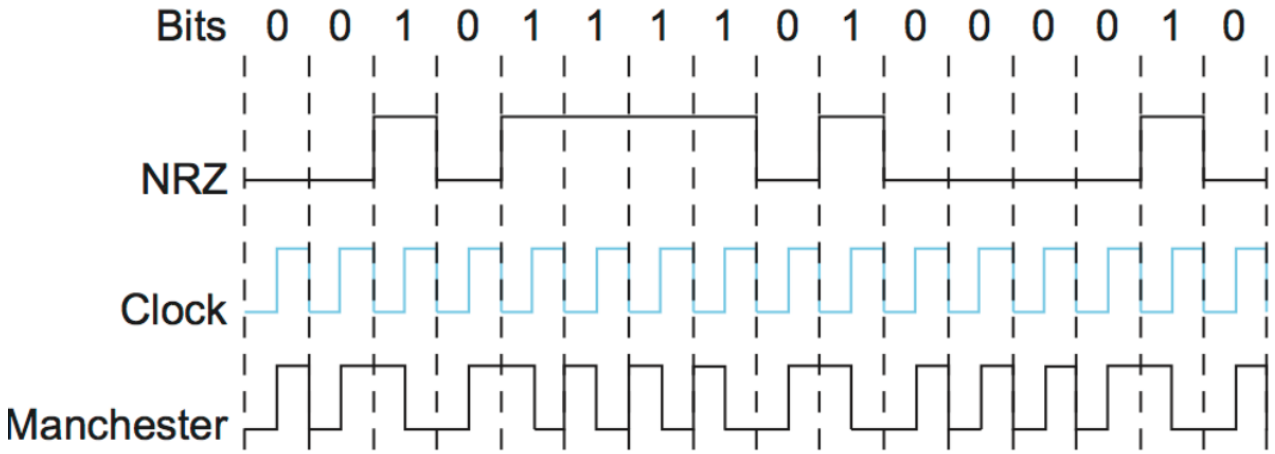


Codage Manchester

1: Transition du niveau haut vers le niveau bas

0: Transition du niveau bas vers le niveau haut

Obtenu en utilisant un XOR du codage NRZ avec l'horloge :



Avantages :

- Pas d'ambiguïté
- Les transitions inhérentes à ce codage permettent la synchronisation des horloges (émetteur/récepteur)

Code en bloc

Utilisé avant transport des signaux pour des raisons de fiabilité → introduire redondance pour pouvoir corriger des erreurs de transmission ou pour éviter longues séquences de zeros

Code en bloc 4B5B :

4 bits de données sont transformés en 5 bits avant tranmission

Data		4B5B code
(Hex)	(Binary)	
0	0000	11110
1	0001	01001
2	0010	10100
3	0011	10101
4	0100	01010
5	0101	01011
6	0110	01110
7	0111	01111

Data		4B5B code
(Hex)	(Binary)	
8	1000	10010
9	1001	10011
A	1010	10110
B	1011	10111
C	1100	11010
D	1101	11011
E	1110	11100
F	1111	11101

Symbol	4B5B code	Description
H	00100	Halt
I	11111	Idle
J	11000	Start #1
K	10001	Start #2
L	00110	Start #3
Q	00000	Quiet (loss of signal)
R	00111	Reset
S	11001	Set
T	01101	End (terminate)

- Max trois zeros consecutifs
- Symboles supplémentaires pour signalisation
- Utilisé avec plusieurs codages

Les standards de la couche physique Ethernet

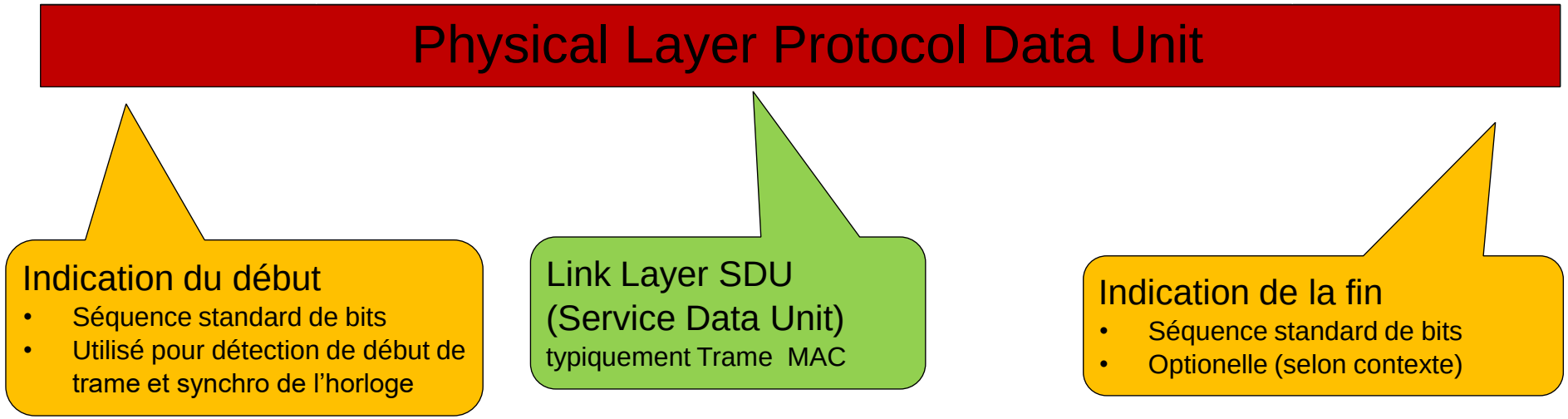
Phisical layer	Débit	Matériel	Codage
10Base-T	10 Mbps	Paires torsadées	Manchester
100Base-TX	100 Mbps	Paires torsadées	4B5B + MLT-3
100Base-FX	100 Mbps	Fibres	4B5B + NRZ-I
1000Base-T	1 Gbps	Paires torsadées	8B1Q4 + 4D-PAM5
10GBase-X	10 Gbps	Fibres	64B/66B + NRZ

Remarque: “Full Duplex” (transmissions et emissions indépendantes)

Trame de la couche physique

Une séquence de bits envoyé par un dispositifs physique s'appelle ***trame*** (« Frame »).

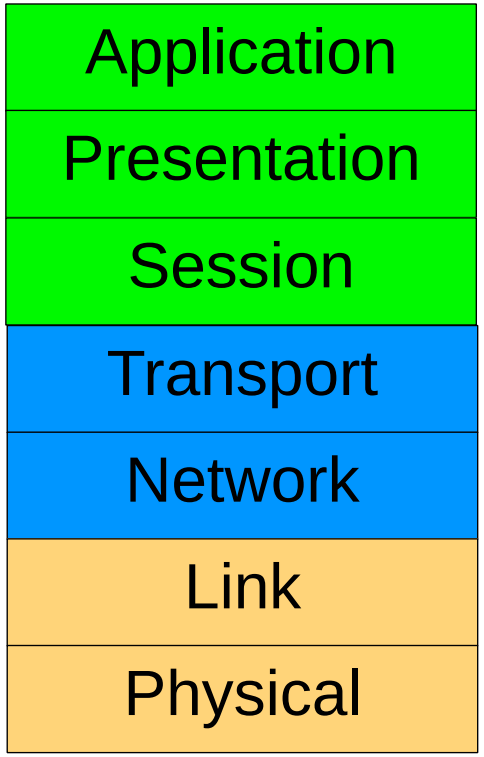
Structure de la Trame



Taille de la trame

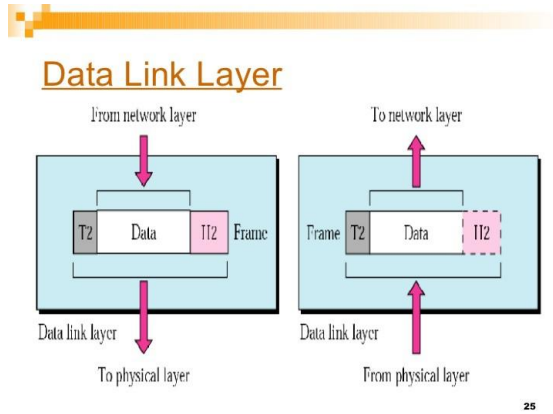
- Selon la technologie, peut etre fixe ou non

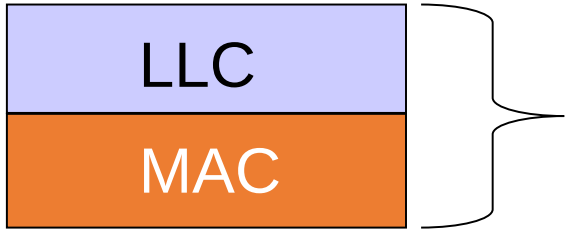
Le role du « Link layer »



Link Layer:

Responsable de la création d'une liaison logique entre nœuds connectés directement (e.g. Point-to-Point Protocol).

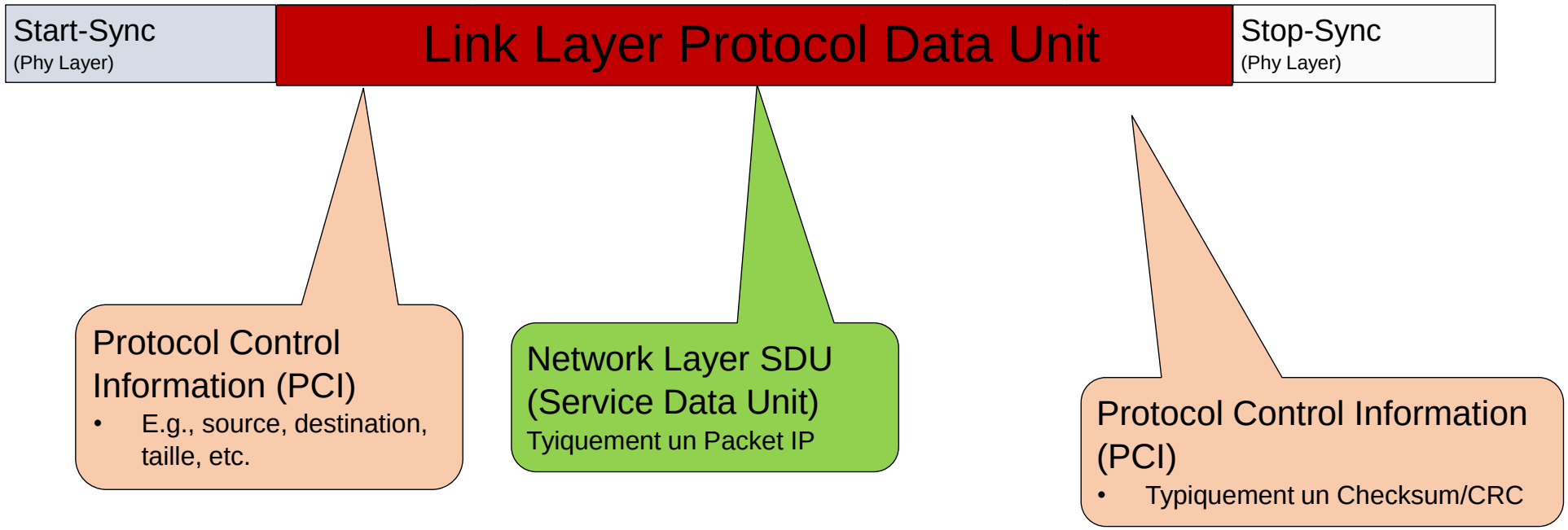




Data-Link Layer

Trame de la couche Link

Structure de la Trame



Trame Ethernet

- **Preamble**:
  - 56 bit sequence de synchronization
- **SFD – Start Frame Delimiter:**
  - Indique le début du contenu de la trame
- **Ethernet Header**
  - (Detaillé dans la suite)
- **Ethernet Payload**
  - Contenu de la trame (typiquement un paquet de la couche Réseau)
- **FCS – Frame Check Sequence**
  - 4 Octets (32 bits) CRC

Entête Ethernet

- **Adresse MAC** pour identifier les bouts de communication (interfaces réseaux)

- L'entête contient les adresses source et destination
  - Adresse Ethernet = 6 octets (48 bits)
- EtherType
  - 2 Octets (16 bits)
  - Represente le "type" de contenu
  - Par exemple :
    - 0x0800 = Payload is IPv4
    - 0x0806 = = Payload is ARP (Address Resolution Protocol)
    - 0x86DD = Payload is IPv6
    - 0x8100 = Payload is IEEE 802.1Q tag

Numération hexadecimal

- Très populaire dans le domaine informatique
  - Système positionnel en base 16
  - Conversion facile Hex to Binary et vice versa
  - Indiqué par la présence d'un "0x", i.e. 0x34
  - Chaque nibble (4-bits) est un caractère Hex
  - 4 bits -> 16 combinaisons

```
      100s | 10's | 1's        16's | 1's
52:   0    |    5 | 2           3|  4
172:  1    |    7 | 2           A|  C
```

Decimal (Base 10)	Binary (Base 2)	Hexadecimal (Base 16)
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

L'adresse MAC (ou addresse Ethernet)

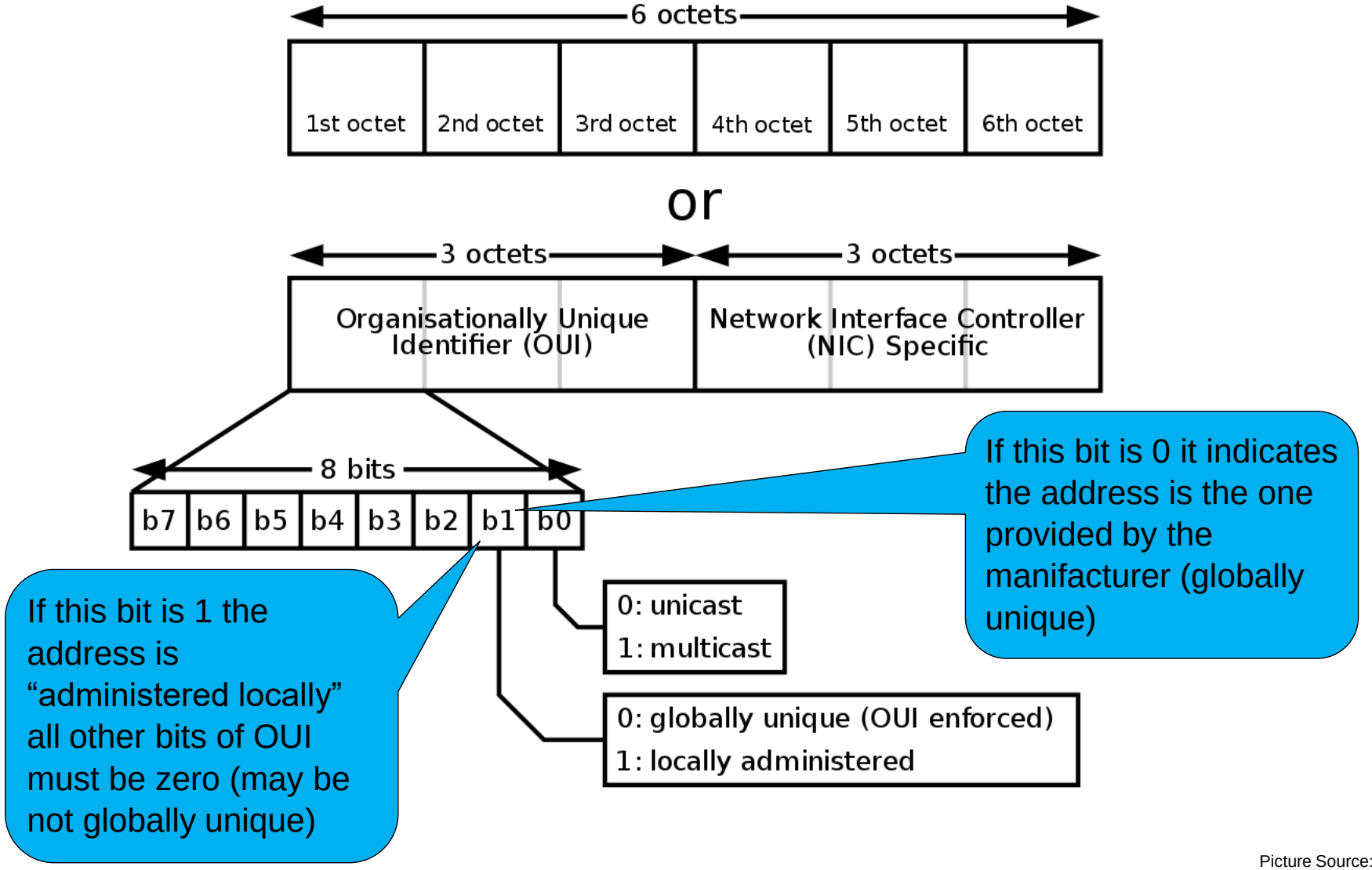
- L'adresse MAC est universel :
  - Garantie que pour chaque interface connecté à un réseau Ethernet il y aura une adresse unique

- Les premières 24 bits sont assigné au constructeur par le IEEE
  - IEEE = Institute of Electrical and Electronics Engineers
  - IEEE est l'entité qui standardise Ethernet

- OUI = Organizationally Unique Identifier
- Les dernières 24 bits sont choisi par le constructeur du NIC
  - 16 million de possibilités

- Le format d'écriture d'une adresse MAC est une séquence de numéros Hex separé par un double point :
  - Exemple: 98:01:A7:90:51:25

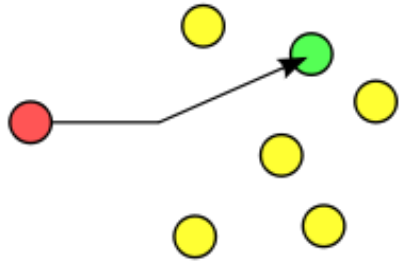
Structure de l'adresse MAC



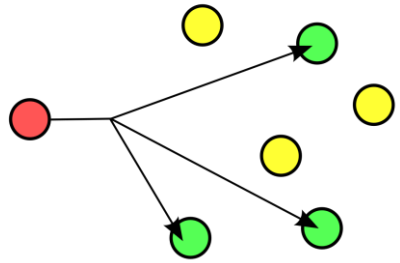
Picture Source: https://fr.wikipedia.org/wiki/Adresse_MAC

Communication modes

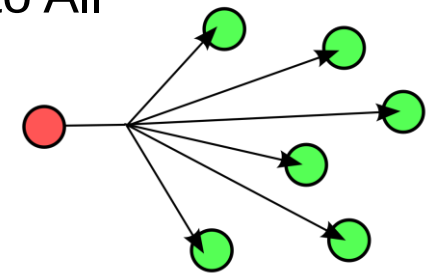
- Unicast: one to one



- Multicast: one to a selected group

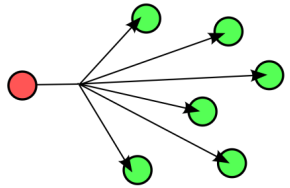


- Broadcast one to All

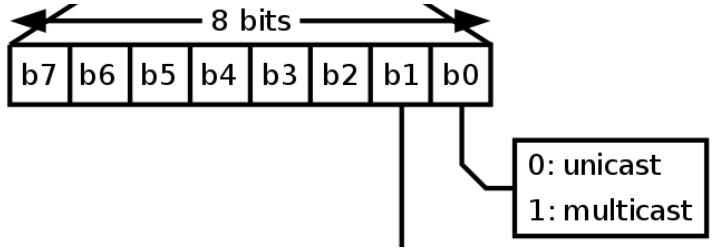


Ethernet special addresses

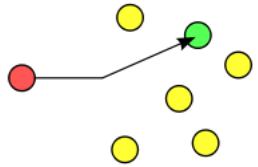
- Pour les communications de type Broadcast (all nodes connected on the same link) on utilise l'adresse speciale constitué par des "1" :
  FF:FF:FF:FF:FF:FF



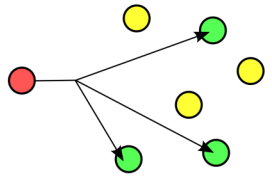
- En général :



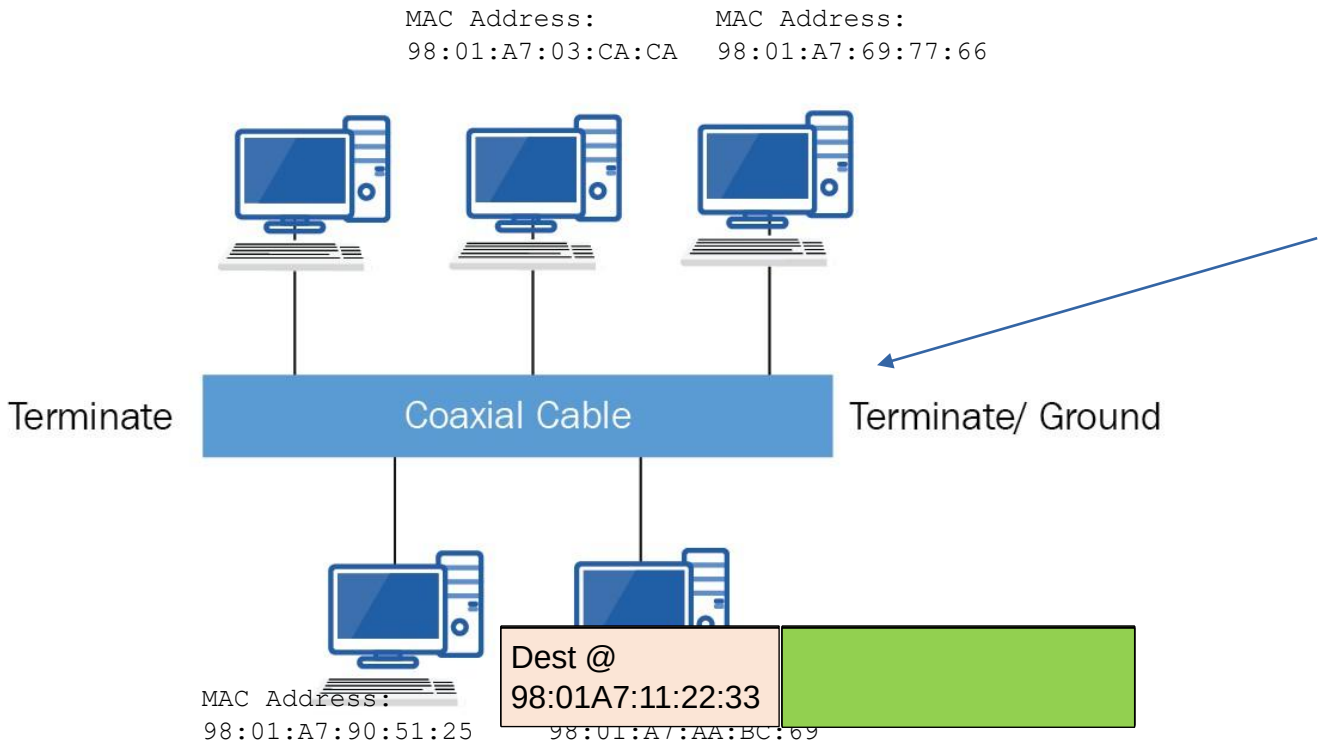
  - Si *b0* est 0 l'adresse est Unicast
    - i.e. unique localement pour communication one-to-one



  - Si *b0* est 1 l'adresse est Multicast
    - L'adresse appartient à un groupe (dans le même lien) standardisé par le IEEE
    - E.g.: 01:80:C2:00:00:00 est le Spanning Tree Protocol group
    - Il est possible de configurer si un NIC fait partie d'un groupe ou pas



Ethernet dans le passé

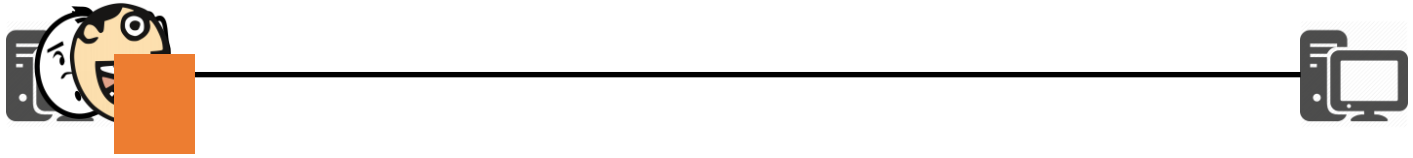


Tout le monde est connecté à un même câble : besoin de partager le médium

- Trames Ethernet transportées par signaux électriques à tous les noeuds connectés
  - Chaque carte Ethernet (*NIC*) peut extraire l'adresse MAC Destination, et donc choisir s'il accepte la trame ou pas

Accès partagé :Rappels (1/3)

- Liaison point à point:
  - Règle : Ecouter avant parler : si le canal est libre, on peut transmettre



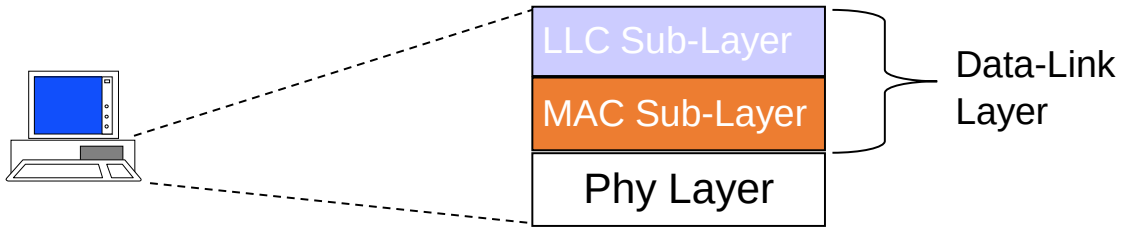
Simple, mais avec possibilité de *collision*

- Collision peuvent arriver si plusieurs transmissions arrivent au même instant

Accès partagé : Rappels (2/3)

- Médium partagé
  - C'est le support de la communication (e.g. câble; fréquence radio pour WIFI; …)
  - Propage les données à tout les stations connectées
    - Par le moyen de la transmission de signaux électromagnétiques ou optiques

- Collision:
  - Deux (ou plusieurs) dispositifs utilise le canal simultanément, et par conséquence le signal est altéré
  - Possibilité de détecter si le média est utilisé ou pas
    - Pour les médias câblés, il est possible de transmettre et recevoir en même temps
      - **Détection de collisions possible (voir: CSMA/CD)**
    - Pour les médias sans fils, ceci n'est pas possible
      - Les collisions ne peut pas être détectées
      - On doit essayer de les éviter !
      - **Voir: CSMA/CA**

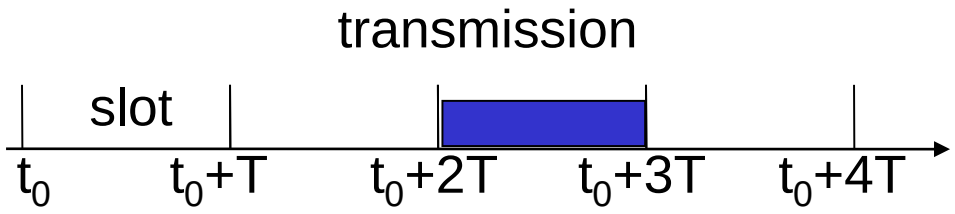


- Sous-coûche MAC :
  - Définie les fonctions/méthodes et protocoles pour l'accès au média (voir partie *invariants fonctionnels*)

Accès partagé : Rappels (3/3)

- Transmission asynchrone:
  - L'envoie des trames peut commencer à tout moments
  - Pas besoin d'une horloge synchronisée

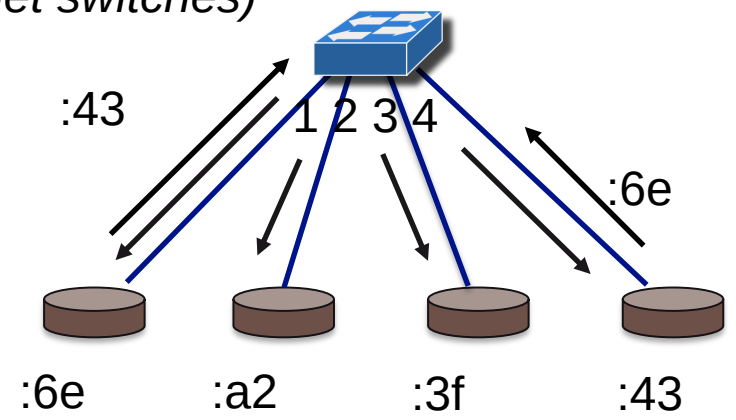
- Transmission synchrone:
  - Le tems est divisé en "slots"
    - Nécessaire un horloge pour synchronisation
  - La transmission est possible au début du time slot
  - Dans chaque slot on peut y avoir :
    - 0 dispositifs émetteurs : slot non utilisé
    - 1 dispositif émetteur: slot utilisé
    - 2 (ou plusieurs) dispositifs émetteurs: slot utilisé et présence de collisions



- <u>Ecoute du Medium</u> :
  - Chaque émetteur peut écouter le médium avant de commencer la transmission
  - Exemple: protocoles de la famille CSMA

Modern Ethernet

- Aujourd'hui, Ethernet est totalement **full duplex**
- Les réseaux sont connectés avec des **Commutateurs Ethernet** *(Ethernet switches)*



- Simplex:
  - Communication seulement dans un sens
  - E.g. remote control pour ouvrir un garage

- Half-duplex:
  - Communication possible dans les deux sens, un à la fois
  - E.g. CSMA-CD sur un câble Ethernet
  - Plusieurs dispositifs peuvent se connecter au même câble

- Full-duplex :
  - Transmission & Réception en même temps (pas de collisions)
    - Soit en utilisant deux "lignes" indépendantes pour les deux sens (100 Mb Ethernet)
    - Soit en utilisant la même ligne avec codage différentiel (10Gb Ethernet)
  - Communication de type Point-to-point seulement (pas de collisions)

Interconnection des réseaux locaux: Hub

Répéteur (ou ***hub)***

– Il assure des fonctions de couche 1 (PHY), il n a donc pas d'adresse MAC

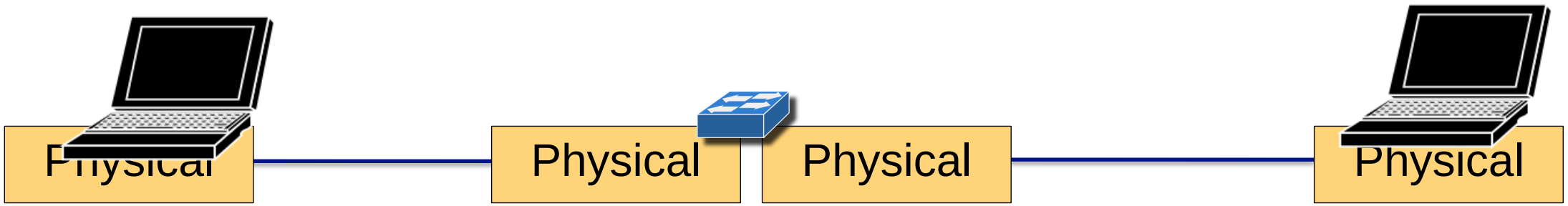
– Un répéteur peut recevoir et décoder les données venant d'un segment.

– Il retransmet les données sur tous les segments auxquels il est attaché :
les segments restent dans le même **domaine de collision**.

– L'amplitude est restaurée et les éventuelles distorsions du signal sont supprimées.

– Si une collision est détectée, il propage la collision en envoyant un signal de bourrage (jam : 101010...).

– Un répéteur peut permettre: (i) le passage à un type de support différent (ii) extension de couverture



Interconnection des réseaux locaux: Switches

Commutateur Ethernet (ou *Switch*) :

– Dispositif de la couche 2 *Data link*

– Il est composé de d'un certain nombre de « *ports* » *Ethernet,* reliées entre eux (par un bus interne à haut débit, commutateurs *non bloquants*).

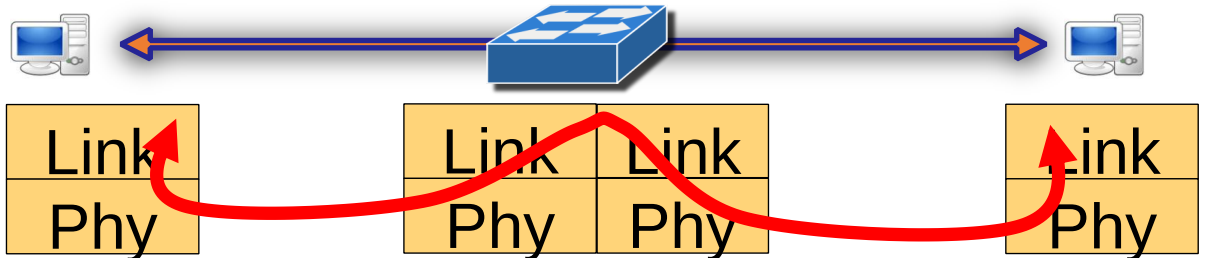
– Chaque carte dispose d'une mémoire tampon (*buffer*).

– Les stations directement reliées à un port dialoguent en point-à-point full-duplex avec le commutateur.

– Le commutateur est typiquement ***store-and-forward***

– Séparation des domaines de collision (au dessus de MAC)

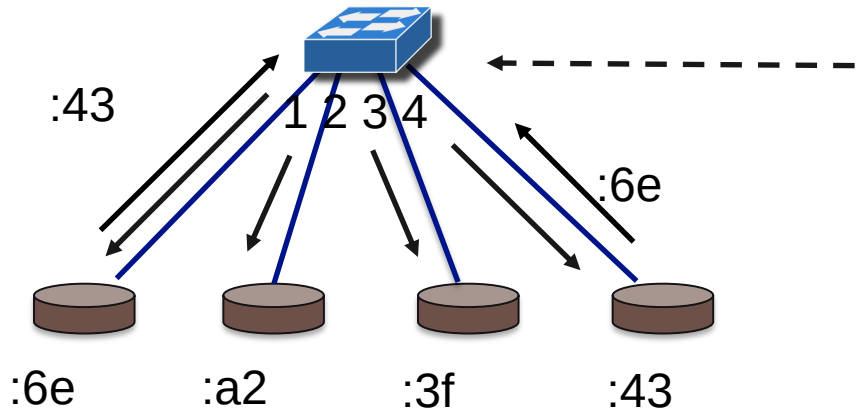
– Transparent : aucune configuration à effectuer pour les « hosts »



Switching Filtering & Forwarding

- Les Switches peuvent apprendre depuis quel port le trafic a été reçu*
  - Utilisation d'une « table de commutation»
    - quand la trame est reçue, le switch garde l'adresse de l'éxpediteur
      - Ceci est aussi stoqué dans la filtering table
- Mécanisme de fonctionnement pour l'expédition d'une trame
  - Envoyer la trame vers le port où l'adresse destination est connecté (si connu)
  - Envoyer la trame vers tous les ports (except input port) autrement
  - Ceci s'appelle envoie en **Broadcast**

*Port = network interface

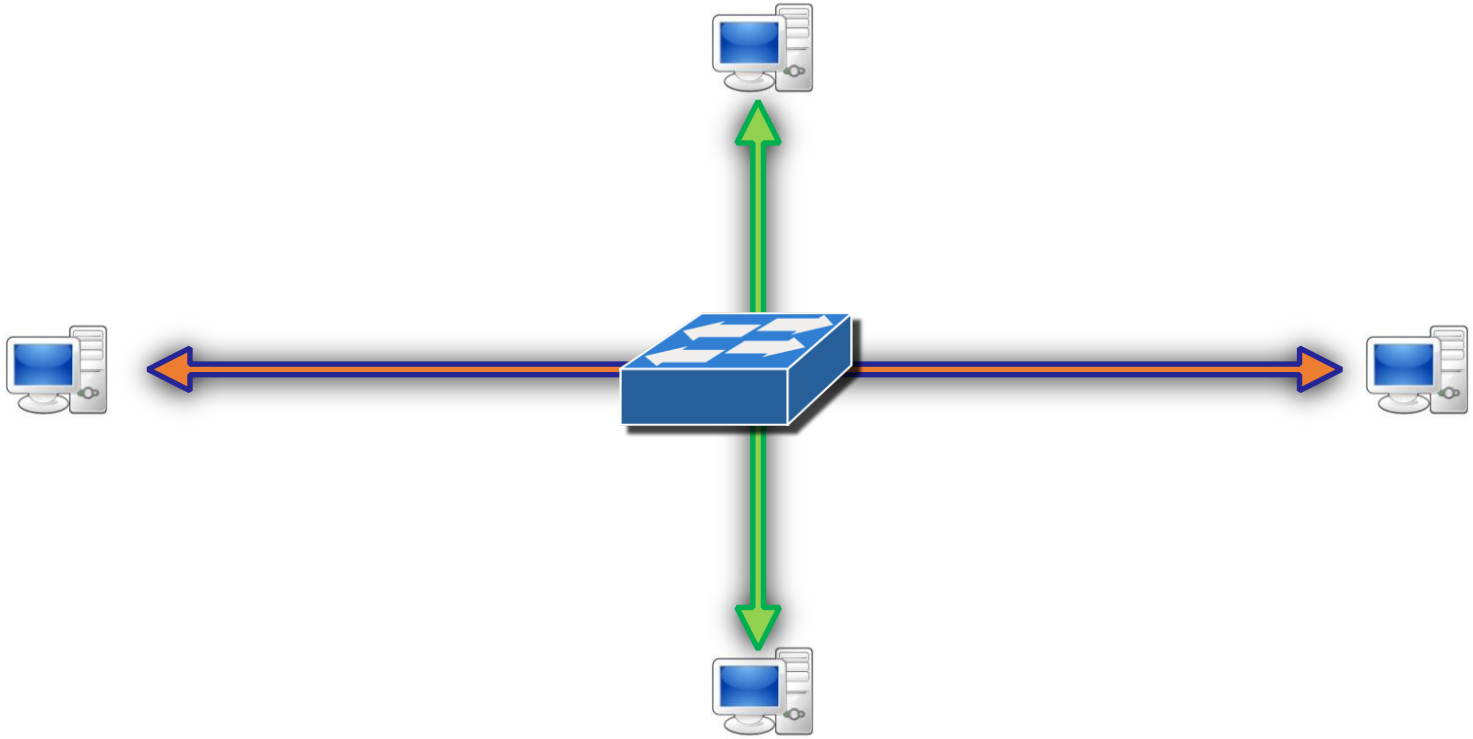


Switching Table

MAC	Port	TTL
:3f	*3*	*2:32*

Segmentation avec les switches

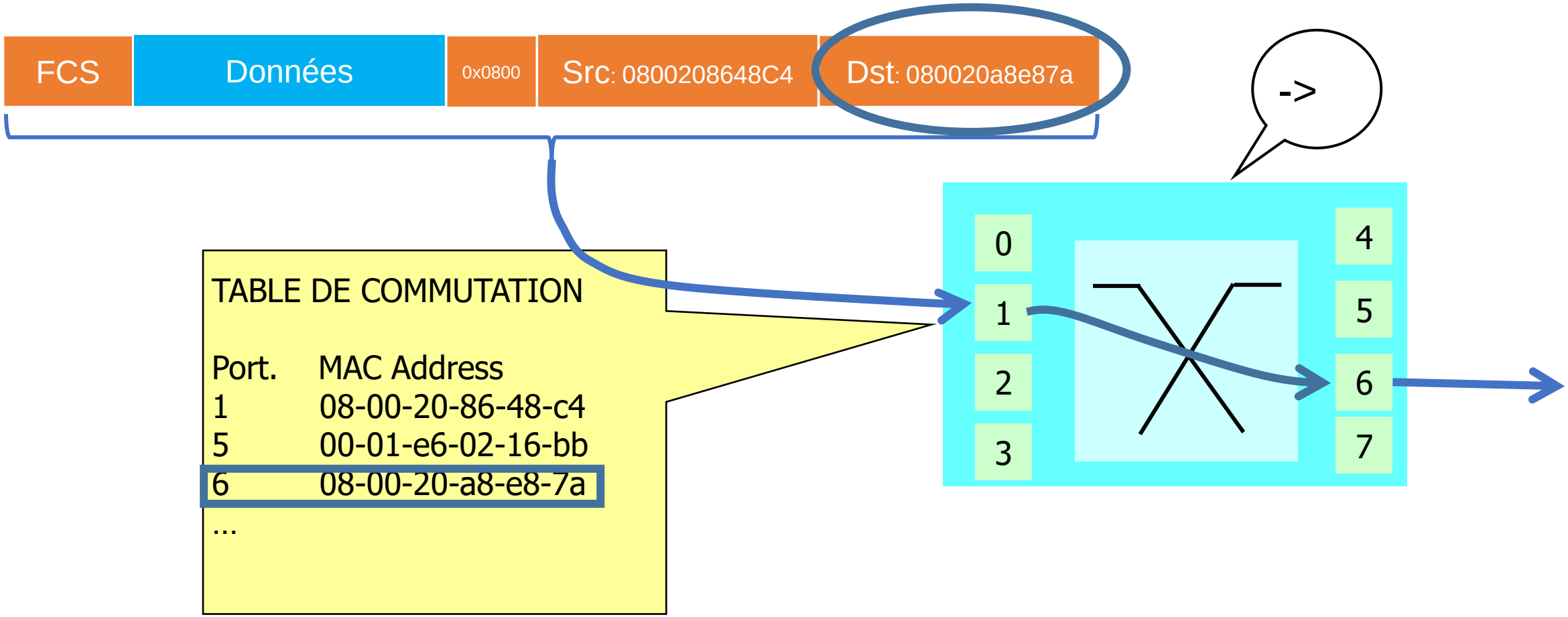
- Les commutateurs peuvent envoyer le trafic en “parallèle”
  - Vrai dans le cas de *ports* distincts
  - Dans l’exemple de la figure “vert” et “bleu” sont envoyé à la vitesse du lien



Commutation Ethernet- 1

Vers quel port envoyer un paquet ?

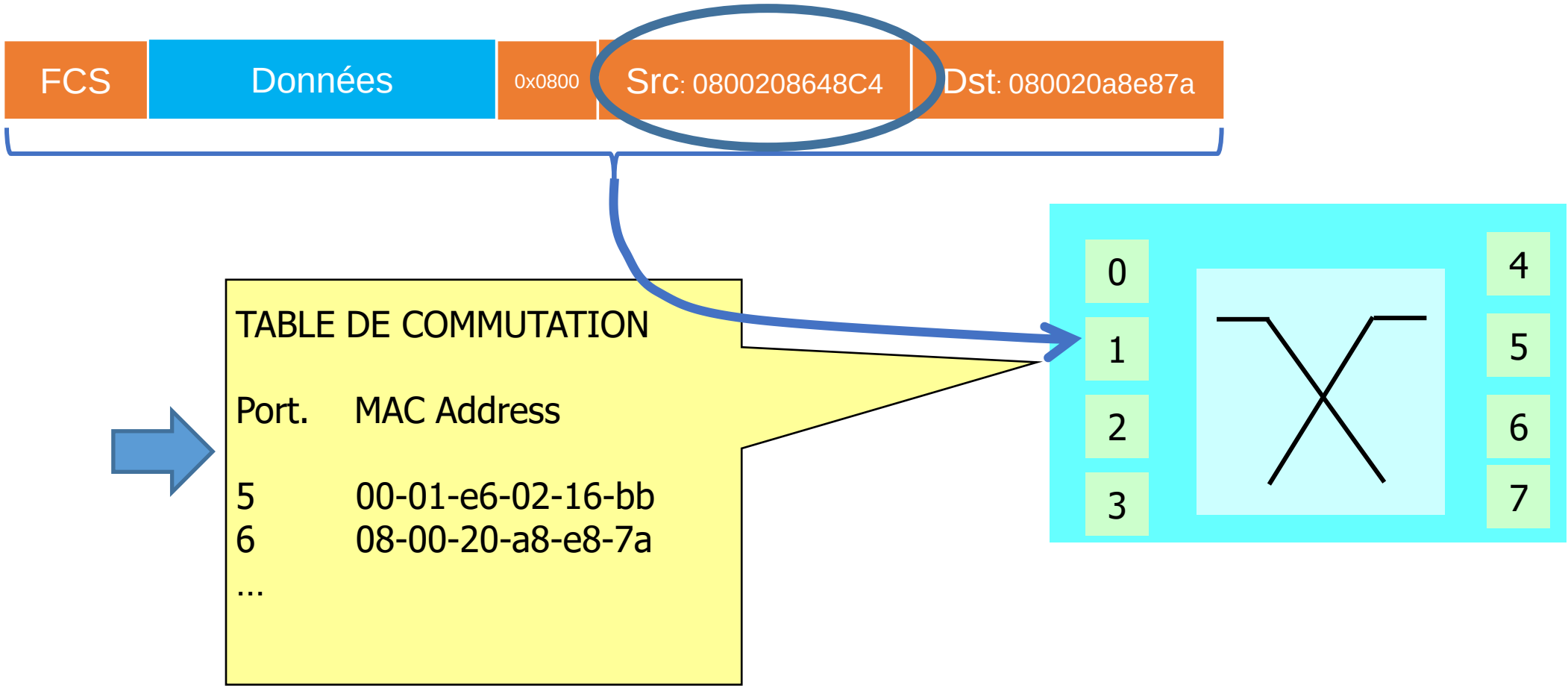
Nécessite de connaître la position des différentes adresses MACs (table de commutation)



Commutation Ethernet- 2

Comment construire la table de commutation ???

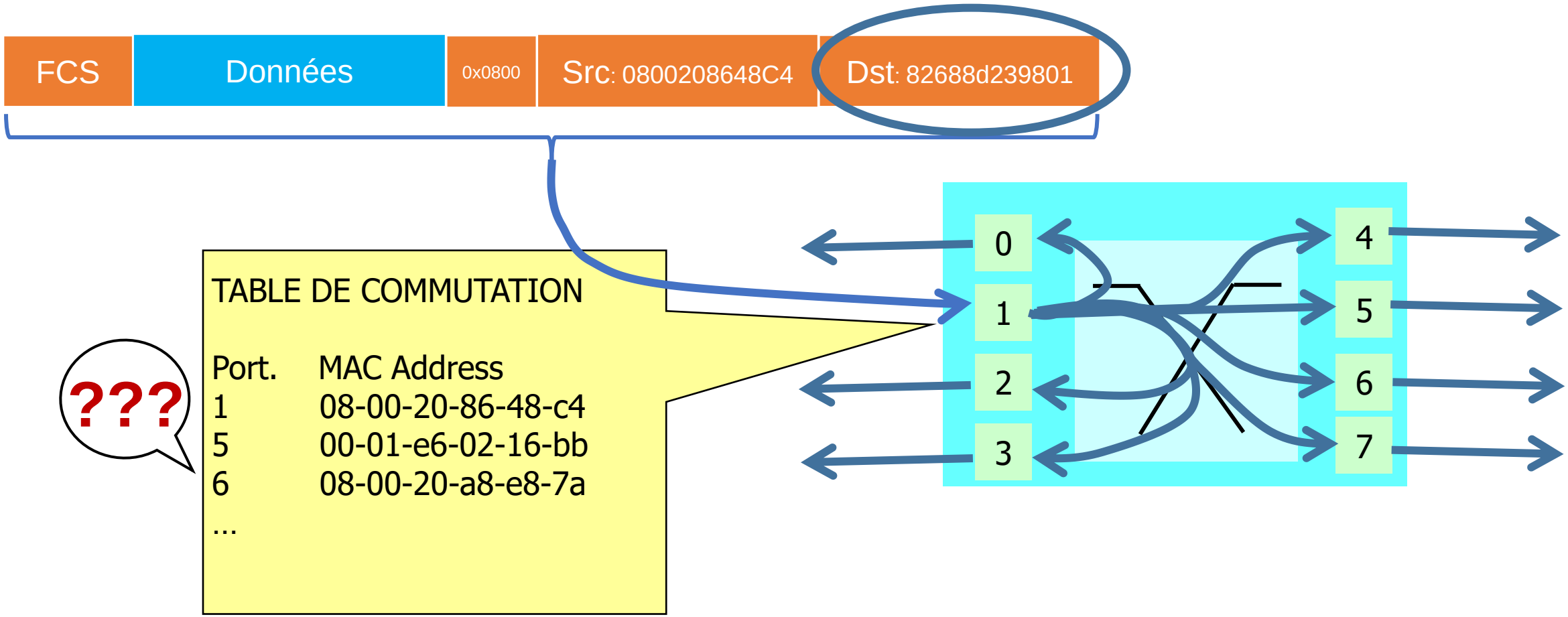
Auto-configuration (en analysant les adresses sources des paquets reçus)



Commutation Ethernet- 3

Qu'arrive-t-il si le commutateur ne connait pas les adresses destinations ?

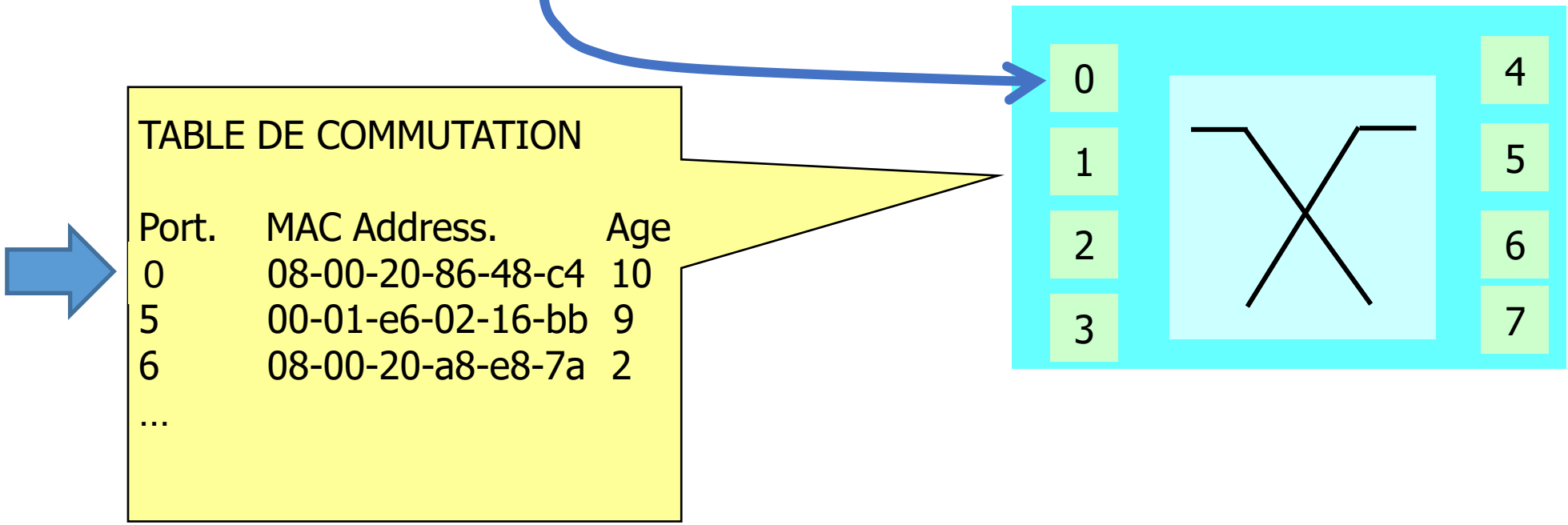
Relayage (forward) sur TOUS les ports



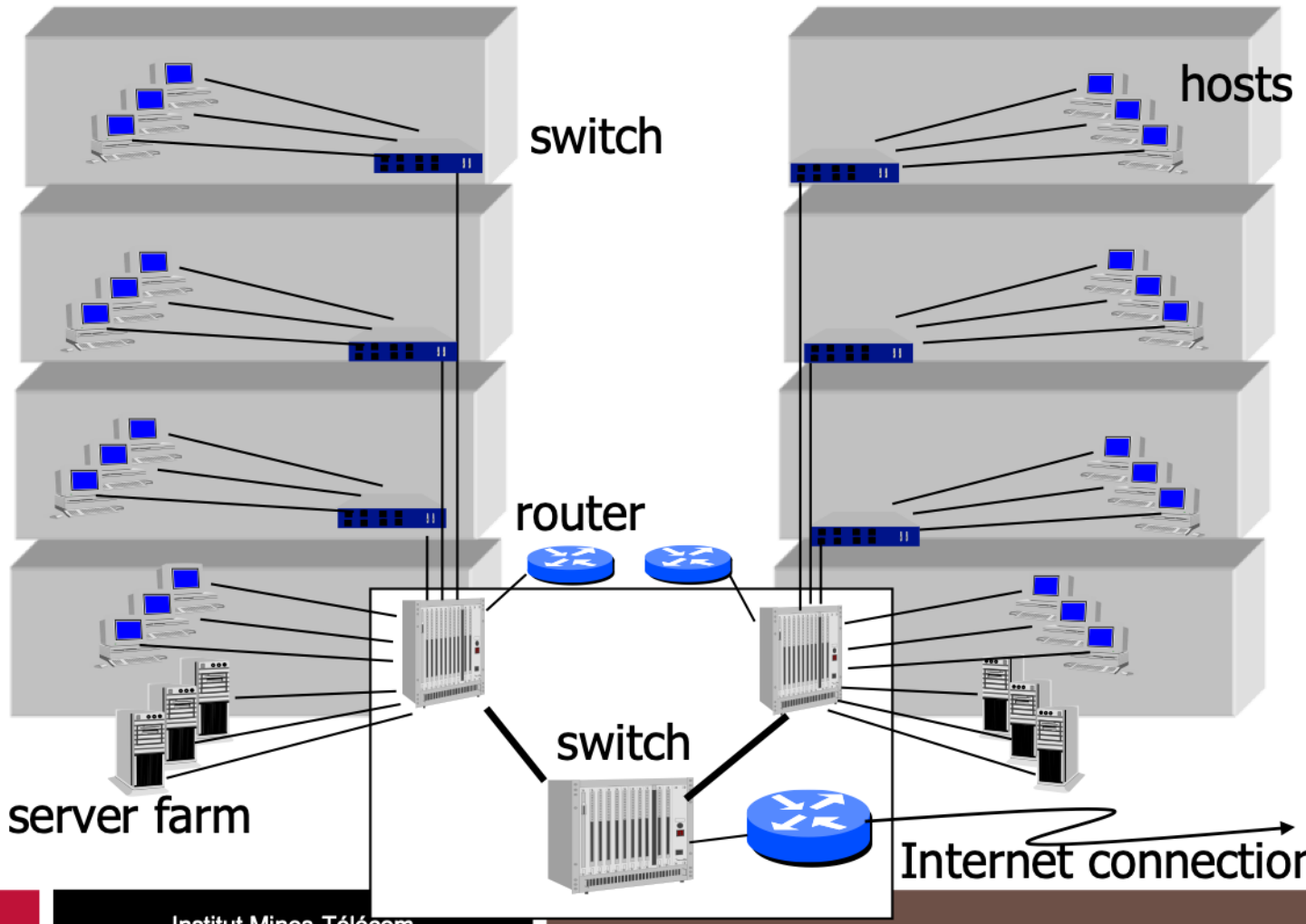
Commutation Ethernet- 4

Comment gérer la mobilité ?

- Mise à jour de la table (auto-apprentissage à partir des adresses Sources)
- Durée maximum des entrées dans la table de commutation (destruction après durée max)



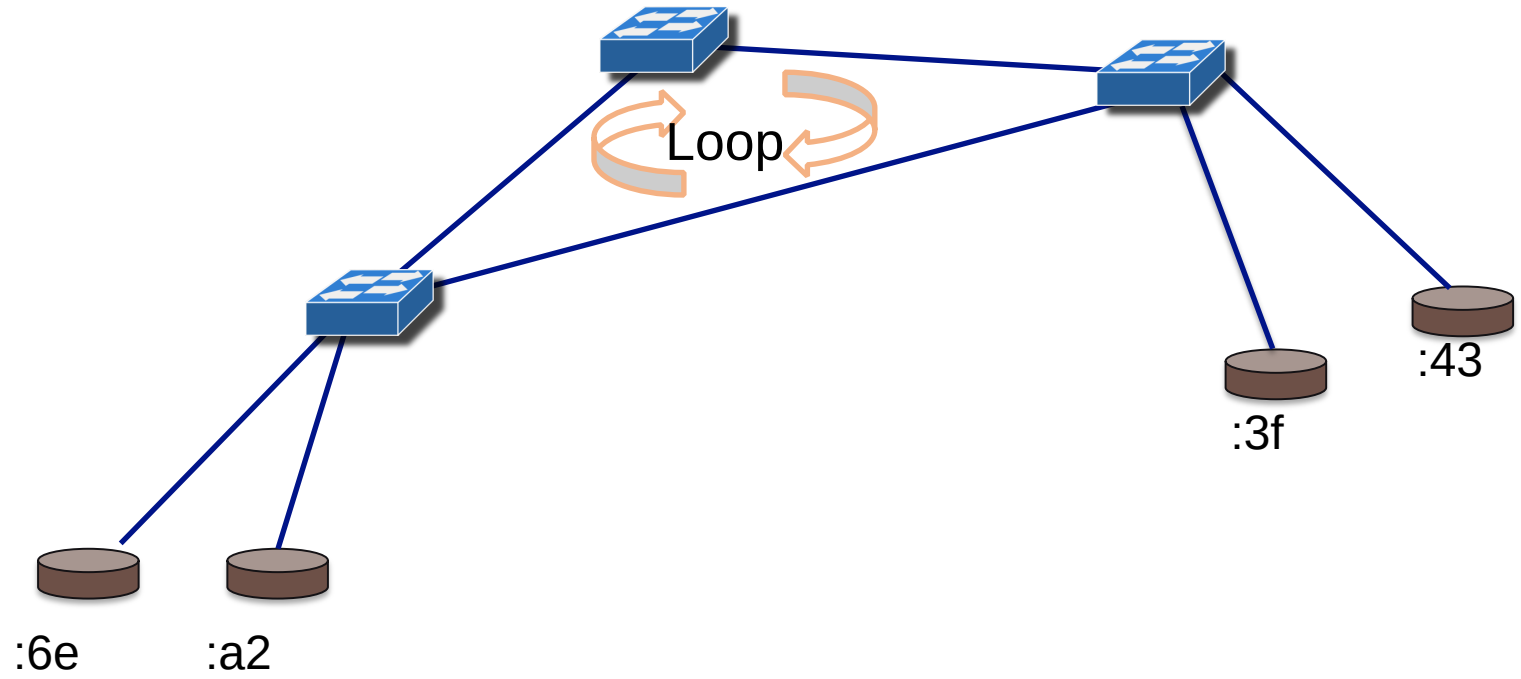
Architecture typique: Commutation Ethernet



The Broadcast Storm Problem and the Spanning Tree Protocol

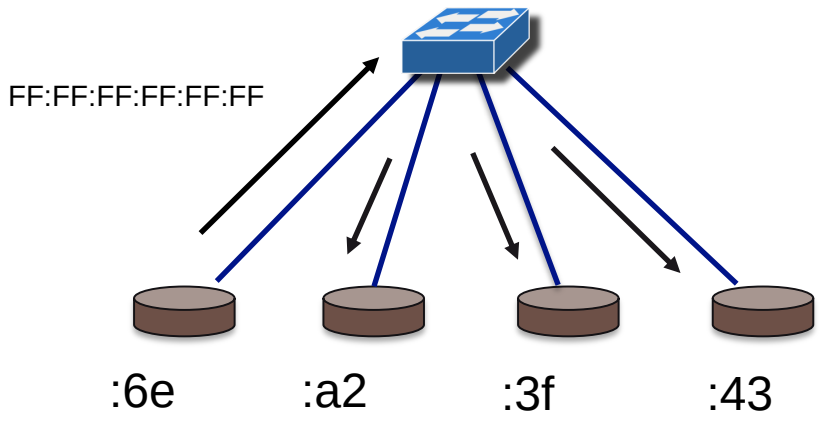
Interconnecting several links

- **Possibilité de créer des boucles**
  - Les trames en broadcast peuvent boucler entre plusieurs commutateurs
  - Le réseau peut devenir surchargé, et donc inutilisable
  - L'utilisation des « switching tables » peut devenir problématique



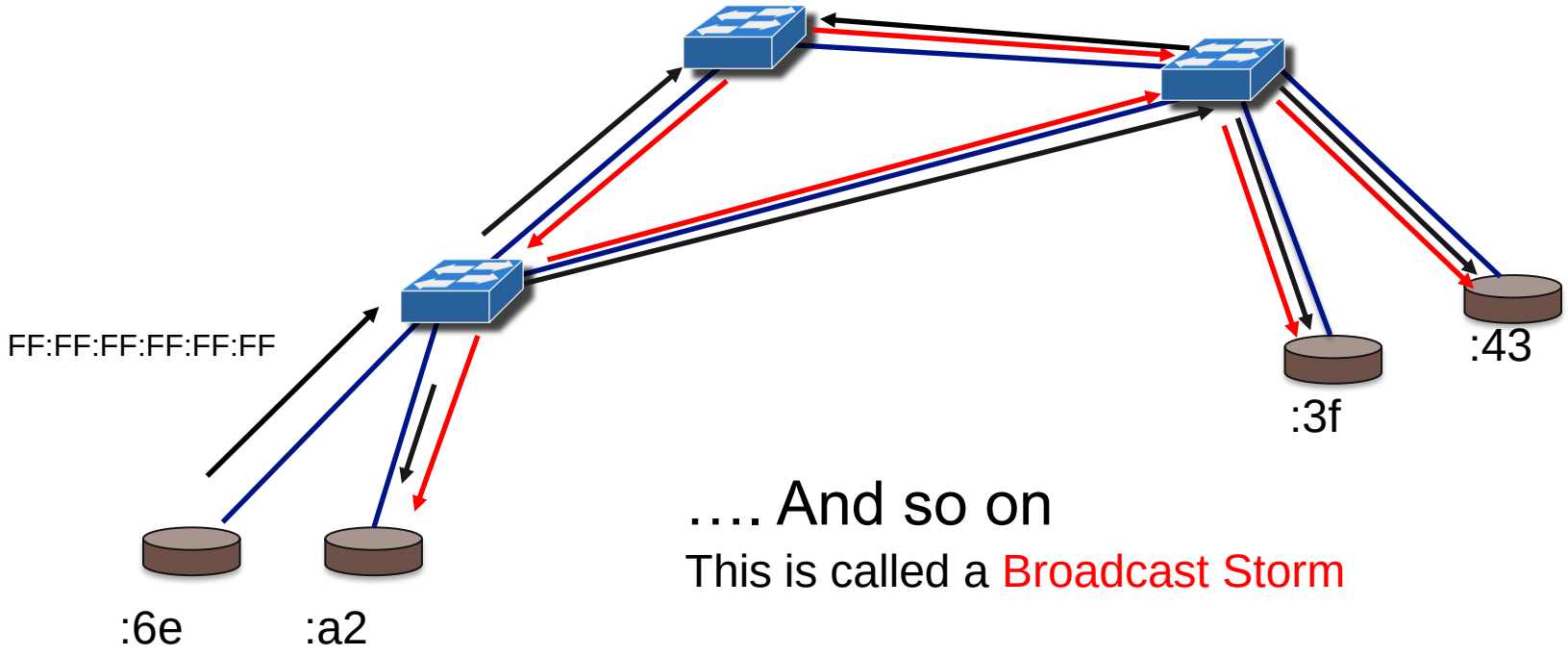
Example: broadcast in simple scenarios

- Broadcast Principle
  - Envoyer vers tous les ports



Example: a more complex scenario

- Broadcast Principle
  - Envoyer vers tous les ports
  - Problème : Ethernet n’a pas un moyen de détecter si une trame a déjà traversé un nœud ou pas
  - En couche L2 il n’y a pas la notion de “graphe”

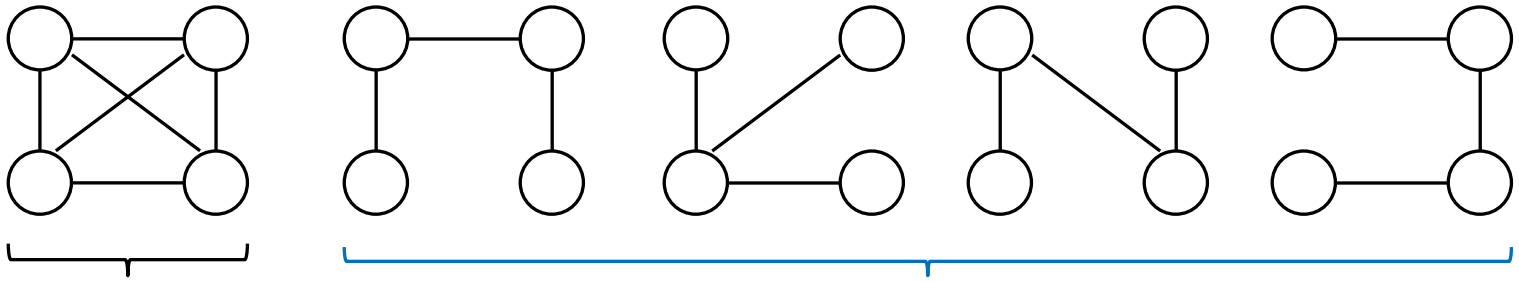


…. And so on

This is called a Broadcast Storm

Avoiding loops: spanning tree

- On considère un graphe non orienté (*undirected graph*)
  - Connexe : un seul tenant → tout sommet est joignable a partir de tout
  - Non orienté : les arêtes entre les sommets n'ont pas une direction fixé
- ...On appelle **spanning tree** du graphe un sous-graphe connexe sans boucles



Spanning Tree Protocol - STP (IEEE 802.1d)

- Characteristiques:
  - Permet d'obtenir des parcours « loop-free » dans un réseau avec liens redondants
  - On peut choisir un parcours unique entre chaque couple de noeuds
  - Toutes alternatives sont bloqués (de manière a ne pas introduire des boucles)
  - Dans le cas d'échec, il peut automatiquement utiliser un des parcours précédemment bloquées

Principe de fonctionnement :

- Choisir un switch "root"
- Chaque switch calcule le plus cour chemin vers le root
- Construire un spanning tree qui couvre la topologie entière

- Protocol:
  - Comme un protocole classique, basé sur l'échange de messages standardisés
    - BPDU – Bridge* Protocol Data Unit

The STP algorithm

- L'algorithme STP convergera vers une topologie loop-free en trois étapes

Convergence STP

1. Elect one Root Bridge
2. Elect Root Ports
3. Elect Designated Ports

- Pour le choix des root bridge, root ports et designated ports, le STP utilise quatre critères:
  - Four-Step decision Sequence
    1. Lowest BID (Bridge Identifier)*
    2. Lowest Path Cost to Root Bridge
    3. Lowest Sender BID
    4. Lowest Port ID (Identifier)*

*Plus de détail dans la diapositive suivante

Three Steps of Initial STP Convergence

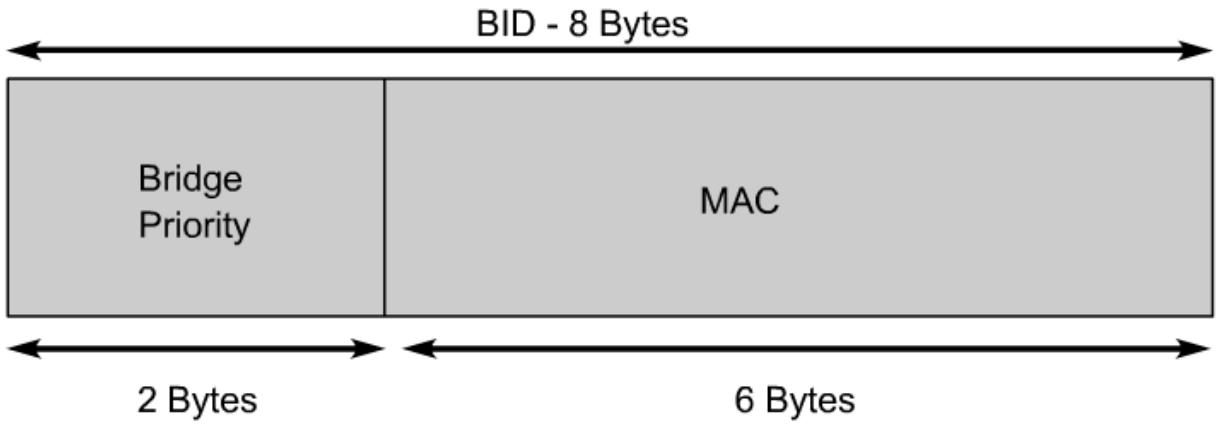
STP Convergence

Step 1 Elect one Root Bridge

Step 2 Elect Root Ports

Step 3 Elect Designated Ports

Bridge Identifier (BID)



- Bridge ID (BID) | utilisé pour identifier chaque commutateur.
  - BID est utilisé aussi pour choisir le root bridge
  - Ceci sera la racine pour le spanning tree

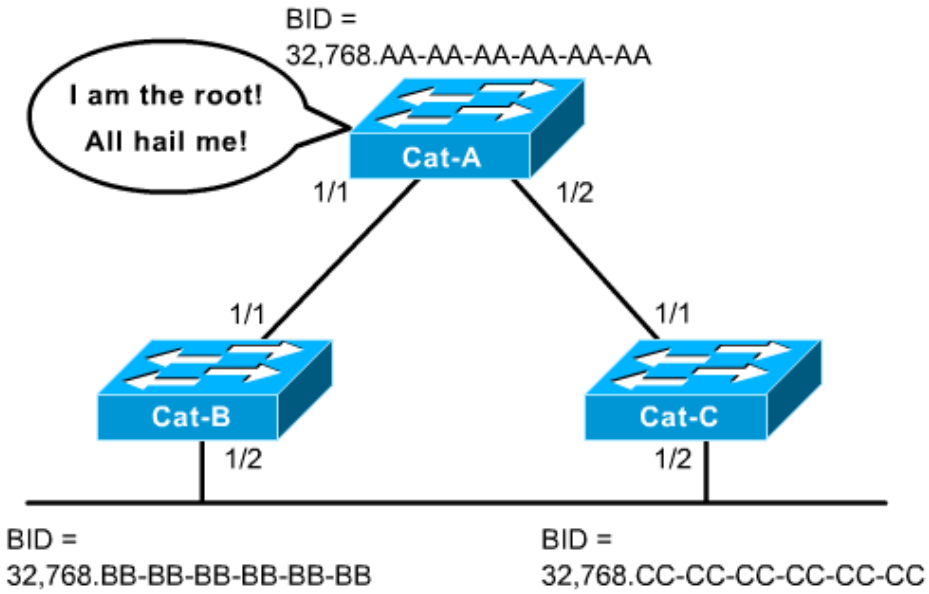
- Le BID a deux parties:
  - 2-octets: Bridge Priority
    - Les switch Cisco ont **32,768** ou 0x8000 par défaut
    - Peut être modifié par l'opérateur du réseau
  - 6-octets: MAC address

STP Root Selection

- Le Bridge Priority dans le BID est typiquement représenté en format décimal
- L’adresse MAC dans le BID est représenté en format hexadécimale
- Le plus petit BID est le root switch
  - Si tous les dispositifs connectés ont la meme Bridge priority, le switch avec le MAC plus petit devient automatiquement le root switch
    - Équivalent à effectuer un choix aléatoire, car le MAC est fixé par le constructeur

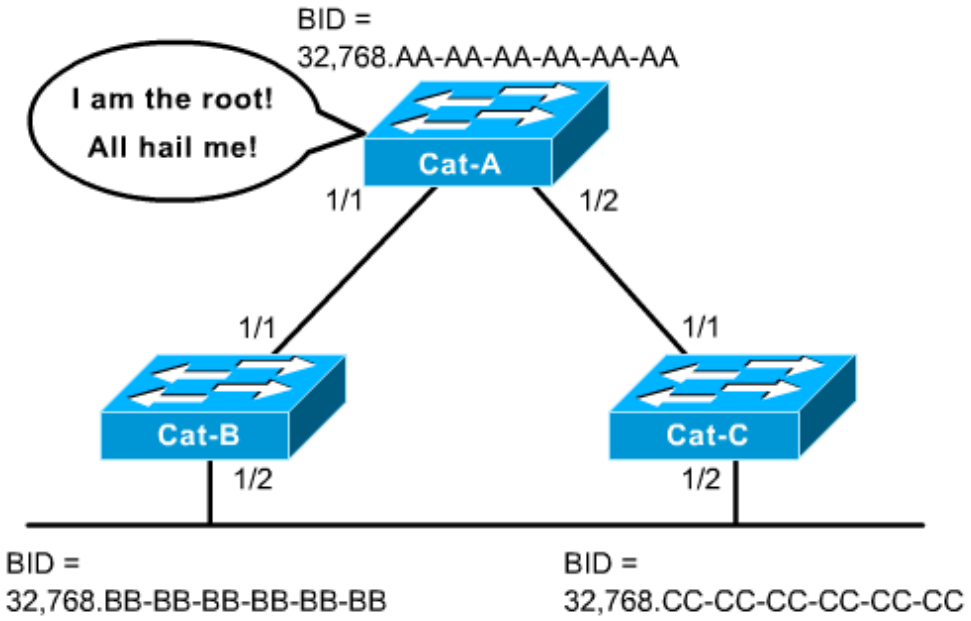
STP: Select one root bridge

- Four-Step decision Sequence
  1. Lowest BID (Bridge Identifier)
  2. Lowest Path Cost to Root Bridge
  3. Lowest Sender BID
  4. Lowest Port ID (Identifier)



- Quand le réseau est demarré, les switch propagent un enseble de BPDUs
- Depuis, les switch appliqueront la séquence en quatre étapes pour choisir le root
- Quand l'algorithme convergera, un seul root switch sera elu
- **Le switch avec BID** plus petit gagne
  - Note: « haute priorité » est équivalent à « BID plus petit ». Faites gaffe !
- Ce mécanisme est connu comme "Root War" (la guerre pour la racine).

STP: Select one root bridge



Les trois commutateurs ont la meme priorité de 32,768

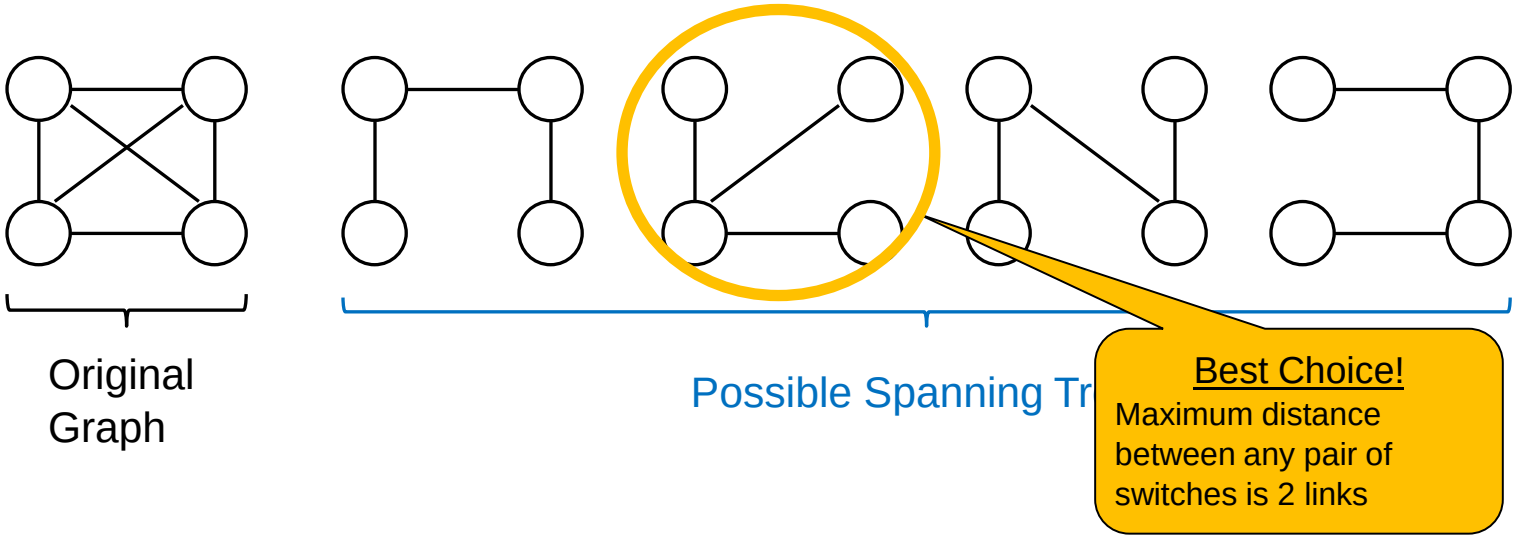
Le switch Cat-A est celui avec le MAC plus petit, donc il gagne la Root War!

Remarques sur le Root Switch

- Dans un vrai réseau, il n'est pas souhaitable de laisser le choix du root switch à un comportement aléatoire du aux adresses MAC.

- En effet, un root switch mal placé peut donner lieu à utilisation non-optimale du réseau, notamment pour la présence de chemins plus long.

- Par conséquence, il est recommandé de choisir un root switch en utilisant les valeurs de priorité



Three Steps of Initial STP Convergence

STP Convergence

Step 1 Elect one Root Bridge

Step 2 Elect Root Ports

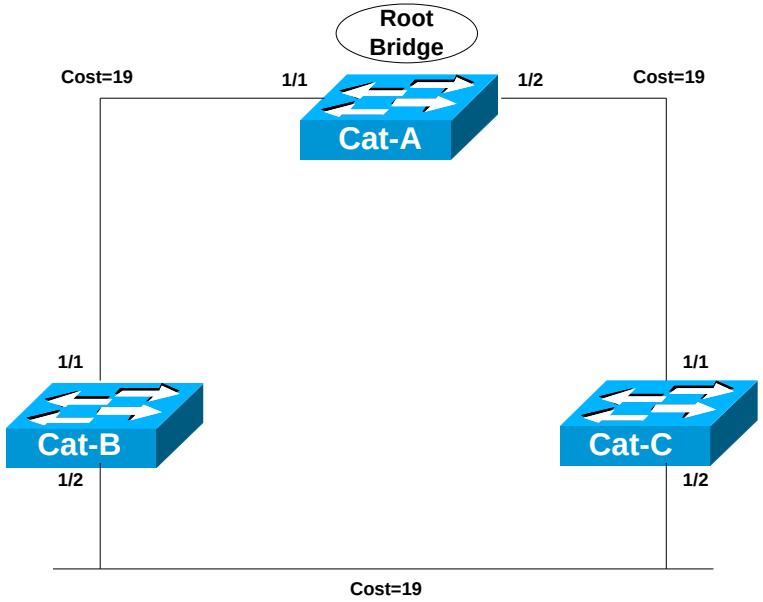
Step 3 Elect Designated Ports

Coût pour chaque lien

Link Speed	Cost(Revised IEEE Spec)	Cost (Previous IEEE Spec)
10 Gbps	2	1
1 Gbps	4	1
100 Mbps	19	10
10 Mbps	100	100

- Chaque lien a un coût, qui dépend du débit de transmission
- L'IEEE utilise une **echelle non-linéaire** ave les valeurs suivantes:
  - 4 Mbps 250 (cost)
  - 10 Mbps 100 (cost)
  - 16 Mbps 62 (cost)
  - 45 Mbps 39 (cost)
  - 100 Mbps 19 (cost)
  - 155 Mbps 14 (cost)
  - 622 Mbps 6 (cost)
  - 1 Gbps 4 (cost)
  - 10 Gbps 2 (cost)

STP: Elect Root Ports



- Un Root Port est le port **le plus proche** au root switch.
- Chaque switch non-Root doit choisir un root port.
- **Proche = Moin cher →cost plus petit** (on rencontrera ce concept très souvent)
  - Pour faire ça, un switch doit tracer de manière additive tous les coûts des liens qui emmènent aux root switch.

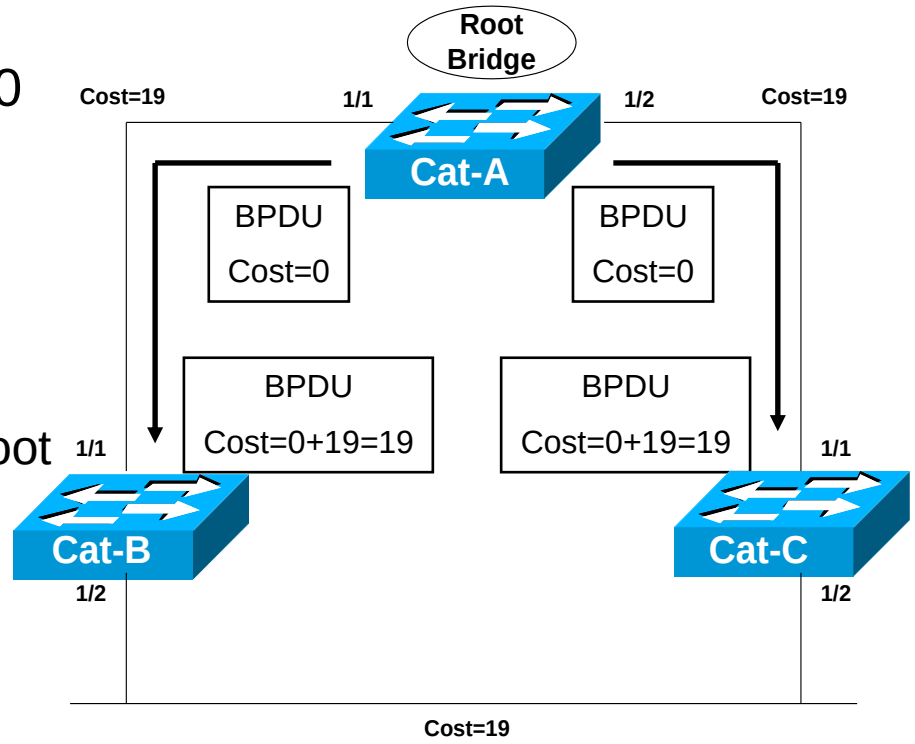
STP: Elect root ports

Step 1

- Le switch Cat-A envoie des BPDUs avec Root Path Cost=0
  - Cela représente qu'il est le root!

Step 2

- Le switch Cat-B reçoit les BPDUs et il ajoute la valeur 0 au Root path cost du Port 1/1
  - Root Path Cost = 0 + Port 1/1 cost (19) = 19



STP: Elect root ports

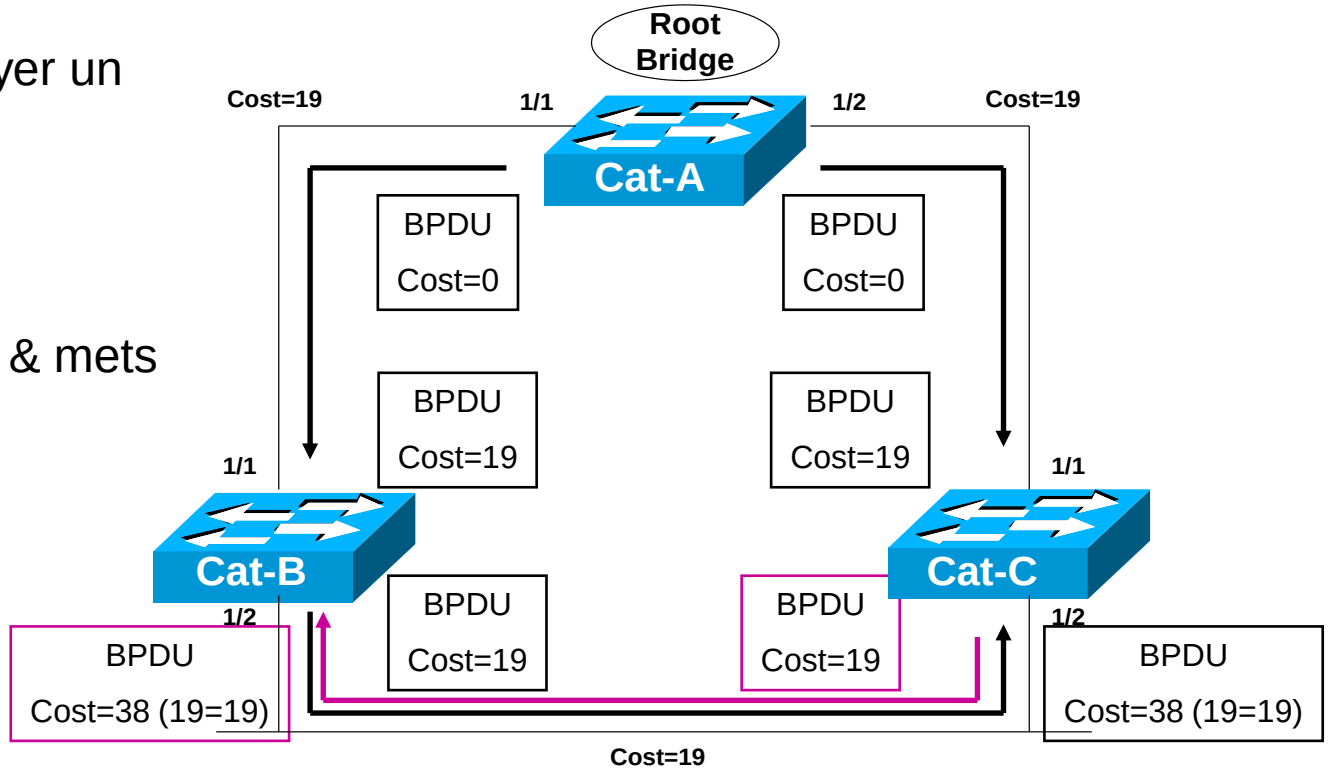
Step 3

- Le switch Cat-B utilisera la valeur 19 pour envoyer un BPDU avec Root Path Cost 19 vers le port 1/2

Step 4

- Le switch Cat-C obtient le BPDU depuis Cat-B & mets à jour le Root Path Cost à 38 (19+19)

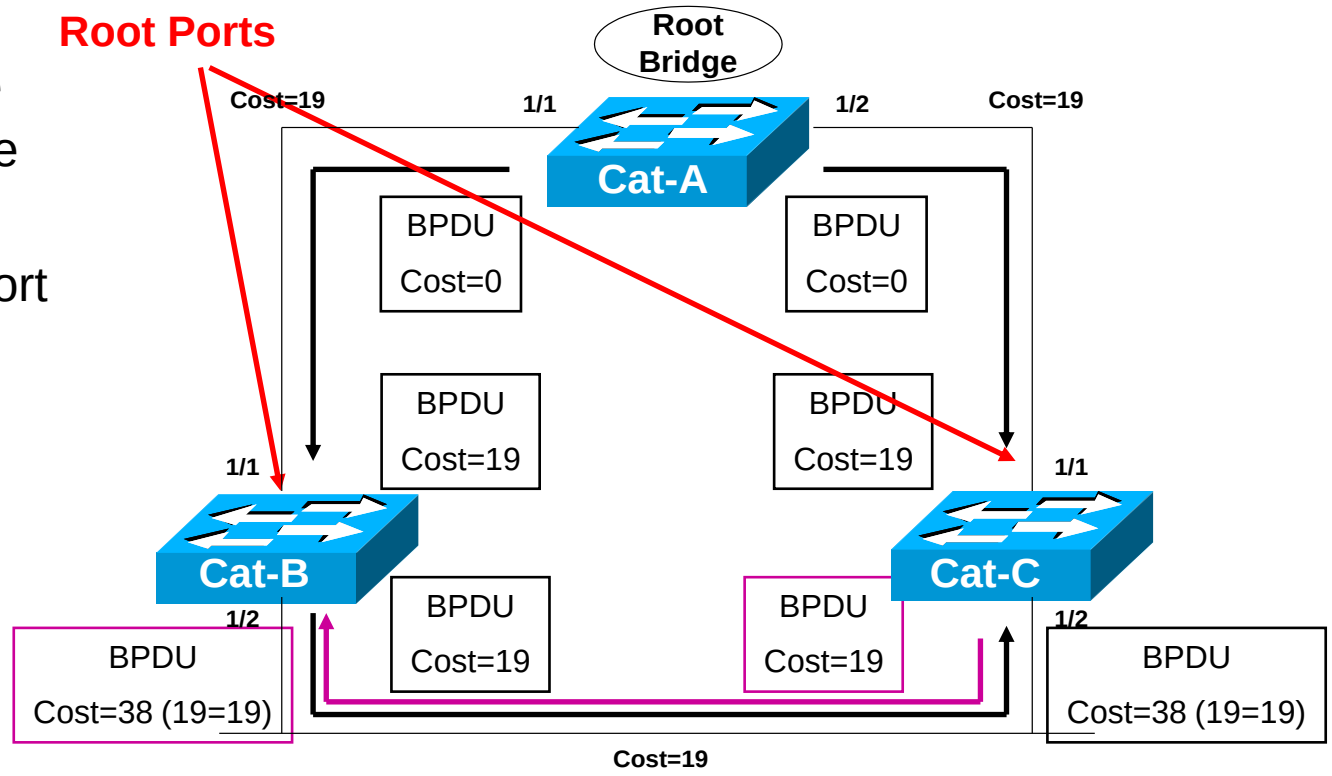
- Meme chose avec Cat-C et Cat-B.



STP: Elect root ports

Step 5

- Cat-B doit choisir entre joindre le Root Bridge avec un coût de 19 via Port 1/1, ou un coût de 38 via Port 1/2
- Port 1/1 devient le Root Port pour Cat-B, le port le plus proche au Root switch
- Cat-C fera un calcul similaire.



- Four-Step decision Sequence
  1. Lowest BID (Bridge Identifier)
  2. Lowest Path Cost to Root Bridge
  3. Lowest Sender BID
  4. Lowest Port ID (Identifier)

Three Steps of Initial STP Convergence

STP Convergence

Step 1 Elect one Root Bridge

Step 2 Elect Root Ports

Step 3 Elect Designated Ports

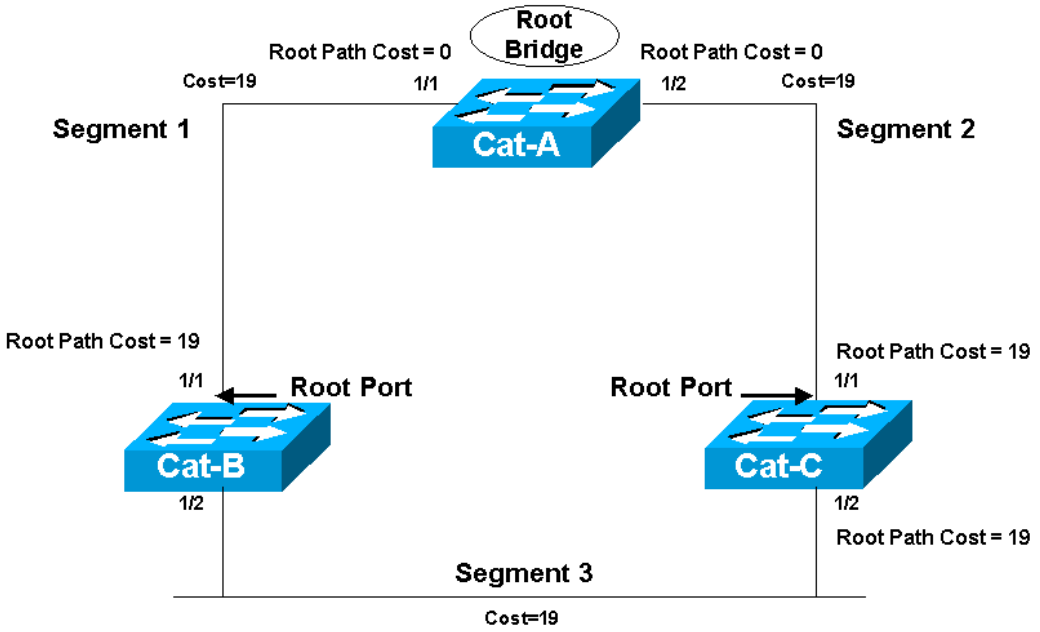
STP: Elect designated ports

- Cette étape est la plus importante pour la prévention des boucles dans le réseau

- Un Designated Port est *le port d'un lien qui a le meilleur chemin vers le Root switch*
- Le designated port est utilisé pour envoyer et recevoir le trafic depuis/vers le root switch.

- Chaque lien (entre deux nœuds) dans un réseau a un seul designated port
  - Choisi, comme dans les cas précédents, en minimisant le Root Path Cost vers le Root Bridge

- Le switch qui contient le Designated Port s'appelle Designated switch (pour le lien considéré).

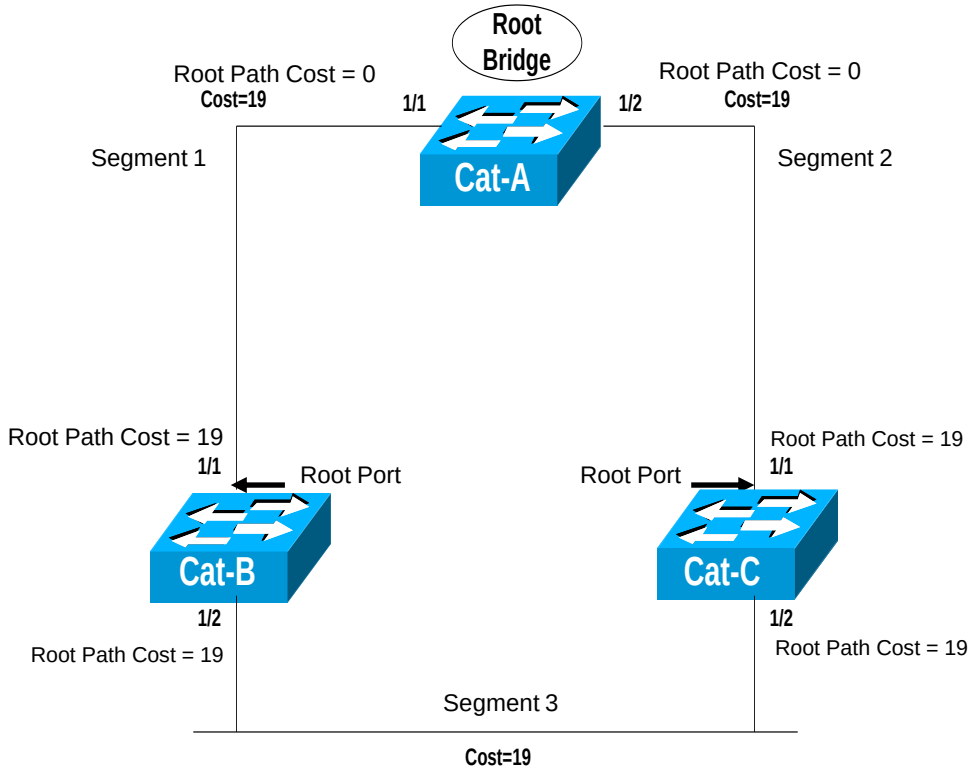


STP: Elect designated ports

- **Segment 1**:
- Root Path Cost Cat-A:1/1 = 0
- Root Path Cost Cat-B:1/1 = 19

- **Segment 2**:
- Root Path Cost Cat-A:1/2 = 0
- Root Path Cost Cat-C:1/1 = 19

- **Segment 3**:
- Root Path Cost Cat-B:1/2 = 19
- Root Path Cost Cat-C:1/2 = 19
- *It's a tie!*



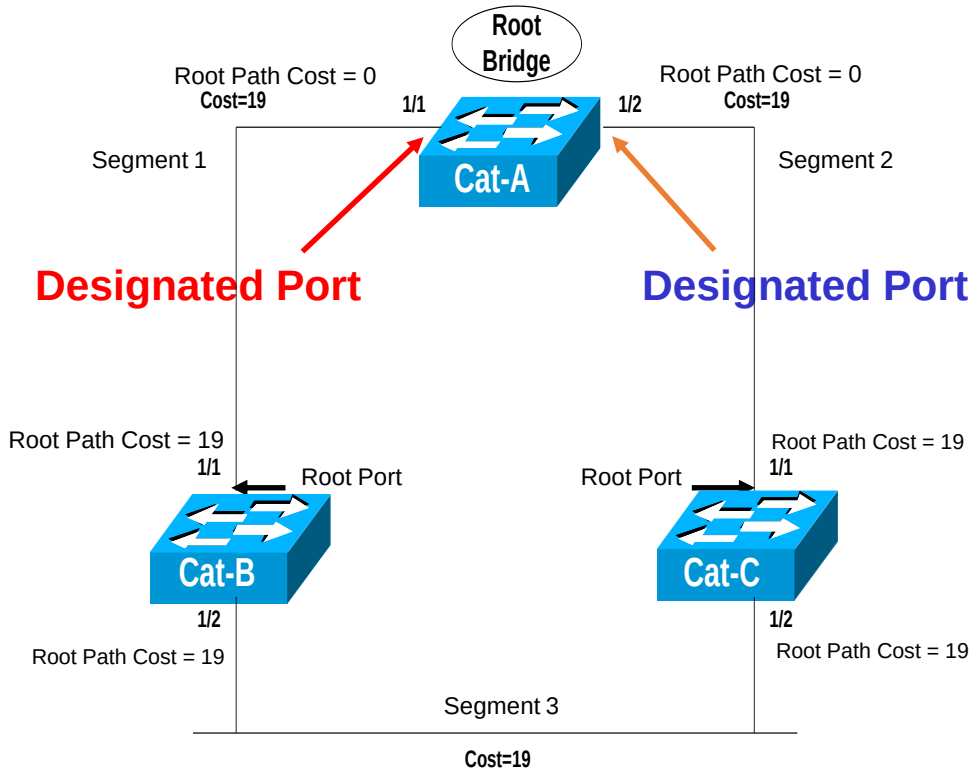
STP: Elect designated ports

Segment 1

- Comme Cat-A:1/1 a le meilleur Root Path Cost, il sera choisi comme Designate Port pour le Segment 1

Segment 2

- Comme Cat-A:1/2 a le meilleur Root Path Cost, il sera choisi comme Designated Port pour le Segment 2



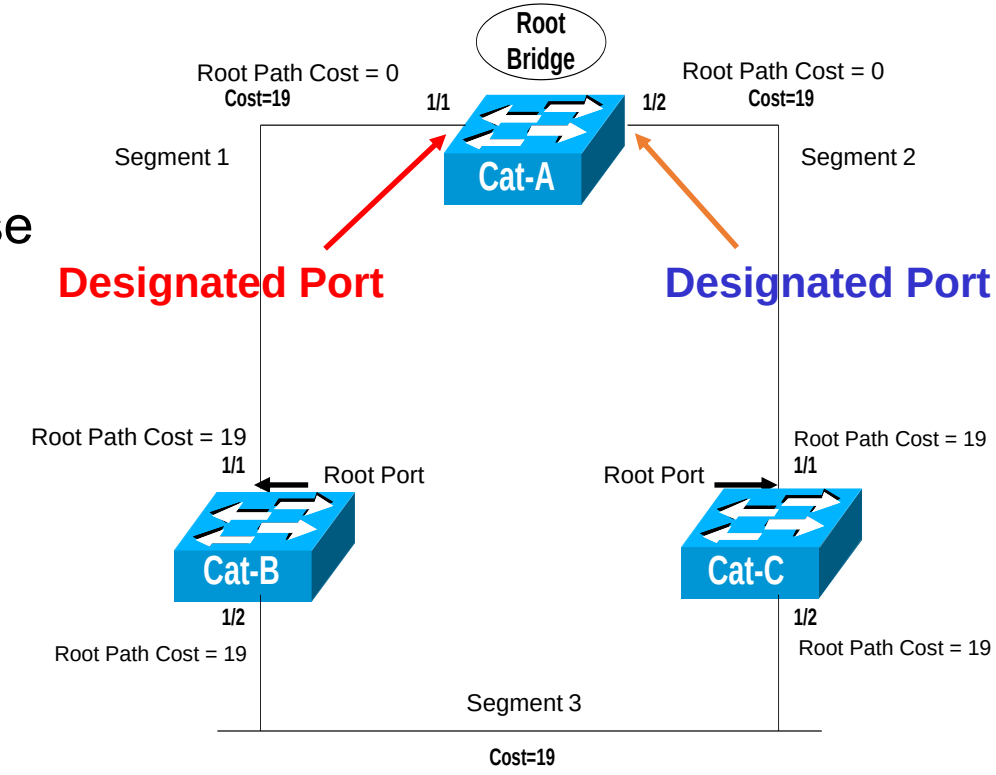
STP: Elect designated ports

Segment 3

Cat-B and Cat-C ont un Root Path Cost de 19, il faudra un bris d'égalité!

- À l'occurrence de situation d'égalité le protocole STP utilise toujours l'algorithme en quatre étapes déjà rencontré

  - Four-Step decision Sequence
    1. Lowest BID (Bridge Identifier)
    2. Lowest Path Cost to Root Bridge
    3. Lowest Sender BID
    4. Lowest Port ID (Identifier)

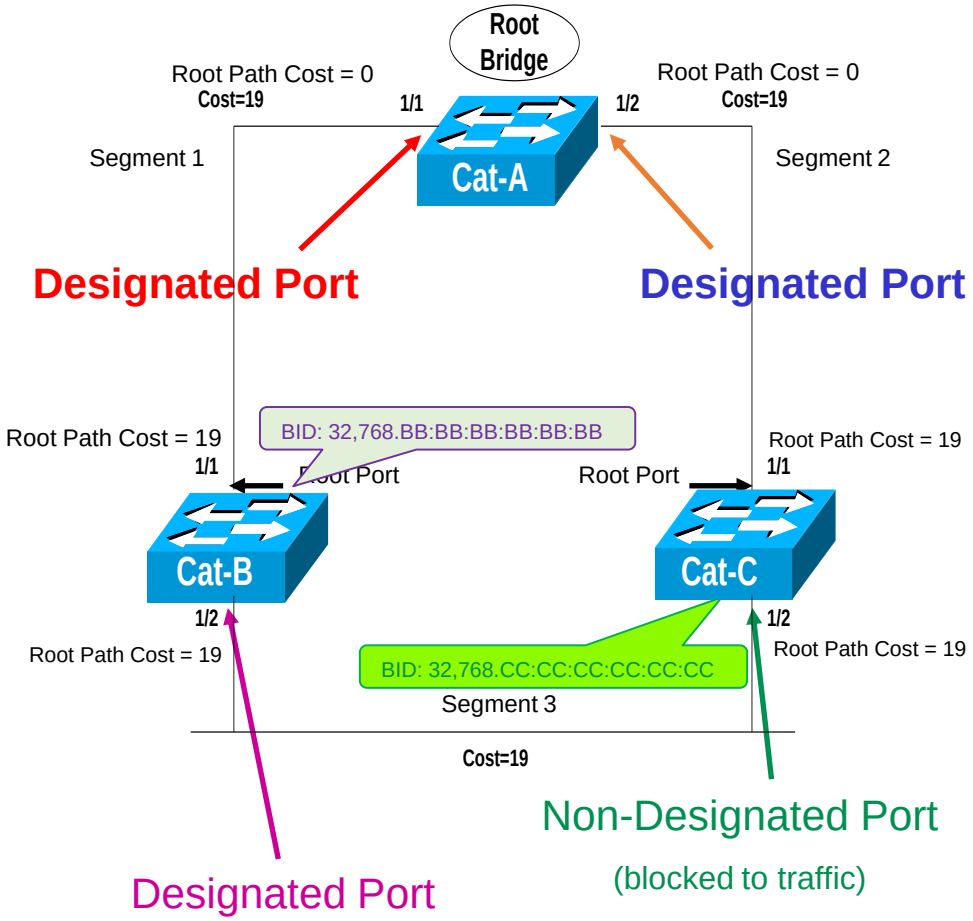


STP: Elect designated ports

- Four-Step decision Sequence
  1. Lowest BID (Bridge Identifier)
  2. Lowest Path Cost to Root Bridge
  3. Lowest Sender BID
  4. Lowest Port ID (Identifier)

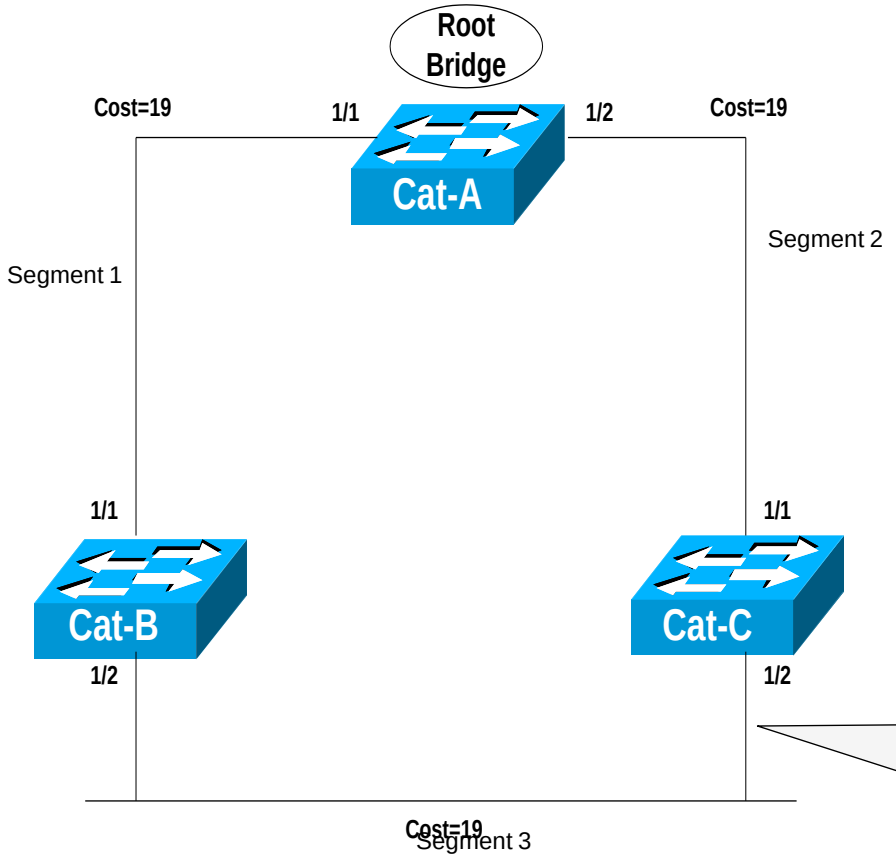
Segment 3

1. Tous noeuds sont d'accord que Cat-A est Root Bridge
   - tie: go to step 2
2. Root Path Cost pour Cat-B et CAT-C est 19
   - tie: go to step 3
3. Le BID est plus petit sur Cat-B que sur Cat-C → Cat-B: Port 1/2 sera le Designated Port pour le Segment 3



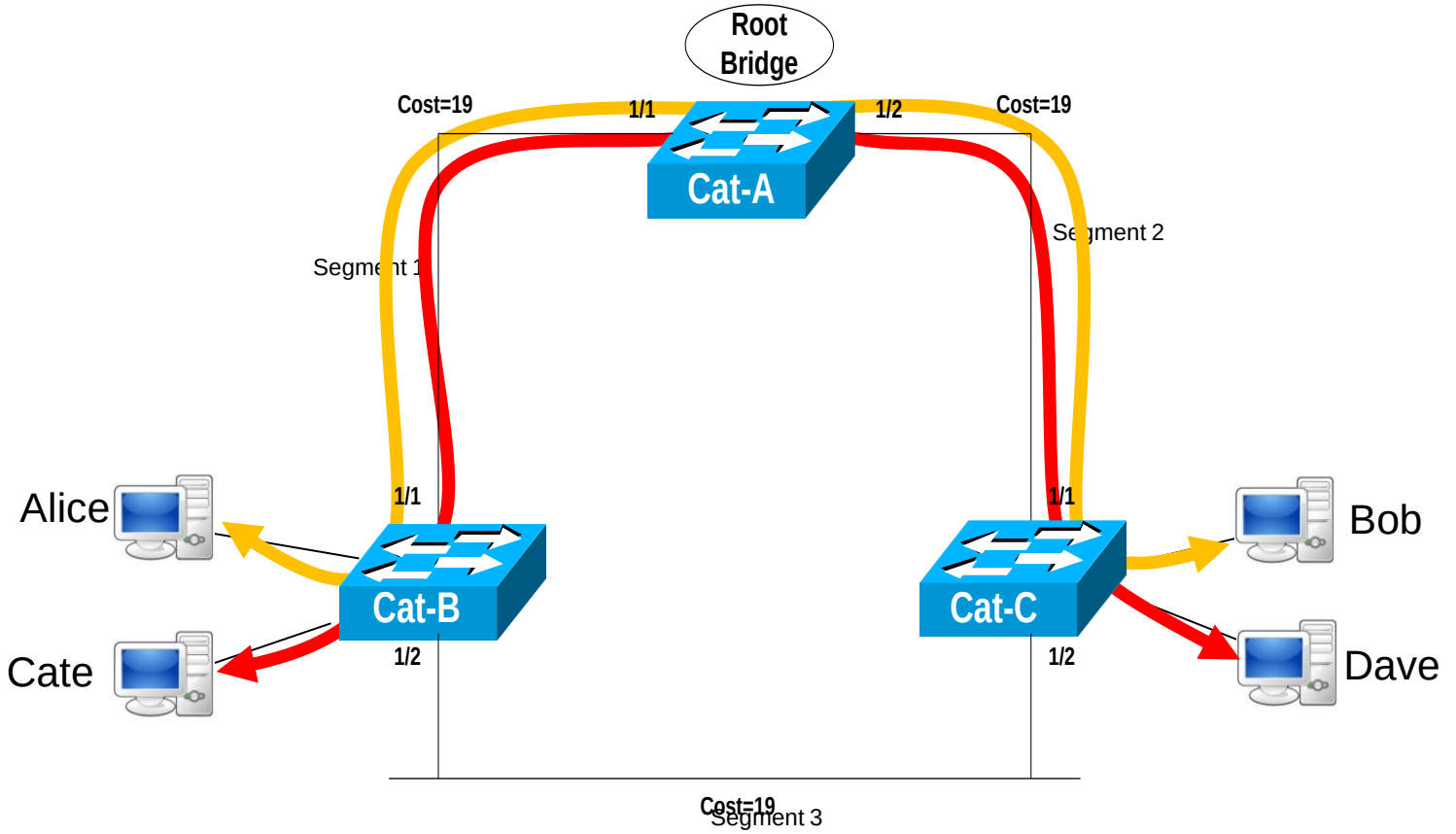
Note: Cat-C:1/2 sera non-Designated Port pour le Segment 3 |non-designated = bloqué

The network after convergence of STP



Les non-designed ports sont bloqués sur le segment 3 → non-connecté à Cat-C

STP drawback



À cause de le perte de connexion du segment 3, les couples <Alice,Bob> et <Cate, Dave> doivent partager la bande passante des segments 1 & 2, et pourtant le Segment 3 reste inutilisé !

TELECOM Paris

IP PARIS

- **MATERIAL FOR ETHERNET AND SPANNING TREE**
- **BONAVENTURE –** Ch. 3.19.2 “Ethernet”
- **DORDAL –** Ch. 2.5 “Spanning Tree”

- **Questions?**

Wireless networks: 802.11

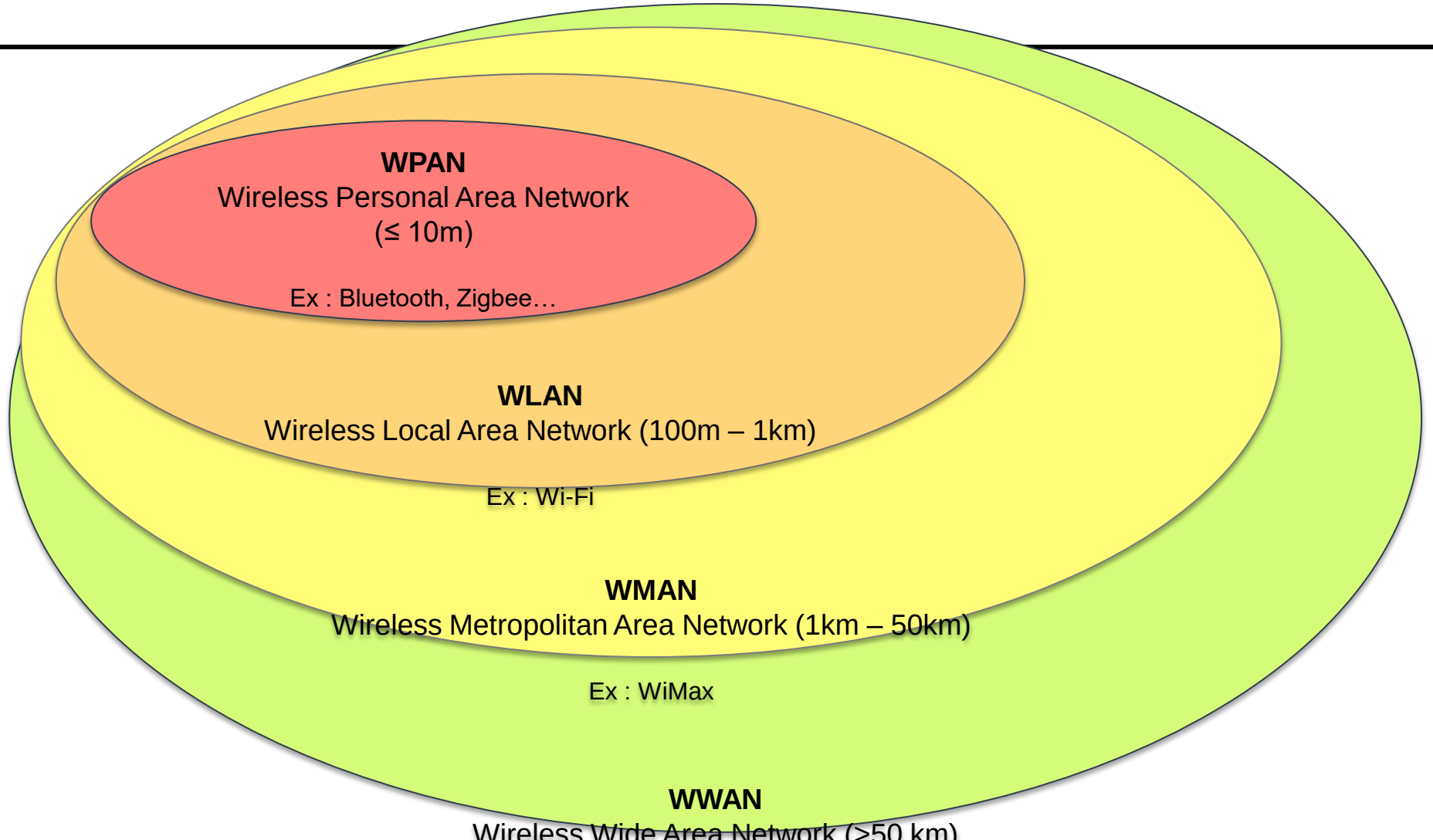
Application des réseaux sans fil

- Mobilité
  - Dans la zone de couverture
  - Handover (changement de point d'accès)

- Installation
  - Rapide et simple pour l'utilisateur
  - Même en environnement particulier (câblage impossible)

- Nouveaux équipements
  - Téléphones
  - Tablettes
  - Imprimantes
  - Internet of Things (IoT)
  - …

Taxonomie des réseaux sans fil



63

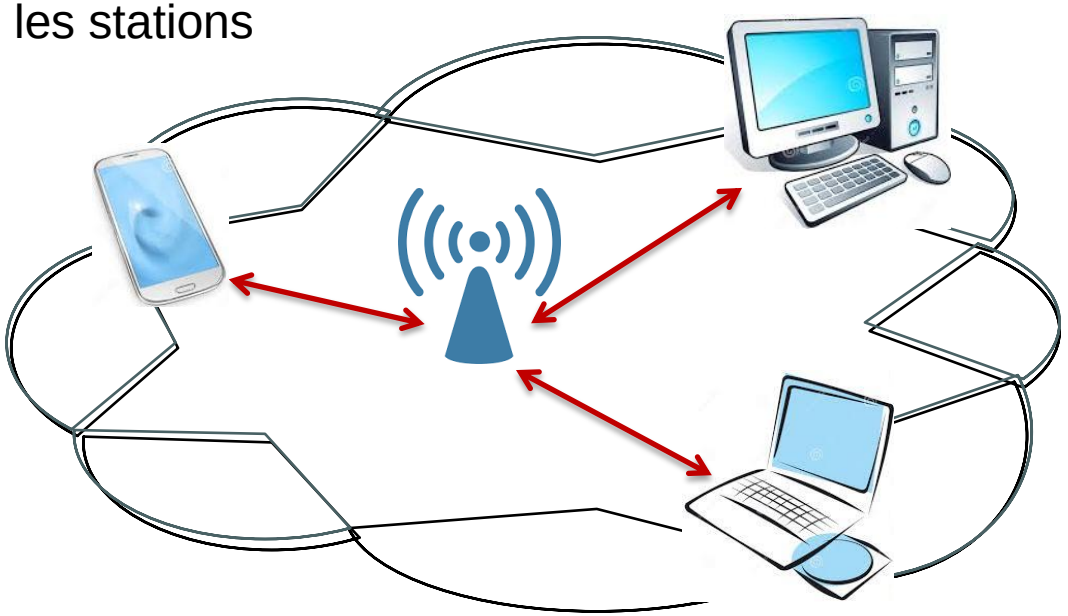
Acces à un média sans fil

- Accès multiple
  - Chaque utilisateur dispose d'une portion du canal
  - Division du canal
    - En fréquence (FDMA, OFDMA)
      - (Orthogonal) Frequency Division Multiple Access
    - En temps (TDMA)
      - Time Division Multiple Access
    - En code (CDMA)
      - Code Division Multiple Access

- Accès aléatoire
  - Les utilisateurs utilisent le même canal à tour de rôle de manière aléatoire quand ils ont un paquet à transmettre
  - Tirage d'un instant d'utilisation
    - Aloha
  - Ecoute avant (et non pendant) l'utilisation du canal
    - CSMA/CA
      - CSMA/Collision Avoidance

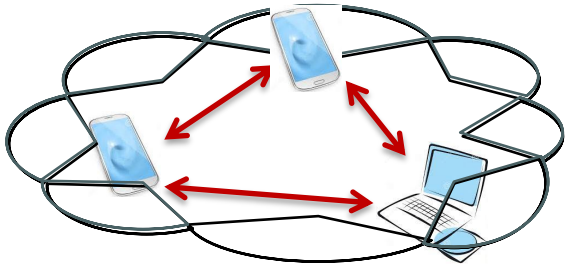
Architecture

- BSS
  - Basic Service Set
  - Il existe un point d’accès (AP)
  - Toutes les communications passent par l’AP
  - La bande passante est partagée entre toutes les stations

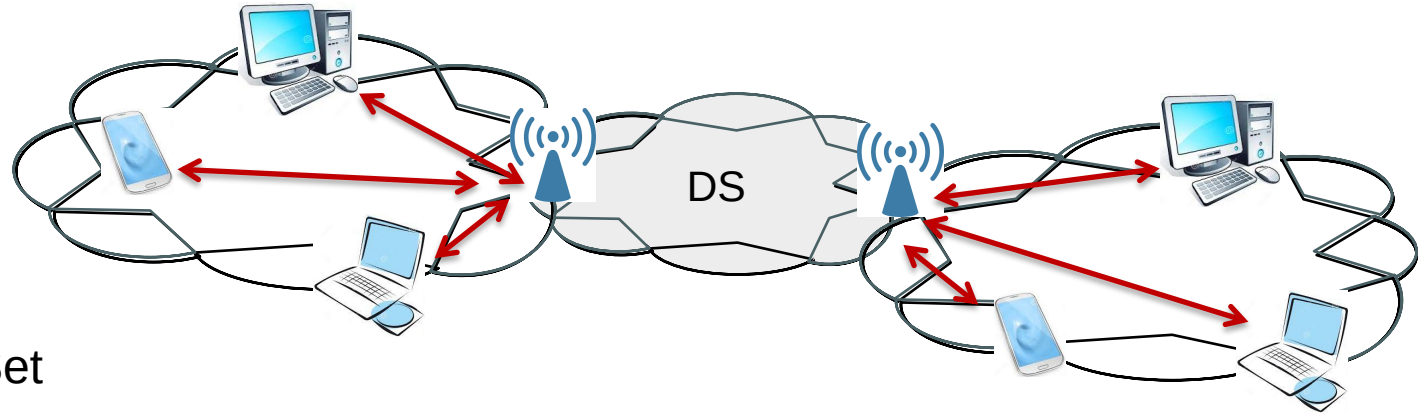


Architecture

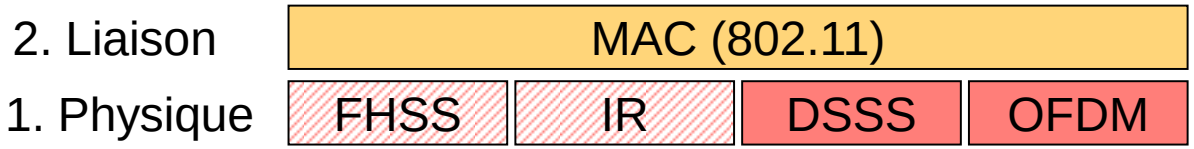
- IBSS
  - Independent Basic Service Set
  - Réseau Ad-Hoc



- ESS
  - Extended Service Set
  - Chaîne de BSS reliés par un système de distribution (DS)



Protocol stack



FHSS: Frequency Hopping Spread Spectrum

IR: InfraRed

DSSS: Direct Sequence Spread Spectrum

OFDM: Orthogonal Frequency Division Multiplexing

MAC: Medium Access Control

- **Une seule couche MAC**
  - Norme 802.11
- **Plusieurs couches PHY**
  - Normes 802.11a, b, g, n, ac
  - FHSS et IR uniquement dans la norme d'origine (1997)

MAC Layer: DCF (Distributed Coordination Function)

- Nécessité
  - Un terminal ne peut écouter et émettre en même temps
    - Détection de collisions impossible
    - On ne peut pas utiliser CSMA/CD

- DCF
  - Technique de contrôle d'accès de la norme 802.11
  - CSMA/CA (obligatoire)
    - Carrier Sense Multiple Access with Collision Avoidance
  - RTS-CTS (optionnel)
    - Request To Send
    - Clear To Send

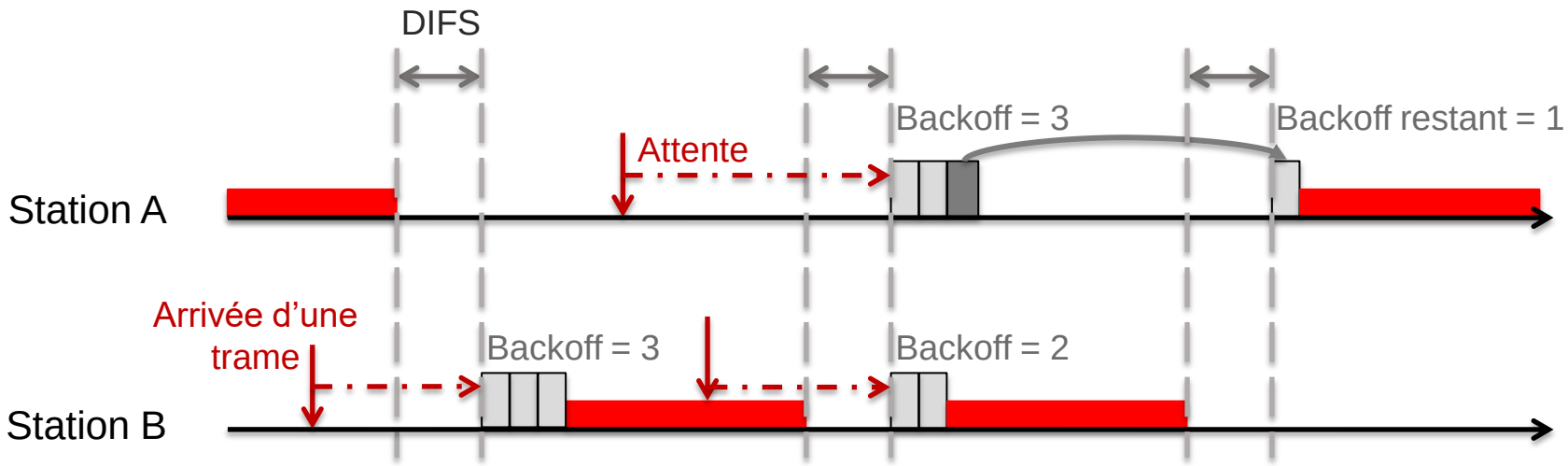
- Alternatives
  - PCF (Point Coordination Function)
    - La gestion du partage du canal est centralisé au point d'accès
    - Très peu implémenté
  - HCF (Hybrid Coordination Function)
    - Période dédiée où le canal est réservé pour le trafic avec QoS (Quality of Service)

CSMA/CA | Delay

- Carrier Sense Multiple Access with **Collision Avoidance**
- Principe
  - On écoute avant d'émettre
  - Quand le medium est libre, on attend un délai fixe avant d'émettre
    - DIFS (DCF Inter-Frame Space) : délai minimal avant toute transmission

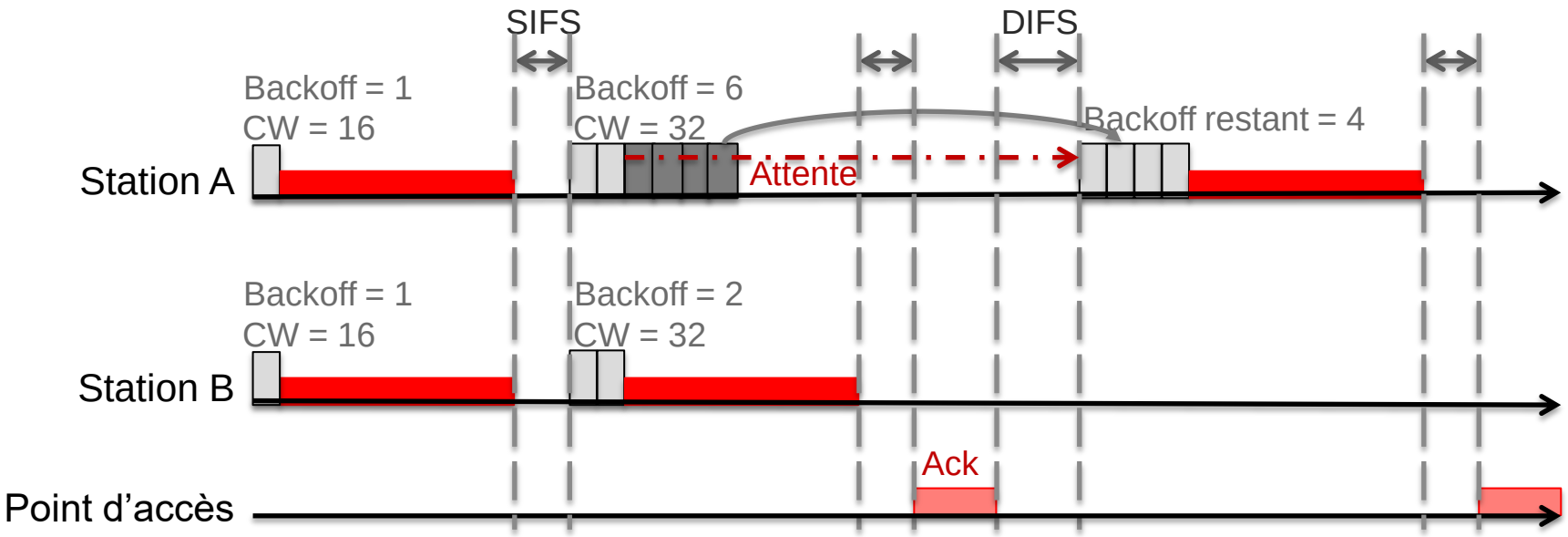
CSMA/CA | Backoff et Contention Window (CW)

- Principe
  - Quand le medium se libère après avoir été occupé, on attend un délai aléatoire avant d'émettre (après le délai fixe)
    - Le backoff est tirée aléatoirement dans une fenêtre de contention (CW)
    - La taille initiale de la fenêtre de contention est de 16 (2 en CSMA/CD)
    - La valeur du backoff est reportée au prochain essai en cas de perte de la contention
  - On attend un délai aléatoire entre deux trames successives
    - Backoff permettant de laisser l'accès au medium aux autres stations



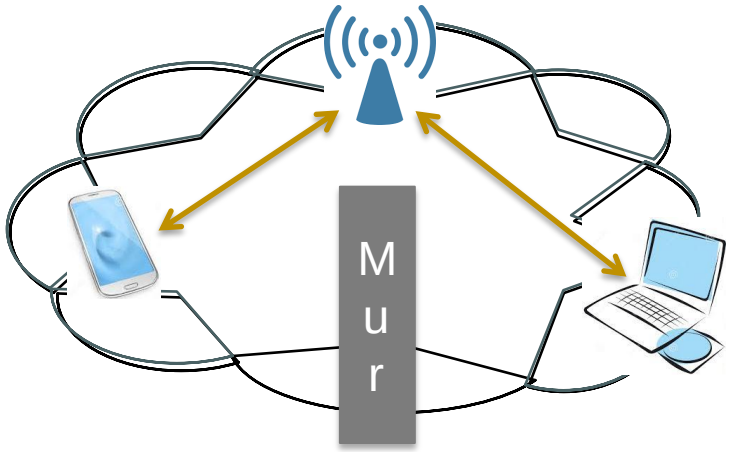
CSMA/CA | Ack and retransmissions

- Principe
  - Toutes les trames (sauf broadcast) sont acquittées
    - SIFS (Short Inter-Frame Space) : délai entre une trame et son acquittement
    - En l'absence d'acquittement :
      - Retransmission de la trame
      - La taille de la fenêtre de contention double (jusqu'à 1024)
      - Suppression de la trame après un nombre de retransmissions maximum



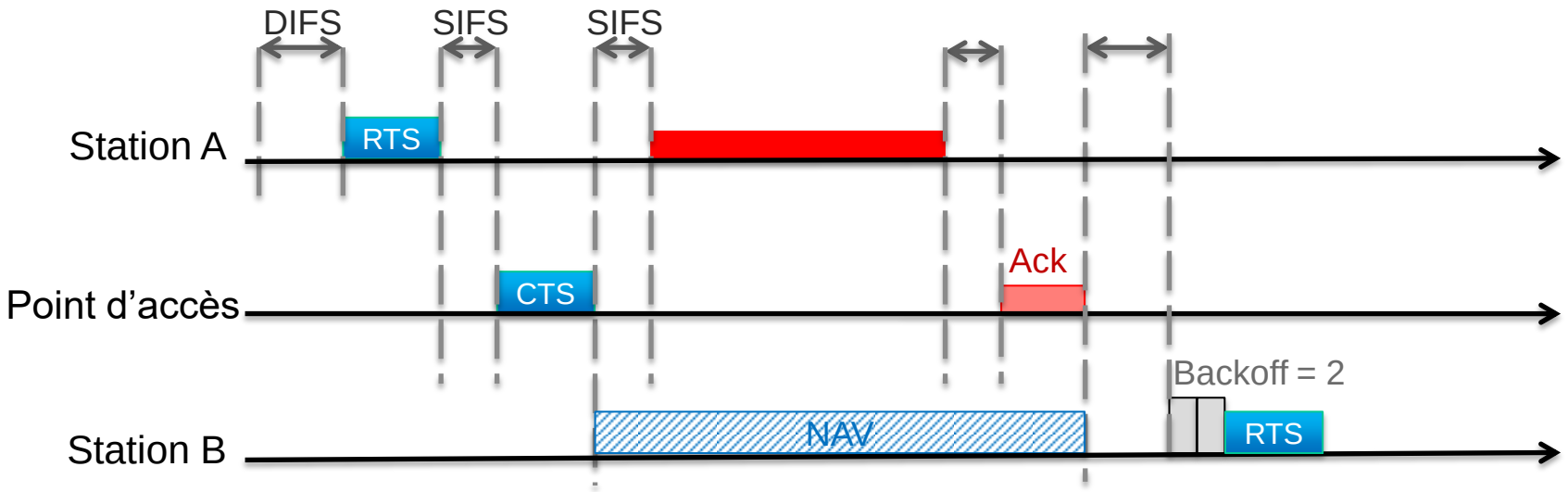
Hidden terminal

- Problèmes
  - Si deux stations peuvent ne pas entendre leurs signaux
    - Séparées par un mur
    - De part et d'autre du point d'accès
  - Collision possible au niveau du point d'accès
  - L'écoute et l'attente ne suffisent pas pour éviter les collisions
  - Si les trames sont longues
    - Collisions à répétition
    - Coûteuses à re-émettre



RTS and CTS

- Mécanisme
  - L'émission de données est précédée par un échange de trames courtes
  - RTS (Request To Send)
    - L'émetteur envoie au récepteur une demande d'autorisation d'envoi
    - Contient le temps estimé de la transmission
  - CTS (Clear To Send)
    - Le récepteur autorise l'émetteur à envoyer
    - Contient le temps estimé de la transmission
    - Canal en diffusion : toutes les stations du réseau voient le message CTS
  - NAV (Network allocation Vector)
    - Les stations voisines attendent pendant le temps estimé de l'envoi de la trame
    - « Virtual carrier sensing » (vs « Physical carrier sensing »)



Pairing with a Wi-Fi network

- SSID
  - Service Set Identifier
  - « Nom du réseau »
  - Le point d'accès et les stations doivent avoir le même SSID pour s'associer
  - Diffusé en clair périodiquement (balise / beacon)
    - Possibilité de désactiver l'émission périodique
  - Diffusé en clair dans la trame d'association
- Étapes
  - Écoute (« scanning »)
    - Connaître le canal du point d'accès
    - Synchronisation fréquentielle puis temporelle
  - Association
    - Requête d'association
    - Réponse par une trame « probe » contenant le SSID
  - Allocation d'une adresse IP
  - Authentification optionnelle

Wireless security

- WiFi Protected Access

- Principe
  - Clé unique pour toutes les stations en mode personnel
  - Authentification par utilisateur en mode entreprise
  - Chiffrement par flot TKIP (Temporal Key Integrity Protocol) dans WPA
    - Utilisation de RC4 (Rivest Cipher 4) avec une clé périodiquement modifiée et un vecteur d'initialisation haché
  - Chiffrement par bloc CCMP/AES dans WPA2
    - CCMP: Counter Mode Cipher Block Chaining Message Authentication Code Protocol
    - AES: Advanced Encryption Standard
  - Intégrité vérifiée par MIC (Message Integrity Code)

Questions?

- **MATERIAL FOR THE Wireless**
- **BONAVENTURE –** Ch. 3.19.3 “802.11 wireless networks”
- **DORDAL –** Ch. 4.2 “WiFi” excluding 4.2.8