

COURS #4

Data Link (L2), partie 2

Introduction aux réseaux 2025 (Bloc 2)

Corentin Badot-Bertrand

Rappels & mise en contexte

Quelques rappels sur le cours précédent avant de commencer



Dans l'épisode précédent

Nous avons découvert la couche Data Link (OSI L2) :

- Adresses MAC
- Broadcast & multicast
- Protocole Ethernet
- Hub, bridge et switch



7. Application

6. Presentation

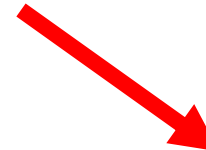
5. Session

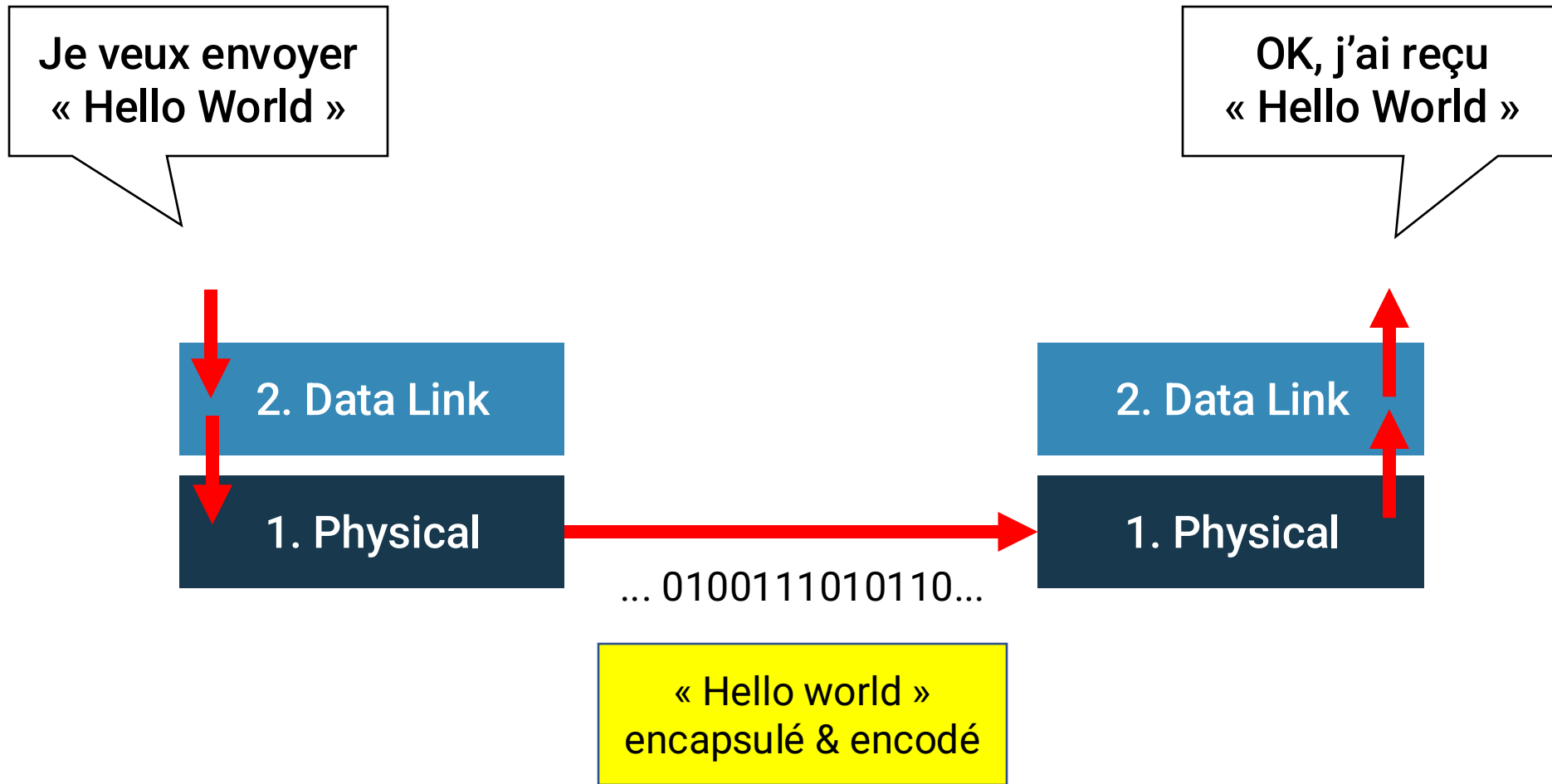
4. Transport

3. Network

2. Data Link

1. Physical





Questions
pour un
Champion



**Quelles sont les
responsabilités de la
couche Data Link ?**

Les responsabilités de Data Link

Effectuer une gestion du trafic réseau local

- Transmettre correctement des trames (*frames*)
- Entre nœuds adjacents
- Corriger les erreurs de la couche physique
- Eviter les collisions de données au niveau local





**J'ai un switch avec 8 ports
et adresse(s) MAC.
Quel est le nombre ?**

8 adresses MAC

Une adresse MAC **identifie une interface réseau**

- Une carte réseau d'un ordinateur, puce WiFi, etc.
- Gravée dans carte
- Avec préfixe constructeur
- Possible de changer au niveau de l'OS

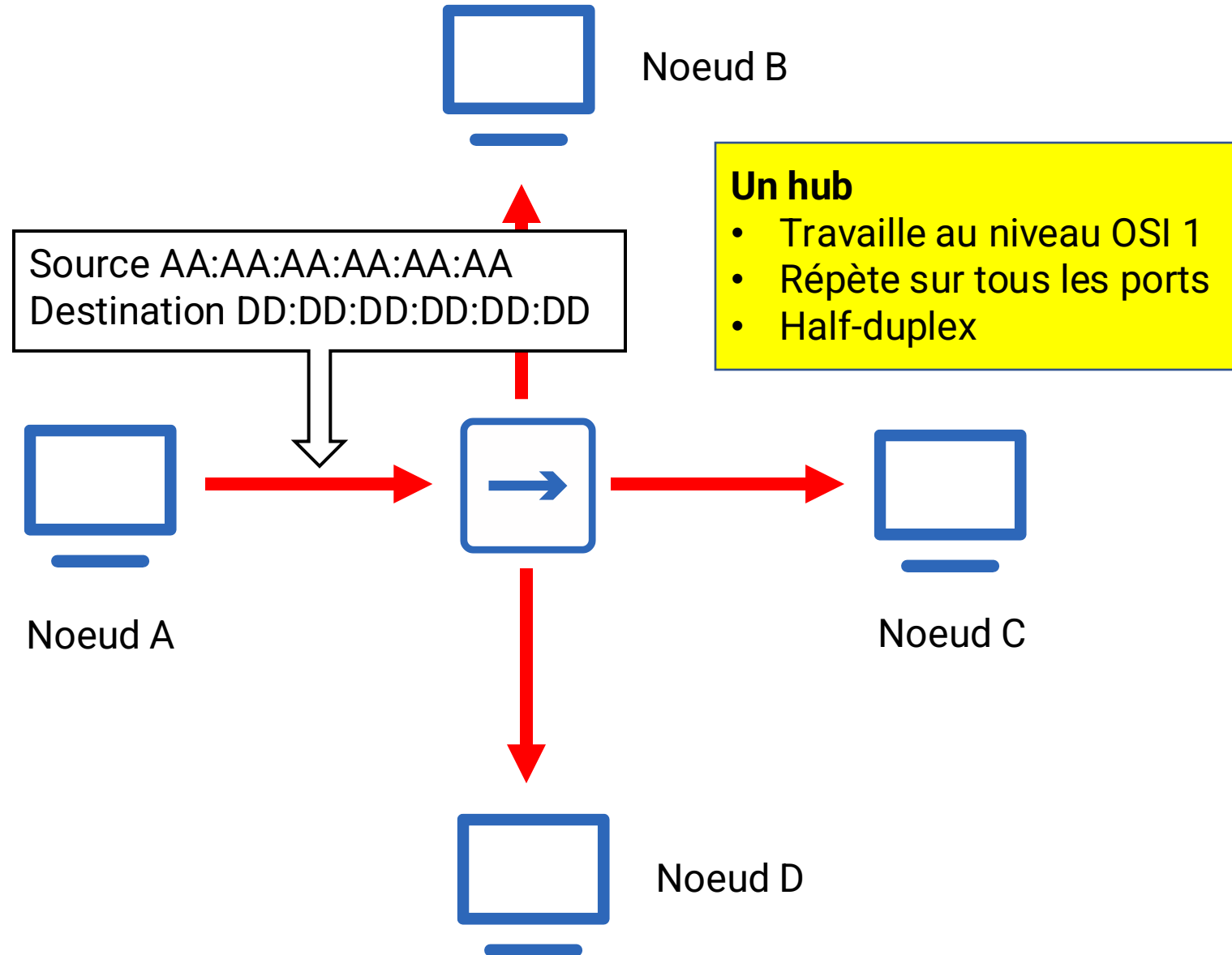
Adresses de broadcast FF:FF:FF:FF:FF:FF

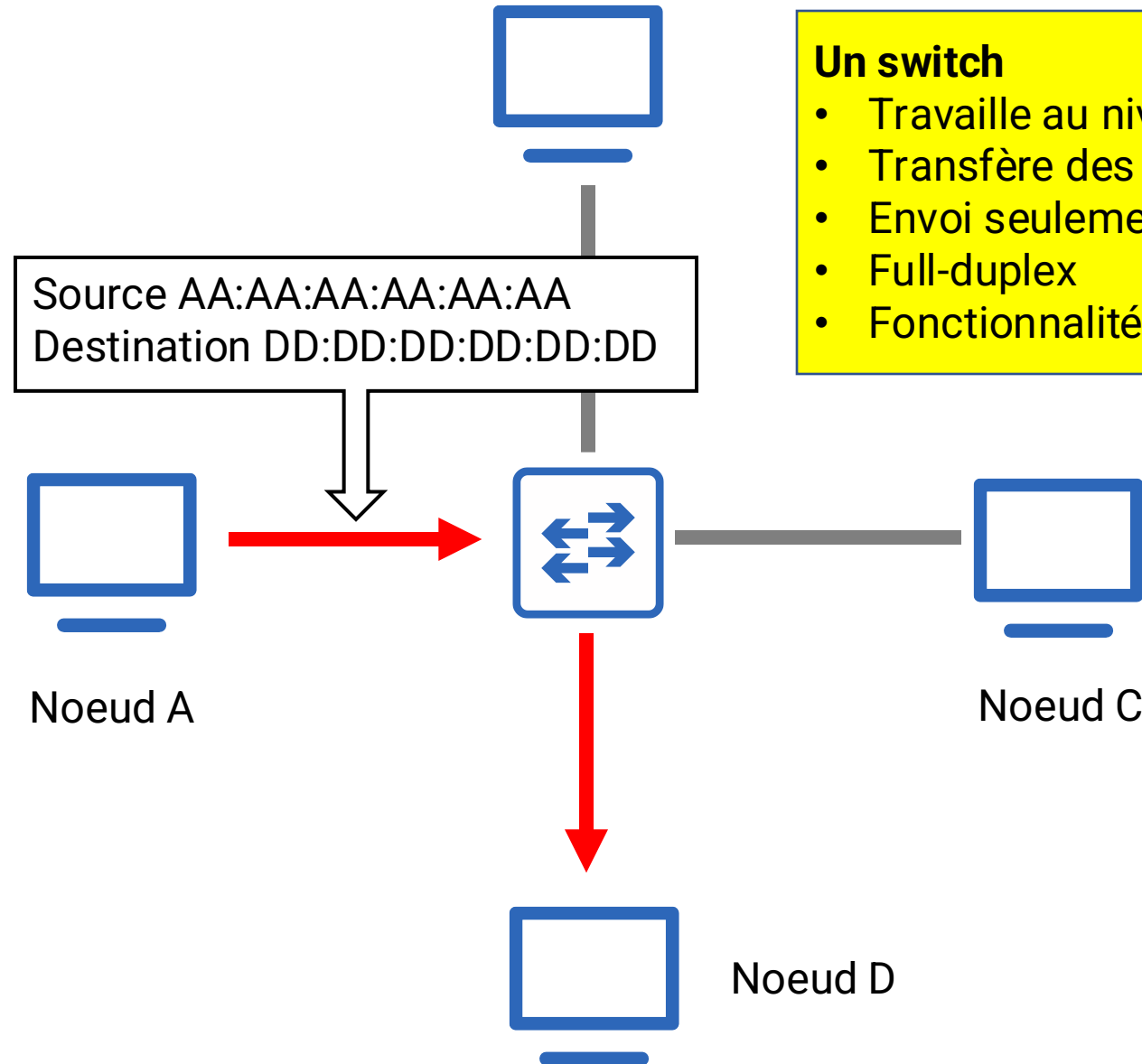


~ numéro de série d'un véhicule



**Quelle est la
différence entre un
switch et un hub ?**





Un switch

- Travaille au niveau OSI 2
- Transfère des trames Ethernet
- Envoi seulement vers destination
- Full-duplex
- Fonctionnalités avancées

PARTIE #1

Le switch en détails

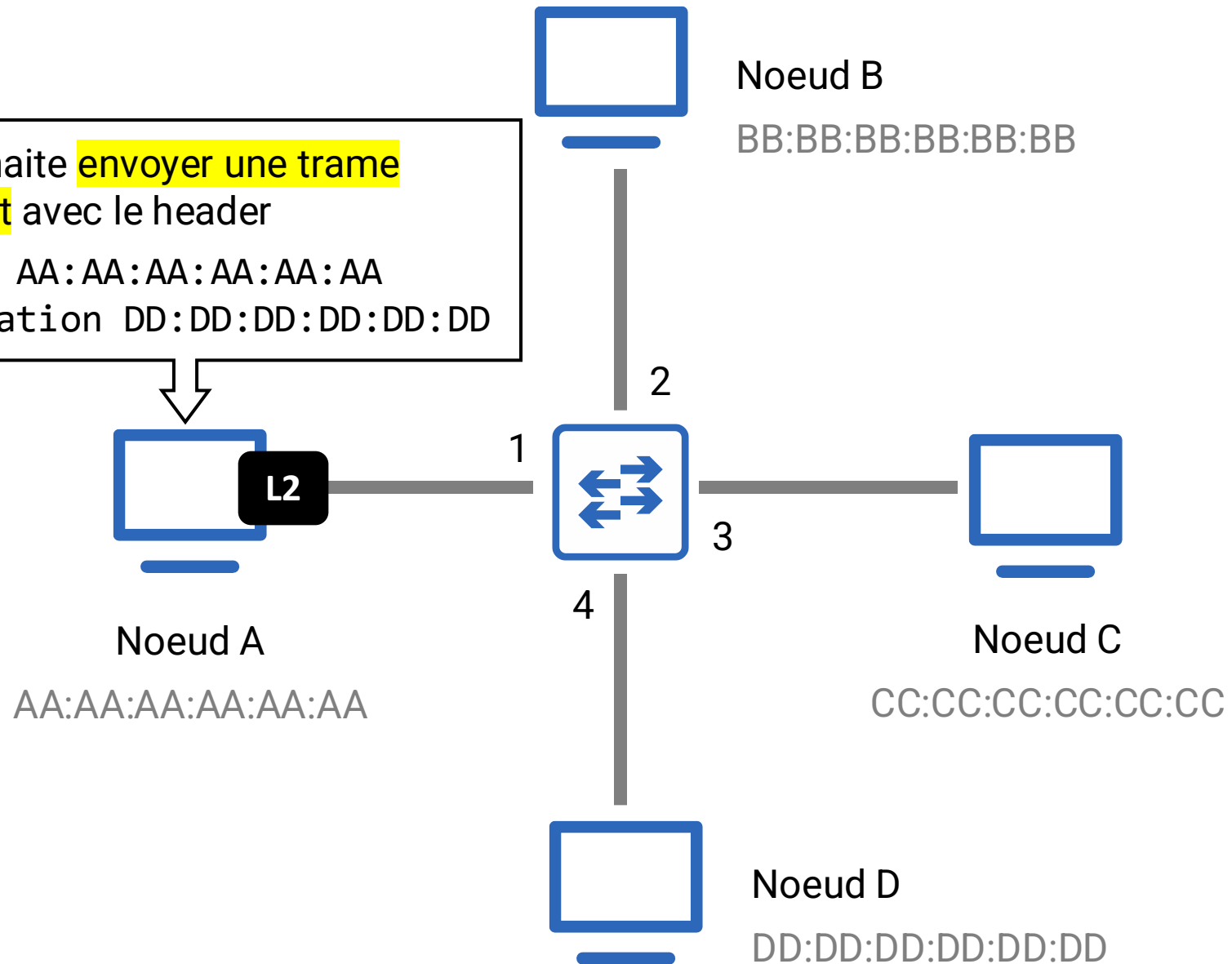
Equipement réseau indispensable,
découvrons quelques concepts avancés

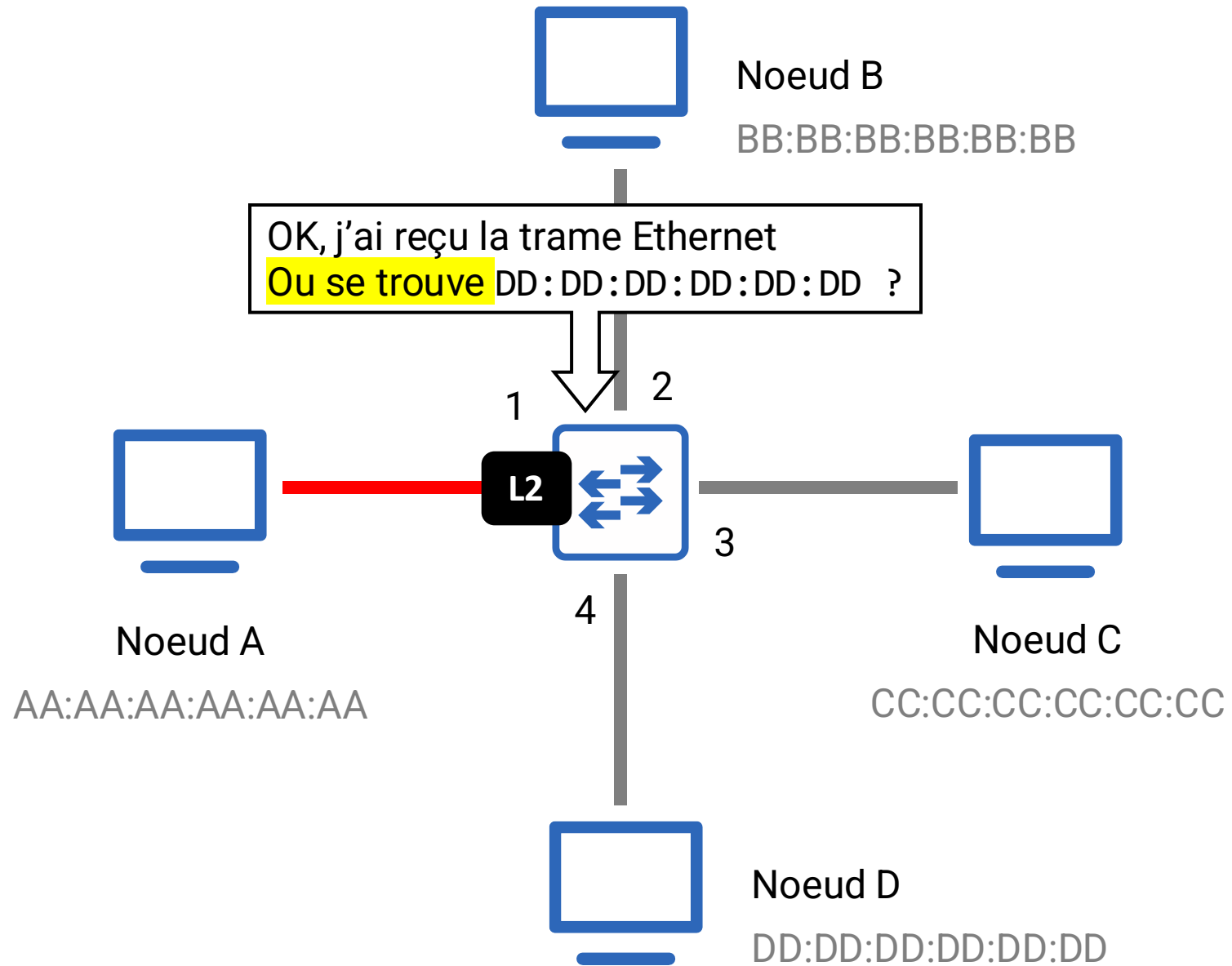


Je souhaite envoyer une trame Ethernet avec le header

Source AA:AA:AA:AA:AA:AA

Destination DD:DD:DD:DD:DD:DD







Apprentissage d'adresses

Le switch a besoin de connaître l'adresse MAC connectée sur un port

- Essentiel pour rediriger les trames Ethernet vers le bon port
- Le switch est capable d'effectuer un apprentissage
- Opération automatique, pas de configuration
- Sur base de l'adresse MAC source dans le header Ethernet

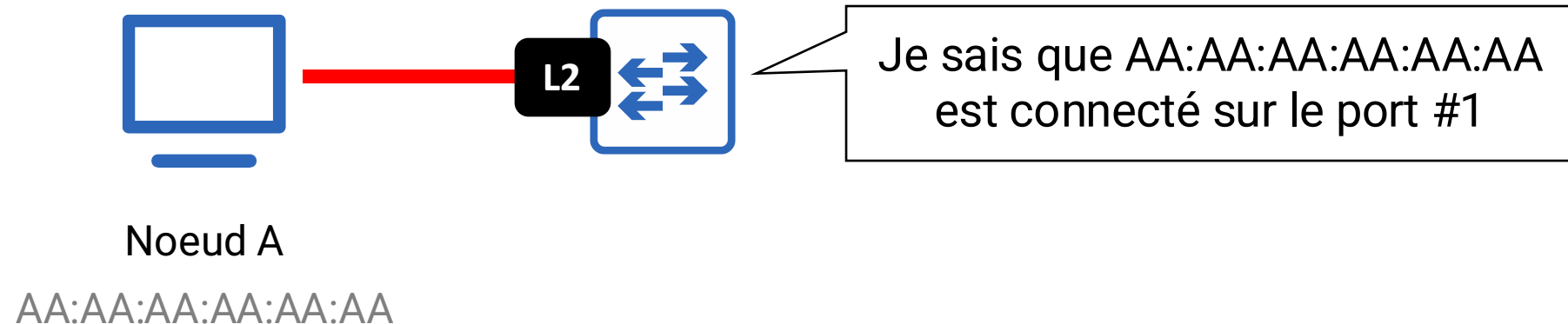


Table d'adressage

Le switch maintient une table (*forwarding database*) avec les adresses MAC connectées à ses ports

Port	Adresse MAC connectée
1	AA:AA:AA:AA:AA:AA
2	?
3	?
4	?

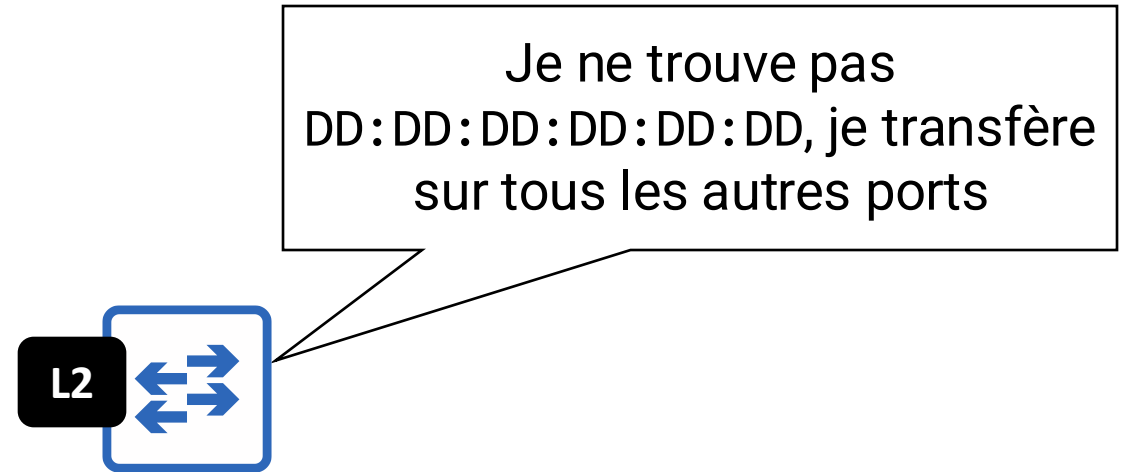


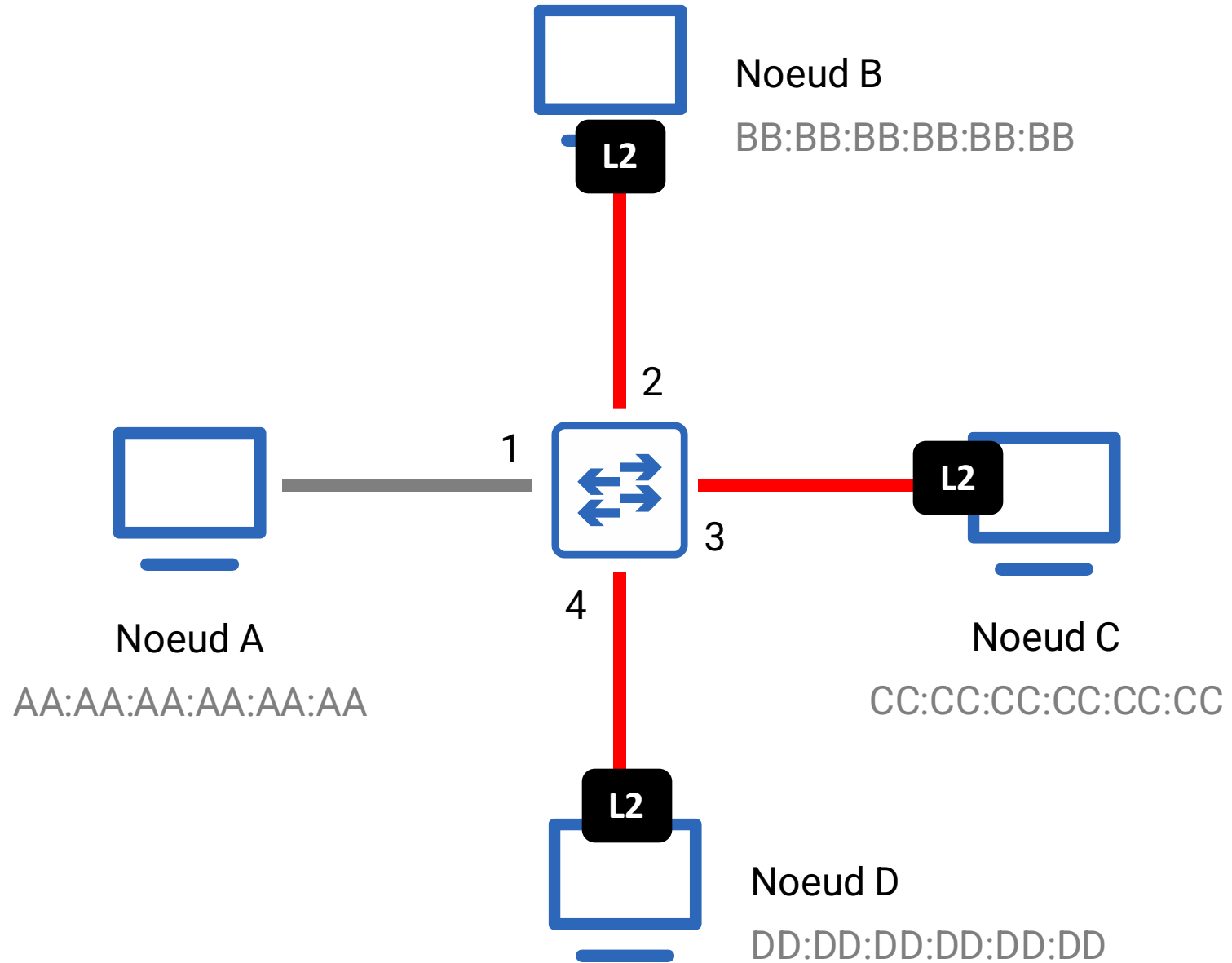
**Comment le switch peut-il
connaître le port de
DD : DD : DD : DD : DD : DD ?**

Flooding

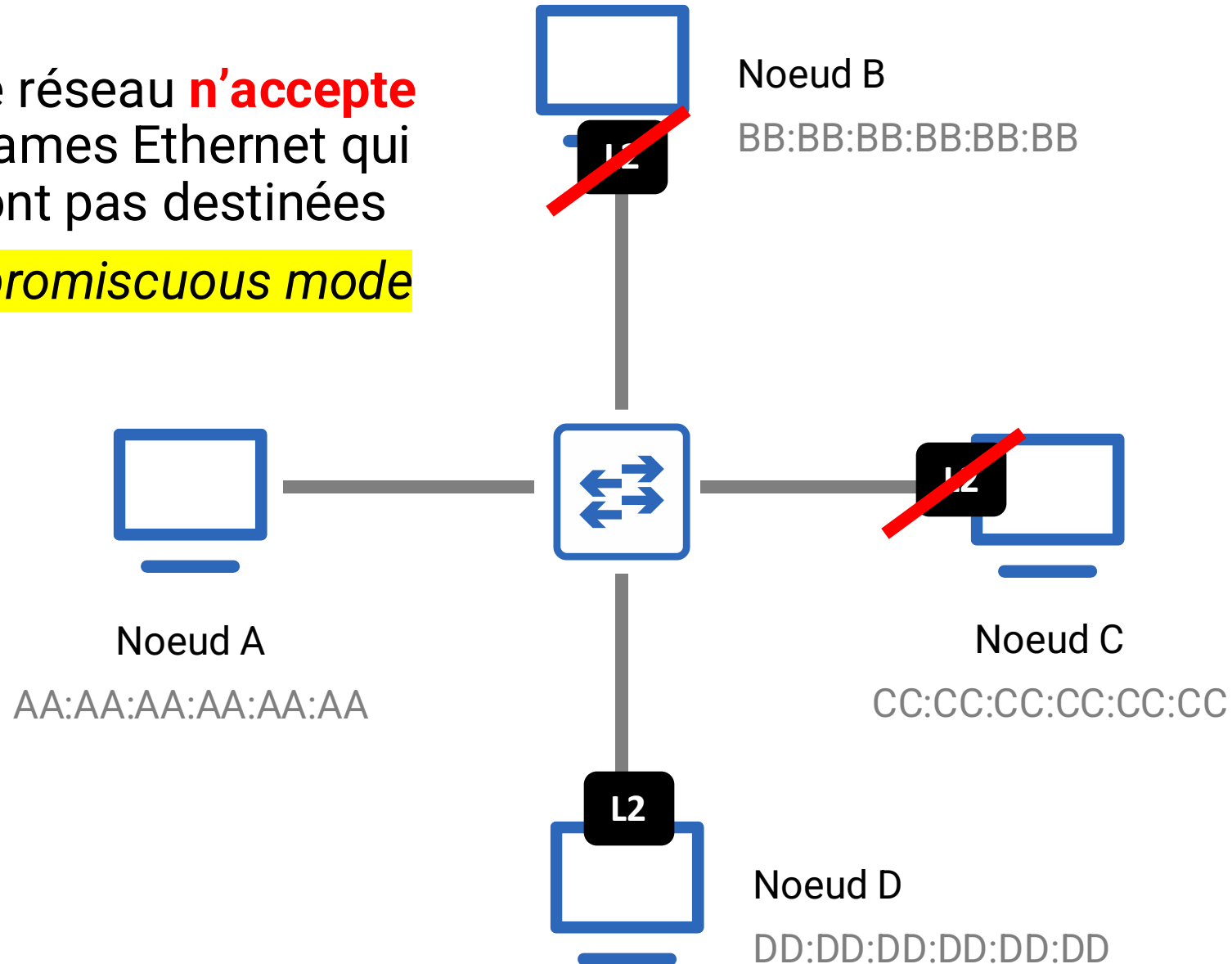
En cas d'absence de l'adresse MAC dans la table, le switch transfère sur tous les ports – sauf le port d'origine

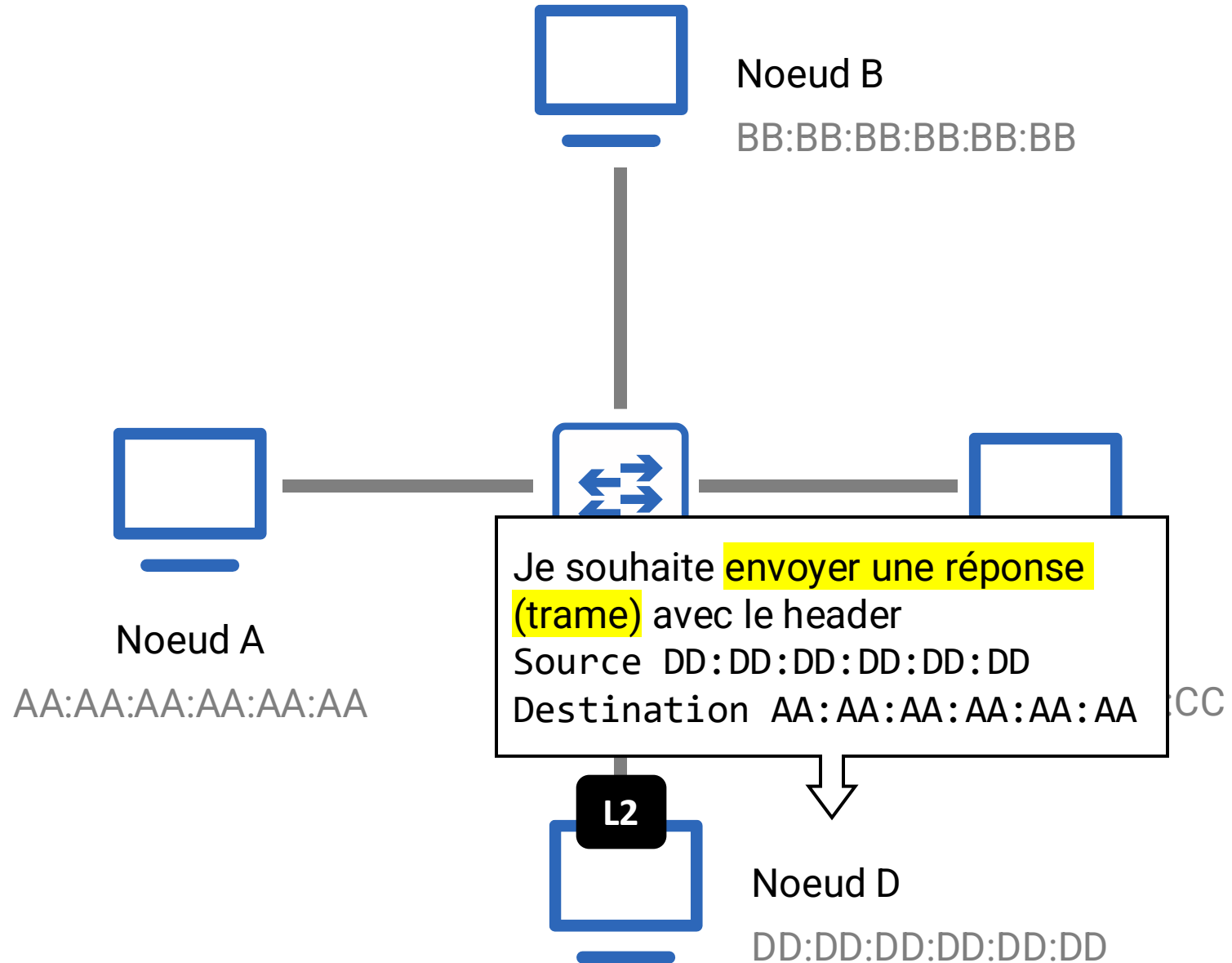
Port	Adresse MAC connectée
1	AA:AA:AA:AA:AA:AA
2	?
3	?
4	?





Une carte réseau **n'accepte pas** de trames Ethernet qui ne lui sont pas destinées
Sauf en *promiscuous mode*





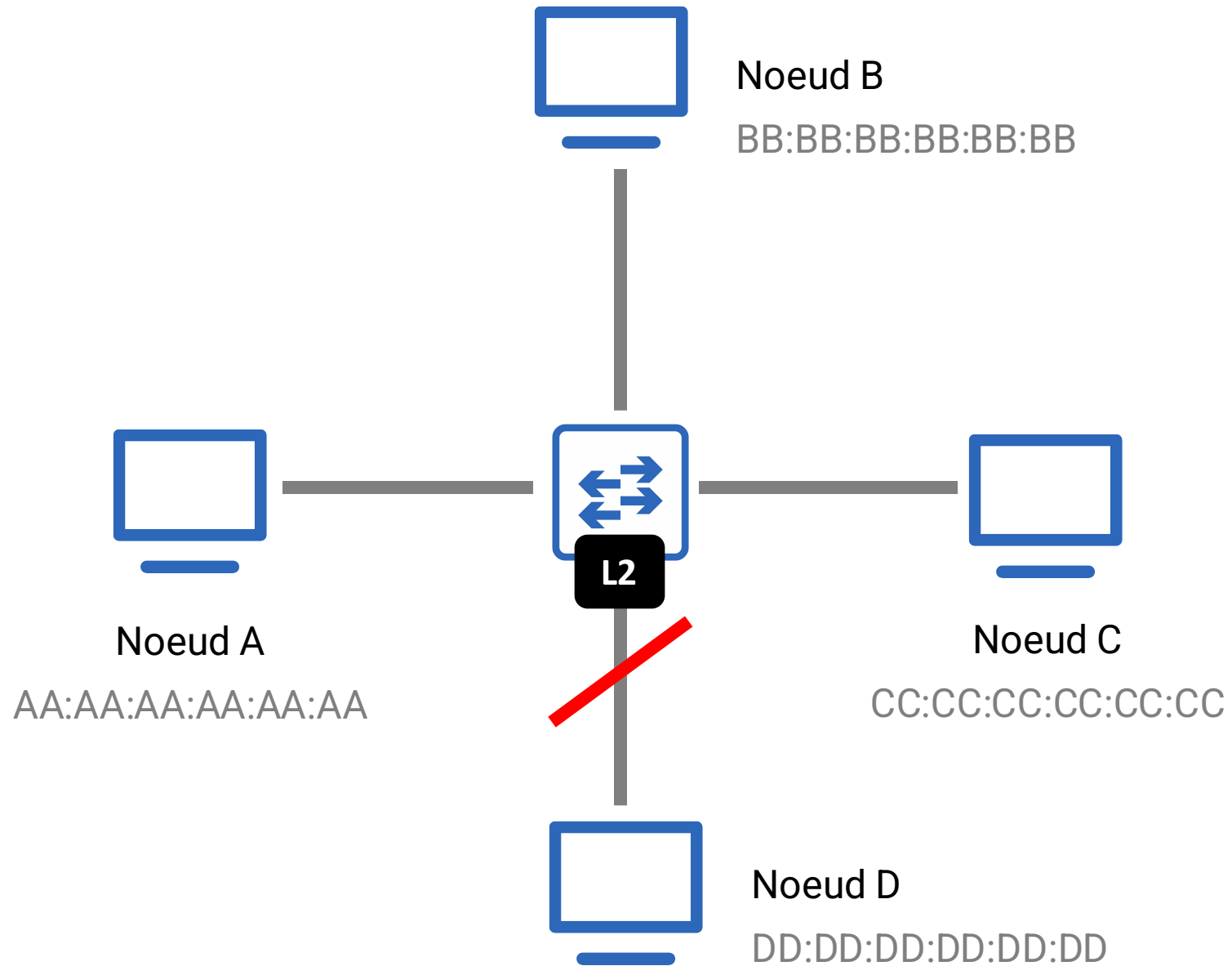
Et l'apprentissage continue...

Port	Adresse MAC connectée
1	AA:AA:AA:AA:AA:AA
2	?
3	?
4	DD:DD:DD:DD:DD:DD

Quelques règles par défaut

Le switch permet une gestion de trafic optimale dans un réseau

- Capable d'apprendre automatiquement
- Si une adresse MAC est dans la table... alors seul l'adresse recevra la trame
- Si un port est occupé, le switch est capable de mettre la **trame en attente**
- Le switch **ne modifie pas** par défaut la trame Ethernet

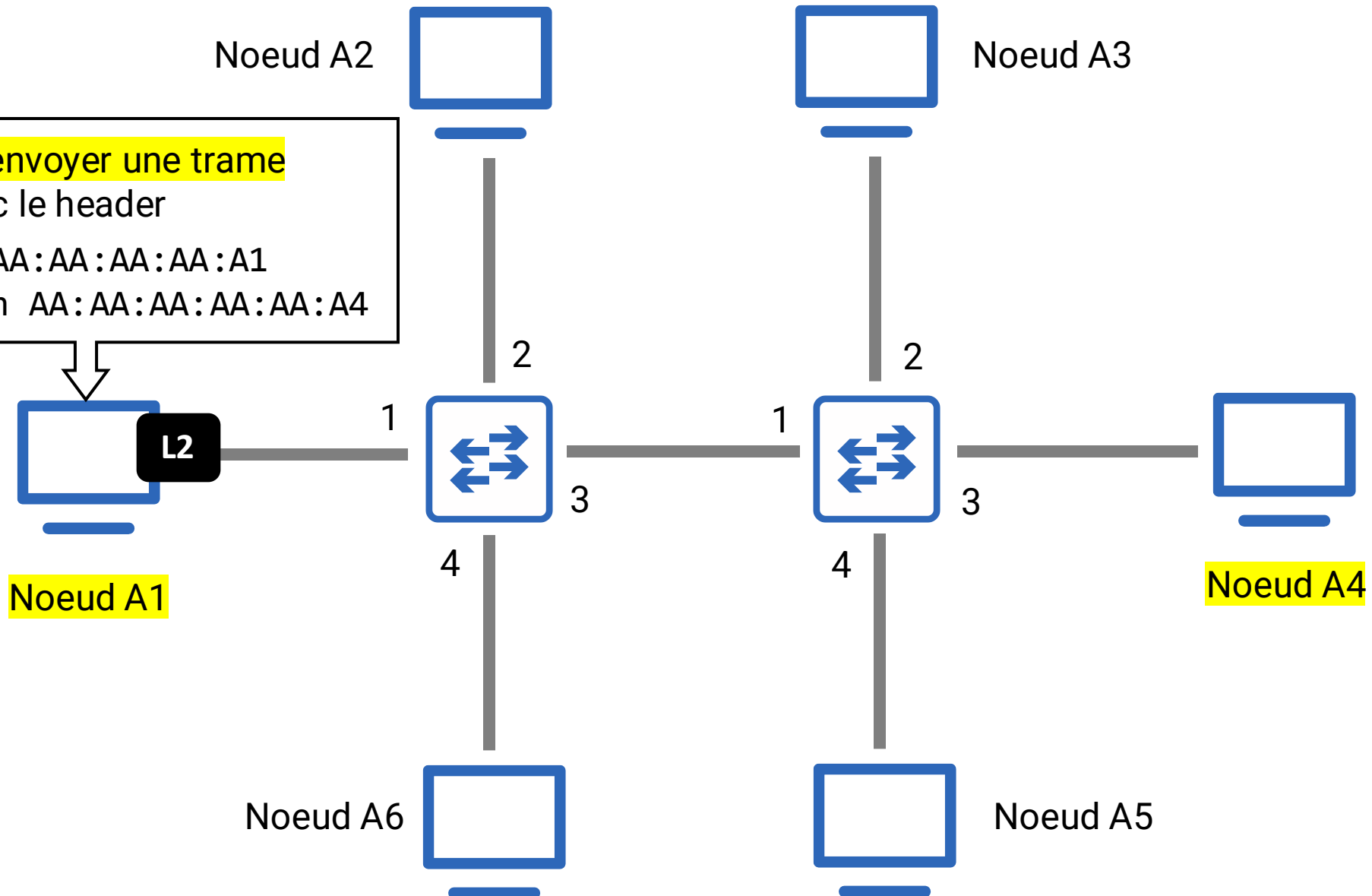


Expiration d'adresses MAC

Si une adresse MAC n'a pas été aperçue en source depuis un port pendant une durée (5 minutes par exemple), l'adresse est purgée

Port	Adresse MAC connectée
1	AA:AA:AA:AA:AA:AA
2	?
3	?
4	Adresse MAC purgée après 5m

Je souhaite envoyer une trame Ethernet avec le header
Source AA:AA:AA:AA:AA:A1
Destination AA:AA:AA:AA:AA:A4



Exemple : Switch Cisco industriel



Exemple : Switch Cisco industriel

vlan	mac address	type	port
9	000c.291e.96f0	dynamic	GigabitEthernet1/1
9	000c.293c.7cac	dynamic	GigabitEthernet1/1
9	000c.2950.e3e9	dynamic	GigabitEthernet1/1
9	000c.29ba.fe28	dynamic	GigabitEthernet1/2
9	842b.2ba6.3a7d	dynamic	GigabitEthernet1/3
9	d067.e50b.1975	dynamic	GigabitEthernet1/5
9	d067.e51e.e35a	dynamic	GigabitEthernet2/1
9	f04d.a2f6.d37b	dynamic	GigabitEthernet2/2



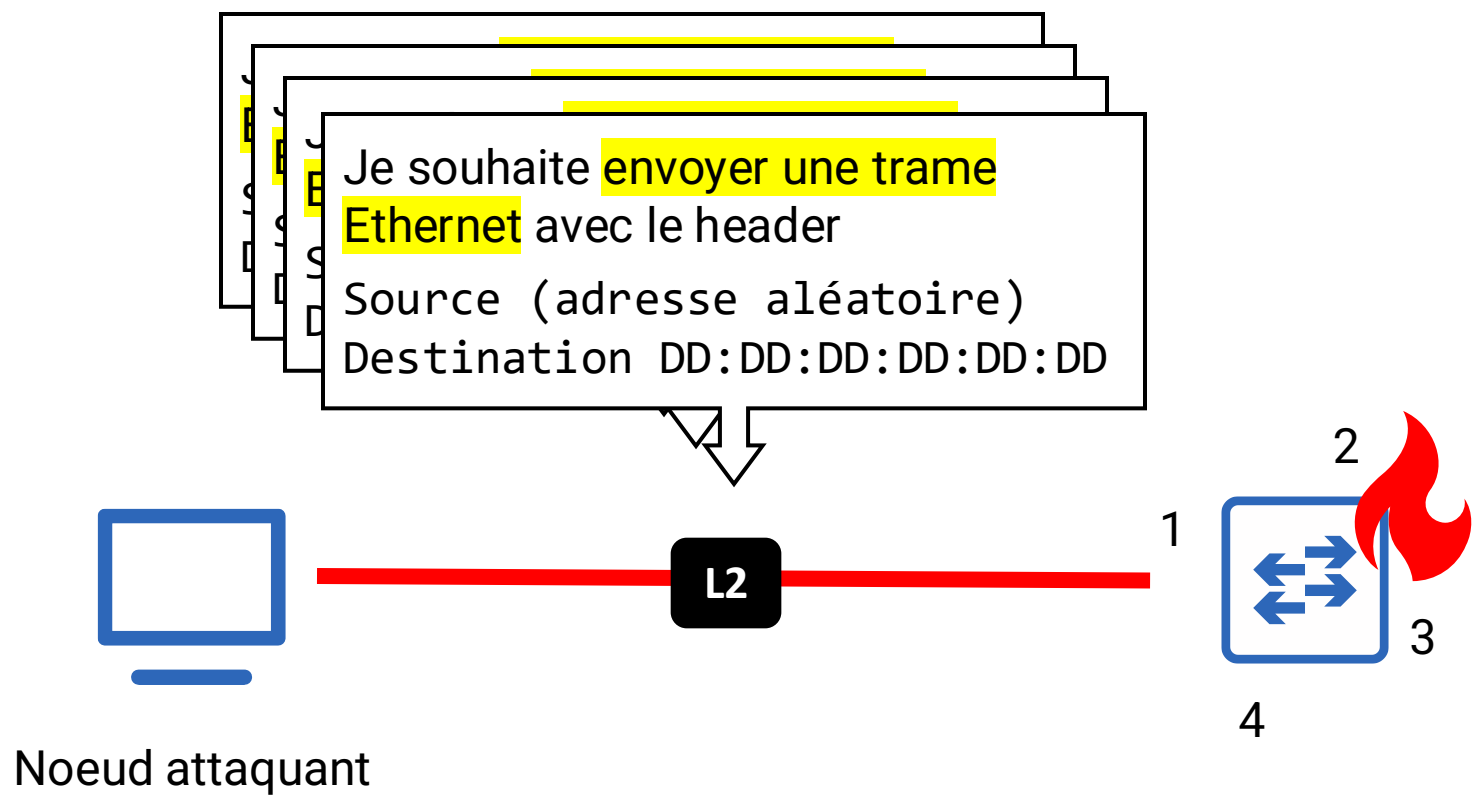
Comment attaquer un switch réseau ?

MAC flooding, l'attaque

Un switch possède une **capacité mémoire limitée**

- C'est également le cas de la *forwarding database*
- Un attaquant effectue des envois de trames
- ... avec une **adresse source différente**
- Objectif : remplir la table d'adressage
- ... et remplacer des adresses légitimes ou autre





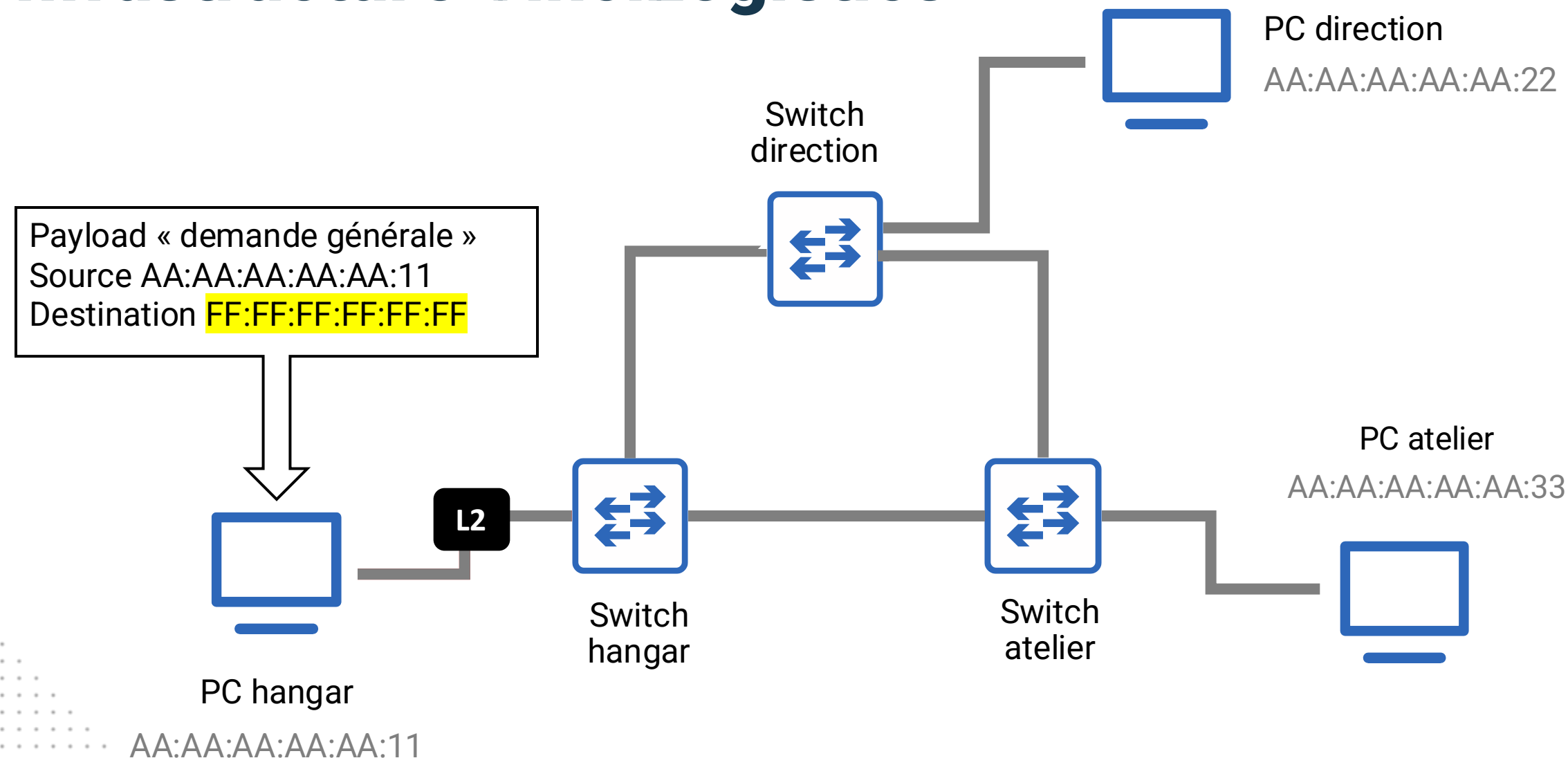
PARTIE #2

Le protocole STP

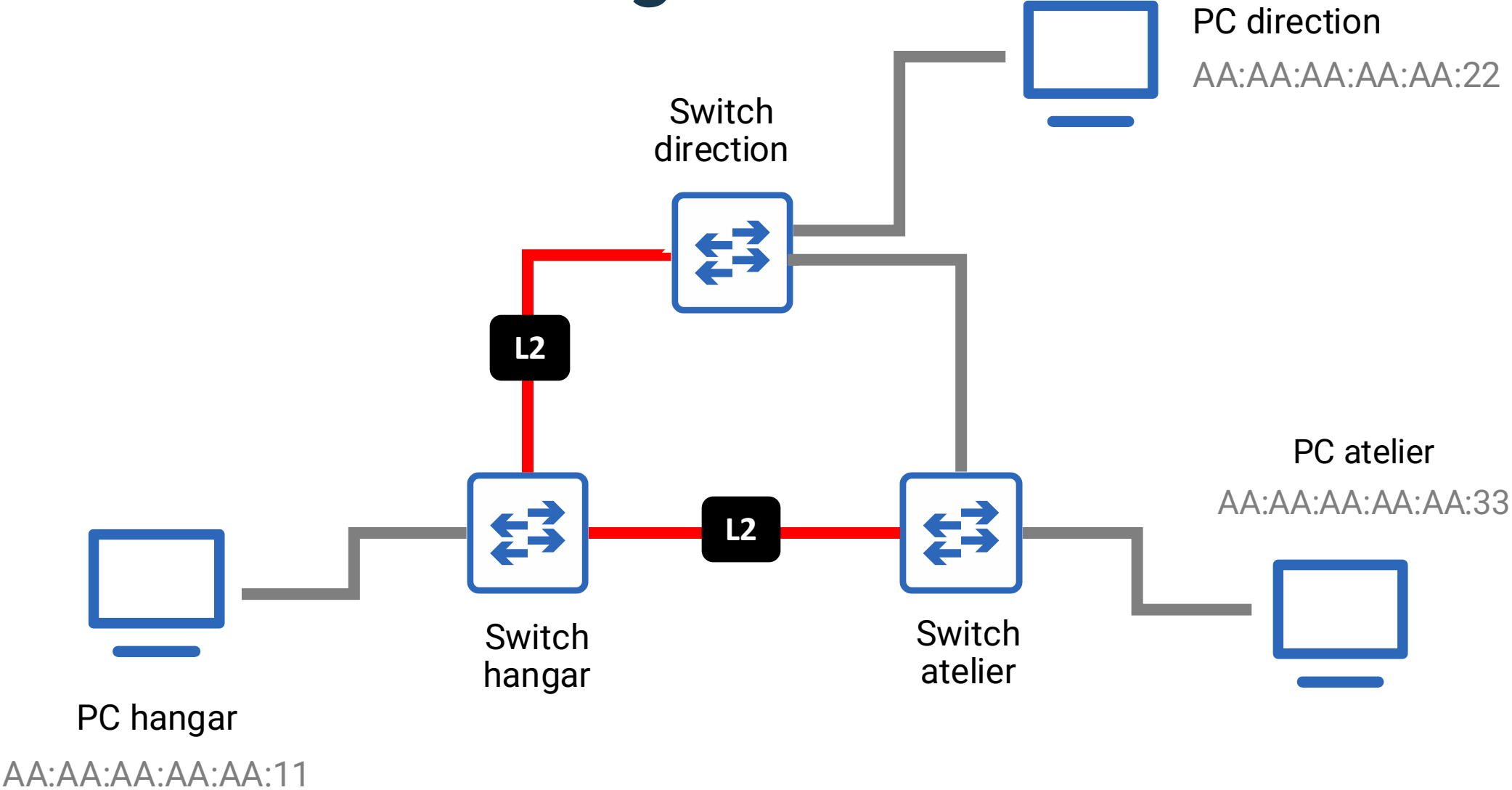
Spanning Tree Protocol, l'essentiel pour gérer les boucles dans un réseau



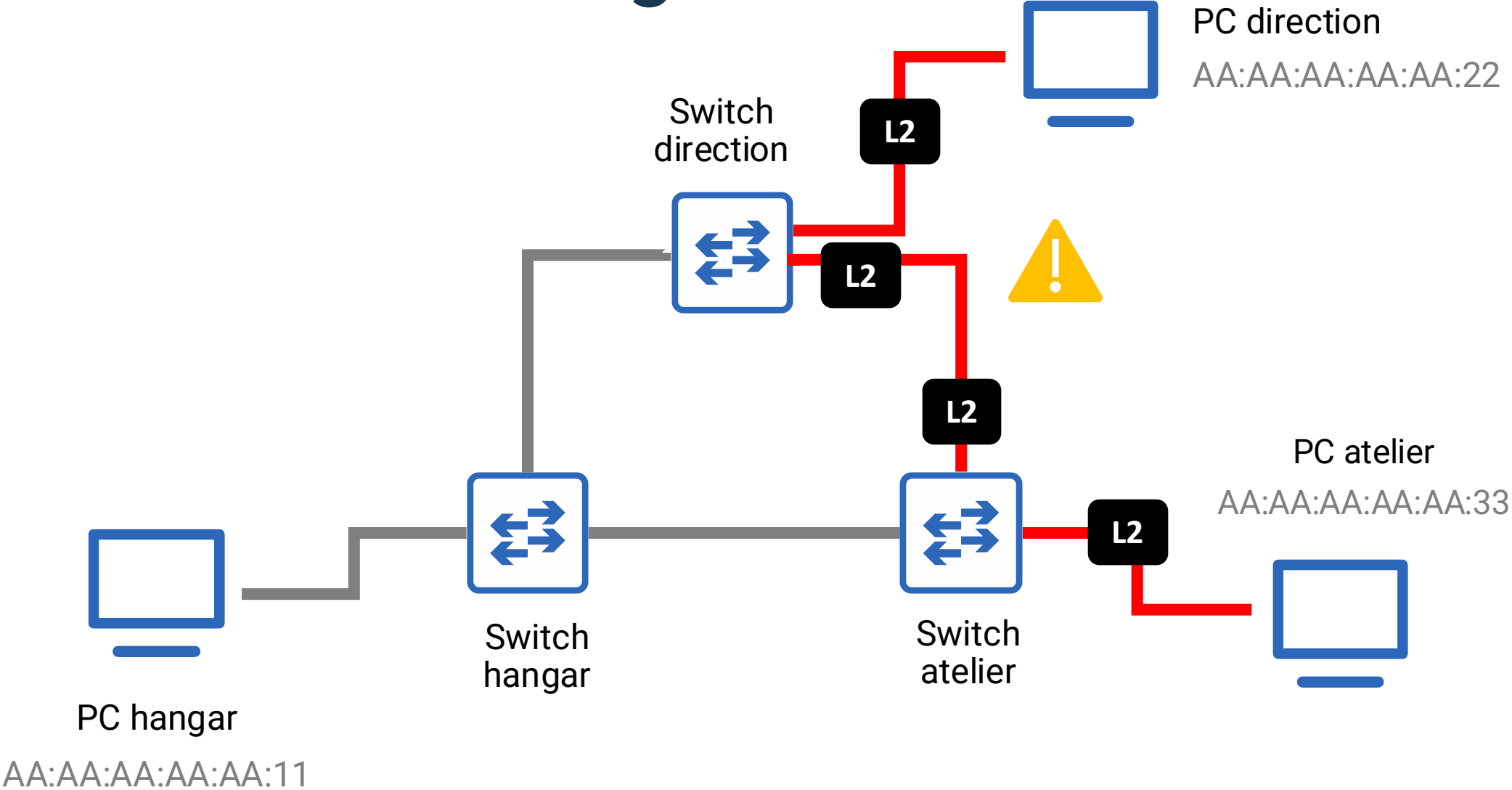
Infrastructure VinciLogistics



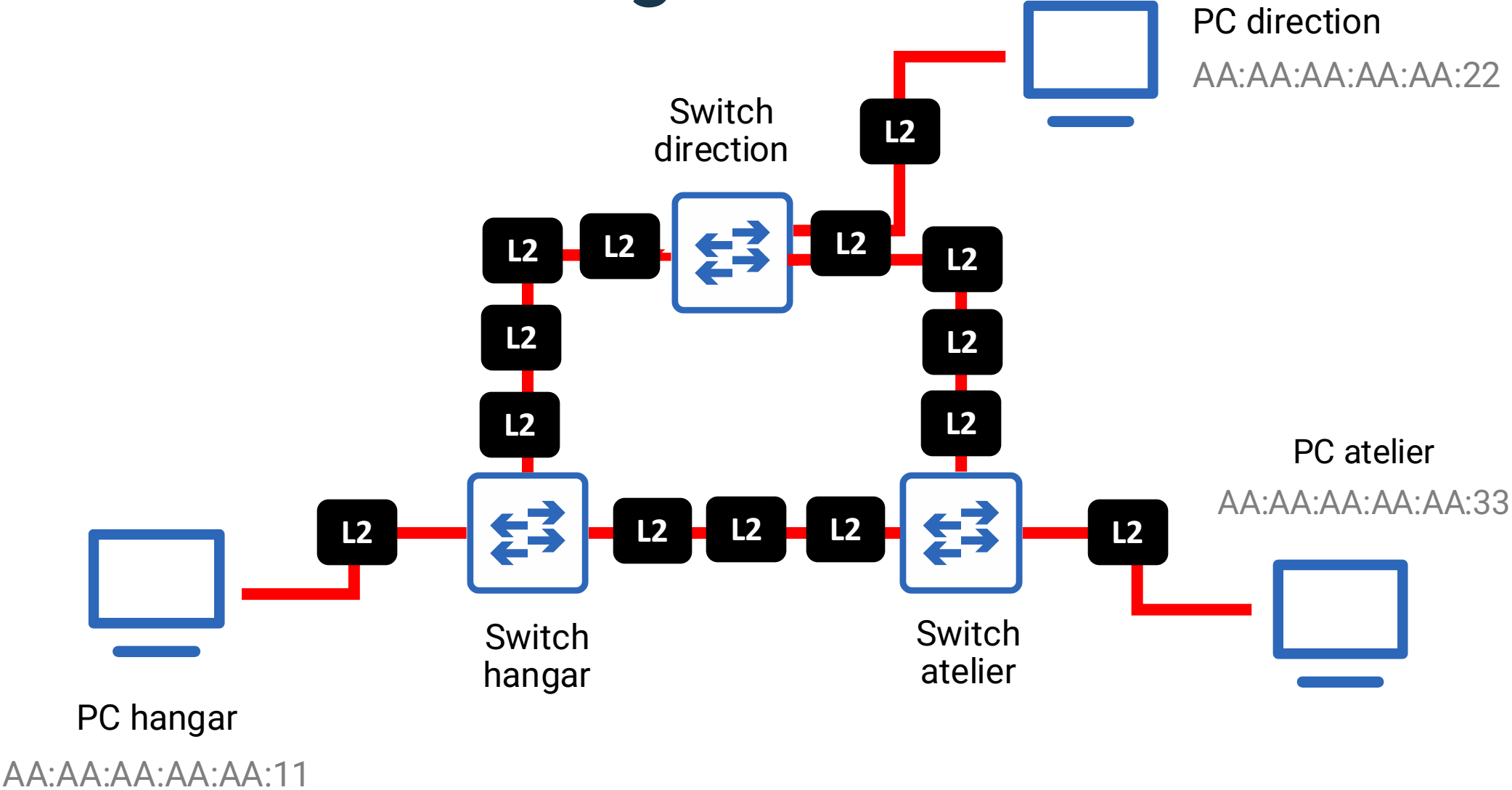
Infrastructure VinciLogistics



Infrastructure VinciLogistics



Infrastructure VinciLogistics



GAME
OVER

Broadcast storm

Souvent déclenché par une trame **broadcast avec une boucle réseau**

- Chaque switch diffuse la trame sur tous ses ports
- Pas d'expiration (TTL) sur une trame
- ... et donc le message reste indéfiniment dans le réseau local

Montée en charge jusqu'à arriver à la saturation des équipements (DOS)

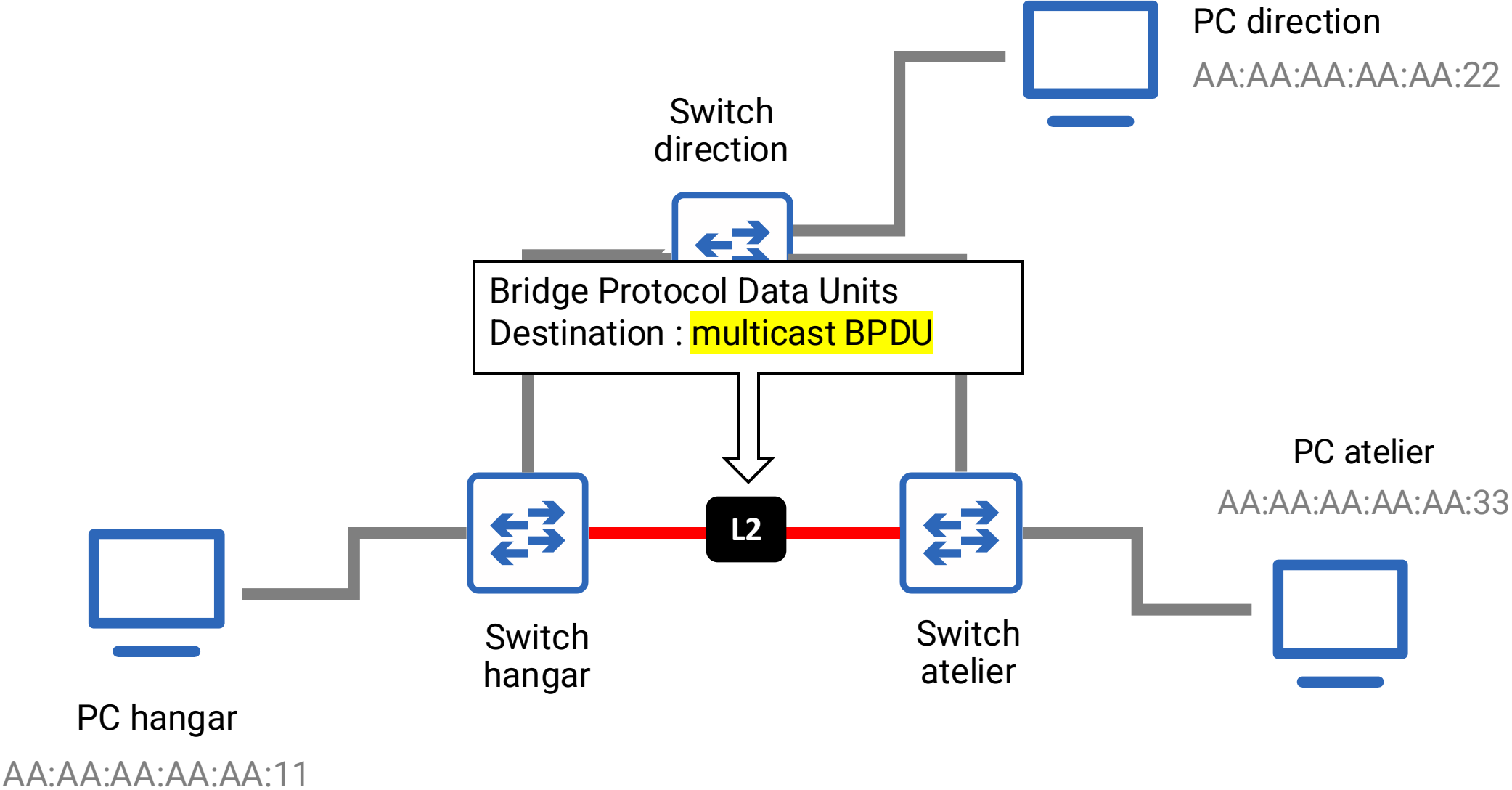
Spanning Tree Protocol

Protocole L2 (Data Link) permettant d'éviter les boucles réseau

- Le protocole STP est supporté par tous les **switchs modernes**
- Uniquement pour switchs, vos équipements ne l'ont pas
- Election d'un **root bridge** et fermeture de ports sur les autres switchs

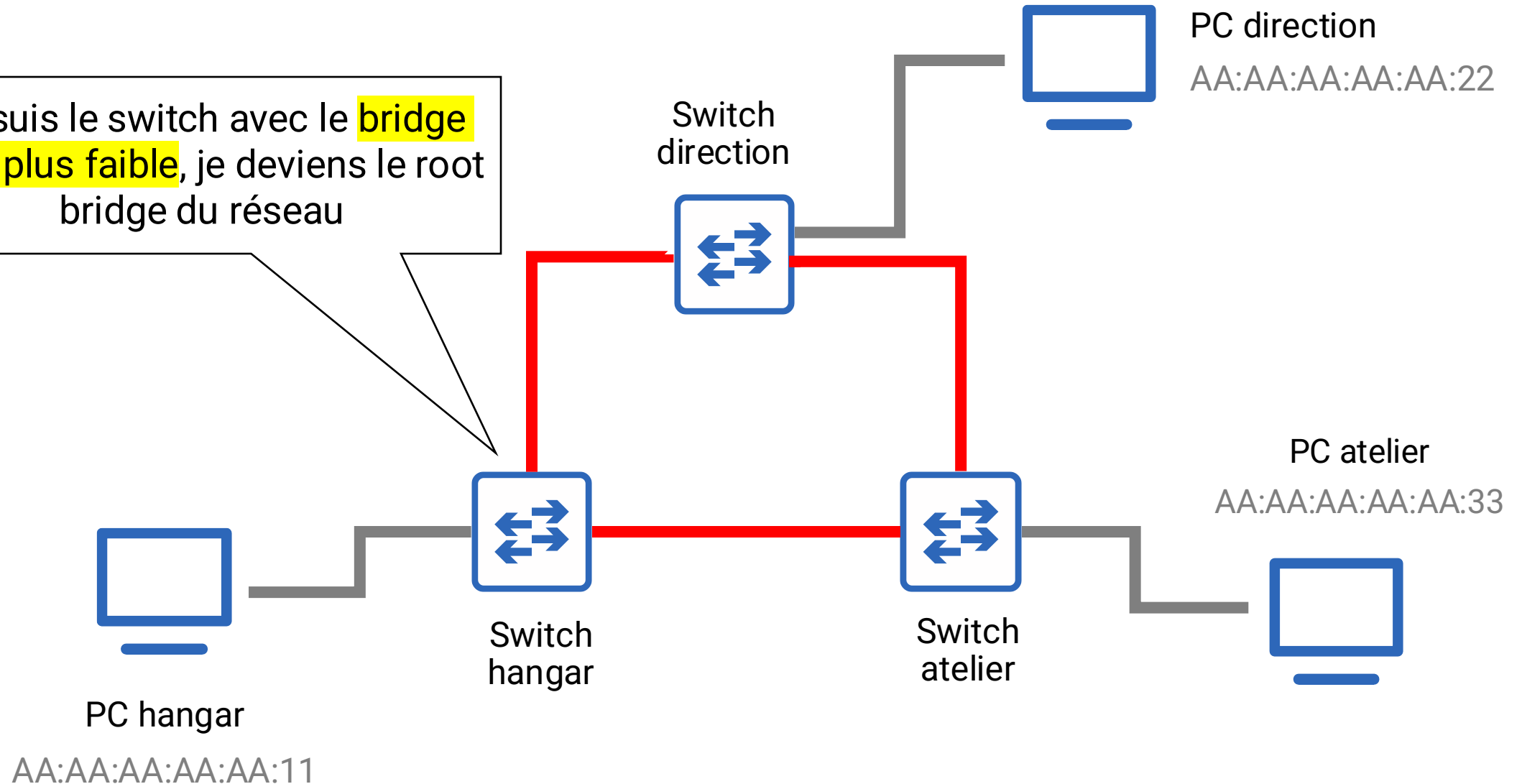
Transforme la boucle réseau en arbre réseau optimal

Processus d'élection

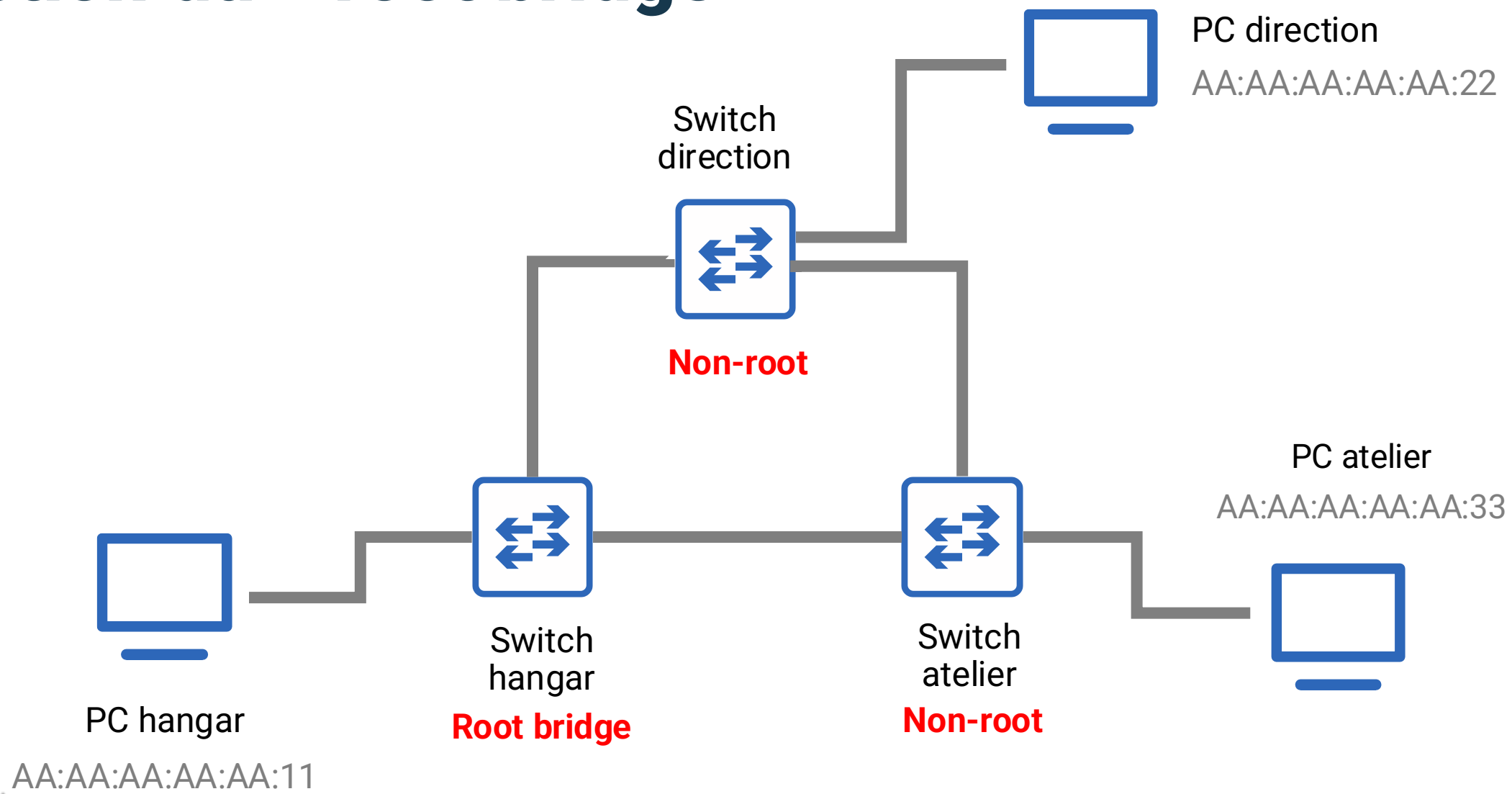


Processus d'élection

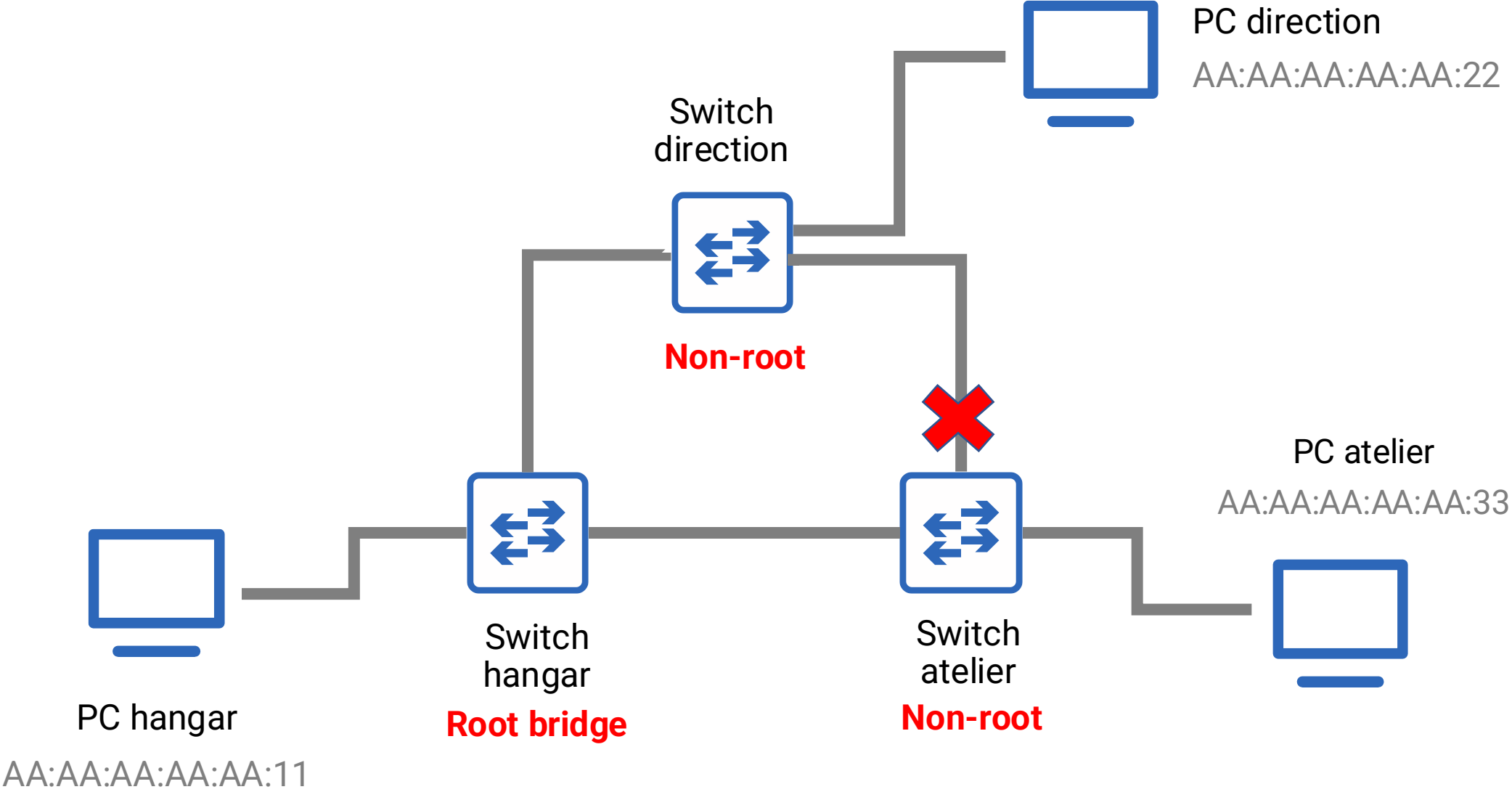
Je suis le switch avec le **bridge ID le plus faible**, je deviens le root bridge du réseau



Election du « root bridge »



La boucle se transforme en arbre



Et les autres protocoles ?

La couche Data Link contient d'autres protocoles qui ne seront pas abordés :

- PPP
- MPLS
- Token Ring
- Frame Relay
- ...