COURS #4

L2 Data Link, deuxième partie

Introduction aux réseaux 2023 (Bloc 2)

Corentin Badot-Bertrand

Dans l’épisode précédent

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

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

Objectifs du cours

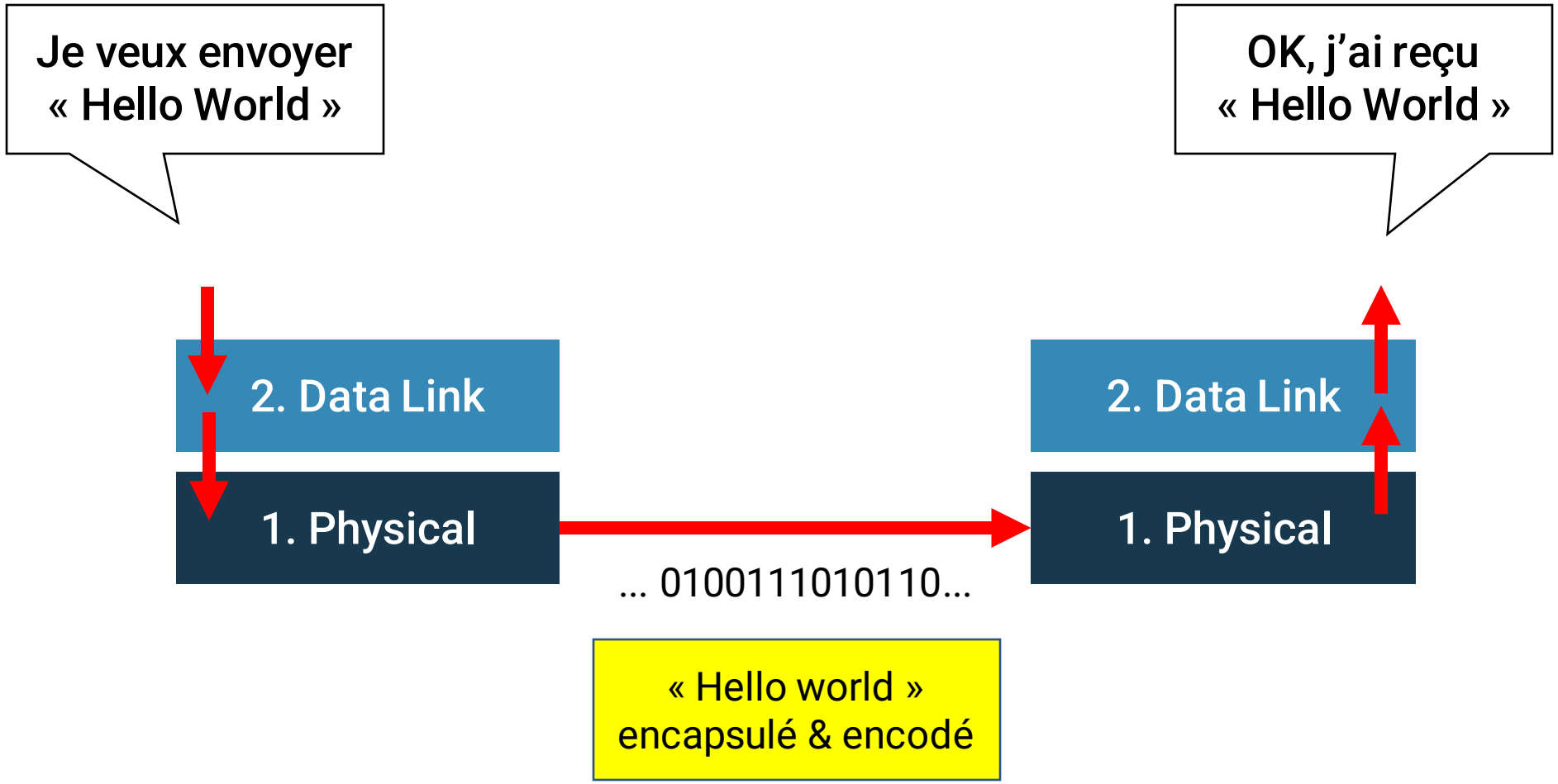
Découvrir des notions avancées de la couche Data Link (OSI L2) :

- Fonctionnement d’un switch
- Les boucles réseau

PARTIE #1

Rappel & concepts

Quelques rappels de la couche Data Link


Je veux envoyer
« Hello World »
OK, j'ai reçu
« Hello World »
2. Data Link
1. Physical
2. Data Link
1. Physical
... 01001110101110...
« Hello world »
encapsulé & encodé

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 ou dans un réseau local
- 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

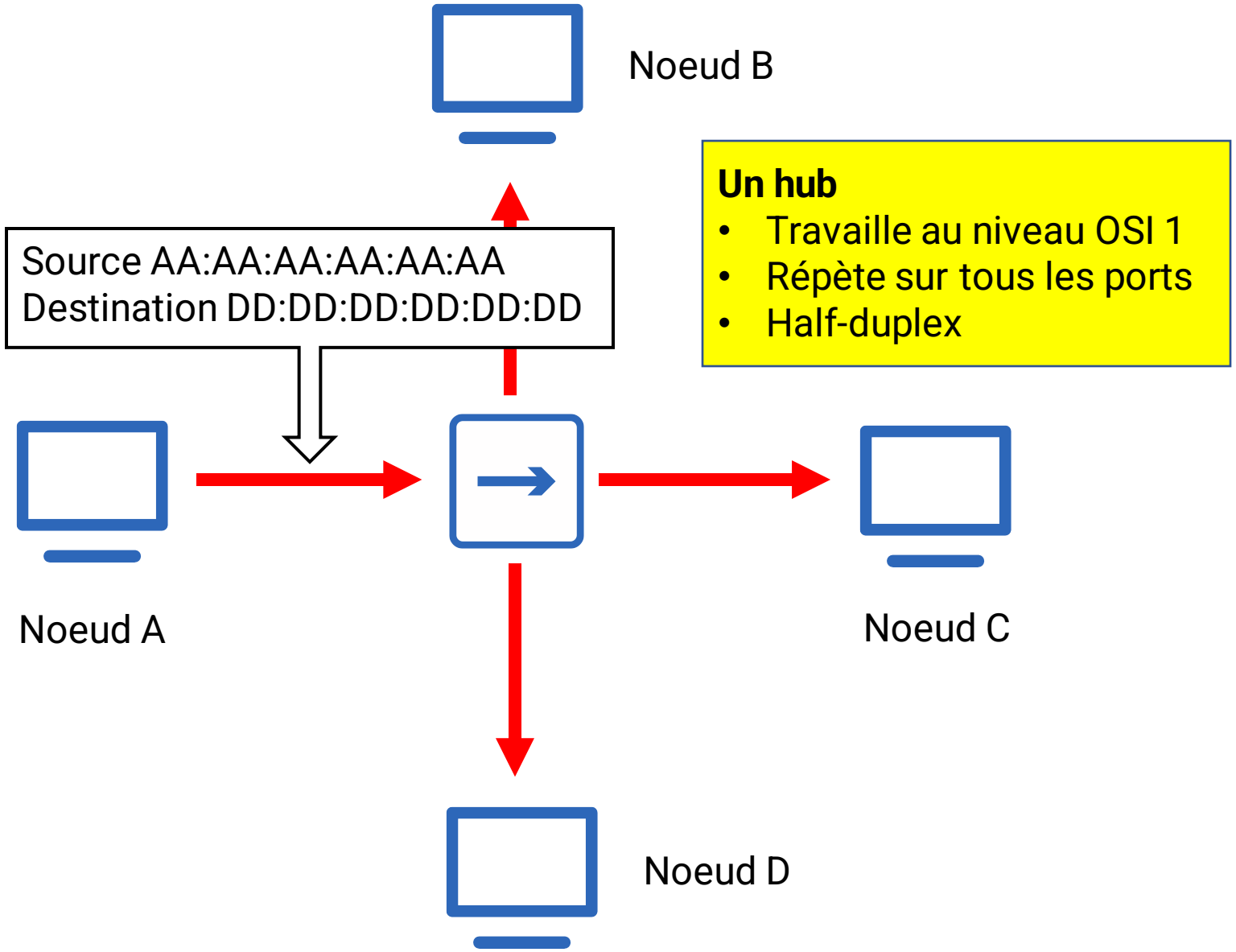
Une adresse MAC identifie une interface réseau

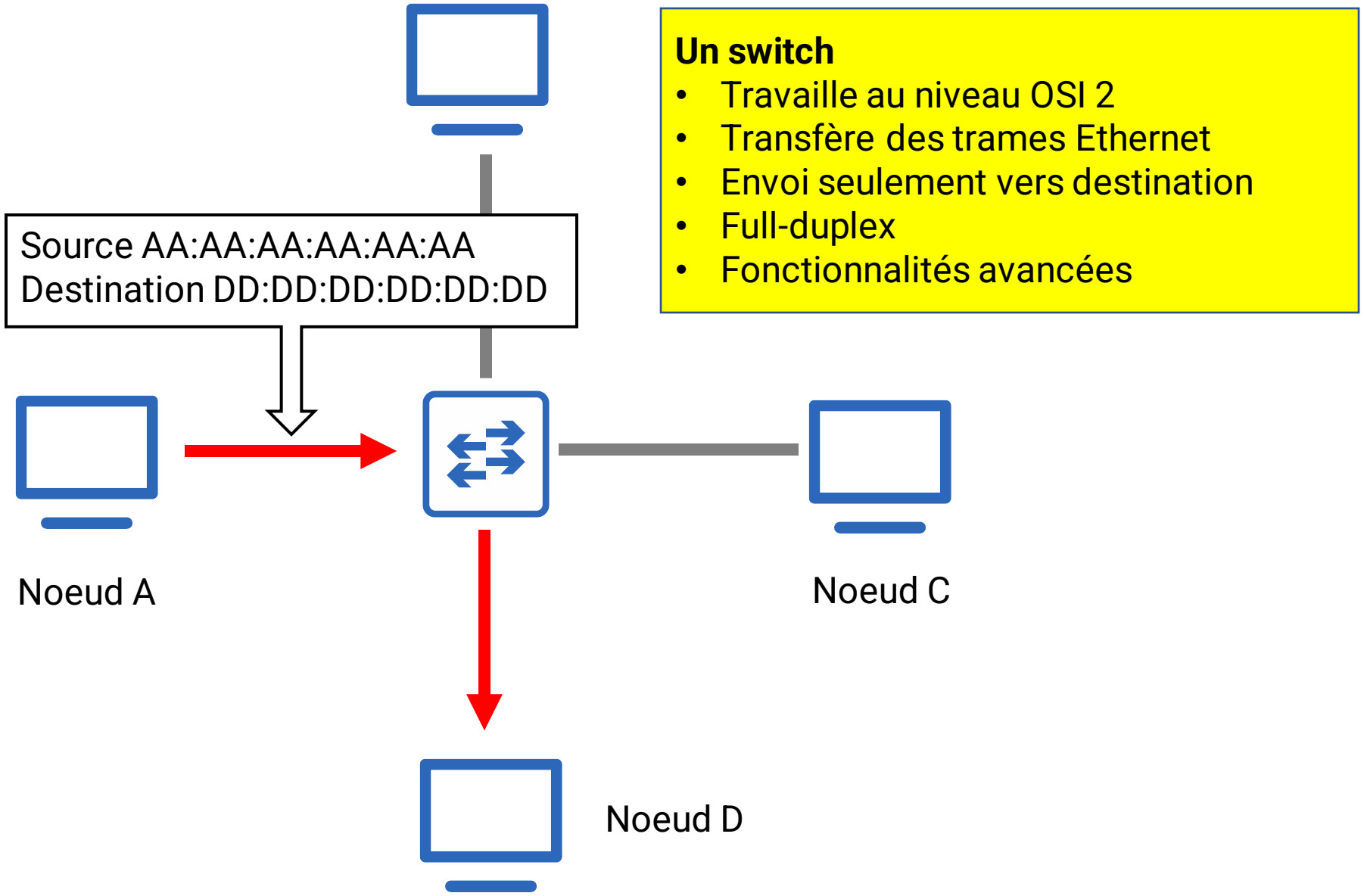
- Une carte réseau d'un ordinateur, puce WiFi, etc.
- Gravée dans carte
- Avec préfixe constructeur
- Possible de changer au niveau de l'OS

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 ?


Noeud B
Un hub
• Travaille au niveau OSI 1
• Répète sur tous les ports
• Half-duplex
Source AA:AA:AA:AA:AA:AA
Destination DD:DD:DD:DD:DD:DD
Noeud A
Noeud C
Noeud D



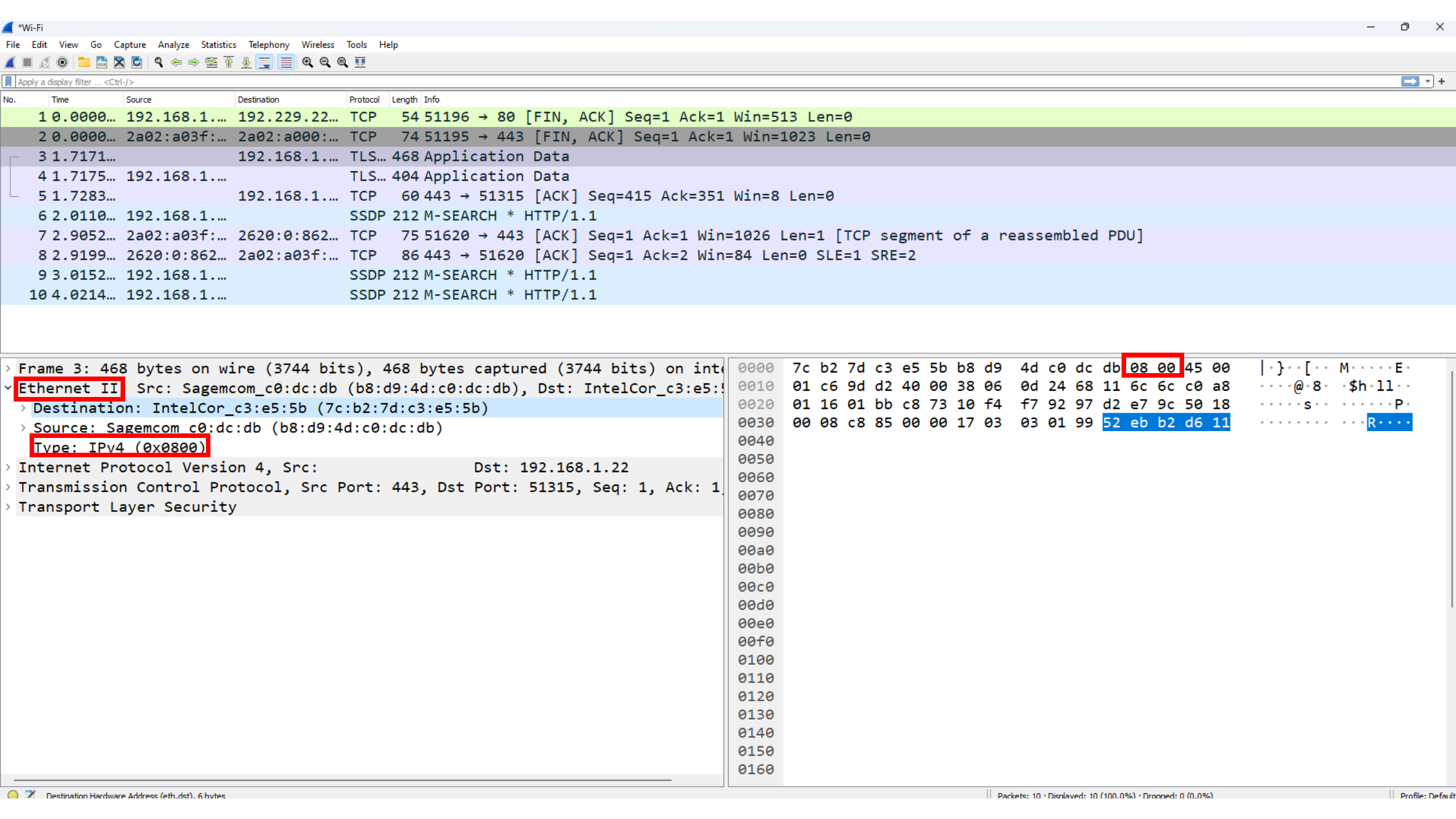
Un switch

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

Ethernet II

Les 2 bytes sont maintenant dédié au « RtherType » : le protocole encapsulé

		Header Ethernet (14 bytes)				
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	46 – 1500 bytes	4 bytes
Préambule	Délimiteur	MAC destination	MAC source	EtherType	Données …	CRC


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.0000… 192.168.1.… 192.229.22… TCP 54 51196 → 80 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0
2 0.0000… 2a02:a03f:… 2a02:a000:… TCP 74 51195 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1023 Len=0
3 1.7171… 192.168.1.… TLS… 468 Application Data
4 1.7175… 192.168.1.… TLS… 404 Application Data
5 1.7283… 192.168.1.… TCP 60 443 → 51315 [ACK] Seq=415 Ack=351 Win=8 Len=0
6 2.0110… 192.168.1.… SSDP 212 M-SEARCH * HTTP/1.1
7 2.9052… 2a02:a03f:… 2620:0:862… TCP 75 51620 → 443 [ACK] Seq=1 Ack=1 Win=1026 Len=1 [TCP segment of a reassembled PDU]
8 2.9199… 2620:0:862… 2a02:a03f:… TCP 86 443 → 51620 [ACK] Seq=1 Ack=2 Win=84 Len=0 SLE=1 SRE=2
9 3.0152… 192.168.1.… SSDP 212 M-SEARCH * HTTP/1.1
10 4.0214… 192.168.1.… SSDP 212 M-SEARCH * HTTP/1.1
Frame 3: 468 bytes on wire (3744 bits), 468 bytes captured (3744 bits) on inte
Ethernet II Src: Sagemcom_c0:dc:db (b8:d9:4d:c0:dc:db), Dst: IntelCor_c3:e5:5
Destination: IntelCor_c3:e5:5b (7c:b2:7d:c3:e5:5b)
Source: Sagemcom_c0:dc:db (b8:d9:4d:c0:dc:db)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: Dst: 192.168.1.22
Transmission Control Protocol, Src Port: 443, Dst Port: 51315, Seq: 1, Ack: 1
Transport Layer Security
0000 7c b2 7d c3 e5 5b b8 d9 4d c0 dc db 08 00 45 00
0010 01 c6 9d d2 40 00 38 06 0d 24 68 11 6c 6c c0 a8
0020 01 16 01 bb c8 73 10 f4 f7 92 97 d2 e7 9c 50 18
0030 00 08 c8 85 00 00 17 03 03 01 99 52 eb b2 d6 11
Destination Hardware Address (eth.dst), 6 bytes
Packets: 10 · Displayed: 10 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

EtherTypes

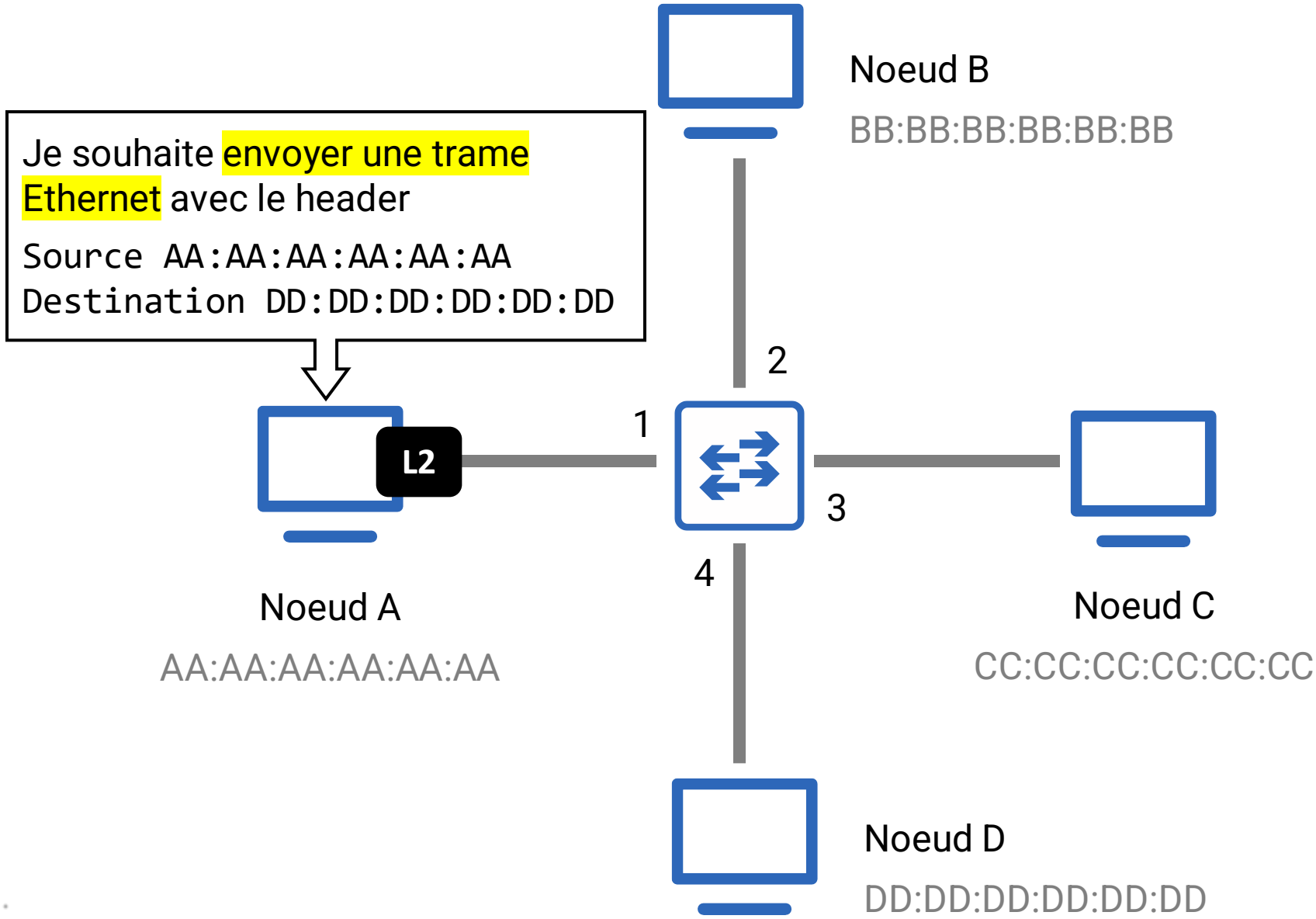
Quelques Ethertypes standardisés :

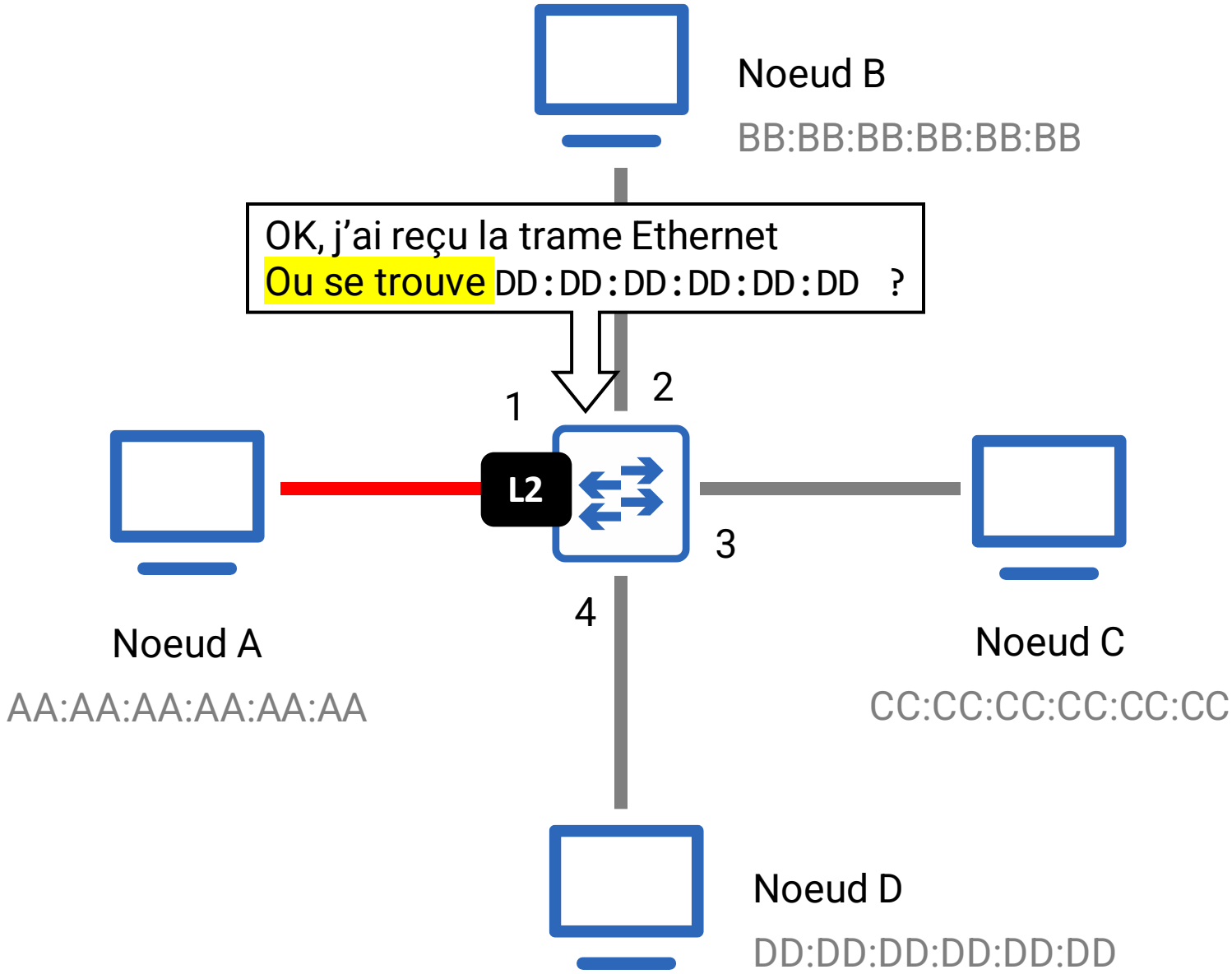
- 0x0800 IPv4
- 0x0806 ARP
- 0X86DD IPv6

PARTIE #2

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
L2
1
2
3
4
Noeud A
AA:AA:AA:AA:AA:AA
Noeud B
BB:BB:BB:BB:BB:BB
Noeud C
CC:CC:CC:CC:CC:CC
Noeud D
DD:DD:DD:DD:DD:DD

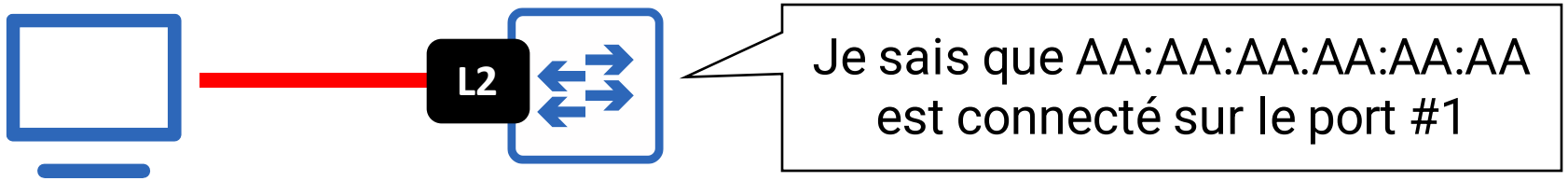

Noeud B
BB:BB:BB:BB:BB:BB
OK, j'ai reçu la trame Ethernet
Ou se trouve DD:DD:DD:DD:DD:DD ?
1
2
L2
3
4
Noeud A
AA:AA:AA:AA:AA:AA
Noeud C
CC:CC:CC:CC:CC:CC
Noeud D
DD:DD:DD:DD:DD:DD


TL-SG1005P
tp-link
5-Port Gigabit Desktop Switch with 4-Port PoE
Power
PoE Max
1
2
3
4
5

Apprentissage d’adresses

Le switch a besoin de connaitre 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



Noeud A

AA:AA:AA:AA:AA:AA

Table d’adressage

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

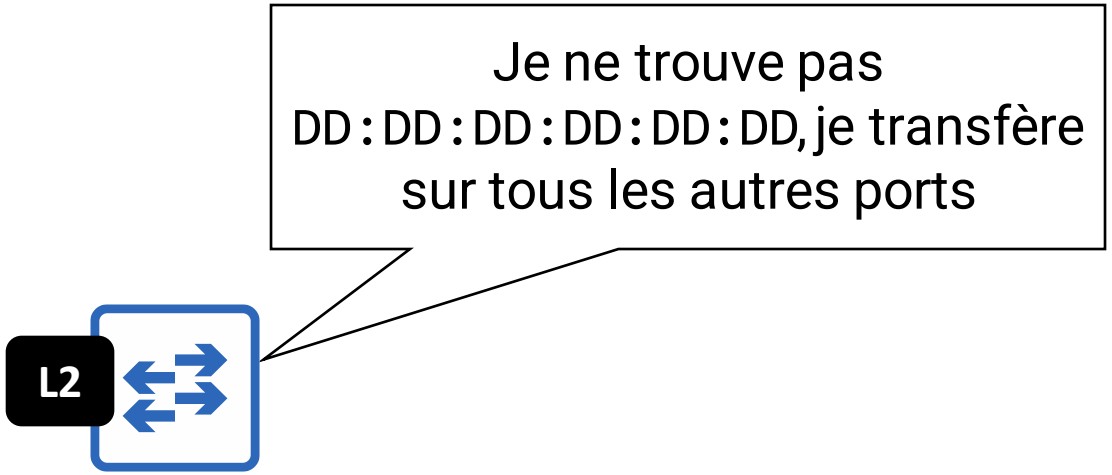
Port	Adresse MAC connectée
1	AA:AA:AA:AA:AA:AA
2	?
3	?
4	?

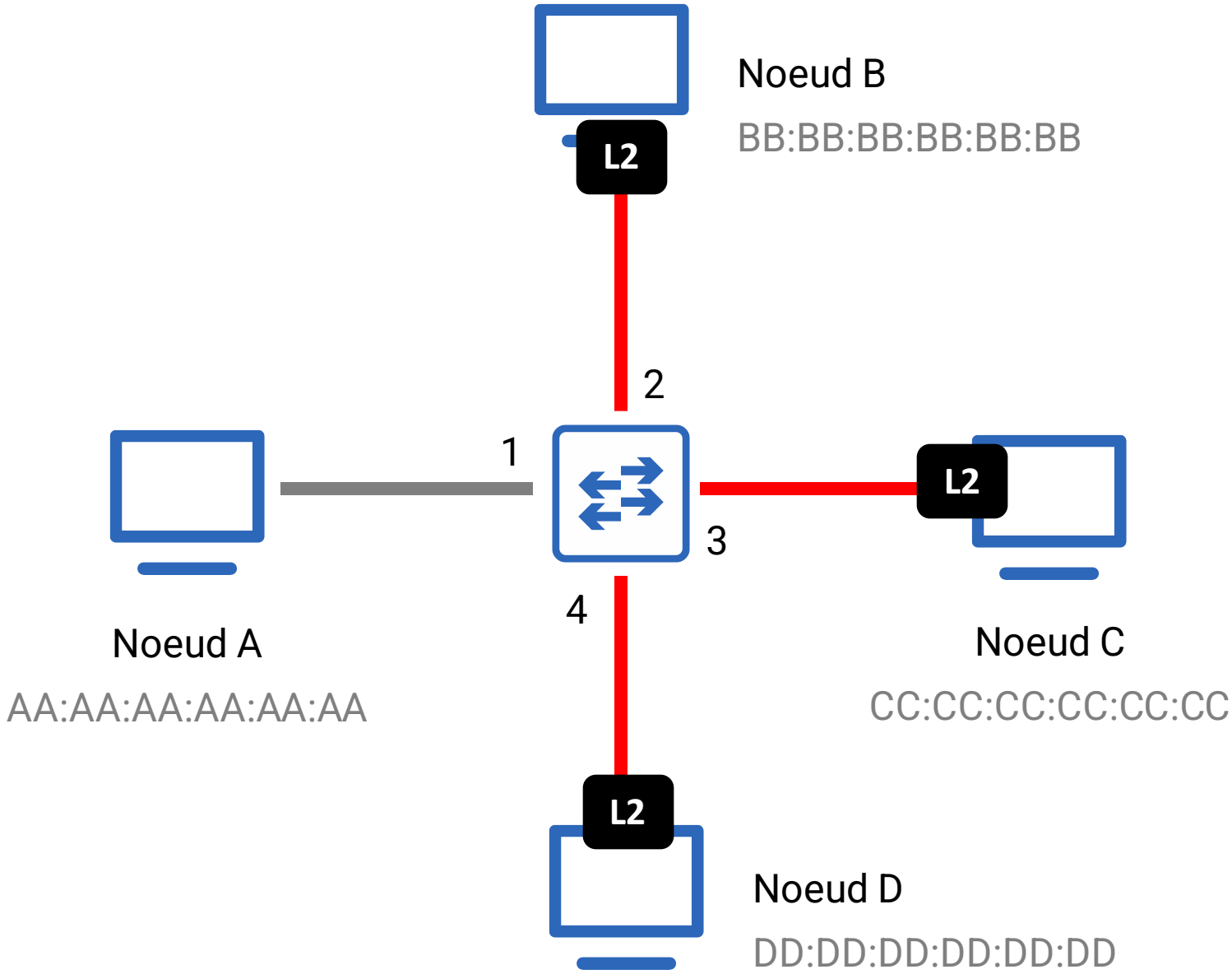
Comment le switch peut-il connaitre le port de DD:DD:DD:DD:DD:DD ?

Flooding

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

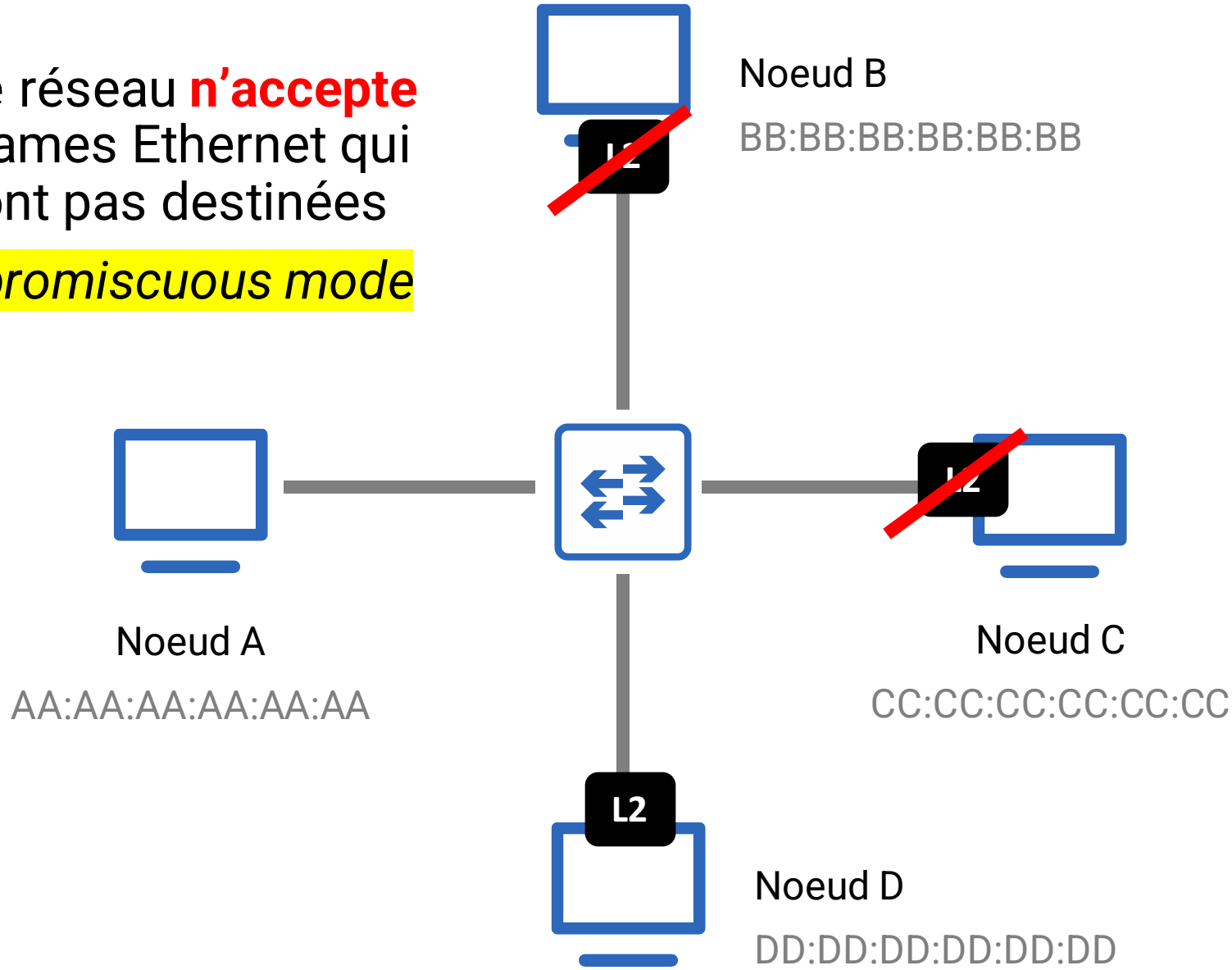
Port	Adresse MAC connectée
1	AA:AA:AA:AA:AA:AA
2	?
3	?
4	?

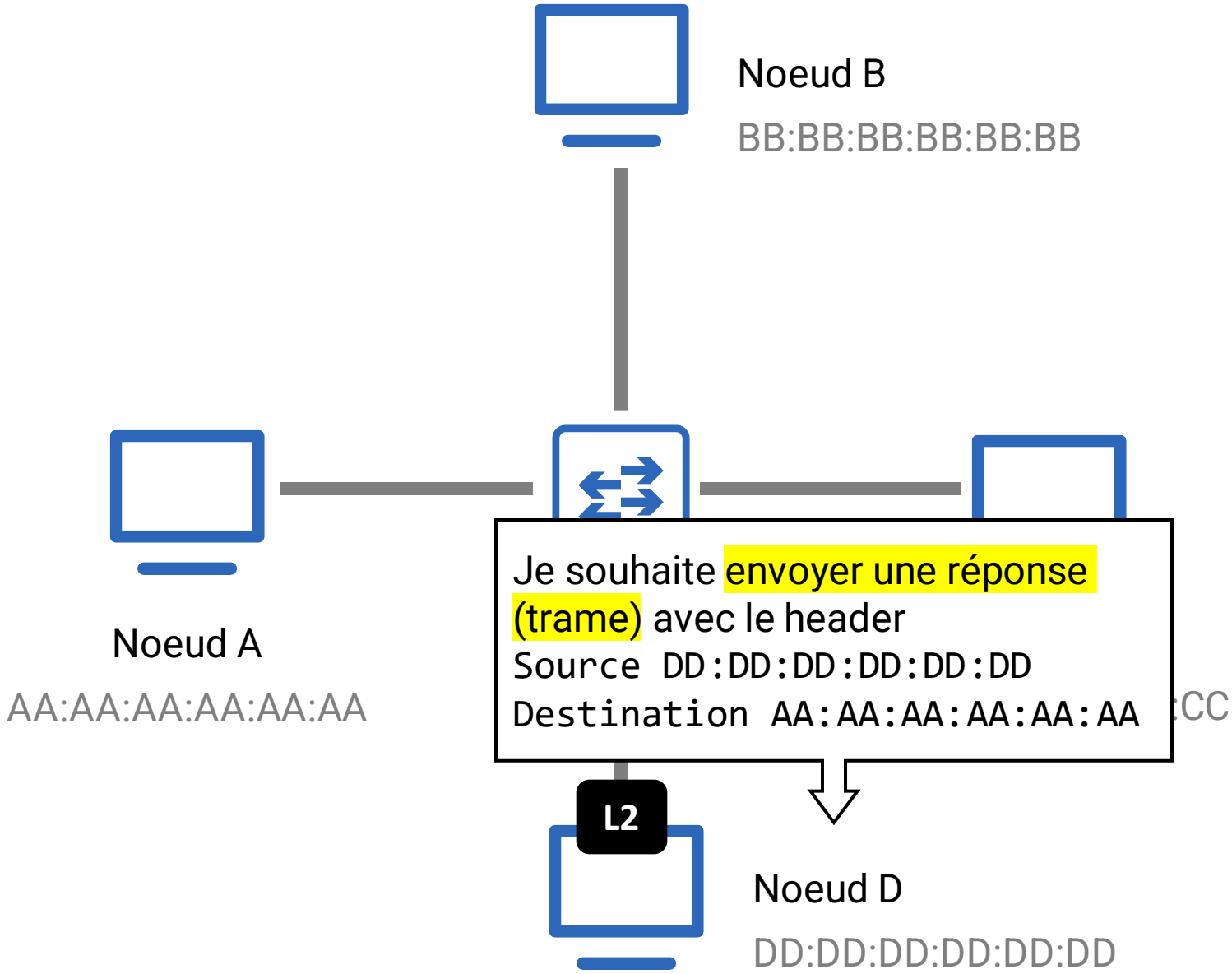



Noeud B
BB:BB:BB:BB:BB:BB
L2
2
1
3
4
L2
L2
Noeud A
AA:AA:AA:AA:AA:AA
Noeud C
CC:CC:CC:CC:CC:CC
Noeud D
DD:DD:DD:DD:DD:DD

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

Sauf en *promiscuous mode*




Noeud B
BB:BB:BB:BB:BB:BB
Noeud A
AA:AA:AA:AA:AA:AA
Je souhaite envoyer une réponse (trame) avec le header
Source DD:DD:DD:DD:DD:DD
Destination AA:AA:AA:AA:AA:AA
L2
Noeud D
DD:DD:DD:DD:DD:DD

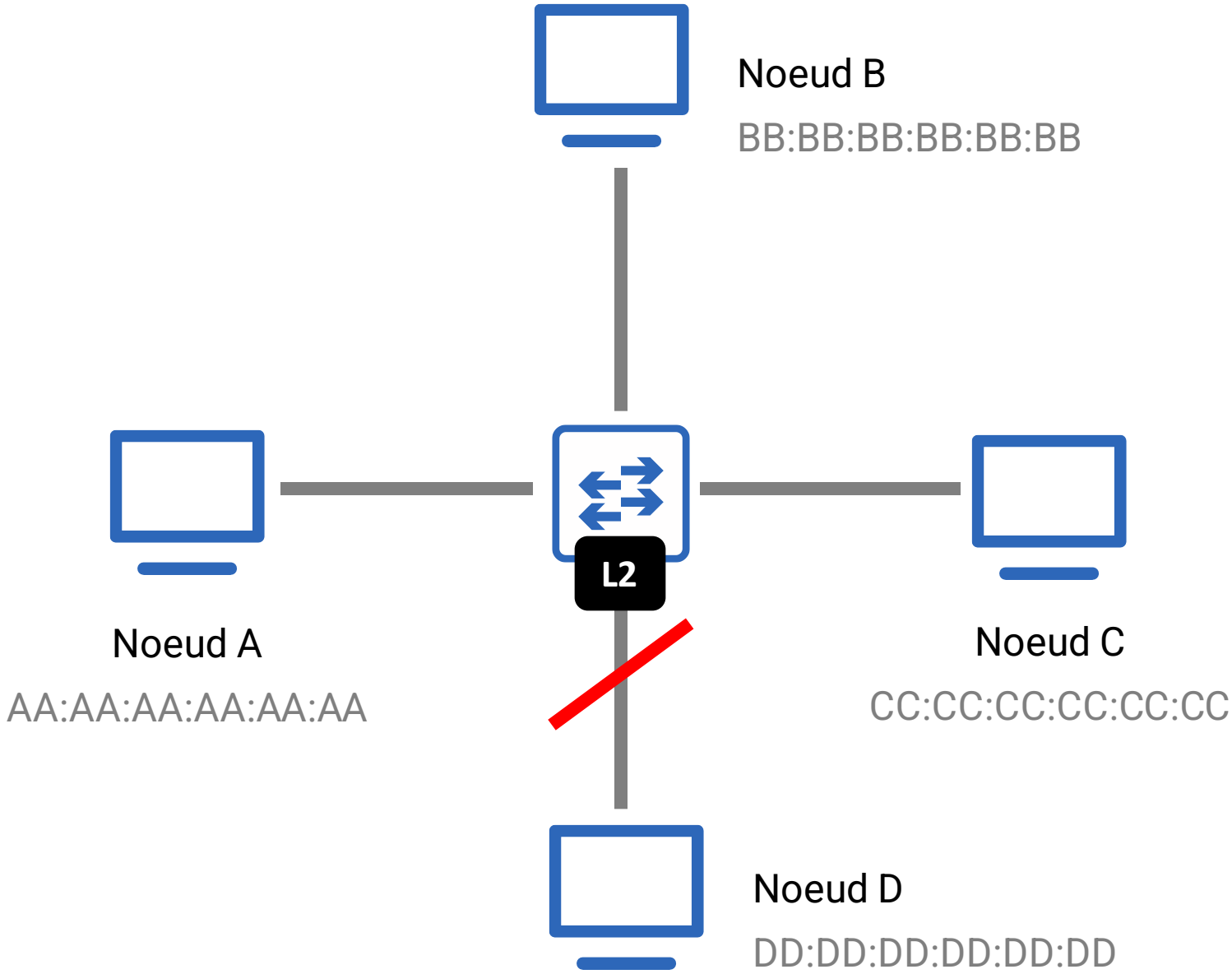
Et l’apprentissage continue…

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

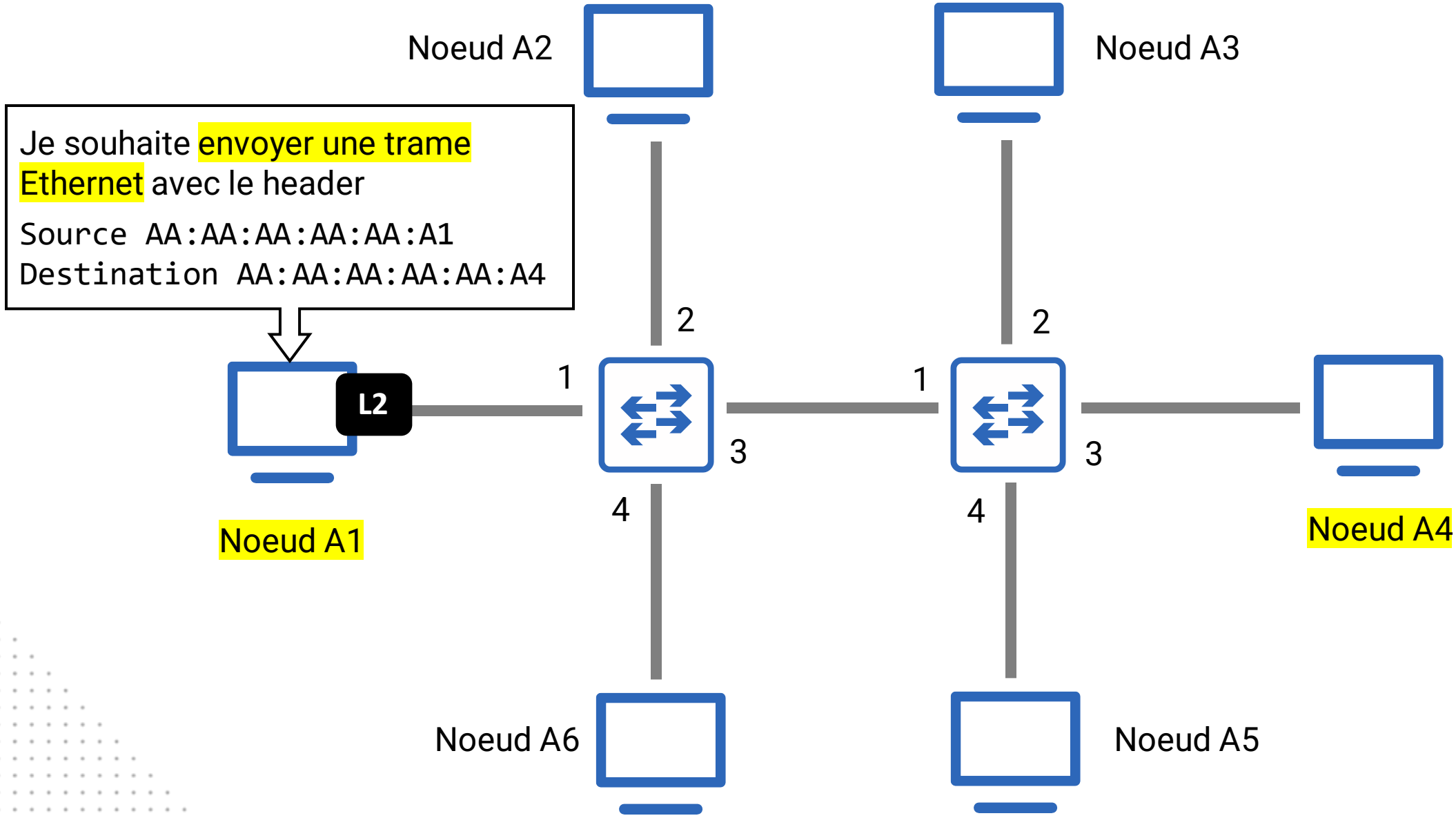
- Capable d’apprendre automatiquement
- Si une adresse MAC est dans la table… alors seul l’adresse recevra la trame
- Si un port est occupé, le switch est capable de mettre la trame en attente
- Le switch ne modifie pas par défaut la trame Ethernet


Noeud B
BB:BB:BB:BB:BB:BB
L2
Noeud A
AA:AA:AA:AA:AA:AA
Noeud C
CC:CC:CC:CC:CC:CC
Noeud D
DD:DD:DD:DD:DD:DD

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


Noeud A2
Noeud A3
Je souhaite envoyer une trame Ethernet avec le header
Source AA:AA:AA:AA:AA:A1
Destination AA:AA:AA:AA:AA:A4
2
2
L2
1
1
3
3
4
4
Noeud A1
Noeud A4
Noeud A6
Noeud A5

Exemple : Switch Cisco industriel

Exemple : Switch Cisco industriel

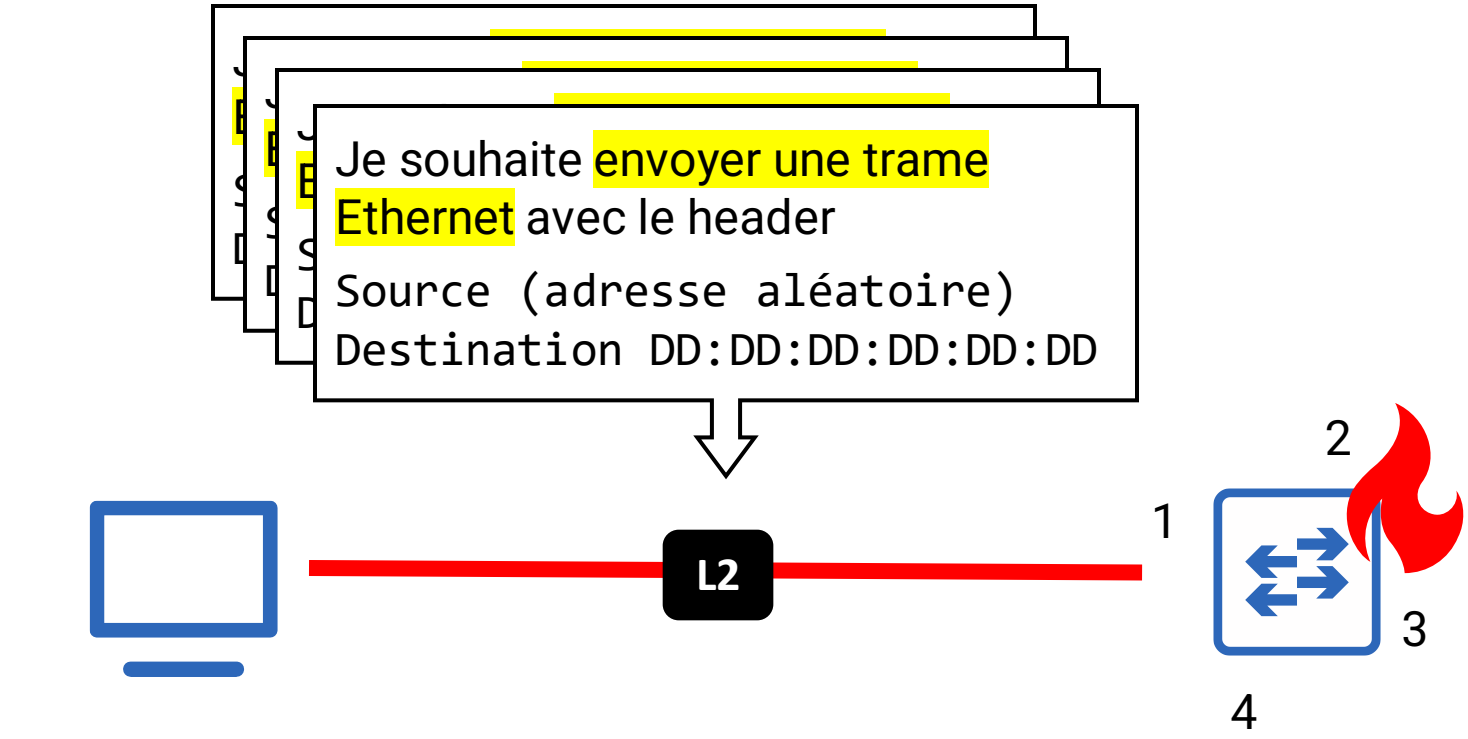
vlan	mac address	type	port
9	000c.291e.96f0	dynamic	GigabitEthernet1/1
9	000c.293c.7cac	dynamic	GigabitEthernet1/1
9	000c.2950.e3e9	dynamic	GigabitEthernet1/1
9	000c.29ba.fe28	dynamic	GigabitEthernet1/2
9	842b.2ba6.3a7d	dynamic	GigabitEthernet1/3
9	d067.e50b.1975	dynamic	GigabitEthernet1/5
9	d067.e51e.e35a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

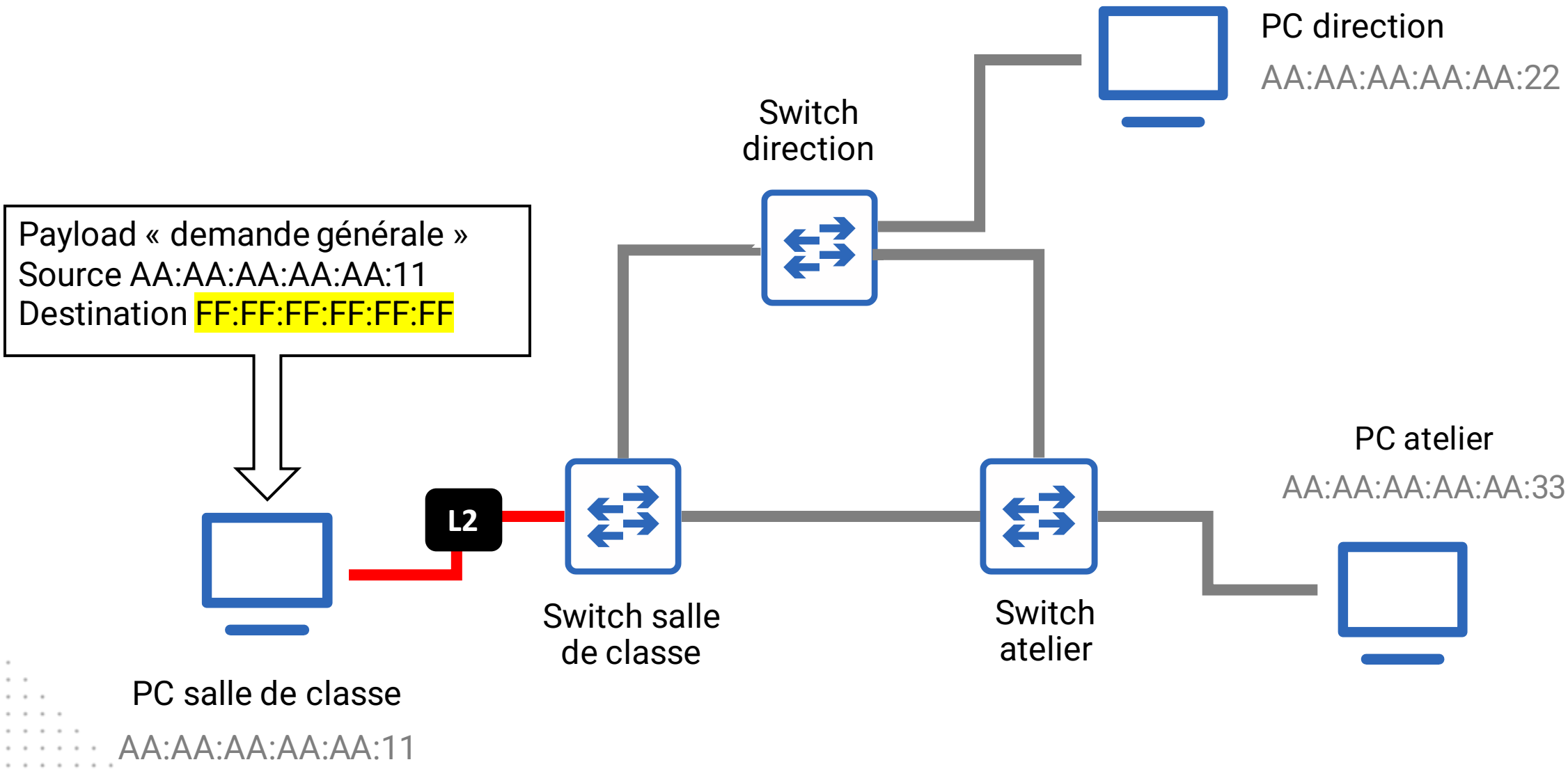

Je souhaite envoyer une trame Ethernet avec le header
Source (adresse aléatoire)
Destination DD:DD:DD:DD:DD:DD
L2
1
2
3
4
Noeud attaquant

PARTIE #3

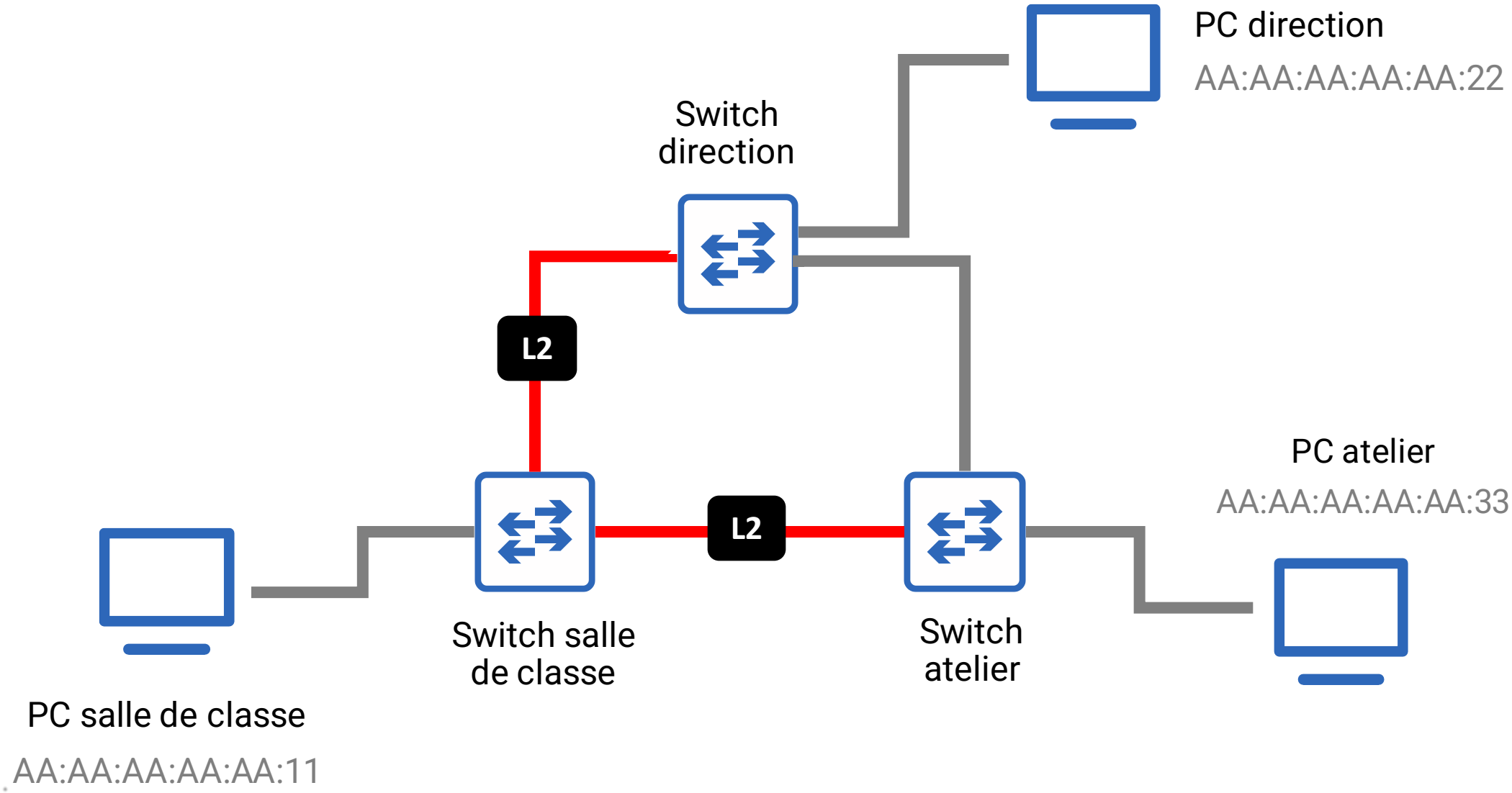
Le protocole STP

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

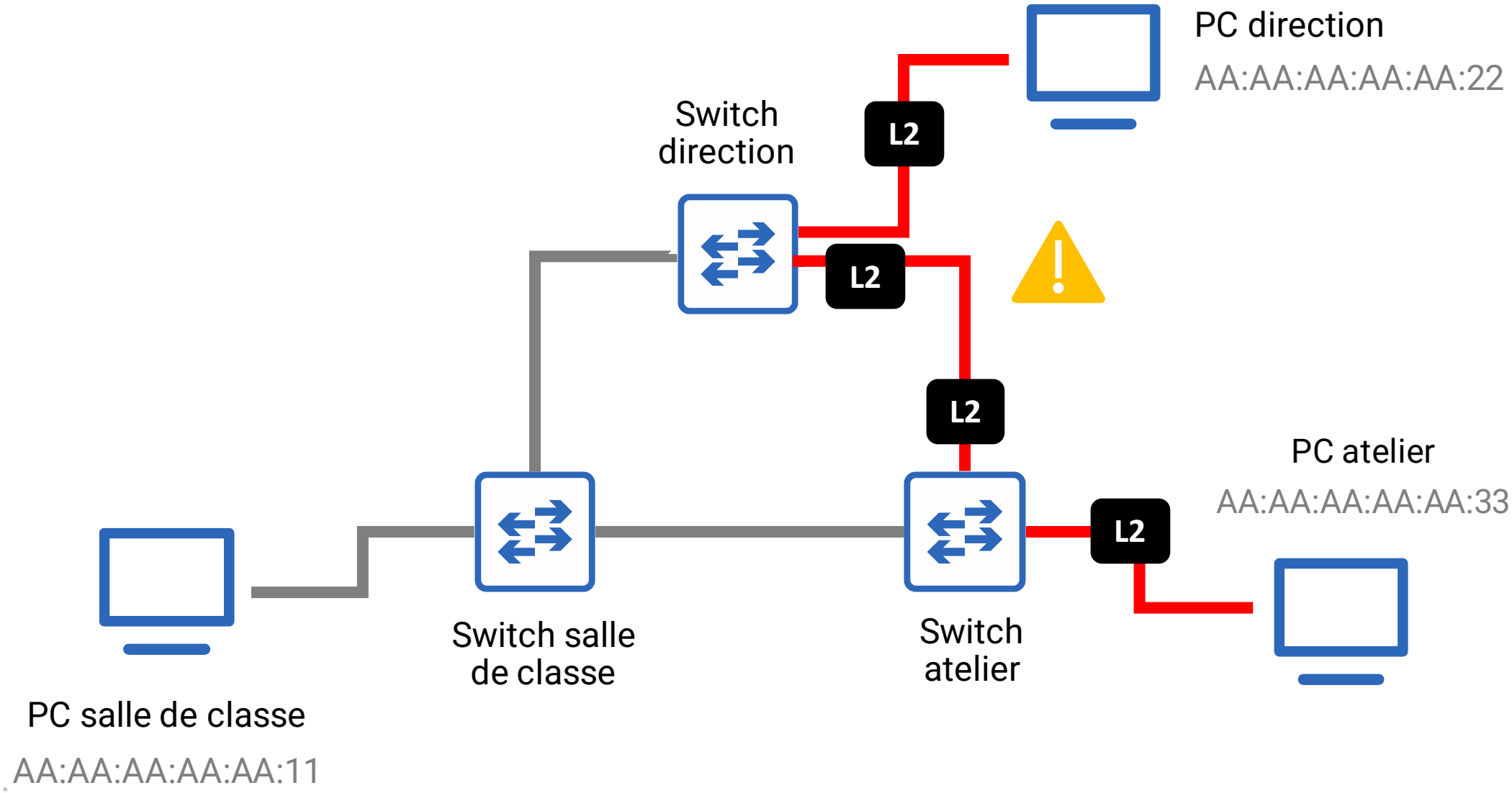
Infrastructure de l'école



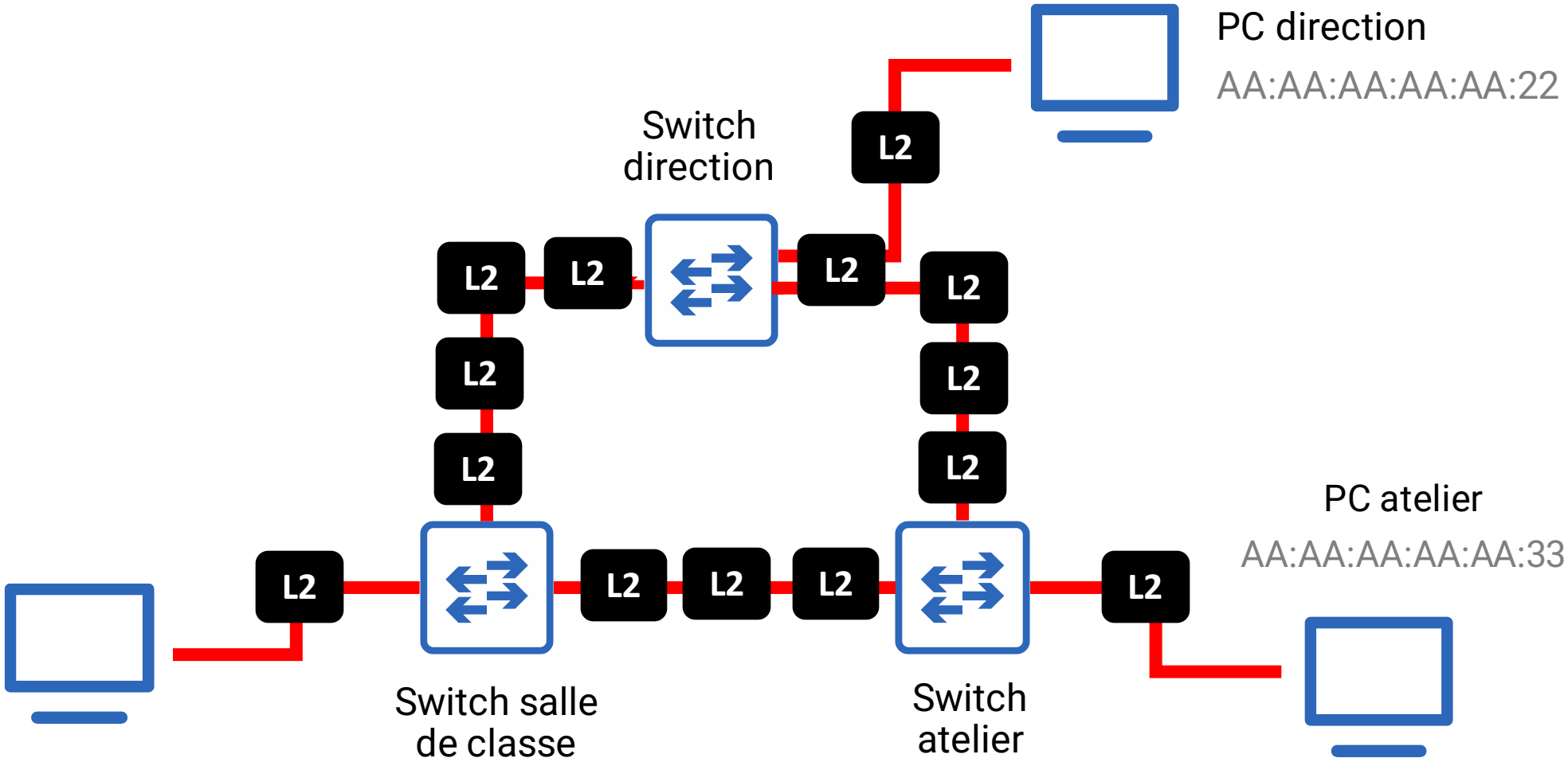
Infrastructure de l'école



Infrastructure de l’école



Infrastructure de l’école




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)

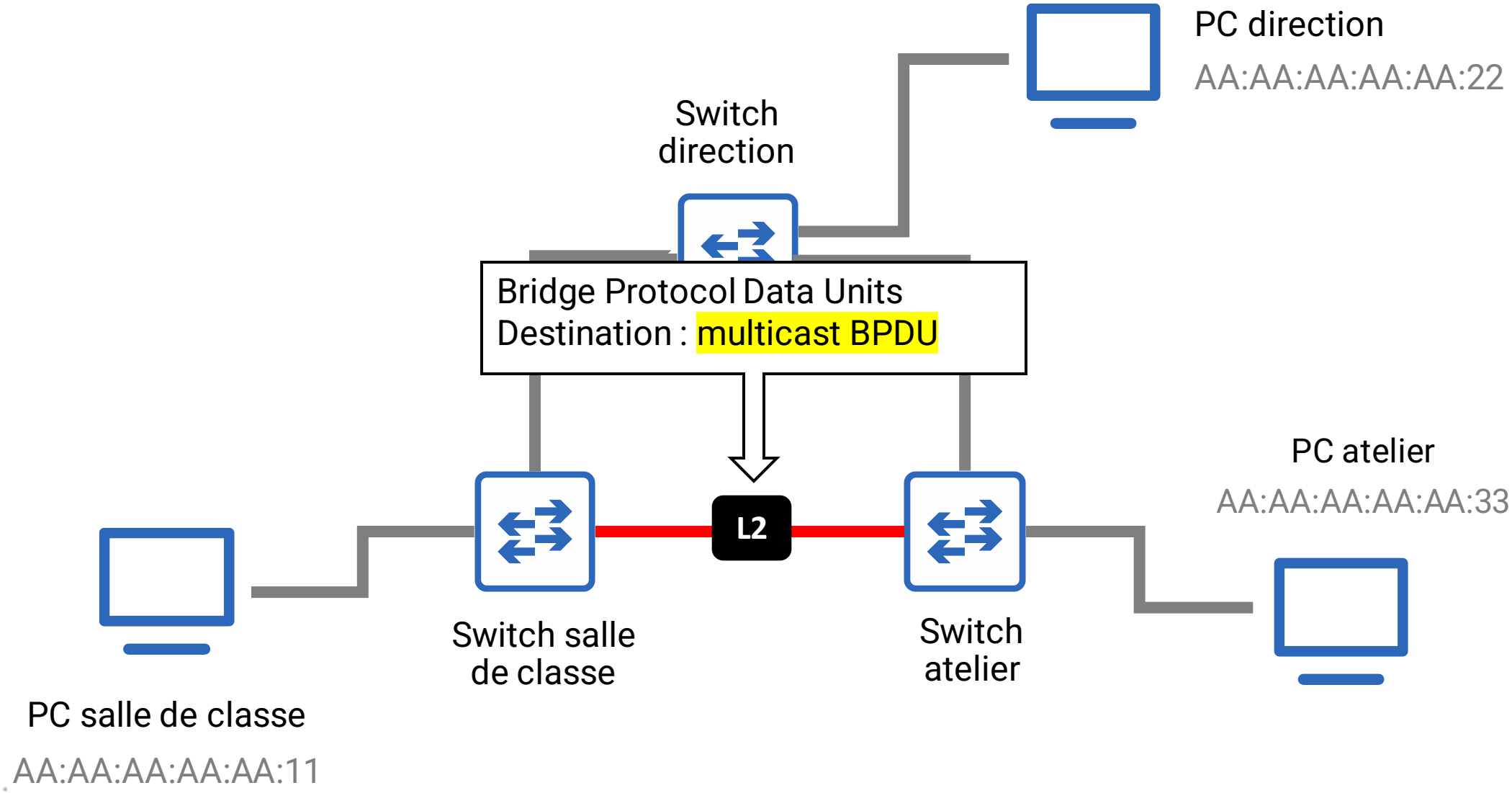
Spanning Tree Protocol

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

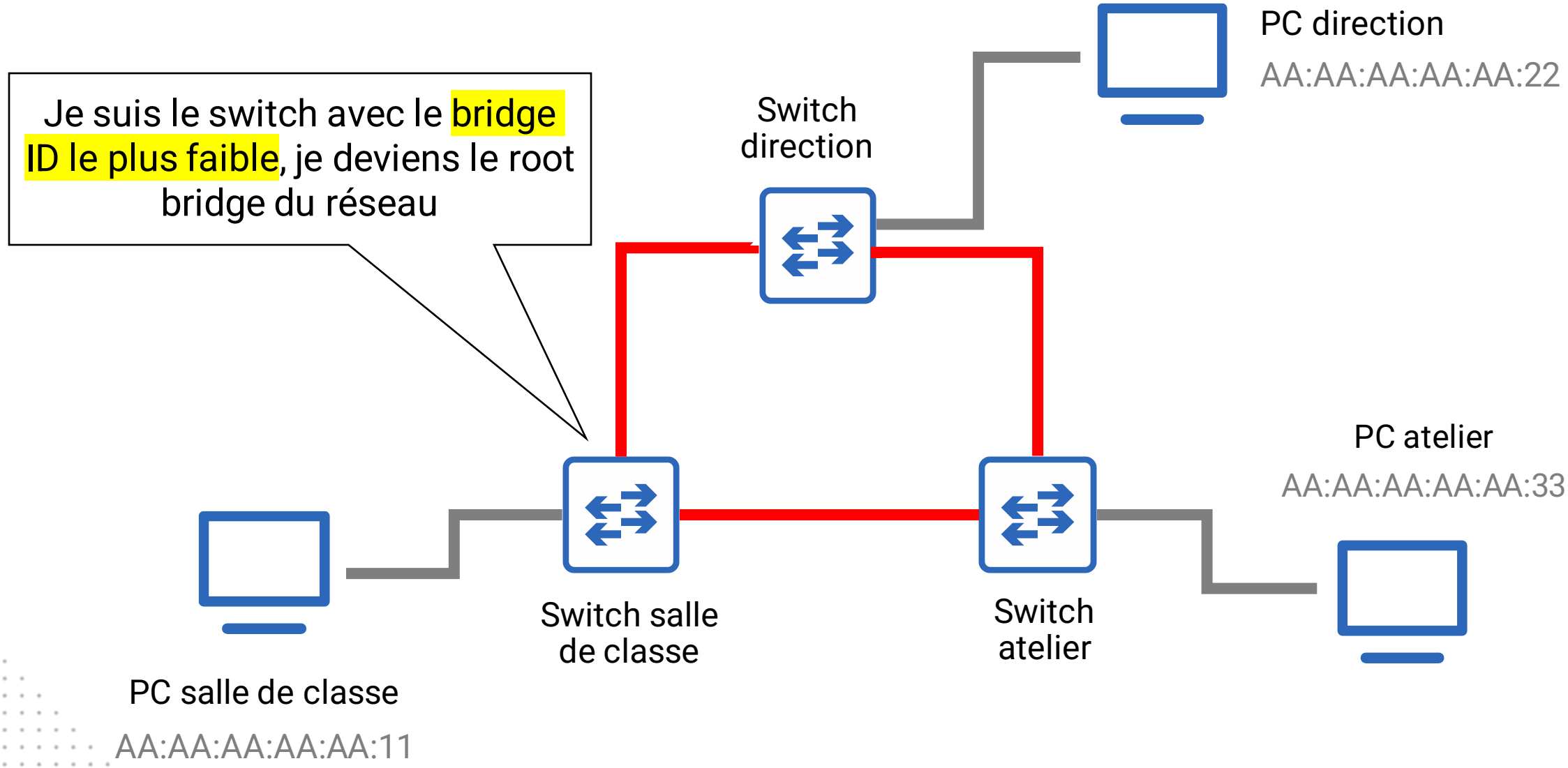
- Le protocole STP est supporté par tous les switchs modernes
- Uniquement pour switchs, vos équipements ne l’ont pas
- Election d’un root bridge et fermeture de ports sur les autres switchs

Transforme la boucle réseau en arbre réseau optimal

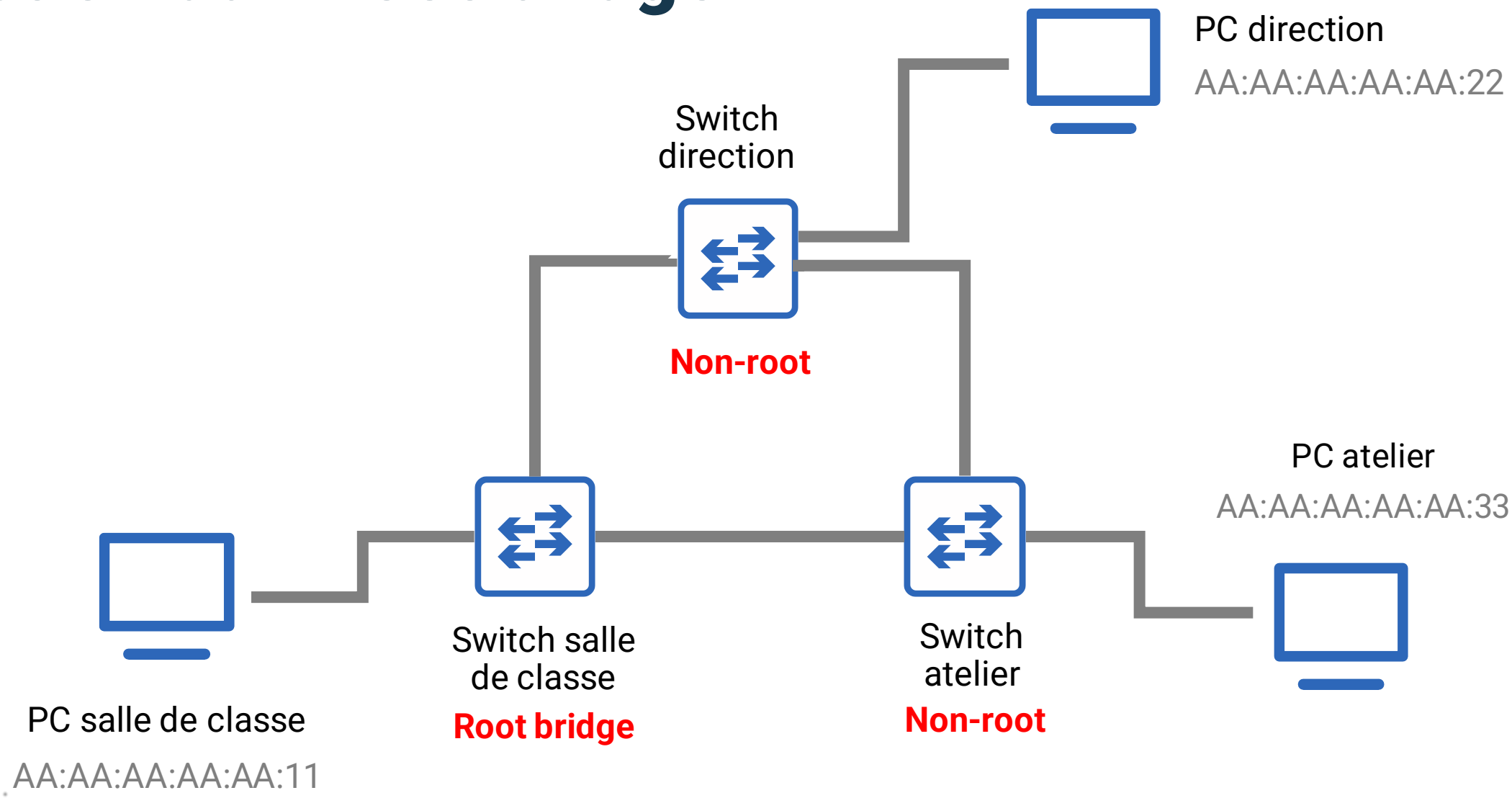
Processus d'élection



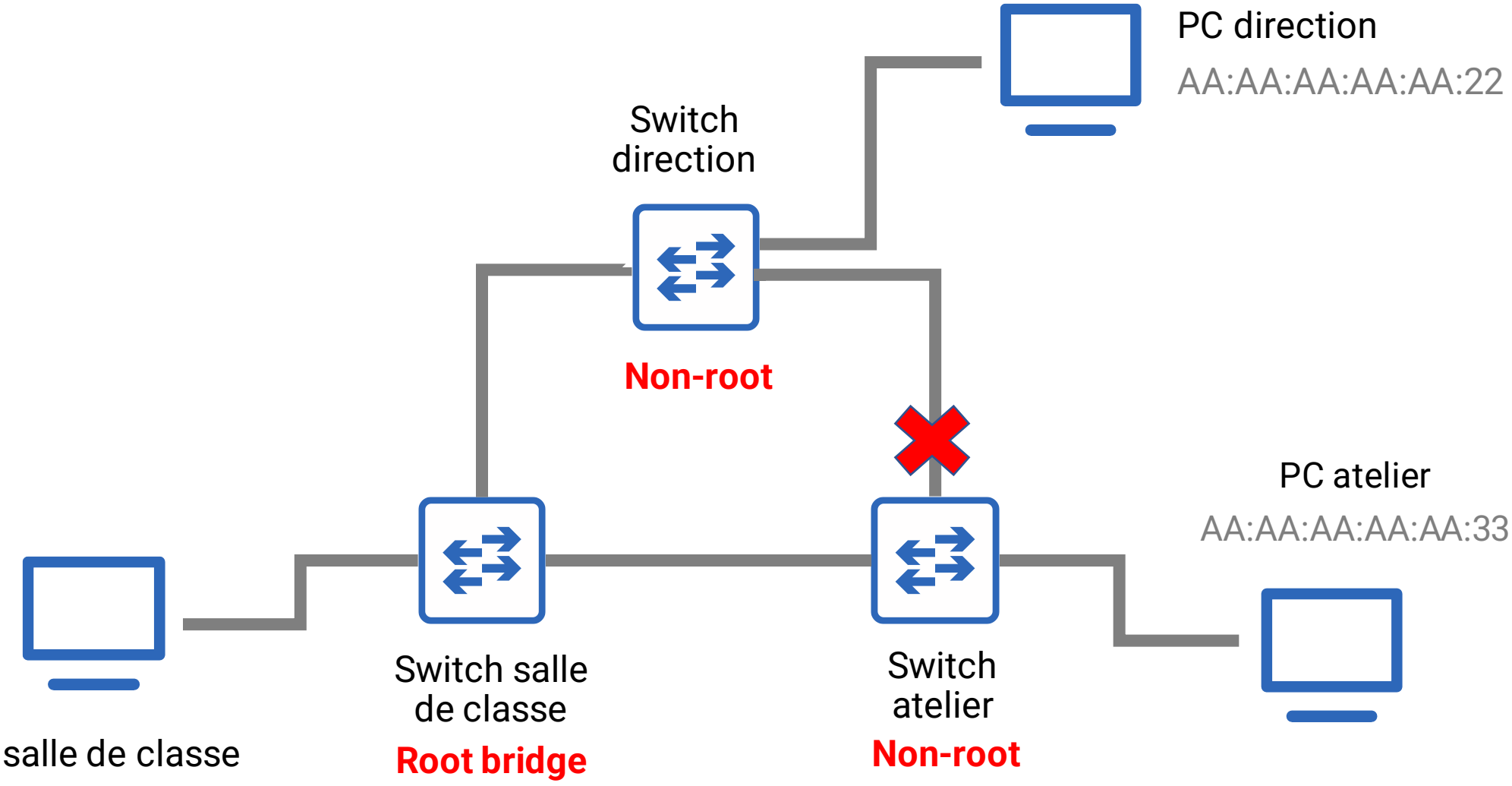
Processus d'élection



Election du « root bridge »



La boucle se transforme en arbre



Et les autres protocoles ?

La couche Data Link contient d’autres protocole qui ne seront pas abordés :

- PPP
- MPLS
- Token Ring
- Frame Relay
- …