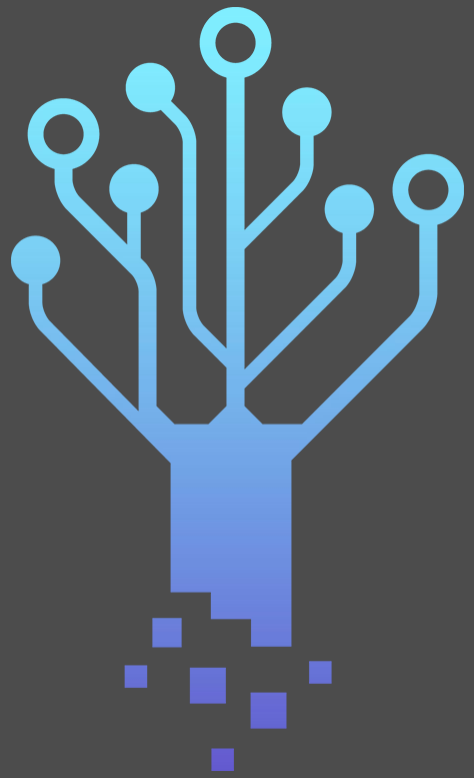


Network 102

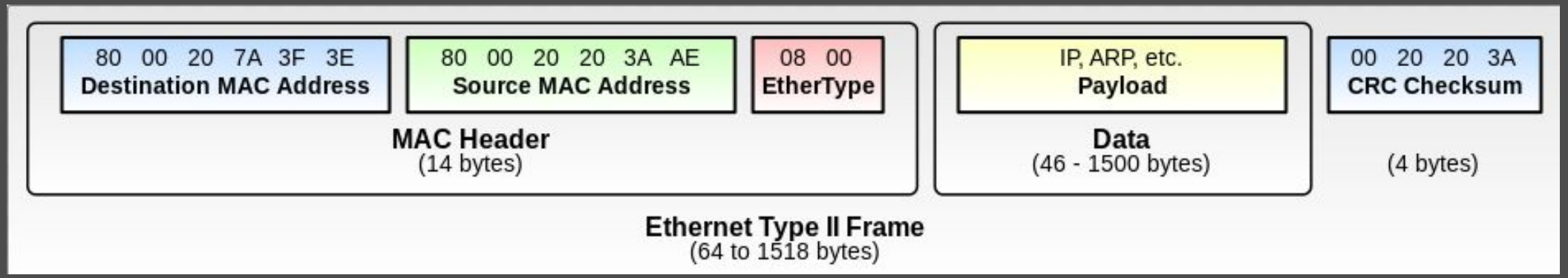
Find your way to disconnect people

Network 102 - Objectifs

- Comprendre le fonctionnement des réseaux switchés
- Comprendre les VLANs
- Comprendre le routage
- Découvrir l’infrastructure de la rez

Réseau Switché

Réseau switché = Réseau couche 2



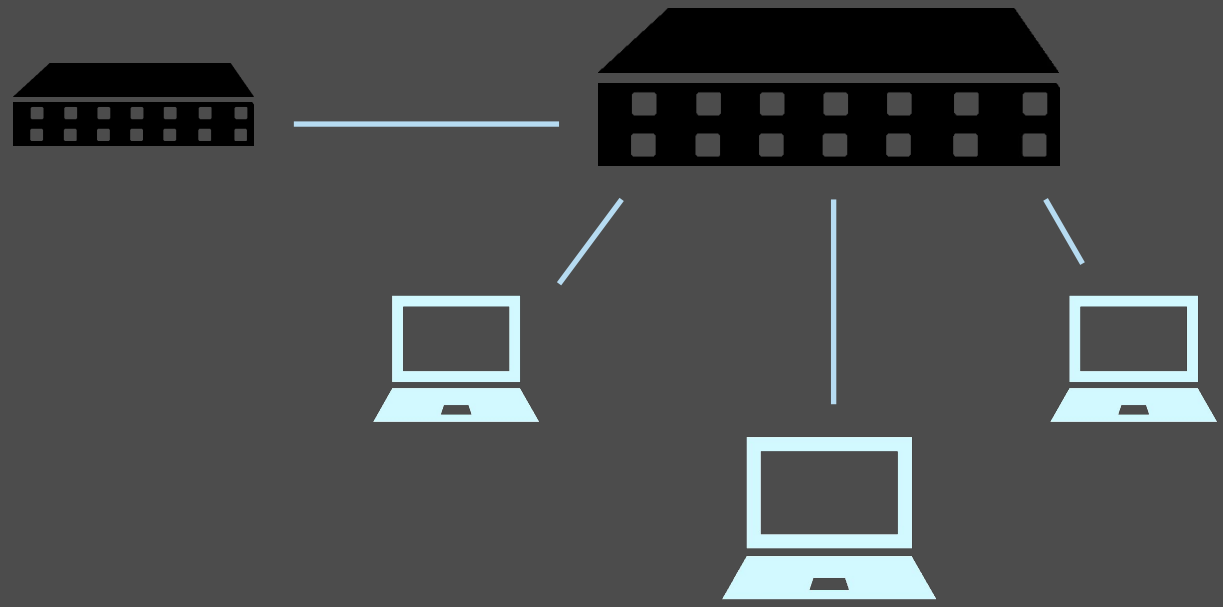
Switch

Table FDB: Correspondance adresse MAC / port

```
Slot-1 Router-d.3 # sh fdb
Mac                    Vlan       Age  Flags          Port / Virtual Port List
-------------------------------------------------------------------------------
00:01:30:11:8c:e1      vlcs(0002) 0047  d m           1:1
00:01:30:11:8d:24      vlcs(0002) 0047  d m           1:1
```

Réseau switché

Comment deux appareils communiquent-ils entre eux ?



Le switch dirige les trames selon l'adresse MAC de destination

Et en couche 3 ?

Pour que les appareils puissent communiquer, ils doivent avoir une adresse IP !

A un sous-réseau correspond une plage d'adresses IP

Exemple:

PC 1 : 192.168.2.1 \24

PC 2 : 192.168.2.2 \24

Comment passer de l'IP à la MAC ?

Pour parler sur un réseau switché, on doit mettre **l'adresse MAC** de destination

Comment connaître la **MAC** d'un appareil dont on ne connaît que l'adresse **IP ?**

Le Broadcast

L’adresse MAC **ff:ff:ff:ff:ff:ff** est réservée au broadcast

= adresse MAC générique pour dire “tout le monde sur le sous-réseau”

-> Un switch transmet une trame avec **ff:ff:ff:ff:ff:ff** comme MAC de destination sur **tous** ses ports

Ainsi, un appareil peut parler **à tout le monde en même temps !**

Comment passer de l'IP à la MAC ?

Pour parler sur un réseau switché, on doit mettre **l'adresse MAC** de destination

Comment connaître la **MAC** d'un appareil dont on ne connaît que l'adresse **IP ?**

Les requêtes ARP

ARP = Address Resolution Protocol

PC 1 : 192.168.2.1 \24

PC 2 : 192.168.2.2 \24

PC 1 envoie une requête du type “**Qui a l’adresse 192.168.2.2 ?**”

Tout le monde reçoit le paquet, seul **PC 2** répond avec son **adresse MAC**

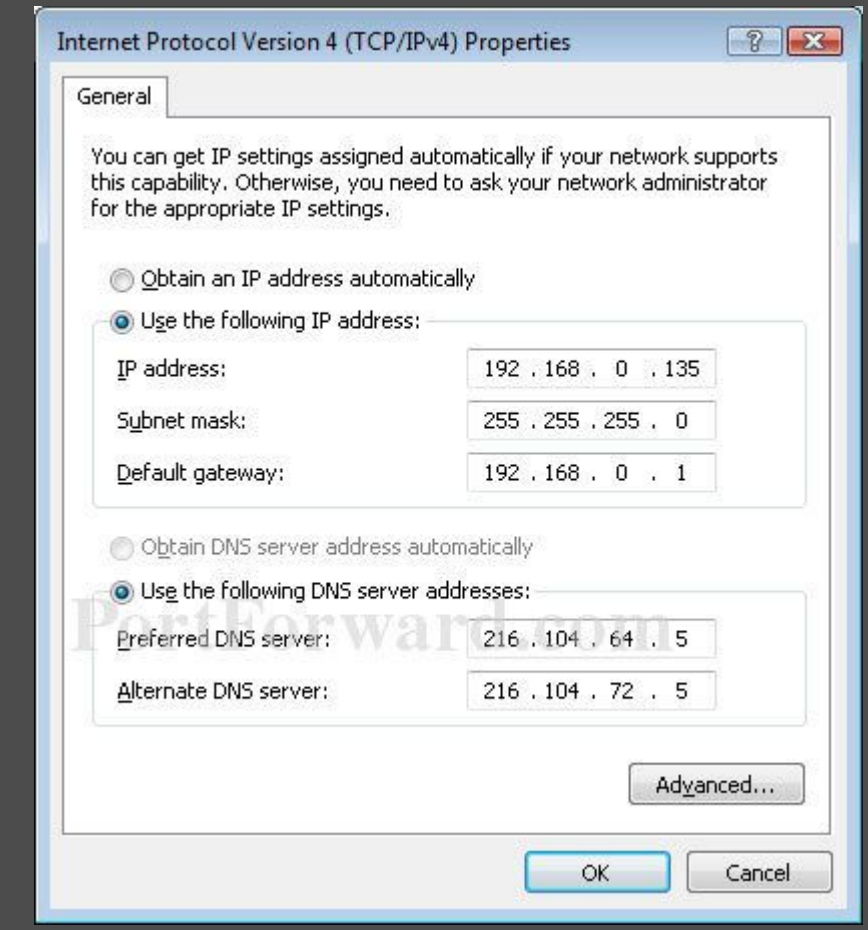
PC 1 enregistre la réponse dans son **cache ARP** pour ne pas redemander à chaque fois

Comment obtient-t-on une IP ?

Comment sont attribuées les adresses IP ?

- **statiquement:** on les entre manuellement sur chaque appareil

- **dynamiquement:** on utilise un **serveur DHCP**



Le DHCP

Que se passe-t-il lorsqu'on se connecte à un réseau ?

- La **table FDB** du switch est mise à jour

```
Slot-1 Router-d.3 # sh fdb
Mac                   Vlan       Age  Flags          Port / Virtual Port List
-------------------------------------------------------------------------------
00:01:30:11:8c:e1     vlcs(0002) 0047  d m            1:1
00:01:30:11:8d:24     vlcs(0002) 0047  d m            1:1
```

- Le client veut maintenant avoir une **adresse IP**
- Il utilise le **DHCP (Dynamic Host Configuration Protocol)**

Le DHCP

- Le client demande une **adresse IP** au **serveur DHCP**
- Il ne **sait pas** qui est le DHCP -> broadcast !
  - **DISCOVER:** (PC1 en broadcast): Hello, j'aimerais bien avoir une IP !
  - **OFFER:** (DHCP -> PC1): Hello, je suis le DHCP. **192.168.0.37 est libre !**
  - **REQUEST** (PC1):Je veux bien prendre **192.168.0.37 !**
  - **ACK:** (DHCP): Ca marche !

Le DHCP

Le **DHCP** renvoie aussi:

- la **durée du bail** (lease)
- **le masque de sous-réseau**
- **la gateway**
- l'adresse d'un ou plusieurs **serveurs DNS**

Résumé

FDB: Correspondance **MAC / port**

ARP: Correspondance **IP / MAC**

DHCP: Permet d'obtenir une **adresse IP** (et d'autres infos)

Limite des réseaux switchés

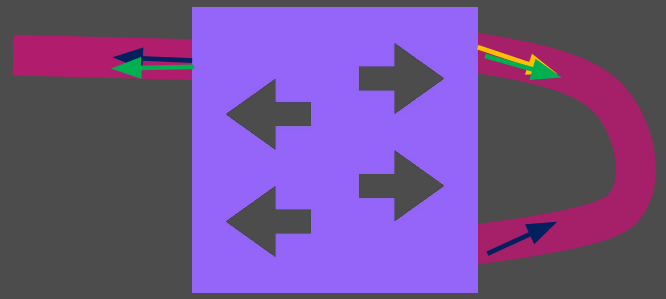
- **Tout le monde** broadcast vers **tout le monde !**

Au bout d'une taille critique (~1000 appareils), tout le monde se fait spammer de broadcast et la connexion est ralentie !

- On ne peut pas **isoler des machines** ! (sécurité...)
- Il peut y avoir des boucles !

Les boucles

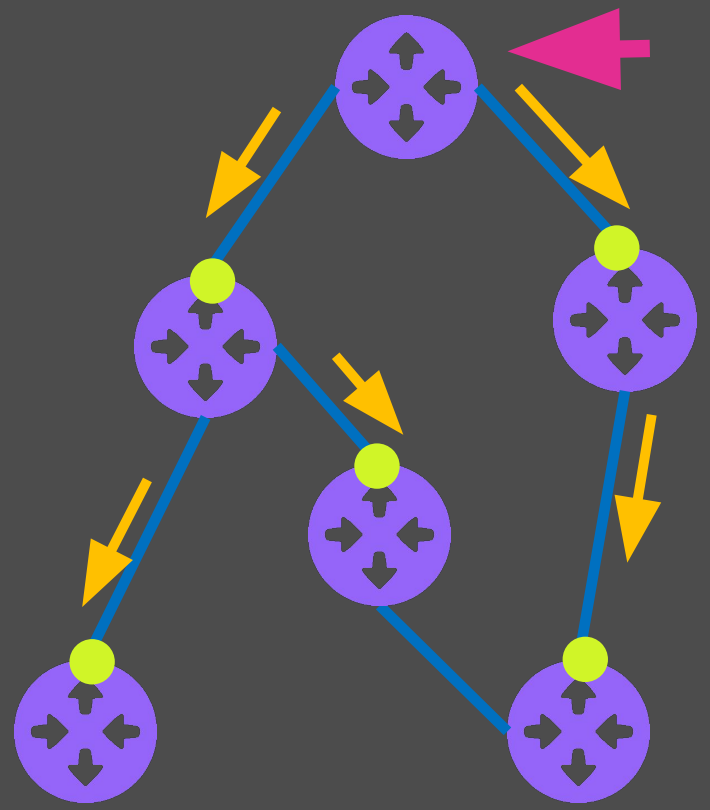
Si on fait une boucle sur un switch...



Les broadcast sont **rediffusés à l'infini** dans la boucle !

Le STP

Pour éviter les boucles, on **désactive certains liens:** Le protocole STP permet de choisir quels liens garder en calculant un arbre de poids minimal

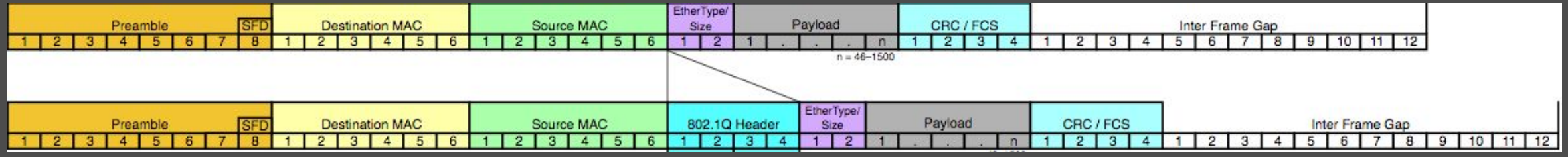


Les VLANs

LAN = Sous-réseau = réseau switché = domaine de broadcast

Comment mettre **plusieurs réseaux switchés différents** sur le **même câble ?**

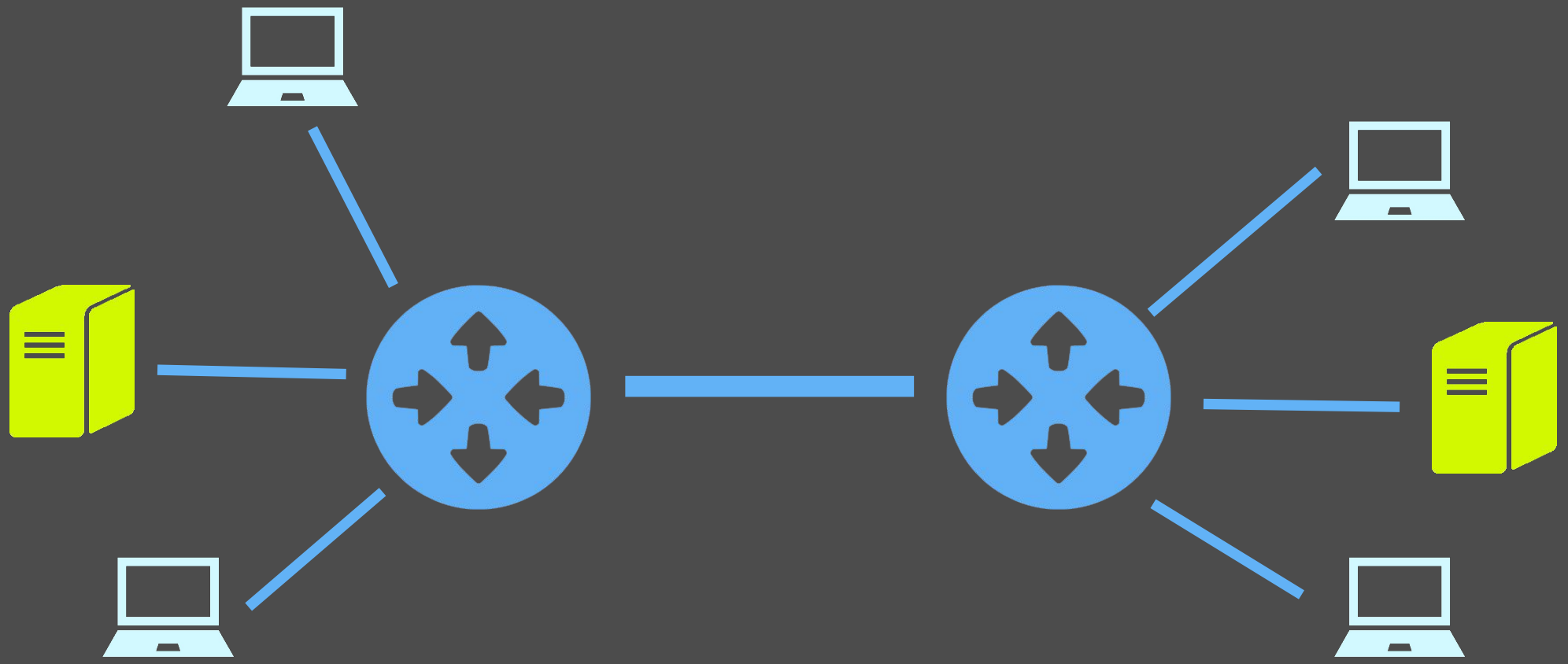
VLAN = Virtual LAN



On rajoute un **tag de VLAN** sur la trame dans l'entête couche 2

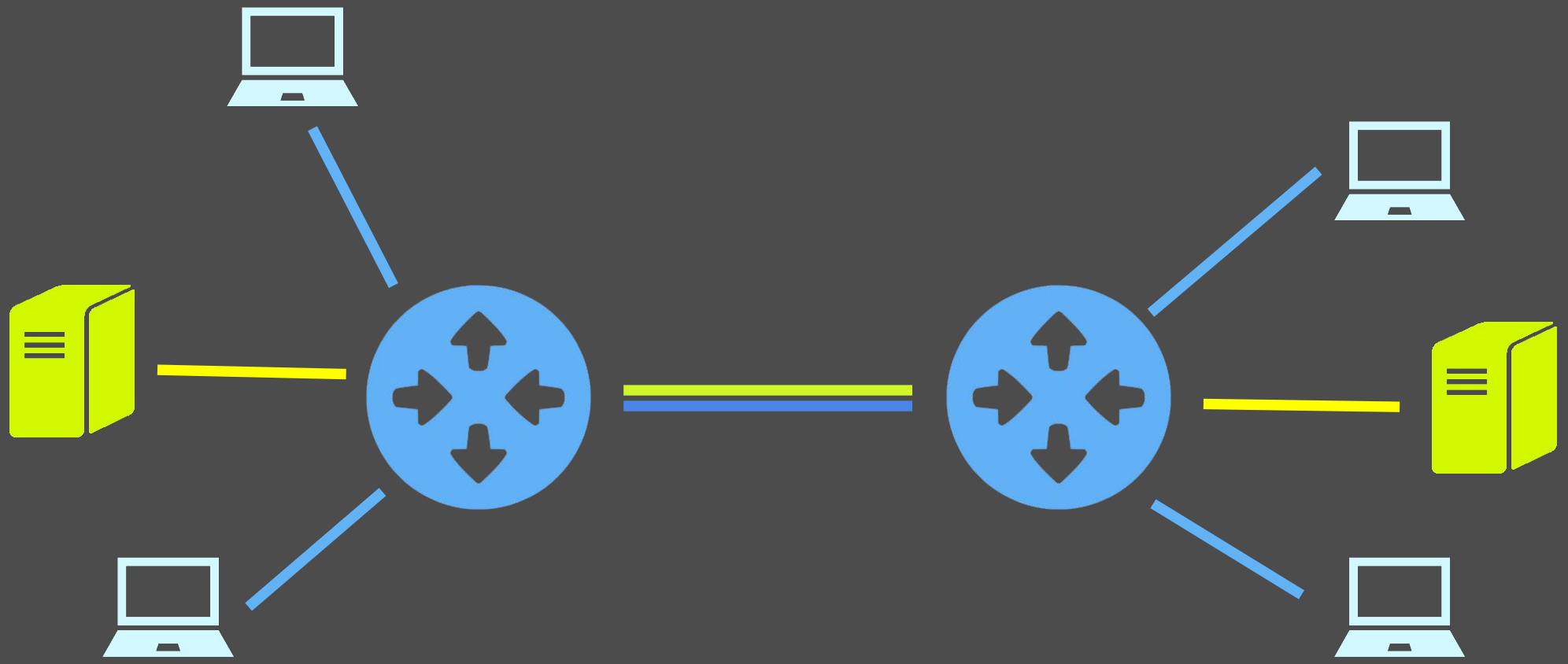
Les VLANs

Un seul câble physique



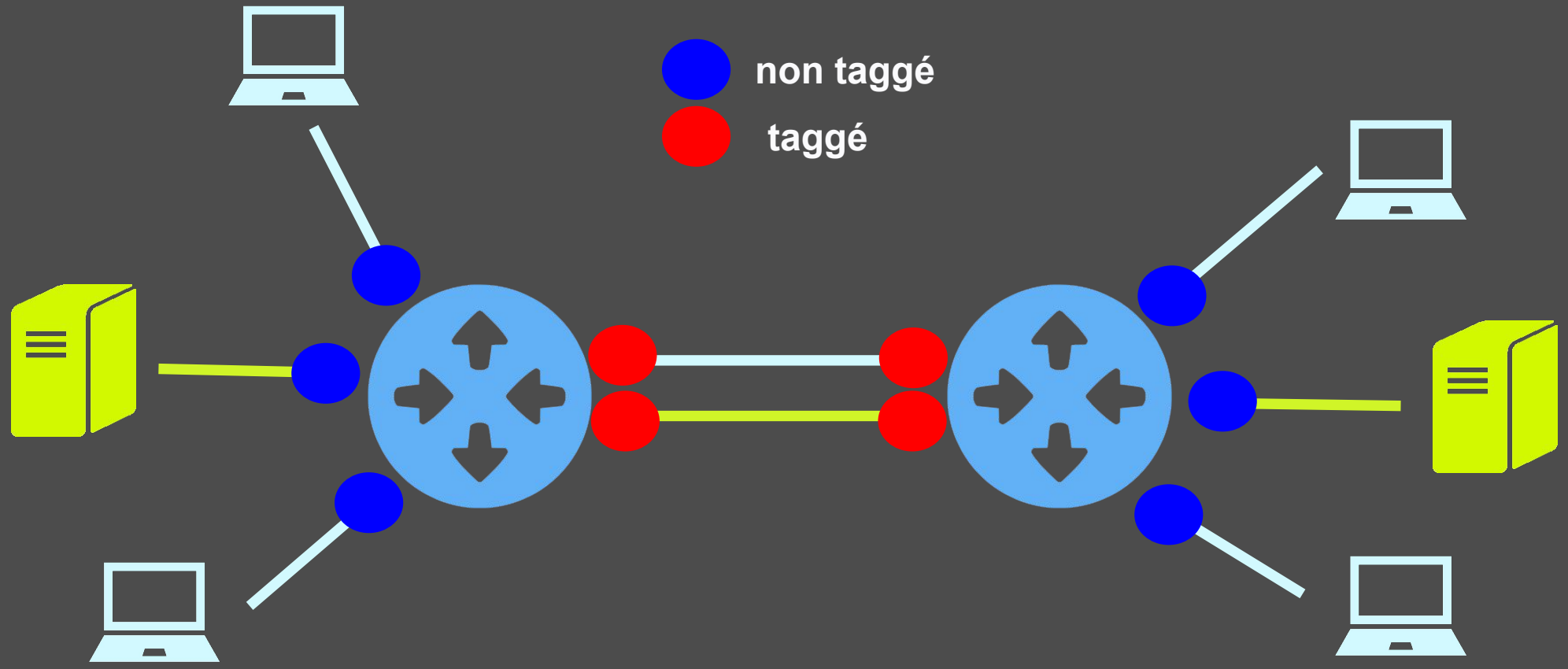
Les VLANs

Plusieurs réseaux sur le même câble !



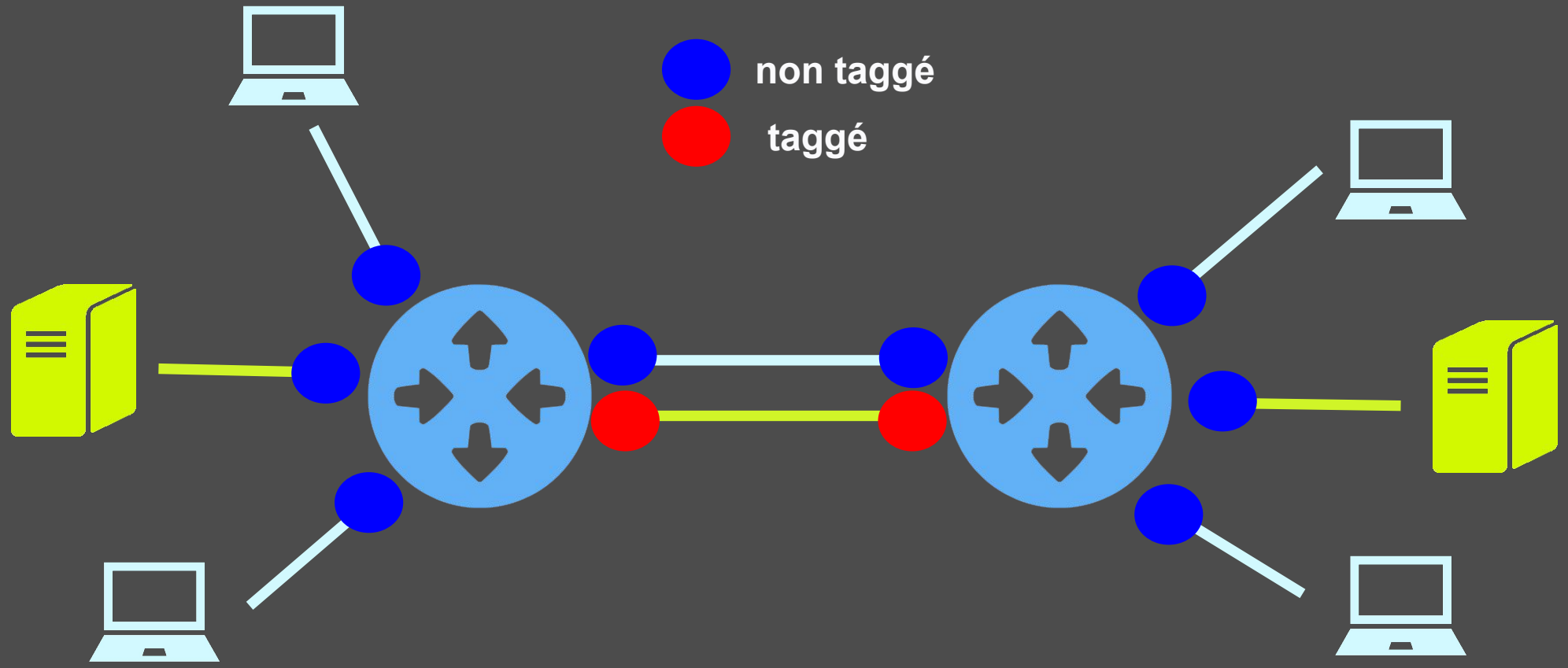
Trames taggées

Un PC lambda **n'est pas configuré pour recevoir des trames taggées !**



Trames taggées

On ne peut avoir **qu'un VLAN non taggé par port !**



Isolation des machines

Les paquets ne peuvent pas forcément **passer d'un VLAN à l'autre**

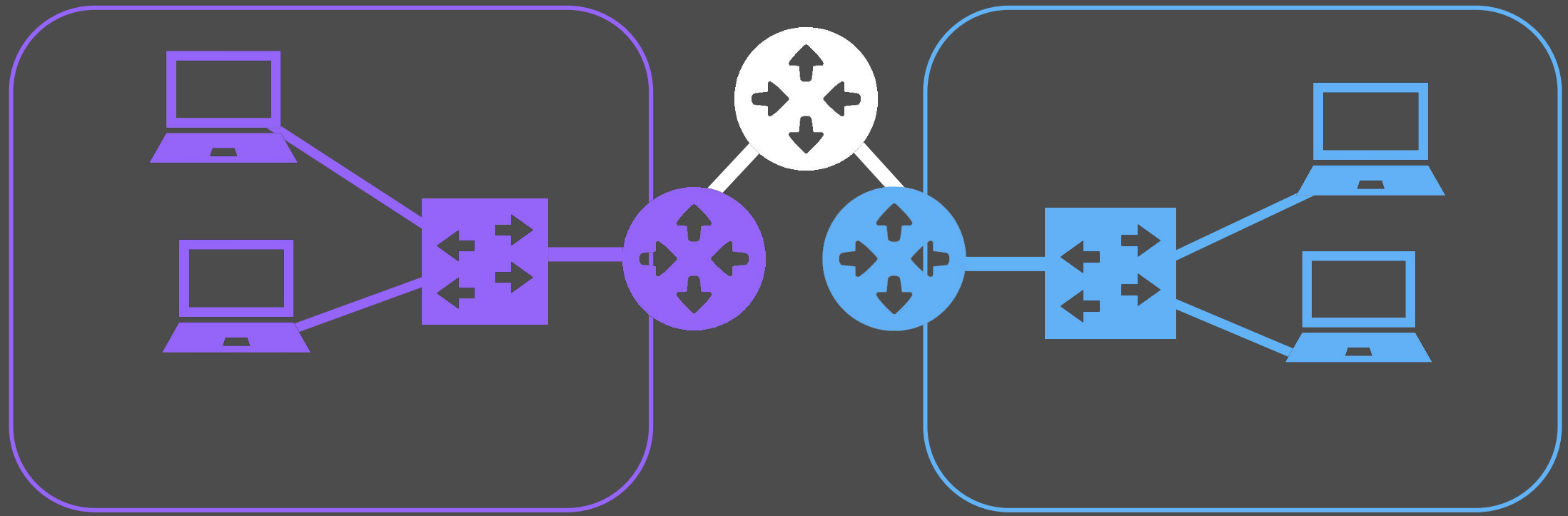
- On peut activer ou désactiver **l'IP Forwarding**

et le DHCP?

Si le DHCP n'est **pas dans le même VLAN**, il ne recevra pas les requêtes DHCP des appareils...

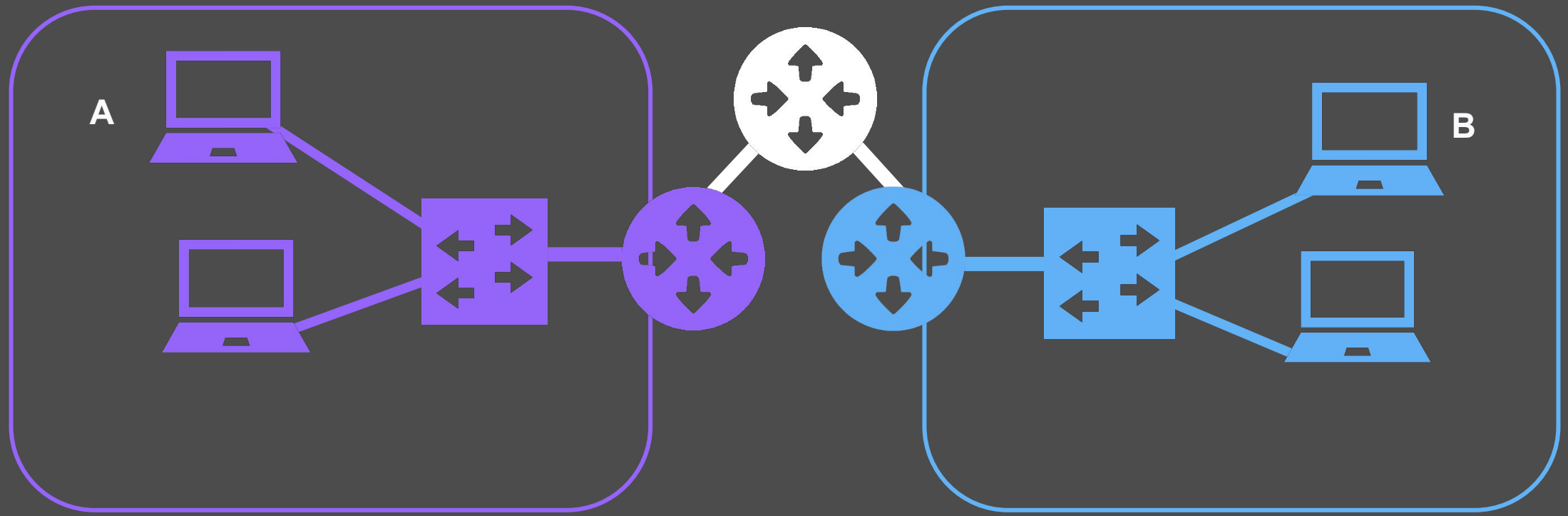
- On utilise le **DHCP Relay** sur le switch
- Le switch **transfère les requêtes DHCP** sur le bon VLAN

Routage



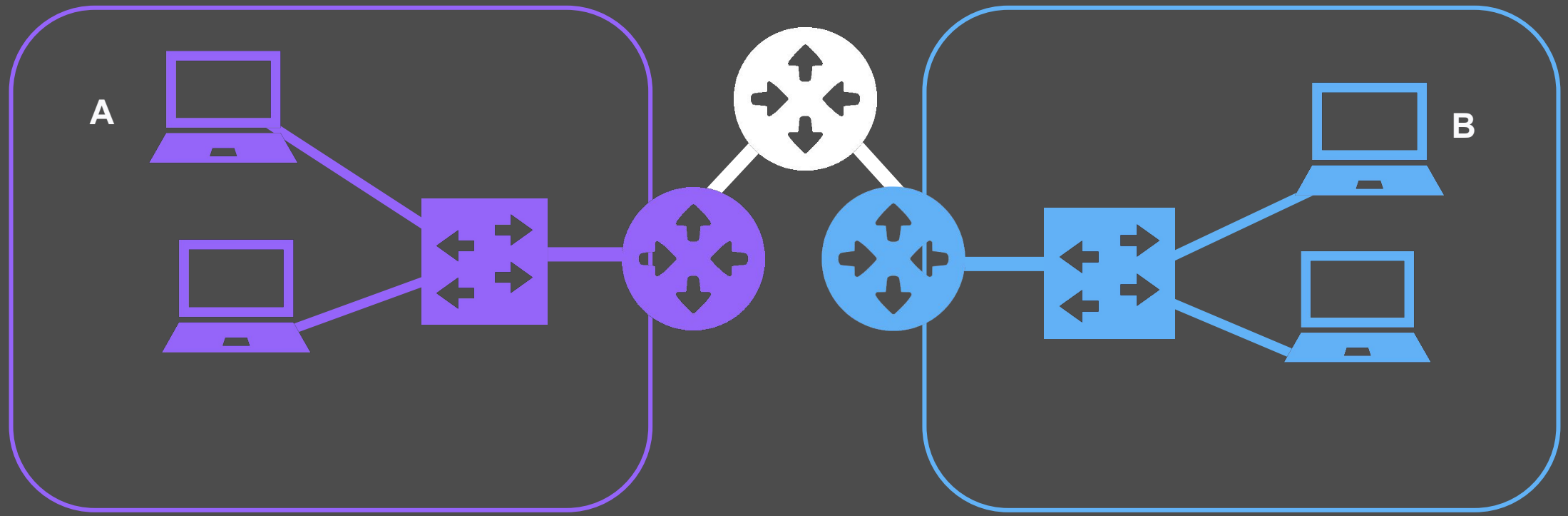
- A veut contacter B

Routage



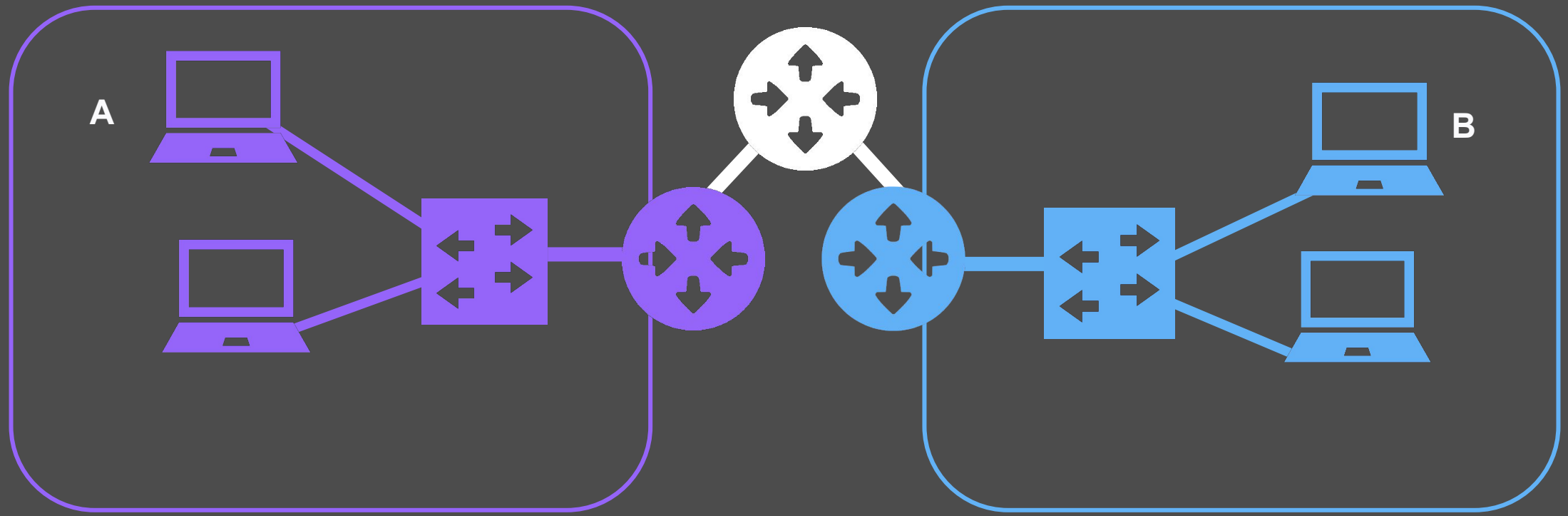
- Le DHCP a donné à A l’adresse IP le la gateway (routeur qui permet de sortir du sous-réseau)

Routage



- Le DHCP a donné à A l’adresse IP le la gateway (routeur qui permet de sortir du sous-réseau)
- A fait une requête ARP pour connaître l’adresse MAC de la gateway

Routage

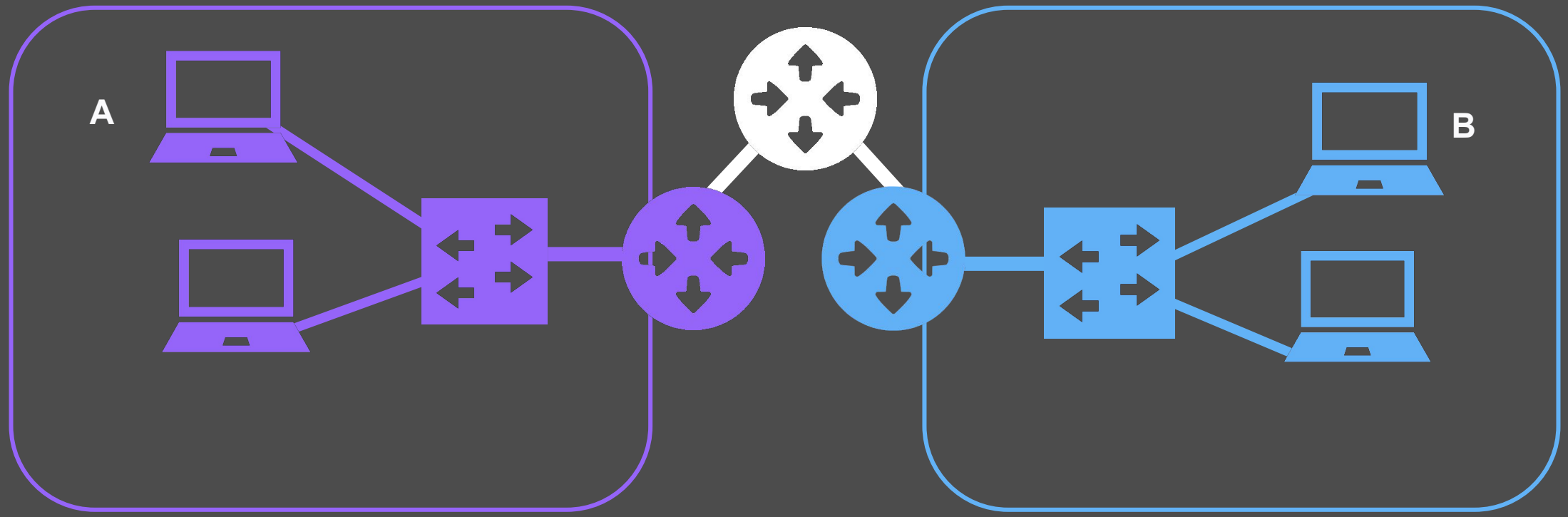


A met:

- la MAC de la gateway comme MAC de destination

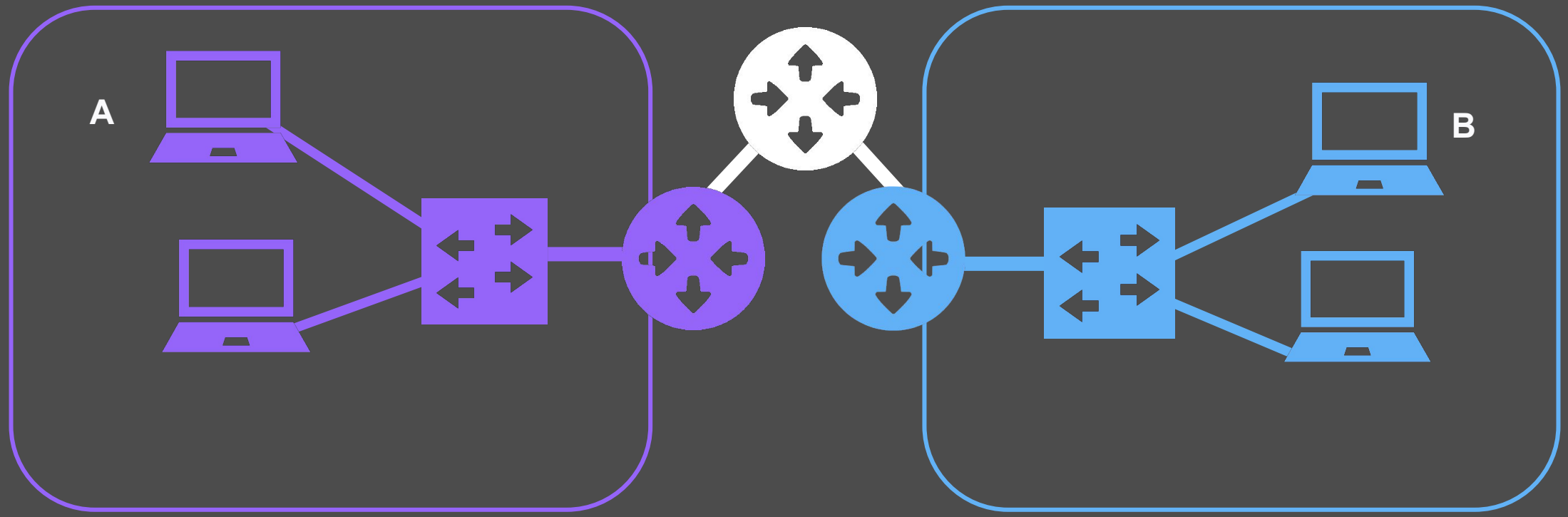
- l'IP de B comme IP de destination

Routage



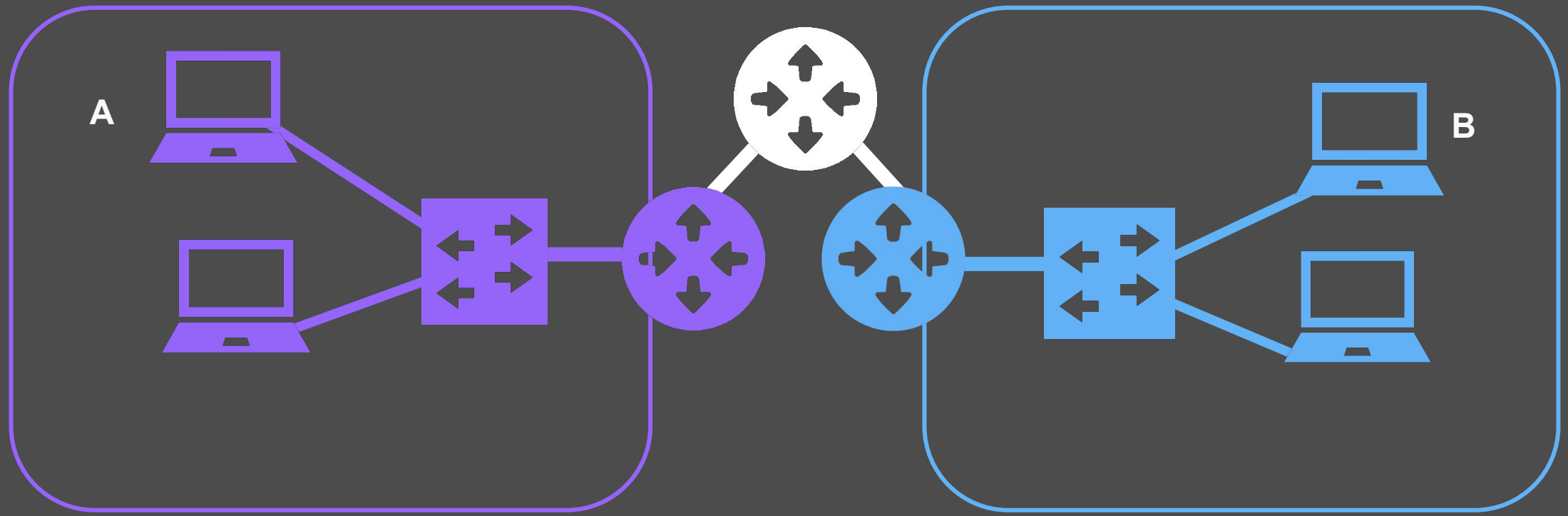
Le paquet est switché jusqu’à la gateway, ou sa MAC de destination change pour le prochain routeur

Routage



Le paquet arrive sur le routeur du sous-réseau de B, qui voit que l'IP de destination est dans la plage d'IP du sous-réseau

Routage



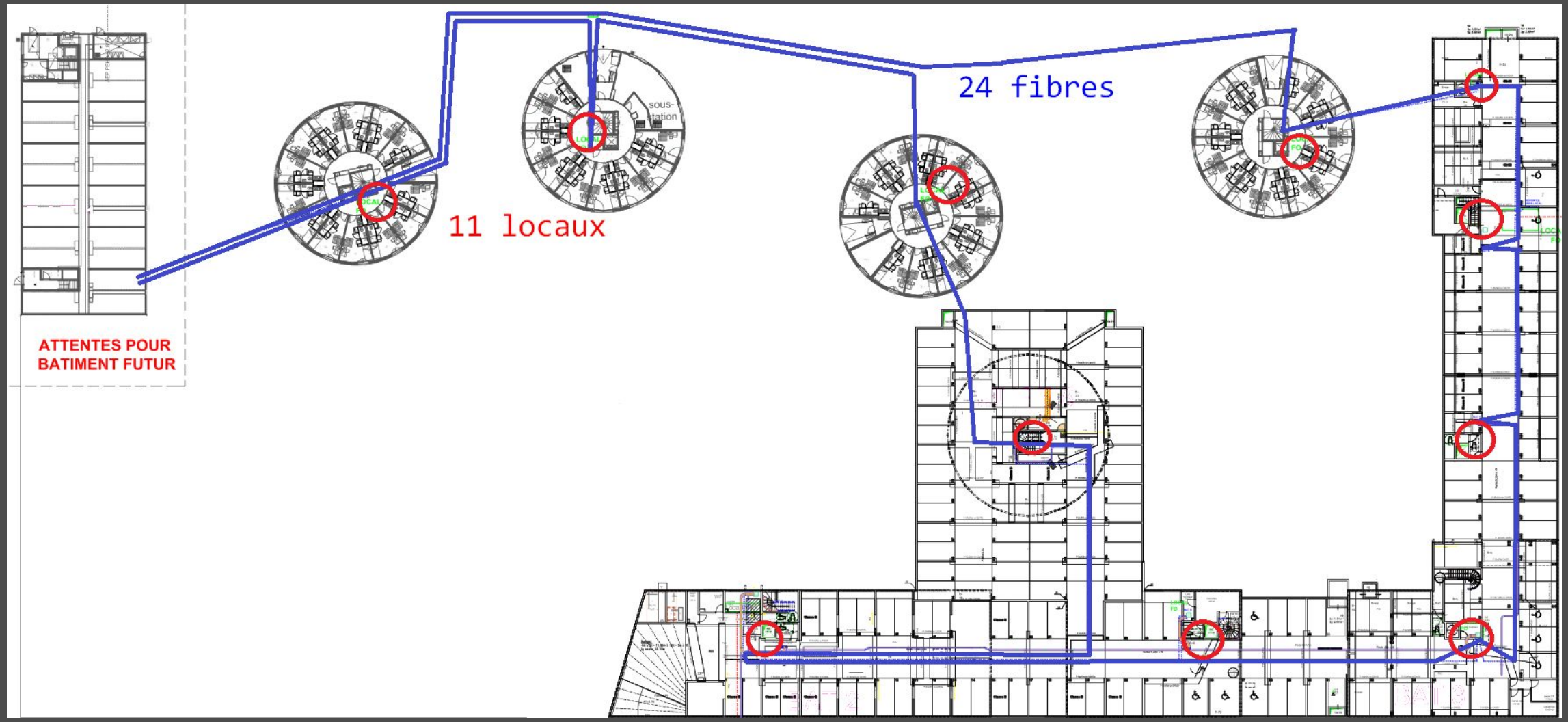
Le routeur de B regarde dans sa table ARP la MAC de B et change la MAC de destination pour la MAC de B.

Le paquet est alors switché jusqu’à B

Pratique

Avec **Wireshark**, essayez de voir vos requêtes **DHCP** et **ARP** passer !

L’infrastructure de la Rez 4



Le NAT (Network Address Translation)

Par **manque d'adresse IP,** certaines plages sont réservées pour un **usage local:**

- **10.0.0.0/8**
- **172.16.0.0/12**
- **192.168.0.0/16**

Aucun appareil n'a cette adresse IP sur Internet

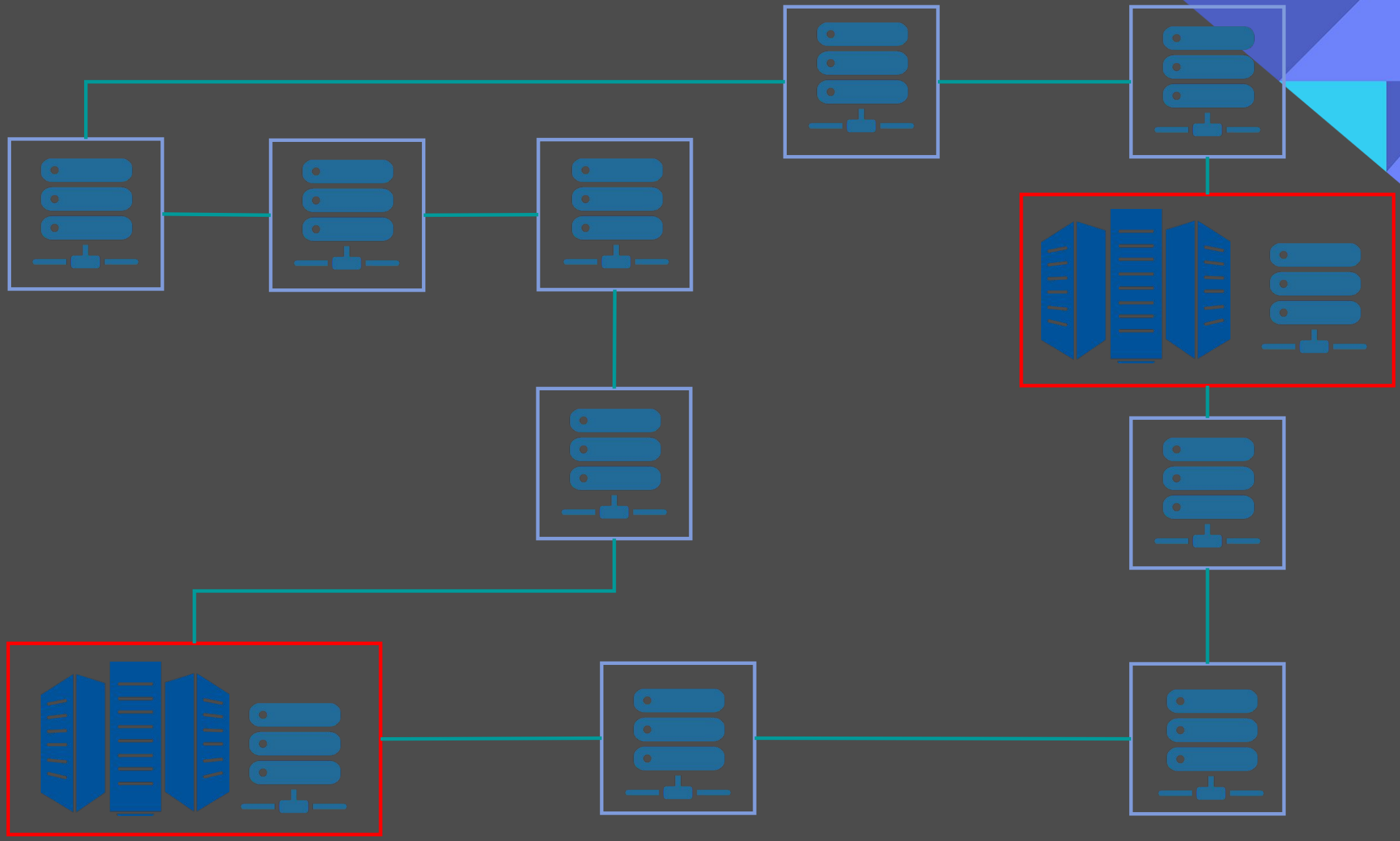
Le NAT (Network Address Translation)

Principe: On met **plusieurs IP locales** derrière une **IP publique**

La machine qui fait le NAT substitue l'adresse **IP source des paquets sortants** et l'adresse **IP de destination des paquets entrants**

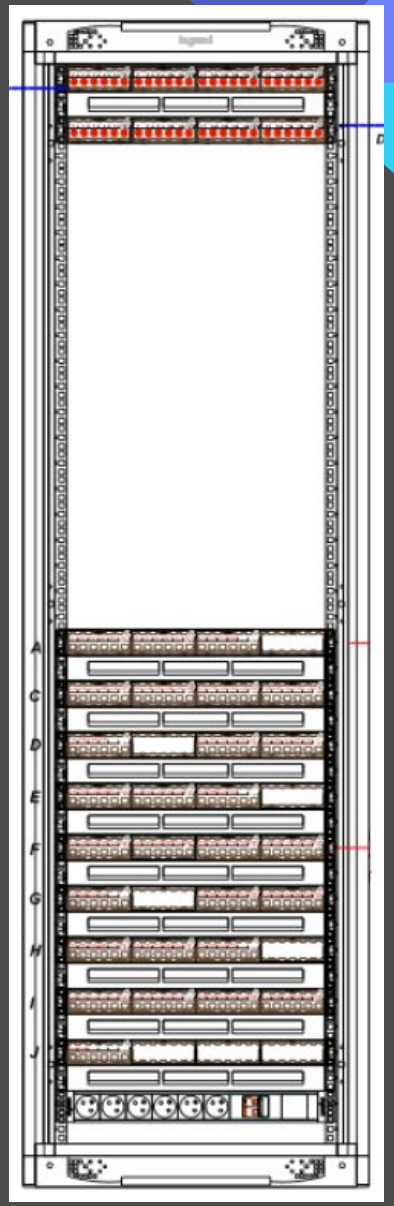
Sur une Livebox, **193.168.0.0/16** est utilisé

Inconvénient: on ne peut initier une **connexion entrante que vers un seul appareil** (par port)



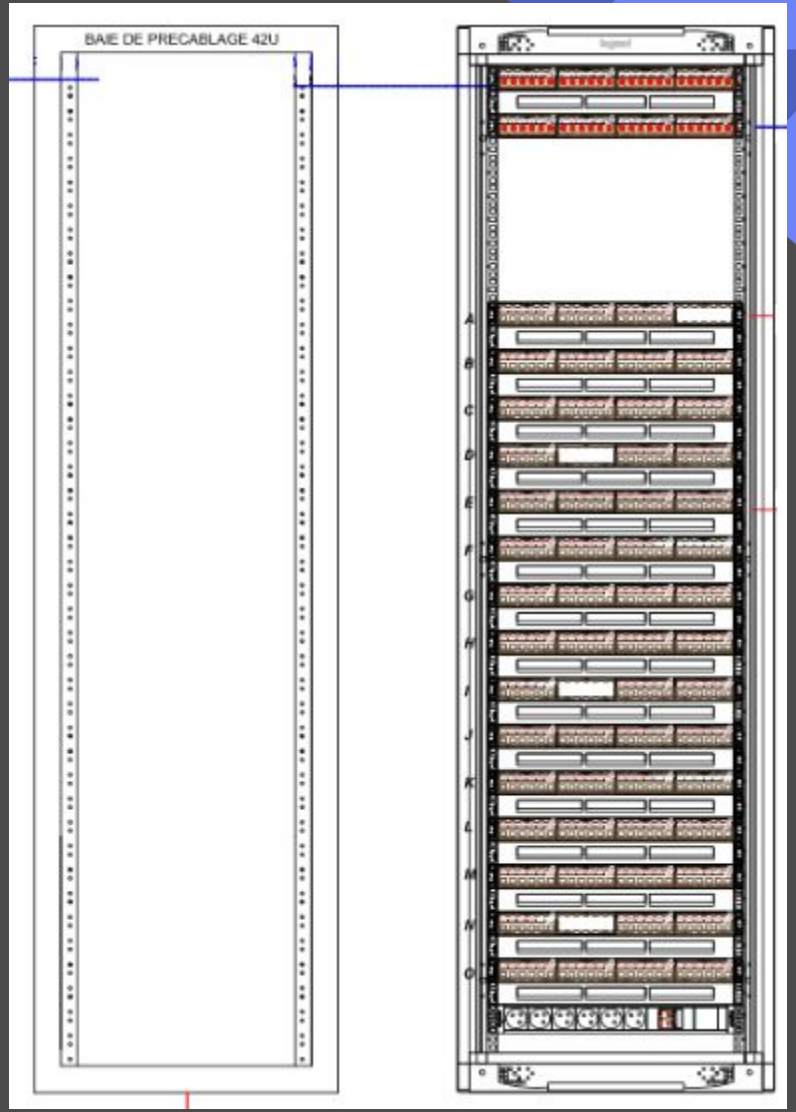
Architecture d'une salle de brassage

- 75 à 150 chambres à connecter
- Environ 15 bornes Wifi à alimenter et connecter
- Une armoire de rack par salle de brassage:
  - Boucle optique
  - 1 à 3 switches 48 ports (Juniper EX3400 48T)
  - 1 switch 48 ports **PoE** (EX3400 48P)
  - Platines qui desservent les chambres

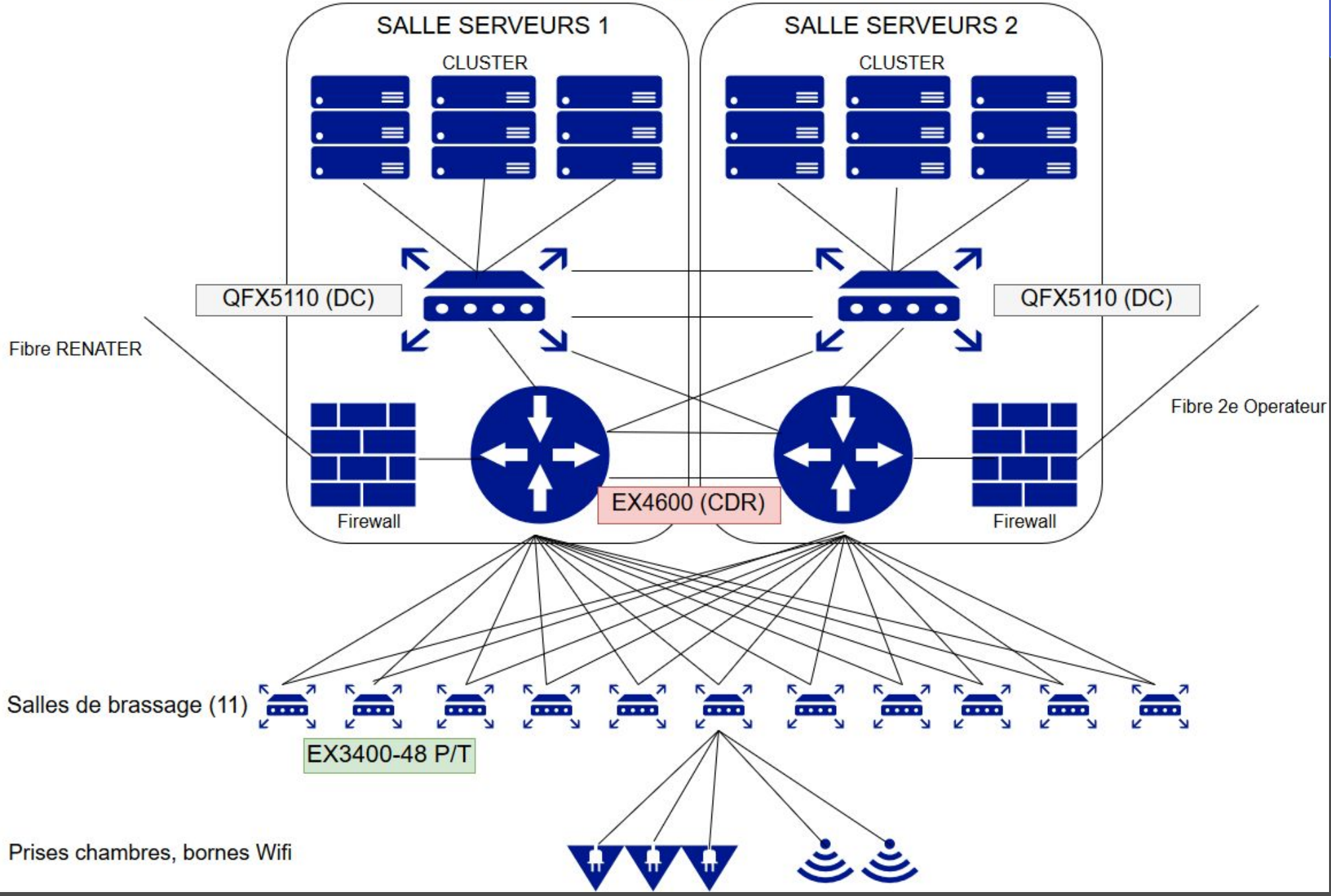


Architecture d’une salle serveur

- Partie brassage identique
- Arrivée d’une fibre (Renater ou Interoute)
- Firewall
- Un cœur de réseau (EX4600)
- Switch pour les machines du cluster (QFX5100)
- Machines du cluster



RESEAU VIA CESAL 4



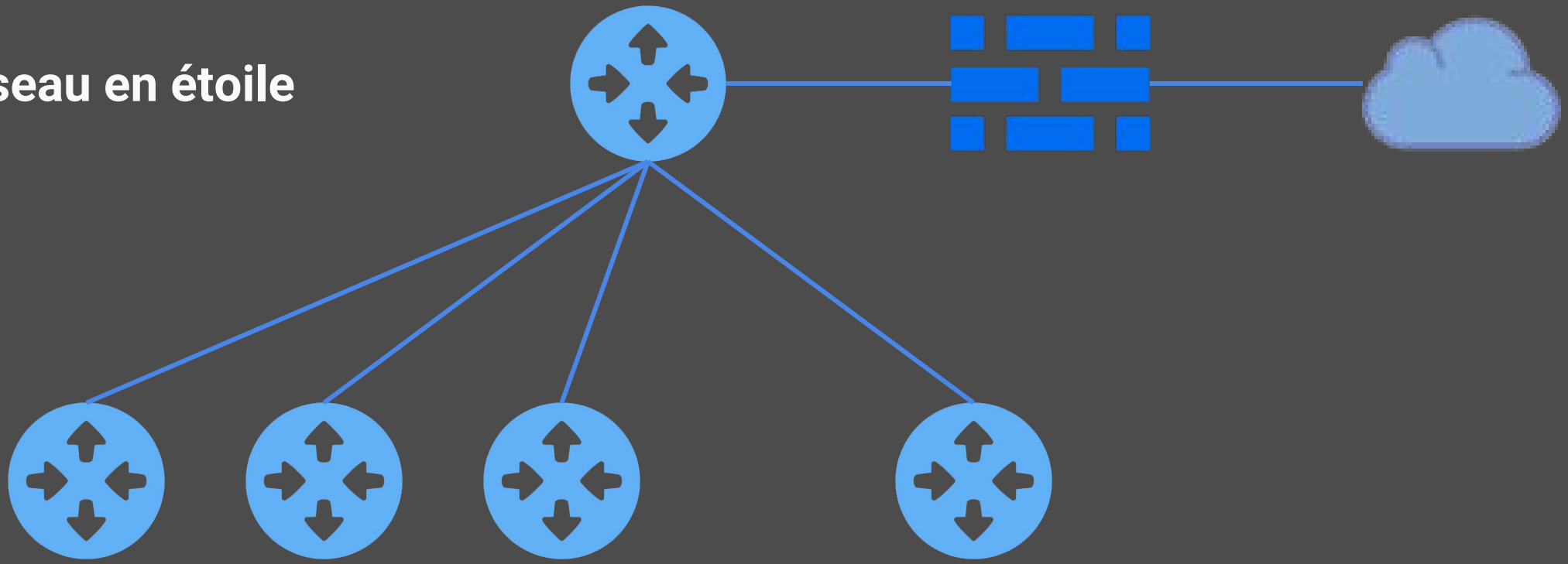
Aggrégats de liens physiques

Le protocole **802.3ad** permet d'aggréger plusieurs liens physiques pour faire comme s'il n'y en avait qu'un

- **load-balancing** du traffic -> **2 fois plus de débit**
- **redondance des liens**

Architecture logique

Réseau en étoile



Architecture des VLANs

Un VLAN par adhérent !

Chacun a **son propre sous-réseau en /24 (255 adresses possibles)**

Chaque sous-réseau est **NATé derrière une IP publique** (Une IP publique par adhérent)

Avec une plage d'IPs de la forme **10.x.y.0/24**

Authentification

Comment déployer les VLANs dynamiquement sur les ports ?

Protocole 802.1X:

Authentification -> Déploiement d’un certain VLAN

Authentification avec le **protocole RADIUS**

Authentification

802.1X

RADIUS

Serveur freeradius

Credentials

Webaz

Autorisation?

Pratique

Avec **Wireshark**, regardez passer vos requêtes **EAP** vers le **serveur RADIUS !**