COURS #8

NAT, DHCP & protocoles L7

Introduction aux réseaux 2025 (Bloc 2)

Corentin Badot-Bertrand

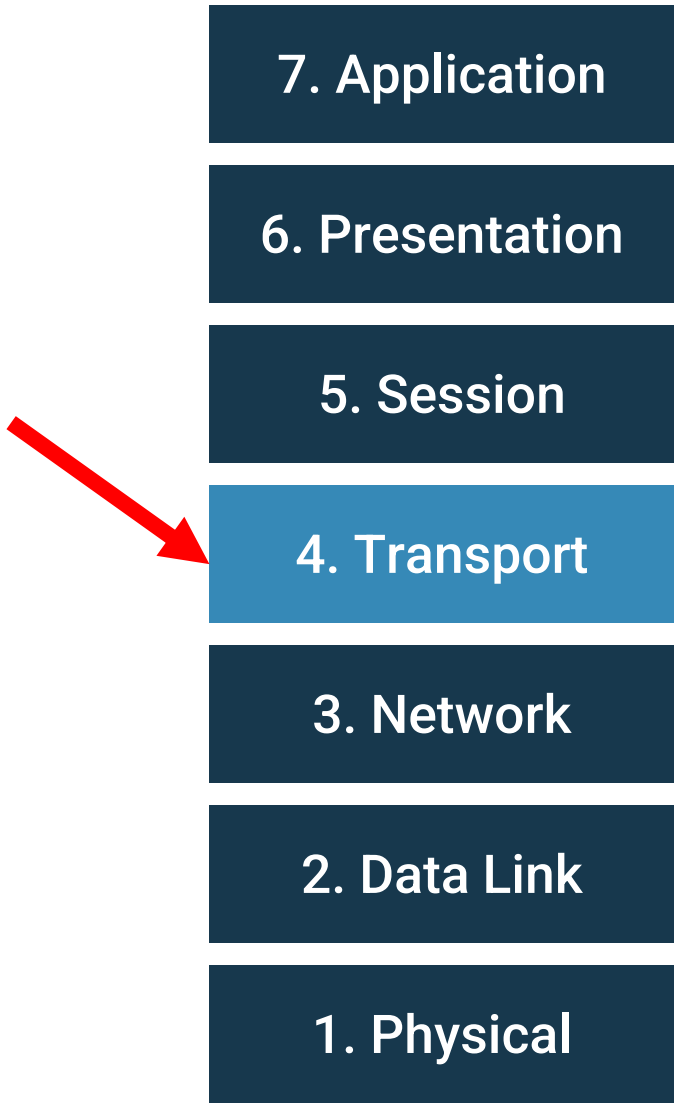
PREAMBULE

Rappels & mise en contexte

Quelques rappels sur le cours précédent avant de commencer

Dans l’épisode précédent

- Couche Transport (L4)
- Limites de la couche L3
- Protocoles TCP & UDP
- Cas d’usages




Questions
pour un
Champion

Que signifie un « port » d’un point de vue réseau ?

Concept de ports

Une « boite aux lettres » virtuelle pour contacter un processus

- Chaque paquet dans un segment de la couche OSI L4
- … contient un port source & destination
- Un processus peut écouter sur le réseau via un port
- Les ports entre 0 et 1023 nécessitent des droits

Quelles sont les différences entre TCP & UDP ?

TCP vs UDP

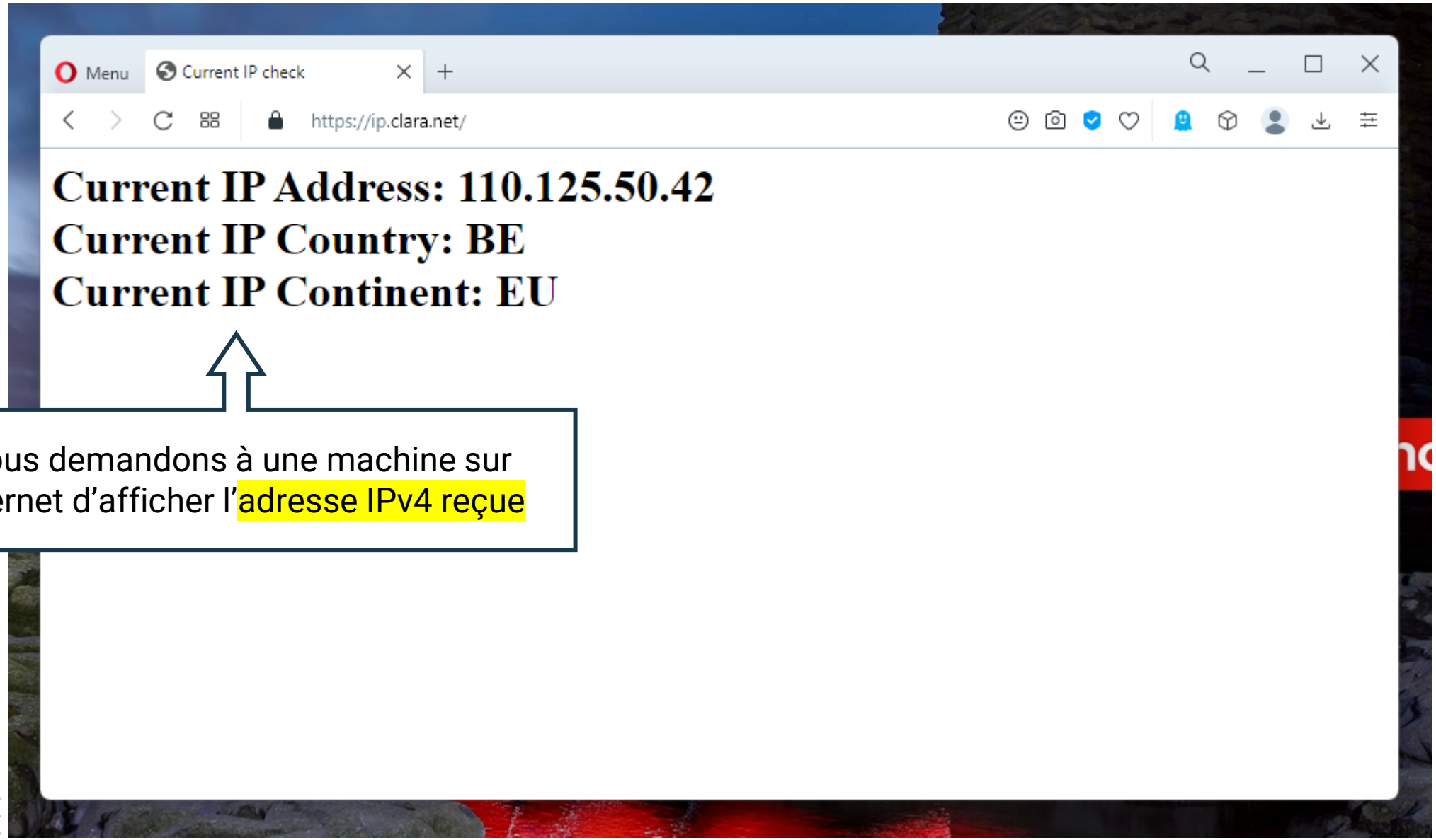
Quelques différences entre les protocoles de la couche L4

	Protocole TCP	**Protocole UDP**
Connexion	*3-way handshake*	Sans connexion
Fiabilité de livraison	Très fiable	Non-fiable
Gestion des erreurs	Complète (garantie d'intégrité, …)	Minime (checksum basique, …)
Vitesse	Lent	Rapide
Ordre	Garanti	Non-garanti

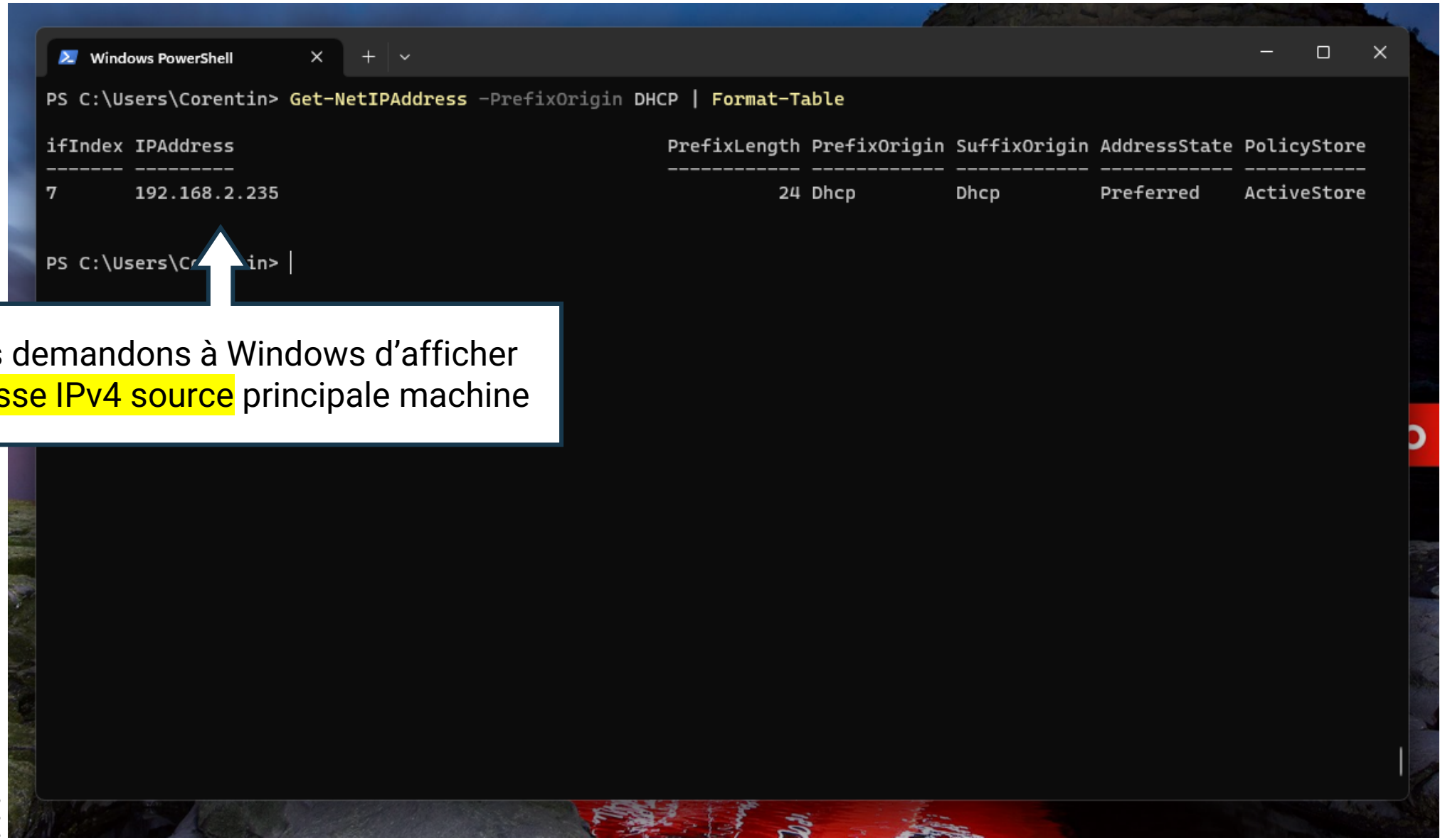
PARTIE #1

Réseaux privés & technique NAT

Network Address Translation,
la traduction d'adresses IPv4



Nous demandons à une machine sur Internet d'afficher l'adresse IPv4 reçue



Nous demandons à Windows d'afficher l'adresse IPv4 source principale machine

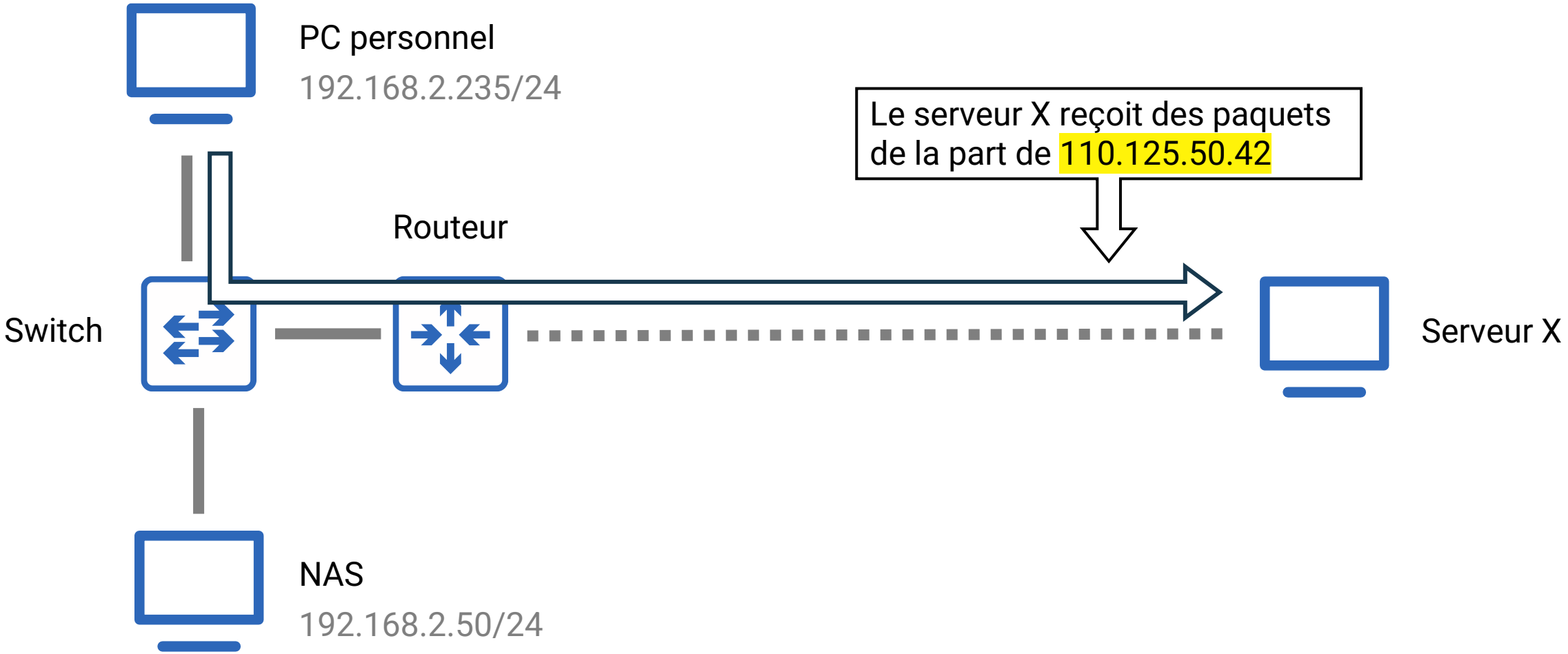

IPv4 source : 192.168.2.235
Adresse privée
IPv4 source : 110.125.50.32
Adresse publique
PC personnel
192.168.2.235/24
Serveur X

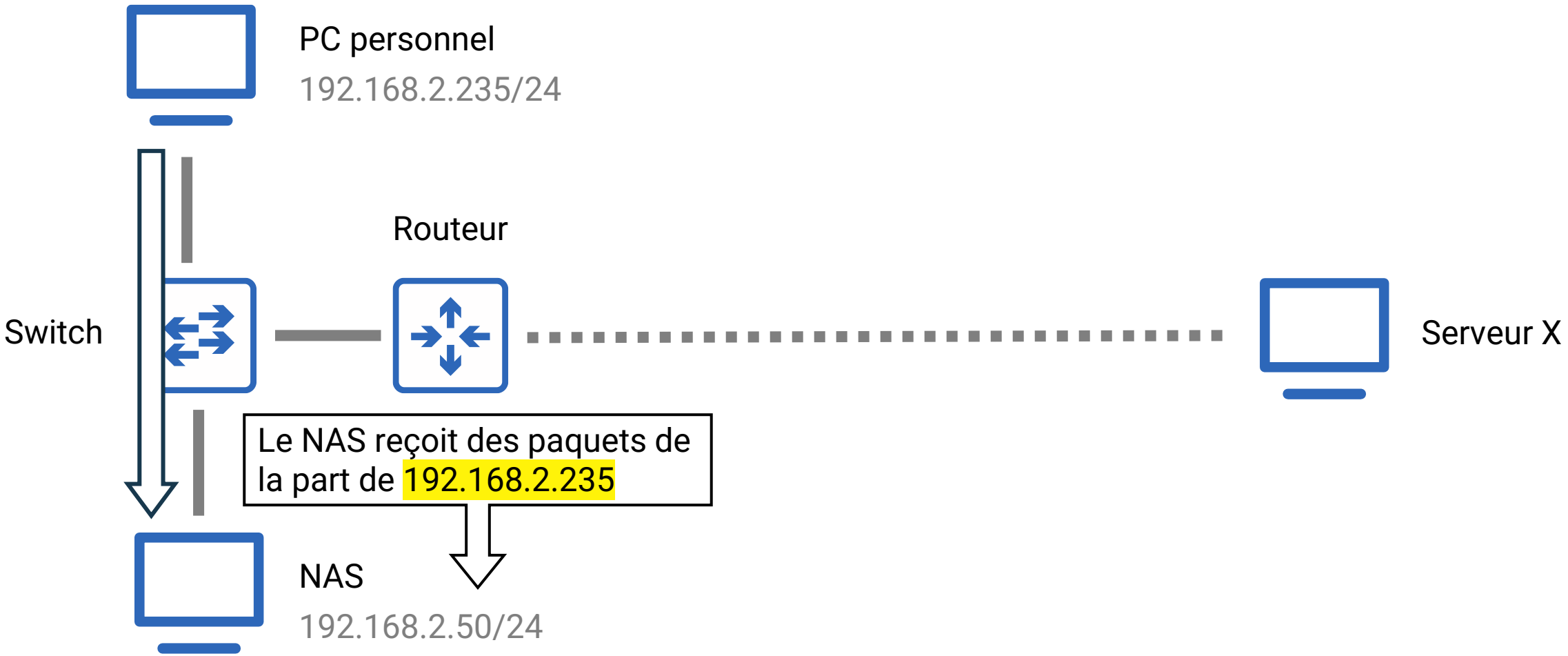
Deux adresses différentes pour une machine… Pourquoi ?

Contexte d’un réseau local

Dans un réseau local standard IPv4 (domestique, école, …)

- Chaque machine possède une IPv4 privée
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
- Les machines peuvent communiquer en interne
- Les adresses IP privées ne sortent pas du réseau local
- Vous recevez une IPv4 publique pour communiquer au-delà


PC personnel
192.168.2.235/24
Le serveur X reçoit des paquets de la part de 110.125.50.42
Routeur
Switch
Serveur X
NAS
192.168.2.50/24


PC personnel
192.168.2.235/24
Routeur
Switch
Serveur X
Le NAS reçoit des paquets de la part de 192.168.2.235
NAS
192.168.2.50/24

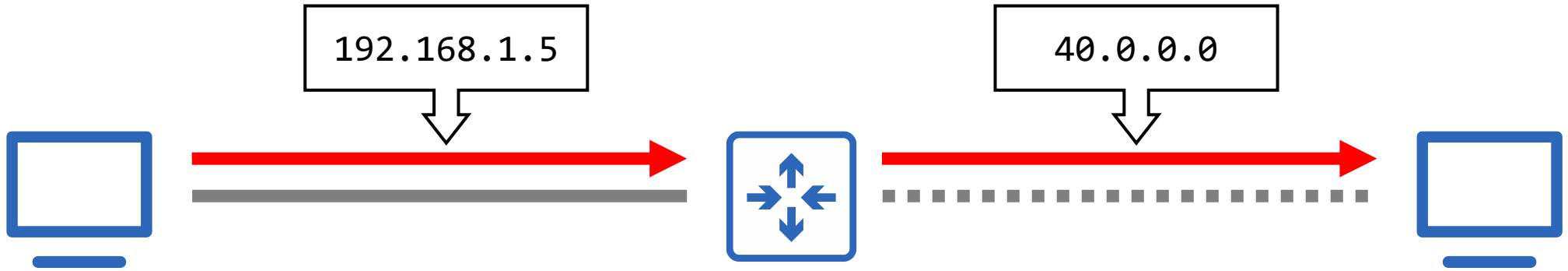
Network Address Translation (NAT)

Le routeur remplace l’adresse IP privée par une adresse IP publique

- Conçu – entre autres – pour apporter une réponse au manque d’IPv4
- Plusieurs appareils partagent la même adresse IPv4
- 3 catégories
  - NAT statique
  - NAT dynamique
  - NAT overlay

NAT statique (one-to-one)

Chaque adresse IP privée est reliée à une adresse IP publique statique



Noeud interne
192.168.1.5

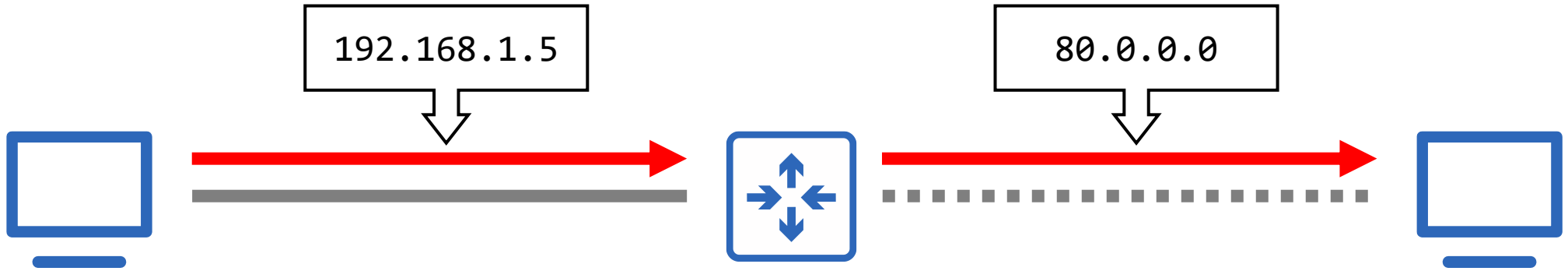
Local	Externe
192.168.1.4	30.0.0.0
192.168.1.5	40.0.0.0

Noeud externe
50.0.0.0

NAT dynamique

Chaque connexion sortante est associée dynamiquement à une IP publique

(de façon temporaire et partagée entre les machines locales)



Noeud interne

192.168.1.5

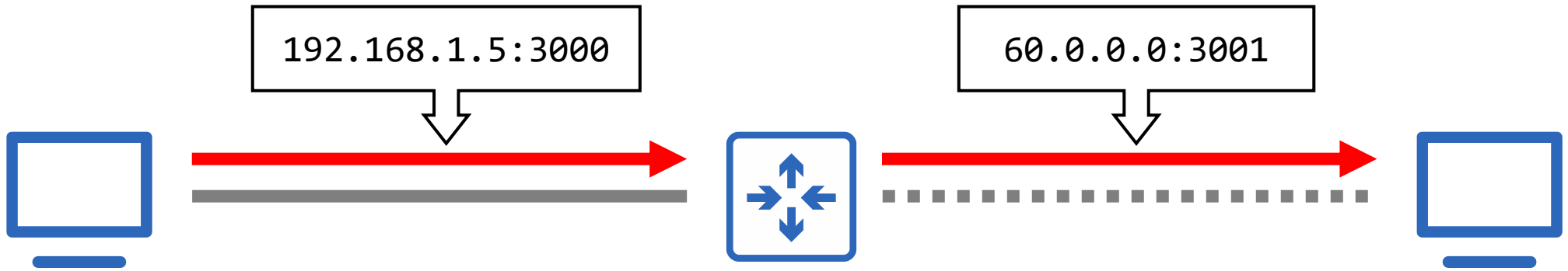
Adresse IP	Statut
70.0.0.0	Occupé
80.0.0.0	Libre pour connexion

Noeud externe

50.0.0.0

NAT overlay (Port Address Translation)

Utilise les ports (TCP/UDP) pour partager une même adresse IPv4



Noeud interne

192.168.1.5

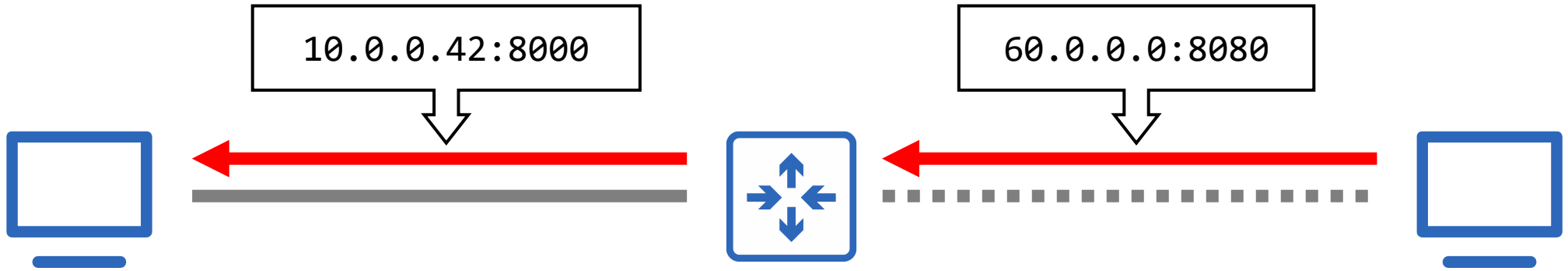
Noeud externe

50.0.0.0

IP interne	Port interne	IP externe	Port externe
192.168.1.5	3000	60.0.0.0	3001
192.168.1.6	3000	60.0.0.0	3002

Port Forwarding

Autoriser du trafic entrant vers une machine via une règle NAT statique



Noeud interne

10.0.0.42

Noeud externe

50.0.0.0

IP externe	Port externe	IP interne	Port interne
60.0.0.0	8080	10.0.0.42 (NAS)	8000

Port Forwarding

Risque de sécurité pour votre réseau domestique

Access Control

Parental Control | Portmapping | Firewall | Remote Access

Port Map Rules

#	Enable	Service	Protocol	External start	External end	Lan port	Internal host	Remote host	Description
1	On Off	UPNP	UDP	57669	57669	57669	192.168.1.3	0.0.0.0	Teredo

#	Enable	Service	Protocol	External start	External end	Lan port	Internal host	Remote host	Description	

Create new portmap

Cancel OK

PARTIE #2

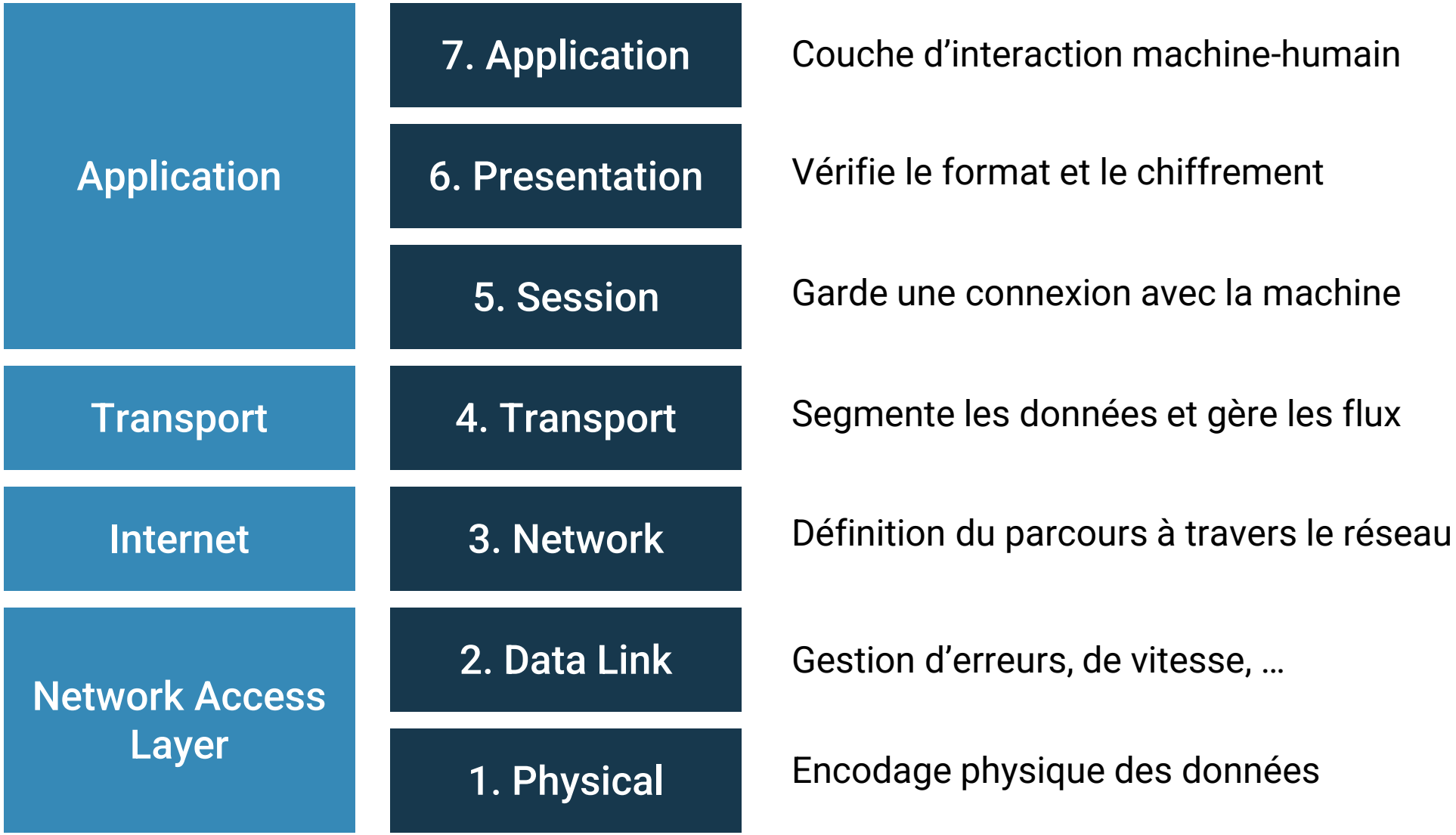
Découverte des protocoles OSI L7

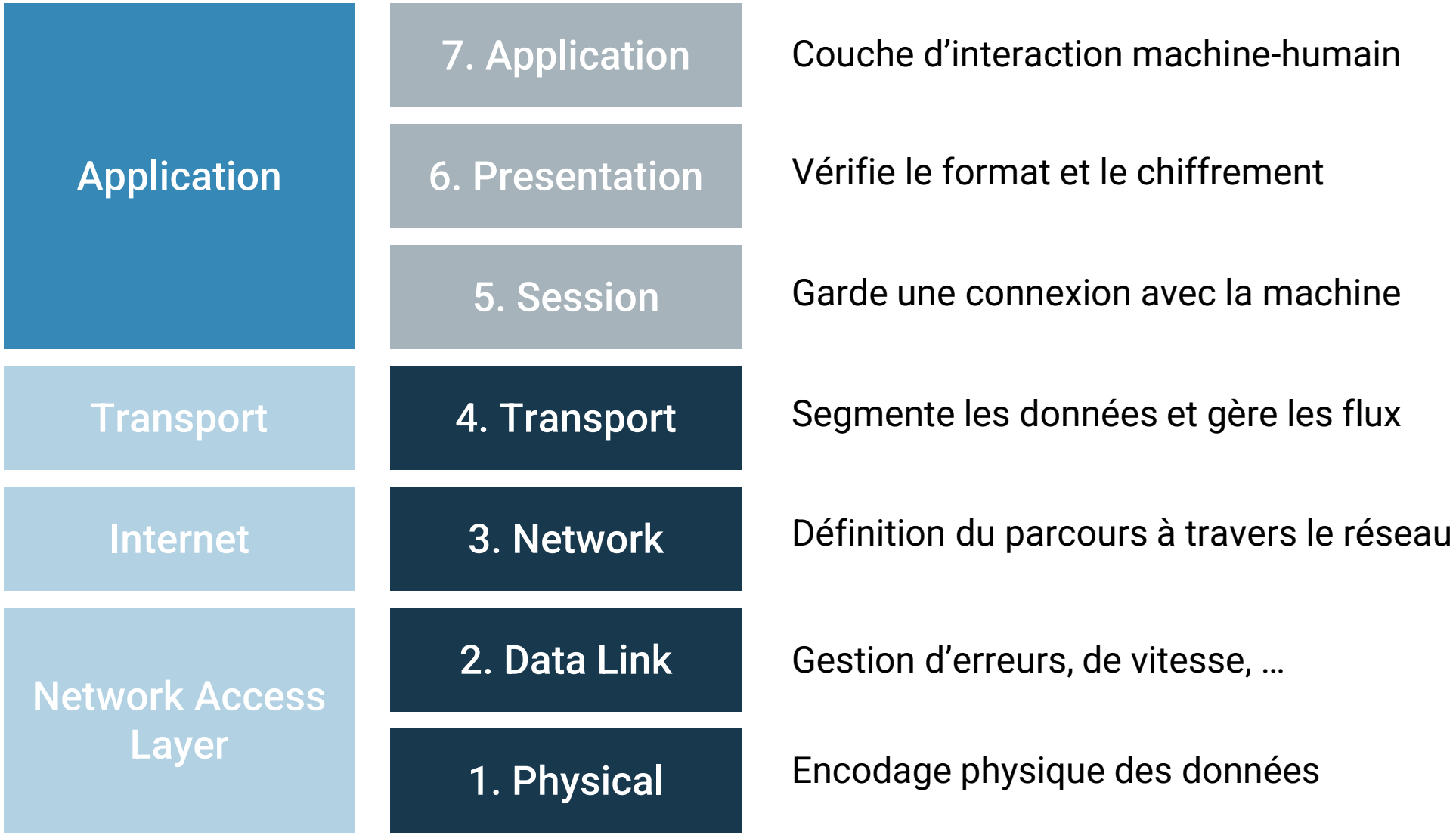
Les protocoles de la couche applicative qui reposent sur TCP & UDP

Introduction

Présentation des protocoles « applicatifs » les plus répandus

- On parle souvent de protocoles L7 Application
- … car ils se reposent sur les autres couches réseau
- Les couche L5 Session & L6 Presentation sont trop théoriques
- … et ne seront pas abordées dans ce cours (cf. TCP/IP)


Application
Transport
Internet
Network Access Layer
7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data Link
1. Physical
Couche d’interaction machine-humain
Vérifie le format et le chiffrement
Garde une connexion avec la machine
Segmente les données et gère les flux
Définition du parcours à travers le réseau
Gestion d’erreurs, de vitesse, …
Encodage physique des données


Application
Transport
Internet
Network Access Layer
7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data Link
1. Physical
Couche d’interaction machine-humain
Vérifie le format et le chiffrement
Garde une connexion avec la machine
Segmente les données et gère les flux
Définition du parcours à travers le réseau
Gestion d’erreurs, de vitesse, …
Encodage physique des données

Liste de ports TCP & UDP (bases)

Port	Protocole	TCP	UDP	Description
21	FTP			Transfert de fichiers (non-sécurisé)
22	SSH			Secure Shell & transfert de fichiers (sécurisé)
23	Telnet			Communications textuelles (non-sécurisé)
25	SMTP			Protocole d'envoi email (non-sécurisé)
53	DNS			Domain Name System
67/68	DHCP			Configuration de réseau dynamique
80	HTTP			Hypertext Transfer Protocol (non-sécurisé)
110	POP3			Protocole de réception email (non-sécurisé)

Liste de ports TCP & UDP (bases)

Port	Protocole	TCP	UDP	Description
123	NTP			Network Time Protocol, synchronisation du temps
143	IMAP			Protocole de réception email (non-sécurisé)
443	HTTPS			Hypertext Transfer Protocol (sécurisé, TLS/SSL)
465	SMTP (s)			Protocole d’envoi email (sécurisé, TLS/SSL)
993	IMAP (s)			Protocole de réception email (sécurisé, TLS/SSL)
995	POP3 (s)			Protocole de réception email (sécurisé, TLS/SSL)
3306	MySQL			Base de données MySQL
5432	PostgreSQL			Base de données PostgreSQL

PARTIE #3

Protocole DHCP

Configuration dynamique de votre réseau local

Le réseau devient opérationnel…

Nous avons maintenant

- Plusieurs machines connectées (>100)
- De la commutation (L2)
- Du routage (L3)
- Du transfert fiable (L4)
- Une façon de partager une même IP publique

Comment est-ce que les machines reçoivent une IPv4 privée ?


55
56
57
58
68
71
72
73

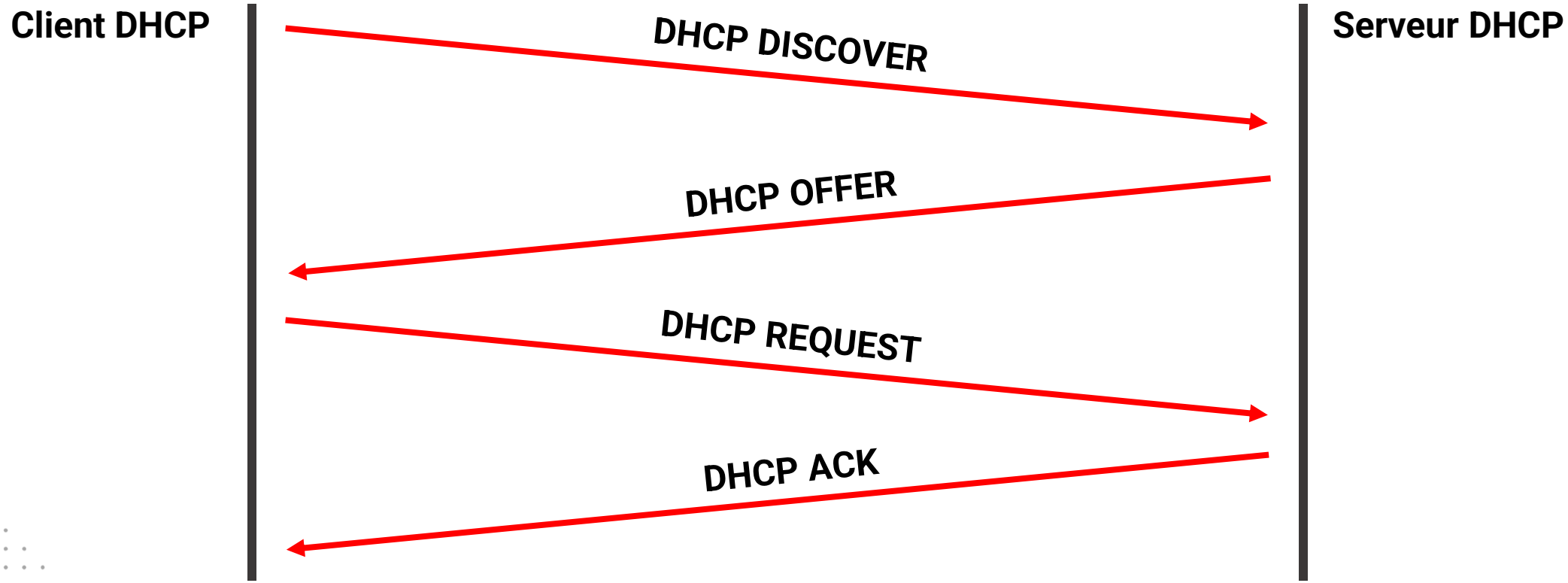
DHCP

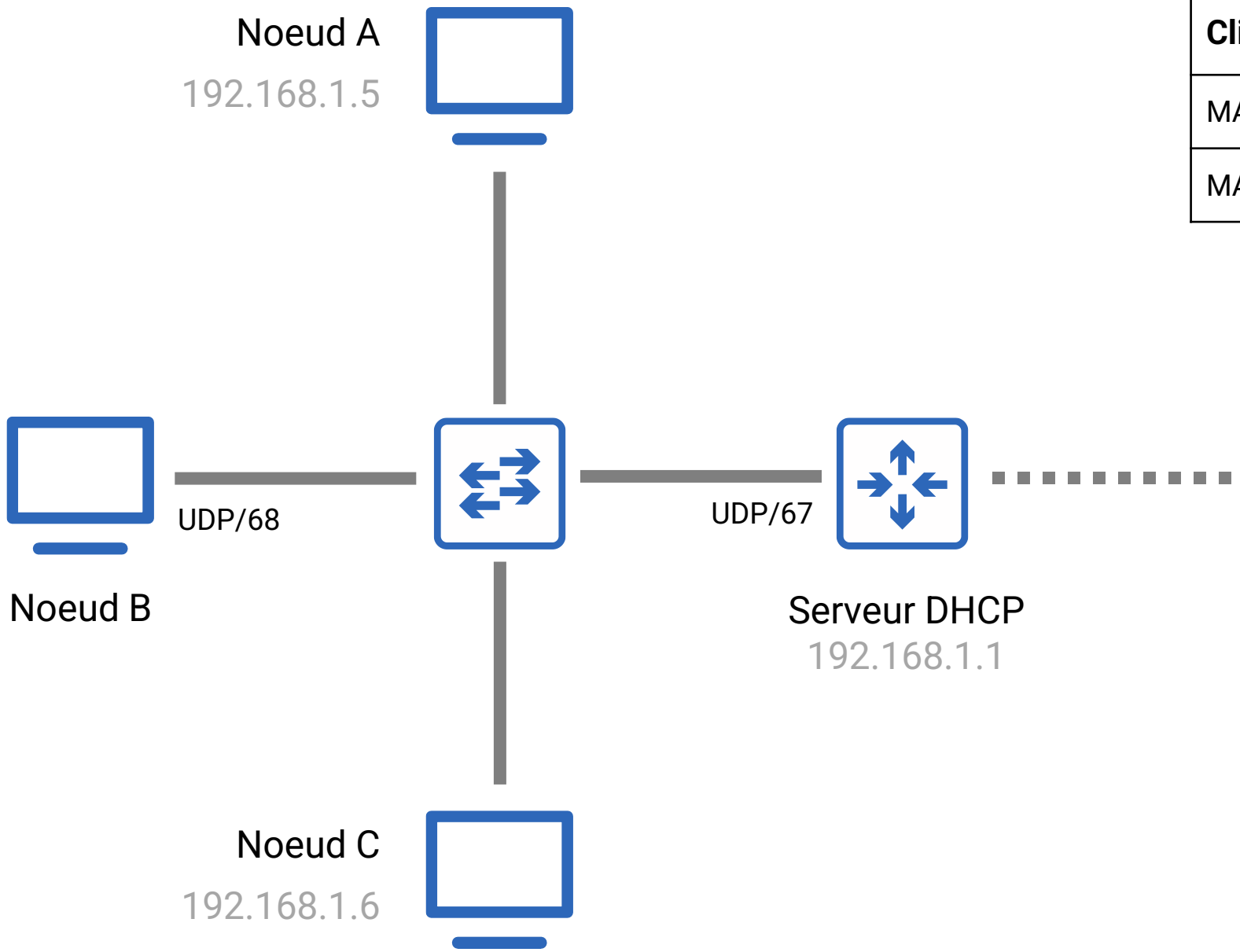
Dynamic Host Configuration Protocol

- Fournit automatiquement une adresse IP dans un réseau
- Propose également d'autres informations (network mask, default gateway, …)
- Serveur DHCP gère un « pool » d'adresses disponibles
- Une adresse « expire » au bout d'un certain délais (bail)
- Permet de faire une attribution statique pour certains clients (imprimantes, …)

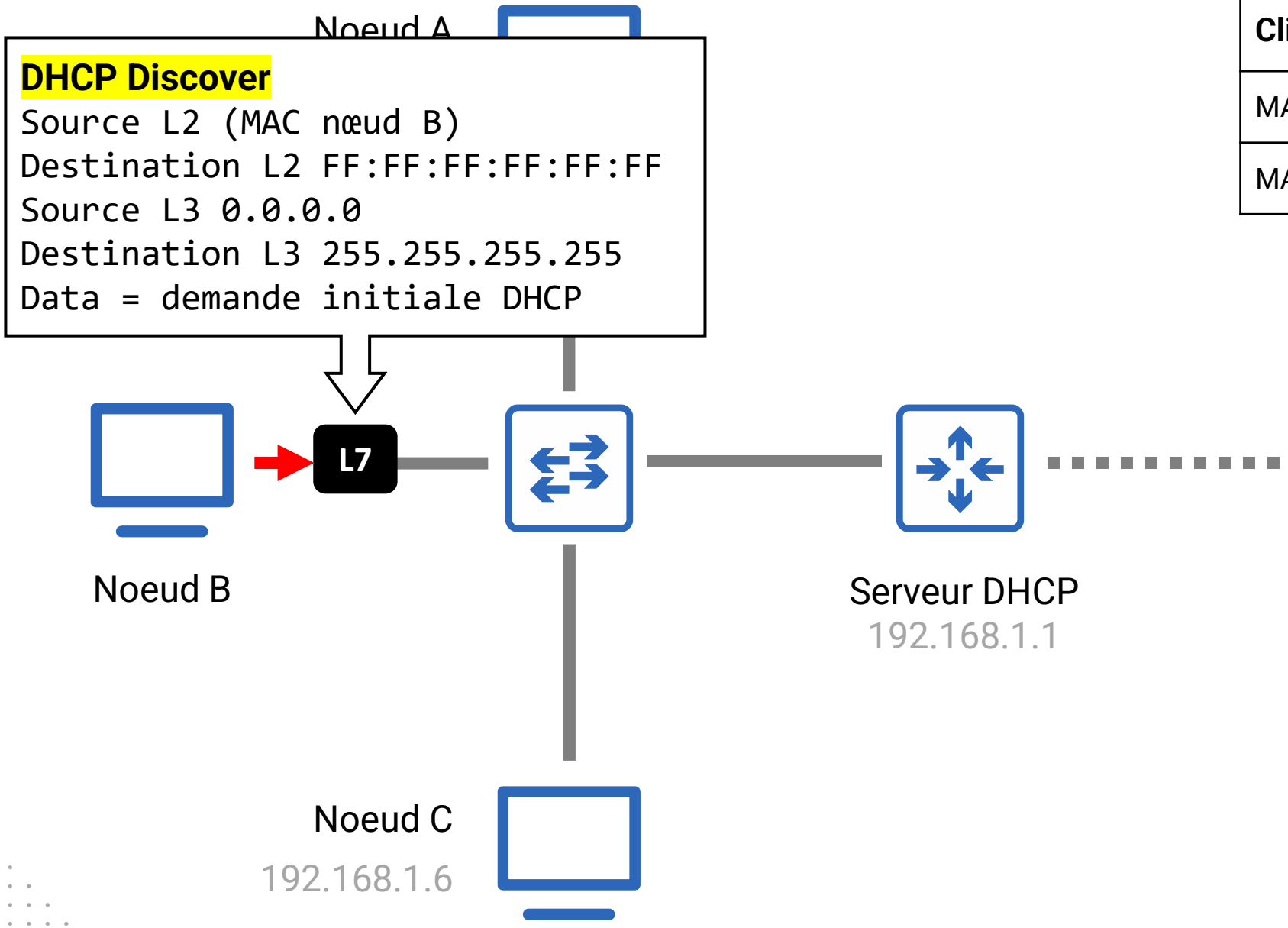
DHCP, le déroulement

L’obtention d’une adresse IP se déroule en 4 phases

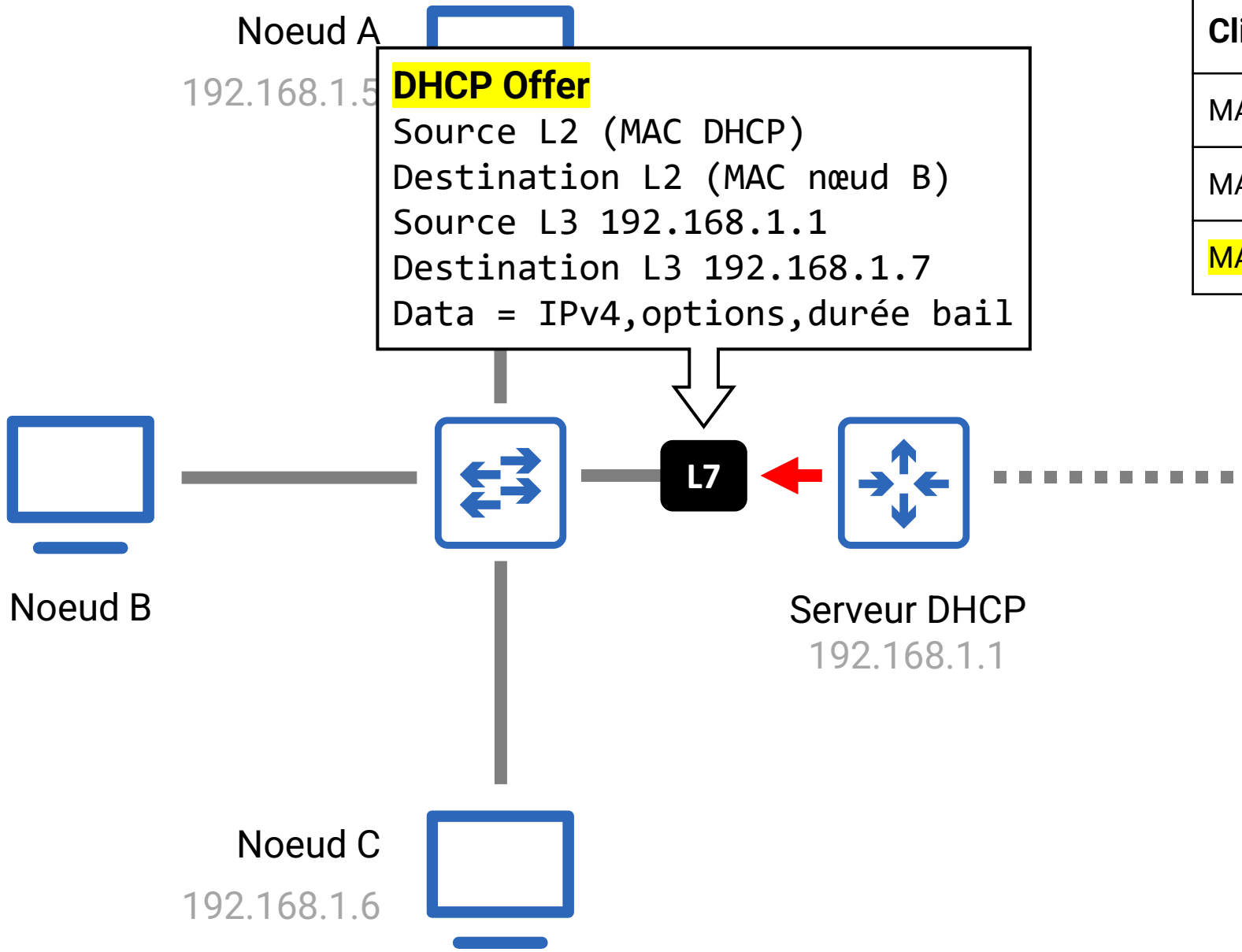




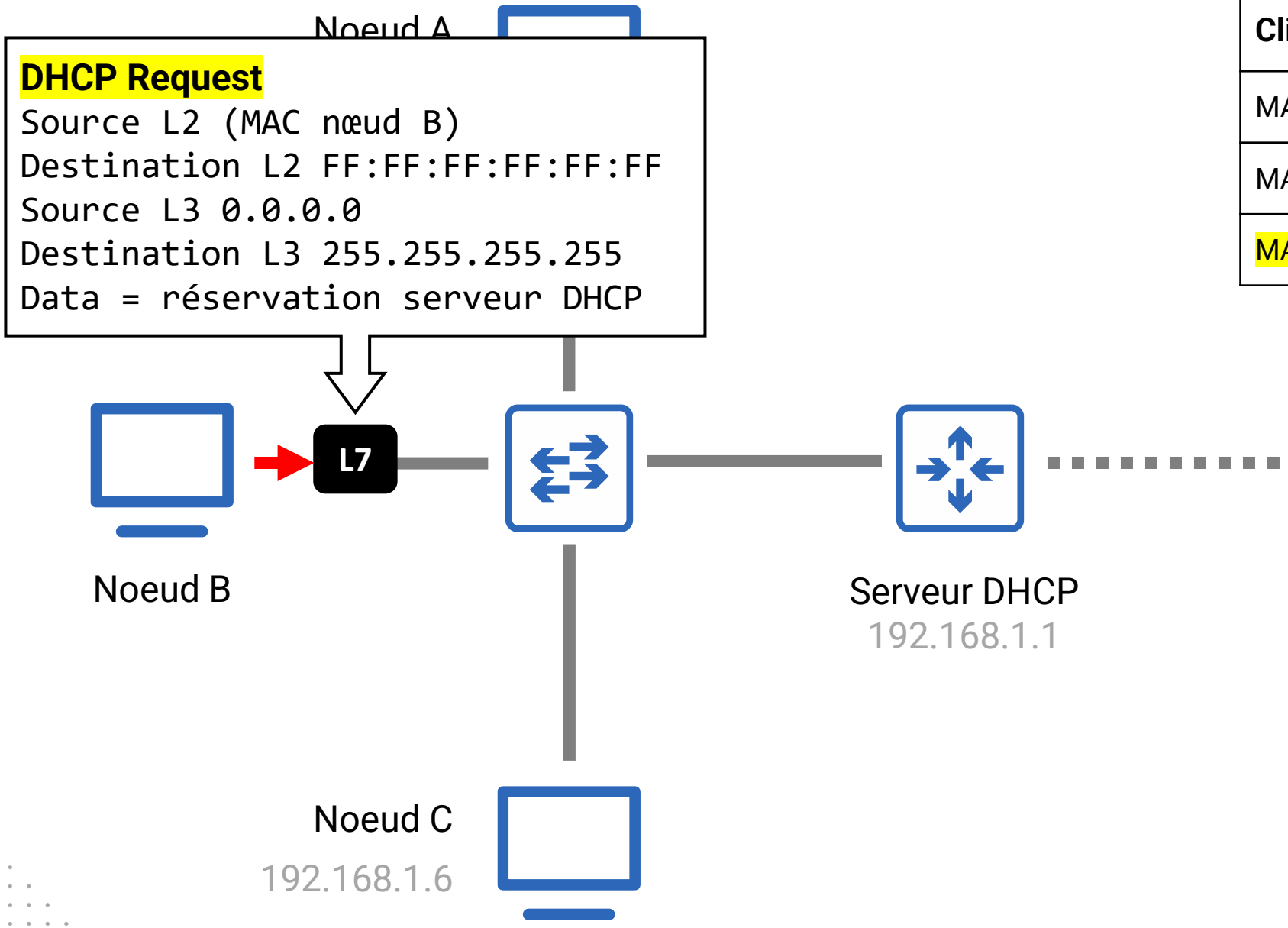
Client ID	IP réservée
MAC A	192.168.1.5
MAC C	192.168.1.6



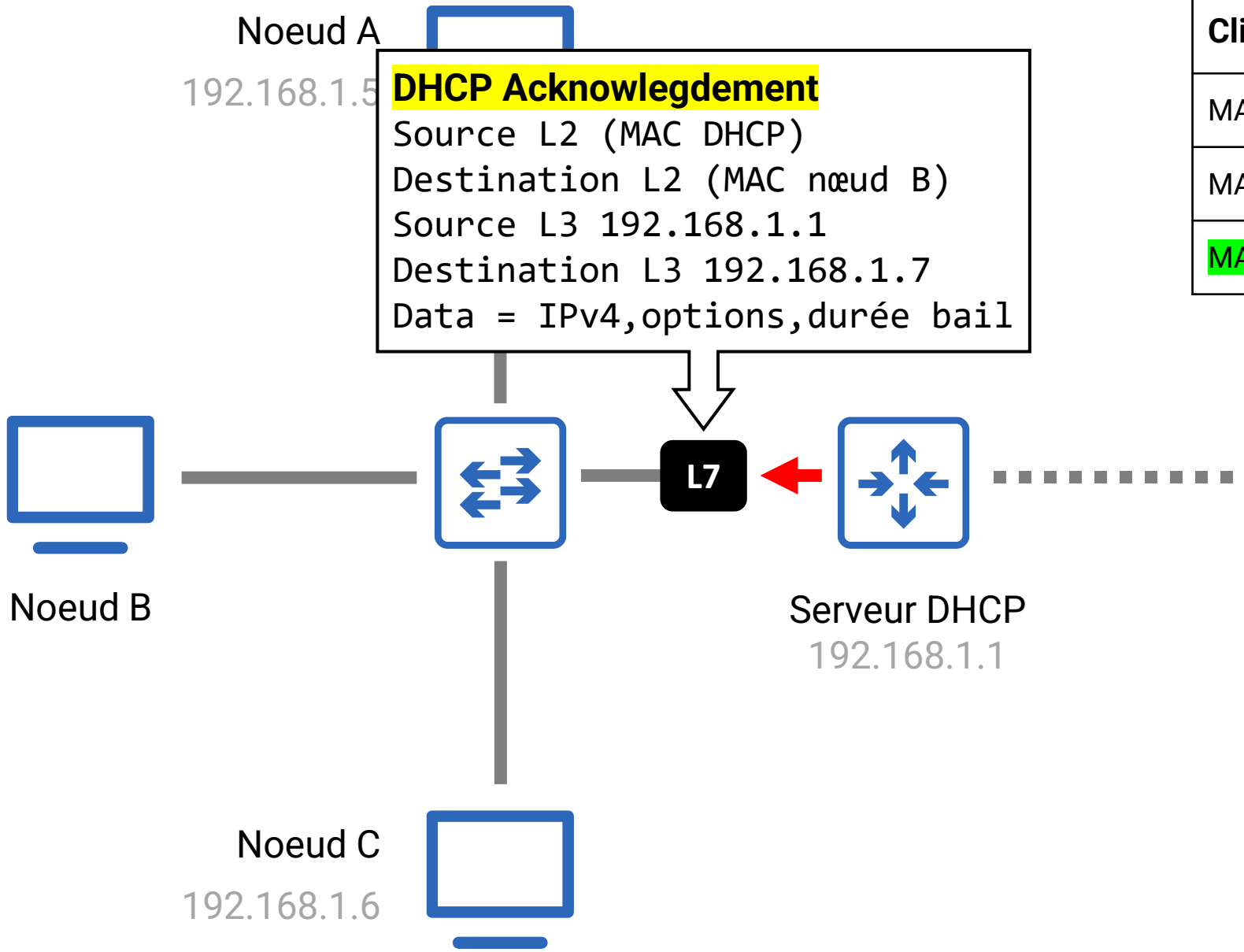
Client ID	IP réservée
MAC A	192.168.1.5
MAC C	192.168.1.6



Client ID	IP réservée
MAC A	192.168.1.5
MAC C	192.168.1.6
MAC B	192.168.1.7



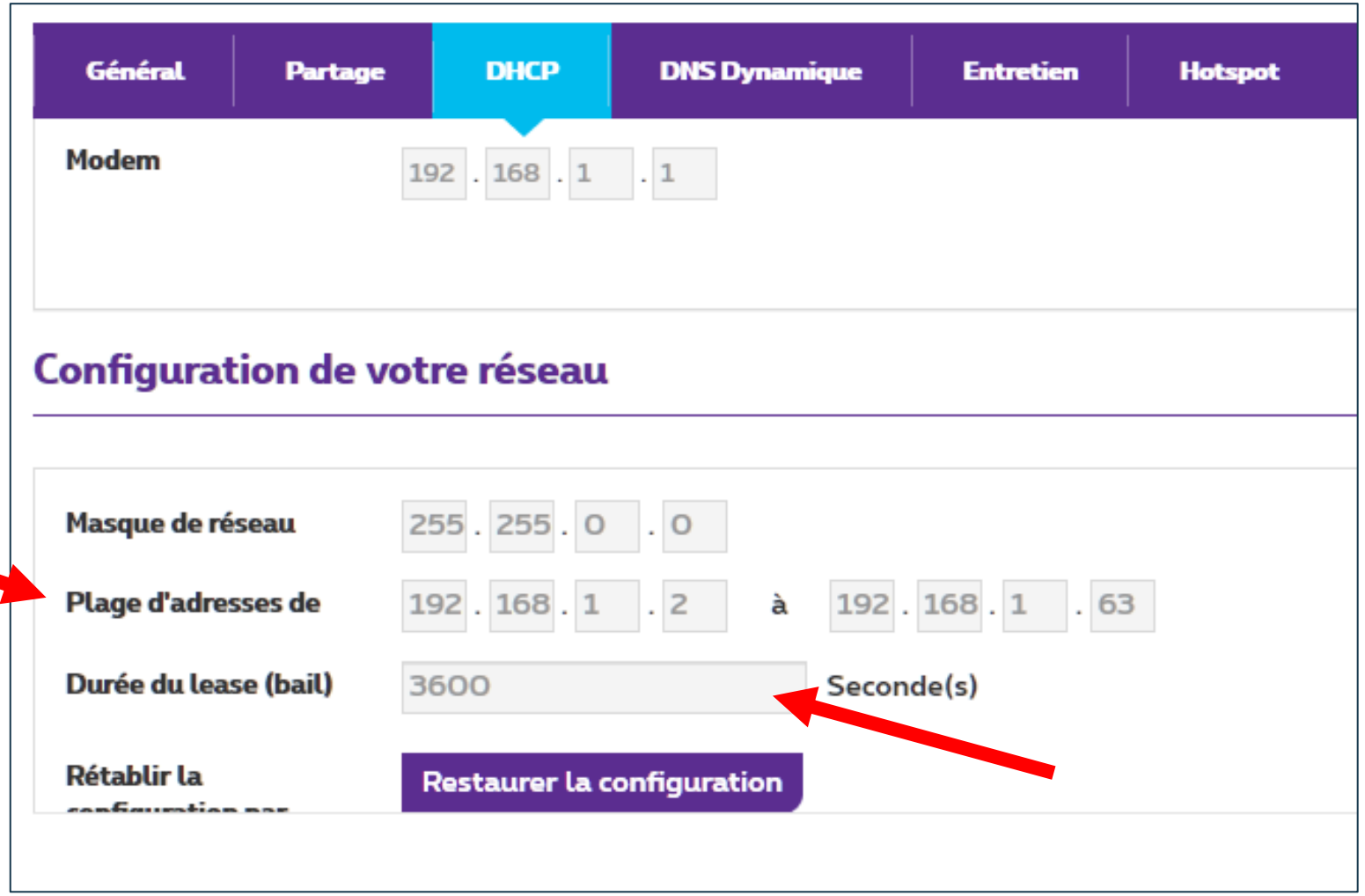
Client ID	IP réservée
MAC A	192.168.1.5
MAC C	192.168.1.6
MAC B	192.168.1.7



Client ID	IP réservée
MAC A	192.168.1.5
MAC C	192.168.1.6
MAC B	192.168.1.7


Scan to connect
WPS
INT
1
2
3
4
2.5 Gbps
TEL
1
2

DHCP


Général
Partage
DHCP
DNS Dynamique
Entretien
Hotspot
Modem
192 . 168 . 1 . 1
Configuration de votre réseau
Masque de réseau
255 . 255 . 0 . 0
Plage d'adresses de
192 . 168 . 1 . 2
à
192 . 168 . 1 . 63
Durée du lease (bail)
3600
Seconde(s)
Rétablir la
Restaurer la configuration

Options DHCP

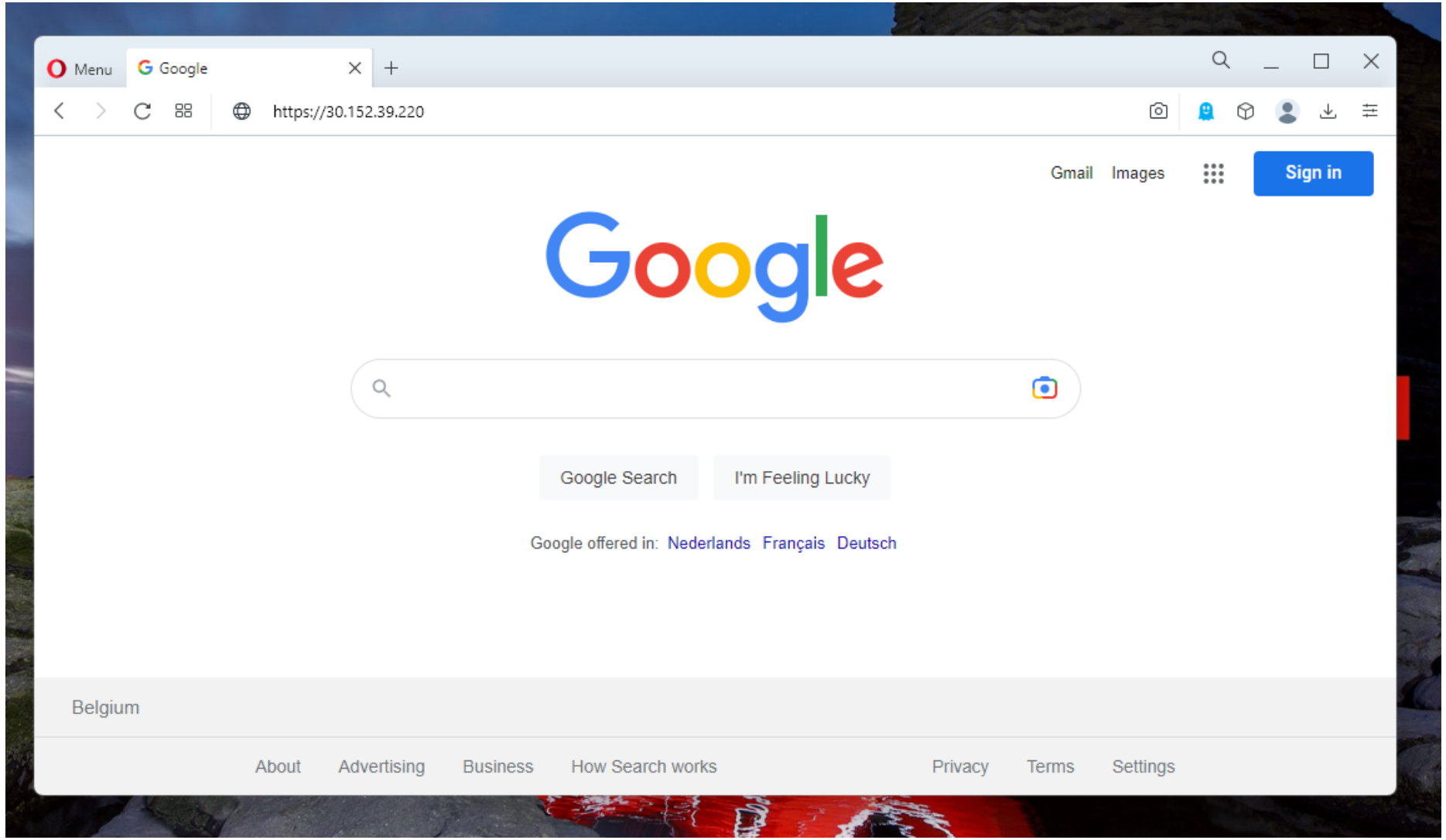
DHCP fournit – en plus d'une IPv4 - aux clients également des options

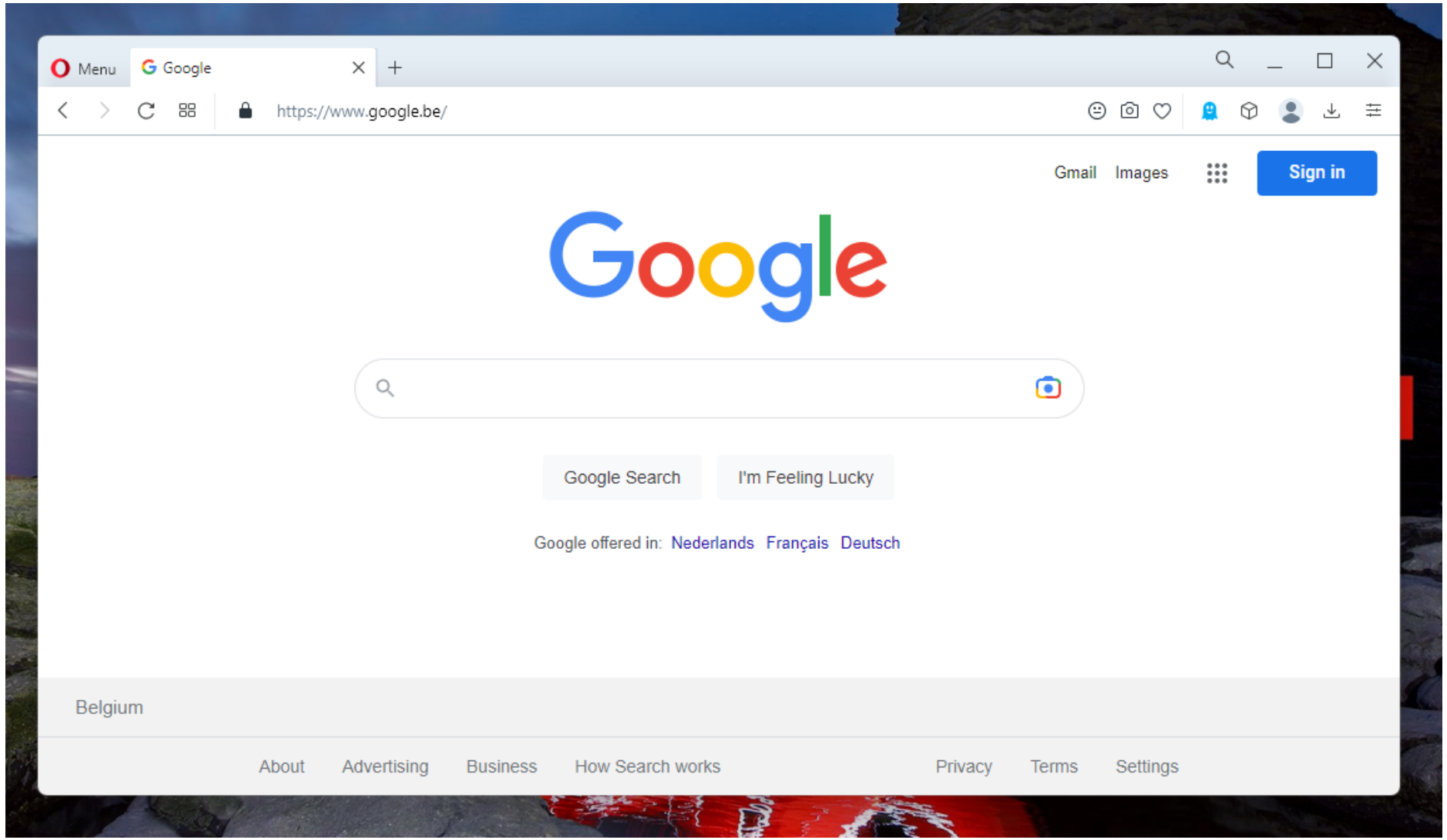
- Masque réseau
- Route par défaut (router)
- Serveur NTP
- Serveur DNS
- Configuration personnalisée

PARTIE #4

Protocole DNS

La conversion entre noms & adresses IP, pour un réseau plus agréable


Menu
Google
https://30.152.39.220
Gmail
Images
Sign in
Google
Google Search
I'm Feeling Lucky
Google offered in: Nederlands Français Deutsch
Belgium
About
Advertising
Business
How Search works
Privacy
Terms
Settings

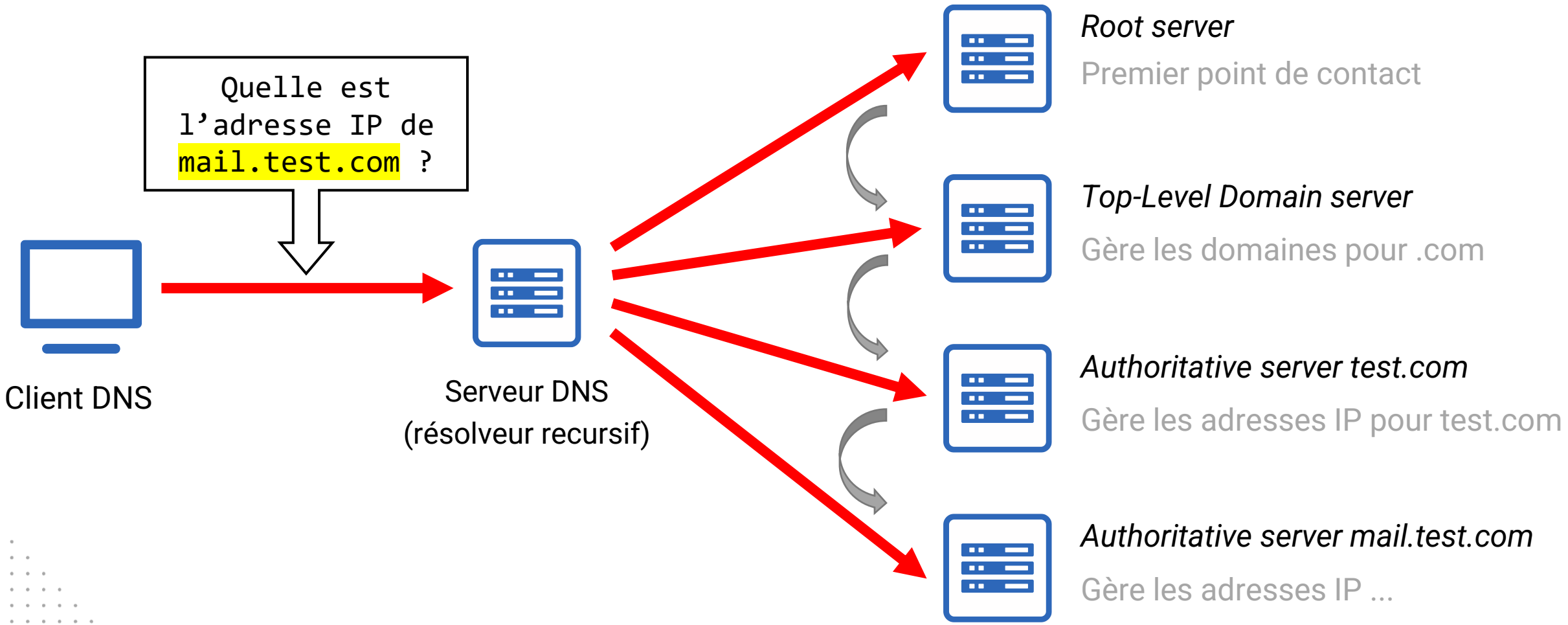

Menu
Google
https://www.google.be/
Gmail
Images
Sign in
Google
Google Search
I'm Feeling Lucky
Google offered in: Nederlands Français Deutsch
Belgium
About
Advertising
Business
How Search works
Privacy
Terms
Settings

DNS

Domain Name System

- Effectue de la résolution de noms vers des adresses IP
- Permet d'organiser les machines avec une nomenclature logique
- Principalement UDP, fonctionne également en TCP (pour transfert de zone)
- Registre mondial qui peut être requeté

Résolution DNS

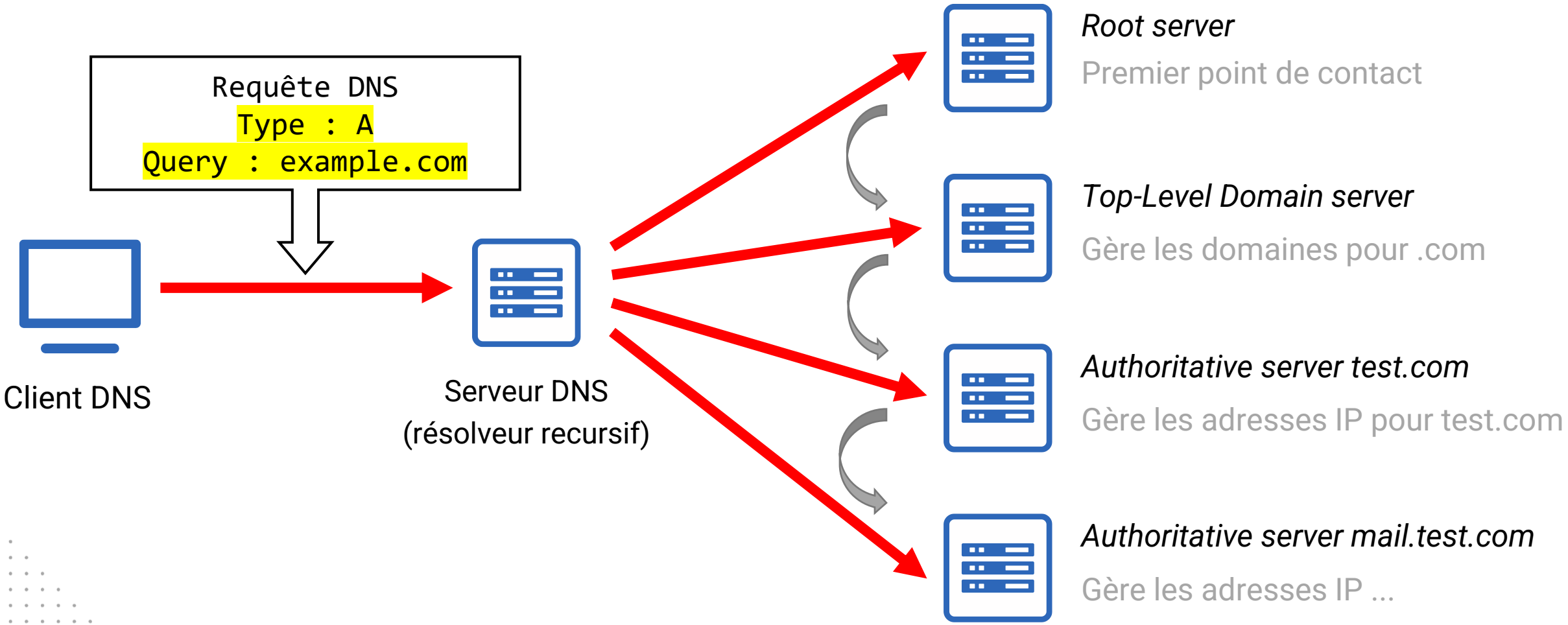


Les types de serveur DNS

Serveurs DNS

- Résolveur récursif : premier point de contact, gère appels DNS & cache
- … par exemple 1.1.1.1 (CloudFlare) ou 8.8.8.8 (Google)
- Root server : 13 serveurs, connu de tous résolveurs – redirigent vers TLD
- TLD server : contient toutes les informations des *top-level domains*
- … par exemple .com, .be, .fr – **mais ne fais pas autorité**
- Authoritative server : contient informations spécifiques au nom de domaine
- … il possède donc les **enregistrements DNS**

Résolution DNS



Enregistrements DNS

Type	Signification
A	Adresse IPv4
AAAA	Adresse IPv6
CNAME	Alias de domaine
NS	Serveur DNS (enfant, backup, …)
MX	Serveur mail relié au domaine
TXT	Informations textuelles

Load balancing DNS

Le load balancing est une technique de répartition de charge

- L'objectif est d'offrir de la résilience et de soulager l'infrastructure
- Le DNS peut servir de *load balancer*
- Via l'assignation de plusieurs cibles A/AAAA sur un même domaine
- **Attention à la mise en cache DNS**

Exemple de load balancing (cloud AWS)

Windows possède un client « nslookup » (« dig » sous Linux)

```
nslookup -type=a aws.com
```

Exemple de load balancing (cloud AWS)