

TCP/IP avec les mains

Les modèles de réseau

- Création de modèles destinés à :
 - uniformiser les communications réseau,
 - assurer une compatibilité et une interopérabilité entre les différentes technologies réseaux
- Deux modèles:
 - OSI (Open System Interconnection)
 - TCP/IP

Le modèle de référence de l'OSI

Couche application

- Fournit et gère les interfaces entre la machine et les utilisateurs
- Ces interfaces sont constituées des différents programmes des utilisateurs
- Définit un format de données par lequel les informations circuleront sur le réseau

Couche présentation

- Démarrer véritablement la communication
- S'occupe de la synchronisation
- Détermine le mode de transmission

Couche transport

- Accepte les données de la couche supérieure
- Découpe les données en unités plus petites
- S'assure que ces unités arrivent à destination
- Chargée de transporter les Paquets de la source vers la destination.

Couche réseau

- Doit connaître la topologie du réseau
- Fournit un moyen de transmission exempt d'erreur
- Doit éviter les routes surchargeées à la couche réseau

Couche liaison

- Fractionne les données en trames
- Transmet les trames en séquence

Couche physique

- Gère les trames d'apportement
- Résout les problèmes provoqués par des trames erronées
- Fournit la connexion
- Détermine le nombre de broches du connecteur

Le modèle de référence de l'OSI

Couche application

Service aux utilisateurs

Couche présentation

Gestion de la syntaxe

Couche session

Gestion de la communication

Couche transport

Contrôle de la communication

Couche réseau

Acheminement des données

Couche liaison

Architectures réseau

Couche physique

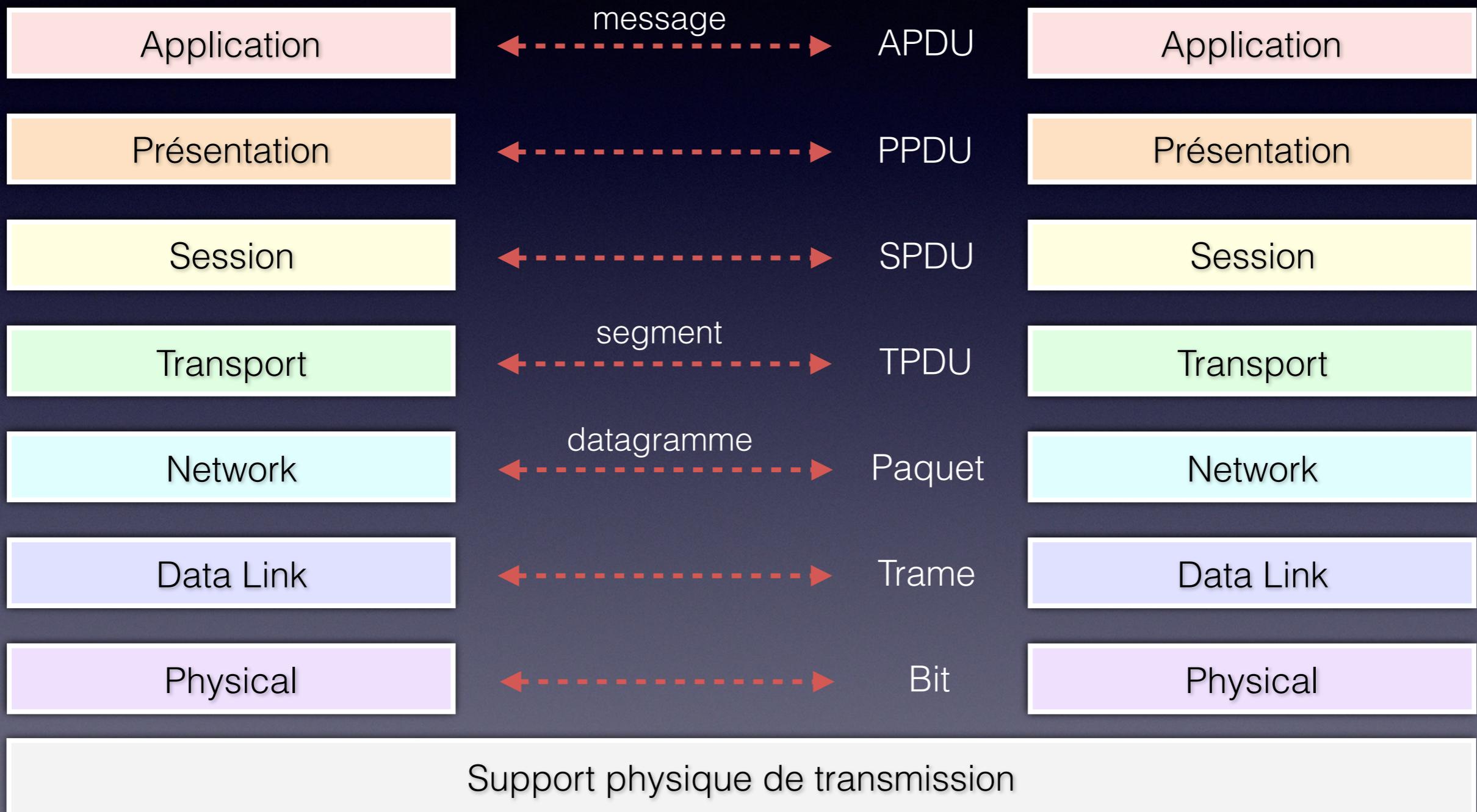
Procédés physiques pour le transfert

Les unités de protocole

- Communication de couche à couche
- L'unité de donnée d'une couche a une forme particulière correspondant à un protocole particulier lié à cette couche
- PDU (Protocol Data Unit)

Le modèle ISO

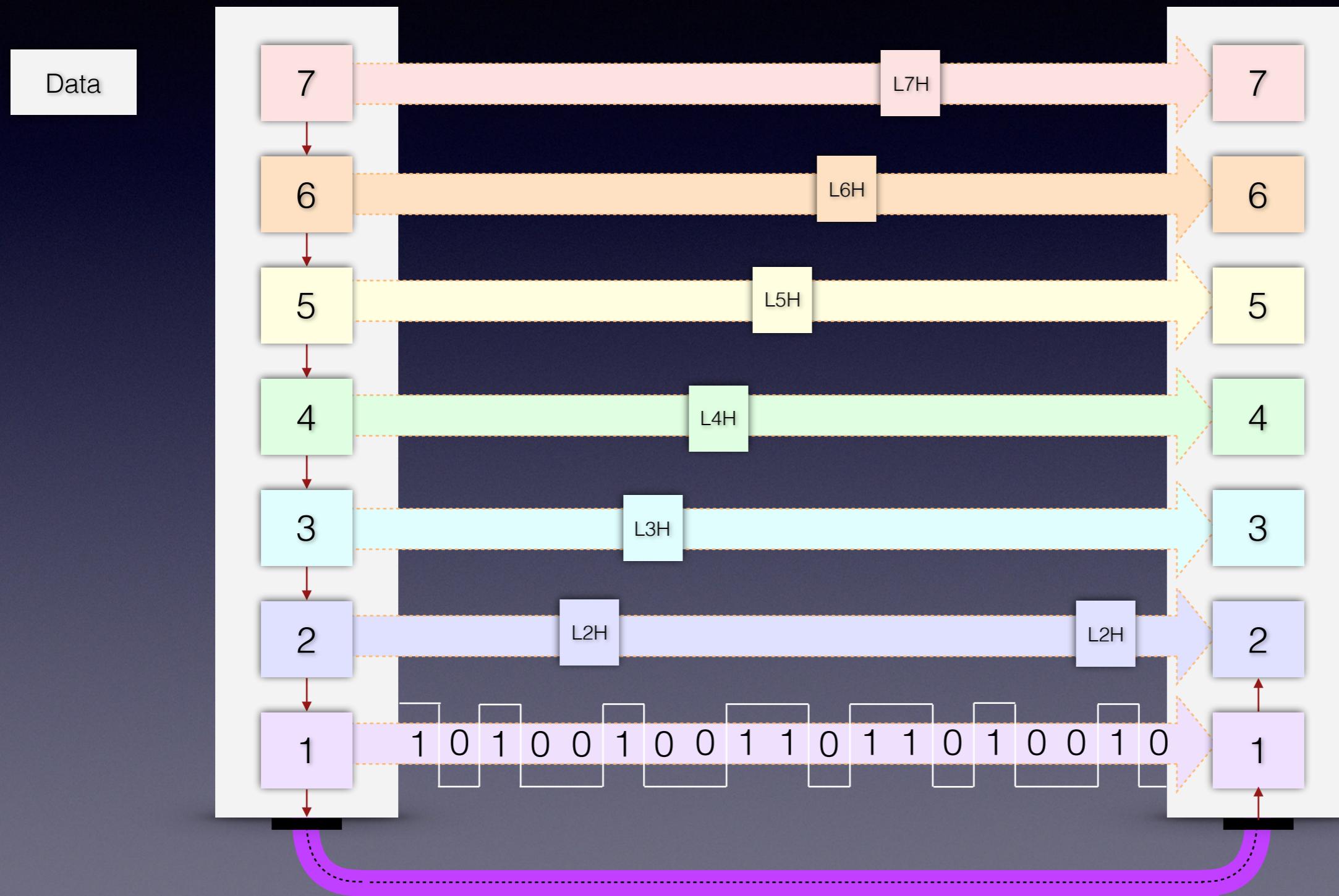
Couches et unités de données



PDU : Protocol Data Unit

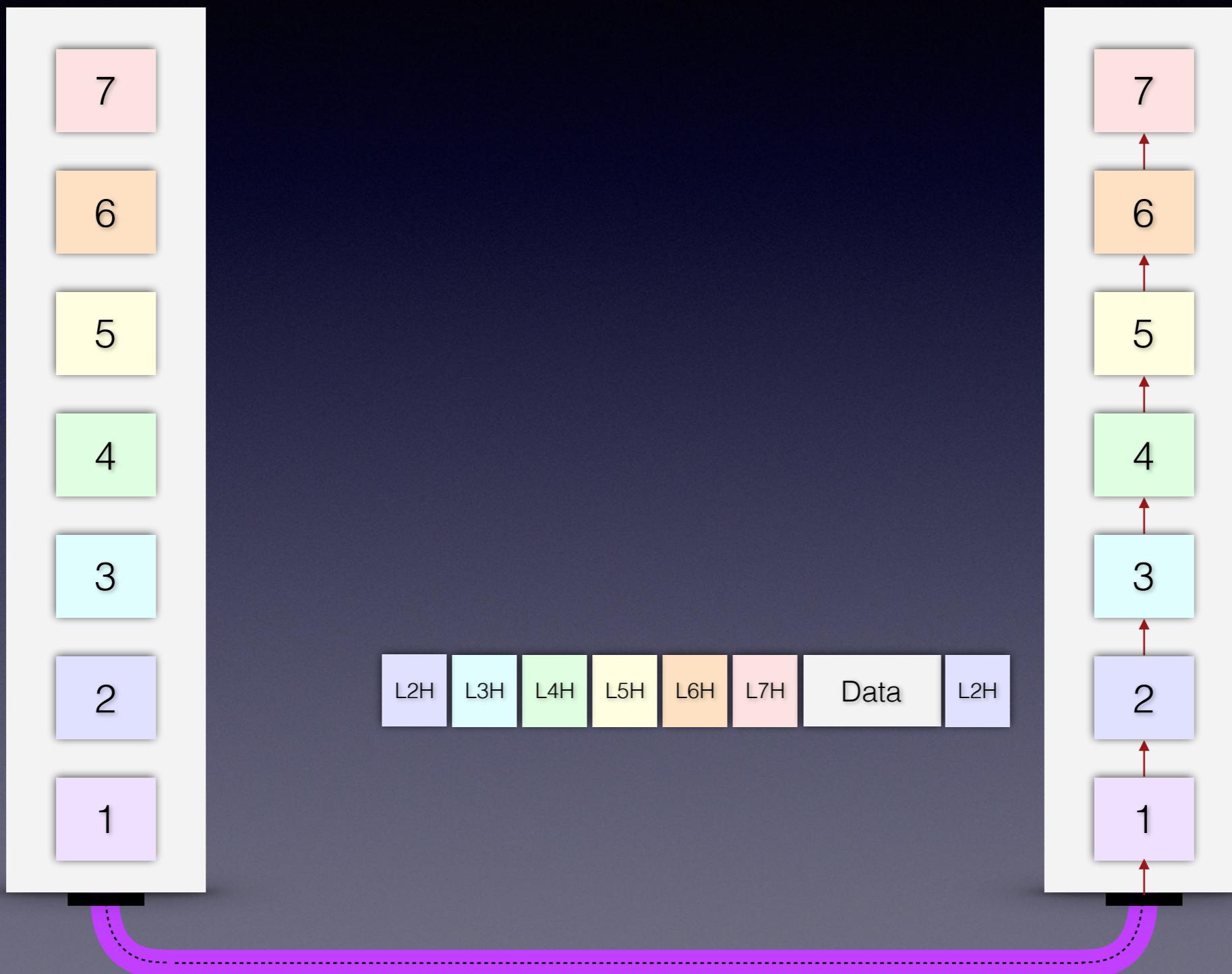
Le modèle ISO

Principe de l'encapsulation



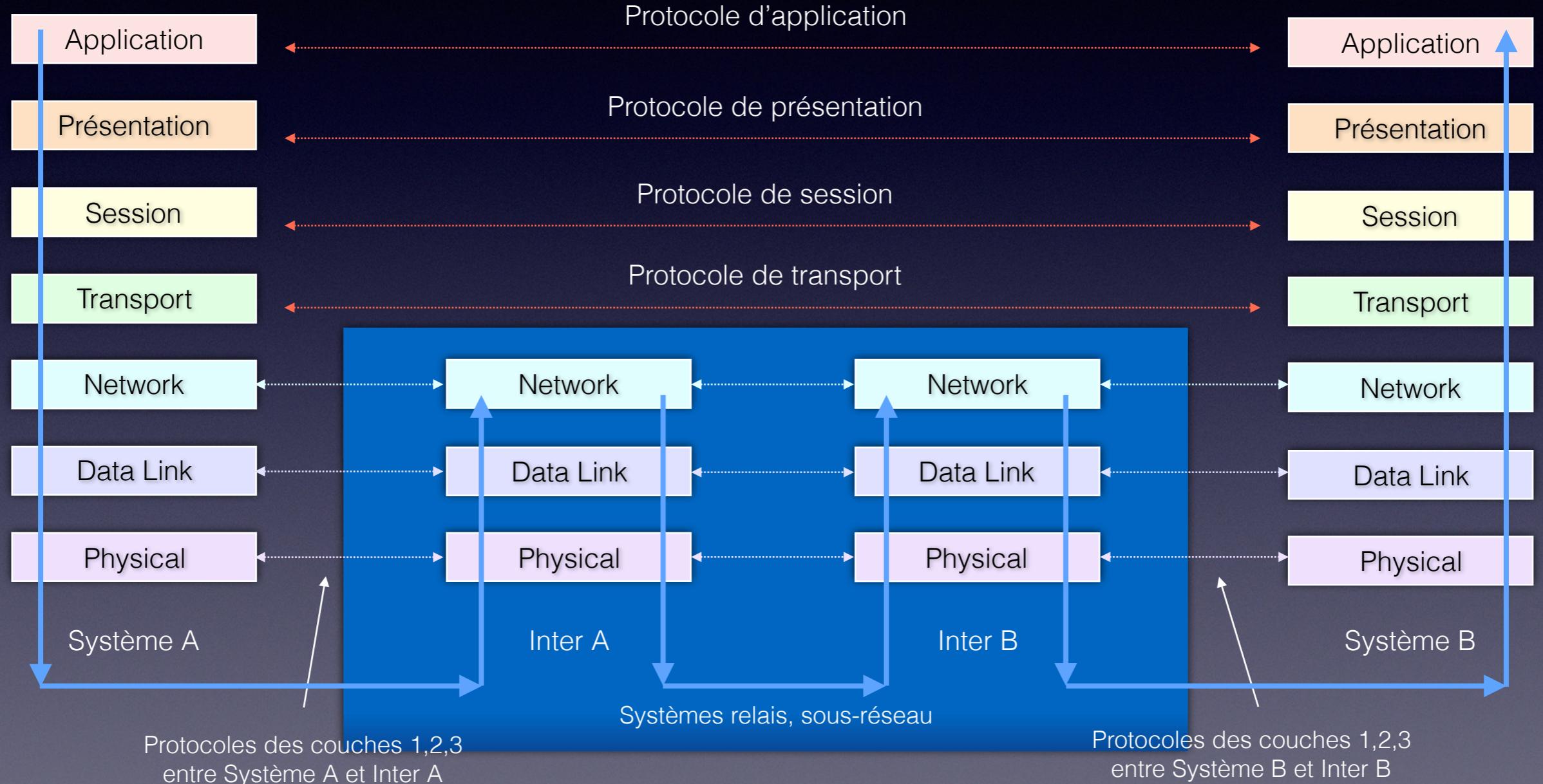
Le modèle ISO

Principe de l'encapsulation



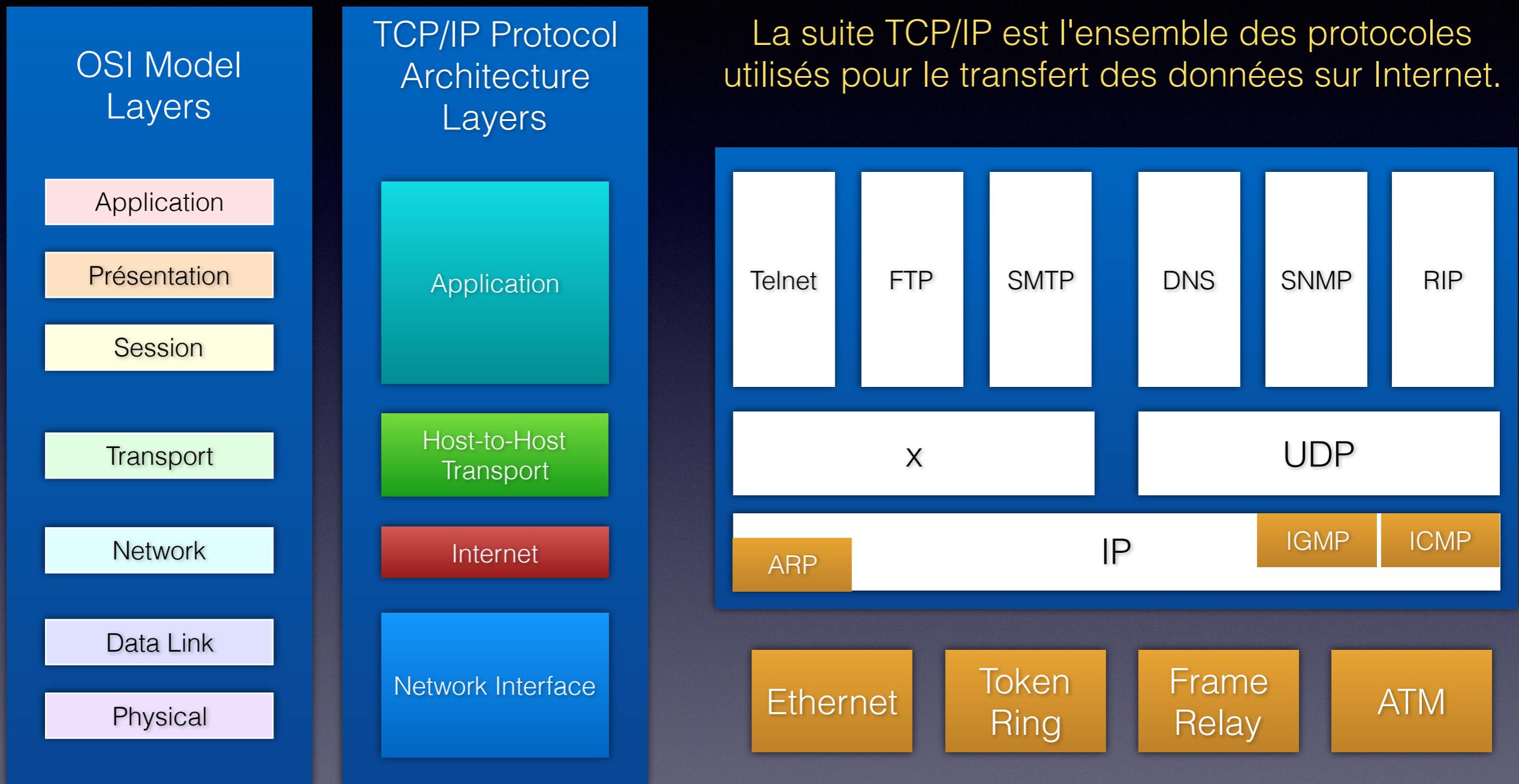
Le modèle ISO

Principe de relais



Support physique de transmission

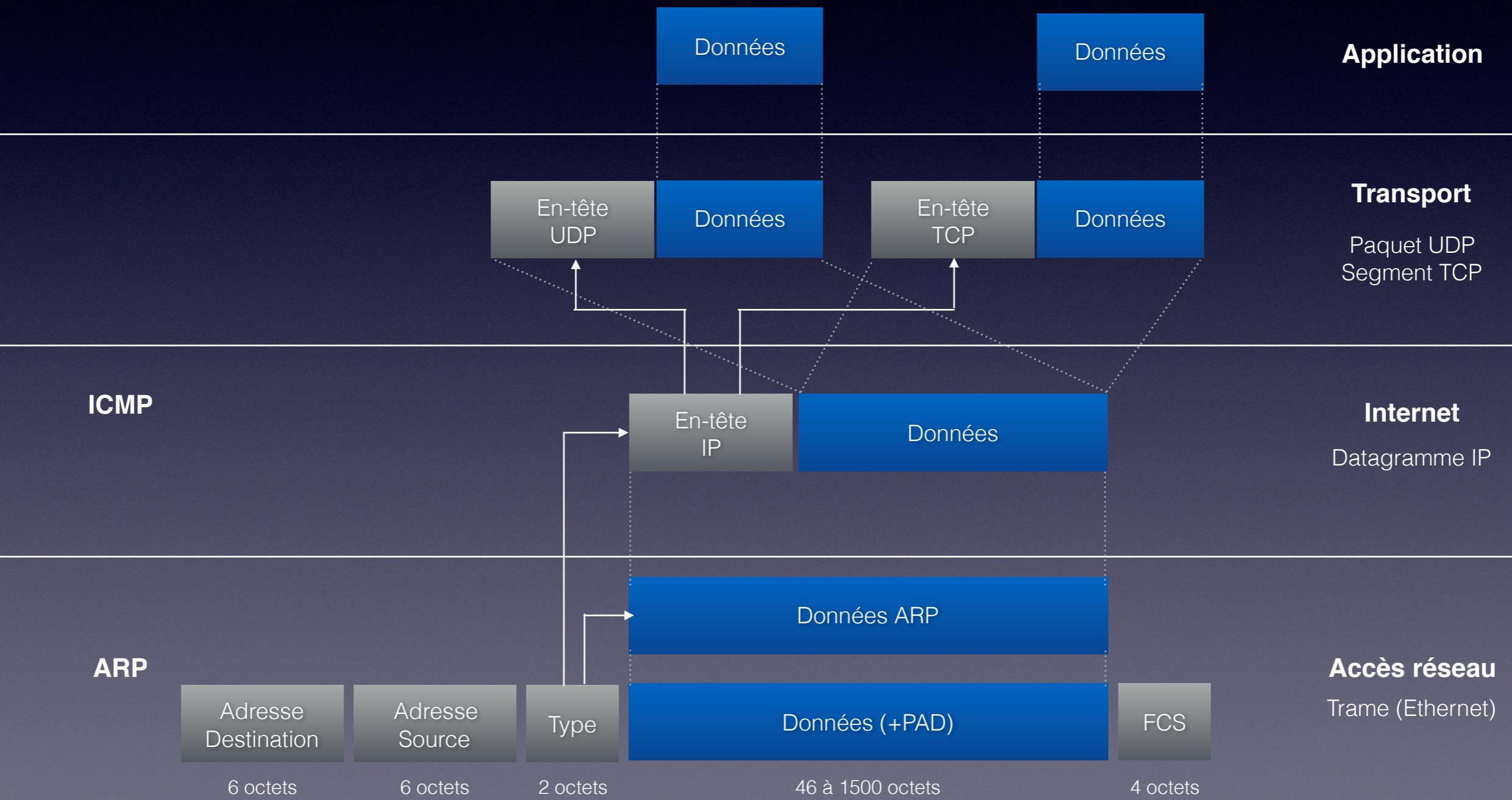
Le protocole TCP/IP



Encapsulation protocolaire

Protocoles

Couches



Le protocole Ethernet

- Ethernet est un protocole de réseau local à commutation de paquets
- Ethernet a été standardisé sous le nom IEEE 802.3
- Les deux attributs importants sont les adresses physiques (MAC) des cartes réseau.

80 00 20 7A 3F 3E

Destination MAC Address

80 00 20 20 3A AE

Source MAC Address

08 00

EtherType

IP, ARP, etc...

Payload

00 20 20 3A

CRC Checksum

MAC Header

(14 bytes)

Data

(46 to 1500 bytes)

Ethernet Type II Frame (64 to 1518 bytes)

Le protocole IP

- IP (Internet Protocol) est défini dans la RFC 791 (1981)
- Protocole de bout en bout, non connecté et non fiable, transportant uniquement des paquets de données entre émetteur et un / plusieurs destinataires.
- Protocole dit « best effort »
 - Aucune garantie d'acheminement ;
 - Aucune garantie de résultat.
- Nécessite une adresse IP unique par machine ;
- La route d'un paquet est déterminée par le réseau :
 - Pour chaque paquet
 - Indépendamment des paquets précédents

Name:

Dany:

IP: 23.75.345.200

Honn:

Le protocole IP

Les classes d'adresse



Classe A

1.0.0.1 à 126.255.255.254

Le réseau 127.0.0.0 est réservé pour les communication en boucle locale

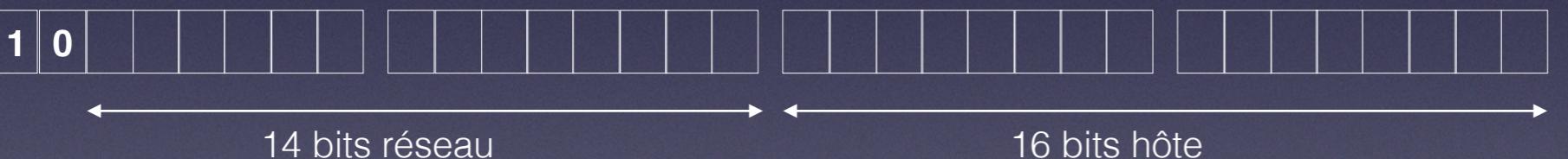


24 bits hôte



Classe B

128.0.0.1 à 191.255.255.254

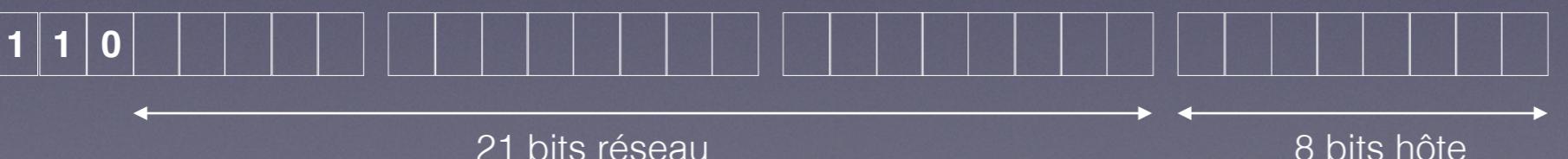


16 bits hôte



Classe C

192.0.0.1 à 223.255.255.254



8 bits hôte

16384 adresses réseau
65 534 ordinateurs

2 097 152 adresses réseau
254 ordinateurs

7 bits réseau

Le protocole IP

Les classes d'adresse

1 | 1 | 1 | 0 | | | |

Classe D

224.0.0.0 à 239.255.255.255

1 | 1 | 1 | 0 | | | | | | | |

adresses uniques
services de multidiffusion vers
les groupes d'hôtes.

1 | 1 | 1 | 1 | | | |

Classe E

240.0.0.0 à 255.255.255.255

1 | 1 | 1 | 1 | | | | | | |

adresses uniques
Réservées par l'IANA pour
des expérimentations

Le protocole IP

Masque de sous-réseau

- Utilisation de bits de la partie hôte comme bits d'adresse réseau supplémentaire (réduction du nombre d'ordinateurs dans le réseau)
- Usage d'un masque de sous-réseau
 - permet principalement à un ordinateur de déterminer les paquets IP qu'il peut émettre directement à une autre machine dans passer par une passerelle ;
 - permet de définir l'adresse du réseau et l'adresse de diffusion du réseau (broadcast).

Le protocole IP

Masque de sous-réseau

- Adresse du réseau : adresse IP qui désigne un réseau (tous les bits de la partie hôte à 0)
- Adresse de diffusion du réseau (broadcast) : adresse IP qui désigne toutes les machines du réseau (tous les bits de la partie hôte à 1)

Le protocole IP

Masque de sous-réseau

- Réalisation d'un **ET Logique** avec le masque de sous-réseau
- Si l'adresse réseau est identique alors les machines sont **sur** le même réseau
- Sinon elles ne sont pas sur le même sous-réseau et ne pourront pas communiquer directement. Elles devront utiliser une passerelle pour relayer leurs paquets.

Le protocole IP

Adresse du réseau

130 . 45 . 12 . 164

Adresse IP

Masque de 255 . 255 . 255 . 0

Réalisation d'un ET Logique

Adresse du réseau 130 . 45 . 12 . 0

Le protocole IP

Adresse de diffusion

130 . 45 . 12 . 0

Adresse du réseau

1|0|0|0|0|0|1|0 0|0|1|0|1|1|0|1 0|0|0|0|1|1|0|0 0|0|0|0|0|0|0|0

Complément à 1
du masque de
sous-réseau

255 . 255 . 255 . 255

0|0|0|0|0|0|0|0 0|0|0|0|0|0|0|0 0|0|0|0|0|0|0|0 0|0|0|0|0|0|0|0

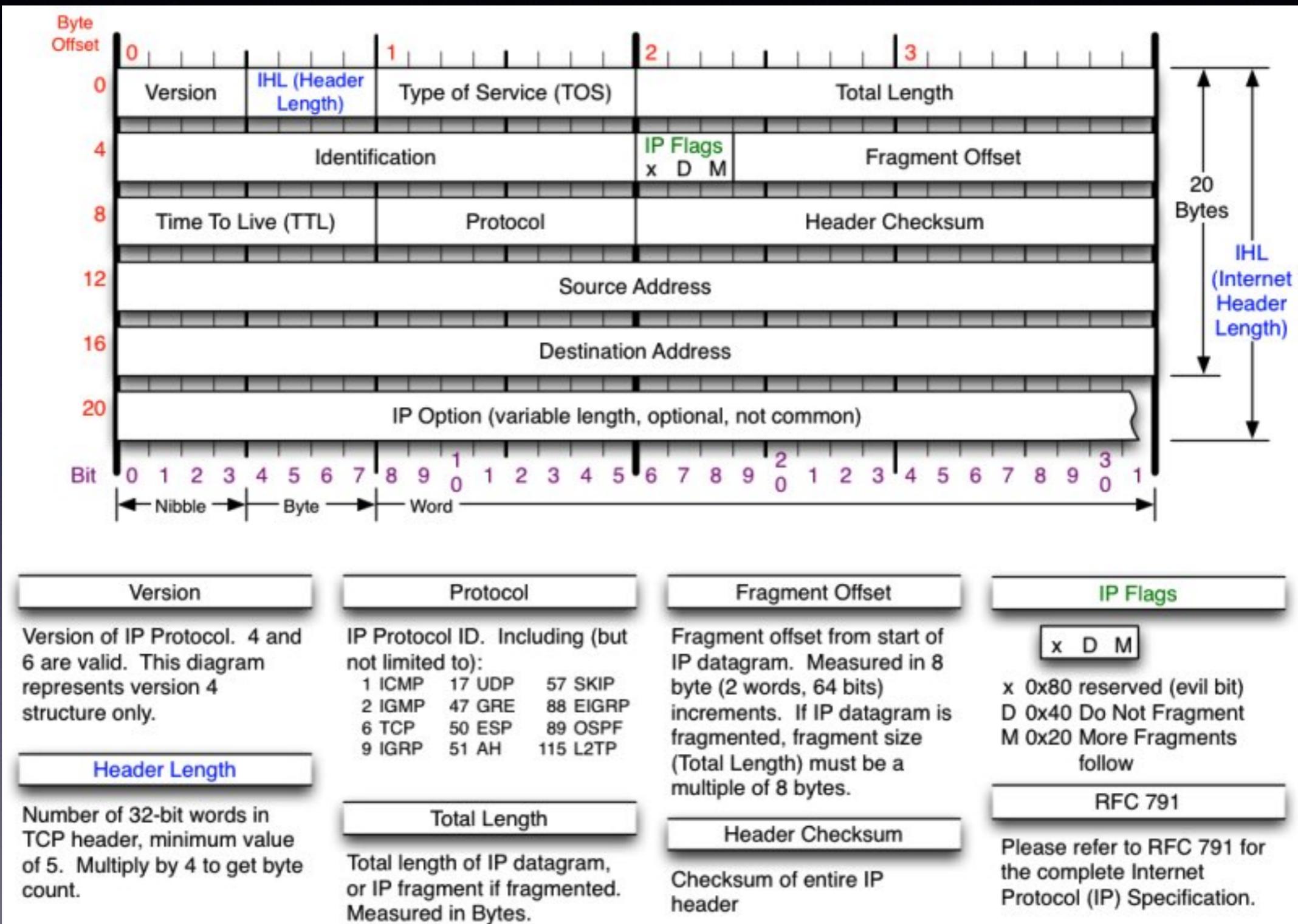
Réalisation d'un OU Logique

Adresse de diffusion

1|0|0|0|0|0|1|0 0|0|1|0|1|1|0|1 0|0|0|0|1|1|0|0 1|1|1|1|1|1|1|1

130 . 45 . 12 . 255

Le protocole IP



Le protocole IP



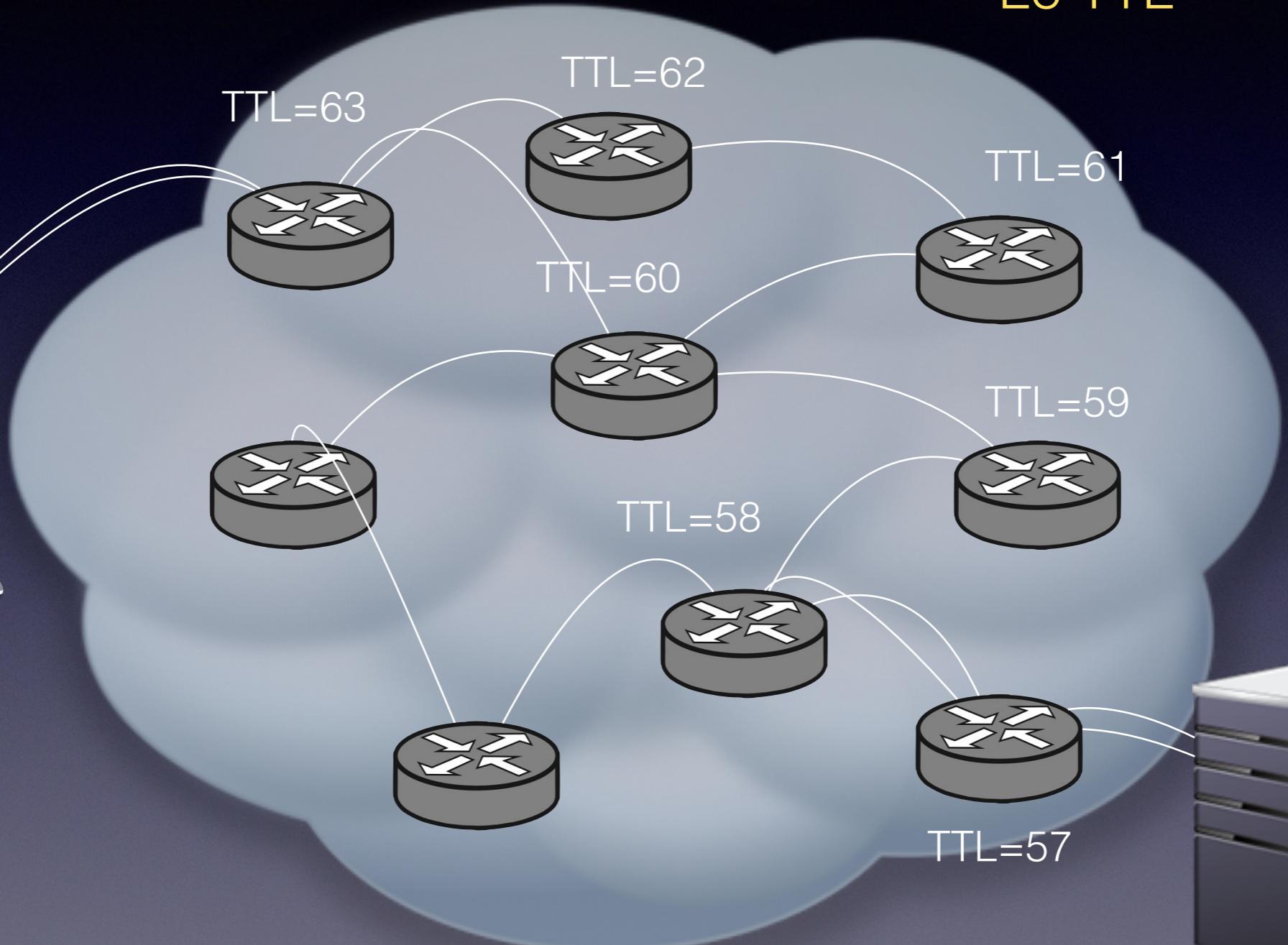
Time to Live (durée de vie du paquet)

- Compteur auquel on supprime une unité à chaque routeur ;
- Paquet détruit quand le compteur arrive à 0 ;
- Permet d'obtenir le nombre de sauts jusqu'à la destination.

Le protocole IP

Le TTL

Paquet IP
TTL=64



Le protocole IP



Le champ d'identification ID

- Identifie un paquet
- Nécessaire pour identifier un paquet lors de la fragmentation
- Permet d'évaluer la charge d'une machine si les champs ID sont incrémentaux
- Permet d'obtenir des renseignements sur l'architecture mise en place (Load balancing)
- Note: souvent ID=0 lors de la présence de répartiteurs de charge

```
kali: hping3 www.free.fr -S
HPING www.free.fr (eth0 212.27.48.10): S set, 40 headers + 0 data bytes
len=46 ip=212.27.48.10 ttl=57 DF id=51365 sport=0 flags=RA seq=0 win=0 rtt=25.8 ms
len=46 ip=212.27.48.10 ttl=57 DF id=5129 sport=0 flags=RA seq=1 win=0 rtt=27.2 ms
len=46 ip=212.27.48.10 ttl=57 DF id=51449 sport=0 flags=RA seq=2 win=0 rtt=27.0 ms
len=46 ip=212.27.48.10 ttl=57 DF id=6637 sport=0 flags=RA seq=3 win=0 rtt=29.2 ms
len=46 ip=212.27.48.10 ttl=57 DF id=51633 sport=0 flags=RA seq=4 win=0 rtt=28.2 ms
len=46 ip=212.27.48.10 ttl=57 DF id=7145 sport=0 flags=RA seq=5 win=0 rtt=27.4 ms
len=46 ip=212.27.48.10 ttl=57 DF id=53154 sport=0 flags=RA seq=6 win=0 rtt=28.1 ms
len=46 ip=212.27.48.10 ttl=57 DF id=8750 sport=0 flags=RA seq=7 win=0 rtt=27.7 ms
len=46 ip=212.27.48.10 ttl=57 DF id=54045 sport=0 flags=RA seq=8 win=0 rtt=25.8 ms
len=46 ip=212.27.48.10 ttl=57 DF id=10695 sport=0 flags=RA seq=9 win=0 rtt=26.0 ms
len=46 ip=212.27.48.10 ttl=57 DF id=55309 sport=0 flags=RA seq=10 win=0 rtt=27.4 ms
len=46 ip=212.27.48.10 ttl=57 DF id=12419 sport=0 flags=RA seq=11 win=0 rtt=27.5 ms
len=46 ip=212.27.48.10 ttl=57 DF id=55538 sport=0 flags=RA seq=12 win=0 rtt=25.5 ms
len=46 ip=212.27.48.10 ttl=57 DF id=13169 sport=0 flags=RA seq=13 win=0 rtt=27.0 ms
len=46 ip=212.27.48.10 ttl=57 DF id=57315 sport=0 flags=RA seq=14 win=0 rtt=27.5 ms
len=46 ip=212.27.48.10 ttl=57 DF id=14972 sport=0 flags=RA seq=15 win=0 rtt=27.5 ms
len=46 ip=212.27.48.10 ttl=57 DF id=17000 sport=0 flags=RA seq=16 win=0 rtt=27.1 ms
len=46 ip=212.27.48.10 ttl=57 DF id=7181 sport=0 flags=RA seq=17 win=0 rtt=27.3 ms
len=46 ip=212.27.48.10 ttl=57 DF id=17950 sport=0 flags=RA seq=18 win=0 rtt=29.9 ms
```

Le protocole ARP

- ARP (Address Resolution Protocol) RFC 826 (1981)
- Permet d'obtenir l'adresse physique d'une carte réseau (adresse MAC sur Ethernet) par rapport à une adresse IP.
- Implémenté via un « cache » dans le système d'exploitation.

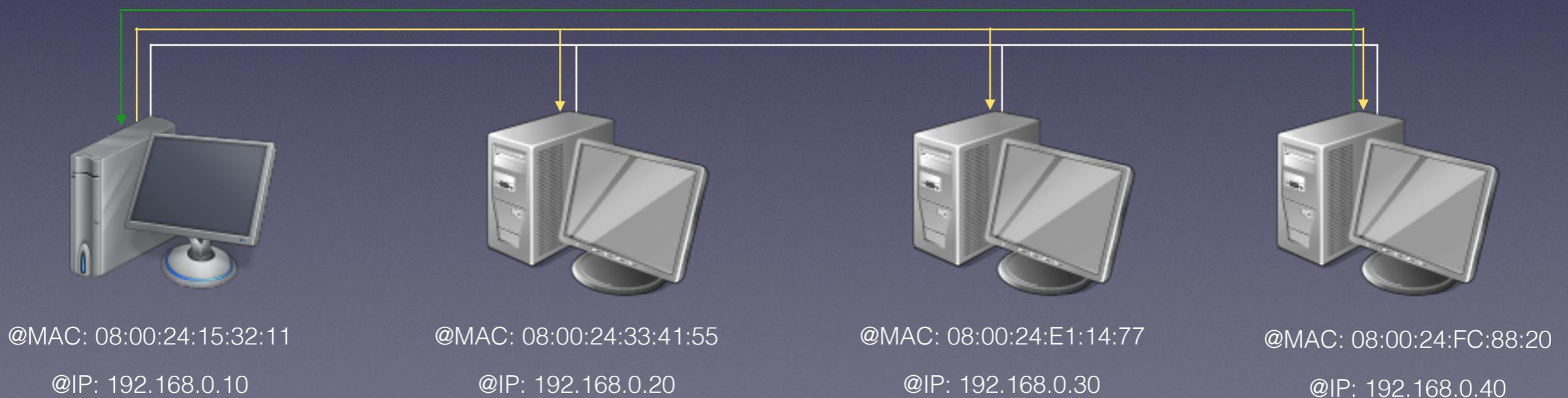
Le protocole ARP

Principe de fonctionnement

192.168.0.10 chercher à parler
avec la machine 192.168.0.40

A destination ~~de destination~~ @MAC:08:00:24:15:32:11 :
« JE suis 192.168.0.40 et j'ai la Presse 192.168.0.40:00:24:FC:88:20 »

NB : seul l'intéressé répond à la question



Le protocole ICMP

- ICMP (Internet Control Message Protocol), RFC 792 (1981)
- Protocole de gestion d'erreur IP
- Lorsqu'une erreur est rencontrée pour un paquet donné, le paquet ayant provoqué l'erreur est renvoyé en tant que données

Le protocole ICMP

Byte									8 Bytes													
Offset	0	1		2		3																
0	Type	Code		Checksum																		
4	Other message specific information...																					
Bit	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
	← Nibble →				Byte →				Word →													
ICMP Message Types												Checksum										
Type	Code/Name	Type	Code/Name	Type	Code/Name	Type	Code/Name	Type	Code/Name	Type	Code/Name	Checksum	Checksum of ICMP header									
0	Echo Reply	3	Destination Unreachable (continued)	11	Time Exceeded	11	Time Exceeded	0	TTL Exceeded	0	TTL Exceeded	RFC 792										
3	Destination Unreachable	12	Host Unreachable for TOS	13	Communication Administratively Prohibited	12	Parameter Problem	1	Fragment Reassembly Time Exceeded	1	Fragment Reassembly Time Exceeded											
0	Net Unreachable	4	Source Quench	5	Redirect	0	Redirect Datagram for the Network	1	Missing a Required Operand	0	Pointer Problem	Please refer to RFC 792 for the Internet Control Message protocol (ICMP) specification.										
1	Host Unreachable	1	Redirect Datagram for the Host	2	Redirect Datagram for the TOS & Network	1	Redirect Datagram for the TOS & Host	2	Bad Length	1	Timestamp											
2	Protocol Unreachable	8	Echo	9	Router Advertisement	8	Echo	1	Timestamp Reply	14	Timestamp Reply											
3	Port Unreachable	10	Router Selection	10	Router Selection	9	Router Advertisement	15	Information Request	15	Information Request											
4	Fragmentation required, and DF set	11	Address Mask Request	11	Address Mask Request	10	Router Selection	16	Information Reply	16	Information Reply											
5	Source Route Failed	12	Traceroute	12	Traceroute	11	Address Mask Request	17	Address Mask Reply	17	Address Mask Reply											
6	Destination Network Unknown	13	Traceroute	13	Traceroute	12	Traceroute	18	Traceroute	18	Traceroute											
7	Destination Host Unknown	14	Traceroute	14	Traceroute	13	Traceroute	30	Traceroute	30	Traceroute											
8	Source Host Isolated	15	Traceroute	15	Traceroute	14	Traceroute	16	Traceroute	16	Traceroute											
9	Network Administratively Prohibited	16	Traceroute	16	Traceroute	15	Traceroute	17	Traceroute	17	Traceroute											
10	Host Administratively Prohibited	17	Traceroute	17	Traceroute	16	Traceroute	18	Traceroute	18	Traceroute											
11	Network Unreachable for TOS	18	Traceroute	18	Traceroute	17	Traceroute	30	Traceroute	30	Traceroute											

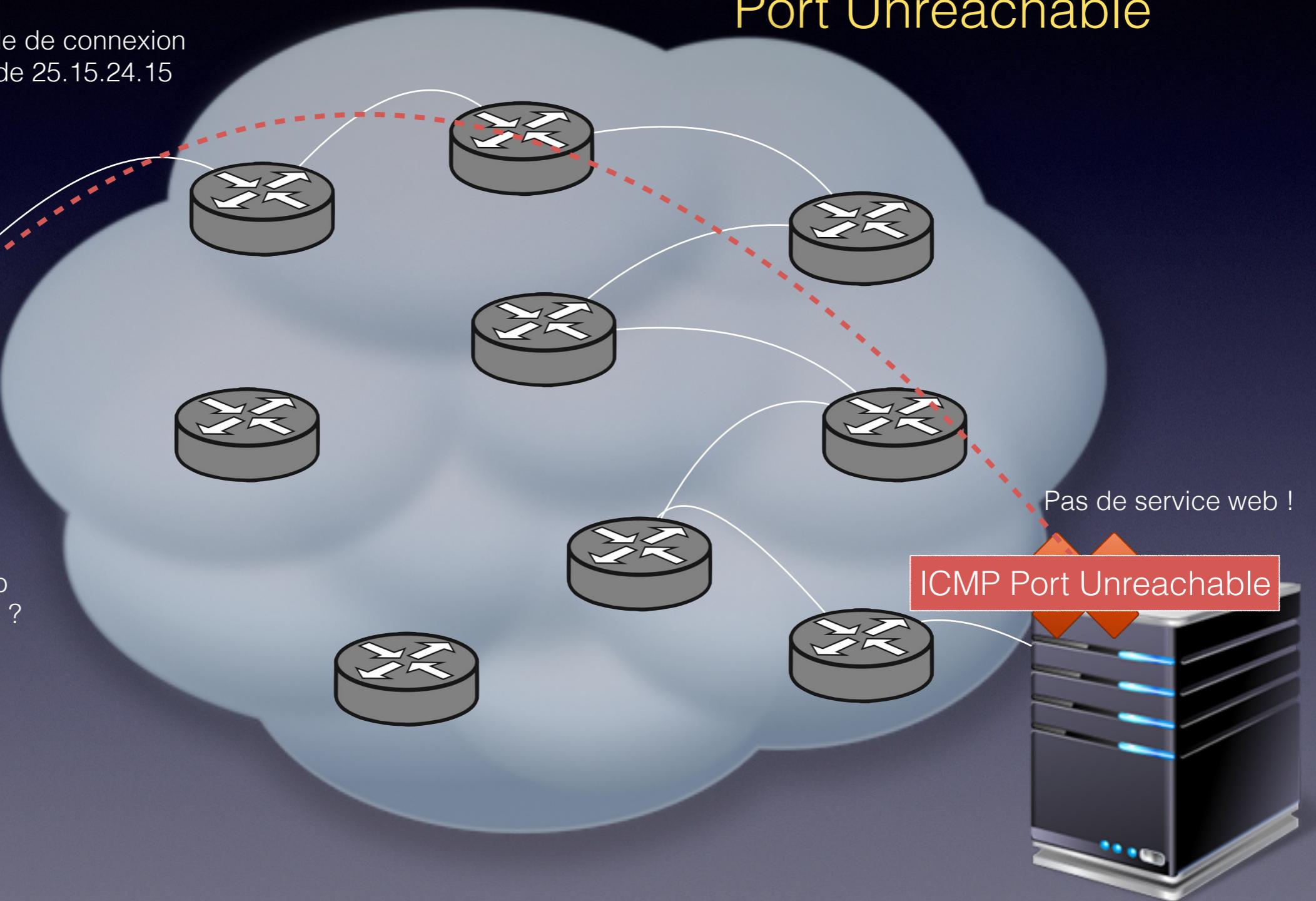
Le protocole ICMP

Port Unreachable

Envoi d'une demande de connexion
sur le service web de 25.15.24.15



Y a-t-il un serveur Web
à l'adresse 25.15.24.15 ?



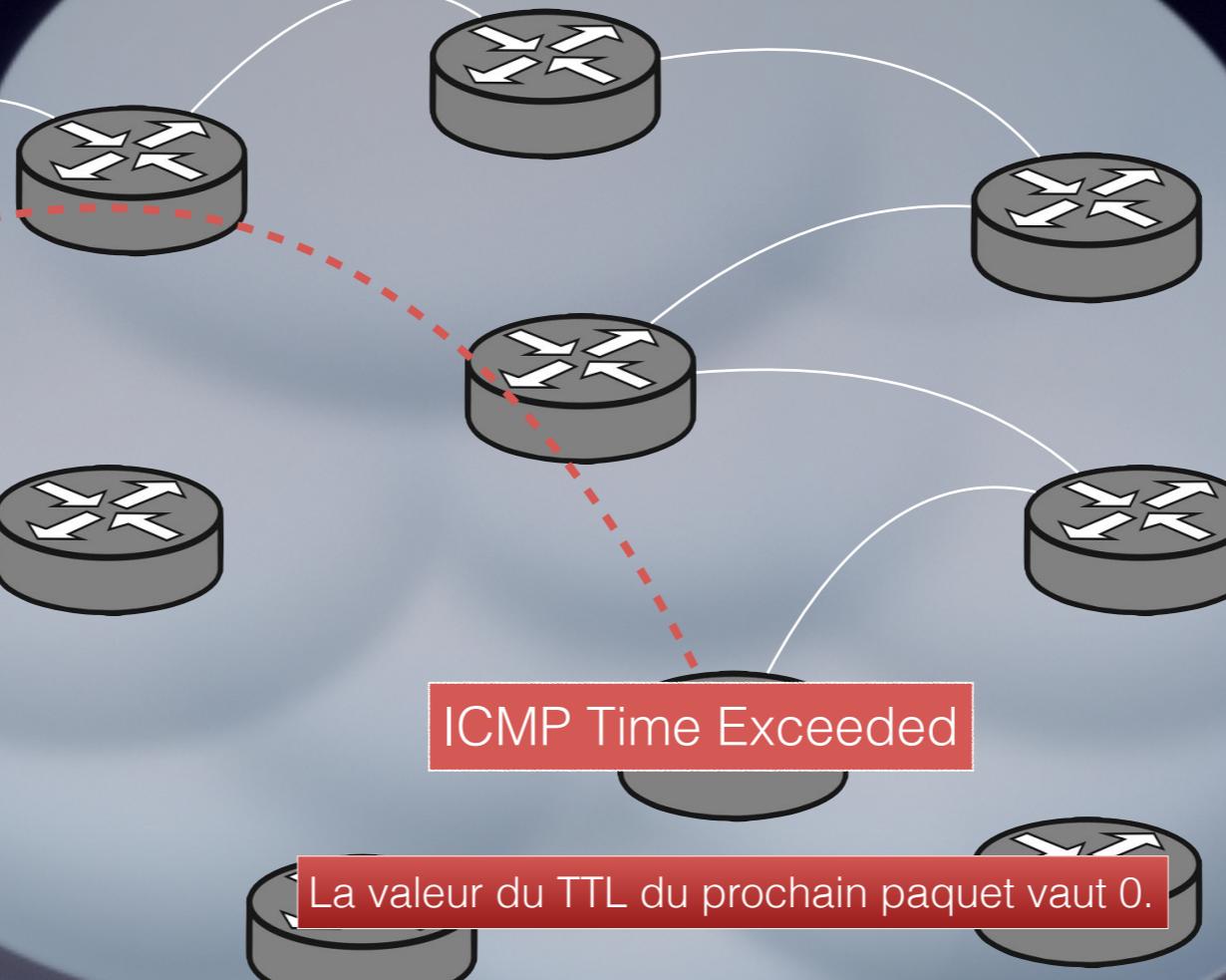
25.15.24.15

Le protocole ICMP

Envoi d'une demande de connexion
sur le service web de 25.15.24.15

Port Time Exceeded

TTL=0

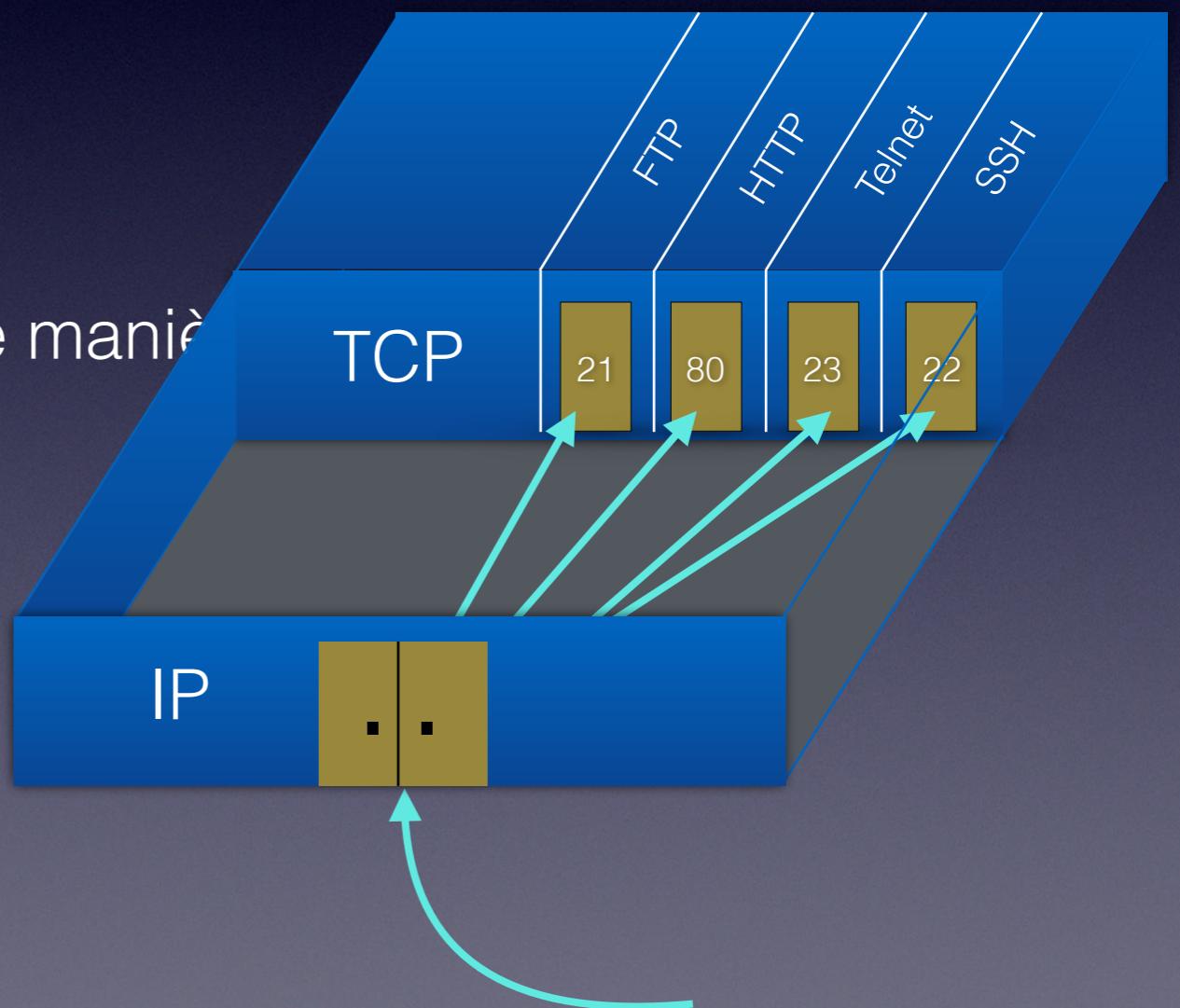


Le routeur informe l'émetteur du paquet
qu'il n'a pas pu joindre la destination dans les « temps »

25.15.24.15

Les ports de service

- Un port sert à identifier le processus émetteur et le processus récepteur
- Il y a 65535 ports de service
- Les ports < 1024 sont attribués de manière fixe à des applications

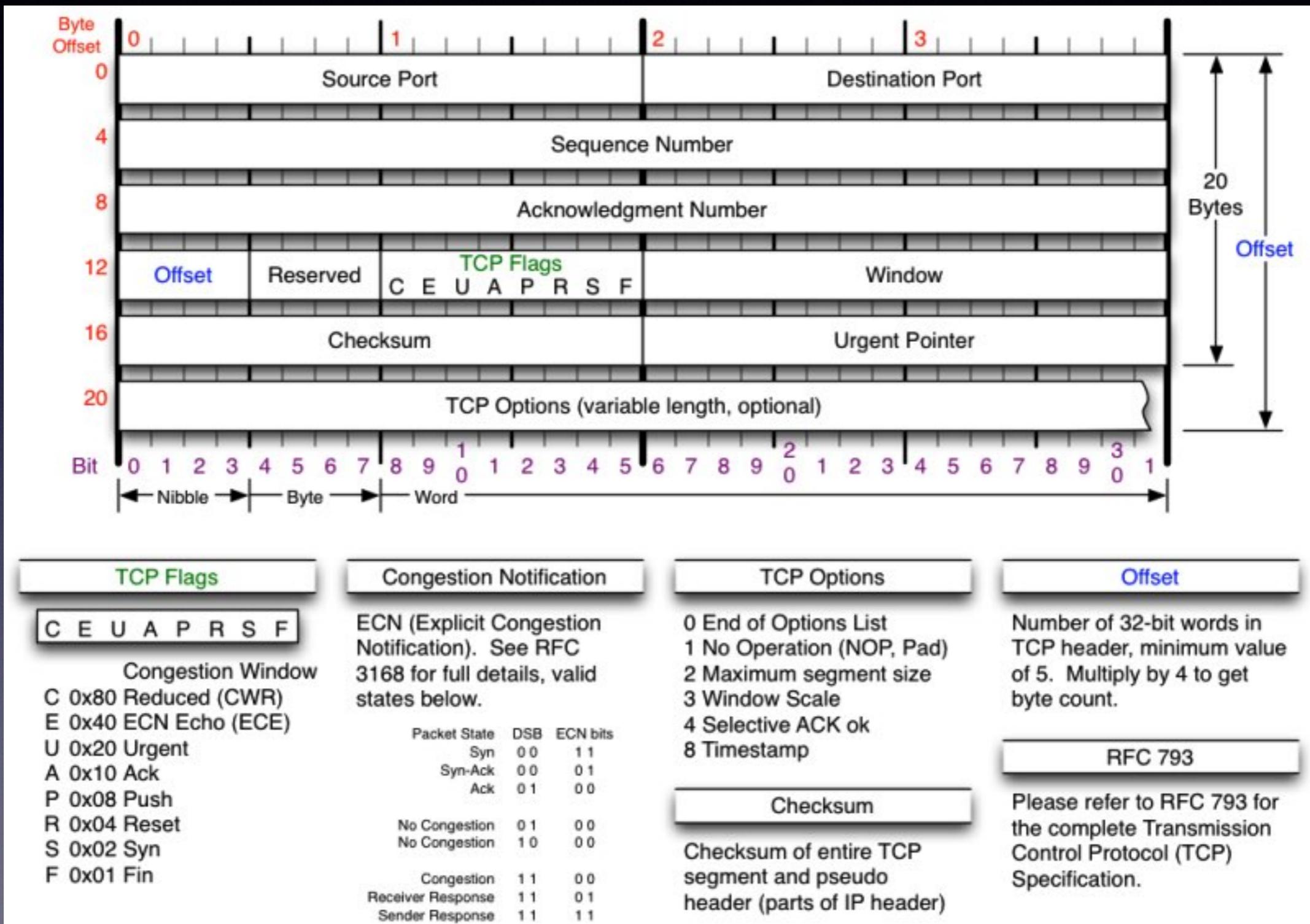


NB : sous *X, seul root est autorisé à utiliser des ports < 1024.

Le protocole TCP

- TCP (Transmission Control Protocol), RFC 793 (1981)
- Notion de port dédié (ex: HTTP/80) et de multiplexage
- Notion de connexion
 - contrôle d'erreur
 - contrôle de flux
 - contrôle de congestion
 - numéro de séquence unique pour chaque segment TCP
- Notion de drapeaux (SYN, ACK, RST, FIN...)

Le protocole TCP



Le protocole TCP

Les drapeaux TCP (flags)

- SYN : demande de synchronisation ou établissement de connexion
- ACK : signale que le paquet est un accusé de réception (ACKnowledgement)
- RST : rupture anormale de la connexion (ReSeT)
- FIN : demande la fin de la connexion
- PSH : données à envoyer tout de suite (PuSH)
- URG : signale la présence de données URGentes

Le protocole TCP

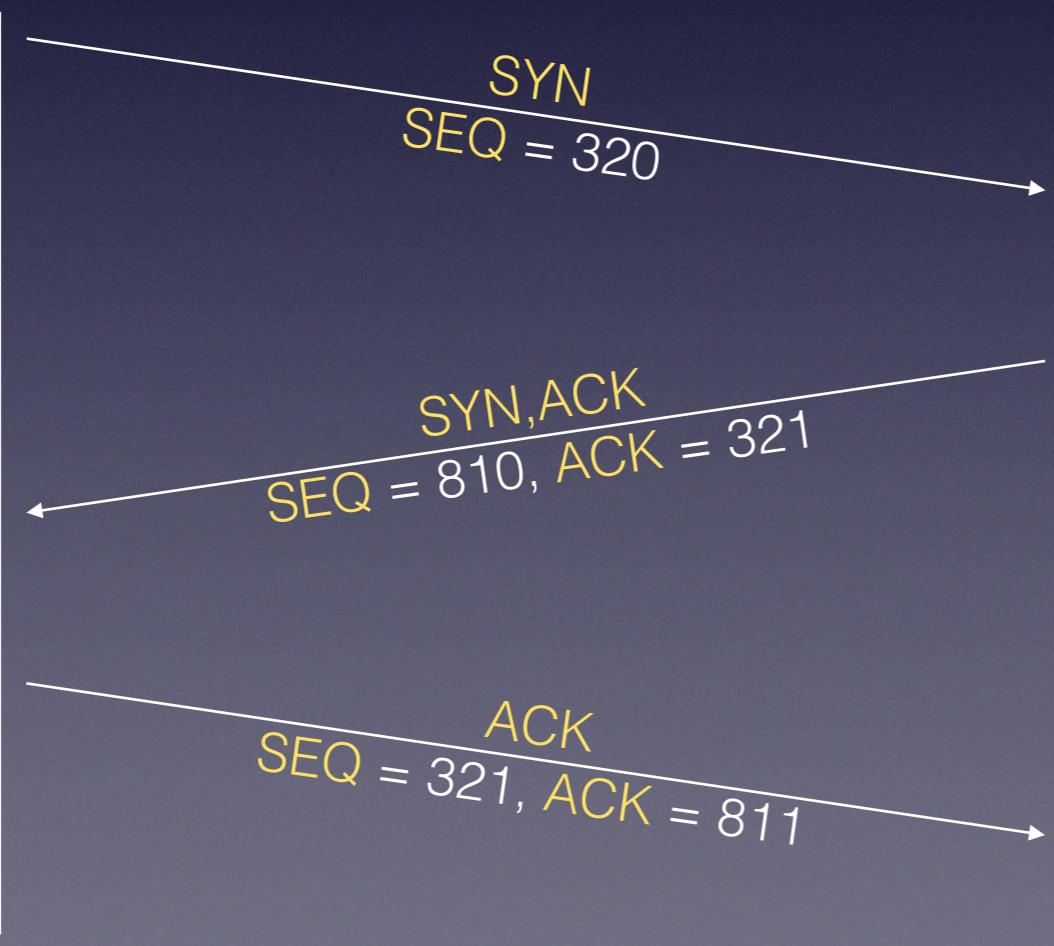
Etablissement d'une connexion



(client)



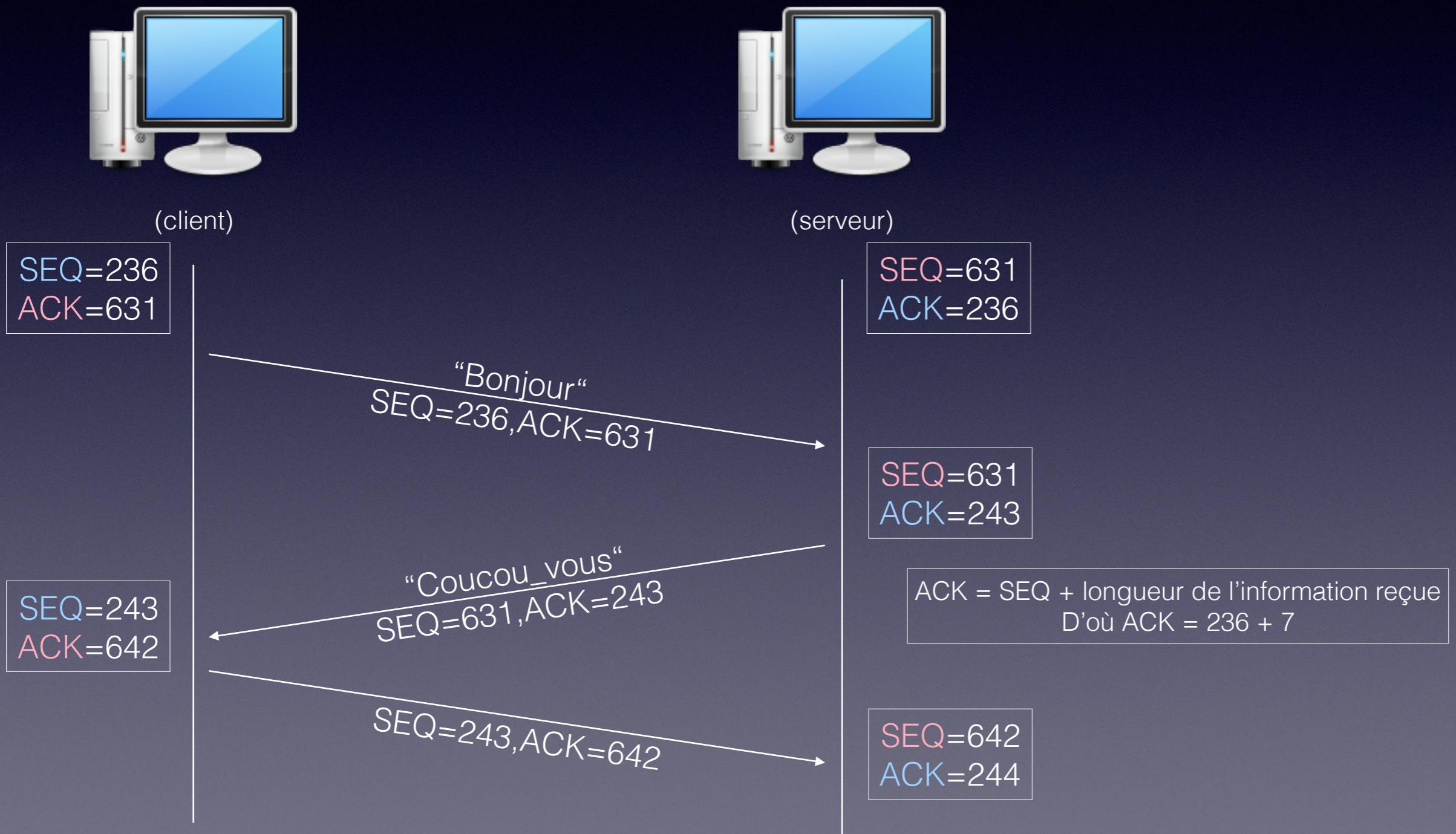
(serveur)



Three-way handshake

Le protocole TCP

Contrôle du flux



Le protocole TCP

L'option TCP Timestamp

- Permet de connaître le temps de fonctionnement d'une machine (uptime) et permet d'évaluer le nombre de machines.

```
kali:hping3 www.google.fr -p 80 -S --tcp-timestamp -c 4
HPING www.google.fr (eth0 74.125.206.94): S set, 40 headers + 0 data bytes
len=56 ip=74.125.206.94 ttl=45 id=45079 sport=80 flags=SA seq=0 win=42780 rtt=31.1 ms
TCP timestamp: tcpts=1907158939

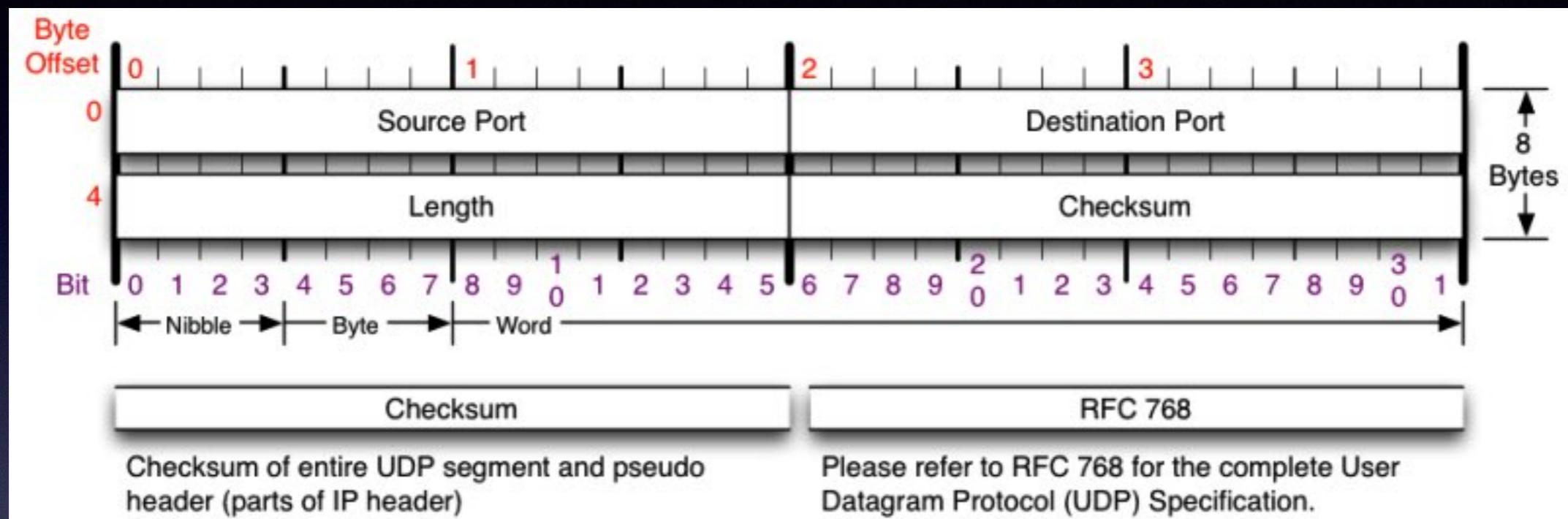
len=56 ip=74.125.206.94 ttl=45 id=10355 sport=80 flags=SA seq=1 win=42780 rtt=32.1 ms
TCP timestamp: tcpts=1882404234

len=56 ip=74.125.206.94 ttl=45 id=6768 sport=80 flags=SA seq=2 win=42780 rtt=35.8 ms
TCP timestamp: tcpts=1902939851
HZ seems hz=1000
System uptime seems: 22 days, 0 hours, 35 minutes, 39 seconds

len=56 ip=74.125.206.94 ttl=45 id=6545 sport=80 flags=SA seq=3 win=42780 rtt=32.7 ms
TCP timestamp: tcpts=1907764662
HZ seems hz=1000
System uptime seems: 22 days, 1 hours, 56 minutes, 4 seconds

--- www.google.fr hping statistic ---
```

Le protocole UDP

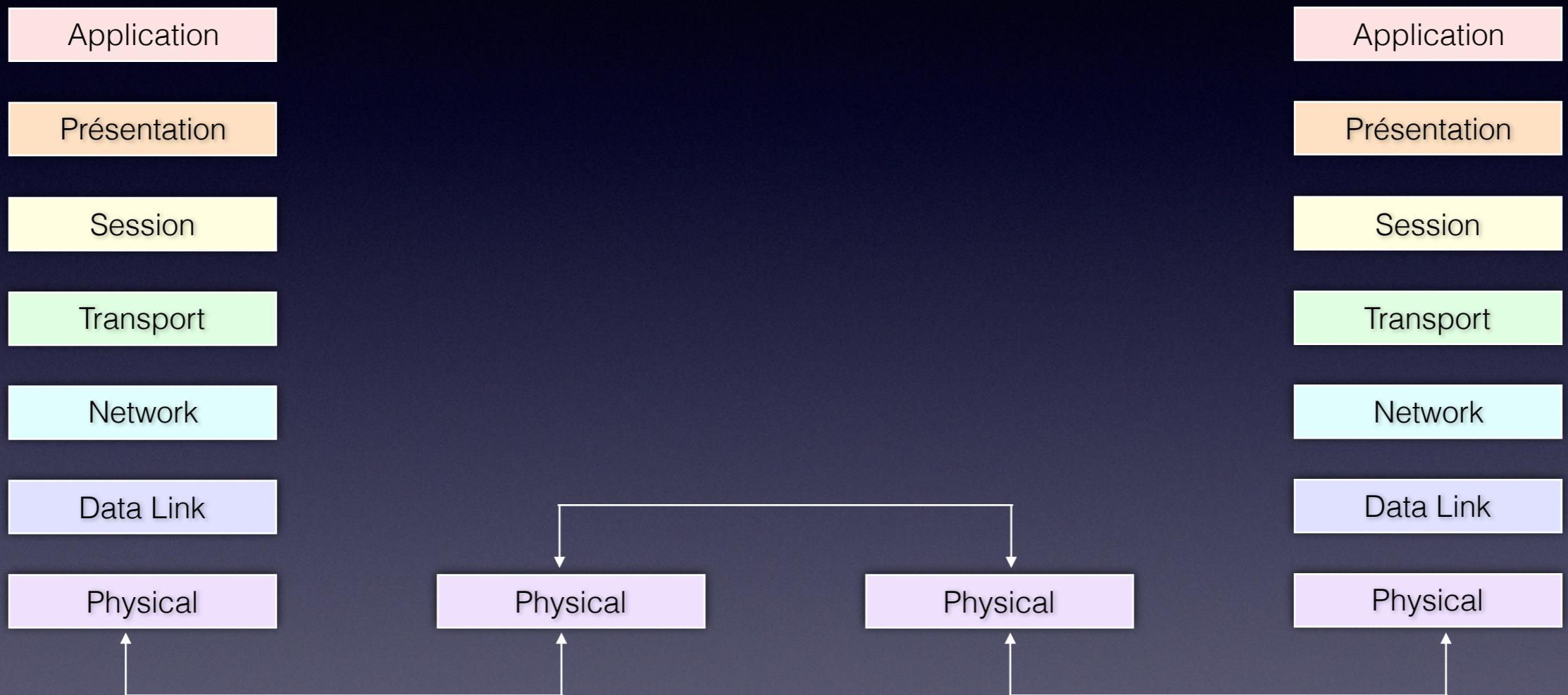


- Mode déconnecté
- Transmission sans garantie de succès
- Pas d'ordonnancement, pas de gestion d'erreur
- Pas de maintien de port ouvert
- Services utilisateurs : DNS, TFTP, SNMP, Netbios...

Send and Pray!

Niveau d'interconnexion

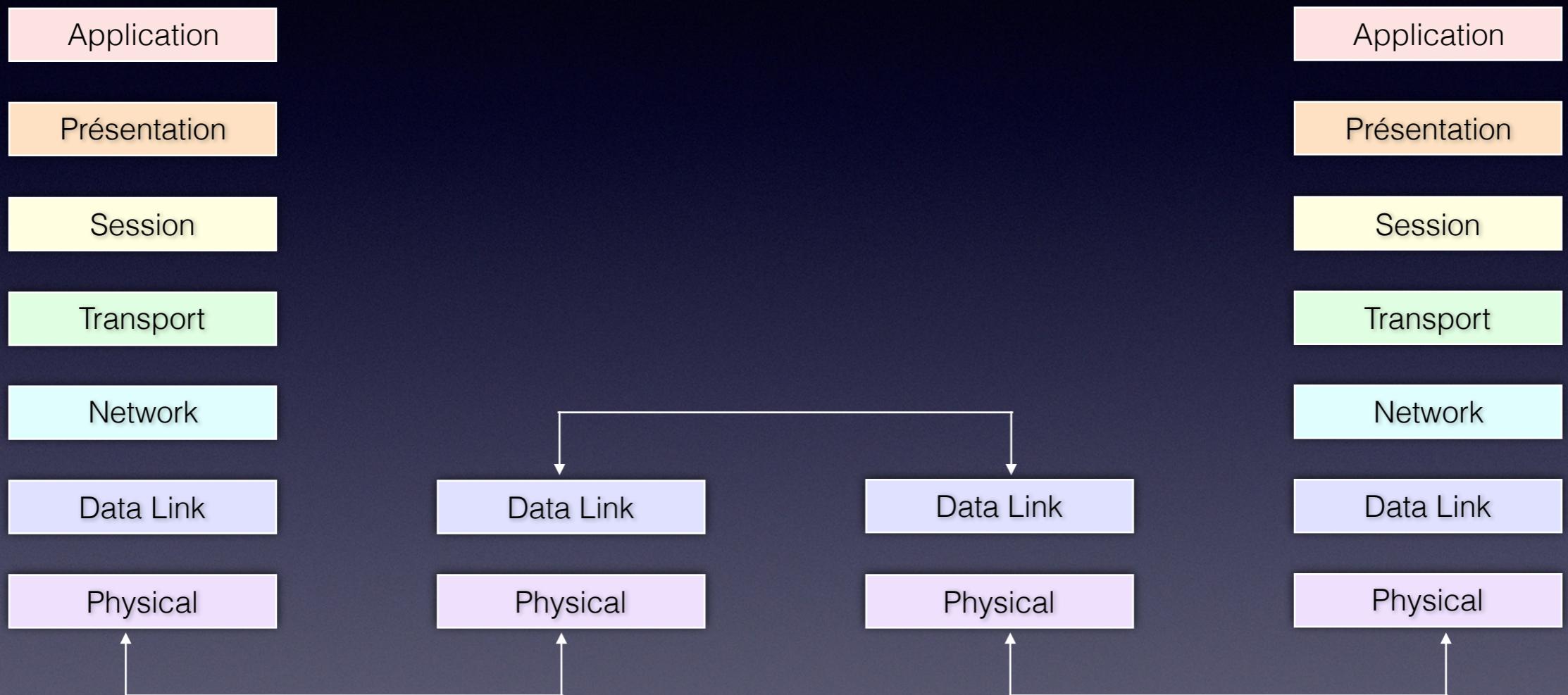
Répéteur ou amplificateur (« Repeater »)



- Amplification du signal pour augmenter la taille du réseau
- Conversion de signaux (vers fibre optique)

Niveau d'interconnexion

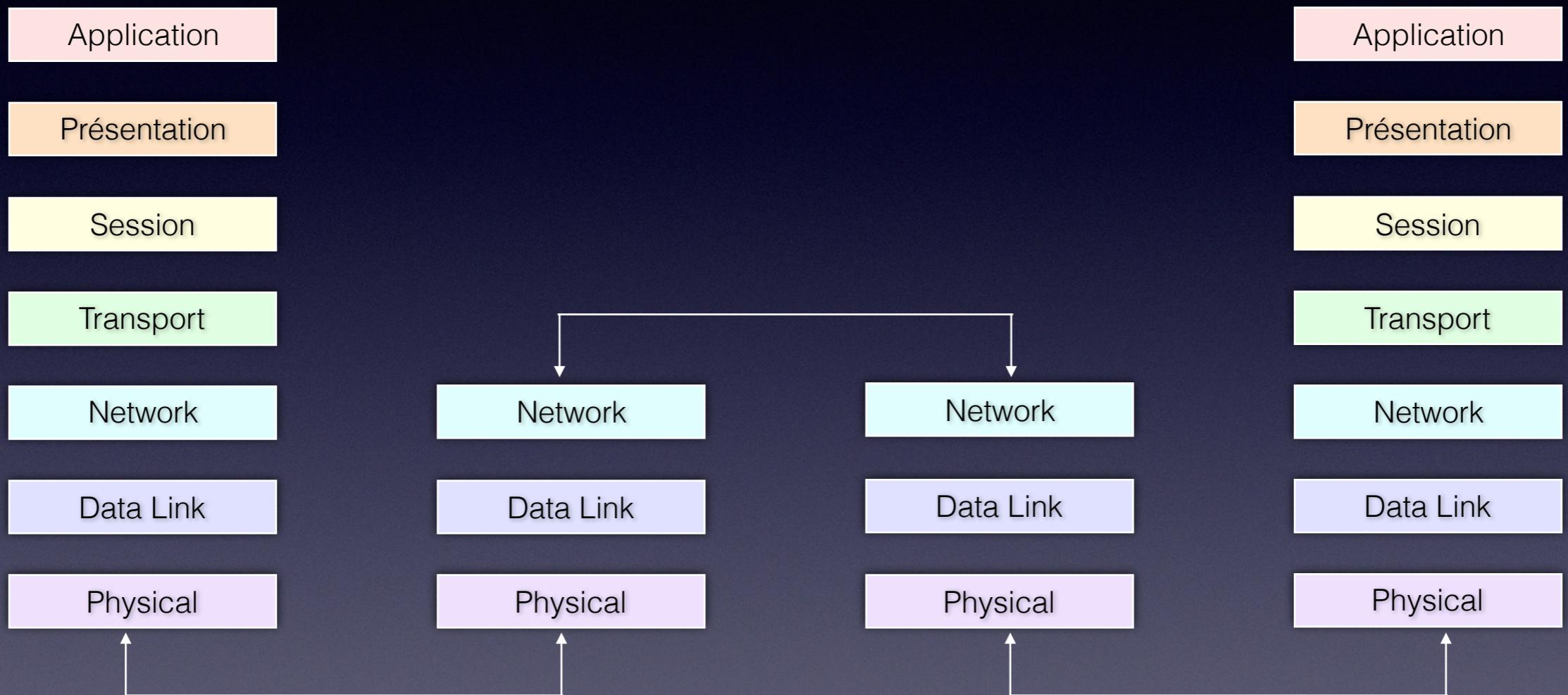
Pont (« Bridge »)



- Conversion de signaux (couche 1) et de format de trames (couche 2)

Niveau d'interconnexion

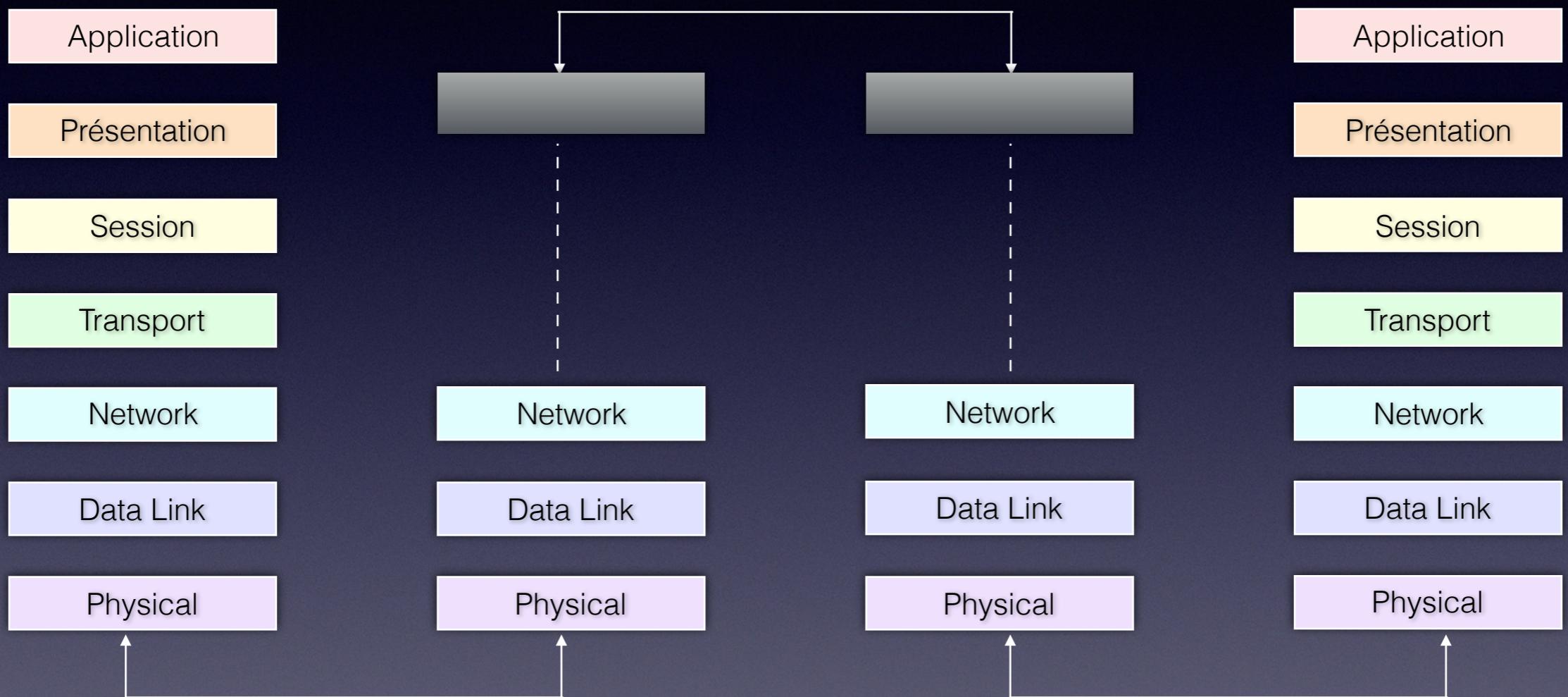
Routeur (« Router »)



- Conversion de format des paquets et adresses
- Routage des paquets

Niveau d'interconnexion

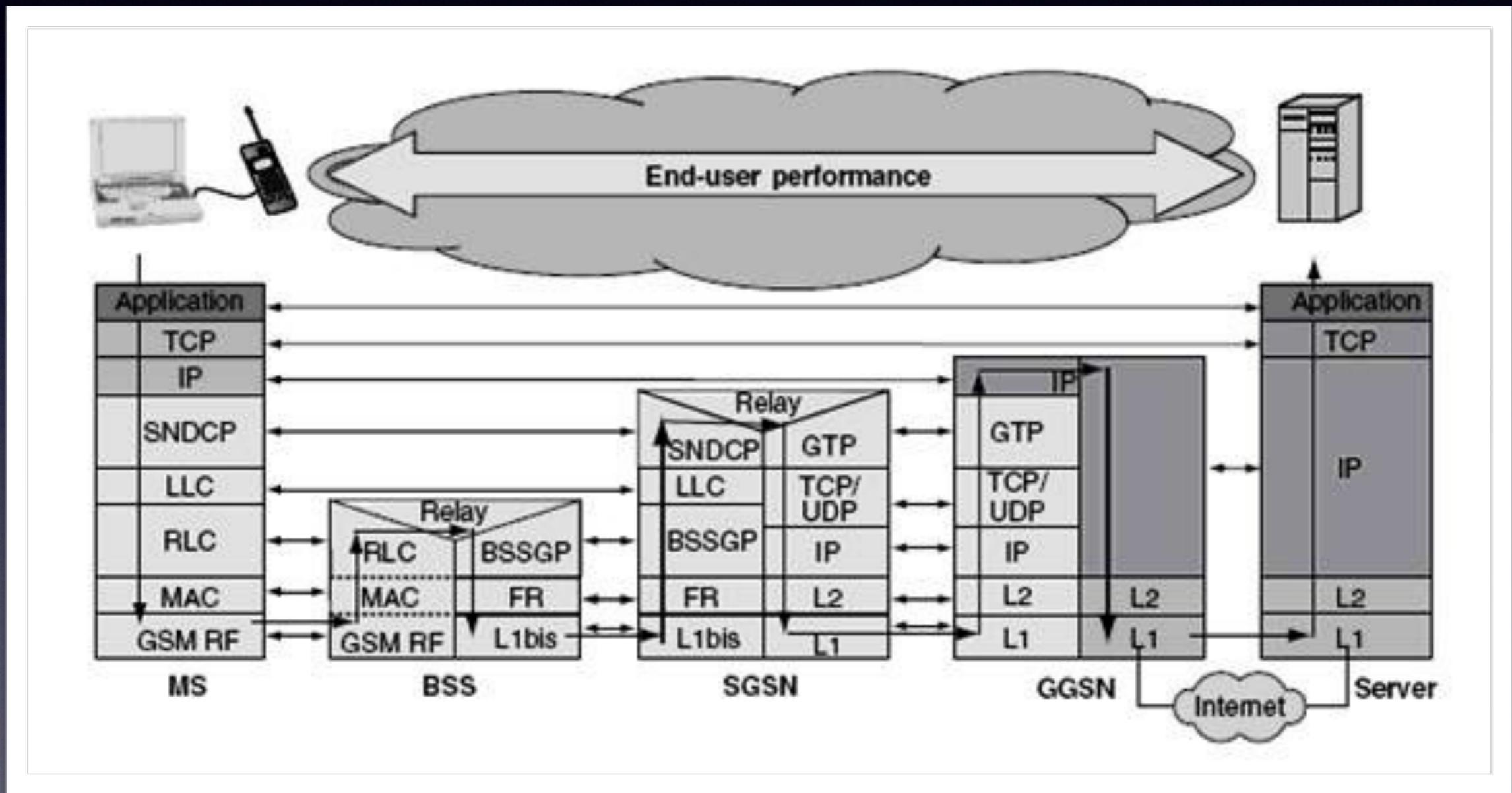
Passerelle (« Gateway »)



- Conversion de format de messages d'une des couches supérieures (4 à 7)

Niveau d'interconnexion

Exemple de la téléphonie mobile



MS : Mobile Station

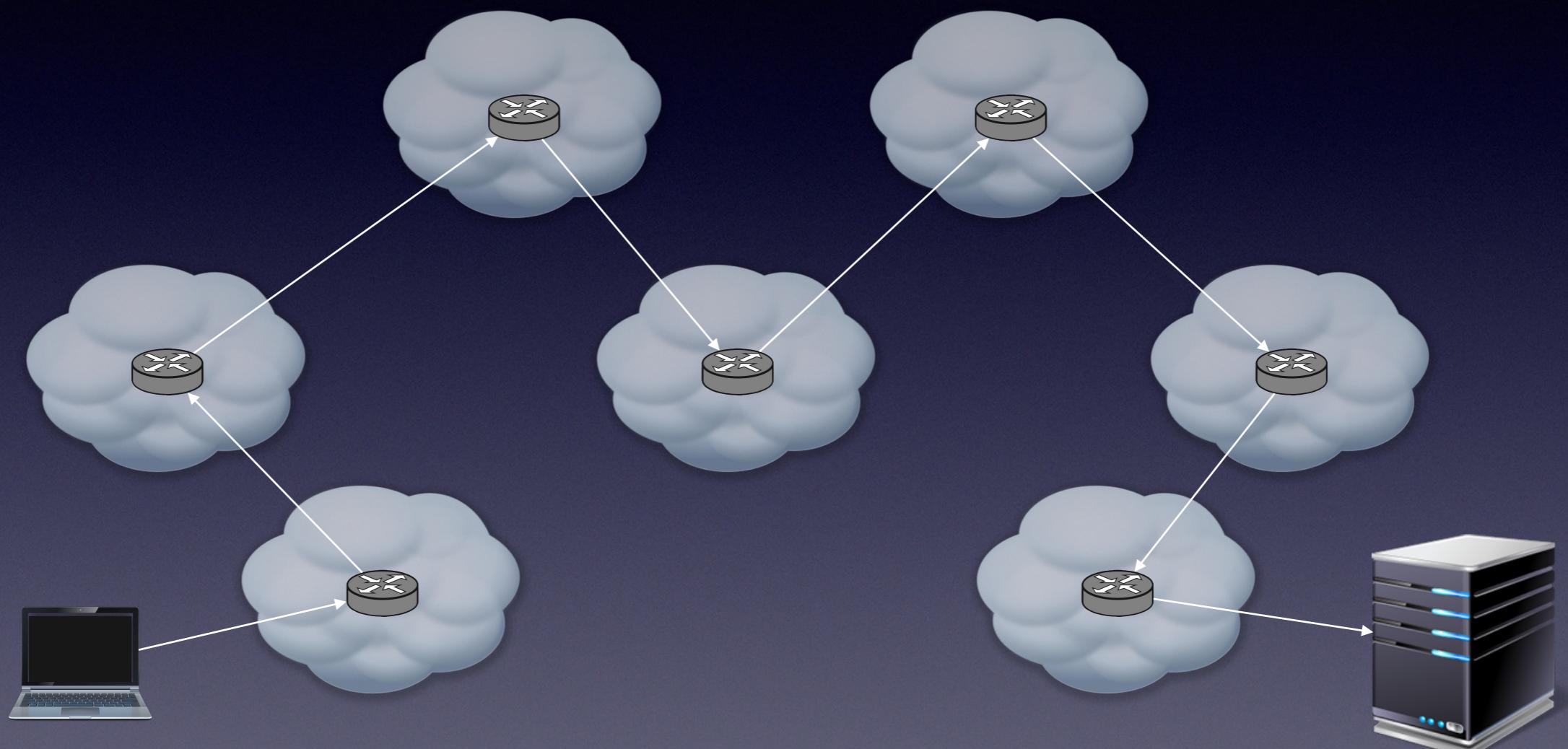
BSS : Base Station System

SGSN : Service GPRS Support Node

GGSN : Gateway GPRS Support Node

Routage

Définition

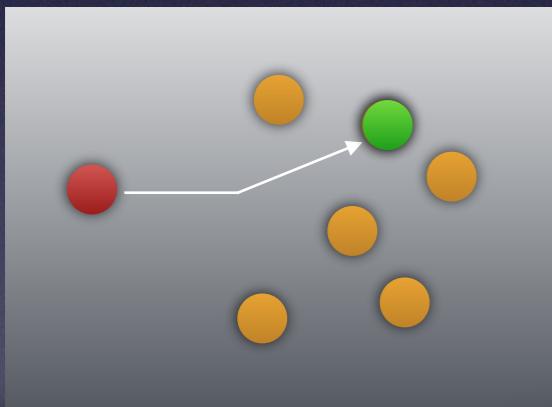


Dispositif relié à au moins deux réseaux, dont le travail est de déterminer le prochain noeud du réseau auquel un paquet de données doit être envoyé.

Routage

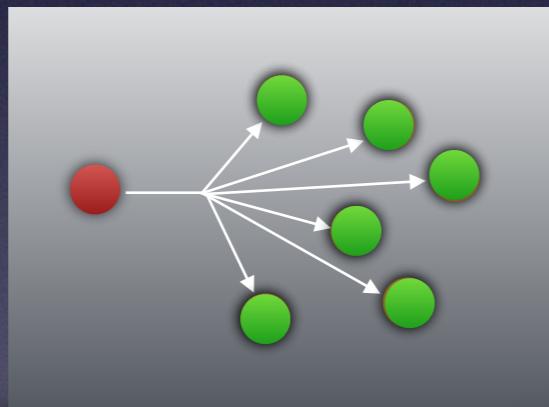
Type de communication

Unicast



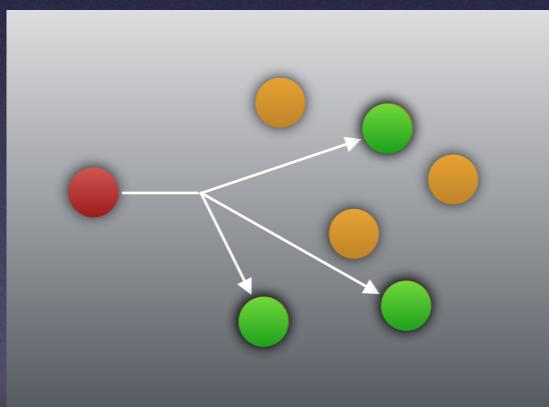
Communication 1 vers 1

Broadcast



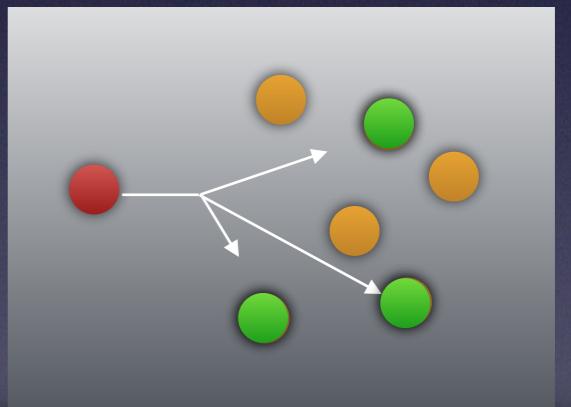
Communication 1 vers tous

Multicast



Communication 1 vers plusieurs
(mais pas tout le monde)

Anycast



Communication 1 vers 1
le plus proche ou le plus efficace

Routage

Table de routage

Etablit la correspondance entre une machine destination, le prochain routeur et l'interface réseau à utiliser pour suivre ce chemin.

2 types de routage :

- routage statique
- routage dynamique

Routage

Routage statique

L'administrateur réseau paramètre de façon statique la table de routage.

Inconvénients : c'est long, fastidieux, source d'erreur, donc pas très efficace.



« Je connais les réseaux A et B »

L'administrateur m'a indiqué que le routeur 2 connaissait le réseau C



« Je connais les réseaux B et C »

L'administrateur m'a indiqué que le routeur 1 connaissait le réseau A

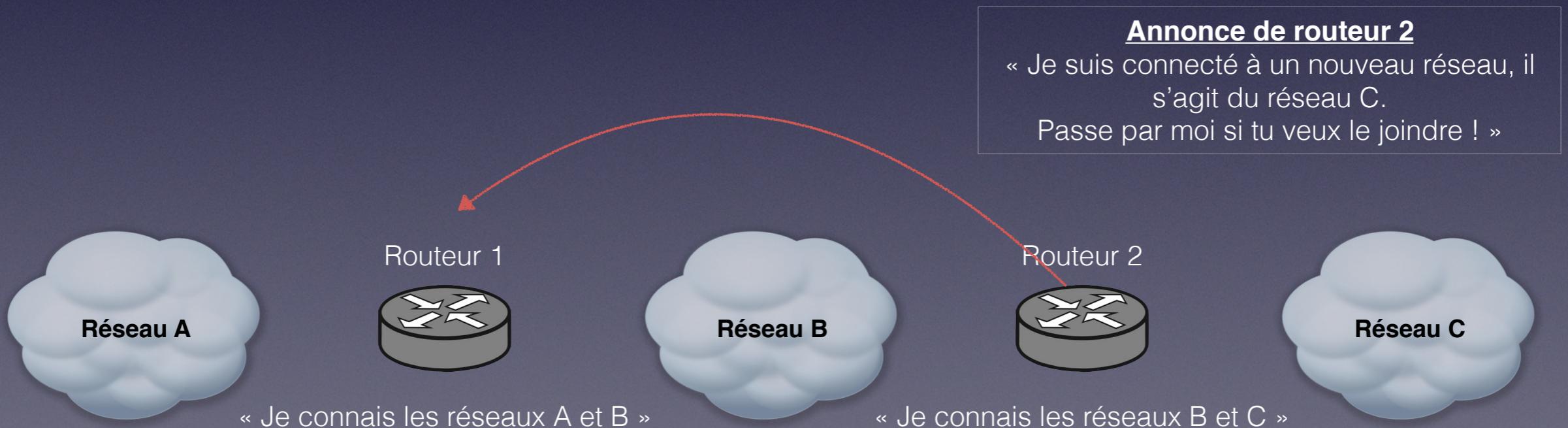


Routage

Routage dynamique

La table de routage est mise à jour automatiquement

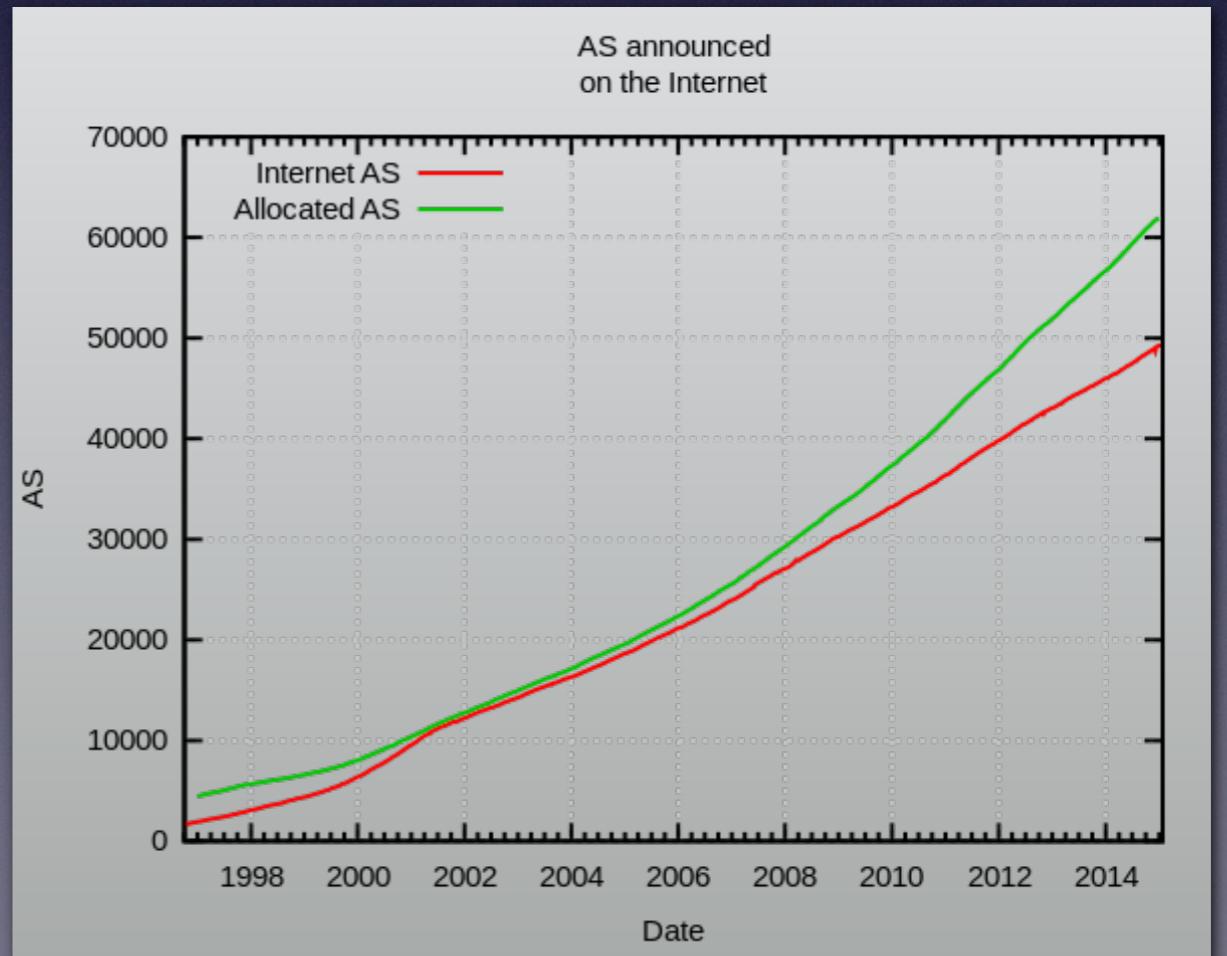
Dans le cas où la topologie réseau change (incident, coupure, maintenance, surcharge...), il faut maintenir le routage (Ex: Internet)



AS

Système Autonome

- Un AS est un ensemble de réseaux sous la même autorité (Ex: FAI)
- Les routes sont générées par des protocoles de routage intérieurs.
- Les interconnexions d'AS sont effectuées par des protocoles de routage extérieur.
- Chaque AS est identifié par un numéro (ASN) de 16 ou 32 bits.



AS

Système Autonome

www.free.fr

Source : <https://www.robtex.com/dns/www.free.fr.html#records>

Records

Displays various information related to AS, BGP, Routes and Location.

Base	Record	Preference	Name	IP Number	Reverse	Routes	AS	Location
www.free.fr	A		www.free.fr	212.27.48.10	www.free.fr	212.27.32.0/19	AS12322 PROXAD	France
			free.fr			ProXad network /		
			freenes1-g20.free.fr	212.27.60.19	freenes1-g20.free.fr	Free SA		
	NS (primary)		freenes2-g20.free.fr	212.27.60.20	freenes2-g20.free.fr	FR-PROXAD		Paris, France
			mx1.free.fr	212.27.48.6	mx1.free.fr	Proxad / Free SAS		
	MX		mx1.free.fr	212.27.48.7	mx2.free.fr	Server internal infrastructure		
			mx2.free.fr	212.27.42.58	mx19-g26.free.fr	(SLB) Bezons, France		France
				212.27.42.59	mx20-g26.free.fr			

AS

Système Autonome

www.free.fr

Source : <https://www.robtex.com/as/as12322.html#pd>

- Network Name : Free SAS
- Name Aliases : ProXad / IliadPrimary
- ASN : 12322
- Website : <http://www.free.fr/>
- IRR AS-SET : AS-PROXAD
- Network Type : Cable/DSL/ISPApprox
- BGP Prefixes : 60
- Traffic Levels : 1 Tbps+
- Geographic Scope : EuropeSupported
- Public Notes : Free SAS is a french leading Broadband ISP part of the Iliad group (www.liiad.fr)

AS

Système Autonome

www.free.fr

Source :<http://www.cidr-report.org/cgi-bin/as-report?as=12322&view=2.0&v=4>

Prefix	AS Path	Aggregation Suggestion
62.147.0.0/16	4777 2497 12322	
78.192.0.0/10	4777 2497 12322	
78.192.0.0/11	4777 2497 12322	- Withdrawn - matching aggregate 78.192.0.0/10 4777 2497 12322
78.224.0.0/11	4777 2497 12322	- Withdrawn - matching aggregate 78.192.0.0/10 4777 2497 12322
81.56.0.0/15	4777 2497 12322	
81.56.128.0/17	4777 2497 12322	- Withdrawn - matching aggregate 81.56.0.0/15 4777 2497 12322
82.64.0.0/14	4777 2497 12322	
82.142.0.0/18	4777 2497 12322	
82.224.0.0/11	4777 2497 12322	
82.224.0.0/12	4777 2497 12322	- Withdrawn - matching aggregate 82.224.0.0/11 4777 2497 12322
82.240.0.0/12	4777 2497 12322	- Withdrawn - matching aggregate 82.224.0.0/11 4777 2497 12322
82.248.0.0/13	4777 2497 12322	- Withdrawn - matching aggregate 82.224.0.0/11 4777 2497 12322
83.152.0.0/13	4777 2497 12322	
83.158.0.0/15	4777 2497 12322	- Withdrawn - matching aggregate 83.152.0.0/13 4777 2497 12322
83.214.0.0/16	4777 2497 12322	
88.120.0.0/13	4777 2497 12322	
88.160.0.0/11	4777 2497 12322	
88.160.0.0/12	4777 2497 12322	- Withdrawn - matching aggregate 88.160.0.0/11 4777 2497 12322
88.176.0.0/12	4777 2497 12322	- Withdrawn - matching aggregate 88.160.0.0/11 4777 2497 12322
88.190.0.0/15	4777 2497 12322	- Withdrawn - matching aggregate 88.160.0.0/11 4777 2497 12322
91.160.0.0/12	4777 2497 12322	
212.27.32.0/19	4777 2497 12322	
213.36.0.0/16	4777 2497 12322	
213.228.0.0/18	4777 2497 12322	

Protocoles de routage

Routage intérieur

RIP (Routing Information Protocol)

- A chaque route est associée une métrique qui est sa distance exprimée en nombre de routeurs à traverser.
- Chaque routeur envoie régulièrement à ses voisins ses informations de routage
- En fonction des informations reçues par ses voisins, le routeur va sélectionner les meilleures routes (en fonction du facteur distance) et mettre à jour ses propres tables de routage.

Protocoles de routage

Routage intérieur

OSPF (Open Shortest Path First)

- Chaque routeur identifie son voisinage réseau
- S'il y a plusieurs routeurs sur un réseau, un routeur principal est élu parmi eux
- Chaque routeur acquiert la base de données de ce routeur
- Chaque routeur construit sa table de routage sous forme d'un arbre qui minimise les coûts des routes vers les réseaux cibles.

Protocoles de routage

Routage intérieur

EIGRP (Enhanced Interior Gateway Routing Protocol)

- à vecteur de distance IP, avec une optimisation permettant de minimiser l'instabilité de routage due aussi bien au changement de topologie qu'à l'utilisation de la bande passante et la puissance du processeur du routeur.

Protocoles de routage

Routage extérieur

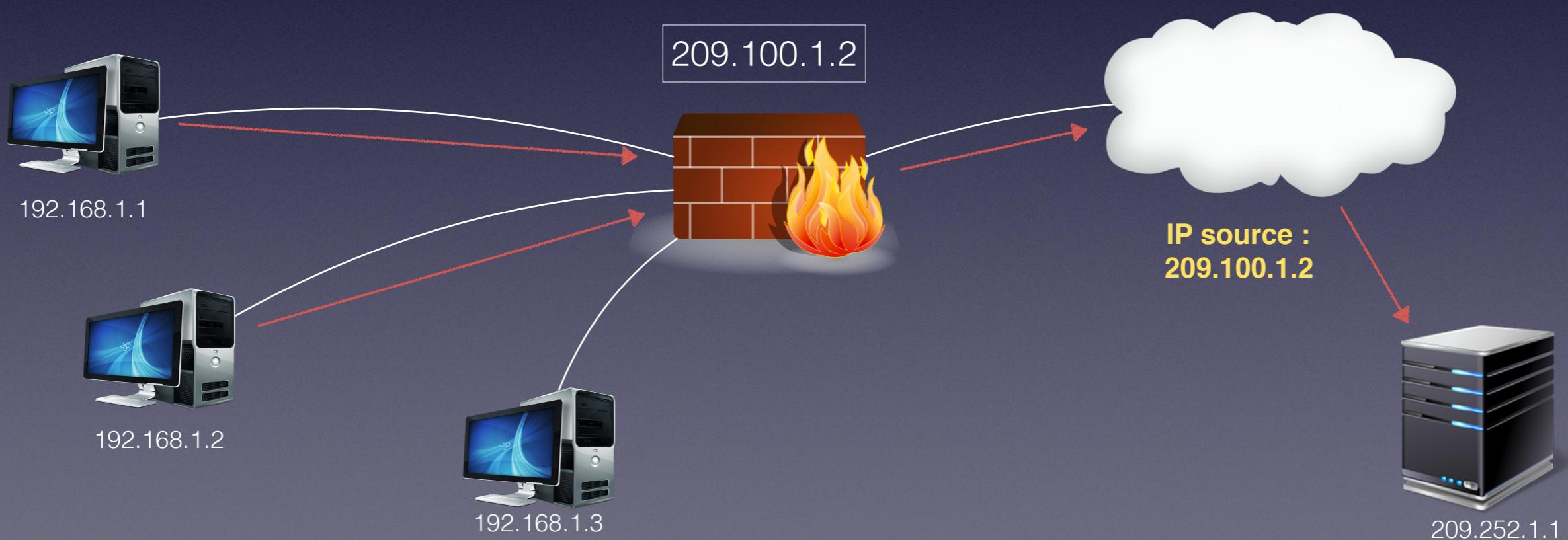
BGP (Border Gateway Protocol)

- Echange d'informations d'accessibilité entre AS
- Principalement utilisé par les Fournisseurs d'Accès Internet
- Pas de métrique
- Echange d'informations entre deux routeurs voisin sur TCP/179
- iBGP
 - Utilisé à l'intérieur d'un AS
 - Connexion entre des adresses logiques
 - En cas de coupure, la session iBGP reste active et un autre protocole prend le relai (OSPF)
- eBGP
 - Utilisé entre deux AS
 - Connexion point-à-point
 - En cas de coupure, les routes sont supprimées de la table de routage

Translation d'adresse

Permet aux machines d'un réseau de n'apparaître que sous l'identifiant d'une seule adresse IP

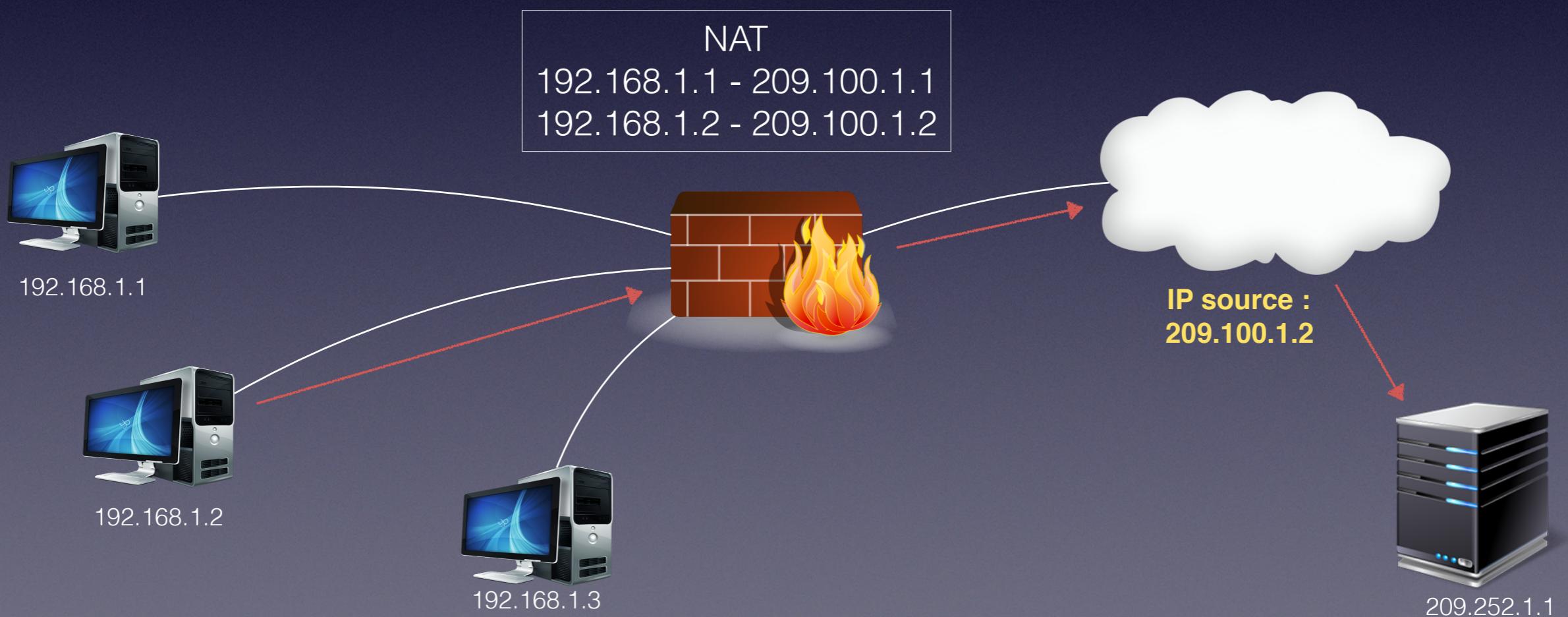
Les correspondances entre les adresses privées et publiques sont stockées dans une table NAT.



Translation d'adresse

NAT Statique

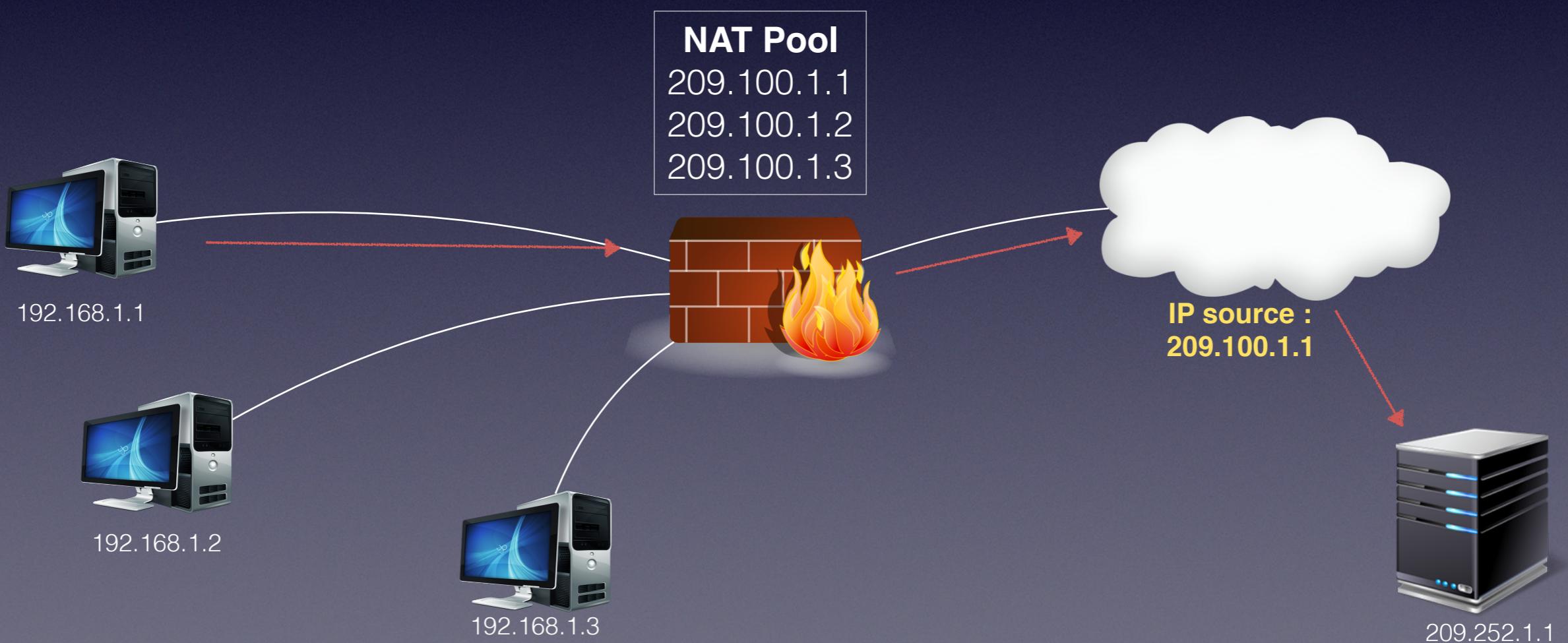
On affecte une adresse IP publique à chaque IP privée.



Translation d'adresse

NAT Dynamique

On affecte une IP publique temporairement à une IP privée
(Similaire au commutateur RTC)

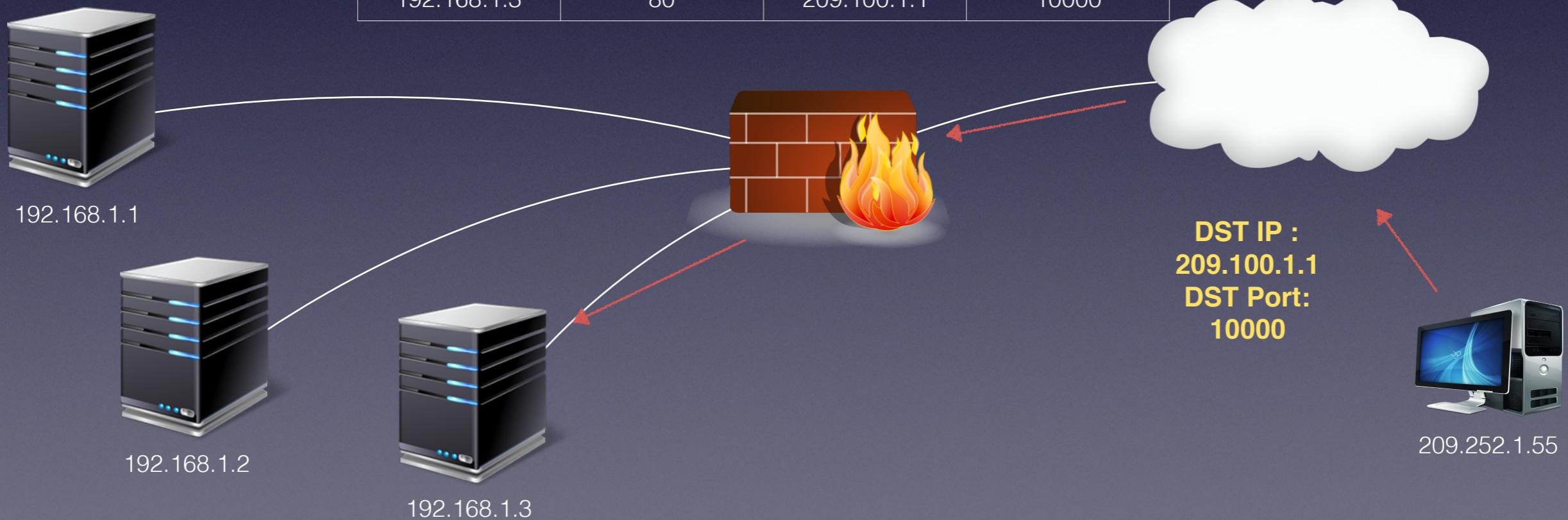


Translation d'adresse

NAPT (Network Address End Port Translation)

On affecte un couple IP/port publique temporairement à un couple IP/port privée

IP Address	Port	NAT IP	NAT Port
192.168.1.1	43	209.100.1.1	12451
192.168.1.2	80	209.100.1.1	80
192.168.1.3	80	209.100.1.1	10000



Translation d'adresse

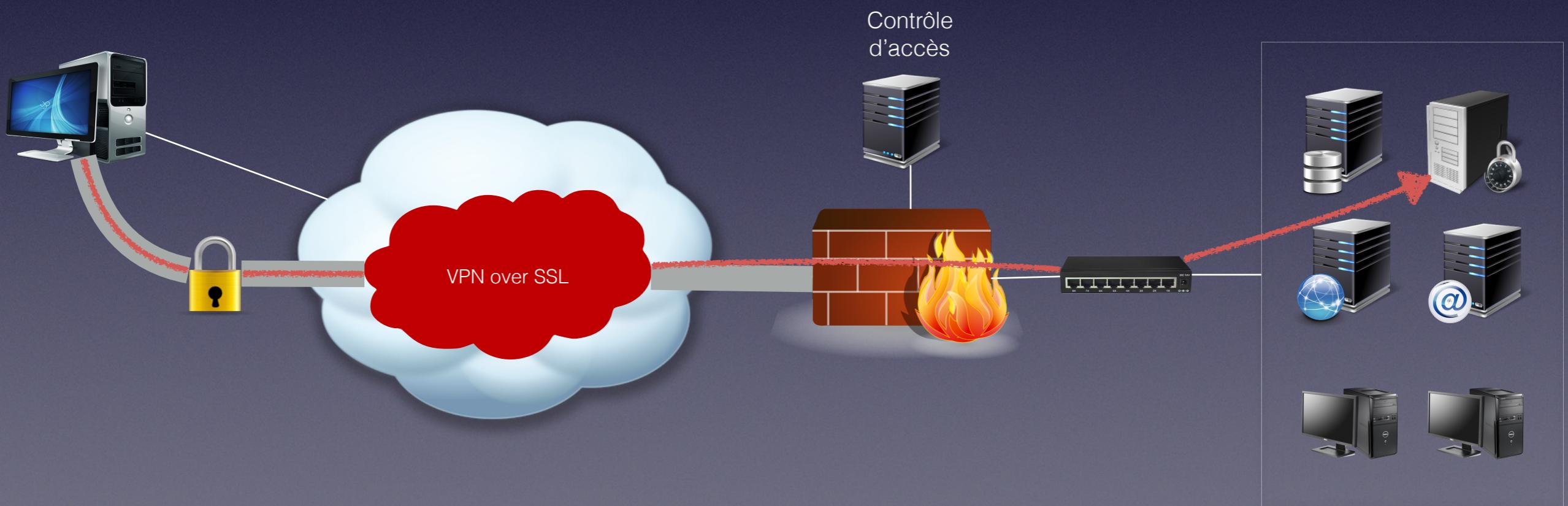
NAT Statefull

- Problème
 - Certains protocoles ne fonctionnent pas (DNS, FTP, H.323, SIP, IPSEC, SNMP,...)
- Solution
 - Routeurs NAT à inspection de contenu (Statefull)
 - Nécessite un traitement pour chaque protocole
- Exemple : IPTABLES
 - /sbin/modprobe ip_conntrack_ftp
 - Iptables -A INPUT -p tcp -sport 21 -m state -state ESTABLISHED -j ACCEPT
 - Iptables -A OUTPUT -p tcp -dport 21 -m state -state NEW,ESTABLISHED -j ACCEPT

VPN

Virtual Private Network

- Permet de se connecter de manière sécurisée à un réseau local
- Le VPN permet l'authentification et la confidentialité



- GRE (Generic Routing Encapsulation)
 - pas d'authentification, pas de chiffrement
 - IPsec over GRE (couche 3)
- PPP (point-to-point protocol)
 - Authentification => PAP & CHAP
 - Compression de data
 - PPPoX
 - PPPoA => encapsulé dans ATM
 - PPPoE => encapsulé dans ethernet
 - L2F => encapsulé dans UDP
 - PPTP => encapsulé dans des trames GRE
- PPTP (Point-to-point tunneling protocol)
 - Encapsulation ppp sur IP (couche 2)
 - ancêtre de L2TP et Ipsec, implémenté sur windows
- Confidentialité des données
- L2TP (layer 2 tunneling protocol)
 - Concurrent public (ietf) à PPTP
 - PPTP+L2F (couche 2)
 - Confidentialité, intégrité et non répudiation (assurance sur l'identité de l'expéditeur) des données
- IPSec
 - Confidentialité, intégrité et non répudiation (couche 3)
- SSL/TLS (Secure sockets layer/ Transport layer security)
 - SSL renommé en TLS (2001)
 - Authentification(certificat), Confidentialité, intégrité
 - navigateur web
- SSH

Le réseau Internet

Le réseau Internet

- 1969 : la DARPA (Defense Advanced Research Projects Agency) commande le développement d'un réseau de communication devant :
 - résister à une attaque nucléaire (maillage)
 - fonctionner indépendamment de tout contrôle centralisé
 - Il est composé de 4 calculateurs
 - Les principes de base
 - compatibilité avec de nombreux matériels ;
 - services reposant sur le modèle client - serveur
- 1972 : Démonstration de ARPANET
 - IMP : Interface Message Processor - mode connecté (X.25)
 - NCP : Network Control Program - non connecté (ancêtre de TCP)

Le réseau Internet

- 1977 - 1979 : les protocoles TCP/IP prennent leur forme définitive
- 1980 : l'université de Berkeley intègre TCP/IP dans Unix (BSD)
- 1980 - Janvier 1983 : tous les réseaux raccordés à ARPANET sont convertis à TCP/IP
- 198X : TCP/IP devient le standard de facto pour l'interconnexion de réseaux hétérogènes
- 1988 : Mise en place du Backbone de la NFSnet (12 réseaux régionaux)
- 1992 : EBone et RENATER
- 199X : Explosion de l'offre et de la demande de services Internet y compris pour les particuliers.

Le réseau Internet

Qu'est-ce qu'Internet ?

- 3 définitions :

1.Une famille de protocoles de communication appelée :

- TCP/IP : Transmission Control Protocol / Internet working Protocol
- ou Internet Protocol Suite,

2.Un réseau mondial constitué de milliers de réseaux hétérogènes, et interconnectés au moyen des protocoles TCP/IP :

- Réseaux locaux d'agences gouvernementales, institutions d'éducation, hôpitaux, des commerciaux, ...
- Réseaux fédérateur de Campus,
- Réseaux Régionaux, Nationaux, Intercontinentaux (Américains, Européen, Eunet, Ebone, Asiatiques, ...)

3.Une communauté de personnes utilisant différents services

- Courrier électronique, Web, Transfert de fichiers FTP,...

Le réseau Internet

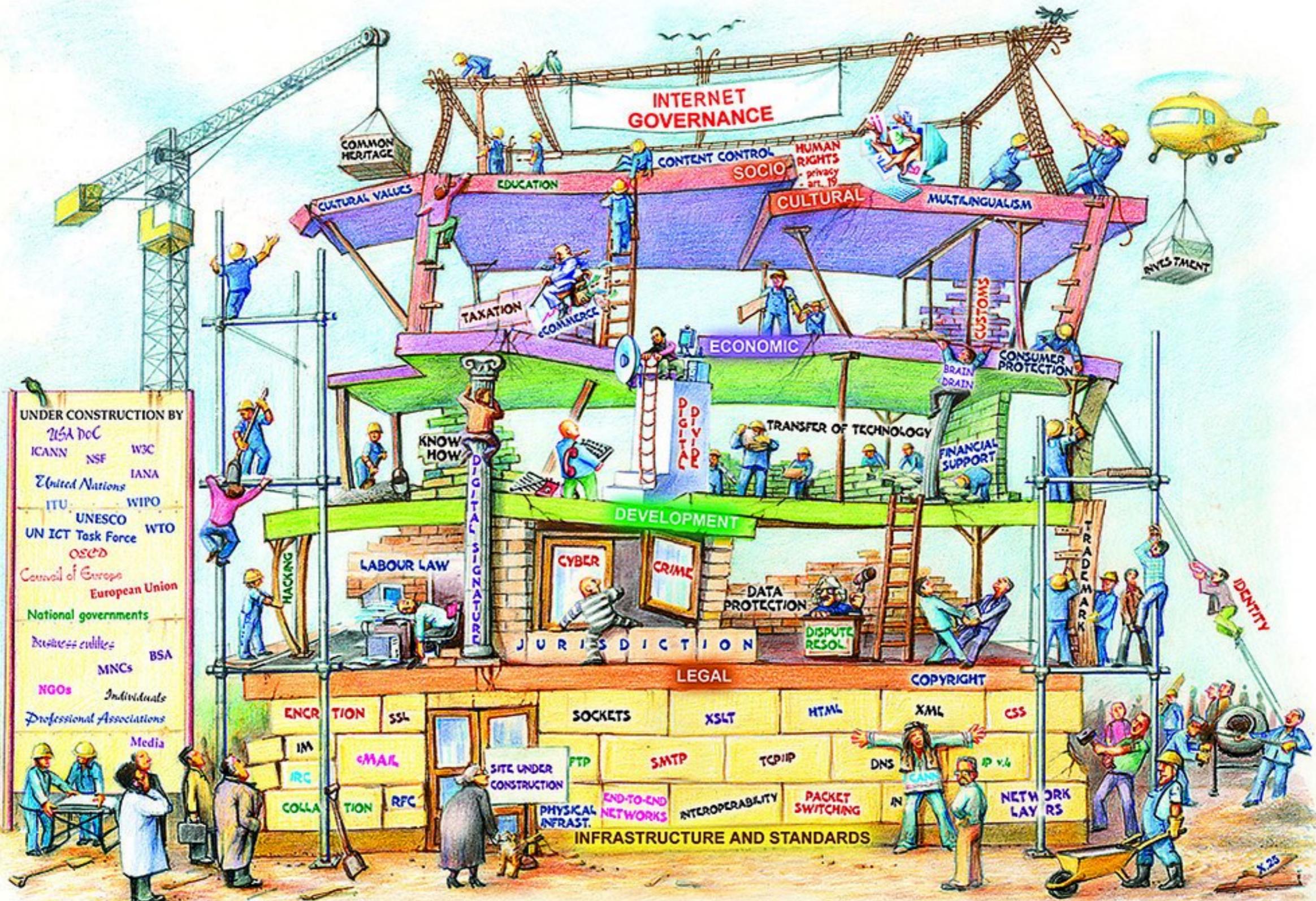
Qui normalise l'Internet ?

- Technologie Internet développée par un organisme bénévole : l'IETF (Internet Engineering Task Force)
- Les normes sont appelées RFC (Request for Comment)
 - Exemple : RFC 791 (décrit IP) - RFC 793 (décrit TCP)
 - Documents gratuits accessibles à www.ietf.org
- Tout le monde peut proposer une RFC !
 - L'IAB (Internet Activities Board) gère le processus d'acceptation des RFC
- Les standards sont publiés par une association sans but lucratif : l'internet society

Le réseau Internet

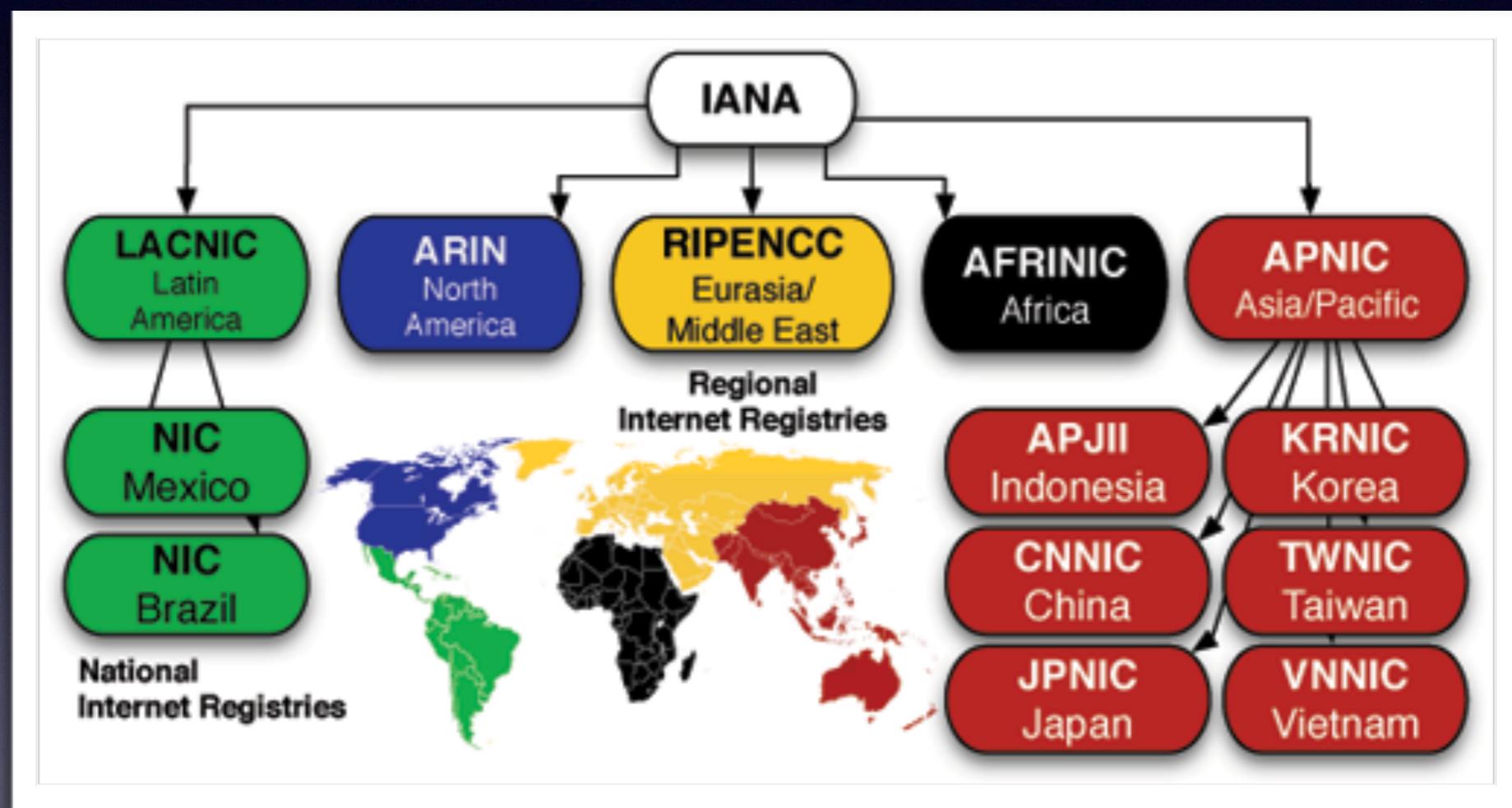
Qui gère Internet ?

- Normes techniques : IETF (internet Engineering Task Force)
- Noms de domaines :
 - ICANN (USA), RIPE (France)
 - ICANN : Internet corporation for Assigned Names and Numbers;
- Adresses IP, N° port, N° AS :
 - ICANN depuis décembre 1998;
- Réseaux :
 - ISP (Internet Service Provider),
 - NSP(Network Service Provider)
- Fibres :
 - Opérateurs télécoms
- Serveurs, contenus :
 - le monde (particuliers, entreprises, université,...)



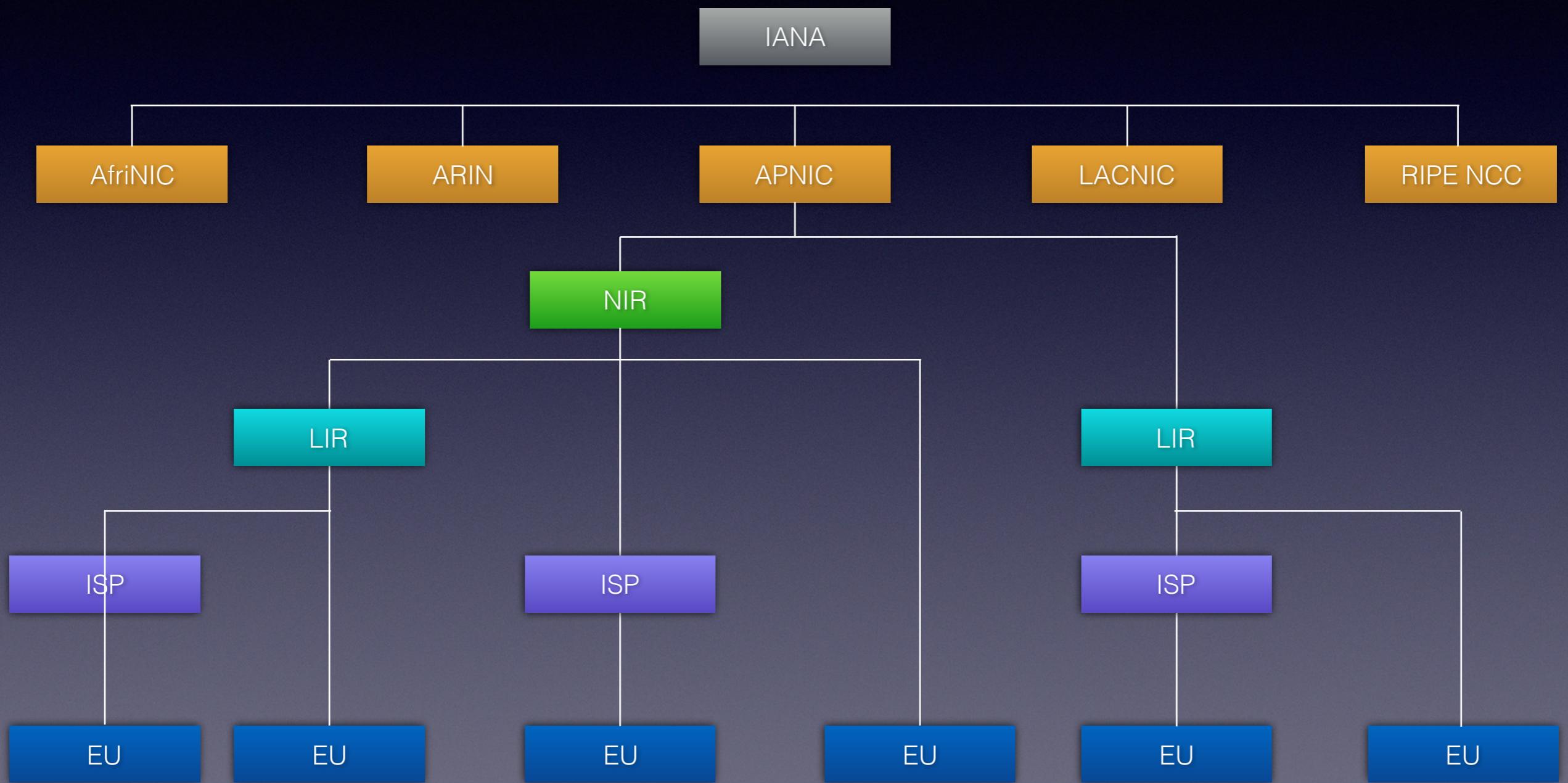
Le réseau Internet

Qui alloue les adresses ?



Le réseau Internet

Qui alloue les adresses ?



NIR : National Internet Registries

LiR : Local Internet Registries

EU : End Users

Le réseau Internet

Allocation des Adresses / Noms



Internet Corporation For
Assigned Names and Numbers



RIR
Regional Internet Registries



NIR
National Internet Registries



LIR
Local Internet Registries



End Users

Questions ?